

Mirasys VMS Networking White Paper



Table of Contents

1. Glossary of terms.....	3
2. Topology legend.....	12
3. Introduction.....	13
4. Network Requirements.....	14
5. Mirasys VMS Applications.....	18
6. Mirasys VMS communication.....	20
7. System Services.....	25
8. Mirasys VMS System components.....	28
9. Using Mirasys VMS With Different Networking Components.....	30
10. Network Connection Types.....	35
11. Mirasys VMS Bandwidth Usage.....	52
12. Solution Examples.....	80
13. ThruCast.....	89
14. Troubleshooting Network Issues.....	95
15. Networking Best Practices.....	102
16. Copyrights.....	111

1. Glossary of terms

.dhc	The file format used to export and import information and settings for a remote user connection in the VMS
API	The application programming interface is a set of programming routines, protocols, and tools for building software applications
Applet	A small, single-task application that does not require installation in any system using it
ARP	Address Resolution Protocol, a link layer protocol used to resolve network layer addresses of connected devices into link-layer addresses
Artefact	An aberration appears in an image as a result of the image being compressed with a lossy codec
AVM	Agile Virtual Matrix, a Spotter for Windows plugin where numerous security camera feeds are displayed in an array on a wall with multiple screens
b/s	Bits per Second, a measure of bandwidth. Usually prefixed with k (Kilo, $\times 10^3$), M (Mega, $\times 10^6$), G (Giga, $\times 10^9$), etc. for brevity
B-Frame	Bi-directional predictive inter-frame, a frame referencing preceding and successive I-frame and P-frame (or two P-frames) to remove unchanged regions from the image
Broadcast	Network-wide transmission of an audio or video stream
Capture Card	A hardware card used on recording servers set up as digital recorders (DVRs) to convert analogue signals into digital information
CIF	Common Intermediate Format, a video resolution format for analog cameras. 352x240 (NTSC) or 352x288px (PAL) resolution at 30000/1001 FPS frame rate

Mirasys VMS Networking White Paper

CLI	Command Line Interface, a method of interacting with a computer system through a text representation (example: MS-DOS)
Closed network	An information network of computers or other digital devices not connected to an internetwork, e.g. the Internet
Codec	Format of video compression done by a device or software that enables compression or decompression of digital video
Digital noise	random fluctuations and deviations in a digital signal
DNS	Domain Name System, a method of converting IP addresses to hostnames
Domain	A shared network of computers and the user accounts for them in a corporate environment
DoS	Denial-of-Service is a digital attack aimed at flooding a network or networked device with connection requests, drowning out legitimate requests or overloading a connected device's capabilities
Driver	A software component used to interact with hardware devices
DVRServer	VMS recording server service
Ethernet	A physical network connection standard, most commonly known as "LAN cable"
Firewall	The network security measure, screening incoming and outgoing network traffic and blocking unauthorized or harmful packets
FPS	Frames Per Second, a measure of image refresh rate
Gain	The relationship between the number of electrons acquired on an image sensor and the analogue-to-digital units that are generated represents the image signal
Gateway	An edge device between two networks, providing routing information for data traffic between the networks

Mirasys VMS Networking White Paper

GPS	Global Positioning System, a network of satellites sending data to receivers, lets the device calculate its position on the globe. Can also be used for time syncing.
GPU	Graphics Processing Unit, a processor chip specialized in calculating, generating and outputting images from data. Can be harnessed for other complex computational tasks, such as distributed computing.
GUI	Graphical User Interface, a method of interacting with a computer system through a graphical representation (example: Windows)
H.264	A video compression format. Also known as MPEG-4 Part 10. Advanced Video Coding.
H.265	A video compression format. Also, known as MPEG-H Part 2 or High-Efficiency Video Coding(HEVC), Designed to be a successor to H.264
High-Dynamic-Range Imaging	Multiple-exposure imaging method aimed at creating a recorded image with similar luminosity levels as those seen by the human eye
Hop	The action of data packets crossing between network interfaces
Hostname	Plain name of a digital device in a network
HTTP	Hypertext Transfer Protocol, an application layer Internet protocol used for sending requests from a web client (e.g. a web browser) to a web server, returning web content (web pages) from the server back to the client
HTTPS	Hypertext Transfer Protocol over TLS, an application layer Internet protocol used for sending requests from a web client (e.g. a web browser) to a web server, returning web content (web pages) from the server back to the client over TLS-secured communications

Mirasys VMS Networking White Paper

ICT	Information and Communications Technology, the term for fields relating to telecommunications and information networking
I-Frame	Intra-frame, a full image frame in a video stream
IGMP	Internet Group Management Protocol, a communications protocol used by hosts and network devices on IP networks to establish multicast group memberships
IP	Internet Protocol, an OSI Layer 3 networking protocol
IP Encoder	A hardware device that converts analogue signals into IP packets and sends them to an IP network. Can also be referred to as a video server.
IPSec	Internet Protocol Security Architecture, security suite used to secure packets between routers, forming VPN tunnels over IP networks
ISP	Internet Service Provider
IT	Information Technology, a catch-all term for fields relating to computers and other digital devices
Java	A programming language often used on websites for scripts and applets
JRE	Java Runtime Environment (JRE), part of the Java Development Kit, a set of programming tools for developing Java applications
LAN	Local Area Network, a small, usually home or office-level networked area
Layer 2	2 nd layer (Data Link) of the OSI model, transfers data between adjacent network nodes in a WAN or between nodes on the same local area network segment
Layer 3	3 rd layer (Network) of the OSI model, used for packet forwarding, including routing through intermediate routers

Mirasys VMS Networking White Paper

Load	Network traffic through or on network components, such as connections or devices
MAC address	Media Access Control address, a physical-layer identifier composed of six pairs of hexadecimal characters for network interfaces of digital devices. The first three pairs identify the device/interface manufacturer.
Managed switch	A Layer 2 networking device that can be configured through a workstation or web browser connection to manage connections on the device or information traffic going through it
Master	VMS server device with the Mirasys SMServer service installed on it
Megapixel	A million pixels. Shorthand statistic for camera resolution or image fidelity.
MJPEG	Motion-JPEG (Joint Photographic Experts Group), a video compression format
Multicast	Transmission of an audio or video stream from one computer to others selected to be the targets
Multi-channel device	A device that can send multiple signal channels, each carrying a certain number of video streams
Multistreaming	Method for a digital device to send multiple video streams with each having a different end target
NAT	Network Address Translation, translation of an internal network's IP addresses to outside IP addresses
Network	Logical structure existing between a collection of interconnected digital devices
NIC	Network Interface Controller, a computer device's LAN adapter card

Mirasys VMS Networking White Paper

NTP	Network Time Protocol, a communication protocol used to sync a networked devices time with a time server
NTSC	National Television System Committee, an analogue video standard specified for video surveillance at 525 lines per frame with a 59.94Hz refresh rate. Used in the Americas.
NVR	Network Video Recorder, networked digital device that records video feeds over an IP connection
OSI model	Open Systems Interconnection model, an abstract layered representation of a communication system
PAL	Phase Altering Line, an analogue video standard specified for video surveillance at 625 lines per frame and a 50Hz refresh rate. Used in Europe, Asia and Australia
P-Frame	Predictive inter-frame, a frame referencing a preceding I-frame to remove unchanged regions from the image
PIM	Protocol Independent Multicast, a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a TCP/IP network
PoE	Power over Ethernet, a method of powering devices through their Ethernet connection to a computer or networking device
Port	Software construct serving as a network communications endpoint for a computer or other digital device
Port forwarding	Application of NAT that redirects communications from one address and port number combination to another while the packets are traversing a network gateway
PTZ	“Pan, Tilt, Zoom,” two-axis remote-controlled camera
Quantization	A lossy compression technique is achieved by compressing a range of values to a single quantum value
RAID	Redundant Array Of Independent Disks, a method of saving data across multiple disks. RAID levels are used to categorize readiness of data integrity and redundancy

Mirasys VMS Networking White Paper

RTP	Real-time Transport Protocol, a networking protocol used for delivering audio and video over IP networks
RTP	Real-Time Protocol, a networking protocol used to
RTSP	Real-Time Streaming Protocol, a connectionless networking protocol used to control video streaming between a viewing client and a video source
RTSPS	Real-Time Streaming Protocol over TLS, a secure networking protocol used to control video streaming between a viewing client and a video source
SDP	Session Description Protocol, a format for describing streaming media initialization parameters
Slave	A recording VMS server with the Mirasys DVRServer service installed and enabled on it
SMS	Short Message Service, a telephone text messaging system
SMServer	System Manager Server, VMS master controller service
SMTP	Simple Mail Transfer Protocol, standard transfer protocol for e-mail transmissions
SNTP	Simple Network Time Protocol is a communication protocol used to sync a networked devices time with a time server. A simplified version of NTP with only a millisecond in accuracy loss
SQL	Structured Query Language, a programming language for managing data held in a database
Static IP Address	An unchanging IP address for a digital device in a network
Stream	Continuous audio or video transmission over a network
Subnet	A network segment sharing a range of IP addresses. Subnet size is represented with a prefix signifying the number of bits (most significant first) reserved for a subnet. The IPv4 prefix is 8-32 bits, IPv6 is 4-128 bits.
TCP	Transmission Control Protocol, networking protocol

Mirasys VMS Networking White Paper

ThruCast	Mirasys proprietary multistreaming method, where traffic from an IP camera can be directed to a Spotter client directly, instead of going through a recording VMS server
TLS	Transport Layer Security, formerly known as SSL (Secure Sockets Layer), is a cryptographic protocol that provides secure communication over an IP network
Tunnel	A channel that allows untouched packets of one network to be transported over another network
UDP	User Datagram Protocol, a connectionless networking protocol
Unicast	Transmission of an audio or video stream from one computer to another
Unmanaged switch	A Layer 2 networking device that can be used out-of-the-box and all connections can be considered plug-and-play. Devices like these cannot be accessed or configured remotely.
UPnP	Universal Plug and Play, is a set of networking protocols that permits networked devices to discover each other's presence on the network and establish functional network services
UPS	Uninterruptible Power Supply, a reserve power source in the event of electrical failure in a device's power cord or building power network
URL	Uniform Resource Locator, a reference to a resource that specifies its location network and a mechanism for retrieving it
VCA	Video Content Analytics, the capability of automatically analyzing video to detect and determine temporal and spatial events
VLAN	Virtual Local Access Network, a logical method of partitioning a layer-2 network by assigning Ethernet ports to virtual networks
VMD	Video Motion Detection, method of detecting motion in a video stream by comparing frames with each other; changes are logged as motion











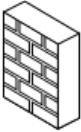
Mirasys VMS Networking White Paper

VMS	Video Management System, networked system connecting cameras, recording servers and viewing clients
VPN	Virtual Private Network, secure communication line between end devices over a larger network
WAN	Wide Area Network, geographically large networked region
WDR	Wide Dynamic Range, multiple-exposure imaging method aimed at increasing image details and eliminating dark areas
WinPcap	Windows port of the Pcap packet capture driver
Wireshark	A network monitoring application
WLAN	Wireless LAN, wireless local networking. Also known as Wi-Fi.
XMC	XMC is a database module for VMS servers. It can store data on alarms and events into a Microsoft SQL database.

[Next](#)



2. Topology legend

	Server devise with recording capability		Database (SQL)
	Server device		Smartphone
	Desktop workstation		Analogue camera
	Layer 2 switch		IP camera
	Layer 3 switch		IP camera with PTZ capability
	Firewall device/router		

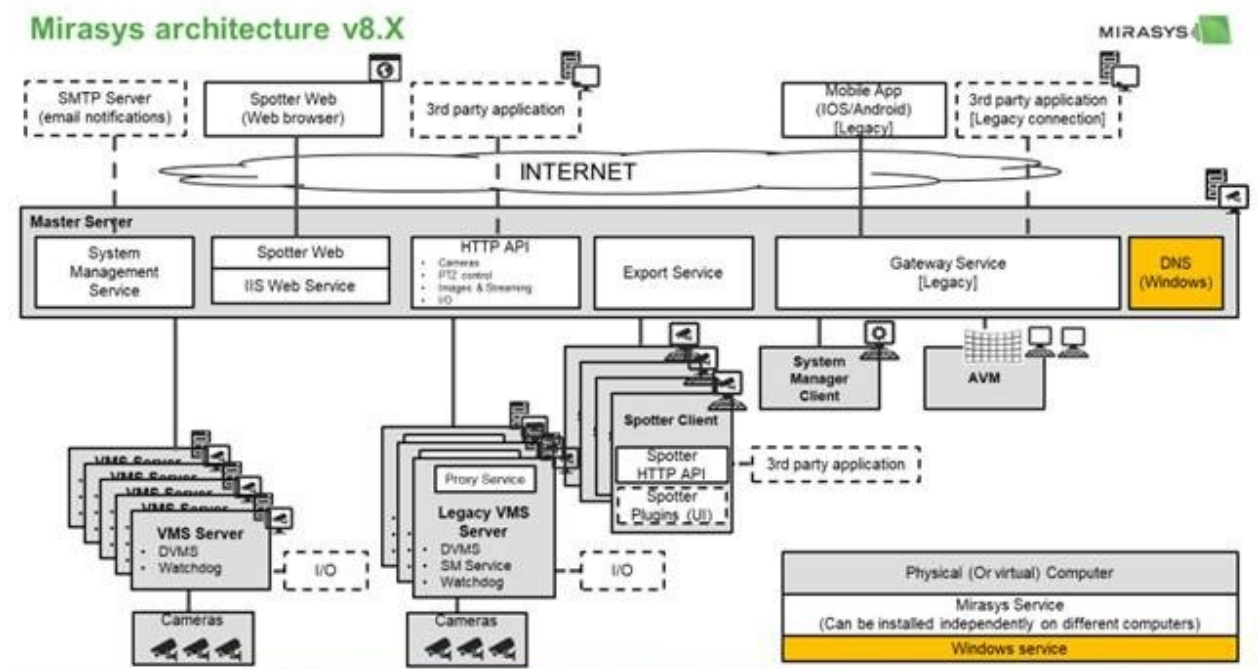
[Previous](#) [Next](#)

3. Introduction

This document contains a brief description of the network configurations used on Mirasys VMS systems and network planning considerations that need to be taken into account when planning and implementing the systems. It should be noted that this document concentrates on providing a general overview of building working surveillance systems in various network models. All data communication within the Mirasys VMS system uses TCP/IP protocol and networks.

The use of VPNs (Virtual Private Networks) and effective software or hardware firewalls is highly recommended. If a computer within the system network is used for other than surveillance purposes and is vulnerable to viruses or other harmful attacks, anti-virus protection is heavily recommended.

Building a functional and secure surveillance system requires a clear and detailed understanding of the network and its elements. If there are any uncertainties regarding the network or its elements, consulting an ICT expert, the company's internal IT department or the ISP is heavily recommended.



[Previous](#) [Next](#)

4. Network Requirements

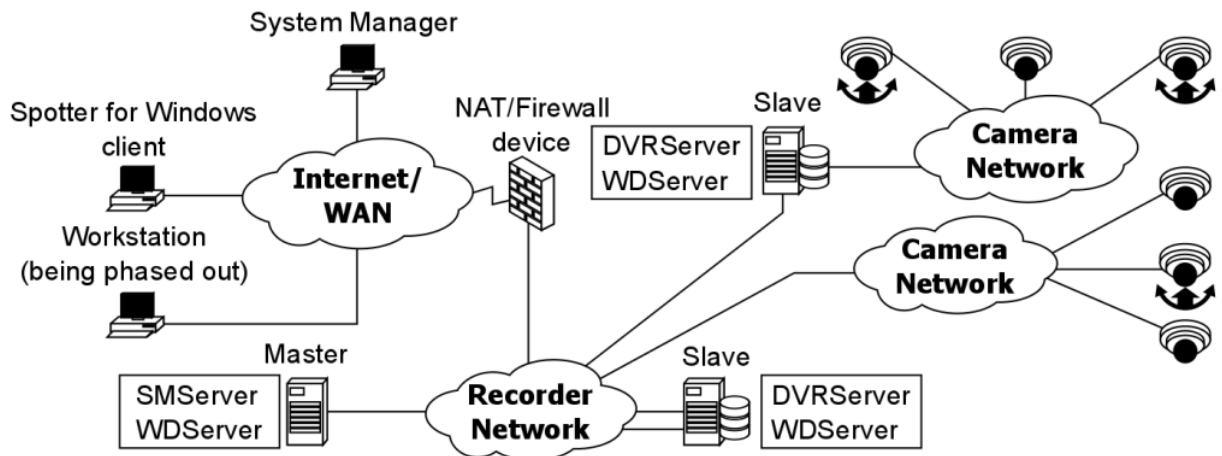
Given requirements apply to all Mirasys VMS installations.

General

Gigabit Ethernet is required on both the client and the server-side. Data can be transmitted over the Internet, or any other network using TCP/IP. It is heavily recommended to have two 1 Gb/s network adapters on each server: one for the camera connections and another for server-client and server-server communications.

In the case of large systems with multiple high resolution and high frame rate cameras, separating specific camera sets into their own networks (and adding network adapters to servers) can be recommended. However, this is done case-by-case and requires case-specific calculations on network load. Control of PTZ cameras requires the network to have low latency in order to make dome control as responsive as possible.

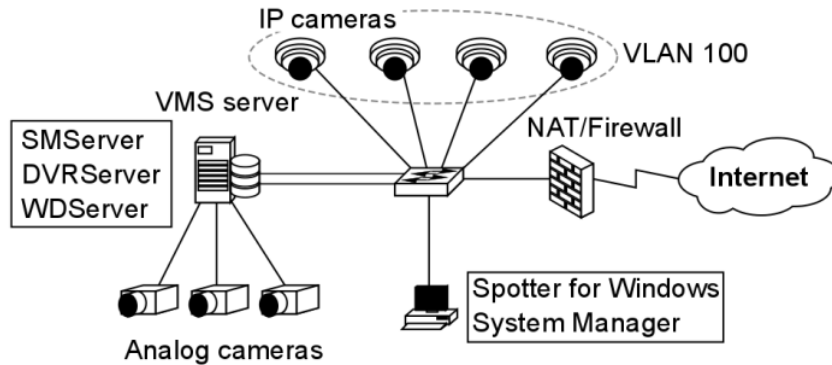
Example Network configuration:



The best practice with the system for security and network performance would be to have the cameras separated from the rest of the network. This can be done in two ways: having them physically separated or having them logically separated. Physically separating cameras would involve connecting them to their own local network switch and having the switch connect to a recording server's network adapter assigned to the camera network.

Mirasys VMS Networking White Paper

Example topology of this network principle is presented in the above network. Another method of separating the cameras in the network would be to use VLANs (Virtual LAN) on the switch to logically separate them to their own virtual network. This manner of networking should be left for smaller operators and isolated surveillance sites with their own ICT workers. VLANs are elaborated in chapter 4.5. An example of this network principle is presented below.



Camera Power

Though it is not strictly a networking issue as far as data transmission is concerned, PoE (Power over Ethernet) devices have to be considered when setting up a network. Many IP cameras that are set up today for indoor and sheltered outdoor use PoE, meaning they strain a server's or switch's power source, with each PoE-enabled port providing up to 30W of power (under 25W normally, up to 30W on PoE Plus).

