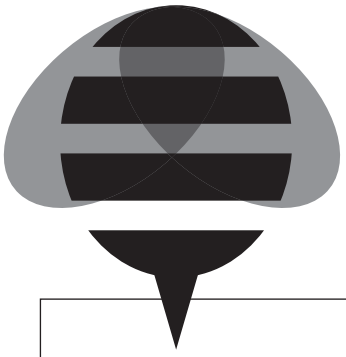


802.1x - the "Sting"

To explain or better yet, to understand why do intelligent IT folks fall for the ’802.1x Sting’, we may need a behavioral scientist rather than an IT professional. The industry with the blind adaptation of the 802.1x protocol resembles a ’herd like’ stampede. Many are following the 802.1x path just because that’s where the ’herd’ goes. We believe that, after looking at the 802.1x performance facts, adopting the 802.1x protocol for LAN security is - like blindly stampeding with the herd, on a misguided attempt to find a security solution.

While voicing an opinion against the ’all mighty’ 802.1x protocol may be viewed by some as a slaughter of a ’holy cow’, the protocol’s performance points the other way. The Holy cow of the IEEE standard or not, fact is that in spite of being supported by industry giants and marketed by sophisticated ’sales teams’, the 802.1x is a sting. It is heavy, cumbersome, limited in functionality, complicated to assimilate and maintain, expensive beyond reach for most, ineffective as a LAN security solution.

So, why do intelligent and knowledgeable IT professionals fall for the ’802.1x Sting’ to begin with? Even if it is only until they find out that they’ve been stung. Isn’t it advisable to figure the 802.1x first, rather than march with the herd to the drum beat of industry vendors’ sales folks?

more...

The anatomy of the 802.1x "Sting"

The portnox solution vs. the 802.1x "Sting"

The anatomy of the 802.1x "Sting"

First and foremost and like any other respectable 'sting' operation which never is what it represents itself to be, so does the 802.1x 'sting'- it is neither an effective LAN security nor, the LAN security some wish it to be. The first professional step to be taken is to look at what does it do, and what it doesn't do. The second step ought to be to assess the real cost of the 802.1x doing what it claims to do. And thirdly, yet no less important is to assess what the speculative cost will be if it does not do what it claims.

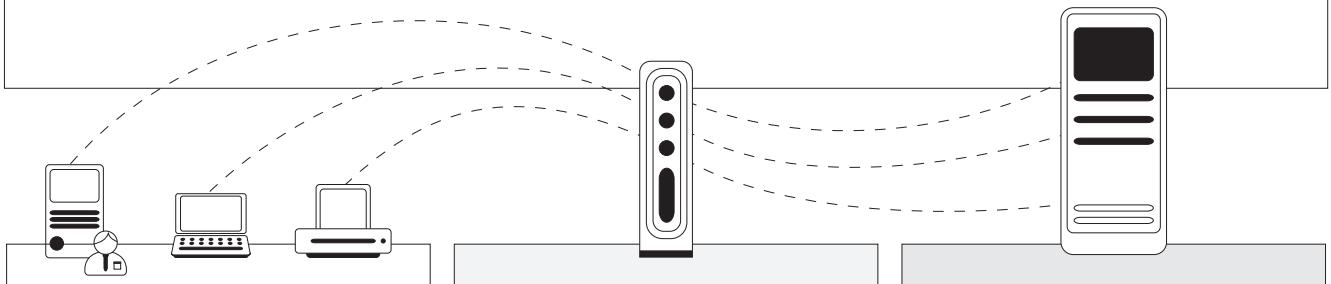
Although the 802.1x forces all devices to be authenticated before they can access the network, the mandatory configuration of the end points is as any IT professional knows; a tedious, error prone, time consuming and if at all, extremely expensive and taxing process for any organization.

Within any Network Access Control (NAC) the use of 802.1x protocol is very limited in its scope because it addresses a device authentication agent. For the 802.1x, if "Samantha" is a valid and authenticated printer with a 802.1x supplicant, "Samantha"' can access your corporate network and do as she pleases, when she pleases, with whatever organizational resources she deems useful to her. In addition, if "Samantha" isn't turn off, she remain legitimately 'Authenticated'.

True, the 802.1x can verify a request of access as being done by a valid device, but then following the Authentication the 802.1x provides a 'card blanch' to the device with no control as to what that device and the user can do on your network. Meaning - the 802.1x provides no 'post-admission' or any authorization controls.

