Scalable IP Networks for Video Surveillance
Enabled with MPLS for Reliable Non-Stop Monitoring
Table of contents

1 Introduction

1 IP Video Surveillance Architecture

3 The Alcatel-Lucent IP/MPLS Network

4 Building the Multicast Network
5 Adding VPLS for Cost-Effective Aggregation

7 Capitalizing on MPLS Capabilities
7 High Availability through MPLS
7 MPLS Traffic Engineering
7 Hierarchical Quality of Service
7 Effective Management for Easier Day-to-Day Operations

8 The Alcatel-Lucent Advantage

8 Summary

8 Abbreviations
Introduction

Industries and governments have been using video surveillance to support their operations for many years. Today, video surveillance has become a mandatory requirement across multiple sectors. For example:

- Governments rely heavily on video surveillance as an integral part of crime prevention and homeland security measures.
- Energy companies and utilities use video to monitor the condition of remote equipment and to ensure the physical security of their critical assets; in some regions, specific standards exist that must be adhered to (e.g. the National Electric Reliability Corporation standards in the U.S.).
- Rail, highway authorities and airports depend on video surveillance to safeguard critical assets from possible terrorist attacks and for day-to-day traffic monitoring to ensure passenger safety.
- Seaports and freight companies use video surveillance for theft prevention.

A modern video surveillance system is now IP-based and it is becoming integrated with the information technology infrastructure of the organization. Managing video traffic can be a challenge for organizations that are still using traditional IP and Ethernet networks. Adding CCTV traffic into a network unprepared for video traffic can negatively impact all services on the network.

It is, therefore, critical for organizations to select a network solution that can technically address their video surveillance requirements. They need a reliable, “always-on” solution that can handle many high quality video streams, and accommodate the convergence of video, voice and data traffic. The network architecture must be capable of handling future growth, including significant increases in bandwidth.

Alcatel-Lucent has an advanced IP/MPLS communications solution that can meet the requirement for guaranteed delivery of mission-critical CCTV video traffic and concurrent support of other critical data and voice traffic on a single converged network.

IP Video Surveillance Architecture

Traditional video surveillance systems rely on proprietary analog-based platforms. In recent years, these traditional systems have evolved to ones based on IP, using the distributed network architecture. As a result, video surveillance and its associated equipment such as cameras and recorders are no longer just the responsibility of the security department — now it also has a significant impact on the information technology (IT) and telecom departments. As surveillance becomes one of the many applications supported by the corporate IP network, the IT/telecom department must be involved in the planning and implementation of the video surveillance strategy.

Network-based video surveillance, which enables the aggregation and delivery of CCTV video to many locations across the network, puts a heavy demand on network resources. The IP network must be able to support the high bandwidth required by video traffic, with multiple, stringent quality of service (QoS) levels. The bandwidth required for video surveillance traffic is affected by many factors:

- Number of cameras in the network
- Frame rate
- Frame size
- Level of motion in the picture
- Video compression
- Optional audio channels
- Remote control of video cameras
- Number of control rooms in the network
- Number of storage locations in the network
Although compromises can be made to minimize the required bandwidth, there is increasing pressure to ensure that video captured is of high quality. For example, an image must be of sufficient clarity for investigative purposes and for submission as court evidence. Also, video analytics software is becoming a common tool for automated detection of anomalies, and the software will require a specific video quality. High quality video may require several Mb/s per stream. However, it’s not just about bandwidth, although that is obviously essential. The video surveillance network must also be able to handle the jitter and latency requirements of video traffic.

A distributed video surveillance architecture offers many advantages, including support for real time video streaming to multiple parties at many locations, and the flexibility to deploy video analytics software remotely. This architecture enables local recording and the use of existing storage server farms on the network. For example, a transit authority’s security department may share its CCTV streams with the transit police, a municipal emergency center, the security division of regional transit operations, and other neighboring operators. Since access and distribution of CCTV streams can be very dynamic and mission-critical in nature, a highly reliable IP/MPLS network is the ideal solution for handling the requirements for video and other traffic.

