Device-to-Device Linking with Broadband HamNet Mesh Software on Ubiquiti Radios

By Michael E. Fox, N6MEF

Table of Contents

Overview

One of the main advantages of the Broadband Hamnet (BBHN) mesh software is its simplicity of deployment. With minimal configuration and no knowledge of routing protocols, a multi-node network can be easily established which will automatically find the best path between any two points. It's a simple way to provide tens of Megabits per second (Mbps) of data throughput between multiple locations.

If two nodes A and B are located such that they cannot hear each other, but both can hear node C, then the mesh software will automatically route any traffic between nodes A and B through node C. If the three nodes are all operating on the same frequency, then the bandwidth between nodes A and B is cut in half because node C must repeat everything on the same frequency. For most event-sized networks, that's not a problem given the starting bandwidth of tens of Mbps and the relatively small size of the network.

If the loss of bandwidth due to repeating on the same frequency is an issue, then it can be remedied by using multiple radios, each covering a different sector and/or band. In the example above, node C might consist of two radios, one with a directional antenna pointed at node A and the other with a directional antenna pointed at node B. This is a more traditional hub site design for a wireless network, such as a mobile phone cell site (typically 3 x 120 degree sectors) or a WiFi ISP hub site. The BBHN software still handles the route selection automatically, without the user needing to understand much, if anything, about routing protocols. But the LAN connection between the collocated radios at site C may require some configuration, depending on whether a managed or unmanaged Ethernet switch is used.

This paper covers device-to-device linking using both an unmanaged and managed Ethernet switch. First, an example network is defined. Then the use of VLANs in the BBHN software will be explained. Next, VLAN connectivity on both an unmanaged and managed switch is shown, followed by discussion of DHCP Configuration and Mesh Status screens from a BBHN node. Finally, actual configurations of different brands of managed switches will be shown.

Note: Configuration of multiple sector antennas in the same band, at the same location requires careful planning and construction to ensure that the radios do not interfere with each other. Attention to antenna placement, channel selection, and shielding are all important factors. Radio vendors such as Ubiquiti and others provide good documentation on the subject. Therefore, this paper focuses solely on the interconnection between the radios. Antenna and RF issues are beyond the scope of this paper.

Example Scenario

The scenario used in this paper is as follows:

- Site “A” has a BBHN node in the 2.4 GHz band
- Site “B” has a BBHN node in the 5 GHz band
- Site “C” is a hub site which will provide connectivity to and between sites “A” and “B” using two nodes/radios – one in the 2.4 GHz band and one in the 5 GHz band.
- Site “C” also connects the BBHN mesh network to a WAN network. For this example, the WAN gateway function will be provided by the 2.4 GHz node at Site C.
- Site “C” also has a laptop PC and a Voice over IP (VoIP) phone.

A diagram of the overall network is as follows:

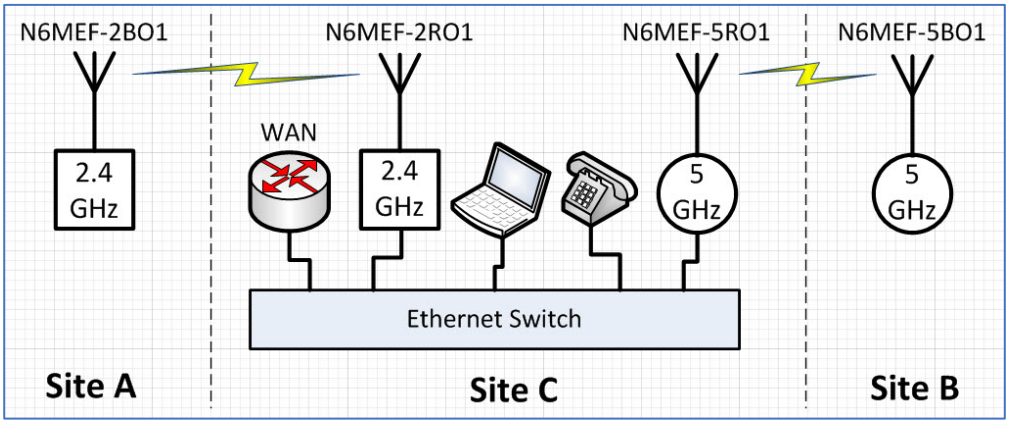


Figure 1: High-level network diagram for example scenario

The objective is to provide the desired connectivity between all of the equipment at site “C”. For the managed Ethernet switch, VLANs will be used to isolate and direct traffic between ports. Next, the VLANs used in the BBHN software will be reviewed.

BBHN Virtual LANs

Virtual LANs or VLANs provide a way to separate different types of traffic into different virtual interfaces even though it is all flowing through a single physical interface. Each VLAN is numbered with a unique ID of 1 through 4096. Each packet on the network can be "tagged" with the VLAN ID to identify the VLAN to which it belongs. When a packet is "tagged" with a VLAN ID, the VLAN ID is placed inside an additional 32-bit header field inserted into the Ethernet frame after the Source MAC address field and before the EtherType/Length field. (Consult documentation for IEEE 802.1Q for more information.)

In a BBHN mesh network, there are three distinct traffic types:

- WAN traffic: This is traffic between the BBHN mesh network and some other external network.
- OLSR node-to-node link traffic: This is traffic that flows between BBHN nodes. This the same type of traffic that is normally transmitted over the air between mesh nodes.
- User access traffic: This is traffic between the BBHN node and the edge devices such as servers, Voice over IP (VoIP) phones, user PCs, and other devices which are accessing the mesh network.

Since the Ubiquiti radios have a single Ethernet interface, the BBHN software separates the WAN, node-to-node and user access traffic into three virtual LANs. This makes it easy to identify and separate the three distinct traffic types. In version 3.x BBHN software, the VLANs are identified as follows:

- WAN traffic is tagged with VLAN ID 1
- OLSR node-to-node link traffic is tagged with VLAN ID 2
- User access traffic is untagged

Since the BBHN software already tags the WAN and OLSR node-to-node traffic with VLAN IDs 1 and 2 respectively, the Ethernet switch configuration must use those same VLAN IDs. But the user access traffic is untagged. So, additional VLAN IDs will be configured in the Ethernet switch to identify the user access traffic.

Note: The choice of VLAN ID numbers in the BBHN software is unfortunate. Most managed LAN switches use VLAN 1 as a management LAN by default. Some switches also have default uses for VLANs 2 and 3. As you'll see in the switch configuration screens that follow, the smaller, consumer-grade switches assign default names to those VLANs (such as "Management" for VLAN 1) and some don't allow those defaults to be changed. We can still use these VLAN IDs for our own purposes by ignoring the names and turning off some of the other default functionality. But it would be better if we could simply pick VLAN IDs which are not already in use in the default switch configuration. Perhaps the BBHN developers will realize the problem and allow the VLAN IDs to be configured at some point in the future.

Managed vs. Unmanaged Switches

The IEEE 802.3 standard was updated in 1998 to accommodate slightly longer packets which include VLAN tags and prioritization. Most modern Ethernet switches support the longer frames, even if they cannot be managed to configure how the VLANs are used.

Managed Ethernet switches allow control over how the VLANs are used on each port. VLANs can be mapped to specific ports and VLAN tagging can be turned on or off for each VLAN on each port. In contrast, unmanaged Ethernet switches treat all the ports the same way and typically pass traffic out the way it is received. For example, if the switch receives incoming traffic tagged with VLAN ID 1, it will send the traffic out tagged with VLAN ID 1. If the switch receives untagged traffic, it will send the traffic out without a tag.

VLANs on an Unmanaged Switch

The following diagram (Figure 2a) shows how the BBHN VLANs would traverse an unmanaged switch. All traffic, tagged or untagged, appears on all ports. The "T" and "U" in the diagram indicate whether the traffic in each VLAN is tagged ("T") or untagged ("U") on each port.

