Traffic Filtering and DSCP Marking in vDS 5.5

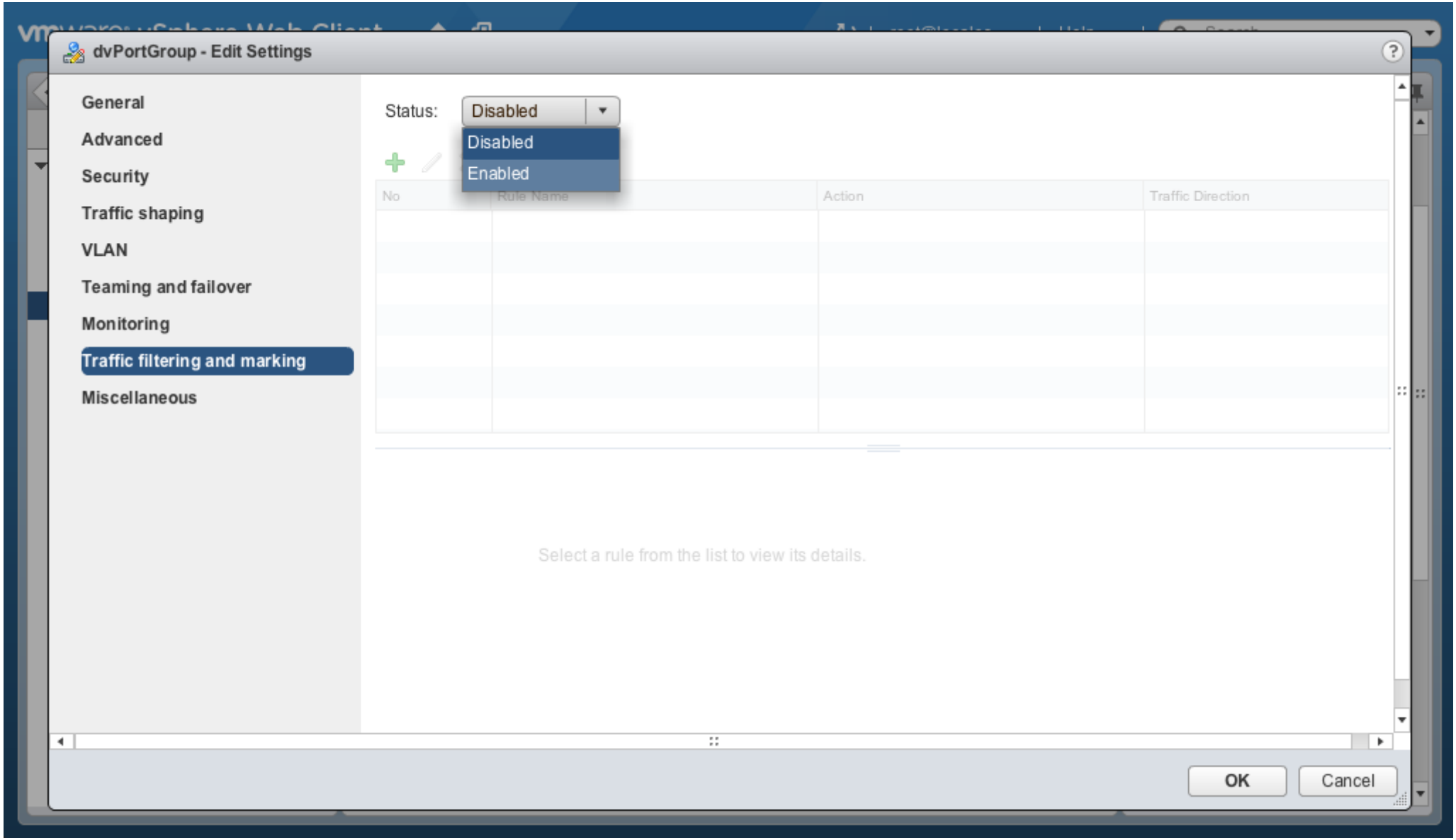
Do you know when you use a vSphere distributed switch 5.5, you can protect the virtual network from unwanted traffic and security attacks or apply a QoS tag to a certain type of traffic by using the traffic filtering and marking policy.

The traffic filtering and marking policy represents an ordered set of network traffic rules for security and for QoS tagging of the data flow through the ports of a distributed switch. In general, a rule consists of a qualifier for traffic, and of an action for restricting or prioritizing the matching traffic.

