FSM73xx GSM73xx GMS72xxR – Shared access to the Internet across Multiple routing VLANs using a Prosafe Firewall

This document describes how to:

- Create multiple routing VLANs
- Obtain Internet access on multiple VLANs using one Internet gateway

The procedure described can apply to most Layer 2 and Layer 3 Switches and VPN Firewall with new Web Interface (defined as the one with the Menus appearing horizontally on top).

Hardware differences among different models must be taken in consideration.

NOTE:
This document is not intended to illustrate how to perform full Layer3 separation, for which Access Control Lists (ACLs) should be used.

Table of Contents

1. VLAN-Definition .................................................................................................................. 2
2. Notes when setting-up VLANs ............................................................................................ 2
3. 1 - Physical Setup ................................................................................................................. 3
4. 2 - Logical Setup .................................................................................................................. 3
5. 3 - Configuring the Switch management IP address ............................................................... 4
6. 4 - Creating a routing VLAN ............................................................................................... 6
7. 5 - Remove ports’ VLAN membership ................................................................................... 8
8. 6 - Enable DHCP and create a DHCP pool per VLAN ........................................................... 10
9. 8 – Configuring the switch default route ............................................................................... 14
10. 9 – Configuring static routes on the Internet Default Gateway ............................................ 16
11. 10 – Saving the configuration ............................................................................................ 17
VLAN-Definition

VLANs are logical subgroups within a Local Area Network (LAN), which combine user stations, and network devices into a single unit, regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs use software to reduce the amount of time it takes for network changes, additions, and moves to be implemented.

Notes when setting-up VLANs

- A VLAN does not have a minimum number of port
- VLANs work at the OSI Layer 2
- A VLAN can be created per unit, device or via logical connection/combination
- Broadcast and Multicast traffic is transmitted only in the VLAN in which traffic is generated.
- To allow traffic between VLAN a device working at protocol level (Layer 3) is required

GSM7xxx - Shared access to the Internet across Multiple Routing VLANs using a Prosafe Firewall

Default IP route: 192.168.2.254

VLAN 2: Ports 0/1 – 0/8
PVID = 2
DHCP = 192.168.2.254/24

VLAN 3: Ports 0/9 – 0/28
PVID = 3
DHCP = 192.168.3.254/24

VLAN 4: Ports 0/31 – 0/40
PVID = 4
DHCP = 192.168.4.254/24
1 - Physical Setup

1x GSM7352S Prosafe Layer3 - Firmware 7.2.1.6
3x Windows XP Computers (1 on each VLAN)
1 x Prosafe Firewall Router DGFV338

2 - Logical Setup

DGFV338:
LAN IP 192.168.2.254/24
DHCP enabled (192.168.2.0/24, DG 192.168.2.1, DNS 192.168.2.254)
Static routes:
192.168.3.0 255.255.255.0 192.168.2.1
192.168.4.0 255.255.255.0 192.168.2.1

GSM7352S:

VLAN1: Management VLAN
IP 192.168.1.1
DG 192.168.1.254
DHCP disabled

VLAN2:
IP 192.168.2.1
DHCP enabled on DGFV338
(192.168.2.0/24, DG 192.168.2.1, DNS 192.168.2.254)

VLAN3:
IP 192.168.3.1
DHCP enabled (192.168.3.0/24, DG 192.168.3.1, DNS 192.168.2.254)

VLAN4:
IP 192.168.4.1
DHCP enabled (192.168.4.0/24, DG 192.168.4.1, DNS 192.168.2.254)
3 - Configuring the Switch management IP address

The Management IP address (by default on VLAN1) can be setup using the CLI (Command Line Interface).
The CLI should be access via HyperTerminal (or similar applications) using the Console cable included in the box.

User: admin
Password:
(FSM7352S) >enable
Password:

(GSM7352S) #

(GSM7352S) #network protocol none

Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n)y

(GSM7352S) #network parms 192.168.1.1 255.255.255.0 192.168.1.254

(GSM7352S) #show network

IP Address................................. 192.168.1.1
Subnet Mask............................... 255.255.255.0
Default Gateway.......................... 192.168.1.254
Burned In MAC Address.................... 00:1F:33:E6:81:A5
Locally Administered MAC Address....... 00:00:00:00:00:00
MAC Address Type........................ Burned In
Network Configuration Protocol Current... None
Management VLAN ID...................... 1
Web Mode.................................. Enable
Java Mode.................................. Enable

(GSM7352S) #
When a Management IP address is configured, the Web Interface of the switch can be accessed. It will be possible to modify the Management IP configuration via System – Management – IP configuration including the IP address, Subnet Mask, Default Gateway and Management VLAN ID.
4 - Creating a routing VLAN

To create routing VLANs access the VLAN Routing Wizard via Routing VLAN.

