Raimo Hokkanen

Mirasys VMS Networking

Video Monitoring System Networking Considerations

Metropolia Ammattikorkeakoulu
Tietotekniikan insinööri
Tietoverkot
Insinöörityö
6.5.2015

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Raimo Hokkanen Mirasys VMS Networking 37 sivua + 2 liitettä (4 sivua) 6.5.2015
Tutkinto	Tietotekniikan Insinööri
Koulutusohjelma	Tietotekniikka ja liikenne
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Oppilasohjaaja Janne Salonen Tuotantopäälikkö Petri Bäckström, Mirasys Oy

Opinnäytetyö perustuu tekijän työnantajan tilaamaan Mirasys Oy:n VMS 7.3 Networking white paper –verkotusasiakirjaan. White paperin ja opinnäytetyön tarkoituksena on valoittaa lukijaa Mirasys Oy:n VMS 7.3 –videohallintajärjestelmän verkotusperiaatteista ja –tekijöistä.

Teos sisältää lyhyehkön kuvauksen Mirasysin VMS-järjestelmän osista, verkkokonfiguraatioista ja asioista, joita on huomioitava järjestelmän verkon suunnittelussa ja implementoinnissa, mukaanlukien käytettävien kameroiden verkkoliikenteeseen vaikuttavat piirteet.

Videohallintajärjestelmä on verkotettu järjestelmä IP-kameroiden ja vastaavien valvontajärjestelmien ja näiden tuottamaa dataa tallentavien servereiden välillä. Valvontadataa käytetään turvallisuuden ja valppauden ylläpitoa varten herkillä alueilla.

Verkotetut järjestelmät vaativat tietoverkon asentamista ja ylläpitoa, jotta laitteiden yhteydet keskenään ja Internetiin toimisivat. Tietoturvallisuus, datan eheys ja laitteiden tuottama verkkokaistan kulutus asettavat omia vaatimuksiaan valvontajärjestelmän verkolle.

Työn tutkimus perustuu suurimmaksi osaksi yrityksen omiin materiaaleihin ja ensikäden kokemuksiin järjestelmän kanssa. Työn yhteydessä on suoritettu tiedonhakua ja yhteistyötä yrityksen tuotekehitys- ja asiakasneuvontaosastojen kanssa.

Avainsanat	turvavalvonta, verkotus, videohallintajärjestelmä, serveri, video

Abstract

Author(s) Title Number of Pages Date	Raimo Hokkanen Mirasys VMS Networking 37 pages + 2 appendices (4 pages) 6 May 2015
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Communication and Data Networks
Instructor(s)	Janne Salonen, Principal lecturer Petri Bäckström, Chief of production, Mirasys Ltd.

This thesis was carried out for the author's current employer Mirasys Ltd. The purpose of this thesis, and the Mirasys Ltd. VMS 7.3 Networking white paper it is based on, is to elaborate on the Mirasys Ltd. VMS 7.3 video management system's basic components and networking principles, considerations and factors.

The work contains a brief description of the networking configurations used on Mirasys VMS systems and network planning considerations that need to be taken into account when planning and implementing the systems.

The research is largely based on company materials relating to the system and possible network configurations that can be used with the system. First-hand cooperation was conducted with the company's product development and support departments.

The Video Monitoring System is a networked system between IP cameras and other surveillance devices and servers that record the data gathered by them. Surveillance data is used to maintain security, safety and vigilance at sensitive locations.

A networked system requires the setup and maintenance of networks between the system components and the internet. Information security, data integrity and high bandwidth consumption by the surveillance equipment place their own demands on any network used for video surveillance.

Keywords	Virtual, surveillance, video, network, monitoring, server

Table of Contents

Glossary of Terms

Administrator	A privileged computer system user
Analog camera	A camera sending its data in a continuously variable electrical signal
Applet	A small, single-task application that does not require installation
Artifact	An aberration appearing in a compressed image
AVM	Agile Virtual Matrix, a Mirasys proprietary plugin where security camera feeds are displayed in an array on a wall with multiple screens
b/s	Bits per Second, measure of bandwidth.
B-Frame	Bi-directional predictive inter-frame
Broadcast	Network-wide transmission of an audio or video stream
Capture Card	A hardware card used on recording servers to convert analog signals into digital information
CIF	Common Intermediate Format, a video resolution format for analog cameras
CLI	Command Line Interface, a method of interacting with a computer system through a text representation
Closed network	An information network of computers or other digital devices not connected to an internetwork
Codec	Format of video compression that enables digital video compression
DNS	Domain Name System, method of converting IP addresses to hostnames
Domain	Shared network of computers and the user accounts for them in a corporate environment
DoS	Denial-of-Service, a digital attack that floods a network target with connection requests
Driver	A software component used to interact with hardware devices
DVRServer	VMS recording server service
Encoder	A device that converts analog signals into IP packets and sends them over an IP network
Ethernet	A physical network connection standard
Firewall	A network security measure, screening network traffic and blocking potentially harmful packets
FPS	Frames Per Second, measure of image refresh rate

Gain	The relationship between the number of electrons acquired on an image sensor and the image signal
Gateway	An edge device between two networks, providing routing information for data trafficked between them
GPU	Graphics Processing Unit, a processor chip specialized in calculating, generating and outputting images from data
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.
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
Hostname	Plain name of a digital device in a network
HTTP	Hypertext Transfer Protocol, an application layer Internet protocol used for sending requests between a web client and a web server
ICT	Information and Communications Technology, term for fields relating to telecommunications and information networking
I-Frame	Intra-frame, a full image frame in a video stream
IP	Internet Protocol, a layer 3 networking protocol
IPSec	Internet Protocol Security Architecture, security suite used to secure packets between routers, forming VPN tunnels over IP networks
IPv4	A version of Internet Protocol. Allows 32 bit IP addressing
IPv6	A version of Internet Protocol. Allows 128 bit IP addressing
ISP	Internet Service Provider
IT	Information Technology
Java	A programming language, often used on web sites for scripts and applets
LAN	Local Area Network, a small, usually home or office-level networked area
Layer 2	2nd layer (Data Link) of the OSI model, transfers data between adjacent network nodes in a WAN or between nodes on the same LAN segment
Layer 3	3rd layer (Network) of the OSI model, used for packet forwarding, including routing through intermediate routers
MAC address	Media Access Control address, a physical-layer identifier
Master	VMS server device with the Mirasys SMServer service installed on it
MJPEG	Motion-JPEG, a video compression format

Multi-channel device	A device that can send multiple signal channels, each carrying a certain number of video streams
Multicast	Transmission of an audio or video stream from one computer to others selected to be the targets
Multistreaming	A digital device sending multiple 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
NTP	Network Time Protocol, a communication protocol used to sync a networked devices time with a time server
OSI model	Open Systems Interconnection model, an abstract layered representation of a communication system
P-Frame	Predictive inter-frame
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 through a network gateway
PTZ	"Pan, Turn, Zoom," two-axis remote-controlled camera
Quantization	A lossy compression technique achieved by compressing a range of values to a single quantum value
RTP	Real-time Transport Protocol, a networking protocol used for delivering audio and video over IP networks
RTSP	Real-Time Streaming Protocol, a networking protocol used to control video streaming between a client and a video source
Slave	A recording VMS server with the Mirasys DVRServer service installed and enabled on it
SMServer	System Manager Server, VMS master control service
SMTP	Simple Mail Transfer Protocol, standard transfer protocol for e-mail transmissions
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
TCP	Transmission Control Protocol, networking protocol
UDP	User Datagram Protocol, a connectionless networking protocol
Unicast	Transmission of an audio or video stream from one computer to another
UPnP	Universal Plug and Play, a set of networking protocols that permits networked devices to discover and establish connections
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
VM	Virtual Machine, a virtualized computer running in a physical computer’s programming
VMD	Video Motion Detection, method of detecting motion in a video stream by comparing frames with each other; changes are logged as motion
VMS	Video Monitoring 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
WLAN	Wireless LAN, wireless local networking. Also known as Wi-Fi.

