SerVision

➢ Application Solution

FLEET MONITORING

Using SerVision Video Gateways to Monitor a Fleet of Vehicles from a Control Center

Overview

SerVision Video Gateways are powerful, multi-featured security systems that can stream high-quality video to remote PCs and other devices over a variety of types of networks. They are uniquely optimized for streaming data at exceptionally low bit rates, and are even capable of transmitting video from sites where only GPRS coverage exists. The units can record video on-site, stream live or recorded video to remote users, monitor sensors, interface with GPS tracking systems (MVG series only), and notify users instantly if events are detected.

This document explains how SerVision Video Gateways can be deployed in vehicles to enable a control center to monitor a fleet. This solution can be successfully implemented in large or small fleets and with all types of vehicles, from motorcycles, taxis, police cars, ambulances, and armored cash-transport vehicles, to buses, trains, and semi-trailers. A single control center can have up to 20 control-center operators working at one time and can monitor hundreds or even thousands of vehicles simultaneously.

SerVision supplies two models of Video Gateways for deployment in vehicles: the four-channel MVG400 and the two-channel MVG200. Both models are designed for full integration into a mobile environment, drawing their power from the vehicle battery, providing support for GPS tracking, and transmitting video, audio, and other data over cellular and WiFi networks. Additional features can be incorporated into the systems by connecting sensors, switches, and a closed-circuit monitor to the units. For example, an optional built-in g-force sensor (accelerometer) can generate alarms when erratic driving behavior is detected, a door sensor can indicate when the vehicle door is opened or closed, a panic button can be attached to the unit for use in emergency situations, and the driver can use a touch-screen monitor to keep tabs on what is happening in all parts of the vehicle.

Setting up a fleet-monitoring system requires preparing three venues: the vehicles, the control center, and the fleet parking depot. Live monitoring of vehicles in transit is performed from the control center in real-time. When the vehicles are on the road, video and other data can be transmitted to the control center over the internet via the cellular network. Routine downloading of recorded video can be performed when the vehicles enter the parking depot, using a WiFi connection to a local network.

SerVision offers two alternative monitoring solutions for PCs:

- **SVMultiClient**: A PC-based monitoring system that uses the free-of-charge SVMultiClient client application to interact directly with the Video Gateways in the field, this solution enables users to monitor up to 70 Video Gateways, with minimal infrastructure. SVMultiClient features a multi-stream video player, configurable alarms, downloading of recorded video, and many other features. SVMultiClient is available free of charge to all SerVision customers.
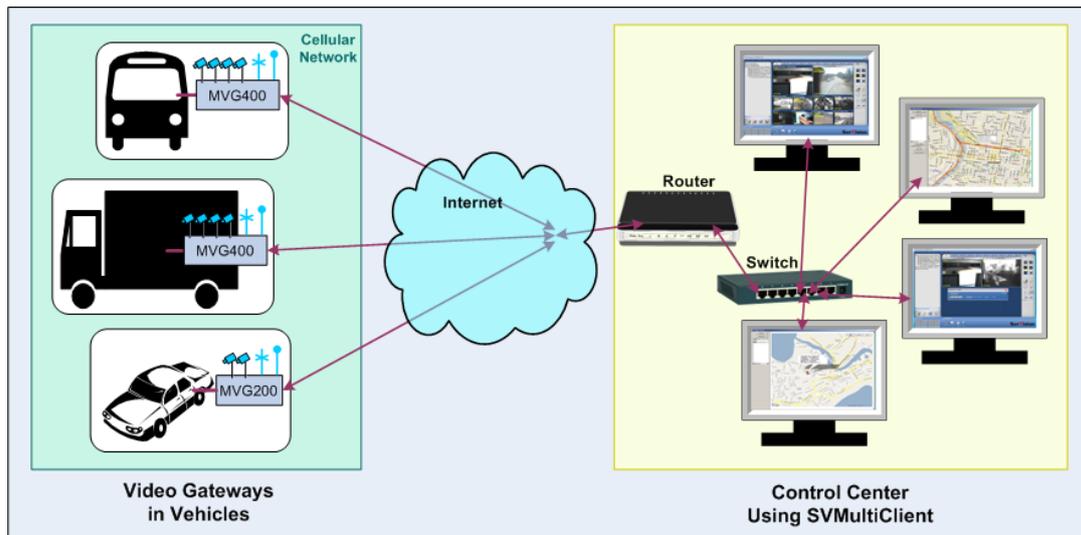
Control Center setup using the SVMultiClient PC-based application for vehicle monitoring

