



CAROLINA ADVANCED DIGITAL, INC
IT INFRASTRUCTURE | SECURITY | MANAGEMENT

www.cadinc.com | 800.435.2212

802.1X AND NAC: BEST PRACTICES FOR EFFECTIVE NETWORK ACCESS CONTROL

NAC Extends 802.1X to Achieve Network-wide Security, Control and Visibility

- **Introduction**.....1
- **802.1X Basics**1
 - › Key Elements
 - › How It Works
 - › Benefits
 - › Limitations and Challenges
- **NAC Basics**.....4
 - › Key Elements
 - › How It Works
 - › Benefits
 - › Limitations and Challenges
- **Conclusion**.....8
- **References**.....8
- **About Bradford Networks**.....8



INTRODUCTION

IEEE 802.1X is an IEEE (Institute of Electrical and Electronics Engineers) standard for port-based network access control. Its main purpose is to provide an authentication mechanism for devices and users attempting to connect to wired and wireless LANs so that only authorized connections are allowed.

Network Access Control (NAC) is a term that has been widely adopted for solutions that provide both authentication of users and devices – much like 802.1X – as well as validation of the security posture of devices attempting to connect to a network.

There is often confusion between the functions and benefits of 802.1X and those of commercially available NAC solutions, leading one to wonder which one is best for securing access to a particular network environment. This paper explores the fundamentals of 802.1X and NAC technologies, and explains why a combination of both is often required to provide the level of security, control and visibility needed in today's networks.

802.1X BASICS

The 802.1X standard was first published in 2001 (IEEE Std 802.1X-2001) and later updated in 2004 (IEEE Std 802.1X-2004). Further updates were drafted in 2010 (IEEE Std 802.1X-2010), but have not yet been published by the IEEE as of the date of this whitepaper, so 802.1X-2004 is the active standard.

The published document for 802.1X-2004 is 179 pages in length and fairly technical. As such, the intent of this whitepaper is not to cover the standard in detail, but to describe at a high level its purpose, key elements, how it works, and its benefits and limitations.

Key Elements

The key elements of 802.1X, as depicted in Figure 1, include the supplicant, the authenticator, the authentication server and EAPoL (Extensible Authentication Protocol over LAN). We will describe each of these elements briefly and then discuss how they all work together in 802.1X.

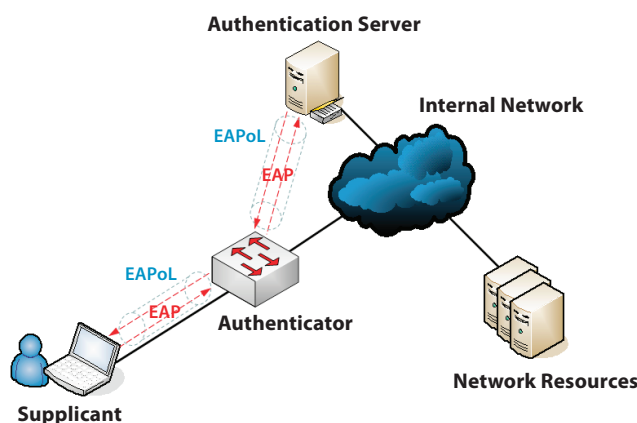


Figure 1: Elements of IEEE 802.1X

SUPPLICANT

The term supplicant is used in two different ways within 802.1X. It refers to the endpoint (or client) device attempting to connect to a network, and is also used to refer to client software that is required on endpoint devices in order to participate in the 802.1X authentication process.

AUTHENTICATOR

The authenticator is a network device – a managed switch or wireless access point – that facilitates authentication by relaying credentials between the supplicant and authentication server. Access control also occurs at the authenticator, whereby a port will remain in an “unauthorized” state (not allowing access) prior to authentication occurring, and the port will be changed to an “authorized” state (allowing access) after successful authentication occurs.

AUTHENTICATION SERVER

The authentication server – typically a RADIUS server – validates the credentials of the supplicant requesting access. Credentials might include username/password, digital certificate or other methods.

EAP / EAPoL

The authentication framework used by 802.1X is a protocol called EAP (Extensible Authentication Protocol), or EAPoL (EAP over LAN), which allows a number of different authentication methods to be used. EAP or EAPoL can be thought of as the “language” that is used by supplicants, authenticators, and authentication servers in 802.1X.

In Layman's Terms

For a simplified example of the 802.1X process and its key elements, consider the analogy of a patron approaching the door of a private night club. The patron wanting to get into the club is the supplicant in 802.1X.

The patron may be asked for identification by a security guard at the door who will either allow entry or not, after checking to see if the patron is on an authorized member list or guest list. The security guard is the authenticator in 802.1X.

The security guard may call in to the club manager to confirm whether the patron is authorized to enter. The club manager (the keeper of the list) is the authentication server in 802.1X.

