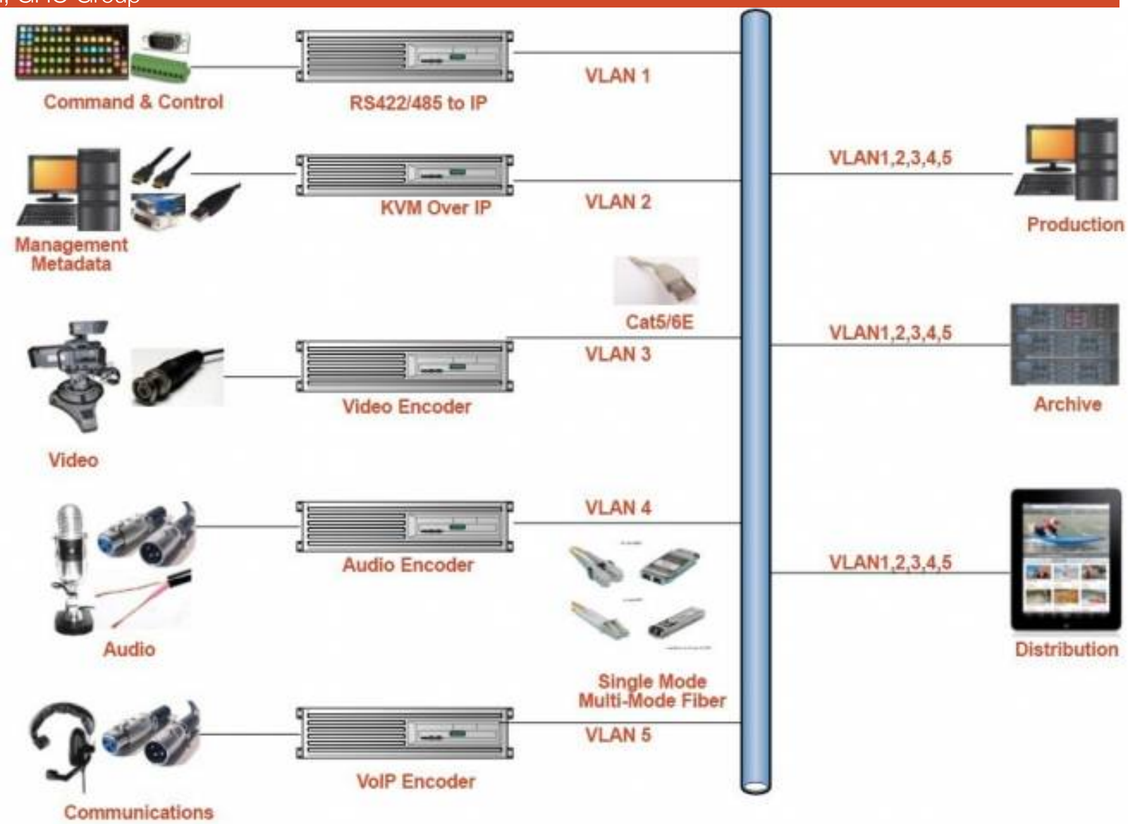
How Coax became a VLAN

July 28th 2014 - 06:35 PM

Gary Olson, GHO Group



There have been many significant changes in the core technologies that make up the infrastructure of the broadcast facility. The cable plant is or was the heart of the broadcast facility. And there are many different types of cables. Now the IP network is the primary backbone and the IP routers and switches play a significant role in media transport, command and control and monitoring. There are many layers within the IP topology. In an SDI environment most of these layers communicate or transport media using different cables and/or fiber optics and are managed by a different type of switching, routing and distribution architecture. In the IP world these layers are known as VLANs (Virtual Local Area Networks) which are segments within the core IP network.

Instead of individual cables the IP network can be segmented and each of the different signal types co-exist in the same packet stream using the same routing and switching environment on the same cable and/or fiber. They can do this while being isolated, traveling separately and protected.

The signal handling within the SDI architecture is managed by each signal type having its own cable type. There is some sharing, however the paths and devices that manage the signal flow are unique to the signal. There is SDI video (SD, HD. UltraHD and 4K) with embedded Audio and sometimes data, analog, AES & Madi audio, 2, 4 Wire and VoIP Communications, RS422 & RS485 and IP control and management.

