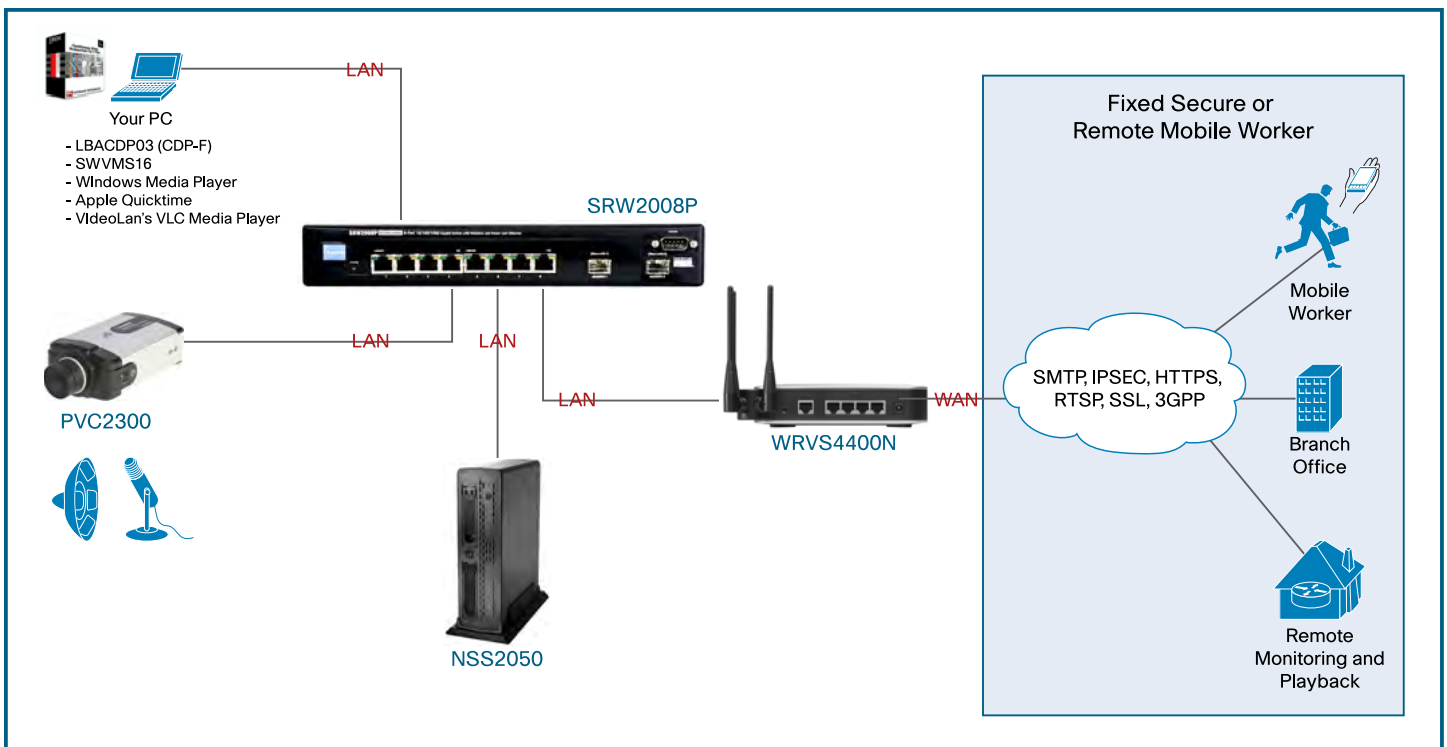




Video Surveillance Camera with Network Storage System Demonstration Kit Version 1.0



Contents

- Introduction 3**
 - Document Sections 3
 - Demo Kit Objective..... 3
- Solution Overview 3**
 - Why Video Surveillance Cameras and a Network Storage System? 4
 - Why IP Video Surveillance? 4
 - Why Network Attached Storage? 4
 - Why Continuous Data Protection? 5
- Components of the Demo Kit..... 5**
 - Demo Kit Contents 5
 - Product Information 6
- Setting up the Demo Kit..... 12**
 - Physical Installation 12
 - Cisco WRVS4400N Wireless-N Gigabit Security Router Configuration 12
 - Cisco SRW2008P 8-Port Gigabit Switch Configuration 14
 - Cisco PVC2300 Business Internet Video Camera Configuration 15
 - Cisco NSS2050 2-Bay Gigabit Storage System Configuration..... 17
 - Your PC's Configuration 19
- Performing Demonstrations 22**
 - Demonstrate Backup from a PC to the NSS2050 Share with CDP-F 22
 - Demonstrate Sending Video (with Audio) Motion Detection Data from the Surveillance Camera to the NSS via FTP..... 32
 - Demonstrate Monitoring/Playback from the SWVMS16 Utility 38
 - Demonstrate Monitoring RTSP Video (with Audio) from Any PC (Local or Remote) or 3GPP Smart Phone 45
- Appendix A: Demonstration Kit Supporting Data 49**
 - Computer Minimum Requirements for Camera Utility 49
 - Camera and Camera Monitor Utility Compatibility..... 49
 - RAID Definitions 49
 - NSS Performance Data 50
 - Estimated Bit Rates of Video Data 50
 - Estimated Storage Space Requirement for Video Data 51
 - NSS Model Differences 51
 - CDP-F Competitive Table..... 51
- Appendix B: Support 53**
- Appendix C: Release Notes..... 54**

Introduction

Welcome to the Cisco® Small Business Video Surveillance Camera and Network Storage Server Demonstration Kit 1.0. This documentation is intended to accompany the demonstration kit and provides you with everything you need to demonstrate a range of functions and features to Cisco partners selling Cisco Small Business products or to end customers considering a purchase of an IP video camera and network storage system (NSS) for their small business.

The Cisco Small Business Video Surveillance Camera and Network Storage Server Demonstration Kit can convince customers that a comprehensive Cisco solution is right for their business. This solution provides Cisco hardware and industry-standard protocols and interfaces that satisfy business requirements while maximizing the cost-saving benefits of an IP convergence network at an attractive price point and with the support and services of Cisco Small Business solutions.

Document Sections

This document starts with a brief overview that defines the solution and its capability. It then provides setup instructions designed to achieve:

- Physical interconnection of the solution
- Configuration of all components into a complete solution, which can be used for demonstration
- Operation instructions that help promote:
 - Awareness of what the solution can do and how to do it
 - Knowledge of the key functions of each component and of the solution as a whole
 - Understanding of why this solution is unique and its competitive advantage

Demo Kit Objective

This demo kit will help you easily cover topics of interest to technical decision makers (TDMs) by focusing on the solution's implementation and also cover areas that concern business decision makers (BDMs) by focusing on the benefits and operation in the workplace. This is accomplished by having a ready-built system that you can show up with, connect, power up, and begin demonstrating in minutes.

Solution Overview

The Cisco Small Business Video Surveillance Camera with Network Storage System solution can be integrated into any existing routed and switched infrastructure, since it uses industry-standard interfaces and protocols. We recommend a Cisco Small Business router and switch, which can meet the needs of a few cameras and associated traffic. For your actual deployment solution, we will determine the proper router and switch for your requirements. This can include the Cisco Unified Communications 520 for Small Business and Cisco Catalyst® Express 520 Series Switch (both components of the Cisco Smart Business Communications System).

The turnkey demo kit allows a complete end-to-end IP demonstration with reduced complexity and ease of integration.

This section describes points of interest to BDMs at the technology level, without mentioning the specific products included in the demo kit, to give you the information you need to speak to their needs.

Why Video Surveillance Cameras and a Network Storage System?

Implementing a video surveillance solution can address the following requirements of small businesses in many industries:

- Decrease theft and vandalism
- Increase employee safety
- Reduce accidents through process monitoring
- Allow local or remote monitoring by the business owner
- Increase raw storage capacity
- Meet requirements for PC data protection and disaster recovery

Why IP Video Surveillance?

Using IP video for surveillance involves transmitting video using open Internet protocols and standards for the purpose of recording and live monitoring. This should not be confused with more proprietary methods of transmitting video in which only the manufacturer of the camera can decode the video for the purpose of recording and/or display. The advantages of this technology are as follows:

- High-resolution IP cameras with proper lenses can exceed the image detail available from conventional closed-circuit TV (CCTV) cameras
- Nonlinear file storage allows improved search, retrieval, and management
- Encryption makes stored data tamper proof
- Storage, preservation, duplication, and transmission are better
- Sharing your existing IP infrastructure and cabling reduces system costs
- Complexity is reduced because the data is carried on your existing IP network, eliminating the need for a separate system
- Power over Ethernet (POE, 802.3af) offers flexibility, allowing one cable to handle both power and data.
- Camera control commands for internal configuration as well as pan, tilt, and zoom (PTZ) can be transmitted using an RS-485 interface over the same common Ethernet interconnection
- Automated alerts via email with simultaneous file transfer in response to video motion detection, dry-contact alarms, or scheduled time-of-day recording
- PC software is included to control recording and storage

Why Network Attached Storage?

A network-attached storage (NAS) system provides shared hard disk storage space on the local LAN for all client computers to share. The NAS is set up with its own network address and is accessible by all computers on that network, as well as by hosts you want to allow from any location with public IP access. A NAS system offers the following advantages:

- Reduces expense and possible overprovisioning of extra storage or backup drives for every computer in your office
- Backs up anything that can be delivered over IP

- Employs multiple disks configured as a Redundant Array of Independent Disks (RAID)¹, helping protect your data against disk failure
- Can allow for replacements and additions of hot-swappable disks
- Improves your odds of never losing critical data
- Increases the mean time between failures (MTBF) by using multiple disks
- Increases fault tolerance by storing data redundantly and in a different location
- Provides the option of storing data in Advanced Encryption Standard (AES) encrypted format

Why Continuous Data Protection?

Continuous data protection (CDP), also called continuous backup or real-time backup, refers to backup of computer data by automatically saving a copy of every change made to that data, essentially capturing every version of the data that the user saves. It allows the user or administrator to restore data to any point in time. CDP-based solutions offers the following advantages:

- Captures changes to data to a separate storage location.
- Can provide fine granularity of restorable objects such as files, mailboxes, messages, and database files and logs.
- Is a logical compliment to a NAS solution and provides a turnkey backup solution for network data backup for small businesses.

Components of the Demo Kit

This section describes the Cisco solution and the products included in this demo kit. This kit presents a turnkey solution from a single vendor using industry standards and protocols that Cisco has been implementing for decades.

Also included in this section is a description of each product. Use these descriptions to compare the Cisco solution to those available from competitors.²

Note: You will need to integrate your PC into this kit. To accomplish this, you will need to install some application software on the PC, as a customer would.

Demo Kit Contents

The demo kit is built as a turnkey system with the following components.³

Note: The software components will be installed on your own Windows laptop, which is not provided in the demo kit. This document specifies some minimum requirements for this PC. We are currently planning to deliver a DVD with the Cisco software on it to make setting up the PC easier, but this document also shows you where to find the software on Cisco.com. In addition, you will need to download some free application software, as indicated here.

¹ Definition of some common RAID configurations found in small business are given in Appendix A.

² Appendix A provides some recent performance data on the Cisco network storage systems from the well-respected Tolly Report.

³ For more information about Cisco Small Business products, visit <http://www.cisco.com/smb>.

Hardware

- Cisco NSS2050 2-Bay Gigabit Storage System
- Cisco WRVS4400N Wireless-N Gigabit Security Router with Gigabit Ethernet interfaces
- Cisco SRW2008P 8-Port Gigabit Switch with PoE
- Cisco PVC2300 Business Internet Video Camera

Software

- LBACDP03 Continuous Data Protection for Files (CDP-F): 3-user
- Cisco SWVMS16 Video Monitoring System SW 16 Camera (free with camera)
- Cisco NSS Discovery Tool for Windows (free with NSS)
- Apple QuickTime player (optional)
- VideoLAN's VLC media player (optional)
- Windows Media Player

Other

- 7 Ethernet cables
- Your PC (your own laptop computer will be part of the demonstration)

Product Information

This section provides specific information about the products listed below. It will provide TDMs with the information they need to ascertain the capabilities and features of the Cisco products, so they can compare them with competitive solutions:

- Cisco PVC2300 Business Internet Video Camera
- Cisco NSS2050 2-Bay Gigabit Storage System
- Video monitoring system software
- CDP-F software

Cisco NSS2050 2-Bay Gigabit Storage System

We have chosen the Cisco NSS2050 for the demo kit because it weighs less than the other Cisco network storage systems, the NSS4000 and NSS6000 Series, but has the same capabilities. The intelligent chassis of the Cisco NSS2050 gives administrators and integrators the flexibility to optimize the NSS for performance, capacity, and a company's storage and sharing needs. The NSS2050 includes two 250-GB hard drives and supports up to 15 concurrent, connected Common Internet File System (CIFS) (Windows, Macintosh, Linux) users. Cisco NSS products bring robust NAS within reach of today's budget-minded workgroups and small businesses. They are ideal for storing, backing up, sharing, and archiving critical information. The feature set of the Cisco NSS products sets them apart from entry-level, desktop NAS systems, while their competitive pricing gives small businesses the opportunity to realize substantial cost savings when compared with more expensive storage systems.

Unlike other NAS systems, which need to contain operating system software on one or more of the hard drives, each Cisco Small Business NSS product features a unique and intelligent chassis that contains the Linux 2.6 operating system that controls it. This gives the Cisco NSS system added stability and reliability, as well as the flexibility to be configured without connected drives and reconfigured at any time—even hot swapping and re-sorting hard drives to different storage bays. This flexible architecture makes the Cisco NSS products ideally suited for budget-conscious companies that are constantly growing and evolving.

The following list highlights some of the many selling points of the Cisco Small Business Network Storage Systems:

- Network storage system chassis supports two 3.5-inch serial ATA (SATA) disk drives, with RAID 0/1 and file encryption support
- Supports Microsoft Distributed File System and network virtualization of RAID sets across Cisco Small Business Network Storage Systems (requires at least one Cisco NSS6000/6100)
- Advanced data protection and security features: On-disk file encryption (AES), VLANs, Self-Monitoring, Analysis, and Reporting Technology (SMART) drive support, and file journaling
- Gigabit LAN interface supporting VLAN and quality of service (QoS)
- Hardware-accelerated on-disk file encryption (Data Encryption Standard [DES], Triple Data Encryption Standard [3DES], and AES256)
- Simultaneously supports Mac/PC (CIFS), Linux (NFS), and FTP clients
- HTTPS/HTTPS: Unnoticeable limit of HTTP/HTTPS connections for network management
- FTP(S) and CIFS allow some flexibility
 - Standard mode (default): 16 CIFS and 2 FTP(S) connections simultaneously
 - Alternate IP camera FTP mode: 8 CIFS and 16 FTP(S) connections
- Offers a profile configuration wizard for setting the system up for the use case needed
- Runs with only physical RAM (no virtual memory), allowing it to operate diskless and enabling unrestricted drive hot swap.
- 600-MHz CPU, 256-MB internal flash memory
- Intelligent SATA hard disk spin-up/spin-down with built-in hysteresis to avoid “flapping” on hard disk power-up and power down
- File sharing via FTP, and secure sessions are supported via secure FTP (FTPS)
- XFS file system journaling created by Silicon Graphics, originally for their IRIX operating system and later ported to the Linux kernel. XFS is particularly proficient at handling large files and at offering smooth data transfers
- Helps prevent possible file corruption by providing a common file-locking mechanism to allow simultaneous, multiprotocol access to common shares by Windows/Mac (CIFS), Unix/Linux (NFS), and FTP
- Enables the use of multiple NAS systems as a single system via Distributed File System (DFS)
- Port-based VLANs, 802.1Q/p, 802.1Q trunk groups
- Supports 802.1p QoS
- Up to 9K jumbo frame support
- Windows-like access control lists (user, group, access, and filters)
- MAC/IP address filtering
- “Just a bunch of disks” (JBOD), RAID0 (striping) or RAID1 (mirroring) configuration
- A spare hard drive can be designated as a hot spare in the event of a disk failure in the RAID set to provide maximum data protection
- HTTP/HTTPS web management
- Simple Network Management Protocol (SNMP) version 3 monitoring

- Active Directory and NTV4 domain support
- Microsoft Vista support
- Dynamic Host Configuration Protocol (DHCP) client
- Integrated cable diagnostics
- 60W, 12V external AC power
- Low power consumption—16W with no drives, 38W with two 250-GB drives
- System reset/factory network reset button available on unit
- Calculated 300,000+ hours MTBF
- 3-year warranty

Continuous Data Protection for Files

Continuous Data Protection for Files (CDP-F) can be bundled with any NSS product and addresses a business's need to protect valuable data. CDP-F offers continuous data protection, as opposed to the traditional checkpoint-style scheduled backup, and has no direct feature-to-feature competitors. Bundling the Cisco NSS2050 and CDP-F can provide a simple, low-cost entry-level solution that provides enterprise-class backup and recovery, along with the IBM partner name and reputation. Advantages or chief selling points include:

- Option for both continuous protection and scheduled backups
- Local on-machine cache offers fastest and most available restore
- Tolerance of network instability; backups never fail
- Widest target device support
- Ease of deployment and administration
- Range of use cases, from single user to massive enterprise
- Extremely efficient client email backup
- Separates our NSS solution from the competition
- End user can install CDP-F, or it can be deployed via scripting
- Protects data continuously rather than on a scheduled basis, which leaves data protection gaps
- Allows individual, interactive configuration for single users as well as a mass configuration option
- Runs continuously as data is saved, providing true background protection and the ability to back up to any point in time
- Configuration wizard guides you to configure the protection that meets your needs, allowing you to initiate protection quickly and easily
- Restore wizard helps you pick the version of the file you want and allows you to choose where to restore it
- Enables a small business to have enterprise PC backup capabilities at a small business price

The following are the software and hardware requirements for the demo kit 1.0 CDP-F client software:

Hardware

Minimum hardware for the CDP-F client is an Intel Pentium III machine with the following specifications:

- 500 MHz CPU
- 384 MB RAM
- Free disk space:
 - 21 MB for install footprint
 - Additional space to store local backup copies

Note: You must configure as much space as is needed to store at least one backup copy of every file that you protect. The hardware configuration must also support the Microsoft Windows operating system.

Software

The CDP-F client supports the following versions of Windows:

- 32-bit Windows 2000 Server, Advanced Server, SP2 and up (x86-32)
- 32-bit Windows XP Professional, SP1 and up (x86-32)
- 32-bit Windows 2003 Server, Standard Edition and Enterprise Edition (x86-32).
- 32-bit Windows Vista Ultimate and Business Edition (x86-32)

Browser

The CDP-F user interface supports the following browsers:

- Internet Explorer, version 6.0 and later
- Mozilla Firefox, version 1.5.0.7 and later

Cisco PVC2300 Business Internet Video Camera

Cisco Small Business Video Surveillance Cameras provide customizable ways for small business owners to monitor and protect their companies. These high-quality solutions can be optimized for many different applications and sites. Each camera can be quickly mounted using the bracket included in the package. The cameras' compact form factor also enables them to be put inside a protective enclosure for interior or exterior installations. The cameras use removable CS-mount or C-mount lenses and can be customized with optional zoom, wide-angle, vari-focal, auto-iris, or other types of lenses as required for a specific application or setting.