1 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 on building working surveillance systems in various network models.

All data communication within the Mirasys VMS system use TCP/IP protocol and networks. The use of virtual private networks (VPN) 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. [1]

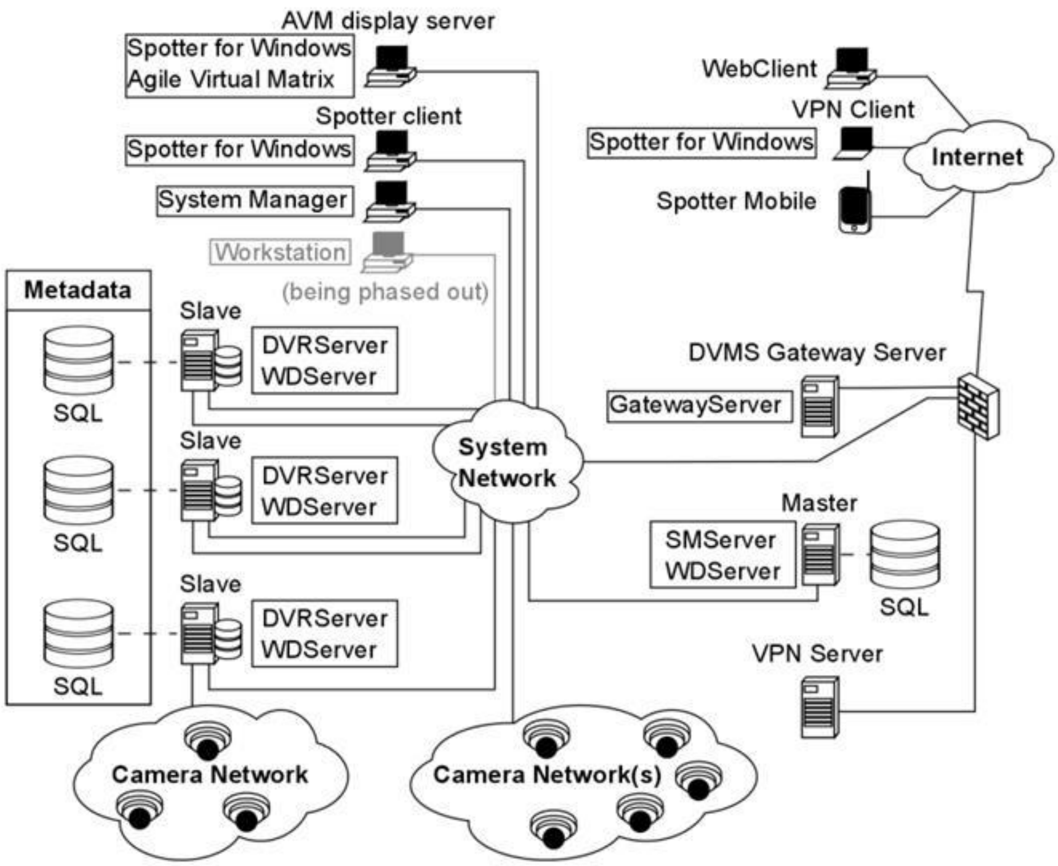


Figure 1. Representation of the VMS system network architecture and the components that are included in it [2, p.3]

2 Network Requirements

Given requirements apply to all Mirasys VMS installments. [1]

2.1 General

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. Each connection between the system devices over a TCP/IP network need to be with Gigabit Ethernet.

Control of PTZ cameras requires the network to have low latency in order to make dome control as responsive as possible. [1, p.5]

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:

- **Physical separation**, where the cameras are connected to their own switch, and this is connected to a recording server
- **Logical separation**, using VLANs on a common switch to separate device and user groups and route their traffic accordingly

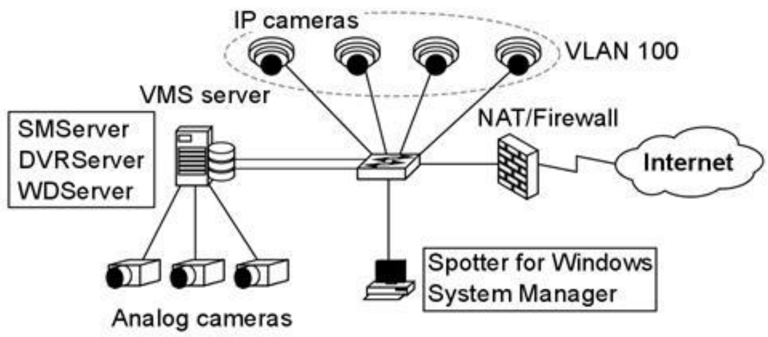


Figure 2. Single-server, single-switch site network using VLANs to separate IP cameras.

2.2 Network card settings

Network card setting requirements:

- Interrupt Moderation Rate → Extreme
- Receive Buffers/Receive Descriptors → 2048
- Transmit Buffers/Transmit Descriptors → 2048

[1, p.6]

3 Mirasys VMS system components

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.

3.1 Signaling and streaming protocols

- **UDP** (User Datagram Protocol)
    - Used to stream video feeds from the connected cameras
    - Any connection difficulty is immediately noticed as a loss in video feed
    - System network needs to be well constructed
- **RTSP** (Real-Time Streaming Protocol)
    - Used to establish and control video streams over a network.
    - Communications between a client and a recording VMS server send instructions on playback and play speed
- **TCP** (Transfer Control Protocol)
    - Used for signaling between the devices and components of the VMS network and the Internet at large

- **HTTP** (Hypertext Transfer Protocol) and **HTTPS** (Hypertext Transfer Protocol over TLS)
    - 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
    - Used to contact camera GUI in direct connection
    - Some drivers may also use HTTP to receive motion detection data, video streams or PTZ signaling

3.1.1 System Ports

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

- Port 5008
    - For signaling 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 signaling between SMServer and DVRServer for time synchronization, setting 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

WebClient, Spotter Mobile and GatewayServer specific ports:

- Ports 9000 and 9999
    - Between WebClient / Spotter Mobile and GatewayServer.
    - Port rule: open inbound

[1]

AVM specific ports

- Port 8084
    - Between SMServer and the Spotter for Windows client
    - Port rule: open inbound

Cameras can use the following ports in their operation:

- HTTP Port 80
    - Default port for HTTP traffic, used by some cameras for communications
- HTTP Port 8080
    - Used by some cameras for PTZ control communications
- HTTPS Port 443
    - Default port for HTTPS traffic, used to securely communicate with a camera's system
- RTSP Port 554
    - Default port used on the VMS to traffic stream control signals
- RTSP port 7070
    - Default stream control port for some camera drivers
- UDP Ports 3556-4556
    - Used on the VMS to receive feeds from the cameras. Each video stream occupies two sequential ports in the port range.

3.2 Applications

3.2.1 VAU

VAU (VMS Application Updater) is a service application without a user interface. It is used to automatically update user applications to the latest versions from the Master SMServer during startup.

