

# Authentication and Authorization

## Abstract

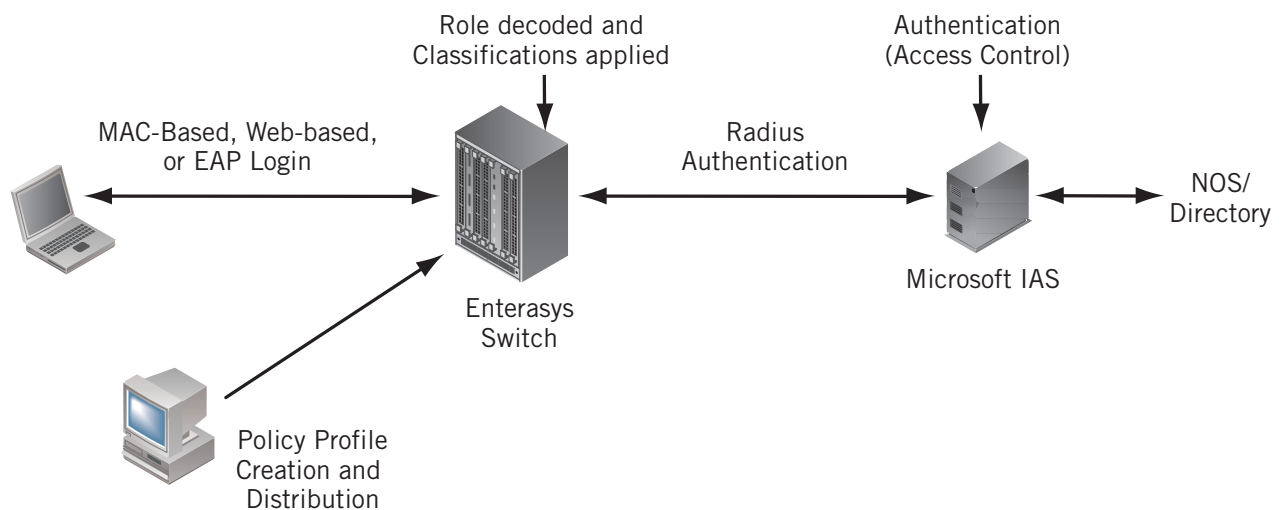
This document details the integration of access-layer authentication with Microsoft RADIUS and Active Directory Services available in Windows Server 2000/2003/2008. This also includes validation of Microsoft 802.1X supplicants available in Windows 2000/XP/Vista, leveraging various EAP methods (such as PEAP, EAP-TLS among others), in both wired and wireless environments. Such integration has been thoroughly tested in Enterasys and Microsoft labs.

## Authentication / Authorization Overview

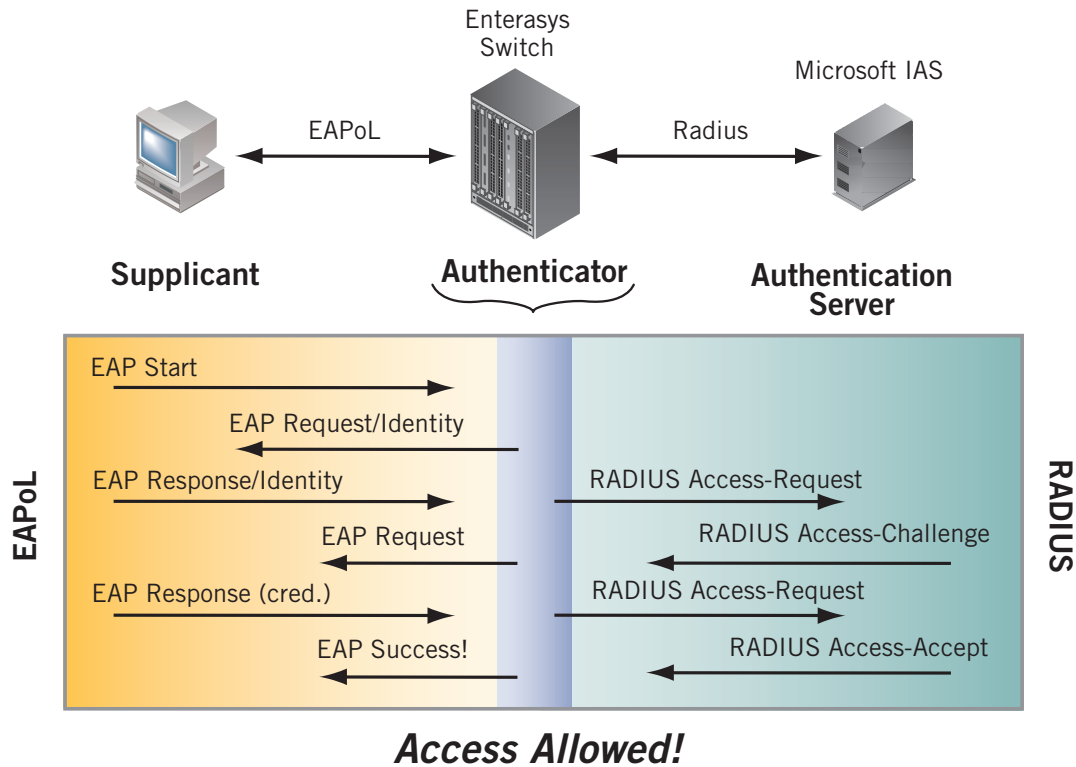
In order to effectively enforce appropriate network communication policy rules for individual users or devices connecting to a network, an identity must be established for the user or device. User-centric and machine-centric authentication technologies at the access-layer of the network infrastructure must be employed to identify the user and/or device. Authentication then allows for the authorization of the appropriate network usage by the association of the user or device to an appropriate organizational role. Various access control and authentication types are provided in Enterasys access-layer and distribution-layer switches, and also in Enterasys wireless products. These authentication types work in conjunction with services such as Microsoft's RADIUS and Active Directory Services to authenticate and authorize users and end-systems in the network environment. Microsoft RADIUS services are available through Microsoft IAS (Internet Authentication Services) in Windows Server 2000/2003 and Microsoft NPS (Network Policy Server) in Windows Server 2008.

