

ProSAFE M4100 Managed Switches

Software Administration Manual

Software Version 10.0.1

March 2015 202-11161-02

350 East Plumeria Drive San Jose, CA 95134 USA



Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at http://support.netgear.com/general/contact/default.aspx.

Contact your Internet service provider for technical support.

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.

See the regulatory compliance document before connecting the power supply.

Trademarks

© NETGEAR, Inc. NETGEAR and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

Publication Part Number	Publish Date	Comments
202-11161-02	March 2015	Made the document specific to the M4100 series switches by removing sections and chapters that do not apply to the M4100 series switches.
202-11161-01	February 2013	Updated the document.
	October 2012	Added iSCSI features.
202-11153-01	August 2012	Added Private VLAN features.
202-10515-05	August 2012	Added MVR feature.
202-10515-05	July 2011	Added DHCPv6 and DHCPv6 mode features.
202-10515-04	November 2010	New document template.
202-10515-03	June 2010	Moved some content to the Software Setup Guide.
202-10515-02		Software release 8.0.2: new firmware with DHCP L3 Relay, color conform policy, DHCP server in dynamic mode, and configuring a stacking port as an Ethernet port.
202-10515-01		Original publication.

Table of Contents

Chapter 1 Documentation Resources

Chapter 2 VLANs

VLAN Concepts	14
Create Two VLANs.	15
CLI: Create Two VLANS	15
Web Interface: Create Two VLANS.	15
Assign Ports to VLAN2	16
CLI: Assign Ports to VLAN2	16
Web Interface: Assign Ports to VLAN2	16
Create Three VLANs	18
CLI: Create Three VLANS	18
Web Interface: Create Three VLANS	18
Assign Ports to VLAN3	20
CLI: Assign Ports to VLAN3	20
Web Interface: Assign Ports to VLAN3	20
Assign VLAN3 as the Default VLAN for Port 1/0/2	21
CLI: Assign VLAN3 as the Default VLAN for Port 1/0/2	21
Web Interface: Assign VLAN3 as the Default VLAN for Port 1/0/2	22
Create a MAC-Based VLAN	22
CLI: Create a MAC-Based VLAN	23
Web Interface: Assign a MAC-Based VLAN	24
Create a Protocol-Based VLAN	25
CLI: Create a Protocol-Based VLAN	26
Web Interface: Create a Protocol-Based VLAN	27
Virtual VLANs: Create an IP Subnet-Based VLAN	28
CLI: Create an IP Subnet–Based VLAN	29
Web Interface: Create an IP Subnet–Based VLAN	30
Voice VLANs	31
CLI: Configure Voice VLAN and Prioritize Voice Traffic.	32
Web Interface: Configure Voice VLAN and Prioritize Voice Traffic	34
Private VLANs	41
Assign Private-VLAN Types (Primary, Isolated, Community)	43
CLI: Assign Private-VLAN Type (Primary, Isolated, Community)	43
Web Interface: Assign Private-VLAN Type (Primary, Isolated, Community)	44
Configure Private-VLAN Association	45
CLI: Configure Private-VLAN Association	45
Web Interface: Configure Private-VLAN Association	45
Configure Private-VLAN Port Mode (Promiscuous, Host)	46
CLI: Configure Private-VLAN Port Mode (Promiscuous, Host)	46

Web Interface: Configure Private-VLAN Port Mode (Promiscuous, Host)	. 46
Configure Private-VLAN Host Ports	. 48
CLI: Configure Private-VLAN Host Ports	. 48
Web Interface: Assign Private-VLAN Port Host Ports	. 48
Map Private-VLAN Promiscuous Port	. 49
CLI: Map Private-VLAN Promiscuous Port	. 49
Web Interface: Map Private-VLAN Promiscuous Port	. 50

Chapter 3 LAGs

LAG Concepts
Create Two LAGs
CLI: Create Two LAGs 53
Web Interface: Create Two LAGs 53
Add Ports to LAGs
CLI: Add Ports to the LAGs 54
Web Interface: Add Ports to LAGs 54
Enable Both LAGs
CLI: Enable Both LAGs 56
Web Interface: Enable Both LAGs 56

Chapter 4 Port Routing

Port Routing Concepts
Port Routing Configuration
Enable Routing for the Switch 59
CLI: Enable Routing for the Switch 59
Web Interface: Enable Routing for the Switch
Enable Routing for Ports on the Switch
CLI: Enable Routing for Ports on the Switch
Web Interface: Enable Routing for Ports on the Switch
Add a Default Route
CLI: Add a Default Route63
Web Interface: Add a Default Route63
Add a Static Route
CLI: Add a Static Route 64
Web Interface: Add a Static Route

Chapter 5 VLAN Routing

VLAN Routing Concepts	67
Create Two VLANs	67
CLI: Create Two VLANs	68
Web Interface: Create Two VLANs	69
Set Up VLAN Routing for the VLANs and the Switch	72
CLI: Set Up VLAN Routing for the VLANs and the Switch	72
Web Interface: Set Up VLAN Routing for the VLANs and the Switch	73

Chapter 6 Proxy ARP

Proxy ARP Concepts	75
Proxy ARP Examples	75
CLI: show ip interface	75
CLI: ip proxy-arp	75
Web Interface: Configure Proxy ARP on a Port	76

Chapter 7 ACLs

ACL Concepts
MAC ACLs
IP ACLs
ACL Configuration
Set Up an IP ACL with Two Rules
CLI: Set Up an IP ACL with Two Rules
Web Interface: Set Up an IP ACL with Two Rules
One-Way Access Using a TCP Flag in an ACL
CLI: Configure One-Way Access Using a TCP Flag in an ACL
Web Interface: Configure One-Way Access Using a TCP Flag in an ACL 88
Use ACLs to Configure Isolated VLANs on a Layer 3 Switch
CLI: Configure One-Way Access Using a TCP Flag in ACL Commands101
Web Interface: Configure One-Way Access Using a TCP Flag in an ACL 103
Set up a MAC ACL with Two Rules
CLI: Set up a MAC ACL with Two Rules112
Web Interface: Set up a MAC ACL with Two Rules
ACL Mirroring
CLI: Configure ACL Mirroring115
Web Interface: Configure ACL Mirroring117
ACL Redirection
CLI: Redirect a Traffic Stream120
Web Interface: Redirect a Traffic Stream
Configure IPv6 ACLs
CLI: Configure an IPv6 ACL
Web Interface: Configure an IPv6 ACL128

Chapter 8 CoS Queuing

QoS Queuing Concepts
CoS Queue Mapping133
CoS Queue Configuration134
Show classofservice Trust
CLI: Show classofservice Trust135
Web Interface: Show classofservice Trust
Set classofservice Trust Mode135
CLI: Set classofservice Trust Mode135
Web Interface: Set classofservice Trust Mode 136
Show classofservice IP-Precedence Mapping136
CLI: Show classofservice IP-Precedence Mapping136

Web Interface: Show classofservice ip-precedence Mapping 136
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode 137
CLI: Configure Cos-queue Min-bandwidth and Strict Priority
Scheduler Mode
Web Interface: Configure CoS-queue Min-bandwidth and
Strict Priority Scheduler Mode138
Set CoS Trust Mode for an Interface139
CLI: Set CoS Trust Mode for an Interface
Web Interface: Set CoS Trust Mode for an Interface
Configure Traffic Shaping140
CLI: Configure traffic-shape141
Web Interface: Configure Traffic Shaping141

Chapter 9 DiffServ

DiffServ Concepts143
Configure DiffServ144
CLI: Configure DiffServ144
Web Interface: Configure DiffServ146
DiffServ for VoIP159
CLI: Configure DiffServ for VoIP160
Web Interface: Diffserv for VoIP161
Auto VoIP
CLI: Configure Auto VoIP167
Web Interface: Configure Auto-VoIP
DiffServ for IPv6170
CLI: Configure DiffServ for IPv6170
Web Interface: Configure DiffServ for IPv6
Color Conform Policy
CLI: Configure a Color Conform Policy178
Web Interface: Configure a Color Conform Policy

Chapter 10 IGMP Snooping and Querier

Internet Group Management Protocol Concepts
IGMP Snooping
CLI: Enable IGMP Snooping
Web Interface: Enable IGMP Snooping187
Show igmpsnooping
CLI: Show igmpsnooping188
Web Interface: Show igmpsnooping
Show mac-address-table igmpsnooping
CLI: Show mac-address-table igmpsnooping189
Web Interface: Show mac-address-table igmpsnooping
External Multicast Router190
CLI: Configure the Switch with an External Multicast Router
Web Interface: Configure the Switch with an External Multicast Router 190
Multicast Router Using VLAN191
CLI: Configure the Switch with a Multicast Router Using VLAN191

Web Interface: Configure the Switch with a Multicast I	Router Using VLAN191
IGMP Querier	
Enable IGMP Querier	
CLI: Enable IGMP Querier	
Web Interface: Enable IGMP Querier	
Show IGMP Querier Status	
CLI: Show IGMP Querier Status	
Web Interface: Show IGMP Querier Status	

Chapter 11 MVR

MVR Concepts	198
Configure MVR in Compatible Mode	199
CLI: Configure MVR in Compatible Mode	200
Web Interface: Configure MVR in Compatible Mode	202
Configure MVR in Dynamic Mode	205
CLI: Configure MVR in Dynamic Mode	205
Web Interface: Configure MVR in Dynamic Mode	207

Chapter 12 Security Management

Port Security	. 212
Set the Dynamic and Static Limit on Port 1/0/1	. 213
CLI: Set the Dynamic and Static Limit on Port 1/0/1	. 213
Web Interface: Set the Dynamic and Static Limit on Port 1/0/1	. 213
Convert the Dynamic Address Learned from 1/0/1 to a Static Address	. 214
CLI: Convert the Dynamic Address Learned from 1/0/1 to the	
Static Address	. 214
Web Interface: Convert the Dynamic Address Learned from	
1/0/1 to the Static Address	. 215
Create a Static Address	. 215
CLI: Create a Static Address	. 215
Web Interface: Create a Static Address	. 216
Protected Ports	. 216
CLI: Configure a Protected Port to Isolate Ports on the Switch	. 217
Web Interface: Configure a Protected Port to Isolate Ports on the Switch	219
802.1x Port Security	. 222
CLI: Authenticating dot1x Users by a RADIUS Server	. 223
Web Interface: Authenticating dot1x Users by a RADIUS Server	. 224
Create a Guest VLAN	. 228
CLI: Create a Guest VLAN	. 230
Web Interface: Create a Guest VLAN	. 231
Assign VLANs Using RADIUS	. 234
CLI: Assign VLANS Using RADIUS	. 235
Web Interface: Assign VLANS Using RADIUS	. 237
Dynamic ARP Inspection.	. 240
CLI: Configure Dynamic ARP Inspection	. 241
Web Interface: Configure Dynamic ARP Inspection	. 242
Static Mapping	. 246

Chapter 13 SNTP

SNTP Concepts
Show SNTP
show sntp
show sntp client
show sntp server
Configure SNTP
CLI: Configure SNTP
Web Interface: Configure SNTP263
Set the Time Zone
Set the Named SNTP Server
CLI: Set the Named SNTP Server
Web Interface: Set the Named SNTP Server

Chapter 14 Tools

Web Interface: Download a Backup Image and Make It Active	276
Outbound Telnet	277
CLI: show network	278
CLI: show telnet	278
CLI: transport output telnet	279
Web Interface: Configure Telnet	279
CLI: Configure the session-limit and session-timeout	
Web Interface: Configure the Session Timeout	