3.2.2 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 DVRServer 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. [4]

3.2.3 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. Spotter can be used as a specialized video wall application, as well. [5]

3.2.4 WebClient & Spotter Mobile

The WebClient application can be used with 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. [1]

3.3 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 DVRServer requiring two NICs and lots of digital storage space.

Each service must be installed on a computer or server with Microsoft operating systems Windows 7, Windows 8, Server 2008, Server 2008 R2 or Server 2012. The server can also be a virtual device run in Hyper-V and VMware virtual machine platforms. Microsoft Server 2008 and Server 2008 R2 are not able to support capture cards. [1]

3.3.1 SMServer

System Management Server (SMServer) 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.

[1]

3.3.2 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. 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. Servers running DVRServer also capture analog signals through 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. [1]

3.3.3 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.

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 error-tolerant state. Rebooting will never be done more than once per 6-hour cycle, with subsequent reboot-triggering errors 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. [1]

3.3.4 Optional Servers

AVM Display Server

AVM (Agile Virtual Matrix) Display Servers are any devices that run a Spotter for Windows client and display footage over multiple (more than two) screens simultaneously.

GatewayServer

The GatewayServer contacts the SMServer through TCP port 5008.

When the WebClient applet or the Spotter Mobile application is used, GatewayServer and the applet or application communicate by default through TCP ports 9999 (applet download) 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). [1]

Failover Server

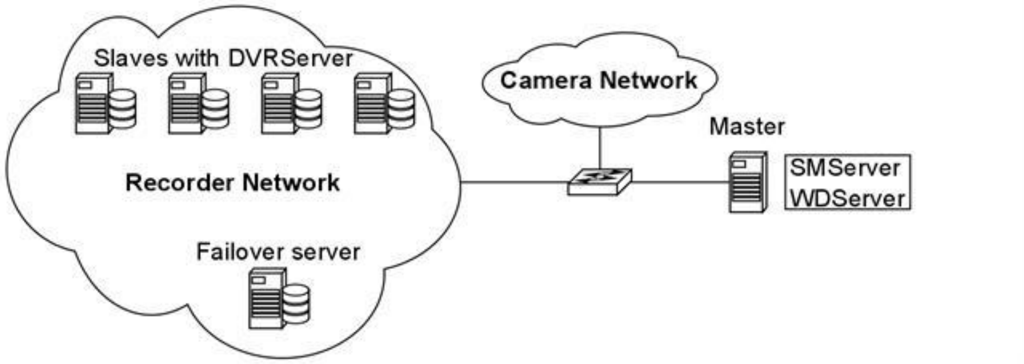


Figure 3. VMS with a Failover Server in the Recorder network

Failover servers are networked devices that are on 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.

Failover settings can be controlled from 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. [6]

4 Using Mirasys VMS with different networking components

When building a Mirasys VMS system, usability, security issues and 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 virtual private network (VPN) or an effective firewall are good alternatives.

4.1 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 is the number of network bits in the address, ranging 8-32. The smaller this is, the more hosts are allowed on a subnet.
  - In a subnet, the first address is always the network address and the last address is the broadcast address. All addresses between these can be assigned to hosts.
- 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. The subnet is prefixed /N, where N indicates the number of network bits, ranging 4-128
  - The subnet is marked with the octet pairs included in the networking segment followed by the prefix.

IPv6 allows 2^{128} addresses, significantly more than the 2^{32} in IPv4. However, networked monitoring systems are usually small and closed to other network traffic, so IPv4 is used for ease and simplicity of configuration and use without fear of address exhaustion.
[7]

4.1.1 IP Addresses or Hostnames

The system can be configured to contact the servers through their IP addresses or hostnames.

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 (Agile Virtual Matrix) Display Servers in the system should also have either static addresses or static hostnames, as the connection from AVM operator console to the display servers is done with either the IP address or the hostname. [6, p.15]

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 first connection for initial configuration. Some camera models could 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.

If the system is intended to be used from outside a closed network, it is recommended to build the system using VMS server hostnames instead of IP Addresses. This makes it possible to contact the system from outside the LAN with minimal effort.

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.

4.1.2 Public IP Addresses

When using public IP Addresses with the Spotter for Windows and System Manager applications outside the LAN, an IP address is required for each DVRServer and for the SMServer.

LANs can use a private network subnet and assign addresses for devices in it 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 LAN to contact the devices therein.

Network edge devices, such as routers between the LAN and WAN, use NAT (Network Address Translation) to translate public addresses (WAN) to private addresses (LAN) and vice versa. Routers that run NAT take addresses on the LAN (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).

4.1.3 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
- 172.16.0.0/16 - 172.31.0.0/16
- 10.0.0.0/8

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 to plan and configure, and /24 subnets can be segmented into even smaller subnets as needed. [7]

4.2 Local Connections

Today most LAN connections in networks are done through 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 LAN they're connected to.

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. [7]

4.3 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.

4.4 Closed network

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 a Layer 2 switch. However, being disconnected may not be feasible or desirable in all cases, if email alerts are to be used in the system or if Internet access is required for user activities.

4.5 VLANs

VLANs (Virtual LANs) are a method of logically segmenting a LAN 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.

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. With multiple VLANs, each device needs to have an IP address configured, so the Layer 3 device can route the traffic between them.

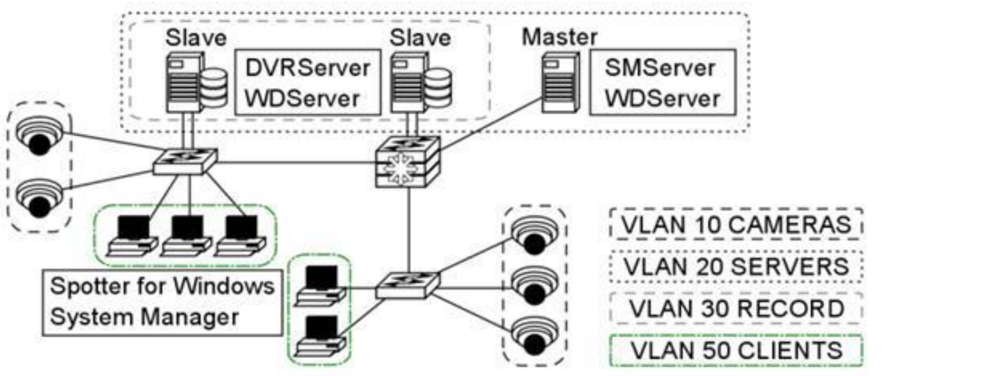


Figure 4. Example of using VLAN to segregate devices over multiple switches. Note the Slaves both have two network connections, each of which is connected to a separate VLAN. IP addresses are not shown for brevity. [8]

4.5.1 QoS

Quality of Service is a set of strategies aimed at improving data availability. Commands for them are 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 VLANs are classed for QoS, it prioritizes their bandwidth so it is not as readily consumed by other traffic and that the information going through switches does not degrade. [7]

4.6 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 LAN sites.