The Cisco PVC2300 Business Internet Video Camera is a PoE device, so it can be powered from three sources: the supplied DC power pack or a PoE switch or power injector via Ethernet cabling. The later two options enable installation near ceilings, on rooftops, or anywhere that power outlets may not be available. The Cisco PVC2300 camera can be mounted on any pan-tilt (PT) base that supports the Pelco D protocol and can be remotely rotated and controlled through an RS-485 interface. It also has two input and two output ports, which can be used to connect the camera to an alarm panel, siren, passive infrared (PIR) sensor, smoke detector, lighting switch (on/off), door sensor, or other devices.

The Cisco PVC2300 uses a high-quality progressive-scan charge-coupled device (CCD) sensor, delivering good-quality video. The CCD sensor also has low-light sensitivity, so video can be captured even in environments with very little light or during near-dark times of day. Additionally, the camera incorporates an infrared (IR) cut filter that, when used with a separate IR lamp, allows for video capture in total darkness.

The Cisco PVC2300 camera supports dual codecs (MPEG-4 and MJPEG), which can be used simultaneously. MPEG-4 gives efficient bandwidth consumption with good-quality compression and is optimal for real-time viewing of video. MJPEG gives optimal video quality with lossy compression, making it ideal for large-volume storage to a NAS device.

The Cisco PVC2300's audio capabilities include two-way audio, embedded microphone, external speaker and microphone ports, and voice compression. With extensive feature support, such as IP multicast, Real-Time Streaming Protocol (RTSP), Real Time Protocol (RTP), and 3rd Generation Partnership Project (3GPP), it allows video to be viewed from multiple endpoints and client applications, such as 3G phones and QuickTime clients on PCs or Wi-Fi phones. Support for multiple network protocols, such as 802.1p priority, 802.1Q VLANs, and Dynamic DNS (DDNS), make the solution ideal for multiple IP surveillance applications. The camera can also be managed securely using HTTPS. Other features of the camera include:

- 10/100 Ethernet LAN port supporting PoE
- 2-way audio capability via G.726 or G.711 codec
- LED status front and rear (can be disabled manually)
- Pan/tilt capable (mount required)
- Motion detection and manual recording
- Event-triggered recording (I/O)
- Digital magnification
- VGA resolution (640 x 480, 320 x 240, 160 x 120) @ 30 frames per second (fps)
- Image quality: very high to very low, selectable
- Bit rate: constant bit rate 64 kbps to 1.2 Mbps
- Frame rate: 1 to 30 fps
- Simultaneous MJPEG/MPEG-4 codec support
- Night vision with IR cut filter
- Interchangeable CS lenses
- 1/4-in. CCD image sensor
- PoE
- General-purpose I/O (GPIO) ports allow for flexible installation and control of external devices and sensors
- High-quality Sony CCD sensor with low light sensitivity provides optimal video image under a wide variety of lighting conditions; low light sensitivity (0.74 lux vs. 1.0 for 210A)
- IP multicast, IPv6, 3GPP and Samba client provide advanced feature set
- HTTP/HTTPS web GUI management

- MPEG video capability for motion detection:
 - Detects events up to 5 seconds before and 5 seconds after event
 - File in Advanced Streaming Format (ASF), MPEG-4, or 3GPP format
 - File stored on flash in camera
 - Can be saved to NAS via FTP
 - Can be sent via email via Simple Mail Transfer Protocol (SMTP)
- JPEG image:
 - Saved at 1 to 10 images per second
 - File in MJPEG format
 - Detects events up to 5 seconds before and 5 seconds after event
 - Can be saved to NAS via FTP

Cisco SWVMS16 Video Monitoring System

The Cisco SWVMS16 Video Monitoring System offers centralized management and monitoring of up to 16 Cisco cameras, allowing you to watch feeds in continuous playback mode or to opt for scheduled monitoring. Additionally, the software offers programmable manual or event-triggered recording, combined with adjustability for brightness, contrast, and gray scale for concise image capture. The camera's real-time video enhancement is also controlled with digital zoom and variable playback speeds (both forward and backward).

Additional features of the SWVMS16 Video Monitoring System include:

- Monitor console:
 - Multilevel user accounts
 - Up to 16 cameras on one screen
 - Nine viewing formats: 1, 4, 5+1, 9, 12+1, 16+1, 8+2, 12+1, 16
 - Supports MPEG-4 and MJPEG video compression formats
 - Rotating camera image (when viewing in a single window)
 - PTZ camera ready (controls)
 - Report listing free storage space
 - Save/load configuration allows for multiple camera sets to be viewed on the same PC
 - Recording can be scheduled by dragging the bar across different time periods
 - Schedules/settings can be copied to other cameras
 - Link to play back recorded files from console screen
 - Motion detection can be defined using 10 windows
 - Motion detection of up to 30 seconds before and 30 seconds after motion
 - Recording of up to 30 fps
 - 2-way audio support
- Playback console:
 - Full-screen display
 - Each camera's recording can be searched by date and time
 - Each view can be digitally enhanced in real time during playback
 - Log file

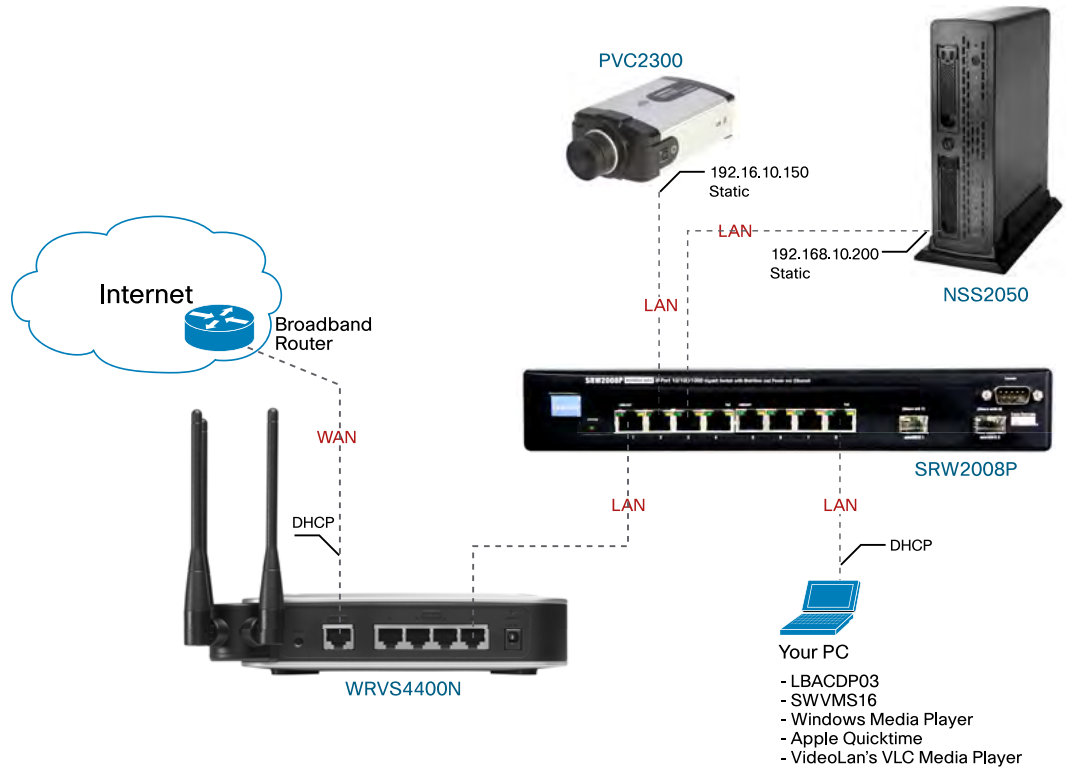
- Forward and backward speeds variable at 1x, 2x, 4x, 8x, and 16x
- 4x digital zoom on playback
- Export video to standard AVI format or make snapshots of captures

Setting up the Demo Kit

Physical Installation

To begin setting up the demo kit, interconnect all devices with Category 5 (CAT5) Ethernet cables as shown in Figure 1. You can power up all the devices at this time as well. The WAN connection of the WRVS4400N must be a public routable IP address (DHCP or static) if it will be used for public access. Once everything comes up and is running, you can plug your PC into the switch port and begin configuring the software.

Figure 1. Connecting the Demo Kit Hardware



Cisco WRVS4400N Wireless-N Gigabit Security Router Configuration

The demo kit comes with a Cisco WRVS4400N, one of the fastest routers (800 Mbps per interface) with copper Gigabit Ethernet interfaces and IP Security (IPsec) VPN capability (the Cisco RVS4000 is the wired cousin to this router and will support this demo as well).

WAN Assignment

The default configuration for the Internet connection type of the WRVS4400N's WAN interface is DHCP, and this is fine for placing the router behind a broadband router (with DSL, DOCSIS[®] cable modem, MetroE, etc.). The connection can be to a corporate network only if the remote PC will be demonstrated on that same network (otherwise, corporate firewall rules will block this). A public WAN Internet connection works from any remote station. If the environment you will be demonstrating in requires that you assign a static IP address to the router, adjust that configuration and specify an IP address, subnet mask, default gateway, and DNS. The router will come ready to be connected for DHCP.

The default IP stack is IPv4, which is fine unless you are in an IPv6 environment, in which case you will need to adjust this setting on the setup GUI.

The default behavior is Gateway mode, which is what you want for the demo kit configuration.

Note: WAN connectivity is required if you want to demonstrate remote capability over the WAN (configuration, video monitoring, and remote FTP server access to the NSS). A DHCP address is fine for demonstration purposes, but in a production environment you would be more likely to use a DDNS service with a DHCP address or just use a static IP address.

LAN DHCP Server

The WRVS4400N supports multiple VLANs, but the demo kit uses one VLAN (default VLAN 1) for the camera, NSS, and monitor/client PC traffic. This is assigned as either an access port or a general port in the L2 Switch section of the configuration GUI, allowing untagged traffic. So you will have one local subnet: 192.168.10.0/24.

Navigate to the SETUP:LAN GUI page. Find the default gateway ip address for the computer/laptop you are using. This can be found by using the ipconfig command at command prompt. Once you get that ip address, goto <http://<ip address>> and enter the GUI with username/password of admin/admin.

Set the local address to 192.168.10.1. This will become the LAN client's default gateway. This address was chosen because it is the default data VLAN for the Cisco Smart Business Communications System (SBCS) IP-PBX solution, in case you want to attach the camera and NSS to it.

Set the IP address pool to start with 192.168.10.100 and allow 10 leases (more than enough for the demo kit, but this would obviously be set larger for a small business implementation, since you would give IP address to all clients from the router).

You can either leave the lease time set to 0 (1 day) or adjust it. You will not be using MAC address filtering or port restrictions for the demonstration, but you could use them with this router.

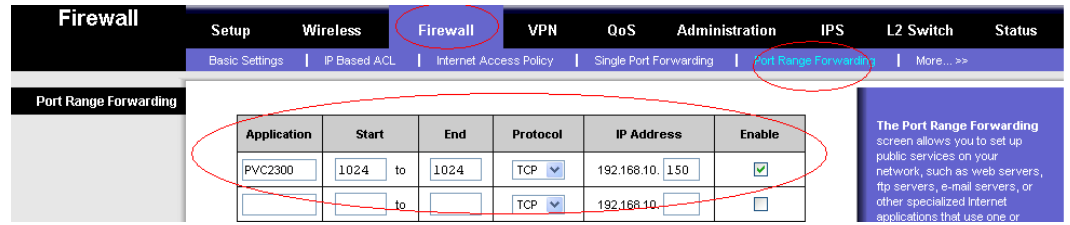
Port Forwarding Rules

For remote HTTP access to the camera, we have built a port to forward WAN originated requests to the static IP addresses assigned to the PVC2300:

```
Port 1024 -> 192.168.10.150 (the camera)
```

This is accomplished with settings on the camera and the router. Figure 2 illustrates this configuration.

Figure 2. Configuring Port Forwarding Rules

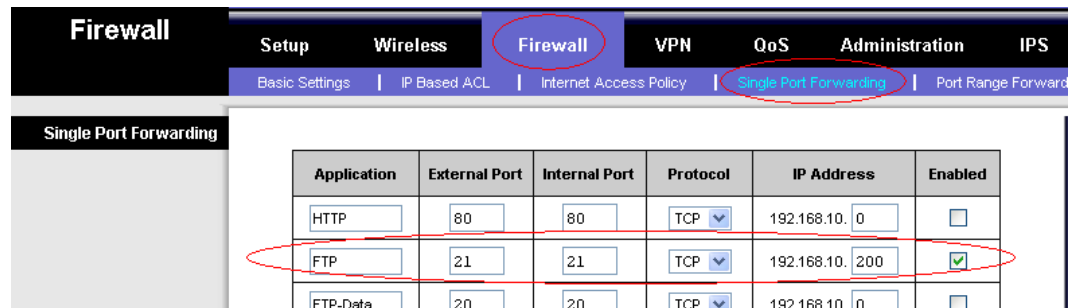


For remote access to the camera RTSP, we use the default port 554 configured on the camera. Just enable the forwarding on the router:

RTSP-PVC230	554	554	TCP	192.168.10.	150
-------------	-----	-----	-----	-------------	-----

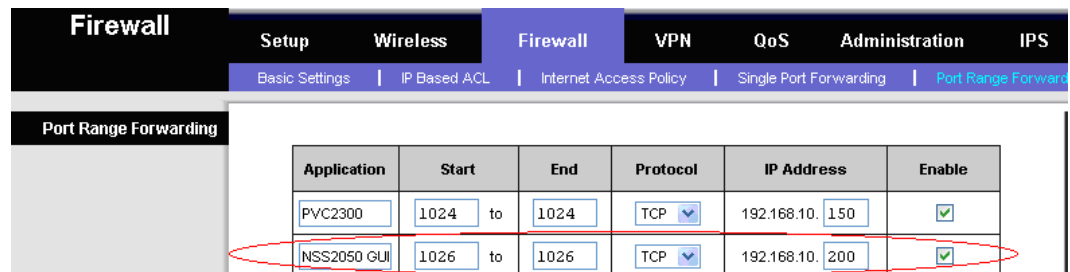
For remote access to the FTP server (the NSS2050 provides this capability), we set a port forwarding rule in the router, as shown in Figure 3.

Figure 3. Configuring Access to the FTP Server



For remote access to the NSS2050 web GUI, we enable a unique TCP port 1026 in the NSS configuration. This is shown later in the section on the NSS2050's configuration. In the router, we add the rule shown in Figure 4.

Figure 4. Configuring Remote Access to the NSS2050 GUI



Cisco SRW2008P 8-Port Gigabit Switch Configuration

The demo kit comes with the Cisco SRW2008P, which provides eight copper Gigabit Ethernet ports of LAN connectivity and has web GUI management.

You will be running the switch as is, with all control of devices handled by the router, so no configuration is necessary.

Cisco PVC2300 Business Internet Video Camera Configuration

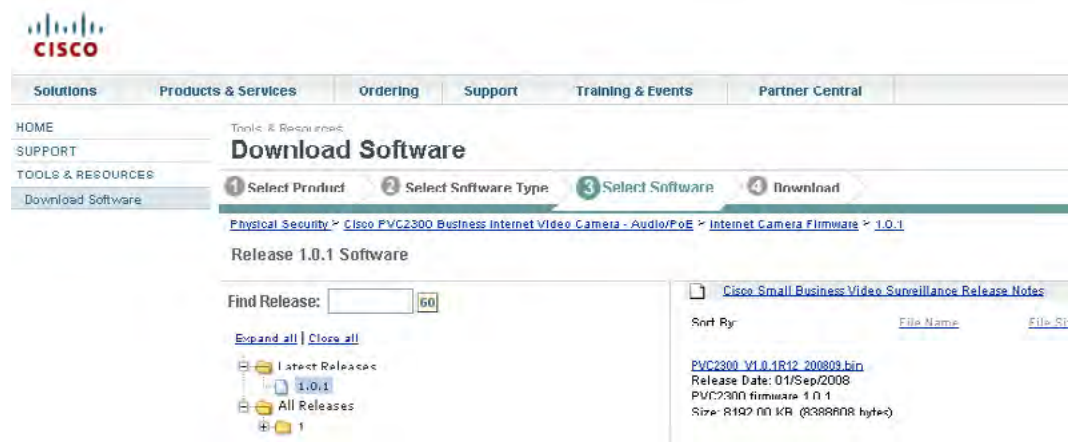
Firmware

The camera must be running the latest firmware, version 1.0.1, in order to interoperate with the new camera utility, which you will install on your PC and use later. Navigate to <http://www.cisco.com/smb> and then to “Video Surveillance” and “SW Download” to find version 1.0.1 of the firmware for this camera (see Figure 5).

Download the firmware to your PC and upgrade your camera using Camera GUI Administration -> Firmware drawer.

You don’t need to do this if the camera already has firmware version 1.0.1 installed (to check, go to Camera GUI Administration -> Firmware drawer).

Figure 5. Downloading the Latest Version of the Firmware

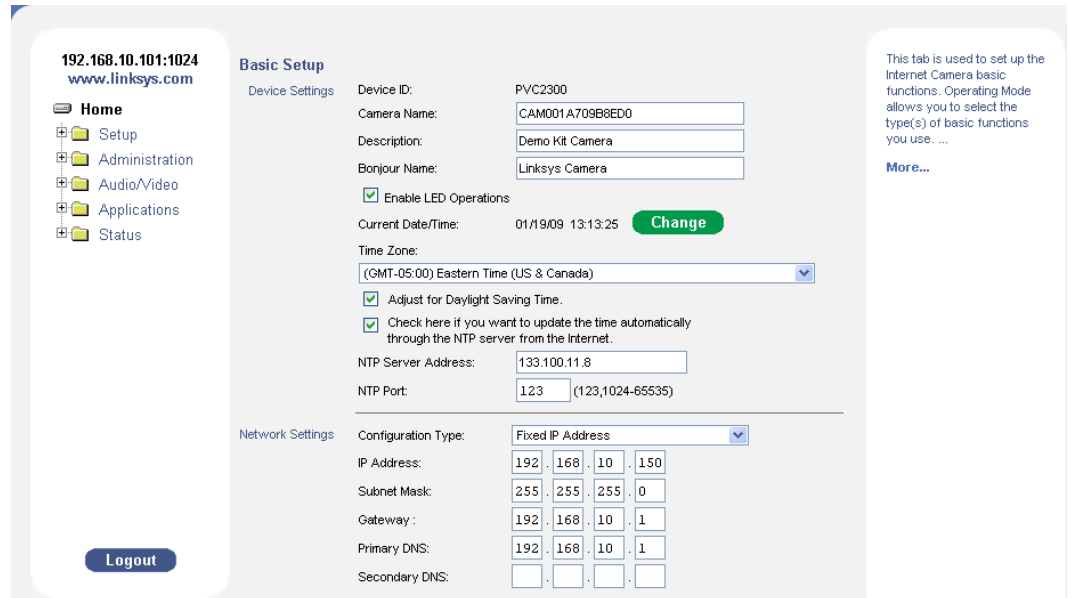


IP Address

The factory default for the camera is to use DHCP to get an address from the router. Since this would not result in a dependable IP address, we have assigned a static IP address within the LAN subnet of the router but outside the IP address pool set aside for DHCP. In our case, we have assigned the camera an IP address of 192.168.10.150/24 with a default gateway of 192.168.10.1.