Chapter 15 Syslog

Syslog Concepts
Show Logging
CLI: Show Logging
Web Interface: Show Logging
Show Logging Buffered
CLI: Show Logging Buffered
Web Interface: Show Logging Buffered
Show Logging Traplogs
CLI: Show Logging Traplogs
Web Interface: Show Logging Trap Logs
Show Logging Hosts
CLI: Show Logging Hosts
Web Interface: Show Logging Hosts
Configure Logging for a Port
CLI: Configure Logging for the Port
Web Interface: Configure Logging for the Port
Email Alerting
CLI: Send Log Messages to admin@switch.com Using Account
aaaa@netgear.com

Chapter 16 SNMP

Chapter 17 DNS

DNS Concepts	. 302
Specify Two DNS Servers	. 302
CLI: Specify Two DNS Servers	. 302
Web Interface: Specify Two DNS Servers	. 302
Manually Add a Host Name and an IP Address	. 303
CLI: Manually Add a Host Name and an IP Address	. 303
Web Interface: Manually Add a Host Name and an IP Address	. 303

Chapter 18 DHCP Server

DHCP Server Concepts	305
Configure a DHCP Server in Dynamic Mode	305
CLI: Configure a DHCP Server in Dynamic Mode	305
Web Interface: Configure a DHCP Server in Dynamic Mode	306
Configure a DHCP Server that Assigns a Fixed IP Address	308
CLI: Configure a DHCP Server that a Assigns Fixed IP Address	309
Web Interface: Configure a DHCP Server that Assigns a Fixed IP Address	309

Chapter 19 DVLANs and Private VLANs

Double VLANs	312
CLI: Enable a Double VLAN	. 313
Web Interface: Enable a Double VLAN	. 313
Private VLAN Groups	. 316
CLI: Create a Private VLAN Group	317
Web Interface: Create a Private VLAN Group	. 318

Chapter 20 STP

SPT Concepts
Configure Classic STP (802.1d) 323
CLI: Configure Classic STP (802.1d) 323
Web Interface: Configure Classic STP (802.1d)
Configure Rapid STP (802.1w)
CLI: Configure Rapid STP (802.1w)
Web Interface: Configure Rapid STP (802.1w)
Configure Multiple STP (802.1s) 326
CLI: Configure Multiple STP (802.1s)
Web Interface: Configure Multiple STP (802.1s)

Chapter 21 DHCP L2 Relay and L3 Relay

DHCP L2 Relay	330
CLI: Enable DHCP L2 Relay	330
Web Interface: Enable DHCP L2 Relay	332
DHCP L3 Relay	335
Configure the DHCP Server Switch	335

Configure a DHCP L	.3 Switch	
--------------------	-----------	--

Chapter 22 MLD Snooping

Multicast Listener Discovery Concepts	346
MLD Snooping Concepts	346
CLI: Configure MLD Snooping	347
Web Interface: Configure MLD Snooping	347

Index

Documentation Resources



Before installation, read the Release Notes for this switch product. The Release Notes detail the platform-specific functionality of the switching, routing, SNMP, configuration, management, and other packages. In addition, see the following publications:

- The NETGEAR installation guide for your switch
- Managed Switch Hardware Installation Guide
- Managed Switch Software Setup Manual
- ProSAFE Managed Switch Command Line Interface (CLI) User Manual
- ProSAFE M4100 Managed Switch Web Management User Manual

VLANs

Virtual LANs

This chapter includes the following sections:

- VLAN Concepts
- Create Two VLANs
- Assign Ports to VLAN2
- Create Three VLANs
- Assign Ports to VLAN3
- Assign VLAN3 as the Default VLAN for Port 1/0/2
- Create a MAC-Based VLAN
- Create a Protocol-Based VLAN
- Virtual VLANs: Create an IP Subnet–Based VLAN
- Voice VLANs
- Private VLANs
- Assign Private-VLAN Types (Primary, Isolated, Community)
- Configure Private-VLAN Association
- Configure Private-VLAN Port Mode (Promiscuous, Host)
- Configure Private-VLAN Host Ports
- Map Private-VLAN Promiscuous Port

2

VLAN Concepts

Adding virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast. Like a router, it partitions the network into logical segments, which provides better administration, security, and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You can have different reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station might omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet can either reject it or insert a tag using its default VLAN ID. A given port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.

The Private Edge VLAN feature lets you set protection between ports located on the switch. This means that a protected port cannot forward traffic to another protected port on the same switch. The feature does not provide protection between ports located on different switches.

The diagram in this section shows a switch with four ports configured to handle the traffic for two VLANs. Port 1/0/2 handles traffic for both VLANs, while port 1/0/1 is a member of VLAN 2 only, and ports 1/0/3 and 1/0/4 are members of VLAN 3 only. The script following the diagram shows the commands you would use to configure the switch as shown in the diagram.



Figure 1. Switch with 4 ports configured for traffic from 2 VLANs

The following examples show how to create VLANs, assign ports to the VLANs, and assign a VLAN as the default VLAN to a port.

Create Two VLANs

The example is shown as CLI commands and as a Web interface procedure.

CLI: Create Two VLANS

Use the following commands to create two VLANs and to assign the VLAN IDs while leaving the names blank.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2
(Netgear Switch) (Vlan)#vlan 3
(Netgear Switch) (Vlan)#exit
```

Web Interface: Create Two VLANS

- 1. Create VLAN2.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VIAN STP	Multicast /	Address Table	Ports LAG					
	VLA	V Configura	ation					
Cardigerature	Re	set						
Advanced	Reset	Configuration						
	VL	AN Configura	ition			1.82		
		VEAN ED	VLAN Name	-	VLAN TY	pe		
		2	VLANZ		Static	1		
		1	Default		Default			

- **b.** Enter the following information:
 - In the VLAN ID field, enter 2.
 - In the VLAN Name field, enter VLAN2.
 - In the VLAN Type list, select Static.
- c. Click Add.
- 2. Create VLAN3.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VIAN STP	Multicast 0	Address Toble	Ports LAG				··	
Beette	VLA	N Configura	tion					
Cityligenment	R	eset				00		
Advanced	Reset	Configuration		5				
	VI	AN Configura	tion			.00		
		VLAN ID	VLAN Name		YLAN TY	pe		
		3	VLAN3		Static			
		1	Default		Default			
	E		3.0 4.9.7		Static			

- **b.** Enter the following information:
 - In the VLAN ID field, enter 3.
 - In the VLAN Name field, enter VLAN3.
 - In the VLAN Type list, select Static.
- c. Click Add.

Assign Ports to VLAN2

This sequence shows how to assign ports to VLAN2, and to specify that frames will always be transmitted tagged from all member ports and that untagged frames will be rejected on receipt.

CLI: Assign Ports to VLAN2

(Netgear	Switch)	#config
(Netgear	Switch)	(Config)#interface range 1/0/1-1/0/2
(Netgear	Switch)	(conf-if-range-1/0/1-1/0/2)#vlan participation include 2
(Netgear	Switch)	(conf-if-range-1/0/1-1/0/2)#vlan acceptframe vlanonly
(Netgear	Switch)	(conf-if-range-1/0/1-1/0/2)#vlan pvid 2
(Netgear	Switch)	(conf-if-range-1/0/1-1/0/2)#exit
(Netgear	Switch)	(Config)#vlan port tagging all 2
(Netgear	Switch)	(Config)#

Web Interface: Assign Ports to VLAN2

- 1. Assign ports to VLAN2.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

System Swit	ching Routin	g Qo5	Security N	Monitoring M	aintenance	Help	Inde
VIAN STP Mult	cost Address Toble	Ports DAG					
Basic Advanced	VLAN Membe	rship					
* VLAN	VLAN Membe	rship					
Configuration	VLAN ID	2 🕷		Group Operation	Unteg All		
VLAN Plantherster	VEAN Name	VLAN2		UNTAGGED PORT ME	IMAERS.		
MAC Barad VI AN	VLAN Type	Static		TAGGED PORT MEN	MAERS	<u> </u>	
Port PVID	- Dails S						
Configuration • Port DVLAN Configuration	Port 1 2 3 T T 25 26 27	456789 28	10 11 12 13	14 15 16 17 18	19 20 21 22	23 24	

- b. In the VLAN ID list, select 2.
- c. Click Unit 1. The ports display.
- d. Click the gray boxes under ports 1 and 2 until T displays.

The T specifies that the egress packet is tagged for the ports.

- e. Click Apply to save the settings.
- 2. Specify that only tagged frames will be accepted on ports 1/0/1 and 1/0/2.
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration.

System 5	witching	Routing	QoS !	Security Manitor	ing Mainte	nance	Help	Index	
VLAN I STP I N	Whicest	Address Table	Ronta LAG						
Basic	Port	VLAN Id Co	nfiguration						
VLAN	P	/ID Configurati	on				10		
Configuration	3.	All Go To Interface 00							
VLAN Membership VLAN Status MAC Based VLAN		Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (to 7)	(a)		
Configuration		1 7							
* Port DVLAN	R	1/0/1	1	Admit All	Disable	0			
Configuration	R	1/0/2	1	Admit Ali	Disable	0			
VLAN Groun	D	1/0/3	1	Admit All	Disable	0			
Configuration	Г	1/0/4	1	Admit All	Disable	0			

- b. Under PVID Configuration, scroll down and select the check box for Interface 1/0/1.
 Then scroll down and select the Interface 1/0/2 check box.
- c. Enter the following information:
 - In the Acceptable Frame Type polyhedron list, select VLAN Only.
 - In the PVID (1 to 4093) field, enter 2.
- d. Click Apply to save the settings.

Create Three VLANs

The example is shown as CLI commands and as a Web interface procedure.

CLI: Create Three VLANS

Use the following commands to create three VLANs and to assign the VLAN IDs while leaving the names blank.

(Netgear Switch) #vlan database (Netgear Switch) (Vlan)#vlan 100 (Netgear Switch) (Vlan)#vlan 101 (Netgear Switch) (Vlan)#vlan 102 (Netgear Switch) (Vlan)#exit

Web Interface: Create Three VLANS

- 1. Create VLAN100.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help Inde
VLAN Aut	o-VolP ISCSI	STP Multi	cast MVR	Address Ta	ole Ports LAG		
Basic	N	/LAN Confi	guration				
- VLAN		Reset					(7)
Advanced		Reset Configur	ation				11-11
		Internal VLAN Configuration					
	1	Internal VLAN Allocation Base			4093		
		Internal VLAN	Allocation Policy	<i>,</i>	Ø Ascending		
		VLAN Conf	iguration				(<u>)</u>
	1	VLAN ID	VLAN Name		VLAN Type	Make Static	
		100	VLAN100			Disable 👻	
		1	default		Default	Disable	
	1	2	Auto VoIP		AUTO VoIP	Disable	

- **b.** Enter the following information:
 - In the VLAN ID field, enter 100.
 - In the VLAN Name field, enter VLAN100.
- c. Click Add.
- 2. Create VLAN101.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VEAN Auto	-VolP ISCSI	STP Mul	ticast MVR	Address Table	Ports LAG			
lasic		VLAN Conf	iguration					
VLAN		Reset					(2)	
Advanced		Reset Configu	ration		83			
		Internal VLAN Configuration						
		Internal VLAN	Allocation Base		4093			
		Internal VLAN	Allocation Policy		Ascending (Descending		
		VLAN Cor	figuration				Ō	
		VLAN ID	VLAN Name		LAN Type	Make Static		
		101	VLAN101			Disable 🚽		
		1	default	1	Default	Disable		
		2	Auto VoIP	3	UTO VOIP	Disable		

- **b.** Enter the following information:
 - In the VLAN ID field, enter 101.
 - In the VLAN Name field, enter VLAN101.
- c. Click Add.
- 3. Create VLAN102.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

System Switch	ng Routin	g QoS Secur	rity Monitoring	Maintenance	Help Index			
VLAN Auto-VolP I	SCSI STP M	ulticost MVR Add	ress Table Ports LAG					
Basic	VLAN Cor	figuration						
e VLAN	Reset				(1)			
Advanced	Reset Config	puration	13					
	Internal	VLAN Configuration			(j)			
	Internal VL	AN Allocation Base	4093					
	Internal VL/	AN Allocation Policy	Ascending	Ascending Descending				
	VLAN CO	onfiguration			٢			
	VLAN I	D VLAN Name	VLAN Type	Make Static				
	101	VLAN101		Disable 🚽				
	1	default	Default	Disable				
	2	Auto VoIP	AUTO VoIP	Disable				

- **b.** Enter the following information:
 - In the VLAN ID field, enter 102.
 - In the VLAN Name field, enter VLAN102.
- c. Click Add.

Assign Ports to VLAN3

This example shows how to assign the ports that will belong to VLAN 3, and to specify that untagged frames will be accepted on port 1/0/4. Note that port 1/0/2 belongs to both VLANs and that port 1/0/1 can never belong to VLAN 3.

CLI: Assign Ports to VLAN3

```
(Netgear Switch) (Config)#interface range 1/0/2-1/0/4
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#vlan participation include 3
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#vlan acceptframe all
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Assign Ports to VLAN3

- **1.** Assign ports to VLAN3.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

A screen similar to the following displays.

