



Deploying and Managing the 802.1X Network with Beacon

Endpoint Profiling allows the rapid deployment of 802.1X and secures access for Non-EAP endpoints

One of the most often overlooked or underestimated requirements of deploying and managing 802.1X authentication in the enterprise LAN is the accommodation and management of endpoints that are not 802.1X capable. Today's enterprise data network supports a myriad of different devices, including Printers, VOIP phones, HVAC systems, and building access control readers. The location of these endpoints is seldom accurately documented and with the widespread adoption of DHCP, it has become more common in many environments for devices to be added to the network without the approval or knowledge of the IT staff. For endpoints that either do not have an 802.1X client (called a supplicant in the 802.1X standard) available or are unable to successfully authenticate via 802.1X for other reasons, steps must be taken to ensure that these endpoints can still access the network reliably without diminishing the value of deploying a strong authentication system.

The implementation of 802.1X authentication changes way all network endpoints access the network. As a result, one of the first tasks required in planning a deployment is determining what devices are connected to the access ports, and what their respective capabilities are in supporting client-side 802.1X authentication. Few enterprises have the processes in place necessary to maintain documentation of what every endpoint device in the environment is, and on what physical port of the edge infrastructure it is utilizing at any given time—let alone the type of device and its capabilities. Performing a manual site-survey to gather this information even in networks of relatively modest scale can be labor intensive and subject to error.

Enabling the realistic deployment of 802.1X

The Beacon System from Great Bay Software, Inc. is a solution that supports the effective deployment and ongoing management of 802.1X authentication in enterprise networks. The primary functions provided by Beacon are Endpoint Profiling and Behavior Monitoring. Endpoint Profiling addresses the challenge outlined in the paragraphs above and more. Essentially it provides a highly reliable and automated solution for discovering and gathering critical information about each and every endpoint connected to the network, regardless of device type or capability. Behavior Monitoring allows non-EAP host behavior to be tracked so that if someone attempts to subvert the authentication system by spoofing a MAC address of a printer or phone or simply swaps the port with one of these devices that network administrator can be alerted and that port or endpoint can be quarantined, or removed from the network

Unlike other tools that simply determine that an endpoint is connected to an access port, the Endpoint Profiling functionality of Beacon gathers the data about each endpoint necessary for the successful planning and implementation of 802.1X authentication. Specifically, Endpoint Profiling determines the operational/behavioral characteristics of the device; how it is using the network resources (e.g., a desktop computer running Windows and supporting users) or providing services on the network (e.g., a network-attached printer.) In addition, it determines on what port of what device the endpoint is currently connected to and the history of that device over time.

This information is critical in the determination of what has to be done to accommodate each endpoint as 802.1X is implemented. The most critical capability of Beacon in this regard is the identification and location of the endpoints that will *not* support an 802.1X supplicant and cannot be authenticated via 802.1X. These endpoints require that other measures to be put in place to support their access to the network once 802.1X enabled—they will not use the EAP protocol for authentication, and will need to rely on some alternative mechanism to provide secure access.

Authentication for non-authenticating hosts

In many cases, the alternative means of authentication for non-802.1X capable endpoints is to utilize the physical address (MAC address) of the LAN adapter of the device as a unique identifier for some level of authentication. This is commonly referred to as MAC-based authentication. In order to support MAC-based authentication of non-802.1X devices, the edge devices must have the capability to recognize the a non-802.1X capable station attempting to connect on a port, and request that the authentication server make an authentication decision based on the MAC address of the station.¹ In addition, MAC authentication requires that the Authentication Server either be configured with the list of MAC addresses of known devices that are to be provided network access through MAC authentication itself, or be configured to proxy the authentication decision to another system where a list of the non-EAP hosts is stored.

The Beacon Endpoint Profiling capability can be used to automate the discovery, location and identification of endpoints as the 802.1X implementation is planned. Additionally, it can also be utilized in the final implementation to serve as the non-EAP endpoint directory, much in the way Microsoft's Active Directory would serve as the data store for endpoints that will authenticated via EAP.