## Basic Architecture

Authentication is enabled through the use of various methodologies (802.1X, Web-Based, and MAC-Based authentication). When a user or device connects to the network, the Enterasys switch initiates access control through an authentication challenge. The appropriate credentials are passed from the user or device to the Microsoft IAS/NPS server through RADIUS communications standards. Here the user or device is authenticated and associated to the appropriate business policy role. A RADIUS Return Attribute ("Filter-ID"), identifying the correct role is used to communicate the appropriate set of network communication policy rules to be enforced by the Enterasys switch where the user and device has connected.



The specific Policy Enforcement Point (PEP) is the Enterasys switch where the end-system and user is connecting. It is at this point where the appropriate policy rules will be enforced based upon the user's or device's role in the business that was mapped during the authentication and authorization process. The specific role identity is received from the Microsoft IAS/NPS Server upon successful authentication of the end-system and/or user. Using this role identification (in the form of a standard "Filter-ID" RADIUS Return Attribute), the Enterasys switch can now apply all of the appropriate policy rules that are important for that specific user and end-system.



Radius Authentication Diagram

## Authentication / Authorization Technical Description

If authentication is enabled on a network port, a user connected through that port may not be allowed to access network resources unless the user's user name and password are authenticated by the RADIUS authentication server. The unauthenticated port may be configured with some default access permissions, through the use of a default role, or the port may be configured to deny all network access until a user authenticates.

When a user logs in, the RADIUS server is contacted to determine whether or not a policy profile (role) exists for the user in its database. If a role exists, the user is allowed to access the network, and that user's role becomes the current role for the port. If authorization fails, the user is not allowed on the network, and the port assumes the default role for the port. (Only one default role is allowed per port.) Once a role is assigned to a port, the port's current role takes precedence over its default role, and the only way it can be replaced with another role is via authentication, or if the user logs out.

### Port Authentication States

When deploying an Enterasys switch, there are three primary port authentication states that can exist:

- **Authentication off/Port on** - This is simply the network behaving the way it would without authentication. Authentication is not required, and there may or may not be static policy rules applied.
- **Authentication on/Port off** - This occurs when users must authenticate to the interface prior to getting any kind of connectivity. It is the strictest of the port states, as the user can neither send nor receive any network traffic, except for authentication traffic, until he or she has successfully authenticated to the system

- **Authentication on/Port on with default policy** - This involves the enabling of authentication on the interface, but allowing certain traffic to traverse that interface, either prior to authentication, or after a failed attempt to authenticate. In this scenario, it is likely that users would be allowed to use basic network services, such as Internet, or NOS login, but not access other areas of the network, or consume large amounts of network bandwidth. Alternately, all of the ports that don't have authenticated users might restrict all of their traffic to a lower priority until they authenticate. This allows the network administrator to allow basic network connectivity to users that need it, such as consultants, or temporary employees but to not expose them to all of the organization's resources and available services.

## Authentication Mode

Authentication mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic will be handled.

- **Authentication Behavior** (Authentication Status) – Defines whether or not end users are required to authenticate on the port (device).
  - **Active** (Enabled) – Normal authentication procedures are implemented. End users must log in before their traffic is allowed on the network.
  - **Inactive** (Disabled) – Authentication of end users is not required.
- **Unauthenticated Behavior** – Defines how the traffic of unauthenticated end users will be handled on the port.
  - **Default Role** – If the end user is unauthenticated, the port will implement its default role. If there is no default role, there will be no role on the port.
  - **Discard** – If the end user is unauthenticated, no traffic is allowed on the port.

These two settings can be combined to create four possible authentication modes. The default authentication mode for ports is Inactive/Default Role.

- **Inactive/Discard Mode:** In this mode, authentication is inactive for the port. All traffic from users connected to the port is discarded. This effectively turns the port off.
- **Inactive/Default Role Mode:** In this mode, authentication is inactive for the port. All users connecting at this port will use the default role, if one has been assigned to the port, in combination with any existing static classifications. If there is no default role assigned to the port, the port uses only the static classification rules which exist. If there are no static rules, the port uses the PVID and default class of service for the port. This is the default authentication mode for ports.
- **Active/Discard Mode:** Authentication is active for the port, and end users are required to authenticate. The behavior of the port with regard to roles is as follows:

*Web-Based Authentication:* Prior to authentication, a default role has no meaning on an Active/Discard port, since all unauthenticated traffic is discarded. If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded.

*802.1X Authentication:* Prior to authentication, if a default role is assigned to the port, the user will have access to the network according to the default role. However, if there is no default role assigned to the port, all unauthenticated traffic is discarded.

- **Active/Default Role Mode** (Web-Based authentication only) - In this mode, authentication is active on the port, and end users are required to authenticate. Prior to authentication, the Current Role is the Default Role, if there is one, or none, if there is not. If authentication is successful, the port is assigned the user's role as its Current Role. If unsuccessful, the port is assigned the port's Default Role, if it has one. When the authenticated user logs out, the port's Current Role reverts to the port's Default Role, if there is one, or to None, if not.

## 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](http://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.

**Microsoft**