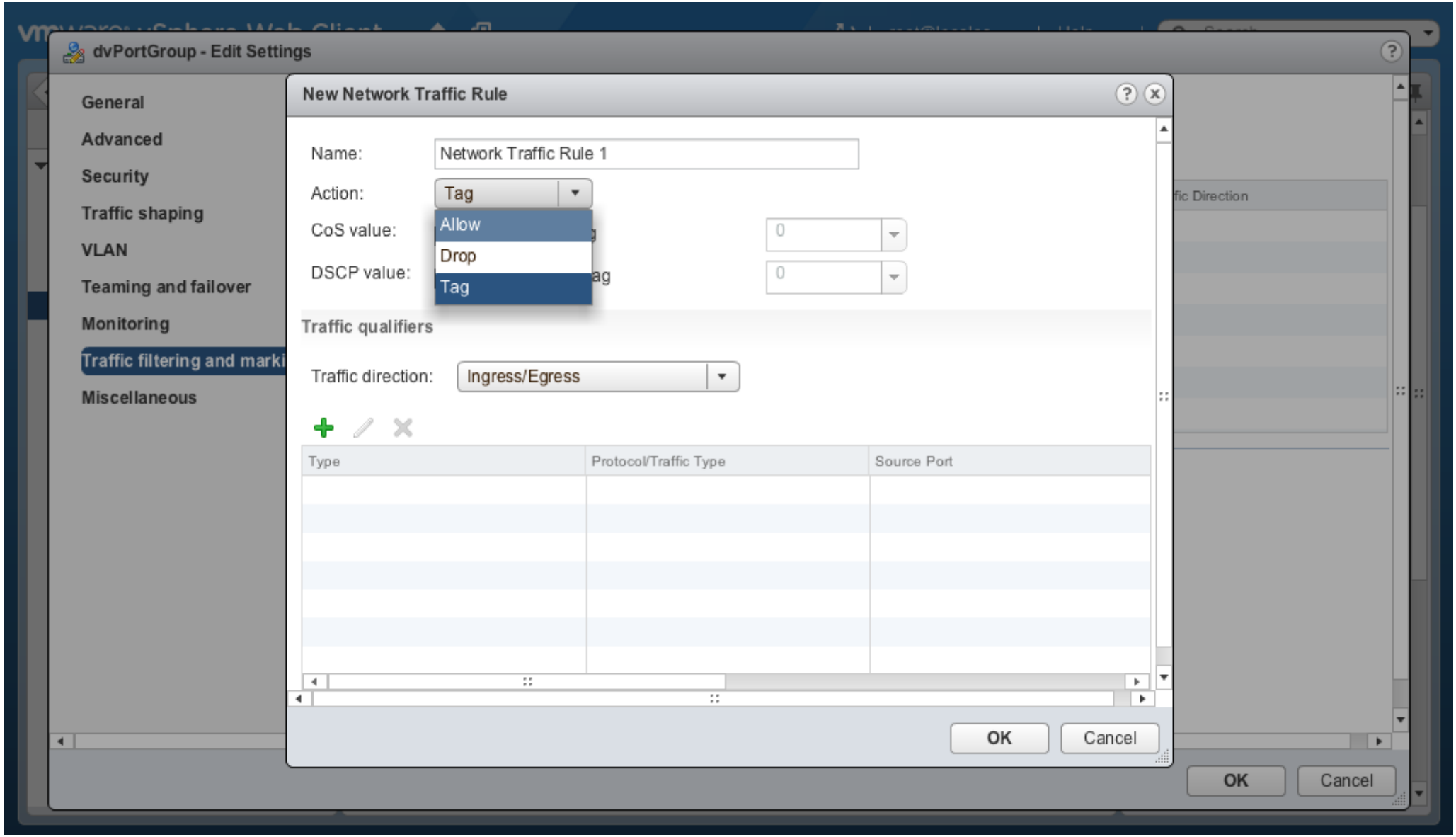
The vSphere distributed switch applies rules on traffic at different places in the data stream. The distributed switch applies traffic filter rules on the data path between the virtual machine network adapter and distributed port, or between the uplink port and physical network adapter for rules on uplinks.

Filtering is equivalent to the Access Control List (ACL) feature available on physical switches. That means basically you’re either allowing traffic, or you are dropping it. It is stateless as well, i.e, it is based purely on a property of the traffic classification such as IP address & MAC Address etc.

You need to define filtering rules at the Port group level.

