araknis NETWORKS

PORT-BASED VLAN SETUP GUIDE

FOR ARAKNIS NETWORK PRODUCTS

Related Products: AN-210/310 Managed Switches
AN-300-RT-4L2W Router
All Wireless Access Point Models

1 - Contents

Araknis Networks supports other VLAN setup methods not covered in this document. See the full manuals on the product page support tabs or contact us for more information.

2 - Introduction

This guide will help you understand the basic operation and setup of Araknis port-based VLAN features using the following Araknis Networks equipment:

- AN-300-RT-4L2W Router
- 210 and 310 Managed Network Switches
- 100, 300, 500, and 700 Series Wireless Access Points

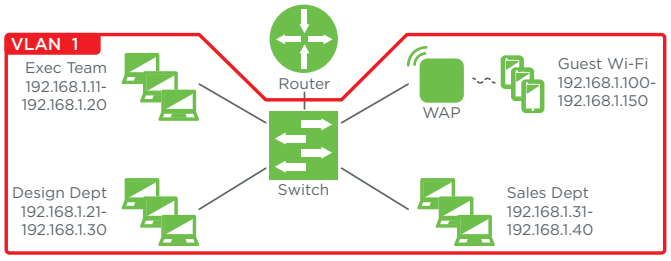
> **Note –** We do not recommend implementing VLANs unless you have at least one managed switch in the LAN to serve as the core switch.

3 - VLAN Basics

VLANs, or **V**irtual **L**ocal **A**rea **N**etworks, segment a LAN into logical sub-networks with isolated broadcast domains over the same physical topology.

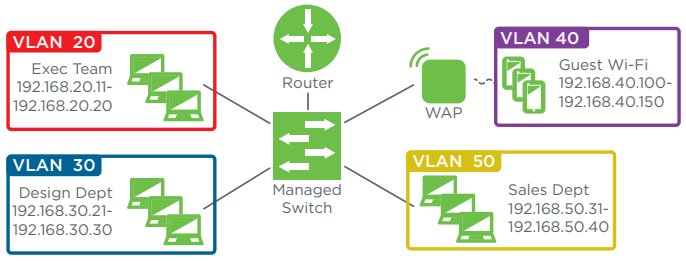
In other words, different VLANs behave like isolated networks, even though data is moving through the same physical network. VLANs logically group together client devices that need to communicate, and restrict data from clients that shouldn't be receiving it.

Logical Topology Without VLANs



All devices can freely communicate

Logical Topology With VLANs



Traffic is restricted to the specified VLAN

Port-based setup assigns physical LAN ports to a specific VLAN. You must know which ports client devices are connected to and which ports link between network switches and the router. This method is easy to set up and maintain as long as the physical network doesn't change often. Modifying or adding connections later will also require appropriate VLAN settings.

Why Set Up VLANs?

- **Added Security –** Clients sharing sensitive data can be placed in a separate VLAN to restrict other users from listening in on traffic. This is often the most useful application for VLANs in small home and office networks.