With all applications going IP and the convergence of data, voice and video traffic on a single network, organizations need high capacity networks that support high bandwidth and flexible any-to-any communications. The WAN core must be able to handle traffic of several Mb/s per camera and thousands of multicast streams. An IP/MPLS WAN is capable of connecting thousands of CCTV cameras. Figure 1 shows the Alcatel-Lucent IP/MPLS communications network for video surveillance.

Figure 1. Alcatel-Lucent IP/MPLS Communications Network for Video Surveillance
The Alcatel-Lucent IP/MPLS Network

IP networks have grown significantly in recent years, but they often lack the necessary scalability to support traffic that requires QoS levels other than best effort. Traditional IP and Ethernet networks also lack the ability to optimize the use of network resources and the capability to react to network events fast enough to guarantee end-to-end service level agreements. By adding MPLS, an organization gets the best of both worlds — an IP network that has the robustness and predictability of a circuit-based one. The IP/MPLS infrastructure enables the deployment of a video surveillance system while continuing to support and improve voice and data services. With an MPLS-enabled IP network, an organization has a system that:

- Is highly scalable and reliable
- Addresses a range of QoS requirements
- Optimizes bandwidth usage through traffic engineering
- Has extensive OAM tools for troubleshooting and maintenance

In addition to these MPLS advantages, the Alcatel-Lucent IP/MPLS WAN solution supports advanced MPLS capabilities such as virtual private LAN service (VPLS), pseudowire service, and IP virtual private networks (IP-VPNs). The Alcatel-Lucent multiservice MPLS solution can also support existing TDM, frame relay and ATM traffic, so organizations can have cost-effective support of both legacy and IP applications on a converged IP/MPLS WAN.

The Alcatel-Lucent IP/MPLS implementation provides a service-oriented approach that focuses on service scalability and quality, and per-service operations, administration and maintenance (OAM). With a service-aware infrastructure, the network administrator has the ability to tailor services such that mission-critical applications have enough bandwidth to meet peak requirements and non-critical applications have sufficient bandwidth to meet an acceptable performance level.

The components of the IP/MPLS network include the Alcatel-Lucent 7710/7750 Service Router (SR) product family, the Alcatel-Lucent 7450 Ethernet Service Switch (ESS), the 7705 Service Aggregation Router (SAR) as well as the Alcatel-Lucent 7210 Service Access Switch (SAS) for access connectivity. The Alcatel-Lucent service routing products support IP routing and switching, complete with multiservice capabilities. They enable an organization to extend MPLS to the remotest network access and their non-stop service functionality provides unparalleled reliability.

The administration of the Alcatel-Lucent IP/MPLS network is handled by the Alcatel-Lucent 5620 Service Aware Manager (SAM), which simplifies and automates routine tasks while facilitating the easy introduction and maintenance of new services.

The Alcatel-Lucent IP/MPLS network has proven very successful in helping industries, governments, and enterprises to deploy mission-critical voice, data and video services. The solution was designed to deliver differentiated services to users while maintaining QoS for each type of application. This carrier-grade design is ideal for supporting video surveillance systems because it is capable of coping with tens of thousands of video and other data and voice streams simultaneously.

The network must provide a comprehensive set of QoS and traffic engineering capabilities to meet the stringent delay and jitter requirements of the CCTV traffic. This is especially important if the network is being used to deliver a multitude of other services with different characteristics. The Alcatel-Lucent 7710/7750 SR product family, the 7450 ESS and the 7210 SAS have the QoS resources to meet these requirements.
The underlying attributes of a QoS system capable of providing this level of service include:

- Rich, wire-rate, packet classification at Layers 2 and 3
- Fine-grained range of packet priorities, each with an associated service queue, in order to ensure that user traffic is handled in accordance with the required precedence (priority of importance)
- Packet buffering dedicated to traffic in each service queue
- Ingress and egress traffic shaping so that the traffic associated with each service can be managed such that traffic flows do not have a cross-impact between services
- Hierarchical scheduling, which allows maximum bandwidth delivery while simplifying the management task

Although Ethernet has emerged as the de-facto standard for LANs, it has also become the standard with the CCTV camera. Each camera has an IP/Ethernet-based interface and is recognized by means of an IP address and a media access control (MAC) address. Ethernet has also become a standard offering in metropolitan area applications. Ethernet provides scalable bandwidth in flexible increments. It is a cost-effective technology which is well understood by organizations as it has been in LANs for years. Troubleshooting does not require additional training since network administrators are already familiar with Ethernet. Integrating video surveillance into the corporate WANs delivers cost savings in terms of equipment, facilities, provisioning and maintenance. This translates to capital expenditure (CAPEX) and operating expenditure (OPEX) reductions. Cameras in the LAN can be aggregated to a 1 Gb/s or 10 Gb/s uplink to an IP/MPLS network.