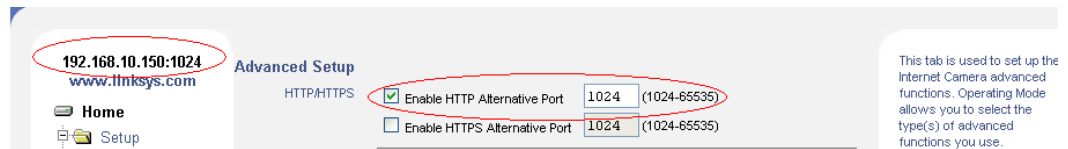
In the event that the camera you have is not configured already, the easiest way to accomplish this is to let the camera get the DHCP address; you then have to change only one field (the IP address). Also adjust the time zone so that the camera date and time are correct (Figure 6).

Figure 6. Setting the Camera's IP Address



We assigned an alternate HTTP address for the camera so it can be accessed through the router from remote locations (Figure 7). In real implementations, you can use HTTPS just as easily.

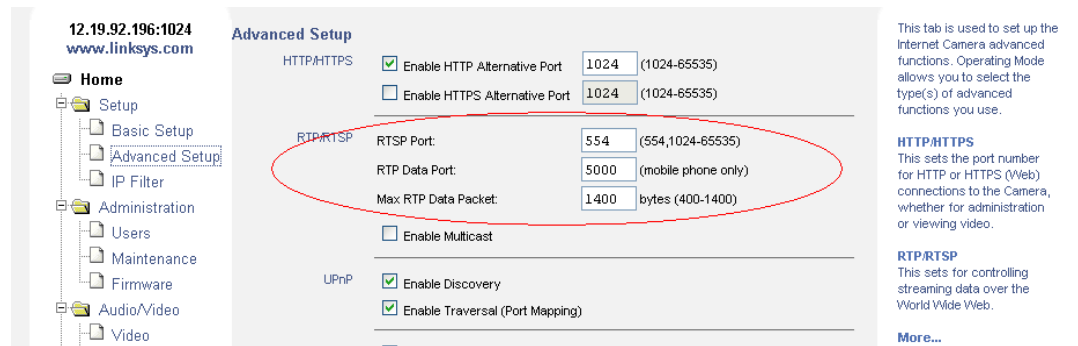
Figure 7. Alternate HTTP Address for the Camera



Note: This configuration will require even local web GUI access to use the TCP port. So use 192.168.10.150:1024 locally to access the camera GUI. Use <the router WAN IP>:1024 to access the camera remotely.

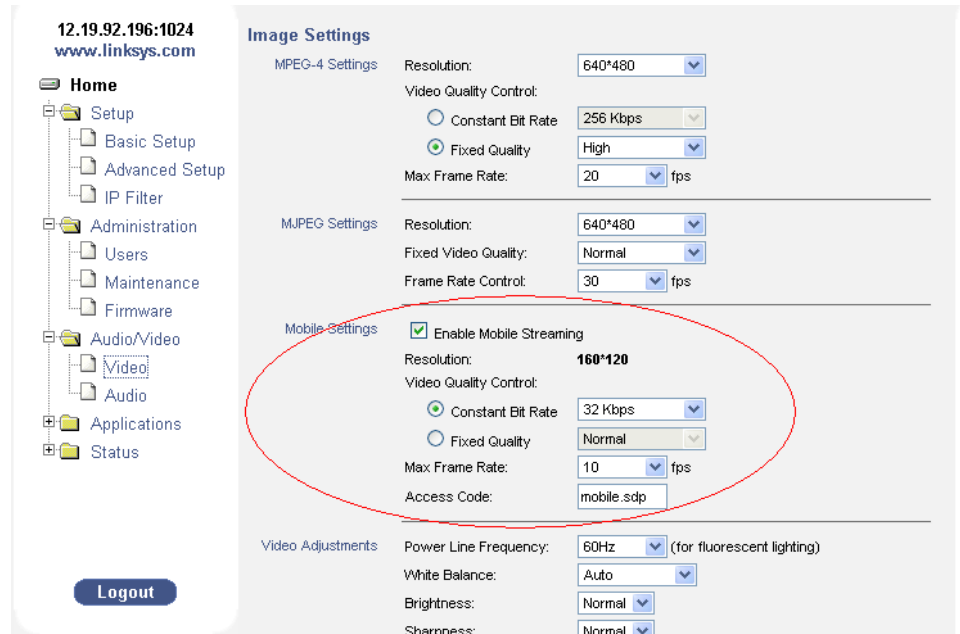
We use the default RTSP port 554 and RTP media dynamic ports 5000–5020 (Figure 8).

Figure 8. RTP/RTSP Port Configuration



We have enabled mobile streaming so RTSP can be used to access the camera from the Apple QuickTime viewer, the VLC player, or a mobile 3GPP phone (Figure 9).

Figure 9. Mobile Settings for the Camera



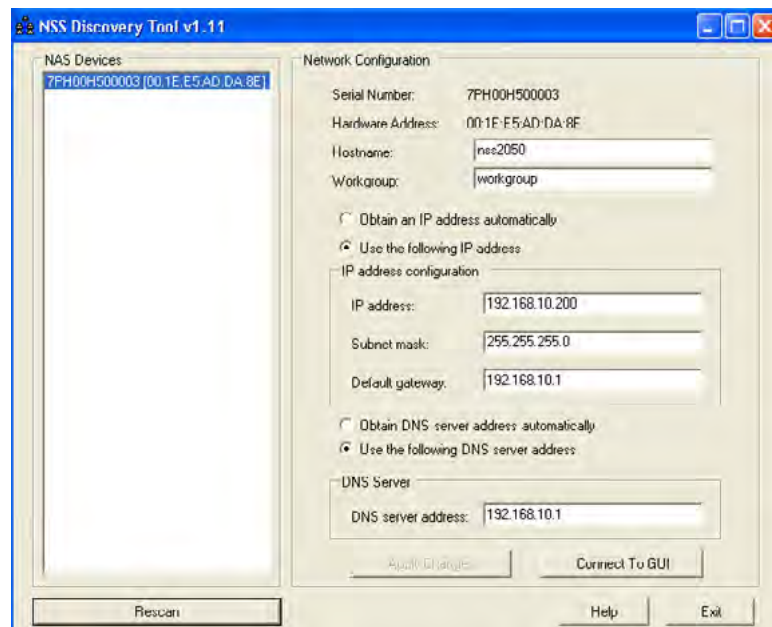
Cisco NSS2050 2-Bay Gigabit Storage System Configuration

Having a static Network Address Translation (NAT) IP address on the NSS allows it to be accessed reliably in two ways:

- As a local share on the network accessible via CIFS, NFS, FTP or HTTP/HTTPS
- As an FTP server for remote clients

The IP address for the NSS is 192.168.10.200. This is outside the DHCP scope but within the LAN subnet. The NSS Discovery Tool makes this assigning this address easy and also allows you to launch the web GUI (Figure 10).

Figure 10. NSS Discovery Tool



The Initial Setup wizard can be used to create a RAID1 array (two 250-GB disks that are mirrored, hence having half the capacity of the two disks if run as RAID0 [striped] with slightly lower performance).⁴ Figure 11 shows how to access the wizard at any time from the NSS web GUI. You can also perform this setup manually using the other GUI drawers at the left.

Figure 11. Accessing the Initial Setup Wizard

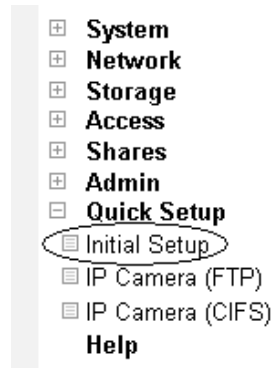


Figure 12 shows the sequence to follow to configure the demo kit, regardless of whether you use the wizard or do it manually from the web GUI.

Figure 12. Steps for Configuring File Sharing on the NSS

Welcome to the NSS Setup wizard. Follow the steps listed next to set up your NSS for basic filesharing

1. Create a RAID Array
2. Create a Volume
3. Create a Share
4. Create Users
5. Grant Share Access

The volumes created on the RAIDA are listed in Table 1.

Table 1. Volumes Created on the RAIDA and Their Capacity

Volume	Amount of RAIDA
Surveillance	100 GB
CDPF	100 GB
Maintenance	10 GB

The three users created on the NSS2050 and their passwords are:

- cisco/cisco, member of group nasusers with home directory in maintenance
- camera1/cisco, member of group nasusers with home directory in maintenance
- readonly/cisco, member of group nasusers with home directory in maintenance

⁴ See Appendix A for an explanation of RAID0 and RAID1.

The shares created on the volumes are shown in Table 2.

Table 2. Shares Created on the RAID A Volumes

Share	Volume	User Access	Protocol
Anonymousftp	Surveillance	R/W by all users	FTP, CIFS
Pvc2300	Surveillance	<ul style="list-style-type: none"> • RO by readonly • R/W by cisco and camera1 	FTP, CIFS
Backup	CDPF	<ul style="list-style-type: none"> • RO by readonly • R/W by cisco 	CIFS
Configuration	Maintenance	<ul style="list-style-type: none"> • RO by readonly and camera1 • R/W by cisco 	CIFS, FTP

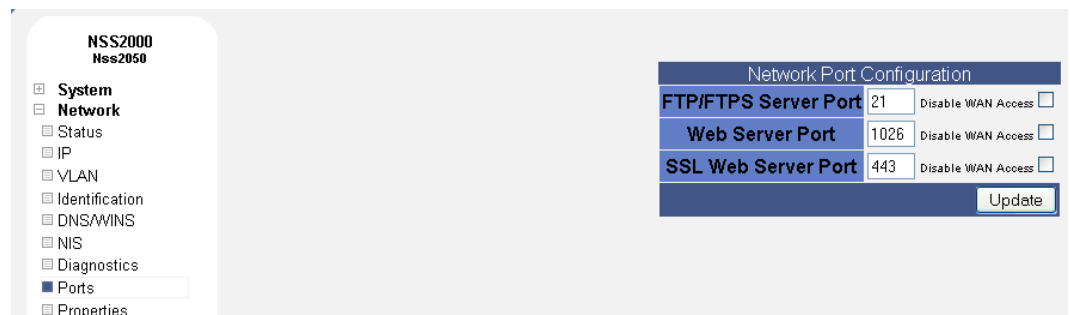
We also enabled FTP on the NSS so that it can be accessed by FTP clients.

WAN Access

THE NSS is set up as an FTP server for the small business, using the configuration previously shown in the router section.

The NSS2050 supports SMTP email alerts as well as full-blown SNMP traps. As a result, it is very manageable without having to be accessed manually from a remote monitoring office. But you can also allow remote access into the GUI and into the FTP server from remote stations on the WAN. This involves modifying the web server port and not disabling WAN access, as shown in Figure 13.

Figure 13. Allowing Remote Access to the NSS2050's GUI and FTP Server



Your PC's Configuration

CDP-F

The demo kit comes with a CD containing the license SKU for three CDP-F clients.

You will install this software on your PC in advance of the demonstration, unless you want to demonstrate installing and configuring CDP-F on the client PC. It doesn't take long. It installs into C:\Program Files\Cisco\CDP_for_Files

Follow these steps to interactively install CDP-F on a single computer.

1. Double-click on the Continuous Data Protection for Files installer icon. The installer displays the language selection dialog. The default is English.
2. Choose your preferred language and click OK. The Continuous Data Protection for Files information window will display with the build number.
3. Click Next. The License Agreement window will display.

4. Read the License Agreement, then select the radio button if you accept the terms of the agreement. Click Next. The Destination Folder window will display.
5. Accept the default install location, or click Change to specify another location. The default install location is recommended. Click Next. The Ready to Install the Program window will display.
6. Confirm that the information is correct and click Next.

The installation window will display a progress bar indicating that the necessary files are being installed on your computer. You will also see a command prompt window open as the installer runs several scripts.

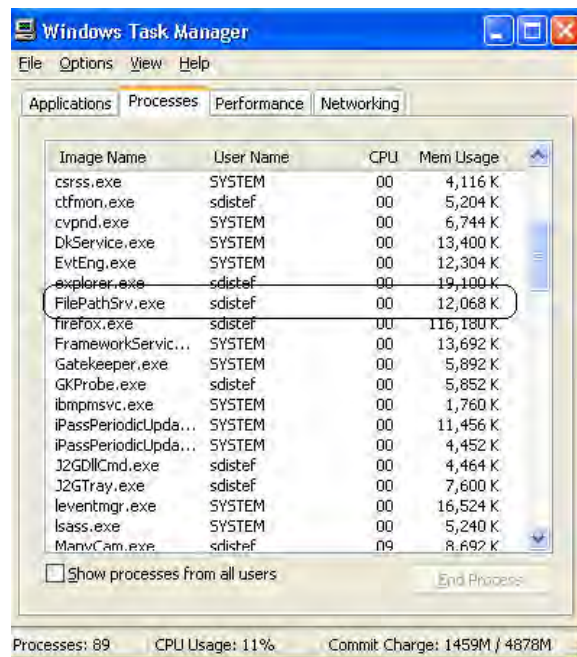
The Installation Complete window will display.

7. If you are installing the client on Windows Vista, and there is an existing Continuous Data Protection for Files client, you will see the Files in Use window. Click OK. You will also see a warning that the setup was unable to automatically close all requested applications. Click OK.
8. If this is your first installation of Continuous Data Protection for Files on this computer, a configuration wizard will help you choose your protection settings. Don't use this wizard, since the setup will be part of the demonstration.
9. Click Finish. The installer will indicate that you must reboot in the following situations:
 - You are reinstalling or upgrading Continuous Data Protection for Files.
 - A product that uses the Tivoli Storage Manager API is installed and running.

When CDP-F starts, it will launch a setup wizard via an HTTP GUI, using your PC's loop-back address and port 9003.

Confirm that it is running by opening Windows Task Manager (Ctrl-Alt-Del) and looking for this service (Figure 14).

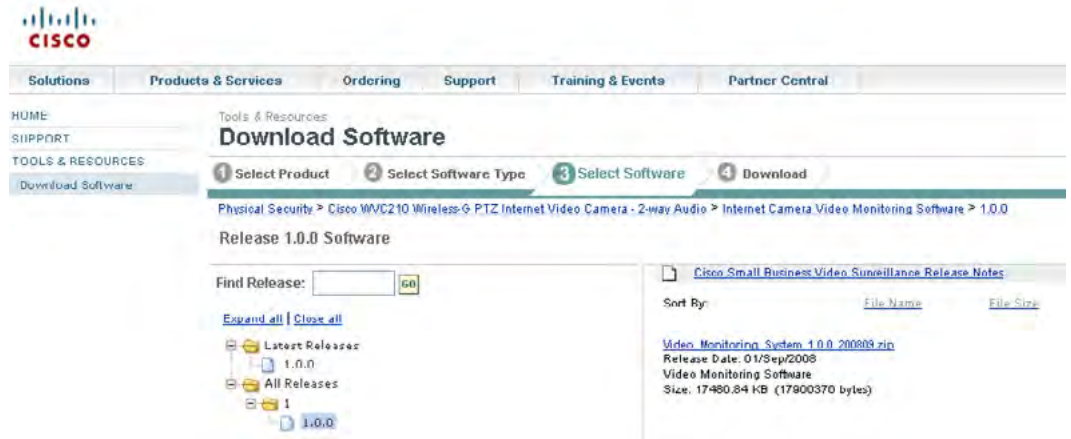
Figure 14. Confirming That the Setup Wizard Is Running



Cisco SWVMS16 Video Monitoring System SW 16 Camera

Install the Cisco SWVMS16 Video Monitoring System SW 16 Camera utility on your PC after downloading it from the demo kit CD or Cisco.com (the same place where you downloaded the firmware for the PVC2300 camera; see Figure 15). Because the PVC2300 works with both the old and new utilities, the new one is reflected on the new cameras at this time.

Figure 15. Downloading the SWVMS16 Video Monitoring System SW 16 Camera Utility



VideoLAN VLC Player

Download the VLC media player to your PC and install it (Figure 16).

Figure 16. Downloading the VLC Media Player



Performing Demonstrations

You have now accomplished the physical setup and configuration of the demo, including installing the software on your PC.

Some very basic capabilities have already been demonstrated implicitly during the interconnection and setup, but they are reiterated here:

- You can use the NSS Discovery Tool to find the NSS on your network and do some initial configuration.
- The PoE switch provides power to the Cisco PVC2300.
- The local LAN interconnection between all the elements occurs on the 192.168.10.0/24 network we created.
- The web GUI provides access to all devices (admin/cisco).
- Public WAN Internet occurs via the WRVS4400N (if you connected the WAN to a broadband router).

You will now demonstrate the capabilities of this system in a way that highlights features you can easily show. Some of these demonstrations may involve making minor edits to configurations, and part of the demonstration includes showing the user-friendly GUI interface of the products.

Demonstrate Backup from a PC to the NSS2050 Share with CDP-F

Demonstrate the use of one of the NSS2050 file shares (backup) for your PC files, using the CDP-F software you installed on your PC in the previous section. Show how to back up the files and view them on the NSS from the PC, using the Microsoft “workgroup” (default) of the NSS (the NSS can also integrate with a full-blown domain controller, but for demonstration purposes, this is easier.) Open a Microsoft Word document with any content, save it into the file folder you will be backing up, and leave it open, making periodic edits during the demonstration.

