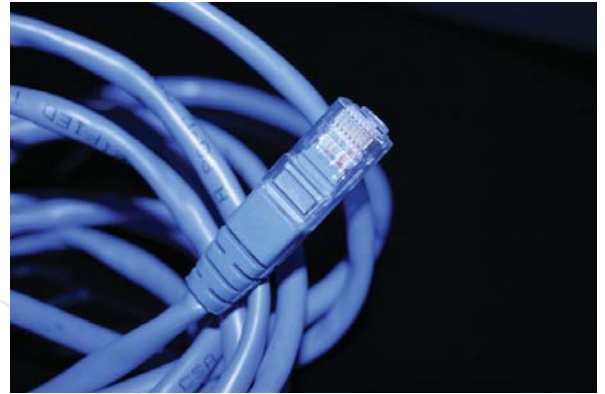


The Importance of Network Topology

As developer of core CCTV software components for manufacturers, OEM partners and other third parties such as integrators, we have seen an increase in the need to understand the networking aspects of each project right from initial conception. One of our customers recently asked us to assist with a proposal involving a video management suite for installation across multiple remote rail platforms using an existing trackside gigabit fibre network.



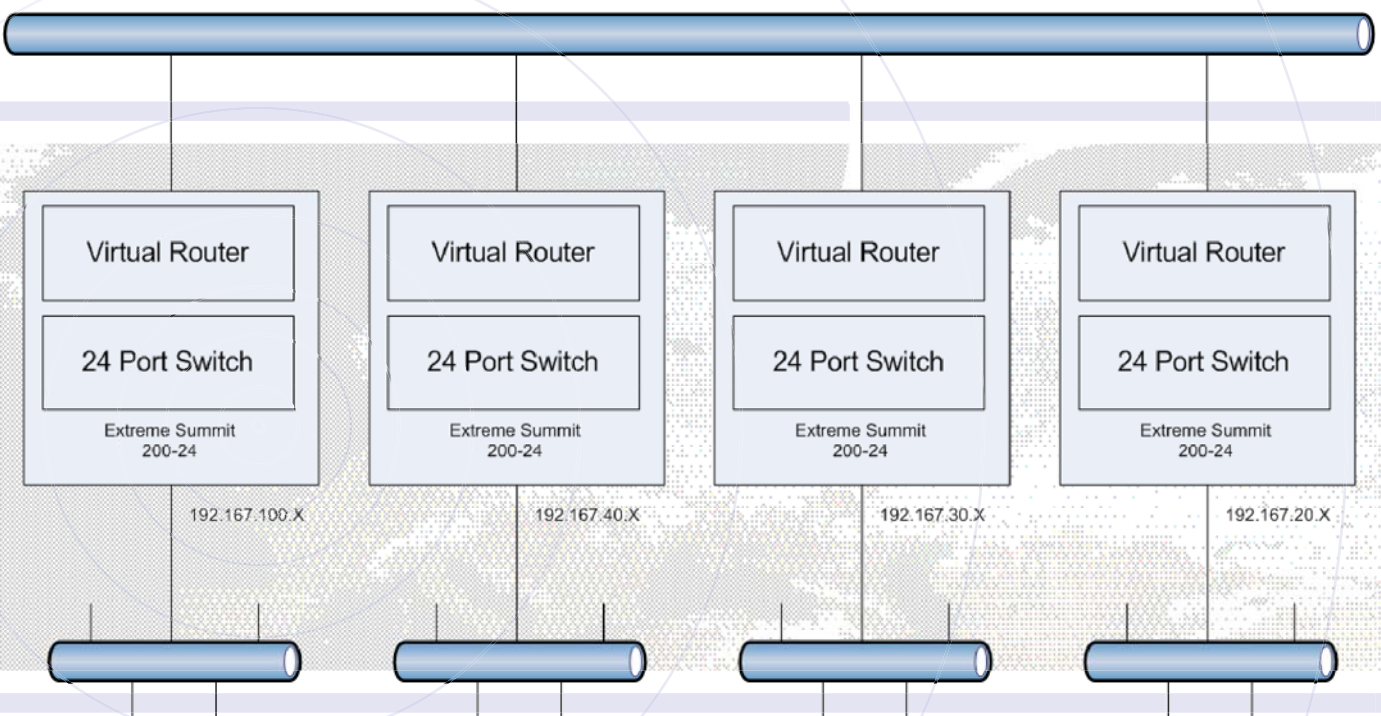
The management suite will be used to manage existing Digital Video Recorders and add new IP Video cameras along with the associated Network Video Recording.

Our initial investigations highlighted a few fundamental issues that are worth sharing and discussing.

■ System Elements & Topology

Composed of 30+ stations located along a rail network, each consisting of up to 16 cameras, a DVR and a GBit switch, the existing topology follows a traditional wide area network configuration of backbone with routed subnets. The virtual IP routing capability of the switches is utilised to implement the topology shown:

1 Gbit Fiber Backbone – 192.167.70.X



■ Multicast Ability

Of course, routing of this nature may result in the dropping of multicast packets. Using the multicast test utility provided by Microsoft called “mping.exe” we were able to test that the router configurations were capable of routing multicast packets. However, the multicast client/server discovery mechanism implemented by Codestuff to help operator stations find recorders and management servers was being dropped as a result of the hop count of the configuration.

It's good practice to set the time-to-live of multicast packets to a low value, in this case 2, as this prevents leakage of packets outwith the local area network as a result of a misconfigured routing device.

Normally this would suffice as most networks implemented for IP video are of a flat nature with routing being avoided at all costs. This was easily solved by increasing the time-to-live value to 5 to allow operation over the existing network. We also implemented a static discovery mechanism that avoids the need for multicast packets for networks where the time-to-live is unknown.