The transformation of the enterprise network to support an application like video surveillance brings with it additional management challenges. In a video surveillance solution, every camera is an IP endpoint, expanding the IP address space exponentially. This brings added complexity to the management of IP addresses, domain name servers and the dynamic host configuration protocol. Without effective management of these crucial services, the mission-critical network can quickly be brought to a standstill. Additionally, performance management of the dozens of real-time and non-real-time applications becomes increasingly complex. Central visibility and management become not only desirable, but essential in a mission-critical network. Alcatel-Lucent offers IP address management (VitalQIP DNS/DHCP IP Management Software) and application performance management software (VitalSuite Performance Management Software) to take control of the mission-critical network and keep it running smoothly.

### Building the Multicast Network

A video surveillance system can consist of thousands of high quality CCTV cameras each generating a multicast IP video stream. CCTV cameras have Ethernet and IP interfaces and support Internet group management protocol (IGMP) to register to a multicast group. These video streams can generate bandwidths of up to several Mb/s, which are transported in real time to multiple locations. This application requires a reliable high-capacity communications network that can transport a massive amount of multicast streams in a many-to-few topology.

The simplest way to implement the delivery of CCTV traffic is to deploy an interior gateway protocol (IGP), such as intermediate system-to-intermediate system or open shortest path first (OSPF), and an IP-multicast protocol, such as protocol independent multicast-sparse mode (PIM-SM) across the network. Using this approach, PIM is responsible for setting up individual multicast trees, one for each CCTV channel, to deliver the traffic to the devices in the aggregation part of the network. Each CCTV channel belongs to a different multicast group. Therefore, each channel has a different multicast IP address assigned to the packets carrying footage for the channel. IGMP is used by the video management workstation to tell the edge router which channel the operator is requesting.

There are, however, several problems associated with this pure IP approach, and some of these may cause unacceptable delays when failures in the network occur. Using PIM multicast trees as the
delivery mechanism for traffic from the CCTV to the aggregation network has a significant negative impact on network resiliency. Any failure in the IP-only network will result in substantial recovery delays related to the reconvergence of the underlying IGP network, followed by the rebuilding of the affected multicast trees. The total recovery times will typically be in the order of tens of seconds and will result in an interruption in monitoring. Furthermore, running PIM throughout the network significantly increases CAPEX and OPEX because it adds to the complexity of the network, making it more difficult to deploy and maintain. The debugging of problems in a multicast network is challenging and can lead to significant periods of service downtime.

Adding VPLS for Cost-Effective Aggregation
Using the multicast capabilities of VPLS technology in the aggregation network provides a more powerful and cost-effective solution for the delivery of CCTV traffic, and resolves several problems inherent in the PIM-based solution:

- VPLS is based on MPLS, and therefore offers 50 ms recovery times to dramatically improve recovery times after a node or link failure.
- Removing PIM from the aggregation network dramatically reduces the operational complexity of deploying and maintaining the system, and debugging problems.
- Network scalability is increased as a result of an increase in the number of video streams served by each aggregation node.
- A reduction in resource consumption makes it possible to support different types of services concurrently.

Replacing PIM in the aggregation network with VPLS significantly reduces the capital costs associated with deploying or upgrading a network to deliver the CCTV service. This is because edge devices consume fewer resources with VPLS than with PIM. The consequences of this are twofold. First, the scalability of the network is increased: more services can be served by each edge device, reducing the number of edge devices that need to be deployed. Second, because there is less overall load on the network, the network administrator can use the same infrastructure to deliver a wider range of other services and applications. Using VPLS to deliver a CCTV service also improves network resiliency, thanks to the 50 ms recovery capability.