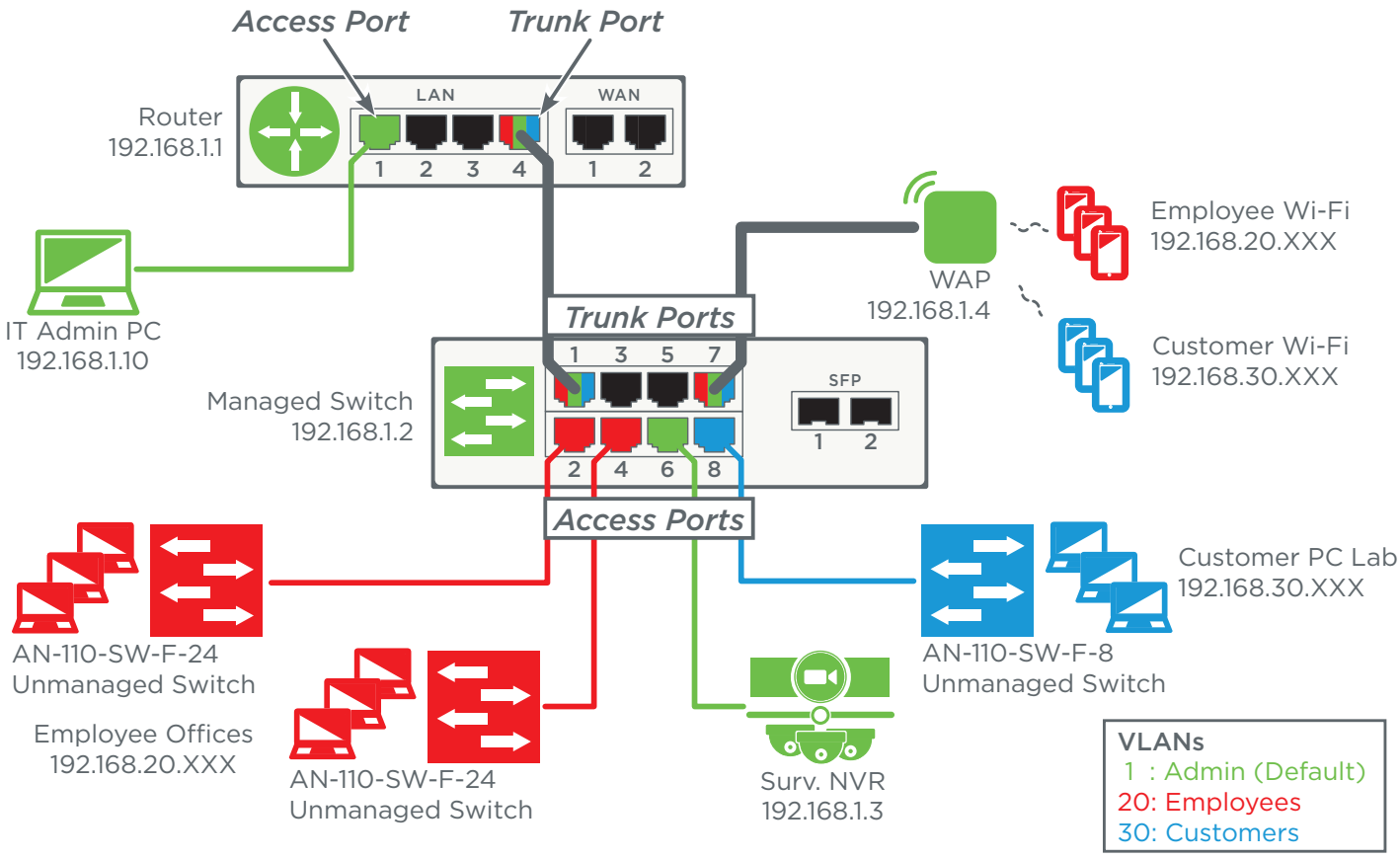
- **Reducing Traffic –** Broadcasts, or data sent to all LAN devices, makes up a large part network traffic. Small LANs can handle this with no problems, but larger networks can begin to slow down. Using VLANs, broadcasts can be limited to reaching only relevant devices.

4 - How Araknis Port-Based VLANs Work

Araknis equipment utilizes the IEEE 802.1Q VLAN tagging protocol to manage port-based VLANs. Ports being actively used in a VLAN are assigned to one of two roles:

- **Access ports** are assigned to only one VLAN and are generally used to connect clients. Also known as **untagged** ports because all traffic moving through is assumed to belong to the specified VLAN. Multiple clients can connect to a single access port by using a switch as long as they are all in the same VLAN.
- **Trunk ports** carry traffic for more than one VLAN to other network devices such as a router, managed switch, or access point. Also known as **tagged** ports, because they need to keep track of each VLAN's data simultaneously.

Ports may also be excluded from a VLAN (or disabled altogether) to prevent any connected device from gaining access.



5 - Best Practices

- **Planning** is the key to success with port-based VLANs. Identify your needs, plan the network topology accordingly, then complete equipment setup.

