

Secure Networks

Multi-User Authentication and Policy (MUA+P) vs. Multi-User Authentication (MUA)—A Comparison

by Markus Nispel
Office of the CTO
Enterasys Networks



Introduction

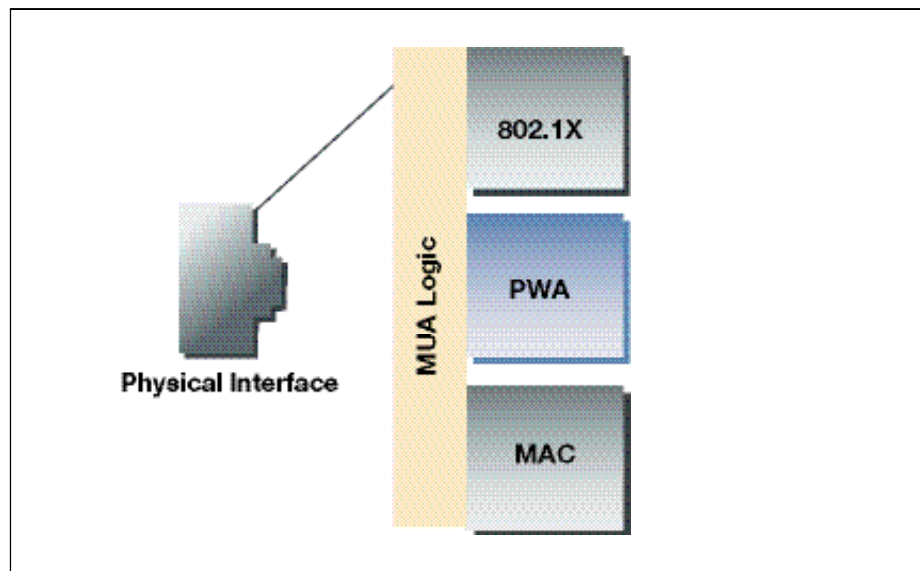
Many manufacturers of network components in the market are now opting to follow Enterasys' long-term Secure Networks strategy and choosing to integrate security into their network infrastructures. There are immense differences, however, between the various implementation methods applied. This whitepaper discusses one specific element in detail: the capacity to authenticate several users or devices simultaneously at the port and to assign different policies to them. This feature is of particular importance in Voice-over-IP and fiber-to-the-office environments.

Enterasys defines this function as Multi-User Authentication and Policy (MUA+P). This feature is unique to Enterasys solutions; all other solutions available in the market do NOT allow you to assign differing policies and refer to this function as simply Multi-User Authentication (MUA).

Multi-User Authentication and Policy (MUA+P) in Detail

When an organization wishes to introduce authentication procedures, the first step is to decide which specific procedure to select. There are various options to implement authentication. To a large scale, they depend on the end system used and could include:

- **802.1x** for individual PCs and laptops; in the future this will also be applied in part to IP phones
- **MAC address** for printers, IP phones, and other machines on the network (security surveillance cameras, production control, sensors, etc.)
- **Web portal** for guests, consultants, service technicians, etc.
- **Default** features for end systems such as TFTP/Bootp-to-boot diskless stations