PoE type/Class	Max power at source	Max power at camera w/ 100m cable	Security uses
802.3af (Class 0)	15.4	0.44 - 12.95	Indoor/outdoor
802.3af (Class 0)	4.0	0.44 - 3.84	Uncommon
802.3af (Class 0)	7.0	3.84 - 6.49	Uncommon

Mirasys VMS Networking White Paper

802.3af (Class 0)	15.4	6.49 - 12.95	Most devices
802.3at (Class 0) PoE+, High PoE	30.0	12.95 - 25.50	PTZ cameras, high-power heaters
**All power measurements are in Watts			

A 48 PoE+ port switch at full use and full power draw would be under a total demand of 1440W, though the power output of the device could be much lower. Connecting too many devices reliant on PoE to a networking device or computer may cause network or system disruptions due to having insufficient power.

Negative consequences of using too many PoE devices at a time on a PoE-providing switch or computer:

- A blown-out power supply
 - Often produces smoke and is a potential fire hazard
 - If no backup power supplies are installed, the device is disabled
- Reduced power to all devices with degraded service from all the attached devices
- Additional PoE-using devices cannot be powered
- Shorter UPS battery life. Normally a UPS can provide around 20 minutes of backup power, but PoE use can shorten this down to 3 minutes.

Keep in mind the power requirements of the cameras, whether they require their own electrical network connection or use PoE. Some additional hardware on cameras may require their own power source, e.g. dome heater, integrated IR, PTZ, etc. Consult your device documentation when handling PoE solutions.

Network Card Settings

Network card setting requirements:

- Interrupt Moderation Rate: **Extreme**
- Receive Buffers/Receive Descriptors: **2048**
- Transmit Buffers/Transmit Descriptors: **2048**

Mirasys VMS Networking White Paper

These settings must be according to the requirements, or the NIC does not function with the system. If the buffers are set to too low, it will cause issues with signalling and video transmissions. Windows updates could reset NIC settings to their defaults, so Windows updates need to be monitored and NIC settings need to be checked with every update. The necessity of installing Windows updates in a closed network should be evaluated.

In a connected network, all instances of installing Windows updates need to be performed as planned maintenance activities, as software firewall port settings might be reset along with NIC settings. NIC settings can be changed in Microsoft operating systems, such as Windows 7 and Server 2012, through the Device Manager.

The following guide is for modifying Windows 7 NIC settings, where Interrupt Moderation Rate and Buffer/Descriptors settings are concerned:

1. **Open the device manager**
 - a. Open the Start menu
 - b. Select Control Panel
 - c. Click Hardware & Sound
 - d. Click Device Manager
2. **Open the Network Card settings**
 - a. In the Device Manager, expand Network Adapters
 - b. Select the computer's physical network connection
 - i. Usually marked with "Network Connection" in the label
 - c. Right-click the selected adaptor and click Properties
3. **Edit the settings**
 - a. Open the Advanced tab
 - b. Select Interrupt Rate
 - i. Make sure the drop-down bar has "Enabled" on it
 - c. Select Interrupt Moderation Rate
 - i. Select "**Extreme**" on the drop-down bar
 - d. Scroll down and select Receive Buffers (could also be labelled Receive Descriptors)
 - i. Enter **2048** in the Value bar.
 - e. Scroll down and select Transmit Buffers (could also be labelled Transmit Descriptors)
 - i. Enter **2048** in the Value bar.

[Previous](#) [Next](#)

5. Mirasys VMS Applications

VAU

VAU (VMS Application Updater) is a service application without its own user interface.

It is used to automatically update user applications to the latest versions from the Master SMServer.

VAU is installed during the application installation, and the application is started automatically when the System Manager is run.

VAU uses the Master's IP Address or hostname to contact the SMServer (TCP port 5008).

After VAU has established a connection to the SMServer, it downloads the latest version information.

If the version information differs from the information detected during the previous application start-up, VAU downloads all needed update files.

If the downloaded version information matches the local version information, only the configuration files will be downloaded.

The configuration information includes, but is not limited to, the SMServer address which the Spotter for Windows or System Manager will contact at start-up.

After updating the version or downloading the configuration files, Spotter or System Manager will be started and VAU will close.

System Manager

When the System Manager or Spotter for Windows application is started, the user's username and password are used to download the corresponding user profile from the SMServer (TCP port 5008).

The profile data includes all information regarding the servers connected to the system and available for the user profile.

The applications access the servers through TCP port 5009. Video, audio and data streams requested through the applications use TCP port 5011.

The System Manager is the primary system management and configuration application.

It contacts SMServer and accesses information pertaining to the system. The application allows a user to add, modify and remove servers, cameras and other devices to the service, manage alarm conditions and actions, etc.

Spotter For Windows

Spotter for Windows is the primary desktop monitoring application.

A Spotter client contacts the SMServer and accesses the devices connected to it running DVRServer.

Through this, it accesses live and recorded surveillance data. A spotter can be used as a specialized video wall application, as well.

Currently, only one instance of the SMServer service at a time can be accessed by the Spotter for Windows application.

More information on the System Manager can be found in the Mirasys VMS 7.3 - Spotter User Guide documentation.

WebClient & Spotter Mobile

The WebClient applet can be used on any web browser from any computer on the Internet, but Java needs to be enabled.

If the GatewayServer server application is installed with the default values, TCP ports 9999 and 9000 must be open between the WebClient browser computer and the GatewayServer server computer.

The default ports can be changed during the GatewayServer installation or at a later point by editing the ServiceLauncher.exe.config configuration file in the service's installation folder (default C:\Program Files\DVMS\Gateway).

[Previous](#) [Next](#)

6. Mirasys VMS communication

Mirasys VMS system components can be divided into applications and servers. Applications are used to open communication with and between the system's servers, and to send connection requests to servers. Meanwhile, servers accept connection requests from applications or from other servers.

Communication between the system components is implemented with TCP/IP protocol through TCP ports 5008-5011.

Signaling And Streaming Protocols

UDP (User Datagram Protocol) is a transport-layer protocol used to stream the video feeds from the connected cameras. The protocol is connectionless and lightweight, so it is often used to discover connectivity issues in a network. In the VMS, any connection difficulty is immediately noticed as a loss in the video feed. For streaming to function properly, the network for the system needs to be well constructed and the connections need to be reliable.

UDP

UDP (User Datagram Protocol) is a transport-layer protocol used to stream the video feeds from the connected cameras. The protocol is connectionless and lightweight, so it is often used to discover connectivity issues in a network. In the VMS, any connection difficulty is immediately noticed as a loss in the video feed. For streaming to function properly, the network for the system needs to be well constructed and the connections need to be reliable.

RTSP

RTSP (Real-Time Streaming Protocol) is used to control video streams over a network. RTSP communications between a client and a recording VMS server send instructions on playback and play speed. As with UDP, RTSP is a stateless communication protocol that requires a solid network to function reliably. Usually, the interaction between VMS and camera goes in the following order:

VMS sends DESCRIBE request to camera

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com

Mirasys VMS Networking White Paper

Camera answers with DESCRIBE response contain information about supported video/audio streams in SDP (Session Description Protocol) format

VMS sends SETUP request to camera

Camera answers with SETUP response needed to create a new RTSP session for a specific stream

VMS sends PLAY request to camera

Camera answer with PLAY response after this camera starts video/audio sending to VMS – usually, RTP (Real-Time Protocol) over UDP protocol is used for data sending

Periodically VMS sends KEEPALIVE request – if no camera stops video stream sending

VMS sends TEARDOWN request when video should be stopped

RTSPS

RTSPS (Real-Time Streaming Protocol over TLS) is a secure version of RTSP, similar to how HTTPS is a secure version of HTTP. The protocol uses TLS (Transport Layer Security) to secure communications, requiring a stable connection for TCP traffic.

TCP

TCP (Transfer Control Protocol) is used for signalling between the devices and components of the VMS network and the Internet at large.

TCP is an ordered, error-checked and reliable signalling protocol that can function even if there are some minor faults in the network, at the cost of latency.

HTTP

HTTP (Hypertext Transfer Protocol) is used to communicate control signals for IP cameras in the system. Many drivers use HTTP/HTTPS for setting and retrieving parameters to/from the cameras. In a direct connection, a user contacts the camera GUI with HTTP/HTTPS. Some drivers may also use HTTP to receive motion detection data and video streams. Some camera drivers traffic PTZ signalling through HTTP.

HTTPS

Mirasys VMS Networking White Paper

HTTPS (Hypertext Transfer Protocol over TLS) is a secure version of HTTP. The protocol uses TLS to secure communications.

Mirasys VMS Ports

In all VMS installations, the following TCP ports must be open on all servers for the applications and servers to function correctly:

Port **53**

The default port for DNS service (Required by Mirasys VMS 8.5 and newer versions)

Port **5008**

For signalling between SMServer and client applications, and inbound communications from clients to the SMServer

Port rule: open inbound

Port **5009**

For remote connecting between DVRServer and client applications, and signalling between SMServer and DVRServer for time synchronization, settings changes, event information, etc.

Port rule: open inbound

Port **5010**

For Watchdog monitoring communication between WDServer, client applications and DVRServer

Port rule: open inbound

Port **5011**

For streaming between the Streaming Service and client applications

Port rule: open inbound

Optional ports:

IP cameras and auxiliary devices may need specific ports opened. Please refer to device-specific documentation for instructions.

WebClient, Spotter Mobile and GatewayServer specific ports

Mirasys VMS Networking White Paper

Ports **9000** and **9999**

Between WebClient/Spotter Mobile and GatewayServer.

Port rule: open inbound

AVM specific ports

Port **8084**

Between SMServer and the Spotter for Windows client

Port rule: open inbound

IP Camera Ports

Cameras use their own ports to keep contact with the VMS and transmit data to the recording servers.

Please refer to device-specific documentation for instructions.

If there are firewalls between the cameras and recording VMS servers running DVRServer, the relevant ports need to be open through the firewall.

HTTP

Port **80**

The default port for HTTP traffic used to communicate with a camera's system

Port **8080**

Used by some cameras for PTZ control communications

HTTPS

Port **443**

The default port for HTTPS traffic used to securely communicate with a camera's system

RTSP

Port **554**

The default port used on the VMS to traffic stream control signals

Port **7070**

Default stream control port for some camera drivers

Mirasys VMS Networking White Paper

UDP

Port **53**

The default port for DNS service (Required by Mirasys VMS 8.5 and newer versions)

Ports **3556-4556**

Used on the VMS to receive feeds from the cameras. Each video stream occupies two sequential ports in the port range. To verify device port use, reading of device manufacturer driver read me files is highly recommended.

[Top](#) [Previous](#) [Next](#)

[Previous](#) [Next](#)

7. System Services

System Services

SMServer

SMServer (System Management Server) is the Master server service. SMServer is used to assign a server in the system as a Master that acts as the focal point in communicating with the client applications and the other servers in the system.

A VMS must have a server assigned as a Master with SMServer on it connected to the system network.

SMServer listens on TCP port 5008 for the client applications. SMServer uses TCP port 5009 to connect to the system network's other servers for time synchronization, settings changes, receiving event information etc. The service maintains the system state and system data, e.g. server information, system clock, users and profiles. SMServer maintains connections to all the watchdog services in the system and receives and logs monitoring events. Upgrading the system servers and clients is done through SMServer. Alarm events and the audit trail are recorded in the server database. In larger environments, a SQL Server database can be used to store alarm and audit trail databases.

Audit trails record user activities in the system. A Master server with SMServer can support up to 150 recording VMS servers that are referred to as Slaves. A Slave can be any server device with the DVRServer service installed and enabled. The service must be installed on a computer or server with Microsoft operating systems Windows 10, Windows 11, Server 2012, Server 2016 R2 or Server 2019. The device can also be a virtual device running in Hyper-V and VMware virtual machine platforms.

DVRServer

DVRServer is the service installed on servers set up as recording devices in the VMS network.

This sets them up to store video data sent by the cameras. They receive footage and save it on their hard drives with metadata saved on the common database.

Mirasys VMS Networking White Paper

The servers also perform VCA, motion detection and send out alarms, should pre-defined criteria for such be fulfilled. Servers with DVRServer require two NICs on their hardware: one to communicate with IP camera networks, the other for server-server/server-client communication. Devices meant to capture footage from analogue cameras need to have capture cards installed or instead receive traffic from an IP encoder with the analogue cameras connected to it. It is advisable to keep IP cameras on a separate network from the recording servers and the only cameras directly connected to the recording servers are analogue cameras connected to said servers' capture cards. DVRServer listens on TCP port 5009. Video, audio and data streams require TCP port 5011 to be open. DVRServer never contacts the applications (Spotter for Windows and System Manager) or SMServer. However, if IP cameras are installed in the system, servers contact the IP cameras using TCP or UDP depending on the camera model. The service must be installed on a computer or server with Microsoft operating systems Windows 10, Windows 11, Server 2012, Server 20016 R2 or Server 2019. The device can also be a virtual device running in Hyper-V and VMware virtual machine platforms.

WDServer

WDServer is the Watchdog server service that functions as the system monitor. It monitors local DVRServer and SMServer services and is responsible for seeing that both services are running and operating normally.

During normal monitoring, it will save events to a local event buffer (max. 100 individual events).

These events can be used to trigger digital outputs in DVRServer. WDServer can also be configured to send emails.

Even if neither is configured, WDServer will always log the events in a log .txt file, with C:\Users\[Window user]\AppData\Roaming\DVMS\DVR Application\Logs folder being the default.

In severe situations such as a system malfunction or hard drive failure, Watchdog can do a number of preset tasks, e.g. restart the affected computer or send e-mail messages containing information about the malfunction.

If the system Master is down, the error situations will be notified once the SMServer service is up again.

Error situations will not cause the watchdog to initiate a rebooting loop.

Any reboots by WDServer will be followed by changing the faulty component to an error-tolerant state (e.g., disabling a faulty channel).

Mirasys VMS Networking White Paper

Rebooting will never be done more than once per 6-hour cycle.

If other faults or errors normally resulting in a reboot occur, these will be logged but not acted upon.

WDServer is automatically installed with SMServer and DVRServer.

WDServer takes care of the connections and operational reliability of the VMS system through TCP port 5010.

The Watchdog records GatewayServer and SMS service up/down events if they're installed on the same device as the Watchdog. If these services go down, the application restarts them.

The service must be installed on a computer or server with Microsoft operating systems Windows 10, Windows 11, Server 2012, Server 2016 R2 or Server 2019. The device can also be a virtual device running in Hyper-V and VMware virtual machine platforms.

GatewayServer

The optional GatewayServer service must be installed on a computer with Microsoft Windows 7, Server 2008, Server 2008 R2 or Server 2012 operating systems.

The computer must have HTTP software installed. Mirasys VMS software is not required on the server.

The GatewayServer contacts the SMServer through TCP port 5008.

When the WebClient Java applet or the Spotter Mobile application is used, GatewayServer and the applet or application communicate by default through TCP ports 9999 (download applet) and 9000 (direct communication between the server and the applet/application).

These TCP ports can be changed during the GatewayServer installation or at a later point by editing the ServiceLauncher.exe.config configuration file in the service's installation folder (default C:\Program Files\DVMS\Gateway).

[Previous](#) [Next](#)

8. Mirasys VMS System components

System servers

Servers are devices configured to perform tasks and play specialized roles for a networked system. These devices are usually desktop computers or specialized computer hardware that can be placed in server racks, but they can also be virtual devices running within another computer's programs. They often run operating systems or software that maximizes their performance in their tasks. In the VMS, servers are devices that run Mirasys server services that form the basis of the system. Actual server hardware requires little specialization, with the exception of devices meant to run DVRServer requiring two NICs and lots of digital storage space.

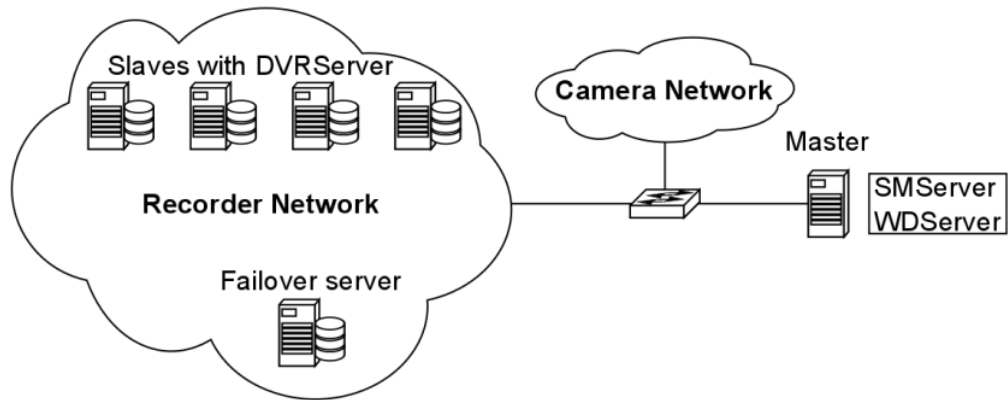
Note that the 8.5 and newer versions of Mirasys VMS also need a DNS (Domain Name Service) server to work properly. It's used for hostname searches during the logins with client software, and with connections between servers.

Failover servers

Mirasys VMS 7.0 and later releases support failover servers. Failover servers are networked devices that are on a passive standby until the system recognizes that one of the active Slave servers has broken down; at this point, a failover server takes the place of the failed server. The failed server can be repaired and replaced as a new failover server, while the failover server that took its place can continue operating as an active server. Currently, only Slave servers can be placed under failover protection, as Failover Server is not yet configured to replace failed Masters running SMServer.



Mirasys VMS Networking White Paper



Failover servers expected to function as recording Slave servers must have the same file system (same drive letters) as the Slaves under failover protection, and they can only be used for IP camera backup purposes. When in standby mode the failover servers appear under a separate folder in the server list. When any Slave is deemed to be broken or inaccessible, they are moved under the “broken recorders” folder and any available failover server takes on the responsibilities of the broken Slave. Failover settings can be controlled from the general settings of the Slave. The failover transition is done if all material disks on the affected recording server are broken or the Slave is inaccessible for longer than a user-defined period of time.

Note: When a failover server is taking the place of an active server, any Spotter plugins (such as the ANPR+ license plate recognition software or Activity Map Plugins) are not included in the failover switch and must be re-installed manually after a server restore. Contact Mirasys for more information on failover functionality and licensing.

[Previous](#) [Next](#)

9. Using Mirasys VMS With Different Networking Components

When building a Mirasys VMS system, usability, security issues and the need to contact system components outside of surveillance sites are extremely important factors to be considered. When contacting the system with a System Manager application from outside of a closed network, a VPN (Virtual Private Network) or an effective firewall are good alternatives.

IP Addressing

Devices communicating over an IP network identify each other through their IP addresses.

An IP address is a unique identifier on a given network that signifies a networking device's interface.

Addresses within a closed network are arbitrary, but larger networks have addresses that are either in constant use or are reserved for an organizational entity's use. An IP address is made of a group of octets and a subnet mask.

IPv4 addresses use four octets (groups of eight bits, so 32 bits), some of which are reserved to indicate the network a host is in, and the non-reserved bits are used by the host.

An IPv4 address format allows addresses from 0.0.0.0 to 255.255.255.255, and the subnet is indicated by a prefix /N, where N indicates the number of bits reserved for the network portion of the address, ranging 8-32. The subnet mask is an expanded presentation of the prefix and can range from 255.255.255.255 to 255.0.0.0.

The smaller the number on the subnet mask, the more hosts are allowed on its network.