1) Type the VLAN ID (in the example the VLAN ID is 2)

2) Specify the IP address (192.168.2.1) and the subnet mask (255.255.255.0)

3) Expand the Port list by clicking on Unit 1

4) Select the correct option for each port that will be member of the VLAN

Three options are available:

- No membership (no symbol appearing in the gray box underneath the port number)
- Untagged membership (U)
- Tagged membership (T)

In order to browse through the options just continuously click on the gray box until the correct one is set. For this scenario we will be using the U (Untagged) option on all the ports.

5) Apply the changes
Once all the relevant VLANs have been added – a summary can be found in the VLAN routing section of the menu.

In this case VLAN 2, 3, and 4 have been added to the configuration. A new Virtual port is assigned to each VLAN.
5 - Remove ports’ VLAN membership

To remove port memberships from a VLAN, the VLAN configuration must be accessed via Switching – VLAN – VLAN Membership.

In order to remove a port from the VLAN memberships just continuously click on the gray box underneath the port number, until no symbol appears as in the picture below.

The VLAN Status page will show the update membership for all the VLAN
In this scenario we require to remove from VLAN1, membership to those ports that appear in any of the other VLANs to ensure total VLAN separation.

When setting a routing VLAN the PVID (Port VLAN ID) is automatically set to the VLAN ID. This can be confirmed using the Port PVID Configuration page.
The DHCP server can be enabled via the System – Services – DHCP Server Configuration page.

To create a new DHCP pool, access the DHCP Pool Configuration page:

1) Select the Pool name - for ease of configuration this might be same as the VLAN name if the pool will be associate to a VLAN
2) Specify the Network number (subnet address), Subnet mask, Default router and DNS Server

The association between a DHCP pool and a VLAN will be on the basis of the IP address assigned to the VLAN itself and the subnet mask.

Therefore if it is required to associate a DHCP Pool to a VLAN ensure that the IP address assigned to the VLAN falls within the network number (or subnet) specified in the pool.

For example VLAN 2 which in this scenario is assigned with IP address 192.168.2.1 and subnet mask 255.255.255.0 falls within the subnet 192.168.2.0/24.
When creating the DHCP for VLAN2 we have made sure that the network address specified would be 192.168.2.0 with subnet mask 255.255.255.0. Automatically the switch will associate such DHCP pool with VLAN2.
7 – VLAN routing

By default RIP is enabled on the Layer 3 switches.

RIP can be disabled on all the ports via Routing – RIP – RIP configuration

or alternatively it can be disabled on a per port basis, including the VLAN virtual ports.

The picture below shows RIP enable on all the Virtual ports associated to each of the VLAN created and the Link State for each port as “Link Down”.

The reason for this is due to no device being plugged in any of the VLAN ports – RIP requires at least one interface to be active in order for the protocol to be able to send routing updates.
The next picture shows that at least one device has been connected to one of the ports in VLAN 2 (Interface 0/2/1) and VLAN 4 (Interface 0/2/3) changing the Link state to “Link up”. 
8 – Configuring the switch default route

Although RIP is enabled by default, this is not necessary for routing to take place and can be disabled.

When creating a routing VLAN a static route is added to the Layer 3 switch routing table.

A summary of the routes can be found in Routing – Routing table – Route configuration.

In the same page it is possible to set the DefaultRoute.

This is necessary to instruct the Layer 3 switch that any traffic not destined to the local VLANs should be sent to a Default Gateway.

In our scenario the Internet Default Gateway is the DGFV338 on IP address 192.168.2.254. The DefaultRoute is configured accordingly in the next picture.
## Route Configuration

### Configure Routes

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Network Address</th>
<th>Subnet mask</th>
<th>Next Hop IP Address</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.2.254</td>
<td>1</td>
</tr>
</tbody>
</table>

### Learned Routes

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Network Address</th>
<th>Subnet mask</th>
<th>Protocol</th>
<th>Next Hop Interface</th>
<th>Next Hop IP Address</th>
<th>Preference</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic</td>
<td>192.168.2.0</td>
<td>255.255.255.0</td>
<td>Local</td>
<td>VLAN 2</td>
<td>192.168.2.1</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>Dynamic</td>
<td>192.168.3.0</td>
<td>255.255.255.0</td>
<td>Local</td>
<td>VLAN 3</td>
<td>192.168.3.1</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>Dynamic</td>
<td>192.168.4.0</td>
<td>255.255.255.0</td>
<td>Local</td>
<td>VLAN 4</td>
<td>192.168.4.1</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>
9 – Configuring static routes on the Internet Default Gateway

In order to ensure the Internet Gateway is aware on how to return traffic to devices in VLAN not directly attached to it, static routes must be configured for each VLAN.

The following two pictures provide a summary of how this is achieved on the DGFV338 via the Network Configuration – Routing page.

In this scenario two routes are required as two are the VLANs not directly connected to the DGFV338 LAN interface.
10 – Saving the configuration

The switch does not save the configuration automatically every time a change is performed, either via the CLI or the WEB GUI.

It is necessary to force the saving, which can be achieved via Maintenance – Save Config