Vigitron IP Infrastructure Design Educational Series

20 YEARS Transmission Leadership

VIGITRON

Layers: What Do They Really Mean?

Layers: What Do They Really Mean?

When it comes to setting the criteria for network switchings, how often do we hear “I only want a Layer 3 switch”? Naturally, we assume a Layer 3 switch must be better than a Layer 2 switch because the number is bigger. However, it may come as a surprise when you learn that it may not be the case when it comes to video security applications. In fact, the opposite is true.

Defining a network switch is already a difficult task. Adding the concepts of layers to it make it even more difficult. Layer is defined as the organization of protocols reflecting certain functions that must be performed in a certain order for programs contained within physical devices to communicate with each other. To make it simple, layering (as applied to computers) is a marketing term that has no relationship to any particular standards.

Layer 2 operates by learning the Media Access Control (MAC) address of the device connected to each port and when commanded, forwarding the requested information from that device to the requested port. For example, assume that we have two cameras - one connected to port 1 and the other connected to port 2 of the switch. At port 3, we have a VMS server. By knowing the MAC addresses of these devices when the VMS server requests information from the cameras, the switch knows that camera 1 is connected to port 1 and forwards this information on to port 3. The process holds true for the camera connected to port 2. Keep in mind that every device (including computers and cell phones) has its own unique individual MAC address. This process also applies to many of the internal workings of a network switch such as setting up VLANs and spanning tree operations, both requiring the routing of the devices between ports.

There is one significant drawback to the Layer 2 process. All devices must be on the same subnet. For example, “192.168.1.100” and “192.168.2.100” may seem to be similar IP addresses, but the difference between the 1 and the 2 puts them on different addresses and prevents communication between the two addresses. The same is true if the addresses are the same, but exist on different subnets. This is when a Layer 3 switch is used. It involves different types of hardware and software based on the signal routing of IP addresses. This is common to all devices, regardless of the protocol used. The simple difference between a Layer 2 and a Layer 3 switch is that Layer 3 has a routing process that allows it to operate across different subnets. Your ability to access Google and other websites exists due to Layer 3 switching operations. The questions you’re asking of these services and the responses you’re receiving exist on different subnets.

To complicate the matters, we often hear of the term “Layer 2+”. What is Layer 2+? If the number and features applied to define any layer are made up, then the term Layer 2+ can be applied to any switch by any manufacturer for any reason. There are no standards. Since we assume 2+ is better than 2, then a Layer 2+ switch must be a better choice than the standard Layer 2 switch.

We often get tied up in the details and often overlook how equipment performance applies to our actual application; whether our system is analog or digital (CCTV standars for closed circuit). Thus, you have to question why any security system would want to pay extra for a feature that should not be used. Of course, Layer 3 switches cost more than Layer 2 switches and expose themselves to a high potential outside access. So, why would a video security system want to run on different subnets? Most security systems are usually not major networks and the primary concern is the amount of usable bandwidth allowing all of the cameras to be fed to a single recording point. What role does Layer 3 play in this? You can configure switches within the same network using Layer 2 to communicate with each other. You can establish a single switch to serve as a network backbone communicating with other switches to create a single communication point. Using the stacking process, you can designate one switch as a “Master” to receive access to the other switches in the network. These can all be accomplished with Layer 2 switches. Using Vigitron switches, you can stack with the same or different subnets.

What is the advantage of operating a single security system as different networks? If numbers are that important, consider this, there is a Layer 7.

What is the solution if my project involves a very large system?

Vigitron's unique network switch programming found in their Vi3026, Vi3326, and Vi3010 switches has the ability to overcome many of these problems cost effectively, while still maintaining the security of Layer 2 and eliminating a single failure point.

To learn how you can reduce the cost of large scale systems while increasing reliability, contact Vigitron at support@vigitron.com or your local Vigitron product representative. Vigitron offers free and without obligation Design Center Services staff by trained factory engineers. To access Vigitron's Design Center, click here.

Vigitron, Inc.
Office: (858) 484-5209
Email: support@vigitron.com
Vigitron website: www.vigitron.com | Design Center