Magnum MNS6K Vlan Configuration Guide

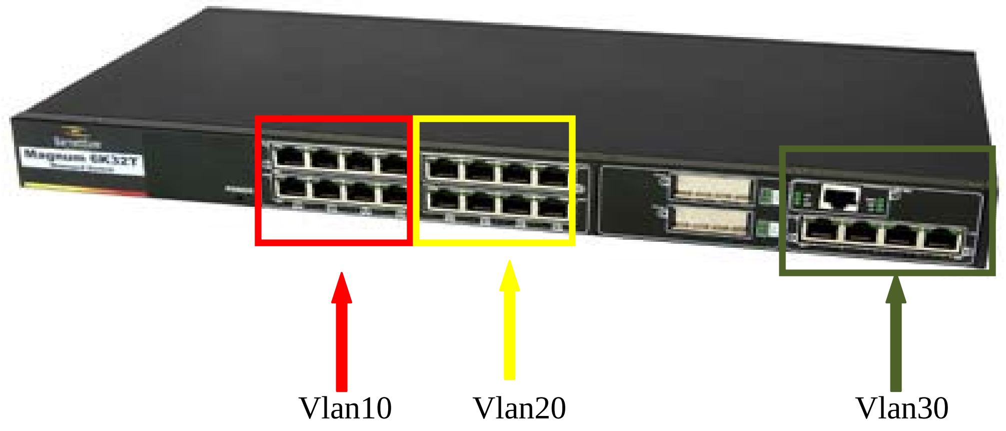
Abstract

This guide seeks to explain the concept behind the working of Virtual Local Area Networks (VLAN) and how to implement VLANs in Garrettcom Magnum 6K Series Switch environment using the Command Line Interface (CLI).

VLAN: An Introduction

Virtual Local Area Networks or VLANs in short, are logical groupings of network resources in such a way that though they may be placed at different physical locations yet communicate with each other as if they are on the same broadcast domain (or ethernet switch). VLANs prevents traffic and the broadcast storms originating in one part of the network from reaching other parts of the network thereby reducing operation overheads on the network nodes. By establishing separate broadcast domains, network administrators can protect the resources in one particular logical segment from sending out or receiving unwanted traffic to and from the other segments on the network and thereby ensuring efficiency, security and optimum bandwidth utilization to resources on each separate network segment. The IEEE 802.1Q specifications establish a standard method of inserting VLAN information into the Ethernet frames, when VLANs span across multiple switches.