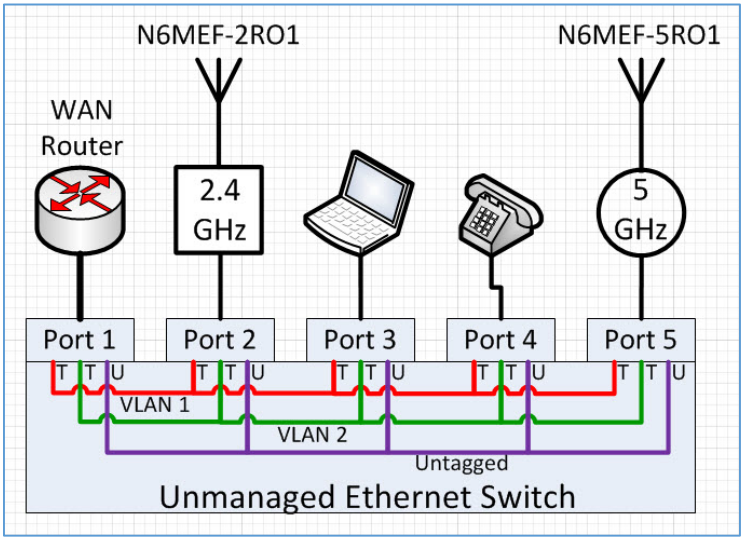


Figure 2a: VLANs in an unmanaged switch

Following is an explanation of each VLAN

- VLAN ID 1
  - WAN traffic is tagged with VLAN ID 1. Since VLAN 1 traffic is distributed to all switch ports, all BBHN nodes will have access to the WAN router.
  - If the WAN gateway feature will be used to distribute WAN connectivity to the rest of the network, it may be best to enable the feature on only one node. This ensures that all WAN traffic will always use the same WAN address, even if the mesh routing changes.

  - Note that the BBHN nodes send out WAN traffic tagged with VLAN ID 1 and they expect incoming WAN traffic to be tagged with VLAN ID 1. Therefore, the WAN router must be configured to send and received traffic tagged with VLAN ID 1.
- VLAN ID 2
  - Node-to-node linking traffic is tagged with VLAN ID 2.
  - Both nodes tag the traffic with VLAN ID 2 when they send it out and both nodes expect to receive node-to-node traffic tagged with VLAN ID 2.
- Untagged traffic
  - User access traffic to and from both nodes is untagged.
  - By default, all BBHN nodes have their DHCP server function enabled. This means that a client (PC, phone, camera, etc.) that connects to any switch port might receive an address from any BBHN node – whichever node answers the DHCP request first. For most purposes, it's best to disable DHCP on all but one of the nodes.

VLANs on a Managed Switch

The following two diagrams show how the VLANs will be configured in a managed Ethernet switch at site "C" to allow each traffic type to flow between the desired virtual interfaces. For the purpose of showing some complexity in the example, the laptop will be connected to the 2.4 GHz node at Site C and the phone will be connected to the 5 GHz node at Site C.

The first diagram (Figure 2b) shows a 5-port switch. The second diagram (Figure 2c) shows an 8-port switch. The "T" and "U" in both diagrams indicate whether the traffic in each VLAN is tagged ("T") or untagged ("U") on each port.

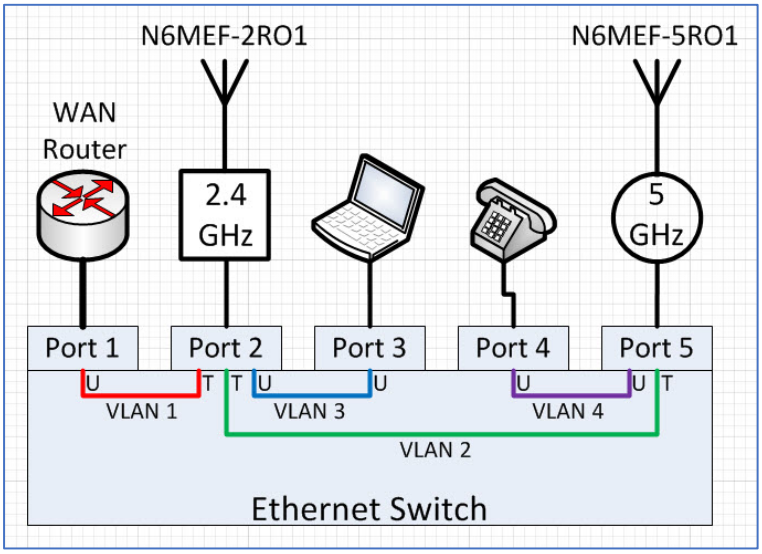


Figure 2b: Port and VLAN assignments for a 5 port switch

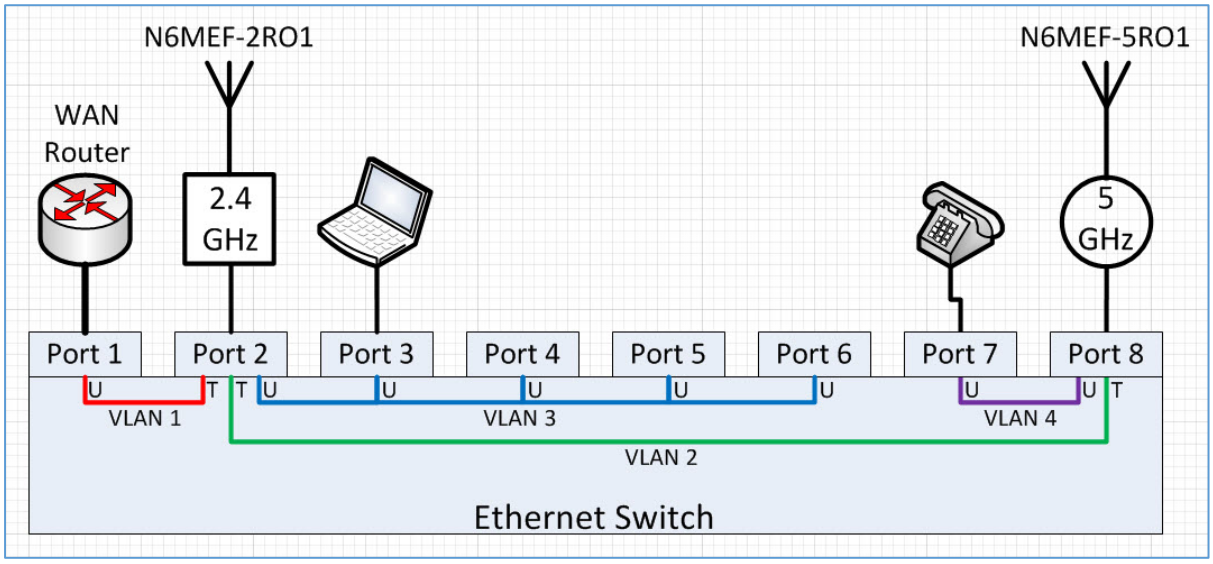


Figure 2c: Port and VLAN assignments for an 8 port switch

Following is an explanation of each VLAN:

- VLAN ID 1
  - WAN traffic uses VLAN ID 1. In this example, only the 2.4 GHz node will be connected directly to the WAN. The rest of the network, including the 5 GHz node and any other nodes to which it connects, can reach the WAN through the 2.4 GHz node.
  - Traffic from the 2.4 GHz node to the WAN exits the BBHN node tagged with VLAN ID 1.
  - For the sake of this example, the WAN devices connected to port 1 do not use VLAN tags. So, the switch will be configured to send WAN traffic from the 2.4 GHz node out port 1 as untagged traffic.
  - The switch will also be configured to accept incoming untagged traffic on port 1, tag it with VLAN ID 1, and send it to port 2.
- VLAN ID 2
  - Node-to-node linking traffic is tagged with VLAN ID 2.
  - Both nodes tag the traffic with VLAN ID 2 when they send it out and both nodes expect to receive node-to-node traffic tagged with VLAN ID2. The switch doesn't need to add or remove any tags.
- VLAN IDs 3 and 4
  - User access traffic for each node is untagged.
  - Even though the traffic will not be tagged, a VLAN ID must be defined so that individual switch ports can be assigned membership to the VLAN. In this example, VLAN ID 3 will be used in the switch to identify which ports carry the untagged user access traffic for the 2.4 GHz node and VLAN ID 4 will identify which ports carry the untagged user access traffic for the 5 GHz node.