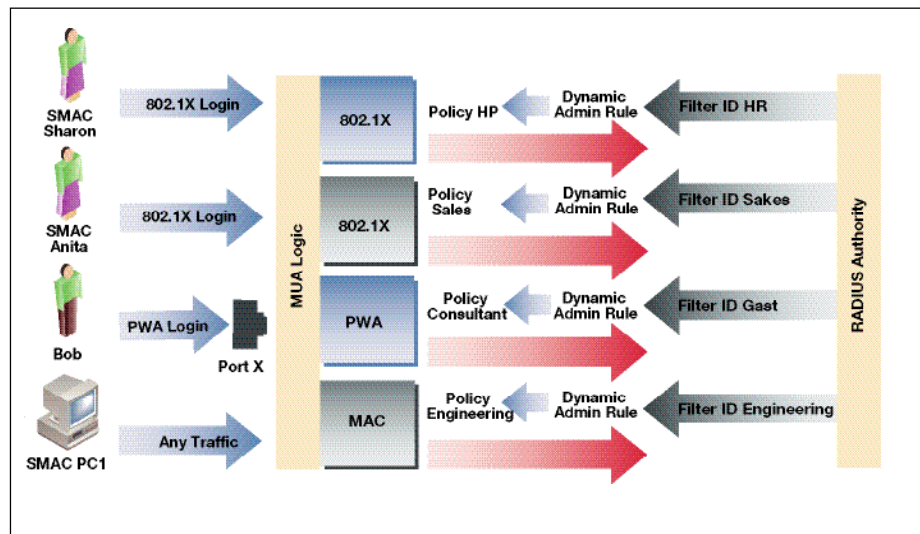


A switch optimally should support all procedures **SIMULTANEOUSLY** per port to avoid unnecessarily increasing the administrative effort—otherwise, the authentication procedure will have to be re-applied every time a system is moved. With the Matrix™ N-Series switching platform, Enterasys supports all procedures **simultaneously per port**.

When authenticating different users/devices simultaneously at a port, it has to be assumed that different sets of rules must apply, according to the specific user and/or device in question. A PC, for instance, should be assigned different rules than those for an IP phone at the same port. A guest user should be assigned different rules than those for an employee, etc.

This means that after successful authentication, **policies must be assigned per user/device**. Otherwise, the authentication processes performed are of little value.

Enterasys supports this procedure by means of Multi-User Authentication and Policy (MUA+P) as indicated in the diagram below.

