How To | use 802.1x VLAN assignment

Introduction

In a network environment that contains multiple VLANs, it can be very desirable for roaming users to be assigned to the same VLAN, no matter at which point they connect to the network. This means that they will always have access to the same set of network resources (and, of course, be subject to the same set of access restrictions) irrespective of which physical location on the network they happen to be connected to.

One solution that has been used on AT-9800 series and Switchblade switches to satisfy this requirement is the MAC-address based VLAN. But the MAC-address based VLAN is not easy to configure, as all the MAC addresses belonging to any given VLAN have to be configured onto every edge switch. Also, with MAC-address based VLANs, it is not possible to simultaneously satisfy the twin desires of, on the one hand, providing data separation between different MAC-address VLANs, and on the other hand, making it possible for any given port on an edge switch to be a member of multiple MAC-address VLANs.

To address these shortcomings of the MAC-address based VLAN, a new solution is now being provided, called *802.1x VLAN assignment*.

802.1x VLAN assignment is a technology allowing a port to become a member of one out of group of possible pre-configured VLANs, by using 802.1x Port Authentication.

Which product and software version does this document apply to?

The information provided in this document applies to the following products:

- AT-8624, AT-8948, AT-9900, AT-9800, and Rapier series switches, and SwitchBlade

running software version 2.7.3 onwards.

How 802.1x VLAN assignment works

When a PC is connected to a switch port, firstly the port issues an 802.1x authentication challenge to the attached device (the 802.1x supplicant). The supplicant replies with username and password and then an authentication request is passed to a configured Radius server. The authentication server's user database supports Extended Authentication Protocol (EAP), which allows particular VLAN membership to be defined for each individual user. After authorisation, the port connected to the authenticated supplicant then becomes a member of the specified VLAN.

A fuller description of 802.1x authentication is available in the reference document [1]. The url for this is mentioned on page 5.

Note that port-based VLAN membership is used. The authenticated port will be removed from any previously configured VLANs. The port cannot be a member of multiple VLANs.

So, when multiple users each connect to a port on the same edge switch, if the Radius database entries for those users all specify different VLANs, the ports they have connected to will all be put into different port-based VLANs. By this method, 802.1x VLAN assignment can provide truly secure data separation.

In contrast, the limitation of MAC-based VLANs was because VLAN membership was considered on a packet-by-packet basis. Therefore, the switch port could easily be a member of several VLANs at once, and this makes data separation difficult.

A typical example

Consider the 802.1x VLAN assignment solution below. It provides a solution for a school, which has three groups of users:

- students
- trusted students
- staff

The requirements are:

- a member of one of the three groups can connect to any port on any edge switch, and immediately be assigned to the VLAN appropriate to their group.
- complete data separation is achieved between the three VLAN groups - no member of one group can exchange data with a member of another group.

Configuration for an ATI device as the authenticator

In this example the Radius server is accessed via the "authentication" VLAN. This is the only VLAN with an IP address. All other ports provide simple Layer 2 switching after VLAN membership is confirmed.

Note that all VLANs must be pre-defined (i.e. created) before 802.1x supplicant ports can be dynamically added to the appropriate VLAN by 802.1x.

The following steps are required to configure the Allied Telesyn device as the Authenticator, having port authentication and VLAN assignment enabled on ports 1 through 23:

▶ Configure the pre-defined VLANs:

```
create vlan="students" vid=2
create vlan="trusted students" vid=3
create vlan="staff" vid=4
```

It is not necessary to add edge ports to VLANs in the configuration. 802.1x VLAN assignment will add ports dynamically.

▶ Add tagged uplink ports to all the VLANs:

```
add vlan=2 port=24 frame=tagged
add vlan=3 port=24 frame=tagged
add vlan=4 port=24 frame=tagged
```

▶ Enable IP:

Only the "authentication" VLAN has a port and IP address assigned, to allow Radius authentication

```
enable ip
add ip int=vlan1 ip=10.0.10.254 mask=255.255.255.0
```

▶ Define the Radius authentication server:

```
add radius server=10.0.10.10 secret="testing123" port=1812
```

▶ Configure port authentication on ports 1 through 23:

```
enable portauth=8021x

enable portauth=8021x port=1-23 type=authenticator
```

Any school user can now connect to ports 1-23 - they will be 802.1x authenticated and then have appropriate VLAN assigned.

Configuring your Radius server for EAP authentication and VLAN assignment

It is possible, for example, to use a FreeRadius Radius Authentication Server on the Linux Operating System. Extended Authentication Protocol (EAP) is used to authenticate users and define VLAN membership. Other EAP capable Radius Servers could also be used.

FreeRadius defines the users in a file called *users*. The RADIUS administrator needs to edit the "users" file to add in approved users. In the *users* file you can specify the VLAN memberships for users using EAP authentication, by using the following format:

```
mary  Auth-Type := EAP, User-Password == "moretest"

      Reply-Message = "Hello, %u",

        Tunnel-Type = "VLAN",

        Tunnel-Medium-Type = "IEEE-802",

        Tunnel-Private-Group-ID = "students"
```

The `Tunnel-Private-Group-ID` field defines the VLAN name or number that this user must join.

When you add your user definitions, ensure that the syntax is correct for all the tunnel definition fields, as shown above. On FreeRadius, a definition file is available which defines the correct syntax for all the fields. The file is called *dictionary.tunne*l.

An example of 802.1x supplicant configuration

An example of 802.1x supplicant configuration is available in the reference document [1]).

Reference Document

[1] 802.1x Port Authentication

Available at: *http://www.alliedtelesyn.co.nz/support/technotes/pdf/8021x.pdf*

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesyn.com