BBHN Node DHCP Configuration

The DHCP configuration of the Broadband Hamnet (BBHN) software is simple. Figure 3a shows the Basic Setup screen of the 2.4 GHz node named N6MEF-2RO1. The "DHCP Server" function is enabled.

If the Ethernet switch being used for node-to-node linking is unmanaged, it is usually best to disable DHCP on all but one node. This insures that all clients will receive an IP address in the same subnet and can talk directly to each other without having to traverse a node.

If the Ethernet switch being used for node-to-node linking is managed, then untagged user traffic can be isolated such that each client can only connect to one node. In the examples shown in Figures 2b and 2c above, DHCP can be enabled on both the 2.4 GHz and the 5 GHz nodes since the VLAN configuration of the Ethernet switch ensures that each user access port is connected to only one of the nodes. Devices plugged into the Ethernet switch ports assigned to VLAN 3 will be assigned addresses from the 2.4 GHz node's LAN IP address range. Devices plugged into the Ethernet switch ports assigned to VLAN 4 will be assigned addresses from the 5 GHz node's LAN IP address range.

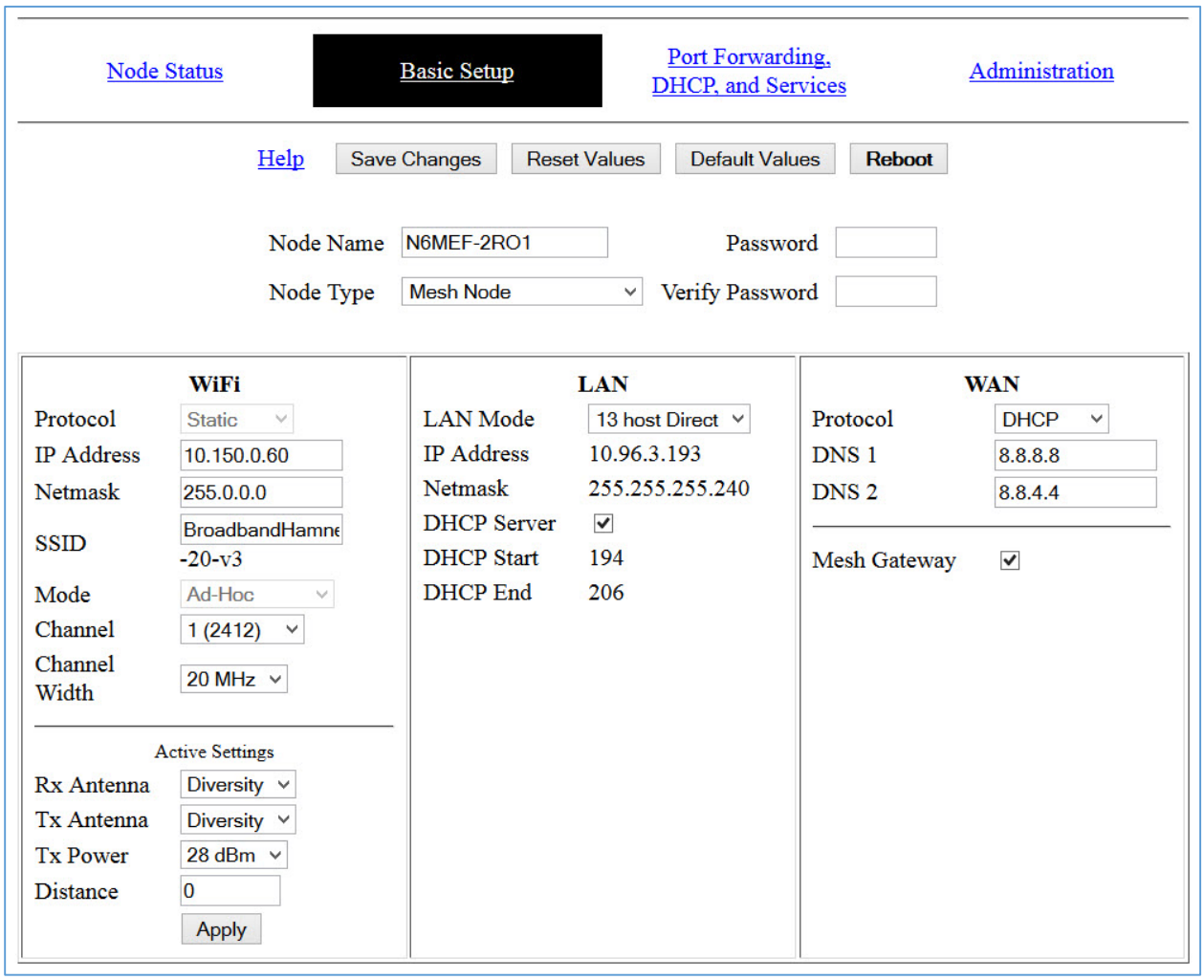


Figure 3a: Basic Setup screen of 2.4 GHz node N6MEF-2RO1

The managed Ethernet switch needs an IP address. In this example, the switch has been configured with a static address that is in the LAN subnet of the 2.4 GHz node. The static address allows configuration of the switch even if the 2.4 GHz node is not attached or running. But it also means that the address must be reserved so it will not be assigned to another device by the DHCP server in the 2.4 GHz node.

The next screenshot shows a DHCP address reservation configured for the address used by the Ethernet switch. Since the IP address is statically configured in the Ethernet switch, the switch will not request an address via DHCP and the DHCP server doesn't need to know the actual MAC address of the switch. Therefore, the actual MAC address doesn't matter and a bogus MAC address of all-zeros was used instead of the real MAC address.

The current leases section of the screen shows the dynamic address assigned to the laptop PC ("mef-sp2").