- Use the fewest number of VLANs possible to accomplish your goals, especially in small networks. You might use one VLAN for guests, and leave everything else on the default, untagged VLAN. Or, place all users in a separate VLAN and leave the default for admin use and equipment access only.

- Consider shared resources such as printers and file servers. Ensure that clients have access to all the resources they need. If clients need access to other VLANs, you may need to complete some advanced setup (contact us for help) or provide additional equipment for each VLAN.

- Minimize cost and setup time by using fewer managed switches. Instead of configuring an access port for each client in a VLAN, connect a managed switch access port to an unmanaged switch, then connect more clients to that VLAN as needed.

- Designate one VLAN ID for IT device management and configure one or more LAN ports specifically for IT management, then remain connected to these ports during setup to avoid losing access. We recommend using the default VLAN ID 1. In the following example, we use a router port, but it can be any LAN port configured as an access port on the default or management VLAN.

6 - Planning and Setup

This section uses a real-world example to demonstrate proper port-based VLAN planning and setup. In the example, we are reconfiguring a flat LAN in a growing small business and implementing VLANs to separate client and employee traffic.

Step 1 – Identify your needs.

Why are you planning to use VLANs? Clearly defined solutions to problems will make it much easier to implement VLANs successfully. Discuss past issues and current and future needs with your client to avoid unexpected surprises.

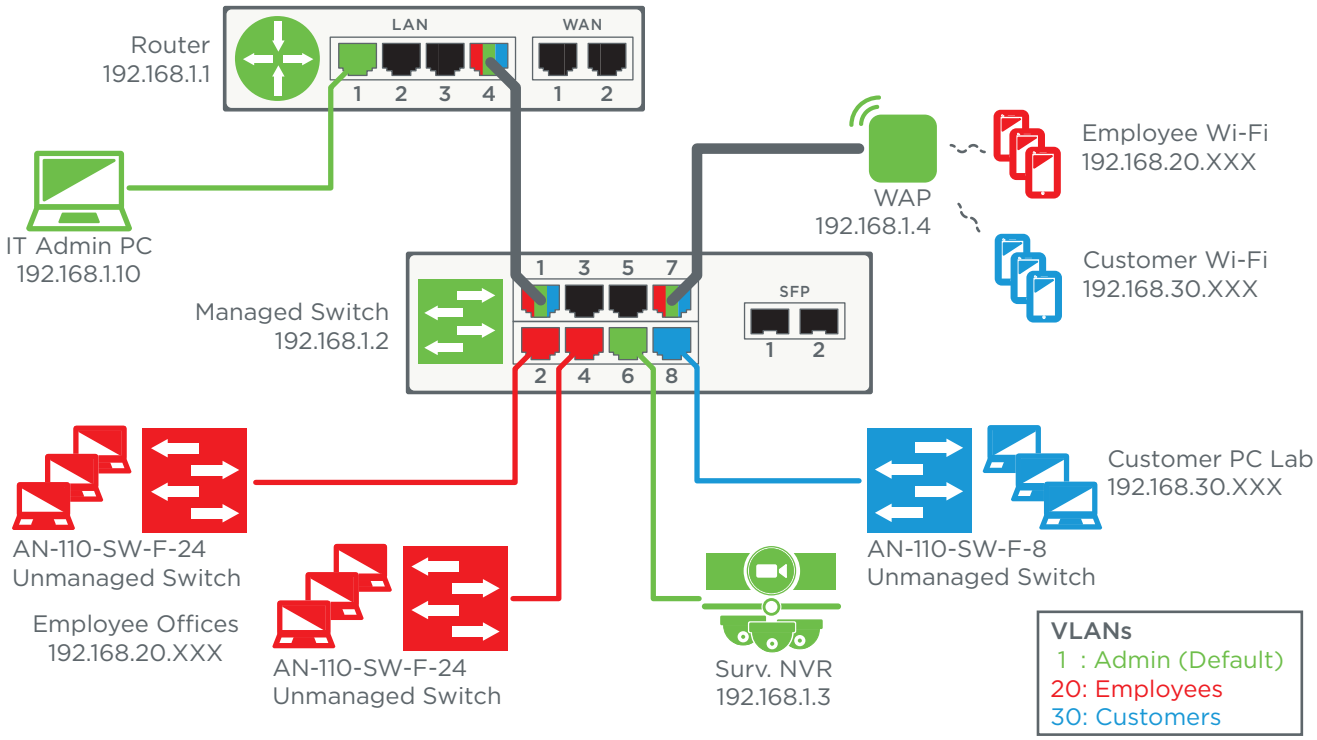
Example Goals:

