



# *Comply to Connect*

**OPTIONS ARE AVAILABLE FOR AGENCIES IN MEETING GOVERNMENT NETWORK ACCESS CONTROL REQUIREMENTS.**

**By PETE LINDSTROM**

For good reasons, many U.S. government agencies are in the process of implementing network access control (NAC), a security requirement to permit only authorized personnel and systems to access sensitive government resources and information.

Federal agencies have looked to different authorities for guidance regarding the best NAC architectures. Civilian agencies take guidance from the National Institute of Standards and Technology, while defense organizations look to recommendations provided in the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) for Access Control in Support of Information Systems.

The DISA STIG lists the 802.1x architecture as the preferred option for authentication and port control. The 802.1x process is fairly straightforward. When a device first attaches to a network, the client supplicant software on that device transmits an authentication request to the authenticator, which is usually a network switch.

The switch recognizes the request and is preconfigured to forward it to the appropriate authentication server. The authentication server makes its determination and transmits an “allow” or “deny” message back to the switch. Finally, the switch makes the port assignment and notifies the supplicant software on the client. At that point, the 802.1x process is complete.

802.1x, which is a IEEE standard, has three major benefits: It is a standard adopted by IT vendors for basic interoperability in authentication capabilities; it is built into modern IT infrastructure, allowing for potential cost savings; and it works.

## ***ERECTOR SET?***

Unfortunately, using 802.1x to solve your NAC problems is like trying to build the Eiffel Tower with an erector set. There is nothing

wrong with the erector set, but it wasn't designed with the Eiffel Tower in mind. The simplistic nature of .1x makes it functional for its single purpose—to provide an authentication framework for network devices. But the standard falls short of the expectations associated with a full NAC solution. Though it is probably unfair to assert there are “shortcomings” to the standard, enterprises must significantly lower their expectations for a NAC solution if 802.1x is all they want.

The tricky part of 802.1x is that any failure means the whole procedure fails. So any minor problem immediately creates a major challenge with a system that has little resilience and no graceful means for failover. For example, an increasingly common problem concerns laptops with supplicants from another 802.1x environment—for example, a contractor's home environment. These supplicants are not recognized by alternative environments, and therefore the authentication process fails.

While authentication at the network layer is somewhat new, there is no need to elevate the notion to something bigger than it really is. The dynamics of NAC that make it worthy of notice involve the real-time, contextual posture assessment, network assignment and remediation capabilities of a fully implemented solution. Authentication is a welcome control to the NAC, but it is insufficient on its own when considering the key benefits of a NAC solution.

As designed, 802.1x makes no attempt to assess the security posture of an endpoint or identify device types or attributes. It assumes every device is “clean enough” and will have supplicant software to initiate the authentication request; there is no attempt at introspection. In addition, since the process is a point-of-entry process, there is no way to identify changes that occur after an endpoint is allowed on the network. For example, 802.1x makes no attempt to determine

whether printers have become users, patches have been rolled back, or malware is propagating.

As a standard, 802.1x doesn't get into prescriptive details or elegant approaches to real-world exceptions. The return result from an authentication request is simple: allow or deny. There are no considerations for context of the device, tolerances for configuration errors, further actions on failure, or any other outcome.

There is a presumption that all devices in an 802.1x NAC environment will be managed and support the applicable supplicant software. This requirement has the same limitations as any solution that requires an agent on the endpoint—devices that are unmanaged due to ownership constraints or simply don't have supplicant support cannot authenticate.

Fortunately, the DISA STIG lists other options which are better able to accommodate environments with older switches (that do not support 802.1x), devices that do not have .1x supplicants, and environments where you need more complete verification of endpoint security posture prior to network admission. Commercial NAC solutions on the market do offer greater environment flexibility and substantial pre- and post-admission security posture assessment for more extensive controls.

## ***BROADER SET OF FUNCTIONS***

Over a three-year period, one large U.S. defense agency has tested and studied more than 30 different NAC solutions. Their experience



**Automated Security Control**

**Network Access Control**

- Port-based access control using: 802.1x, SNMP-based VLAN steering, SSH-based ACL Enforcement
- Worldwide DOD deployment; FIPS 140-2, DISA UC APL

**Real-time Endpoint Compliance**

- Native posture checks: AV, P2P, IM, external storage devices
- Enterprise scalable and integrated: HBSS, IAVA

**Mobile Security**

- See and control wireless access
- Personnel / guest smartphones and tablets

**Threat Management**

- Block advanced persistent threats
- No signatures, no false positives

See how we have helped federal and defense agencies accelerate situational awareness and meet network access control requirements.

[forescout.com/gov](http://forescout.com/gov)



has proven illuminating. The agency initially tried rolling out an 802.1x system, but they quickly learned that deploying .1x is neither simple nor trouble-free. The lead consultant on the job cited the unforgiving nature of .1x as a major stumbling point.

On three separate occasions, a large number of users were blocked from the network due to a simple configuration mistake within the .1x system. The consultant points out the challenge of configuring appropriate GPO policies on the supplicant and the need to manage software on all clients to ensure it is up to date. The lack of thresholds and the inability to deal gracefully with non-compliant systems has caused this organization to slow down its .1x deployment and look to other NAC architectures that are easier and more capable.

When the agency realized the brittle nature of 802.1x, they turned to a product called ForeScout CounterACT as an alternative. It has proved easier to roll out than .1x, plus it includes the aforementioned broader set of functions and features than their previous .1x solution. The agency has also realized strong network discovery and reporting capabilities, which allow it to identify assets as they enter the network and classify them according to type.

The solution has been deployed to multiple environments and is answering the age-old question of “what is on the networks” from both hardware and software perspectives. The unique capabilities of the solution then provide the agency with reports on network devices such as anti-virus software, USB devices, retina scans, applicable users and other critical artifacts. When comparing this commercial NAC solution to 802.1x, the results have yielded cost savings, enhanced security features, enterprise management and auto-remediation.

802.1x is really just about authentication, and as such, it provides a subset of the NAC functionality described above. A NAC system that is based on 802.1x may be a good choice for an organization that has already invested in devices (switches and endpoints) that support 802.1x in a static, homogeneous network environment. At some point, it is likely that the environment will become too dynamic—that is, where the number of exceptions exceed those that define the rule—and may need to upgrade to a more full-featured NAC system.

802.1x can appear attractive because it is “free,” but the economics have proven illusory. In practice, 802.1x has been costly and cumbersome to roll out, particularly for large organizations. The erector-set characteristic of 802.1x is not for the faint of heart or for anyone who wants to implement NAC quickly.

When choosing between 802.1x and alternative NAC approaches, enterprises should assess their needs regarding the types of devices supported, dynamic nature of the environment, level of flexibility and security controls required, and degree of situational awareness wanted. Many enterprises will realize that a fuller, context-driven, NAC environment provides more capabilities and room to grow than one solely based on 802.1x. ★

*Excerpted from “Network Access Control and 802.1x; Advantages, Constraints and Capabilities” by Pete Lindstrom, an industry analyst and director of research at Spire Security. He holds a CISSP and is the chief operating officer of the International Systems Security Association.*

Contact Editor Harrison Donnelly at [harrisond@kmmidiagroup.com](mailto:harrisond@kmmidiagroup.com).  
For more information related to this subject, search our archives at [www.MIT-kmi.com](http://www.MIT-kmi.com).