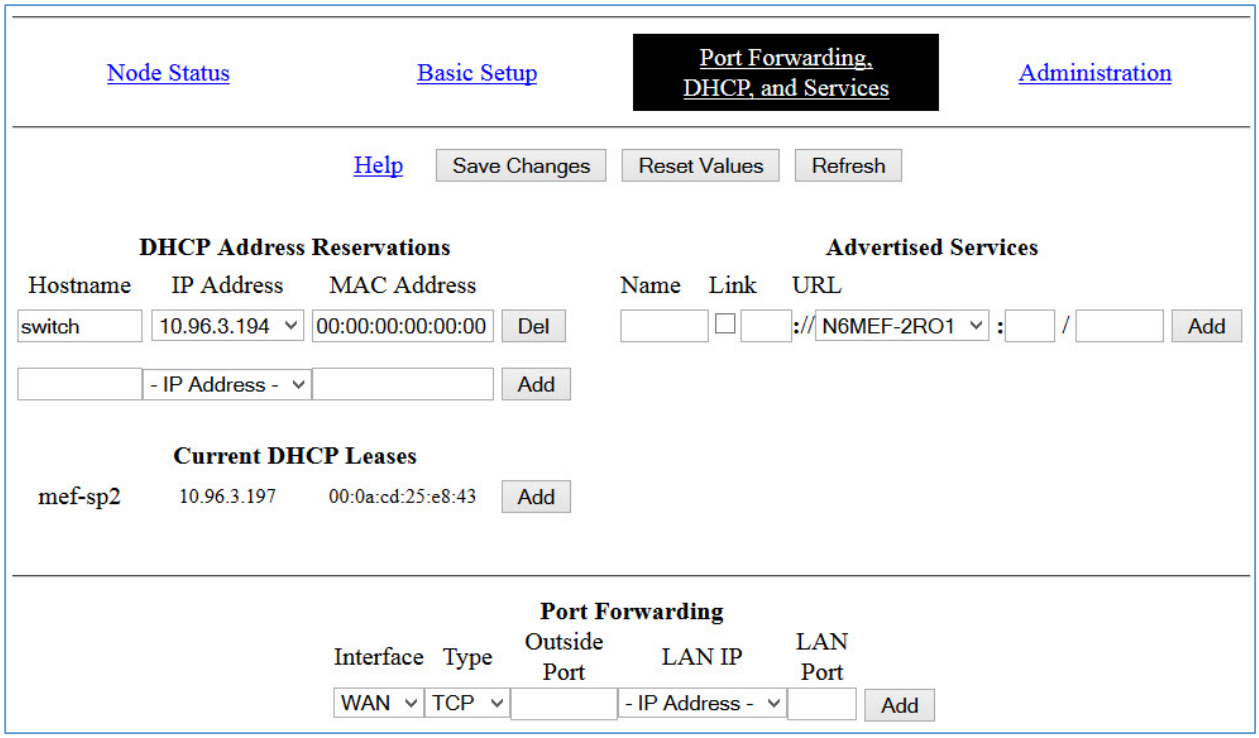


Figure 3b: DHCP Setup screen for 2.4 GHz node N6MEF-2RO1

BBHN Node WAN Connectivity and Mesh Gateway

There are several issues to consider when enabling WAN connectivity and even more when enabling the Mesh Gateway function, including network security and compliance with FCC Part 97 rules. These issues are beyond the scope of this paper.

For the purpose of the example network shown in Figure 1, the 2.4 GHz node will provide Mesh Gateway access to the WAN. An example usage scenario would be for downloading additional packages or software updates to the other nodes in the mesh network.

Figure 3a above shows that the WAN interface on the 2.4 GHz node is enabled (WAN Protocol is not set to "Disabled") and the Mesh Gateway function has been enabled. This means that the node will be able to communication with the WAN and will advertise WAN connectivity to the rest of the mesh network.

In the example network, the WAN interface for the 5 GHz node could be disabled. Referring to Figures 2a, 2b or 2c, traffic from the 5 GHz nodes to the WAN would be tagged with VLAN ID 2 (node-to-node link traffic) and sent across the Ethernet switch to the 2.4 GHz node. The 2.4 GHz node would then tag the traffic with VLAN ID 1 and send it back across the Ethernet switch to the WAN router.

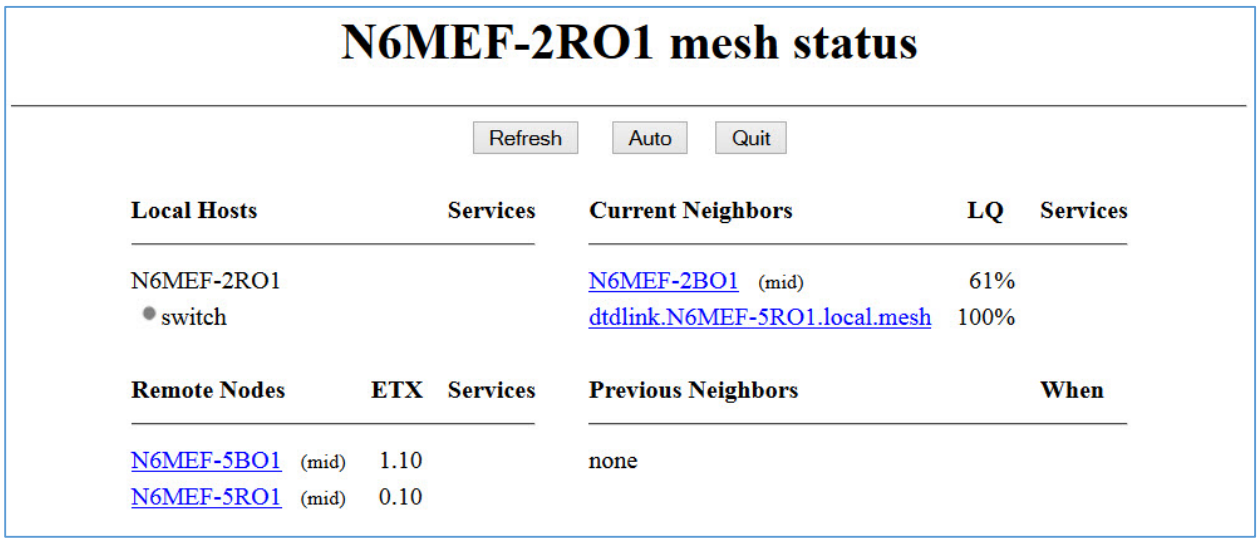
If an unmanaged switch is used, the WAN router connected to port 1 would need to accept and send traffic tagged with VLAN ID 1 (Figure 2a). A managed switch could be used to strip the tag as it exits the switch on port 1 (Figures 2b or 2c). Again, more complex WAN configurations are possible but they are beyond the scope of this paper.

BBHN Node Mesh Status

The following image shows the Mesh Status screen from the 2.4 GHz node N6MEF-2RO1 in the operating network. Compare the information shown here with the example network diagram shown in Figure 1.

The "Current Neighbors" list shows two neighbors: the 2.4 GHz node at Site A, N6MEF-2BO1, which has a direct link over the air; and the LAN-attached 5 GHz node at Site C, N6MEF-5RO1. The LAN interface apparently acts as a pseudo-node in the BBHN software and has a special node name beginning with "dtdlink."

The "Remote Nodes" list also shows two neighbors. The LAN-attached 5 GHz node at Site C, N6MEF-RO1, is reachable through the "dtdlink.N6MEF-RO1…" pseudo-node with a metric of 0.10. The OLSR mesh routing protocol uses a metric of 0.10 for Ethernet links. The 5 GHz node at Site B, N6MEF-5BO1, is reachable via the N6MEF-5RO1 node and has a metric 1.10 which is the sum of the 0.10 metric to reach N6MEF-5RO1 plus an additional radio hop.



N6MEF-2RO1 mesh status

Refresh Auto Quit

Local Hosts	Services	Current Neighbors	LQ	Services
N6MEF-2RO1		N6MEF-2BO1 (mid)	61%	
switch		dtdlink.N6MEF-5RO1.local.mesh	100%	

Remote Nodes	ETX	Services	Previous Neighbors	When
N6MEF-5BO1 (mid)	1.10		none	
N6MEF-5RO1 (mid)	0.10			

Figure 4: Mesh Status of 2.4 GHz node N6MEF-2RO1

Managed Switch Configuration Examples

Following are examples of the configuration screens for different managed Ethernet switches.

Ubiquiti ToughSwitch PoE Configuration

The Ubiquiti ToughSwitch is a 5-port switch capable of supplying 24 volt PoE power to the attached devices. Like many VLAN-capable switches, the Ubiquiti switch assumes that VLAN ID 1 will be used for management. It pre-assigns the name "Management" to VLAN 1 and does not allow it to be changed. Since the BBHN software does not allow the VLAN ID numbers to be changed, the user will simply need to ignore the "Management" name assigned to VLAN 1 and remember that VLAN 1 is for "WAN Traffic".

Like most managed switches, this switch has a built-in web interface. The following image is a screen shot of the VLAN configuration page. This single screen is used to create the VLAN IDs and names, and to assign them to ports. Compare the configuration shown here with the visual representation of the port and VLAN assignments in Figure 2b.

