VIRSIG

Resilient Temporary Networks

By Shelomo Alfassa, *Director of Communications for Virsig, LLC.*

A specialty service in the high-tech security industry that is not often discussed, is the establishment of the Resilient Temporary Network (RTN). These are temporary, field-deployable, purpose-built IP networks that can be installed and broken down quickly. Commonly, they are used by public safety and others, at events where temporary but increased situational awareness is needed. They are usually installed outdoors, often connecting buildings to mobile command post vehicles, or linking a command post in a tent to a set of high-resolution cameras, or just about any other configuration imaginable.

When the President of the United States arrives to give a speech, or when a local law enforcement agency is preparing for a major public event, the authorities always must prepare the locality for a certain level of expected criminal activity. This may be anywhere from illegal civil disobedience on the street, all the way up to preparing and anticipating a man-made act of terrorism. To meet these needs, the design and tactical implementation of a (wired or wireless), Resilient Temporary Network is employed.

On the surveillance side of the network may be numerous temporary cameras—including infrared, thermal, and night vision. The network may also include technologies such as people counters, area detection lasers, vibration sensors, etc. The Resilient Temporary Network must address all needs, such as power, uninterruptable power, or anything related to IT bandwidth, secure data services, the ability to send encrypted audio and video, etc.

While Resilient Temporary Networks can be wired (Spanning Tree Protocol {STP}) or wireless (Wireless Mesh Architecture), they essentially work in a similar manner. Yet, while each comes with a unique set of pros and cons, what both do well—is they can repair themselves. Utilizing a mesh configuration, in place of a point-to-point configuration, allows data packets to be reconfigured and re-routed around broken paths, using self-healing algorithms. Using dynamic connections between the nodes, data packets have the availability to seek multiple paths as they travel through the network, making the overall network substantially more stable. The Resilient Temporary Network must be able to maintain up-time, as mission-critical data flows across it.

The specific hardware chosen should be able to withstand changing weather conditions, and when there is trouble, must be able to recover quickly and automatically. Therefore, selection of cables, of peripherals, and of climatic conditions should be considered in advance.

As a chain is only as strong as its weakest link, information transport systems laden with associated peripherals (e.g. digital voice, data, video, sensory, imagery, etc.) are only as strong as the network they're on, and that's why these networks must be strong and resilient.