System 5	witching	Routing	QoS	Security	Monitoring	Maintenance	Help I	nda
VUAN I STP I N	Willicost Ad	Idress Table	Ports LAG	÷				
Basic Advanced	VLAN	Member	ship					
VLAN	VLA	N Member	ship				(2)	
Configuration	VLAN I	D .	3 💌 📖		Group Operat	ion Untag All		
VLAN Hambersh	VLANP	tanse	VLANI		UNIAGGED P	ORT MEMAERS		
MAC Baced VI Al	VEAN 1	ype	Static	-	TADDED FO	AT MEMBERS		
Port PVID	- 0	sit t						
Configuration	Port 1	2 3 4	5678	9 10 11 1	2 13 14 15 16 1	7 18 19 20 21 22	23 24	
Port DVLAN Configuration	2	5 26 27 2	10					

- b. In the VLAN ID list, select 3.
- c. Click Unit 1. The ports display.
- d. Click the gray boxes under ports 2, 3, and 4 until T displays.

The T specifies that the egress packet is tagged for the ports.

- e. Click Apply to save the settings.
- 2. Specify that untagged frames will be accepted on port 1/0/4.
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration.

VIAN STP Multi	cost	Address Table 1	Rorts LAG	ecurity Monitor	ing Mainte	nance He	ip Index
Basic Advanced + VLAN		Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)	
Configuration		1/0/4	1	Admit All	Disable 💌	0	
VLAN Membership	E.	1/0/1	1	Admit All	Disable	0	
> MAC Reced VI AN	1	1/0/2	1	Admit All	Disable	0	
+ Fost FVID		1/0/0	1	Admit All	Disable	0	
Configuration :	2	1/0/4	1	Admit All	Disable	0	
> Port DVLAN		1/0/5	1	Admit All	Disable	0	

b. Scroll down and select the Interface **1/0/4** check box.

Now 1/0/4 appears in the Interface field at the top.

- c. In the Acceptable Frame Types list, select Admit All.
- d. Click Apply to save the settings.

Assign VLAN3 as the Default VLAN for Port 1/0/2

This example shows how to assign VLAN 3 as the default VLAN for port 1/0/2.

CLI: Assign VLAN3 as the Default VLAN for Port 1/0/2

(Netgear	Switch)	#config	
(Netgear	Switch)	(Config)#interface 1/0/2	
(Netgear	Switch)	(Interface 1/0/2)#vlan pvid 3	5
(Netgear	Switch)	(Interface 1/0/2)#exit	
(Netgear	Switch)	(Config)#exit	

Web Interface: Assign VLAN3 as the Default VLAN for Port 1/0/2

1. Select Switching > VLAN > Advanced > Port PVID Configuration.

A screen similar to the following displays.

Basic Allwancod > VLAN	Port	VLAN Id Co VID Configuration	nfiguration m			Ð	
Configuration		All		Go To Interf	ate 00)	
VLAN Membership VLAN Status MAC Based VLAN		Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)	
Catifiguration:		1/0/2	3	Admit All 💌	Disable -	0	
Port DVLAN	Π.	1/0/1	1	Admit All	Disable	0	
Configuration	12	1/0/2	1	Admit All	Disable	0	
VI AN Group	1	1/0/3	1	Admit All	Disable	0	
Configuration	1	1/0/4	1	Admit All	Disable	0	
Protocol Based		1/0/5	1	Admit All	Disable	0	
VLAN Group	Γ.	1/0/6	1	Admit All	Disable	ō	
Membership	1	1/0/7	1	Admit All	Disable	0	

- 2. Under PVID Configuration, scroll down and select the Interface 1/0/2 check box. Now 1/0/2 appears in the Interface field at the top.
- 3. In the PVID (1 to 4093) field, enter 3.
- 4. Click **Apply** to save the settings.

Create a MAC-Based VLAN



The MAC-based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet.

You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified using a source MAC address and the appropriate VLAN ID. The MAC to

VLAN configurations are shared across all ports of the device (i.e., there is a system-wide table that has MAC address to VLAN ID mappings).

When untagged or priority tagged packets arrive at the switch and entries exist in the MAC to VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged it will maintain this value; otherwise, the priority will be set to 0 (zero). The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped. This implies that you can configure a MAC address mapping to a VLAN that has not been created on the system.

CLI: Create a MAC-Based VLAN

1. Create VLAN3.

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 3
(Netgear Switch)(Vlan)#exit
```

2. Add port 1/0/23 to VLAN3.

```
(Netgear Switch)#config
(Netgear Switch)(Config)#interface 1/0/23
(Netgear Switch)(Interface 1/0/23)#vlan participation include 3
(Netgear Switch)(Interface 1/0/23)#vlan pvid 3
(Netgear Switch)(Interface 1/0/23)#exit
```

3. Map MAC 00:00:0A:00:00:02 to VLAN3.

```
(Netgear Switch)(Config)#exit
(Netgear Switch)#vlan data
(Netgear Switch)(Vlan)#vlan association mac 00:00:00A:00:00:02 3
(Netgear Switch)(Vlan)#exit
```

4. Add all the ports to VLAN3.

```
(Netgear Switch)#config
(Netgear Switch)(Config)#interface range 1/0/1-1/0/28
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#vlan participation include 3
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#exit
(Netgear Switch)(Config)#exit
```

Web Interface: Assign a MAC-Based VLAN

- 1. Create VLAN3.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VUAN STP	Multicast	Address Toble	Ports LAG				1997 1997 1997	
Seet.	VLA	N Configura	ation					
Cinfiguration	R	teset				00		
Advanced	Rese	et Configuration		5				
	V	LAN Configura	tion			0		
	-	VLAN ID	VLAN Name		YLAN TY	pe		
		3	VLAN3		Static	1		
	. 🗖	1	Default		Default			
	E	2	VLAN2		Static			

- **b.** Enter the following information:
 - In the VLAN ID field, enter 3.
 - In the VLAN Name field, enter VLAN3.
 - In the VLAN Type list, select Static.
- c. Click Add.
- 2. Assign ports to VLAN3.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

System 5v	ritching	1	Ro	utin	9	G	105		50	cur	ity.	Т	N	loni	tori	ng.	Т	Μ	aint	tena	nce	ų.	12	Halp
VIAN STP I M	discost	Add	r688	Table	60	lorts	u	G																
Dasic	VLA	NN	/ler	nbe	ersh	ip																		
+deenced • VLAN	v	LAN	Me	mbi	rshi	p																		T
Configuration	VLA	N ID			3	1	Ξ.							Gre	nap (lgree	atio	n.	. 6	Jritas	a All			-
VLAT THIS beaution	YEA	NiNa	me		1	LANS								I.u	NTAC	IGED	POS	T MI	IMBE	81				
VLAN Statul	YLA	N Ty	9 10	_	5	tetic									TAG	GED I	hoat	ME/	MBER	5.0				
Port PVID	- 47	Unit																						
Configuration	Port	1	2	3	4 3	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Port DVLAN		U	0	U	U	υU	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
Configuration		25	26	27	20																			
and the second		U	U	U	U																			

- b. In the VLAN ID list, select 3.
- **c.** Click **Unit 1.** The ports display.
- **d.** Click the gray box before Unit 1 until **U** displays.
- e. Click Apply.
- **3.** Assign VPID3 to port 1/0/23.
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration.

System 5	vitching	Routing	GoS S	iecurity Monitor	ing Mainter	nance Help	Index
VLAN STP M	alticast.	Address Table F	forth LAG				
Basic	Port	VLAN Id Co	nfiguration				
Advanced	P	VID Configuratio	on			101	
Configuration	1	All		Go To Inter	lece 00.		
 VLAN Membershi VLAN Status MAC Based VLAN 	р 4	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)	
Configuration		1/0/23	3	Admit All	Disable 💽	0	
Port DVLAN		1/0/1	1-	Admit All	Disable	0	
Configuration	F	1/0/2	1	Admit All	Disable	0	

- **b.** Scroll down and select the **1/0/23** check box.
- c. In the PVID (1 to 4093) field, enter 3.
- d. Click Apply to save the settings.
- **4.** Map the specific MAC to VLAN3.
 - a. Select Switching > VLAN > Advanced > MAC based VLAN.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VUAN STP	Multicast Ad	dress Toble	Ports LAG					
Basic	MAC E	Based VLAM	V Configu	ration				
- VLAN	Con	figuration					Đ.	
Configuration	150	MAC Ad	dress			VLAN ID		
VLAN Membersi	hip	00:00:0	A:00:00:02			2		

- **b.** Enter the following information:
 - In the MAC Address field, enter 00:00:0A:00:00:02.
 - In the PVID (1 to 4093) field, enter 3.
- c. Click Add.

Create a Protocol-Based VLAN

Create two protocol VLAN groups. One is for IPX and the other is for IP/ARP. The untagged IPX packets are assigned to VLAN 4, and the untagged IP/ARP packets are assigned to VLAN 5.

CLI: Create a Protocol-Based VLAN

1. Create a VLAN protocol group vlan_ipx based on IPX protocol.

```
(Netgear Switch)#config
(Netgear Switch)(Config)#vlan protocol group vlan_ipx
(Netgear Switch)(Config)#vlan protocol group add protocol 1 ipx
```

2. Create a VLAN protocol group vlan_ipx based on IP/ARP protocol.

```
(Netgear Switch)(Config)#vlan protocol group vlan_ip
(Netgear Switch)(Config)#vlan protocol group add protocol 2 ip
(Netgear Switch)(Config)#vlan protocol group add protocol 2 arp
(Netgear Switch)(Config)#exit
```

3. Assign VLAN protocol group 1 to VLAN 4.

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 4
(Netgear Switch)(Vlan)#vlan 5
(Netgear Switch)(Vlan)#protocol group 1 4
```

4. Assign VLAN protocol group 2 to VLAN 5.

```
(Netgear Switch)(Vlan)#protocol group 2 5
```

5. Enable protocol VLAN group 1 and 2 on the interface.

```
(Netgear Switch)(Vlan)#exit
(Netgear Switch)#config
(Netgear Switch)(Config)#interface 1/0/11
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 1
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 2
(Netgear Switch)(Interface 1/0/11)#exit
```

Web Interface: Create a Protocol-Based VLAN

- 1. Create the protocol-based VLAN group vlan_ipx.
 - a. Select Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration.

A screen similar to the following displays.