Finally, in the simplest terms, the language that everyone uses for communicating throughout this process is analogous to EAPoL, the protocol used in 802.1X.

How It Works

802.1X is port based, meaning that it enforces access control at the “port” (or point of connection) to the network. For wired LANs, control is enforced at each managed switch port. For wireless LANs, control is enforced at each wireless Access Point (AP).

802.1X provides pre-connect (or pre-admission) access control, requiring authentication of devices and/or users before a connection to the network is authorized. As a result, in an 802.1X environment, all network ports default to an unauthorized state prior to authentication. A port is dynamically changed to an authorized state after successful authentication occurs.

In simple terms, referring to the elements in Figure 1, the 802.1X authentication process is as follows:

1. Authenticator (switch or AP) sends an EAP-Request message
2. Supplicant replies with an EAP-Response message
3. Authenticator forwards the EAP-Response to authentication server
4. Authentication server issues a challenge request to the supplicant
5. Supplicant replies to the challenge (proxied through authenticator)
6. Authentication server accepts or rejects the supplicant's credentials
 - If accepted, authenticator changes port to authorized state
 - If rejected, authenticator changes port to unauthorized state
7. When the network connection is terminated or times out, the port is returned to an unauthorized state and the process repeats for future connection attempts

The description above is a bit oversimplified, but gives a general outline of the 802.1X process. Using 802.1X, authentication can be a one-time process (so that once a connection is authorized it remains authorized until the connection is terminated by the supplicant), or re-authentication may be required after a specified time interval. Network connections can also be configured to time out and then force re-authentication for any new connections.

802.1X can also enforce role-based, or identity-based, access control by leveraging RADIUS attributes during authentication such that a user's identity or group membership is used in determining the level of network access allowed. This is typically accomplished by assigning VLAN membership – so, for example, employees can be placed in one VLAN while guests are placed in a different VLAN.

Benefits

802.1X is an IEEE standard originally published nearly ten years ago, and as a result it is supported (at least to some extent) almost universally by today's network infrastructure devices – managed switches, wireless access points and controllers, etc. While some inconsistencies still exist among different manufacturers' products, once can be reasonably confident that network infrastructure purchased today or even in the past few years should be 802.1X-capable.

Similarly, most personal computers and laptops have featured embedded 802.1X supplicant software for several years, and there are many commercially available and open-source supplicant software offerings on the market for most popular operating systems.

Encryption of Wireless Keys

For wireless networks, 802.1X enables secure encrypted communications over the air through the use of dynamic keying. In these environments, the authentication server is responsible for providing key material to both the authenticator and the supplicant in order to take advantage of dynamic WPA/WPA2 security. Without 802.1X, management and distribution of keys is much more difficult and error-prone.

Strong Authentication

802.1X delivers security benefits by enabling strong authentication mechanisms through the use of EAPoL. EAPoL leverages various standard authentication mechanisms, which provides choice and flexibility for organizations to deploy the mechanism (or mechanisms) best suited to their particular environment and security requirements.

Secure Access Control

Network security is further enhanced with 802.1X since it forces authentication to occur before network access is permitted. All ports or points of access to the network can be configured to remain in an unauthorized state until successful authentication is completed, which helps to ensure that only authorized (successfully authenticated) users and devices are permitted onto the network.

As discussed previously, 802.1X also allows the flexibility of role-based access control by enabling dynamic VLAN assignment during the authentication process, allowing different levels of network access based on the identity of the authenticated user.

Limitations and Challenges

Complexity in deploying and managing 802.1X, particularly in wired LANs for reasons discussed below, is perhaps the greatest challenge which limits its widespread adoption. 802.1X also has inherent design limitations – particularly its dependence on supplicant software on endpoints – that reduce the benefits it can otherwise offer.

Further, there are important network security considerations that are simply outside the scope of 802.1X, which means that other solutions are required – either in addition to or in place of 802.1X – in order to address those needs. Examples include endpoint-compliance verification (posture checking) and post-connect compliance monitoring of network connections and endpoints.

802.1X Deployment Lags in Wired LANs

802.1X is used extensively in wireless LANs today, but is much less prevalent in wired LANs. In wireless LANs, driving factors for 802.1X adoption have been the widespread use of EAP / RADIUS authentication, and the fact that EAPoL supports encrypted transmission of security key information between authenticators and supplicants (as discussed previously). Further, most devices that commonly connect to wireless LANs – predominantly laptops, but increasingly tablets and smartphones – tend to have 802.1X supplicant software.

In wired LANs, there are still a number of challenges that make 802.1X deployment complex and costly. In some cases, legacy switches or other network infrastructure devices lack 802.1X support. More commonly, switches from different manufacturers are inconsistent in the way they must be configured to support 802.1X, particularly in how they handle mixed environments of 802.1X and non-802.1X endpoints. This and other factors make initial configuration and ongoing management of 802.1X in wired LANs very resource intensive – and therefore expensive.

