Simplifying your 802.1X deployment

The rapid growth in the number and variety of mobile devices connecting to corporate networks requires strengthening security measures at the moment of connection. IEEE 802.1X has emerged as the standard, but implementation can be challenging. The Mancala Network Controller simplifies and secures 802.1X deployment.

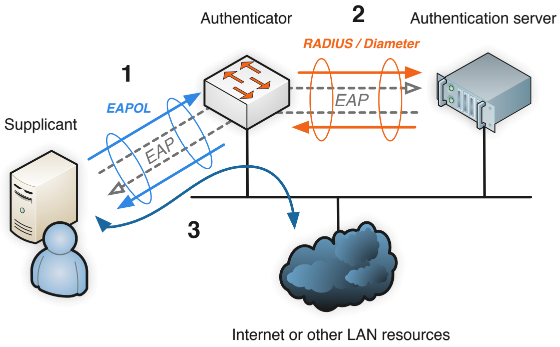
802.1X OVERVIEW

Mobility presents a number of challenges for enterprise network management. One of the key challenges is identifying devices and users as they connect, to assign appropriate access rights in compliance with enterprise security policies. The IEEE 802.1X standard provides for authentication based on user or machine credentials, using a central authentication server.

Typical 802.1X infrastructure

There are three principal elements in an 802.1X deployment:

- The device seeking access to the network, known as the *supplicant*.
- The network infrastructure element (switch, access point, etc.) that the device is connected to is known as the *authenticator*.
- The server providing validation of the credentials, or *authentication server*. This is typically a RADIUS server interfacing with the enterprise directory (Active Directory or LDAP).



To perform 802.1X authentication end-point devices (supplicants) and the network infrastructure device (authenticators) must support 802.1X. End-point devices must be capable of participating in an 802.1X dialogue with the authenticator and exchanging credentials with the authentication server. Network infrastructure elements must be capable of interacting with the authentication server to authorize or reject authentication attempts.

Controlling access to the network

In an 802.1X-controlled network, the switches and wireless access points that form the network infrastructure are also used to enforce network access controls.

When a new device attempts to connect, the switch or access point will identify the device as “unauthorized”. When the device is in the “unauthorized” state, only 802.1X EAP Over LAN packets will be allowed to ingress. The switch or access point will then prompt the connecting device to start an EAP dialogue with the authentication server.

If the dialogue completes and the authentication server signals that authentication was successful, the switch port or access point will set the device state to “authorized”, allowing the device to communicate with other hosts on the network. If the dialogue did not complete or the authentication server indicates that authentication failed, then the device’s connection will remain in the “unauthorized” state.

MIGRATING TO 802.1X

Difficulties

The biggest challenges when migrating to 802.1X almost always involve the supplicant. Whilst initial configuration of network infrastructure may be challenging or require a high level of expertise, the result may be applied to all devices of the same type on the network, with a high level of certainty that they will operate consistently.

Although only a dozen or so supplicants are used by the majority of devices connecting to enterprise networks, the supplicant software is running under different operating systems, on different hardware, and using different networking drivers. These variations in the state of the underlying machine may cause supplicant software to perform incorrectly, or fail to function completely.

Anything from corrupt Windows registry entries to firewalls dropping EAPOL packets, can cause supplicant issues, so if it is imperative that the migration be non-disruptive, every machine that may be required to perform 802.1X, must checked independently for readiness. This is often a very time consuming task, so many administrators compromise, enabling 802.1X port by port or switch by switch, verifying that the expected devices authenticated correctly.

Unfortunately the partial migration approach is somewhat flawed. If a faulty supplicant is offline at the time of migration, or a supplicant later develops a fault, the first time the administrator is made aware, is usually when a user contacts the IT Department’s helpdesk to complain about the lack of connectivity.

The Mancala Network Controller (NC) facilitates and accelerates the move to an 802.1X secured network by allowing for a two-step migration, supporting devices incapable of performing 802.1X authentication as well as those with full support. Every network infrastructure device may become 802.1X enabled at the same time, but because 802.1X is only enforced for devices known to be 802.1X capable and ready, there is no loss of connectivity.

