



Secure and differentiated access in enterprise wireless networks

by Santhosh Cheeniyl

Wireless LANs offer flexibility in accessing enterprise resources. Anyone with a laptop or a smartphone has free access to network resources, since wireless systems use airwaves that extend beyond the physical perimeter of the enterprise.

An increasing amount of incidents involving data breaches, bandwidth stealing and denial of service attacks on wireless networks have made it a business requirement to deploy secure, authenticated wireless networks. Security protocols such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are outdated and it is no longer prudent to expect that basic authentication and encryption schemes such as those using pre-shared keys are sufficient against today's more sophisticated attacks.

Even though access control through the use of VLAN steering and ACLs has been available at a port level on Ethernet switches, in many wireless deployments today the granularity of access control has been limited to the SSID-level VLAN, ACL and QoS settings. In many cases, this has resulted in parallel network topologies in the enterprise – one for wireless and the other for wired access. Wireless network deployments must balance user accessibility and mobility with hardened secu-

urity and a greater degree of access control. What is required is a combination of secure wireless clients, wireless infrastructure, and a network policy system that supports the latest encryption and authentication standards with granular, per-session access control.

Wireless security and the IEEE 802.1X standard

The most secure way of implementing wireless security is 802.1X, which is an IEEE standard, used to authenticate access to both wireless and wired networks. Enhanced security and access control provided by 802.1X includes support for centralized authentication, authorization, accounting and dynamic key management. 802.1X uses the Extensible Authentication Protocol (EAP) for message exchange during the authentication process, which means that it supports secure authentication methods that make use of X.509 certificates and passwords.

There are three components involved in typical 802.1X interactions: A supplicant (on the client device), an authenticator (on the wireless controller), and a backend authentication server. A high level description of 802.1X interactions follows:

1. Secure authentication. When a wireless client (running a supplicant) attempts to connect to a wireless controller, the supplicant and the authentication server negotiate a secure TLS tunnel.

In password based authentication, the client sends credentials to the authentication server in the secure tunnel. In certificate based authentication, the client presents its X.509 certificate. In both cases, the wireless controller forwards the packets between the supplicant and the authentication server.

2. Granular enforcement. On successful authentication, the authentication server sends a message to the wireless controller to permit or deny access. It can also send other network enforcement attributes such as VLAN, ACL, QoS, etc. Note that this enforcement is applied to network traffic from the authenticated client.

3. Dynamic keys and data encryption. At the end of the authentication exchange, the authentication server also sends a key (co-derived with the supplicant during the authentication exchange) to the wireless controller; this key is then used by the supplicant and the wireless controller to derive dynamic session keys for data encryption.

As can be seen from the above flow, IEEE 802.1X offers a framework for:

- Performing strong authentication
- Generating dynamic keys for data encryption, and
- Enforcing granular access control in the network.

Deploying 802.1X for employee access

Employees in enterprises typically log in from corporate managed devices (laptops, desktops). These managed devices can be configured to access the network via 802.1X with minimal effort. For a smooth transition from

pre-shared key based wireless access to 802.1X based access, a phased deployment is recommended.

Phase 1 – Secure access

Step 1 - Wireless controller configuration

- Configure a subset of controllers with an SSID that requires 802.1X-based authentication
- Configure the authentication servers on the controller (A policy/AAA server that terminates RADIUS/EAP protocol)
- Turn on RADIUS accounting by configuring RADIUS accounting servers, so authentications can be tracked.

Step 2 - Policy/AAA Server Configuration

- Add the controllers that were configured in Step 1 as RADIUS clients
- Configure the appropriate EAP methods for user authentication. Microsoft Windows and MAC OS X clients support the EAP-PEAP [EAP-MSCHAPv2] method natively, so this is a good choice for an authentication method. Note that the authentication method you configure also depends on the identity store in which your user records are stored. Microsoft Active Directory, for example, is compatible with the MSCHAPv2 authentications.
- Configure the identity store for authentications. This is typically an enterprise directory
- Add a policy that permits access if authentication is successful, and denies access otherwise.

