

White Paper - Surveillance Suite Design Considerations

Surveillance suites provide a mechanism primarily for viewing, recording and reviewing video via computer network hardware, networked cameras, networked digital video recorders (DVR), networked computers, systems software and bespoke software.

Digital IP Video surveillance suites make use of Internet Protocol based computer networks. The construction of such networks is beyond the scope of this document however the network design must take into full consideration the large quantity of data transferred across networks by surveillance systems.

This white paper provides a high level discussion of the major areas that should be addressed when designing such a network and choosing the communication parameters of the IP cameras and networked digital video recorders attached to the network.

Terminology

The following terminology is used in this paper:

Client	A client is a software entity that presents a view of the current state of the surveillance suite. It makes requests to a server which permits certain actions to be carried out by the client. The client can also act in an administrative capacity allowing the configuration and maintenance of the whole system.
Server	The server is a software entity that acts as a central decision and control centre for the whole system. It provides a series of services to clients. It ensures that actions made by the clients, if appropriate, update the surveillance system.
Networked Video Recorder	The NVR is a software entity that stores network streams originating from IP cameras and networked digital video recorders onto a storage device and retrieves these at a later time. The "recorded" stream is not tampered with in any manner so the evidential integrity of recorded video is maintained.
Video-wall	The Video-wall is a software entity that displays video originating from IP cameras and networked digital video recorders in a matrix style layout.
Transcoder/Broadcaster	A combined transcoder/broadcaster software entity converts media streams originating from network streams from IP cameras and networked digital video recorders, from folders of image files and from video files and broadcasts media streams transcoded to alternative encoding, framerate, resolution and bit-rates. These transcoded and broadcasted streams are later consumed by Clients, Video-walls or Networked Video Recorders
Media Analytics processor	A media analytics processor is a software entity that carries out stream analytics tasks using various algorithms and provide a series of alarms to subscribed Server and Networked Video Recorder entities.

Surveillance Suite Architecture

When the system components are installed on computer hardware and interconnected via a computer network, and given access to compatible IP cameras and networked digital video recorders, the components act together to form a surveillance system. Many systems use hardware from different manufacturers, with different feature sets and characteristics. In these cases, adherence to standards is vital to make the overall system work. The system architecture is based on an Internet Protocol (IP) network — all communication is performed over IP networks.

Typically the surveillance system will consist of:

- at least one networked video source, either camera or recorder (but ordinarily many more)
- a single server
- at least one client (but ordinarily several)
- Video-wall, NVR, analytics and transcoder/broadcaster components are optional. There can be several NVR and Video-wall components within the system.

There is only one server component within the surveillance system. There can be several surveillance systems on the same network but note that each system has a single server component at its core.

Network Traffic

Video streamed from IP cameras and networked digital video recorders is the major configurable source of traffic on the network. The quantity of data traffic from each source accumulates as bandwidth is consumed by increasing numbers of devices.

Furthermore, since NVRs replay recorded network streams, the amount of data traffic generated is the same as that of the original recorded stream. Multiple playback sessions of the same recorded stream result in an accumulation of data traffic in line with the number of playback sessions. A transcoder/broadcaster software component also adds to network load since it must consume media streams for analysis.

It is therefore critical that IP cameras and networked digital video recorders are configured with a view to the number of potential viewing clients, Video-walls and NVRs recording them. Where there is a requirement for remote sites to view media streams over a restricted bandwidth connection, a transcoder/broadcaster software component can be used to present suitable bandwidth streams.

Infrastructure

When planning system infrastructure, you should take the following into account:

- Cable connections to a typical network switch device have maximum rates of 100 or 1000 megabits per second.
- Network connections between a device and a network switch can be:
 - Half-duplex – they can either send or receive traffic at any given moment
 - Full-duplex – they can send and receive traffic at the same time.
- A network connection might have traffic from:
 - a single IP camera or networked digital video recorder (DVR) only.
 - many IP cameras and networked DVRs (in the case of Video-walls) Or it could have traffic for
 - IP cameras, networked DVRs and played-back network streams (in the case of NVRs)
 - a transcoder/broadcaster. This software component receives media streams and generates them.
- an analytics server consumes media streams.
- There may be non-surveillance network data on the same network.
- Multicast traffic may help reduce bandwidth requirements. However, it may not be supported by the surveillance suite components.
- A network time server. The presence of a hardware or software based time server is a mandatory requirement. All IP cameras, encoders, networked digital video recorders, server and client computers should obtain their base time from the network time server. For evidential purposes, the central time server should synchronise itself with an external real-world time source. Where there are multiple surveillance site locations, local time servers in each location should provide time to the site. Each local time server should coordinate with the same external real-world time source.

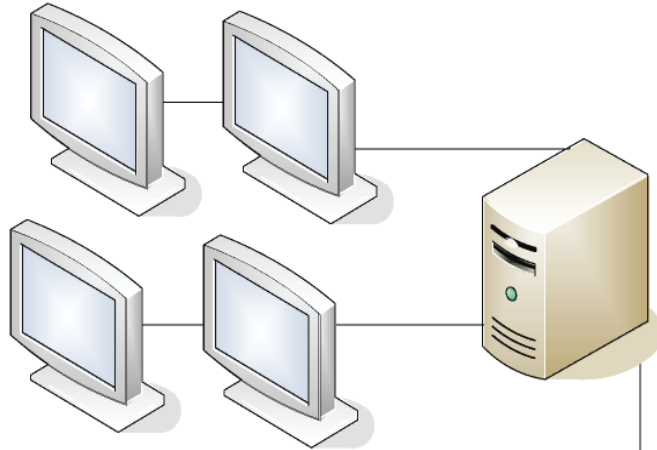
Surveillance Server

- Authenticated and audited access to networked surveillance resources on a users and group membership basis, including access to video, control of PTZ, recording control, playback permission, video-wall control and transcoder/broadcaster session access.
- Provides alarm management, PTZ control arbitration, map serving.
- Presents IP camera/encoder, recorders, video-wall, encoder/broadcasters and analytic servers as logical hierarchy.



