

Authentication, Authorization and Detection

Abstract

This document is intended to provide an overview of authentication, authorization and detection features developed by Enterasys as part of the Secure Networks™ architecture. Authentication allows controlling network access and provides mobility to users and devices. It provides a way to know who or what is connected to the network and where this connection is at any time.

Hardware Platforms

The following table lists the hardware platforms potentially referenced in this document, along with the associated firmware versions.

Hardware Platform	Firmware Version
SecureStack A2	2.01.00
SecureStack B2	4.01.01
SecureStack B3	1.01.01
SecureStack C2	5.01.01
SecureStack C3	1.01.01
Matrix V2	2.6.0.4
Matrix C1	2.00.22
Matrix E1	3.07.02
Matrix GEN-2/3	5.08.29/5.09.19
Matrix DFE-G	6.01.01
Matrix DFE-P/D	6.01.01
Matrix X	1.5.1
RoamAbout AP 3000	3.1.24
RoamAbout AP 4102	1.01.51
RoamAbout R2	6.08.03
RoamAbout RBT 8X00	6.0.5.1
X-Pedition XP	E10.0.0.19
X-Pedition XSR	7.6.12

Authentication Back-end

All Enterasys devices supporting network authentication use RADIUS as a back-end authentication protocol. RADIUS fundamentals are defined by RFC2865. RADIUS provides a single gateway to authenticate users and devices across the network, abstracting user credentials and directory connectivity to the devices implementing the RADIUS client. It's up to the RADIUS gateway (server) to connect to the various directories available, like LDAP, NDS, AD, etc.

Authentication Front-end

IEEE 802.1X Authentication:

802.1X authentication is a standard defined by IEEE as “Port-Based Network Access Control”. The 802.1X standard was released in 2001 (802.1X-2001) with an update in 2004 (802.1X-2004). 802.1X leverages the EAP standard and allows different EAP types to be used, like PEAP, EAP-TLS, EAP-TTLS, etc. PEAP and EAP-TLS are the most commonly used EAP types. 802.1X requires the installation of a “supplicant” on the end-system (client) side. Most operating systems are implementing natively an 802.1X supplicant (e.g. Windows XP, Windows Vista). 802.1X can be used to authenticate users and machines. In the case of user authentication, user certificates may or may not be used to facilitate deployment. In the case of pure machine authentication where there is no user/password provided, machine certificates are used.

MAC Authentication:

MAC authentication provides a way to authenticate devices on the network using the MAC address of the connecting device. This authentication method is not fully secure as it does not prevent spoofed MAC addresses from being authenticated, but provides an acceptable first line security mechanism to prevent unknown MAC addresses from connecting to the network. Note that when MAC authentication is enabled on the network, the MAC address is sent in the User-Name RADIUS attribute and the User-Password RADIUS attribute is set to a well-known password configured on the switch (default is NOPASSWORD). Note that MAC authentication requires no software on the end-system side. Authentication of the MAC address is attempted by the switch once the first frame is received on the switch port, before the IP stack is even enabled on the end-system. If **MAC Authentication Masking** is supported and configured on the switch then a two stage authentication is performed: it will attempt to authenticate the full MAC address and then the masked MAC address (only if the full MAC address failed to authenticate). Note that the length (in bits) of the mask is configurable: the default length value is 48, which means that no masking will happen as it corresponds to the full MAC address.

Web-Based Authentication:

Web-Based authentication, as known as Port Web Authentication (PWA), provides a way to authenticate users on the network only requiring that a web browser is installed on the end-system. This is especially useful when user authentication is required and when 802.1X roll-out may be challenging due to the existence of a variety of deployed operating systems and the lack of control of the end-system (e.g. higher education where students are using their own machine, guest networking where guests use their own machine, etc). When web-based authentication is enabled, the user is prompted with a web login page when connecting to the network. This allows the user to provide credentials (username/password) for network authentication. The RADIUS client on the switch then verifies the inputted username and password with the RADIUS server to permit or deny network access.

