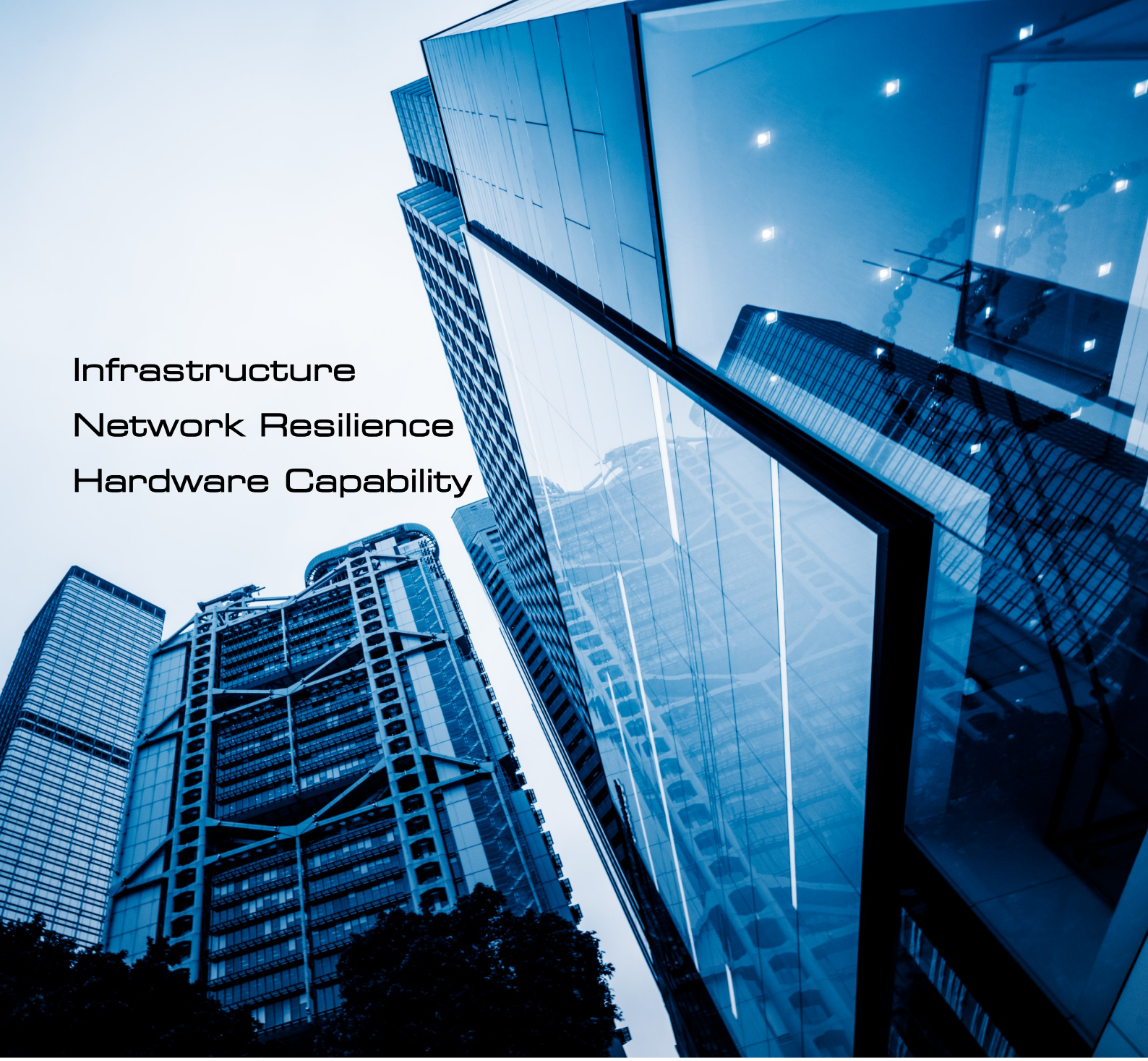


CYBER SECURITY

securing edge devices

comnet
Communication Networks

www.comnet.net

Cyber Security - Challenges & Opportunities

The term cyber security is a very common one in our world today, and can affect anything and anyone from national governments and global corporate entities, to individuals both young and old. Due to its ubiquitous association, our comprehension of cyber security is based around the global internet where software attacks, such as malware and denial of service, threaten our working days and everyday lives - websites become unreachable and corporate servers are hacked, with expensive consequences for both owners and operators alike. But what we fail to relate cyber security to, is the threat to autonomous computer networks. In these cases, a third party physically breaks into a system via its infrastructure devices resulting in the system being compromised or failing completely with disastrous outcomes from either scenario.

