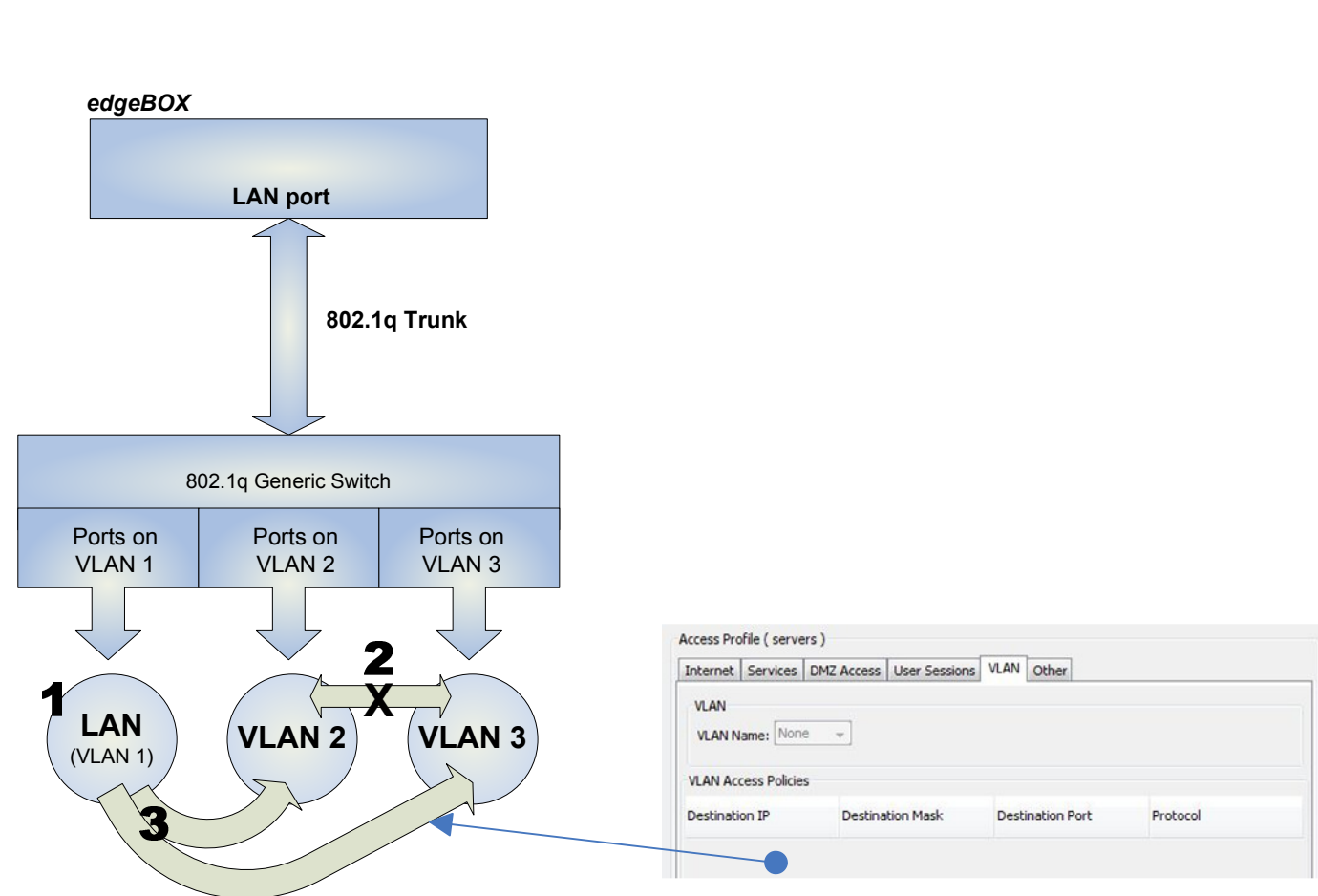


VLAN Scenario 1

- Standard 802.1q compatible switch
 - No 802.1x port based authentication
 - No Dynamic VLAN assignment
 - No native Guest Vlan on switch

