Contents

[Preparation 2](#_Toc13211414)

[Required VLANs and Respective Subnets 2](#_Toc13211415)

[Configuring the DHCP Relay Agent 2](#_Toc13211416)

[Prerequisites 2](#_Toc13211417)

[Installation 2](#_Toc13211418)

[Configuration 3](#_Toc13211419)

[Testing 4](#_Toc13211420)

[Adding VLANs to vSphere 5](#_Toc13211421)

[Testing vSphere VLANs 5](#_Toc13211422)

[Hyper-V VMs and VLANs 5](#_Toc13211423)

[Configure the Virtual Switch 5](#_Toc13211424)

[NIC Compatibility 6](#_Toc13211425)

[Configure the VM 6](#_Toc13211426)

[ESXi VLAN Trunk Configuration 6](#_Toc13211427)

[Configuring DHCP Relay Agent in Sonic OS 6](#_Toc13211428)

[Configuring SonicWALL ports for VLANs 9](#_Toc13211429)

[VPN with VLANs 9](#_Toc13211430)

[RDP with VLANs 10](#_Toc13211431)

[Fileserver Shares Across VLANs 10](#_Toc13211432)

[Switch Configurations 10](#_Toc13211433)

[Configuring Switch Ports for VLANs 10](#_Toc13211434)

[Configuring Switch Ports for Voice VLAN (802.1p Encapsulation) 10](#_Toc13211435)

[Configuring Trunks 11](#_Toc13211436)

[Configuring Servers 11](#_Toc13211437)

[Workstations after Configuration of VLANs 11](#_Toc13211438)

[Computers Statically Assigned to .64 Network 11](#_Toc13211439)

[Network Down Time 12](#_Toc13211440)

[Moving Ports 12](#_Toc13211441)

[Switch and Router Configurations 12](#_Toc13211442)

[Addressing Possible Complications 12](#_Toc13211443)

# Preparation

- Backup all the configurations on the router and switches. Take snapshots of virtualized servers. Save a backup of the settings file for Sonic OS. Here is a link with the instructions: <https://www.sonicwall.com/support/knowledge-base/?sol_id=170504841802992>

- Configure VLAN scope(s) on DHCP server(s) ([Redacted])

- Configurations for switches can be done ahead of time and added to them.

## Required VLANs and Respective Subnets

[VLAN configurations and IP addressing redacted]

\*\* A separate voice VLAN is required because the configuration and encapsulation are different (802.1p vs 802.1q) because normal 802.1q encapsulation makes it so standard priority does not apply, but 802.1p encapsulation adds priority to the header.

# Configuring the DHCP Relay Agent

## Prerequisites

* Host must have a NIC installed for each subnet/VLAN.
* Relay agent **cannot** be a DHCP server.
* DNS records will also be passed with the DHCP relay agent by default.

## Installation

* Install **remote access role** through server manager
* In the **Select role services** page, select **Routing** and allow it to install any required features to go with it. This install should not require a restart.



## Configuration

* Run **Routing and Remote Access** (will appear if typed in the start menu)
* Under the **Action** tab, select **Configure and enable routing and remote access**.
* Select **Custom configuration**
* Select **LAN routing** and start the service
* After service is started, under the server’s name and under IPV4, right click on **General**. Select **New routing protocol** and select **DHCP Relay Agent**.
* Once the routing protocol is added, right-click **DHCP Relay Agent** and click **Properties** and add the DHCP server’s NIC(s) that are on the subnet(s) that the DHCP server is **not** on.

For example, if I have two subnets 192.168.1.0 and 192.168.2.0, and my DHCP server is on 192.168.1.0, my DHCP relay agent will have NICs for each of those subnets, but the 192.168.2.0 will be the one added as the DHCP relay agent interface.

* Ipconfig /release and ipconfig /renew to test to see if the workstation is getting the right IP address if any afterwards.