In fewer words - the 802.1x provides neither accounting nor accountability!

For the successful implementation of the 802.1x protocol on your network there are three elements which have to be aligned perfectly and be compatible, function harmoniously and in concert. To do that, they ought to be of the same manufacturer or support the 802.1x in the same way. Otherwise there is no guarantee whatsoever for the 802.1x functionality.



The Supplicant:

In fact this is nothing but sort of an agent device already existing in the Windows XP and newer versions as a default option, however it requires an installation on all IP devices on the network such as Printers like our "Samantha", servers, IP telephones etc. e.g. anything which isn't a Windows...

The Authenticator:

This device, which in reality is a communication switch (wireless or wired), that supports this protocol. Older switches are not necessarily supporting this protocol. How about different switch vendors under the same setup? You got that right - don't hold your breath here.

Authenticator Server:

This is the Radius Server which receives the Authenticator's request.

This server is aligned with other organizational data servers, directory servers and CA.

!

Although all the switch vendors say their devices support the 802.1x protocol, the fact is that they may support it but not in the same fashion. Consequently, the compatibility and cooperation among the devices may not be possible. Nor is the homogeneous implementation of the 802.1x on your network.

As the Communication switch is defined for the implementation of the 802.1x, each and every time an IP device engages the network, that accessing device will be isolated / disconnected from the network and will remain isolated up to and until the point of a successful authentication process.

The switch then approaches the ‘Supplicant’ requesting identification details for the IP device requesting the access. In case and there is no ‘Supplicant’ or if there is no compatibility among the system’s devices due to vendor differences, the station will be denied access to the network. In the best case scenario, when and if the station provides identification, this information in turn is passed along to the Radius Server which is the one that actually replays to the switch whether the IP device was approved for access or denied one.

Add to this infrastructural process with the PKI (public key infrastructure) implementation and you get a ’super complicate’ picture of all the various devices. At the day’s end all these non synchronized roles of the Supplicant, the Authenticator, the Radius and the CA service etc. provide your network with a partial solution at best.

No joke, this is how the 802.1x sting works... when and if it does work!

portnox™

The portnox solution vs. the 802.1x "Sting"

If the 802.1x protocol is cumbersome, limited in functionality, complicated to assimilate and maintain, Then the portnox LAN security solution is a swift, functional, efficient and reliable tool.

Look at the facts and you do the math –

Function	The 802.1x sting	portnox solution	notes
Policy	A totally sweeping ON/OFF action, unable to deal with or, confront exceptions.	Flexible at preface or a single port or device in various configurations.	Pre-Connect. Post-Connect. Partial Pre-Connect. Alert only.
Policy	Limited to authentication only. Incapable to isolate a station on the basis of compliance alone.	Flexible on all access levels by the results of the alignment verification and ratification jointly and individually.	A station not conforming to organizational Policy has to be isolated prior to accessing the Network, so to avoid possible contamination.
Redundancy	Mandatory. Expensive and cumbersome. A single point of Failure.	Not needed.	It is possible to implement an unlimited number of servers as well as virtual infrastructures. A miss functioning portnox server does not lock-out users but disable network access control (e.g. fail open).
Designated Infrastructure	Requires establishment of Radius Servers and in most cases CA (PKI) infrastructures as well.	Servers set up is not needed with the exception of a single server capable of handling up to 15,000 access points.	
Switches infrastructure	Requires similar switches, generally of the same manufacturer and supporting the protocol in an identical fashion. Usually required alignments and upgrades.	Accepting combination of managed switches from various manufacturers and of different versions with no common denominator.	portnox employs standard SNMP for the management and the enforcement at the switch level without being enslaved to one manufacturer or another.

portnox™

The portnox solution vs. the 802.1x "Sting"