In a subnet, the first address (e.g. 192.168.1.0/24) is always the network address and the last address (e.g. 192.168.1.255/24) is the broadcast address.

All addresses between these can be assigned to hosts, e.g. in a /24 subnet, the final octet for a host's address ranges from 1 to 254.

IPv6 addresses use sixteen octets in eight hexadecimal pairs (total of 128 bits), with some reserved to indicate a host's network.

The address format allows addresses from 0::0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, with

Mirasys VMS Networking White Paper

any octet pairs marked as 0 between other pairs omitted in a written address. The subnet is prefixed /N, where N indicates the number of bits reserved for the network portion of the address, ranging from 4-to 128

The subnet is marked with the octet pairs included in the networking segment followed by the prefix. e.g. the subnet for address 200f:0db8:ab00:0000:0000:000:4567:8901/48 (written 200f:0db8:ab00::4567:8901), has a subnet notation of 200f:0db8:ab00::/48.

IPv6 is meant to counteract Internet address exhaustion, as it allows 2^{128} (c. $3,40 \times 10^{38}$) addresses, significantly more than the 2^{32} ($4,3 \times 10^9$) in IPv4. However, networked monitoring systems are usually smaller and closed to other network traffic either through physical isolation or address translation, so IPv4 is used for ease and simplicity of configuration and use without fear of address exhaustion.

IP addresses are also classed to make their subnetting easier. In general, the relationship between potential unique addresses in a network, and the total potential number of unique sub-networks supported is a decision well beyond a surveillance system.

The three most common network classes are limited as follows:

Class A ranges from 0.0.0.0/8 to 127.255.255.255/8

- The first octet is reserved for subnets (NNNN.HHHH.HHHH.HHHH)
- 128 subnets of 16 777 214 host addresses

Class B ranges from 128.0.0.0/16 to 191.255.255.255/16

- The first two octets are reserved for subnets (NNNN.NNNN.HHHH.HHHH)
- 16 384 subnets of 65 534 host addresses

Class C ranges from 192.0.0.0/24 to 223.255.255.255/24

- The first three octets reserved for subnets (NNNN.NNNN.NNNN.HHHH)
- 2 097 152 subnets of 254 host addresses.

IP addresses or Hostnames for the older versions of Mirasys VMS

The system can be configured to contact the servers through their IP address or hostname. in the new versions of Mirasys VMS (8.5 and further), only hostnames are

Mirasys VMS Networking White Paper

used.

the servers must have static IP addresses configured for their network connections so that the client programs can connect to them. Any servers set up to function as AVM Display Servers in the system should also have either static addresses or static hostnames, as the connection from the AVM operator console to the display servers is done with either the IP address or the hostname.

While servers and the AVM must have static addresses, clients with the network can be addressed with DHCP (Dynamic Host Configuration Protocol). DHCP servers are configured to provide a set pool of IP addresses, which are reserved by connected devices every time they restart. Addresses are given out on a first-come-first-serve basis. DHCP servers can also be set to reserve specific addresses for specific devices. Cameras should also be statically addressed, and DHCP should be used only when establishing the first connection for initial configuration. Some camera models can support zero-configuration, where a camera directly connected to a computer generates random IP addresses in the 169.254.0.0 /16 network for both devices. This allows for an initial condition for a connection through which the camera can be configured. Consult the documentation for IP cameras to see if they support this feature.

If the system is intended to be used from outside a closed network, it is recommended to build the system using server hostnames instead of IP Addresses. This makes it possible to contact the system from outside the local network with minimal effort. Please refer to the *Mirasys VMS System Administrator's Guide* for further information on setting the server hostnames through the System Manager application.

Even if the system uses public IP Addresses, is run on a closed network, or is used through VPN, using hostnames instead of IP addresses for the system components can enhance user-friendliness and general usability.

Public IP Addresses

When using public IP Addresses with the Spotter for Windows and System Manager applications outside the local network, an IP address is required for each DVRServer and for the SMServer. Local networks can use a private network subnet and assign addresses for devices in it to facilitate contact between them. But these internal addresses are not congruent in a WAN environment, so public IP addresses are used on the outside of the local network to contact the devices therein. Network edge devices, such as routers between the local network and WAN, use NAT

Mirasys VMS Networking White Paper

(Network Address Translation) to translate public addresses (WAN) to private addresses (LAN) and vice versa. Routers that run NAT take addresses on the local network (Inside) and assign WAN/Internet (Global) IP addresses to the traffic. As far as the end-user is concerned, NAT is primarily performed in two ways by routers:

- **NAT Pools**, where a segment of addresses is reserved and they are dynamically given to connecting inside devices on a first-come-first-serve basis for translation
- **Static NAT**, where an inside address is statically translated to a specific global address by the server.

A more secure and efficient method of using a limited number of public IP Addresses in the system is by using the WebClient application. By providing a public IP for the GatewayServer, it is possible to access cameras in real-time and playback modes through a Java-enabled browser, the Spotter Mobile application, or custom applications based on the Gateway SDK (Software Development Kit).

Private IP Addresses

Portions of the 172.0.0.0 and 192.0.0.0 address ranges are designated for private networks. The remaining addresses are public, and routable on the global Internet. Private networks can use IP addresses anywhere in the presented networks:

192.168.0.0/24 - 192.168.255.0/24

Class C networks, allowing 256 addresses per subnet (including network and broadcast addresses).

All subnets have the /24 prefix.

172.16.0.0/16 - 172.31.0.0/16

Class B networks, allowing 65 536 addresses per subnet (including network and broadcast addresses).

All subnets have the /16 prefix.

10.0.0.0/8 - 10.255.255.255/8

Class A network, allowing a single 16 777 215 address subnet (including network and broadcast addresses).

The subnet has the /8 prefix.

192.168.0.0/24 is the most popular private network subnet type in use, as most private subnets usually have up to 254 hosts in each, network segmentation is easy

Mirasys VMS Networking White Paper

to plan and configure, and /24 subnets can be segmented into even smaller subnets as needed.

DNS For the newer versions of Mirasys VMS

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

It translates more readily memorized hostnames to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses and vice versa.

In the Mirasys VMS 8.5 and newer, the system is configured to contact the servers through hostname with the help of DNS.

This is because hostname allows the use of certificates in the VMS servers, which allows the VMS system to be protected better.

You must have a working and reachable DNS server at your disposal.

All the Mirasys servers (master, slave, AVM etc.), their hostnames and IP Addresses must be added to the DNS server configuration.

In case you don't have any DNS servers available, there's an option to install a DNS server from the Mirasys installation package.

It's recommended to be used only with Windows 7 or 10 installations, Windows server installations have a built-in DNS server available.

Clients or cameras do not have to be added to the DNS. Cameras should have a static IP address, and DHCP or static IP addresses can be used with the clients.

You can optionally use DNS service and hostnames for older versions of Mirasys VMS (7 through 8.3.1) too, though IP addresses are used by default.

[Previous Next](#)

10. Network Connection Types

Local Connections

Today most local network connections are with the use of switches, while hubs were an inexpensive way of connecting devices. Layer 2 switches offer direct networking with a small number of devices through their MAC addresses. Layer 3 switches are a step up the ladder and offer expanded capabilities.

Routers are also Layer 3 devices, but their use is more relevant on the LAN/WAN border and they function as default gateways for the devices in the local network they're connected to.

Hubs are an older form of local connection technology and are on the way out. Hubs do not inspect the packets they receive and broadcast them to all other ports and the devices connected to them.

The use of hubs is discouraged, the use of switches is recommended. Layer 2 switches can be managed or unmanaged. Unmanaged switches are used to connect a limited number of devices to each other or to a network core. Managed switches allow users to configure VLANs and set up monitoring and alerts. Layer 3 switches have the same capabilities and can additionally route IP traffic between VLANs.

Physical local connections over Ethernet wires should not exceed the usual maximum of 100m.

Wireless Connections

The use of wireless cameras or wireless switches, bridges or routers as a part of the VMS or its network is **strongly discouraged** due to the cameras' security concerns and uncertain connection reliability of WLAN. All VMS connections should be made with physical cables.

Closed Networks

The most secure way for a surveillance system to be built is to use a dedicated self-contained network that does not have connections to the outside. The simplest model of this would be to have the system devices connected to an unmanaged Layer 2 switch.

Mirasys VMS Networking White Paper

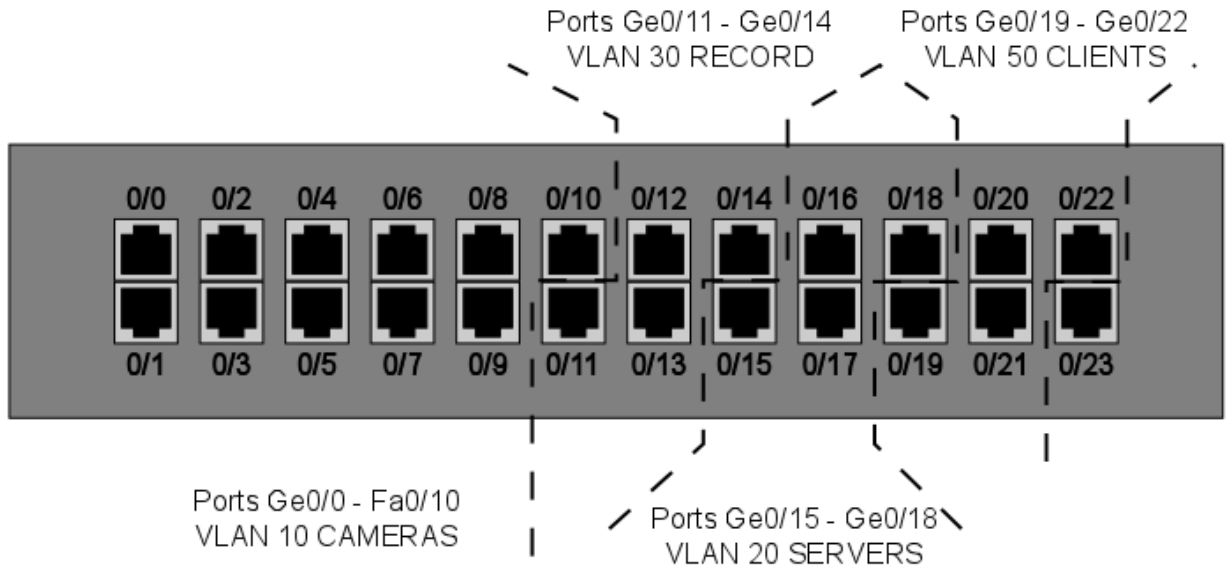
However, being disconnected may not be feasible or desirable in all cases, if e-mail alerts are to be used in the system or if Internet access is required for user activities.

VLANs

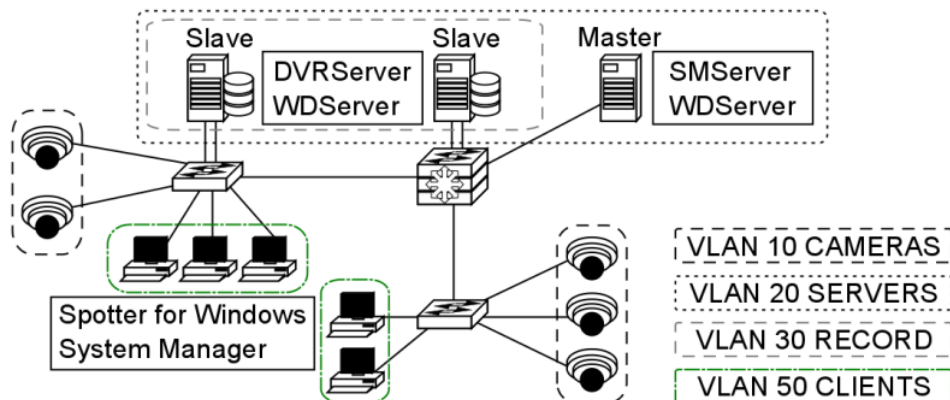
VLANs (Virtual LANs) are a method of logically segmenting a local network between different components of the system. VLANs are configured on switches to segment the device's ports for enhanced data traffic control. Setting up a VLAN is an alternative to setting up physical segmentation for a network. It is recommended that you consult an ICT expert or your IT department before planning and configuring VLANs on your VMS network's networking devices. Layer 2 switches forward data based on device MAC addresses, and any VLANs configured on the switch would shunt data from certain ports to named trunk ports. This can be used in isolating the camera network to communicate with only a VMS server's network card. Any VLANs configured on a Layer 2 switch cannot communicate between each other without the device being connected to a Layer 3 network device and the VLANs trunked to it through the interface connecting it. Layer 3 switches with IP routing can support multiple VLANs that can communicate between each other, as data is routed based on target IP addresses. Each VLAN could also be in charge of its own subnet, and IP addresses need to be assigned for them. One example of a VLAN setup in the VMS would have (if all system devices are ultimately connected to the same Layer 3 switch) a VLAN for the camera network, a VLAN for the recorder network's camera network NICs, a VLAN for the recorder network's server-server/server-client network NICs along with the SMServer's NIC and a VLAN for local computers running Spotter for Windows and System Manager. Ports should be reserved for these purposes as needed. Layer 2 switches can be used to allow more devices to be connected to the network, as long as these are connected to the VLAN-configured ports.



Mirasys VMS Networking White Paper



VLANs can be used across multiple switches. Having multiple VLANs in the network will necessitate having routing capabilities in the network in order to route IP packets between the VLANs. This can be done with a Layer 3 switch, a router or with router-on-a-stick, where you have a routing device with a single LAN connection to the Layer 2 switch. The device routes between the VLANs, allowing traffic between them. With VLAN segregation, the exact physical location of each system device is largely irrelevant to the network. To the network, VLANs are their own local networks that the router routes traffic between. With multiple VLANs, each device needs to have an IP address configured, so the Layer 3 device can route the traffic between them.



Inter-VLAN routing requires configuring the Layer 3 switch and enabling routing on it. Specific actions and commands are dependent on the manufacturer of the device, but usually, the procedure is as follows:

Mirasys VMS Networking White Paper

1. Enable IP routing
2. Assign addresses to the VLANs (e.g. VLAN 10 would have 192.168.10.1/24)
 - o These will be the default gateways for the end devices in the VLANs
3. Configure a default route for the switch

QoS

Quality of Service is a set of strategies usually standardized with network device manufacturers.

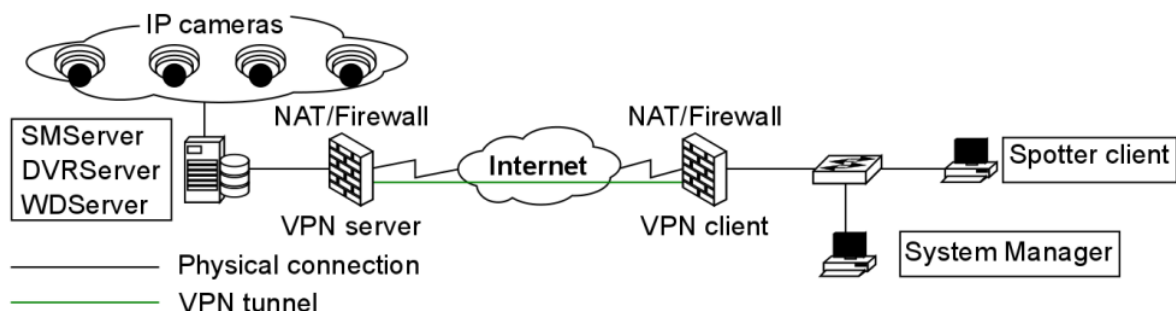
QoS is used to ensure a certain standard of quality in the transmissions configured on a managed device that is serving as a part of a shared network. When QoS is configured on VLANs, it prioritizes their bandwidth so it is not as readily consumed by other traffic and that the information going through switches does not degrade.

While QoS can be used with any application connection or by users, using it with VLANs is easier to manage and configure. QoS is generally not needed on dedicated networks, as there's no need to prioritize the traffic the network is dedicated to transmitting. In larger, shared networks, however, it becomes vital in preventing performance fluctuations.

Virtual Private Network (VPN)

VPN (Virtual Private Network) can be used to establish secure connections between two or more LANs or to have a well-protected point-to-point connection over the Internet.

VPN uses encryption and authentication protocols preventing unknown computers from accessing data delivered between two or more local network sites.



VPN tunnels for LAN-to-LAN connections can be created using hardware-to-hardware connections, usually with routers that can be used as firewalls or dedicated VPN devices.

Mirasys VMS Networking White Paper

VPN tunnels for point-to-point connections are typically created with the combination of a hardware firewall functioning as a VPN server and software VPN client connections. After VPN is configured, Mirasys VMS can be installed and used as if it were in a closed network. Do note that the use of a VPN connection might reduce available bandwidth and consume other resources used by the VMS, which may have a negative impact on the performance of the system or its network. A data packet can have an MTU (Maximal Transmission Unit) size of 1500 bytes (12 kilobits) before it's fragmented by a Layer 3 device for delivery over IP networks. VPN adds additional information to the packet header, so the packet is fragmented. This fragmentation could lead to packets arriving in the wrong order and not playing the video properly on some end applications. It is recommended to set the cameras in the system to have their TCP and UDP MTUs set to 1300 bytes.

VPN Methods

VPNs can be set up with a certain variety of methods afforded by the ICT networking industry.

Routers can be set up to create Layer 3 VPN tunnels between them, connecting large sites to each other, a site can have dedicated hardware for VPNs or a server can be configured through software settings to manage VPN tunnels. It is recommended to consult an ICT expert or your IT department for in-depth details on how to set up VPNs and what type of solution is best.

Layer 2 Tunneling Protocol

L2TP (Layer 2 Tunneling Protocol) is a tunnelling protocol used to support VPNs. The protocol itself doesn't provide any encryption or data confidentiality but relies on an encryption protocol that it passes within the tunnel to provide privacy. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination is generally known as L2TP/IPsec. When a VPN connection has been established in an L2TP/IPsec VPN tunnel, L2TP packets are encapsulated by IPsec, so no data about the private network can be ascertained from the secured packets. Also, it is not necessary to open UDP port 1701 on firewalls between the tunnel endpoints, since the secured packets are not acted upon until after IPsec data has been decrypted and stripped at the endpoints. L2TP allows the creation of a VPDN (Virtual Private Dialup Network) to connect

Mirasys VMS Networking White Paper

remote clients to their corporate network by using a shared infrastructure, such as the Internet or the ISP WAN. Desktops and laptops using Microsoft Windows Vista and later operating systems can form remote L2TP VPN connections with a private network. A short setup guide example is presented in chapter 4.6.3.

Layer 3 VPNs

VPN tunnelling between Layer 3 devices is used to connect LANs with each other. This is commonly done between routers connected to a WAN such as the Internet.

Routers and routing hardware firewalls (e.g. Cisco ASA or SonicWall devices) can maintain IPSec VPNs between each other over the Internet.

VPN concentrators

VPN concentrators are networking devices specialized in providing secure VPN connections and message delivery between VPN nodes. Its capabilities are realized by adding data and network security to communications that it routes. It is meant to create and manage a large number of individual VPN tunnels.

A VPN concentrator is typically used for creating site-to-site VPN connections. Their tasks include:

- Establishing and configuring VPN tunnels
- Authentication of users
- Assigning tunnel/IP addresses to users
- Encryption and decryption of data
- Insurance of end-to-end data delivery

VPN Servers

VPN servers come in two general types: hardware servers and software-based servers.