- **SVControlCenter:** A complete server-based monitoring system that is optimized for large enterprises (up to 5,000 Video Gateways), SVControlCenter is a highly customizable system featuring a multi-stream video player, configurable alarms, and an alarm management system. In addition, a Downloader module enables automated downloading of video to an internal database for long-term storage. SVControlCenter is available for purchase from SerVision.
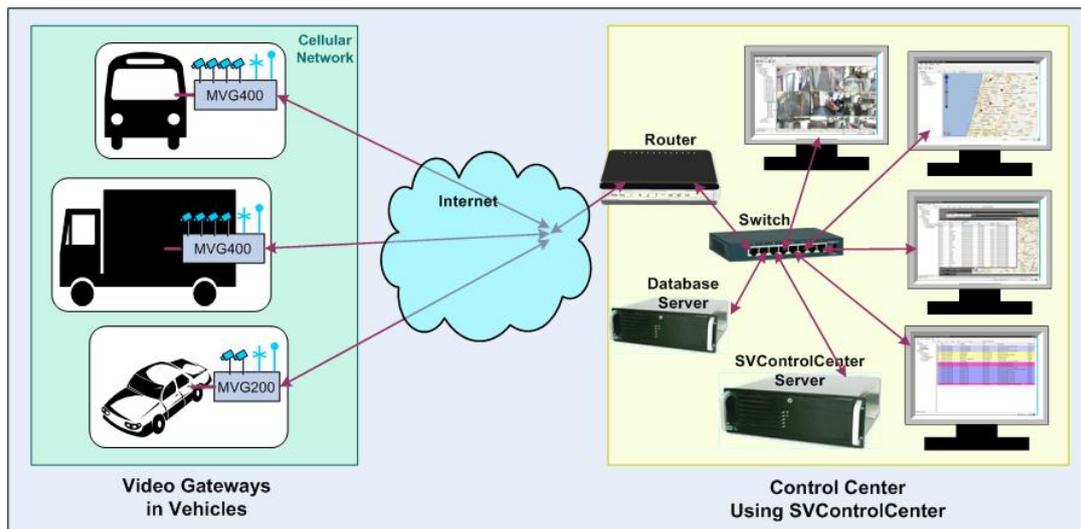
Control Center setup using the server-based SVControlCenter solution for vehicle monitoring.

Video Gateways can also be accessed remotely using a client application running on a smartphone or tablet. SerVision client applications are available free of charge for iPhone, iPad, Android, Windows Mobile, and Symbian devices. SerVision also provides a free SDK/API that can be used to develop alternative client software or to integrate SerVision's protocol into third party client software.
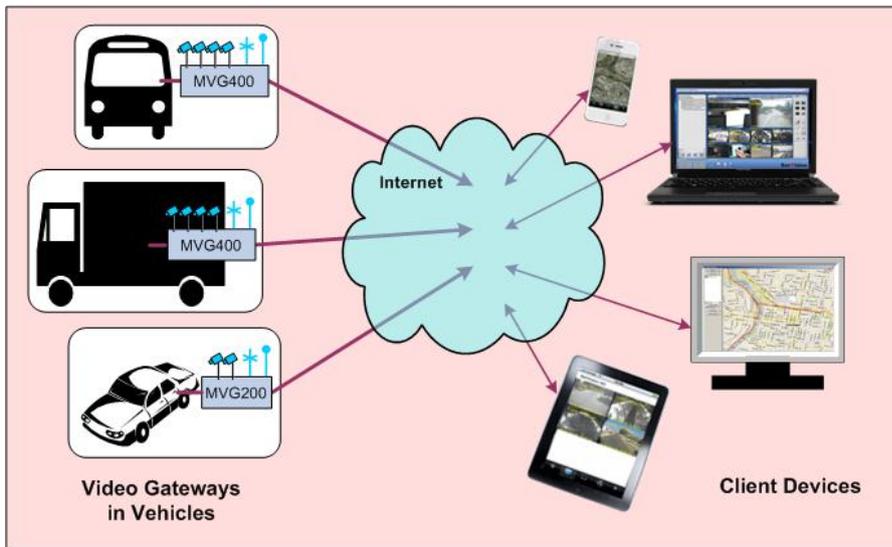
Client devices using SVMultiClient or cellular clients to connect to Video Gateways through the internet

