Networking infrastructure

Prerequisites

To deploy 802.1X within your organisation you will require suitable infrastructure capable of supporting it.

You will require at least one RADIUS server which is accessible by all Authenticator PAEs (switches and access points). However, as the RADIUS server is integral to authenticating your organisation will most likely require multiple redundant RADIUS servers for business continuity purposes; the number of which depends upon the size of the organisation and the number of clients being authenticated. The location of RADIUS servers needs to be carefully considered as authentication traffic from all devices will be handled by these servers.

Switches

To offer 802.1X, your organisation will require edge switches which are capable of providing 802.1X port control. For most organisations with full managed switching architecture this should not be an issue. However older managed switches (incapable of 802.1X), unmanaged switches and hubs will need to be replaced with new modern equipment. Finally the software and firmware on switches may need to be upgraded to the latest versions to provide full compatibility; some older device firmware may only have partial 802.1X support.

Cisco® Catalyst Switches

Cisco® Catalyst switches offer the ability to control edge port access by using 802.1X to authenticate, authorise and provide accounting for the client. This can be configured through a terminal connection to the switch.

Please note: All examples use private IP address ranges; you will need to change these for the relevant network infrastructure at your site.

To configure a Catalyst switch the RADIUS servers must first be defined in the switch configuration together with their shared secrets. An entry must be added for each of your organisation’s RADIUS servers. To do this type:

switch# conf t

switch(config)# radius-server host 192.168.10.50 auth-port 1812 acct-port 1813 key <shared_secret>

After adding RADIUS server definitions, global settings need to be added for the RADIUS

servers. Add entries for the timeout between the switch and the server, as well as the maximum number of retries and how many minutes to cease communications to a dead server. Finally instruct the switch to allow the sending of vendor specific attributes for authentication:

switch(config)# radius-server timeout 2

switch(config)# radius-server deadtime 1

switch(config)# radius-server retransmit 0

switch(config)# radius-server vsa send authentication

The next step is to enable AAA login and configure an AAA model for the RADIUS servers:

switch(config)# aaa new-model

switch(config)# aaa group server radius RADIUS-SERVERS

switch(config-sg-radius)# server 192.168.10.50 auth-port 1812

acct-port 1813

switch(config-sg-radius)# aaa authentication dot1x default group RADIUS-SERVERS

switch(config)# aaa authorization network default group RADIUS-SERVERS

switch(config)# aaa accounting dot1x default start-stop group RADIUS-SERVERS

After creating definitions for RADIUS servers and an AAA model, 802.1X can then be enabled on the switch:

switch(config)# dot1x system-auth-control

If required the switch can be configured to allow client supplicants to request a guest VLAN:

switch(config)# dot1x guest-vlan supplicant

After configuring the global settings for the switch individual, port settings need to be applied. First 802.1X needs to be enabled per port, and the switch configured to initiate an 802.1X authentication when a client plugs in and not wait for the client to initiate an authentication:

switch(config)# int range fa0/1 – 48

switch(config-if-range)# dot1x pae authenticator

switch(config-if-range)# dot1x port-control auto

The next option to set is the behaviour of an authenticated port. This will set whether the switch will allow multiple devices or a single device (or a multi domain) to connect:

switch(config-if-range)# dot1x host-mode single-host

To configure periodic reauthentication and set the number of times the switch will request authentication from the client. The final line will set the switch to honour the session timeout value set by the RADIUS server:

switch(config-if-range)# dot1x max-req 1

switch(config-if-range)# dot1x max-reauth-req 1

switch(config-if-range)# dot1x reauthentication

switch(config-if-range)# dot1x timeout reauth-period server

To set the guest and authentication failure VLANs:

switch(config-if-range)# dot1x guest-vlan 301

switch(config-if-range)# dot1x auth-fail vlan 301

Finally to set timeouts for the various 802.1X settings:

switch(config-if-range)# dot1x timeout quiet-period 5

switch(config-if-range)# dot1x timeout server-timeout 5

switch(config-if-range)# dot1x timeout tx-period 5

switch(config-if-range)# dot1x timeout supp-timeout 5

More information on Cisco® configuration can be found within the technical paper ‘Configuring 802.1X Port-Based Authentication’ on their technical support site:

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/
[1]

Wireless Networks

You are most likely to see 802.1X deployment alongside 802.11 wireless networking in enterprise sites, such as a university or large college. This additional layer of protection is essential due to the inherent insecurity of wireless networks not using a physical medium, in this case a cable. There are various solutions within the marketplace that attempt to address the wireless network security issue; however it is difficult to mitigate all the risks with wireless technology without fully implementing 802.1X.

To use the argument that user experience should negate 802.1X as a deployment strategy is not likely to benefit the organisation in the long term. The advantages of a fully deployed 802.1X client or supplicant will allow users to take advantage of the JANET Roaming service at other participating organisations as well as enjoying a secure wireless networking experience at their home site.

Links

[1] http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/Sw802