## Testing

* Because of the firewall/router not yet being configured to allow the DHCP relay agent servers as trusted DHCP relay agents, any test hosts may not successfully get an IP address through DHCP.
* To see if the relay agent is working, the following commands can be used on the ***DHCP server***:
* To start: **netsh trace start scenario=NetConnection capture=yes report=yes persistent=no maxsize=1024 correlation=no traceFile=C:\Temp\NetTrace.etl** (the C:\Temp\NetTrace.etl can be replaced with file name and location of your choosing, but the .etl should be maintained)
* Allow the process for long enough to capture the DHCP packets. Make sure the test host is actively trying to use DHCP and that the relay agent is receiving the packets. You can check this by opening Routing and Remote Access, looking under DHCP Relay Agent, and next to the interface it should show Requests received. Ignore the rest for now. This will not refresh, to see the numbers go up you must close Routing and Remote Access and re-open it. Do this to confirm the packets have been sent. This shouldn’t take more than 5 minutes.
* Once a few minutes have passed and packets have been confirmed to be sent, use the command: **netsh trace stop**. It may take a few minutes to complete the report.
* To analyze the etl file, you must install **Microsoft Message Analyzer**. This can be on any computer, as long as you can get the file to it. You can download this from Microsoft’s website.
* Once the app is opened, open the file and allow the program to load it, which may take awhile. Once loaded, you can sort by module in alphabetical order by clicking the module tab above the data to easily find all the DHCP packets. Ideally, you’re looking for the DHCPOffer packets.

In the DHCPOffer packets, you want to confirm that the YourIP section has an appropriate IP assigned as per the VLAN’s scope, that the ServerIP is the DHCP server’s, and that the RelayAgentIP is that of your relay agent. If it is, then the relay agent is working. If you are not seeing DHCPOffer packets for the relay agent at all, try running the report again but for a little longer. If nothing shows up again then check your relay agent configurations again. You can also check the DHCP relay agent using the same commands to see if they are receiving a DHCPDiscover from the test host. If not, then troubleshoot the communication between the test host and the DHCP relay agent.

# Adding VLANs to vSphere

Click the **main VMware server** on the left sidebar. Click on the **Configure** tab on the top. On the new sidebar to the right of the initial sidebar, under **Networking**, select **Virtual switches**.

Under **Virtual switches**, click on **Add Networking**.

The first window is **Select connection type**. Select **Virtual Machine Port Group for a Standard Switch**.

Click **Select an existing standard switch**, select the desired switch.

On the next page **Connection settings**, you can create any Network label you want, but **the VLAN ID has to match the one on the switch configurations** on the physical switches.

For more information: <https://kb.vmware.com/s/article/1004074>

## Testing vSphere VLANs

Due to the simple nature of the configuration of VLANs in vSphere, you may want to test the configuration. Before the rest of the network is ready for VLANs, you can test by creating test hosts on the same ESXi server and seeing if they communicate. Or, if the DHCP relay agent is up and running, you can see if you can ping the appropriate VLAN assigned NIC on the DHCP relay agent from a test host on the same VLAN, (make sure the firewall is not preventing this, you might have to disable Windows firewall)

# Hyper-V VMs and VLANs

## Configure the Virtual Switch

Open **Hyper-V Manager**

From the **Actions** menu, click **Virtual Switch Manager**

Under **Virtual Switches**, select the virtual switch connected to the physical network adapter for which the VLAN resides

In the right pane under **VLAN ID** select **Enable virtual LAN identification** then type the VLAN ID

## NIC Compatibility

**The physical NIC on the host needs to support VLAN tagging**

On [Server Name Redacted] the VLAN ID section is greyed out in the Virtual Switch Manager. This is due to a compatibility issue with [Network Card Name Redacted]. Fortunately, the compatibility issue is simply that this setting cannot be changed with the Virtual Switch Manager at first, and must be configured first in the properties of the adapter itself. Once the VLAN ID is added there, when you reopen Virtual Network Manager, you will be able to do the virtual switch configurations.