Hardware VPNs are purpose-built networking devices that connect to an Internet connection from within a service site and provide improved VPN capabilities when compared to application-based servers. Usually, these devices can support multiple simultaneous connections. Servers are normally managed through web browsers contacting their IP addresses. Software-based VPN servers can be made from stripped-down or bare-bones desktop computers with the appropriate VPN software application or server operating system installed and network connections configured. There are

Mirasys VMS Networking White Paper

numerous applications available through a myriad of providers that can form a stand-alone VPN server on a desktop/server operating system environment. Some server operating systems come with built-in capabilities to function as VPN servers. The number of supported connections depends on the running server software and the number of ports on the computer's NICs.

NOTE: *some VPN server applications may be incompatible with other VPN standards.*

Configuring A VPN

When the Mirasys VMS system is used with VPN, tunnels are created between the system's servers with DVRServer, SMServer, and client applications. An easy way to use VPN is to create a network-to-network connection between sites. The recording servers should be on the VPN server's network, and the clients on the VPN client's network, as DVRServer, does not automatically send data to the applications.

All data connections are initiated by the client applications. The following points are quick guidelines on how to use VPN with the VMS. To have more comprehensive instructions, it is advised to consult an ICT expert and VPN software/hardware documentation.

To use VPN:

- Create a VPN tunnel for the local network where the Mirasys VMS system is located. This is configured on a VPN server.
- Create a similar tunnel on the client site-local network (Spotter for Windows/System Manager).
- Select a VPN model that allows for a continuous connection.
- Test the connection. Once connections are viable, start configuring the Mirasys VMS system.

Example Of Setting Up A VPN Remote Connection

Devices using Microsoft Windows can form L2TP VPN connections to private networks without the express need of a separate gateway. The remote user contacts the Layer 3 device on the private network to establish a secure line of communication over a WAN, such as the Internet. A Windows 7 user would go through the following steps to establish a VPN connection between their computer and a Layer 3 device:

1. Open the Start Menu and type "VPN" in the search box

Mirasys VMS Networking White Paper

2. Click the "Set up a virtual private network (VPN) connection" icon to open the VPN creation window
3. Enter the server information
 - a. Type the VPN server hostname in the "Internet address" field
 - b. Type the name of your VPN destination in the "Destination Name" field
 - c. Check the "Don't connect now; just set it up so I can connect later" box
 - d. Click "Next"
4. Enter your VPN account username and password in the appropriate fields and click "Create"
5. Open the Network and Sharing Center from the Start Menu by searching Network in the search box
6. Click "Connect to a network," a list of VPNs pops up.
7. Right-click on the VPN connection you just created and choose "Properties"
 - a. Click on the "Type of VPN" pop up menu and select "L2TP/IPSec"
 - b. Click on the "Advanced Settings" button.
8. In the "IPSec Settings" dialogue, click the radio button labelled "Use preshared key for authentication"
 - a. Enter the key to the VPN into the textbox labelled "Key"
 - b. Click the "OK"
9. In the VPN connection properties, open the "Networking" tab
 - a. Make sure the "Internet Protocol Version 4(TCP/IPv4)" and "Client for Microsoft Networks" items are checked
 - b. If other protocols are checked, uncheck them by clicking on the checkbox.
10. Click "OK" to finish, then connect to the VPN server by this connection

DynDNS

Dynamic DNS (Domain Name System) services resolve IP addresses to simpler hostnames, e.g. recorder.DynDNS.xx instead of 127.0.0.1. The DynDNS service updates the IP addresses corresponding to each hostname periodically or in some cases automatically detects changes and updates immediately.

DynDNS is most commonly used with recording servers and cameras. Many manufacturers host their own private DynDNS services free to users who purchase their equipment.

Domain

Mirasys VMS Networking White Paper

Building a Mirasys VMS system in a domain does not significantly differ from working with other networks. In a domain, only administrative users can install the server software and the client applications. User rights policies can be used to restrict or permit user access to the client applications.

In a domain, all computers are named, and the VMS servers can be named according to the domain infrastructure. Static IP Addresses are to be used with the devices running DVRServer and the SMServer.

SQL Databases

SQL databases refer to shared relational databases in a local network that uses the SQL (Structured Query Language) programming language. In larger setups of the VMS, the SQL database is handled by the SMServer and client applications receive information from it whether or not there's a database in use. In smaller VMS environments, VMS servers running DVRServer are responsible for alarm event data storage.

SQL databases are used in the system to store:

- DVRServer metadata
- Watchdog events on the SMServer
- With the XMC (eXtended Monitoring Center) license
- Audit trails
- The recording servers' alarm events
- Alarm configurations
- Alarm occurrences
- Alarm edits/changes

Virtual Machine Network Traffic Routing

Virtual machines can have two IP addresses simulating two NICs: "inside" (host-only) IP addresses and "outside" addresses that are seen by the local network. The purpose of a virtual machine host is to essentially simulate a network segment and device collection.



Mirasys VMS Networking White Paper



Machines on the same VLAN on the same switch can communicate with each other. Machines on different VLANs on the same switch cannot communicate unless the traffic passes through a Layer 3 device (router or Layer 3 switch). **Note:** some virtual machine mediums have a cap on the number of virtual machines that can be configured for a single host.

VMs on the same VLAN on the same host.

Virtual machines can be in the same VLAN connected to the same virtual switch within the VM host's internal (virtual) network. All communication between the virtual machines is done internally and the host's physical NIC is not involved.

VMs on different VLANs on the same host

Virtual machines in separate VLANs communicate in the same manner as any VLAN-connected device would: traffic between VLANs is routed by a Layer 3 device. Traffic is sent through the host's NIC to the Layer 3 device and is sent back to the other VLAN within the host.

VMs on different Switches on the same host.

If a VM host is configured to have two or more virtual switches in its system, the virtual machines need to send their traffic to an outside networking device to reach the other virtual switches. The device can be Layer 2 or Layer 3.

VMs on different hosts on the same VLAN.

Mirasys VMS Networking White Paper

Virtual machines on the same VLAN communicate exactly like physical devices on the same VLAN would. Intra-VLAN communication is a Layer 2 process, so communication between them is trafficked through their physical hosts' NICs and a switch. The physical hosts must have a distributed virtual switch, however.

Universal Plug And Play

Universal Plug and Play are meant to automate device discovery and configuration on a local network, aiming to eliminate manual port forwarding and create an automatic port mapping. However, UPnP is often unreliable in practice. The technology is meant for consumer/home networking and is usually unsuitable for business network use. The function is usually disabled on networking devices and port forwarding is manually configured. As far as maintenance and troubleshooting are concerned, UPnP rarely provides error information in the event of a port mapping failure.

Time Protocols

Time protocols are used to sync device times with the rest of the world. In video surveillance, this is paramount to the entire purpose of the service. When setting up the VMS, every managed device should have its time synced to provide maximum reliability on the reported time of the video feeds.

There are three-time protocols used for time syncing:

- **NTP** (Network Time Protocol), is intended to synchronize all participating computers within a few milliseconds of UTC (Coordinated Universal Time).
 - The protocol does not transmit time zone or daylight savings time information, so these need to be configured on devices manually.
- **SNTP** (Simple Network Time Protocol), is the most commonly used time protocol in the IT/ICT industry and, as the name implies, a simplified version of NTP, being only up to a millisecond less accurate.
- **Windows Time**, a Microsoft proprietary time protocol used in Microsoft Networks.
 - Use is ***not recommended***, as configuring and managing this requires changes in the Windows registry and accuracy cannot be guaranteed.

Mirasys VMS Networking White Paper

A time server running one of these protocols provides time to networked devices on request.

Synchronization is most often performed every hour, though users can choose to have syncing occur more often, in cases where high accuracy is required. Surveillance devices often state 'time synchronization' instead of SNTP or NTP specifically. It is recommended to have all devices in the system network receive time synchronization from the same source.

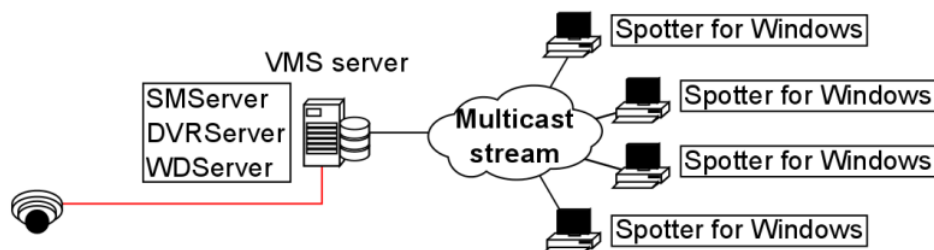
There are three basic ways to serve time to a network:

- **Public Servers** on the internet, such as time.gov and ntp.org. Accessing these sources requires an Internet connection.
- **Private Servers** can receive time from public servers and function as the local network's time servers. These must be configured with third-party programs on any computer or server on the network.
- **GPS Servers** are a solution for closed surveillance networks. These devices receive GPS data from the system's satellites via an antenna.

Multi-Channel Devices

Some camera models may be equipped to send their video feeds as separate channels, with each channel capable of carrying a number of video streams. These cameras are treated by the system as being separate video devices sharing a common IP address. As each channel is treated as a separate camera, these extra channels take up a place in the system's license.

Multicasting



Mirasys VMS Networking White Paper

When a unique Spotter stream is opened multiple times, the recording VMS server and the network connected to it face unnecessary strain as each stream is treated as a separate entity.

Multicasting enables a single stream to be opened and sent to multiple spotter clients simultaneously.

When using multicast, only a single instance of each video channel is sent to the local network.

All applications in the local network can receive the single stream, so network bandwidth usage is much lower than when sending streams for each streaming application separately.

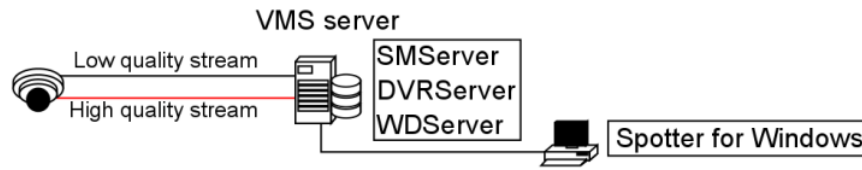
The feature needs to be configured in the System Manager application. As some network hardware may be incompatible with multicasting, the compatibility of all network components (such as routers and switches) should be checked before configuring multicasting.

A multicast network must meet the following requirements:

- Routers must support multicast
- Routers that connect multiple networks must support PIM (Protocol Independent Multicast)
- Ethernet switches must support IGMPv2 (Internet Group Multicast Protocol version 2) snooping
- Most out-of-the-box Ethernet switches are not configured to properly support Multicast
- An IGMP querier is required in each VLAN
- IGMP Query is normally supported by routers and high-end Layer 3 switches
- One querier per VLAN is needed

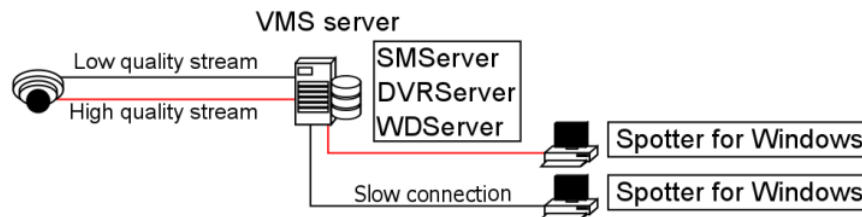
Multistreaming

Mirasys VMS Networking White Paper



Multistreaming enables separate video feeds from a single camera. The feature allows for separate streams to be used for recording and viewing, as well as an additional stream for remote streaming. Support for this feature is dependent on the specific camera model. Please refer to the camera manufacturer documentation and the supported cameras list to see what cameras support the feature. It should be noted that the extra stream causes additional network load. Bandwidth factors are further elaborated in chapter 5. The feature needs to be configured in the System Manager application.

Remote Workstation

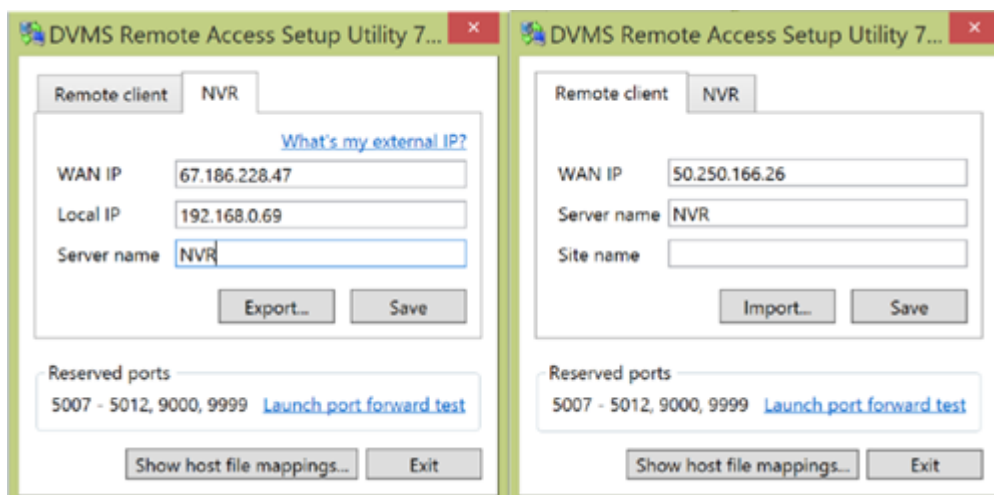


Mirasys VMS Networking White Paper

In some cases, it is necessary to open the same video stream in different locations with different image quality. For example, a separate image quality might be required for the security centre and a separate one for off-site use with slow network connections. The remote workstation functionality enables users to open an additional video stream with different image quality in comparison to the “prime” viewing stream. The feature is currently supported by specific camera drivers. Please refer to the *Mirasys VMS supported IP cameras* guide and the camera manufacturer documentation to see what cameras support the feature. It should be noted that the extra stream causes additional network load. Bandwidth factors are further elaborated in chapter 5. The feature needs to be configured in System Manager, and in the Spotter / GatewayServer XML settings for the computer in which the remote workstation stream is used.

Remote Access Setup

Remote access can be set up with the DVMS Remote Access Setup Utility. This is required only when DynDNS and VPN will not be used for the system.



To set up a remote connection, you need to know which VMS server needs to be contacted:

1. A static IP address needs to be assigned to the server-server/server-client NIC on the server running DVRServer.



Mirasys VMS Networking White Paper

- a. To see the remote access target name, open the System Manager application and navigate to System Settings Change Recorder Address on the System tab
2. Run the DVMSRemoteAccessSetupUtility.exe executable with the admin account on the server.
 - a. Select the NVR tab on the utility window shown above. The utility will auto-import your WAN static IP address and the server's local static IP Address.
 - b. Enter the copied PC name under Server Name.
 - i. Ports 5007-5012, 9000 and 9999 have to be forwarded to the local IP address of the server.
 - ii. You can test to make sure the ports are open by clicking on the "Launch port forward test" link in the utility.
 - c. Click Save
 - d. Click Export.
 - i. This will export a .dhc file that will need to be used on the remote client-side.

To import the .dhc file to the remote client-side:

1. Open the Remote Client tab in the utility
2. Click Import to open the file browser
 - a. Explore the location of the .dhc file and open it.
3. After the information has been imported, create a name for the remote site
 - a. The name can be the location of the remote client or customer name.
 - b. The name has no impact on the connection, but it would be useful in maintaining the service.
 - c. The name will be automatically imported into the Spotter client.
4. Click Save when finished.

After the information has been imported create a name for the remote site. The name can be the location of the remote client or customer name. The name has no impact on the connection, but it would be useful in maintaining the service.

The name will be automatically imported into the Spotter client. Click Save when finished.

Edge Storage

The Edge Storage functionality enables uninterrupted recording during network disconnects between the camera and the DVRServer.

Mirasys VMS Networking White Paper

During connection failures, the recorded footage is saved on the camera's local data storage, e.g. an SD-card. Once the network connection has been re-established, the saved video is transmitted from the camera's local storage to the DVRServer. Support for this feature is dependent on specific camera models. Please refer to the camera manufacturer documentation and the supported cameras list to see which camera models can support the feature. This feature is configured solely through the camera's own configuration utility, and it doesn't require any modifications in the System Manager application. Please refer to the camera's documentation for instructions on enabling Edge storage.

[Previous](#) [Next](#)

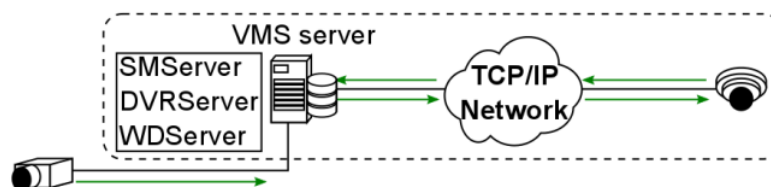
11. Mirasys VMS Bandwidth Usage

Mirasys VMS system components are optimized for effective bandwidth usage. The amount of bandwidth used by the system is determined by the system's component structure and functional requirements. In case of network bandwidth problems, the system can automatically prioritize presentation functions and restrict image display rates to avoid network load problems.

The total bandwidth consumption by cameras in the network needs to be noted and taken into account when planning and implementing the VMS network. As each individual camera consumes bandwidth on its connection, the cameras in the system have a sum of bandwidth that they consume as a whole. Each connection with multiple cameras should be planned with this in mind. When the end-user logs into the system by starting the Spotter for Windows or System Manager applications, the invisible background updater application – VAU – connects to SMServer to check for application updates. If the applications are up to date, the user is successfully logged in and the Master will deliver profile information including the IP addresses of the Slaves to the client application.

After the end-user has successfully logged into the system, the end-user can view or edit the system settings through the System Manager application, or access information from the analogue and digital devices through the Spotter application.

Local Recording



Mirasys VMS Networking White Paper

Local recording consists of cameras relaying video signals to recording VMS servers either directly or through the network. Signals from analogue video cameras and microphones are transmitted through analogue cables to VMS servers physically set up to function as DVRs (Digital Video Recorders) and as such have no bandwidth requirements. As an exception, an analogue camera can be connected to an IP encoder, which would connect to the recorder through the local network. In these cases, the digital video streams create network traffic only between the encoders and the servers. An encoder gives each analogue camera its own IP address.

The signal from a digital IP based video camera is relayed in a digital format from the camera to the recording VMS servers through the local network. A recording VMS server is by default an NVR (Network Video Recorder) server. The digital video streams create network traffic only between the IP cameras and the servers.

The bandwidth requirements of a digital data stream from an IP camera depends on the format (typically H.264, H.265 or MJPEG) of the video, as well as the image rate and the resolution of the digital video stream.

Real-time Monitoring

In real-time monitoring, the end-user can view one or multiple videos or audio streams from one or multiple servers. Each video or audio stream is transmitted from the servers running DVRServer to the Spotter client as a separate stream. As the client requests each presented image from the DVRServer, the system can automatically adjust the display rate in case the load exceeds the capabilities of the network or of the Spotter client. The display rate is adjusted by reducing the number of images displayed. However, at least one image per second is displayed. This adjustment does not affect the recording process, only the real-time monitoring function.