Fig 1.1

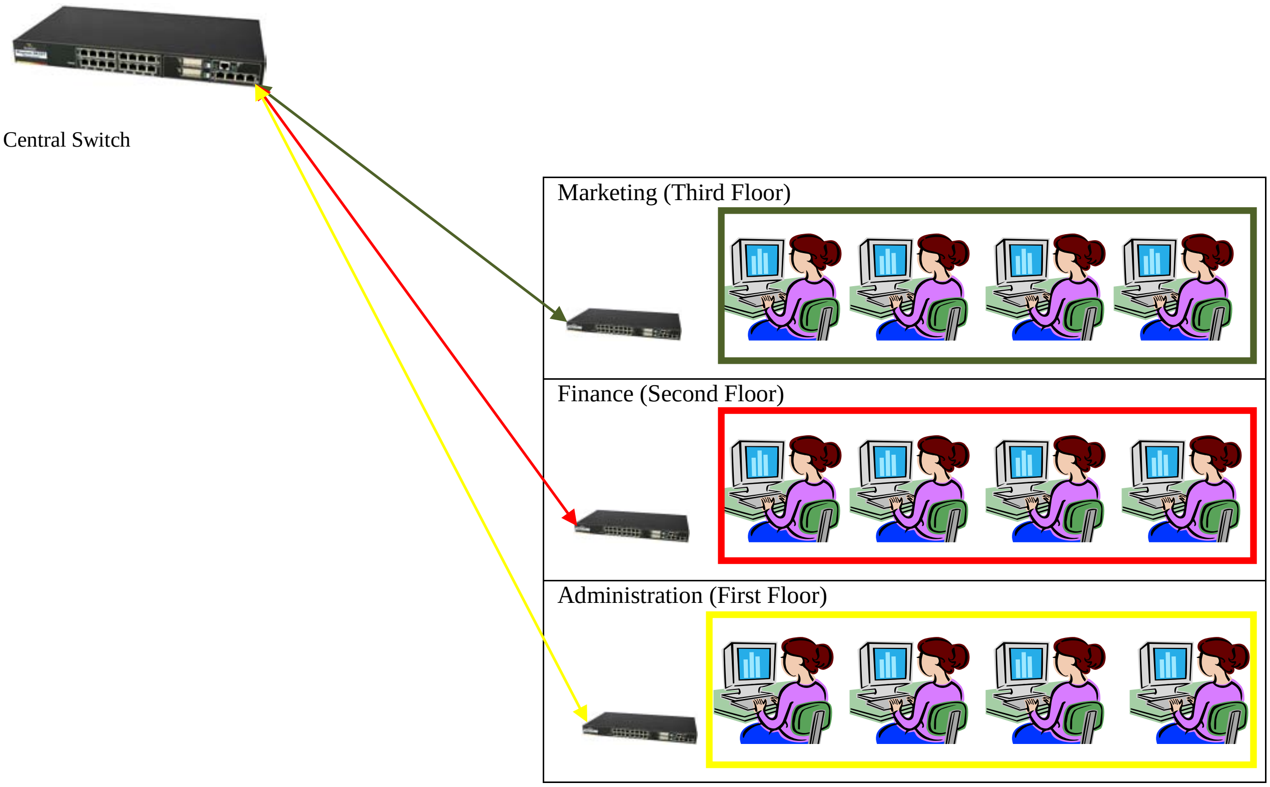


VLANs work on the layer 2 (Data Link Layer) of the OSI model. As shown in the image above, the switch can be logically divided into several VLANs and nodes in one VLAN cannot communicate with or see traffic from the other VLANs, as each VLAN is a separate broadcast domain. Any host on VLAN 20 will not be able to talk to any host on either VLAN 10 or VLAN 30 even though they are on the same physical switch. The only difference between the VLANs and the IP subnet is that, VLANs divided the network on the layer 2 level (Data Link Layer), while the IP subnets divide the network on the layer 3 level. The ports do not have to be assigned to the VLANs in contiguous blocks. VLANs membership is assigned on individual port basis. A port belonging to VLAN 10 could be the first port on switch module A and the second port on the same module A could belong to VLAN 14 and the third port on the module may belong to VLAN 20 and so on.

Planning For VLANs

There are several ways a network administrator can choose to plan and implement VLANs on their networks. One way to implement VLANs is to create them on departmental functionality. It is a common practice that users in a particular department sit near to each other, on the same floor or part of the building. For example Administrators usually occupy the first floor, while users in the Finance department will be seated on a different floor (above ground) and so are the users in Marketing division, who will have a separate floor or a building assigned to them to perform their day-to-day duties and tasks. So a network administrator can create a separate VLAN for each department and will put each shared network resource of a department into its respective VLAN. One of the advantages of implementing VLANs is the flexibility of the of bringing together resources in the same department within one domain irrespective of their physical location. It could be possible that some users, like VP of sales, engineering, marketing may have their offices at a different location other than where most of the users in their respective department sit, still they would be able to access the resources that they need without having the need to install a new switch or pull a new cable. A network administrator can simply configure the local switch with the appropriate VLAN and put the computer on that particular VLAN allowing the executives to access the resources in their respective departments.

