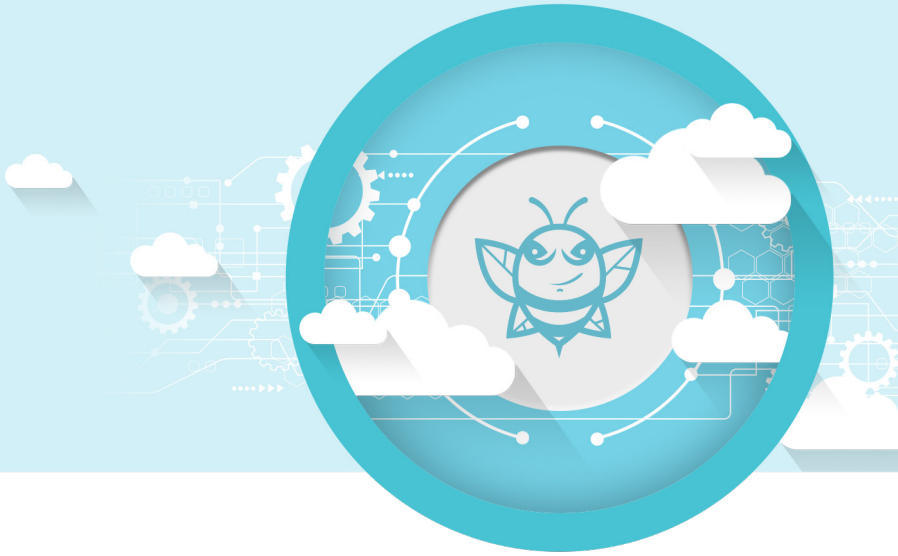
portnox™

WHITE PAPER

802.1x - The "Sting"



To explain, or better yet to understand, why intelligent IT folks fall for the '802.1x Sting' may require a behavioral scientist rather than an IT professional. That's because it seems that IT professionals are blindly adopting the 802.1x protocol in a 'herd-like' fashion. However, behavioral science aside, even after analyzing substantive 802.1x performance facts, adopting the protocol for LAN security has largely proven a misguided attempt in arriving at a sound security solution.

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

802.1x is heavy, cumbersome, limited in functionality, complicated to assimilate and maintain, expensive beyond reach for most, and, above all, ineffective as a LAN security solution

So, why do IT professionals fall for the '802.1x Sting' to begin with?

The Anatomy of the 802.1x "Sting"

First and foremost, and like any other respectable 'sting' operation, 802.1x is not presented per its actual capabilities - it is not an effective LAN security solution. That said, the first thing an IT professional would do is to look objectively at what 802.1x does do, and what it cannot accomplish. The second step ought to be to assess the true cost of 802.1x based on its capabilities. The third and final step is to assess what the speculative cost would be if 802.1x does not perform as it should.

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

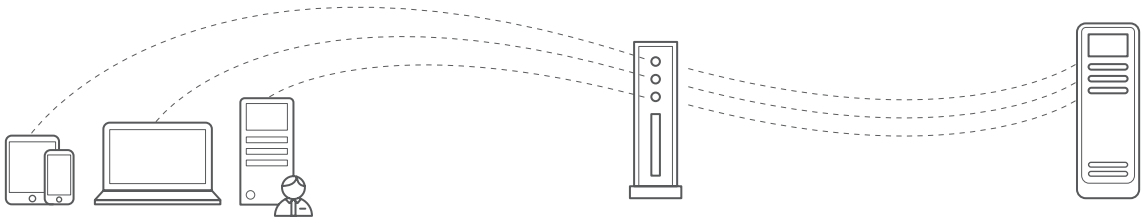
Within the sphere of Network Access Control (NAC), the application of the 802.1x protocol is limited in scope as it's sole purpose is to act as a device authentication agent. For example, with 802.1x, a valid and authenticated

The mandatory configuration of the endpoints is, as any IT professional knows, a tedious, error prone, time consuming, extremely expensive and taxing process for any organization

printer with a 802.1x supplicant can access your corporate network and do as it pleases, when it pleases, with whatever organizational resources it deems useful. In addition, if the printer isn't turned off, it remains legitimately 'authenticated' on the network even during downtime.
True, 802.1x can verify a request for access from a valid device, but then, according to the 802.1x Authentication procedure, the device receives a 'carte blanche' to access and do what it pleases on your network. This means that 802.1x provides no 'post-admission' or further authorization controls after granting network access.

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

For the 802.1x protocol to be successfully implemented on your network, there are three elements that must be aligned perfectly and function harmoniously. To accomplish this, these elements ought to be from the same manufacturer or support 802.1x in the same way. Otherwise there is no guarantee that 802.1x will function properly.



The Supplicant:

This is nothing but sort of an agent device that already exists on Windows XP (there is even a default option in newer versions), however it requires installation on all network IP devices such as printers, servers, telephones etc.

