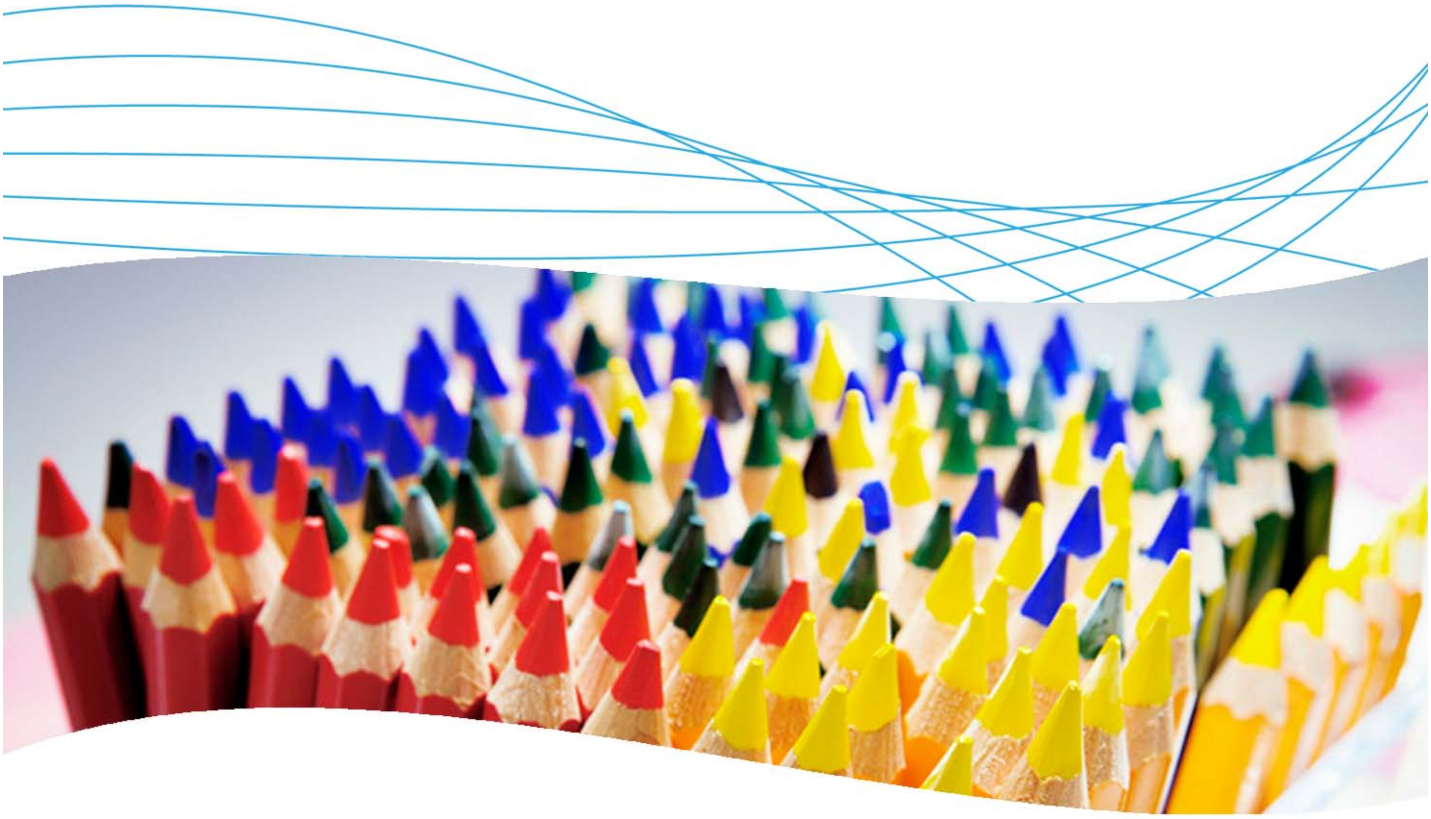
An HP ProCurve Networking Application Note

How to configure 802.1X authentication on ProCurve switches



Contents

1. Introduction

This application note explains the use of the IEEE 802.1X standard for Network Access Control, and how to configure IEEE 802.1X on a ProCurve switch.