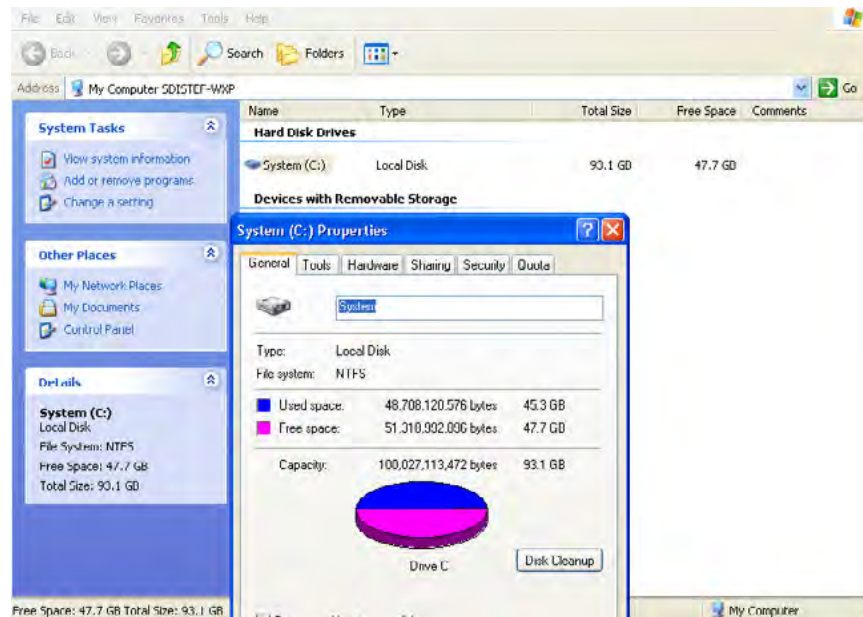
The CDP-F Client

Launch CDP-F from your PC (Start -> Programs -> Cisco CDP-F), and notice that it opens a web browser to expose the HTTP GUI interface to port 9003 of your PC’s loop-back address. Click on the Setup drawer to quickly configure the following:

General

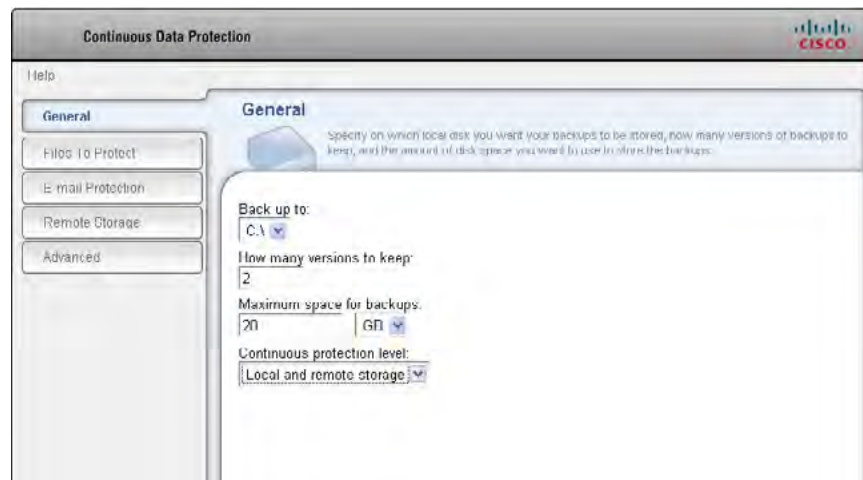
If you want to enable local backups, specify the local disk on which you want your backups stored, the number of versions of backups to keep, and the amount of disk space you want to use to store the backups (remember that CDP-F will keep both local and remote copies). Mail files are usually very large, so keeping a local copy will consume a lot of disk space on the PC. Check your PC’s free disk space before doing this (Figure 17).

Figure 17. Determining the Amount of Free Disk Space on the PC



In Figure 17, there is enough disk space to support two versions of each mail folder in MS Outlook, so the maximum space is set to 20 GB, with two versions of each file to be backed up locally (onto the C: drive) and remotely (NSS) (Figure 18).

Figure 18. Setting the Backup Parameters for CDP-F



The settings shown in Figure 18 will result in the C:\Backup folder being created on your PC. The remaining file structure under this folder will mimic the file and folder structure of the backup source.

Files to Protect

The “explicitly specified folders” and/or “well-known application extension” recognition can be used to define the data that are continuously protected. The second one is nice to demonstrate, since it will find files regardless of where they are stored.

Click Details and specify a folder. (For the demonstration, pick the folder that contains an open Word document) (Figures 19 and 20). Select an application as well. Unless you have a lot of time to spend, don't pick Adobe Acrobat or Microsoft Word or PowerPoint, since those files are everywhere and will likely take more than 30 minutes to find and back up.

You don't need to specify vault files for this demonstration, but do check the "Start an initial backup" checkbox.

Figure 19. Specifying Folders and Applications to Protect

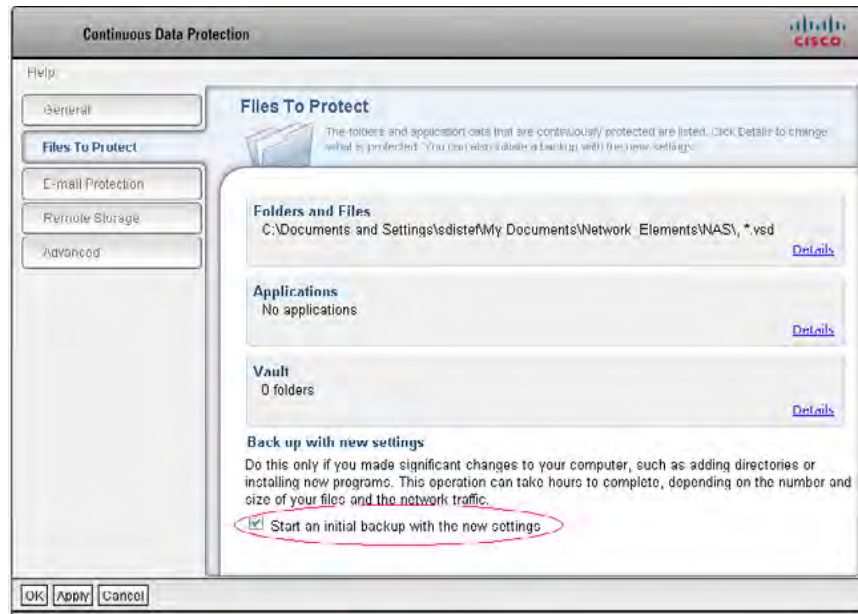
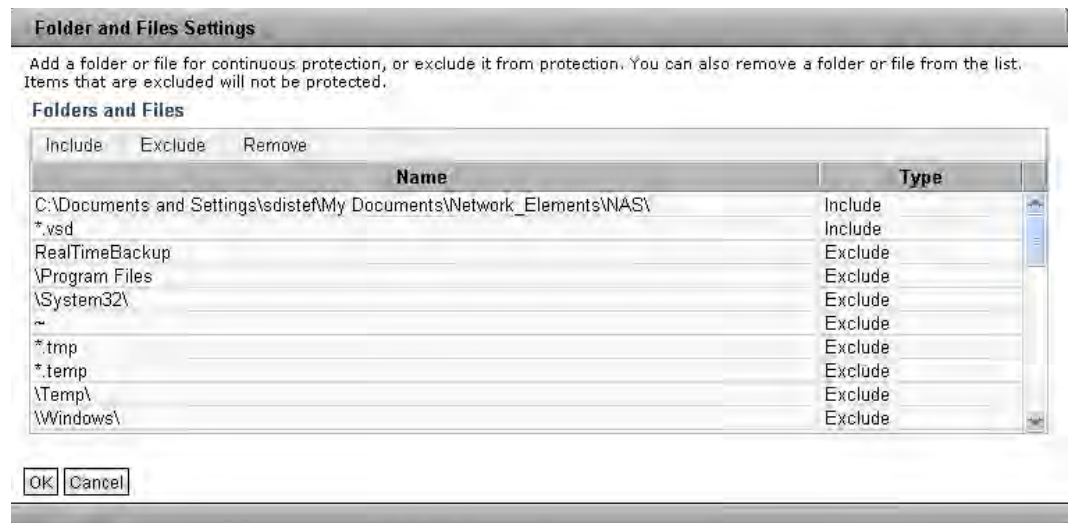


Figure 20. The Details for Folders and Files



Email Protection

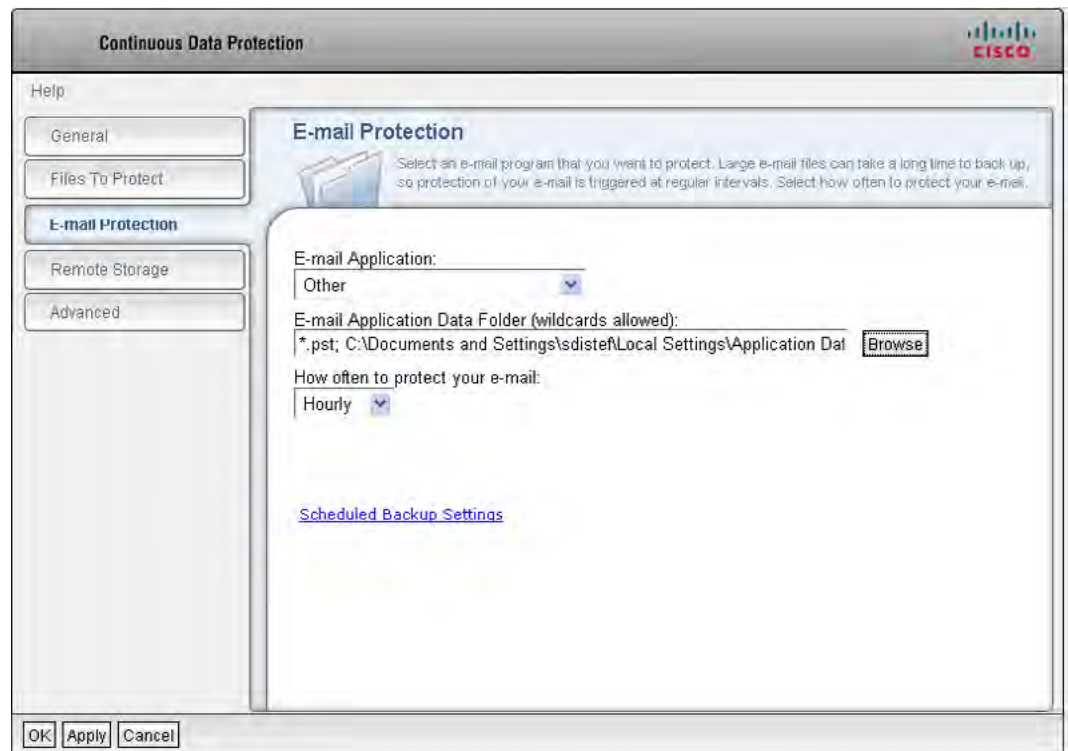
You can include email protection if you have some time, since these files are very large and take a while to back up.

For demonstration purposes, select “Other” as the email application. This will save some time and allows you to pick the folder on your PC containing the mail files. For Microsoft Outlook, you would select the following folder:

C: ->Documents and Settings -> <user id> -> Local Settings -> Application Data -> Microsoft -> Outlook (Figure 21).

You can select one of the other options, but it will find e-mail files for all user profiles that use that machine. For example, if you are using Outlook Express you can select Outlook Express from the drop-down menu rather than the options shown in Figure 21.

Figure 21. Specifying Email Protection

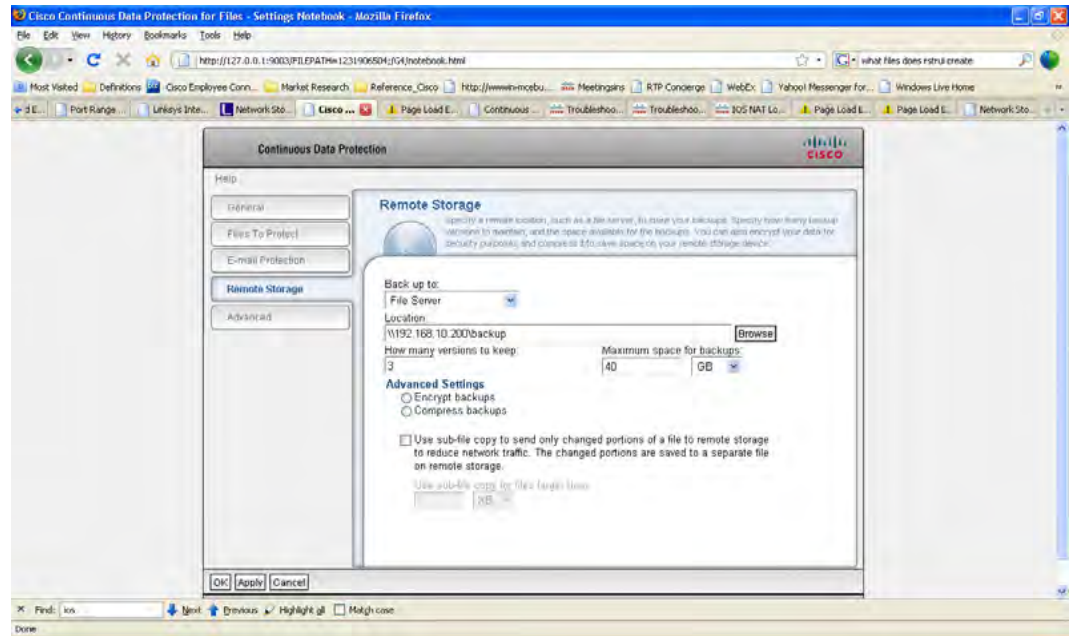


Remote Storage

Specify the NSS2050 as the remote location to store your backups. Specify how many backup versions to maintain and the space available for the backups (for each PC, allow for that much disk space on the NSS). You can also optionally encrypt your data for security purposes and compress it to save space on the NSS.

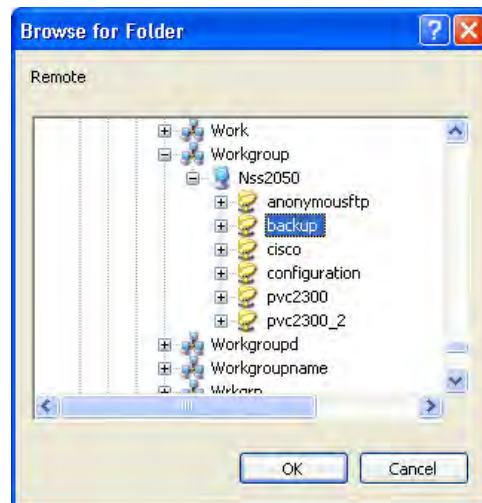
You can enter the absolute IP address for the location. With a Cisco laptop, however, the absolute IP address and share folder work best, as shown in Figure 22, since the PC won't show workgroups unless you are connected to the corporate network, which won't be the case for most demonstrations.

Figure 22. Entering Remote Storage Settings



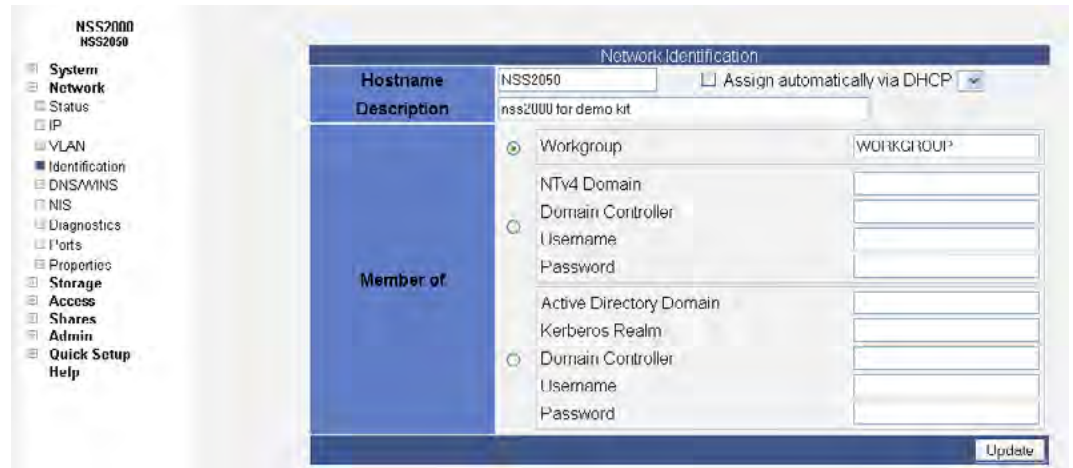
If your PC is not configured for operation in corporate workgroups, you can click Browse on this screen to select the share. In that case, your computer is on the LAN and has an address of 192.168.10.10X, and the NSS will be found in the Windows XP operation system under My Network Places -> Entire Network -> Microsoft Windows Network -> Workgroup -> <host name of NSS2050> Other operation systems may differ slightly or you may need to map a drive. (Figure 23). Use the username and password created on the NSS for read/write access (cisco/cisco).

Figure 23. Browsing for the NSS2050 Location



Note: The NSS is configured with a default affiliation to "Workgroup" and a host name you define in the screen shown in Figure 24. Goto <http://192.168.10.200:1026/> with username/password of (admin/admin) to verify settings on the NSS.

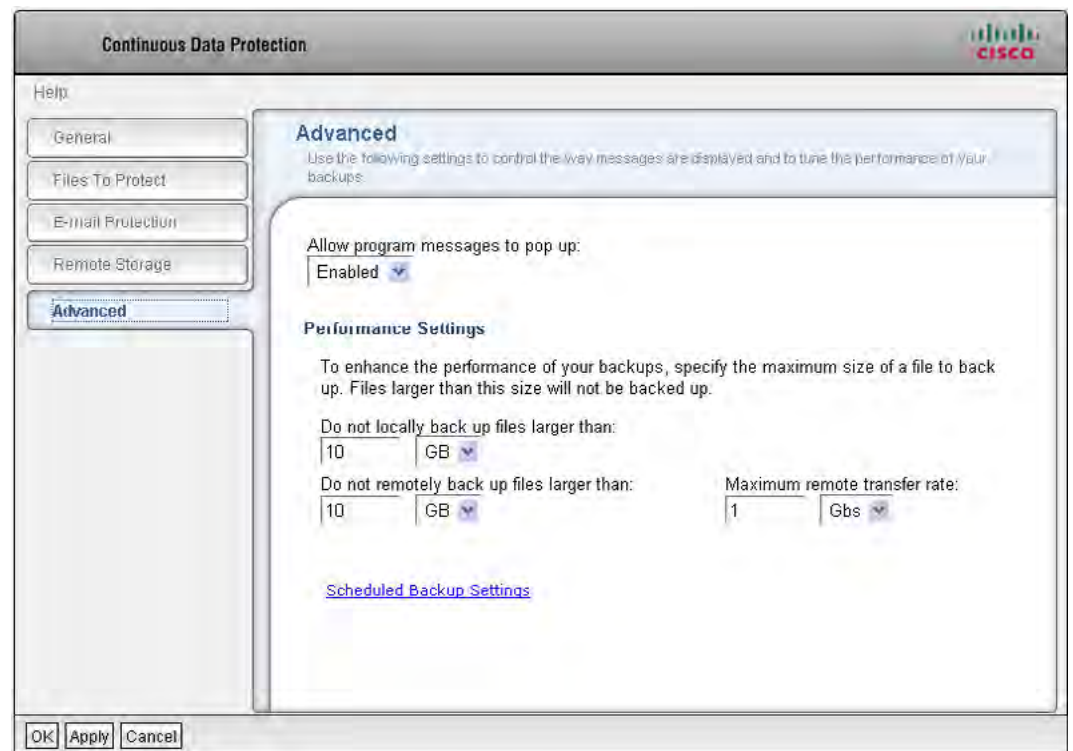
Figure 24. Network Identification Settings



Advanced Settings

In the Advanced drawer, make sure the maximum file size will accommodate large .pst mail files (Figure 25).