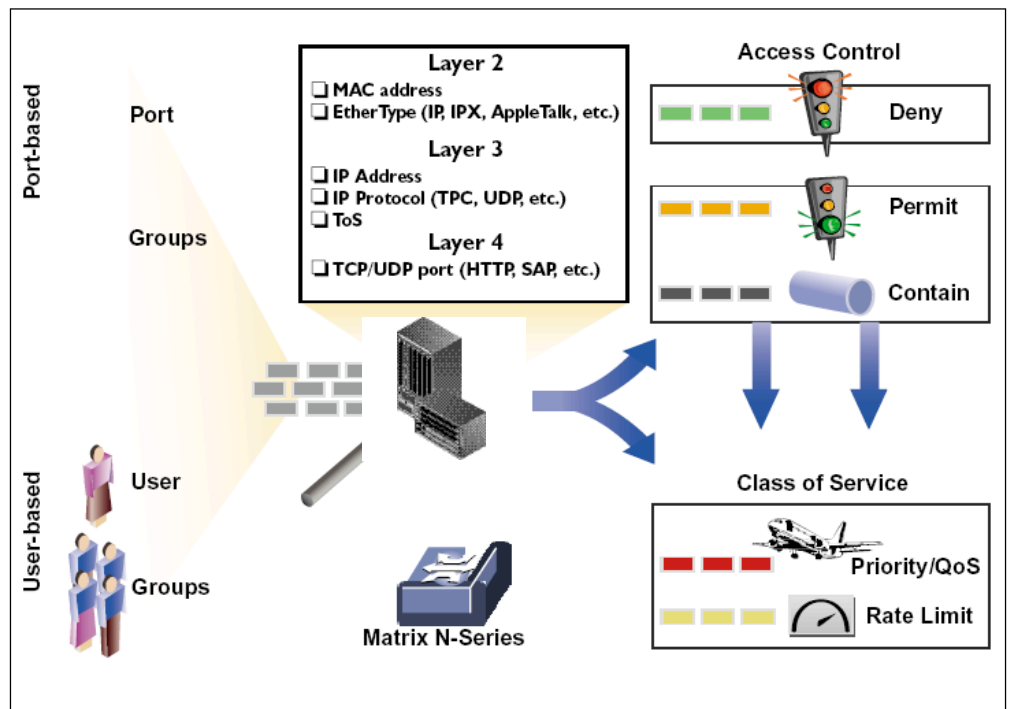


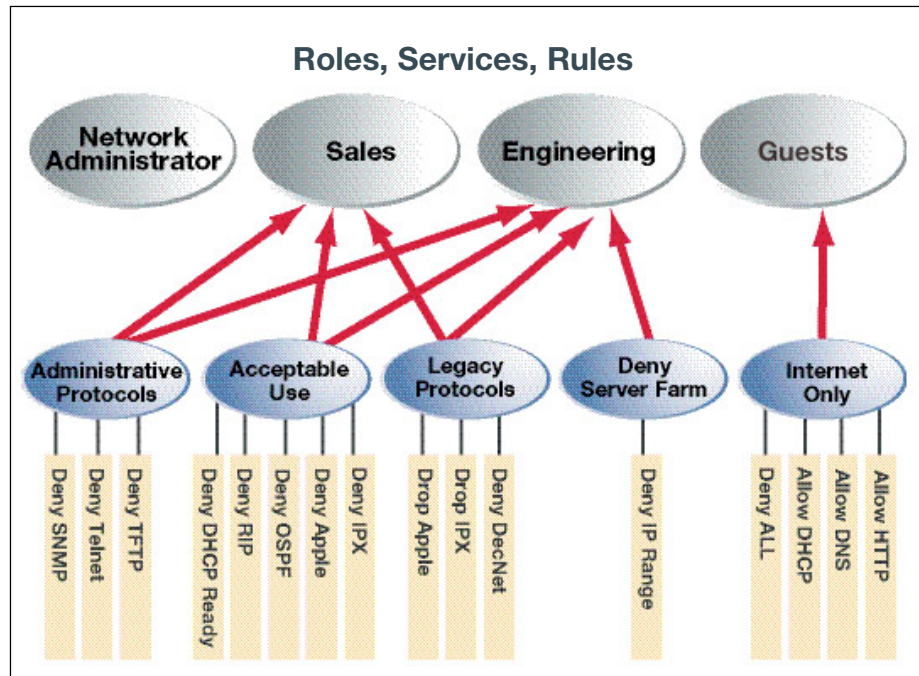
Here, up to 256 users per port can dynamically be assigned to different policies through any authentication procedure. Another point to note is the type of policy assigned. In the case of other solutions, only simple VLAN policies are supported. Within the VLAN itself, there is no control at all.

- What happens if someone connects an unauthorized DHCP server to the VLAN (and logs on with appropriate credentials)?
- How do you distinguish VoIP from data traffic on a softphone (on the PC)?
- How can you stop the propagation of a worm **within** a VLAN?

The answer can be found in the port policies of Enterasys solutions, which are also effective between the ports in the same VLAN and which also recognize information from Layer 2 (VLAN/MAC address) through Layer 4 (application—e-mail, VoIP).

A simple summarization and structuring via Enterasys' NetSight® Policy Manager make the performance of network services for the individual policies (roles) an easy-to-view and efficient procedure as seen in the diagram on the following page.





Summary

Secure Networks directly integrates security technologies into a distributed network infrastructure. All security-relevant components work together and can be automated. Thus, they represent a closed security architecture, which can be administered in an easy and efficient manner via a common management interface and homogeneous policy management—in essence, a distributed firewall is set up. Further solutions are integrated into this policy management, such as desktop integrity control (Trusted End System Agent-Based via ZoneLabs or Sygate solutions or Trusted End System Network-Based via TAAG Trusted Authentication and Assessment Gateway) and Dynamic Intrusion Response to form a distributed intrusion prevention system.

For more information on Secure Networks technology, please visit enterasys.com/secure-networks.

All contents are copyright © 2005 Enterasys Networks, Inc. All rights reserved.

Lit. #9014045 7/05

Page 6 of 6 • Whitepaper

