Best Practices in Authentication and Access Control

Comparing 802.1x to the Nevis LAN Security Approach

By Nevis Networks

Persistent LAN Security Solutions

This whitepaper describes 802.1x and its role in pre-connect LAN Security. Following a brief overview of the technology, we give some pros and cons of an 802.1x deployment. We then describe a phased plan for LAN security that incorporates 802.1x as well as other user authentication alternatives and that can be used in the meantime, should 802.1x not be near-term feasible.

1 Introduction

User authentication is necessary for identity based access control, and 802.1x clearly promises to meet this need.

802.1x has been around for a number of years and has been proposed as the user authentication solution for both wired and wireless LANs. Formally known as the IEEE Standard for Local and metropolitan area networks – Port Based Access Control, IEEE Standard 802.1x-2004 was initially published in 2001 and later revised in 2004. Since then it has become available in virtually all shipping managed switches. Most switch products even offer the ability to configure the port VLAN based on the user identity, and some even support configuring port-based ACLs.

Given its widespread availability, 802.1x would seem the obvious choice for implementing user based authentication in enterprise networks.

So why isn't everyone using it?

1.1 802.1x in Plain English

First of all, we need some technical background. At its core, 802.1x is really quite simple, but this simplicity is not so obvious to someone who just picks up the IEEE standard. In common with many other standards, IEEE Standard 802.1x-2004 has its share of jargon and not particularly a "user friendly" read. So the following paragraphs describe all you need to know about 802.1x, in plain English.

802.1x specifies three things: a model for authorization, a communications channel for authentication, and an enforcement point.

802.1x participants can play one of two roles, that of an "authenticator" that guards entry to the network, or that of a client, the "supplicant," that is trying to gain access to the network. Think of the authenticator as an all-or-nothing on-off switch. Until the port is "authorized" it is "closed" and only accepts local authentication handshakes with a supplicant. Once the port is authorized it is "opened" so that all traffic can flow.[1]

[1] Well, mostly, but the exceptions are not relevant yet.

It is important to recognize that 802.1x defines how to carry authentication information back and forth but does not specify the actual authentication mechanisms. In other words, it is not a complete authentication scheme in and of itself, but relies on other standards to specify how users actually get authenticated. Leveraging work done for other protocols such as PPP, 802.1x uses the Extensible Authentication Protocol (EAP), the model for which can be found in IETF RFC3579. So, 802.1x actually defines just the "EAP over LAN" (EAPOL) frames that carry EAP messages between the supplicant and authenticator. It also recommends, but does not mandate, use of a back-end AAA protocol, such as RADIUS, for communicating with an authentication service. This back-end authentication server may or may not be on the same platform as the authenticator, but usually isn't. Conveniently, RADIUS can carry EAP frames as attribute values, and so for practical purposes 802.1x specifies how to take EAP request frames from the client, send them along to the authentication server, and get back response frames to pass along to the client.

In virtually all cases, though, the actual authentication exchange happens between the client and the AAA server. When all goes as planned, the server tells the authenticator when the exchange is done. It tells the authenticator whether the user is acceptable or not, and depending on the outcome, some attributes for the session, such as the VLAN or port ACLs.

1.2 Some Good Points

802.1x has a lot going for it. It is widely available, and permits things like re-authentication almost at any time, including changing the VLAN and other attributes.[2]

Also, it was intended for entity authentication but can and has been readily extended to support other features, in particular, communicating pre-connect NAC posture attributes. All major NAC architectures, including Cisco's CNAC, Trusted Computing Group's TNC, and Microsoft's NAP, support 802.1x both for carrying attributes between client and server and for enforcement based on the compliance result. For TNC, it is the only method defined as of this writing.

1.3 And Some Caveats

Many enterprises report that they are interested in deploying an 802.1x-like solution but have found current products less than adequate. This section summarizes some of those issues.

As we have said, 802.1x was apparently written by professional standards attendees and this makes configuration more complicated than it needs to be. Unfortunately, most vendors have taken the approach of conforming quite literally to the standard without regard for usability. This makes it

[2] This requires the supplicant to get the endpoint to reacquire its IP address, but modern supplicants now do this

awkward to configure and not at all user friendly or even sensible and, hence, error prone and time consuming. As an example, the standard specifies that you enable the feature system-wide, that is, on all ports. However suppose there is a port where it is not desired, such as a printer. For this 802.1x must be disabled on a per interface basis using arcane commands like “force authorized” that return the port to its pre-802.1x condition. However, to make things symmetric, there also is a “force un-authorized.” What is the purpose? Who wants the port to be operationally and administratively enabled but not pass traffic?[3]

The 802.1x authorization model is rather limited and does not accommodate many use cases without proprietary extensions. In particular, vendor-specific extensions are often used to handle IP phones with integral switches so that PCs can be connected through them to share an access port, or for devices that are not 802.1x enabled. There are no standard ways to accommodate IP phones, nor are there standard attributes for port-based ACLs, making it difficult to mix switches from more than one vendor for other than basic 802.1x.