■ Routing with large packets

Routing has the potential of adding a bottleneck to the system where a number of video streams need to be processed by one device. If the device isn't designed to handle high bandwidth, time sensitive data then packet loss and delays may be introduced.

For best results when routing is required it should always be provided by a dedicated device designed for high performance routing. When routing is combined as a function of a Layer 3 switch it is often implemented by a software engine and therefore can perform poorly. Even switches advertising wire speed routing can severely limit the performance of video streams.

Turning our attention to video quality we find the performance to be poor in comparison to other installations on networks with similar wide area requirements.

On investigation with Wireshark we found a large number of data packets were being dropped or corrupted somewhere between the server at a remote station and the client application running in the monitoring station.

When testing with the DVR manufacturer's web client, video quality appeared to be good but on closer examination it was clear that it too had the same issues. As a result, the TCP/IP connection used to stream video was buffering the stream in order to wait for retries, which in turn only served to exacerbate the problems. This gave reasonable video quality but greatly reduced the frame rate whilst adding latency to the system.

Further investigation using “ping.exe” initially showed a health network with 100% responses over several minutes of testing. Only after increasing the test payload size using the switch “-l” did we start to see packet loss related to the data size. We did not perform any measured testing but it appeared that the larger the packet size the more likely it was to be lost on the network. At some points we saw percentage losses as high as 85%.

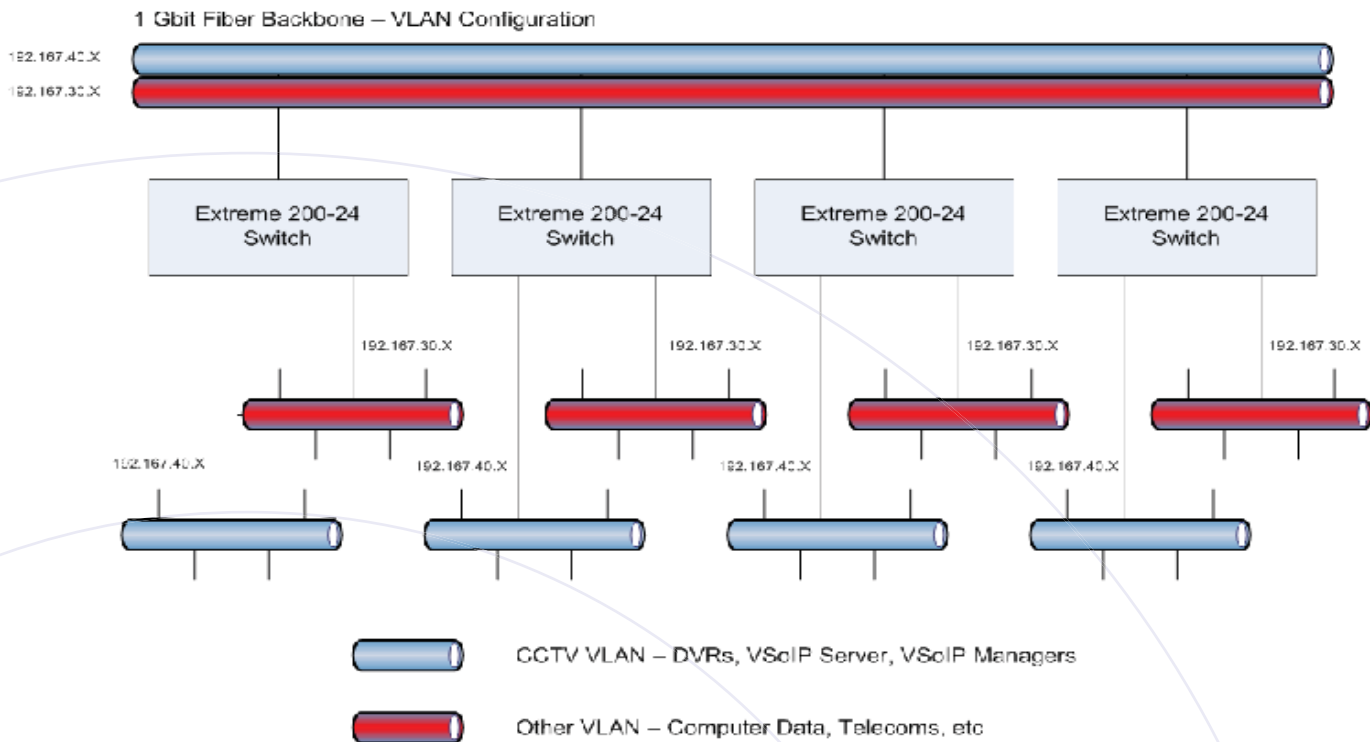
Clearly this has a huge impact on the overall performance of all applications utilising this network.

■ VLAN Solution

Given the short comings of the existing topology the recommendation was to adopt a flat topology avoiding the existing issues.

Without understanding the whole requirements of a network it is hard provide the best topology, however most installations today can be catered for by implementing a VLAN topology and linking switches via VLAN trunks.

This has the advantage of presenting a flat structure to the network devices but at the same time allowing the segmentation of traffic based on application type or departmental requirements. When inter-application or departmental communication is required we can either assign particular users as members of both VLANs or introduce a routing element to pass traffic from one VLAN to another – assuming the addressing scheme of each lends itself to this. The following diagram shows such a configuration:



Conclusion

The VLAN topology avoids all the issues of the previous topology; the virtual flat network removes any hops from the system and allows multicast traffic to pass freely and with no routing overhead but still having the ability to segment and control the distribution of traffic.