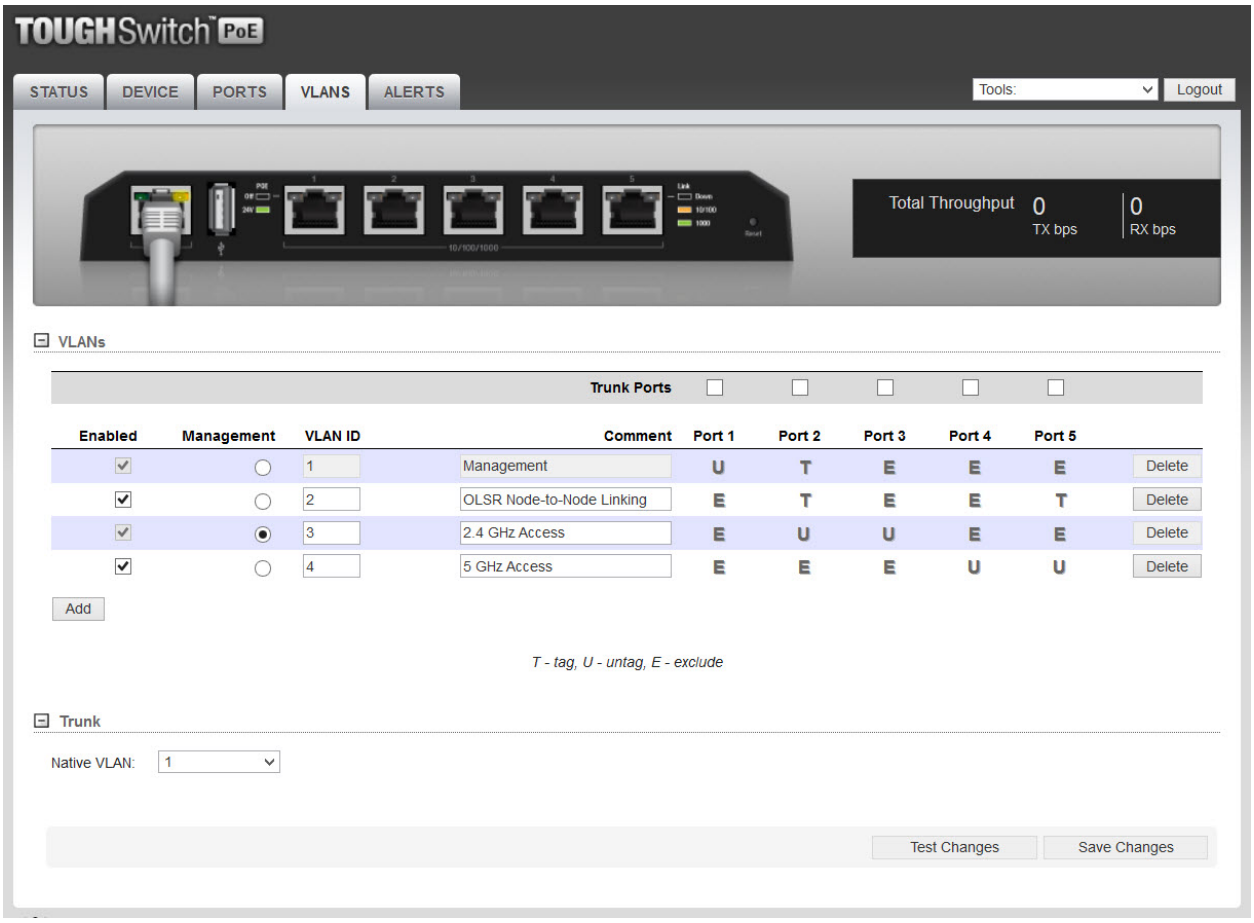


Figure 5: VLAN Configuration of Ubiquiti ToughSwitch PoE

Note the following about the above screen image:

- The Comment/Name assigned to VLAN 1 is "Management". This is the default from Ubiquiti and can't be changed. The user must simply ignore the name and remember that VLAN 1 is used to carry the WAN traffic.

- Note that the Management VLAN has been set to VLAN ID 3. This enables management access to the device from machines that are part of VLAN 3, such as the laptop PC in the example configuration

Netgear GS108T Configuration

Like many VLAN-capable switches, the Netgear switch assumes that VLAN ID 1 will be used for management. It also assumes that VLAN ID 2 will be used for voice traffic and VLAN ID 3 will be used for video traffic. It also has some enhanced features to automatically detect voice and video traffic and associate each traffic type with the appropriate VLANs. The automated features may be nice for some consumers, but they will need to be turned off to ensure they don't change the desired behavior.

The GS108T also pre-assigns the names "Default", "Voice VLAN" and "Auto-Video" to VLANs 1, 2 and 3, respectively, and it does not allow those three names to be changed. Since the BBHN software does not allow the VLAN ID numbers to be changed, the user will simply need to ignore the names for VLANs 1, 2 and 3 and remember that they are actually being used for "WAN Traffic", "OLSR Node-to-Node Linking Traffic", and "2.4 GHz Access Traffic", respectively.

Configuration of the Netgear switch is more complicated than the Ubiquiti switch. This is partly due to it having more features, and partly due to a user interface design that requires much more mouse clicking and many more screens than the Ubiquiti switch.

By default, the Netgear switch is configured to accept management traffic from VLAN 1. Since the example configuration will use VLAN 1 on port 1, plug the management PC into port 1 to perform the following steps.

Configuration begins with creating and naming the VLAN IDs that will be used. The Netgear GS108T comes preconfigured with VLAN IDs 1-3 and these cannot be changed. VLAN ID 4 will need to be added to carry the 5 GHz access traffic.

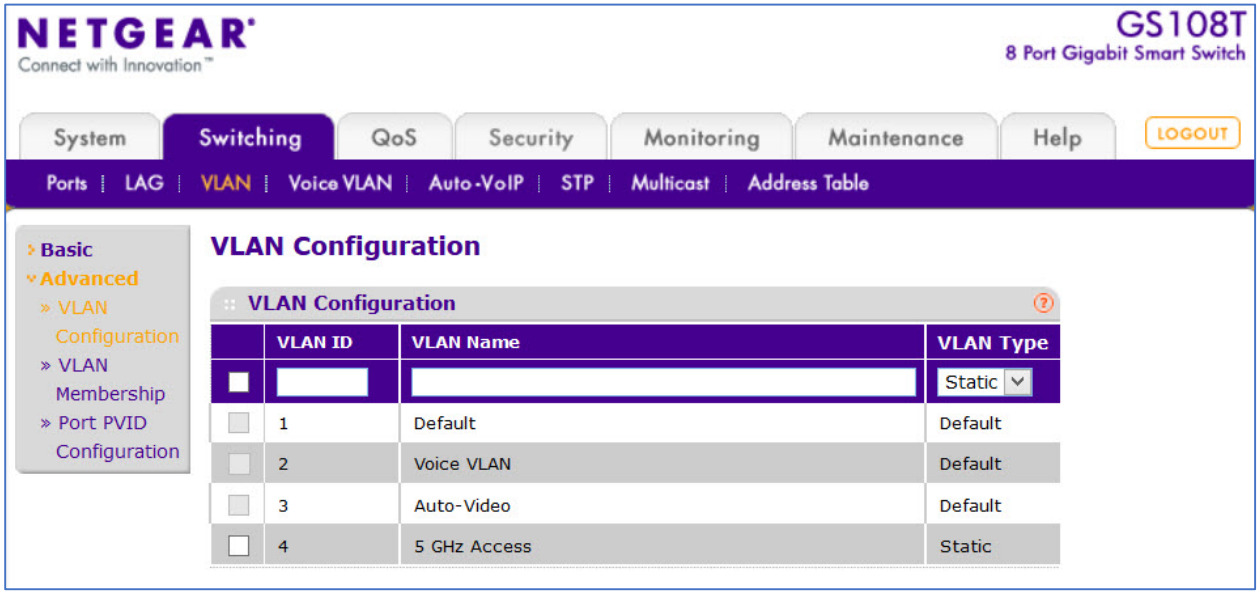


Figure 6: VLAN identification. (VLANS 1-3 come pre-configured and cannot be changed.)

Next, the port assignments for each VLAN are made. The following four screen shots, (Figures 7a-d) show the port number and tagging assignments for VLANs 1-4. Compare the configuration shown here

with the visual representation of the port and VLAN assignments shown in Figure 2c. A similar convention of “U” for untagged and “T” for tagged is used to mark each port that belongs to a VLAN.

