IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

PARITY NETWORKS LLC,	§	
	§	
Plaintiff,	§	
	§	CIVIL ACTION NO. _______________
v.	§	
	§	
NETGEAR, INC.,	§	**JURY TRIAL DEMANDED**
	§	
Defendant.	§	

ORIGINAL COMPLAINT

Plaintiff Parity Networks LLC ("Plaintiff" or "Parity Networks"), by and through its attorneys, file its Original Complaint against NETGEAR, Inc. ("Defendant" or "NETGEAR"), and demanding trial by jury, hereby alleges as follows:

I. NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 271, *et seq.*, to enjoin and obtain damages resulting from Defendant's unauthorized use, sale, and offer to sell in the United States of products, methods, processes, services and/or systems that infringe Parity Networks' United States patents, as described herein.

2. Defendant manufactures, provides, uses, sells, offers for sale, imports, and/or distributes infringing products and services; and encourages others to use its products and services in an infringing manner, including their customers, as set forth herein.

3. Parity Networks seeks past damages and prejudgment and post-judgment interest for Defendant's past infringement of the Patents-in-Suit, as defined below.

II. PARTIES

4. Plaintiff Parity Networks is a limited liability company organized and existing under the laws of the State of Texas.

5. On information and belief, Defendant is a corporation organized under the laws of Delaware, with a place of business located at 350 East Plumeria Drive, San Jose, CA 95134. Defendant's registered agent for service of process in Delaware is Incorporating Services, Ltd., 3500 S Dupont Highway, Dover, DE 19901.

III. JURISDICTION AND VENUE

6. This is an action for patent infringement arising under the Patent Laws of the United States, in particular 35 U.S.C. §271, 281, 283, 284, and 285. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §1331 and 1338(a).

7. Upon information and belief, Defendant transacts substantial business in the State of Delaware and in this District. Defendant, directly and through subsidiaries or intermediaries (including distributors, retailers, resellers and others), has purposefully and voluntarily placed one or more of their infringing products, as described below, into the stream of commerce with the expectation that these infringing products will be purchased and used by customers in the District. Defendant has committed acts of patent infringement within the District.

8. This Court has personal jurisdiction over Defendant because it has committed acts giving rise to this action within the State of Delaware and within this District. The Court's exercise of jurisdiction over Defendant would not offend traditional notions of fair play and substantial justice because Defendant has established minimum contacts with the forum with respect to both general and specific jurisdiction.

9. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1400(b) and 28 U.S.C. § 1391(b) because Defendant resides here and because Defendant has committed acts of infringement in this judicial district.

IV. FACTUAL ALLEGATIONS

PATENTS-IN-SUIT

10. Parity Networks is the owner of all right, title, and interest in and to U.S. Patent No. 6,252,848 (the "'848 Patent," attached as **Exhibit 1**), entitled "System Performance in a Data Network through Queue Management Based on Ingress Rate Monitoring," issued on June 26, 2001.

11. Parity Networks is the owner of all right, title, and interest in and to U.S. Patent No. 6,763,394 (the "'394 Patent," attached as **Exhibit 2**), entitled "Virtual Egress Patent Classification at Ingress," issued on July 13, 2004.

12. Parity Networks is the owner of all right, title, and interest in and to U.S. Patent No. 6,870,844 (the "'844 Patent," attached as **Exhibit 3**), entitled "Apparatus and Methods for Efficient Multicasting of Data Packets," issued March 22, 2005.

13. Parity Networks is the owner of all right, title, and interest in and to U.S. Patent No. 7,103,046 (the "'046 Patent," attached as **Exhibit 4**), entitled "Method and Apparatus for Intelligent Sorting and Process Determination of Data Packets Destined to a Central Processing Unit of a Router or Server on a Data Packet Network," issued on September 5, 2006.

14. Parity Networks is the owner of all right, title, and interest in and to U.S. Patent No. 7,107,352 (the "'352 Patent," attached as **Exhibit 5**), entitled "Virtual Egress Packet Classification at Ingress," issued on September 12, 2006.

15. Parity Networks is the owner of all right, title, and interest in and to U.S. Patent No. 7,719,963 (the "'963 Patent," attached as **Exhibit 6**), entitled "System for Fabric Packet Control," issued on May 18, 2010.

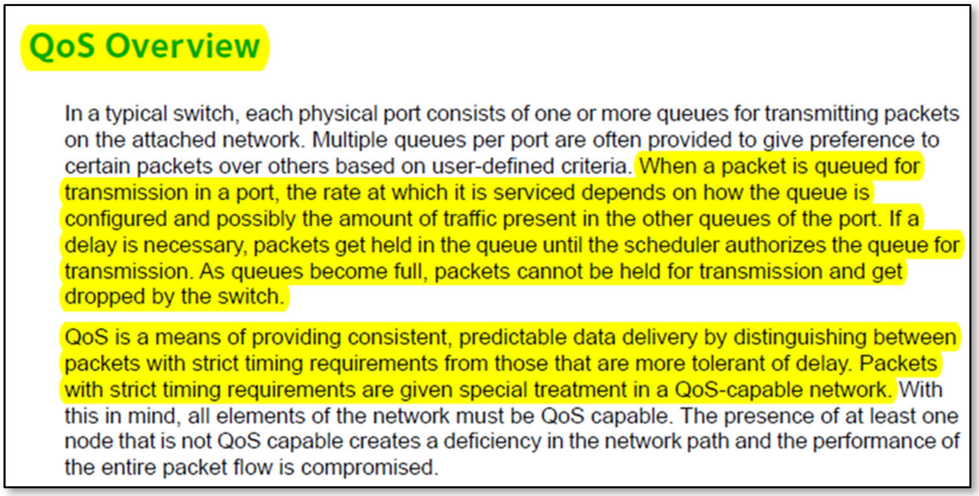
16. Together, the foregoing patents are referred to herein as the "Patents-in-Suit." Parity Networks is the assignee of the Patents-in-Suit and has all rights to sue for infringement and collect past damages for the infringement thereof.

DEFENDANT'S ACTS

17. Defendant is a provider of data networking products and solutions and provides hardware and software directed to switching and routing network data to its customers in the United States, including in this District. Defendant provides a variety of networking switches.

18. On information and belief, Defendant designs, develops, supports, and coordinates the importation into the United States of the exemplary accused products set forth below.

19. Defendant provides instructions on how to make and use the patented inventions of the '848 Patent by configuring the CoS and QoS software components in its accused switches and routers, including "Diffserv Policy," of its products in accordance with its instructions and specifications. For example, Defendant instructs as follows:

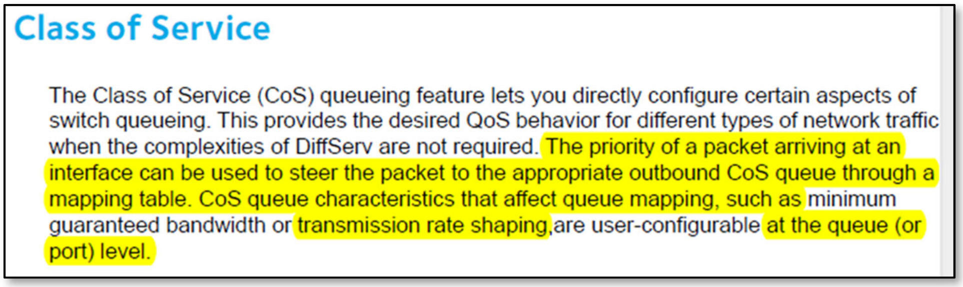


QoS Overview

In a typical switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets cannot be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets with strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS capable. The presence of at least one node that is not QoS capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

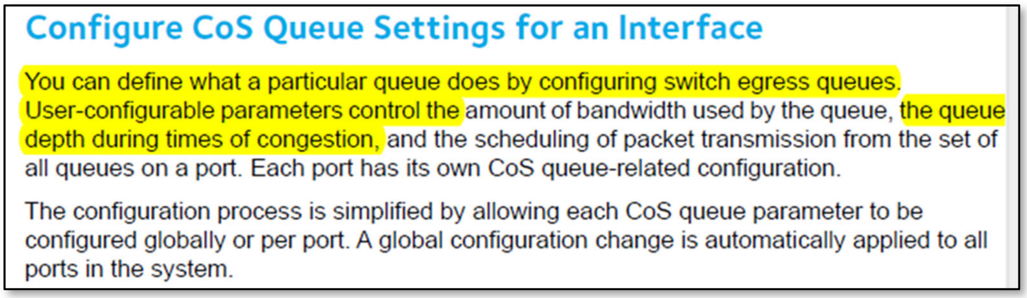
M6100, M5300, and M7100 Series Managed Switches User Manual, Page 511, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf



Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth or transmission rate shaping,are user-configurable at the queue (or port) level.

M6100, M5300, and M7100 Series Managed Switches User Manual, Page 511, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf

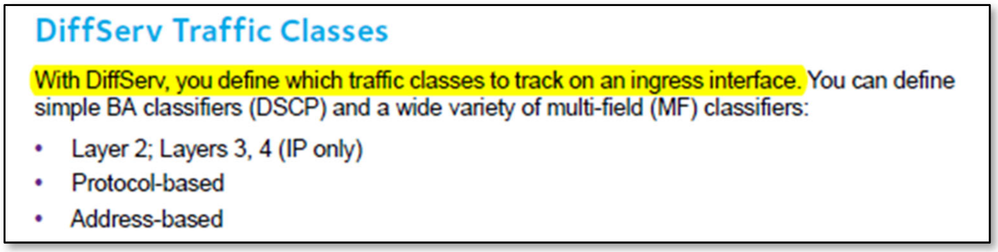


Configure CoS Queue Settings for an Interface

You can define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port. Each port has its own CoS queue-related configuration.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally or per port. A global configuration change is automatically applied to all ports in the system.

