The Anatomy of the IP Network, Part 1

November 3rd 2014 - 02:00 PM

by Gary Olson, President, GHO Group

Stuart Miles, FreeDigitalPhotos.net

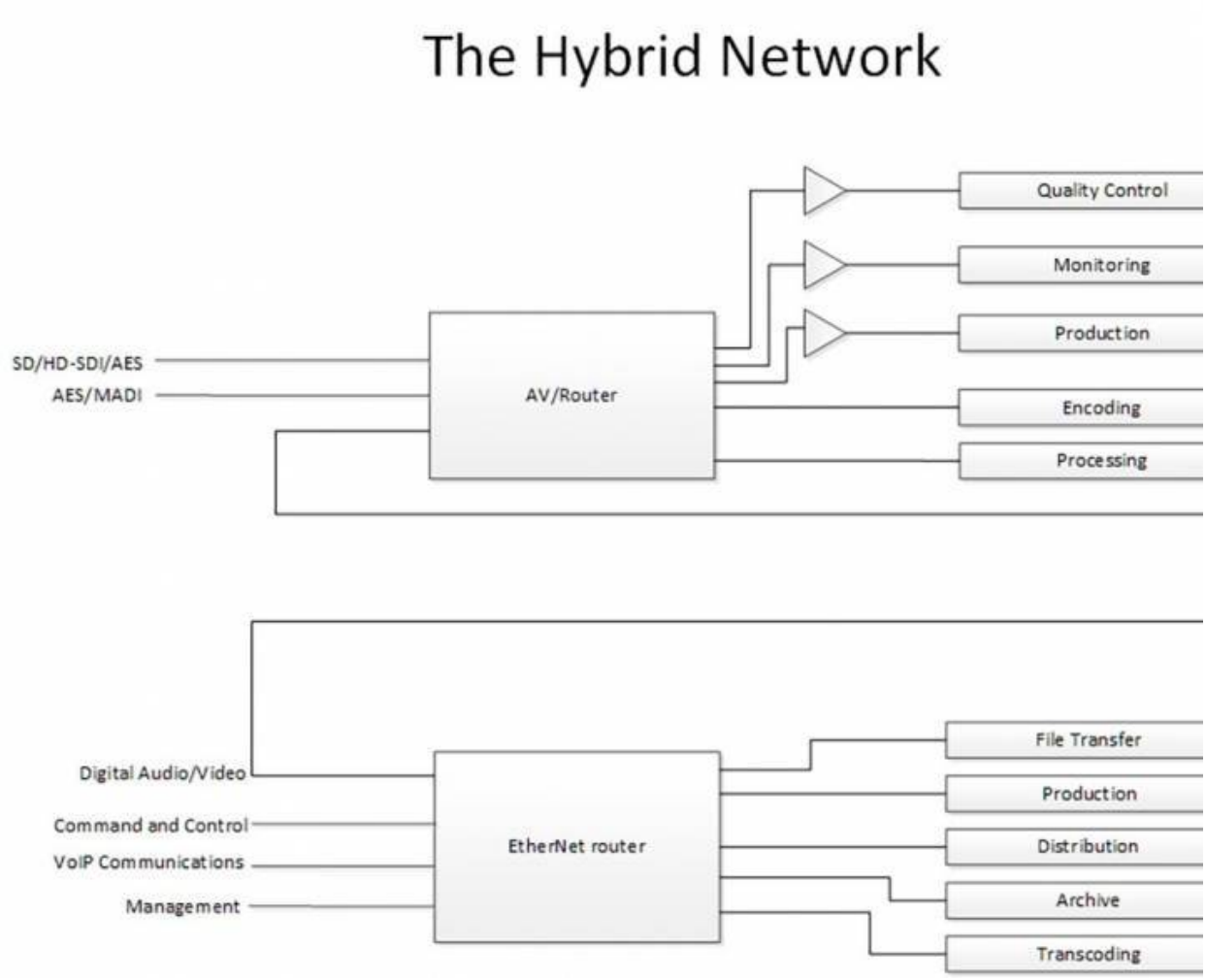
This is the first in a three-part series of articles to help engineers and technical managers better understand the IP network, which has become the core technology in the broadcast center.

The term IP is derived from the original Internet communication protocol, Transmission Control Protocol/ Internet Protocol, more commonly known as TCP/IP. When Ethernet was introduced for networks, so was TCP/IP as the transmission protocol. The Information Technology (IT) sector has been using Ethernet switching since 1983 when it first became commercial. As the technology matured and other protocols such as User Datagram Protocol (UDP) was introduced for large packet transmission, the generic term for networks and computer systems became IP and the terms TCP, UDP and others now refer only to the transmission protocols.

Recently the IP network router and switch has been replacing the SDI router as the most prominent technology in the core infrastructure. It has been one of the key technologies in the broadcast plant for quite some time, handling command and control communications of devices plus functioning as the management layer of systems and devices that use web browsers or interfaces. The IP router has now moved front and center, handling all aspects of media, from creation to production to archive and distribution.

The broadcast center is very much a hybrid environment. There will always be legacy content in the

archives and remote production will continue to use removable media that includes tape.



The diagram above highlights the primary functionality of the SDI and IP systems. More and more of these processes are moving into the IP environment. First and foremost is quality control, there are different parameters and different tools to measure, analyze and diagnose files and streams. The IP network has its own measurement and monitoring requirements for performance, in addition to measuring and monitoring the quality of files and streams.