Figure 25. Specifying the Maximum File Size



You are now ready to apply these settings by clicking either Apply or OK (they do the same thing). The CDP-F software will start creating a folder structure on the NSS backup share that mirrors your file path structure. We will take a closer look at this in the next section.

When you click OK, you will be brought back to the main GUI screen. All icons should be blue.

If you have a yellow Remote icon, it means your PC can't see the NSS2050. You will need to rectify this before proceeding.

Access the open word document in a folder that is set for backup and make a minor edit to the open Word file and save it with the same name and note the versions which are copied to the C:\RealTimeBackup (Local) and the <http://192.168.10.200/backup> (remote) (Figures 30 through 32).

Figure 26. Clicking View Report to See the Backups

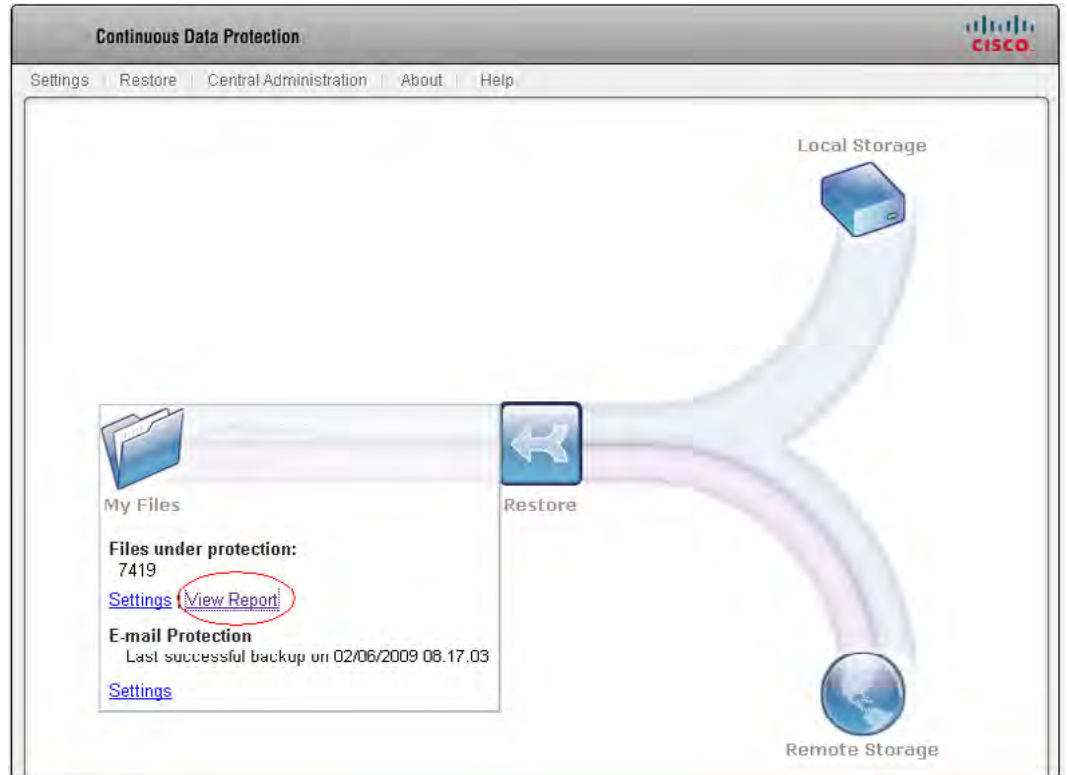


Figure 27. Viewing the Backup Activity Report

Activity Report		Friday, February 06, 2009 8:12:02 AM	
Failures			
The following lists the operations that failed. Look for repeated failures as a basis for troubleshooting. For information on how to correct issues, see Troubleshooting .			
Date and Time	File Name	Activity	Reason for Failure
Successful			
The following is a list of recent successful operations.			
Date and Time	File Name	Activity	
02/06/2009 08:12:01	IP_Video_Surv_with_Net_Store_Demo_Kit_sdistef_02042009.doc	Backup (Remote)	
02/06/2009 08:11:54	IP_Video_Surv_with_Net_Store_Demo_Kit_sdistef_02042009.doc	Backup (Local)	
02/06/2009 08:07:09	Product.pst	Version (Remote)	
02/06/2009 08:07:09	Product.pst	Purge (Remote)	
02/06/2009 08:03:23	fpa.txt	Report (Remote)	
02/06/2009 08:03:23	2009-02-06_08:00:06_BackupErr.xml	Report (Remote)	
02/06/2009 08:03:22	2009-02-06_08:00:06_BackupLog.xml	Report (Remote)	
02/06/2009 08:03:21	outlnk.nst	Backup (Remote)	

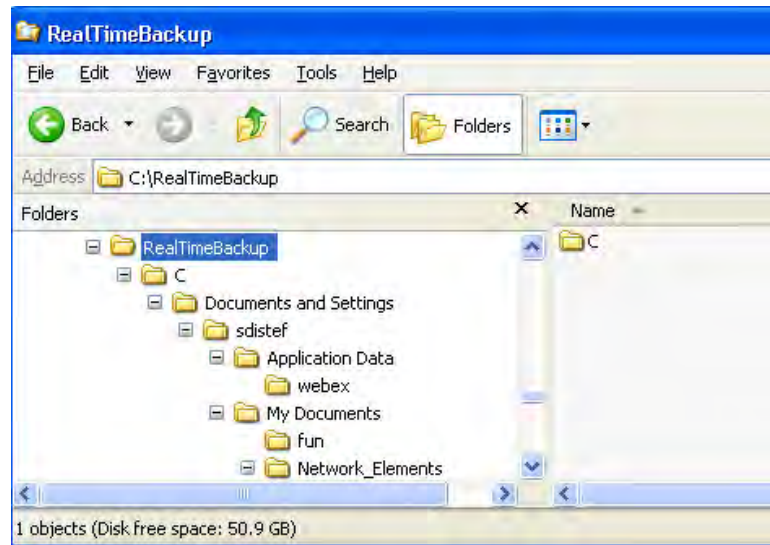
You will also notice that the CDP-F is creating directories for your file structure and finding and backing up data files for the application you selected (Figure 28). The figure shows that .vsd files are being backed up.

Figure 28. Directory Creation and Application File Backup

Time	File Name	Category
02/06/2009 08:14:29	SIP_Trunk_MS_sdistef.vsd	Backup (Remote)
02/06/2009 08:14:21	may-04-2008-b1716_pm74120_fwupgrade.tar.gz	Backup (Remote)
02/06/2009 08:14:16	1.13-12	Mkdir (Remote)
02/06/2009 08:14:16	lga	Mkdir (Remote)

Confirm that both the local and remote files are there (Figure 29).

Figure 29. Local Backup on the PC



Make a minor edit to the open Word file, save the file, and note the versions (Figures 30 through 32).

Figure 30. Versions of the Open Word Document in the Local Backup

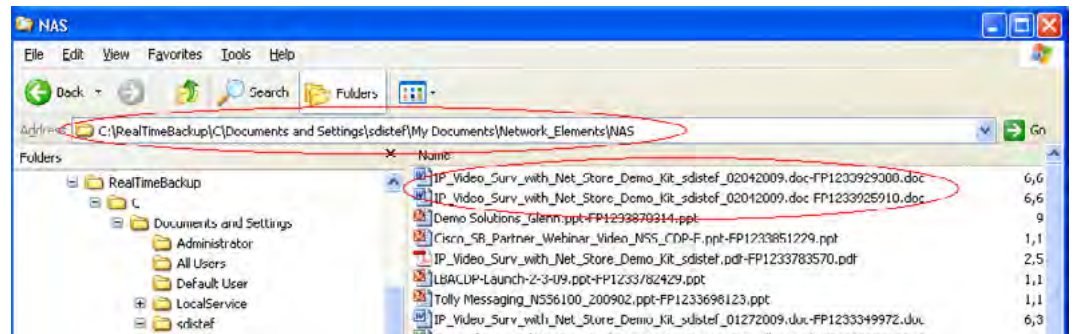


Figure 31. Versions of the Open Word Document in the Remote Backup on the NSS2050

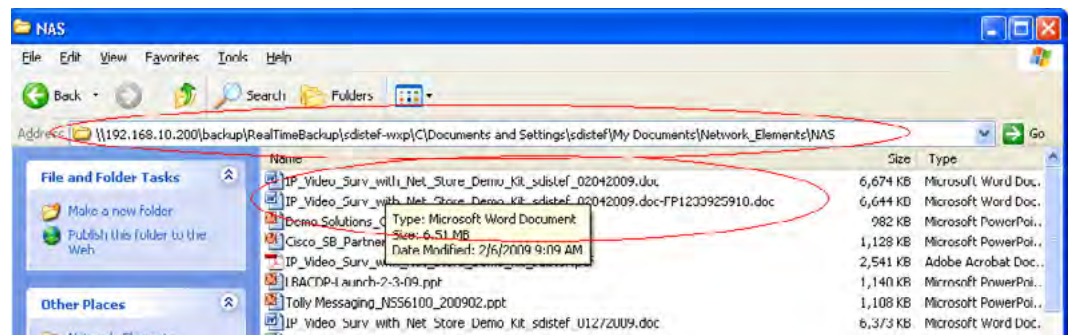
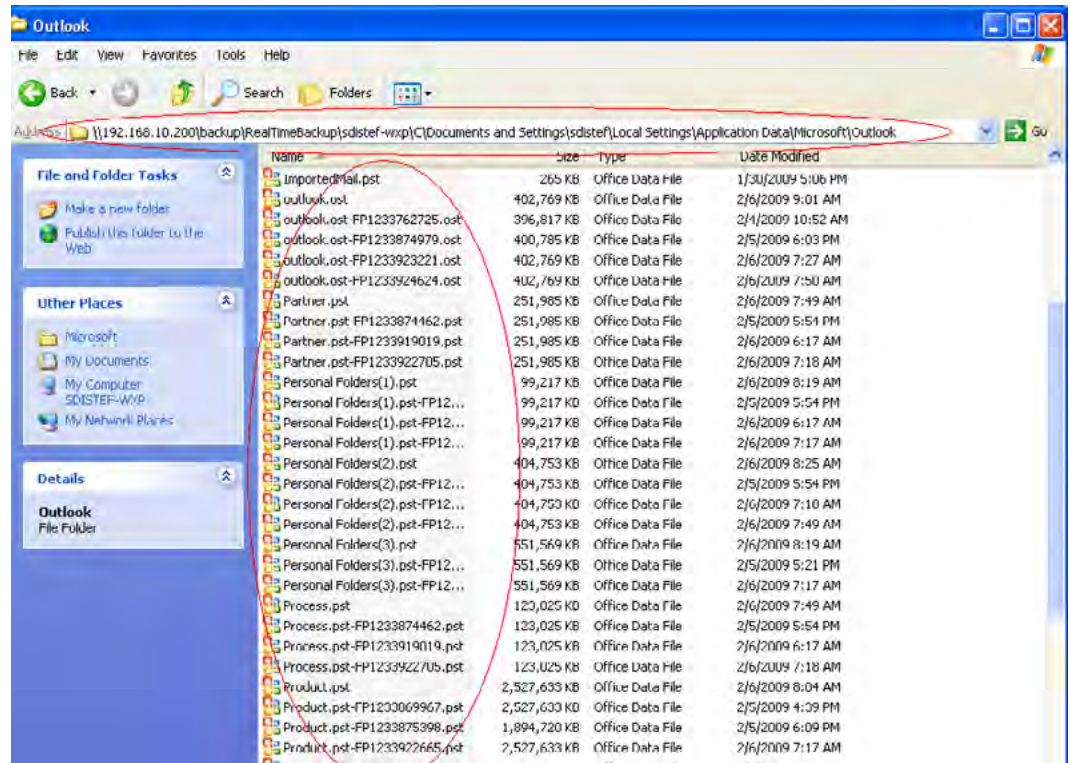


Figure 32. Remote Backup of Email Files



This example shows the backup Outlook files on the remote location. The location of these files depends on which e-mail program is used on the machine, and where these files are stored on the machine. The remote files would be located on \\192.168.10.200\backup\[ComputerName]\C:\[Path on Disk]

Cisco NSS2050 Network Place Shortcut on the PC

On your laptop, which is connected to the Cisco SRW2008P and has a 192.168.10.x (DHCP) address, navigate to My Network Places and click “Add a network place” to launch the Add Network Place Wizard.

Select “Choose another network location” and enter the IP address of the NSS2050 as the network address (Figure 33).

Figure 33. Specifying a Network Address



Click Browse to open the shares you created in the NSS2050 default workgroup called "Workgroup" to find the backup share, or just type the file path, and click Next.

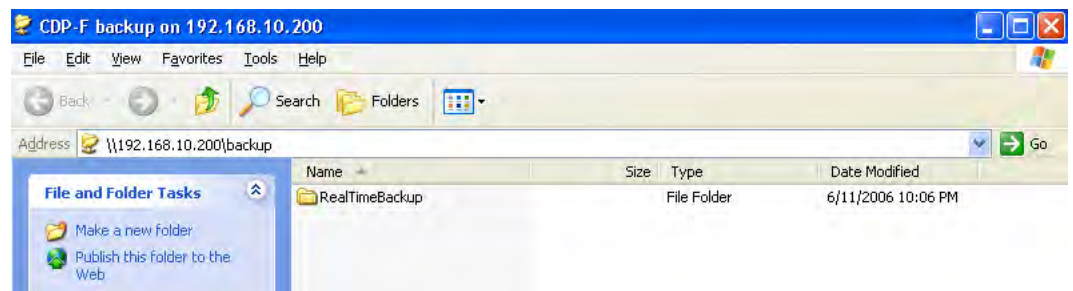
Windows will suggest a name, which you can accept or modify and click Next (Figure 34).

Figure 34. Naming the Shortcut



Click Finish and open it (Figure 35).

Figure 35. Connecting to the Backup Share via the Shortcut

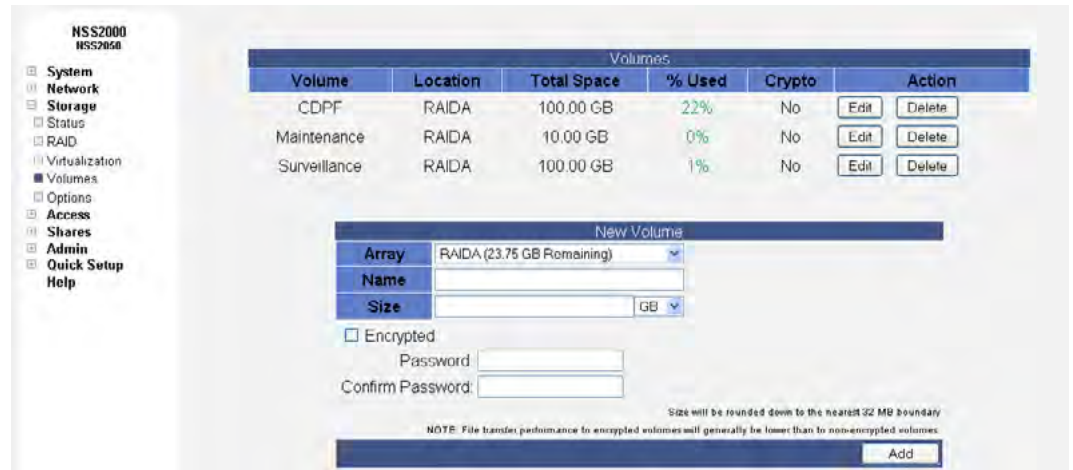


Now the backup share is saved in your network places. You can use this shortcut to connect to the NSS share.

Go to the web GUI of the NSS2050 (<http://192.168.10.200:1026/>) and check the volumes. To check the volumes go to Storage -> Volumes in the GUI menus.

Note: You have to make a significant dent in the NSS to see this grow, so it make take a few thousand files to see the percentage move even a little (Figure 36).

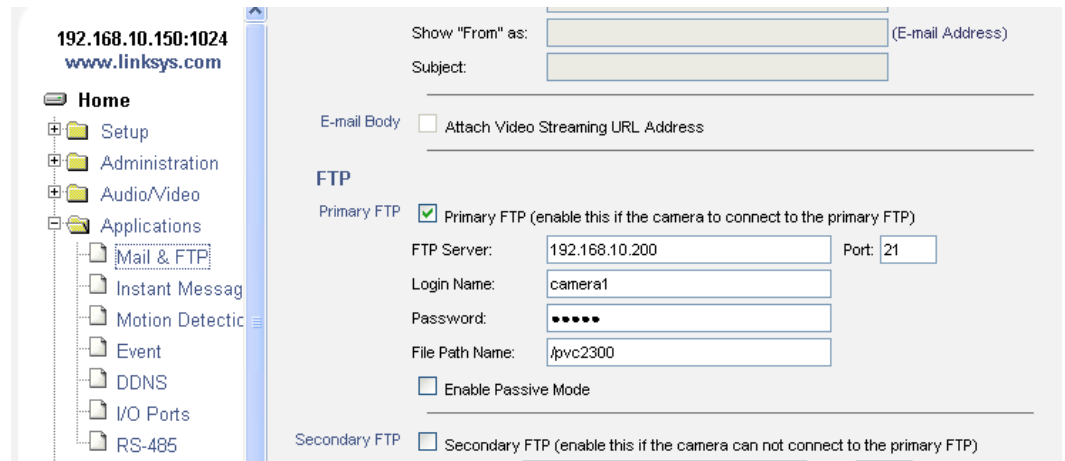
Figure 36. Checking the Volumes via the Web GUI



Demonstrate Sending Video (with Audio) Motion Detection Data from the Surveillance Camera to the NSS via FTP

Log in to the camera GUI (192.168.10.150:1024) and add the NSS2050 IP address to the FTP server definition. Include the login credentials that the camera will use (camera1/cisco) as well as the share you want to write to (Figure 37).

Figure 37. Specifying FTP Settings and Login Information for the Camera



Using Internet Explorer, configure the motion detection window(s). You may be prompted to install an ActiveX plug-in (Figures 38 and 39). You must allow this in order to see the video.

