

# Configuring 802.1x authentication and Unauthenticated VLAN on a PowerConnect 6024

Written by: Greg Gibbs 4/25/2005

The 2.x firmware for the PowerConnect 6024 adds support for 802.1x port authentication and Unauthenticated VLAN. IEEE 802.1x port authentication provides another layer of security for network devices. When a client connects to a port on the switch, they must provide a username and password to be granted access to the network. The IEEE standard defines the following terms:

- **Supplicant** – The 802.1x agent or application running on the client
- **Authentication Server** – The system performing authentication (typically a RADIUS server)
- **Authenticator** – The intermediary device between the Supplicant and Authentication Server (typically a switch or Wireless Access Point)

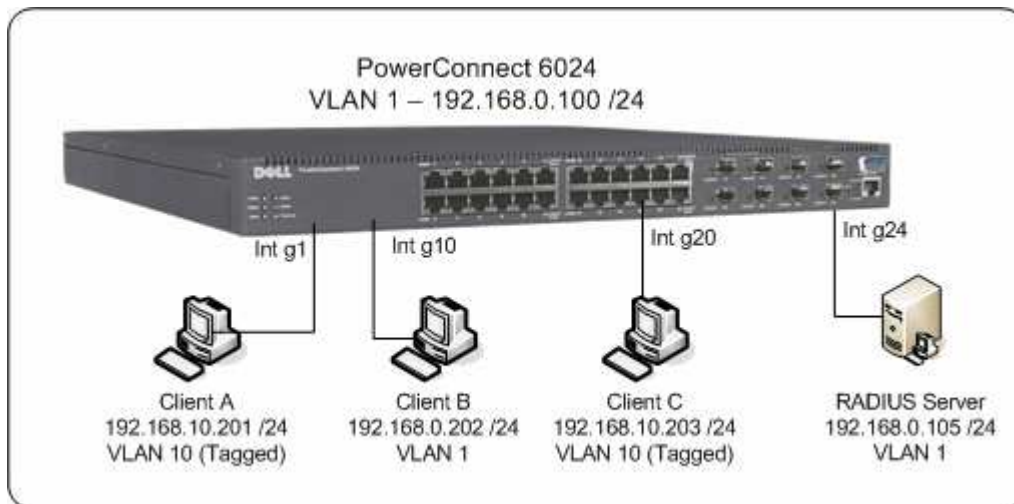
The following steps outline the procedure used for 802.1x port authentication:

1. A client is connected to an 802.1x enabled port
2. The Authenticator detects the active link and sends an “EAP Request, Identity” packet to the Supplicant.
3. The Supplicant prompts the user for a username and password and replies to the Authenticator by sending an “EAP Response, Identity” packet, which is then passed to the Authentication Server.
4. The Authentication Server sends an authentication challenge to the Authenticator which is then re-packaged and sent to the Supplicant.
5. The Supplicant replies to the challenge and the Authenticator passes it to the Authentication Server.
6. If the proper credentials are given, the Authentication Server sends a “RADIUS Access Accept” packet to Authenticator, which then re-packages it and passes it to the Supplicant as an “EAP Success” packet. In this case, the switch would set the port mode to Authorized and the client would gain access to the LAN using the default VLAN configuration for the port.

If the proper credentials are not given, the Authentication Server sends a “RADIUS Access Reject” packet the Authenticator, which then re-packages it and passes it to the Supplicant as an “EAP Failure” packet.

If authentication passes, the client is given access to the network and the VLAN configuration on the port will be used.

An Unauthenticated VLAN can be configured on the switch for a scenario in which authentication fails. When the port is in an UNAUTHORIZED state, it will only accept traffic tagged with the VID (VLAN ID) of the Unauthenticated VLAN. All untagged traffic will be dropped.



The configuration listed in this document is based on the following topology:

For this example, the Client A and Client C NICs have been configured to use tagged frames (using Intel ProSet) with VLAN ID 10. This was done because a port cannot be configured as an untagged member of an Unauthenticated VLAN.

### **Basic Configuration:**

```
console# configure
console(config)# vlan database
console(config-vlan)# vlan 10
console(config-vlan)# exit
console(config)# interface vlan 1
console(config-if)# ip address 192.168.0.100 /24
console(config-if)# exit
console(config)# interface range ethernet g1,g20
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 10
```

### **802.1x Configuration:**

(Define VLAN 10 as the Unauthenticated VLAN)

```
console# configure
console(config)# interface vlan 10
console(config-vlan)# dot1x auth-not-req
```

(Define the RADIUS server & key)

```
console(config)# radius-server host 192.168.0.105
console(config)# radius-server key mysecretkey (must match RADIUS server config)
```

**(Configure AAA to use the RADIUS server for 802.1x authentication)**

```
console(config)# aaa authentication dot1x default radius
```

**(Enable 802.1x globally)**

```
console(config)# dot1x system-auth-control
```

**(Configure ethernet interfaces to automatically authenticate)**

```
console(config)# interface range ethernet g1,g10
```

```
console(config-if)# dot1x port-control auto
```

**(Disable 802.1x Multiple-Host support on g1 & g10 since only one client should be connected)**

```
console(config)# interface range ethernet g1,g10
```

```
console(config-if)# no dot1x multiple-hosts
```

### **Conclusion:**

When Client B is connected to the switch, the user will be prompted for a username and password. If the correct credentials are used, port g10 will transition to an AUTHORIZED state and Client B will communicate with other members of VLAN 1.

If Client A is configured to use tagged frames on VLAN 10, port g1 will remain in the UNAUTHORIZED state and will only allow tagged frames with VID 10. With this configuration, Client A will communicate with other members of VLAN 10.

If the VLAN configuration is removed from Client A (or Client A is replaced with another untagged 802.1x client), the client will be prompted for a username and password. If the correct credentials are used, port g1 will transition to an AUTHORIZED state and Client A will communicate with other members of VLAN 1.