- *Separate customer and employee traffic to improve security.*
- *Limit access to network and surveillance equipment to IT staff only.*
- *Dedicate one Internet connection for employees and one for customers.*
- *Configure one router port for IT device management.*
- *Disable unused router ports to avoid security issues.*
- *Create one secured Wi-Fi SSID for employees.*
- *Create one secured Wi-Fi SSID for customers.*

Step 2 – Plan the topology.

Your topology should detail which VLAN each client is a part of, which access ports connect those clients, and which trunk ports connect between equipment. You may also want to configure unused ports for future expansion, or disable them to prevent unwanted access. Example:

VLAN 01 Admin (Default)	VLAN 20 Employees	VLAN 30 Clients
IT Admin PC	Sales Team (20 workstations)	Client Wi-Fi
Surveillance System NVR	Accounting (12 workstations)	Client Work Area (5-10 clients)
Router Web GUI	Employee Wi-Fi	
Managed Switch Web GUI		
WAP Web GUI		



Step 3 – Build a setup checklist.

List the VLAN IDs to be configured on each port and make note of custom settings that are required.

Router	
Port	VLAN IDs
LAN 1 (Access)	1
LAN 2	—
LAN 3	—
LAN 4 (Trunk)	1, 20, 30

Switch					
Port	Type	VLAN IDs	Port	Type	VLAN IDs
1	Trunk	1, 20, 30	5	None	—
2	Access	20	6	Access	1
3	Access	20	7	Trunk	1, 20, 30
4	Access	20	8	Access	30

*Configure route binding: VLAN 1, 20 on WAN1; VLAN 30 on WAN2 (see router setup).

*Configure WAP SSIDs with correct VLAN ID (see WAP setup).

Step 4 – Connect and configure equipment.

The last step is setting up the equipment. First, you need to make the right connections, then you can configure the ports using the setup menus. We recommend setting up the router first.

Each of the following sections details correct setup for the example we have been using. Refer to the previous page to better understand the settings being configured.

7 - Configuring the Router

Adding new VLANs in the router is fairly easy, but the port settings can be confusing. We recommend creating all the new VLAN IDs, saving the settings, then configuring settings for each port.

Step 1 – Create New VLANs

A. Connect your computer to the designated IT management port. In our example, this is router LAN port 1.

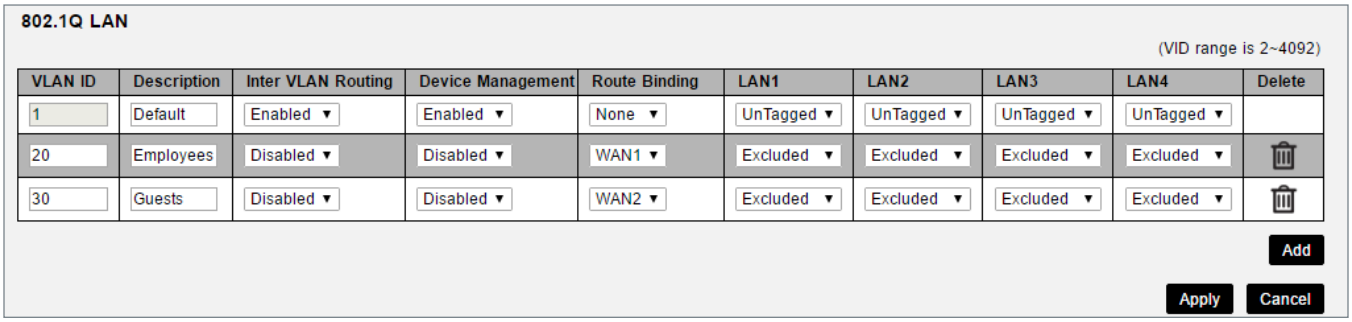
B. Log into the router as an administrator and navigate to Advanced, VLANs.