Figure 38. Prompt for Installing the ActiveX Plug-In

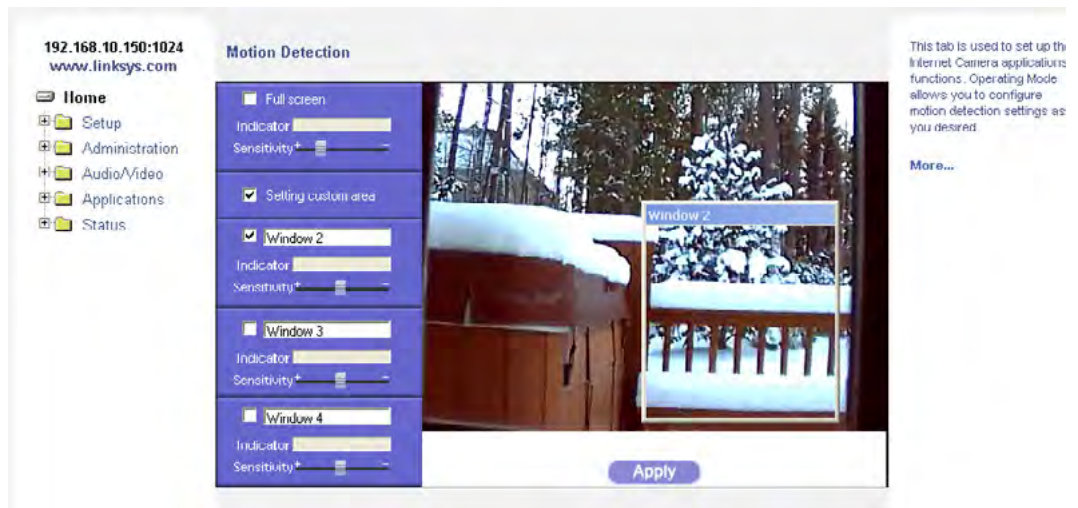


Figure 39. Security Warning for ActiveX Plug-In



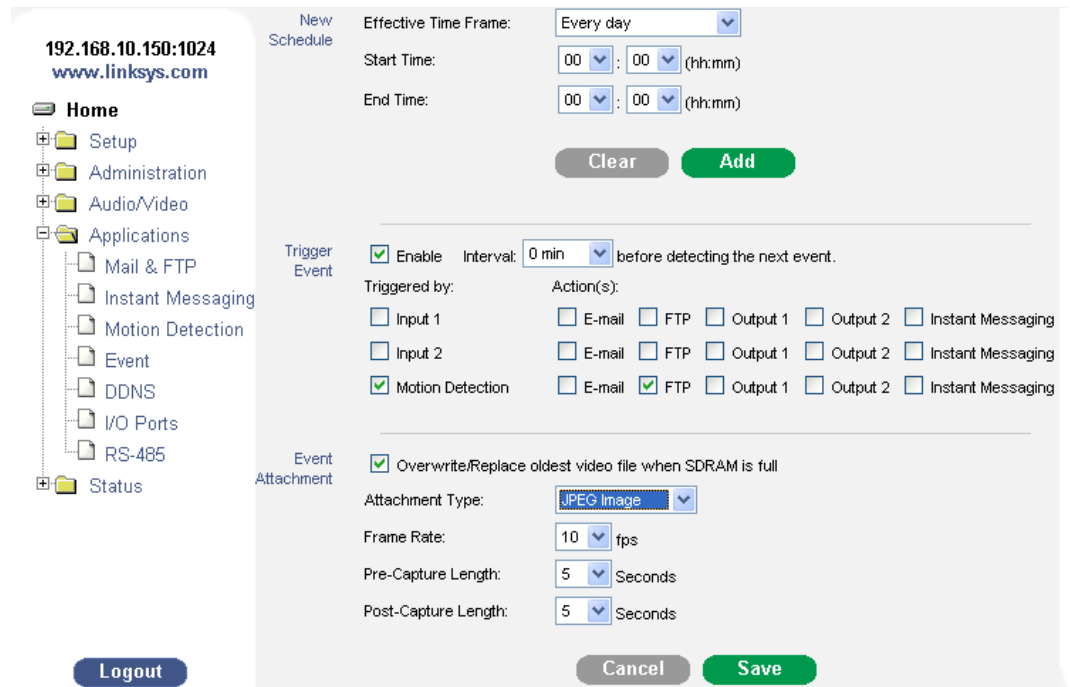
The Applications drawer in the GUI contains a Motion Detection subdrawer. Use this to enable motion detection, selecting one custom window, and set the area just to the right of your video view (as shown in Figure 40). Sensitivity can be adjusted so birds or snow (for example) do not trigger it.

Figure 40. Creating a Motion Detection Window



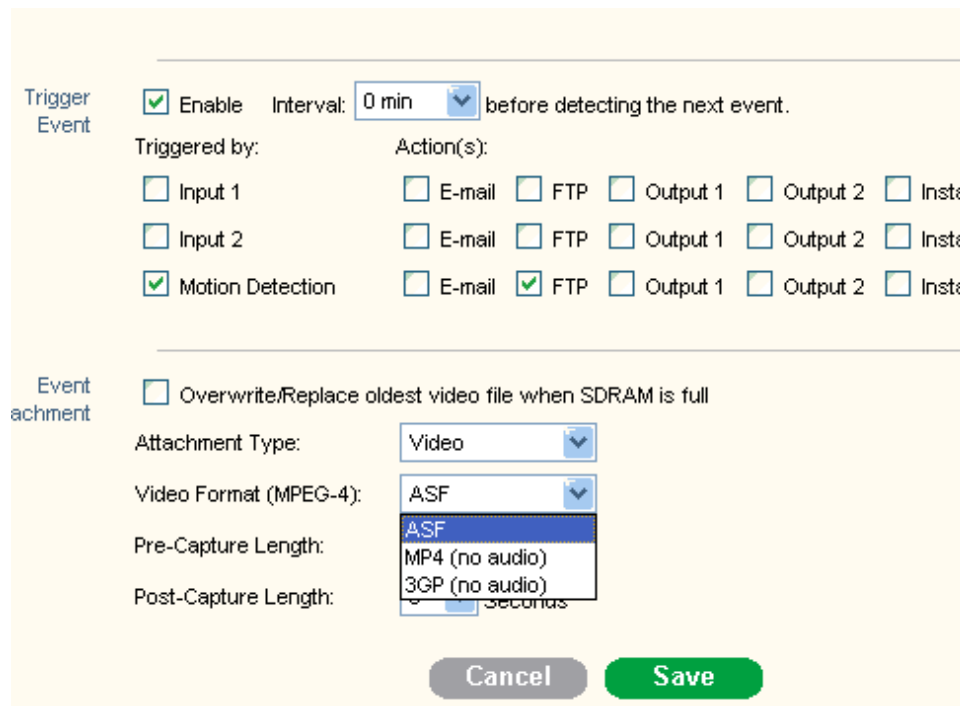
Using the Event drawer of the GUI, enable Motion Detection and check FTP (Figure 41).

Figure 41. Enabling Motion Detection



Try sending both video and MJPEG (both 5 seconds before and 5 seconds after the detected motion at 10 fps) to the FTP server (NSS2050). For video FTP attachments, the supported video formats are ASF, MP4 (MPEG-4), and .3gp (Figure 42).

Figure 42. Sending Video Output to the NSS2050



Double-check the video and audio quality and compression settings. You can also add the camera name and time stamp here (Figures 43 and 44).

Figure 43. Viewing the Image Quality Settings

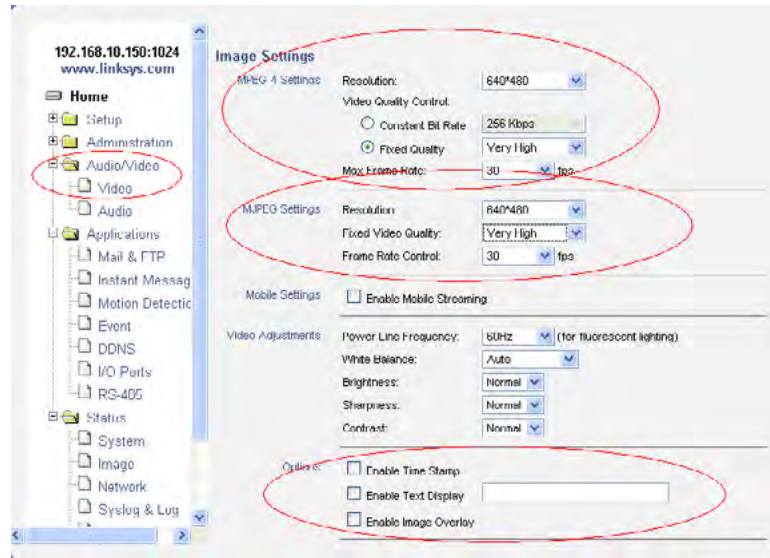


Figure 44. Viewing the Audio Settings

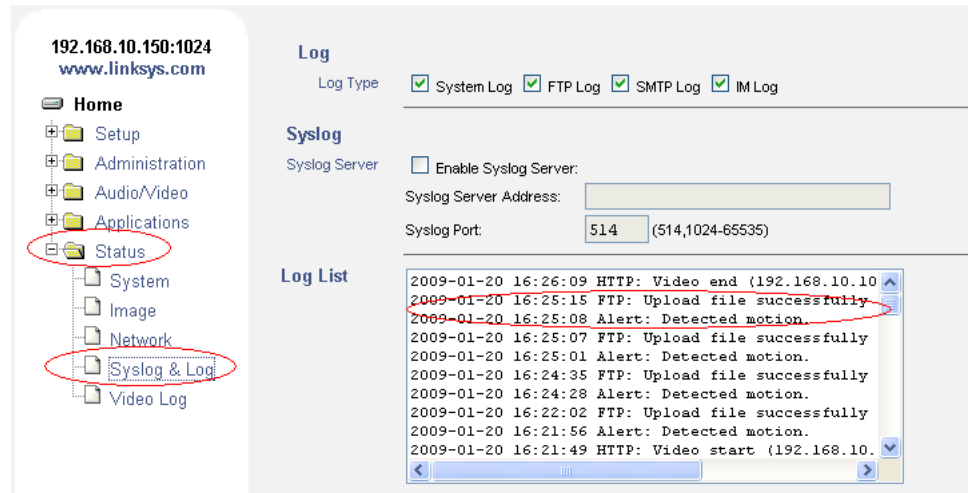


After saving your desired changes in the camera configuration, create some motion in front of the camera, and confirm that the content is sent to the NSS. Demonstrate the three techniques described below.

First, on the camera, go to the Status drawer of the GUI and click Syslog & Log.

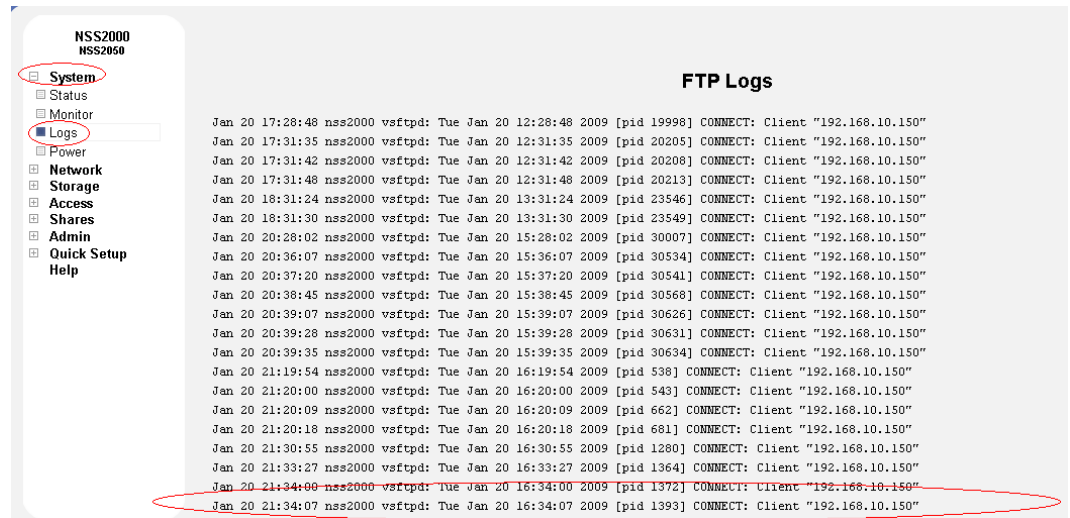
Note: The successful upload via FTP and the alert regarding detected motion (Figure 45).

Figure 45. Checking the Log in the Status Drawer of the Camera GUI



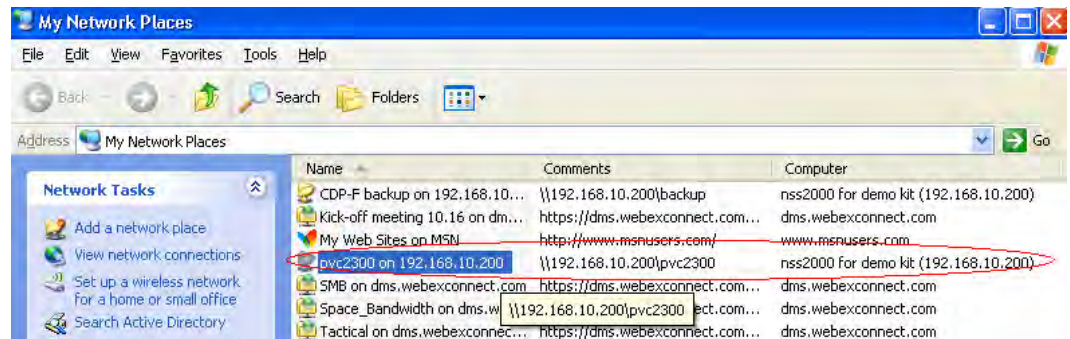
Second, on the NSS, go to the Status drawer of the GUI and display the Logs subdrawer. Confirm that the camera accessed the FTP service and left a log (Figure 46).

Figure 46. Checking the Log on the NSS



Third, using your PC and a shortcut to the PVC2300 share you created (you can also just go to Run:cmd, type \\192.168.10.200\pvc2300, and log in with cisco/cisco), check the share for the files (Figure 47).

Figure 47. Checking for the Files on the Local Share



Change the camera between MPEG-4 (movie) and JPEG to see each type. Double-click a movie file to see and hear it (Figures 48 and 49).

Figure 48. Viewing a Movie File

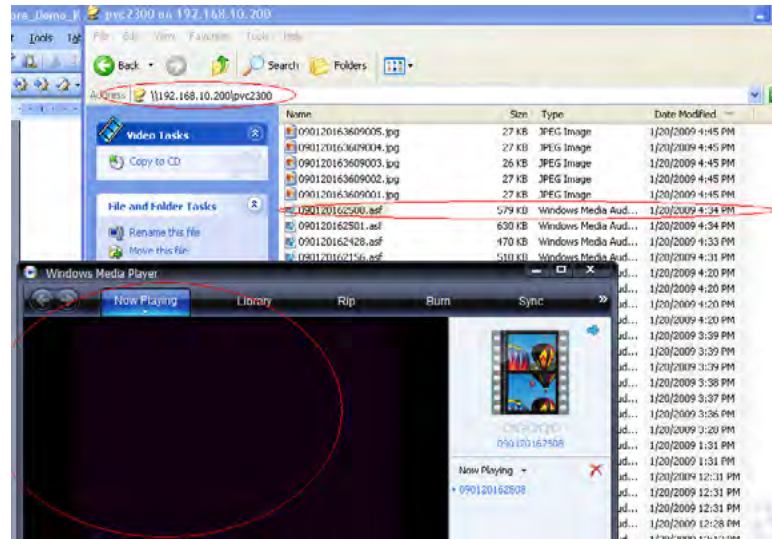
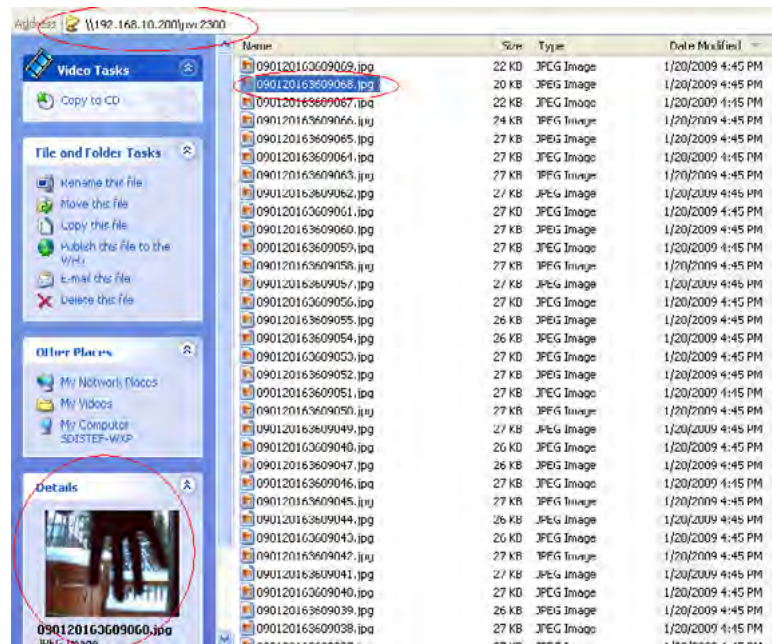


Figure 49. Viewing a JPEG File



You can copy these files to your PC for further use or store them on the NSS2050 file share for as long as you like.

As you can see, the process is very easy. Remember that the PVC2300 provides a true dual codec stream, so it can do this and send email simultaneously.

You can also demonstrate that when connecting to the NSS2050 share with the readonly user credentials, you cannot copy files from the NSS, and a user with no access rights to a share cannot access it.

When switching between users or shares, you may want to disconnect from the drive using the DOS CMD:`net use \\192.168.10.200 /delete`. However, since the CDP-F relies on the connection as well, using a limited access user will cause problems for CDP-AF and so this is not suggested. Instead, connect another PC to perform this optional step.

Demonstrate Monitoring/Playback from the SWVMS16 Utility

Launch the SWVMS16 Video Monitoring System on your PC, go into Setup -> Settings, and configure the following:

- **General:** Default values are fine with storage of recorded video on the PC hard drive in the specified location (you can also store this utility's video files on the NSS2050 file share).
- **Camera:** Scanning for cameras would work fine if no port adjustments had been made (the default configuration uses port 80), but since we've changed the port you need to enter the port manually and click OK (Figure 50).