System	Switchin	g Routin	g QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP	Multicast	Address Table	Ports LAG					
Basic	P	rotocol Base	d VLAN Gro	up Configura	ation			
Advanced	6	Protocol Bas	ed VLAN Group	Configuration			(7)	
Configurati > VLAN Memi	on bership	Group Name	Group ID	Proto	ol VLA	N ID Port	s	
» VLAN Statu » Port PVID	IS	vlan_ipx		IP ARP IPX	4			

Enter the following information:

- In the Group Name field, enter vlan_ipx.
- In the **Protocol** list, select **IPX**.
- In the VLAN ID field, enter 4.
- b. Click Add.
- 2. Create the protocol-based VLAN group vlan_ip.

a. Select Switching > VLAN >Advanced > Protocol Based VLAN Group Configuration.

System	Switching	Routing	g QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP /	Multicost	Address Table	Ports LAG					
Basic	Pro	tocol Base	d VLAN Grou	up Configur	ation			
Advanced	1	Protocol Base	d VLAN Group	Configuration			(?)	
Configuration > VLAN Membersi	hip	Group Name	Group ID	Proto	ol VLA	N ID Por	ts	
» VLAN Status » Port PVID		vlan_ip		IP ARP IPX	- 5			
Configuration		vlan_ipx	1	IPX	4			

- **b.** Enter the following information:
 - In the Group Name field, enter vlan_ip.
 - In the **Protocol** list, select **IP** and **ARP** while holding down the **Ctrl** key.
 - In the VLAN field, enter 5.
- c. Click Add.
- **3.** Add port 11 to the group vlan_ipx.
 - a. Select Switching > VLAN > Advanced > Protocol Based VLAN Group Membership.

VIAN STP M-N	conting Address Table	Parts IAG	tennoring maintenance neip	mare
Dasic Advanced	Protocol Base	d VLAN Group Membership	m	
Configuration - VLAN Membership	Group ID Group Name	1 💌	ENT MEMBERS	
MAC Based VLAN	Port 1 2 3 4	5 6 7 8 9 10 11 12 13	14 15 16 17 10 19 20 21 22 23 24	
Configuration > Port DVLAN	25 26 27 2	28		

- b. In the Group ID list, select 1.
- c. Click the gray box under port 11. A check mark displays in the box.
- d. Click the Apply button.
- **4.** Add port 11 to the group vlan_ip.
 - a. Select Switching > VLAN > Advanced > Protocol Based VLAN Group Membership.

A screen similar to the following displays.

System Sv	itching		Ros	itin	2.	1	Qo	s	T	5	ocui	rity	1	N	loni	tori	ng	Ĩ	. N	lair	iten	an	08.	T	н	elp	1	Ind	eх
VEAN STP M	ditions!	Addre	ur J	able	a l	Ports	41.4	LAC	3																				
Basic	Pro	tocol	B	ase	d	/LA	N	Gro	oup	o N	1en	nbe	ersi	hip															
+ VLAN	P	rotoc	ol I	lase	ed V	LAN	G	nou	p M	em	ber	ship														8			
Configuration	Gros	ip 10				2																							
 VLAN Membership 	Gros	ap Nam					lan,	ip					1	URR	ENT /	MEM	icki												
 NAC Based VI AN 		then I																											
· Port PVID	Port	1 2		3 -	4 3	5 (1	8	9	10	11	12	13	14	15	16	17	18	19	26	1 21	1 23	23	3 2	4			
Configuration Port DVLAN		25 2	26 3	27 3	20	in a per				24		4							1.000	19.220		e	T II	¥. 00					

- b. In the Group ID list, select 2.
- c. Click the gray box under port 11. A check mark displays in the box.
- d. Click Apply.

Virtual VLANs: Create an IP Subnet–Based VLAN

In an IP subnet–based VLAN, all the end workstations in an IP subnet are assigned to the same VLAN. In this VLAN, users can move their workstations without reconfiguring their network addresses. IP subnet VLANs are based on Layer 3 information from packet headers. The switch makes use of the network-layer address (for example, the subnet address for TCP/IP networks) in determining VLAN membership. If a packet is untagged or priority tagged, the switch associates the packet with any matching IP subnet classification. If no IP subnet classification can be made, the packet is subjected to the normal VLAN classification rules of the switch. This IP subnet capability does not imply a *routing* function or that the

VLAN is routed. The IP subnet classification feature affects only the VLAN assignment of a packet. Appropriate 802.1Q VLAN configuration must exist in order for the packet to be switched.



Figure 2. IP subnet-based VLAN

CLI: Create an IP Subnet–Based VLAN

(Netgear	Switch)	#vlan database
(Netgear	Switch)	(Vlan)#vlan 2000
(Netgear	Switch)	(Vlan)#vlan association subnet 10.100.0.0 255.255.0.0 2000
(Netgear	Switch)	(Vlan)#exit

Create an IP subnet-based VLAN 2000.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/24
(Netgear Switch) (conf-if-range-1/0/1-1/0/24)# vlan participation include 2000
(Netgear Switch) (conf-if-range-1/0/1-1/0/24)#exit
(Netgear Switch) (Config)#
```

Assign all the ports to VLAN 2000.

```
(Netgear Switch) #show mac-addr-table vlan 2000
MAC Address Interface Status
------
00:00:24:58:F5:56 1/0/1 Learned
00:00:24:59:00:62 1/0/24 Learned
```

Web Interface: Create an IP Subnet–Based VLAN

- 1. Create VLAN 2000.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays.

System S	witching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP A	Aviticent	Address Table P	orta LAG					
Basic	VLA	N Configurati	on					
Advanced > state	R	eset						
Contraction .	Res	et Configuration			C			
 VLAN Membersh VLAN Statue 	- I	nternal VLAN Co	nfiguration				۲	
 Port PVID Configuration MAC Based VLA 	Inte Inte	mal YLAN Allocatio mal YLAN Allocatio	an Base an Policy		4093 C Asce	nding 🧭 Descending		
> IP Subnet Based ULAN	V	LAN Configuratio	on					
* Port DVIan		VLAN ID	VLAN	Name	V	LAN Type		
Configuration		2000				2.2		
VLAN Group	Г	1	Defau	it.	D	efault		
Configuration	T I	10			51	tatio		

- **b.** Enter the following information:
 - In the VLAN ID field, enter 2000.
 - In the VLAN Type list, select Static.
- c. Click Add.
- 2. Assign all the ports to VLAN 2000.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

System S	witching		Ros	iting	Т	00	5	3	Secu	rity	1Ĩ	N	oni	torir	ng:	13	Ma	inten	anc	8	1	Help	Inde
VLAN STP A	Aulticost 1	Add	ess T	able	Por	T i	LAG	t.															
Basic	VLA	NM	lem	bers	hip																		
- VLAN	V	LAN	Men	nbers	hip																	0	
Configuration	VLA	VLAN 10 2000 -								Ge	sup O	l geen	stion	5	Unt	ig A	ā,						
· VLAS Providents	VLA	N Nat	-										.u	NTAD	GED	POR	MIN	MERS.					
Port PVID	VLA	N Typ			Sta	se		;					1	TAGE	201	NG#1	MEM	MRS.					
Configuration	1	Unet	1																				
 MAC Based VLA IP Subnet Based VLAN 	N Port	1 U 25	2 U 26	3 4 U U 27 28	5	6 U	U 1	9 U U	10 U	11	12 U	13	14 U	15 U	16 U	17 I U	U	9 20	21	22 U	23 U	24 U	
> Port DVIan	_																						

- b. In the VLAN ID list, select 2000.
- **c.** Click **Unit 1**. The ports display.
- d. Click the gray box before Unit 1 until U displays.
- e. Click Apply.
- 3. Associate the IP subnet with VLAN 2000.
 - a. Select Switching > VLAN > Advanced > IP Subnet Based VLAN.

Desic	IP Subnet Based VL/	AN Configuration		
VLAN	IP Subnet Based VLAN	Configuration		0
Configuration	IP Address	Subnet Mask	VLAN ID	
VLAN Membership	10.100.0.0	255.255.0.0	2000	

- **b.** Enter the following information:
 - In the IP Address field, enter 10.100.0.0.
 - In the Subnet Mask field, enter 255.255.0.0.
 - In the VLAN (1 to 4093) field, enter 2000.
- c. Click Add.

Voice VLANs

The voice VLAN feature enables switch ports to carry voice traffic with defined priority to enable separation of voice and data traffic coming onto port. Voice VLAN ensures that the sound quality of an IP phone does not deteriorate when the data traffic on the port is high. Also, the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that clients attached to the network cannot initiate a direct attack on voice components.



Figure 3. Voice VLAN

The script in this section shows how to configure Voice VLAN and prioritize the voice traffic. Here the Voice VLAN mode is in VLAN ID 10.

CLI: Configure Voice VLAN and Prioritize Voice Traffic

1. Create VLAN 10.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#exit
```

2. Include the ports 1/0/1 and 1/0/2 in VLAN 10.

```
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan tagging 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
```

3. Configure Voice VLAN globally.

(Netgear Switch) (Config)# voice vlan

4. Configure Voice VLAN mode in the interface 1/0/2.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#voice vlan 10
(Netgear Switch) (Interface 1/0/2)#exit
```

5. Create the DiffServ class ClassVoiceVLAN.

(Netgear Switch) (Config)#class-map match-all ClassVoiceVLAN

6. Configure VLAN 10 as the matching criteria for the class.

(Netgear Switch) (Config-classmap)#match vlan 10

7. Create the DiffServ policy PolicyVoiceVLAN.

(Netgear Switch) (Config) #policy-map PolicyVoiceVLAN in

8. Map the policy and class and assign them to the higher-priority queue.

```
(Netgear Switch) (Config-policy-map)#class ClassVoiceVLAN
(Netgear Switch) (Config-policy-classmap)#assign-queue 3
(Netgear Switch) (Config-policy-classmap)#exit
```

9. Assign it to interfaces 1/0/1 and 1/0/2.