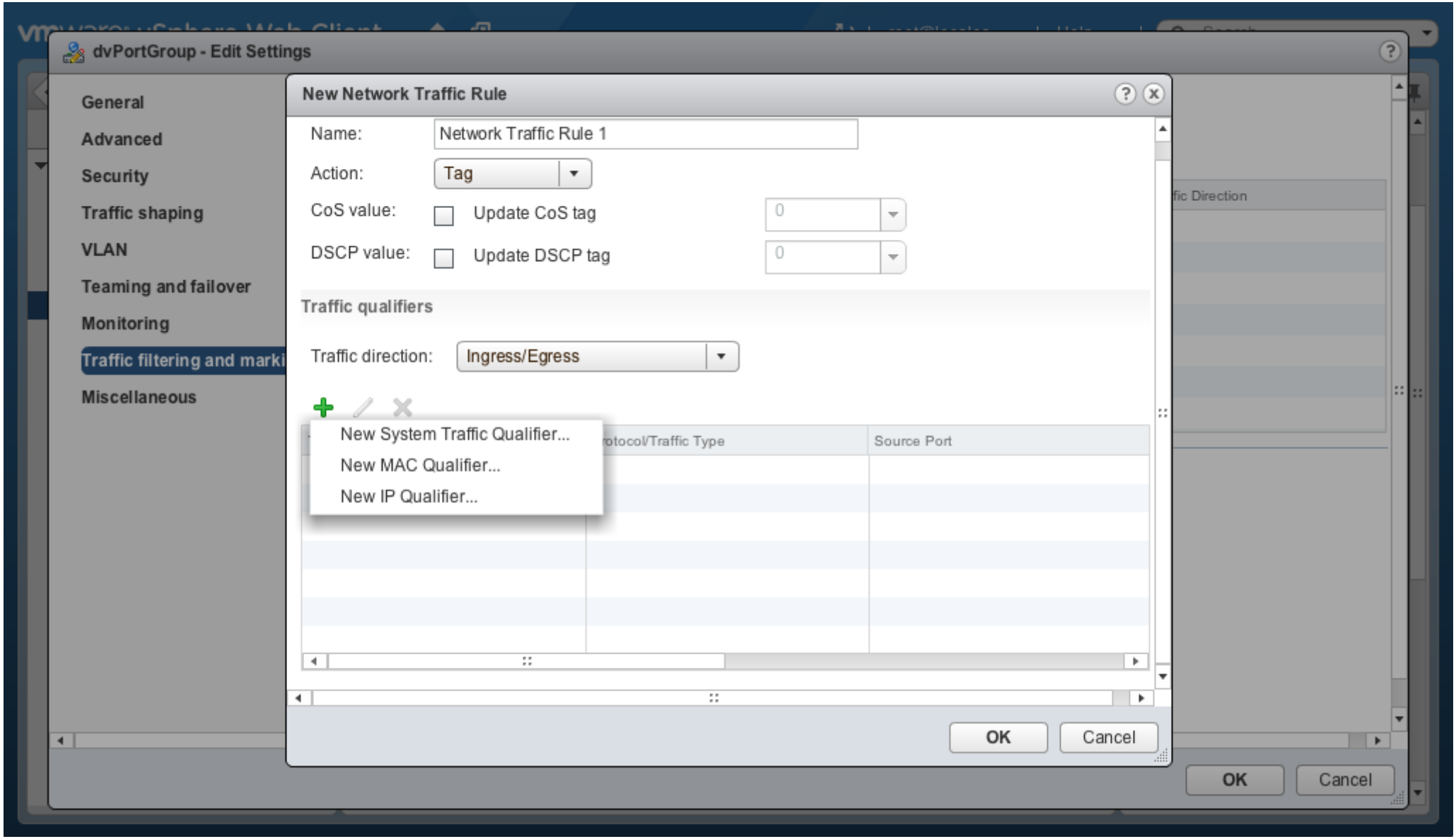


When you click on the green "+" sign, you can create a rule set by allowing or dropping or tagging traffic based on the rule. The default action is "Tag". You also need to define the traffic classification factors to be in.



The traffic that you want to filter or want to mark with QoS tags can be matched to the type of carried infrastructure data, such as data for storage, vCenter Server management, and so on, and to Layer 2 and Layer 3 properties. To match the traffic in the scope of the rule more precisely, you can combine criteria for system data type, Layer 2 header, and Layer 3 header.

Now let me describe the three different Traffic type.



System Traffic Type

You can select the type of traffic through the ports of the group that carries system data, that is, traffic for management from vCenter Server, storage, vMotion, and vSphere Fault Tolerance. You can mark or filter only a specific traffic type, or for all system data traffic. For example, you can mark with a QoS value or filter the traffic for management from vCenter Server, storage and vMotion, but not the traffic carrying the Fault Tolerance data.

MAC Traffic Qualifier

By using the MAC traffic qualifier in a rule, you can define matching criteria for the Layer 2 (Data Link Layer) properties of packets such as MAC address, VLAN ID, and next level protocol that consumes the frame payload.

IP Traffic Qualifier

By using the IP traffic qualifier in a rule, you can define criteria for matching traffic to the Layer 3 (Network Layer) properties such as IP version, IP address, next level protocol, and port.

DSCP or Differentiated Services Code Point helps provide end to end Quality of Service and Service Level Agreement (SLA). This is the tagging mechanism near the source of the traffic and that is why it is best to tag as close to the source of the traffic as possible in order to ensure full benefits are realised. It can classify network traffic and provide QoS. 6 bits in the IP header are for packet classification and has 64 different traffic classes.

Similar to the filtering rule tagging rule is also applied at the Port group level.