Wired LANs also tend to support a greater variety of legacy endpoints, many of which do not support 802.1X supplicant software. The number of non-802.1X endpoints in wired LANs often exceeds 802.1X-capable ones. As mentioned above, it is challenging to configure different switches (particularly in multi-vendor networks) to handle a mix of both 802.1X and non-802.1X endpoints. The combination of these factors in wired environments can outweigh the intended benefits of deploying 802.1X in the first place.

Factors Limiting 802.1X Deployment in Wired LANs

- Legacy switches and unmanaged devices lack 802.1X support
- Configuration challenges in multi-vendor networks
- High proportion of non-802.1X endpoints
- Resource-intensive (and therefore costly) to configure and maintain

Dependence on Supplicants

802.1X requires supplicant software on endpoint devices so that they can participate in the authentication process. This is fine for traditional endpoints like PCs and laptops, and even newer devices like increasingly tablets and smartphones, for which supplicant software is commonly available.

However, many endpoint devices do not support supplicant software and therefore cannot participate in the 802.1X authentication process. Examples include devices such as those used for physical security in many facilities, including surveillance cameras, ID card readers, entry keypads and the like.



Various industries such as manufacturing, retail, healthcare, energy and many others support unique types of endpoints in their networks for which 802.1X supplicant software is not available. In many environments, non-802.1X endpoints can far outnumber 802.1X-capable ones.

As a result, a significant challenge for implementing 802.1X in many networks involves what to do about all the non-802.1X endpoints and how to handle network connectivity for those devices. There are options and workarounds, but each one involves some compromise in terms of network security and/or management complexity.

Options for Handling Non-802.1X Endpoints

- Deny All (not realistic!)
- Whitelist All (not secure!)
- MAC Authentication Bypass (doable, but manually intensive)

One option (though seldom feasible) is to simply deny network access to all non-802.1X endpoints. For most organizations this is really not an option since many of the non-802.1X endpoints are critical to business operations. Machines on a manufacturing floor, cash registers in a retail store, heart monitors and other patient care devices in a hospital – all must be allowed on the network. So denying access for these and other non-802.1X endpoints is typically not realistic.

Another option is to whitelist all non-802.1X endpoints so they are automatically allowed onto the network. This approach bypasses 802.1X authentication for devices that are not able to participate, effectively defeating the purpose of attempting to secure network access with 802.1X in the first place. Some organizations will employ this approach on specific network ports if they are reasonably confident that only authorized devices would be able to be connected to those ports. However, this can involve a great deal of manual configuration on the network and also jeopardize network security.

A third option is to use MAC Authentication (or MAC Authentication Bypass), which many network infrastructure devices support. In this case, if the authenticator (switch or wireless access point) finds that an endpoint is not responding to 802.1X EAP-Request messages, it can attempt to authenticate the endpoint using just its MAC address. In other words, it can check with the authentication server to see if the MAC address is included in a list of authorized MAC addresses.

While MAC authentication is probably the best alternative for handling non-802.1X endpoints, it too can involve a great deal of manual configuration on the network as well as significant tradeoffs in security. Configuration requirements for MAC authentication vary widely for

network infrastructure from different manufacturers, which makes the initial setup and ongoing management difficult. From a security perspective, MAC authentication relies only on the MAC address of the endpoint, which can be spoofed by savvy users and hackers, making it much less secure than most of the authentication methods enabled by EAPoL used in 802.1X.

Lack of Endpoint Posture Checking

Validation of the security posture of endpoint devices is outside the scope of 802.1X. So, while 802.1X ensures that users and devices are *known* by authenticating them, it does not provide a means for determining whether they are *safe* and in compliance with an organization's security policies.

Validating the security posture of endpoints can answer questions like the following:

- Are endpoint devices running an approved operating system (OS)?
- Are endpoint devices up-to-date with security patches?
- Are anti-virus/anti-spyware tools up-to-date and running?
- Are all mandatory applications installed and running?
- Are any prohibited applications/processes present?

This information, in addition to authenticating the endpoint device and/or its user, is important to determine before allowing access to the network. Even authorized users can unknowingly bring “unsafe” devices onto the network, which can then put the entire network and the organization at risk.

For example, an employee's laptop that has not been updated with the latest anti-virus / anti-spyware updates can introduce the risk of propagating viruses and other malware that can take an entire network down or expose confidential information outside of the organization.

Checking the security posture of endpoints to ensure they are in compliance with security policies before allowing access is an important step in securing the network and is not addressed by 802.1X.

Consider This

Relying only on 802.1X for network access control without endpoint posture checking is analogous to having airport security screeners check only for passenger IDs without scanning passenger baggage for potential threats.