```
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)# service-policy in PolicyVoiceVLAN
```

Web Interface: Configure Voice VLAN and Prioritize Voice Traffic

- 1. Create VLAN 10.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays.

System	Switching	Lauting	QoS	Security	Monitoring	Maintenance	Help
VIAN STP	Multicost	Address Toble	Ports LAG	2			-
* Basic		VLAN Confi	guration				
+ VLAN		Reset					٢
Advanced		Reset Configur	ation		2		
	7-4	Internal VI	AN Config	ration			
		Internal VLAN	Allocation Ba	6e	4093		
		Internal VLAN	Allocation Po	ðcy.	C Ascending	Descending	
		VLAN Conf	iguration				
		VLAN ID	VLAN Nam	•	VLAN Type	Make Stati	c
						Dirable -	
L		13 1	Default		Default	Disable	

- **b.** In the VLAN ID field, enter 10.
- c. In the VLAN Name field, enter Voice VLAN.
- d. Click Add. A screen similar to the following displays.

System	Switching	Lauring	QeS	Security	Monitoring	Maintenance	Help
VIAN STP	Multicost	Address Toble	Forts LAG				-
* Basic		VLAN Confid	guration				
+ VCAN		Reset					10
Advanced		Reset Configura	ation		2		
	1-1	Internal VL	AN Configu	ration			
		Internal VLAN	Allocation Ba	6e	4093		
		Internal VLAN	Allocation Pol	licy	C Ascending	Descending	
		VLAN Confi	guration				
		VLAN ID	VLAN Name		VLAN Type	Make Stati	·
						Dirable -	
		23 1	Default	10. In 19	Default	Disable	-

- 2. Include the ports 1/0/1 and 1/0/2 in VLAN 10.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

System	Switching	Routing	QoS	Security	Monitoring	Maintenana	e Help
VEAN STP	Multicost	Address Table F	orts LAG				
Basic		VLAN Memb	ership				
> VLAN		VLAN Memi	bership				Ū
Configurati	on	VLAN 1D	1 -		Group	Operation 1	Intag All 👻
+ VLAN Herri	verstigt ;	VLAN Name	Default		UNTA	OGED PORT MEMAE	15
> VLAN Statu	5	VLAN Type	Default		IAC	GED PORT MEMBER	1
Configurati	on la	• Unit 1					

- b. In the VLAN Membership table, in the VLAN ID list, select 10.
- **c.** Select Port 1 and Port 2 as tagged.

Address 1	able							. in	e 1		mo	nite	PLAN I	9		(a)	nie	nan	cu.			erb	
]_₽	orts	T a	AG																		
VLAN	Me	mb	ers	ship	2																		
VLA	IN M	emt	ers	hip	i .																		
VLAN I	0			10									G	oup	Oper	atie	on		Unt	ag A	8		
VLAN P	varme			Vo	ceVi	LAN	1							INTA	GGED	10	£7.34	EMS	ERS.				-
VLANT	ype			Sta	tic									JAC	GED	i Oil	IT ME	EMBE	85				
- 0	it tie																						
Port 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	2
2	5 26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	61	42	43	44	45	46	47	4
4	9 50	51	52				1011				1011					-	101	103					
	VLAN VLAN VLAN VLAN Port 1 2 4	VLAN Me VLAN M VLAN 10 VLAN Name VLAN Type - Unit 1 Port 1 2 T T 25 26 49 50	VLAN Memb VLAN Memb VLAN ID VLAN Name VLAN Type - Unit I Port I 2 3 T T 25 26 27 49 50 51	VLAN Members VLAN Members VLAN ID VLAN Name VLAN Type - Unet I Port I 2 3 4 T T 25 26 27 28 49 50 51 52	VLAN Membership VLAN Membership VLAN IO 10 VLAN Name Vio VLAN Type Sto • Unet I 2 3 4 Port I 2 3 4 5 T T 25 26 27 28 29 49 50 51 52 3 5 3	VLAN Membership VLAN Membership VLAN 10 10 • VLAN Name VoiceV VLAN Type Static • Unet 1 Port 1 2 3 4 5 6 T 25 26 27 28 29 30 49 50 51 52	VLAN Membership VLAN Membership VLAN Name VLAN Name VLAN Type Static - Unit 1 Port 1 2 3 4 5 6 7 T T 25 26 27 28 29 30 31 49 50 51 52	VLAN Membership VLAN Membership VLAN 10 10 V VLAN 10 10 V VLAN 10 Static - Unit 1 Port 1 2 3 4 5 6 7 8 T T 25 26 27 28 29 30 31 32 49 50 51 52	VLAN Membership VLAN Membership VLAN 10 10 • VLAN Name VOICeVLAN VLAN Type 5 thet 1 Port 1 2 3 4 5 6 7 8 9 T 25 26 27 28 29 30 31 32 33 49 50 51 52	VLAN Membership VLAN Membership VLAN 10 10 VoiceVLAN VLAN Type Static - Unit 1 Port 1 2 3 4 5 6 7 8 9 10 T 25 26 27 26 29 30 31 32 33 34 49 50 51 52	VLAN Membership VLAN Membership VLAN 10 10 VOICeVLAN VLAN Type Static - Unit 1 Port 1 2 3 4 5 6 7 8 9 10 11 T T 25 26 27 28 29 30 31 32 33 34 35 49 50 51 52	VLAN Membership VLAN Membership VLAN ID 10 - VLAN Name VoiceVLAN VLAN Type Static - Unit 1 Port 1 2 3 4 5 6 7 8 9 10 11 12 T T 25 26 27 28 29 30 31 32 33 34 35 36 49 50 51 52	VLAN Membership VLAN Membership VLAN 10 10 - VLAN 10 10 - VIAN Type Static - that 1 Port 1 2 3 4 5 6 7 8 9 10 11 12 13 T T 25 26 27 28 29 30 31 32 33 34 35 36 37 49 50 51 52	VLAN Membership VLAN Membership VLAN 10 10 C VLAN Name VOICEVLAN VLAN Type Static - Unit 1 Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 T 25 26 27 28 29 30 31 32 33 34 35 36 37 38 49 50 51 52	VLAN Membership VLAN Membership VLAN 10 10 Crowp VLAN Name VOICEVLAN VLAN Type Static - Unet 1 Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 T 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 49 50 51 52	VLAN Membership VLAN Membership VLAN 10 10 Crowp Oper VLAN Name VIAN Name VIAN Type Static TADGID Cover VAN VIAN Type Static TADGID Crowp Oper VIAN Type Static TADGID Crowp Oper VIAN Type Static TADGID Crowp Oper TADGID Crowp Oper VIAN Type Static TADGID Crowp Oper TADGID Crowp Oper Crowp Oper Crowp Oper TADGID Crowp Oper Crowp Oper TADGID Crowp Oper Crowp Oper C	VLAN Membership VLAN Membership VLAN 10 10 0 00000000000000000000000000000	VLAN Membership VLAN Membership VLAN Membership VLAN Nome 10 Croup Operation VLAN Name Voice/VLAN Untractor point and the point and	VLAN Membership VLAN Membership VLAN 10 10 € crosp Operation VLAN Name VoiceVLAN UNRACID Foot MEMA VLAN type Stabic Tadded Foot MEMA * Unix Unix Tadded Foot MEMA Port 1 2 3 4 5 6 7 9 10 11 12 14 15 16 17 18 19 T T Z 2 66 7 29 10 11 12 13 14 15 16 17 18 19 T T Z 2 66 7 29 10 11 12 13 14 15 16 17 18 19 49 50 51 52 2 33 34 35 36 37 39 40 41 42 43	VLAN Membership VLAN Membership VLAN Nome 10 0 Crowp Operation Unit VLAN Name VoiceVLAN UnitAction Unit Unit VLAN Name VoiceVLAN UnitAction Total Membership UnitAction UnitAction VLAN Name VoiceVLAN UnitAction Total Membership Total Membership UnitAction UnitAction Point I 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 10 19 20 ZS 26 27 28 29 3 3 3 3 3	VLAN Membership VLAN Membership VLAN No 10 20 Crowp Operation United A VLAN No 10 20 Crowp Operation United A VLAN Nome VoiceVLAN United A United A VLAN Name VoiceVLAN United A United A Point 1 2 3 4 5 6 7 9 10 11 12 14 15 16 17 18 19 20 21 25 26 27 28 29 3 34 35 36 37 38 39 40 41 42 43 44 45 49	VLAN Membership VLAN Membership VLAN No 10 0 Crowp Operation Untag All VLAN Nome VoiceVLAN Untag CD POET MEMAERS Untag All VLAN Nyme Static 7 Addition 20 at 22 at 23 at 23 at 25 a6 37 36 39 40 41 42 43 44 45 46 49 50 51 52	VLAN Membership VLAN Membership VLAN 10 10 ▼ VLAN Nome 10 ▼ VLAN Nome VoiceVLAN VLAN Nype Static * Unix Nype 5 table * Unix Nype 5 tabl

- d. Click Apply.
- 3. Configure Voice VLAN globally.
 - a. Select Switching > VLAN > Advanced > Voice VLAN Configuration.

System	Switching		Routing	QoS Sec	urity Monitoring	Maintenan	ce Help	Index
VLAN STP	Multicost	Addre	na Table Po	orta LAG				
Basic		Voi	ce VLAN	Configuration				
* Advanced			voice VLAN	Global Admin				_
 VLAN Configuratio 	0	Ade	min Mode	Barren and and and		Disable 🔿 En	able	_
+ VLAN Memb	ership							
> VLAN Status	Real Property lies	12	Voice VLAN	Configuration				
Configuratio	6.6 M	13	All		Go To Interface		0	
+ MAC Based	VLAN		Interface	Interface Mode	Value	CoS Override Mode	DSCP Value	Ope
VLAN				- 11		-	1	
> Port DVLAN	6.6	10	1/0/1	Disable	0	Disable	0	Dise
Configuratio	n.		1/0/2	Disable	0	Disable	0	Disa
VLAN Group		四	1/0/3	Diseble	0	Disable	0	Dise
Configuratio	n:	0	1/0/4	Disable	0	Disable	0	Disa
» Protocol Bas	ed	13	1/0/5	Disable	0	Disable	0	Disa
VLAN Group		173	1/0/6	Disable	0	Disable	0	Dist
Membership		10	1/0/7	Disable	0	Disable	0	Disa
		E	1/0/8	Disable	0	Disable	0	Dist
> GARP Switch	h.	0	1/0/9	Disable	0	Disable	0	Dist

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply.

System Switching		Routing	QoS Sec	urity Monitorin	g Maintenar	ice Help	Index
VLAN STP Multicast	Addre	ess Table P	orts LAG				
Basic	Voi	ce VLAN	Configuration				
> VI AN	1	Voice VLAN	Global Admin				
Configuration	Ade	min Mode			🐑 Disable 🔮 En	able	
> VLAN Membership							
> VLAN Status		Voice VLAN	Configuration				
> Port PVID	1	All		Go To Interface		0	
MAC Based VLAN IP Subnet Based		Interface	Interface Mode	Value	CoS Override Mode	DSCP Value	Operationa State
VLAN				1	· ·	1	
> Port DVLAN	175	1/0/1	Disable	0	Disable	0	Disable
Configuration	173	1/0/2	Disable	0	Disable	0	Disable
> Protocol Based	175	1/0/3	Disable	0	Disable	0	Disable
Configuration	121	1/0/4	Disable	0	Disable	0	Disable
> Protocol Based	21	1/0/5	Disable	0	Disable	0	Disable
VLAN Group	1775	1/0/6	Disable	0	Disable	0	Disable
Membership	125	1/0/7	Disable	0	Disable	0	Disable
* Verse VLAN	171	1/0/8	Disable	0	Disable	0	Disable
Canfiguration	275	1/0/9	Disable	0	Disable	0	Disable
a construction	In succession	ALCONOM	design of the second se	100	2 Key Dillow	100	hand a second second

- 4. Configure Voice VLAN mode in the interface 1/0/2.
 - a. Select Switching > VLAN > Advanced > Voice VLAN Configuration.
 - b. Select the 1/0/2 check box.
 - c. In the Interface Mode list, select VLAN ID.
 - d. In the Value field, enter 10.

System	Switching	Routing	QoS Sec	urity Monitoring	Maintenar	ice Help	Index
VLAN STP	Multicost	Address Table	Ports LAG				
Basic		Voice VLA	N Configuration				
Advanted		Voice VL	AN Global Admin				
 VLAN Configuration 		Admin Mode			🔿 Disable 🚇 En	able	
 VLAN Member VLAN Status 	rship	Voice VL	AN Configuration				10
Port PVID Configuration		I All		Go To Interface	10	0	
 MAC Based V IP Subnet Ba 	LAN	Interfac	ce Interface Node	Value	CoS Override Mode	DSCP Value	Operational State
VLAN	885 C.	1/0/2	VLAN ID 👻	10	Disable 👻	d	Disable
* Port DVLAN		1/0/1	Disable	0	Disable	0	Disable
Configuration	ar	2 1/0/2	Disable	0	Disable	0	Disable
LI AN Conus	9	1/0/3	Disable	0	Disable	0	Disable

- e. Click Apply.
- 5. Create the DiffServ class ClassVoiceVLAN.
 - a. Select QoS > Advanced > DiffServ > Class Configuration.
| System | Switching | Routing | QoS | Security | Monitoring | Maintenance | Help | | |
|--------------|-----------|------------|-----|------------|------------|-------------|------|--|--|
| Co5 DillSe | R. | | | | | | | | |
| Diffserv Wiz | ard | Class Name | | | | | | | |
| Auto VoIP | | Class Name | | | | | | | |
| Advanced | | Class Non | ne | Class Type | | | | | |
| > DiffServ | | | | | • | | | | |
| Configuratio | ND : | | | | | | | | |
| Carriqueeto | | | | | | | | | |
| > IPv6 Class | | | | | | | | | |

- b. In the Class Name field, enter ClassVoiceVLAN.
- c. In the Class Type list, select All.

A screen similar to the following displays.

System	Switching	Routing	Qo5	Security	Monitoring	Maintenance	Help
CoS DillS	erv:		301 D	-			
Diffserv Wi	zard	Class Name					
Auto VoIP		Class Name	£2				đ
Advanced		Class Nan	ne		lass Type		
> DiffServ		ClassVoio	eVLAN		AR 👻		
Configurati	ion			10.73			
	inter a						
► IPv6 Class							
Configurati	ion						

- **d.** Click **Add**. The Class Name screen displays, as shown in the next step in this procedure.