M6100, M5300, and M7100 Series Managed Switches User Manual, Page 517, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf

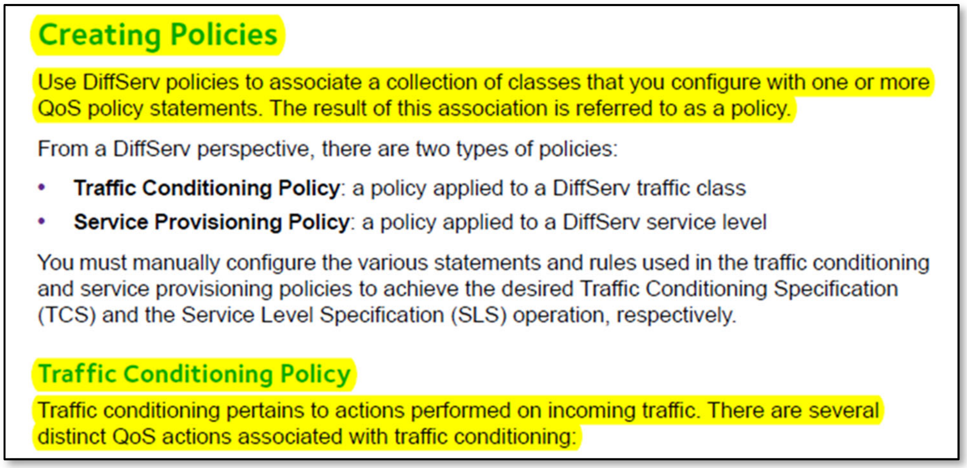


DiffServ Traffic Classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multi-field (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

M6100, M5300, and M7100 Series Managed Switches User Manual, Page 750, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf



Creating Policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, there are two types of policies:

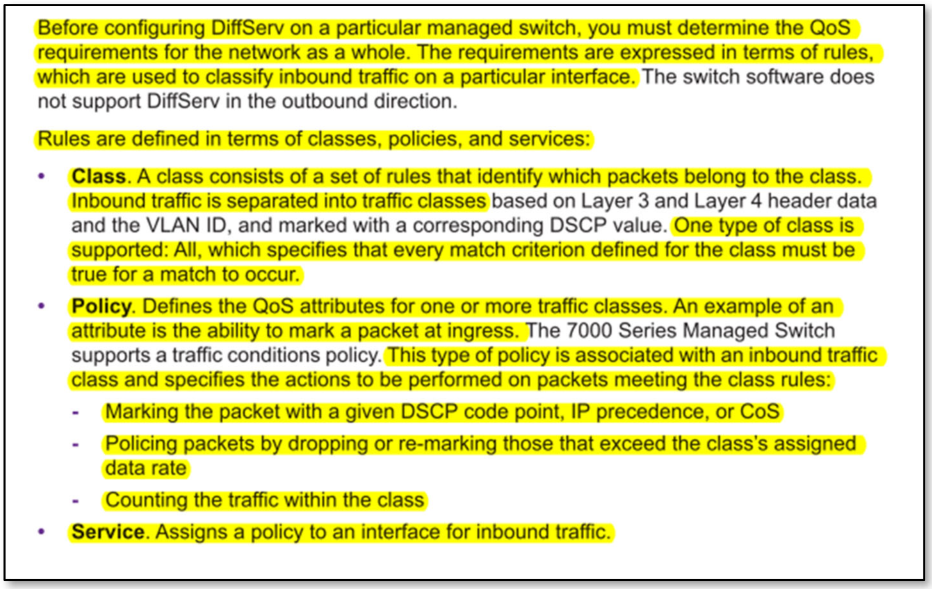
- **Traffic Conditioning Policy**: a policy applied to a DiffServ traffic class
- **Service Provisioning Policy**: a policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

Traffic Conditioning Policy

Traffic conditioning pertains to actions performed on incoming traffic. There are several distinct QoS actions associated with traffic conditioning:

M6100, M5300, and M7100 Series Managed Switches User Manual, Page 751, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf

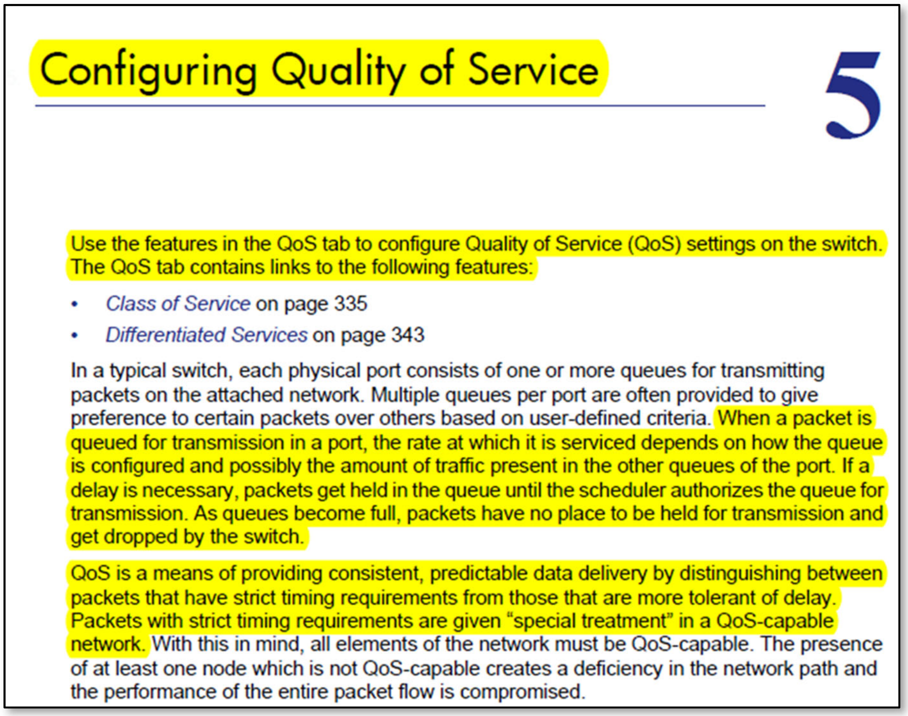


Before configuring DiffServ on a particular managed switch, you must determine the QoS requirements for the network as a whole. The requirements are expressed in terms of rules, which are used to classify inbound traffic on a particular interface. The switch software does not support DiffServ in the outbound direction.

Rules are defined in terms of classes, policies, and services:

- **Class**. A class consists of a set of rules that identify which packets belong to the class. Inbound traffic is separated into traffic classes based on Layer 3 and Layer 4 header data and the VLAN ID, and marked with a corresponding DSCP value. One type of class is supported: All, which specifies that every match criterion defined for the class must be true for a match to occur.
- **Policy**. Defines the QoS attributes for one or more traffic classes. An example of an attribute is the ability to mark a packet at ingress. The 7000 Series Managed Switch supports a traffic conditions policy. This type of policy is associated with an inbound traffic class and specifies the actions to be performed on packets meeting the class rules:
  - Marking the packet with a given DSCP code point, IP precedence, or CoS
  - Policing packets by dropping or re-marking those that exceed the class's assigned data rate
  - Counting the traffic within the class
- **Service**. Assigns a policy to an interface for inbound traffic.

M5300, M6100, and M7100 Series Prosafe Managed Switches Software Administration Manual, Page 280, https://www.downloads.netgear.com/files/GDC/M5300/M5300-M6100-M7100_SWA_v11_30Oct2015.pdf



Configuring Quality of Service

5

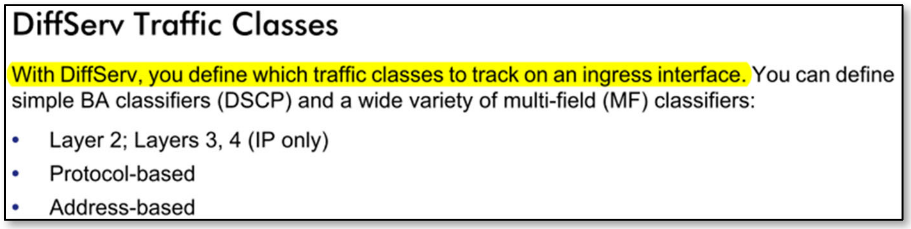
Use the features in the QoS tab to configure Quality of Service (QoS) settings on the switch. The QoS tab contains links to the following features:

- *Class of Service* on page 335
- *Differentiated Services* on page 343

In a typical switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets have no place to be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given "special treatment" in a QoS-capable network. With this in mind, all elements of the network must be QoS-capable. The presence of at least one node which is not QoS-capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

ProSafe XSM7224S 10G Managed Stackable Switch Software Administration Manual, Page 336, https://www.downloads.netgear.com/files/XSM7224S_UM_14June11.pdf

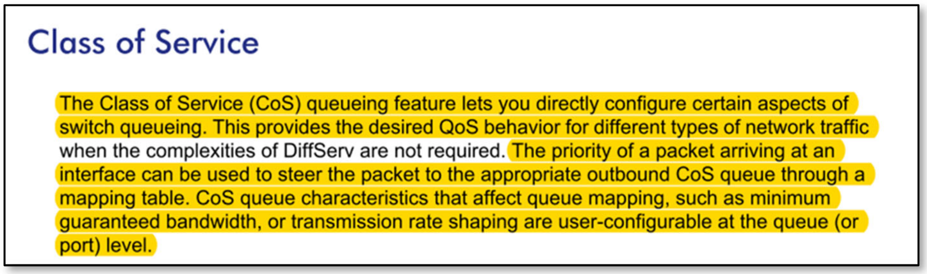


DiffServ Traffic Classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multi-field (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

ProSafe XSM7224S 10G Managed Stackable Switch Software Administration Manual, Page 517, https://www.downloads.netgear.com/files/XSM7224S_UM_14June11.pdf

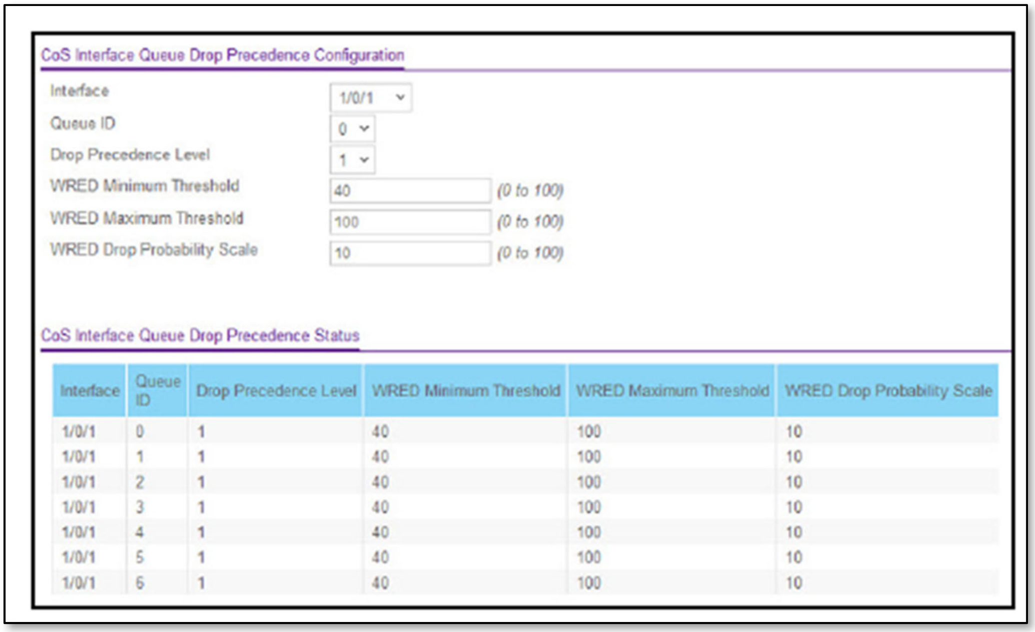


Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, or transmission rate shaping are user-configurable at the queue (or port) level.

