Lantech™

Lantech Communication Global, Inc.

Pioneering Industrial and IP Networks

White Paper

Network Security

IES-2008-67

IES-2208F-67

IPES-2208GF-M12

How IP security function and EN50155 series benefit Ethernet network security?

Network security for switches and network infrastructure is gaining more attention than it once did as more people and businesses rely on their networks as a normal course of their daily lives and businesses. Most people who have direct oversight of their network security are concerned about the safety and security of their network, especially as it relates to data exchanges between offices, cites, states and countries. With the critical nature of networks to keep businesses moving forward and the amount of mission critical data that is pushed and pulled across these networks, the more vulnerable these systems appear to be. The looming doom of a security threat or infrastructure failure can have cascading affects on any business that relies heavily on their network to conduct their daily operations and the threat is not as simple as trying to achieve the task of keeping the bad guys out, this threat is a multi-headed monster or Hydra.

The Hydra's perceived strength came from a multiple head attack and it defense was the re-growth of two heads for every one head that was lost; the Hydra's attack and defense is very similar to today's security threats meaning you find a way to stop one and then two more pop up in its place. One of the heads / threats being man made (Viruses and Hackers) , another head / threat is self inflected issues (receiving an infected email or using an unauthorized device such as a USB Drive) and yet another head / threat comes from several single points of hardware failure that can cause cascading down line failures.

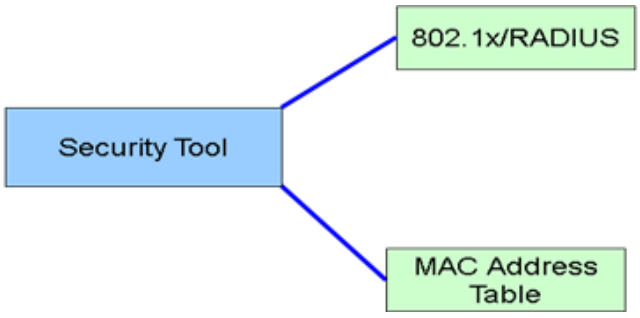
Man-made security threats are the most difficult ones to try and control and the difficulty comes from the fact that most of these threats are unleashed by innocent users of the system; an email, a random CD or a USB memory stick. These users are not master mind computer hackers, most of the time they are unaware of their simple acts of just receiving an email that contains a network crippling virus. This is the challenge that IT directors across the world have to try and be prepared for, part of this preparation is to be pro-active in their attempts to try and limit their networks exposure to these threats and they do this with hardware, software and strict policies but as we all know the best laid plans of mice and men are not always enough. This article will address how hardware and technology developers are making great strides towards providing a solution to protect networks from all the threats that

exist today.

IP security (SSH、SSL)

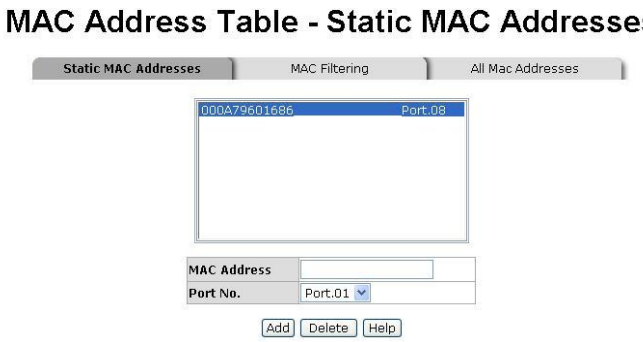
IP security is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

Some other internet security system, such as SSH and SSL are common widespread use in network. User can use SSH to prevent unauthorized access to critical devices. SSH is a network protocol that allows data to be exchanged using a secure encryption between two networked devices. SSH uses public/private key RSA authentication to check the identity of communicating peer machines, and provides data encryption using algorithms. SSL is a protocol that uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message.



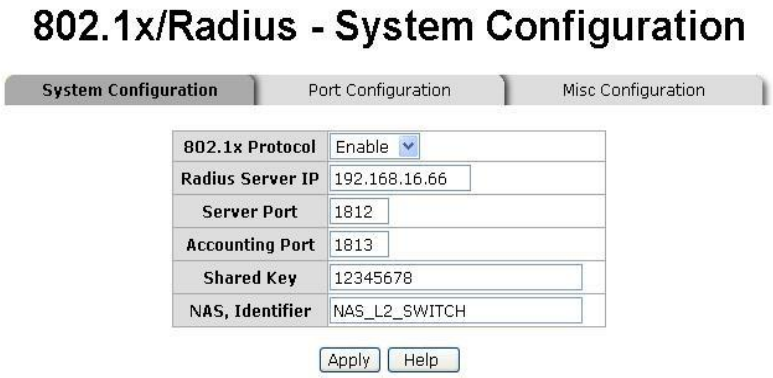
Mac filtering

Mac filtering is another security access control method in computer networking. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and white lists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a white list entry for each device that he or she would use to access the network.