The rest of this document provides additional information about setting up each of the three venues of the fleet-monitoring solution, including information about the various options available and the resources each option requires.

Vehicle Setup

Each vehicle in the fleet must have a Video Gateway, cameras, and other peripheral equipment installed in it. Installing the Video Gateway unit and its peripheral equipment in a vehicle should be performed by a professional installer who has been trained by a SerVision-authorized partner.

In addition, the Video Gateway must be configured to ensure that it functions as required, can be accessed by the control center remotely, and will connect automatically to the WiFi access point in the parking depot. Instructions and support for the configuration process are provided by SerVision.

Required Equipment

The following equipment is required for each vehicle:

- Video Gateway unit (MVG400 or MVG200) and other hardware (including cables and antennas) supplied with the unit (supplied by SerVision)
- 3G USB cellular modem (appropriate GSM or CDMA modems can be supplied by SerVision or provided by the local operator; a list of supported modems is available on the SerVision website, http://www.servision.net)
- SIM card for the cellular modem (for GSM networks; supplied by the customer)
- Up to four video cameras (supplied by SerVision or purchased separately)
- Additional cabling for cameras, power, and other hardware, as required for installation of all devices (supplied by the installer)

Optional Equipment

In addition to the required equipment, you may wish to use some or all of the following optional equipment:

- Dry-contact sensors

- Panic button

- Microphones

- External speaker (All Video Gateway units have built-in speakers.)

- CCTV monitor

- For Video Gateways that will be installed in trucks or buses, an insulated enclosure with a built-in fan in which to place the Video Gateway unit (supplied by the installer)

- Switches for changing the CCTV display or the unit's settings

- Additional storage media that have been approved by SerVision (hard-drives for MVG400 units; microSD cards for MVG200 units)

- Converter for connecting extra sensors and/or switches (ADAM module or IA relay board)

Selecting a Video Gateway Model

Either an MVG400 or a MVG200 Video Gateway must be installed in each vehicle in the fleet. You do not have to use the same model in all of the vehicles; choose the most appropriate model for each vehicle.

MVG400

The MVG400 is optimized for deployment in large vehicles, like buses and trucks, for which three or four cameras are required. The standard MVG400 unit comes with a 160GB removable hard drive, which provides sufficient storage capacity for recording four video channels continuously (24/7) at the default quality setting (10FPS, 128kbps, SIF), for nearly 30 days of recorded video. The unit can be supplied with a larger-capacity hard drive (up to 500 GB) upon request.

MVG200

The MVG200 is ideal for smaller sites, both stationary and moving, for which only one or two cameras, and minimal peripheral equipment, are required. The unit is supplied with a removable 4GB microSD card that can store over two days of recorded video. MicroSD cards of up to 64GB capacities can be used in the unit.

Choosing Cameras and Other Peripherals

SerVision can supply a compact video-camera that is ruggedized for use in vehicles. However, since any analog camera is compatible with the Video Gateways, many installers prefer to source cameras locally. This enables them to select a suitable model camera that is fully compliant with the project specification and will meet the customer's expectations.