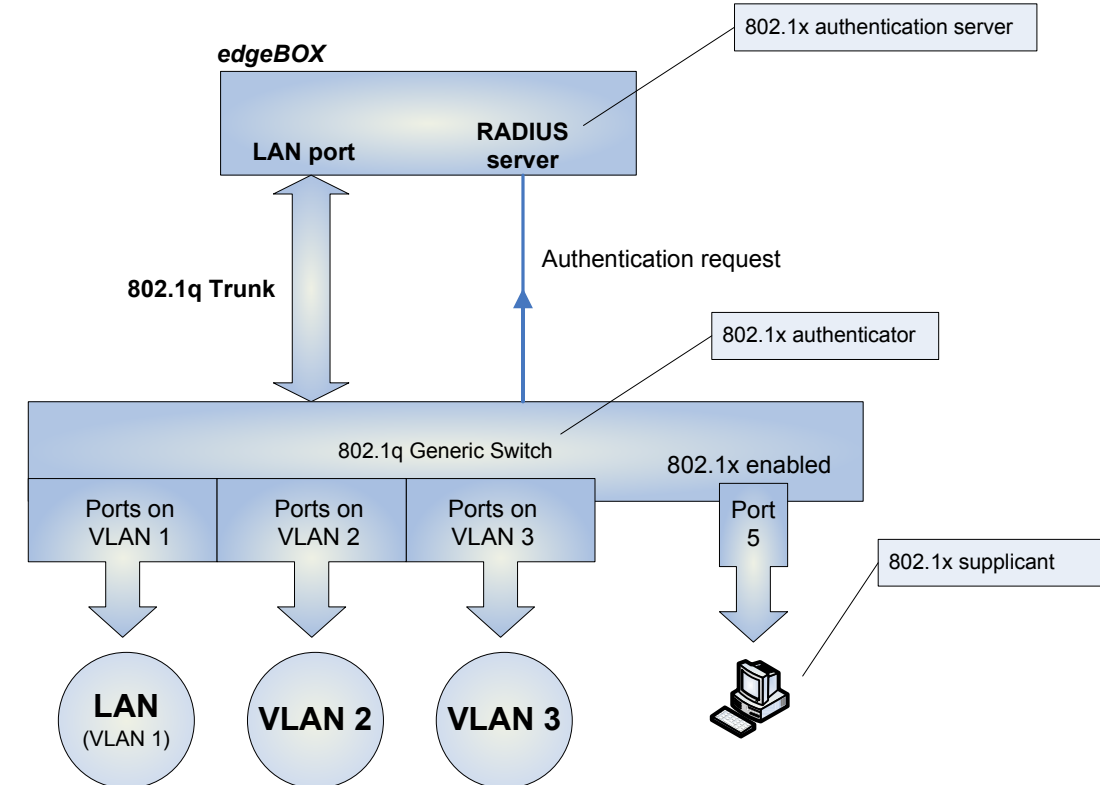


This is the most basic scenario when deploying VLANs with edgeBOX. In this case the LAN port of the edgeBOX is connected to a trunk port in the switch. The port on the switch must be configured as 802.1q trunk, allowing all configured VLANs to pass through the link.

- When using VLANs, the LAN zone is the same as VLAN 1 (id 1). In most cases the VLAN 1 is the default VLAN on a new installed switch, and this means all ports are by default configured as being part of that VLAN.
- By default, all traffic between VLAN zones is blocked. This means the edgeBOX firewall does not allow routing of traffic between VLANs unless the administrator configures it with different type of access rules.
- Access Rules between VLAN segments can be configured per access profile in the VLAN tab.
- The only type of user authentication available is Web Login. When a user authenticates successfully, the firewall enforces the configured User Access Profile rules for WAN, DMZ and access to other VLAN segments. If the user is not able to authenticate with success, then all traffic to and from this user will be filtered with the default rules for non-authenticated users.

VLAN Scenario 2

- Standard 802.1q compatible switch with 802.1x
 - Support for 802.1x port based authentication
 - No Dynamic VLAN assignment
 - No native Guest Vlan on switch



This is basically the same as Scenario 1. The only addition is that we have some or all ports on the switch configured for 802.1x port based authentication.