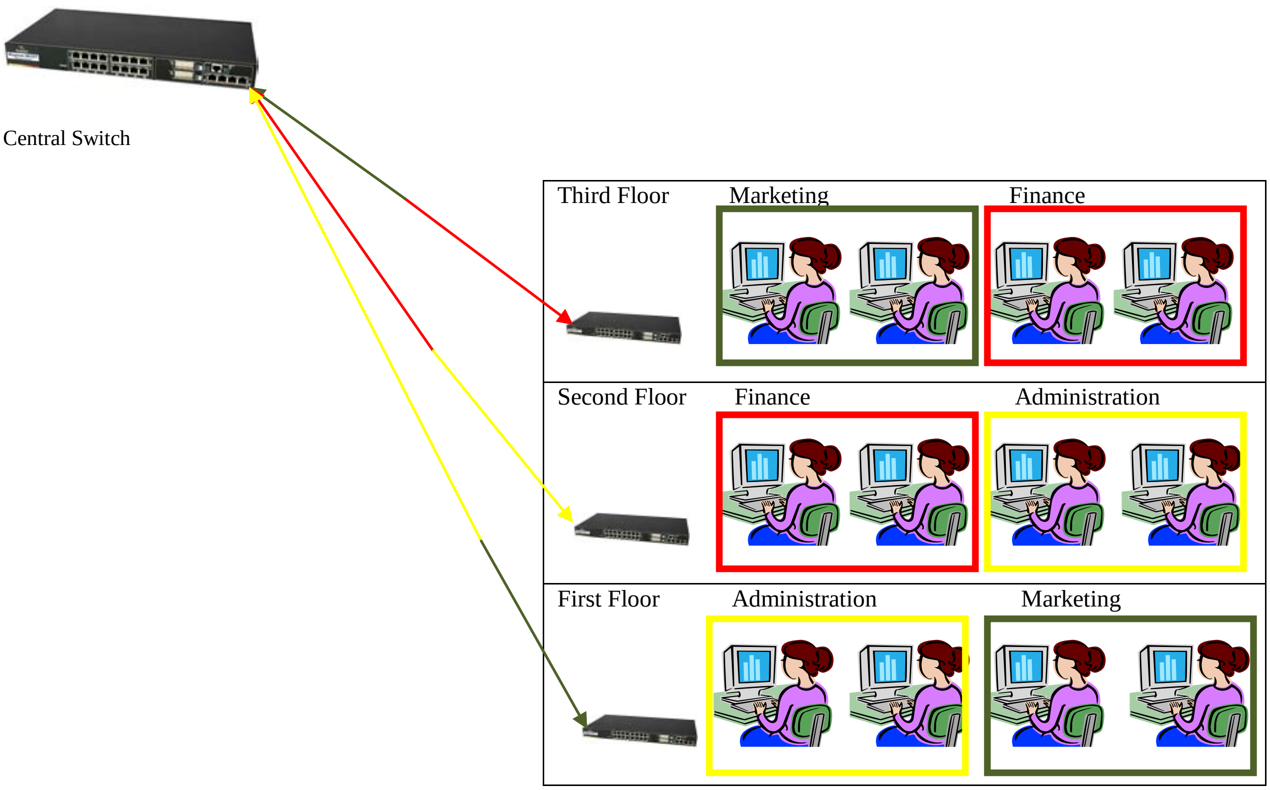
Fig 1.2



Here each floor represents a different department, each with its staff doing specific tasks and performing their set of duties. The network administrators can thus divide their network using VLANs and create VLAN for each department on the local switch and put all the users in that department in that VLAN. This way traffic generated on the network by users in Finance department is restricted to only their part of the network and does flow over into either Marketing or Administration department's part of the network. Thus the resources in each department are efficiently managed with less network overheads to deal with.

VLANs can also be configured to span multiple switches, if the users are spread out topographically or geographically.

Fig 1.3



In the Fig 1.3 above, we see that users in various departments are sitting on various levels on the same building or in other words the users not sitting at the same location as their peers from their department. Still through the VLANs users on each department can access resources on their respective VLANs even though they are on different levels within the same building. The users of Administration division on the first floor can share information and resources with their coworkers on the second level, while the users in the Finance division on the second floor can share information and resources with their coworkers on at the third level. The users belonging to the Marketing group on the third level will not see information or the traffic that is shared between the users in the Finance division on the second and the third floor even though the both Marketing and Finance users are physically connected to the same ethernet switch on the third floor. This is because the switch on each floor has been logically divided into separate VLANs thereby isolating the traffic originating from one VLAN from another VLAN.