Video Gateways support a variety of other optional peripheral equipment, such as sensors, switches, and CCTV monitors (see *Optional Equipment*, above). SerVision can supply some of this equipment, but you must purchase other items on your own.

Selecting Locations for the Video Gateway Units

There are many possible locations in which a Video Gateway can be installed in a vehicle. The ideal location is determined based on the type of vehicle and on parameters such as the

degree to which the location provides ventilation for cooling the unit, a stable surface on which to install it, and unimpeded reception of Wi-Fi and cellular signals.

Calculating 3G Data-Consumption Requirements

The cellular line each Video Gateway uses to transmit live video and other data to the control center must have a data plan that is sufficient for the amount of traffic that will be handled by the 3G cellular network. The required capacity varies depending on a number of factors: the number of cameras in use, the quality of the video that will be transmitted, and how much video will be transmitted. The requirements are highest if video from all cameras is continuously streamed live at high quality to the control center. Most customers do not need to transmit data continuously all day. Instead, they only transmit data over the cellular network in a very limited fashion; they may check on each vehicle briefly at fixed time intervals and they sometimes view live video when an alarm is set off. Assume, for example, that in a typical fleet, each vehicle generates an average of ten daily events that require real-time monitoring by control-center operators. For each such event, the operators can be expected to view live video from two cameras for about five minutes each. This means that the cellular line is used for about 100 minutes (10 events x 5 minutes per event x 2 cameras) every day. If each camera transmits video at 128 kilobits/second (kbps), the total amount of data transmitted over a month via the 3G connection is about 2.88 GB (see calculation below).

To calculate your cellular data-consumption requirements for a Video Gateway, in GB, use the following formula:

$$\frac{\text{bitrate}\left(\dfrac{kilobits}{seconds}\right) \div 8 \times \text{time}(seconds) \times \text{number of cameras}}{1{,}000{,}000}$$

For example, here is how you would calculate the data-consumption requirements for 50 minutes of video from two cameras transmitting at 128 kbps for 30 days:

$$\frac{128\,\frac{kilobits}{sec} \div 8 \times 60_{sec} \times 50_{min} \times 30_{days} \times 2_{cameras}}{1{,}000{,}000} = 2.88_{GB}$$

In real-world conditions, the live-stream bitrate of the Video Gateway will vary according to network conditions (network signal strength, network traffic, etc). SerVision Video Gateways are optimized to achieve the best streaming results given the network's limitations. Even if the Video Gateway is configured to transmit at a rate of 128 kbps, it is highly unlikely that the data will actually be transmitted in a constant stream at this rate. In effect, this is the maximum rate, and the actual rate will often be slower. The Video Gateway automatically corrects for these fluctuations, transmitting stable video streams at a lower quality level – and at speeds as slow as 5kbps – to match the available bandwidth and data rate, so the total data consumption will likely be lower than the value that is derived using the formula.

In addition, even if you are *recording* in high resolution (SerVision Video Gateways support both VGA and D1 resolutions.), you do not necessarily have to transmit live video at the same quality. By default, the Video Gateways support three standard video-quality settings for live streaming in SIF resolution: High (128 kbps), Medium (96 kbps), and Low (36 kbps). Users can also choose a different resolution or custom quality setting to suit the available bandwidth or to control or minimize data consumption. Based on our experience, a 1-5GB monthly plan is suitable for most project applications.

Control-Center Setup

Control-center operators use SerVision client software, running on standard Windows-based PCs, to monitor the fleet. Smaller control centers can employ the SVMultiClient client, which is supplied by SerVision free of charge, for this purpose. Larger enterprises must run the SVControlCenter client application, which is supplied as part of the SVControlCenter system, on each operator PC. All customers must provide the PCs for their operators.