ProSafe XSM7224S 10G Managed Stackable Switch Software Administration Manual, Page 337, https://www.downloads.netgear.com/files/XSM7224S_UM_14June11.pdf

20. Defendant instructs and encourages users to configure infringing WRED functionality in the following manner:

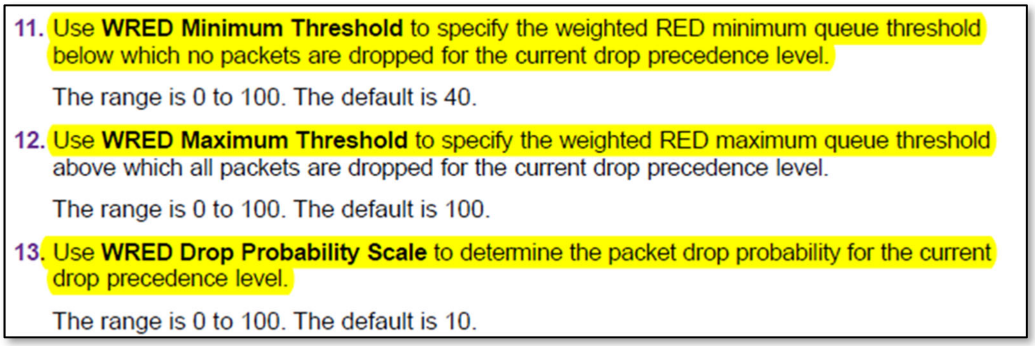


CoS Interface Queue Drop Precedence Configuration

Interface	1/0/1	
Queue ID	0	
Drop Precedence Level	1	
WRED Minimum Threshold	40	(0 to 100)
WRED Maximum Threshold	100	(0 to 100)
WRED Drop Probability Scale	10	(0 to 100)

CoS Interface Queue Drop Precedence Status

Interface	Queue ID	Drop Precedence Level	WRED Minimum Threshold	WRED Maximum Threshold	WRED Drop Probability Scale
1/0/1	0	1	40	100	10
1/0/1	1	1	40	100	10
1/0/1	2	1	40	100	10
1/0/1	3	1	40	100	10
1/0/1	4	1	40	100	10
1/0/1	5	1	40	100	10
1/0/1	6	1	40	100	10



11. Use **WRED Minimum Threshold** to specify the weighted RED minimum queue threshold below which no packets are dropped for the current drop precedence level.

    The range is 0 to 100. The default is 40.

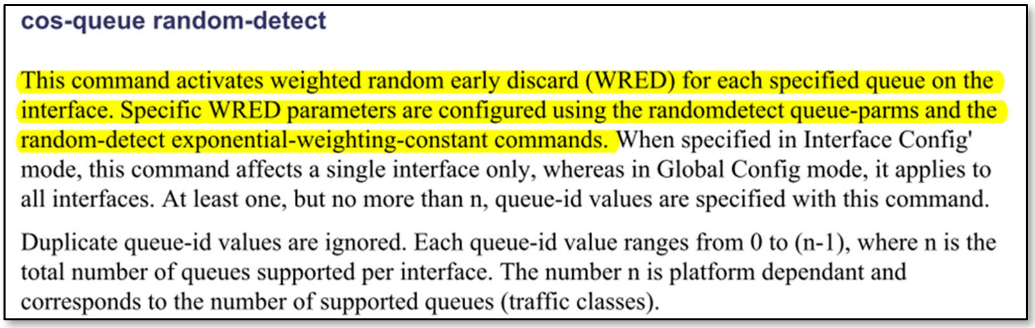
12. Use **WRED Maximum Threshold** to specify the weighted RED maximum queue threshold above which all packets are dropped for the current drop precedence level.

    The range is 0 to 100. The default is 100.

13. Use **WRED Drop Probability Scale** to determine the packet drop probability for the current drop precedence level.

    The range is 0 to 100. The default is 10.

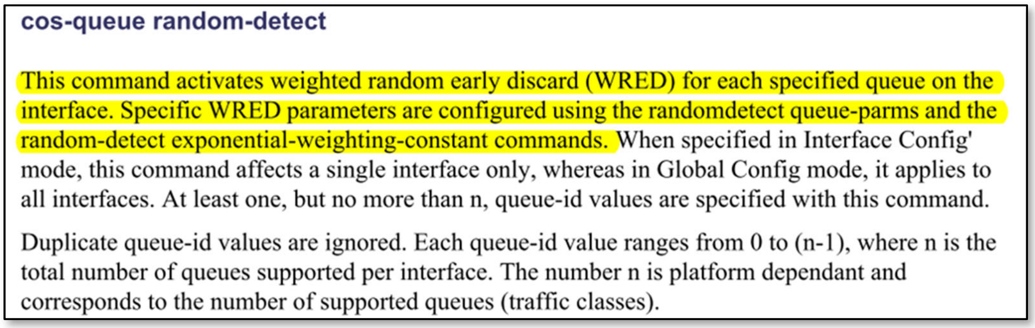
M6100, M5300, and M7100 Series Managed Switches User Manual, Page 519, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf



cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the randomdetect queue-parms and the random-detect exponential-weighting-constant commands. When specified in Interface Config' mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. At least one, but no more than n, queue-id values are specified with this command.

Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (n-1), where n is the total number of queues supported per interface. The number n is platform dependant and corresponds to the number of supported queues (traffic classes).



cos-queue random-detect

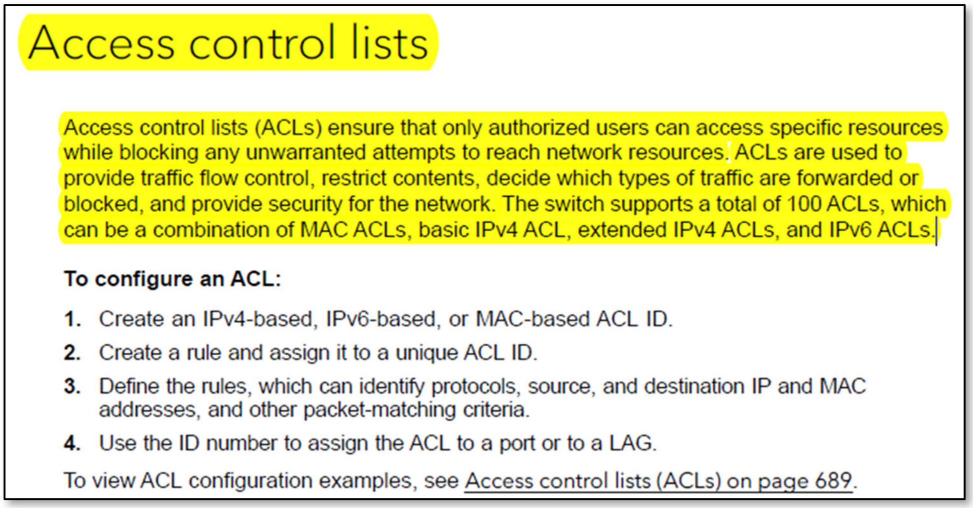
This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the randomdetect queue-parms and the random-detect exponential-weighting-constant commands. When specified in Interface Config' mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. At least one, but no more than n, queue-id values are specified with this command.

Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (n-1), where n is the total number of queues supported per interface. The number n is platform dependant and corresponds to the number of supported queues (traffic classes).

ProSafe XSM7224S Managed Stackable Switch CLI Manual, Page 279, https://www.downloads.netgear.com/files/CLI7200_9-0_15Nov10.pdf

21. Defendant provides instructions on how to make and use the patented inventions of both the ’394 Patent and the ’352 Patent by configuring access control lists (ACL’s) on ingress and egress traffic in its accused switches and routers in accordance with its instructions and specifications.

22. Defendant describes configuring pass/drop rules for ACL’s using packet header information with or without an egress port identity:



Access control lists

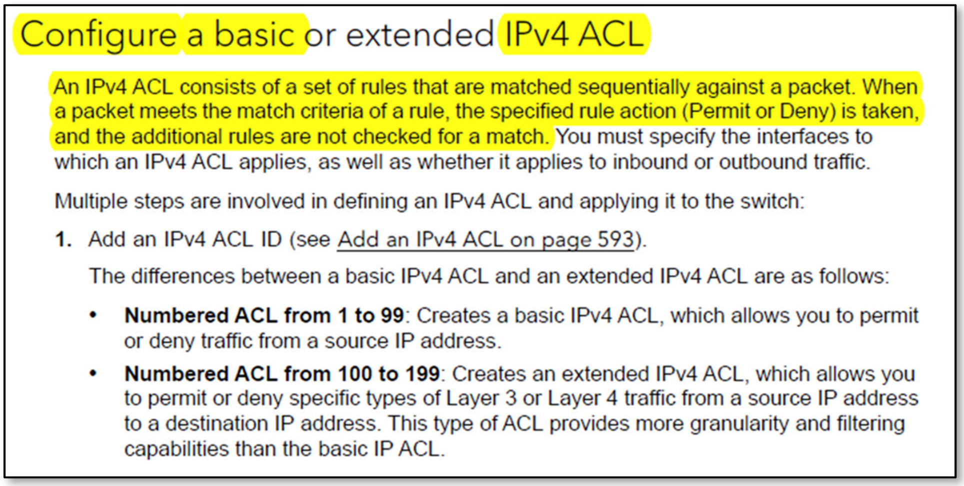
Access control lists (ACLs) ensure that only authorized users can access specific resources while blocking any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents, decide which types of traffic are forwarded or blocked, and provide security for the network. The switch supports a total of 100 ACLs, which can be a combination of MAC ACLs, basic IPv4 ACL, extended IPv4 ACLs, and IPv6 ACLs.

To configure an ACL:

1. Create an IPv4-based, IPv6-based, or MAC-based ACL ID.
2. Create a rule and assign it to a unique ACL ID.
3. Define the rules, which can identify protocols, source, and destination IP and MAC addresses, and other packet-matching criteria.
4. Use the ID number to assign the ACL to a port or to a LAG.