The model only allows a single endpoint to authenticate. After that any additional endpoints get a free ride. Because the protocol is designed to be general and allow either the client or authenticator to send first, the destination address may not be known, and so a broadcast destination address was specified. In fact the whole EAPOL exchange can be, and often is, carried out using broadcast management frames (MPDUs). Although the standard does allow unicast, most supplicants always send to the broadcast destination. Since switches are not allowed to pass such frames along but must consume them, multiple supplicants cannot be connected through an IEEE 802.1d compliant switch to an upstream 802.1x interface.

The biggest obstacle, though, comes with installing, configuring, and using supplicants. Microsoft includes one with Windows 2000 and later operating systems, but it needs some configuration – it has to be enabled per interface, the EAP type has to be specified, and other confusing options like “authenticate as computer when user is not logged in” need to be properly set. There are subtle but significant differences between the Windows 2000, XP, and Vista supplicants. On Vista, the 802.1x service is not started by default but is on earlier platforms. Furthermore, Microsoft endpoints need to access the network during boot or to be remotely managed, and this requires configuring the ability for the computer itself to authenticate using the supplicant and authorize the port when there is no user present. Third-party supplicants may support more features, but still need to be installed and managed. Note that third-party supplicants tend to work better with their respective vendor’s RADIUS server.

---

[3] There are other settings, such as “controlled direction” that may not be what they seem at first.

To make matters worse, there is no standard for EAP, although vendors have agreed among themselves to support certain EAP types. Again, not all supplicants support all vendor EAP types.

So, although 802.1x has much to recommend it, it comes with some issues that will hopefully be resolved by the IEEE or IETF in future iterations of their standards, as well as more mature product implementations.

2 The Alternative is LAN Security

What should one do if they want the benefits promised by 802.1x but are not ready to cope with the limitations? What if upgrading switches is not an option, nor is only using switches and AAA servers from a single vendor? What if they want to mix employees and guests, multiple operating systems, as well as devices such as PDAs and cell phones that don't have supplicants?

There are LAN security alternatives to 802.1x that can accomplish most if not all of the same goals while, at the same time, are easier to deploy in a typical switched network. In some cases, these may even be preferable in the longer term since they provide more security features than just "on-off" 802.1x. These features can be integrated into the access switches, such as the Nevis Secure Switch, or integrated into special security "bridges" that sit in uplinks between the existing wiring closet access switch infrastructure and the rest of the LAN, such as the Nevis Security Appliance.

2.1 Authentication

There are other authentication options available today that provide a comparable user experience to that of 802.1x, but without the need for clients to be configured, and that can work with all sorts of users and devices.

Many vendors support MAC authentication for devices such as printers that don't do 802.1x. MAC authentication tends to be inconvenient to configure, but effective. It is only useful for limited cases, and unfortunately is easy to spoof using readily available user interfaces.

A better option is some form of transparent or "single sign on" approach. This can be done by snooping user login traffic such as the Kerberos exchange used by Windows 2000 and later. This can provide the same, and in some cases better user experience as 802.1x.

Many vendors provide a Captive Portal feature that allows users to authenticate using a standard Web browser. This can be used by everyone, even guests with PDAs, but the need for users to login twice affects the user experience. Furthermore, it may be impossible to use VLAN steering for post-connect access control– the device would need a way to coax the client to reacquire an IP address in the new VLAN, which few if any devices support.

2.2 Access Control

As mentioned, the access control options afforded by 802.1x are quite limited without resorting to proprietary extensions. In particular, on-off granularity is only useful for enforcing policies at a gross level, such as confining guests to a single VLAN or subnet. It is not able to support finer grained policies, such as allowing partners or contractors temporary access to specific LAN resources.

In fact, these kinds of policies may not even be achievable using vendor specific port ACL extensions. Most switches support a limited number of rules, and some only support a few pre-configured ACL groups. Some only allow use of port ACLs instead of other types of ACLs. If not using the vendor's RADIUS server, port ACLs may be very difficult to impossible to use.