Figure 50. Specifying Camera Settings from SWVMS16

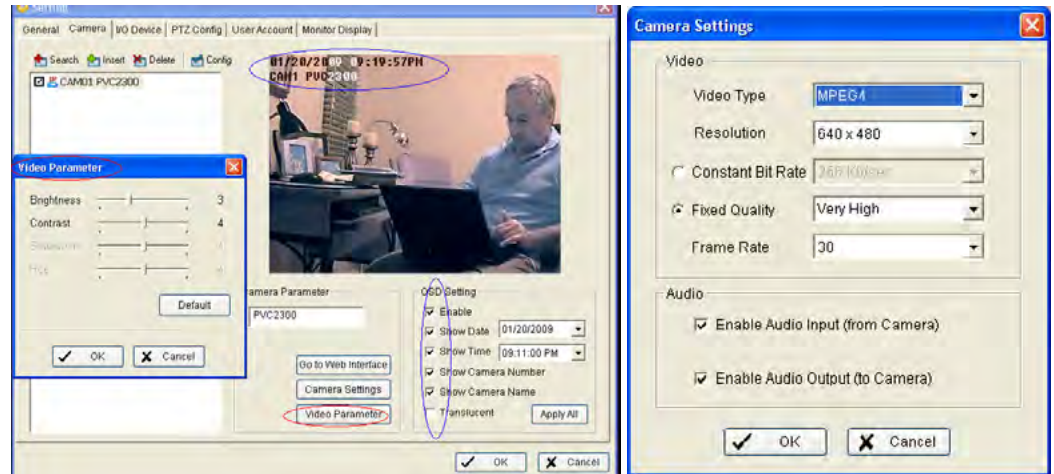
The screenshot shows a dialog box titled "IP Camera / Video Server Setting". It has a blue title bar with a close button. The dialog is organized into three main sections:

- Network:**
 - Name: PVC2300
 - IP Address: 192 . 168 . 10 . 150 (with a "Use DNS" checkbox to the right)
 - Http Port: 1024
 - User Name: admin
 - Password: *****
 - Protocol: TCP UDP HTTP
- Device:**
 - Vendor: LINKSYS (dropdown menu)
 - Camera Model: PVC2300 (dropdown menu)
 - Auto Detect button
- Description:**
 - Video Codec: MPEG4 MJPEG
 - Audio Codec: G.726
 - Camera:1, DI:2, DO:2

At the bottom of the dialog are two buttons: "OK" (with a checkmark icon) and "Cancel" (with an X icon).

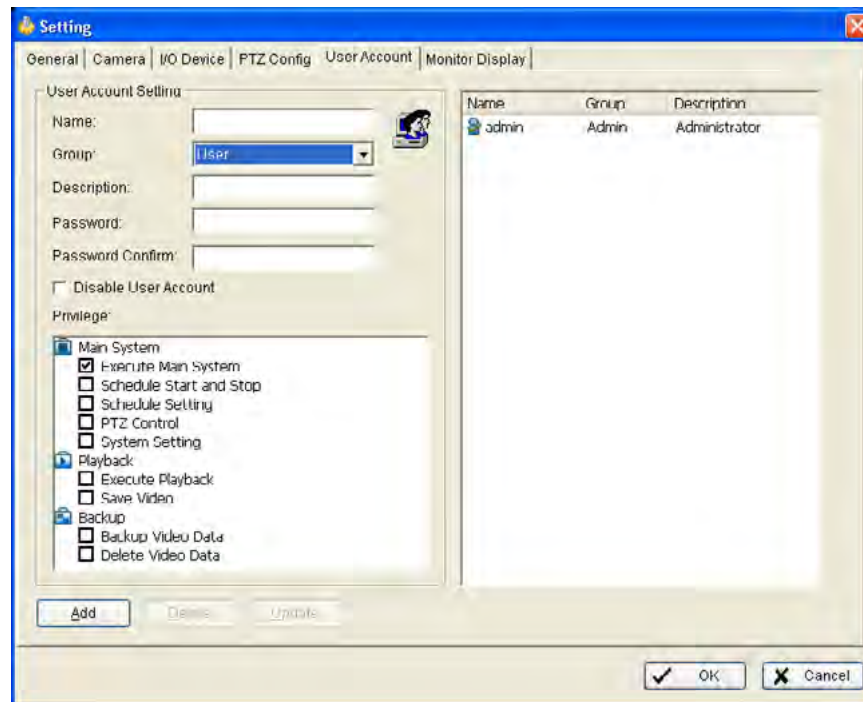
The camera will now show up on the GUI Camera Setup screen, where you can indicate what text is also present in the camera view, adjust the basic picture image, set advanced video attributes, or just launch the camera GUI from here if you needed to (Figure 51).

Figure 51. Camera Setup



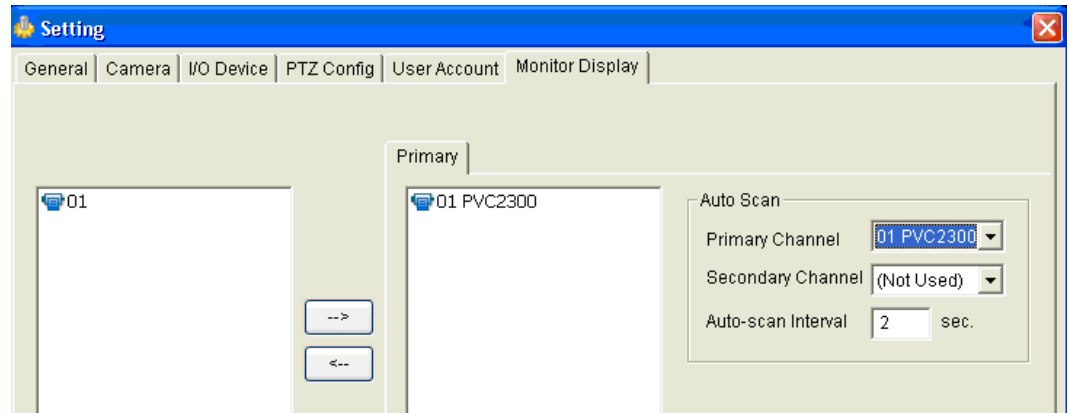
- **User Account tab:** You can build a role-based user account and select the capabilities of the user (use admin/cisco for the demo). This is a big improvement over the previous camera utility (Figure 52).

Figure 52. User Account Tab



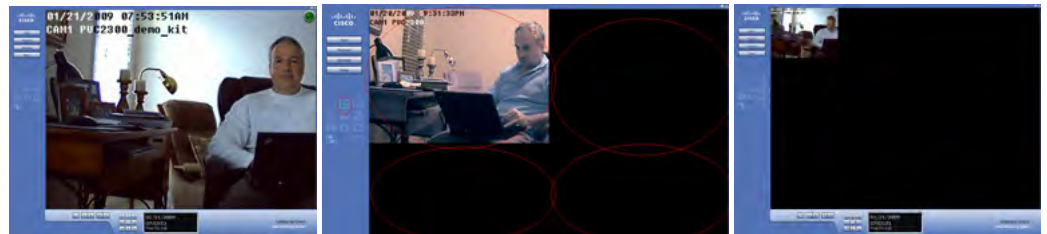
- **Monitor Display tab:** This tab should be set up already, but you can add the camera as a primary channel (Figure 53).

Figure 53. Monitor Display Tab



Click Save; the PVC2300 is now on the monitor. It can be the only camera or one of many (up to 16) (Figure 54).

Figure 54. Camera Output Displayed Onscreen



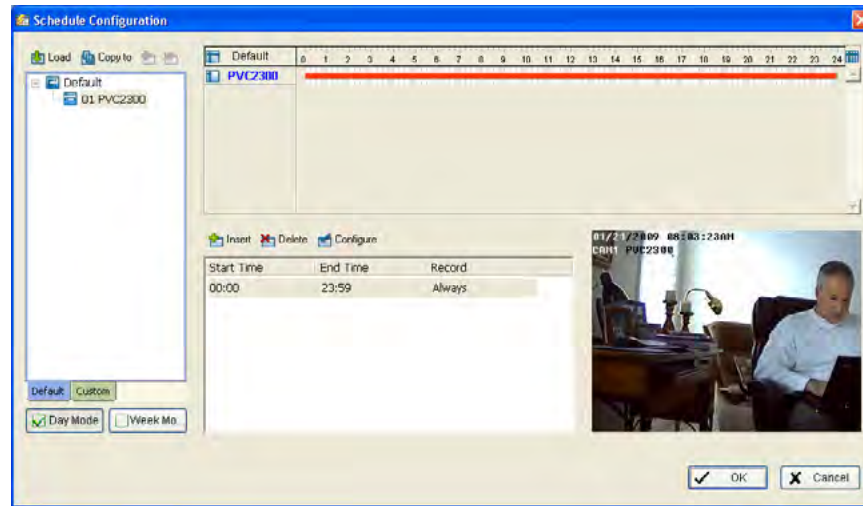
Whether you are on the local LAN or remotely monitoring via a VPN connection or port-forwarding camera access, you can monitor up to 16 cameras in various locations in this way.

Once the camera is added, you need to define the schedule for the SWVMS16 utility. There are two options:

- **Record Always:** This is the default; it allows you to click the Start button on the monitor to begin recording.
- **Motion Detected:** This option allows you to configure motion detection–based recording that can be started from the monitor.

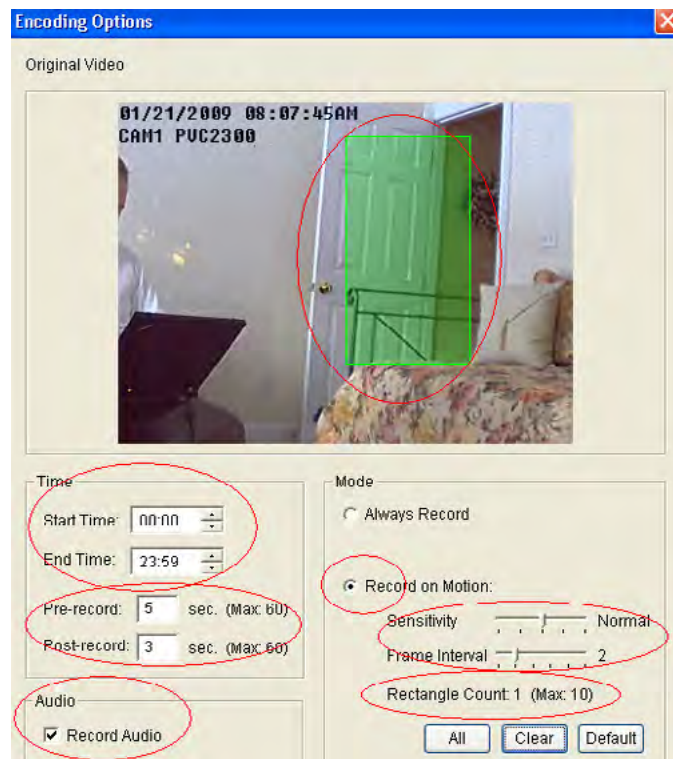
Click Schedule from the main monitor and access the PVC2300 camera. Click Configure just above the middle frame, showing the default (Record Always) (Figure 55).

Figure 55. Scheduling Recording in the SWVMS16 Utility



The configuration window shown in Figure 56 will open.

Figure 56. Configuration Window



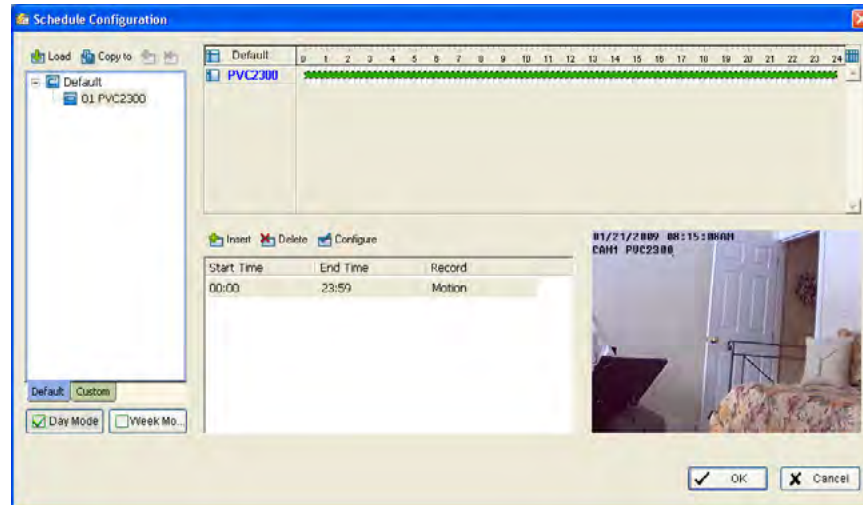
Configure recording as shown in the figure. Once you click Record on Motion, you can draw up to 10 green rectangles to cover areas in which you want to detect motion (it will record the entire camera view but detect motion in the green areas only).

If you want to detect motion only during certain parts of the day, you can adjust the start and end times. You can capture up to 60 seconds of premotion and postmotion frames. On its own, the camera can record only 5 seconds each. The SWVMS16 utility can do much more due to the PC being used as the buffer memory.

Record Audio needs to be explicitly set by you.

Walk in and out of the rectangle you set for motion detection, and notice whether it turns red. Adjust the sensitivity so that the desired amount of motion will set it off. When you're done, save the settings and then click OK on the main screen (Figure 57).

Figure 57. Main Screen of the SWVMS16 Utility, Showing Recording When Motion Is Detected



There is one last thing to do. On the main monitor, click on the camera frame and you will hear the audio in real time. Click Start on the Monitor GUI and notice the green dot in the upper right corner of that camera view (Figure 58). It is now ready to detect and record motion.

Figure 58. Green Dot Indicating That the Camera Is Ready to Detect and Record Motion



Now and walk through the door (or whatever area you set up in your environment). The green dot will turn red for a few seconds, indicating that it captured something.

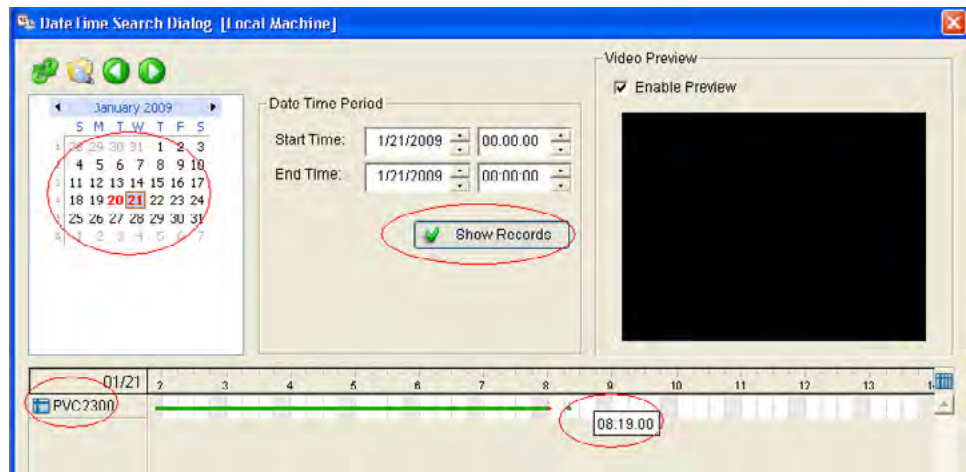
Click Playback on the monitor GUI. A new window opens with some new controls. Click Open Recording (Figure 59).

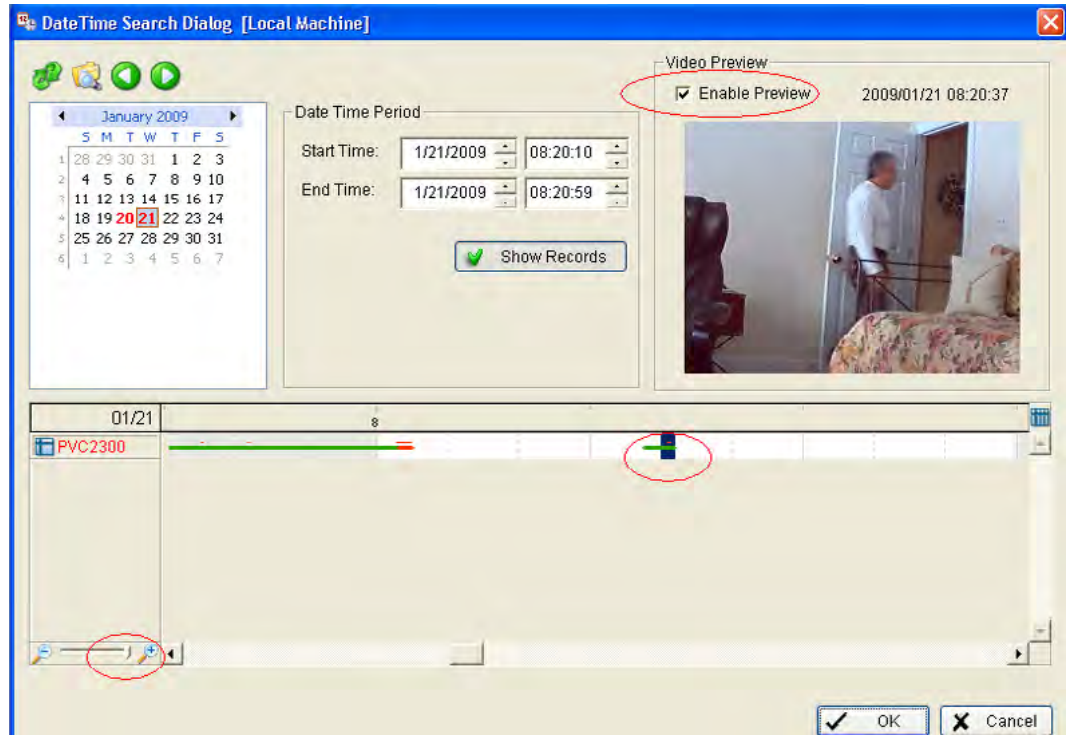
Figure 59. Clicking the Open Recording Button



In the GUI that appears (Figure 60), click Show Records. The default is today's date, but you can adjust it if you are looking for records from another day. Locate a record that you want to play back. In the figure, there is a small record at 8:19 a.m. that we are interested in seeing. Check Enable Preview, zoom in so to make it easier to see the time period you're interested in, and click over the green bar to see a preview of the record.

Figure 60. Locating and Previewing a Record





Click OK, and the recording appears on the Playback screen, where you can control it (speed, pause, frame advance, take snapshot (.bmp), save video (.avi), and so on) (Figure 61).

