The Anatomy of the IP Network, Part 3

November 17th 2014 - 02:00 PM
by Gary Olson, President, GHO Group

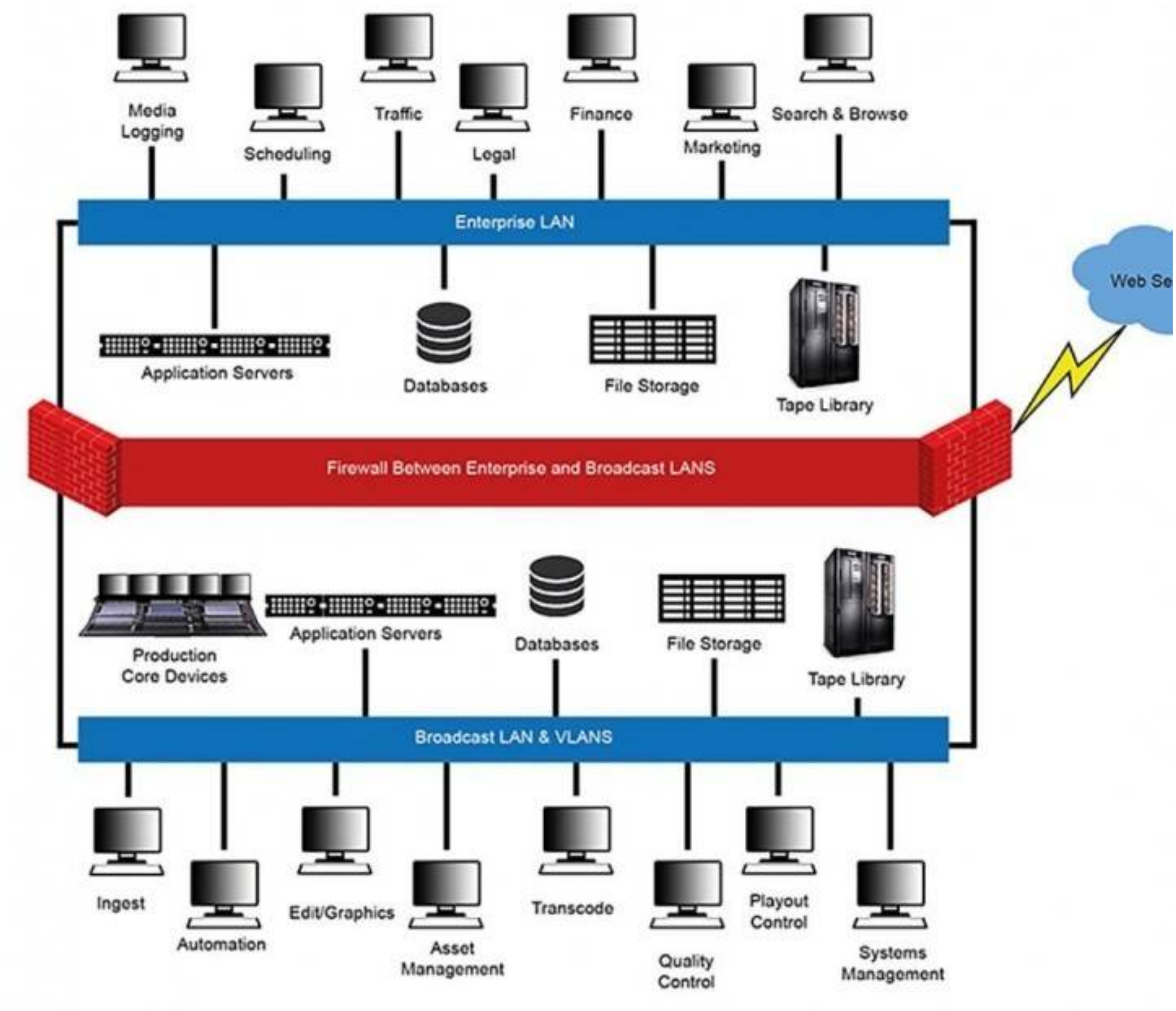
Stuart Miles, FreeDigitalPhotos.net

In this third and last part of the series on IP networking, we will look at the components that make up the network infrastructure.