VLAN and IP Subnet Mapping

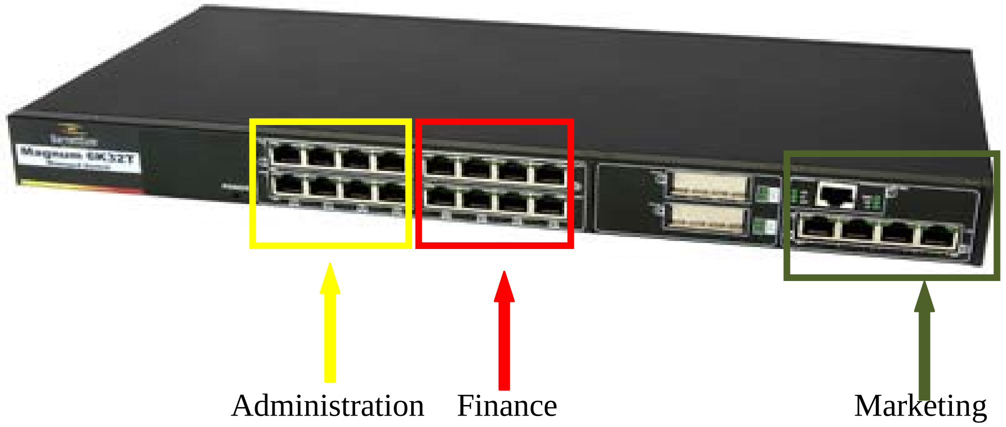
There are two ways of mapping VLANs to IP subnets. The network administrator has to choose a unique IP subnet for each VLAN. This type of arrangement between VLANs and IP subnets is called “One-to-one” mapping. The other type of mapping, where in multiple IP subnets can be mapped to a single VLAN. This particular operation is done on routers or a switch capable of performing layer 3 functions (routing etc.) where inter-VLAN routing is required. The above has been mentioned only for information purpose and the configuration and implementation of inter-VLAN routing is beyond the scope of this guide.

The Garrettcom MNS 6K Implementation of VLANs

The Garrettcom MNS6K VLAN implementation strictly follows the IEEE802.1Q standards and the VLANs are implemented, in design, the same way as described earlier. The MNS6K supports only TAG based VLANs. There is no support for Port based VLANs on the Garrettcom MNS6K firmware. We can assign all the ports on a single switch to just one VLAN or assign the ports on the same switch evenly between the VLANs as per our requirements. The Garrettcom MNS6K version supports up to 32 VLANs and the SECURE-MNS6K version supports up to 256 VLANs per switch.

Creating and Implementing VLANs

A network administrator has to create some VLANs and assign ports to those VLANs. The following steps will help the network engineer to configure VLAN on a single switch. For example, let us take that there is a need to create three VLANs, one for Administration, one for Finance and one for Marketing. Let us say we want VLAN 2 for Administration, VLAN 3 for Finance and VLAN 4 for Marketing. We want all the ports on slot ‘A’ from 1-8 to be on VLAN 2. Ports on slot ‘B’ from 9-16 on VLAN 3 and ports on slot ‘D’ to be on VLAN 4



The following steps allow a network engineer to configure the VLANs as required in the above described scenario. Log into the switch either via TELNET or console port of the switch, using the privilege mode credentials.