To enable support for 802.1x port based authentication we need to configure the switch to use the edgeBOX as the Radius server for authentication and enable the ports where we want this enforced. On the edgeBOX this 802.1x based switch, the radius client, needs to be authorized, and this is done in System->Radius->Add.

The edgeBOX supports protocol PEAP-EAP-MSCHAPv2. Both Windows XP and Vista include supplicants with native support for this authentication type.

In this scenario, for a client PC connected to one of the switch ports configured with 802.1x, the switch detects the presence of a client and initiates the 802.1x protocol. The authentication request, made by the Client PC supplicant, will be forwarded by the switch to the configured Radius server for authentication. If the authentication is successful the switch will open the respective port and the client will be part of the static VLAN configured on that Port. At this point the client will get an IP address if configured with dhcp and the edgeBOX DHCP server is enabled.

If the authentication is not successful then the port will be closed and the user will not get access to the network.

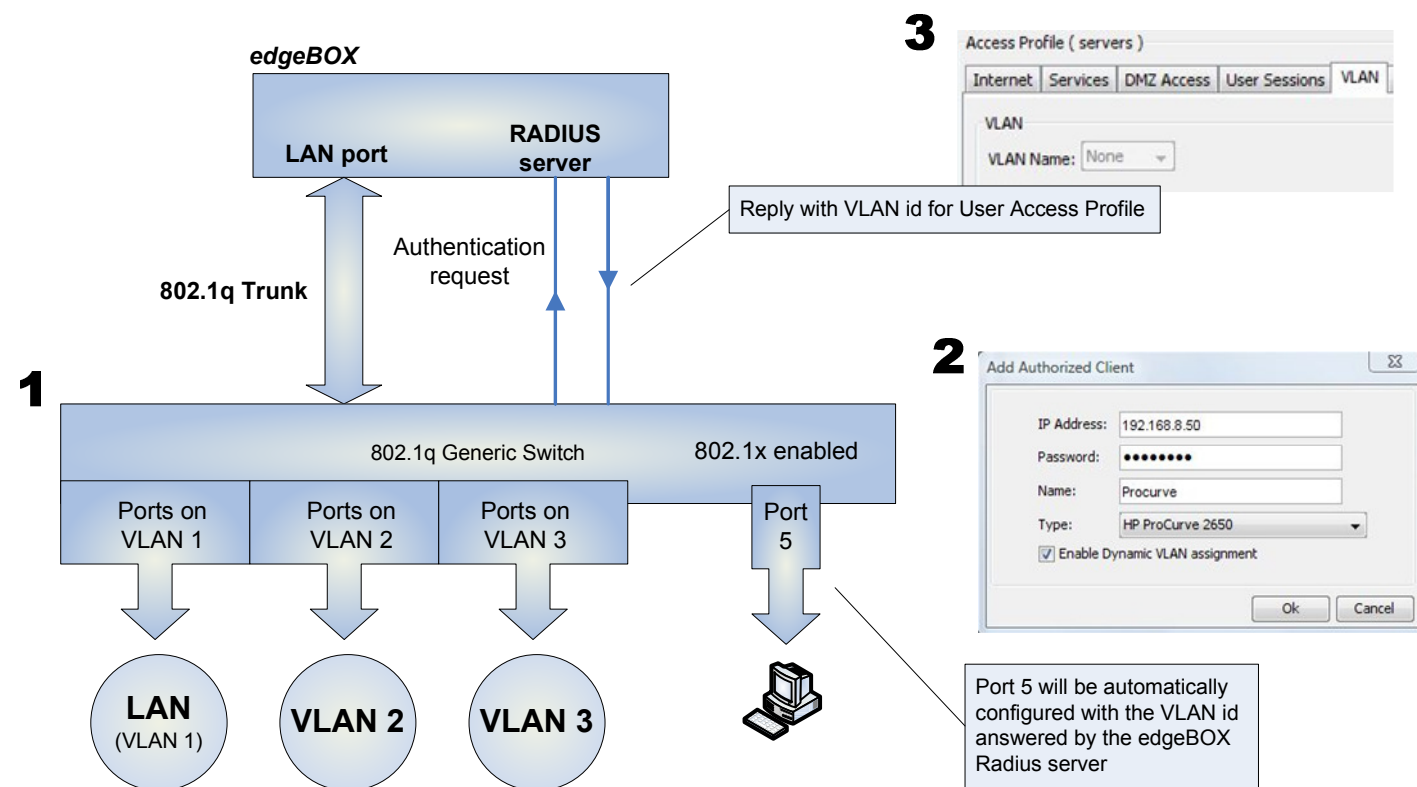
The main advantage of using 802.1x is that the user will not be able to access the network until he is able to get a successful authentication.