In addition to the PCs and client applications, some projects may also require the following systems:

- SVProxy3 server: A system that facilitates network connections in certain environments and expands video transmission capacities

- SVMonitor system: An application that monitors the system for technical problems and malfunctions affecting the Video Gateways. (This application is only required for small projects that are using the SVMultiClient PC application for monitoring. The server-based SVControlCenter solution has its own internal mechanism for monitoring Video Gateway statistics.)

SVMultiClient-Based Control Centers

Smaller operations, with fleets of fewer than 70 vehicles, can use the SVMultiClient client application for PCs to monitor their vehicles. SVMultiClient can play live and recorded video, track the locations of vehicles via GPS, and display notifications when sensors are activated. It also allows operators to remotely control PTZ cameras and devices that are connected to the system's alarm outputs, to communicate with the vehicle driver, and to download video to the PC.

setup that is using the PC-based application for video monitoring.Required Equipment

Control centers using SVMultiClient for vehicle monitoring require the following equipment and infrastructure:

- PCs for each operator (supplied by the customer; operators working different shifts can share a single PC)

- A high-speed internet connection (supplied by the customer)

Optional Equipment

Control centers using SVMultiClient for vehicle monitoring may also require the following equipment:

- SVProxy3 server (supplied by SerVision; for additional information, see page 7)

- Designated PC for SVMonitor application (supplied by the customer)

SVMonitor

Control-centers using SVMultiClient for vehicle monitoring may also choose to set up a dedicated PC on which to run the SVMonitor application. This application helps control-center operators monitor the Video Gateway units for technical problems that may require maintenance, such as malfunctioning storage media, overheating of Video Gateway units, and lost video connections. It automatically connects to each Video Gateway it monitors at specified intervals and retrieves status information from it. If any of the information indicates a possible problem, the system generates an alarm.

SVMonitor is highly recommended for monitoring relatively large fleets with a large number of Video Gateways; smaller fleets do not generally require an SVMonitor system.

SVControlCenter-Based Control Centers

Larger-scale operations require the server-based SVControlCenter for vehicle monitoring. SVControlCenter is an enterprise-level management and video-monitoring system that can monitor up to 5,000 Video Gateway units. The system's server retrieves data from Video Gateways, stores it in an internal database, and manages the alarm and notification system. Control-center operators receive information from the SVControlCenter servers via SVControlCenter client applications. Each operator runs an SVControlCenter client application on a PC workstation at the control center. Both the server and the operator workstations are located at the control center and connected to the same LAN. The system can handle up to 20 SVControlCenter clients simultaneously.

All the SVControlCenter clients in the system are locally connected to the database server whenever they are open, and the SVControlCenter server automatically relays event information and alarm notifications to them. In addition, operators can connect directly from the SVControlCenter client application to play back and Video Gateways in order to view live video and to play back recorded video that is stored on the Video Gateway.

SVControlCenter is supplied by SerVision as two separate industrial-strength servers that are preloaded with all the required software: one server with Windows Server 2008 and the SVControlCenter server application, and the other server with Windows Server 2008 and a licensed copy of Microsoft's SQL server. When large numbers of Video Gateways are being monitored, the system should be scaled to several computers to improve performance. All of the servers must be physically located in the control-center and connected to the same LAN as the PC workstations that will be used by the control-center operators.

A Downloader module is available for use with SVControlCenter (see *Parking-Depot Setup*, below).

setup that is the server-based solution for video monitoring.Required Equipment

Control centers using SVControlCenter for vehicle monitoring require the following equipment:

- SVControlCenter server (supplied by SerVision)
- MS SQL server (supplied by SerVision, or supplied by the customer if only the SVControlCenter license is purchased)
- PCs for each operator (supplied by the customer; operators working different shifts can share a single PC)
- A high-speed internet connection (supplied by the customer)
- SVProxy3 server (optional, as explained below; supplied by SerVision)