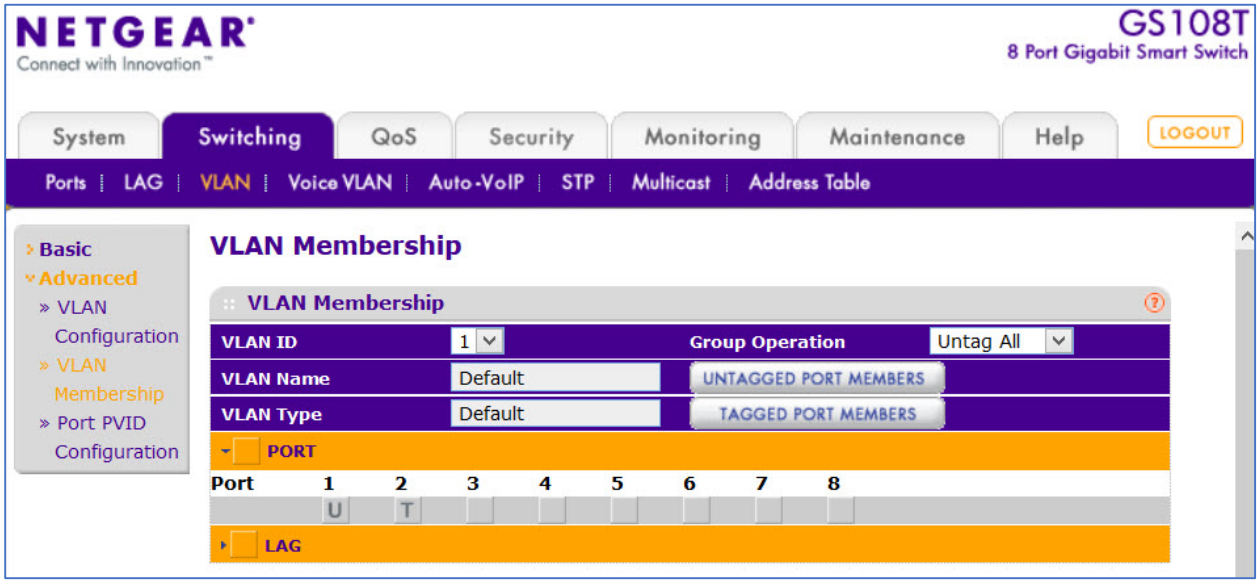


Figure 7a: Port assignments for VLAN 1 (WAN Traffic)

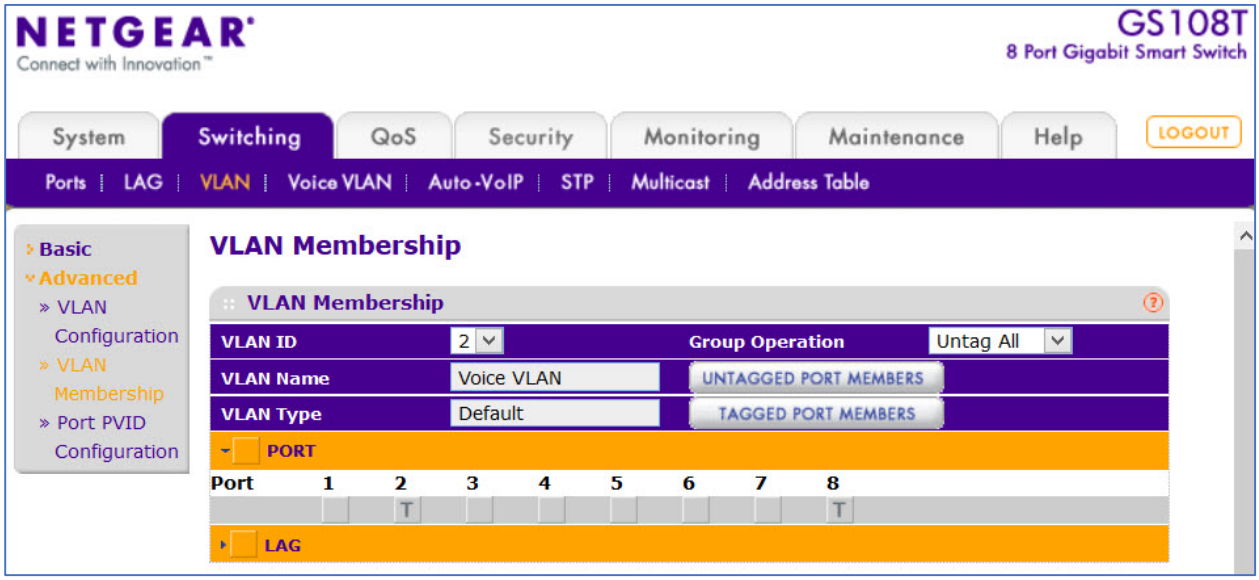


Figure 7b: Port assignments for VLAN 2 (OLSR Node-to-Node Linking Traffic)

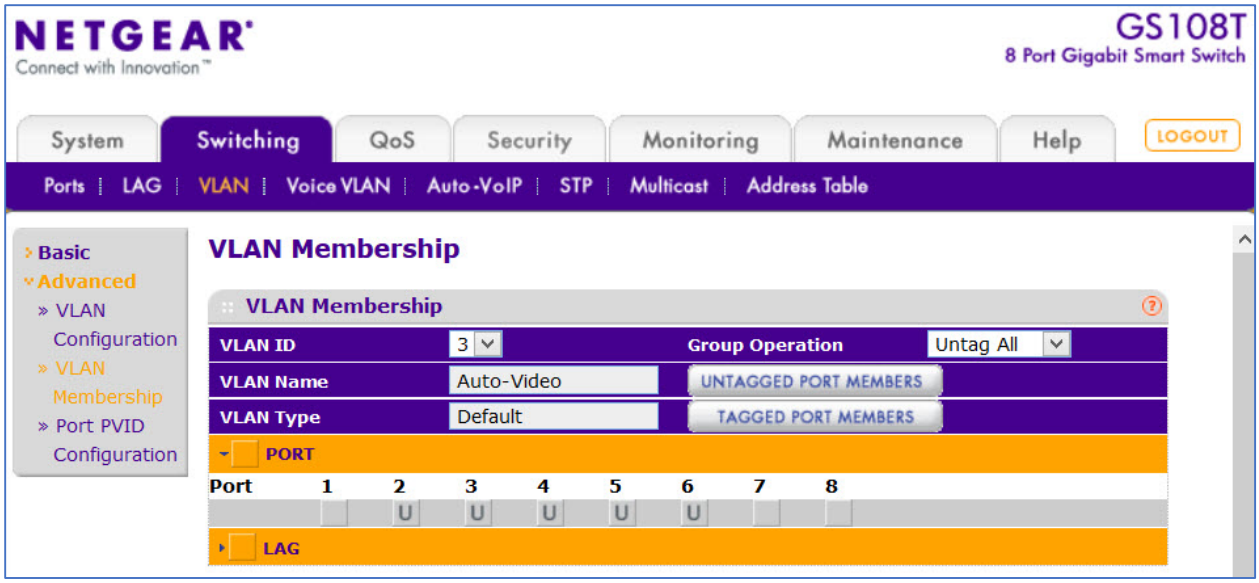


Figure 7c: Port assignments for VLAN 3 (2.4 GHz Access Traffic)