C. Click the **Add** button to create the desired number of new VLAN IDs, then change the IDs and descriptions for each one. For our example, we added two new entries, VLAN IDs 20 and 30.

D. You may also configure other general setting for each VLAN at this time:

- **Inter-VLAN Routing –** Enable this feature for any VLANs that need to communicate. Disabled by default. Do not use if security between VLANs is a concern.
- **Device Management –** When enabled, the router setup menu may be accessed from that VLAN. **Important:** Disabling this Device Management on all VLANs will cause you to lose access to the router! A factory default will be required to regain access. We recommend enabling this setting on one "management" VLAN only. Enabled on VLAN 1 by default.
- **Route Binding –** Tie all Internet traffic for a VLAN to WAN 1 or WAN 2 port. Disabled by default. In our example, WAN 1 is used for all employee traffic and WAN 2 is for all client traffic.

E. Click **Apply** to save the settings once you have all VLANs configured to this point.



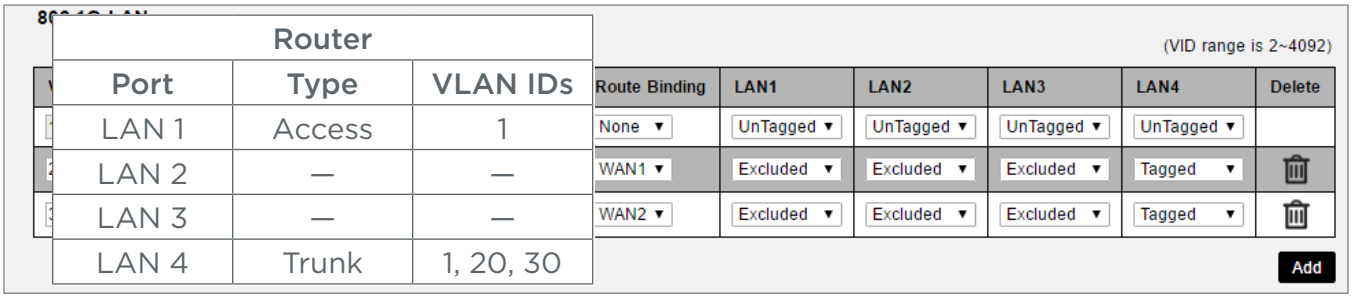
This screenshot illustrates the settings used for our example. The default VLAN 1 is used for managing IT devices. We added VLAN 20 for employees and 30 for guests, with route binding configured as specified for each one.

Step 2 – Configure LAN Ports for VLANs

A. Each router LAN port's role in each VLAN must be configured separately. Click the dropdowns to change each setting for your application.

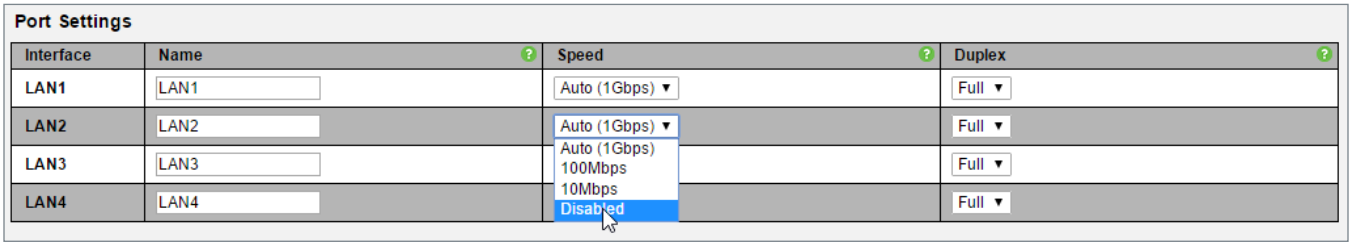
- **Access** ports should be set to **Untagged** for that VLAN, and set to **Excluded** for the remaining VLANs. (Access = all connected devices belong to a single VLAN ID.)
- **Trunk** ports should be set to **Untagged** for the default VLAN ID, **Tagged** for other included VLANs, and **Excluded** for VLANs not connected. (Trunk = connected devices belong to multiple VLAN IDs.)