Redundancy Solutions

To ensure system stability in case of equipment failures, key system functions and data can be duplicated. Redundancy solutions, including such as failover clustering, database mirroring, and database mirroring using a witness server, can all be implemented. Consultation with a SerVision support engineer is recommended.
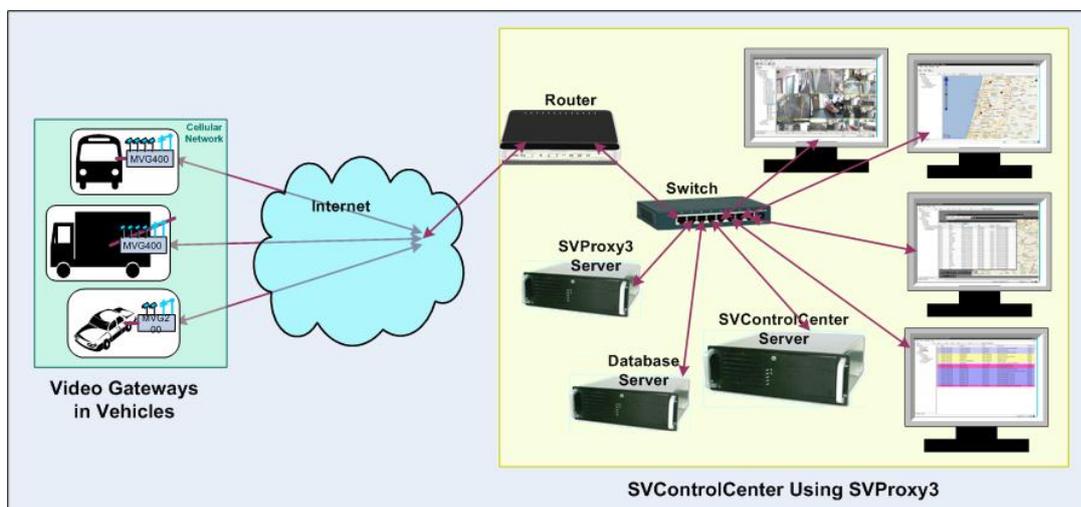
SVProxy3

In addition to the PCs, control-centers may require an SVProxy3 server. SVProxy3 provides a number of services:

- **Proxy service (SVProxy):** This service facilitates connections between client applications and Video Gateways that do not have public IP addresses. The proxy server is required in the event that the local cellular provider is not able to assign a public IP address to its cellular lines.

- **Video-Distribution service (SVDistributor):** This service distributes a single live video stream from a Video Gateway to multiple clients simultaneously without compromising the quality of the image. This is helpful if many control-room operators need to access images from the same camera simultaneously.

- **Dynamic DNS (SVDDNS):** This service can be used to assign a name to a Video Gateway, whether it has a fixed public IP address or not.

If your cellular lines all have public fixed IP addresses or connect to a VPN with a fixed IP address, the SVProxy3 server is not necessary. In these cases, the other services are not required for successful operation of the control center either.

Both the hardware and software of SVProxy3 are supplied by SerVision. One SVProxy3 server can support connectivity for up to 300 Video Gateway units.

SVProxy3 deployed in a control center

Control-Center Bandwidth Requirements

Live video and other data is relayed from Video Gateways over the cellular network to the internet, and is transmitted over the internet to the control center. The control center must have an internet connection that provides enough bandwidth to allow operators to view live video as required.

To calculate the required bandwidth, determine the maximum number of live video streams that will be opened by the control center simultaneously, and then multiply this number by the maximum transmission bitrate of each video stream. If, for example, the control center will have four PCs, and each one will have at most eight video streams open at one time, at a maximum bitrate of 128 kbps per stream, the required network capacity would be about four Mbps ($128_{kbps} \times 8_{streams} \times 4_{clients} = 4,096_{kbps} \approx 4_{Mbps}$).

This calculation should be viewed as the absolute minimum bandwidth requirement. It is highly recommended to get a more robust internet connection than the initial calculation suggests you need, especially if other devices are also connecting to the internet over the same connection. For most projects, we recommend a download capacity of at least 10 Mbps.