Figure 61. Viewing the Recording on the Playback Screen



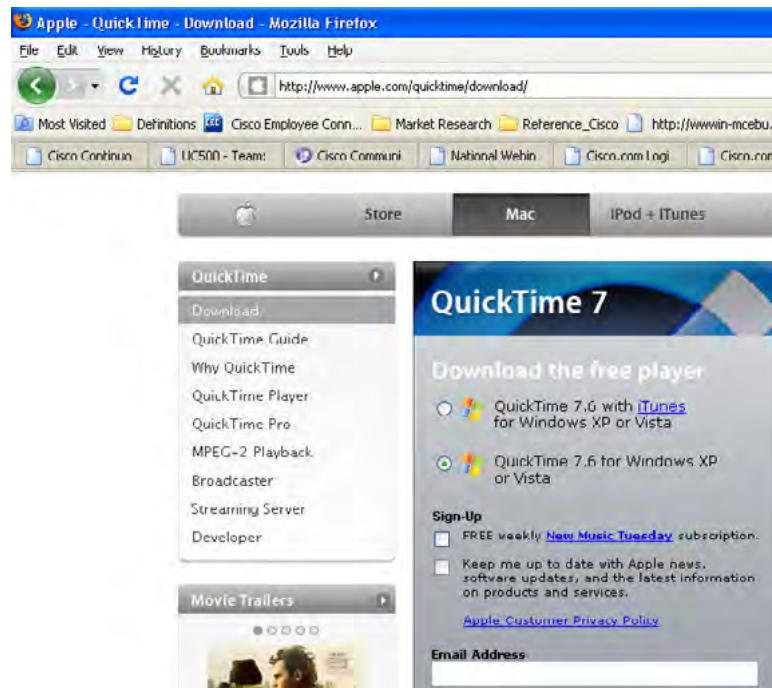
Demonstrate Monitoring RTSP Video (with Audio) from Any PC (Local or Remote) or 3GPP Smart Phone

These demonstrations will be done from the local LAN to prove the protocol and capability while eliminating the firewall port issues. However, the configuration of the demo kit equipment will support remote access if you can connect your PC behind a different router on the public Internet (separate from the demo kit but routable to it).

Installing QuickTime on Your PC

Download the Apple QuickTime 7 player and install it on your PC (this takes about 5 minutes) (Figure 62).

Figure 62. Downloading QuickTime



RTSP Streaming Video on a PC (media.sav)

From the local LAN, connect to the camera using the VLC media player on your PC by choosing Media -> Open Network, specifying the RTSP protocol, and using the following target on the camera itself to retrieve video and audio (Figure 63).

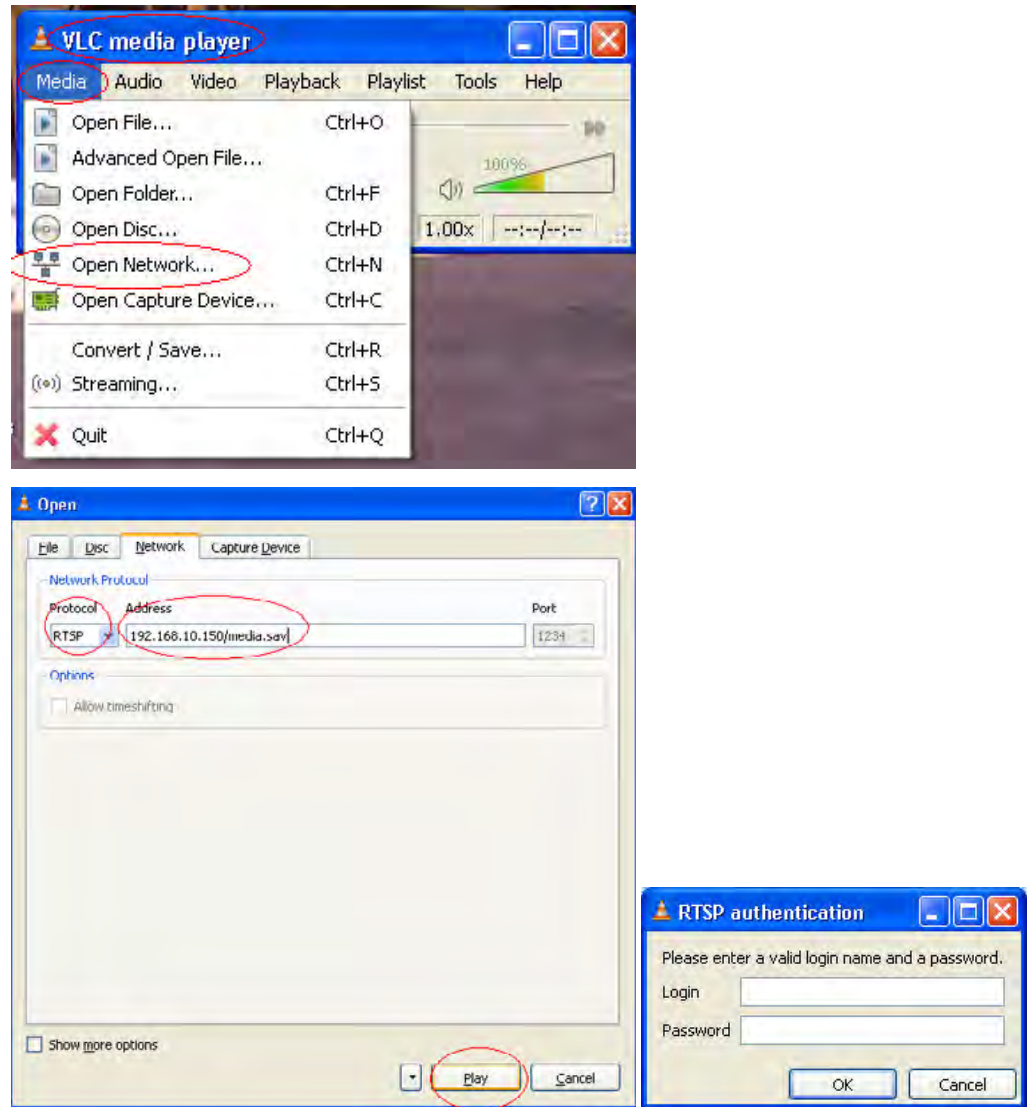
```
192.168.10.150/media.sav
```

You can also do the same from a PC connected remotely on another network with WAN access to this demo kit:

```
<WAN IP of WRVS4400N>/media.sav
```

You will be challenged for a username and password, which you will enter as admin/admin. The media player will then show the camera view.

Figure 63. Connecting to the Camera via the VLC Media Player



After you log in, the VLC media player will expand and show you what the camera sees. This works for both local and remote PCs (Figure 64).

Figure 64. Viewing RTSP Streaming Video via the VLC Media Player



Playback Options: RTSP playback will use the settings specified in MPEG-4 Settings for image quality. For example, increasing the MPEG-4 resolution to 640x480 will enable the RTSP stream to use this same resolution. The same applies for the video quality and maximum frame rate.

Up to 10 simultaneous RTSP streams are supported on the camera. User Datagram Protocol (UDP) ports 5000 through 5020 will be used. Audio is supported when using the QuickTime player and when audio is enabled on the Camera.

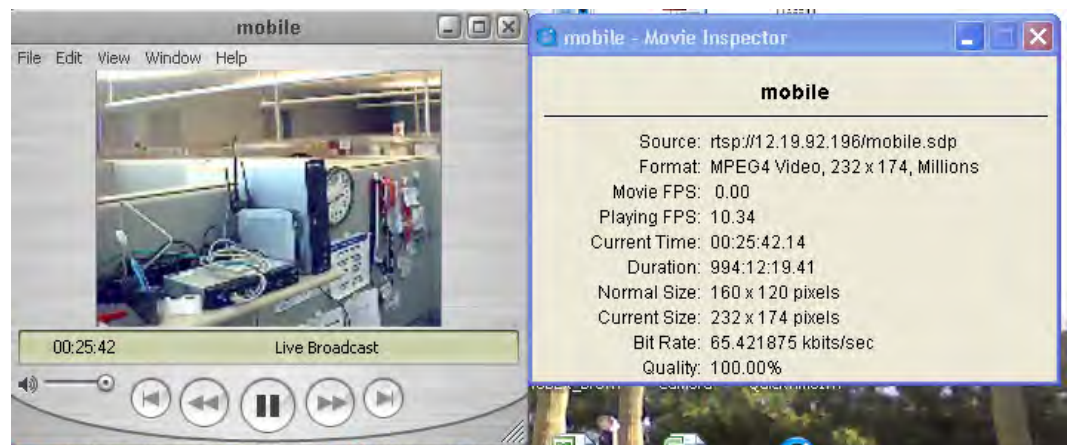
RTSP Streaming Video on a Mobile Phone (mobile.sdp)

Follow these steps to access the camera video from a 3GPP phone (Figure 65).⁵

Note: Mobile streaming is video only (no audio).

```
RTSP://192.168.10.150/mobile.sdp <- do this from your PC
RTSP://<WAN IP of WRVS4400N>/mobile.sdp <- do this from a PC
connected to a different network6
```

Figure 65. Viewing RTSP Streaming Video via mobile.sdp



⁵ Supported mobile phones: Blackberry Pearl 8130, some Nokia models, Samsung BlackJack II.

⁶ Note: If the QuickTime player is used remotely on the Internet, it is likely to be sitting behind a NAT router, in which case ports will need to be opened to allow RTSP and RTP data to reach the client player (open UDP ports 5000 through 5010 and 6970 through 6999).

```
RTSP://<WAN IP of WRVS4400N>/mobile.sdp <- do this from your 3GPP  
smart phone
```

You will not be challenged for a username and password. On a PC, the media player will then show the camera view, if you enabled this on the camera. On a phone, the phone's Internet Explorer will show the camera view (Figure 66).

Figure 66. 3GPP Phone Display



Appendix A: Demonstration Kit Supporting Data

Computer Minimum Requirements for Camera Utility

For One Camera	
CPU	Pentium 4 class, 2GHz
Memory	512 MB
Operating System	Microsoft Windows 2000, XP, or Vista
Hard Drive	500 MB of available space
Graphics Card	AGP with a minimum 128 MB
Browser	Internet Explorer 6.0 (or above), Mozilla Firefox, Netscape 7.0 (or above)
For Up to Eight Cameras	
CPU	Pentium 4 class, 3GHz
Memory	1 GB
Operating System	Microsoft Windows 2000, XP, or Vista
Hard Drive	4 GB of available space
Graphics Card	NVidia high performance or equivalent with a minimum 256 MB
Browser	Internet Explorer 6.0 (or above), Mozilla Firefox, Netscape 7.0 (or above)

Camera and Camera Monitor Utility Compatibility

	“Original Utility”	Video Monitoring System LBAVMS16 SW-AVM316
WVC200	Yes	No
WVC2300	Yes	Yes
PVC2300	Yes	Yes
WVC210	No	Yes
PVC300	No	Yes
Future Cameras	No	Yes

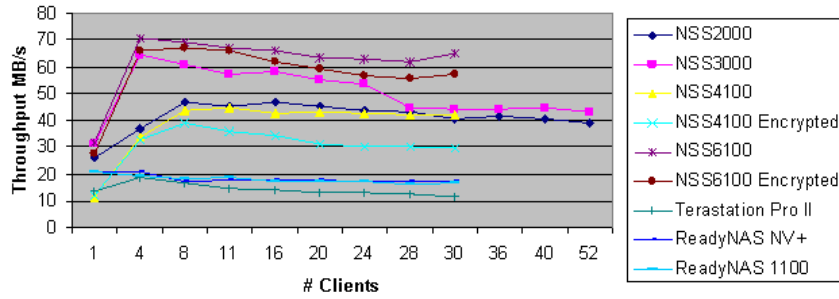
RAID Definitions

A Redundant Array of Independent Disks (RAID) appears to the operating system to be a single logical hard disk. RAID employs the technique of disk striping, which involves partitioning each drive's storage space into units ranging from a sector (512 bytes) up to several megabytes. The stripes of all the disks are interleaved and addressed in order. Shown are the RAID capabilities of the 2-bay NSS2050 system included with the demo kit.

- **RAID0:** This technique has striping but no redundancy of data. It offers the best performance but no fault tolerance.
- **RAID1:** This type is also known as disk mirroring and consists of at least two drives that duplicate the storage of data. There is no striping. Read performance is improved since both disks can be read at the same time. Write performance is the same as for single disk storage. RAID1 provides the best performance and the best fault-tolerance in a multiuser system.

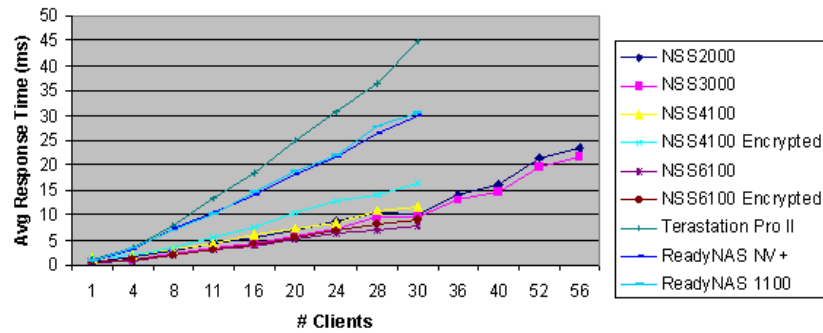
NSS Performance Data

Figure 67. Benchmarks – RAID1 Throughput



* NSS2000/NSS3000 Performance Data is preliminary based on proto firmware. Official Tolly report lists NSS6100 only. All other testing done in-house.

Figure 68. Benchmarks – RAID1 Response Time



* NSS2000/NSS3000 Performance Data is preliminary based on proto firmware. Official Tolly report lists NSS6100 only. All other testing done in-house.

Estimated Bit Rates of Video Data

Resolution	Quality Level	Bit Rate
640 x 480	Very High	4000kbps
640 x 480	High	3200kbps
640 x 480	Normal	1200kbps
640 x 480	Low	480kbps
640 x 480	Very Low	160kbps
320 x 240	Very High	1000kbps
320 x 240	High	800kbps
320 x 240	Normal	300kbps
320 x 240	Low	120kbps
320 x 240	Very Low	40kbps
160 x 120	Very High	800kbps
160 x 120	High	400kbps
160 x 120	Normal	200kbps
160 x 120	Low	100kbps
160 x 120	Very Low	40kbps

Estimated Storage Space Requirement for Video Data

3 cameras, continuous recording:

- 15 fps
- 640 x 480 resolution
- "Normal" quality
- MPEG-4
- = 10 GB per day**

1 camera, continuous recording for 1 hour:

- 15 fps
- 640 x 480 resolution
- "Normal" quality
- MPEG-4
- =150 MB per hour**

120 motion events:

- 30 seconds before and 30 seconds after event
- At 15 fps = 64 MB**
- At 30 fps = 90 MB**

NSS Model Differences

Some flexibility is built into the NSS so you can accommodate the operation environment of the unit:

Each NSS unit supports two different connection profiles that are user configurable. This allows for a different mixture of CIFS and FTP connections based on the use case. The higher FTP connection profile is especially useful for video surveillance applications when the camera is set up to transfer data over FTP.

CDP-F Competitive Table

	NSS2000	NSS3000	NSS4000	NSS6000	Benefits
Ethernet LAN Interfaces	(1) GigE	(1) GigE	(2) GigE	(2) GigE	Redundancy
Hot Swap Back-Plane	Yes	Yes	Yes	Yes	Higher Availability
RPSU Support	No	No	Yes	Yes	Higher Availability
RAID Types Supported	0/1	0/1/5/10	0/1/5/10	0/1/5/10	Flexibility
Max CIFS users	15	15	15	132	# of simultaneous users
Max FTP users	15	15	15	50	# of simultaneous users
Microsoft Distributed File System	Yes	Yes	Yes	Yes	Simple expansion without user impacts
256bit AES File Encryption	Yes	Yes	Yes	Yes	Data Security
Virtualization Master	No	No	No	Yes	Greater Expansion
Snapshot	No	No	No	Yes	Data Availability
Form Factor	Desktop	Desktop	Rack Mount	Rack Mount	Flexible form factor selection

NSS2000, NSS3000, NSS4000

Standard profile: 15 CIFS + 2 FTP

Advanced/network video recorder: 8 CIFS + 16 FTP

NSS6000

Standard profile: 32 CIFS + 20 FTP

Advanced/network video recorder: 117 CIFS + 50 FTP

Figure 69. CDP-F Competitive Table

	Tivoli	NTI Shadow	Rapid Rest	Dantz	Microsoft	Symantic	Connected	Live Vault	Storage
Ease of Deployment	Green	Green	Green	Green	Red	Red	Yellow	Yellow	Yellow
Continuous	Green	Green	Red	Red	Yellow	Yellow	Yellow	Yellow	Red
Price	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Simplicity (TCO)	Green	Green	Green	Green	Red	Red	Yellow	Yellow	Yellow
Scheduled	Green	Yellow	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow
Local Cache	Green	Red	Green	Red	Red	Red	Red	Yellow	Yellow
Single User Capable	Green	Green	Green	Green	Red	Red	Red	Red	Red
GUI Appeal	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green
Workstation Protection	Green	Green	Green	Green	Red	Green	Green	Green	Green
File Server Protection	Green	Red	Red	Red	Green	Green	Yellow	Yellow	Yellow
System Protect	Yellow	Red	Green	Yellow	Red	Red	Green	Green	Green
Scalability	Green	Yellow	Red	Red	Green	Green	Green	Green	Green
Encryption	Green	Red	Yellow	Yellow	Yellow	Yellow	Green	Green	Green
Compression	Green	Red	Green	Green	Yellow	Yellow	Green	Green	Green
Throttling	Green	Red	Red	Red	Yellow	Yellow	Green	Green	Green
Email (Client)	Green	Green	Red	Red	Red	Red	Green	Green	Green
Email (Server)	Red	Red	Red	Red	Red	Red	Red	Red	Red
Sub-file	Green	Green	Red	Red	Yellow	Yellow	Green	Green	Green
Web-Server Target	Green	Green	Red	Red	Red	Red	Red	Red	Red
Backup-target (TSM, BackupExec)	Green	Red	Red	Red	Red	Red	Red	Red	Red
Corporate Viability	Green	Green	Green	Green	Green	Green	Yellow	Green	Green
Maturity	Green	Green	Yellow	Green	Yellow	Yellow	Yellow	Green	Yellow
USB-bundle Suitability	Green	Green	Green	Green	Red	Red	Red	Red	Red
ISP Suitability	Green	Red	Red	Red	Red	Red	Red	Red	Red

Appendix B: Support

The Partner/Reseller Help number for the United States is 1-800-GO-CISCO

Hours of operation:

- United States: 6:00 a.m. to 4:00 p.m. Pacific Time
- Latin America: 7:00 a.m. to 6:00 p.m. CST
- Europe,* Middle East, and Africa and emerging markets: 9:00 a.m. to 5:00 p.m. CET

*UK hours are 9:00 a.m. to 5:00 p.m. GMT

- Asia Pacific: English-speaking countries' support windows

600 hours (GMT +5.30) to 1600 hours (GMT +5.30)

Monday through Friday, except public holidays

No weekend support provided. Web cases can be opened on weekends and holidays; all web cases received are processed the following business day. Case initiation types are web, phone, or chat (No email as best practice).

Cisco Confidential.

Appendix C: Release Notes

The Data VLAN was modified to 192.168.10.1 to make the kit compatible as a bolt-on kit for the Cisco Smart Business Communications System UC520.

The RVS4000 was replaced with WRVS4400N to make it more flexible for use with wireless cameras.



Americas Headquarters
 Cisco Systems, Inc.
 San Jose, CA

Asia Pacific Headquarters
 Cisco Systems (USA) Pte. Ltd.
 Singapore

Europe Headquarters
 Cisco Systems International BV
 Amsterdam, The Netherlands

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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0812R)