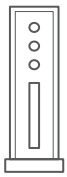
The Authenticator:

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 many switch vendors claim that their devices support the 802.1x protocol, the fact is that they may support it, but not in the same fashion. Consequently, compatibility and cooperation among network devices may not be possible, inhibiting the homogeneous implementation of 802.1x on your network.



Communication switches are essential in the implementation of 802.1x, communicating with the protocol every time an IP device engages with the network. A device requesting access will be isolated / disconnected from the network and will remain in that state until the authentication process is successful.

The switch then approaches the 'Supplicant' requesting identification details for the IP device requesting the access. In the case where there is no 'Supplicant' or if there is no compatibility among the systems' 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 is passed along to the Radius Server that replies to the switch whether an IP device is approved or denied access.

Add to this infrastructural process with the PKI (public key infrastructure) implementation and you get a complex picture of all the various network devices. In summary, the non-synchronized roles of the Supplicant, the Authenticator, the Radius and the CA service provide your network with a partial network access solution at best.

This is how the 802.1x sting works... when and if it does work!

The Portnox Solution vs. the 802.1x "Sting"

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

Look at the facts and 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.*
	Limited to authentication only. Incapable of isolating station on the basis of compliance alone.	Flexible on all access layers - 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 required but available at minimal cost.	*It is possible to implement an unlimited number of servers as well as virtual infrastructures.* *A poor functioning Portnox server does not lock-out users, but disables network access control (e.g. fail open).*
Designated Infrastructure	Requires establishment of Radius Servers and in most cases CA (PKI) infrastructures as well.	Requires establishment of Radius Servers and in most cases CA (PKI) infrastructures as well. Serversetup not required with the exception of a single server capable of handling up to 20,000 devices with easy expansion via VM structure.	
Switch Infrastructure	Requires similar switches, generally of the same manufacturer and supporting the protocol in an identical fashion. Usually requires alignments and upgrades.	Accepts combination of managed switches from various manufacturers and of different versions with no common denominator.	*Portnox employs standard SNMP for management and enforcement at the switch level without being tied to one manufacturer or another.*
CA Infrastructure	Most implementations of 802.1x use the existing PKI organizational infrastructure.	Not required. Can be used in parallel to the existing infrastructure.	

Function	The 802.1x Sting	Portnox Solution	Notes
Authentication method	Radius password or certificate (See CA infrastructure above).	Over 20 different methods for the authentication of devices including the creation of a designated profile for differing hardware (fingerprinting).	*Portnox's solution is flexible, efficient and effective.*
Digital Certificates	Use of Digital Certificates is on the computer/device level and is NOT related to the user who is logging on 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.*
	With an agent device assimilated at the end station.	Not required. 100% 'agentless'.	*Operational reproductions at the deployment stage and ongoing maintenance makes the agent an additional device to be managed on each computer.*
Implementation	Limited, and those implemented only have partial functionality.	Complete implementation of all network members.	*It is possible to implement 802.1x 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 organizational devices are 802. 1x ready (according to analysts). In case there is a VOIP system or other IoT devices implemented in the organization, the number is drastically lower. In general, the devices that are not 802.1x ready will have to be verified by MAC address management or, by the purchase of designated Supplicant devices.	Over 20 different methods for the verification of devices including the creation of a designated profile (fingerprint) for authentication and control of any IoT device Practically, all devices are verified without MAC address management.	*This fact sheds light on the blown price an organization has to pay for the implementation of 802.1x as well as on the fact that in the best cases, the solution is only effective with up to 50% of the network devices.*
	Devices that do not support 802.1x will be defined by MAC or, worst of all they will be connected to unsecure switches.	All access points in 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.*
	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 telephone systems are with converged implementation.*

Function	The 802.1x Sting	Portnox Solution	Notes
Reliability & Credibility	From the moment the access point is verified, there is no additional inspection of that endpoint until its next connection.	The access points, and the devices attached to it, are continuously inspected, never on the basis of a single verification and access event.	*Aided by a verified device, one can connect a HUB following the opening of the access point - without an additional verification in the 802.1x authentication model.*
Compliance	Does not exist.	Unlimited infrastructure for examination of antivirus, operating system updates, etc.	*A station that does not conform to organizational policy is isolated prior to access to the network thus, eliminating 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.*
	Once the end station/device fails verification, it must 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 allows the team to release the device from its 'lock- out' state.	
Handling Exceptions	An exceptional device cannot be attached in an immediate or controlled manner.	The captive portal module enables the interactive verification of the user station.	
	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.	

TO SUM UP

this white paper, 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's in spite of the top notch IT professionals we have on staff and the cutting edge communications equipment we purchased.

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

Here's some food for thought....

Four servers + Top professionals in their field, well paid management and IT staffers + Up to date and expensive communications equipment + Thousands of man-hours

It's a sting!

Contact Us

Americas: usinfo@portnox.com | 1.855.476.7866
Europe: dotell@portnox.com | (44) 1273.256325

www.portnox.com

portnox™