Parking-Depot Setup

When the vehicles are on the road, the control center can connect to them via the cellular network as necessary. Nonetheless, although live downloading over the cellular network is possible, it is not likely to be a cost-effective option, especially for large quantities of video. Downloading over a WiFi network is faster and far cheaper than downloading over the cellular network, and is the ideal choice for routine backup of video.

Control-center operators can use either SVMultiClient or SVControlCenter to download video to their PCs. Operators using SVControlCenter can also download video to the SVControlCenter database. In addition, SVControlCenter's Downloader module can be configured to download video to the SVControlCenter database automatically when a Video Gateway comes within range of the depot access point. The Downloader can be configured to automatically download all the locally recorded video from the Video Gateway to the database, or to only download video of events that were detected by sensors.
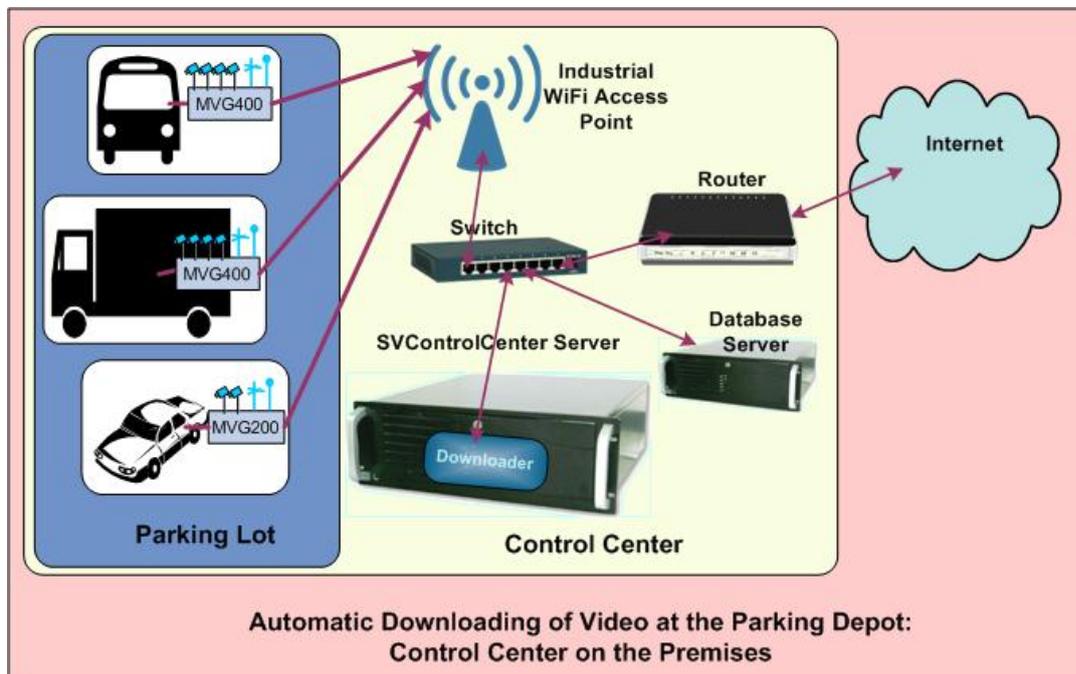
Routine downloading of data at the parking depot via a WiFi connection to the SVControlCenter database

When SVControlCenter's Downloader module is used to automatically download video to SVControlCenter servers, an industrial-strength hotspot must be set up at the fleet parking depot, and ideally, the SVControlCenter servers should also be installed at the depot. To implement this solution optimally, it is essential to work closely with a professional IT company that has prior experience in deploying enterprise-level hotspot solutions. To ensure the system is deployed correctly, it is also necessary to consult with a certified engineer from SerVision, as well as a representative of the WiFi equipment manufacturer.