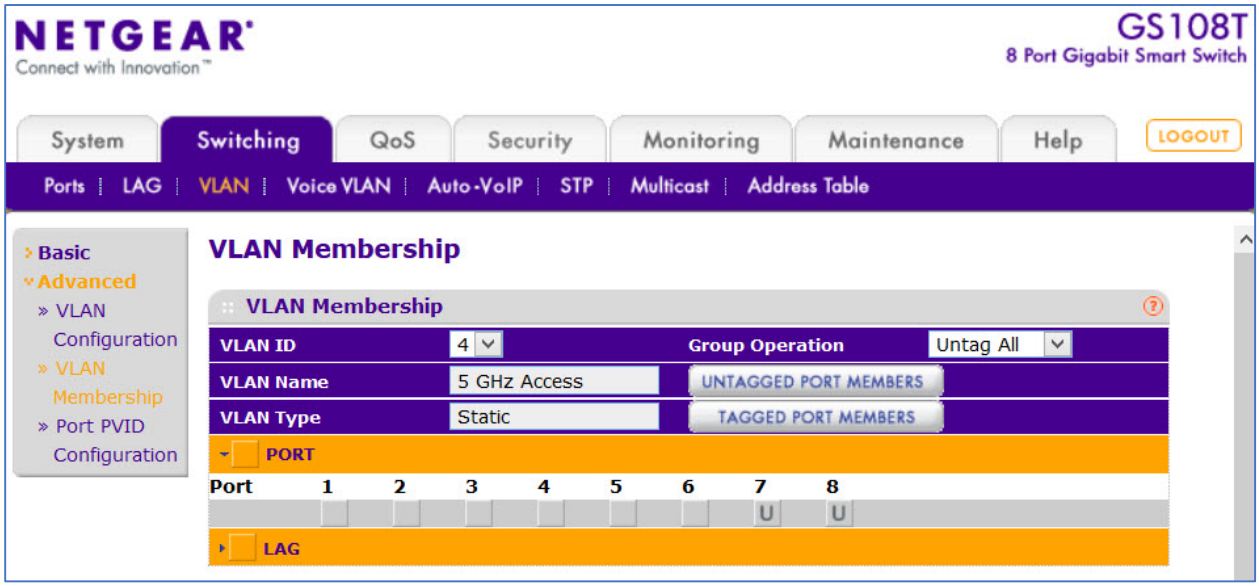


Figure 7d: Port assignments for VLAN 4 (5 GHz Access Traffic)

Next, the VLAN ID to be assigned to untagged, inbound packets must be defined for each port. This is on another screen called the Port PVID (Port VLAN ID) Configuration. Note the "PVID Configured" column in the following screenshot.

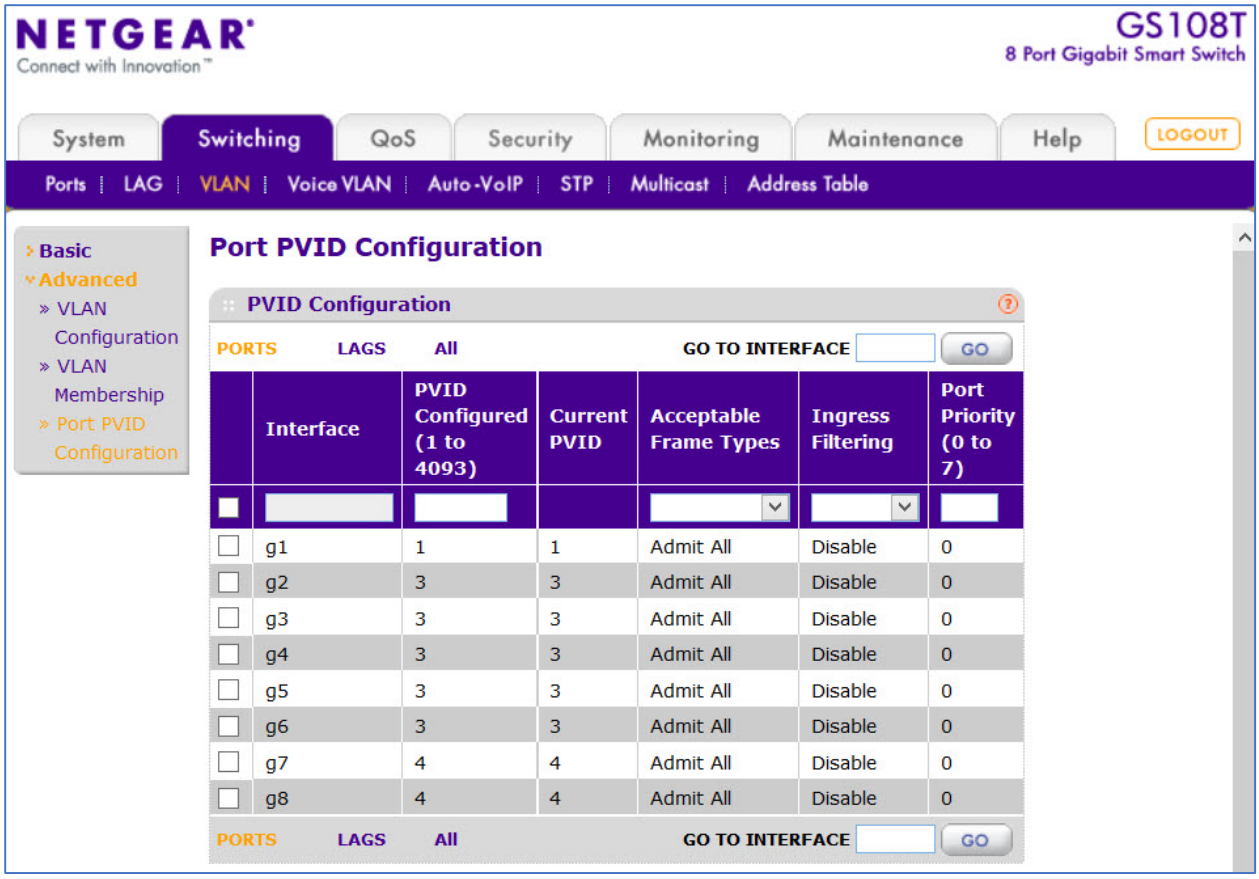


Figure 8: PVID – VLAN ID assigned to inbound, untagged frames

Since the pre-configured VLANs will be used for a purpose other than their default purpose, it's a good idea to make sure the automated functions are turned off. This will avoid the possibility that user traffic will automatically be redirected to an unintended VLAN. In the next screen the "Voice VLAN Status" is set to "Disable".

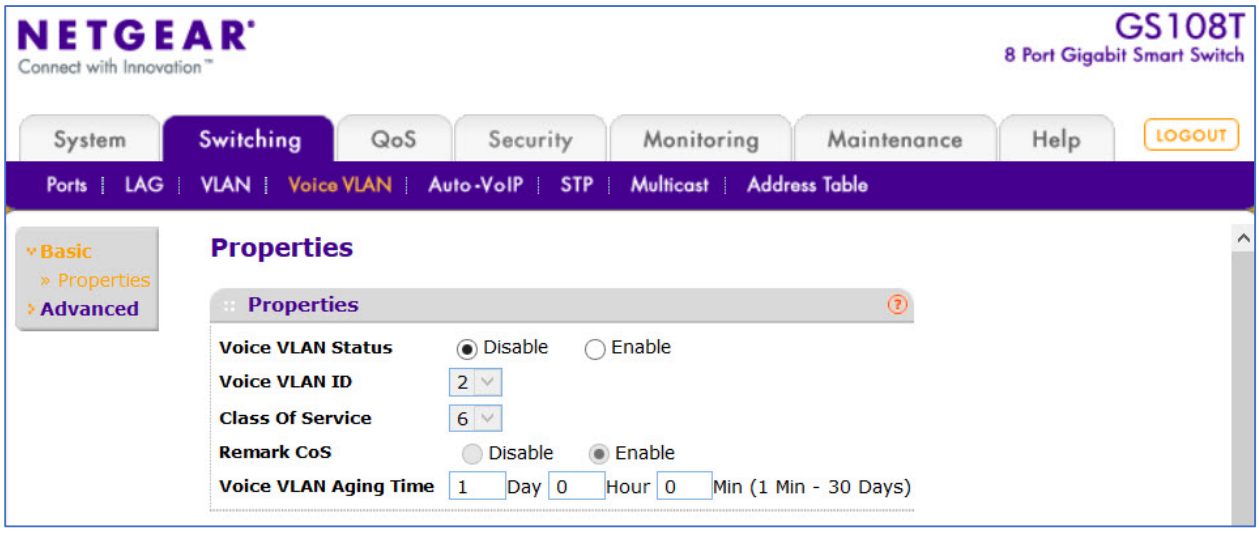


Figure 7: Voice VLAN function disabled

Finally, confirm that the Auto-VoIP Mode is set to “Disable” for all interfaces.