The PIM multicast protocol can be deployed and limited to the IP/MPLS core by using VPLS in the aggregation network (see Figure 2).

Figure 2. Enhanced Video Services with VPLS
Alcatel-Lucent has developed a comprehensive service assurance toolkit that exceeds the traditional ping and trace-route debugging capabilities of a typical router/switch. These tools allow the network operator to quickly test each VPLS segment and isolate a problem. A second tier of MAC level tools can then be used to resolve the problem in the VPLS segment quickly and efficiently. Because the network is less complex, fewer network problems will arise and, when problems do occur, the resolution times will be shorter for an Alcatel-Lucent VPLS based solution, thereby improving customer satisfaction.

**VIDEO STREAM WALKTHROUGH**

Figure 3 illustrates the processing of a video stream. The CCTV camera is the source of the multicast traffic. The receiver of the traffic is the central video control server and storage, as well as other local monitoring and storage centers where required.

When a camera is powered up, it streams its traffic to the aggregation switch which forwards the traffic by default to the core of the network. The traffic has the source address (S) of the camera and the multicast group address (G) as the destination address. At the core, one router acts as the rendezvous point and stores the (S,G) combination in its routing database. As there are no receivers yet, the stream ends at the rendezvous point.

At the receiver side, the central video control server sends an IGMP request to the neighboring router. Only the multicast group address (G) is known by the central video control server as it is populated statically in the server. The server sends a message containing a (*,G) join request.

The neighboring router forwards the request via a PIM-SM message to the rendezvous point, which knows the source address of the multicast group address. The rendezvous point confirms the join request by sending the source address of the multicast camera to the receiver. The receiver sets up, by means of PIM-SM, a leaf from the source to the receiver. The branch is set up by finding the shortest path from the receiver to the sender. If the router already has a branch of this multicast tree (identified with (S,G)), it doesn’t have to go back to the rendezvous point. Instead, it establishes a new branch and replicates the traffic to the new receiver.

![Figure 3. Video Stream Walkthrough](image-url)
MPLS has received broad market attention and now an increasing number of enterprises are deploying their own MPLS-based WANs. MPLS brings the advantages of a circuit-based network to an IP network, and enables network convergence, virtualization and resiliency.

In the Ethernet aggregation and core network layers of the WAN, MPLS is used to transport different types of traffic using VPLS, pseudowire and IP-VPNs. In an enterprise network, OSPF is commonly used as the IGP supporting the set up of MPLS paths.

**High Availability through MPLS**

The IP/MPLS core network assures high availability through fast path restoration and network re-convergence within 50 ms. Network resiliency is achieved by means of the end-to-end restoration capabilities of MPLS’s fast reroute feature. High availability is essential to a communications network, which carries mission-critical voice, video and data information. With MPLS fast reroute, video, voice and data service interruption is minimized during network failures.

The Alcatel-Lucent IP/MPLS implementation includes additional high-availability support for non-stop routing and non-stop services. The Alcatel-Lucent 7710/7750 SR and 7450 ESS products support non-stop routing and non-stop services, providing unparalleled availability and reliability:

- **Non-stop routing** ensures that a control card failure has no service impact, as label distribution protocol adjacencies, sessions and the database remain intact if there is a switchover.
- **Non-stop service** ensures that VPLS and IP-VPN services are not affected when there is a control card or switch fabric module switchover.

To protect the network against node or optical interconnection failures, end-to-end standby MPLS paths are provisioned. MPLS offers the flexibility to provision hot or cold standby paths to protect an active path.

**MPLS Traffic Engineering**

MPLS supports traffic engineering, which allows for the selection of the best path across the network, taking the physical paths of the links and interfaces into account. Traffic engineering is used in networks to ensure that the best link is chosen to optimize network bandwidth.