Note that PWA supports different modes of operation: PWA and PWA+ (as known as PWA Enhanced Mode). In PWA mode, the user must enter the exact URL of the switch-hosted web login page (<http://secureharbour> by default) or the PWA IP address, of which both are configurable. In PWA+ mode, any URL (with a resolvable hostname) or IP address may be entered by the user, and the HTTP connection is spoofed by the switch where the user is subsequently redirected to the web login page automatically. PWA+ is easier to deploy but creates a problem when the unauthenticated behavior of a port is set to use a default policy role. In this configuration used for guest networking, the default policy role is applied to user traffic before, during, and after failed authentication. However, PWA+ will still redirect all HTTP traffic to the web login page until successful authentication, interrupting web connectivity for guest users. Therefore, support for PWA guest networking was added by allowing a configuration on the switch to specify a default username and password that are automatically populated in the username and password fields, respectively, on the web login page when opened by a user. So the guest user needs no prior information about credentials for network login, because they are automatically supplied in the web login page for allowing guest network access. The switch can be configured to either locally verify these credentials or transmit these credentials to the RADIUS server for validation and dynamic policy assignment.

The other point worth noting is that there are really two implementations of web-based authentication (including PWA and PWA+): the “legacy” Matrix E-Series (E1, GEN-2/3) implementation, and the Matrix N-Series DFE and SecureStack B2/B3/C2/C3 implementation. The main difference is related to the fact that in the Matrix N-Series DFE and SecureStack B2/B3/C2/C3 implementation, the switch is not providing IP assignment (DHCP) and resolution (DNS) services locally. Therefore for the Matrix N-series and the SecureStack B2/B3/C2/C3, the port that is authenticating users via PWA must be configured (with a default policy role or VLAN) to allow an end-system access to network resources it needs to generate an HTTP packet; such as DHCP, DNS, ARP, RARP, and HTTP. On the Matrix E-Series GEN-2/3 and Matrix E1 implementation, these services are spoofed locally by the device and therefore a default policy role or VLAN is not required to be configured on ports implementing PWA.

Furthermore, another difference in the PWA implementation on Enterasys platforms is the exclusivity of the functional mode: on the Matrix E-Series GEN-2/3 and Matrix E1, PWA runs in exclusive mode, meaning that it cannot be globally enabled with other authentication methods, like 802.1X and MAC. Therefore, if PWA is enabled on a port for these platforms, PWA may only be used, and not 802.1X nor MAC-based authentication, for user authentication on all other ports of the switch. On the Matrix N-Series DFE and SecureStack B2/B3/C2/C3, PWA may be globally enabled with 802.1X and/or MAC authentication, allowing the implementation of PWA for certain ports and 802.1X and MAC authentication on other ports. Refer to the user manuals for exact details of implementation.

Multi-User Authentication:

Historically, authentication operates in a single-user fashion, meaning that only one user can authenticate on a single physical port. If more than one user is connected then the first user will authenticate and subsequent ones will inherit from previously authenticated user's authorization. This can be a security issue. In those scenarios, dynamic MAC locking should be deployed with a window of one (1), so only one user is allowed per port.

When a switch supports multi-user authentication, it means that multiple users can be connected to the same physical port, and that each one can be authenticated individually. The value exists in the ability to authorize multiple users, either using dynamic policy or VLAN assignment for each authenticated user. Therefore, a disjoint set of network resources can be allocated to multiple users that have authenticated to the network on the same port. In the case of dynamic policy, this is called **Multi-User Policy**. Note that policy support may vary, depending of the hardware platform, especially in multi-user environments.

Note that on the Matrix N-Series DFE-G platform, multi-user authentication is limited to two (2) users, allowing the deployment of a user and another end-system (like an IP phone, IP camera, printer, etc) per physical port.

Note that on the SecureStack B2/B3/C2/C3 platform, multi-user authentication is limited to two (2) users, allowing the deployment of a user and an IP phone per physical port (in fact the user is authenticated and authorized with User policy role, and the IP phone is authenticated and tagged traffic is mapped to IP Phone policy role). This is called **User + IP Phone Authentication**.