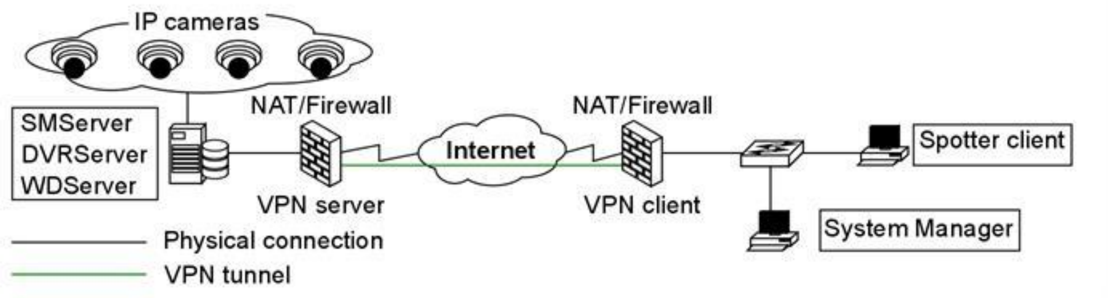


Figure 5. VPN connection between two LANs through their respective firewalls

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. 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.

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. [9] 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.

4.6.1 VPN methods

VPNs can be set up with a certain variety of methods afforded by the modern 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.

Layer 2 Tunneling Protocol

L2TP allows the creation of a Virtual Private Dialup Network (VPDN) to connect 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. [10]

Layer 3 VPNs

VPN tunneling 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) form 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 quantity 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

[11]

VPN servers

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

- Hardware VPNs
    - Purpose-built networking devices that connect to an Internet connection from within a service site and provide VPN capabilities when compared to application-based servers.

    - Usually these can support multiple simultaneous connections.
    - Normally managed through web GUIs.
- 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
    - 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 interfaces on the computer's NICs

4.6.2 Configuring a VPN

When the Mirasys VMS system is used with VPN, tunnels are created between the system's recording servers, SMServer, and client applications.

An easy way to use VPN is to create a LAN-to-LAN connection between sites. The recording VMS servers should be on the VPN server's network, and the remote site 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:

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

4.7 Firewall with NAT/Port Forwarding

Firewall devices and programs protect computers from cybersecurity threats (e.g. viruses, denial-of-service attacks and intrusions) by controlling communication between local and WAN (Internet) networks. Firewalls can be used to multiply usable IP Address space in a network and to manage NAT (Native Address Translation) changes.

In this section, firewalls are considered as firewall devices protecting all computers in the LAN in which the servers with DVRServer and the Master with SMServer are located. In a Mirasys VMS system with a firewall with NAT/Port Forwarding configured, server hostnames should be used instead of IP Addresses.

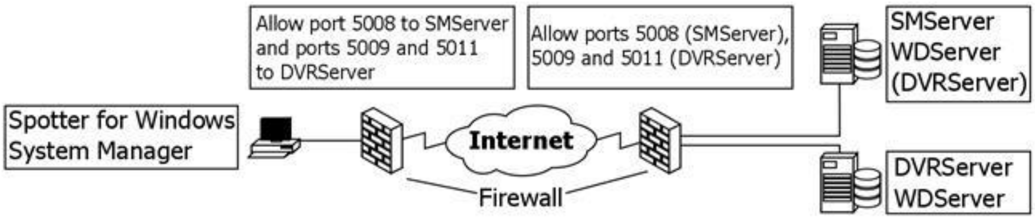


Figure 6. Basic firewall solution for a VMS system

A further note on NAT solutions for the system would be:

- Static NAT can be used between the servers and the client programs.
- Dynamic NAT **cannot** be used because the IP addresses would change.
- Single-address NAT works if there is only one VMS server in the NAT system. It does not work if there is more than one server in the same system.

4.7.1 Configuring the firewall

If the system is contained behind a firewall, and System Manager application client is located outside of the LAN, necessary communication ports have to be opened in the firewall. If a software firewall is used, make sure that the dedicated ports are open on all Mirasys VMS system computers.

Guidelines for systems with firewalls:

- Use static IP Addresses on the system devices
- Allow ports 5008-5011 to be open in the firewall to enable connections from outside the LAN (the client applications)
- In the client application computers run from outside the LAN, change the settings in the file hosts as described above
- If port forwarding technique is used, define the SMServer and DVRServer addresses to be WAN site firewall addresses
- In the LAN, no additional changes to the settings need to be done
- GatewayServer needs ports 9000 and 9999 to be open to the outside
- If e-mail notification is used in the system, keep SMTP port 25 open
- If IP cameras are used in the camera network, allow HTTP port 80 (default, can be configured to other ports) to be open to the servers

4.7.2 Configuring external client computers

If a firewall with NAT or port forwarding is used, the client computers need to be configured to use server names instead of their IP Addresses.

If there is only one public IP Address (NAT, port forwarding), there can be only one device running DVRServer at the site, and the SMServer needs to be installed in the same computer.

4.8 DynDNS

Dynamic DNS (Domain Name System) services resolve IP addresses to simpler hostnames, e.g. recorder.dyndns.xx instead of 127.0.0.1. When addresses are dealt to the devices by a DHCP service, 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. [7]

4.9 Domain

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 services 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.

4.10 SQL Server databases

SQL databases refer to shared relational databases in a LAN that use 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.

4.11 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 LAN. The purpose of a virtual machine host is to essentially simulate a network segment and device collection. 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.

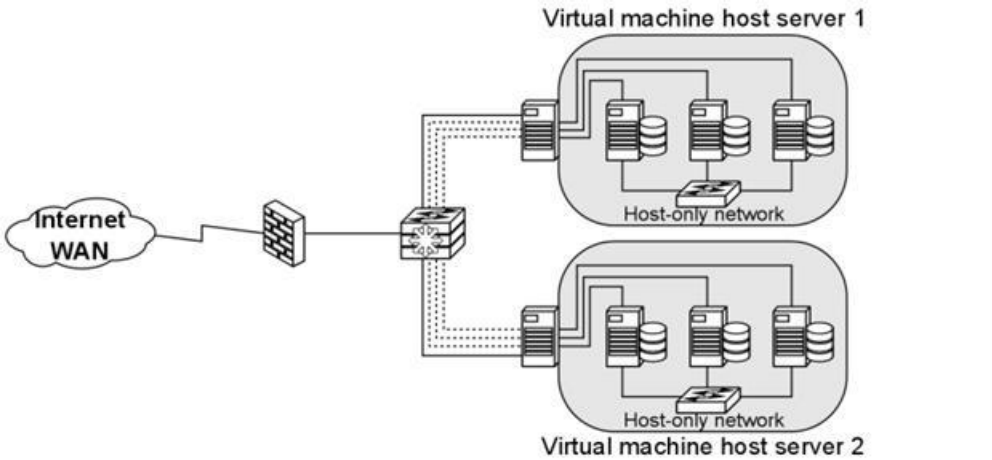


Figure 7. Internal (virtual) networking of virtual machines inside VM hosts and exterior connections to the physical network. [12]

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 L3 switch).
[13]

Table 1. Behavior of VM communication when connected to VLANs [13]

	Same VLAN	**Different VLAN**
Same host	All communication between the virtual machines is done internally through a virtual switch external devices are not involved	Traffic between VLANs is routed by a Layer 3 device.
Different host	Communication is trafficked through their physical hosts' NICs and a switch. **Physical hosts must have a distributed virtual switch.	Traffic between VLANs is routed by a Layer 3 device.

4.12 UPnP

Universal Plug and Play is meant to automate device discovery and configuration on a LAN, aiming to eliminate manual port forwarding and create automatic port mapping.
[7]

4.13 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 from the same source. This source should be either a public time server or a device set up as a time server in the LAN.

There are three time protocols used for time syncing:

- NTP (Network Time Protocol), intended to synchronize all participating computers to within a few milliseconds of UTC (Coordinated Universal Time). The protocol does not transmit time zone or daylight savings time information.
- SNTP (Simple Network Time Protocol), 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. **Not recommended**.