- 6. Configure matching criteria for the class as VLAN 10.
 - a. Select QoS > DiffServ > Advanced > Class Configuration.

A screen similar to the following displays.

System Sw	tching	Routing	QoS	Security	Monitoring	Maintenance	Help				
CoS DiffServ											
Diffserv Wizard	c	lass Name									
Auto VoIP Basic	1 6	Class Name									
Advanced		Class Nan	ne	Class Type							
▶ DiffServ					•						
Configuration Class Configuration > IPv6 Class	E	ClassVoice	VLAN	4	ár:						

b. Click the class **ClassVoiceVLAN**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
CoS DillServ							
> Diffserv Wizar	a i	Class Name					
Auto VoIP		Class Name					0
Advanced		Class Nam	10	· •	lass Type		
> DiffServ					-		
Configuration							
Carifiguerelium							
> IPv6 Class							

- c. In the DiffServ Class Configuration table, select VLAN.
- **d.** In the VLAN ID field, enter 10.

A screen similar to the following displays.

System Switch	ing Routing	GoS Security	Monitoring	Maintenance	Help
CoS DillSore	anne an				
Diffserv Wizard	Class Configura	ition			
Auto VoIP	Class Informati	on			1
Advanced > DiffServ	Class Name Class Type		ClassVoyce/L/	411	
Configuration	DiffServ Class	Configuration			
IPv6 Class Configuration	 Match Every Reference Class 	Any -			
 Policy Configuration Service Interface 	Class Of Service	0 - 10 (0 to 409	5)		
Configuration	Ethernet Type	Appletalk	+ (600	to ffff hesi)	

e. Click Apply.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
CoS DillSo	ñi .	المحيدية					
Diffserv Wiz	ard	Class Config	uration				
Auto VoIP		Class Inform	nation				(
Advanced > DiffServ		tlass Name Class Type	angu ya ka s		ClassVoiceVC/ All	01	
Configuratio	in:	DiffServ Cla	ss Configu	ration			
 IPv6 Class Configuratio Policy Configuratio 	n n	 Match Every Reference Cl Class Of Service VLAN 	lass rice	07 =			
 Service Inte Configuratio 	erface 20	C Ethernet Typ		ppletalk -	(600)	te Miliked	

- 7. Create the DiffServ policy PolicyVoiceVLAN.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
CoS DiffServ	āĽ						
Diffserv Wizar	-d F	Policy Confi	guration				
Auto VoIP		Policy Conf	iguration				
Advanced		Policy Na	me	Policy Type	Men	ber Class	
* DiffServ						-	
Configuration							
Configuration							
* IPv6 Class							
Configuration							
Critifiguration	-						
> Service Interf	ace						
Configuration							

- b. In the Policy Name field, enter PolicyVoiceVLAN.
- c. In the Policy Type list, select In.
- d. In the Member Class list, select ClassVoiceVLAN.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help			
CoS Diff5										
Diffserv Wi	zard P	olicy Confic	uration							
Auto VoIP	1	Policy Configuration								
Advanced		Policy Nar	ne	Palicy Type	Men	iber Class				
► DiffServ		PolicyVoic	evlan	In 🔹	Cla	ssVoiceVLAN -				
Class Configurati IPv6 Class Configurati Today Configurati	on on									
 Service Int Configuration 	erface. 90									

e. Click Add.

The Policy Configuration screen displays, as shown in the next step in this procedure.

- 8. Map the policy and class and assign them to the higher-priority queue.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System Swite	hing Routing	Qo5	Security	Monitoring	Maintenance	Help	
CoS DiffServ							
Diffsery Wizard	Policy Con	liquration					
Auto YolP	Policy Co	nfiguration					
Advanced	Policy N	ame	Policy Type	Hem	Hember Class		
> DiffServ			-		-		
Configuration	E Policy.Voi	COVLAN	In	Class	VoiceVLAN		
 Class Configuration IPv6 Class 							
Configuration							
» Service Interface							

b. Click the **Policy PolicyVoiceVLAN**.

A screen similar to the following displays.

ing Routing	GoS	Security	Monitoring	Maintenance	Help	index		
Policy Class	s Configur	ation						
Policy Name Policy Type Member Class	Name			ndicy Voice VEAN mini Class Voice VEAN				
Policy Attribute								
Policy Atribut	Assign 1 Drop Mark IP Mark IP Mark IP Mark IP	Queue 0 COS 0 Precedence 0 DSCP af1	• • •					
	Policy Class Class Info Policy Name Policy Type Hember Class Policy Attribute	Policy Class Configur Class Information Policy Name Policy Type Hember Class Name Policy Attribute Policy Attribute Policy Attribute Nark IP Nark IP	Routing Cos Security Policy Class Configuration Class Information Policy Name Policy Type Member (Lass Name Policy Attribute Policy Attribute Policy Attribute Policy Attribute Orop Hark IP DOS Hark IP DOS Simple Policy Simple Policy	Routing Cos Security Monitoring Policy Class Configuration Class Information Policy Name Policy Name Policy Type Member (Lass Name Policy Attribute Policy Attribute Policy Attribute Policy Attribute Orop Mark IP DSCP Mark IP DSCP Simple Policy	Ing Routing Gos Security Monitoring Maintenance Policy Class Configuration Class Information Policy Name Policy Name Policy Name Policy Vice VLAN Policy Type In Member Class Name Class Voce VLAN Policy Attribute Policy Attribute Policy Attribute Assign Queue 0 • Ø Mark IP OSS 0 • Ø Mark IP DSCP #11 + Ø Single Policy	Routing Cost Security Monitoring Maintenance Help Policy Class Configuration Class Information Policy Name Policy Name Policy Name Policy Name Policy Volce VLAN Policy Name Policy Name Policy Type In In Member Class Name Class Vone VLAN Policy Attribute Policy Attribute Policy Attribute Assign Queue 0 * Orop Mark IP 005 0 * Mark IP DSCP @fill + O Simple Policy		

c. In the field next to the Assign Queue radio button, select 3.

A screen similar to the following displays.

System Switchi	ng Routing Qo	5 Security	Monitoring	Maintenance	Help	Index		
CoS DillServ								
Diffsery Wizard	Policy Class Confi	guration						
Auto YoIP	Class Information							
Advanced > DiffServ Configuration	Policy Name Policy Type Member Class Name			PuticyUpiceVLAN Ta CrassVoiceVLAN				
Configuration	Policy Attribute							
Configuration	Policy Abribute 🧕 Ass 💮 Dro 💮 Mar	ngan Queruer 3 - nga 4x 1P COS 0 -	1					

- d. Click Apply.
- 9. Assign it to interfaces 1/0/1 and 1/0/2.
 - a. Select QoS > DiffServ > Advanced > Service Interface Configuration.

System	Switching	Routing	QoS	Security	Monito	oring M	aintenance	Help
CoS DillSe	IN L							
Diffserv Wi	zard	Service Inte	rface Co	nfiguration				
Auto VoIP	and a	Service Int	erface Con	figuration				
Advanced		L All		Go To Interfac	•	00	l	
* DiffServ		Interface	8. T	Policy Name		Direction	Operationa	l Status
Configuration Class	on				*	Concession of the		
Configuratio	in	1/0/1				In		
+ IPv6 Class		1/0/2				In		
Configuratio	on	1/0/3				In		
> Policy		1/0/4				In		
Configuratio	on	1/0/5				In		
Contraction		1/0/6				In		
a Service Sta	tistics	1/0/7				In		

- **b.** Select the check boxes for Interfaces 1/0/1 and 1/0/2.
- c. Set the Policy Name field as PolicyVoiceVLAN.

System Swi	tching	Routing	GoS	Security	Monitori	ing Ma	aintenance	Help
CoS DiffServ								
Diffserv Wizard	s	ervice Inte	rface Co	nfiguration				
Auto VoIP	6	Service Int	erface Con	figuration				
Advanced		All		Go To Interface	Š	60		
> DiffServ		Interface		Policy Name		Direction	Operationa	l Status
Configuration		1		PolicyVoiceVLA	w .			
 Class Confiduration 		/0/I				In		
+ IPv6 Class		1 1/0/2				In		
Configuration	1.2	1/0/3				In		
* Policy	1 12	1/0/4				In		
Configuration	1	1/0/5				In		
	12	1/0/6				In		
· Service Statistics	12	1/0/7				In		
	2 18	- 40 M				1425		

d. Click Apply.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Ma	intenance	Help
CoS DillServ								
Diffserv Wizard	1 3	Service Inte	rface Co	nfiguration				
Auto VoIP		Service Int	erface Con	figuration				
Advanced		1 All		Go To Interface	4	60		
> DiffServ		Interface		Policy Name	Dir	ection	Operationa	Status
Configuration					· ·			
Configuration		1/0/1		PolicyVoiceVLA	N In	1	Up	
» IPv6 Class		1/0/2		PolicyVoiceVLA	N In		Up	
Configuration		1/0/3			In			
» Policy	1	1/0/4			In			
Configuration	-	1/0/5			In			
Carlingation		1/0/6			In			
» Service Statisti	cs	1/0/7			In			

Private VLANs

The Private VLANs feature separates a regular VLAN domain into two or more sub domains. Each sub domain is defined (represented) by a primary VLAN and a secondary VLAN. The primary VLAN ID is the same for all sub domains that belong to a private VLAN. The secondary VLAN ID differentiates sub domains from each other and provides Layer 2 isolation between ports of the same private VLAN.

There are three types of VLAN within a private VLAN:

- **Primary VLAN**. Forwards the traffic from the promiscuous ports to isolated ports, community ports, and other promiscuous ports in the same private VLAN. Only one primary VLAN can be configured per private VLAN. All ports within a private VLAN share the same primary VLAN.
- **Community VLAN**. A secondary VLAN that forwards traffic between ports which belong to the same community and to the promiscuous ports. There can be multiple community VLANs per private VLAN.
- **Isolated VLAN**. A secondary VLAN that carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN.

There are three types of port designation within a private VLAN:

- **Promiscuous port**. Belongs to a primary VLAN and can communicate with all interfaces in the private VLAN, including other promiscuous ports, community ports, and isolated ports.
- **Community port**. Communicates with other community ports and promiscuous ports.
- **Isolated port**. Communicates only with promiscuous ports.

The following figure illustrates that Private VLANs can be extended across multiple switches through inter-switch/stack links that transport primary, community, and isolated VLANs between devices.



Figure 4. Private VLANs

The following figure illustrates the private VLAN traffic flow. Five ports A, B, C, D, and E make up a private VLAN. Port A is a promiscuous port which is associated with the primary VLAN 100. Ports B and C are the host ports which belong to the isolated VLAN 101. Ports D and E are the community ports which are associated with community VLAN 102. Port F is the inter-switch/stack link. It is configured to transmit VLANs 100, 101 and 102. Colored arrows represent possible packet flow paths in the private VLAN domain.



Figure 5. Packet flow within a Private VLAN domain

Assign Private-VLAN Types (Primary, Isolated, Community)

The example is shown as CLI commands and as a Web interface procedure.

CLI: Assign Private-VLAN Type (Primary, Isolated, Community)

Use the following commands to assign VLAN 100 to primary VLAN, VLAN 101 to isolated VLAN, and VLAN 102 to community VLAN.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#vlan 100
(Netgear Switch) (Config)(Vlan) #private-vlan primary
(Netgear Switch) (Config)(Vlan) #exit
(Netgear Switch) (Config)(Vlan) #private-vlan isolated
(Netgear Switch) (Config)(Vlan) #exit
(Netgear Switch) (Config)#vlan 102
(Netgear Switch) (Config)(Vlan) #private-vlan community
(Netgear Switch) (Config)(Vlan) #private-vlan community
(Netgear Switch) (Config)(Vlan) #end
```