Step 3 - Client configuration

- Enable the native 802.1X supplicant on the client computers. Microsoft Windows, MAC OS X and most Linux distributions have native support for 802.1X. Note that there are tools available to ease this configuration process.
- Enable single sign-on. The credentials that are entered in the login window of the OS are used as 802.1X authentication credentials. This is supported on both Windows and MAC OS X based computers.

Expected benefits of a Phase 1 deployment entail the following:

- Secure authentication of all employees
- Dynamic keys for strong wireless data encryption
- Improved tracking of user access.

Phase 2 - Differentiated access

Once Phase 1 is fully deployed, granular access control based on roles of the employees can be implemented. Depending on how your network is configured and the capabilities of your wireless controller, granular access control can range from role-based network segmentation (VLAN), Access Control List (ACL) and Quality of Service (QoS), to a per-user stateful firewall.

If the right network design is in place, this phase requires configuration only on the policy/AAA server:

- Configure policy server to extract user attributes from the identity store. The extracted identity attribute can be group, department, title or any other attribute associated with user.
- Configure policies to send access control primitives (VLAN, ACL, etc.) to the wireless controller, based on one or more of the extracted identity attributes.

The benefit of deploying phase 2 is that users get access to network resources based on their role in the organization. As users move around in the network, from building to building, their access permissions follow them around.

Phase 3 - Advanced access control

Differentiated access deployed in Phase 2 can be further enhanced by taking into consideration other identity, health or session based attributes. For example, the following are some of the attributes commonly used to provide a finer degree of differentiated access:

- Time of day
- Location
- Access type (wireless, wired)
- Device OS and type (laptop vs. handheld)
- Device health (Anti-Virus, Anti-Spyware) checks. Device health can be collected and evaluated by:
 - An agent that is available in the OS (such as the Microsoft NAP Agent that is available with the Windows XP SP3, Windows Vista and Windows 7)
 - A vendor-specific permanent agent.

Machine Authentication (extending employee access to include known devices)

In many enterprises, devices that the user logs in from must be corporate approved devices. Machine authentication can be done alongside with 802.1X-based user authentications, and tied together by the backend policy system. Machine authentication can be done by verifying the presence of a machine's MAC address in an inventory database, or by performing a separate 802.1X machine authentication against an identity store that has the "computer" account (For example, Microsoft Windows computer accounts in Active Directory).

Tackling guest access

Guests typically get a temporary username and password to log into the network. They are given restricted privileges to the network – typically only Internet access. Since 802.1X requires computer configuration, enterprises typically do not enforce 802.1X-based access for guests. So how is a wireless guest access handled?

Guest access configuration steps are outlined below:

Step 1 - Wireless controller configuration

- Configure a guest SSID on the wireless controllers
- Optional data encryption can be configured by requiring a WPA2 pre-shared key (which is handed out to the guest, along with the temporary username and password)
- Access control for this SSID can be statically configured (unless different guests get different levels of access, in which case policies need to be configured on the Policy/AAA server)
- Configure the authentication servers on the controller (A policy/AAA server that terminates RADIUS protocol)
- Most controllers have a built-in guest portal that acts as a captive portal. The look and feel of this portal can be customized. Most controllers also have support for a portal hosted on an external "guest system". This latter configuration has several advantages:
 - A Portal can be used for wired, wireless and VPN use cases.

- Support for health checks by means of a dissolvable agent loaded through the portal.
- Portal customization can be on a central server, without having to distribute it to multiple controllers.
- Ability to support a single landing page and multiple portals (guest, contractor, partner, employee portals, for example) by attaching to a single SSID.

Step 2 - Policy/AAA server configuration

- Add the controllers that were configured in Step 1 as RADIUS clients
- Configure the identity store for authentications. This is typically the database that is resident on the server
- Configure sponsor accounts that allow permission to add guest accounts in the local database
- Add a policy that permits access if authentication is successful, and denies access otherwise. If granular access is required, configure policies appropriately.