B. Click **Apply** to save the new settings.



As you can see in the screenshot, the settings for each LAN port can get confusing as the number of VLANs increases. Use the notes from the planning phase to easily determine the settings required for each port, and remember that each LAN port must be set to Untagged on exactly one VLAN ID.

- **LAN 1 –** In our application, LAN Port 1 will only be used by IT for access to the default VLAN ID 1. The default settings are already correct. If data tagged with VLAN ID 20 or 30 reaches the port it will be dropped.
- **LAN 4 –** LAN Port 4 is the trunk between the router and the managed switch for all VLAN IDs. We set VLAN 1 to Untagged and VLANs 20 and 30 to Tagged. If untagged data reaches the port it will be tagged with the default VLAN ID.
- **LAN 2 & 3 –** These ports will not be used, but they can't be totally disabled in this menu. We will leave the default VLAN settings and disable the ports in the Settings > LAN > Port Settings menu, shown below, by changing the Speed dropdowns for LAN Ports 2 and 3 to **Disabled** as shown below:



Remember to click **Apply** before leaving a page to save all of the new settings. Once you have these settings configured, router setup for VLANs is complete.

8 - Configuring Managed Switch Ports

VLAN setup in the Araknis managed switch is similar to the router, but instead of using the settings, tagged, untagged, and excluded, ports are configured as either, trunk, access, or none for each VLAN ID.

When configuring port-based VLANs in the Araknis switch, we recommend creating all the new VLAN IDs first, saving the settings, then configuring the port settings for each VLAN ID.

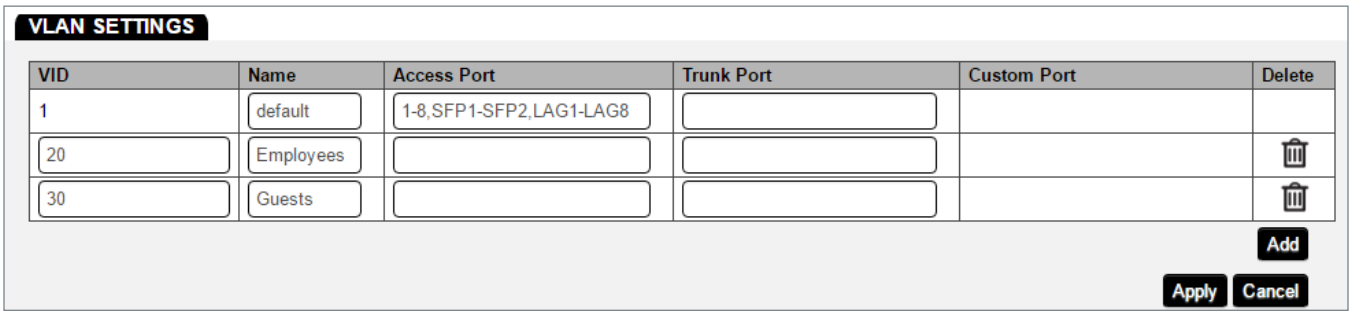
Step 1 – Create New VLANs

> **Note –** Leave your computer connected to the specified IT management port used for router setup to avoid losing access to the switch during setup. See section "5 - Best Practices" on page 4 for more information about setting up IT management ports.

A. Log into the switch as an administrator and navigate to Settings > VLANs.

B. Click the **Add** button to create the desired number of new VLAN IDs, then change the IDs and descriptions for each one. For our example, we added two new entries, VLAN IDs 20 and 30.

C. Click **Apply** to save the settings once you have all VLANs configured to this point.



This screenshot illustrates the settings used for our example. The default VLAN 1 is used for managing IT devices. We added VLAN 20 for employees and 30 for guests.

