

ZebOS®  
Network Platform

---

## Port Authentication Module

### Overview

The ZebOS® Network Platform Port Authentication Module provides port-based network access control to Local Area Network (LAN) devices in support of the IEEE 802.1X Port-Based Network Access Control standard. Port Authentication is valuable for Enterprise LANs where users are restricted to certain services or organizations. It is also useful where a LAN offers connectivity to areas of a business building accessed by the public. Ports in Media Access Control (MAC) bridges used to attach routers to a LAN can also benefit from the features of Port Authentication.

The ZebOS Port Authentication Module supplies an extension to system functionality by providing the means to prevent unauthorized access by a Supplicant to restricted system services, or to prevent a Supplicant from attempting to access an unauthorized system. In addition, ZebOS Port Authentication can prevent an unauthorized system outside of the network from connecting to a Supplicant LAN. Port authentication is desirable

### Port Authentication Basics

802.1X Port Authentication is a means to authenticate devices that attempt to attach to a LAN (or, system) port. A point-to-point connection establishes once a device authenticates successfully. A connection fails if authentication fails. Port Authentication thus enhances security for systems as it protects against unauthorized access from either directly connected or wireless supplicants. Port Authentication uses the physical access characteristics of LAN infrastructures to provide a means of authenticating and authorizing devices attached to LAN ports.

There are three distinct roles in the Port Authentication process

1. *Authenticator* - the port that enforces authentication before clients can access to services accessible via that port.
2. *Supplicant* - a port or device that wants to access services offered by the authenticator.
3. *Authentication Server* - a server that performs authentication required to check the credentials of the supplicant on behalf of the authenticator to indicate whether the supplicant can access the services provided by the authenticator.

Using a RADIUS (Remote Authentication Dial in User Service) server is one way to authenticate supplicant requests. RADIUS servers are responsible for receiving connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver the service requested.

### Authorization States

A parameter in the ZebOS Port Authentication Module allows administrative control over the port's authorization status. Valid values and definitions are implemented in the ZebOS Port Authentication Module as follows:

- *Force Authorized* forces the Authenticator PAE state machine to set the status of the controlled port to authorized

- *Force Unauthorized* forces the Authenticator PAE state machine to set the status of the controlled port to unauthorized
- *Auto* allows the Authenticator PAE state machine to control the value of the port status to reflect the outcome of the authentication exchanges between the Supplicant PAE, Authenticator PAE, and the Authentication Server

## Features

- Port Authentication Exchange (PAE) messaging between supplicant and authentication server
- Denial of access to unauthorized requests
- Support for co-located or external authentication server designation
- RADIUS functional support, including server key exchange
- Easily add or remove ports from Port Authentication management
- Enable or disable Port Authentication system-wide or on a per-port basis
- Industry-standard Command Line Interface (CLI)

## Benefits

- Security from unauthorized access by clients, other systems, or Bridged LANs
- Protection from unauthorized wireless users who are within a wireless access point area
- SHOW commands display summary or detailed information or statistics for an entire system or a single port
- Flexible software module extends to new ports as the system grows

## Standards Support

- IEEE 802.1X — Local and Metropolitan Area Networks: Port-Based Network Access Control
- draft-ietf-bridge-8021x-03 — Definitions for Port Access Control (IEEE 802.1X) MIB

## Requirements

- ZebOS Network Services Manager Module
- ZebOS Layer 2 VLAN Module

## Standard Deliverables

- Source Code (written in ANSI compliant C)
- Installation Guide
- Configuration Guide
- Command Reference Guide
- Developer Guide