[7]

4.14 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.

4.15 Multicasting

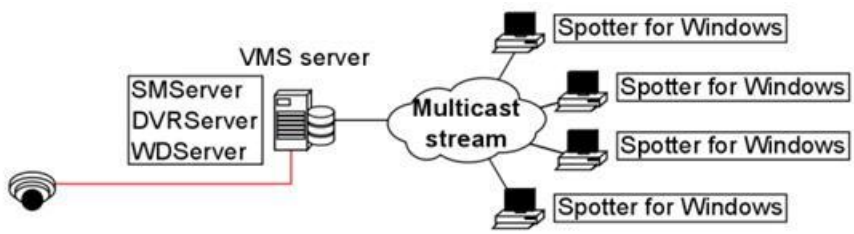


Figure 8. Multicast streaming from the VMS server to multiple viewing clients

When using multicast, a single instance of each video channel is sent to the LAN. All applications in the LAN can receive the stream, so network bandwidth usage is much lower than when sending stream for each streaming application separately.

4.16 Multistreaming

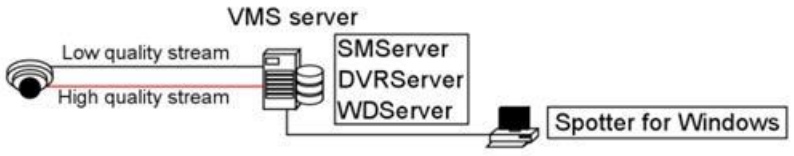


Figure 9. A low quality stream is used for real-time monitoring and a high-quality stream is used for recording

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.

Remote Workstation

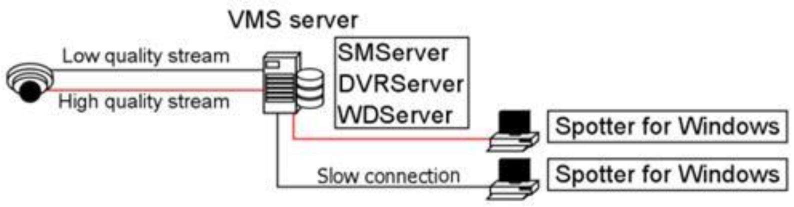


Figure 10. Connecting a remote workstation to the VMS server

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 center, 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.
[1]

4.17 Edge Storage

The Edge Storage functionality enables uninterrupted recording during network disconnects between the camera and the server with DVRServer. During connection failures, the recorded footage is saved on the camera's local data storage, e.g. a SD-card. Once network connection has been re-established, the saved video is transmitted from the camera's local storage to the server.

This feature is configured solely through the camera's own configuration utility, and it doesn't require any modifications in the System Manager application.

5 Mirasys VMS 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.

Note that if monitoring is performed directly on a server (e.g. a Spotter client is installed directly on a server running DVRServer), the video streams do not create any network load, but may require more computing power from the server itself.

5.1 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.

5.2 Local Recording

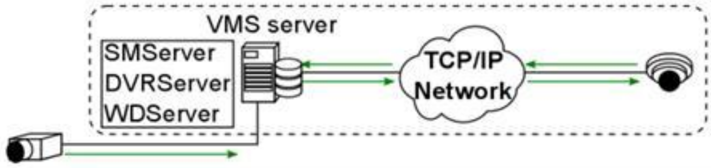


Figure 11. Recording footage with analog and IP cameras

Local recording consists of cameras relaying video signal to the recording VMS servers either directly or through the network. Network feeds are always received from IP sources, which are either IP cameras or IP encoders. Analog signals are received directly.

5.3 Real-Time Monitoring and Playback Viewing

An end user can view one or multiple video or audio streams from one or multiple instances of DVRServer. 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.

In playback viewing, the user can view one or multiple video or audio streams from one or multiple instances of DVRServer. Each video or audio stream is transmitted from the recording servers to the Spotter client as a separate stream. 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. [1, 4, 5]

5.4 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 amount of resources provided to the additional views based on the needs of the alarm view.

5.5 Exporting Media

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 medium. Exporting can also be done with a command line exporter that is included with the GatewayServer and is also available through Mirasys customer support.

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 undue burden on the network.

5.6 Bandwidth Usage Examples

The following table shows examples of how much bandwidth different image formats can consume. Different environments affect the bandwidth that a camera consumes, along with any special attributes with the hardware.

Table 2. Camera resolution, frame rate, hardware and location effects on bandwidth

Resolution	FPS	Location	Bandwidth (Mb/s)	Notes
CIF	5	Office	0.05	-
720p	10	Conference Room	0.50	-
720p	30	Intersection	4.00	-
1080p	10	Conference Room	2.00	-
1080p	30	Intersection	8.00	IR
5MP	15	Office	4.50	Panoramic
4K	30	Intersection	7.00	-

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

5.7 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. One of these is scene complexity. Scene complexity denotes activities and details contained within a viewed scene, but this factor is not a straightforward thing to evaluate.

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 a video transmission, the more resources are used on the other end to "unpack" the video. While this chapter focuses on balancing video performance and quality with bandwidth, there is a third dimension of computer performance in the background. [14]

5.7.1 Resolution

Image resolution is classified into different resolution formats, with defined dimensions. On average, a linear relationship exists between pixel count and bandwidth. However, while resolution might be a reasonable ballpark indicator of bandwidth, different camera models can have different rates of increase. [15]

- Analog format is dependent on analog transmission
    - Resolutions are based on the CIF standard
    - Analog sources produce no IP traffic, except when converted and transmitted by IP encoders
- Digital images are transmitted as collections of pixels
    - Each image defined as columns and rows pixels
    - Most resolutions fall on a 4:3 or 16:9 aspect ratio

5.7.2 Frame rate

Frame rate impacts bandwidth, but for inter-frame codecs such as H.264, 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. [16]

5.7.3 Color

Color can be thought of as a third dimension for an uncompressed frame's size. Each pixel has a certain pixel depth that determines its color. At most, 32 bits can be used for a pixel's color code. Oversaturated image colors increase image complexity through more pronounced colors and color bleeding. Desaturation gives small decreases in bandwidth, usually about 10%. [17]

5.7.4 CODECs, compression and I- and P-frames

CODECs are information storage methods that compress image data for transmission over a connection for decompression at the other end. This is the primary method of saving bandwidth with video and image data. Various CODECs function in slightly different ways in compressing images and displaying video streams.

Compression has an inverse relationship to bandwidth: the more compressed a video or image is, the lower bandwidth will be. Compression simplifies the data in an image file by reducing blocs of pixels into single quantum values. These values are decompressed by playback media.

