TECHNOLOGY SOLUTION BRIEF

Enhancing 802.1X Deployments with ConSentry Networks

CONSENTRY™ NETWORKS

Contents

What is 802.1X?

IEEE 802.1X is a standard method for port-based network admission control. In a wired or wireless network, user credentials must be validated before a physical LAN port or wireless access point can be used for network access. If the user authentication process fails, the LAN or wireless port remains closed and network access is denied. 802.1X uses the Extensible Authentication Protocol (EAP, RFC 2284), which works on Ethernet or wireless LANs, for message exchange during the authentication process.

802.1X is an IEEE Standard

For more information, please visit: http://www.ieee802.org/1/pages/802.1x.html

Why the Need for 802.1X?

Traditionally, one option for IT to prevent unauthorized network access was to physically shut down unused LAN ports and allow only defined MAC addresses on the active ports (e.g., MAC filtering or lockdown). Access control lists (ACLs) were also used to control network access based on IP addresses. However, maintaining a list of MAC and IP addresses is difficult to manage in large/dynamic networks. And the fact that users can bypass these methods by forging or spoofing an address makes this "security technique" far from secure.

IEEE 802.1X port-based network access control resolves these network vulnerabilities and provides a more secure approach to controlling user access to the network.

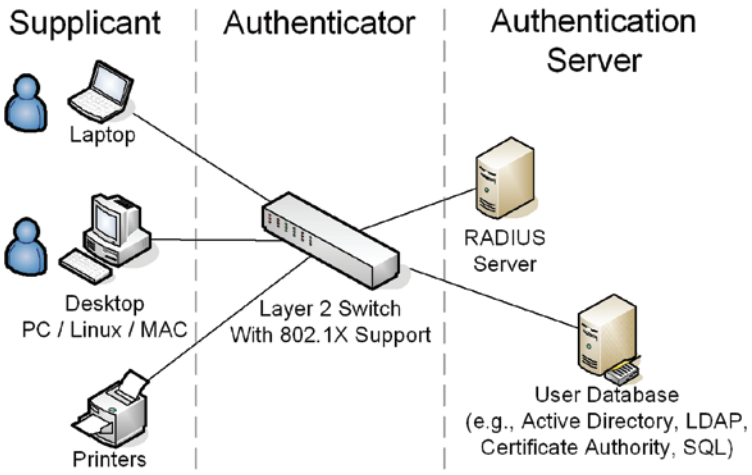
How 802.1X Works

An 802.1X system comprises three components:

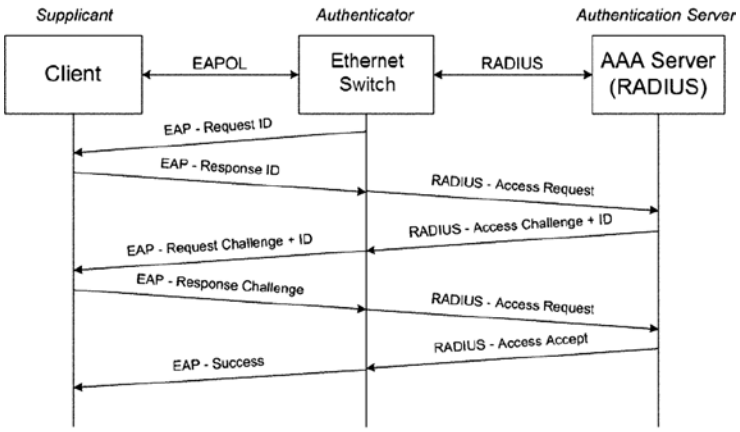
1. **Supplicant** – The client, or Supplicant, is the device that needs authenticating to the network.
2. **Authenticator** – The Authenticator performs the 802.1X port security and controls access to the network.
3. **Authentication Server** – The Authentication Server validates the username and password information from the Supplicant and specifies whether access should be granted. (This element is typically a RADIUS server.)

802.1X has three components:

1. **Supplicant**
2. **Authenticator**
3. **Authentication Server**



The Authenticator blocks all traffic from the Supplicant except for EAPOL (EAP over LAN) packets. A client (or Supplicant) sends an EAPOL start message to an 802.1X-enabled Ethernet switch (acting as the authenticator). The Authenticator sends a request for identification. Upon receiving the identification from the Supplicant, the Authenticator forwards the information to an Authentication Server – typically a RADIUS server. The RADIUS server looks up the user in its own database or a back-end database such as LDAP and validates the user's credentials. Depending on the chosen authentication method, the Authenticator opens the port for network access



EAP (Extensible Authentication Protocol) provides different types of authentication methods during the exchange. Options include TLS, PEAP, MD5, TLS, and TTLS. The following table provides an overview of each method.