In this flow, when guests associate with the “guest” SSID and bring up a browser and visit any web site, they are redirected to the captive portal. They enter their credentials and get access.

Handling unmanaged device access

Unmanaged devices are those that are not managed by the enterprise. Laptops or other computing devices brought in by guests can be handled as described in the previous section. Access policies for other unmanaged devices – for example, those brought in by employees – can be handled in multiple ways:

- Users can register these devices (typically, a function provided by the policy server). Once registered, these devices are allowed access into the network based on their MAC address. Any device that is not in the MAC address database is denied access.
 - Some policy servers also have the capability to perform device fingerprinting (by port scanning or by using the services of an external device profiler). The access policy then takes into account both the MAC address and the device fingerprinting information. This makes MAC address spoofing much harder.

- Unmanageable devices such as wireless printers and VoIP phones can also be given access by combining MAC address authentication with device fingerprinting.
- Some devices such as the iPhone, Droid, Nexus One, etc., natively support 802.1X. These devices can be given access to the network if an enterprise user authenticates from these devices. The other option is to have these devices go through a registration process, which registers their MAC address in a database. Once registered, employees can access the network using 802.1X. (This ensures that employee is accessing the network from a known and approved device).

Unmanaged device access configuration steps are outlined below:

Step 1 - Wireless controller configuration

- Configure an SSID with MAC filtering enabled
- Optional data encryption can be configured by requiring a WPA2 pre-shared key
- Access control for this SSID can be statically configured (unless different device types require different levels of access to the network)
- Configure the authentication servers on the controller (A policy/AAA server that terminates RADIUS protocol).

Step 2 - Policy/AAA server configuration

- Add the controllers that were configured in Step 1 as RADIUS clients
- Configure the identity store or white lists for MAC-based authentications. This is typically the database that is resident on the server (An external device profiler that supports LDAP can also be used as identity store.)
- Add a policy that permits access if authentication is successful, and denies access otherwise. If granular access based on device type is required, configure policies appropriately.

802.1X client-side deployment considerations

When deploying 802.1X-based authentication, a few deployment hurdles need to be taken into account.

Modern operating systems have native support for 802.1X, both for wired and wireless access.

However, when rolling out 802.1X enterprise-wide, these supplicants need to be configured with the right parameters (such as EAP method, single sign on, machine authentication, CA certificate, fast-reconnect, to name a few). This is a tall order for most end users.

In Microsoft Windows-only environments that use Active Directory-based authentication, a Group Policy Object (GPO) that configures these parameters can be provisioned. When the user logs in, the GPO is pushed to the client and the 802.1X parameters are automatically configured. There are also third-party wizards that are not limited to deploying 802.1X in Windows-only environments. 802.1X configuration for MAC OS X, Linux and some smart phones can also be deployed. The goal is provide the IT team and user with a trusted method for configuring an endpoint and making that first 802.1X connection.

Conclusion

As enterprises increasingly rely on wireless networks throughout their infrastructure as a standard business practice, network administrators must address the security issues that accompany the technology. With the emergence of the 802.1X standard, most networking equipment now offers the basic tools to address secure wireless access with a finer degree of control.

In closing, without a strategy and the proper tools to manage these controls, security administration becomes expensive, time consuming, and potentially unreliable. The idea is to think big, but definitely use a phased or adaptive deployment model that meets your immediate needs.

Santhosh Cheeniyil is the Founder and VP of Engineering of Avenda Systems (www.avendasys.com). He has over 19 years of product design, development and management experience in the computer industry. Prior to co-founding Avenda Systems, Santhosh was at Cisco Systems for over 7 years, where he was a Senior Manager and Technical Leader in security, voice and network management technology groups; he led the design and development of several successful products in the VoIP and network management areas. He was a Principal Engineer at Devsoft Corporation, which was acquired by Cisco in 1998.

Want to reach a large audience of security professionals by writing for (IN)SECURE?



Send your idea to editor@insecuremag.com