A better option would be to use a LAN security solution that incorporates fine grained access control with a large number of rules, and with a management approach that allows easy configuration of multiple such rules for different user groups.

2.3 Endpoint Posture Compliance

802.1x can carry the endpoint posture attributes needed to establish compliance in addition to, or even without the user authentication attributes, encrypted within the EAP frames. This would normally be done pre-connect but could also be done post-connect on re-authentication exchange. Enforcement options are similar for authentication, that is, VLANs or port-based ACLs.

To make 802.1x support endpoint compliance checking, however, the supplicant needs to be interfaced with some sort of NAC client running on the endpoint. The RADIUS server needs to have a corresponding verifier component. The built-in Windows supplicants do not have this capability today, although the supplicants that Microsoft will provide for NAP-enabled (Vista and Windows XP) endpoints will. However, this approach limits the server side choices to the Microsoft NPS, which will only be available with Windows 2008 Server. NAP will be Windows only for the foreseeable future. There are third-party alternatives available today that use a RADIUS proxy server, but these all require installing a new supplicant.

In the meantime, a "dissolvable" agent provides an acceptable alternative. Dissolvable agents do not require software installation or configuration, but instead are downloaded on demand using a Web browser equipped with Java or ActiveX. While the user experience is not always as transparent, a dissolvable agent could be used for Windows and non-Windows platforms alike.

An alternative LAN security approach to endpoint compliance could similarly provide finer grained policies for quarantine enforcement. The advantage over using a remediation VLAN is that vulnerable endpoints waiting to be updated are not susceptible to being attacked by an unpatched, but infected endpoint.

3 Nevis LAN Security

Nevis delivers persistent LAN security in both secure switch and transparent security bridge form factors. The Nevis LAN security solutions provide a combination of pre-connect and post-connect security functions for endpoint compliance, identity based access control, and continuous threat detection.

3.1 Functionality of 802.1x without the Hassle

Should the functionality of 802.1x be desired, Nevis supports industry standard 802.1x on Nevis Secure Switch access ports. In addition, Nevis provides per-port identity-based stateful access control and VLAN assignment based on the authentication results. The Nevis 802.1x solution works with any RADIUS server.

For other, multi-user secure port types, Nevis provides all of the above mentioned alternative authentication schemes: MAC authentication, transparent authentication, and Captive Portal authentication, without the need to install client software or configure supplicants. For these methods, each user session is independently tracked and gets individualized access control policies applied.

Thus, authentication can be on a per-port basis for individual users, or on a shared uplink basis to leverage existing switch infrastructure without the need for network or switch reconfiguration. Designated groups of users can be restricted to certain areas of the network, no matter which ports they connect from, rendering critical servers that they have no access rights to invisible.

3.2 Endpoint Compliance

Nevis includes a dissolvable agent for performing endpoint compliance checks, with scanning and enforcement independent of 802.1x.

Nevis' Clientless Endpoint Integrity (CEI) can assure that only endpoints with up to date security patches, up to date anti-virus and anti-spyware signature files, and recent full-disk scans for malware are allowed on the network. This hardens the internal network, and significantly reduces its risk exposure.

3.3 Post-Connect Threat Detection

In addition, Nevis provides continuous threat detection on all flows. This uses a combination of anomaly detection and signature matching to detect and block zero-day as well as known attacks. Nevis is unique in its focus on endpoint malware detection as a complement to endpoint compliance. Infected endpoints can be identified by their behavior and traffic patterns, as well as traffic content.

4 Conclusion

In summary:

- 802.1x is widely available but rigid and still immature.
- It doesn't provide a complete solution to many organizations' authentication and policy enforcement requirements, even when integrated with a NAC solution.
- Today, Nevis supports 802.1x in its LANenforcer™ secure switch, along with more full-featured authentication and access control mechanisms. This allows users to seamlessly integrate Nevis into an existing 802.1x environment without a difficult transition, and allowing them to take advantage of the additional security features over time.
- The Nevis LAN security approach offers a compatible, flexible alternative ideally suited for providing granular policies in an integrated security solution.

Nevis Networks, Inc.
295 Bernardo Ave., Suite 100
Moutain View, CA 94043
www.nevisnetworks.com

International:

Nevis Networks
Delegate House
30 Hart Street
Henley On Thames, UK
RG9 2AL

Nevis Networks India
C301 Pune IT Park
Bhau Patil Marg
34 Aundh Road
Pune 411020, India