Intra-frame codecs broadcast their entire videos in full I-frames, while inter-frame codecs transmit far fewer full frames and fill the gaps with predictive P-frames. P-frames only display the parts that have changed in comparison to a reference frame. B-frames predict both of the previous, enabling further compression at the cost of additional encoding artifacts. In almost all security camera 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 encoding artifacts, while more than one I-frame per second provides little visible benefit. [18, 19]

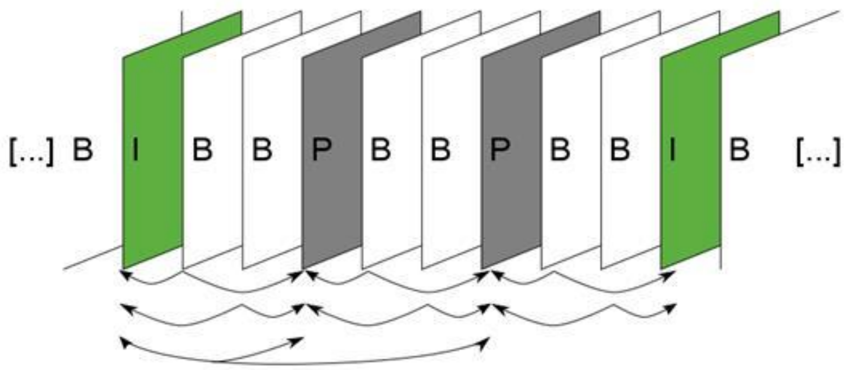


Image 1. Relation of I-frames, P-frames and B-frames. The lines of arrows represent the reference relations for the B-frames and P-frames. [18]

5.7.5 Lighting Levels, Gain control and Wide Dynamic Range

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. [20, p.30]

Table 3. Lighting levels of varying conditions [20]

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

Digital noise in low light conditions can be reduced primarily with two methods:

- **Digital noise reduction** compensates for and smooths out digital noise
- **Integrated infrared** functions as low-level night vision, improving image lighting levels

[21]

Gain control is a critical factor in low light surveillance video. It is generally only noticed when the negative side effective of aggressive gain levels are seen, namely noise on the video. To maintain good video quality, gain control is necessary. [22]

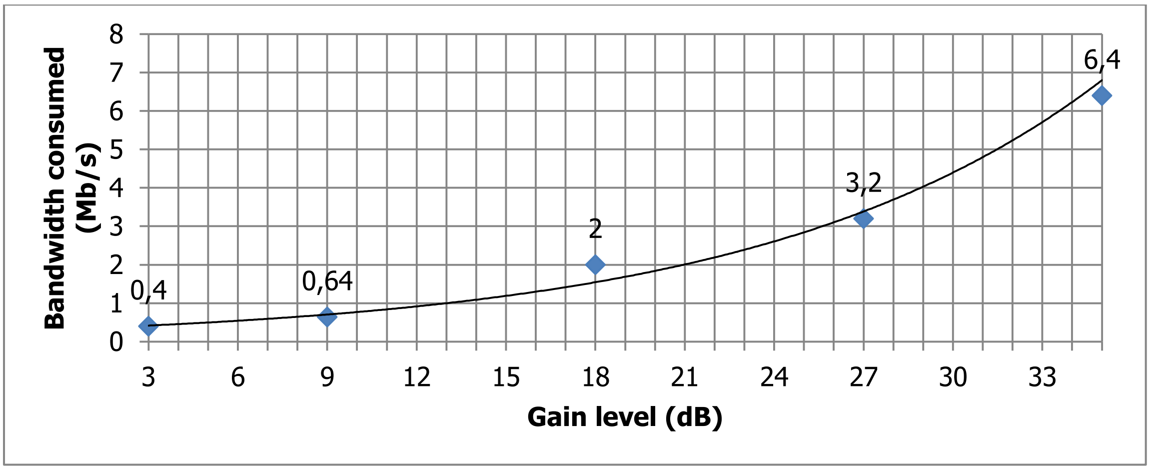


Chart 1. Bandwidth vs gain level tradeoffs [22]

Wide Dynamic Range (WDR) 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 colors in some scenes, making compression easier. [17]

5.7.6 Field of View

Camera field of view impacts video bandwidth with two factors: 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. Tightening the field of view can usually screen out unnecessary areas from the recorded video. Conversely, 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.
[24]

Aspect ratio

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. [25]

Camera placement

- **Overhead**
  - Records large areas from long distances
  - Fine detail not needed, so standard definition sensor with wide-angle lens would be sufficient
- **Detail view**
  - Records specific scenes from a short distance
  - HD or megapixel sensors needed, PTZ capability optional

[26]

5.7.7 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. [24]

5.7.8 Camera driver solutions

Choosing between variable bitrate (VBR) vs constant bitrate (CBR) 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. VBR enables a higher frame rate in the event of alarm activation. [27]

5.7.9 Motion Detection

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.

5.8 Streaming options

The 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. Each transmission multiplies the bandwidth from a particular camera.

5.9 Network planning impact on bandwidth

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

- Bandwidth consumption by camera model
- Number and distribution of cameras
- The distance (administrative or physical) to the server from the cameras assigned to it through the system

- Network connection bandwidth capacity
- Pre-existing load on networks
- 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

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. The video needs to be transmitted between the end devices. If it goes over an IP network, bandwidth is required.
- **Server to client**: Often, a user is viewing the footage on a device that is connected to a different IP network than the server.

6 Conclusions

The Mirasys VMS is at its core a relatively simple idea as far as networking is concerned, but this simplicity can be deceptive, as the primary concern of bandwidth is affected by a myriad of factors, some of which can never be in the user's control. While the vast majority of factors can be counted for in planning the implementation of the system, compromises will sometimes need to be made between the desired bandwidth consumption and the desired image/video quality.

The use of the different servers and the user applications (System Manager in particular) allow for great latitude in controlling and monitoring the relevant system network bandwidth use even on small, closed networks with unmanaged devices. The scalability of the service and its readiness to be used with various secured measures for WANs (namely VPN, NAT and web service) are also of great use in larger environments requiring large enterprise-level networks.

On a small scale, the system and local networking can be easily taught to primary users. The required knowledge base for configuring and maintaining larger system networks should be well within the expertise of an average network-specialized ICT engineer.

References

1 Mirasys VMS Networking White Paper. 2013. Mirasys Ltd.

2 Mirasys VMS System Architecture PowerPoint. 27.05.2014. Mirasys Ltd.

4 Mirasys VMS 7.3 - Administrator Guide EN. 2015. Mirasys Ltd.

5 Mirasys VMS 7.3 - Spotter User Guide EN. 2015. Mirasys Ltd.

6 Mirasys VMS 7.3 Installation Guide. 2015 Mirasys Ltd.

7 IPVM 2015 Networking Book. 2015. IP Video Market.

8 www.axis.com/products/video/about_networkvideo/vlan.htm Axis Communications AB. VLANs. Retrieved 13.3.2015.

9 http://tools.ietf.org/html/rfc894 Network Working Group of the IETF. RFC 894. Charles Hornig. April 1984. Retrieved 23.3.2015.

10 www.networkworld.com/article/2163334/tech-primers/what-can-l2tp-do-for-your-network-.html NETWORKWORLD. What can L2TP do for your network? Tom Parkin. Posted 6.2.2013. Retrieved 11.3.2015.

11 www.techopedia.com/definition/30748/vpn-concentrator Techopedia. VPN Concentrator definition. Cory Janssen. Retrieved 11.3.2015.

12 http://blog.sourcehosting.net/2008/04/18/routing-between-vmware-host-only-networks/ Source Hosting. Routing Between Virtual Machines on Separate Physical Servers. Greg Larkin. Posted 18.4.2008. Retrieved 9.4.2015.

13 http://theithollow.com/2012/03/vmware-network-traffic-routing/ The IT Hollow. VMware Network Traffic Routing. Eric Shanks. Posted 16.3.2012. Retrieved 9.4.2015.

14 http://digital.ni.com/public.nsf/allkb/E366BB70207394A186257C200067FEB8 National Instruments. Bandwidth Used by Common Digital Video Resolutions. Retrieved 11.3.2015.

15 http://ipvm.com/report/h264_mjpeg_bandwidth_quality_test IP Video Market. H.264 vs MJPEG - Quality and Bandwidth Tested. John Honovich. Posted 28.6.2010. Retrieved 2.2.2015.