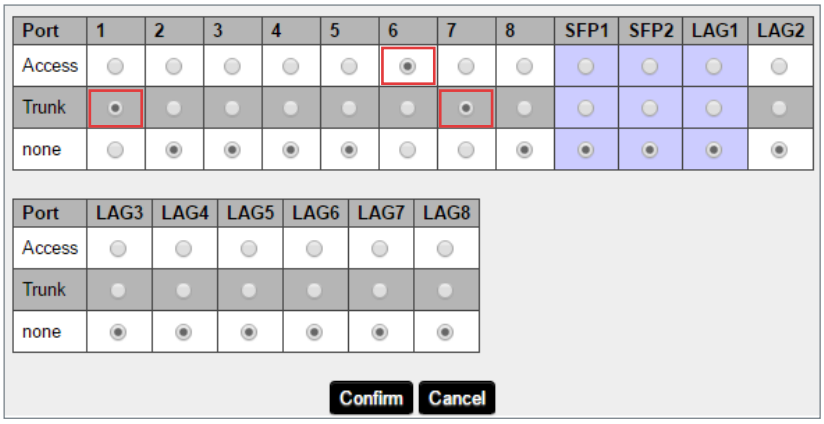
Step 2 – Configure LAN Ports for VLANs

A. Click the Access or Trunk Port field for default VLAN ID 1 to open the port settings menu, then configure each LAN port's role for that VLAN. Refer to the notes you made during the planning phase to make it easier.

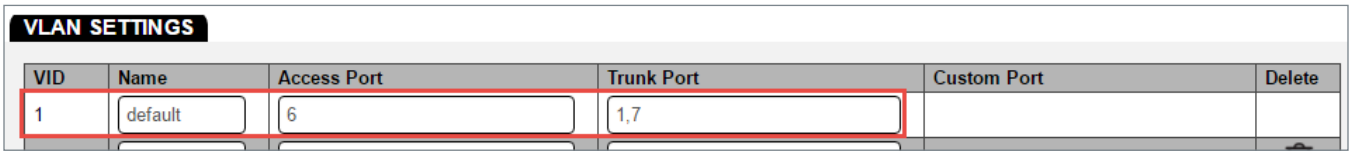
- Set the **Access** and **Trunk** ports accordingly.
- Set any ports that are not included in the VLAN to **none**.

The VLAN ID 1 settings for our example are shown in the screenshot below. We set all unused ports for the VLAN to **none** to avoid any possibility of traffic reaching the wrong destination.

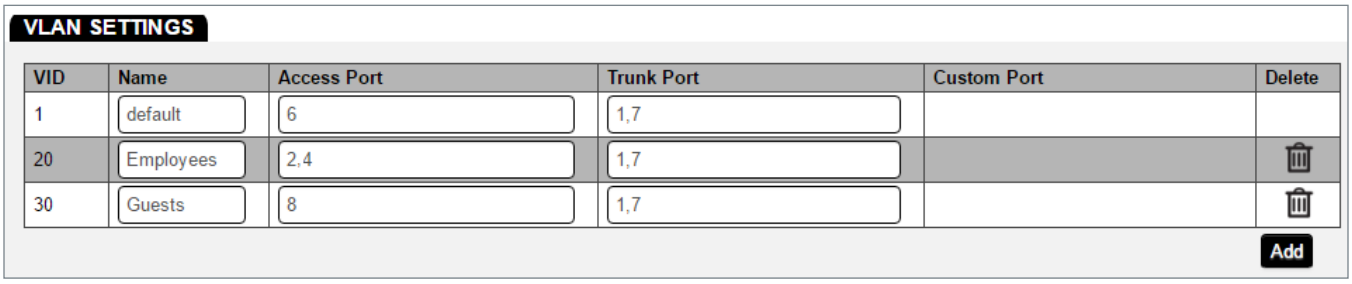
Switch		
VLAN ID	Access	Trunk
1	6	1,7
20	2,4	1,7
30	8	1,7



B. Click **Confirm** to save the settings. You will see the new settings appear in the VLAN menu:



C. Complete the setting changes for the remaining VLAN IDs, then click **Apply** to save the new settings. Completed settings for our example are shown below.