Multi-Method Authentication:

This is the ability to run multiple authentication methods (802.1X, MAC, and PWA) on a single physical port. This is very useful when end-systems are mobile and multiple authentication methods are deployed for different types of connecting end-systems (e.g. PC's, IP phones, printers, etc). In those scenarios, the switch will automatically implement the correct authentication method for the authenticating end-system. Note that there is an authentication method precedence ordering, with the default being first 802.1X, then PWA, and MAC authentication last, and that this precedence ordering is configurable per device.

On Matrix E-Series GEN-2/3 and Matrix E1, 802.1X and MAC can be enabled at the same time. This is called **IEEE 802.1X + MAC Authentication** (as known as **Hybrid Authentication**). However, this is very different than enabling 802.1X and MAC authentication concurrently on a Matrix N-Series device's port. **IEEE 802.1X + MAC Authentication** first attempts to MAC authenticate a connecting end-system. Once an EAP (802.1X) frame is received on the port, the MAC authentication session (if successful) is terminated, and 802.1X is attempted. MAC authentication will not be attempted again on the port until a link down occurs or the user logs out of the network. Contrastingly, when 802.1X and MAC authentication are enabled concurrently on the Matrix N-Series platform, a user may be first MAC authenticated and will remain MAC authenticated although it fails 802.1X authentication to the network. As previously discussed, if PWA is selected on the Matrix E-Series GEN-2/3 and Matrix E1, then it will run in exclusive mode, meaning that PWA authentication is enabled on a port and other authentication methods may not be enabled on the device.

Authorization

Dynamic Policy Assignment:

Once authenticated, a user or a device may be dynamically assigned to a defined policy role (i.e. policy profile). The policy role's name, usually stored in the RADIUS server (or the directory), will be returned by the RADIUS server to the RADIUS client on the switch as a RADIUS return attribute called "Filter-ID". Subsequently, the indicated policy role, as well as the associated classification rules, will be applied to the physical port where the user is connected in the case of single-user authentication. When running multi-user authentication, the policy is applied to the user's end-system (represented by its MAC address) on the physical port where the user is connected; this is called Multi-User Policy.

Dynamic VLAN Assignment (RFC3580):

Once authenticated, a user or a device may be assigned to a defined VLAN ID. The user's VLAN ID, usually stored in the RADIUS server (or the directory), will be returned by the RADIUS server to the RADIUS client (the switch) as multiple RADIUS return attributes called "Tunnel". Subsequently, the VLAN ID will be applied to the physical port where the user is connected in the case of single-user authentication. When running multi-user authentication, the VLAN ID is applied to the user's end-system (represented by its MAC address): this is called **Multi-User VLAN**.

RFC3580 and Policy Interaction:

On devices supporting both Dynamic VLAN Assignment (RFC3580) and Dynamic Policy Assignment, like the Matrix E1, both Filter-ID and Tunnel RADIUS return attributes are supported, and translation mechanisms exist to turn Tunnel attributes into the assignment of a specified policy role. This is useful in multi-vendor environments where VLAN IDs are stored at the RADIUS (or directory) level and a subset of edge devices are policy-capable switches (from Enterasys).

Controllable Unauthenticated Behavior:

In “strict” 802.1X authentication mode, when authentication fails, user’s traffic is dropped at the port’s ingress. This can be an issue when deploying guest networking, as guests will always fail to authenticate.

In “non strict” 802.1X authentication mode, when authentication fails, user’s traffic is forwarded according to port’s physical configuration. This is useful when deploying guest networking, as guests will always fail to authenticate. In the case of non strict authentication a default policy or a default VLAN can be pre-configured. Note that “non strict” authentication mode (for all authentication methods) has been implemented since day one in policy-enabled environments. It has not been initially implemented in VLAN centric environments where 802.1X and RFC3580 have been deployed.