There are some terminology challenges to overcome in understanding IP networks. The IP router is a completely different technology than an SDI router. Where the SDI router can “route” any input/source to one or many outputs/destinations in a one way or simplex path, the IP network is fully duplex and all ports can receive and transmit simultaneously to each and all of the connected devices.

When looking at the network topology there is the architecture of the network and how it connects to the end points, the server infrastructure and storage layers. There are the different network protocols to address the transmission requirements of data, files and streams.

The broadcast and enterprise networks have different performance requirements and they should be

segregated to better control and manage the security and integrity of each network. The integration of business and media workflows requires that touch points aka integration is allowed between the two segments, however these touch points need to be managed and controlled.

The entire IP infrastructure is comprised of a number of different types of networks. There are different protocols within each of these networks, however they are all based on Ethernet standards and protocols.

- Local Area Network [LAN] – This is the core network infrastructure and it is in the same geographical location with physical connections to users and devices. The LAN will typically have a single router and then can be comprised of multiple switches. The LAN is the backbone that the WLAN and WAN interface with that provides the necessary connectivity for network services.
- Wide Area Network [WAN] These are geographically separated and connected using telecommunication services (ie. ATM, MPLS and SONET). There are routers and firewalls at each endpoint of the WAN before it is connected into the LAN at each end.
- Virtual Private Network (VPN) is a subset of the WAN. It enables remote users using secure protocol over open Internet to access the core LAN. VPN creates a tunnel or private path within the open Internet protocols that prevents others from seeing the tunnel or any data transmissions.
- Wireless Local Area Network [WLAN] also known as Wi-Fi. Wi-Fi actually doesn't stand for anything, it was a humorous play on Hi-Fi (High Fidelity) as something catchy to pay homage to audiophiles. Wi-Fi is a sub network or segment to the core network. It has its own protocols and is behind the firewall. Wi-Fi is connected to the core Ethernet switch and attached devices are assigned IP addresses the same as wired connections from the core router. A Wi-Fi network can operate without connectivity to external networks or the Internet. This is used in secure areas to provide mobility to maintenance personnel. Wi-Fi is less secure than a wired connection. It is important to understand that mobile wireless services (3G, 4G & LTE) are different than Wi-Fi.
- Storage Area Network [SAN] Storage networks are different than Network Attached Storage (NAS) devices. Network Attached Storage are devices that are attached individually to the network. The SAN is a storage cluster is attached to the network from a Single connection port. SAN's have their own protocols that are not always Ethernet based. There are Fiber Channel and Ultra Wide SCSI protocols to name a few, which are higher bandwidth than Ethernet. However as Ethernet bandwidth increases to 10Gb/s, 40Gb/s and 100Gb/s bitrates, it is making Ethernet an attractive option for the throughput demands of media.

One of the most critical components in network design is the firewall. This is neither a switch nor a router. It can be software running on a server or a dedicated hardware appliance. The firewall is what manages the rules and policies that govern access to the network from external applications, other networks and when internal applications are reaching out to outside networks**.** The firewall is the gateway between the network and the Internet as the first but only tier of security preventing intrusion and isolating the network users from unauthorized access. Security is one of highest priorities in network design.

IP Addressing

All devices, including dedicated appliances, computers, tablets, servers and storage on the network require an IP address for them to communicate with each other. There are different types of IP addresses. First, there are public and private IP addresses. There is Point to Point Over Ethernet (PPOE), Dynamic Host Configuration Protocol (DHCP) and Static IP addressing. Public IP addresses were originally assigned by the Internet Corporation for Assigned Names and Numbers (ICANN) and as of 2011 by Internet Assigned Numbers Authority (IANA). IP addresses are typically issued in blocks or ranges. IPV4 (Internet Protocol Version 4) is the most recognizable and was developed and in use since 1981. It is based on a 32bit address with ~4.8 billion addresses, however with the global proliferation of connected systems and devices, they have used up all the available numbers. There is now IPV6 (version 6) that's based on a 128bit address that will provide approximately 3.4×10^{38} network addresses. Which should last a while.

Courtesty publicpolicy.telefonica.com

There are private IP addresses that are restricted to ranges that have been reserved for private networks. These are non-public protected ranges that can be used by anyone and are not restricted to any one user group. These private addresses are configured and assigned by the router on each network and based on the requirements of the device can be DHCP or a static address within the restricted range (The most common is 192.168.xxx.xxx). One of the roles of the router or the firewall is to provide Network Address Translation (NAT). NAT is needed because private IP addresses are non-routable on the public Internet, so they must be translated into public IP addresses before they can access the Internet. The router is assigned a Public IP address or addresses, within the router the different subnets and VLAN's are assigned private IP ranges, devices can then be assigned static or DHCP (network assigned) addresses.

In the next article of this series, we will discuss Network Layers and Protocols.

This article is part of Olson's continuing series "Smoothing the Rocky Road to IP". Other articles include:

The Anatomy of the IP Network, Part 1

The Anatomy of the IP Network, Part 2

The Anatomy of the IP Network, Part 3

Changing Technology: Panacea or Pandemonium

ASSOCIATED RESOURCES:

The Anatomy of the IP Network, Part 2

The Anatomy of the IP Network, Part 3