To view ACL configuration examples, see Access control lists (ACLs) on page 689.

M4250 Managed Switches – User Manual, Page 578, https://www.downloads.netgear.com/files/GDC/M4250/M4250_UM_EN.pdf



Configure a basic or extended IPv4 ACL

An IPv4 ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit or Deny) is taken, and the additional rules are not checked for a match. You must specify the interfaces to which an IPv4 ACL applies, as well as whether it applies to inbound or outbound traffic.

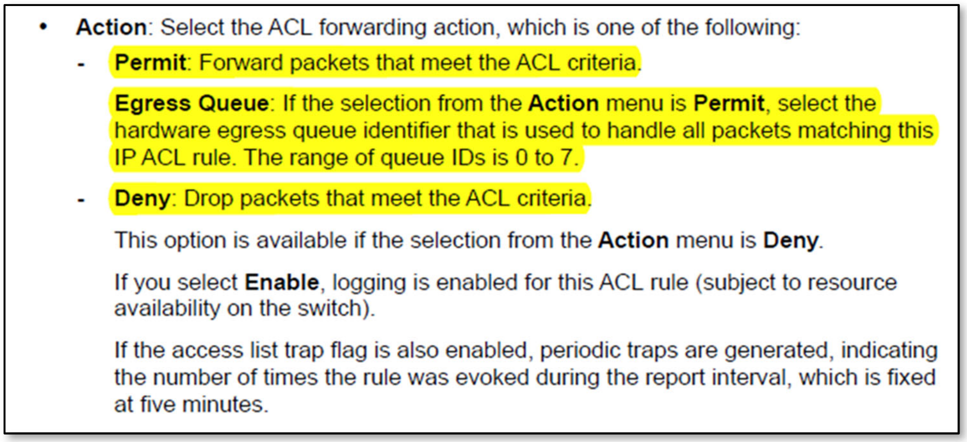
Multiple steps are involved in defining an IPv4 ACL and applying it to the switch:

1. Add an IPv4 ACL ID (see Add an IPv4 ACL on page 593).

   The differences between a basic IPv4 ACL and an extended IPv4 ACL are as follows:

   - **Numbered ACL from 1 to 99**: Creates a basic IPv4 ACL, which allows you to permit or deny traffic from a source IP address.
   - **Numbered ACL from 100 to 199**: Creates an extended IPv4 ACL, which allows you to permit or deny specific types of Layer 3 or Layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the basic IP ACL.

M4250 Managed Switches – User Manual, Page 592, https://www.downloads.netgear.com/files/GDC/M4250/M4250_UM_EN.pdf



- **Action**: Select the ACL forwarding action, which is one of the following:
  - **Permit**: Forward packets that meet the ACL criteria.

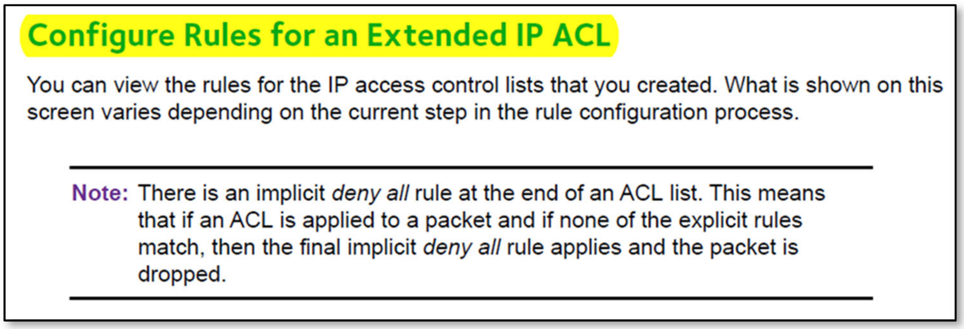
    Egress Queue: If the selection from the **Action** menu is **Permit**, select the hardware egress queue identifier that is used to handle all packets matching this IP ACL rule. The range of queue IDs is 0 to 7.
  - **Deny**: Drop packets that meet the ACL criteria.

    This option is available if the selection from the **Action** menu is **Deny**.

    If you select **Enable**, logging is enabled for this ACL rule (subject to resource availability on the switch).

    If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times the rule was evoked during the report interval, which is fixed at five minutes.

M4250 Managed Switches – User Manual, Page 600, https://www.downloads.netgear.com/files/GDC/M4250/M4250_UM_EN.pdf

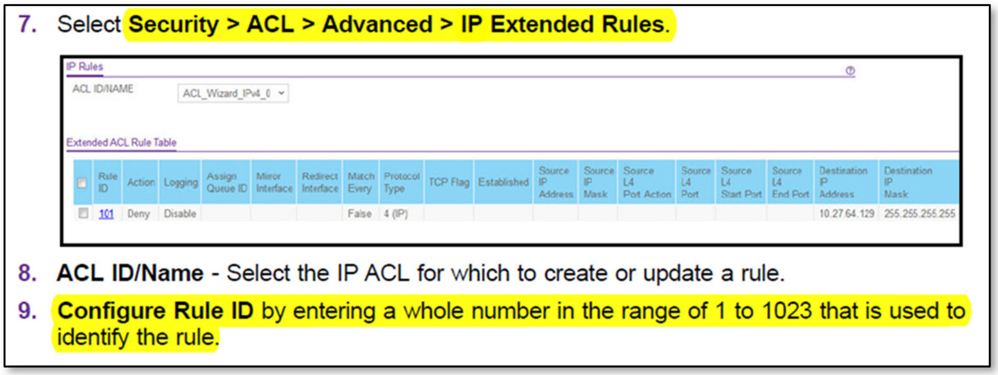


Configure Rules for an Extended IP ACL

You can view the rules for the IP access control lists that you created. What is shown on this screen varies depending on the current step in the rule configuration process.

Note: There is an implicit *deny all* rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit *deny all* rule applies and the packet is dropped.

M5300-28G Managed Switch – User Manual, Page 660, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf



7. Select **Security > ACL > Advanced > IP Extended Rules.**

IP Rules

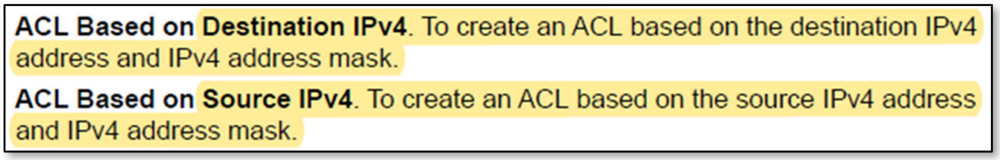
ACL ID/NAME: ACL_Wizard_IPv4_0

Extended ACL Rule Table

□	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Type	TCP Flag	Established	Source IP Address	Source IP Mask	Source L4 Port Action	Source L4 Port	Source L4 Start Port	Source L4 End Port	Destination IP Address	Destination IP Mask
□	101	Deny	Disable				False	4 (IP)									10.27.64.129	255.255.255.255

8. **ACL ID/Name** - Select the IP ACL for which to create or update a rule.
9. **Configure Rule ID** by entering a whole number in the range of 1 to 1023 that is used to identify the rule.

M5300-28G Managed Switch – User Manual, Page 661, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf



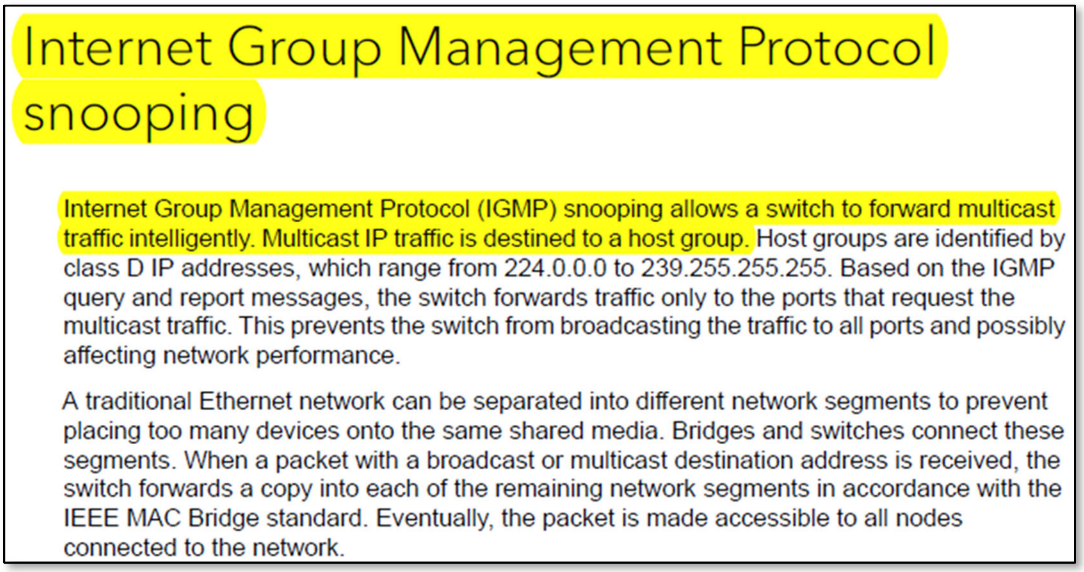
ACL Based on Destination IPv4. To create an ACL based on the destination IPv4 address and IPv4 address mask.

ACL Based on Source IPv4. To create an ACL based on the source IPv4 address and IPv4 address mask.

Netgear M7100 Gigabit managed Switch user manual, Page 647, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf

23. Defendant instructs and encourages customers to make and use the patented inventions of the ’844 Patent by operating the “multicast filtering” software components of its products in accordance with its instructions and specifications. Defendant specifically intends its customers to infringe by implementing “multicast filtering” software modules in its switches that implement multicast protocols, such as Protocol Independent Multicasting (PIM) and Internet Group Management Protocol (IGMP), with a multicast-capable component coupled to the egress and ingress paths of the port in the manner claimed.