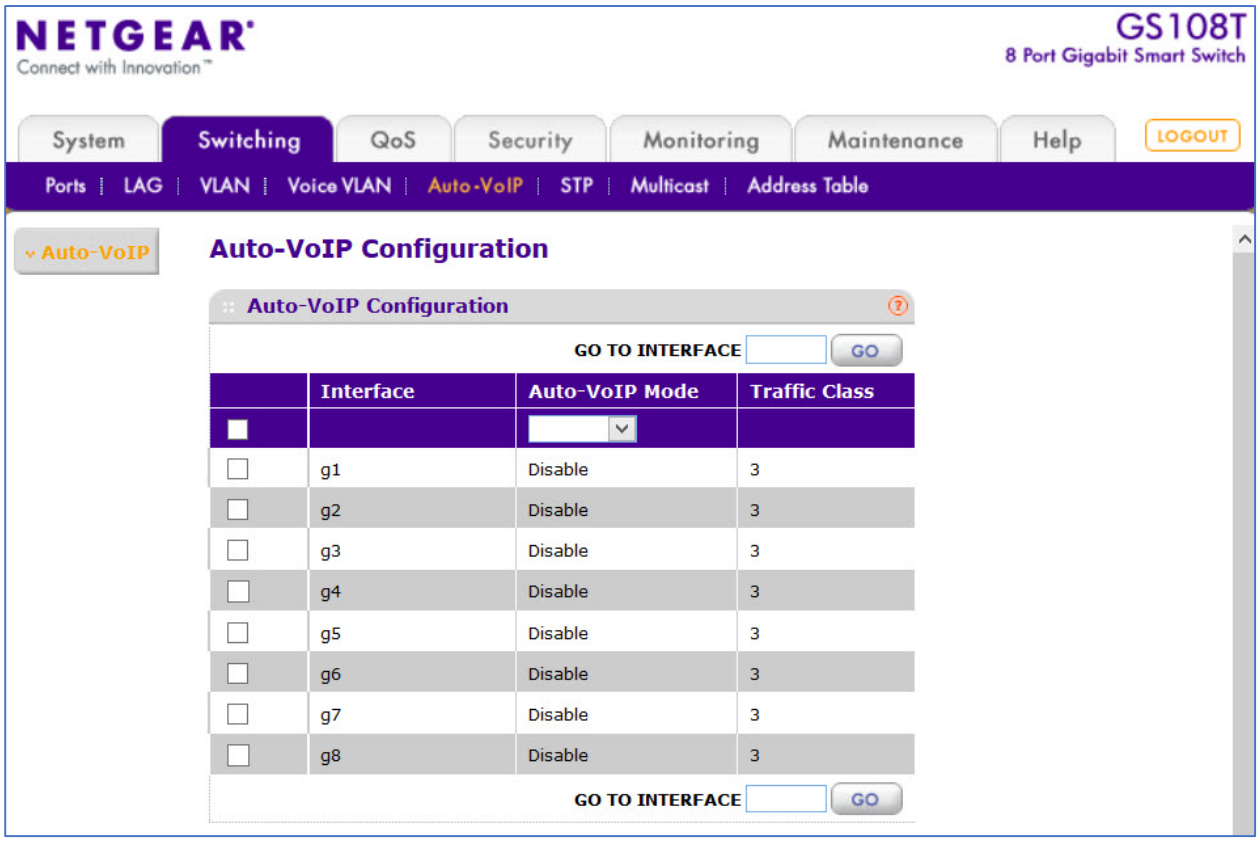


Figure 9: Auto-VoIP Mode disabled on all ports

At this point, the VLAN configuration is completed. But just like with the Ubiquiti configuration, the management traffic should be accepted on VLAN 3. The management VLAN is set on the IP configuration screen as shown in the next screen shot.

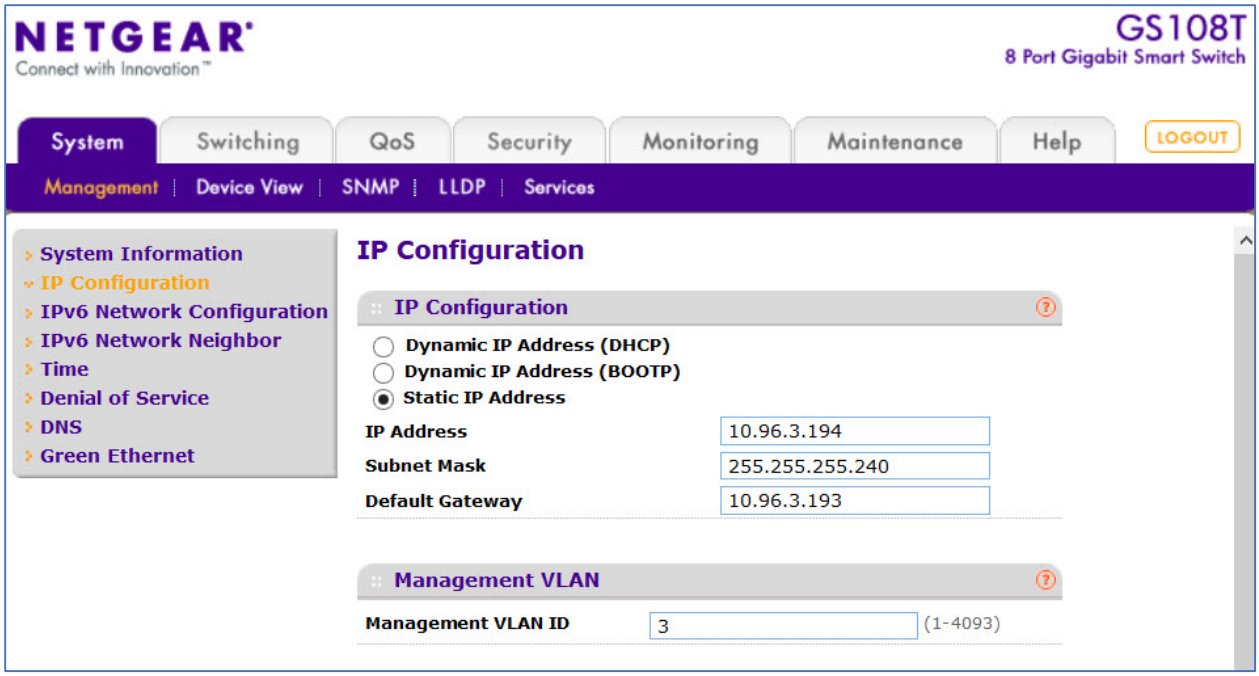


Figure 10: Changing the Management VLAN ID

IMPORTANT: Once the management VLAN is changed to 3 and saved, access will be disabled on port 1 since port 1 is not part of VLAN 3. Therefore, the management PC which is plugged into port 1 will lose connectivity with the switch's management web interface. Unplug the management PC from port 1 and plug it into one of the ports assigned to VLAN 3 (ports 2-6). Management access should be restored.

Conclusion

Hub sites may be configured with nodes on multiple bands and/or nodes in the same band covering multiple sectors. These nodes can be linked via an Ethernet switch that supports VLANs. Unmanaged switches can be used for node-to-node linking, but more control is available is possible with a managed switch. The managed Ethernet switch's VLAN configuration defines which physical ports will carry each VLAN and whether inbound and outbound traffic will be tagged or untagged. The configuration of a managed Ethernet switch is usually straight-forward and user interface similarities exist across different switch vendors, making it easy to extrapolate the information presented here to other devices.