IEEE 802.1X implementation at Janet-connected organisations

022 (04/08)

This document was produced to share knowledge, experience and current developments surrounding campus 802.1X implementation within the JANET community.

Readers are assumed to have a basic knowledge of networking concepts and preventive security awareness. A companion technical guide Security Matters is available [1].

Scope and Audience

Providing network access within large organisations is at best challenging and at worst near impossible. Users want the ability to be able to start up their operating system and have instantaneous network access. However this is usually in conflict with the organisational need to prevent unauthorised access to the network and also to provide accountability of users actions.

An IEEE standard 802.1X [2] see provides a mechanism for network port access control and manages the process of authenticating and authorising attached devices by extending the EAP protocol over the network. Network access ports can take various forms such as: a network socket, switch port, or wireless access point.

EAP (Extensible Authentication Protocol) is a powerful tool in the network administrator's tool box for providing flexible network access through authentication, authorisation and accounting. EAP is an authentication framework which provides multiple methods for authentication (Aboba, Blunk, Vollbrecht, Carlson, & Levkowetz, 2004 [3]). Through the use of 802.1X and 802.11i, EAP can be used to provide enterprise network access control (NAC) for both wireless and wired networks.

This guide aims to provide a background to the implementation of 802.1X as a network control mechanism on both wired and wireless networks at JANET-connected organisations.

Major changes such as the introduction of 802.1X will almost certainly create concerns amongst various people involved in the process. The process of introduction will most likely involve a consultation process with the stakeholders, as it represents a fundamental change to the way users access the network and is a process which requires planning. Implementing 802.1X in an educational environment is a major undertaking and should not be taken lightly.

History of 802.1X

Initially developed by 3Com, HP and Microsoft®, 802.1X was first recognised by IEEE in

January 1999 and was first approved as a standard in June 2001 (IEEE Computer Society, 2001 [4]). It was developed as a mechanism for preventing unauthorised access to a LAN at the switch port level, the goal being to enable organisations to protect networks sockets in public spaces within buildings.

It is important to consider that there are many components to a complete 802.1X implementation and the technologies have evolved over a very short space of time.

EAP is the cornerstone of the 802.1X standard and was originally developed in 1998. The EAP protocol, RFC 2284 [5], has been refined over time until a significant revision in 2004 which lead to the protocol which is familiar to network administrators today.

EAP was originally based upon the Point-to-Point Protocol (PPP) and was associated with Serial and not Ethernet technologies. Within the PPP definition Link Control Protocol is outlined, describing how the link should be established, whilst EAP describes the authentication phase.

RADIUS (Remote Authentication Dial-In Users Service) originated with the Internet Engineering Task Force (IETF) group with a 1994 draft standard submission. In 1997 the first RADIUS RFC was released and then later revised. RFC 2865 [6] was released in June 2000. RADIUS has been expanded with a number of extensions to provide services for modern network deployments. These extensions have largely rendered the proposed replacement for RADIUS, named Diameter [7], redundant.

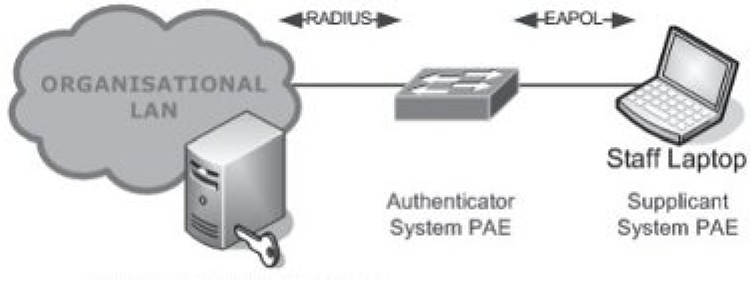
Using 802.1X to Improve Network Security

Through the use of 802.1X, network security can be improved by reducing unauthorised network access. 802.1X is superior to MAC Address Authentication which may already be implemented; significant weaknesses can be found in the ability to spoof the MAC Address of devices connecting. 802.1X operates at the Data Link Layer, Layer 2, of the OSI model and enables the use of EAPOL (Extensible Authentication Protocol Over LANs).

User or device credentials are encapsulated within an EAPOL packet before it is transmitted onto the network before reaching the authenticator. This is a low weight simple protocol with few different types of packet, mainly: Request Identity and Response packets.

EAPOL is simply a mechanism to encapsulate EAP messages within that of the underlying protocol.