If this does not work, another possible work around is using the adapter settings to create a VLAN, which will create a new virtual adapter in the device manager that can be used by the virtual switch. One workaround proposed is using [Redacted] to initially configure the VLANs but there is not a working release for [Redacted].

If any of the available workarounds do not work, the idea of either moving the VM(s) to the ESXi environment might need to be considered.

## Configure the VM(s)

From **Hyper-V Manager**, in the **results** pane under **Virtual Machines**, select the VM and right-click **Settings**

Under **Hardware**, select the virtual switch previously set up with the VLAN

In the right pane select **Enable virtual LAN identification** and then type the VLAN ID.

# ESXi VLAN Trunk Configuration

For VLAN tagged packets to leave ESXi servers, the trunk only needs to be configured on the switch it is attached to. ESXi will pass all VLANs to the respective adapters automatically.

If the VLAN goes across two ESXi servers, their connection to each other must be **set up as a trunk** allowing the VLAN tagged items to pass through. Until this is done, even though they are on the same VLAN, they cannot access each other as they are tagged traffic. This can be done simply between the switches they are attached to and it will act the same. Once all the switches are trunked together, this issue will most likely resolve itself.

# Configuring DHCP Relay Agent in Sonic OS

The DHCP relay agents need to be trusted so that the DHCPOffer packets reach the DHCP relay agents.

Create IP Helper Policy

<http://help.sonicwall.com/help/sw/eng/7634/8/0/0/content/Policies_Network_IPHelper_Snwls.htm>

Trusted DHCP relay agents

<http://help.sonicwall.com/help/sw/eng/5800/25/8/0/Network_ipHelperView.html>





( Sonic OS guide for version 6.2: <https://www.sonicwall.com/support/technical-documentation/sonicos-6-2-admin-guide.pdf> )

**\*\*\* These steps may not be what is required to allow the DHCPOffer packets to be sent from the DHCP server to the DHCP Relay Agent, but something on the firewall needs to be configured to allow DHCP packets with the new VLAN’s IPs to be sent across the network. This may be fixed simply by the VLAN being added to the firewall so that the IPs sent are recognized. Perhaps a route enabled from the DHCP servers to the DHCP relay agents? Configuring the firewall as a DHCP relay agent/ DHCP helper is also an option.**

# Configuring SonicWALL ports for VLANs

**SonicWALL port configuration:**

**[Redacted]**

**This will require a trunk configured between all switches**

**Default gateways must be configured for all VLANs on their respective interfaces on the firewall in order to communicate with each other and to access the internet.**

In the same way you would with a normal router, you would first create sub interfaces for the VLANs that will be on the interface(s) that will be a trunk. Then, those sub interfaces will be given IP addresses which will be the default gateways to the VLANs. Then the trunk must be enabled. In the case there are enough ports, LACP can be configured between the two ports, just as long as the configurations of the VLANs on the two are identical.

SonicWALL LACP - <https://www.sonicwall.com/support/knowledge-base/?sol_id=170505988976495>

SonicWALL sub interfaces with VLANS - <https://www.sonicwall.com/support/knowledge-base/?sol_id=170503889544086>

Configuring default gateways for VLANS on SonicWALL: <https://www.sonicwall.com/support/knowledge-base/?sol_id=170505813100854>

# VPN with VLANs

In the event this needs to be configured differently, or if more VLANs are added to the Workstation group, here is an article outlining configuring different subnets on a SonicWALL VPN: <https://www.sonicwall.com/support/knowledge-base/?sol_id=170503586678319>

If the VPN portal is on a server VLAN, and this is how IP addressing is assigned, then it will receive an IP address on the server VLAN the way the VPN portal is now. In order for the VPN clients to get a [Redacted] IP and not a [Redacted] IP, a server may need to be set up on the workstation side with just the VPN portal installed to it. Again, this depends on how this specific VPN portal works. If the VPN gets the IPs from the firewall, then use the above link to configure it for the new VLANs.