The quality rating, as it is managed through the System Manager application, for each camera is dependent on the camera model. If the camera model's API supports video stream quality settings, the System Manager will use the camera's video quality values as its basis for the VMS video quality value, as measured in percentages. If a camera does not support quality settings, the quality for video streams in the VMS is based on the bitrate of the video. The bandwidth requirements of video and audio streams depend on a variety of

Mirasys VMS Networking White Paper

factors, e.g. the resolution of the streams. Note that if real-time monitoring is performed directly on a VMS server (e.g. a Spotter for Windows client is installed directly on the server running DVRServer), the video streams do not create any network load. However, presenting the video streams locally requires additional system resources from the VMS server running DVRServer.

Playback Viewing

In playback viewing, the user can view one or multiple videos or audio streams from one or multiple DVRServers. Each video or audio stream is transmitted from the recording servers to the Spotter client as a separate stream. In playback viewing, every recorded picture is displayed. If the bandwidth usage between DVRServer and the Spotter client exceeds the capabilities of the network, the system will automatically lower the display rates of the streams, resulting in a slightly slower display rate but ensuring that all images are displayed correctly with no gaps in the presentation. Reverse playback is played at one frame per second. The bandwidth requirements of video and audio streams depend on the resolution and quality of the streams. Note that if real-time monitoring is performed directly on a VMS server (e.g. a Spotter for Windows client is installed directly on the recording server), the video streams do not create any network load. However, presenting the video streams locally requires additional resources from the server.

Alarm Handling

On the occurrence of an alarm, the system prioritizes the alarm procedure, providing maximum possible resources for displaying the alarm view as real-time or playback presentation depending on the system settings. If additional real-time or playback views are active while an alarm view is displayed, the system will automatically determine the number of resources provided to the additional views based on the needs of the alarm view.

Exporting Media

Mirasys VMS Networking White Paper

When exporting segments of the recorded video feed to external media, the system will load the selected clip to the client computer and save the export file to the desired external device (e.g. USB flash drives, CDs/DVDs, or hard drives). Exporting can also be done with a command-line exporter that is included with the GatewayServer and is also available through Mirasys customer support. The GatewayServer CLI exporter does not burn video data onto optical disks. The CLI media export command format is presented below (line broken for better readability). Each argument is preceded by a space and two dashes.

```
"C:\Program Files (x86)\DVMS\SystemManagement\
Vau\Workstation\MediaExporterCA.exe"
--profile "[profile name]"
--username [username] --password [password]
--devicepaths "[/site/device]"
--startdate [DDMMYYYY] --starttime [hhmmss]
--stopdate [DDMMYYYY] --stoptime [hhmmss]
--file "[destination folder]"
--writer [video file format]
--address [SMServer hostname or IP address]
```

As exporting video clips from recording VMS servers running DVRServer is completely unrestrained by timing requirements, a video file can be loaded at a rate that will not place an undue burden on the network.

System Manager

The system administrator can view and edit system settings through the System Manager application. Through the application, the administrator can add and remove recording servers as well as individual devices such as cameras and microphones from the system. In addition, the administrator can define and edit functions affecting bandwidth requirements such as the video quality of specific cameras. For example, the administrator can temporarily lower or raise the quality of video recorded from a camera, and the change will directly affect the network load created in video playback or real-time presentation from the specific camera.

Customer Bandwidth Usage

For bandwidth estimation usually below questions should be addressed:

Mirasys VMS Networking White Paper

- How much bandwidth does each camera use
- How many simultaneous users are connected to the Mirasys VMS?
- How many simultaneous video and audio streams will users access?
- What is the minimum acceptable video resolution and quality required by users?
- What is the maximum amount of bandwidth required by users?

TIP: Calculate this by multiplying the number of users by the maximum number of streams consumed simultaneously

Bandwidth Usage Examples

Resolution	FPS	Bandwidth, MJPEG	Bandwidth, H.264
2CIF (NTSC)	5	0.64	-
2CIF (PAL)	5	0.80	-
4CIF (NTSC)	10	2.60	-
4CIF (PAL)	10	3.20	-
1 megapixel	5	c. 6.70	c. 2.15
2 megapixel	5	c. 8.30	c. 2.24
3 megapixel	5	c. 13.80	c. 3.60
5 megapixel	5	c. 17.20	c. 5.20

***All bandwidth values are in Mb/s*

***Values are averages based on usage. The bandwidth usage can be heavily affected by the amount of movement in the image, camera settings and focus, and environmental circumstances.*

For comparison, an audio stream for a single microphone would require between 8-50 kb/s on playback and 350 kb/s real-time.

Balancing Video Performance vs Bandwidth And Capacity

In the field of video surveillance, bandwidth is one of the most important practical considerations.

Bandwidth is determined by a number of factors pertaining to the video feed, not just frame rate and video resolution. An important consideration that often goes overlooked is the concept of *scene complexity*, where different or changing scenes may require many times more bandwidth, even if viewed through the same camera. Scene complexity denotes activities and details contained within the viewed scene, but this factor is not a straightforward thing to evaluate. Understanding bandwidth is critical because it impacts network load and storage use, both of which incur their own costs. These can be kept down by influencing the recorded scene’s complexity by keeping the factors of it in check. An important consideration beyond the physical attributes of setting up an image is that the more an image is processed or compressed on one end of video transmission, the more CPU resources are consumed on the other end to “unpack” the video and make it presentable. So while this chapter focuses on balancing video performance and quality with bandwidth there is a third dimension of computer performance in the background. It is recommended to test and measure different camera models to find an acceptable balance between performance and bandwidth consumption before any wide-scale deployment. All performance properties have their own impacts on bandwidth. A quick way of estimating basic video bandwidth is to calculate a figure based on single frame file size and the frame rate.

Megapixel count	Resolution	FPS	Bandwidth
1	1280 × 720	7	0.9 - 1.8
		15	1.6 - 3.1
		30	3.1 - 6.2
1.3	1280 × 960	7	1.2 - 2.4



Mirasys VMS Networking White Paper

		15	2.1 - 4.1
		30	4.1 - 8.2
2.0	1920 × 1080	7	1.5 - 3.0
		15	2.6 - 5.2
		30	5.2 - 10.3
3.0	2048 × 1536	7	2.4 - 4.4
		15	4.1 - 7.7
		30	8.2 - 15.4
5.0	2560 × 1920	7	3.5 - 5.7
		15	6.1 - 10.1
		30	12.1 - 16.4
<p><i>**All bandwidth values are in Mb/s</i></p> <p><i>**All resolutions use progressive scanning</i></p>			

Mirasys VMS Networking White Paper

File size for a single uncompressed frame can be calculated from the image properties of the video following the below equations: *Interlaced Factor* equals 1 for progressive scan video and 0.5 for interlaced video. So a quick ballpark for video bandwidth for each camera without taking any other factors, such as compression, into account would be:

Resolution

Format	NTSC-Based	PAL-Based
QCIF	176 × 120	176 × 144
CIF	352 × 240	352 × 288
2CIF	704 × 240	704 × 288
4CIF	704 × 480	704 × 576
D1	720 × 480	720 × 576

Mirasys VMS Networking White Paper

Size/ Format	Pixels
QQVGA	160 × 120
QVGA	320 × 240
VGA	640 × 480
HDTV	1280 × 720
1M	1280 × 960
1M	1280 × 1024
2M	1600 × 1200
HDTV	1920 × 1080
3M	2048 × 1536
5M	2560 × 1920
4K	4096 × 2160

Mirasys VMS Networking White Paper

On average, a linear relationship exists between pixel count and bandwidth. However, variations across manufacturers and models are significant. Some cameras increase at a far less than linear level while others rise at far greater than linear.

There are no obvious factors that distinguished why some models differ in their rate of increase. So while resolution might be a reasonable ballpark indicator of bandwidth (as indicated in the equation in chapter 5.9), it's recommended to test and measure each camera model separately. Some camera models reduce resolution-based bandwidth by cropping an image when lowering the resolution.

Frame Rate

Frame rate impacts bandwidth, but for inter-frame CODECs such as H.264, the potential increase is less than linear. An increase in frame rate by a factor of 10 would likely lead to a smaller than expected increase in bandwidth, often by a factor of only 3 to 5. This is illustrated in the below table.

Video frame rate impact on bandwidth			
FPS	Bandwidth	FPS increase	Bandwidth increase
1	0.18	-	-
10	0.69	1000%	400%
30	1.30	3000%	700%

Mirasys VMS Networking White Paper

***All bandwidth measurements are in Mb/s*

***Measurements were done at 1 frame per second with compression Q =28*

The context of a scene can be used to gauge the normal needed frame rate for regular live footage. The industry has certain standards and recommended frame rates for normal contexts, listed in the table below.

Context	FPS
<i>Nevada Gaming Commission standard</i>	30
Cash register, teller stations	12-15
School or office hallways	4
Parking lot, traffic and overview cameras	1-3
Sports stadiums on non-event days	<1

Mirasys VMS Networking White Paper

As image quality and frame rate increase, so do bandwidth requirements. The frame rate selected should meet business requirements, but it does not need to be higher than what is required and should be considered carefully as frame rate influences both bandwidth and storage requirements. Motion pictures are captured at 24FPS. Human visual capabilities normally register images captured at 24FPS as fluid motion. Regular television sets use 25FPS (PAL) or 30FPS (NTSC) as do analogue video cameras.

These rates are often excessive for some video surveillance applications and in most applications less than 12-15 FPS is normally sufficient.

Colour

Colour can be thought of as a third dimension for a frame's size. Each pixel has a certain pixel depth that determines its colour. At most, 32 bits can be used for a pixel's colour code.

Bit Depth (Bits Per Pixel)	Number of Colors	Binary expression
1	2	2^1
2	4	2^2
3	8	2^3
4	16	2^4
6	64	2^6
8	256	2^8

Mirasys VMS Networking White Paper

16	65 536	2^{16}
24	16 777 216	2^{24}
32	4 294 967 296	2^{32}

In practice, colour generally has little impact on compressed video bandwidth, but saturation is an important aspect. Oversaturated colours increase image complexity through more pronounced colours and colour bleeding. Gain increases can compound this bandwidth inflation. Desaturation gives small decreases in bandwidth, generally under 10%.

Compression

Compression (or quantization), has an inverse relationship to bandwidth: the more compressed a video or image is, the lower bandwidth will be. Compression refers to the compression of pixels in a video or image file.

Mirasys VMS Networking White Paper

The uncompressed video would require excessively high bandwidth for videos. In an example situation where the video is uncompressed, a resolution 1080p, full-colour video, with each frame being an I-frame (further elaborated in 5.8.6), streaming at 30FPS would give the following bandwidth calculation:

Compression ratio is the factor over which the original image file size is larger than the compressed file size. Video or images with a ratio approaching 200:1 are on the higher end of achievable compression with some codecs, and any further compression with lossy formats will lead to significant quality degradation. Quantization (Q) is a form of compressing images in pixel blocks, where the values of pixels in blocks are arranged as mathematical matrixes, such as 8x8 for MPEG. Quantization is measured on a 0-51 scale with H.264, though manufacturers often use their own scales. 23 is seen as an average value and a balanced tradeoff between quality and bandwidth. The higher the number, the higher the compression and the resources digital devices need to invest in encoding and decoding them, conversely, compression leads to quality loss. 0 means a completely lossless (uncompressed) image. Changing H.264 quantization from high (34) to average (28) results in at least a three-fold bandwidth increase, while further lowering compression to very low (22) results in a 5-to-11-fold increase in bandwidth, depending on the model of the camera.

Approximate impact of compression on bandwidth increase

Camera Model	Q = 34	Q = 28	Q = 22
Dahua IPC-HF-3101N	1	x3	x5
Hikvision DS-2CD864FWD-E	1	x3	x10
Samsung SNB-6004	1	x3	x6
Sony SNC-VB630	1	x3	x11

**Bandwidth measurements based on Mb/s

**Scene complexity measured in an office environment.

Scene complexity and camera settings will affect bandwidth.

Mirasys VMS Networking White Paper

Codec

Codecs can be differentiated by their support of inter-frames or using intra-frames only.

Inter-frame-supporting codecs (e.g. H.264) compress similar pixels in a frame, reference preceding frames and transmit only the pixels changed between frames. Intra-frame codecs compress each frame and transmit them. Sending only the changed information instead of each frame of video saves the stream significant bandwidth.

Currently manufactured cameras typically use H.264 for its bandwidth-saving advantages over MJPEG and MPEG-4. The advantage is clearly seen in the below chart.

Intra- and Inter-Frames

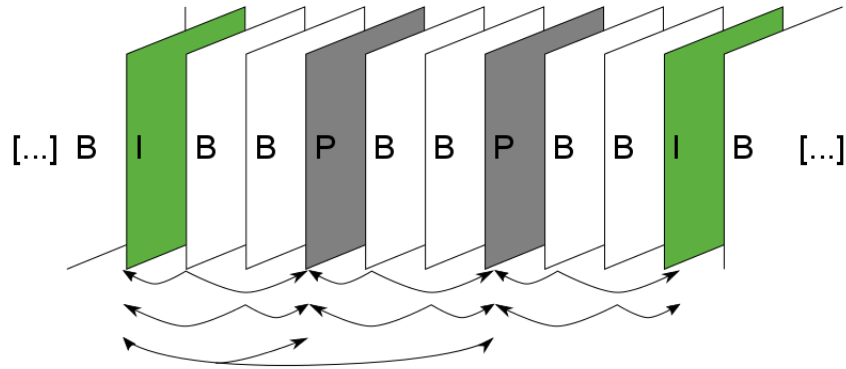
In inter-frame codecs, frames that capture the full field of view are referred to as I-frames, while those sending only changes are P-frames. Because I-frames capture a full image bandwidth is correlated with the number of I-frames in a stream. In almost all cases, one I-frame per second is the best balance between bandwidth and image quality. Too few I-frames in a video stream may negatively impact imaging, with long "trails" of encoding artefacts, while more than one I-frame per second provides little visible benefit.

B-frames are frames that are placed between P-frames and I-frames. B-frames reference both types of preceding and successive frames to form a predictive



Mirasys VMS Networking White Paper

movement frame. B-frames are usually optional since they increase encoding artefacts in the video.



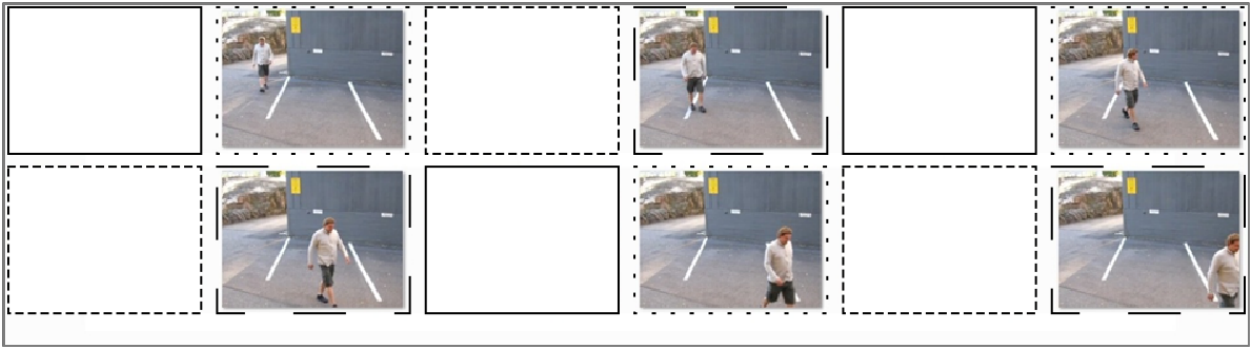
Reducing the number of I-frames (moving from 1 to 2 to 4-second intervals) produces minimal bandwidth reductions, despite the severe negative image quality impact, as seen in the below chart. Increasing the number of I-frames to more than one per second can conversely increase bandwidth, as seen in the below chart. Each set of an I-frame, P-frames referencing it and B-frames referencing (if in use) any of the previous forms a GOP (Group of Pictures/audio). The recording servers in the VMS save each GOP on separate disks, should a server running DVRServer have multiple hard drives installed, connected or assigned to it. This method, called SDD (Secure Data Distribution), ensures that always at least a portion of saved video footage is preserved should disk failures occur. In a four-disk SDD setup, drives C:, E:, F: and G: each store a GOP in sequence



Should drives C: and F: fail, E: and G: will still have enough frames to store a serviceable security recording.



Mirasys VMS Networking White Paper



If even G: fails, the system can present a serviceable security recording at ~25% of the original recording's frame rate.



For further information on Mirasys VMS storage methods, please refer to the *Mirasys VMS System Storage White Paper*.

Scan Type

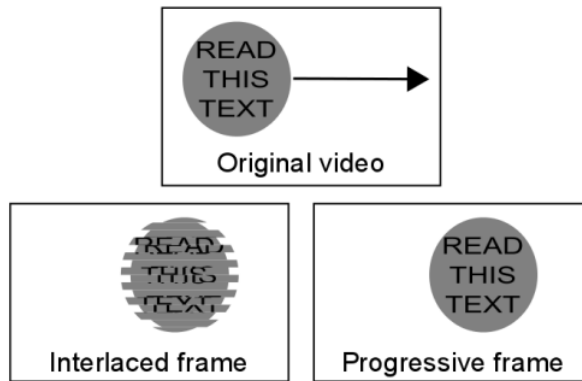
Resolutions are sometimes suffixed with a letter (p or i). This signifies the scan type of the video:

- **Progressive** scan video captures and transmits an entire frame at once, meaning the reported frame rate for resolutions marked with p mean full frames per second
- **Interlaced** scan video captures and transmits alternating lines for every frame scanned.
 - The individual frames take up less space, but the video has a higher perceived frame rate.
 - A common issue with the interlaced video is a noticeable alignment difference between the scan fields when looking at moving objects. Video resolutions marked with I are interlaced.

The interlaced video takes half the bandwidth of progressively scanned video when frame rates and resolutions are shown.

Mirasys VMS Networking White Paper

In the field of video surveillance, progressively scanned images are more useful, as single frames can be as important as a whole video clip. With a moving image, there is a difference in position with the fields of an interlaced scan frame. This can obscure details and make the edges of moving objects fuzzy.



Interlaced video is today largely a hold-over from the days of using CRT (Cathode Ray Tube) monitors, where interlaced scan fields were an easier way to project video with the technology. Computer monitors display progressive images, so the tearing and artefacts inherent in the interlaced video become more pronounced when viewed through a screen. Scan type has become less of an issue with the transition to IP cameras. Most IP cameras use progressive frame scanning, while interlaced scanning is more common with analogue cameras.

Gain Control

Gain control is a critical factor in low light surveillance video. It is generally only noticed when the negative side effects of aggressive gain levels are seen, namely noise on the video. To maintain good video quality, gaining control is necessary. Bandwidth penalty for increased gain becomes increasingly steep as gain levels increase.

There are some camera models with very high noise and very high bandwidth consumption in low light. In situations like these, it's recommended to check one's low light bandwidth consumption. If it is high, the presence of a bandwidth cap should be verified and lowered if necessary. The other option is to use CBR streaming or VBR with a cap of maximum bandwidth. The image below shows our test results of taking a scene with maximum gain and limiting its bandwidth to 1 Mb/s. The overall image quality is practically unchanged but at a fraction of the bandwidth.

Lighting Levels

Camera environments where there are varying light levels present their own challenges to cameras. Camera manufacturers usually indicate in their product documentation what lighting levels their devices can function in. Lighting levels are measured in Lux (lx), the SI unit measuring luminance over an area.

The lower the Lux rating on the camera, the better it can see in low light conditions.