Required Equipment

The Wi-Fi equipment required to set up the hotspot at the parking depot includes industrial-strength access points, controllers, routers, and switches. To determine the exact requirements, the IT company must thoroughly survey the parking depot to identify the number and types of WiFi access points that must be deployed there, and where they must be positioned, in order to build a hotspot that can accommodate the expected number of simultaneous connections. These conclusions depend in part on the number of vehicles that

will arrive at the depot at the same time (see *Required WiFi Capacity*, below) and on the physical layout of the depot.

Note: The Downloader module runs as part of SVControlCenter. If you want to use it to download video at the parking depot, SVControlCenter must be located at the depot. Thus, the control center itself will probably have to be located at the depot. If this is not feasible, it may be possible to use a VPN to connect the parking depot to the control center network. For additional information about this option, consult your IT company.

Required WiFi Capacity

The IT company that builds your parking-depot hotspot will require specific information about the WiFi capacity required. One of the considerations in calculating the requirements is how quickly the video data from a Video Gateway unit can be transmitted over the WiFi network to the SVControlCenter database. This is, among other things, a function of the WiFi *upload* data transfer rate provided by the Video Gateway unit. Under laboratory conditions, the maximum WiFi transfer rate provided by a Video Gateway is around 11 Mbps. To use this value to calculate the time required for downloading the video from a Video Gateway, you must know how many video streams are being downloaded, the bitrate used for each stream, and the time-length of each stream. Consider, for example, an MVG unit that continuously records video streams from four cameras, each at 128 kbps, throughout the time the vehicle is in operation. Over a ten-hour workday, the Video Gateway records 18,432 Mb of video ($128_{kbps} \times 36,000_{sec} \times 4_{cameras} \div 1,000 = 18,432_{Mb}$). At a constant transfer rate of 11 Mbps, it would take 1,676 seconds ($18,432 \div 11$) – just under thirty minutes – to transmit all of the recorded video from the MVG unit to the SVControlCenter database.

Other factors also affect the data transmission rate of a Video Gateway. Primary issues include the maximum data transmission rate of the WiFi access point and the number of Video Gateways that need to transmit data over the WiFi network simultaneously. Additional factors such as the presence of other traffic on the WiFi network, the WiFi signal strength, and the overall robustness of the WiFi network topology, can also bear upon the amount of time it will take to download video in a real-world scenario.

All of these issues must be taken into account by the IT company when it designs and sets up the WiFi hotspot. In order to ensure that the hotspot is set up optimally, you should be prepared to provide the following information to your IT company:

- The maximum data transfer rate of the Video Gateway units in a lab setting (11 Mbps)
- The average number of Video Gateways that will be transmitting video to the SVControlCenter database simultaneously
- How much time each vehicle will spend in the parking depot
- The quantity of data that will be transferred from each Video Gateway to the SVControlCenter database during the time the vehicle is in the parking depot (calculated based on the number of cameras in each vehicle, the bitrates used to record their video streams, and the average length of the vehicle's workday)

Providing this information to the IT company will help them determine what kinds of access points to use, how many are needed, and where they should be located in the parking area.

Setting Up Security

The WiFi network should be protected from unwanted users by implementing security protocols. Ideally, WiFi access points that support N wireless standards (802.11n) should be used, with WPA security enabled. The N standard supports network speeds of up to 450Mbps with the WPA security protocol, or up to 54Mbps with the WEP protocol. Access points that

support 802.11b/g standards can realize a maximum network speed of 54Mpbs using WEP, or WPA security protocols.

Testing the Hotspot

After the equipment is selected, and the hotspot is set up, it must be tested to ensure that it is functioning as intended.

Preliminary testing should measure the actual upload and download speeds of the WiFi network, test the WiFi controller's ability to optimally manage the WiFi clients of all the access points, and check that the entire parking depot is properly covered by the WiFi network and that no dead areas exist in it. If dead areas are found, access points should be repositioned and/or added as necessary to achieve full coverage of the entire depot.

When the system is up and running, routine testing should be performed on a regular basis. Testing should ensure that all of the devices are functioning properly, that there is no significant interference on the channels used for data transmission, and that no rogue devices have circumvented the network security and connected to the WiFi network.