

How to Handle NAC Exceptions

The IEEE 802.1X standard gets all of the attention when NAC is discussed because it works well, and consistently, across many networking vendor's hardware. NAC deployments often depend on 802.1X both for authentication of the end-user and as a mechanism to tunnel end-point posture assessment information. IEEE 802.1X is a key strategy for interoperable and standards-based NAC deployments. Most network engineers understand that some devices can't be full NAC clients with 802.1X support, but what is surprising is that dealing with these "NAC Exception" devices will consume a disproportionate amount of time. The 20% of devices that can't run 802.1X may end up burning 80% of your design and deployment time.

Two strategies for handling non-802.1X devices including MAC-based authentication (typically used with printers, phones, and other embedded devices) and Guest VLAN (typically used with guests, but can also have applicability with employees and contractors).

MAC Authentication

When a host does not have an IEEE 802.1X supplicant, there is another option you can use to identify and authenticate the host: the MAC address. Upon timeout of an 802.1X challenge, enterprise-class network access devices, such as switches and wireless access points, can be configured to request an authentication using the MAC address of the device as a username. If you have a database of MAC addresses (or sometimes just MAC address prefixes, such as the brand of VoIP phone used in your organization), you can use MAC Authentication to allow access to devices that do not have 802.1X. Because MAC Authentication is done using RADIUS, devices authenticated based on their MAC address can be assigned to particular VLANs, just as any fully 802.1X-compliant device can be. By maintaining appropriate network access restrictions on these network segments you can achieve an effective alternative to IEEE 802.1X.

The obvious problem with MAC authentication is that MAC addresses are very easy to forge, or "spoof". It's trivial to emulate or even change your MAC address into one that you picked up from a nearby printer or even IP phone sitting on a desk. Network administrators also know that discovering, creating, and maintaining an inventory of asset MAC addresses is not easy. Fortunately, there are vendors that make tools to help automate the initial discovery and ongoing categorization process of MAC addresses.

Default Guest Access

If a client device isn't in the MAC Authentication database, all is not lost: enterprise-class network access devices have yet another option to try and get the user onto the network. Traditionally, the default configuration for a network device would be to fail "closed." In other words, if a client device without 802.1X ignored 802.1X challenges, and if the MAC authentication failed, then the network device would keep the port in a default, unconfigured VLAN without network connectivity, isolating the user completely from the network.

When deploying NAC, this switch behavior can be used to provide basic Internet access for guest users (if the enterprise wants to provide Internet access, of course). When providing guest access, the best practice is to require some type of user login via a web-based captive portal. Even if the authentication is "null" (i.e., no username/password needed), most enterprises use this as an opportunity to make the user aware of an acceptable use policy. In some NAC products, the browser connection is also an opportunity to try and posture-check the guest user (again, if desired by the enterprise). A second best practice is to direct all guest user traffic through an intrusion prevention system (IPS) to prevent an infected guest computer from making you the source of an attack.

Environments that do not provide guest access may also find the guest VLAN functionality useful for support reasons. Rather than leaving a client device blocked after failing to authenticate, the port may be opened to a

guest VLAN that contains only a support server. In this case, the client device has access to resources on the support server (typically via a captive portal) but has no other network permissions.

Exception Handling Options

To help you better understand many of the gotchas when deploying NAC, we have created a summary of typical networking devices and scenarios and how best to handle them when 802.1X can't help you.

Scenario	Description	Recommendation
Identity-only host supplicants (typically may include 802.1X, but no posture checking)	Older supplicants only provide identity credentials and do not support the newer protocols or security assessment credentials for NAC.	Allow backwards compatibility in your NAC policy to allow identity-only hosts to still access the network.
PDA's	PDA's with 802.11a/b/g/n wireless capabilities are becoming more common.	Try using 802.1X to authenticate them otherwise, use MAC authentication. Any MAC-authenticated device should be on a separate VLAN that is firewalled and only allows expected types of traffic flows.
Agentless host	Network-attached devices that do not or cannot have an 802.1X supplicant: IP phones, printers, photocopiers, IP cameras, specialized appliances and many, many others	Use MAC authentication to identify and categorize the device for network access. (see note on MAC authentication under PDA's, above)
Guests	Any unauthenticated hosts including visitors, anyone without a supplicant, employees who failed authentication, and unknown agentless hosts.	By default, place all unauthenticated hosts into Guest VLAN. Use captive portal to authenticate; use IPS to protect.
Multi-host: IP phones	Most IP phones have at least one port for an attached computer, violating the IEEE 802.1X specification of one host per port.	Enable "multi-host" switch capabilities. Phones may not proxy 802.1X Logon/Logoff messages to the PC.
Multi-host: hubs	Hubs allow up to 12, 24, or even 48 physical devices to attach to a single switch port, again violating 802.1X.	Enable "multi-host" switch capabilities to individually authenticate each device attaching. Otherwise the port will be locked in accordance with 802.1X.
Multi-host: VMware	Virtual machines are popular for software development and PC emulation on an Apple Macintosh.	Enable "multi-host" switch capabilities, but be aware that the VMware host itself may only expose a single MAC address.
Pre-eXecution boot Environment (PXE boot)	PXE is a common BIOS feature that allows computers to be booted remotely over the network for re-imaging or backup tasks.	Lower 802.1X timeouts and retries to expire before the PXE DHCP request times out (typically 60 seconds or less).
Old Hardware	Short 802.1X timeouts can expire before the supplicant is loaded on older hardware with modern, fully-patched operating systems.	Ensure 802.1X timeouts and retries are high enough so older machines do not fall back to agentless handling.