Web Interface: Assign Private-VLAN Type (Primary, Isolated, Community)

- 1. Create VLAN 10.
 - a. Select Security > Traffic Control > Private VLAN > Private VLAN Type Configuration. A screen similar to the following displays.

e faith	mg	nooring	and the second s	moun
Management Security	Access	Port Authent	icotion Traffic Control ACL	
MAC Filter	Pri	vate VLA	AN Type Configuration	
Port Security	1	Private VL	AN Type Configuration	6
Protected Port		VLAN ID	Private VLAN Type	
Private Vian		100	Primary .	
· Privata Viati Type	873	1	Unconfigured	
- Pourte Man	10	2	Unconfigured	
Association	100	100	Unconfigured	
Configuration		101	Unconfigured	
Private Vlan Port	10	102	Unconfigured	

- **b.** Under **Private VLAN Type Configuration**, select the **VLAN ID 100** check box. Now 100 appears in the interface field at the top.
- c. In the Private VLAN Type field, select Primary from the pull-down menu.
- d. Click Apply to save the settings
- 2. Assign VLAN 101 as an isolated VLAN.
 - a. Select Security > Traffic Control > Private VLAN > Private VLAN Type Configuration.

A screen similar to the following displays.

Management Security	Access	Port Authent	ication Traffic Control ACL	
MAC Filter	Pri	vate VL/	AN Type Configuration	
Port Security	650	Private VL	AN Type Configuration	2)-
Protected Port		VLAN ID	Private VLAN Type	
Private Vian		101	Isolated -	
- Privata Vian Type -	23	1	Unconfigured	
Configuration	0	2	Unconfigured	11
Association	10	100	Primary	
Configuration	122	101	Unconfigured	
* Private Vlan Port	10	102	Unconfigured	

b. Under Private VLAN Type Configuration, select the VLAN ID 101 check box.
 Now 101 appears in the interface field at the top.

- c. In the Private VLAN Type field, select Isolated from the pull-down menu.
- d. Click **Apply** to save the settings
- 3. Assign VLAN 102 to community VLAN.
 - a. Select Security > Traffic Control > Private VLAN > Private VLAN Type Configuration.

Monogement Security Acce		
	ss Port Authen	tication Traffic Control Control ACL
MAC Filter	Private VL	AN Type Configuration
Port Security	Private VI	AN Type Configuration
Protected Port	VLAN ID	Private VLAN Type
+ Private Vian	102	Community .
e-Private Vien Type	1	Unconfigured
- Douate Man	2	Unconfigured
Association	100	Primary
Configuration	101	Isolated
» Private Vlan Port	102	Unconfigured

- **b.** Under **Private VLAN Type Configuration**, select the **VLAN ID 102** check box. Now 102 appears in the interface field at the top.
- c. In the **Private VLAN Type** field, select **Community** from the pull-down menu.
- d. Click Apply to save the settings.

Configure Private-VLAN Association

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Private-VLAN Association

Use the following commands to associate VLAN 101-102 (secondary VLAN) to VLAN 100 (primary VLAN).

```
(Netgear Switch) #config
(Netgear Switch) (Config)#vlan 100
(Netgear Switch) (Config)(Vlan) #private-vlan association 101-102
(Netgear Switch) (Config)(Vlan) #end
```

Web Interface: Configure Private-VLAN Association

- 1. Associate VLAN 101-102 (secondary VLAN) to VLAN 100 (primary VLAN).
 - a. Select Security > Traffic Control > Private VLAN > Private VLAN Association Configuration.

Monogement Security Acc	ass Port Authentico	tion Traffic Control Contr	al ACL		
MAC Filter	Private VLA	N Association Config	uration		
Port Security Private Group	Private VL	AN Association			۲
Protected Port	Primary VLAN	Secondary VLAN(s)	Isolated VLAN	Community VLAN(s)	
Private Vian	100 -	101-102			
 Private Vian Type Configuration 	100			Ť	
Resociation					
Climbyuracion					
Configuration	101	Isolated			
 Private Vlan Port Mode Configuration 	102	Unconfigured			

- b. Under Private VLAN Association Configuration, select the VLAN ID 100.
- c. In the Secondary VLAN(s) field, type 101-102.
- d. Click Apply to save the settings.

Configure Private-VLAN Port Mode (Promiscuous, Host)

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Private-VLAN Port Mode (Promiscuous, Host)

Use the following commands to assign port 1/0/1 to promiscuous port mode and ports 1/0/2-1/0/5 to host port mode.

(Netgear Switc	h) #config	
(Netgear Switc	h) (Config)#i	nterface 1/0/1
(Netgear Switc	h) (Interface	e 1/0/1)#switchport mode private-vlan promiscuous
(Netgear Switc	h) (Interface	e 1/0/1)#exit
(Netgear Switc	h) (Config)#i	nterface 1/0/2-1/0/5
(Netgear Switc	h) (Interface	1/0/2-1/0/5)#switchport mode private-vlan host
(Netgear Switc	h) (Interface	1/0/2-1/0/5)#end

Web Interface: Configure Private-VLAN Port Mode (Promiscuous, Host)

- 1. Configure port 1/0/1 to promiscuous port mode.
 - a. Select Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration.

Management Security A	cess Port Auth	entication Traffic Con	itral Control ACL	
MAC Filter	Private	Vlan Port Mode (Configuration	
Port Security	Private	e Vian Port Mode Co	nfiguration	۲
Protected Port	1 LAGS	All	Go To Interface	
Private Vian	Inter	face Port Vlan Mod	e	
Private Vian Type	1/0/1	Promiscuous	•	
Private Vian	V 1/0/1	General		
Association	1/0/2	General		
Configuration	1/0/3	General		
Provable vitan Port	1/0/4	General		
Rode Coolsperateon	1/0/5	General		

b. Under **Private VLAN Port Mode Configuration**, select the 1/0/1 interface check box.

Now 1/0/1 appears in the **Interface** field at the top.

- c. In the Port VLAN Mode field, select Promiscuous from the pull-down menu.
- d. Click Apply to save the settings.
- 2. Configure ports 1/0/2-1/0/5 to host port mode.
 - a. Select Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration.

and the second second second					and the second second			
Monagement Securit	y Access	P	ort Authenticat	ion Troffic	Control C	ontrol ACL		
MAC Filter	1	Priv	vate Vlan	Port Mod	de Config	uration		
Port Security Private Group		1	Private Vlar	Port Mode	• Configurat	ion		20
Protected Port		1	LAGS All		Go	To Interface	GO	
Private Vian			Interface	Port Vlan	Hode			
 Private Vian Type Configuration 				Host				
- Frivate Vlan		0	1/0/1	Promiscuou	15			
Association		W.	1/0/2	General				
Configuration		12	1/0/3	General				
· Frivate slies Port			1/0/4	General				
- Sciusta Man Host	145 E	W.	1/0/5	General				
· Drivate Ulan Host		-	and a state of the					

- **b.** Under **Private VLAN Port Mode Configuration**, select the 1/0/2 to 1/0/5 interface check box.
- c. In the Port VLAN Mode field, select Host from the pull-down menu.
- d. Click Apply to save the settings.

Configure Private-VLAN Host Ports

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Private-VLAN Host Ports

Use the following commands to associate isolated ports 1/0/2-1/0/3 to a private-VLAN (primary=100, secondary=101). Community ports 1/0/4-1/0/5 to a private-VLAN (primary=100, secondary=102).

(Netgear	Switch)	#config
(Netgear	Switch)	(Config)#interface 1/0/2-1/0/3
(Netgear 100 101	Switch)	(Interface 1/0/2-1/0/3)#switchport private-vlan host-association
(Netgear	Switch)	(Interface 1/0/2-1/0/3)#exit
(Netgear	Switch)	(Config)#interface 1/0/4-1/0/5
(Netgear 100 102	Switch)	(Interface 1/0/4-1/0/5)#switchport private-vlan host-association
(Netgear	Switch)	(Interface 1/0/4-1/0/5)#end

Web Interface: Assign Private-VLAN Port Host Ports

- 1. Associate isolated ports 1/0/2-1/0/3 to a private-VLAN (primary=100, secondary=101).
 - a. Select Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration.

System Swite	hing	Routing	Qo5 Security	Monitoring Maint	tenance Help Inde
Management Security	Access	Port Authenticat	ion Traffic Control Co	ntrol ACL	
MAC Filter	F	Private VLA	N Host Interface C	onfiguration	
Port Security		Private VLA	N Host Interface Confi	guration	
Protected Port		LAGS All	Go	To Interface	00
Private Vian Private Vian Type		Interface	Host Primary VLAN (2 to 4093)	Host Secondary VLAN (2 to 4093)	Operational VLAN(s)
Configuration			100	101	
 Private Vlan 		1/0/1	0	0	1
Configuration		2 1/0/2	0	0	
+ Private Vlan Port		2 s/0/3	0	0	
Mode Configuration		1/0/4	0	0	
- Stovaka Vlav. rmm;	10	1/0/5	0	0	1
Interface	1	1/0/6	0	0	
Contextables		T	0	1.0	A

- **b.** Under **Private VLAN Host Interface Configuration**, select the 1/0/2 and 1/0/3 interface check box.
- c. In the Host Primary VLAN field, enter 100.

- d. In the Host Secondary VLAN field, enter 101.
- e. Click Apply to save the settings.
- 2. Associate isolated ports 1/0/4-1/0/5 to a private-VLAN (primary=100, secondary=102).
 - a. Select Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration.

System Swit	ching	Routing	QoS Security	Monitoring Maint	enance Help Inde			
Monogement Security	Access	Port Authenticat	ion Traffic Control Co	ntrol ACL				
AC Filter	P	rivate VLA	N Host Interface Co	onfiguration				
Port Security		Private VLAN Host Interface Configuration						
Protected Port	1	LAGS All	Gol	o Interface	00			
Private Vian Private Vian Type		Interface	Host Primary VLAN (2 to 4093)	Host Secondary VLAN (2 to 4093)	Operational VLAN(s)			
Configuration			100	102				
Private Vian	1	1/0/1	0	0				
Configuration	1	1/0/2	100	101	100-101			
Private Vian Port		1/0/3	100	101	100-101			
Mode Configuration		2 1/0/4	0	0				
		1/0/5	0	0				
Treataon		1/0/6	0	0				
	10	1/0/7	0	0				

- **b.** Under **Private VLAN Host Interface Configuration**, select the 1/0/4 and 1/0/5 interface check box.
- c. In the Host Primary VLAN field, enter 100.
- d. In the Host Secondary VLAN field, enter 102.
- e. Click Apply to save the settings.

Map Private-VLAN Promiscuous Port

The example is shown as CLI commands and as a Web interface procedure.

CLI: Map Private-VLAN Promiscuous Port

Use the following commands to map private-VLAN promiscuous port 1/0/1 to a primary VLAN (100) and to secondary VLANs (101-102).