Approximate lx	Condition
<0.001	Starlight – Overcast night
0.001 – 0.01	Starlight – Clear night
0.01 – 0.1	Overcast night
0.1 – 1	Moonlight at full moon
1 – 100	Dusk/twilight, office hallway lighting
100	Dark overcast day
320 – 500	Office
500 – 1 000	Overcast day, TV studio
10 000 – 25 000	Bright daylight
32 000 – 100 000	Direct sunlight

Mirasys VMS Networking White Paper

Low light environments make cameras suffer from increased digital noise caused by high gain levels. This noise increase bandwidth by a significant degree. A selection of cameras seen in [Table 12] shows a five-fold increase in average bandwidth during night-time when compared to daytime footage.

Camera	Resolution	FPS	Day	Night	Relative increase
Arecont AV3116DNv1	3MP	10	1.25	3.04	144%
Avigilon H3 1MP	720p	10	0.48	2.02	322%
Axis Q1615	1080p	10	0.42	4.28	909%
Bosch NBN-932V	1080p	10	0.64	3.12	388%
Bosch 733	720p	10	0.18	0.30	73%
Dahua HF3100N	720p	10	0.19	3.81	1983%
Hikvision 864	720p	10	0.56	4.72	843%
Samsung 5004	720p	10	0.68	1.86	274%
Samsung SNB-6004	1080p	10	1.89	2.58	37%
Sony SNC-VB630	1080p	10	2.49	8.24	231%
Sony VB600B	720p	10	0.16	0.60	275%
Averages	-	10	0.81	3.27	498%

**All bandwidth measurements are in Mb/s

Mirasys VMS Networking White Paper

Digital noise can be reduced primarily with two methods: Digital noise reduction and integrated IR. Noise reduction decreases bandwidth and space requirements by compensating for and smoothing out digital noise in the footage. Integrated infrared systems function as low-level night vision, improving footage lighting levels and giving a smaller relative increase in bandwidth as seen in the below table.

Camera	Resolution	FPS	Day	Night	Relative Increase
Axis M1144-L	720p	10	1.20	5.44	353%
Avigilon 3.0W-H3A-BO1	1080p	10	1.15	1.32	15%
Dahua HFW3200S	1080p	10	3.20	8.80	175%

Mirasys VMS Networking White Paper

Hikvision DS-2CD2032-I	1080p	10	2.75	7.20	162%
Averages	-	10	2.08	5.69	176%
**All bandwidth measurements are in Mb/s					

When comparing the bandwidth increases of the 1080p resolution cameras in the previous two tables, we see a similar increase in bandwidth (about 3,2Mb/s) when transitioning from day to night, but the relative increase in bandwidth is considerably less when noise reduction methods such as integrated IR are used.

Field Of View

The camera field of view impacts video bandwidth with two factors: the amount of moving elements and scene detail. Normally when a camera records a larger field of view, it might pick up more moving elements from a background, e.g. view of a street corner might pick up vegetation or signs around the street corner, traffic on or near the corner and nearby pedestrian traffic. Tightening the field of view usually screens out unnecessary areas from the recorded video. If a camera is zoomed in on a relatively uniform and repetitive scene with relatively little movement, it will pick up finer static details and encoding the video will be more difficult.

Aspect ratio

Mirasys VMS Networking White Paper

Another way of restricting a camera’s field of view is by adjusting the camera’s aspect ratio.

With aspect ratios, the camera can be set to record only a segment of its total field of view, scanning the desired section of the scene and leaving out the wasted areas. CCTV cameras use a 4:3 aspect ratio. Most IP cameras have a default aspect ratio of either 4:3 or 16:9, but high-definition cameras can have their video’s aspect ratio adjusted.

Some cameras support this function natively. Consult device documentation to see if the model used supports this function.

Camera placement

A camera with an overview scene monitors a large area such as a parking lot or a traffic camera that is viewing vehicle congestion or the number of cars parked in the said parking lot.

Because fine details are not important for overview cameras, standard definition resolution used with a wide-angle lens may be sufficient for the task. Overview cameras may be supplemented with a detail view camera focused on key areas of interest or PTZ cameras to provide real-time analysis of areas of interest at a higher resolution.

Detail view placement means having a camera observing a specific area of interest at a higher resolution than an overview camera. The detailed view is used for point-of-sale transactions and face or license plate recognition.

A camera assigned for a detail view position may have PTZ capability, be close to the monitored area or have a long focal length lens. Megapixel or HD cameras may be deployed to provide a sufficient number of pixels-per-area to accurately represent subjects within the field of view.

Sharpness

Sharpening an image increases detail and fidelity by bringing more definition to fine pattern details and object edges. The tradeoff is that this significantly increases video bandwidth. Conversely, decreasing image sharpness blurs details and edges, but decreases bandwidth.

Camera Model	Minimum	Default	Maximum
Axis Q1604	0.44	0.62	1.72
Dahua HF3101N	0.69	1.64	4.83

Mirasys VMS Networking White Paper

Sony VB600	0.78	0.59	1.09
Average	0.64	0.95	2.55
**All bitrate measurements are in Mb/s			

WDR

WDR (Wide Dynamic Range) is used to balance out varying lighting levels by High-Dynamic-Range Imaging. This allows a camera to maintain detailed video even with backlight and other harsh lighting conditions. WDR allows for increased details compared to video-recorded without WDR and possibly more uniform colours in some scenes, making compression easier.

Camera Driver Solutions

Choosing between VBR (Variable BitRate) vs. CBR (Constant BitRate) has an impact on bandwidth, and is significantly determined by what the camera “sees.” Systems are by default set to CBR. VBR support depends on the capture driver. With CBR, the camera streams its footage at a constant frame rate without regard to what’s actually happening on the screen. VBR enables a higher frame rate in the event of alarm activation. Using VBR saves on storage space and average bandwidth, though the bandwidth will fluctuate. It is recommended to test to find out which solution works better in the camera’s environment.

Motion Detection

Mirasys VMS Networking White Paper

If camera-based motion detection (VMD, Video Motion Detection) is used to trigger an alarm, nothing is sent/streamed (or recorded) unless the camera detects motion and starts to transmit, or if the client application user decides to view the live camera view.

Normally motion detection is handled by the system server-side. DVRServer uses software VCA for motion detection. This is configured through the System Manager application.

In the System Manager application settings, each camera has a default motion detection mask. The mask cannot be edited through the application, so it detects motion in the entirety of the image area when it is used. In addition to the default mask, four more masks can be configured for each camera. The use of these masks can be scheduled in the application.

A mask contains these parameters:

- Selected areas. The system detects motion in areas that are painted red.
- Detection sensitivity.
- Minimum quantity of movement.

Motion detection methods

Three motion detection algorithms are available:

- **Comparative motion detection** compares an image to the image before it. If the differences exceed set limits, the system interprets it as detected motion.
 - Comparative motion detection can be used in most conditions.
 - However, if there is a lot of movement in the background, e.g. rain, moving leaves, or changes in light levels, the use of adaptive motion detection instead is recommended.
- **Adaptive motion detection**, which compares each image to a learned background image. The system learns the background image and the movement that belongs there automatically.
 - Thus, the system does not interpret constant and predictable movements inherent to the scene as motion.
 - Additionally if more than half of the pixels in an image change, the system concludes that the lighting conditions have changed. As a result, it resets the reference image and starts learning it again.
 - Do note that learning the background image can take some time for the system.

Mirasys VMS Networking White Paper

- **Hermeneutic motion detection**, a sophisticated motion detection system for challenging conditions with “noisy” backgrounds (heavy rain, wind tossing tree branches, etc.) and situations in which external VCA (Video Content Analytics) tools are used. It should be noted that hermeneutic detection requires more processing resources from the server than the other detection methods

Mirasys supports a number of cameras with native VMD. Please consult the list of supported [cameras](#) and [camera models](#). For more information on configuring motion detection for cameras through the VMS, please consult the *Mirasys VMS 7.3 Administrator Guide*.

Streaming Options

Choice of depending only on a single stream or multiple streams for different purposes also has an impact (when the camera is sending two or three streams simultaneously, vs. only one) on bandwidth. Using unicast vs multicast has different levels of network impact. This impact is principally seen with routing, but also in cases where two separate DVRServers can capture the same stream simultaneously. Multicasting support depends on the camera drivers. Please consult the list of supported camera models.

Network Planning Impact On Bandwidth

To size a video surveillance network, you will need to know:

- How much bandwidth each camera consumes, depending on the models you have or plan to have
- How many cameras do you plan to use and in how many locations
- The distance (administrative or physical) of the DVRServer to the cameras connected to it, presuming they need an IP network
- What the bandwidth of those network connections is and what pre-existing load those networks must also support
- What cameras must be viewed live and where/how many viewing stations are in the system
- How many servers will there be in the network

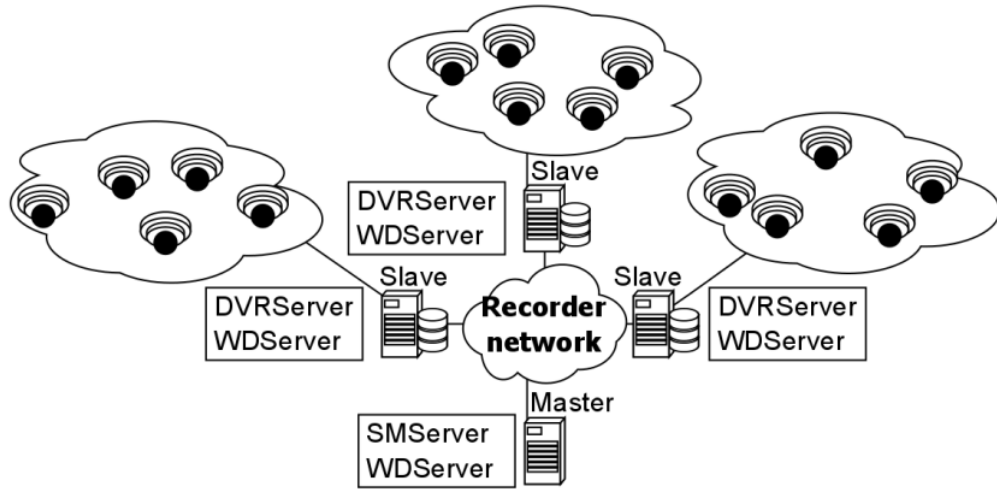
Mirasys VMS Networking White Paper

Video surveillance consumes network bandwidth in two general routes, in some cases at the same time on some networking devices:

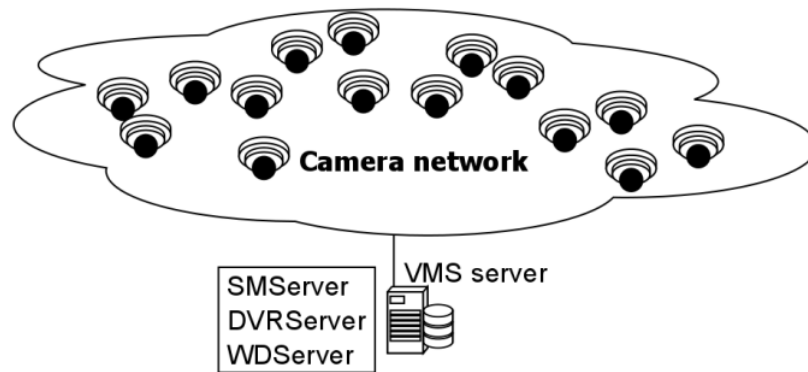
- **IP camera/encoder to server:** Video is generally produced in devices different than what they are recorded on (e.g., a camera generates video; a VMS server running DVRServer records it).
 - The video needs to be transmitted between the end devices. If it goes over an IP network (e.g., IP cameras to a VMS server running DVRServer), bandwidth is required.
- **Server to the client:** Statistically, a very low percentage of video is watched by humans. Often, a user is viewing the footage on a device that is connected to a different IP network than the server.
 - For example, the server might be in a rack in a server cabinet but the client is operated on a laptop, mobile phone or an AVM setup.
 - The connections between these devices require bandwidth every step of the way.

Because of these design realities, the overwhelming majority of bandwidth needed in surveillance systems is dictated by (A) camera type and (B) the relative placement of cameras and servers. In terms of the camera type, analogue cameras do not normally consume bandwidth unless the video is being streamed to clients from DVRServer as each camera has a cable directly connected to said server. However, analogue cameras can be connected to an encoder that converts analogue transmissions into digital signals in their own channels with each having its own IP address in the network the encoder is connected to. Signals from the encoder produce network traffic and consume bandwidth. For all camera types, the relative physical placement of the server near the camera significantly impacts bandwidth needs. A simple scenario, as presented in the below image, has three sites with their own camera network connected to a recording VMS server (Slave). Each camera has its own bandwidth, and each Slave receives the camera network's combined bandwidth. The Master receives bandwidth from the three Slaves.

Mirasys VMS Networking White Paper



In the below setup, the number of cameras is the same, but they're connected to only one recording VMS server as a single combined camera network. The bandwidth received by the sole server is three times greater than what the Master server would receive from its three Slaves.



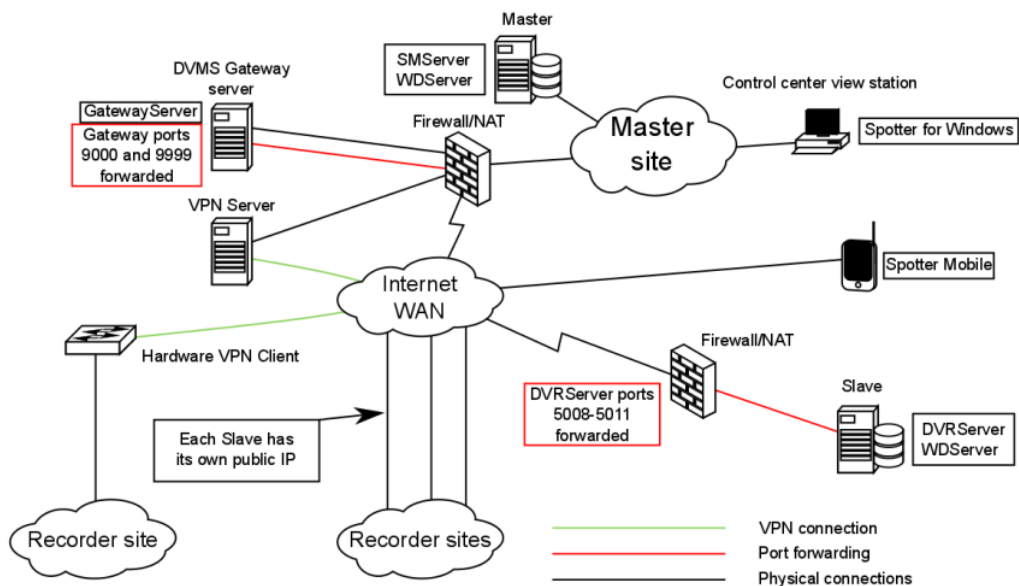
Any networking approach carries with it its own pros and cons, and these must be weighed and balanced before arriving at a solution.

[Previous](#) [Next](#)

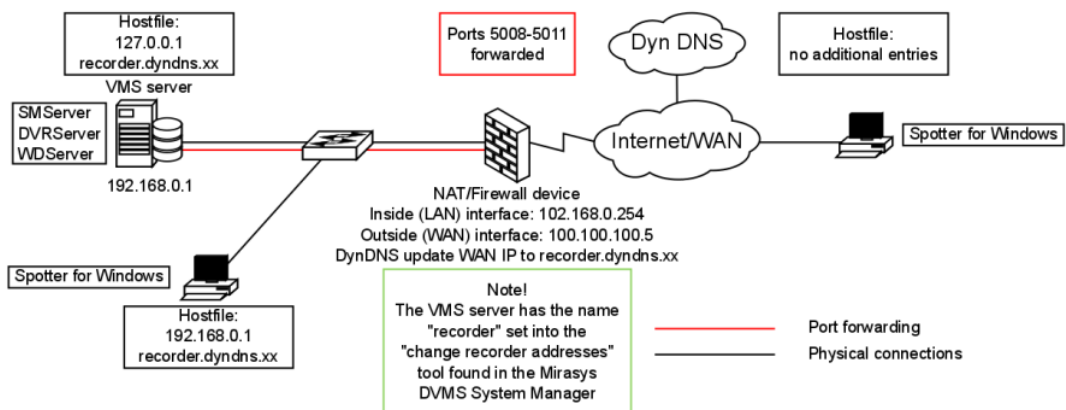
12. Solution Examples

The following chapters include example topology diagrams on various VMS and network configurations. The diagrams are aimed to provide examples, and should not be viewed as recommendations.