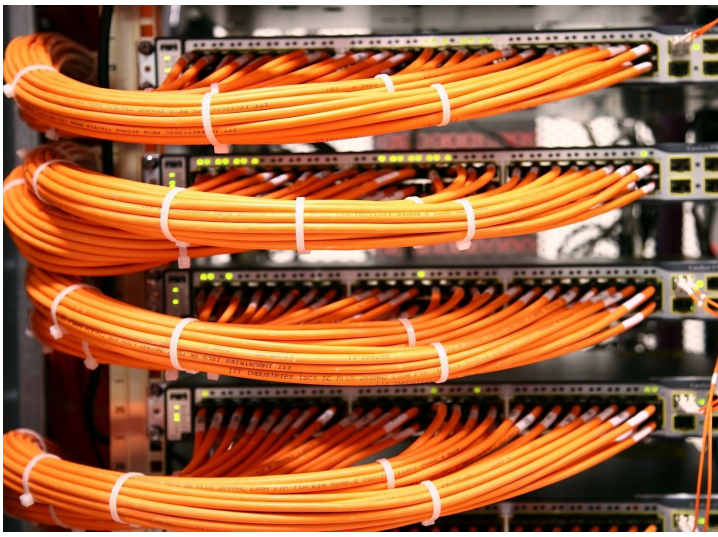
This article focusses on *hardware* cyber security, examining the possible approaches that an attacker can take and describes the features within the active network equipment that can prevent such attacks succeeding. Although we will concentrate on IP security and surveillance networks, this article applies to any Ethernet-based network and, as such, covers a much wider scope of markets.

Due to their nature, security and surveillance networks put network connections in both secure and unsecured locations. Vulnerable positioning, provides ample opportunities for the would-be attacker, so due care and attention must be paid to equipment protection. However, installers must also treat secure sites in exactly the same way. The point of attack could originate from a source fully entitled to be within an area. No chances can be taken.

Infrastructure & Attack

An Ethernet network comprises both **active and passive equipment**. (1) The active equipment includes Ethernet switches (2) and media converters, and the passive, a combination of cables, connectors and management such as cabinets, which might also include additional active equipment for example environmental conditioning and monitoring systems. For the purposes of this article, we will address Layer 2 Ethernet switches.

Ethernet switches act like cable concentrators, bringing together signals from different edge devices and then relaying those signals to other devices, based on address information attached to the signal. They can have combinations of electrical and optical ports (connections) in varying port densities. A media converter is a simple device that coverts electrical signals to optical and vice-versa. The security threat to the network at this level results from a third party physically connecting to the switch, or by removing an edge device from the network and attaching unauthorised equipment in its place. The connection could be to an optical port, but that would require the third party to have the correct optical interface, so, for opportunistic reasons, it tends to be a connection via an electrical interface. Electrical Ethernet ports are based around an industry standard, so connecting to these is relatively simple and as every laptop today has such a connection, the probable weapon of attack is readily available.



Active Equipment Defence

Ethernet switches are available in managed or unmanaged forms, where the managed platform has many more features and allows the user to configure and remotely monitor the device. The unmanaged unit has no such facilities, it simply does the basic job based on its shipped configuration. Media converters tend to be in an unmanaged format only. Where security is concerned, managed units offer a number of facilities to prevent unauthorised entry to the network, whereas unmanaged forms do not, thus managed Ethernet switches should be used throughout your network.

Managed Switch Security Features

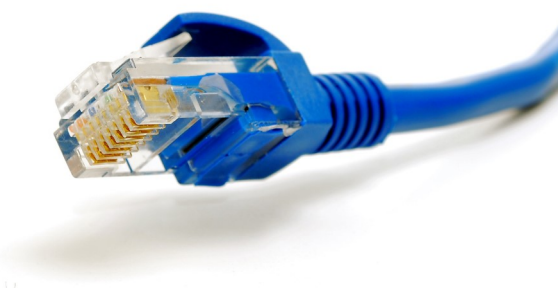
A. It tends to be the case that the simplest features offer the best security, and with Ethernet managed switches, that persists. The ability to disable a switch port that's not being used in the current network configuration, through the management interface, might seem an obvious security feature but it is one that a lot of network operators fail to employ and may not even know exists on their devices. The rules, as you can imagine, are straightforward: if the port is not being used, then disable it, so no unwarranted party can plug directly in to your network. If the port needs to be used for legitimate traffic in the future, then simply open it via the management system. And while we're talking about the simplest features being the best, the default username and password that every managed Ethernet switch is shipped with, to enable you to gain access, should be changed to a username and password, commensurate with your security policy. There is no point in applying all this security, if it could be changed by our attacker connecting to the comms port (3) of the switch and gaining access simply by reading the manual!