24. Defendant instructs and encourages users to configure the Internet Group Management Protocol. For example:

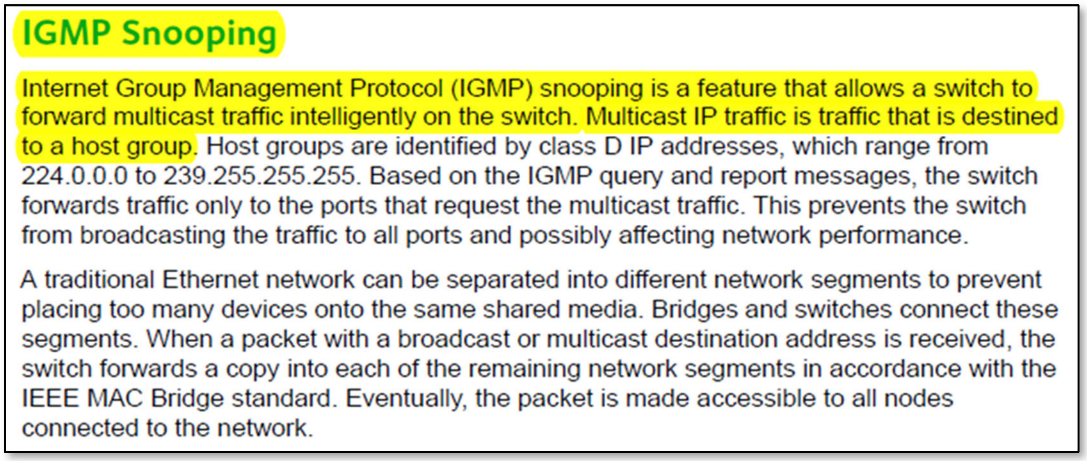


Internet Group Management Protocol snooping

Internet Group Management Protocol (IGMP) snooping allows a switch to forward multicast traffic intelligently. Multicast IP traffic is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

A traditional Ethernet network can be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch forwards a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

M4250 Managed Switches – User Manual, Page 224, https://www.downloads.netgear.com/files/GDC/M4250/M4250_UM_EN.pdf



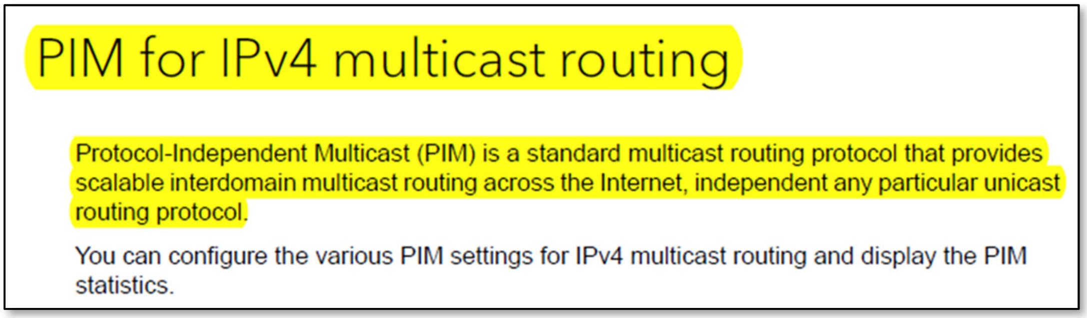
IGMP Snooping

Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

A traditional Ethernet network can be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch forwards a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

M5300 ProSAFE Next-Gen Edge Managed Switches – User Manual, Page 253, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf

25. Defendant instructs and encourages users to configure the Protocol Independent Multicast in the following manner:

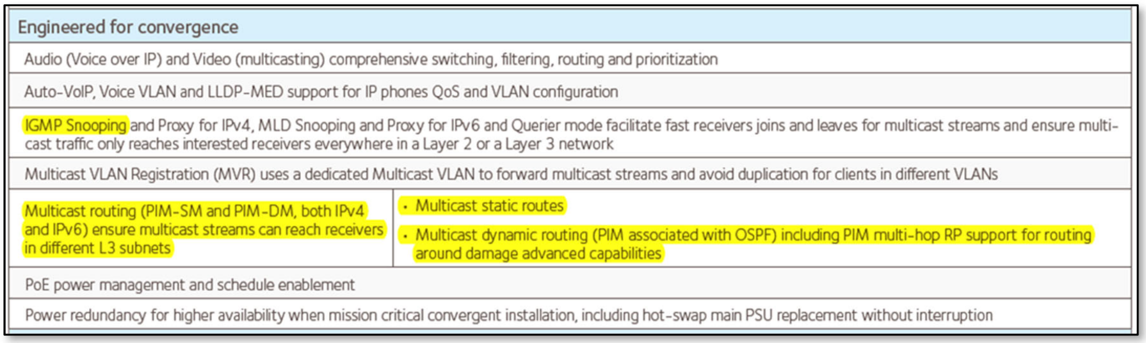


PIM for IPv4 multicast routing

Protocol-Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable interdomain multicast routing across the Internet, independent any particular unicast routing protocol.

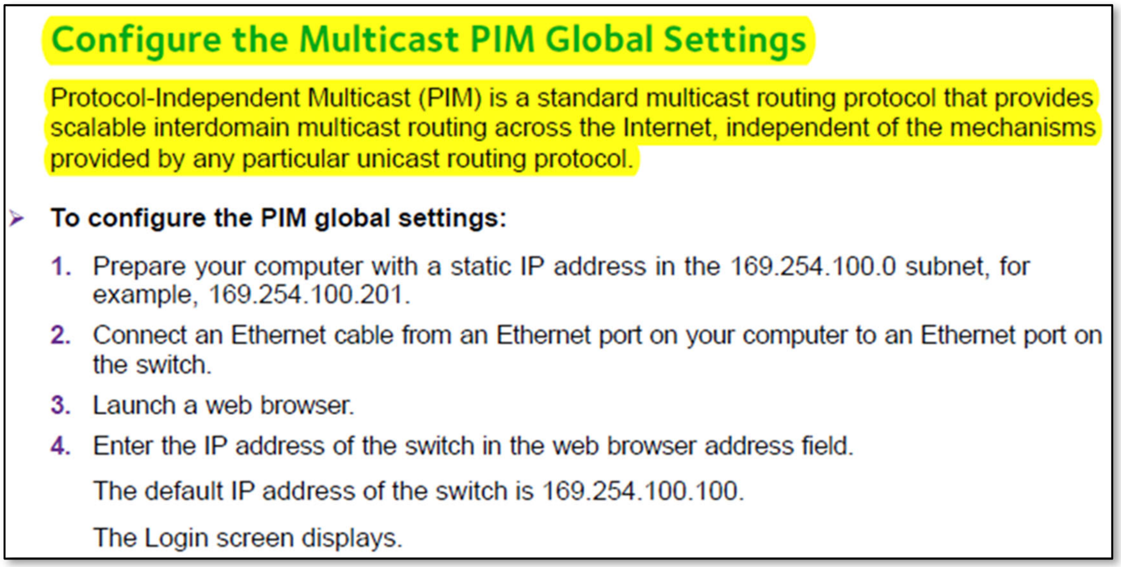
You can configure the various PIM settings for IPv4 multicast routing and display the PIM statistics.

M4250 Managed Switches – User Manual, Page 365, https://www.downloads.netgear.com/files/GDC/M4250/M4250_UM_EN.pdf



Engineered for convergence	
Audio (Voice over IP) and Video (multicasting) comprehensive switching, filtering, routing and prioritization	
Auto-VoIP, Voice VLAN and LLDP-MED support for IP phones QoS and VLAN configuration	
IGMP Snooping and Proxy for IPv4, MLD Snooping and Proxy for IPv6 and Querier mode facilitate fast receivers joins and leaves for multicast streams and ensure multicast traffic only reaches interested receivers everywhere in a Layer 2 or a Layer 3 network	
Multicast VLAN Registration (MVR) uses a dedicated Multicast VLAN to forward multicast streams and avoid duplication for clients in different VLANs	
Multicast routing (PIM-SM and PIM-DM, both IPv4 and IPv6) ensure multicast streams can reach receivers in different L3 subnets	• Multicast static routes • Multicast dynamic routing (PIM associated with OSPF) including PIM multi-hop RP support for routing around damage advanced capabilities
PoE power management and schedule enablement	
Power redundancy for higher availability when mission critical convergent installation, including hot-swap main PSU replacement without interruption	

M5300-28GF3 ProSAFE Next-Gen Edge Managed Switch Datasheet, Page 8, https://www.downloads.netgear.com/files/GDC/datasheet/en/M5300.pdf?_ga=2.74108242.1545122513.1635399696-477895179.1635143394



Configure the Multicast PIM Global Settings

Protocol-Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable interdomain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol.

➤ **To configure the PIM global settings:**

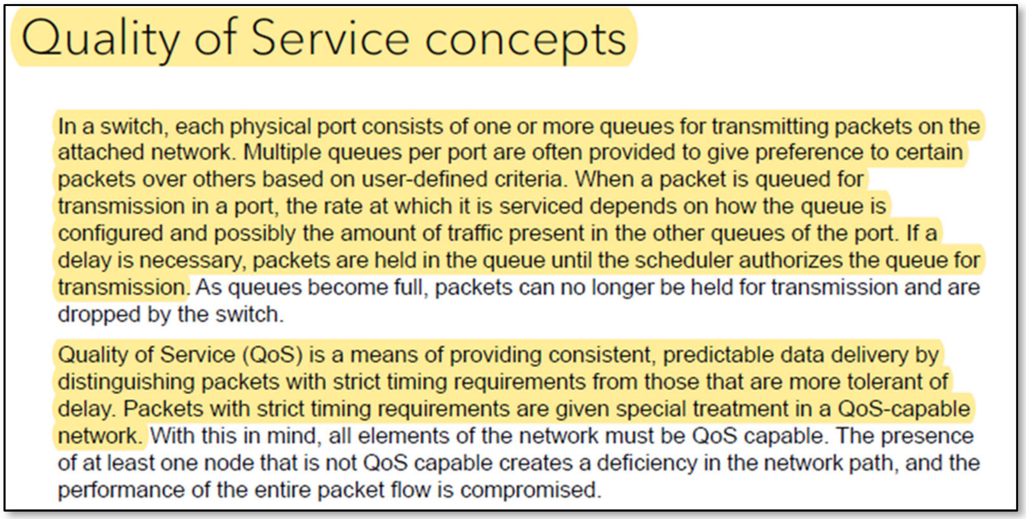
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

   The default IP address of the switch is 169.254.100.100.

   The Login screen displays.