Signal	**Cable**	**Connector**
SDI Video	Coax/fiber	BNC/ST
AES/Madi Audio	Coax, multi pair/fiber	BNC/Phoenix/ST
Analog Audio	Single/Multi Pair	XLR/Bare end
Machine Control RS422/232	Multi Conductor	DB9, Phoenix
Management	Cat5/6e	RJ45, Punch block
Intercom	Single/Multi Pair	XLR, DIN
Router Control	Coax/Multi-pair/CAT5/6e	BNC/phoenix/RJ45, DB9

In the IP architecture, each of these signals are either encoded to IP or originates as IP at which point it will use the same network cable type (CatxE or Fiber). Also once the signals become IP, they all use a similar type of switch. In the IP architecture the way signals or media types are differentiated and segregated is by individual networks or network segments. It is very cumbersome and inefficient to build separate networks with separate switches and cabling to support each of the signal formats, so instead of using separate switches, a virtual network is created within the network. These Virtual Local Area Networks are more commonly known as VLAN's. A VLAN is a network segment or partition that is created inside the core network and established as a separate domain.

In the VLAN network topology, the different devices and their signals are connected to the same switches and it is part of the switches responsibility to "groom" the signals together into a single IP stream. The network can be configured with multiple VLAN's enabling all the different signals and files to co-exist and move about the network infrastructure on the same cable/fibre and using the same switches.

This table shows the how the signals now map to a VLAN, plus there are new VLAN's that are needed for information or data that did not exist in the SDI architecture.

VLANs replacing cable	Format
Video Streams	MPEGTS, JPEG2000, H.264/5
Video Files	MXF, .mov, .QT, DnX
Audio Streams	Madi, CobraNet
Audio Files	Wav, mp3, AIFF, PCM
Intercom	VoIP
Command and Control	xml
Machine control	xml
Router control	xml
New VLANS in the IP infrastructure	
Metadata	Text
Media Management	Text, jpg, proxy, application access
KVM transport	High resolution video, mouse and keyboard

So in essence, each VLAN can be compared to the unique cables previously used for each of the signal types. Now, each of the signals are in the same switch and are groomed into a single IP stream that travels over the same cables/fibers. As it connects to each device on the network, the device understands which VLAN and signal it is taking commands from, whether it is sending or receiving files and what process to execute or what file to manage.

VLAN's provide support for critical network management such as bandwidth management, latency control, access control and security. Interestingly, the KVM is one of the highest bandwidth users since all nodes receive high resolution video all the time. It is critical to isolate this or it will interfere with media movement and command and control.

VLAN's are created in the network router and/or switch and the VLAN's are managed and controlled so that each segment is optimized for the specific signal type or data it will carry. Each VLAN is based on using the primary network addressing structure and creating a unique IP address range per VLAN and specific device addressing under the VLAN address range.

Example

If the main IP network addressing is based on a 10.bbb.ccc.ddd schema, then the first set of numbers or octet 10 identifies the main network address, the second octet bbb is the main network segment, ccc identifies a VLAN and ddd is the specific address for a device. So in this example an server with an address of 10.250.12.25 would indicate it's main network segment is 250 and is on VLAN 12 and the unique device IP address 25 .

In the table below the range addresses change but there can be many devices with the same last octet address without creating a conflict as long as they are on different VLAN's.

If we look at mapping a network's VLANs we might see the following

VLAN Description	**VLAN range**	**Device**	**Device address**
Video Streams	10.250.10.xxx	Encoder	10.250.10.25
Audio/ Video Files	10.250.12.xxx	MAM Server	10.250.12.25
Audio Streams	10.250.13.xxx	Mixer	10.250.13.25
Intercom	10.250.15.xxx	Intercom	10.250.15.25
Command and Control	10.250.16.xxx	Automation	10.250.16.25
Router control	10.250.18.xxx	Router Matrix	10.250.18.25
Metadata	10.250.19.xxx	MAM	10.250.19.25
Media Management	10.250.20.xxx	Storage	10.250.20.25
KVM transport	10.250.21.xxx	Distributed control	10.250.21.25

There are different ways to manage network traffic and the segregation of VLANs. Access Control Lists (ACLs), Trunking and Quality of Service (QoS) are a few.

It's interesting to view the transition from a physical cable carrying different signals to an IP packet and addressing convention where all the signals can be groomed into a single stream, devices can read and resolve the information or commands based on the address and all within one IP network topology.