Parts 1 and 2 of this series can be found here (Part 1) and here (Part 2).

Network Topology

The design and configuration of the broadcast IP network topology is different than the configuration of network topology in the enterprise. In both cases there are many broadcast, production and business layers to the network. In this context the term ***Layer*** is used to describe various processes and operations that are integrated by the network.



Typical IP network with multiple clients, and storage. In this case, one network (top half) serves the business sector, the other (bottom half) is exclusively reserved and protected for content tasks.

Looking at IP network devices, Layer 2 (datalink) and Layer 3 (network) are the most common layers when working with the core network infrastructure for switching and routing. The third most common network component that is not identified by which layer it resides on but is critical to the network architecture is the firewall. The router is a Layer 3 device, switches are typically Layer 2 although there are Layer 3 switches that begin to integrate router (Layer 3) functionality and feature sets into the switch. This reduces the number of unique devices and makes management easier.

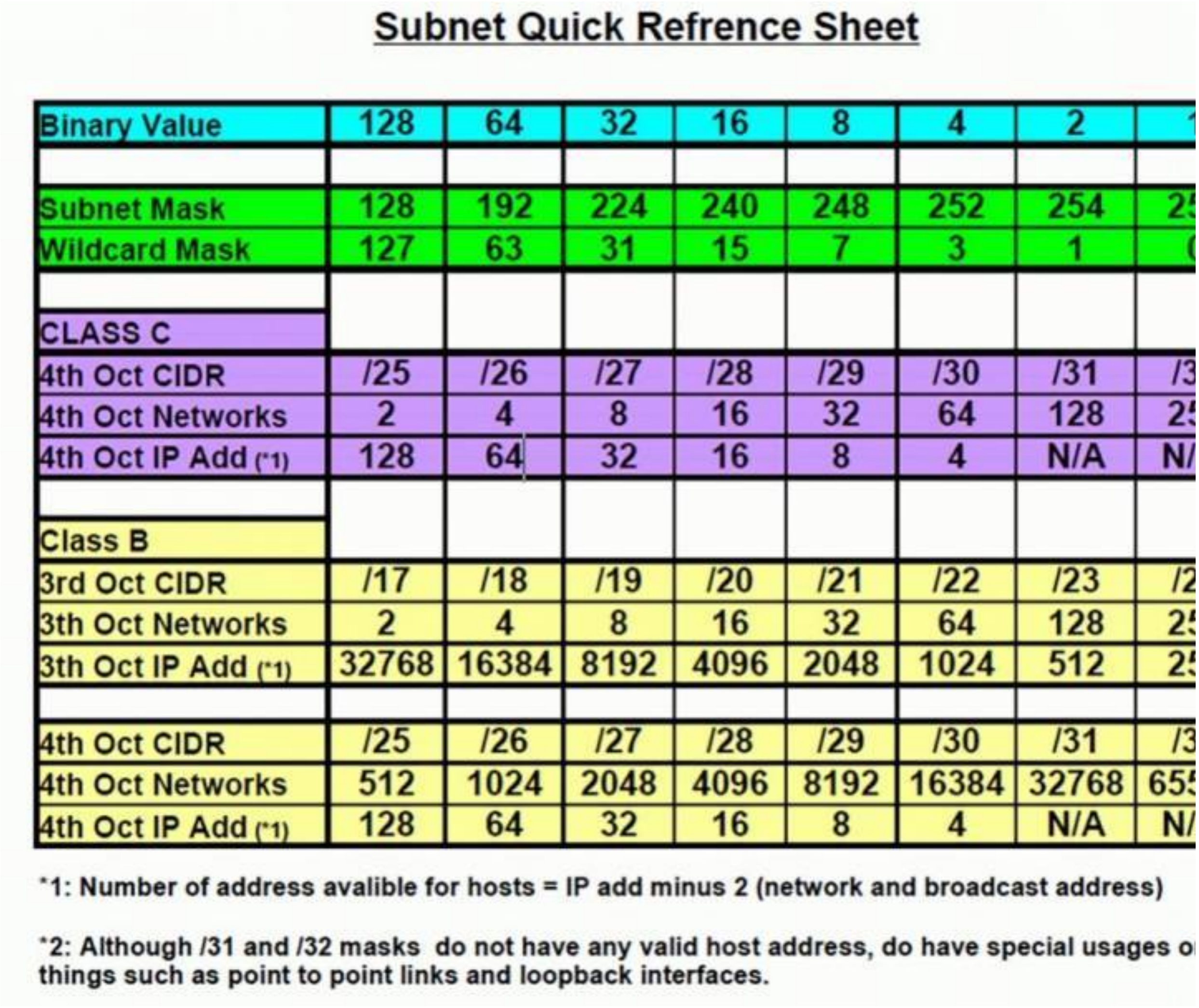
There are different network topologies used for long distances ie. ATM, SONET and MPLS, these are high bandwidth network services for interconnecting geographically separated locations. Taking this a bit further, an IP router is a Layer 3 device, its role and responsibilities are to provide connectivity to the Internet and other networks. It requires a network address from the external network it is connected to and also provides the network addresses to all devices within the internal network it is managing.