Support for Single Sign On (SSO)

Scenarios based on 802.1x include support for automatic user login. The only requirement is that a supported 802.1x switch is used to deploy those scenarios. A supported switch includes the calling station MAC address in the Radius Access Request packet and is able to process session timeout. In case the 802.1x switch does not support the calling station attribute, the port based authentication is still done but the user will need to do a normal weblogin when accessing the Internet or services running on the gateway.

VLAN Scenario 3

- 802.1q compatible switch with 802.1x and dynamic VLAN assignment
- Support for 802.1x port based authentication
- Support for Dynamic VLAN assignment – (HP Procurve switch)
- No native Guest Vlan on switch



This is scenario 2 with a switch that supports VLAN dynamic assignment. In this case, after a successful authentication, the switch moves the associated port to the VLAN configured for that user access profile. Without a successful authentication the port will be closed and the user wont be able to access the network.

During 802.1x authentication and on success, the Radius server sends additional attributes to the 802.1x authenticator in the switch with information regarding the VLAN id for that particular user. The edgeBOX supports assignment of a VLAN per access profile.

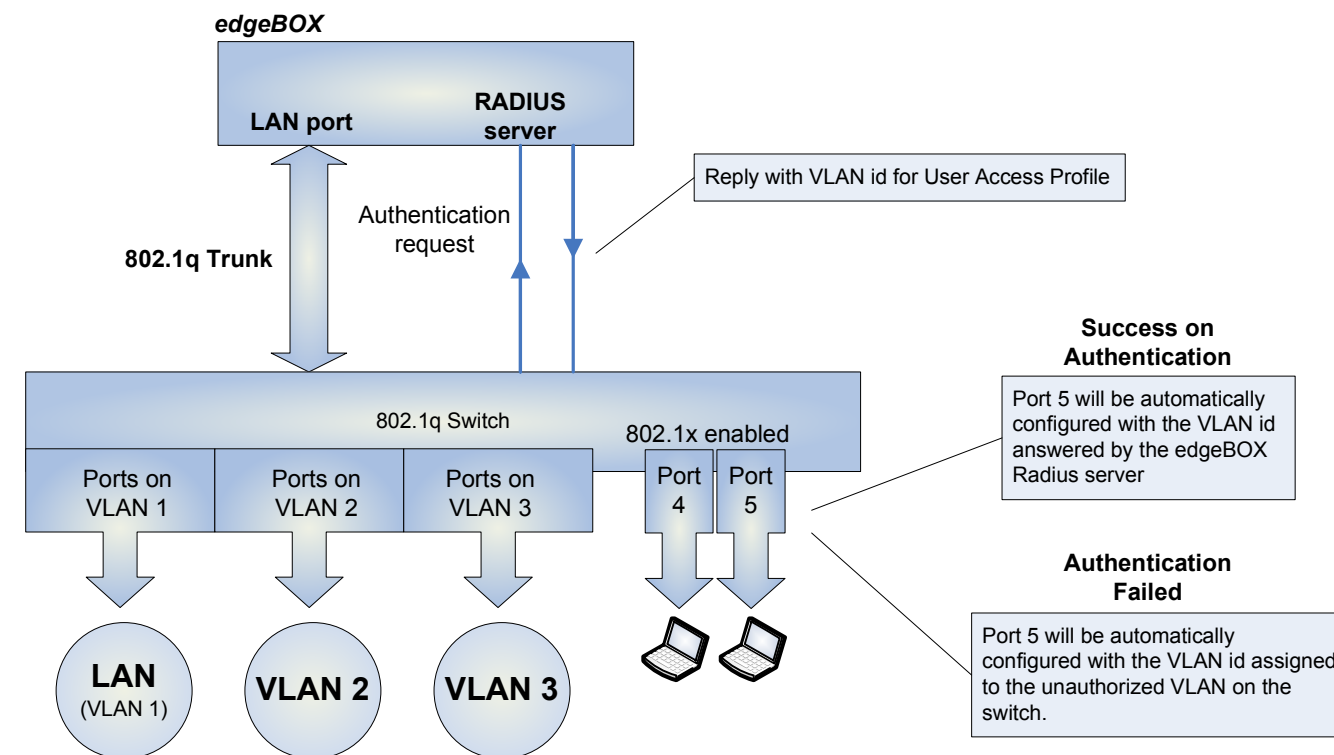
The following is needed to deploy this feature:

- 1** The network infrastructure must be setup with Procurve 2650 or compatible switches in terms of Radius dynamic Vlan assignment. The HP Procurve follows RFC2868 / 3580 with with *Tunnel-Private-Group-ID* of type *string*.
- 2** Configure the radius client as referred in Scenario 2, select the correct client type and enable Dynamic VLAN assignment.
- 3** Configure the User Access Profiles with the correct VLANs. See NAC->Access profiles->"Profile"->VLAN->VLAN Name.

The advantage of this scenario is the fact that we can effectively do network access control by port and at same time we are able to put the User in the correct VLAN even if he does a login outside of his main work space.

VLAN Scenario 4

- 802.1q compatible switch with 802.1x and dynamic VLAN assignment
- Support for 802.1x port based authentication
- Support for Dynamic VLAN assignment – (HP Procurve switch)
- Native Guest Vlan on switch – (HP Procurve switch)



This is scenario 3 with a switch that supports guest VLAN when operating with 802.1x and VLAN dynamic assignment.

This is similar with scenario 3 and the only difference is when the 802.1x user is not able to authenticate. At this point the switch automatically configures the port to another VLAN – the Unauthorized-Client VLAN. The unauthorized-client VLAN can be configured using the 802.1x Open VLAN mode in the Procurve 2650.

As soon as the switch assigns the unauthorized-client VLAN to that port, the connected host is able to get an IP through dhcp. If the edgeBOX authentication is enabled, the user will be presented with the edgeBOX web login page when trying to access the Internet.

A practical example:

- Switch ports 4 and 5 are setup for 802.1x with Unauthorized-Client VLAN assigned to VLAN6. These ports are located in a meeting Room.
- User01 is a member of the engineering profile, configured for VLAN3 (see #3 in scenario 3).
- User01 has his laptop ethernet connection setup for 802.1x authentication.
- Engineering profile has access to Internet, LAN and a few servers located in VLAN2.
- Guest01 is a member of the guest profile.
- Guest01 is a guest user with just a regular dhcp configuration on his laptop.
- Guest profile is configured to have open access to the Internet only. Users in this profile are not able to access any of the other VLANs or LAN.
- When User01 connects to port 4, a successful 802.1x authentication takes place and the switch port is automatically configured for VLAN3. User01 is able to work on his own VLAN and access any other places allowed by his Engineering access profile.
- When Guest01 connects to port 5, the switch is not able to start a 802.1x authentication and automatically opens the port on VLAN6. At this point he is able to get an IP address through dhcp and when trying to access the Internet he will be presented with the authentication page. With a successful web login authentication, the edgeBOX enforces the guest profile for this user and he is able to access the Internet but nothing else.
- Any other user that tries to connect to one of these ports, without a successful authentication, will be isolated in VLAN6.

edgeBOX Business Gateway

eOS 4.6 – VLAN Scenarios v 0.5

Critical

links