Lack of Monitoring or Post-Connect Functions

The job of 802.1X is essentially done after authentication is completed and an authorized connection to the network is established. There are options to periodically re-authenticate users and devices with 802.1X, but what happens *after* they are allowed to connect? How do you monitor the compliance state or behavior of a particular user or device to protect against potential risks after authentication (or re-authentication) is completed?

Like endpoint posture checking, post-connect monitoring for compliance issues, potential risks or anomalies is an important aspect of securing the network that is outside the scope of 802.1X. Best practices for network security require another layer of protection in addition to the authentication functions enabled by 802.1X.

NAC BASICS

NAC can take on many definitions and there are many different approaches. Unlike 802.1X, there is currently no universally supported standard for NAC, and most commercial NAC solutions utilize proprietary architectures and technologies.

In 2005, the Trusted Computing Group (TCG) published the Trusted Network Connect (TNC) Architecture for Interoperability as a standards-based model for NAC. TNC has been updated several times, with the most recent revisions published in 2009. While TNC is recognized as a standard model for NAC, it has yet to become widely adopted by vendors offering commercial NAC solutions.

There are also efforts underway by the Internet Engineering Task Force (IETF) Network Endpoint Assessment (NEA) working group to standardize portions of NAC – particularly aspects associated with endpoint compliance or posture assessment (discussed later in this section). However, those standards efforts are still underway and solutions based on NEA standards are therefore not widely deployed today.

Despite these standards efforts, at present the majority of NAC solutions on the market continue to utilize proprietary architectures and technologies. While solutions vary widely, NAC's primary functions are to provide authentication of users and devices connecting to a network, to validate the security posture of endpoint devices, and to enforce access policy controls. Some commercial NAC solutions provide additional functionality described later in this section.

Consider This

A useful analogy for NAC is the security screening process experienced in airports, which requires travelers to show identification credentials and have their baggage and personal belongings inspected before being allowed to access the gate areas where planes are boarded.

Key Elements

The TNC model for NAC defines specific physical and/or logical elements. These elements have some similarities to elements outlined by the 802.1X standard.

- Access Requestor (AR) – the endpoint device requesting access to the network
 - › The AR plays a similar role to the Supplicant in 802.1X
- Policy Enforcement Point (PEP) – the element that enforces controls (permits or blocks access)
 - › The PEP plays a similar role to the Authenticator in 802.1X
- Policy Decision Point (PDP) – the verifier, or the element that decides whether to grant access
 - › The PDP plays a similar role to the Authentication Server in 802.1X

While there are some similarities with 802.1X, one of the key differences with NAC and the TNC model is the concept of endpoint compliance checks to validate the security posture of endpoints as part of the decision criteria for whether to allow network access. As discussed previously, this is not part of 802.1X. Although few NAC solutions on the market today employ the TNC model directly, most do make use of elements that equate roughly to the functions of the AR, PEP, and PDP. However, since architectures vary considerably, it is better to discuss NAC elements in terms of the functions they provide, including: authentication, endpoint compliance validation, access policy enforcement and remediation.

AUTHENTICATION

Authentication in NAC is much the same as for 802.1X, and in fact NAC solutions can leverage 802.1X as well as other standard means of authentication that are already deployed in most networks today. NAC solutions typically integrate with existing directory systems (e.g., Active Directory, LDAP) and AAA servers (e.g., RADIUS). Some solutions offer the ability to host directory services directly on a NAC server or appliance, but this option is most commonly used only for guest user accounts.

ENDPOINT COMPLIANCE VALIDATION

Validating the security posture of endpoints may involve simple checks of operating system (OS) versions and patch levels, or it may be much more comprehensive. NAC solutions commonly check endpoints for the presence of anti-virus and anti-spyware tools and to make sure those tools include the latest updates and definitions. Some solutions go much further and can check for the presence of required and/or prohibited applications (such as peer-to-peer software), particular files or file types, or even a range of custom registry-level checks.

Endpoint Compliance Checks

- Operating system type, version, patch levels and hotfixes
- Anti-virus applications, updates and definitions
- Anti-spyware applications, updates and definitions
- Required and prohibited applications
- Presence and status of particular files or file types

Endpoint compliance checks may be performed using an agent (client software) that runs on endpoint devices and scans them, or via scans done over the network from a NAC server or appliance. NAC agents are discussed further in another section of this paper.

ACCESS POLICY ENFORCEMENT

The access control portion of NAC can be accomplished in a number of different ways, ranging from simply enabling or disabling physical switch ports and wireless connections (much like authorized and unauthorized port states in 802.1X) to the ability to enable very granular access policies.

Access policies may be tied to just authentication and endpoint compliance criteria, or they may be determined based on a combination of these and other criteria such as the identity or role of a user or device, physical location in the network, connection method (wired or wireless), time of day and other factors. These capabilities vary widely among different NAC solutions.