The IP router is part of Layer 3, the network layer and is the heart and brains of the network. The network switch is a Layer 2 device that moves data based on the Layer 3 routing tables and the data path that is determined by the Layer 3 router. In a typical network configuration the router is a separate device that connects to outside routers for Internet and connecting multiple locations together. In larger networks, the more sophisticated devices are Layer 3 switches which have integrated the feature and functionality of both a switch and router.

The firewall is a hardware device or software technology that protects the network from other networks. The Internet is very much considered a network and is very unsecure. It is the firewall that manages all the incoming and outgoing traffic based on a set of rules. It is firewall technology that is the first line of defense against the proliferation of intrusion and hacking. The network switch handles the distribution of data and controls bandwidth to all the devices on the network. There are managed and unmanaged switches.

- **Unmanaged switch** -allows all traffic on the network to be broadcast to all devices and it becomes the responsibility of the device or application to understand which part of the data stream it needs to perform its function without getting confused or overwhelmed by network traffic.
- **Managed switch** - each port can be controlled and therefore enable or prevent data from reaching a device or application that does not need it or should not have it. This is accomplished by controlling which IP address or MAC addresses can interact with another IP addresses or MAC addresses.

Once the basic network is created, there are configurations and settings that will optimize it for and also be segmented for different systems and file types (ie. Quality of Service [QoS]). This is to maximize network performance, prevent latency and allow protection of the information. Instead of having multiple independent networks each with their own routers, switches and cabling, the core network can be partitioned or segmented. There are two primary types of segments, they are called Subnets and Virtual Local Area Networks (VLANs). The traffic on these can be either fully isolated or enable some amount of cross-over traffic using configurations known as Access Control Lists (ACL's) and Trunking. There are subtle differences between a subnet and a VLAN.



Subnet Quick Refrence Sheet

Binary Value	128	64	32	16	8	4	2	1
Subnet Mask	128	192	224	240	248	252	254	25
Wildcard Mask	127	63	31	15	7	3	1	(
CLASS C								
4th Oct CIDR	/25	/26	/27	/28	/29	/30	/31	/3
4th Oct Networks	2	4	8	16	32	64	128	25
4th Oct IP Add (*1)	128	64	32	16	8	4	N/A	N/
Class B								
3rd Oct CIDR	/17	/18	/19	/20	/21	/22	/23	/2
3th Oct Networks	2	4	8	16	32	64	128	25
3th Oct IP Add (*1)	32768	16384	8192	4096	2048	1024	512	25
4th Oct CIDR	/25	/26	/27	/28	/29	/30	/31	/3
4th Oct Networks	512	1024	2048	4096	8192	16384	32768	655
4th Oct IP Add (*1)	128	64	32	16	8	4	N/A	N/

*1: Number of address avalible for hosts = IP add minus 2 (network and broadcast address)

*2: Although /31 and /32 masks do not have any valid host address, do have special usages o
things such as point to point links and loopback interfaces.