16 http://ipvm.com/updates/2653 IP Video Market. Frame Rate Guide for Video Surveillance. Retrieved 2.2.2015.

17 http://ipvm.com/report/arecont_bandwidth_savings_mode_tested IP Video Market. Arecont Bandwidth Savings Mode Tested. Ethan Ace. Posted 14.2.2014. Retrieved 2.2.2015.

18 www.imakenews.com/kin2/e_article001550736.cfm?x=b11,0,w Kintronics, Inc. Bob Mesnik. 2009. Retrieved 23.3.2015.

19 http://ipvm.com/report/test_i_frame_rate IP Video Market. Test: H.264 I vs P Frame Impact. Ethan Ace. Posted 2.10.2013. Retrieved 2.2.2015.

20 IP Video Security Guide, Global Leaders in Video and Security Systems. 2010. Pelco, Inc.

21 http://ipvm.com/report/testing_bandwidth_vs_low_light IP Video Market. Testing Bandwidth vs Low Light. Ethan Ace. Posted 7.11.2014. Retrieved 2.2.2015

22 http://ipvm.com/report/gain_agc_surveillance_video IP Video Market. Testing: Gain / AGC Impact on Surveillance Video. John Honovich. Posted 9.7.2011. Retrieved 2.3.2015.

24 http://ipvm.com/report/advanced_bandwidth_test IP Video Market. Advanced Camera Bandwidth Test Results. Ethan Ace. Posted 12.8.2013. Retrieved 2.2.2015

25 www.imakenews.com/kin2/e_article000950179.cfm?x=b8v5FDQ,b25tl0b3,w Kintronics, Inc. Calculating Bandwidth. Bob Mesnik. Posted 2007. Retrieved 27.3.2015.

26 www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVS-DesignGuide/IPVSchap4.html Cisco. IP Video Surveillance Design Guide, Planning and Design. Retrieved 10.3.2015.

27 http://ipvm.com/report/vbr_vs_cbr_surveillance_streaming. IP Video Market. CBR vs VBR: Surveillance Streaming. John Honovich. Posted 17.1.2012. Retrieved 26.2.2015.

Network Topology Examples

The following illustrations are example topology diagrams on various VMS and network configurations.