EXAMPLE: Control Center Network Diagram

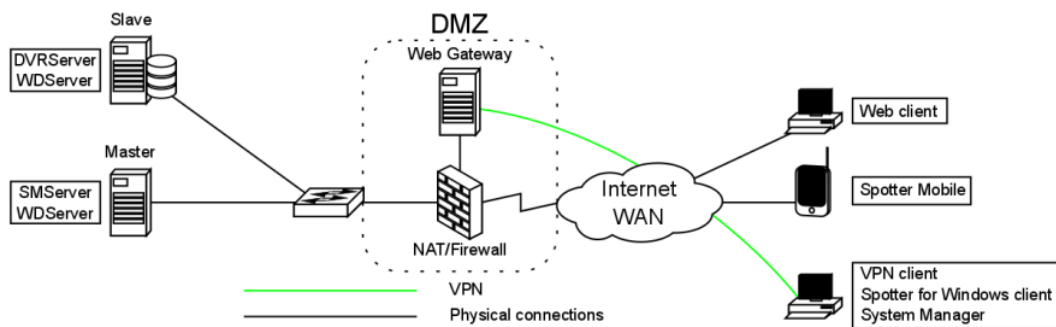


EXAMPLE: Dynamic DNS Service Without Loopback





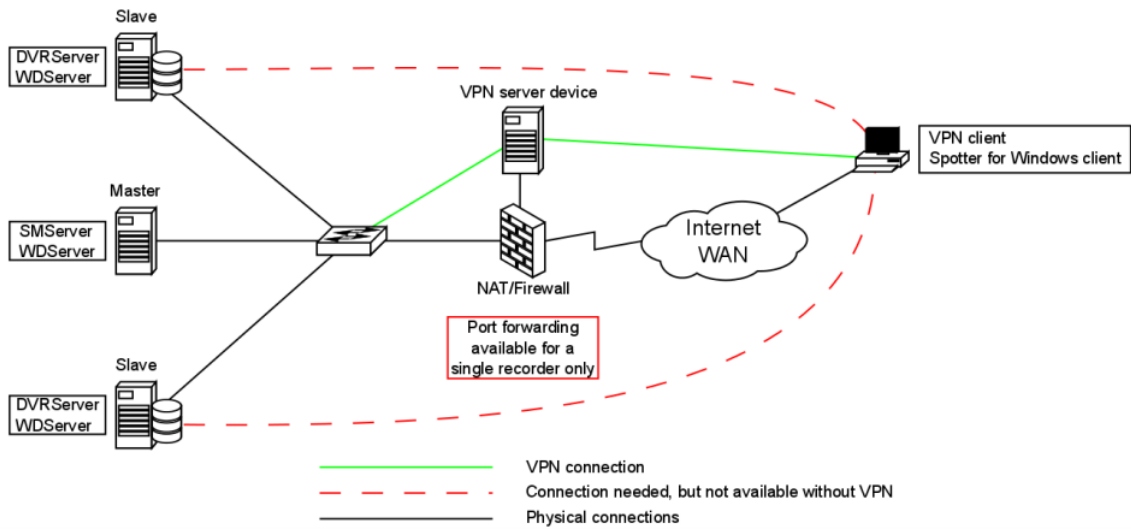
EXAMPLE: Web Gateway On DMZ



EXAMPLE: Network Diagram With NAT



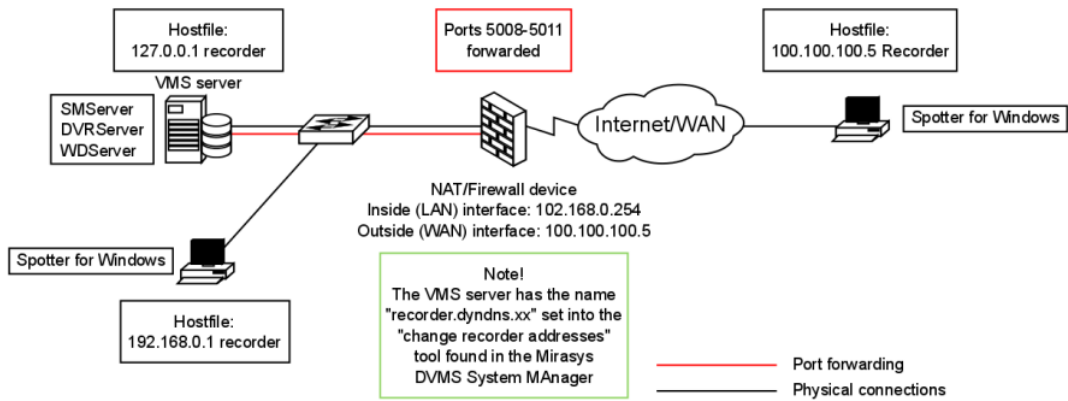
Mirasys VMS Networking White Paper



EXAMPLE: Spotter Clients In The Local Network And Across The Internet Without VPN



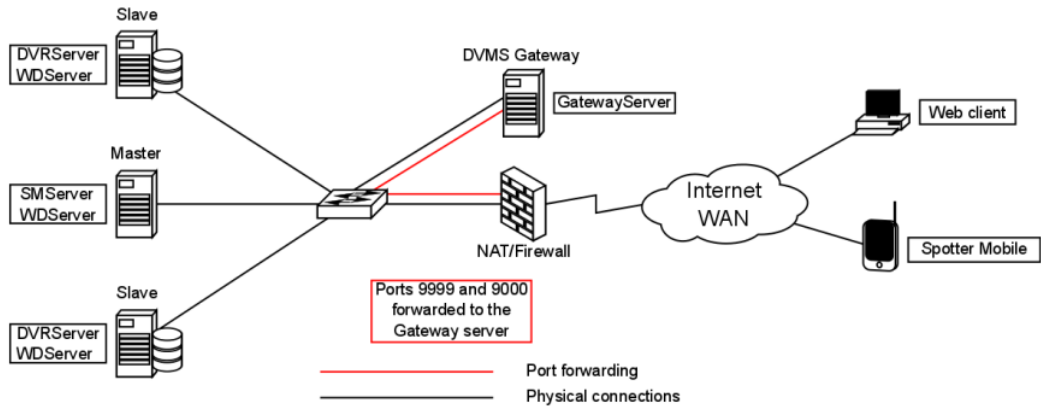
Mirasys VMS Networking White Paper



EXAMPLE: VMS Network With GatewayServer



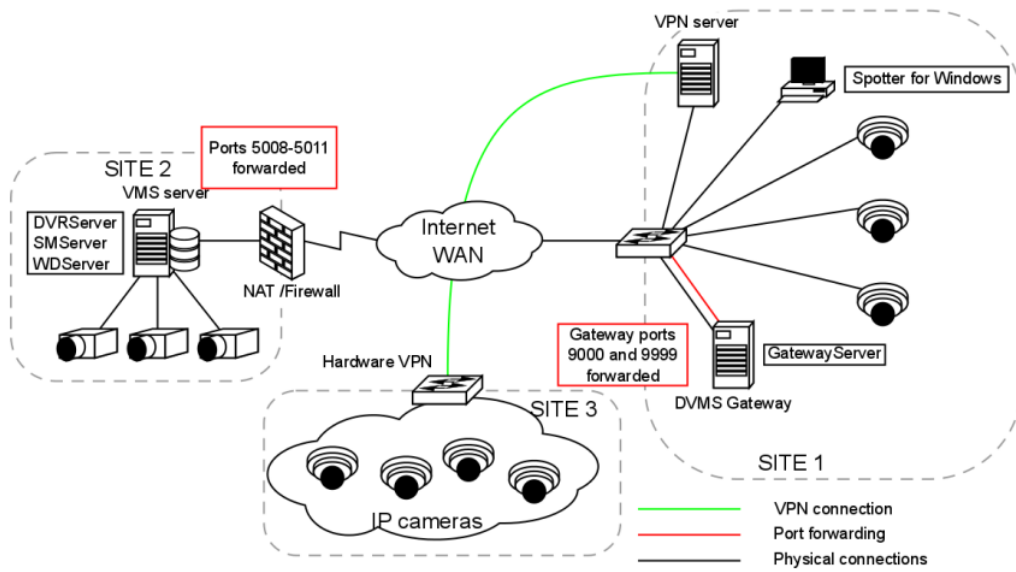
Mirasys VMS Networking White Paper



EXAMPLE: Complex VMS System Between Three Sites



Mirasys VMS Networking White Paper



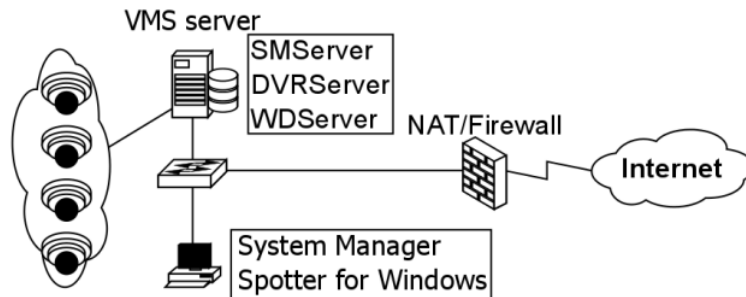
Mirasys VMS Networking White Paper

[Previous](#) [Next](#)

13. ThruCast

ThruCast is a proprietary direct video streaming feature found in Mirasys VMS 7.3 that streams camera video directly to a Spotter client in case of a recording VMS server disconnect or for the purpose of network optimization.

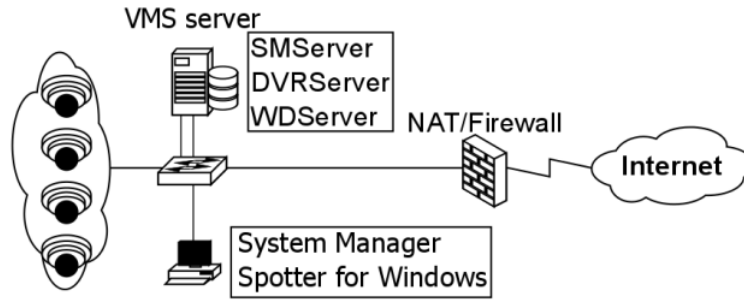
If ThruCast is to be used, the VMS network needs to be planned with this in mind. Normally it is recommended to isolate the camera network physically or logically, routing traffic from IP cameras directly to DVRServer.



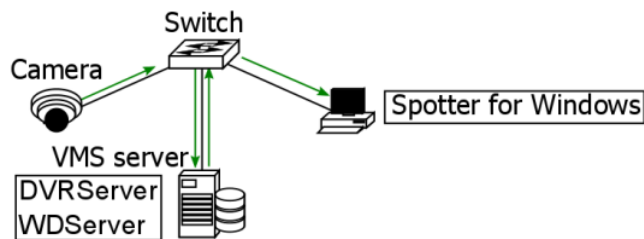
With ThruCast, the cameras need to be able to be routed to Spotter clients in the event of connection difficulties with DVRServer.



Mirasys VMS Networking White Paper



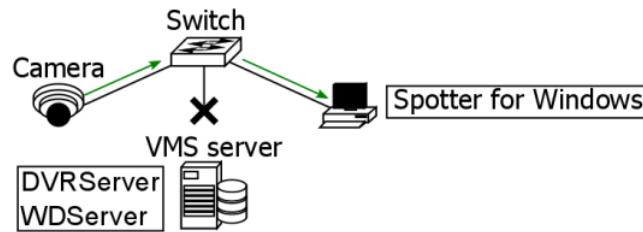
Normally the camera's video feed is routed to the server's camera network card, while it is accessed by a Spotter client through the server's client/server network card.



Mirasys VMS Networking White Paper

In the event of a network disconnect or other failure relating to the server, the spotter takes direct streaming from the camera.

Direct streaming can also be accessed by changing connection settings. This option can be considered when optimizing the network.



Supported Cameras

ThruCast requires a separate camera capture driver for the client.

Currently, drivers exist for the following camera manufacturers:

- ACTi
- Axis
- Bosch
- HIKvision
- Samsung
- Sony
- Stanley
- LILIN

An ONVIF ThruCast driver is also available for cameras that are not on the supported list.

The use of the ONVIF driver requires that the camera is added to the VMS system with the ONVIF driver, not the camera's native driver.

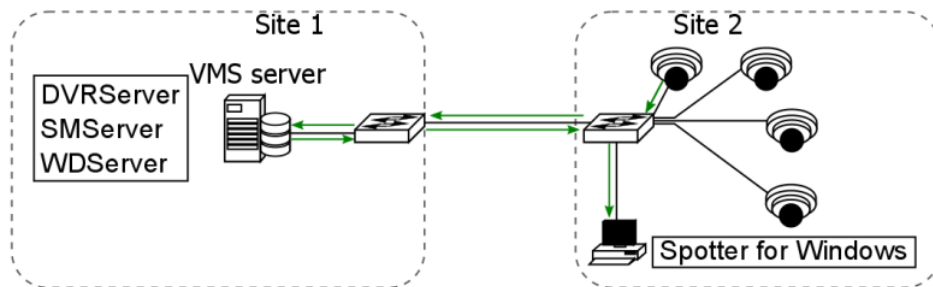
Network Optimization

ThruCast is useful in reducing network load in certain instances. Usually, this is performed when the recording server is on another site and the Spotter client is on the same site as the cameras.

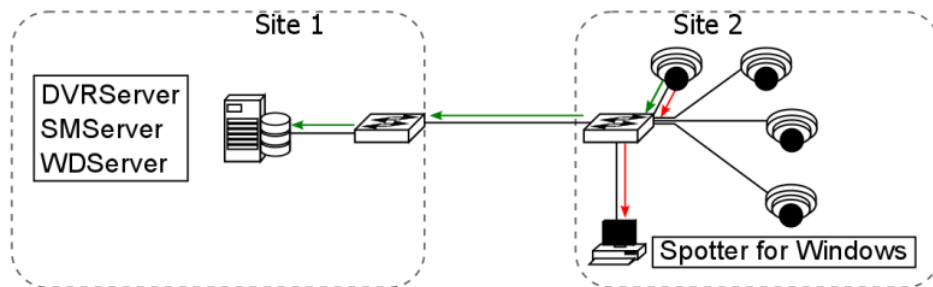
Example 1

Mirasys VMS Networking White Paper

Site 1 contains the recording VMS server and Site 2 contains the other elements of the system, including the cameras and a Spotter for Windows client. In the initial state, camera feeds are sent to the server and from there to the Spotter. Traffic between the sites is increased because of this, with the server streaming the feed to the Spotter.



With ThruCast, the camera sends a direct feed to the Spotter and a recording stream to the VMS server. Traffic from the camera is increased, but the inter-site traffic load is lessened. A user operating the Spotter can determine the framerate of the ThruCast stream coming directly to the Spotter client. The frame rates between the ThruCast stream and the recording stream can be different. A user can determine whether or not they want to directly stream any specific camera through the Spotter client.

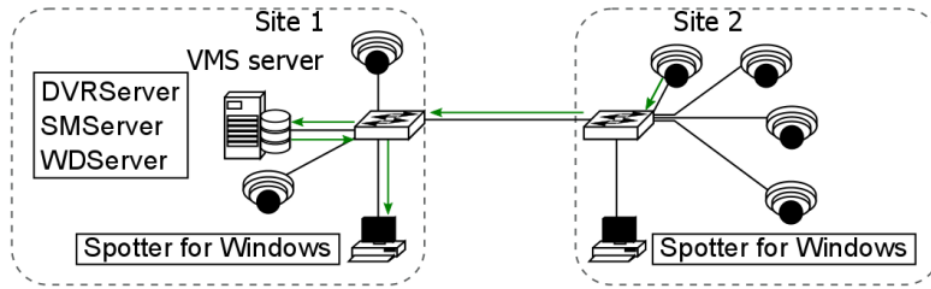


Example 2

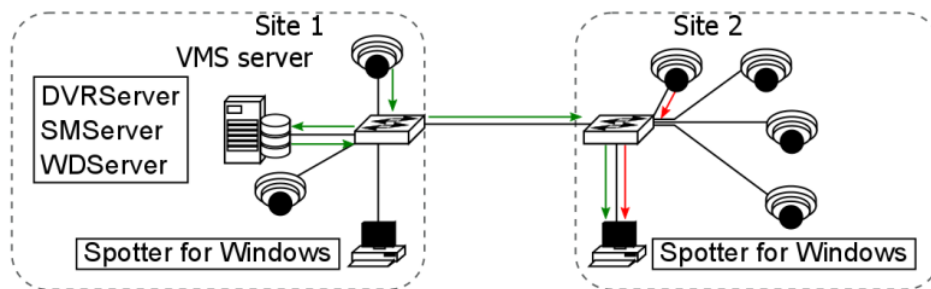
The two sites both have cameras as well as Spotter viewing clients. Site 2 user uses ThruCast with on-site cameras. This service can be chosen for all cameras in the system or only on-site cameras.



Mirasys VMS Networking White Paper



For the Site 1 user, ThruCast only reduces traffic between the server and the network connection.



ThruCast allows users to have control over which cameras are using the service. The setting is saved for each user and camera, and Spotter layouts remember these settings.

Impact Of Multistreaming And ThruCast On Network Optimization And Storage

Network planning is required when ThruCast is expected to be used. The service creates two streams from a camera using the service: a recording stream to the recording server and a live stream to a viewing Spotter client. ThruCast streams can be set for different frame rates, as well. A live viewer might set the recording stream to a lower frame rate (e.g. 8FPS) and have the live stream at a higher frame rate (e.g. 25FPS). This reduces storage and network requirements to the recording server significantly.

Other Considerations

Impact Of ThruCast To Image Delay

The delay of the video stream might be less than in a case where the stream is relayed through a recording server.

Mirasys VMS Networking White Paper

But this difference is not significant enough for a human to notice, as it's only some milliseconds.

Features Not Supported In ThruCast Streaming

ThruCast does not support PTZ (Pan, Tilt, Zoom) camera control or two-way audio transmissions.

The ThruCast only supports one-way streams from the camera. Currently, the service doesn't support replaying recorded images either, as these are always received from the recording server.

Licenses

ThruCast requires the VMS license to have the "ThruCast" feature and the ThruCast client driver identifiers that are being used. These ThruCast driver licenses, and the ThruCast feature, are always enabled in the Mirasys Enterprise product version.

Multiple Viewers

Each individual viewer on ThruCast constitutes an individual video stream from the camera, so users seeking to adopt the service should conduct trials to establish the maximum number of reliable streams from the cameras used. Cameras can usually support three to five streams.

[Previous](#) [Next](#)

14. Troubleshooting Network Issues

The most noticeable error that can occur in the VMS' operation would be a failure to receive a video feed from a camera. The reasons for this include, but are not limited to, physical connection errors (cable disconnected, disrupted or improperly connected), logical connection errors (configuration errors, e.g. wrong addresses incorrect camera login details or command typos) or device or component failures at any point in the network (cameras, servers, networking devices, clients). If a client views footage from a remote site, failures in the connection beyond a VMS site could include connection configuration errors or ISP network faults.

Troubleshooting Tools

Web browsers

Web browsers can be used to troubleshoot IP cameras and networking devices in a few ways if their interface IP addresses are known:

- **Connection testing:** If a web browser is unable to reach a device's GUI interface through its IP address, it indicates some manner of connection problem or issues with its software.
 - This method is a basic "Can I contact it" type of connection testing, only telling if there's a need to use the previously mentioned tools to diagnose network issues.
 - At a later point, it can be used for HTTP connection testing.
- **Remote configuration:** When a web browser has established contact with the device, it usually opens a simple web page that functions as the GUI for the device.
 - The device's settings can be configured through this interface.

WireShark

WireShark is a web sniffer program that allows the user to monitor network traffic that the device the application is installed on can perceive. This allows the user to examine flows of packets to and from the device and whatever end devices there are at the other end of the exchanges. The packets that have been read can be opened and examined by the user. The application is free and it comes with all the necessary components as well as WinPcap, a link-layer packet capture driver for Windows.

Mirasys VMS Networking White Paper

Windump

WinDump is a Microsoft Windows port of tcpdump, a command-line basic packet analyzer program. The program uses WinPcap to capture packets for analysis and inspection. The program is able to view unencrypted traffic and open the information contained therein.

Iperf

Iperf is a network performance measuring tool that uses WinPcap. The basic application is free, but a GUI version is not. The application is installed on two devices at the endpoints of a connection and they're set to transmit TCP or UDP streams between each other. This can be used to test connection issues between end devices. Packet sizes can be easily changed to gauge traffic impact on bandwidth.

Command Lines

Command-line utilities are accessed through the Windows command prompt. The command-line formats presented in this section will be in the format of `command [optional] [required] <description>`. The description within a field explains the argument. An argument outside of the description brackets is the proper syntax for it.

Ping

The command utility ping is used to test communications between the pinging device and the target IP/hostname. A ping can indicate response times from the destination when successful. It can also indicate whether there's a problem on the local end when trying to contact the destination (Request timed out) or if there's a problem on the destination network (Destination host unreachable). The format for the command is presented below. The command can have numerous arguments to specify the actions the command will perform.
`ping [<argument>] [<destination hostname or IP address>]`

Netstat

The command utility netstat displays various network statistics for the device in the command prompt window. This can be used to discover port issues and other connection issues on the device.

Mirasys VMS Networking White Paper

The format for the command is presented below. The command can have numerous arguments to specify the actions the command will perform.

netstat (<arguments>)
Results are displayed in the command prompt or in a text file if so instructed by the user.