Subnetting is key to isolating certain tasks and gear. Look for additional guidance before deciding on a subnet scheme. Courtesy pic2fly.com

- **Subnet -**is the segmentation of a network done at the server or device by using different subnet mask addresses on a single network. In an open network, all subnets on all switch ports are visible to any device configured for that subnet. Subnets do not manage bandwidth or allow optimisation.
- **VLAN** - is the partitioning of the network into isolated segments done in the router and function as if they were physically separate switches. VLAN access is controlled at the switch port, if a port is not configured to pass a specific VLAN, then any device assigned an IP address in that VLAN will not be able to access data even if the device is set up with the correct address. Traffic can cross VLAN's only if configured in the router. In the IP broadcast environment VLAN's are used to segregate different signal types within the same network (ie. video, audio, communications and control).

There are a number of configuration settings within the router and switches to manage priorities, control the amount of bandwidth, synchronize data movement and protect the data as it moves between systems and devices. One example is Quality of Service (QoS), this is a priority structure that determines which packets reach their destination first and without interference from other packets.

Here is an example of QoS: While a large media file is moving from the encoder to the archive, a command is sent from the playout server to the SDI router to switch sources for a program feed to air. . The playout command is a small packet, the media file is large. Without QoS, the playout to router request gets lost and the program does not make it to air on time. QoS insures the control command gets Priority 1. The playout command most likely will be on its own command and control VLAN and the media will be on a different one fully segregated from command and control.

Broadcast and production put high demands on IP networks. The applications that are handling media files and streams are more bandwidth intensive than enterprise applications using documents and spreadsheets. Even large enterprise databases are not bandwidth "hogs". Taking a look forward at the next generation of infrastructure requirements, the industry is pressing for high resolutions like 1080P and SDI is moving towards 3Gb/s. The higher resolutions need more bandwidth and for SDI 3Gb/s will enable it to handle the new formats with higher bitrates like 2K, 4K and 8K. The manufacturers of broadcast and production equipment (ie. Audio video routers, terminal and distribution) are pressed to provide products that will support 3G. These higher bitrate formats can fit comfortably in the IP world as its next generation is 10Gb/s, 40Gb/s and 100Gb/s which in comparison is much bigger than 3Gb/s.

The next generation in networking is *Software Defined Networks* (SDN). The complexity of routers and switches has increased to a critical level where the amount of processing, virtualizations and configurations these devices need to support, has added a layer of overhead and in many cases latency to the core functions. To alleviate this burden, dedicated servers that are tightly integrated to the switch topology became necessary. The next logical step was to "de-couple" the server from the router and switch frames to handle all the processing, routing and management. In this way the switches become slaves or clients with the ports being defined and controlled from the server. In this way the configurations no longer need to reside in each switch. This will change how the network is designed, where Layer 2 and Layer 3 switches are required and the how the entire LAN, WAN, WLAN and VLAN architecture is structured. By using an SDN design, it makes network management less cumbersome. This improves network performance and reduces the requirement to update each device when there are changes or modifications.

The IP network is now the core technology in the IP and file based workflow infrastructure. More than the SDI router, it transports and manages media files and streams, communications; and command and control of the entire IP based architecture. The article "How Coax Became a VLAN" is also part of this series, connecting the evolution from SDI into IP beyond tapeless to the physical cable infrastructure.

This 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 1
- The Anatomy of the IP Network, Part 2