

802.1X Authentication Technical Report

Nick Peelman

Purdue University

Abstract

802.1X is an IEEE specification originally defining port-based authentication for switches and network gear and was adapted to provide a layer 3 and above authentication schema for 802.11 wireless networks. Due to the fact that physical security for devices cannot always be guaranteed, and it was conceivable that a port or ports could be compromised giving attackers access to a network to wreck havoc on. 802.1X hinders this activity by forcing a user to authenticate at a level higher than the link layer, before the port will allow anything more than authentication traffic through. The authentication traffic in question is EAP (Extensible Authentication Protocol), which was built for PPP.

History

EAP – aka: RFC3748

In order to grasp the mechanics of 802.1X, it is better to first know how it came about. A significant component of 802.1x is EAP (Extensible Authentication Protocol), which was written during the dark ages of dial-up provide the Point-to-Point Protocol (PPP) with a remote authentication protocol that would allow for multiple remote access sites to use a centralized user database, with an ultimate objective of proving the user's identity to the system via a password or token of some kind. Given the framework nature of EAP (hint: Extensible!), the method of authentication is not specified; the protocol merely defines the communications required of that method, and provides some common functionality. This allows EAP to carry a variety of methods, including password and certificate authentication. (Roshan 2001; Edney, 2004)

802.1X – Why?

At some point in the late 1990s, the rapid deployment of enterprise networks, and the sudden shift towards network security, revealed many growing pains for anybody worried about controlling network access. Everybody was so concerned about people trying to illegally access corporate networks remotely, that it took a while before anybody considered the issue of unauthorized people gaining unauthorized physical access to the system via an empty switch port. Rather than completely disabling unused ports and requiring them to be reactivated when needed, would it not be great if there was a way for switches and other network devices to authenticate users to a centralized system? This was the original purpose of 802.1X as the first draft of the specification outlined; it was port-based authentication, port referencing the

physical port of a switch, not the more logical and arbitrary TCP network port that most think of when they think network security.

In a similar scenario, soon after the IEEE began to produce feasible wireless networking standards that were adopted and deployed, that same old problem of access control came back, and it was decided that the power of 802.11 networking needed matching security measures in order to be effectively deployed and useful in a corporate environment. It was discovered quickly that a similar situation had been solved already, using 802.1X, and the standard was revised and adapted to work with wireless networking.

How does it work

802.1X outlines a 3 point authentication schema, generally defined as having a Supplicant, an Authenticator, and an Authentication service as seen in Figure 1.

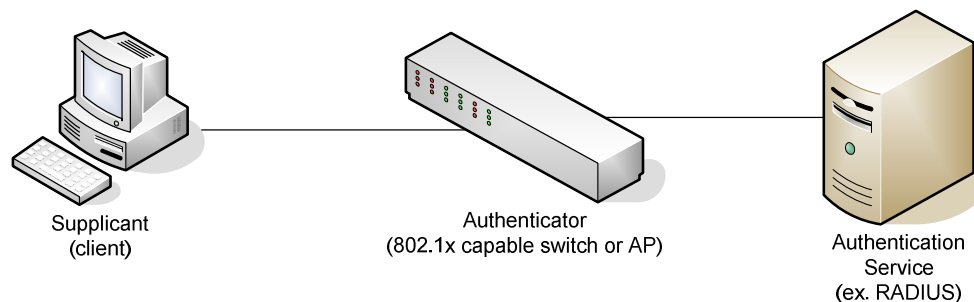


Figure 1: Wired 802.1X

Originally, 802.1X used MAC addresses as the only credential to determine access. This was far too limiting. Currently the standard supports a full spectrum of authentication methods, from passwords to fingerprints and almost everything in between. The Authentication servers can also pass EAP messages back to the Authenticators to specify things such as VLAN IDs. This is discussed more in later sections. In both wired, and wireless scenarios, 802.1X generally works the same way. When a client joins the network they can not communicate with anything else

but the switch or access point they connect in until they authenticate. Some operating systems allow this authentication to happen automatically upon connection. Other systems or other methods, require the user to initiate the process by sending credentials to the switch or access point. This is done using EAP messages, typically using the EAPOL or EAPoW protocol (EAP over LAN / EAP over Wireless). The switch can then either forward the EAP messages directly to the authentication service, or use another protocol to access a RADIUS or other directory server to authenticate the supplicant and permit or deny access. Some of the Authenticator devices are intelligent enough that more configuration than simply switching on the port can be done when a user is successfully authenticated, such as adding that switch port to a specific VLAN based on their login credentials.