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Server Authentication	None	Password Hash	Public Key (Certificate)	Public Key (Certificate)	Public Key (Certificate)
Supplicant Authentication	Password Hash	Password Hash	Public Key (Certificate or Smart Card)	CHAP, PAP, MS-CHAP(v2), EAP	Any EAP, like EAP-MS-CHAPv2 or Public Key

One of the benefits of 802.1X is vendor independence. The following table outlines the vendor product support for each authentication method.

	LEAP	EAP-TLS	EAP-TTLS	PEAP
RADIUS Server Support	Cisco, FreeRADIUS, Funk*, Interlink, Meetinghouse, Radiator	Cisco, FreeRADIUS, Funk*, Interlink, Meetinghouse, Microsoft, Radiator	Funk*, Interlink, Meetinghouse, Radiator	Cisco, Funk*, Interlink, Meetinghouse, Microsoft, Radiator
Supplicant Client Support	Cisco, Funk*, Meetinghouse	Cisco, Funk*, Meetinghouse, Microsoft, Open1X	Alfa-Ariss, Funk*, Meetinghouse, Open1X	Funk*, Meetinghouse, Microsoft
Embedded OS Support	n/a	Windows XP/2000/2003	n/a	Windows XP/2000/2003

*Funk is now owned by Juniper Networks

Limitations of 802.1X

As a pure network authentication protocol, 802.1X operates solely as an Authentication system and does not provide Authorization or Accounting (the other "As" in 802.1X AAA systems). 802.1X can confirm that a user requesting network access is a valid user, but it provides no control over where that user goes once on the LAN.

802.1X Limitation

802.1X will deny unauthorized network access, but it will not control or track network traffic from authorized users.

	AAA Protocol		
	Authentication	Authorization	Accounting
802.1X	✓	✗	✗

Authentication is the process of identifying the user. A user presents some form of identity and credentials to gain admission to the LAN. Examples of credentials are passwords, one-time tokens, digital certificates, and phone numbers (calling/called).

Authorization refers to the granting of specific types of service to a user, based on authentication. Authorization identifies what users can do and which resources they can access on the network. For example, Authorization determines whether the user is

permitted to access a certain file server or execute a certain type of application on the network.

Accounting refers to the tracking of consumed network resources by users. Typically, accounting tracks the user's network activity, the network resources utilized, the type of applications run, or the amount of data a user sent and received.

802.1X authentication

Advantages	Drawbacks
· Forces all users to authenticate before network port is opened	· Limited authorization at Layer 2 only – typically by vLAN.
· Works well with a wide variety of devices (PDAs to full workstations)	· Does not provide granular user network resource control. Does not have the ability to control network traffic from authorized users.
· Independent from OS, infrastructure vendor, or back-end RADIUS server	· Does not have the ability to track network traffic (accounting information) from authorized users (Layer 3 to Layer 7). Only provides START, STOP, and BYTES IN/OUT.

ConSentry Networks' Comprehensive Security Approach

ConSentry Networks augments 802.1X as part of a comprehensive set of LAN security services supported by its LANShield product family, which includes the LANShield Switch and the LANShield Controller. This powerful combination of hardware and software operates at LAN speeds to control every user and secure every port on the LAN. At the heart of ConSentry's devices is the LANShield™ silicon architecture. Comprised of a 128-core processor and custom traffic-processing programmable ASICs, this flexible architecture provides stateful deep packet inspection and flow-based traffic tracking and control at gigabit speeds.

The LANShield platforms provide:

» **Network admission control (NAC)**

ConSentry supports NAC by leveraging an organization's existing AAA servers and identity stores as well as its host integrity infrastructure. Where applicable, the LANShield device can actively participate in user authentication and host posture checks.

» **Visibility**

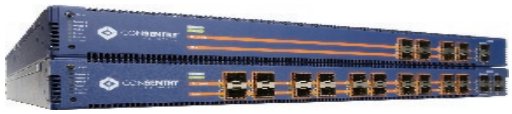
A Layer 2-7 aware device, the LANShield platform provides in-depth packet inspection with full Layer 7 application decode, so it can distinguish between applications using the same L4 port or attempting to mask them using a port number not typically associated with that application. The platform can filter traffic based on packet contents, and by binding a user's name to IP and MAC addresses, ConSentry can track LAN traffic by individual users as well as user group, application, host or other resources, protocol, L4 port, transaction, or file access.

» **User access control**

The LANShield products can apply access controls to everything they see. The platform gives IT the ability to define policies that limit users' access to networked resources based on their role in the organization. This role-based provisioning applies universally, regardless of where or how a user connects to the network.