1.1 Network Access Control methods

Network Access Control relies on different methods to authorize or prevent users and computers to access an enterprise network. ProCurve switches and wireless access points support three access control methods:

- **MAC authentication**: MAC authentication is the default method for devices that do not support web authentication or 802.1X; these devices are authenticated by their MAC address. For more details about this method and its implementation on ProCurve switches, please refer to Application Note AN-S2, *How to configure MAC authentication on a ProCurve switch*.
- **Web authentication**: Web authentication is useful to grant access to visitors, because it does not require any client software on the user machine. It is mainly used in public places, like hotels or airports. For more details about this method and its implementation on ProCurve switches, please refer to Application Note AN-S1, *How to configure Web authentication on a ProCurve switch*.
- **802.1X**: Using 802.1X is the most secure and the most recommended of the three methods. Released as a standard by the IEEE in 2001, 802.1X is an open-standards-based protocol for authenticating network clients on a user-ID basis. It has been implemented by all network vendors. IEEE 802.1X provides automated user identification, centralized authentication, key management, and provisioning of LAN connectivity. It even provides support for roaming access in public areas.

1.2 Benefits of 802.1X

Benefits of 802.1X include:

- Traffic flow on a port is opened up only after a user is authenticated by a RADIUS server.
- 802.1 X enables dynamic VLAN assignment.
- The protocol keeps "guests" under tighter control no matter where they plug in.
- User activity can be accounted for and tracked in a RADIUS server.
- 802.1X authentication provides privileges not only to computers and machines, but also to network services. Upon authorization, 802.1X-capable switches and routers will modify access privileges according to the individual entitlement.

Alone, a RADIUS-authenticated session can provide only a limited degree of service privileges. However, the 802.1X protocol provides a method for authentication in conjunction with a RADIUS (or similar) database, as well as providing subsequent token distribution to compliant network hardware and software. This results in privileged service descriptions that are more robust.

2. The 802.1X authentication process and EAP protocols

The 802.1X protocol takes the RADIUS methodology and separates it into three distinct groups: the Supplicant, the Authenticator, and Authentication Server. The Supplicant and the Authenticator communicate using the Extensible Authentication Protocol (EAP).

2.1 Supplicant

The Supplicant is the client that requests access to the network. Typically, a supplicant is a user workstation, but it may be router, a switch, an IP phone, or any other device that is seeking network services. Supplicant software is already implemented natively in some operating systems, including Microsoft Windows XP and Vista, or can be downloaded and added to the PC. Note that in the HP ProCurve implementation, a switch port can also be configured as a supplicant, in order to secure links between network devices.

The configuration of Windows XP and Vista supplicants for 802.1X is described in ProCurve Application Note AN-S3, *How to configure 802.1X authentication with a Windows XP or Vista supplicant*.

2.2 Authenticator

The Authenticator is the device that provides the entry point for the supplicant into the network. It requires the supplicant to provide 802.1X credentials, which are forwarded to the authentication server. HP ProCurve switches and access points can serve as authenticators.

2.3 Authentication Server

The Authentication Server receives authentication information that originates with the supplicant and verifies the information against its stored name/password pairs. In the HP ProCurve implementation, this is a RADIUS server. In the absence of an external authentication server, a switch can be configured to authenticate 802.1X supplicants using its own local database.

2.4 Authentication with EAP

The Extensible Authentication Protocol (EAP) is defined by the IEEE 802.1X standard as the mechanism that controls interaction between the supplicant and the authenticator. As shown in Figure 1, in the ProCurve implementation, the authenticator is a switch.

To enable 802.1X on a switch port, the port must be configured as a port-authenticator. (See the details of the switch configuration below in section 3.1, "Configure the ProCurve switch".) Port-authenticators are closed to any type of incoming traffic, except the EAP protocol.