802.1x RADIUS

802.1x makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.



Besides firmware system, hardware security protecting also has some functions to protect networks for users. Some infrastructures in harsh environment need solid equipments to against the external environment destruction, such as railway network.

The Switches apply to railway network should design more firmly. Because all the devices are connected with Ethernet, it is easier to integrate new systems and new applications. The ability of high-bandwidth is another theme for discussion. Ethernet backbones are able to provide a reliable network environment for implement of applications such as passenger entertainment systems and high-quality video surveillance applications. Connected with Ethernet cables, the installation and maintenance is much easier with less cost. In order to create the full fine performance, the railway network security would count on well-design switches to meet with critical network environment.

EN50155 series switches may trusty for Ethernet infrastructures. The consideration point of security to use EN50155 series switch might come from the following sources.

EN50155 series switch

Different to the comfortable environment for passengers, the Ethernet devices in railway applications often operate in a narrow and harsh environment with unique requirements. Devices in rail train must be able to suffer under wide range temperature and humidity. Furthermore, severe air pollution, vibration, shock and EMC are commonly seen. That's why Industrial Switches are needed to be certified by EN50155 standard.

The EN50155 standard is "Railways Applications Electronic Equipment Used on Rolling Stock", which is commonly adopted by many countries and electronics manufacturers. Electronic equipment shall be designed and manufactured to meet the full performance specification requirement for the selected categories such as:

● Ambient temperature

According to diverse severe environments, there are four grades of operating temperature requirements defined by the EN50155 standard and are stated in the following table:

Class	Ambient temperature outside vehicle	Internal cabinet temperature	Internal cubicle over-temperature during 10 min	Air temperature surrounding the printed board assembly
T1	-25°C to 40°C	-25°C to 55°C	70°C	-25°C to 70°C
T2	-40°C to 35°C	-40°C to 55°C	70°C	-40°C to 70°C
T3	-25°C to 45°C	-25°C to 70°C	85°C	-25°C to 85°C
TX	-40°C to 50°C	-40°C to 70°C	85°C	-40°C to 85°C

● Shock and vibration

EN50155 adopts testing methods and limitation according to EN 61373 - Railway applications - Rolling stock equipment - Shock and vibration tests. The standard

ensures the equipment to be able to withstand vibrations and shocks and provides the specified useful life under service conditions. To satisfy the requirements, the equipment should be specifically designed with anti-vibration mounts and installed the electronic units completely.

● Relative humidity

EN50155 defines the relative humidity standard that equipment should follow: The equipment should be able to withstand 75 % of the average yearly relative humidity and 30 consecutive days with 95 % relative humidity in the year. IP67 enclosure is one of the best solutions, which provides rugged and waterproof protection to against moisture environments that may cause any malfunction or failure.

● Atmospheric pollutants

The equipment may be exposed in different locations where various pollutants are available, including oil mist, salt spray, conductive dust, Sulphur dioxide. To ensure the durability, the equipment should have IP-rated enclosure to against the negative effects from these pollutants.

● Electrical service conditions

To overcome the severity and provide the stable services in railway applications, EN50155 also defines several standards for electrical service conditions such as input voltage range, input voltage ripple, and input surges. Each category follows clear requirement. For example, the requirements of input voltage are listed below:

Input Voltage Requirements			
Nominal Input	Permanent input voltage range	Brownout 100ms (0.6xVnom)	Transient 1s (1.4xVnom)
24VDC	16.8-30.0V	14.4V	33.6V
37.5VDC	26.2-47.0V	22.5V	52.5V
48VDC	33.6-60.0V	28.8V	67.2V
72VDC	50.4-90.0V	43.2V	100.8V
96VDC	67.2-120.0V	57.6V	134.4V
110VDC	77.0-137.5V	66.0V	154.0V

Electromagnetic compatibility (EMC) is another main category of EN50155 standard. The equipment should be protected in order not to be negatively affected by conducted or radiated interference, which is referred to EN 50121-3-2 and should not

emit radio frequency interference (RFI) that excess the level defined in EN 50121-3-2.

EN50155 series models provide IP-67 protection and M12 connectors with wide operating temperature from -40°C to 75°C for harsh operating environment in railway applications. The rugged and durable switches have long MTBF that ensure the network quality of video entertainment service and high quality video surveillance at the same time with Giga fiber ports. Besides hardware specifications, the powerful software features also ensure the management convenience. A well-design switches security functions are essential to securing modern Ethernet network.

EN50155 Series	
Model Name	Description
IES-2008-67 	8 10/100TX M12 / IP-67 Managed Industrial Switc
IES-2208F-67 	8 10/100TX + 2 100FX M12 / IP-67 Managed Industrial Switch
IPES-2208GF-M12 	8 10/100TX + 2 1000FX M12 / IP-67/IP54 Managed Industrial Switch w/8 PoE Injectors