Many NAC solutions can accommodate role-based access policies, and much like with 802.1X this is often accomplished through the use of VLANs by dynamically changing the VLAN on a switch port or wireless access point based on a user's role or group membership (e.g., Finance, Engineering, Sales, etc.).

Methods used for enforcing access policies vary extensively depending on the architecture of the NAC solution. Some solutions enforce control at the point of access to the network (e.g., switch port or wireless access point), which is similar to enforcement used in 802.1X. Other solutions may enforce controls using software agents residing on endpoint devices, via inline appliances or gateways deployed in the network, or by manipulation of commonly used protocols in the network (e.g., TCP, DNS, DHCP).

QUARANTINE (ISOLATION) AND REMEDIATION

In addition to endpoint compliance validation, NAC also encompasses the concepts of quarantine (or isolation) and remediation. In the event that an endpoint device is found to be non-compliant with security policies – for example, one not having the latest security patches available for its OS – the device can be isolated on the network. Since the non-compliant device is considered to be at risk, network access will typically be significantly restricted to protect the network from threats or vulnerabilities that it may introduce.

A simple example to demonstrate this would be a network that uses a Production VLAN and an Isolation VLAN. Endpoints that are compliant with security policies would be given access to the Production VLAN, while non-compliant ones would be restricted to the Isolation VLAN.

While in isolation, non-compliant endpoints may be allowed very limited access to network resources for purposes of remediation – in other words, to fix their compliance issues. For example, they may have access to specific network servers for installing OS patches and updates, or they may be allowed access to specific websites to download and install updates to anti-virus and anti-spyware applications.

Like many functions of NAC solutions, remediation approaches differ. Some are highly automated and integrate with patch management servers and other systems deployed in the network, while others require more involvement on the part of users and/or IT staff. Ideally, remediation should be automated as much as possible to minimize any potential burden on users or IT.

Similarities and Differences of NAC and 802.1X

Similarities

- Strong authentication mechanisms
 - › 802.1X and NAC both leverage standard authentication mechanisms and directory systems
- Pre-connect enforcement of access policies
 - › All ports are set to unauthorized (or similar state) until successful authentication is completed
- Role-based access control
 - › Dynamic assignment of VLANs is typically used to control access levels for different types of users

Differences

- NAC provides endpoint compliance validation
 - › Security posture of endpoints is used in determining access policy
- NAC is not dependent on supplicants / supplicant software
 - › Some (but not all) solutions do employ agents or client software
- NAC can provide post-connect monitoring and controls
 - › Some solutions can monitor endpoints and/or network connections to ensure ongoing policy compliance
 - › Some solutions can react to outside stimulus from other security systems such as an IDS/IPS

How It Works

As highlighted previously, there are a number of different approaches and vendor implementations of NAC, and each works quite differently. Even so, we can discuss how some of the most common architectures work and how each attempts to deliver on the key elements of NAC.

NAC Architectures

A number of different architectures are employed by commercial NAC solutions. Common approaches include out-of-band, in-band (or inline), client-based (or agent-based), and others. There are also hybrid solutions which combine two or more approaches.

802.1X-BASED

Some NAC solutions rely mainly on 802.1X and add endpoint compliance checking via agents or server-based scans. However, these approaches have most of the same limitations and challenges as 802.1X alone.

OUT-OF-BAND

Out-of-band approaches interface with and control the network infrastructure in a similar way to 802.1X, without the dependency on 802.1X supplicants or the requirement of 802.1X support within the network infrastructure. Endpoint compliance checking is accomplished via agents or server-based scans. Out-of-band approaches tend to be the most scalable and flexible to implement. However, some may work with only a limited number of network infrastructure devices (some work with only one brand of devices), so the portfolio of supported devices should be researched prior to selecting an out-of-band solution.

IN-BAND (INLINE)

In-band, or inline, NAC solutions use servers or appliances that are deployed directly in the data path such that all network traffic needs to pass through them. Enforcement of access policies is done in a gateway fashion by forwarding or filtering network traffic. Endpoint compliance checking is accomplished via agents or server-based scans. In-band approaches do not scale well because of the need to process all network traffic. They can require deployment of numerous server appliances, and can require changes in IP address schemes as well as other network design or topology changes.

CLIENT-SIDE

Client-side NAC solutions rely heavily on client software (agents) installed on endpoint devices. Enforcement of access policies is done by manipulating protocols or configuration settings on the endpoint itself. Endpoint compliance checking is typically accomplished via agents as well. Dependence on agents severely limits the flexibility and effectiveness of these solutions, as not all endpoints on the network are able to run agents.

HYBRID

Hybrid NAC solutions combine two or more different approaches and are often the most complex to deploy and manage, since the deployment approach varies based on the network environment. For example, some hybrid solutions must be deployed in-band in certain areas of a network, while being deployed out-of-band in other areas. Separate server appliances are typically required for each deployment mode, and configuration and management can be complex.