Step 1: Type “vlan” at the switch prompt

```
Magnum6k#vlan

Magnum6k(tag-vlan)##
```

Step 2: Enable VLAN

```
Magnum6k(vlan)##vlan enable
```

Step 3: Create VLANs

```
Magnum6k(tag-vlan)##add id=2 name=Administration port=1-8

Magnum6k(tag-vlan)##add id=3 name=Finance port=9-16

Magnum6k(tag-vlan)##add id=4 name=Marketing port=25,26,28,30,32
```

Step 4: Start VLANs

Magnum6K(tag-vlan)## start vlan=2,3,4

The user can also start all the VLANs together by giving the following command

Magnum6K(tag-vlan)## start vlan=all

Step 5: Configure the access ports (that will connect to the end devices) with default VLAN id

Magnum6k(tag-vlan)##set-port port=1-8 default id=2

Magnum6k(tag-vlan)##set-port port=9-16 default id=3

Magnum6k(tag-vlan)##set-port port=25,26,28,30,32 default id=4

Step 6: Save the changes to the configuration

Magnum6K(tag-vlan)## save

Checking VLAN Configuration

Step 1: Give command “show vlan”

```
Magnum6K(tag-vlan)## show vlan

VLAN ID: 2

Name : Administration

Status : Active

-----------------------------------------------

 PORT |     MODE      |      STATUS

-----------------------------------------------

    1 |      UNTAGGED |       DOWN

    2 |      UNTAGGED |       DOWN

    3 |      UNTAGGED |        UP

    4 |      UNTAGGED |       DOWN

    5 |      UNTAGGED |       DOWN

    6 |      UNTAGGED |       DOWN

    7 |      UNTAGGED |       DOWN

    8 |      UNTAGGED |       DOWN
```

```
VLAN ID: 3

Name : Finance

Status : Active

-----------------------------------------------

 PORT |     MODE      |      STATUS

-----------------------------------------------

    9 |       UNTAGGED |       DOWN

   10 |       UNTAGGED |       DOWN

   11 |       UNTAGGED |       DOWN

   12 |       UNTAGGED |       DOWN

   13 |       UNTAGGED |       DOWN

   14 |       UNTAGGED |       DOWN

   15 |       UNTAGGED |       DOWN

   16 |       UNTAGGED |       DOWN

VLAN ID: 4

Name : Marketing

Status : Active

-----------------------------------------------

 PORT |     MODE      |      STATUS

-----------------------------------------------

   25 |       UNTAGGED |       DOWN

   26 |       UNTAGGED |       DOWN

   28 |       UNTAGGED |       DOWN

   30 |       UNTAGGED |       DOWN
```

The access ports, i.e. the ports that have end devices like servers, cameras, PLCs, RTUs, Sensors, computers and other devices, should always be left “untagged”. Tagging on the port has a separate function, which will be described in detail in the later sections of the configuration guide.

To check the port-wise VLAN configuration, follow the next step described below.