Wired Deployment

802.1X's stomping grounds reside in the wired realm. Information on actual, real live 802.1X deployments in physical port security is scarce, but apparently in use given the number of tutorials and guides available online. Typically, port security is maintained physically, by keeping switches in locked wiring closets and only plugging in cables necessary for connectivity. Any further connectivity needed requires somebody visiting the switch and matching a switch port to a patch panel port, and in some cases, activating the switch port from within the switch's console interface. This becomes cumbersome in large deployments, but even so is still widely used. 802.1X provides a better solution by allowing everything to be pre-wired, preconfigured, locked away, and allowed to gather dust until a hardware failure. It is not without drawbacks though. Devices such as network-capable printers, NAS devices and legacy devices are notorious for not fully supporting 802.1X, if they support it at all. This presents a

problem of having some secured ports, and others wide open with little to no security. If all a malicious user has to do is unplug a printer to gain unrestricted network access, it is not going to provide very much security. A smart deployment can alleviate this somewhat, by using VLANs to segment the physical network into logical blocks, and using a firewall to filter traffic between them. Using this method, an unauthenticated port given to a printer could be placed in a VLAN with other printers, and firewall rules would define that only printer traffic is allowed in or out. Similar VLANs could be created for other groupings of devices, increasing network complexity, but what kind of security is simple? (Robinson, 2006)

Wireless Deployment

802.1X has become a workhorse in wireless security. While a multilayered, “onion” system is still necessary for proper security, the wide-spread support of 802.1X throughout much of today’s network gear almost guarantees that it will be the standard used when authenticating. Given its flexibility and generalized nature, this is not too bad of a deal. You still get the wonders of dynamically assigning VLANS for Wireless supplicants (clients) based on credentials, your choice of authentication credentials and authentication server, the support of the most popular operating systems, and on top of that you get a few more EAP methods designed for wireless use. (Robinson, 2006)

WPA Enterprise

While 802.1X provides a standard for authenticating and authorizing users on the network, it does little in the way of providing wireless security. That is left up to a variety of other IEEE802 standards, including 802.11i (which specifies 802.1X as an integral part). Most people know 802.11i as WPA and WPA2. WPA only partially implements 802.11i, while WPA2 meets the full

standard. The basic premise of WPA is to encrypt traffic using some form of key. In the case of WPA Personal and WPA2 Personal, this key is pre-shared, and is the same for all users of the network. The system is fairly robust and secure, but there is still the problem of there being one key that is distributed to many users, and therefore leaves a gaping security hole. WPA Enterprise and WPA2 Enterprise fix this by using 802.1X to authenticate to an authentication server, which provides a different key for each authorized user. (Bulk, 2006; Wi-Fi Protected Access, 2007)

VPN Support and Deployment

Older wireless systems might have used a VPN system to authenticate and authorize users for network access. This system works well in some cases, but poorly in others where the wireless users may need to create one or more VPN tunnels on top of the tunnel required for their network connectivity. Sometimes this works, most of the time it does not. 802.1X works at a lower layer that does not affect the ability to connect to external VPNs.

On the other side of the coin, most VPNs typically use some sort of PPP, or IPSec, to build a tunnel between the two end points. Since we know that 802.1X uses EAP, and EAP was originally designed for PPP authentication, the same principles can be applied using 802.1X. This is typically only found on high end remote connectivity equipment, and is designed to authenticate users at a remote office, who are connected to a parent office via a persistent VPN. (VPN Access Control, 2006)

EAP Methods

EAP, as mentioned earlier, is an open ended framework designed to be adaptable to a variety of situations. This has made it ideal for many uses, and made popular by the widespread success

of wireless technology, including cell phones which have many EAP methods dedicated to their communications. Below are the major EAP players of 802.11 wireless, each with a set of strengths and weaknesses. (Extensible Authentication Protocol, 2007)

LEAP

LEAP was created by Cisco for use in their authentication systems and is considered to be a very weak protocol. This protocol has been replaced by EAP-FAST, although device support for that protocol is very minimal.

PEAP

PEAP uses a combination of a server certificate (and therefore partial PKI) and TLS encryption to protect the user's credentials during authentication. Upshot is that it was developed by Cisco and Microsoft, so it will probably work well with the major players. The downside to PEAP is that the only user-to-network authentication it supports that does not require certificates uses MSCHAPv2, which is generally less secure than its competitors.

EAP-TTLS

Similar in functionality, capability, and robustness to PEAP, and sharing PEAP's requirement of a PKI for a server certificate, but more open in its user-to-network authentication requirements. Most decisions come down to this protocol or PEAP, and probably the last question asked will be "can we live with MSCHAPv2?"

EAP-TLS

Generally regarded as the toughest of the bunch, in terms of both setup and security, EAP-TLS requires a full PKI system, because it uses certificates for both network and user authentication, which is very restrictive in most environments, but remains top dog for security. (Peretz, 2002)

Future Use

The future of 802.1X is pretty bright. It has become so widespread and heavily used, it will not be going anywhere for a while. 802.1aa was considered an 802.1X “Maintenance” document, and was incorporated into the full 802.1X standard in 2003, and a few other revisions have been integrated since then as well. (802.1X-REV, 2004) As far as current news and evolving standards go, there is not really a replacement for 802.1X on the horizon. Its open-ended nature and use of EAP’s many faces, will probably allow it to adapt to future changes in need, rather than require a successor to take over where it leaves off.

Conclusions

802.1X has become one of the all-stars of the IEEE 802 standards. It applies to both wired and wireless networks, and looks to be able to weather the changes that newer evolving standards will bring. Its open nature and chameleon-like authentication protocols allow it to adapt to a variety of situations and allow network administrators to pick the best solution to suit their needs.