M7100-24X ProSAFE Next-Gen Edge Managed Switch – User Manual, Page 476, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf

26. Defendant provides instructions on how to make and use the patented inventions of the ’046 Patent by configuring QoS, CoS, and 802.1p Priority software components in its accused switches and routers in accordance with its instructions and specifications. For example, Defendant instructs as follows:

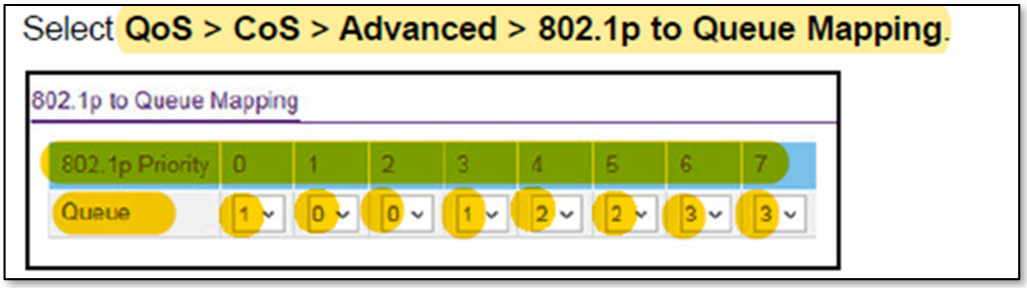


Quality of Service concepts

In a switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets are held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets can no longer be held for transmission and are dropped by the switch.

Quality of Service (QoS) is a means of providing consistent, predictable data delivery by distinguishing packets with strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS capable. The presence of at least one node that is not QoS capable creates a deficiency in the network path, and the performance of the entire packet flow is compromised.

Netgear GS108Tv3/GS110TPv3/GS110TPP user manual, Page 260, https://www.downloads.netgear.com/files/GDC/GS108Tv3/GS108Tv3_GS110TPv3_GS110TPP_UM_EN.pdf

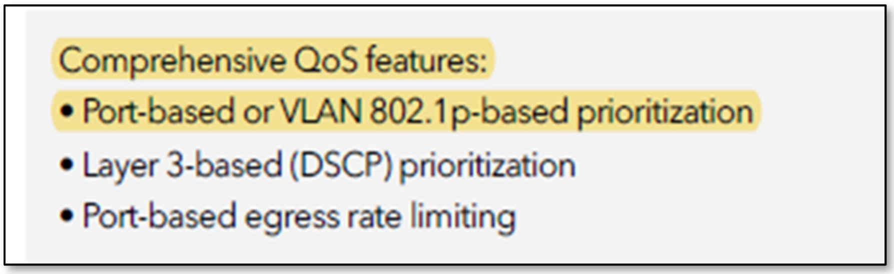


Select **QoS > CoS > Advanced > 802.1p to Queue Mapping**.

802.1p to Queue Mapping

802.1p Priority	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

Netgear GS108Tv3/GS110TPv3/GS110TPP user manual, Page 266, https://www.downloads.netgear.com/files/GDC/GS108Tv3/GS108Tv3_GS110TPv3_GS110TPP_UM_EN.pdf

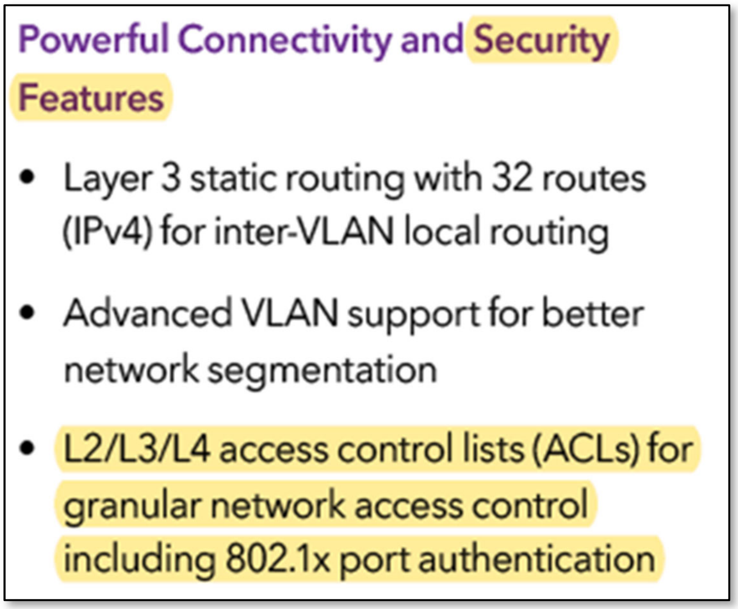


Comprehensive QoS features:

- Port-based or VLAN 802.1p-based prioritization
- Layer 3-based (DSCP) prioritization
- Port-based egress rate limiting

Netgear GS108Tv3 datasheet, Page 4, https://www.netgear.com/images/datasheet/switches/GS108Tv3_GS110TPv3_DS.pdf

27. Defendant describes using configuring its switches and routers as access controllers providing 802.1 port authentication:

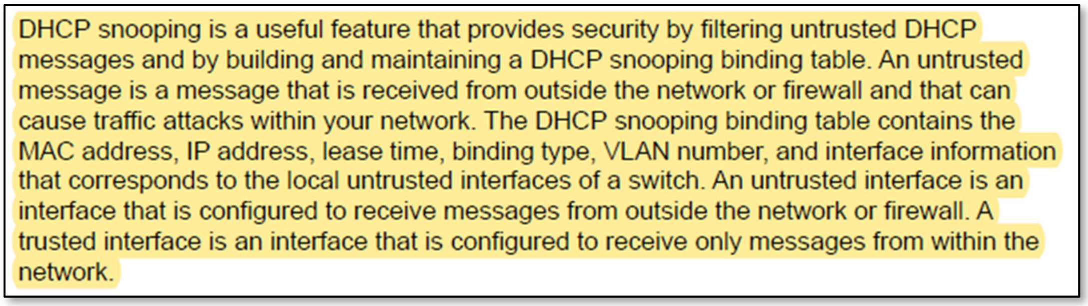


Powerful Connectivity and Security Features

- Layer 3 static routing with 32 routes (IPv4) for inter-VLAN local routing
- Advanced VLAN support for better network segmentation
- L2/L3/L4 access control lists (ACLs) for granular network access control including 802.1x port authentication

Netgear GS108Tv3 datasheet, Page 1,
https://www.netgear.com/images/datasheet/switches/GS108Tv3_GS110TPv3_DS.pdf

28. Defendant describes using DHCP snooping to categorize network traffic based on trustworthiness of the source:



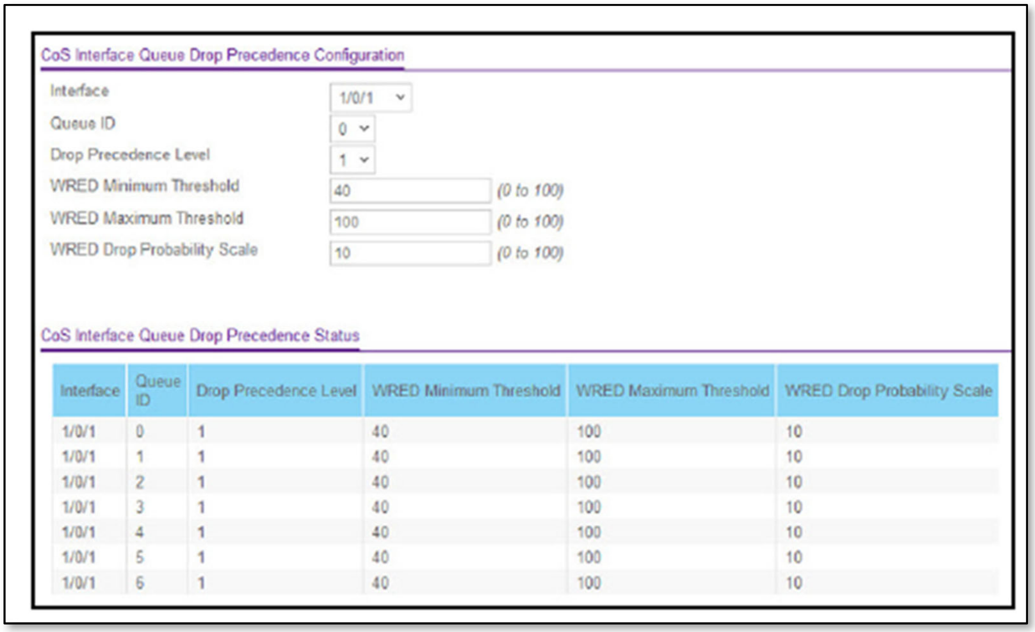
DHCP snooping is a useful feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

Netgear GS108Tv3/GS110TPv3/GS110TPP user manual, Page 266,
https://www.downloads.netgear.com/files/GDC/GS108Tv3/GS108Tv3_GS110TPv3_GS110TPP_UM_EN.pdf

29. Defendant provides instructions on how to make and use the patented inventions of the ’963 Patent by operating the “queuing” software components of its switches and routers that

implement a WRED algorithm on packet queues to drop packets as a function of queue size (or buffer) in order to manage congestion in the switch in accordance with its instructions and specifications.

30. Defendant describes the configuration and use of WRED queuing. For example:



CoS Interface Queue Drop Precedence Configuration

Interface 1/0/1

Queue ID 0

Drop Precedence Level 1

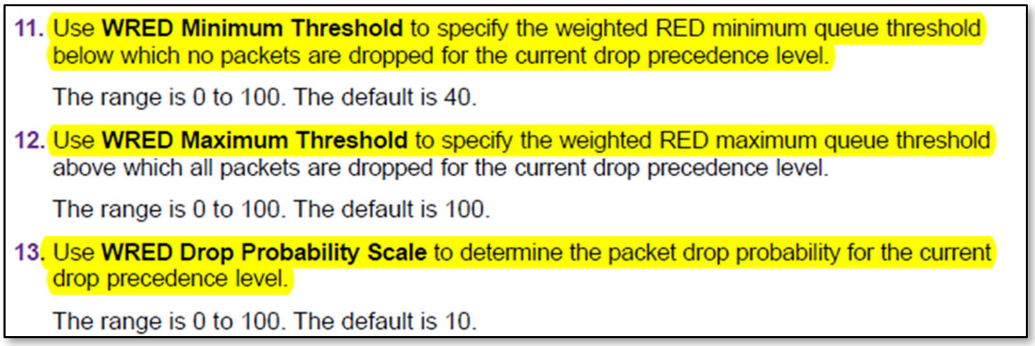
WRED Minimum Threshold 40 (0 to 100)

WRED Maximum Threshold 100 (0 to 100)

WRED Drop Probability Scale 10 (0 to 100)

CoS Interface Queue Drop Precedence Status

Interface	Queue ID	Drop Precedence Level	WRED Minimum Threshold	WRED Maximum Threshold	WRED Drop Probability Scale
1/0/1	0	1	40	100	10
1/0/1	1	1	40	100	10
1/0/1	2	1	40	100	10
1/0/1	3	1	40	100	10
1/0/1	4	1	40	100	10
1/0/1	5	1	40	100	10
1/0/1	6	1	40	100	10



11. Use **WRED Minimum Threshold** to specify the weighted RED minimum queue threshold below which no packets are dropped for the current drop precedence level.