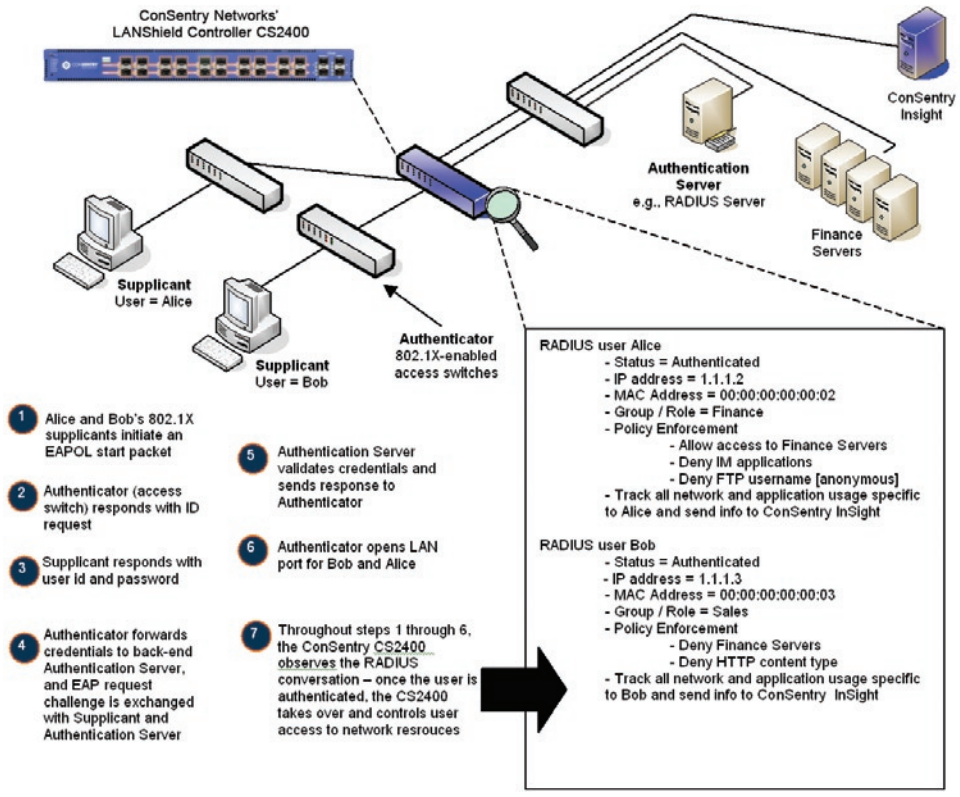
» **Threat control**

The LANShield devices protect against both known and unknown threats, providing more accurate detection with more granular blocking, such as by URL, than security tools operating at lower layers. Incident reporting is based on knowledge of user transactions, and the LANShield platform can stop traffic on a per-user or per-application basis if malware is detected. Attempts to use printers or VoIP phones as a launch point for attacks are also prevented by limiting the protocols those devices can run and the network destinations they can reach.



Authorization and Accounting with ConSentry Networks

ConSentry Networks adds significant value to 802.1X deployments. The LANShield product family enables IT managers to build a complete AAA system with an 802.1X framework. ConSentry allows IT to bind Authorization and Accounting information to authenticated 802.1X users. Authorization and Accounting applies from Layer 2 to Layer 7.



How ConSentry Compliments the 802.1X Authentication Process

Installing a LANShield Controller does not require any change to the network infrastructure – whether it's 802.1X enabled or not. IT managers can install the LANShield Controller between access and core switches without reconfiguring any network protocols. In 802.1X deployments, the LANShield Controller will listen to the RADIUS conversation between the 802.1X-enabled access switch and the back-end RADIUS server. The ConSentry device learns the MAC address, IP address, username, and user group (via RADIUS VSA or CLASS attributes) from the unencrypted RADIUS conversation. Then the LANShield Controller can apply roles and policies to the user to control access to network destinations following authentication.

Post Admission Control

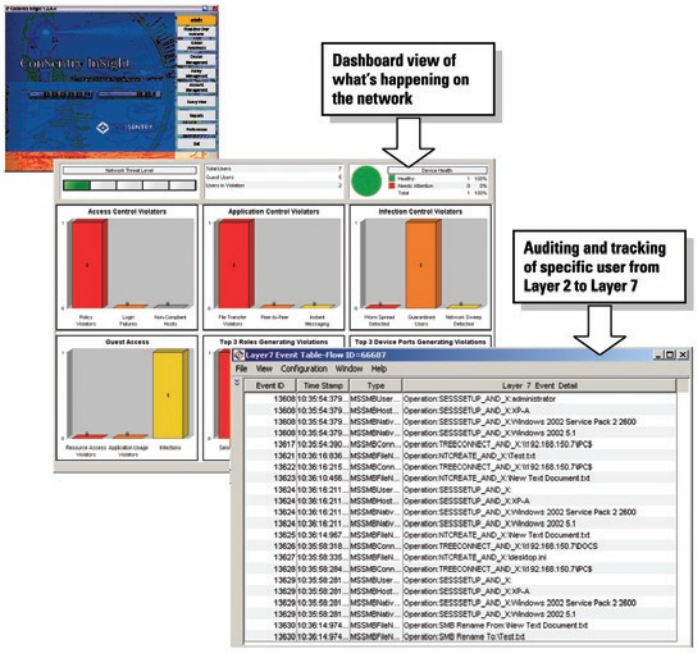
ConSentry Networks' Secure LAN Controller adds Authorization and Accounting to an 802.1X infrastructure.