9 - Configuring WAP SSIDs

Configuring VLANs in Araknis Wireless Access Points is the easiest part of setup. Each SSID can be set to tag traffic for one VLAN ID.

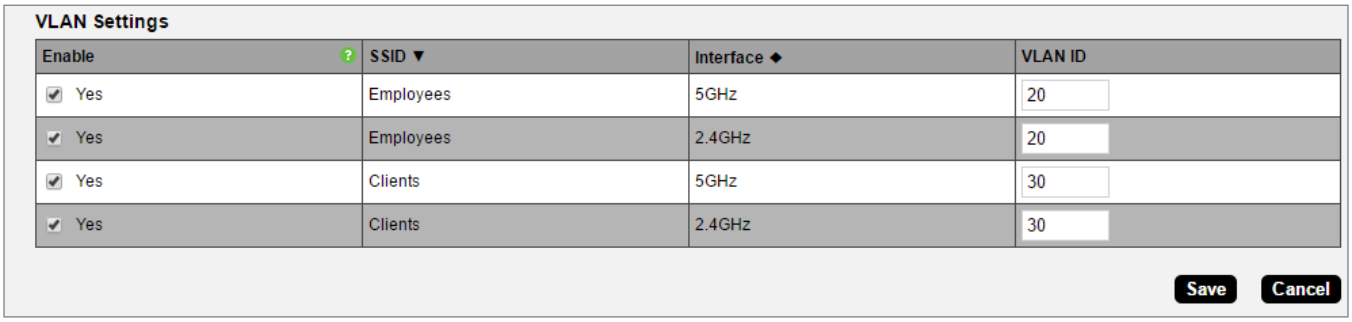
> **Note –** These instructions assume that you have already configured the desired SSIDs and know which SSIDs will carry traffic for a specific VLAN ID. One SSID can only be set to tag traffic for one VLAN ID.

A. Log into the WAP as an administrator and navigate to the Advanced > VLANS menu.

B. Select the check boxes to enable all VLAN-tagged SSIDs.

C. Enter the VLAN ID for each **tagged** SSID. **Do not** set up tagging for the default untagged VLAN ID. VLAN 1 is used in our example.

D. Click **Save**, then **Apply Changes** to save the new settings.



10 - Reboot the LAN

After configuring port-based VLANs, you should always reboot all of the network equipment, and reset the LAN connection on any connected client devices.

After you restore the network:

- If you are using DHCP, check the IP address assigned to each client device and ensure that it has a working LAN connection. All DHCP clients should receive an IP address within the assigned DHCP range set up in the router.
- If you are using static IP addresses, configure each client's NIC card settings, then ensure the client has a working LAN connection.
- See the next section, "Troubleshooting" if you experience problems after setup.

11 - Troubleshooting

Problems	Solutions
I can't access a network device after changing settings.	If using Inter-VLAN Routing, check to ensure that the feature is enabled for both devices' VLAN IDs. If not using inter-VLAN Routing, Check the IP address of your computer versus the inaccessible network device. They must be in the same subnet to allow communication. (Ex. **192.168.010.**106; **bold** must match) If attempting to access network device interfaces, check to be sure that your computer is on the device's configured management VLAN.
I can't access the Internet from a client device.	Confirm that the router settings for the VLAN ID are correct. Turn off route binding to determine if the WAN connection is the issue.
My devices are not being issued an IP address.	Ensure that the VLAN is configured correctly in the router. Check that the DHCP server is configured to issue enough addresses for all connected devices (Default range will issue up to 50 addresses.) Reset the client device's NIC card and ensure that it is set to DHCP.
With Inter-VLAN Routing correctly enabled, one or more devices are not communicating correctly between VLANs.	Certain protocols may not be supported with the Inter-VLAN communication feature in the Araknis AN-300-RT4L2W router, such as Bonjour, mDNS, TCP forwarding (redirects are alllowed), and others. Contact us for more information if you suspect a device is encountering these issues.

12 - Contacting Technical Support

Phone: (866) 838-5052

Email: support@araknisnetworks.com