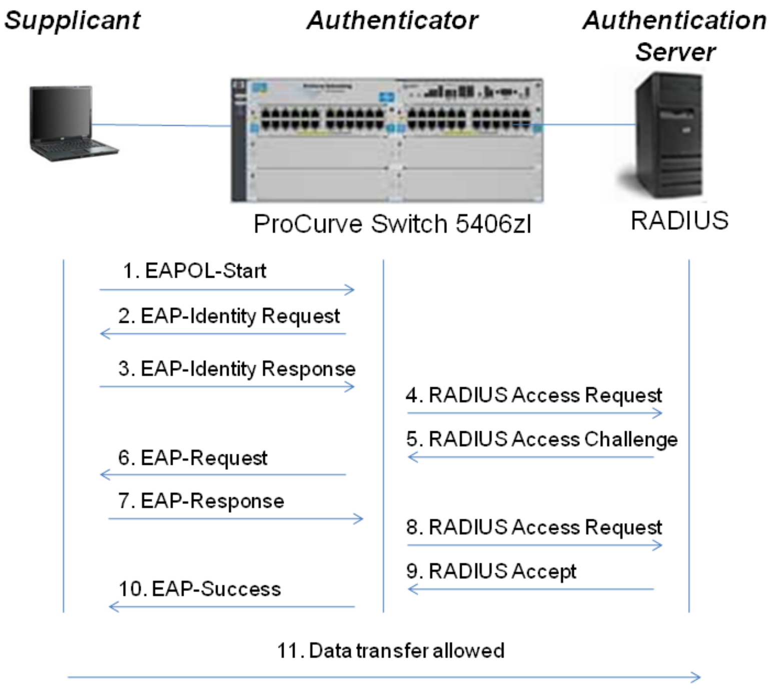


Figure 1. Details of EAP authentication

When the switch sees a client connected on a port-authenticator, it sends an EAP-Identity Request to challenge the user for credentials. The PC replies with its username/password or certificate, and the switch forwards the information to the RADIUS server. Then the switch merely passes messages between the Supplicant and the RADIUS Server, who directly negotiate the type of EAP protocol and the authentication parameters to use.

If the supplicant credentials match the information known in the RADIUS database (a local database or directory—for example, Active Directory in the Microsoft world), the RADIUS server sends a RADIUS Accept message back, and the switch sends the Supplicant an EAP-Success message and opens the port for data transfer.

Once the supplicant has been authenticated by the RADIUS server, other tools can be used to add further control on the supplicant.

2.5 EAP versions

The EAP version known as EAP-MD5 is an open standard. It relies on the MD5 hashing algorithm, which offers only comparatively weak security. (For example, it can be cracked by a dictionary attack.) This EAP version may be secure enough for wired authentication, but should not be considered secure on a wireless network.

Another open standard is EAP-TLS. This version of the protocol offers a good security, because it relies on two certificates: one on the client side and one on the server side. However, the implementation of EAP-TLS can be complicated because of the management required for the many certificates it requires.

EAP- TTLS (Tunneled Transport Layer Security) is another open standard that offers a good security; it requires X509 certificates on the server side only. (Certificates on the client side are optional.) It is not natively implemented on Microsoft systems.

PEAP (Protected EAP) is an open standard that exists in two versions: PEAPv0/EAP-MSCHAPv2 and PEAPv1/EAP-GTC. The PEAP protocol performs authentication in two phases: Phase 1 authenticates the server with a PKI (Public Key Infrastructure), and creates a secure tunnel to encrypt the data exchange for Phase 2. Phase 2, in turn, identifies the client through the encrypted tunnel.

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco-proprietary version. EAP-Fast is also a Cisco version. Designed to correct weaknesses in LEAP, it utilizes a three-phase authentication scheme, and is defined as a draft in IETF.

EAP-SIM (Subscriber Identity Module) is a method used to distribute keys in the GSM network, while EAP-AKA (Authentication and Key Agreement) is used for UMTS networks.

3. The ProCurve access control solution using EAP and 802.1X authentication

The ProCurve Networking access control solution primarily utilizes the PEAP and EAP-TLS versions of EAP. Further control is added if a ProCurve Identity Driven Manager (IDM) agent is installed on the RADIUS server. After authentication of the supplicant by the RADIUS server, IDM can grant or deny access to the network based on user location, time, MAC address, and endpoint integrity status. (For more information about configuring IDM, refer to ProCurve Application Note AN-S8, *How to configure ProCurve Identity Driven Manager*.)