    The range is 0 to 100. The default is 40.

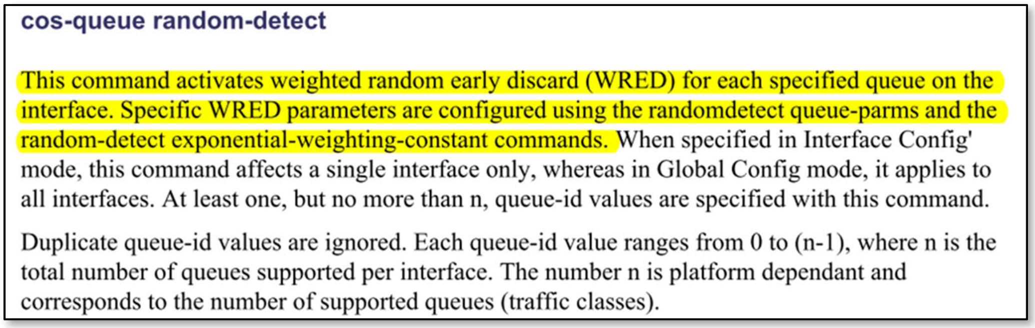
12. Use **WRED Maximum Threshold** to specify the weighted RED maximum queue threshold above which all packets are dropped for the current drop precedence level.

    The range is 0 to 100. The default is 100.

13. Use **WRED Drop Probability Scale** to determine the packet drop probability for the current drop precedence level.

    The range is 0 to 100. The default is 10.

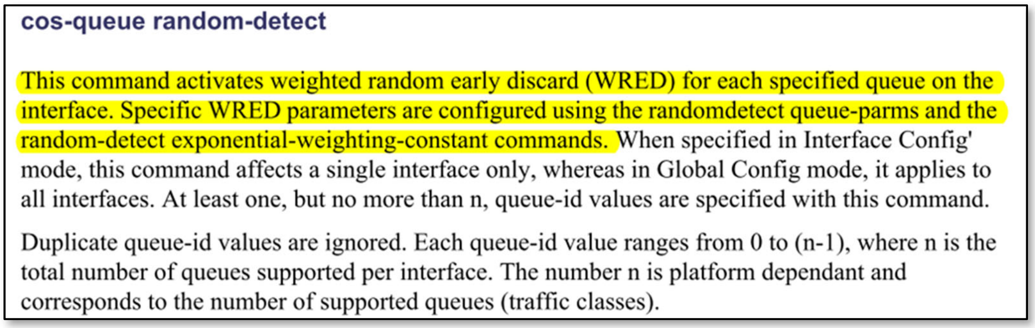
M6100, M5300, and M7100 Series Managed Switches User Manual, Page 519, https://www.downloads.netgear.com/files/GDC/M5300/M6100_M5300_M7100_UM_10apr15.pdf



cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the randomdetect queue-parms and the random-detect exponential-weighting-constant commands. When specified in Interface Config' mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. At least one, but no more than n, queue-id values are specified with this command.

Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (n-1), where n is the total number of queues supported per interface. The number n is platform dependant and corresponds to the number of supported queues (traffic classes).



cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the randomdetect queue-parms and the random-detect exponential-weighting-constant commands. When specified in Interface Config' mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. At least one, but no more than n, queue-id values are specified with this command.

Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (n-1), where n is the total number of queues supported per interface. The number n is platform dependant and corresponds to the number of supported queues (traffic classes).

ProSafe XSM7224S Managed Stackable Switch CLI Manual, Page 279, https://www.downloads.netgear.com/files/CLI7200_9-0_15Nov10.pdf

31. On information and belief, Defendant's customers deploy the accused products on networks in combination with other products. The specific code portions and modules directed to the infringing functionality will be identified as those systems are made available for inspection and review by Parity Networks.

32. On information of belief, Defendant also implements contractual protections in the form of license and use restrictions with its customers to preclude the unauthorized reproduction, distribution and modification of its software.

33. Moreover, on information and belief, Defendant implements technical precautions to attempt to thwart customers who would circumvent the intended operation of Defendant's products.

NOTICE

34. Defendant had actual and/or constructive knowledge of the Patents-in-Suit and the infringing conduct as early as October 5, 2016 and November 28, 2016, when Defendant was sent notice letters by Parity. *See* Exhibits 7 and 8. In addition, NETGEAR has been provided with formal legal notice on the date when Parity Networks effected service of the Original Complaint.

V. COUNTS OF PATENT INFRINGEMENT

COUNT ONE
INFRINGEMENT OF U.S. PATENT NO. 6,252,848

35. Parity Networks incorporates by reference its allegations in the preceding paragraphs as if fully restated in this paragraph.

36. Parity Networks is the assignee and owner of all right, title, and interest to the ’848 Patent. Parity Networks has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

37. On information and belief, at least since the release of the ’848 Exemplary Infringing Products and until the expiration of the ’848 Patent, without authorization or license from Parity Networks, Defendant was directly infringing each and every element of at least claim 1 of the ’848 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, and offering for sale methods and articles infringing one or more claims of the ’848 Patent. Defendant is thus liable for direct infringement of the ’848 Patent pursuant to 35 U.S.C. § 271(a).

38. Exemplary infringing products include Defendant’s 5300 Series Switch, M7100 Series Switch, ProSafe XSM7224S 10G Managed Stackable Switch, all substantially similar switches, all associated computer hardware, software and digital content, and all products operating in a substantially similar manner (“’848 Exemplary Infringing Products”). The ’848

Exemplary Infringing Products include multiple ingress ports with output queues and wherein the ingress ports are configured to receive packets from multiple ingress flows and monitor their characteristics. Each packet is marked with a marking based on criteria including the ingress flow rate and the flow profile.

39. As a result of Defendant's infringement of the '848 Patent, Parity Networks has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement under 35 U.S.C. § 284, but in no event, less than a reasonable royalty.

COUNT TWO
INFRINGEMENT OF U.S. PATENT NO. 6,763,394

40. Parity Networks incorporates by reference its allegations in the preceding paragraphs as if fully restated in this paragraph.

41. Parity Networks is the assignee and owner of all right, title, and interest to the '394 Patent. Parity Networks has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

42. On information and belief, at least since the release of the '394 Exemplary Infringing Products and until the expiration of the '394 Patent, without authorization or license from Parity Networks, Defendant was directly infringing each and every element of at least claim 1 of the '394 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, and offering for sale methods and articles infringing one or more claims of the '394 Patent. Defendant is thus liable for direct infringement of the '394 Patent pursuant to 35 U.S.C. § 271(a).

43. Exemplary infringing products include Defendant's M4250-10G2F-PoE+ Managed Switch, M5300-28G Managed Switch, M7100-24X Gigabit Managed Switch, all substantially similar switches, all associated computer hardware, software and digital content, and

all products operating in a substantially similar manner ("'394 Exemplary Infringing Products"). The '394 Exemplary Infringing Products use access control lists to perform filtering and dropping of packets at the ingress port for egress pass/drop determination, as set forth above and in the excerpts from Defendant's technical manuals.

44. On information and belief, at least since the release of the '394 Exemplary Infringing Products and until the expiration of the '394 Patent, without authorization or license from Parity Networks, Defendant was indirectly infringing each and every element of at least claim 1 of the '394 Patent, either literally or equivalently, including actively and knowingly inducing infringement of the '394 Patent under 35 U.S.C. § 271(b). Such inducements include without limitation, with specific intent to encourage the infringement, knowingly inducing consumers to use infringing articles and methods that Defendant knows or should know infringe one or more claims of the '394 Patent. Defendant instructs and encourages customers to make and use the patented inventions of the '394 Patent by operating Defendant's products in accordance with Defendant's instructions and specifications. Defendant specifically intends its customers to infringe by implementing access control lists for filtering and dropping of packets implemented at the ingress port for egress pass/drop determination, as set forth above and in the excerpts from Defendant's technical manuals.

45. On information and belief, at least since the release of the '394 Exemplary Infringing Products and until the expiration of the '394 Patent, without authorization or license from Parity Networks, Defendant was indirectly infringing each and every element of at least claim 1 of the '394 Patent, including contributory infringement of the '394 Patent under 35 U.S.C. § 271(c) and/or § 271(f), either literally and/or under the doctrine of equivalents. Defendant's contributory infringement includes without limitation, Defendant's offer to sell, a component of a

product or apparatus for use in a process, that (i) is material to practicing the invention claimed by claim 1 of the ’394 Patent, (ii) is not a staple article or commodity of commerce suitable for substantial non-infringing use, and (iii) Defendant is aware or knows to be especially made or especially adapted for use in infringement of the ’394 Patent. Defendant specifically intends its customers to infringe by implementing access control lists for filtering and dropping of packets implemented at the ingress port for egress pass/drop determination, as set forth above and in the excerpts from Defendant’s technical manuals.

46. On information and belief, Defendant’s customers deploy the accused products on networks in combination with other products. The specific code portions and modules directed to the infringing functionality will be identified as those systems are made available for inspection and review by Parity Networks.

47. As a result of Defendant’s infringement of the ’394 Patent, Parity Networks has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement under 35 U.S.C. § 284, but in no event, less than a reasonable royalty.

COUNT THREE
INFRINGEMENT OF U.S. PATENT NO. 6,870,844

48. Parity Networks incorporates by reference its allegations in the preceding paragraphs as if fully restated in this paragraph.

49. Parity Networks is the assignee and owner of all right, title, and interest to the ’844 Patent. Parity Networks has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

50. On information and belief, at least since the release of the ’844 Exemplary Infringing Products and until the expiration of the ’844 Patent, without authorization or license from Parity Networks, Defendant was directly infringing each and every element of at least claim

1 of the ’844 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, and offering for sale methods and articles infringing one or more claims of the ’844 Patent. Defendant is thus liable for direct infringement of the ’844 Patent pursuant to 35 U.S.C. § 271(a).

51. Exemplary infringing products include Defendant’s M4250-10G2F-PoE+ Managed Switch, M5300-28G Managed Switch, M7100-24X Gigabit Managed Switch, all substantially similar switches, all associated computer hardware, software and digital content, and all products operating in a substantially similar manner (“’844 Exemplary Infringing Products”). These products implement multicast protocols such as Protocol Independent Multicasting (PIM) and Internet Group Management Protocol (IGMP) in the manner claimed.