Magnum6K(tag-vlan)## show-port port=x

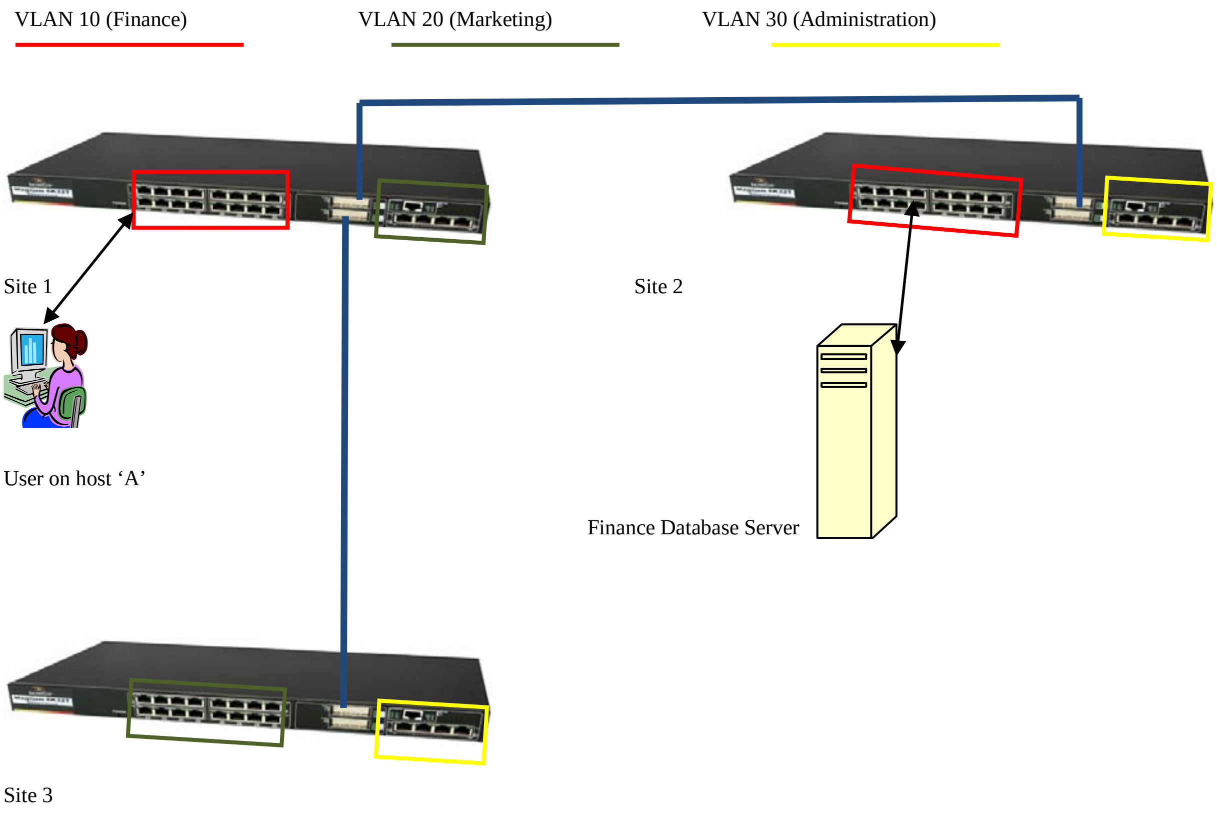
```
Magnum 6K32T(tag-vlan)##show-port port=1-3

VLAN Port Status.

 Port   1

    Default ID              :    2

    Filter Status           : DISABLED.

    VLAN Memberships:

      Vlan:    1 Status:  Active   UNTAGGED

      Vlan:    2 Status:  Active   UNTAGGED

  Port   2

    Default ID              :    2

    Filter Status           : DISABLED.

    VLAN Memberships:

      Vlan:    1 Status:  Active   UNTAGGED

      Vlan:    2 Status:  Active   UNTAGGED

  Port   3

    Default ID              :    2

    Filter Status           : DISABLED.

    VLAN Memberships:

      Vlan:    1 Status:  Active   UNTAGGED

      Vlan:    2 Status:  Active   UNTAGGED

------Output Truncated-------------

Port   9

    Default ID              :    3

    Filter Status           : DISABLED.

    VLAN Memberships:

      Vlan:    1 Status:  Active   UNTAGGED

      Vlan:    3 Status:  Active   UNTAGGED

  Port  10

    Default ID              :    3

    Filter Status           : DISABLED.

    VLAN Memberships:
      Vlan:     1 Status:  Active   UNTAGGED

      Vlan:     3 Status:  Active   UNTAGGED

  Port  11

    Default ID              :     3

    Filter Status           : DISABLED.

    VLAN Memberships:

      Vlan:     1 Status:  Active   UNTAGGED

      Vlan:     3 Status:  Active   UNTAGGED

------Output Truncated---------------

  Port  25

    Default ID              :     4

    Filter Status           : DISABLED.

    VLAN Memberships:

      Vlan:     1 Status:  Active   UNTAGGED

      Vlan:     4 Status:  Active   UNTAGGED
```

Most common step that the engineers working on Garrettcom MNS6K for the first time skip is to change the default IDs of the ports to the VLAN ID of the newly created VLAN. By default, all the ports have the VLAN ID of 1 and this default ID remains even when ports are assigned to VLANs at the time of creating new VLANs. Make sure that the default ID of the port is changed to the VLAN the port is supposed to be the member of.