Pre-Connect and Post-Connect Functions

Many NAC solutions provide both pre-connect (or pre-admission) and post-connect (or post-admission) functions – further differentiating them from 802.1X, which provides pre-connect authentication only. Nearly all NAC solutions provide pre-connect authentication to validate user and/or device identity along with some level of endpoint compliance checking to validate device security posture prior to allowing network access.

Post-connect functions may involve periodic re-authentication, ongoing monitoring of endpoint compliance (re-scanning or monitoring for any change in state), or ongoing monitoring of network activity to provide additional security checks throughout the network session. Some solutions can be integrated with other security systems (such as an IDS/IPS or other device) to enforce access controls based on anomalies or threats detected by those devices. The specific post-connect capabilities supported vary based on the architecture used.

The best scenario is to have both pre-connect and post-connect functions, in order to first ensure that network access is limited to only users and devices that are authorized and compliant with security policies to begin with, and then to be able to ensure that users and devices stay compliant while connected to the network.

NAC Agents

Agents are commonly used for endpoint compliance validation (although some NAC solutions leverage agents for much more. When no agent is used, the alternative – referred to as agent-less – typically involves remote scanning of endpoints from a server or appliance somewhere in the network. For those solutions that do utilize agents, there are two common types: persistent agents and dissolvable agents.

PERSISTENT AGENT

Agent software is installed on endpoint devices and remains installed, running in the background (much like anti-virus software does). Persistent agents are effective for both pre-connect and post-connect scanning and monitoring. They can run transparently on endpoints without requiring user input or otherwise disrupting productivity. However, like most software applications, they do typically require administrative rights to be installed on endpoint devices.

DISSOLVABLE AGENT

(Also referred to as Web Agent or On-Demand Agent). Agent software is downloaded on-demand, most often from a web-based portal, and is executed on the endpoint device. The agent typically runs only once and then deletes itself from the system. Dissolvable agents are effective for pre-connect scanning, but post-connect use involves disruption of a user's network connection (e.g., redirecting to a captive web portal to again download and run the agent). Dissolvable agents generally do not require administrative rights in order to be run on endpoint devices, so they are preferable for use on unmanaged devices, such as those belonging to guest users.

The specific capabilities of agents vary widely among NAC solutions. Some provide only basic endpoint compliance checks to validate the OS version, patch levels, and the presence of up-to-date anti-virus and anti-spyware tools. Others may go much further and check for the presence of required and/or prohibited applications, particular files or file types, or even a range of custom registry-level checks.

In addition to endpoint compliance validation, some solutions (as noted previously) also utilize agents directly in the enforcement of access policies by manipulating protocols or configuration settings on the endpoint itself. However, the effectiveness of those solutions is extremely limited for the same reason as the reliance on supplicants limits the effectiveness of 802.1X, since many endpoint devices will not support the use of agents or supplicants.

Benefits

NAC delivers similar benefits to 802.1X in terms of authenticating users and devices before allowing access to wired and wireless LANs, as well as enabling role-based access through the use of dynamic assignment of VLANs. This is where the similarities end, however, and where the added benefits of NAC become evident.

Additional benefits of NAC include the ability to provide endpoint compliance (security posture) validation and to provide both pre-connect and post-connect security functions. Advanced NAC solutions can add further benefits, including greater visibility throughout the network of all users and devices, dynamic profiling of endpoint devices, comprehensive guest management, as well as detailed logging, reporting, and audit trails of network connection activity – all of which can provide tremendous value in day-to-day management of network security and in complying with industry and government regulations for data security.

It should be noted, however, that these functions vary considerably for different NAC solutions on the market, so some research is necessary before selecting a solution based on one or more of these benefits.

Network Visibility

In order to provide secure access control and to prevent unauthorized connections to the network, an effective NAC solution must have awareness of any and all users and devices that attempt to connect via any point of access – wired or wireless. As a result, NAC can provide valuable visibility across the network for tracking and monitoring network connections, delivering both real-time and historical data about the network topology, users, and endpoint devices.

NETWORK TOPOLOGY

Mapping of all network infrastructure devices and all available points of access to the network.

USERS

Tracking of access by all employees, staff, guests / contractors, as well as failed access attempts by unauthorized users.

ENDPOINT DEVICES

Tracking of all authorized endpoint devices including PCs, laptops, IP phones, smartphones / handhelds, and other IP-enabled devices, as well as failed access attempts by rogue devices.

Logging, Reporting, and Audit Trail Data

The data above can be accessible via a centralized system with graphical views, reports, detailed logs and audit trails. This data is extremely valuable for day-to-day network management, for strategic planning, and to help ensure compliance with regulatory requirements, which can otherwise create a significant burden on IT staff.