52. On information and belief, at least since the release of the ’844 Exemplary Infringing Products and until the expiration of the ’844 Patent, without authorization or license from Parity Networks, Defendant was indirectly infringing each and every element of at least claim 1 of the ’844 Patent, either literally or equivalently, including actively and knowingly inducing infringement of the ’844 Patent under 35 U.S.C. § 271(b). Such inducements include without limitation, with specific intent to encourage the infringement, knowingly inducing consumers to use infringing articles and methods that Defendant knows or should know infringe one or more claims of the ’844 Patent. Defendant instructs and encourages customers to make and use the patented inventions of the ’844 Patent by operating Defendant’s products in accordance with Defendant’s instructions and specifications. Defendant specifically intends its customers to infringe by implementing multicast protocols such as Protocol Independent Multicasting (PIM) and Internet Group Management Protocol (IGMP) in the manner claimed as set forth above and in the excerpts from Defendant’s technical manuals.

53. On information and belief, at least since the release of the ’844 Exemplary Infringing Products and until the expiration of the ’844 Patent, without authorization or license from Parity, Defendant was indirectly infringing each and every element of at least claim 1 of the ’844 Patent, including contributorily infringing the ’844 Patent under 35 U.S.C. § 271(c). Defendant’s contributory infringement includes without limitation, Defendant’s offer to sell, a component of a product or apparatus for use in a process, that (i) is material to practicing the invention claimed by claim 1 of the ’844 Patent, (ii) is not a staple article or commodity of commerce suitable for substantial non-infringing use, and (iii) Defendant is aware or knows to be especially made or especially adapted for use in infringement of the ’844 Patent.

54. On information and belief, Defendant’s customers deploy the accused products on networks in combination with other products. The specific code portions and modules directed to the infringing functionality will be identified as those systems are made available for inspection and review by Parity Networks.

55. As a result of Defendant’s infringement of the ’844 Patent, Parity Networks has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement under 35 U.S.C. § 284, but in no event, less than a reasonable royalty.

COUNT FOUR
INFRINGEMENT OF U.S. PATENT NO. 7,103,046

56. Parity Networks incorporates by reference its allegations in the preceding paragraphs as if fully restated in this paragraph.

57. Parity Networks is the assignee and owner of all right, title, and interest to the ’046 Patent. Parity Networks has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

58. On December 22, 2020, certain claims of the ’046 Patent were ruled indefinite by the U.S. District Court for the Central District of California.[1] *See Parity Networks v. Edgecore USA Corp. et. al.*, Civ. No. SACV 20-699JVS, in the U.S. District Court for the Central District of California at Dkt. No. 51 (the “Edgecore Case”). Subsequently, on January 13, 2021, while the Edgecore Case was still pending, the Court in the Western District of Texas, Waco Division, ruled those same claims as not indefinite. *See Parity Networks, LLC v. D-Link Corp.*, W-20-CV-00093-ADA, in the U.S. District Court for the Western District of the United States, Waco Division at Dkt. No. 41.

59. On information and belief, at least since the release of the ’046 Exemplary Infringing Products and until the expiration of the ’046 Patent, without authorization or license from Parity Networks, Defendant was directly infringing each and every element of at least claim 1 of the ’046 Patent, as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling and offering for sale methods and articles infringing one or more claims of the ’046 Patent. Defendant is thus liable for direct infringement of the ’046 Patent pursuant to 35 U.S.C. § 271(a).

60. Exemplary infringing products include Defendant’s GS108Tv3 Smart Switch, GS110Tv3 Smart Switch, GS110TPP Smart Switch, all substantially similar switches, all associated computer hardware, software and digital content, and all products operating in a substantially similar manner (“’046 Exemplary Infringing Products”). The ’046 Exemplary Infringing Products include one or more packet processors that categorize packets into categories

[1] *See also Parity Networks, LLC v. ZyXEL Communications, Inc.*, Civ. No. SACV 20-697JVS, in the U.S. District Court for the Central District of California; *Parity Networks, LLC v. Moxa Inc. et al.*, Civ. No. SACV 20-698JVS, in the U.S. District Court for the Central District of California.

based on the source of the packet and the packets are placed in a queue and processed by a CPU based on a priority of those categories, as set forth above and in the excerpts from Defendant's technical manuals.

61. As a result of Defendant's infringement of the '046 Patent, Parity Networks has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement under 35 U.S.C. § 284, but in no event, less than a reasonable royalty.

COUNT FIVE
INFRINGEMENT OF U.S. PATENT NO. 7,107,352

62. Parity Networks incorporates by reference its allegations in the preceding paragraphs as if fully restated in this paragraph.

63. Parity Networks is the assignee and owner of all right, title, and interest to the '352 Patent. Parity Networks has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

64. On information and belief, at least since the release of the '352 Exemplary Infringing Products and until the expiration of the '352 Patent, without authorization or license from Parity Networks, Defendant was directly infringing each and every element of at least claim 1 of the '352 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, and offering for sale methods and articles infringing one or more claims of the '352 Patent. Defendant is thus liable for direct infringement of the '352 Patent pursuant to 35 U.S.C. § 271(a).

65. Exemplary infringing products include Defendant's M4250 Line Managed Switch, M5300 Edge Managed Switch, M7100 Gigabit Managed Switch, all substantially similar switches, all associated computer hardware, software and digital content, and all products operating in a substantially similar manner ("'352 Exemplary Infringing Products"). The '352 Exemplary

Infringing Products use access control lists to perform filtering and dropping of packets at the ingress port for egress pass/drop determination, as set forth above and in the excerpts from Defendant's technical manuals.

66. On information and belief, at least since the release of the '352 Exemplary Infringing Products and until the expiration of the '352 Patent, without authorization or license from Parity Networks, Defendant was indirectly infringing each and every element of at least claim 1 of the '352 Patent, either literally or equivalently, including actively and knowingly inducing infringement of the '352 Patent under 35 U.S.C. § 271(b). Such inducements include without limitation, with specific intent to encourage the infringement, knowingly inducing consumers to use infringing articles and methods that Defendant knows or should know infringe one or more claims of the '352 Patent. Defendant instructs and encourages customers to make and use the patented inventions of the '352 Patent by operating Defendant's products in accordance with Defendant's instructions and specifications. Defendant specifically intends its customers to infringe by implementing access control lists for filtering and dropping of packets implemented at the ingress port for egress pass/drop determination, as set forth above and in the excerpts from Defendant's technical manuals.

67. On information and belief, at least since the release of the '352 Exemplary Infringing Products and until the expiration of the '352 Patent, without authorization or license from Parity Networks, Defendant was indirectly infringing each and every element of at least claim 1 of the '352 Patent, including contributory infringement of the '352 Patent under 35 U.S.C. § 271(c) and/or § 271(f), either literally and/or under the doctrine of equivalents. Defendant's contributory infringement includes without limitation, Defendant's offer to sell, a component of a product or apparatus for use in a process, that (i) is material to practicing the invention claimed by

claim 1 of the ’352 Patent, (ii) is not a staple article or commodity of commerce suitable for substantial non-infringing use, and (iii) Defendant is aware or knows to be especially made or especially adapted for use in infringement of the ’352 Patent. Defendant specifically intends its customers to infringe by implementing access control lists for filtering and dropping of packets implemented at the ingress port for egress pass/drop determination, as set forth above and in the excerpts from Defendant’s technical manuals.

68. On information and belief, Defendant’s customers deploy the accused products on networks in combination with other products. The specific code portions and modules directed to the infringing functionality will be identified as those systems are made available for inspection and review by Parity Networks.

69. As a result of Defendant’s infringement of the ’352 Patent, Parity Networks has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement under 35 U.S.C. § 284, but in no event, less than a reasonable royalty.

COUNT SIX
INFRINGEMENT OF U.S. PATENT NO. 7,719,963

70. Parity Networks incorporates by reference its allegations in the preceding paragraphs as if fully restated in this paragraph.

71. Parity Networks is the assignee and owner of all right, title, and interest to the ’963 Patent. Parity Networks has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

72. On information and belief, at least since the release of the ’963 Exemplary Infringing Products and until the expiration of the ’963 Patent, without authorization or license from Parity Networks, Defendant was directly infringing each and every element of at least claim 1 of the ’963 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. §

271(a), including through making, using (including for testing purposes), selling, and offering for sale methods and articles infringing one or more claims of the ’963 Patent. Defendant is thus liable for direct infringement of the ’963 Patent pursuant to 35 U.S.C. § 271(a).

73. Exemplary infringing products include Defendant’s 5300 Series Switch, M7100 Series Switch, ProSafe XSM7224S 10G Managed Stackable Switch, all substantially similar switches, all associated computer hardware, software and digital content, and all products operating in a substantially similar manner (“’963 Exemplary Infringing Products”). The ’963 Exemplary Infringing Products support Queue Management at each port for managing outgoing data traffic. The ’963 Exemplary Infringing Products support a WRED algorithm on packet queues to drop packets as a function of queue size (or buffer) in order to manage congestion in the switch, as set forth above and in the excerpts from Defendant’s technical manuals.

74. As a result of Defendant’s infringement of the ’963 Patent, Parity Networks has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement under 35 U.S.C. § 284, but in no event, less than a reasonable royalty.

VI. JURY DEMAND

75. Plaintiff Parity Networks demands a trial by jury of all matters to which it is entitled to trial by jury, pursuant to FED. R. CIV. P. 38.

VII. PRAYER FOR RELIEF

WHEREFORE, Parity Networks prays for judgment and seeks relief against Defendant as follows:

A. That the Court determine that one or more claims of the Patents-in-Suit is infringed by Defendant, either literally or under the doctrine of equivalents;

B. That the Court award damages adequate to compensate Parity Networks for the patent infringement that has occurred, together with prejudgment and post-judgment interest and costs, and an ongoing royalty for continued infringement; and

C. That the Court award such other relief to Parity Networks as the Court deems just and proper.

Dated: November 21, 2022

Of Counsel:

Andrew G. DiNovo
Adam G. Price
DINOVO PRICE LLP
7000 N. MoPac Expressway, Suite 350
Austin, Texas 78731
Telephone: (512) 539-2626
Facsimile: (512) 539-2627
adinovo@dinovoprice.com
aprice@dinovoprice.com

Respectfully submitted,

FARNAN LLP

/s/ Michael J. Farnan
Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
919 N. Market St., 12th Floor
Wilmington, Delaware 19801
Telephone: (302) 777-0300
Facsimile: (302) 777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Attorneys for Plaintiff