References

- 802.1X-REV (2004) Retrieved 03-22-2007 from <http://www.ieee802.org/1/pages/802.1X-rev.html>
- Bulk, Frank. (01-27-2006). *Crash Course: The ABCs of WPA2 Security*. Retrieved 03-22-2007 from <http://www.networkcomputing.com/showArticle.jhtml?articleID=177103376>
- DeVries, Jeremy (10-30-2005). *WPA-PSK: Step-By-Step* Retrieved 03-22-2007 from <http://www.wi-fiplanet.com/tutorials/article.php/3552826>
- Edney, J., & Arbaugh, W. (2004). *Real 802. 11 Security*. Boston: Addison-Wesley.
- Extensible Authentication Protocol. (2007, March 17). In Wikipedia, The Free Encyclopedia. Retrieved 06:59, March 23, 2007, from http://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&oldid=115729321
- Fleishman, Glenn. (01-10-2005). *Affordable 802.1X for Offices*. Retrieved 03-22-2007 from <http://www.wifinetnews.com/archives/004673.html>
- Gast, M. G. (09-21-2004). *Wireless Security and the Open1X Project*. Retrieved 03-22-2007 from <http://www.macdevcenter.com/pub/a/mac/2004/09/21/open1x.html>
- Gast, M., (2005). *802.11 Wireless Networks*. Sebastopol: O'Reilly.
- Guy, The Cable. (03-2003, updated 06-7-2006). *Wi-Fi Protected Access (WPA) Overview*. Retrieved 03-22-2007 from <http://www.microsoft.com/technet/community/columns/cableguy/cg0303.msp>

Guy, The Cable. (04-2002, updated 01-30-2007). *IEEE 802.1X Authentication for Wireless and Wired Connections*. Retrieved 03-22-2007 from <http://www.microsoft.com/technet/community/columns/cableguy/cg0402.msp>

IEEE 802.1X. (2007, March 22). In Wikipedia, The Free Encyclopedia. Retrieved 06:58, March 23, 2007, from http://en.wikipedia.org/w/index.php?title=IEEE_802.1X&oldid=116982774

IEEE. (2004). *802.1X-2004 IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control*. Los Alamitos: IEEE

Peretz, Matthew. (01-31-2002). *A Very Funky 802.1X Security Solution*. Retrieved 03-22-2007 from <http://www.wi-fiplanet.com/news/article.php/965961>

Robinson, Cornell W. (06-28-2006). *Crash Course: 802.1X: The Great Authenticator*. Retrieved 03-22-2007 from <http://www.networkcomputing.com/channels/wireless/showArticle.jhtml?queryText=&articleID=189601414&pgno=3>

Roshan, Pejman. (09-24-2001). *802.1X authenticates 802.11 Wireless*. Retrieved 03-22-2007 from <http://www.networkworld.com/news/tech/2001/0924tech.html>

Snyder, Joel. (05-06-2002). *What is 802.1X?* Retrieved 03-22-2007 from <http://www.networkworld.com/research/2002/0506whatisit.html>

Thayer, Rodney. (05-14-2004). *Vendors hit the 802.1X mark for access, but security holes remain*. Retrieved 03-22-2007 from <http://www.networkworld.com/research/2004/0510ilabssec.html>

VPN Access Control Using 802.1X Authentication (06-02-2006). Retrieved 03-22-2007 from

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xa/gt_802_1.htm

Wi-Fi Protected Access. (2007, March 21). In Wikipedia, The Free Encyclopedia. Retrieved 06:58,

March 23, 2007, from [http://en.wikipedia.org/w/index.php?title=Wi-](http://en.wikipedia.org/w/index.php?title=Wi-Fi_Protected_Access&oldid=116828693)

[Fi_Protected_Access&oldid=116828693](http://en.wikipedia.org/w/index.php?title=Wi-Fi_Protected_Access&oldid=116828693)

Questions

1. What is the difference between WPA1/2 Personal and WPA1/2 Enterprise?

WPA Personal uses a PSK, WPA Enterprise uses 802.1X for authentication with a separate key for each user.

2. In an 802.1X Authentication relationship, the client machine is referred to as:
 - a. Suppliment
 - b. Client
 - c. Supplicant
 - d. User
3. Why do EAP-TTLS and EAP-TLS Differ?
 - a. EAP-TLS has better encryption
 - b. EAP-TLS requires a full PKI Infrastructure
 - c. EAP-TTLS has another 'T'
 - d. They are the same thing

OR

EAP-TLS Requires a full PKI infrastructure, since both client and network need certificates to authenticate. EAP-TTLS only needs a certificate for the network, the clients can authenticate with other means.

4. What was the original purpose of EAP?
 - a. Providing user authentication on LANs
 - b. Defining an authentication schema for DSL
 - c. Protecting Wireless networks
 - d. Providing user authentication for PPP connections
5. T/F 802.1X requires a RADIUS server be implemented somewhere in the network.