Figure 1: Gaining access to a network using 802.1X



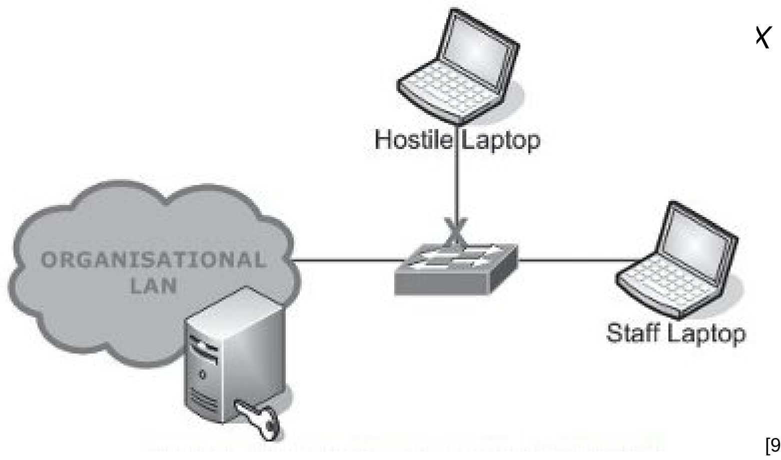
[8]

The operation of 802.1X is covered in detail within Chapter 2 of this Technical Guide. The device running the 802.1X supplicant and the network port secured by 802.1X is referred to as Port Access Entity (PAE).

Preventing Unauthorised Network Access

The very purpose of 802.1X is to control port access and prevent unauthorised users from using your network. How can this behaviour benefit your organisation?

The obvious advantage is that people who are not members of your organisation or authorised visitors will be denied access to your network. This is a valuable tool in preventing electronic crime as it is often very difficult to secure every socket that a visitor could gain access to. However, stopping unknown users is not where the 802.1X functionality ends.



[9]

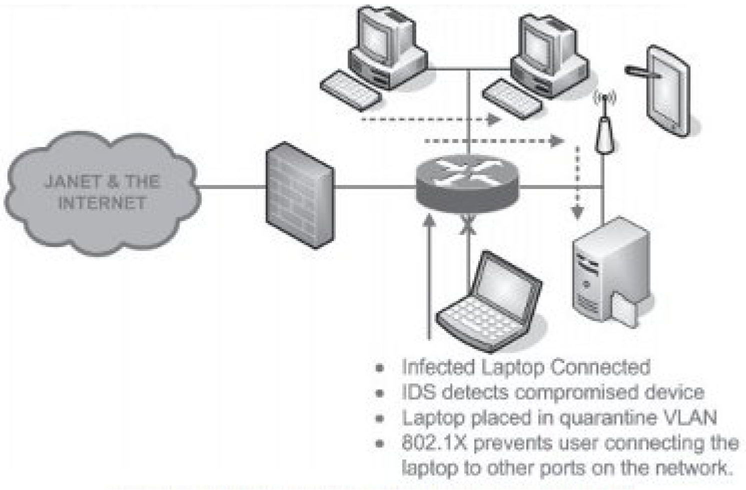
Viruses and Compromised Computers

Every large network is likely to have seen computers which have been compromised by viruses, worms and trojans. Restricting the network access for these computers is a standard requirement of the IT Service provider at any organisation. 802.1X together with other systems can help by providing the facility to quarantine compromised computers.

802.1X is not a mechanism for detecting compromised computers; this role is undertaken by intrusion detection/prevention systems or anomaly detection systems. It is important that the detection device has a feedback mechanism that can utilise 802.1X as part of the mitigation process, ensuring the client moves to a quarantine VLAN by forcing the client to re-authenticate. Subsequent attempts by the infected client to connect to the network will result in the same quarantine VLAN being presented.

Once a machine has been identified as being compromised, the organisation’s RADIUS servers can be instructed to place a machine, and / or user, onto a quarantine VLAN. The RADIUS server can identify the machine by its active directory credentials, user login details, or by MAC address. In most case you will want to quarantine either the MAC address or the active directory credentials (if machine authentication is being used).

Figure 3: Preventing a worm outbreak with 802.1X and IDS


JANET & THE INTERNET
Infected Laptop Connected
IDS detects compromised device
Laptop placed in quarantine VLAN
802.1X prevents user connecting the laptop to other ports on the network.

[10]

Location Aware Networking

Being able to control network access based upon location is very desirable. For example it is common for students to be prohibited from unplugging organisational lab computers and plugging in their own laptops. As 802.1X authentication identifies the point at which the supplicant is trying to access the network, it is very easy to prevent groups of user computers from accessing the network in specific locations.

Furthermore with the accounting and logging provided by authentication servers, attempts to access the network in a prohibited manner can be logged and reported, and if required users can be banned. Other examples include IT Service staff being given appropriate VLANs with elevated access rights.

Per Client Accounting

Using RADIUS servers and 802.1X will provide your organisation with accounting logs for each user on the network. These logs contain information such as: the location; switch port or access point; where the user was connected; the client’s IP Address; the amount of data transferred; and when the session began and ended. This is valuable information when providing audit trials or trying to locate problems. Additionally many IDS/IPS solutions can work in co-operation with RADIUS server accounting to provide enhanced features.