To have the output of a netstat command saved as a text file, enter the command with the modifier ">", followed by a name for the file. The text file is saved on the device's C:/ drive.

```
netstat -abn >output.txt
```

Arp

The command utility arp is used to access the ARP (Address Resolution Protocol) cache on the device. arp -a displays the cache in the command prompt and arp -d deletes named entries in the cache. The ARP cache is refreshed every time the device pings a destination host or the network at large. ARP can be used to view devices on the connected network by their MAC and IP addresses. The format for the command is presented below. ARP [<argument>] (<IP address>) (<MAC address>) (if_addr < IP address of the interface whose address translation table should be modified>)

Traceroute

The command utility tracert is used to map the route packets would take in the network to their destination as well as the time it takes for them to make each hop. This can be used to determine failure points in a network as well as incorrect routing. The format for the command is presented below. The command can have numerous arguments to specify the actions the command will perform.

```
tracert (<arguments>) [<destination hostname or IP address>]
```

Nslookup

The command utility nslookup is used to look up the domain name or IP address in the DNS lookup server. The format for the command is presented below. Typing only the base command displays the information for the device's DNS server. nslookup [-option] (host <destination hostname or IP address>) (server <non-default server's hostname or IP address>)

Telnet

Mirasys VMS Networking White Paper

Telnet is a text-based terminal connection over TCP, allowing direct, unencrypted communication between devices. This can be used to remotely contact, use and, if need be, configure networking devices through their CLI interfaces. To telnet (open a Telnet connection), the command is typed in with the relevant arguments in the command prompt. The format for the command is presented below. The command can have numerous arguments to specify the actions the command will perform. `telnet [<destination hostname or address>] (<port number>)` Telnetting to network devices is highly recommended to be done **within** the local network the device is connected to, as the communication is unsecured.

VLC

The VLC media player is a freeware media player application that can contact streaming addresses over an IP network. To receive a stream from an IP source:

1. Launch the VLC application
2. Click Media Open Network Stream...
3. Click the Network tab
4. Enter the camera URL:
 - `[protocol]://[camera IP/domain name]:[port]/[destination file/function]?[argument]`
5. Play video

The protocol for the connection can be anything. The potential arguments in the URL include but are not limited to, a username and password set for that camera. If camera connections are being tested without having set a password or username on them, the device needs to be kept on an isolated network. Consult the program's documentation for further information on the media player functionalities.

Simultaneous Camera Channel Failures

This issue is more of a concern for larger surveillance system networks involving networking on many levels across many local sites.

Mirasys VMS Networking White Paper

Larger systems require more networking devices between the system components, and every added device brings a potential failure point. If multiple related cameras go offline at once on a video matrix, it would point to a camera cluster losing connectivity.

Usually, it would point to a server or switch failing:

- If cameras opened in the Spotter client disconnect when the client has opened a session with a DVRServer, there are issues with the service, its server or its connection to the system.
- If ThruCast has been enabled, it can stream camera footage without DVRServer.
- If there's a failover server, it will take over, but the client needs to connect to it.
- If some of the cameras fail simultaneously, it would point to a switch losing power, the connection failing or otherwise being disabled.
- Check if the connection is still intact.

The only form of troubleshooting for switch device failures would be replacing the switch as soon as possible.

Master Failover

SMServer failures can be noticed by the end-user with the Spotter for Windows client falling back to the login state. Normally these are recovered from when the service is restarted on the Master. In the event of a SMServer cannot be restored, nothing can currently be done except to physically replace the Master. The functionality for a Failover Server to take over for a crashed Master is currently in development, but for the time being, other means need to be used, such as offline pre-configured spare Masters. This will not make recovery immediate, but it would help reduce downtime.

Port Conflicts

Port conflicts arise in situations where there are two or more applications on a computer that use the same ports for communication. VMS applications' ports do not conflict with each other, but a situation might come up where a third-party program is trying to use the ports that the VMS components use, leading to either program not connecting over the network.

Mirasys VMS Networking White Paper

To discover port conflicts on Microsoft devices, open a command prompt and enter a netstat command to list all ports. It is recommended to use modifiers to narrow down the list.

netstat -abn

- a displays all active TCP connections and the TCP and UDP ports on which the computer is listening
- b displays the executable's name involved in the creation of each connection and/or listening port (this requires running the command prompt as an administrator of the device)
- n displays active TCP connections with addresses and port numbers numerically expressed

For devices using Linux and Mac OS operating systems, lsof command can be used instead of netstat to list all ports. It is recommended to use modifiers to narrow down the list.

lsof -i

- i lists the device's IP sockets

When a port conflict is discovered, the next step is to resolve it. One way of doing this is to reassign an application's port to another number. E.g. if there's a conflict between two applications in TCP port 800, either of the conflicting applications needs to be ported through TCP port 801. If port numbers are to be changed for an application, these changes must be consistent.

Device Discovery

Adding cameras to a camera network is like adding any other networked device to the network. It is recommended to first read the camera instruction manuals and configure the devices **before** connecting them to the network. It is also recommended to **document all vital information** on the devices, including their MAC addresses. Normally camera discovery and adding them to the system is handled through the System Manager application that controls the SMServer. IF the camera has not been configured, including its IP address setting, and have connected it to the network, you can either contact your IT department so they could look up the device's address in the router, or you could use ARP to discover the

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com



Mirasys VMS Networking White Paper

device, should IT not be available. If you have not configured the IP address for the camera and have it connected to the network, you can either contact your IT department so they could look up the device's address in the router, or you could use ARP to discover the device, should IT not be available.

Devices in an IP network are discovered by using ARP (Address Resolution Protocol) requests whenever a ping command is enacted on a networked device. To discover the IP address of a device with a known MAC address, it's possible to perform a reverse ARP request. This involves pinging the connected subnet's broadcast address (the last address of a subnet e.g. 192.168.1.255 on a 192.168.1.0/24 subnet). Pinging will also send automatic ARP requests to the whole subnet. The ping will return a timeout result.

```
C:\Users\ [REDACTED] >ping 192.168.1.255
Pinging 192.168.1.255 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

After pinging the network, type in the command arp -a to get a list of all connected devices in the network and browse them until the newly connected camera is found. Write down the IP address of the device. Use the IP address in the System Manager to add the camera to the VMS. This method can also be used to discover other devices added to your network. If you are unsure about a device added to the network, it's best to investigate it with the help of any resident IT personnel.

[Previous](#) [Next](#)

15. Networking Best Practices

The best way to solve problems is to prevent them before they happen. With best practices in general network implementation, users can save a lot of time, effort and resources when they put in a few extra hours at the planning and implantation phase of setting up networks. Basic rules: Document changes, document addition, document removal, document everything you do or change in the system. If a change causes problems later on with the system due to unforeseen consequences, documentation will help solve said problems.

Network Topologies

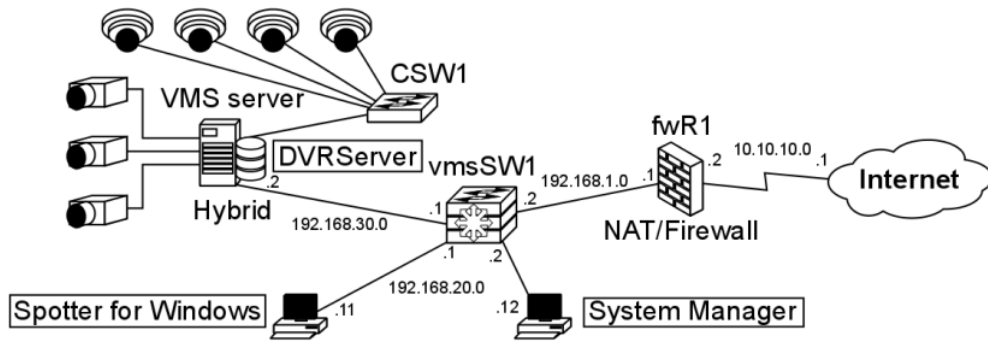
As the first step with system networking, plan out the physical network and maintain current topologies for record-keeping. Anything well planned is already halfway done. A clear network topology is useful in narrowing down network bottlenecks, failure points and sections that could be improved or expanded. A network topology should map the whole network the system would encompass. This includes the cameras, recording devices running DVRServer and other servers, decoders, connection types, network switches and any workstations with Spotter for Windows and System Administrator applications installed and connected to the network.

Also, if the VMS network is connected to the Internet, firewalls or gateway servers should be included in the topology. Networks the devices have been assigned to should also be marked, as well as device IPs on the relevant connections. Switches and routers should have their interfaces marked as well, either on the topology itself or on a list close to the devices. If VLANs have been assigned, these need to be marked as well. The software contained within the end devices do not need to be marked, but these should be recorded in the documentation as well. An example topology below has the VMS network connected to the internet through a firewall running NAT. The clients and the hybrid recording VMS server (running SMServer) are connected to the firewall through a Layer 3 switch, so the connections within the network can be segmented into their own subnets. There are a number of analogue cameras connected to the capture card of the server and it is connected to the VMS network and the camera network.



Mirasys VMS Networking White Paper

The camera network is connected to the DVRServer through an unmanaged Layer 2 switch, so their packets are switched by MAC addresses alone. Segments of the VMS are placed under their own subnets for easier navigation and possible expansion, e.g. with more users or more servers. These subnets can be placed under VLANs in the Layer 3 switch's configuration.



The interfaces of the switches are marked and labelled. The unmanaged Layer 2 switch's IP addresses don't need to be configured for this particular setup.

Hostname	Interface	Interface label
----------	-----------	-----------------



Mirasys VMS Networking White Paper

CSW1	Ge0/0	SWITCH-RECORDER
	Ge0/1	CAMERA1
	Ge0/2	CAMERA2
	Ge0/3	CAMERA3
	Ge0/4	CAMERA4

Hostname	Interface	IP address	Subnet mask	Interface name
vmsSW1	Ge0/0	192.168.1.2	/28	vmsSW1-fwR1
	Ge0/1	192.168.30.1	/24	vmsSW1-Recorder
	Ge0/15-24	192.168.20.1-10	/24	vmsSW1-client

If you are unsure as to how to keep up topology illustrations and related device and network documentation, it is recommended to consult your IT department or an ICT expert.

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300

- info@mirasys.com

- www.mirasys.com

Physical Setup

Along with a clear topology, planning the routes of physical connections through a building or site can save a lot of heartache and time. Mapping the devices and cabling in a site, even if it's a three-room section of a floor, can help in selecting the cabling that will be used as well as the placements of the devices.

With cabling, the appropriate length cabling should be used to reduce the chance of interference or overheating coming from coiled cables or straining them when they're just that inch too short for the required distance. Distances between the ports on networked devices need to be pre-planned or measured to make sure the correct cable will be gotten for it. Cable labelling can be done with taped labels or with cable colours. Colours will help in grouping the cables to the connection groups they're a part of. Cables should also be bunched or guided to make sure they do not get tangled. Using cable trays can keep them out of the way and prevent any tripping or snagging hazards.

The actual cables themselves should be planned by the estimated amount of interference they might face on their routes. Electromagnetic interference affecting cables can lead to image quality deterioration or even complete image loss. Standard cables are UTP (Unshielded Twisted Pair) cables. When interference is expected or encountered, STP (Shielded Twisted Pair) cables should be used.

Elements that cause EMI:

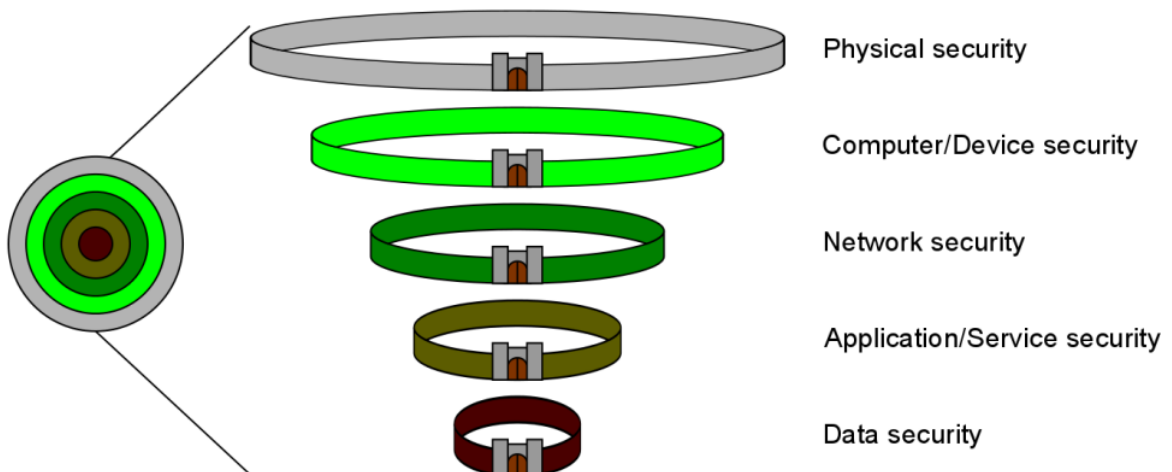
- **High Voltage Wiring:** Power wiring can interfere with data transmission even when run parallel to each other. Even wiring running a compliant distance apart within a grounded raceway can be a source of video interference. The best practice is that any data cabling sharing the same raceway with power cables, regardless of how either is contained, must be run using an STP cable.
- **Inductive Sources:** Data cabling run near common electromechanical components like electric motors, power transformers, magnetic coils, or solenoids can introduce significant EMI.
- **Radio sources:** Common low powered communication radios disrupt data transmission. High-powered repeaters or transmitters necessitate using STP to eliminate problems.

Mirasys VMS Networking White Paper

- **Fluorescent Lights:** Fluorescent lights are common to light fixtures and can cause interference to cable bundles in overhead cable runs. Cable trays or STP cables should then be used.

Cybersecurity

In the field of networked security surveillance, cybersecurity is paramount. To be secure in your network, you must be educated in it. It is advisable to read all the relevant materials for each component that is to be used in or with the VMS. Cybersecurity is considered to be a layered defence against threats that would compromise sensitive systems or data. Protection can be visualized as an onion or concentric walls, with physical access to the system as the outer layer and the protected service or data at the centre.



Security for the layers generally follows the following scheme:

- Physical access to the system's network components and devices is restricted and the devices are secured in cabinets in safe locations
- Computers and other devices accessing the system require authorized login credentials to open and when opened, they're secured by virus protection software

This protects against intrusions from inside the physical location of the system or its components

- The network is secured against snooping, hijacking, DoS attacks and unauthorized outside access by firewalls, private networks or isolation

Mirasys VMS Networking White Paper

This protects against data intrusions from outside the physical location of the system or its components

- System applications on computers and services on servers require authorized logins and a connection to the system for verification
- The recorded data is secured with encryption and is only accessible to the appropriate applications used by authorized users

Each layer is to be maintained to minimize the chance of recorded data or system information ending up in unwanted hands. Remember, security begins with you.

User Privileges

Only allow essential users to have elevated or admin privileges on any of the devices, services or system applications. Grant access only to users you trust and the more privileges a user is supposed to have, the more trustworthy they need to be. A user should always need to check their privileges.

Virus Protection

If you maintain internet connections from within the VMS network, keep all virus security programs and firewalls up to date and functioning. Consult the documentation for the programs you have in use. Even in closed networks, you should check the systems for malware from time to time, because there are still possibilities for your devices to get infected, for example by downloading a file from a USB stick to a PC in the closed network. Also, remember to open needed ports from the firewall to enable Mirasys VMS systems to work properly. too strict firewall protection is the number one cause for problems in the VMS networks.

Passwords

One of the key aspects of cybersecurity beyond installing physical security devices, such as firewalls, is to configure all needed devices and to use non-default passwords.

Default logins and passwords are always the first to be tried in an attack. Always input new passwords to cameras and other devices. Change your devices' passwords regularly.

Another important part when it comes to passwords is to have them secured when

Mirasys VMS Networking White Paper

transmitted over a network. Password transmissions between VMS clients and servers are secured with public key encryptions. However, if you do not use a password at all, attackers snooping on the network connection are able to see this. When a user logs in, there's a login request via a TCP packet from the client to the server.

The part of the query for login that is relevant to this consideration has a string format of [...]userName.password.networkAddress[...] (password as seen by the WireShark network traffic capture tool in bold). When transmitting the query, the Spotter client encrypts it. [output omitted]
Admin....@NpxrzbgelAjA5oaQ4LvF0GGe4seCc9n37apH5goN/buAtucUbY/zwIYW
ByJEAlqQ.....10.10.11.165

[output omitted]
If you use a blank password (as in no password at all), the same query is seen without a password, tipping anyone snooping off to the fact that the system may be unsecured.

And if the server responds with an OK, the system really is unsecured. [output omitted]
Admin.....10.10.11.165

[output omitted]
To counter this, **use a password**. Any password is better than none, and a strong password is better than a simple one.

Password Strength

A strong password is at least 8-10 (recommended 12-14+) characters long, has both cases in use and has special characters and numbers in it. Even if your password is strong, it's best practice to change it regularly. It's best practice to avoid words and phrases that are easily guessed (such as password12345), as crackers can test dictionary words in passwords along with brute force cracking that tries each possible character combination one by one. Computers can also harness graphics cards (GPUs, Graphics Processor Units) to number-crunch the passwords and try each one. As an example, a Radeon HD5770 graphics card (released for the market in 2009) can perform 3.3 billion guesses per second. Moore's law dictates that computing power doubles every two years. With multiple GPUs per computer, newer GPUs becoming available, distributed computing and botnets, computer systems with unrestricted login tries could face significant attempts at breaking through.

Mirasys VMS Networking White Paper

If your password is to be made of a phrase or certain words, they should be as obscure as you can think of, and they need to be turned into a form that is as complex as it can be through character substitution and spelling corruption. User-defined passwords made primarily through word generation can be strengthened through character swapping. Character substitution is a simple way of increasing password complexity. Randomly generated passwords also use the same character ranges. This increase is presented in the below table, where an eight-digit password is made increasingly complex: first with a case-insensitive string of letters, then with some letters made upper/lower case, then substituting characters with numbers, then with special characters.

Character type	Possible characters	Possible combinations	Crack time
Upper/lower case	26	2.09×10^{11}	2s
Mixed case	52	5.30×10^{13}	8min, the 50s
+Numbers	62	1.60×10^{14}	26min, 37s
+Special characters	95	3.03×10^{15}	8h, 24min, the 20s

Making a password nine characters long would extend PC brute force cracking time to 39 days. As an example, "Taek_Mi_2_da_Rivah" is a password that is complex, yet can be easy to remember. The words are corrupted to a degree that they can't fall to dictionary attacks and its brute force strength is brought by the fact that it is an 18-character password with numbers, upper and lower case letters and special characters, giving 3.41×10^{35}

Mirasys VMS Networking White Paper

possible combinations.
This would yield a PC cracking time of 108 quadrillion years. Even the Tianhe-2, the world's fastest supercomputer at this time, running 33.86×10^{15} operations per second would take 319 billion years to break that password with brute force. Add any character to the back of the password and it'll take 32 trillion years for Tianhe-2 to break it with brute force. Cracking a well-constructed password can be an astronomical task indeed.

Network Segmentation And Device Segregation

As mentioned in chapter 2.1, it's best practice to keep the camera and server networks on separate network segments, so there'd be less chance for camera signals to face interference from other traffic in the system and to improve system security as a safeguard against unwanted connections. This should be done with closed networks connected directly to recording VMS servers, or by setting up VLANs in the network devices. Consult an ICT expert on how to best implement network segmentation and device segregation.

[Previous](#) [Next](#)

16. Copyrights

The contents of this document are provided “as is”, and Mirasys Ltd reserves the right to modify this document as necessary and without prior notice. Any products, services, or features discussed in this document are subject to change by Mirasys Ltd. or a third party when applicable. Mirasys Ltd does not guarantee the availability of all products, services, or features.

TRADEMARKS

Mirasys, Mirasys DINA, Mirasys N, Mirasys V, Mirasys NVR, Mirasys NVR Pro, Mirasys NVR Enterprise, Mirasys VMS, Mirasys VMS Pro, Mirasys VMS Enterprise and Mirasys Carbon are the trademarks of Mirasys Ltd. Microsoft and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names may be the registered trademarks of their owners.

[Previous](#)