Vigitron IP Infrastructure Design Educational Series

20 YEARS

Transmission Leadership

VIGITRON

Securing Security

Securing Security

One of the most discussed topics in the security industry is network hacking. When discussing this topic, we start with the concept that nothing on a network is actually secure. We have to first admit this concept to ourselves and take the next steps to secure our networks. It starts with a paradox. We all want our networks to be the network of everything. We want to access our security systems from everywhere. We want to view cameras, receive alarms, and get notifications on our cell phones or from access points which are not our own. We want to cut the cable with wireless transmission. All of these features are just an invitation for making our systems less secure. We blame camera manufacturers, VMS, and NVR providers, and demand more security without wanting to pay more. We want the convenience of accessing everything over the web. No one is safe. In June, anti-virus software provider, Kaspersky Lab, was hacked.

Most of our security devices protect themselves by using user names and passwords, and in most cases, these are ineffective. The really protection is to limit access to your system as much as possible. Again, this is the paradox. In a typical network system, we have cameras connected to a network switch that is fed to a recording device usually in the form of Video Management Server (VMS) or Network Video Recorder (NVR). The first question is how much exposure is it really necessasry? Video security was referred to as CCTV or Closed Circuit Television. The key word is “closed”. Why not think about network video security systems as CNSS or Closed Network Security Systems.

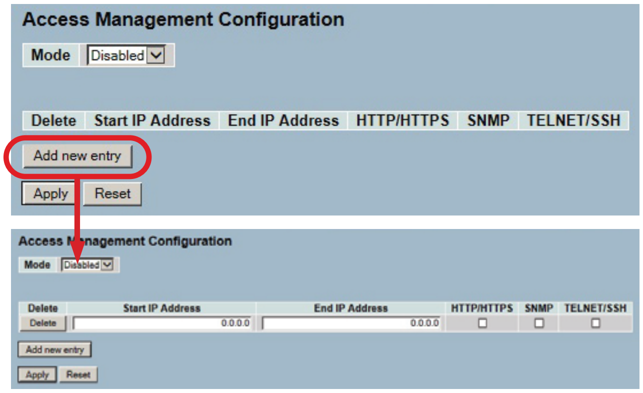
Every access point on a network has the potential to be hacked. Once a security system is hacked, anything is possible. Studies have shown hackers can exchange real video feeds from cameras with fake ones. A play on what used to be cutting the video cord or masking the lens in the analog days. So what can you do to prevent your system from being hacked?

Create a Separate Network

Let’s start with the obvious, make it a CNSS. This can be as political as it is technical, given that governance of security systems is changing from security to IP directors who want to centralize their control. Next is the common sense approach. If you can get access to IP devices by pinging them from any point outside your system, it is an open door for hackers.

Disable Common Access

Disable all common access, especially Port 80, which is most commonly used for Internet traffic. Most network switches can be accessed using a function called Telenet using ports 21 and 23, so disable these as well. How this is accomplished will depends upon your switch's programming.



Access Management Configuration

Mode	Disabled

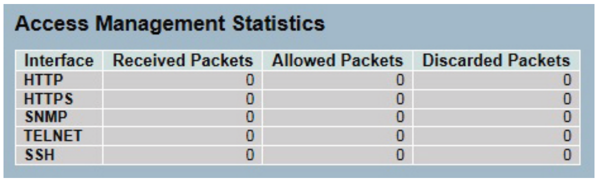
Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH

Access Management Configuration

Mode	Disabled

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	0.0.0.0	0.0.0.0	□	□	□

Vigitron's managed switches not only allow you to enable and disable outside access, but you can program a specific range of client IP addresses that will be granted access. You can also monitor if attempts were made by authorized clients.



Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

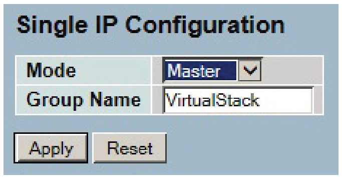
IP source guide allows you to limit the number of specific devices that can access a port. Security protection is provided by specifying not only the device IP address, but also its MAC address.

Create Unique Subnet and IP Address

An IP address is basically a 32 bit number ranging from 0 to 429496794, or the potential to create about 4.3 billion unique addresses. Keep in mind, we are dealing with our own CNSS so any concerns about conflicts outside the network do not exist. For example, if you are using IP address of "192.168.1.xxx" with a subnet of "255.255.255.0", any IP address starting with "192.168.1" will be able to access devices on your network.

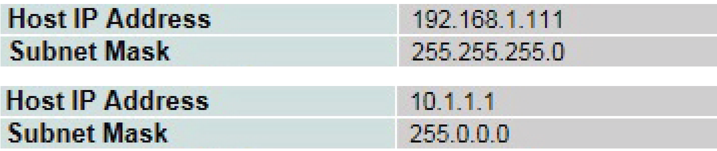
Do you really need a Layer 3 switch?