3.1 Configure the ProCurve switch

To configure the switch, first you define the RADIUS server on the switch, then you specify the authentication protocol to use. Next you define the port-authenticator ports, and finally you activate those ports.

Here is an example of the commands used to configure a ProCurve switch:

```
5400zl> en
5400zl# config term
5400zl>en
5400zl# config
5400zl(config )# radius-server host 10.1.10.10 key procurve
5400zl(config )# aaa authentication port-access eap-radius
5400zl(config )# aaa port-access authenticator A1-A24
5400zl(config )# aaa port-access authenticator active
5400zl(config )# write mem
```

3.2 Configure the RADIUS server

In configuring the RADIUS server, the switches that will serve as authenticators must first be defined as RADIUS clients. Then a remote access policy must be defined: this policy should specify the EAP protocol version to use, the necessary groups, and the type of connections to authenticate.

For more information about configuring the RADIUS server, refer to the following ProCurve application notes:

- For Microsoft IAS (Windows 2003) configuration, refer to Application Note AN-S1, *How to configure Web authentication on a ProCurve switch*.
- For Microsoft NPS (Windows 2008) configuration, refer to Application Note AN-S5, *Integrating ProCurve IDM and Windows NAP*.

4. Multiple 802.1X sessions

The IP phones of most telephony vendors contain an integrated supplicant. The phone typically can be authenticated on the switch port where it is connected, and then be assigned a VLAN through RADIUS attributes or Identity Driven Manager.

4.1 Authenticating a dual-port IP phone

Most IP phones have a dual port where a PC can be connected. This reduces the number of connections to patch for each desk. But the PC and the phone, which are physically plugged on the same port of the switch, have different needs for bandwidth, Quality of Service and access to network resources. Moreover, the PC port on the phone needs to be secured to prevent unauthorized users from connecting through it.

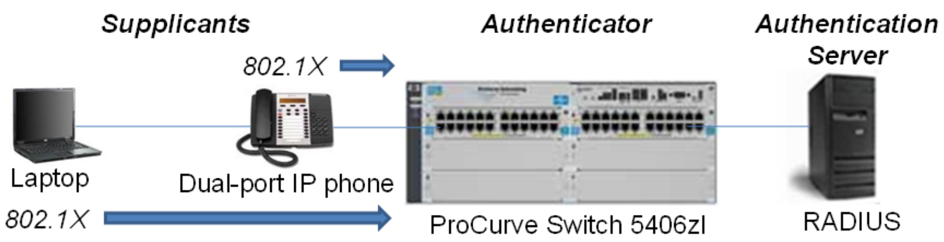


Figure 2. Using multiple 802.1X sessions to authenticate a dual-port IP phone

The solution is to authenticate both the phone and the PC on the same port, and to assign them different profiles (e.g., for VLAN, bandwidth, QoS, and access-lists). ProCurve switches allow this multiple-profile configuration.

4.2 Configure the ProCurve switch with multiple profiles

On the ProCurve switch, the voice VLAN must be tagged and the data VLAN untagged on the port that will be connected to the phone. The data VLAN can be configured statically, or dynamically assigned by Identity Driven Manager. In addition, a client-limit of 3 must be configured on the switch port.

For example:

```
5400zl> en
5400zl# config term
5400zl(config )# vlan 1
5400zl(vlan?1)#untagged B1-B24
5400zl(vlan?1)# vlan 2
5400zl(vlan?2)# voice
5400zl(vlan?2)# tagged B1-B24
5400zl(vlan?2)# exit
5400zl(config )# aaa port-access authenticator B1-B24
5400zl(config )# aaa port-access authenticator B1-B24 client-limit 3
5400zl(config )# aaa port-access authenticator active
5400zl(config )# write mem
```

This concludes the procedure for configuring IEEE 802.1X on ProCurve switches.

5. Reference documents

For further information about how to configure ProCurve switches to support security, please refer to the following links:

- For PCM+ and IDM manuals:
  http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm
  http://www.hp.com/rnd/support/manuals/IDM.htm

- For user manuals for ProCurve 3500yl-5400zl-8212zl switches:
  http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm

- For ProCurve Switch 2610 series manuals:
  http://www.hp.com/rnd/support/manuals/2610.htm

For further information, please visit www.procurve.eu