Two step Migration

A comprehensive inventory of devices connecting to the network is an essential first step in the migration plan. It allows network administrators to identify and classify different devices, and to verify the conditions under which they should be allowed access to the network. The powerful discovery and inventory features of the NC accelerate this mapping phase. Protocol sniffing, ARP scans, MAB (Discussed below) and SNMP are just some of the methods used to quickly and non-intrusively build a comprehensive profile of all devices on the network.

1 Learn

The NC utilizes a switch feature called Multiple Authenticator By-pass (MAB) to allow identification and authorization of non-802.1X devices. MAB allows 802.1X, MAC-Auth and/or Web-Auth (depending on vendor) to run concurrently on the same switch port.

The first step to full 802.1X migration is to set the NC to MAB learning mode. No connections will be blocked, but the network controller will use Mac-Auth to build up a port-by-port mapping of device MAC addresses in a real-time inventory, and determine which devices respond to 802.1X messages.

With this information, and information learnt from the other inventory processes, the network administrator can generate a static inventory.

The conversion strategy can be as simple as transferring all learned devices into static inventory; or in high-risk environments, manually verifying each individual device discovered. Whichever strategy is utilized, the NC provides the tools to execute it quickly and efficiently.

2 Enforce

Using the static inventory as a basis for which devices should be granted network access, the administrator can begin enabling 802.1X enforcement on infrastructure devices.

Once enforcement has been activated, the NC uses successful authentications to determine which devices have correctly configured supplicants. Once a device has authenticated successfully it will no longer be allowed network access unless it performs 802.1X authentication.

This methodology ensures devices which were identified as 802.1X capable but have misconfigured supplicants are not denied network access, and that devices which were not initially identified as 802.1X capable, but have performed authentication successfully, have their authentication profile updated automatically.

Devices which were not included in the original static inventory are assigned to a ‘quarantine’ or ‘remedia - tion’ VLAN where (if allowed by policy) they can be self-registered by their users.

The result is a network with a high level of security, yet flexible enough to adapt to new or unrecognized devices, an important consideration as enterprises seek to accommodate highly mobile user populations and the move to “bring your own device”.

MANAGING NON-802.1X DEVICES

In typical 802.1X enabled enterprise networks, non-802.1X devices (such as printers, VoIP phones, and CCTV cameras) retain access to the network either by being connected to ports configured to be fully open with no authentication, or by being connected to ports which authenticate devices by MAC address.

This presents a potential security hole in an otherwise secure edge network, as attackers can physically connect to an ‘open’ port or ‘spoof’ the MAC address of one of the 802.1X incapable devices to gain network access.

The NC helps prevent these types of intrusions. In addition to discovering a device’s presence and 802.1X capabilities, it also applies advanced OS and traffic profiling techniques to classify devices (VoIP phone, Printer, Workstation etc.). The device classification maps to an expected network traffic profile, listing the protocols and network resources the device is expected to utilize. If a device starts sending types of traffic that fall outside its network profile, remediative action is taken automatically.

Example: If a device classified as a 'printer' attempts to resolve 'facebook.com' this would fall outside its expected traffic profile. The device will either have its network access terminated completely, or it will be placed on a quarantine network (depending on policy).

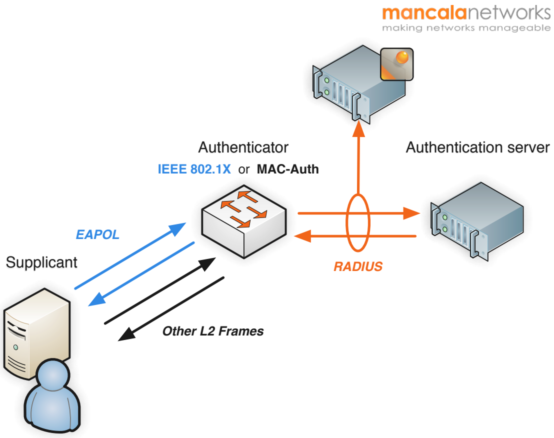
INTEGRATING WITH AUTHENTICATION SERVICES

The NC can operate in multiple modes, depending on the level of integration the network administrator is comfortable to implement.