By virtue of the LDAP functionality included with Beacon, the authentication server can proxy the MAC authentication decision to the Beacon system as an alternative to importing the list of authorized MACs from Beacon into the authentication server database. In many cases, using the LDAP functionality and configuring the authentication to proxy MAC authentication decisions to Beacon is the preferable deployment model. Having Beacon make the MAC authentication decision takes full advantage of the Behavior Monitoring capabilities of Beacon, providing a much more dynamic and inherently more secure approach to MAC authentication as the method of

¹ This functionality varies significantly in implementation from vendor-to-vendor. It is recommended that the reader check the documentation of the specific switch and firmware version in place to determine how devices that are non-802.1X capable are handled, as well as options if 802.1X authentication is attempted by the endpoint and subsequently fails.

choice for supporting non-802.1X capable devices. The advantages of fully utilizing the behavior monitoring capabilities and proxy support in Beacon are outlined in detail in the remainder of the document.

The endpoint Behavior Monitoring capability of Beacon utilizes the Endpoint Profiling functionality to assist in the ongoing management of 802.1X authentication in enterprise networks. Essentially, this capability involves monitoring behaviors on the network edge to detect changes—either new devices being seen on the network or a device exhibiting behaviors that are inconsistent with its current profile alerting network operations and security staff that an investigation is necessary prior to continuing to allow the device access to the network based on MAC address.

Enterprise networks are inherently dynamic and constantly changing as new devices are added to the environment, and others are retired from service. As new 802.1X capable devices are added to the environment, assuming they are configured with the proper credentials, they are able to access the network automatically by completing the 802.1X authentication process. Access for these devices is in principle, self-provisioning.

When new non-802.1X capable devices are added to the environment, for example, a network printer is swapped with a replacement while the other is out for repairs; the process is far from automated. Without a Beacon system in the environment, the MAC address of the replacement printer would have to be determined and registered in the authentication server to enable the MAC authentication of the new device. Up until that point, the new printer would have been isolated from the network. The frequent changes common in enterprise networks necessitate that an automated detection and Endpoint Profiling capability be in place that continually updates the database of stations that should be admitted to the network; Beacon provides this capability.

Behavior Monitoring secure non-authenticating hosts

An important additional consideration is the fact that without some means of dynamically maintaining the validity of each device on the list of authorized MAC addresses, the potential exists for unauthorized access through the “spoofing” or cloning of a MAC known to be authorized by another device. Most or all of the commercially available MAC-based authentication mechanisms suffer from this limitation. Essentially, once a MAC address is added to the list of endpoints to be allowed onto the network, any station using that MAC address will be able to access the network. MAC authentication is based on a single challenge, username (MAC address) only with no other credential required to verify the “identity” of the device (e.g., that the device authenticating at that moment is the device provisioned for access via MAC authentication originally). Utilities to change the MAC address of some devices are widely available, and “MAC address cloning” is often supported in the standard firmware images of home routers and router/WLAN access points.

Beacon can be configured to monitor the behavior of the endpoints being authenticated via MAC-based authentication to proactively detect changes that are indicative that the endpoint device type has changed. For example, if an endpoint that was previously profiled as a printer is observed by Beacon to be running a browser to go to the

Internet, this aspect of the endpoints behavior is a very reliable indicator that something has changed with that device and should be investigated further. Accordingly, the station should have its network access suspended until the reasons for the change in endpoint behavior are fully understood.

Beacon Behavior Monitoring adds a credential-like component to the MAC authentication mechanism that is difficult to defeat. By using the LDAP capability and letting the Beacon System make the MAC authentication decision by proxy, the decision to admit is always based on the most currently available behavior information for that endpoint, not a semi-static list of MAC addresses maintained manually and without context. Because Beacon is using information gleaned at higher levels of the OSI stack, the behavioral attributes it uses to profile endpoints is extremely difficult to spoof. When Beacon is used as the proxy for MAC-based authentication decisions, this capability is easily configured and utilized to enable username- (MAC address) *and* credential (behavior)-based authentication of non-802.1X endpoints based on the best information available. This is arguably a significant enhancement to any MAC-based authentication implementation.

Conclusion

Endpoint Profiling is an important aspect of preparing the network for the deployment of Network Admission Control. Great Bay Software provides a solution that dramatically reduces the time to deploy and the cost of ongoing administering the system as well as enhancing the security and monitoring capabilities for the non-NAC endpoints. Leveraging the Endpoint Profiling data also allows Beacon to perform Behavioral Monitoring of the network endpoints so that events such as MAC Spoofing and port swapping are not permitted in the authenticated network. This combination positions Beacon as a system that provides value leading up to deployment time as well as simplifying the ongoing administrative tasks of maintaining the authenticated network.

For more information, please contact us at:

Phone - 800.503.1715

info@greatbaysoftware.com