B. Once a link has been established between two active units in the network, a LINK acknowledgement (normally an LED indication) is generated and dropped immediately the link is broken. This simple hardware-based trigger can be used to shut a port down on the basis that a loss of link is a potential attack. The feature can be further expanded to shut down ports in the event that power is lost to the active device - just in case our attacker has the smart idea of switching connections once the switch is powered down. If any units are deployed in unsecured locations, then the port receiving communications from that site should be activated with this feature to counter link breaks in these areas.

C. Any IP-based, edge device such as a CCTV camera or speaker will have an Ethernet MAC address. This can be used to logically connect the associated Ethernet switch port to that particular MAC address. If a MAC address that's not registered tries to connect, the switch will simply prevent access. Remember however that the more knowledgeable attacker could use spoofing to find and copy your MAC address, so this form of protection may buy you valuable time but not complete protection.

D. With the IP address of connected devices known, the switch can set up a polling routine with the edge device and then run a pre-programmed procedure if there is no response to the poll. Depending on the switch and the manufacturer, there could be a number of response procedures employed, based on site security protocols. One could be to immediately shut the port down and, at the same time, generate a SNMP (Simple Network Management Protocol) trap. This is like an alert flag that tells the centralised management system that something has happened to the device running SNMP and to start ringing the alarm bells if required. Another response could be to simply send the trap and keep the port open or, if the switch was supplying power to the edge device, a power cycle procedure could be run if the user thinks that the device has stalled or hung-up.

E. 802.1x User Authentication is an IEEE defined standard that should be available on all fully managed switches. It defines an authentication procedure for devices that wish to join the network. The standard defines three parties in the procedure; a Supplicant that wants to join the network, an Authenticator, which is the Ethernet switch, and the Authentication Server. In the system, the Ethernet switch acts to protect the network until the server has verified the credentials of the supplicant and has either allowed or denied it access to the network.



www.comnet.net

Passive Equipment Security

Security should be applied to the passive components of the network as well as the active ones. How many times have you walked along the pavement and observed the door of a utilities company street cabinet hanging off, or even the access flap open on a lamppost? The reason is, that for most cases, the system owner or operator has no idea that the door of their cabinet is open and their system is not secure! If any part of the network is housed within an enclosure, some form of sensor must be on the door to tell you if it is open or closed. If the door is open and you are not aware of it you provide an easy target for any attacker and, at the same time, allow the elements to damage your enclosed equipment. And remember, it doesn't just need to be active equipment. If the enclosure simply houses cable management that could be an opportunity to break in to the network. This requirement is an absolute must in unsecured locations!

Conclusion

The security threat to any Ethernet network could come from known or unknown attackers in both local and remote locations and, as such, owners and operators must protect against all eventualities. In the case of local attacks, the point of entry to the network will be the physical connections within the network. If the attacker is remote, it will be the connectivity. To guard against attacks, managed Ethernet switches should always be used as the active building blocks of the network as they offer the maximum level of security when configured correctly. Managed units will also provide users with the ability to remotely control and monitor network devices, and will generate automatic warning signals if an issue arises. Any managed, Ethernet switch must be configured based on the security levels and operational requirements of the site to ensure correct operation.

Those who ignore the basics of network security and opt instead for cheaper, unmanaged devices, are exposing their networks to the risk of hackers. Hackers who can very quickly turn a sophisticated security network to their own advantage. And with the safety and protection of critical infrastructure, data and communications at stake, are you prepared to take that risk? / it seems an irresponsible risk to take!

(1) Active equipment is defined as that which needs electrical power to operate and passive equipment is that which does not require electrical power.

(2) This article is focused on Layer 2 Ethernet switches based on MAC addresses and not Layer 3 devices that can switch on either IP or MAC address.

(3) The comms port on an Ethernet switch is a serial data communications port that allows local access to the management configuration once a correct username and password are entered.

Having served an engineering apprenticeship with the Ministry of Defence and read for his degree in electronic systems at the Royal Military College of Science, Iain Deuchars worked for a number of years on satellite communications projects for the UK military. Following this he moved to the commercial sector and became involved in optical communications primarily in the security and surveillance markets. Iain has held senior positions in a number of electronic communication companies and is currently Business Development Manager for ComNet, where he is involved in both technical and commercial aspects for the Company

3 CORPORATE DRIVE | DANBURY, CONNECTICUT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427
INFO@COMNET.NET

8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS | UK
LS27 7LE | T: +44 (0)113 307 6400 | INFO-EUROPE@COMNET.NET

www.comnet.net