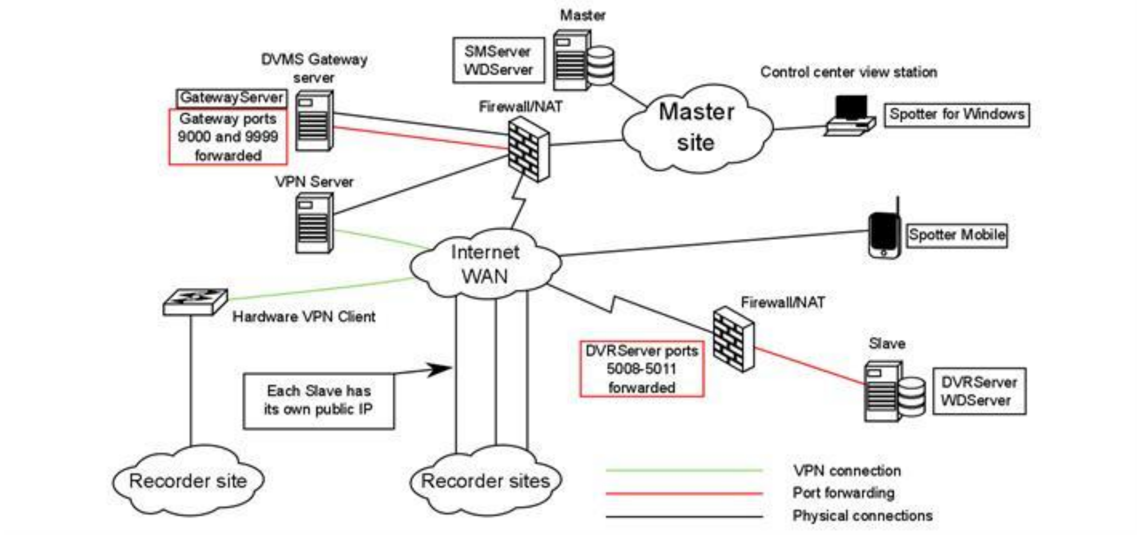


Figure 12. Control Center network diagram

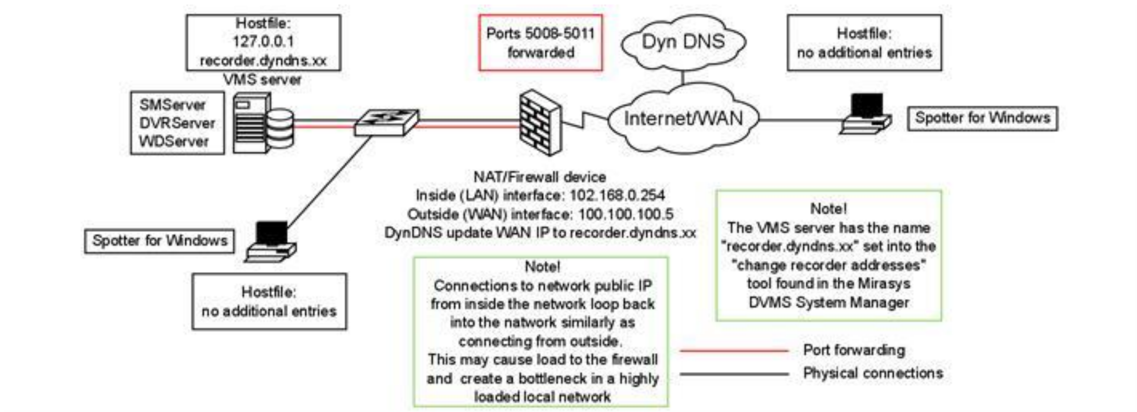


Figure 13. Dynamic DNS service with loopback

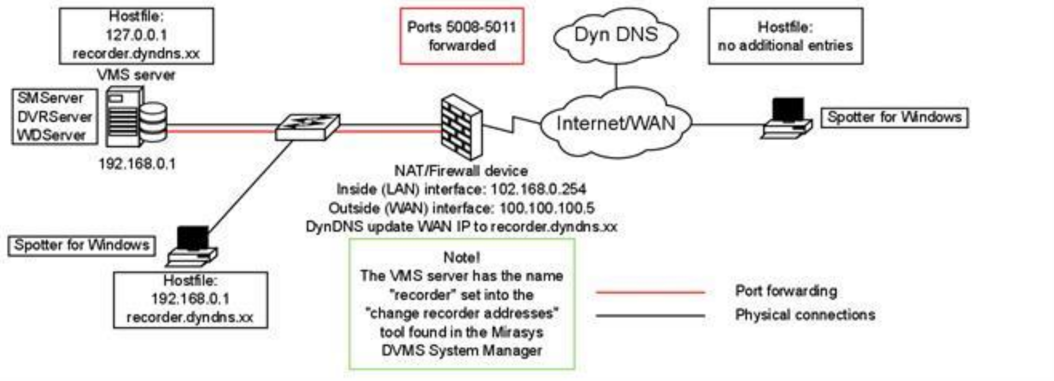


Figure 14. Dynamic DNS service without loopback

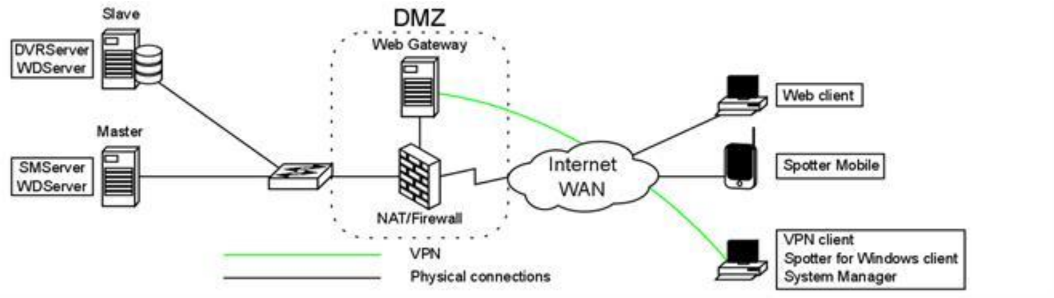


Figure 15. Web gateway on DMZ

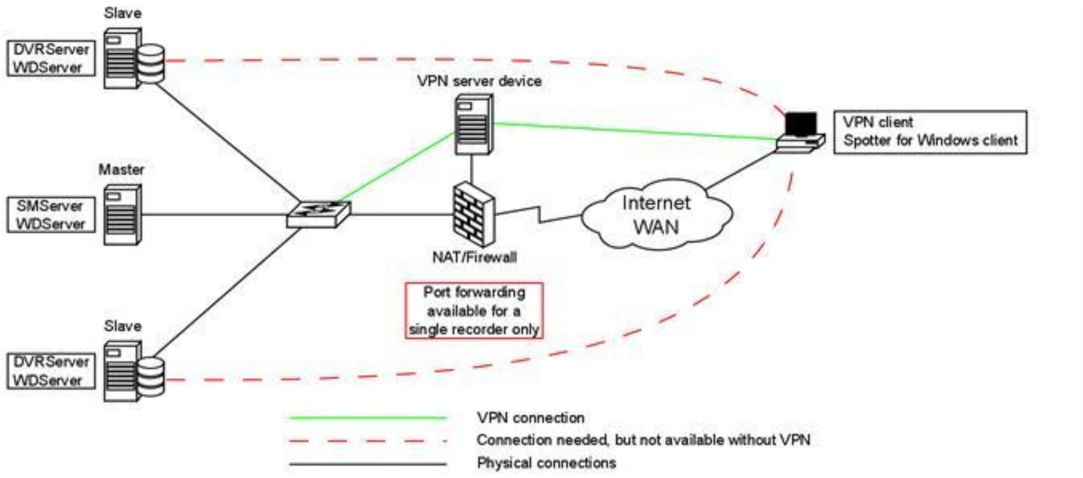


Figure 16. Network with NAT

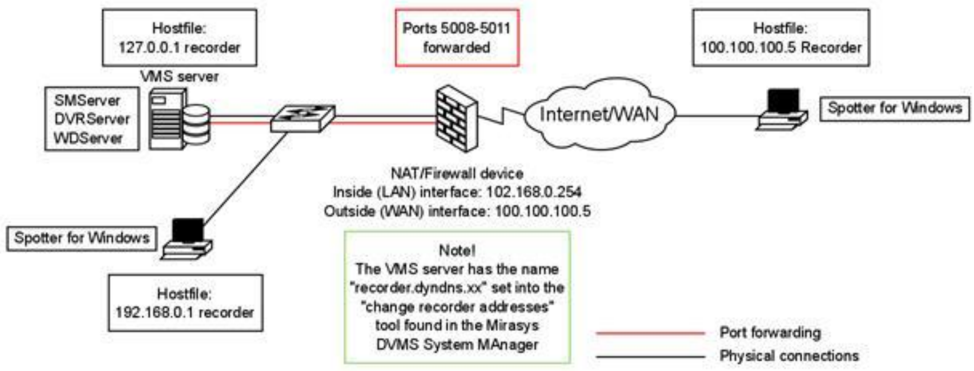


Figure 17. Spotter clients in the LAN and across the internet without VPN

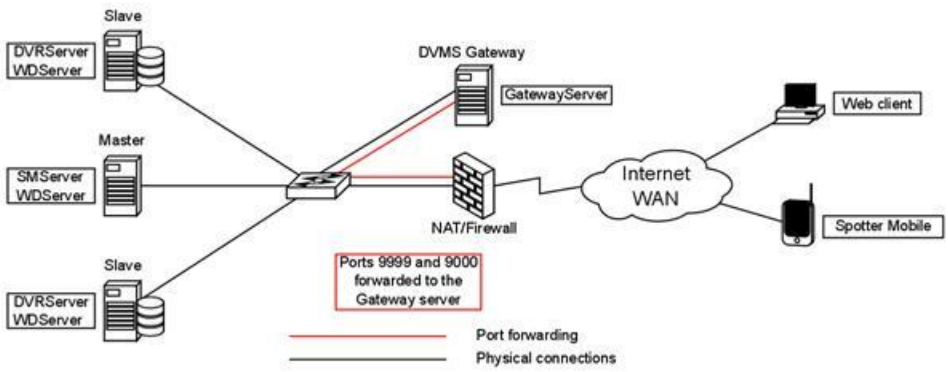


Figure 18. VMS network with GatewayServer

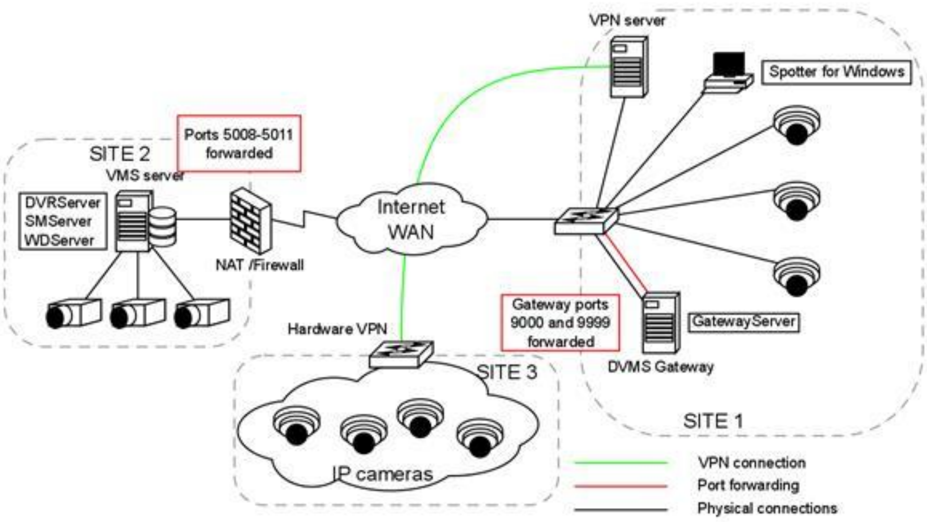
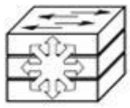
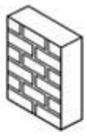
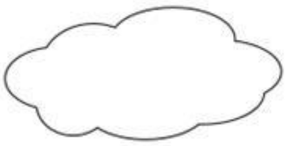
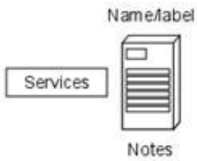


Figure 19. Complex VMS System between three sites

Topology/Illustration Legend

	Server device with record-ing capability		Database (SQL)
	Server device		Smart phone
	Desktop workstation		Analog camera
	Layer 2 switch		IP camera
	Layer 3 switch		IP camera with PTZ ca-pability
	Firewall device/router		
	Network		Labeling format