IP Video Sources

Unicast or multicast media streams from IP cameras, encoders, or networked Digital Video Recorders.

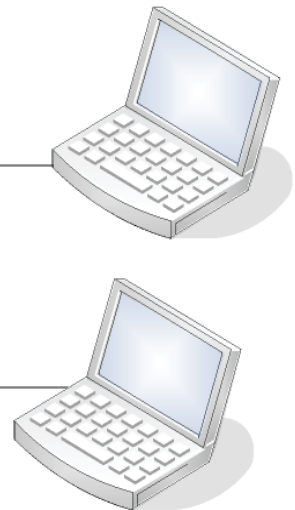


Video-wall software

Converts a PC into a dedicated Video-wall supporting one, two or four monitors using one or two high performance video display adapters.

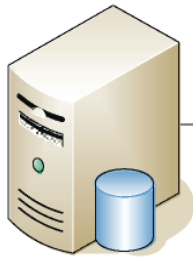
Clients

Provide live and playback control of IP cameras, encoders and networked Digital Video Recorders. Clients could be laptops or even hand-held mobile PDAS, connected via wireless.



Networked Video Recorder software

Converts Server PC to a dedicated networked video recorder supporting evidential grade, native recording of IP cameras, encoders and networked digital video recorders.

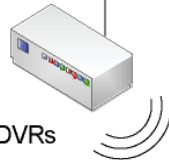


Combined transcoder/broadcaster software

Accepts media streams originating from:

- network streams from IP cameras and networked DVRs
- folders of image files
- video files

...and converts these, then broadcasts media streams using the specified encoding, framerate, resolution and bit-rates to RTSP-compliant viewing client(s).



TCP/IP based network with support for unicast and multicasting including VLAN support.
Mixed LAN and WAN use possible.

Configuring Stream Settings

When configuring IP camera and Networked DVR stream settings, you should consider the following:

- Generally more traffic is generated by:
 - high resolutions
 - high bitrates
 - high frame-rates
 - high frame-rate MJPEG streams, which generally tend to generate more traffic than high frame-rate MPEG4 streams of the same resolution.
- More traffic is generated by MJPEG by high frame quality / low compression factor
- Very high levels of traffic are generated by MJPEG mega-pixel video sources.
- More traffic is generated by MPEG4 by:
 - high I-frame quality
 - excessively high P-frame quality
 - low p-frame frequency/high I-frame frequency
 - virtue of scene observed by camera(s): e.g. more data traffic is generated by: PTZ cameras that move through tours of presets, or are frequently moved; noisy feeds from analogue cameras; night-time viewing and automatic gain causing noise, scene subject to motion – crowd scenes, busy roads, in-vehicle safety cameras, etc.

Using H.264/AVC (MPEG4-part10) encoded video network streams can achieve equivalent video quality to MPEG4-part2 encoded video network streams at lower bandwidth. Consider using H.264 encoding for more efficient use of bandwidth particularly when using mega-pixel video sources.

Careful infrastructure planning will lead to a reliable overall surveillance system. It is important to locate any network links that are heavily loaded by data traffic – typically these will be links to NVRs and Video-walls.

It is also worth noting that when viewing live video from IP cameras and networked DVRs on a switched network, data is routed directly from the IP camera or networked DVR to the client component viewing that camera or networked DVR, i.e. it is not received by the server component and then forwarded on to the viewing clients.

- Some IP cameras allow for different streaming rates, depending on which encoder within the camera is connected. One use of such a facility is to have one encoder on the IP camera set to typical live view settings and another encoder in the same camera set to typical recorder settings.
- Mega-pixel cameras require considerable care when deployed with a surveillance system. They can generate considerable traffic, due to their high resolution when used at 25 or 30 frames per second and when using MJPEG. If NVRs are used to record high-definition, mega-pixel network streams, these put a large load on the recorder, consuming a larger percentage of the available network connection bandwidth and more storage space per second than CIF and 4CIF resolution streams.
- Predicting network traffic can be difficult so it is highly recommended that a safety margin be built in to accommodate sudden bursts of higher than average data traffic caused by a faulty camera, or similar.
- The network's ability to support multicast is important – the discovery system used in the surveillance suite is based on multicast and broadcasting. If multicast support is impossible, computers running the client software component can still locate the server component if the server's IP address is known.

System Hardware Considerations

When considering optimal hardware for the surveillance system, consider the following:

- The server and NVR software components have a serving behaviour and as such will benefit from computer hardware optimised for the role of serving.
- The client and Video-wall components have graphical display behaviour, and so benefit from computer hardware optimised for multi-media graphical display. It may be useful to add specialist display adapters that provide dual- or quad-head capability. Such display adapters must have the functional ability to perform Direct-3D rendering in hardware, i.e. not offload this work to the computer system's host processor.

System Software Considerations

- Anti-virus, anti-spyware and software firewall products should generally not be installed on surveillance computers.
- Take care if installing additional software other than that required for the various surveillance system components. Adding additional software could have unforeseen impact on the satisfactory performance of the system.
- It is important to update all operating system device drivers, particularly for network adapters (and graphic adapters for clients and Video-wall components). It is best to use the latest drivers available from the computer manufacturer. If you find that the computer manufacturer uses hardware from a third party, please be certain that using the third-party's driver is appropriate – often computer manufacturers obtain specially crafted variants of the third party's hardware making the usual driver from the third party less than optimal, or completely incorrect.