Function	The 802.1x sting	portnox solution	notes
CA infrastructure	Most implementations of 802.1x use the existing PKI organizational infrastructure.	Not required. Can be used in parallel to the existing.	
Authentication method	Radius password or certificate (See CA infrastructure above).	16 different methods for the authentication of devices including the creation of a designated profile for differing hardware (fingerprinting).	Flexible, Efficient and Effective.
Digital Certificates	Usage of Digital Certificates is on the computer/device level and is NOT related to the user who in practice logon to that system.	There is no use of certificates at the computer level.	The correlation between the computer system and the user is valuable for the purpose of NAC.
Digital Certificates	These as with an agent device assimilated at the end station.	Not needed. 100% 'agent less'.	Operational reproductions at the deployment stage and the ongoing maintenance. This is an additional device to be managed on each computer.
Implementation	Very few and the ones implemented are very limited and have only partial functionality.	Complete implementation of 100% of the network members.	It is possible to implement the 1x in a homogeneous laboratory environment. However, this will not properly reflect the implementation of a communication network on all its components.
Deployment	Up to 60% of the organization's devices are 802. 1x capable (according to analysts). In case there is a VOIP system implemented in the organization, the number is drastically lower. In general, the devices which are not 802.1x capable will have to be verified by the MAC address management or, by the purchase of designated Supplicant devices.	16 different methods for the verification of devices including the creation of a designated profile for differing hardware (fingerprinting). Practically, all devices are verified without NAC address management whatsoever.	This fact sheds light on the blown price an organization has to pay for the implementation of the 802.1x as well as on the fact that at the best case scenario, the solution is effective with up to 50% of the network devices.
Deployment	Those devices which do not participate in the 802.1x will be defined by MAC or, worst of all they will be connected to not secured switches.	All access points at the organization are routed and secured properly.	100% coverage of the network's devices is mandatory with a NAC solution. A counterfeit of a MAC address is immediate and simple.

portnox™

The portnox solution vs. the 802.1x "Sting"

Function	The 802.1x sting	portnox solution	notes
Deployment	Implementation in a Converged environment complicates the 'solution' even more.	There is a designated module for the implementation of alignments with phones.	The most recently assimilated telephony system most are with converged implementation.
Reliability & Credibility	From the moment when the access point was verified there will be no additional inspection of that point until the next connection.	The access points, and the devices attached to it, are continuously inspected, never on the basis of a single verification and access.	Aided by a verified device, one can connect a HUB following the opening of the access point – without an additional verification in a 802.1x authentication model.
Compliance	Does not exist.	Unlimited infrastructure for examination of Antivirus, operating system updates, etc.	A station which does not conform to the organizational policy has to be isolated prior to access to the network thus, eliminate the possibility of contamination.
Management	Designated tools do not exist. The management layout of the switches lacks sufficient data needs additional development!	Designated management tools for the segmentation of users (RBAC) based on available WEB.	Critical for a successful NAC project.
Management	Once the end station/device failed in its verification has to be 'visited' in person by the IT team to assess and diagnose the problem.	The management infrastructure window is easily accessible to the IT team and affords the to release the device from its 'lock-out' stage.	
exceptions handling	An exceptional device cannot be attached in an immediate and controlled manner.	The captive portal module enables the interactive verification of the user station.	
exceptions handling	A designated isolated network cannot be implemented. The solution here is the ON/OFF type.	A guest device/computer can be classified and routed to designated networks that do not access the manufacturing level.	

portnox™

The portnox solution vs. the 802.1x "Sting"

To sum it all, here's a quick overview of the 802.1x saga at one company:

"The solution by a networking giant offered to our company is based on the 802.1x Protocol. This protocol, we discovered, requires an agent device on each and every access point (port). There is no way of enforcing a NAC policy without the agent.

For the assimilation of the 802.1x, there was need for 4 (four) different server appliances in a cluster configuration.

The assimilation process itself wasn't easy. For over a month the IT team at the organization encountered insurmountable difficulties in activating the 802.1x protocol. That in spite of the top notch IT professional we have and the most recent and cutting edge communications equipment we purchased.

At the end of the day the greatest difficulty with this project was the implementation of the 802.1x. Fact is that over half of the time dedicated to the project had been spent on it. As of today, the 802.1x is implemented on no more than 250 installations of clients' window stations only."

Here's some food for thoughts....

Four servers + Top professionals in their field well paid management and IT staffers + up to date and expensive communications equipment + costly thousands of men hours

All that cost to implement a limited and a partial solution on a total of only 250 (two hundred and fifty) devices while the portnox server supports up to 15,000 (fifteen Thousand) access points?

It's a sting!

Don't get stung with 802.1x, go portnox.
We don't promise what we can't deliver!
For additional information go to our site...
call our partner close to you.....

www.accesslayers.com

portnox™