VLAN Trunking (802.1Q Encapsulation)

The IEEE802.1Q is the standard for sending frames across one "VLAN-aware" switch to another "VLAN-aware" switch where the destination resource sits. Trunking is simply a method of "tagging" an ethernet frame with the appropriate VLAN ID and sending it over the uplink to the receiving switch, which will then take a decision on frame depending upon the tagged information on the received ethernet frame.

Consider the scenario, where the users of each department are not located in one place but physically located on different sites or buildings (or floors). In this scenario we will consider that at each site there are at least two department and they have to communicate and share information with their counterparts working at other remote locations. For example employees of Administrative division at “Site 2” have to share information and resource with their colleagues sitting at “Site 3” and vice versa. The employees of Finance division at “Site 1” have to access finance database servers located at “Site 2”. Let us say that a user on host ‘A’ at “Site 1” belonging to Finance division needs to access the finance database server ‘FDB’ located at “Site 2”.



When the switch at “Site 1” receives the frames for connection request to Finance Database Server on “Site 2”, the switch checks the destination mac address of the frame with its own mac address table and determines the server can be reached via its trunk port (or the port linking the switch at “Site 2”. The switch then tags the packet with the appropriate VLAN ID (3) and passes it over to the switch, via the trunk, at “Site 2”. When the switch at “Site 2” receives the frame, it examines the frame and looks for the VLAN ID, if the VLAN IDs match, the receiving switch strips the packet of the VLAN tag and forwards it to the destination. If the VLAN IDs do not match, the receiving switch will just drop the frame. When the finance database server sends its response back to the host, the whole process of tagging of frame before it is sent over the link and the untagging of the frame at the receiving end is repeated all over again.

The users have to bear in mind that what is usually known as the “Trunk” port in Cisco and other vendor switches, is actually a VLAN-tagged port on the Garrettcom managed switch solution. To enable VLAN tagging, make sure that ports are members of the VLANs they will be tagging on the “Trunk” ports. The commands given below show how to add ports to existing VLANs and steps to configure the “trunk” ports.

```
Magnum6K(tag-vlan)##set-port port=17-18 join id=2
Magnum6K(tag-vlan)##set-port port=17-18 join id=3
Magnum6K(tag-vlan)##set-port port=17-18 join id=4
```

To configure the ports to act as “trunk” or “tagging” ports, give the following commands:

```
Magnum6K(tag-vlan)##set-port port=17-18 tagging id=2 status=tagged
Magnum6K(tag-vlan)##set-port port=17-18 tagging id=3 status=tagged
Magnum6K(tag-vlan)##set-port port=17-18 tagging id=4 status=tagged
```

To verify that the ports are “tagging” the frames with appropriate VLANs, the following command and the command output will display the following

```
Magnum6K(tag-vlan)##show-port port=17-18
Port   17
    Default ID              :    1
    Filter Status           : DISABLED.
    VLAN Memberships:
      Vlan:     1 Status:  Active   UNTAGGED
      Vlan:     2 Status:  Active  TAGGED
      Vlan:     3 Status:  Active   TAGGED
      Vlan:     4 Status:  Active   TAGGED
  Port   18
    Default ID              :    1
    Filter Status           : DISABLED.
    VLAN Memberships:
      Vlan:     1 Status:  Active   UNTAGGED
      Vlan:   2 Status:  Active   TAGGED
      Vlan:    3 Status: Active   TAGGED
      Vlan:    4 Status: Active   TAGGED
```

The default ID of the trunk or tagged ports can be either VLAN1 or any other user chosen VLAN ID (similar to “Native VLAN” of the trunk on Cisco switches) and default id of the trunk ports of two directly connected switches should always be the same and should always be left “untagged”. The switches need one untagged VLAN to exchange VLAN information and STP BPDUs. Cisco recommends that when connecting a Cisco switch with a non-Cisco switch, the default ID of the trunk port should always be set to VLAN 1 for proper communication and exchange of information.