# RDP with VLANs

As long as the firewall is configured to allow Remote Desktop Connections, it should work. By default, RDP only works within the same subnet, but the exception in the firewall allows the connection. If after migrating to VLANs RDP does not work, check group policy firewall settings and verify that it is allowed. You may also need to verify the ACLs on the firewall.

Also, it is vital that DNS is working, as across subnets you cannot use remote desktop without it.

# Fileserver Shares Across VLANs

Make sure the firewall allows filesharing between VLANs. Other than that, DNS should take care of the rest.

# Switch Configurations

Replace f0/0 with whatever interface is to be used and VLANID with the number of the VLAN ID to be used.

The default gateway of all the switches should be the IP of the main interface on the router (not sub interface of any VLAN) if they are not configured as such already.

## Configuring Switch Ports for VLANs

Interface f0/0

Switchport mode access

Switchport access vlan VLANID

If the VLAN does not already exist it will be created.

## Configuring Switch Ports for Voice VLAN (802.1p Encapsulation)

Interface f0/0

Mls qos trust cos

switchport voice vlan VLANID

The VLAN will be recognized as any other VLAN, so you can configure trunks and routers as for any regular 802.1q encapsulated VLAN.

## Configuring Trunks

Interface f0/0

Switchport mode trunk

Switchport trunk encapsulation dot1q

Switchport trunk allowed vlan VLANID (Can add more as more VLANs are added, or if left without this option, untagged traffic can also pass through by being assigned to the native VLAN which by default is 1 on Cisco switches)

## Configuring Servers

Once the ports are assigned to a VLAN, the following adjustments will have to be made:

* Any virtualized server needs to be on the appropriate port group network in vCenter
* The main DHCP scopes need to be assigned the appropriate VLAN ID so that IP addresses are assigned appropriately

\*Because [Redacted network information], no server reboot should be needed.

\*An IP address should be assigned to [Redacted]

# Workstations after Configuration of VLANs

A rolling restart may be required on all workstations after migration to VLANs is complete, because though it may be on the same subnet, [Redacted], it does not have the appropriate VLAN ID for that subnet, so it will not be able to communicate until a new IP lease is received. If any workstations for any reason are statically assigned either an IP that doesn’t exist on the network anymore, or one that is in the incorrect VLAN, it will need to be either reassigned or use DHCP.

In terms of the VPN, the user may simply have to disconnect from it and reconnect from it to get a new IP.

## Computers Statically Assigned to [Redacted]

The following will need to be moved if the [Redacted] is gone:

[Redacted workstation names and IPs]

There’s a reservation for [Redacted server and IP] though it has a static IP of [Redacted] – unsure why that is.

# Network Down Time

## Moving Ports

VLANs get assigned to specific ports, and what is currently plugged in to those ports may not be what should ultimately be on the appropriate VLAN. Because of the way the switches are configured now, the ports can be moved around and no matter what port they are plugged into they should have a connection to the network. If there is a plan of where everything is going and the task can be completed quickly, there will only be a short window of connectivity loss. However, when the actual switch configurations are uploaded, there will be loss of connectivity until the IP lease is renewed.

## Switch and Router Configurations

An exact plan (pre-made switch configurations, clear instruction on what exactly needs to be done on the router,) should be in place as this will require extended down time, especially if there are complications.

## Addressing Possible Complications

* The DHCP Relay Agent never ends up working, even after all options in the settings of the firewall are exhausted. In this case, the firewall itself can be configured as a DHCP relay agent, aka the IP Helper.
* In the event of any major failure, the old switch configurations (because they are not port dependent like the VLAN configurations,) can be loaded back on to the switches, (along with the settings file for the firewall if that doesn’t work with the new settings anymore.) Worst case scenario, if everything is done and is not working during down-time, re-upload the old configurations and settings, document what went wrong, and research later how to fix this issue, test it during another down-time, and keep doing this cycle until a resolution is reached.