Full Control and View of the Network at Layer 7

Once a user is authenticated, the LANShield platform can enforce Layer 7 policies. For example, an IT manager can control which applications a user can run on the network, the amount of bandwidth used, and the specific files or server resources the user can access. The following Layer 7 policies are examples of those the ConSentry device can enforce:

- Selective access to production servers, databases based on user role
- Filter FTP usernames
- Restrict FTP file transfers to a specific or a range of filenames
- Filter HTTP ContentType (e.g., MIME Types)
  - Image/gif
  - text/html
- Filter HTTP Host
  - URL Filtering
- Filter HTTP UserAgent
  - Web browser engine (e.g., Mozilla 5.0)
- Filter CIFS username
- Restrict CIFS file transfers to specific or range of filenames

Since the ConSentry device ties all traffic back to a user and enforces Layer 7 polices, it provides visibility into application transactions, displayed in ConSentry InSight. The InSight command center provides the IT manager a high level view of what is happening on the network, with the flexibility to pinpoint deep down to the source to visualize users, traffic, transactions, and violations.



Threat Control

As an application-aware platform, the LANShield product family protects against both known and unknown threats, providing more accurate detection than security tools operating at lower layers and more granular blocking. ConSentry has developed patent-pending application behavioral algorithms that are highly discriminating in their ability to differentiate worm traffic from normal user behavior. As a result, the LANShield device is a robust malware detector, capable of providing zero-hour protection while requiring almost no tuning or maintenance.

The ConSentry statistical malware algorithms look for application connection anomalies that manifest a significant deviation, over time, from predefined application thresholds. ConSentry monitors many LAN applications for such connection anomalies, including e-mail, file sharing, and infrastructure applications such as DNS, to name a few categories. For example, MS-SQL queries normally operate at a rate of a few per second, but during the Blaster worm outbreak, networks experienced 500 SQL queries per second. ConSentry has developed algorithms that detect, contain, and – if necessary – terminate applications displaying this kind of anomalous behavior, all without the need for attack signatures that are complicated to maintain, especially in a pervasive LAN deployment. To distinguish between "normal" and "deviant" traffic behavior, the ConSentry platform decodes every packet at the application layer and holds traffic history in memory long enough to log a session. To limit false positives, the platform then compares these attempted connection rates and the ratio of attempted to failed connections, over time, to standard levels, per application. These tasks require a degree of processing power that only ConSentry can deliver today.

Summary

Authentication, Authorization, and Accounting (AAA) is a term often used in LAN security. While 802.1X can deliver highly interoperable Authentication, Authorization and Accounting within 802.1X are extremely limited or non-existent.

The ConSentry Networks LANShield product family compliments 802.1X by fulfilling the missing components of AAA. ConSentry provides Authorization through granular policy enforcement up to Layer 7. The LANShield platform provides extensive user access control to restrict which resources users can access and which applications they can run on the network. The LANShield device delivers Accounting by providing IT managers with detailed visibility information on network traffic up to Layer 7, all tied back to a specific user or user group.

With ConSentry, IT managers now have the ability to build a complete AAA system within an 802.1X framework.

About ConSentry Networks

ConSentry Networks delivers comprehensive LAN security, enabling businesses to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry enables this pervasive security while lowering IT's cost of operations through its flexible, high-performance platform powered by ground-breaking custom silicon and revolutionary LAN security software. Backed by blue-chip venture capital firms that include Accel Partners, INVESCO Private Capital, and Sequoia Capital, ConSentry is headquartered in Milpitas, California. For more information, visit the company's web site at www.consentry.com.

Corporate Headquarters

ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035

Tel: 408-956-2100
Toll-Free: 866-841-9100
Fax: 408-956-2199
Email: sales@consentry.com

EMEA Office

ConSentry Networks
Lyoner Strasse 26 D-60528
Frankfurt Germany

Tel: +49 69 677 33 422
Fax: +49 69 677 33 200