



Configuring Identity Networking

- [Information About Identity Networking, page 1](#)
- [RADIUS Attributes Used in Identity Networking, page 2](#)

Information About Identity Networking

In most wireless LAN systems, each WLAN has a static policy that applies to all clients associated with an SSID. Although powerful, this method has limitations because it requires clients to associate with different SSIDs to inherit different QoS and security policies.

However, the Cisco Wireless LAN solution supports identity networking, which allows the network to advertise a single SSID but allows specific users to inherit different QoS or security policies based on their user profiles. The specific policies that you can control using identity networking are as follows:

- **ACL**—When the ACL attribute is present in the RADIUS Access Accept, the system applies the ACL name to the client station after it authenticates, which overrides any ACLs that are assigned to the interface.
- **VLAN**—When a VLAN Interface-name or VLAN tag is present in a RADIUS Access Accept, the system places the client on a specific interface.



Note The VLAN feature only supports MAC filtering, 802.1X, and WPA. The VLAN feature does not support web authentication or IPsec.

- Tunnel Attributes.



Note When any of the other RADIUS attributes (QoS-Level, ACL-Name, Interface-Name, or VLAN-Tag), which are described later in this section, are returned, the Tunnel Attributes must also be returned.

The operating system's local MAC filter database has been extended to include the interface name, allowing local MAC filters to specify to which interface the client should be assigned. A separate RADIUS server can also be used, but the RADIUS server must be defined using the Security menus.

RADIUS Attributes Used in Identity Networking

QoS-Level

This section explains the RADIUS attributes used in identity networking.

This attribute indicates the QoS level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The text boxes are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   | Length   |                               Vendor-Id   |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
|                               QoS Level                               |
+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – Three octets:
 - 3 – Bronze (Background)
 - 0 – Silver (Best Effort)
 - 1 – Gold (Video)
 - 2 – Platinum (Voice)

ACL-Name

This attribute indicates the ACL name to be applied to the client. A summary of the ACL-Name Attribute format is shown below. The text boxes are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   | Length   |                               Vendor-Id   |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
|                               ACL Name...                               |
+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179

- Vendor type – 6
- Vendor length – >0
- Value – A string that includes the name of the ACL to use for the client

Interface Name

This attribute indicates the VLAN Interface a client is to be associated to. A summary of the Interface-Name Attribute format is shown below. The text boxes are transmitted from left to right.

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   | Length |           Vendor-Id           |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Interface Name...
+-----+-----+-----+-----+-----+-----+-----+-----+
    
```

- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5
- Vendor length – >0
- Value – A string that includes the name of the interface the client is to be assigned to.



Note This Attribute only works when MAC filtering is enabled or if 802.1X or WPA is used as the security policy.

VLAN Tag

This attribute indicates the group ID for a particular tunneled session and is also known as the Tunnel-Private-Group-ID attribute.

This attribute might be included in the Access-Request packet if the tunnel initiator can predetermine the group resulting from a particular connection and should be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. Private groups may be used to associate a tunneled session with a particular group of users. For example, it may be used to facilitate routing of unregistered IP addresses through a particular interface. It should be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop and which pertain to a tunneled session.

A summary of the Tunnel-Private-Group-ID Attribute format is shown below. The text boxes are transmitted from left to right.

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   | Length | Tag | String...
+-----+-----+-----+-----+-----+-----+-----+-----+
    
```

- Type – 81 for Tunnel-Private-Group-ID.

- Length – ≥ 3
- Tag – The Tag text box is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. If the value of the Tag text box is greater than 0x00 and less than or equal to 0x1F, it should be interpreted as indicating which tunnel (of several alternatives) this attribute pertains. If the Tag text box is greater than 0x1F, it should be interpreted as the first byte of the following String text box.
- String – This text box must be present. The group is represented by the String text box. There is no restriction on the format of group IDs.

**Note**

When any of the other RADIUS attributes (QoS-Level, ACL-Name, Interface-Name, or VLAN-Tag) are returned, the Tunnel Attributes must also be returned.

Tunnel Attributes

RFC 2868 defines RADIUS tunnel attributes used for authentication and authorization, and RFC2867 defines tunnel attributes used for accounting. Where the IEEE 802.1X authenticator supports tunneling, a compulsory tunnel may be set up for the Supplicant as a result of the authentication.

In particular, it may be desirable to allow a port to be placed into a particular VLAN, defined in IEEE 8021Q, based on the result of the authentication. This configuration can be used, for example, to allow a wireless host to remain on the same VLAN as it moves within a campus network.

The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept. However, the IEEE 802.1X authenticator may also provide a hint as to the VLAN to be assigned to the Supplicant by including Tunnel attributes within the AccessRequest.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

The VLAN ID is 12 bits, with a value between 1 and 4094, inclusive. Because the Tunnel-Private-Group-ID is of type String as defined in RFC 2868, for use with IEEE 802.1X, the VLANID integer value is encoded as a string.

When Tunnel attributes are sent, it is necessary to fill in the Tag text box. As noted in RFC 2868, section 3.1:

- The Tag text box is one octet in length and is intended to provide a means of grouping attributes in the same packet that refer to the same tunnel. Valid values for this text box are 0x01 through 0x1F, inclusive. If the Tag text box is unused, it must be zero (0x00).
- For use with Tunnel-Client-Endpoint, Tunnel-Server-Endpoint, Tunnel-Private-Group-ID, Tunnel-Assignment-ID, Tunnel-Client-Auth-ID or Tunnel-Server-Auth-ID attributes (but not Tunnel-Type, Tunnel-Medium-Type, Tunnel-Password, or Tunnel-Preference), a tag text box of greater than 0x1F is interpreted as the first octet of the following text box.
- Unless alternative tunnel types are provided, (e.g. for IEEE 802.1X authenticators that may support tunneling but not VLANs), it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLANID, the tag text box should be set to zero (0x00) in all tunnel

attributes. Where alternative tunnel types are to be provided, tag values between 0x01 and 0x1F should be chosen.