Passive Mode

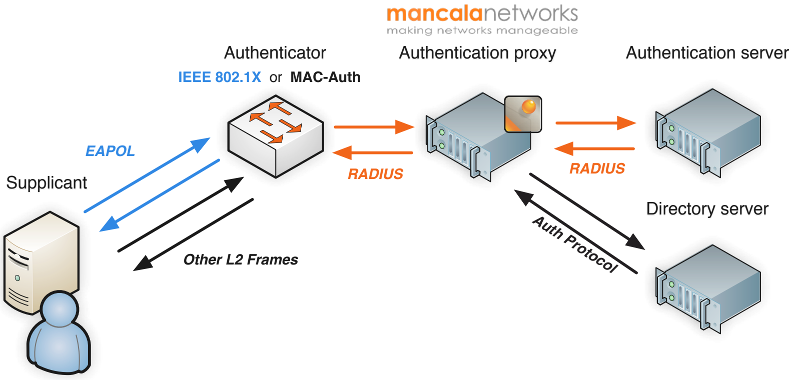
Passive mode has the least impact on existing network configurations. The NC is placed on a mirror port between the Authenticator and Authentication server, where it can passively observe authentication attempts and use this information to populate its real-time inventory.

Passive mode can be used as a non-intrusive initial step to a more secure network, giving the network manager detailed information on network activity. In passive mode the NC cannot perform enforcement or provide open authentication for MAB learning mode.



Inline and Active Mode

In Inline mode the NC functions as a proxy between the existing RADIUS server and Authenticators. In this mode it can observe authentication attempts to help populate the real-time inventory, provide open authentication for MAB learning, and later provide 802.1X enforcement, rewriting RADIUS packets on the fly to enforce policies.



In Active mode the NC translates between the RADIUS protocol and other directory services. Supported directory services include (but are not limited to) NTLM (Active Directory), Kerberos, LDAP, SQL and RSA SecurID. All the functionality of Inline mode is also available in Active mode.

SUMMARY

The explosion in mobility and the take-up of new “prosumer” devices by corporate employees and partners means the network now needs in-depth protection inside the firewall. 802.1X is a key element in internal security, but deployment is frequently delayed due to the complexity of migration, port by port and device by device.

The Mancala Network Controller largely automates, this traditionally very manual and labor-intensive process, allowing the administrator to define multiple steps for maximum operational flexibility. Starting with network-level and device-level default policies, only exceptions to default policies need manual configuration. “Learning” and “migration” modes enable instantaneous site-wide deployment, with no disruption, and the Mancala Network Controller’s dashboard-style monitoring interface allows the administrator to oversea the process as devices migrate to 802.1X authentication mode.

Automated inventory, sophisticated device profiling and smart switch and access point management allow the Mancala Network Controller to accelerate migration to the increased security of an 802.1X-enabled network, while extending the protection to cover non-802.1X compliant devices and their access.

Mancala Network Controller - Enterprise network control and management solution

Built from a patented and award winning technology, the Network Controller’s innovation lies in its capability to not only monitor network control flows, but to also leverage that information to increase network security and management flexibility.

The Network Controller is installed in the local network as a natural complement to routers, switches and firewalls already in place. It interfaces with the network control services (DNS, DHCP, RADIUS, SIP). Easily integrated into existing network infrastructure and solutions, it detects connected devices and users in real-time, analyses their behavior and acts automatically to optimize network security. It brings an unequaled combination of visibility and control to enterprise network environments.

The Network Controller is available in a range of software editions adapted to the specific needs of each vertical market : Enterprises, Systems Integrators, Managed Service Providers, and Hosting Providers. Optionally, the software solution may be preloaded onto a range of physical appliances