Device Profiling

Some advanced NAC solutions offer the capability to automatically profile or classify endpoint devices by type, allowing devices to be accurately identified when connecting to the network and to then be given appropriate network access privileges.

Profiling methods typically leverage information such as MAC address, IP address, DHCP fingerprint, open TCP or UDP ports, location (point of network access), and others. Multiple methods may be used together in a profile to increase the confidence in accurate device identification and to prevent possible spoofing of individual pieces of information such as a MAC address.

Guest Management

Some NAC solutions offer comprehensive guest management features to automate provisioning of guest access and enforce role-based policies that an organization establishes for guests, contractors, business partners, or other non-employee users of the network.

One very beneficial feature in guest management involves the concept of sponsorship, in which non-technical employees and non-IT staff may be empowered as sponsors to create and manage guest access accounts according to policies defined by IT. The main benefits of guest sponsorship are that it alleviates IT staff of the burden associated with administering guest accounts, while enabling other employees and guest users to be as productive as possible with secure access to network resources.

Benefits of NAC over 802.1X

General

- No dependence on supplicant software
- Endpoint compliance (security posture) validation
- Pre-connect and post-connect access control functions

Advanced NAC Solutions

- Network-wide visibility of all users and devices
- Detailed logging, reporting and audit trails
- Dynamic profiling of endpoint devices
- Comprehensive guest management

Limitations and Challenges

As with 802.1X, there are many network security functions that are outside the scope of NAC as well, which means that other technologies are required for a comprehensive, defense-in-depth security solution. Fortunately, however, some NAC architectures – and in fact the TNC model itself with its IF-MAP protocol – allow for integration and data exchange among a variety of networking and security systems, which enables NAC and other technologies to work well together. Examples include integration of NAC with IDS/IPS, DLP, SIEM and other network security systems.

Perhaps the greatest challenge with NAC today is the lack of widely adopted standards, which leads to many different vendor approaches and different architectures. As noted previously, the TCG's TNC model is recognized as a standard model for NAC, but has yet to achieve widespread adoption in the market. This has not necessarily inhibited the deployment of NAC technology, but it does require a bit of due

diligence when contemplating NAC in order to select the architecture that is best for a particular organization and network environment. Areas that should receive particular attention when evaluating NAC architectures include dependence on agents, scalability, and flexibility – all of which can directly impact the effectiveness of a NAC solution as well as the level of complexity involved in deployment.

Dependence on Agents

Many NAC solutions feature agents, which are most commonly leveraged for scanning or assessment of the security posture of endpoints, as discussed previously. In these cases, agents may be optional components, and they are likely to be passive in nature – in other words, they are used to collect information from endpoints to assess compliance with security policies, but they are not otherwise involved in the process of enforcing access controls.

However, some NAC architectures are much more dependent on agents, and agents may be required (rather than optional) when used for more than gathering endpoint compliance data. For example, if agents are used to enforce access policies directly, then they must be installed and running on all endpoints in order for the solution to work. This can significantly inhibit the scalability and flexibility of a NAC solution for reasons discussed in sections below.

Scalability

Depending on the architecture, NAC solutions may or may not scale easily to support larger network environments. Generally, the least scalable NAC solutions are those that utilize in-band, or inline, architectures in which NAC servers or gateways must be deployed directly in the data path with all network traffic passing through them. In-band solutions can require deployment of numerous appliances, making them costly and complex to manage in larger networks. Out-of-band approaches, on the other hand, tend to be highly scalable as they interface with and control the existing network infrastructure (in a similar way to 802.1X), typically requiring far fewer server appliances in larger environments. However, it is important to ensure that an out-of-band solution will interoperate with wired and wireless network infrastructure, particularly in multi-vendor networks.

Scalability of other NAC architectures, including client-side and hybrid models, will vary widely. For example, client-side approaches scale poorly when the majority of endpoints on the network are unable to support the required client software. And hybrid solutions combining in-band and out-of-band server appliances scale poorly if the network environment requires more in-band deployment versus out-of-band.

Flexibility

Every organization and every network is different, so it is important to consider how well a NAC solution will fit the needs of a particular environment, as well as how well it will adapt to potential changes in the environment. Because of the number of different NAC approaches available, there is the risk of getting locked in to one particular vendor's way of doing things. Some solutions work better in wired LANs versus wireless LANs, but will not necessarily work well (or even provide the same capabilities) in both environments simultaneously. Some solutions lack interoperability with a variety of networking and security infrastructure components – switches, wireless gear, routers, VPN gateways, IDS/IPS, etc. – which limits their ability to be deployed in heterogeneous, multivendor networks. Careful consideration should be given to a NAC solution's ability to integrate with and adapt to both current and future network environments.