**Hierarchical Quality of Service**

The Alcatel-Lucent implementation of hierarchical QoS is service-aware, allowing lower priority traffic to burst to fill available bandwidth when higher priority applications go idle. Typical routers offer up to eight QoS levels per port with either strict priority or weighted fair queuing. In contrast to this, the Alcatel-Lucent IP/MPLS solution implements service-based queuing; each logical port (virtual LAN or virtual circuit) within a physical port has a dedicated queue. The Alcatel-Lucent solution also supports queues and QoS for traffic classes within the logical port, and provides each service with committed information rate and peak information rate type guarantees.

**Effective Management for Easier Day-to-Day Operations**

The Alcatel-Lucent IP/MPLS network supports OAM tools that simplify the deployment and day-to-day operation of a communications network. For example, service tests, interface tests and tunnel tests allow for rapid troubleshooting and enable proactive awareness of the state of traffic flows, to help minimize service down time.
The Alcatel-Lucent IP/MPLS communications network is fully managed by the industry-leading Alcatel-Lucent 5620 SAM. The 5620 SAM is a single management platform offering element, network and service management for advanced Layer 2 and Layer 3 network solutions and services. The 5620 SAM provides a template-based provisioning model, which reduces configuration errors and speeds provisioning of new network services.

The Alcatel-Lucent 5650 Control Plane Assurance Manager (CPAM) offers real-time control plane visualization, proactive control plane surveillance, configuration, validation and control plane diagnosis. It enables network administrators to overlay Layer 2 and Layer 3 services, MPLS tunnels and various OAM traces on the control plane map. This simplifies problem resolution, reduces control plane configuration errors, and reduces troubleshooting time.

The Alcatel-Lucent Advantage

Alcatel-Lucent has years of experience in the development of MPLS-based technology and is a leader in IP/MPLS and VPLS networking. Alcatel-Lucent has a complete MPLS offering, which includes solutions for Layer 2 (VPLS), pseudowire and Layer 3 (IP-VPN) services. The Alcatel-Lucent IP/MPLS solution offers organizations the flexibility, scalability and feature sets required for mission-critical operation.

With the broadest portfolio of products and services in the telecommunications industry, Alcatel-Lucent has the unparalleled ability to design and deliver end-to-end solutions that drive next-generation communications networks. Alcatel-Lucent is a leader in fixed, mobile and converged broadband networking, IP technologies, applications, and services. The Company’s Professional Services Portfolio includes Consult and Design, Integrate and Deploy, and Maintain and Operate.

Summary

Organizations requiring video surveillance should ensure that their IP networks are enabled with MPLS, as only MPLS can provide the reliability that is needed for mission-critical services. Furthermore, a service-aware IP/MPLS network provides the additional benefit of supporting consolidated voice, data and video applications that can be managed through configurable QoS levels. The Alcatel-Lucent IP/MPLS product portfolio leads the industry in multicast scalability, reliability and OAM tools, key enablers for meeting the always-on requirement for mission-critical operations. The Alcatel-Lucent network facilitates the integration of a security solution into the corporate IP communications network and eliminates the types of problems encountered when running video surveillance over a traditional IP network.

Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>Asynchronous transfer mode</td>
</tr>
<tr>
<td>CAPEX</td>
<td>Capital expenditure</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed circuit television</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet group management protocol</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior gateway protocol</td>
</tr>
<tr>
<td>IP/MPLS</td>
<td>Internet protocol/multiprotocol label switching</td>
</tr>
<tr>
<td>IP-VPN</td>
<td>Internet protocol virtual private network</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology</td>
</tr>
<tr>
<td>LAN</td>
<td>Local area network</td>
</tr>
<tr>
<td>MAC</td>
<td>Media access control</td>
</tr>
<tr>
<td>OAM</td>
<td>Operations, administration and maintenance</td>
</tr>
<tr>
<td>OPEX</td>
<td>Operating expenditure</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open shortest path first</td>
</tr>
<tr>
<td>PIM</td>
<td>Protocol independent multicast</td>
</tr>
<tr>
<td>PIM-SM</td>
<td>Protocol independent multicast – sparse mode</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of service</td>
</tr>
<tr>
<td>TDM</td>
<td>Time division multiplexing</td>
</tr>
<tr>
<td>VPLS</td>
<td>Virtual private LAN service</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide area network</td>
</tr>
</tbody>
</table>