Guest Access

Providing access to visitors poses major security network risks. The traditional approach has been to make sockets available in public locations and then to lock down those sockets and restrict their network functionality. This was usually done in one of the following ways:

- DMZ – Sockets in public locations are put onto a restricted VLAN which gives limited web and email access, and is firewalled off from the rest of your organisation’s network
- Walled Garden / Captive Portal – Clients using sockets in public locations are redirected to a HTTPS login page. After authenticating in, a hole in the firewall is created for their MAC address and they are able to access the network. This is often combined with a DMZ so that even after logging in visitors are isolated from the rest of the network.

These methods of securing network sockets are simple to implement and work well, but are not without their limitations. Firstly a DMZ offers no ability to restrict who is joining your network. This makes accounting very difficult as you cannot track down who was using a particular MAC address. Captive portals partially address this by denying access until the client logs in; however this is only done by MAC address which can be trivially spoofed.

The 802.1X provision for guest access can offer much greater security and functionality than a captive portal based solution. Firstly 802.1X securely identifies the client using techniques which cannot be spoofed. This means you can identify, with greater certainty, who clients are and you can relax restrictions on VLANs used by visitors. 802.1X also provides the ability to trivially provide different VLANs to different classes of user (or even individual users) through the use of VLAN override options.

VLAN override allows the authentication server to instruct the switch as to which VLAN to put the client on. This is useful as staff who plug into a socket can be given one VLAN, students another, and guests yet another. In advanced deployments VLANs can follow particular individuals around the organisation.

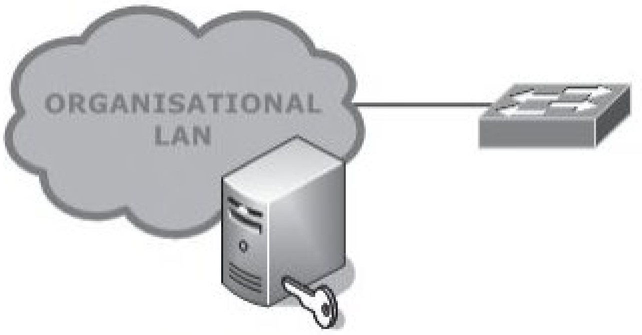
Implementation of 802.1X does not mean existing captive portal based solutions have to be abandoned. 802.1X can happily co-exist with captive portals. In most cases having an alternative solution is preferential as some devices may not be capable of 802.1X authentication. Also a dual system allows for a smoother transition of clients from the old system to 802.1X. To work with a captive portal, switch ports can be configured with a ‘Guest VLAN’; clients which do not attempt to 802.1X authenticate will be given the ‘Guest VLAN’, likewise so will Supplicant PAEs that request the guest VLAN from the Authenticator PAE. This means that clients which do not attempt to 802.1X authenticate can fall through on the existing captive portal based solution. Likewise both visitors who 802.1X authenticate and those who do not can feed a DMZ network.

Using 802.1X, JANET Roaming can easily be provided in areas accessible to visitors from other organisations. When using their JANET Roaming credentials, visitors can authenticate themselves and be provided with your organisation’s Eduroam VLAN for access to the JANET network.

Authentication, Authorisation and Accounting (AAA)

802.1X can act as an enabler to provide AAA functions within an organisation’s network. AAA stands for Authentication, Authorisation and Accounting and is provided by a Network Authentication Server. This acronym is also sometimes referred to as Triple A and may also include a fourth A, Auditing.

Figure 4: Location of the Network Authentication Server



[11]

The Authentication element of AAA verifies the credentials of users presenting access tickets such as passwords, certificates or hardware keys. The Authorisation element of AAA provides details of the services available to the authenticated user in order that the authenticator system can provide the appropriate level of service. In this case the switch is the authenticator system and the appropriate level of service is a VLAN and other related network access control features.

The Accounting element of AAA provides a log of resource utilisation, typically used in the education sector to provide a log of user authentication. However this can also be used for billing, network trend monitoring and within Management Information Systems.

AAA is a standards-based system which allows interoperability with a large number of systems. AAA servers typically take the form of a RADIUS server. Open Source variants exist like FreeRADIUS as well as software for the Microsoft® platform.

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

Links
[1] http://community.ja.net/library/janet-services-documentation/security-matters-technical-guide
[2] http://grouper.ieee.org/groups/802/1/
[3] http://www.ietf.org/rfc/rfc3748.txt
[4] http://standards.ieee.org/getieee802/
[5] http://www.ietf.org/rfc/rfc2284.txt
[6] http://www.ietf.org/rfc/rfc2865.txt
[7] http://www.ietf.org/rfc/rfc3588.txt
[8] http://community.ja.net/system/files/images/tg-ieee8021x-01.jpg
[9] http://community.ja.net/system/files/images/tg-ieee8021x-02.jpg
[10] http://community.ja.net/system/files/images/tg-ieee8021x-03.jpg
[11] http://community.ja.net/system/files/images/tg-ieee8021x-04.jpg