CONCLUSION

The decision of whether to implement 802.1X or NAC, or a combination of the two, comes down to the specific needs of an organization as well as consideration of the challenges and benefits of deploying each within a given network environment. In practice, most organizations will find that 802.1X alone is not enough, and instead a combination of 802.1X and NAC is most beneficial to provide the level of security, control, and visibility needed in today's networks.

NAC can augment 802.1X to provide additional capabilities, or in many cases (depending on the NAC architecture) it can be a viable substitute for 802.1X altogether. In wireless networks, NAC is commonly used to augment 802.1X in order to provide endpoint compliance validation or for more advanced management of guest access than 802.1X alone allows. In wired networks, NAC is more commonly used as a substitute for 802.1X due to the number of deployment challenges for 802.1X in these environments.

Like many technologies, NAC has evolved over a number of years, and some NAC solutions have evolved to provide advanced capabilities and added value. As noted previously, these advanced NAC solutions can greatly enhance network visibility, in addition to offering other functions such as dynamic profiling of endpoint devices, comprehensive guest management, as well as detailed logging, reporting, and audit trails that are extremely valuable for regulatory compliance.

REFERENCES

IEEE Std 802.1X-2004

<http://www.ieee802.org/1/pages/802.1X-rev.html>

Trusted Computing Group (TCG) and Trusted Network Connect (TNC)

http://www.trustedcomputinggroup.org/developers/trusted_network_connect

IETF Network Endpoint Assessment (NEA) Working Group

<http://www.ietf.org/html.charters/nea-charter.html>

CASE IN POINT

Regional Hospital Deploys NAC & 802.1X

Sarasota Memorial Health Care System (SMH) is an 806-bed regional medical center in Sarasota, Florida, with a network of outpatient centers as well as long-term care and rehabilitation facilities. The network at SMH consists of over 4,000 wired LAN ports and more than 350 wireless access points.

When SMH set out to solve a number of network security challenges, it first tried to do so using an 802.1X-based NAC solution offered by its IPS vendor. However, IT staff quickly found that while the solution worked adequately for its wireless network, it was insufficient for its wired LAN due to a number of deployment challenges.



"802.1X worked fine for our wireless network," said John Bozer, Director of Information Systems, "but there were too many difficulties trying to implement it over the wired network, especially in the case of PCs connected to the network through VoIP phones." He also needed a solution that would allow various medical devices incapable of supporting 802.1X to be identified on the network and to have network access provisioned appropriately for those devices.

SMH replaced its 802.1X-based NAC solution with Network Sentry™ from Bradford Networks to manage access control on its wired and wireless networks. "Network Sentry gives us a much greater level of security, with endpoint compliance, complete network visibility, and control over the users and devices on our network," Bozer said. "On our wired network, it provides 802.1X-like functionality to recognize users and devices so we can assign role-based access and block unauthorized users. We can easily identify devices that are out of compliance and ensure remediation. Because we can keep the production and guest networks separate, there is no impact to SMH-owned systems, including medical devices that directly impact patient care."

"We needed a scalable, flexible NAC solution that would be unobtrusive to authorized users, and would be easy to implement and manage," Bozer noted. "It was also important that the solution we chose would integrate with our IPS and other existing technology. This was a key driver for us in choosing Bradford's Network Sentry as the best solution for our environment."



Address 162 Pembroke Road, Concord, New Hampshire 03301, USA
Toll Free +1 866.990.3799
Phone +1 603.228.5300
Fax +1 603.228.6420
Email info@bradfordnetworks.com

Bradford Networks offers the best network security solutions for evolving IT environments. The company's flexible Network Sentry platform is the first network security offering that can automatically identify and profile all devices and all users on a network, providing complete visibility and control. Unlike vendor-specific network security products, Network Sentry provides a view across all brands of equipment and devices so nothing falls through the cracks. Hundreds of customers and millions of users worldwide rely on Bradford to secure their IP networks. Visit www.bradfordnetworks.com

Copyright © 2011 Bradford Networks. All rights reserved. Printed in USA. Bradford Networks and the logo are registered trademarks of Bradford Networks in the United States and/or other countries. Adaptive Network Security, Network Sentry, Campus Manager and NAC Director are either trademarks or registered trademarks of Bradford Networks or one of its affiliated companies in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Bradford Networks reserves the right to change, without notice.

DISCLAIMER

BN-001-06-001

This document provides general information about personal privacy and compliance initiatives in North America. It is intended to be used for resource and reference purposes only and does not constitute legal advice, nor should it be construed as providing any warranties or representations with respect to the products and/or services discussed herein. Readers of this paper are encouraged to speak with their legal counsel to understand how the general issues discussed above apply to their particular circumstances. Bradford Networks disclaims any and all liability for damages, costs, lost profits, fines, fees or financial penalties of any kind suffered by any party acting or relying on the general information contained herein.