IEEE 802.1X

IEEE 802.1X is the standard protocol for allowing hosts and users to be authenticated to the network before obtaining a connection (port-based network admission control). As well as providing very effective access control to wireless and other networks, it is being used increasingly for other aspects of host security and management. (Note that IEEE 802.1X is dependent on the Extensible Authentication Protocol (EAP), which is covered by a companion factsheet [1].)

The Basics

IEEE 802.1X provides the following core capabilities:

- port authorisation on a per-user or per-host basis (the authenticator will not forward frames until the RADIUS server signals that the supplicant is authorised)
- support for multiple authentication methods (thanks to the use of EAP)
- separation of the authenticator from the back-end authentication server, allowing user management and policy decision making to be centralised.

An overview of IEEE 802.1X [1] is shown in Figure 1 below. An EAP [2] exchange encapsulated directly within Ethernet frames is performed between the supplicant and a RADIUS/EAP Server (henceforth RADIUS server), via the authenticator. The EAP exchange between the authenticator and the RADIUS Server is transported by the RADIUS [3] protocol. The RADIUS Server attempts to validate the supplicant's credentials against a user database server, and signals the result to the authenticator. If the result is a success, the authenticator permits forwarding of frames to and from the supplicant.

Figure 1: IEEE 802.1X overview

Dynamic VLAN Assignment

Besides authentication, perhaps the most useful feature of IEEE 802.1X is dynamic VLAN assignment [4]. A supplicant authenticates to the RADIUS Server, which returns a RADIUS Access- Accept packet to the authenticator. The packet also includes attributes indicating which VLAN to assign to the supplicant's port. For example, a student logging into a terminal could be assigned the 'student VLAN'; a member of staff logging in to the same terminal could be assigned the 'staff VLAN'. If no one is logged in, the terminal may have 'computer' credentials that permit access to a 'maintenance VLAN' for software updates and remote

administration. Note that dynamic VLAN assignment is not part of the IEEE 802.1X specification, but most vendors have implemented it.

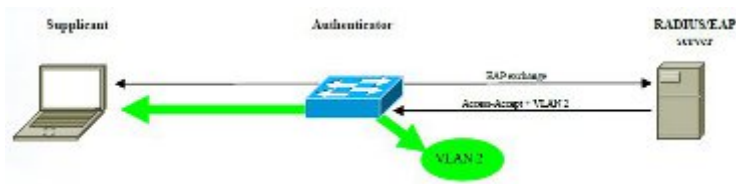Figure 2 below illustrates dynamic VLAN assignment.

Figure 2: dynamic VLAN assignment.

Dynamic Keying

IEEE 802.1X can also improve the encryption provided by IEEE 802.11 [5] wireless networks. The original IEEE 802.11 specification's privacy and authorisation system, Wired Equivalent Privacy (WEP), required that all wireless clients and access points shared the same secret encryption key. While manageable for a few stations, distributing the key to a large number of clients and access points becomes a significant problem. Moreover, because the key is shared, any host can read any other hosts' data. To address these problems, many vendors have used IEEE 802.1X to distribute a unique key to each wireless client. This is called dynamic keying. EAP authentication may produce a key, called the Master Session Key (MSK), that is known only by the supplicant and the RADIUS Server. With WEP (see Figure 3 below), the RADIUS server sends the MSK to the Wireless Access Point (WAP) within the RADIUS Access-Accept packet. The WAP generates a new random key, known as the EAPOL key, encrypts it with the MSK and sends it to the supplicant. The supplicant, knowing the MSK, decrypts the EAPOL key and uses it to encrypt subsequent transmissions between the supplicant and the WAP.

Figure 3: dynamic WEP keying

Dynamic keying for WEP's successors, WPA and WPA2 (both are based on IEEE 802.11i [6]; see also [7]), is similar but differs in a couple of important ways. First, to avoid the poor cryptographic practice of re-using a key in different contexts (in this instance, EAP and WPA/WPA2), the supplicant and RADIUS Server derive a second key from the MSK, called the Pairwise Master Key (PMK) which is used in its place. Secondly, WPA and WPA replace WEP's one-way transmission of the EAPOL key (from the WAP to the supplicant) with a four-way handshake between the WAP and the supplicant. The four-way handshake uses the PMK to derive further keying material used to encrypt subsequent wireless communications.

Network Admission Control

Network Admission Control (NAC) systems enable a network administrator to define a security policy (such as a requirement for a specified patch level) that is tested and enforced whenever a host connects to a network access point, such as a switch, WAP or VPN

concentrator. NAC systems typically provide mechanisms for placing non-compliant devices into a quarantine VLAN for patching. At time of writing (October 2005), three NAC solutions are available or imminent: Cisco®'s Network Admission Control [8], Microsoft®'s Network Access Protection [9] and the Trusted Computing Group's Trusted Network Connect [10]. IEEE 802.1X is a key component of all three solutions.

Supplicants

The table below provides a comparison of the supplicants available in October 2005.

	Operating systems								EAP types	
	W95	W98	WME	W2K	WXP	Linux	OSX	PPC	TLS	PEAP
Native Windows				1						2
Native MacOS							6			
HP ProCurve Client						8	9			
Funk Odyssey										
SecureW2				1						
wpa_supplicant	11	11	11							

Wire1X											

Notes: 1. Requires SP3. 2. EAP-MSCHAPv2 inner-method only. 3. Requires WPA driver from adapter vendor. 4. Requires SP2 or SP1 and WPA driver from adapter vendor. 5. Caches credentials permanently in registry. 6. Requires MacOS 10.3. 7. Requires Airport Extreme. 8. Requires Redhat 9+. 9. Requires MacOS 10.2. 10. WXP only. 11. WEP and WPA only. 12. Advanced 802.1X and 802.11 features; basic, but improving, GUI. 13. No known production use.

Table 1: a comparison of supplicants

Bibliography

1: IEEE Computer Society, 802.1X - Port Based Network Access Control, 2001.

2: B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed., RFC3748 - Extensible Authentication Protocol (EAP), 2004.

3: C. Rigney, S. Willens, A. Rubens, W. Simpson, RFC2865 - Remote Authentication Dial In User Service (RADIUS) , 2000.

4: P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, RFC3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, 2003.

5: IEEE Computer Society, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

6: IEEE Computer Society, Medium Access Control (MAC) Security Enhancements, 2004.

7: WiFi Alliance, WiFi security at work and on the road: http://www.wi-fi.org/ [2].

8: Cisco Systems, Network Admission Control: http://www.cisco.com/en/US/netsol/ns466/ [3]

9: Microsoft Corp, Network Access Protection: http://www.microsoft.com/nap [4].

10: Trusted Computing Group, Trusted Network Connect: http://www.trustedcomputinggroup.org/solutions/network_security/ [5].

Trademarks

Cisco® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the US and certain other countries.

Microsoft® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Source URL: https://community-stg.jisc.ac.uk/library/advisory-services/ieee-8021x

Links
[1] http://community.ja.net/library/advisory-services/extensible-authentication-protocol
[2] http://www.wi-fi.org/
[3] http://www.cisco.com/en/US/netsol/ns466/
[4] http://www.microsoft.com/nap
[5] http://www.trustedcomputinggroup.org/solutions/network_security/