End-point Detection

Convergence End-Point (CEP) Detection:

This detection mechanism allows applying a specific policy when a CEP is detected. A convergence device can be an IP Phone (most scenarios), an IP Camera or any other voice/video enabled device. Once the device is detected (by snooping CiscoDP, Siemens CoreNet, H323/H245 and other protocols), a pre-defined policy role is applied to the physical port. This allows the transparent “plug-and-play” deployment of CEPs, where these devices are dynamically assigned to specific policy roles catering to the traffic generated by those end-points. With CEP detection, dynamic policy assignment for convergence-related devices occurs automatically upon network connection without requiring the deployment of authentication.

Note that on the Matrix N-Series DFE-G/P/D platforms, CEP detection requires multi-user authentication to be enabled, as well as DHCP, DNS, ARP and RARP services to be available (like the PWA implementation). Multiple CEPs can be detected and authorized independently per physical port.

Note that on the Matrix E1 platform, only one CEP can be detected and authorized per physical port. Furthermore, IEEE 802.1X and MAC authentication are overriding CEP detection authorization, and CEP Detection is not supported when Web-Based authentication (PWA and PWA+) is enabled.

	SecureStack						Matrix			
	A2	B2/B3	C2/C3	V2	C1	E1	GEN-2/3	DFE-G	DFE-P/D	X
IEEE 802.1X Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
MAC Authentication	✓	✓	✓	x	x	✓	✓	✓	✓	x
* MAC Authentication Masking	✓	✓	✓	x	x	x	x	✓	✓	x
Web-Based Authentication (PWA)	x	✓	✓	x	x	✓	✓	✓	✓	x
Enhanced Web-Based Auth. (PWA+)	x	✓	✓	x	x	✓	x	✓	✓	x
Multi-User Authentication	x	x	x	x	x	x	x	✓	✓	x
* User + IP Phone Authentication	x	✓	✓	x	x	x	x	✓	✓	x
Multi-Method Authentication	x	✓	✓	x	x	x	x	✓	✓	x
* IEEE 802.1X + MAC Authentication	x	✓	✓	x	x	✓	✓	✓		x
Dynamic Policy Assignment	x	✓	✓	x	✓	✓	✓	✓	✓	x
* Multi-User Policy	x	x	✓	x	x	x	✓	✓	✓	x
Dynamic VLAN Assignment (RFC3580)	✓	✓	✓	✓		✓	x	✓	✓	x
* Multi-User VLAN	x	x	x	x	x	x	x	✓	✓	x
RFC3580 and Policy Interaction	x	x	x	x	x	✓	x	✓	✓	x
Controllable Unauthenticated Behavior	✓	✓	✓	x	x	x	x	✓	✓	x
Convergence End-Point (CEP) Detection	x	x	x	x	x	✓	x	✓	✓	x

RoamAbout

X_Pedition

	AP 3000	AP 4102	R2	RBT 8X00	XP	XSR
IEEE 802.1X Authentication	✓	✓	✓	✓	x	x
MAC Authentication	✓	✓	✓	✓	x	x
* MAC Authentication Masking	x	x	x	x	x	x
Web-Based Authentication (PWA)	x	x	x	✓	x	x
Enhanced Web-Based Auth. (PWA+)	x	x	x	x	x	x
Multi-User Authentication	x	x	x	x	x	x
* User + IP Phone Authentication	x	x	x	x	x	x
Multi-Method Authentication	x	x	x	x	x	x
* IEEE 802.1X + MAC Authentication	✓	✓	✓	✓	x	x
Dynamic Policy Assignment	x	x	✓	x	x	x
* Multi-User Policy	x	✓	✓	x	x	x
Dynamic VLAN Assignment (RFC3580)	✓	✓	x	✓	x	x
* Multi-User VLAN	✓	✓	x	✓	x	x
RFC3580 and Policy Interaction	x	x	x	x	x	x
Controllable Unauthenticated Behavior	x	x	x	x	x	x
Convergence End-Point (CEP) Detection	x	x	x	x	x	x

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2007 Enterasys Networks, Inc. All rights reserved. Enterasys is a registered trademark. Secure Networks is a trademark of Enterasys Networks. All other products or services referenced herein are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.

02/08



Delivering on our promises. On-time. On-budget.