Layering pertaining to network switches is primarily a marketing term; not a standard. The major difference between a Layer 2+ and Layer 3 is routing. A router routes IP packets between IP networks and is a major point of exposure. Think about routing in terms of Google. You ask a question, send it out, and it crosses hundreds, perhaps thousands of access points on different networks until it is finally received at its destination. It then responds to and transmits back to your computer over hundreds or thousands of additional access points. All of these cross different subnets over Wide Area Networks. Do you really need to have your system exposed to this with the privilege of paying more for Layer 3 capability as opposed to Layer 2?



Single IP Configuration

Mode	Master
Group Name	VirtualStack



Host IP Address	192.168.1.111
Subnet Mask	255.255.255.0

Host IP Address	10.1.1.1
Subnet Mask	255.0.0.0

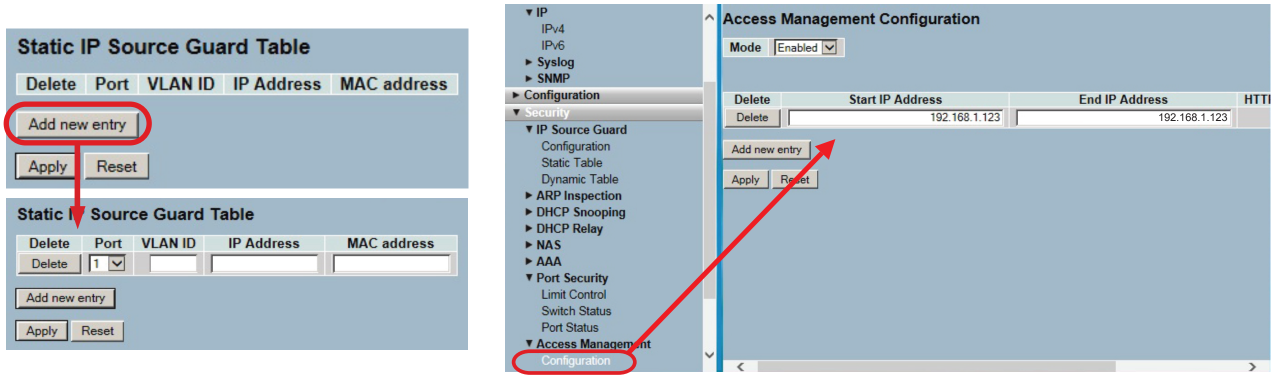
Vigitron's unique virtual stacking function allows you to set up stacking across different subnets controlled from a single IP address providing Layer 3 capability. You can even program VLANs across different subnets.

User Names and Passwords

They give us a sense of security, but in reality, are probably the least secured method. We now know that Android phones can be easily hacked without requiring the user to view a message or open an attachment. In doing so, all your information is exposed including the phone application that allows you to view your security system. While a fix exists, due to the open source nature of Android, it is unlikely to be as effective as single sources such as iOS.

Network Switching

The network switch is your gathering point for your security system. Once you have created your own network, remove access from outside networks by disabling common port access, by avoiding the use of routers or Layer 3 switches. Take additional steps to internally secure your system. One of the most common and effective methods is to use a device's internal system MAC addressing. A MAC is a Media Access Control address. Every IP device has a unique MAC address. Your computer, your cell phone, and every component of your IP based security system has a unique MAC address. Select a managed switch whose programming allows you to secure your system using MAC addressing. Your cameras can be connected to specific switch ports using MAC addresses to prevent unauthorized changes. Most importantly, the MAC address of the client computer can be to tie to the switch preventing outside or even internal access. This feature is known as MAC locking and is directly related to MAC Lockouts, which disables unauthorized MAC addresses from gaining access.



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address

Add new entry

Apply Reset

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

Add new entry

Apply Reset

Access Management Configuration

Mode: Enabled

Delete	Start IP Address	End IP Address	HTTI
Delete	192.168.1.123	192.168.1.123	

Add new entry

Apply Reset

Static IP Source Guard allows only those programmed IP access to access the indvidual port. Access managment configuration allows access to HTTP, HTTPS, and SNMP, TELENET and SSH only from the range of programmed addresses, and rejects non-listed host access to the switch.

In summary, how you construct your network will determine your level of security. Regardless of whether you're using cell phones or thinking that Layer 3 is better than Layer 2, every access point is another open door and is an invitation to hacking your system. Maybe it's time to consider using a "Closed Circuit" approach to networking IP security systems.

Vigitron offers free and without obligation Design Center Services staff by trained factory engineers. To access Vigitron's Design Center, click here or direct any questions on any Vigitron related subjects to support@vigitron.com.

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