(Netgear S	Switch)	#config
(Netgear S	Switch)	(Config)#interface 1/0/1
(Netgear S	Switch)	(Interface 1/0/1)#switchport private-vlan mapping 100 101-102
(Netgear S	Switch)	(Interface 1/0/1)#end

Web Interface: Map Private-VLAN Promiscuous Port

- 1. Map private-VLAN promiscuous port 1/0/1 to a primary VLAN (100) and to selected secondary VLANs (101-102).
 - a. Select Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration.

System Swit	ching	Routing	GoS Security M	onitoring Maintenance	Help Index
Management Security	Access	Port Authentica	tion Traffic Control Control	ACL	
HAC Filter	P	rivate VLA	N Promiscuous Interfac	e Configuration	
Port Security	1.1	Private VL/	AN Promiscuous Interface Co	sfiguration	0
Protected Port		LAGS All	Go	To Interface 00	
Private Vian Type		Interface	Promiscuous Primary VLAN (2 to 4093)	Promiscuous Secondary VLAN(s) Range[2-4093]	Operational VLAN(s)
Configuration		1/0/1	100	101-102	
* Private Vian		/ 1/0/1	0		
Configuration	1	1/0/2	0		100+101
* Private Vian Port	1 1	1/0/3	0		100-101
Node Configuration	1	1/0/4	0		100,102
* Private Vlan Host	1	1/0/5	0		100,102
Interface		1/0/6	0		
Consiguration	1	1/0/7	0		
		1/0/8	D		
Internor	1	1/0/9	0		
		1/0/10	0		

- **b.** Under **Private VLAN Promiscuous Interface Configuration**, select the 1/0/1 interface check box. Now 1/0/1 appears in the **Interface** field at the top.
- c. In the Promiscuous Primary VLAN field, enter 100.
- d. In the Promiscuous Secondary VLAN field, enter 101-102.
- e. Click Apply to save the settings.

LAGs

Link Aggregation Groups

This chapter includes the following sections:

- LAG Concepts
- Create Two LAGs
- Add Ports to LAGs
- Enable Both LAGs

3

LAG Concepts

Link aggregation allows the switch to treat multiple physical links between two endpoints as a single logical link. All the physical links in a given LAG must operate in full-duplex mode at the same speed. LAGs can be used to directly connect two switches when the traffic between them requires high bandwidth and reliability, or to provide a higher-bandwidth connection to a public network. Management functions treat a LAG as if it were a single physical port. You can include a LAG in a VLAN. You can configure more than one LAG for a given switch.



Figure 6. Example network with two LAGs

LAGs offer the following benefits:

- Increased reliability and availability. If one of the physical links in the LAG goes down, traffic is dynamically and transparently reassigned to one of the other physical links.
- Better use of physical resources. Traffic can be load-balanced across the physical links.
- Increased bandwidth. The aggregated physical links deliver higher bandwidth than each individual link.
- Incremental increase in bandwidth. A physical upgrade could produce a tenfold increase in bandwidth; LAG produces a two- or fivefold increase, useful if only a small increase is needed.

Create Two LAGs

The example is shown as CLI commands and as a Web interface procedure.

CLI: Create Two LAGs

```
(Netgear Switch) #config
(Netgear Switch) (Config)#port-channel name lag 1 lag_10
(Netgear Switch) (Config)#port-channel name lag 1 lag_20
(Netgear Switch) (Config)#exit
```

Use the show port-channel all command to show the logical interface IDs you will use to identify the LAGs in subsequent commands. Assume that lag_10 is assigned ID 1/1, and lag_20 is assigned ID 1/2.

(Conso	(Console) #show port-channel all												
	Port-			Link									
Log.	Channel		Adm.	Trap	STP		Mbr	Port	Port				
Intf	Name	Link	Mode	Mode	Mode	Туре	Ports	Speed	Active				
1/1	lag_10	Down	En.	En.	Dis.	Dynamic							
1/2	lag_20	Down	En.	En.	Dis.	Dynamic							

Web Interface: Create Two LAGs

- **1.** Create LAG lag_10.
 - a. Select Switching > LAG > LAG Configuration.

System	Switching	Routing	GoS S	ecurit	y Monit	oring M	oîntenance	Help	Index
VLAN STP	Multicost	Address Toble	Ports LAG						
- LAD Configuration		i Configuratio AG Configuratio	n						
		Log Name	Description	Lag 1D	Link Trap	Admin Mode	STP Mode	Static Mode	Hashin
		lag_10							

- b. In the Lag Name field, enter lag_10.
- c. Click Add.
- 2. Create LAG lag_20.

a. Select Switching > LAG > LAG Configuration. A screen similar to the following displays.

System	Switching	Routing	Qo\$ 5	ecurit;	y Monit	oring M	sintenance	Help	Index
VIAN STP	Multicast	Address Table P	orts LAG						
LAG	LAG	3 Configuratio	n						
LAG Membersh	ip L	AG Configuration	1						
		Lag Name	Description	Lag ID	Link Trap	Admin Mode	STP Mode	Static Mode	Hashin
		lag_20					1		
	F	lag_10		1	Enable	Enable	Enable	Disable	Source I

- b. In the Lag Name field, enter lag_20.
- c. Click Add.

Add Ports to LAGs

The example is shown as CLI commands and as a Web interface procedure.

CLI: Add Ports to the LAGs

(Netgear	Switch)	#config
(Netgear	Switch)	(Config)#interface 0/2
(Netgear	Switch)	(Interface 0/2)#addport 1/1
(Netgear	Switch)	(Interface 0/2)#exit
(Netgear	Switch)	(Config)#interface 0/3
(Netgear	Switch)	(Interface 0/3)#addport 1/1
(Netgear	Switch)	(Interface 0/3)#exit
(Netgear	Switch)	(Config)#interface 0/8
(Netgear	Switch)	(Interface 0/8)#addport 1/2
(Netgear	Switch)	(Interface 0/8)#exit
(Netgear	Switch)	(Config)#interface 0/9
(Netgear	Switch)	(Interface 0/9)#addport 1/2
(Netgear	Switch)	(Interface 0/9)#exit
(Netgear	Switch)	(Config)#exit

Web Interface: Add Ports to LAGs

- **1.** Add ports to lag_10.
 - a. Select Switching > LAG > LAG Membership.

System Sw	itching	Routing	QoS	Security	Monitoring	Maintenance	Help Inde					
VIAN STP M	Ncost Adde	ess Table	Ports LAG									
LAG	LAG Membership											
Configuration LAG Membereliije	LAG M	lembershi	p				00					
	LAG ID		Lag 1 💌	v	G Name	180,10						
	LAG Desc	rigition	- A									
	Admin He	de.	Enable 📄		ak trap	Enable 🖂						
	STP Node	0	Enable 💌	51	atic Mode	Disable 🗵						
	Hash Mode		Source IP	and Source TCP	/UDP Port	3						
	Port Selec	tion Table										
	= theil 1						and the second second					
	Port 1	234	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20 21 22	23 24					
	25 1	26 27 28	<u> </u>									

- b. In the LAG ID list, select LAG 1.
- c. Click Unit 1. The ports display.
- d. Click the gray boxes under port 2 and 3.

Two check marks display in the box.

- e. Click Apply to save the settings.
- 2. Add ports to lag_20.
 - a. Select Switching > LAG > LAG Membership.

System Sw	itching	T	R	outi	ng	ĩ	Q	oS.	T	S	ecur	ily.	1	Mo	nîtori	ing:	ï	Mai	itenc	nce		10.9	Help	81	Ind
VLAN STP MU	ticost 1	Add	dress	Tab	ie (Po	etta (LA	G																
LAG	LAG	M	em	bei	rsh	ip																			
LAG Membership	C.L	AG	Mer	nbe	rshi	ip :																	(2)		
	LAG	10					Lag	2					LAG	Name				lag_	20						
	LAG	Des	e espi	times					_																
	Adm	vin M	lode	1			Ene	ble	1				Link	Trap				Ena	ble	•					
	STP	Mod	R.				Eng	ible.	2				Stat	ic Mor	te.			Dise	ble						
	Hast	e Ho	de				Sou	ince	IP 4	and s	Sour	ce T	CP/U	DP P	int					_	•				
	Port	Sale	ctio	n Ta	ble																				
	- Mr	1. 16									-		-						a cire						
	Port	1	2	3	4	5	6	7	8	9	10	11	12 1	13 1	4 15	16	17	18 19	20	21 3	17	23	24		
		25	26	27	28				4	4		113			-		-		-						

- **b.** Under LAG Membership, in the LAG ID list, select LAG 2.
- c. Click Unit 1. The ports display.
- d. Click the gray boxes under ports 8 and 9.Two check marks display in the boxes.
- e. Click Apply to save the settings.

Enable Both LAGs

The example is shown as CLI commands and as a Web interface procedure.

CLI: Enable Both LAGs

By default, the system enables link trap notification.

```
(Console) #config
(Console) (Config)#port-channel adminmode all
(Console) (Config)#exit
```

At this point, the LAGs could be added to VLANs.

Web Interface: Enable Both LAGs

a. Select Switching > LAG > LAG Configuration.

System	Switchin	Routing	QoS 5	ocurit	y Moni	toring M	aintenance	Help	Index
VIAN STP /	Malticust	Address Table	Porta LAG						
LAG Configuration LAG Nembershi	L/	AG Configuratio	on n						
		Lag Name	Description	Lag 1D	Link Trap	Admin Mode	STP Mode	Static Mode	Hashin
						Enable 💌	2		
	P	lag_10		1	Enable	Enable	Enable	Disable	Tourse 1
	P	Lag_20		2	Enable	Enable	Enable	Disable	Source 1

- b. Select the top check box and the check boxes for lag_10 and lag_20 are selected.
- c. In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.

Port Routing

Port routing, default routes, and static routes

4

This chapter includes the following sections:

- Port Routing Concepts
- Port Routing Configuration
- Enable Routing for the Switch
- Enable Routing for Ports on the Switch
- Add a Default Route
- Add a Static Route

Port Routing Concepts

The first networks were small enough for the end stations to communicate directly. As networks grew, Layer 2 bridging was used to segregate traffic, a technology that worked well for unicast traffic, but had problems coping with large quantities of multicast packets. The next major development was routing, where packets were examined and redirected at Layer 3. End stations needed to know how to reach their nearest router, and the routers had to interpret the network topology so that they could forward traffic. Although bridges tended to be faster than routers, using routers allowed the network to be partitioned into logical subnetworks, which restricted multicast traffic and also facilitated the development of security mechanisms.

An end station specifies the destination station's Layer 3 address in the packet's IP header, but sends the packet to the MAC address of a router. When the Layer 3 router receives the packet, it will minimally:

- Look up the Layer 3 address in its address table to determine the outbound port.
- Update the Layer 3 header.
- Re-create the Layer 2 header.

The router's IP address is often statically configured in the end station, although the M4100 Managed Switch supports protocols such as DHCP that allow the address to be assigned dynamically. Likewise, you can assign some of the entries in the routing tables used by the router statically, but protocols such as RIP and OSPF allow the tables to be created and updated dynamically as the network configuration changes.

Port Routing Configuration

The M4100 Managed Switch always supports Layer 2 bridging, but Layer 3 routing must be explicitly enabled, first for the M4100 Managed Switch as a whole, and then for each port that is to be part of the routed network.

The configuration commands used in the example in this section enable IP routing on ports 1/0/2,1/0/3, and 1/0/5. The router ID will be set to the M4100 Managed Switch's management IP address, or to that of any active router interface if the management address is not configured.

After the routing configuration commands have been issued, the following functions will be active:

- IP forwarding, responsible for forwarding received IP packets.
- ARP mapping, responsible for maintaining the ARP Table used to correlate IP and MAC addresses. The table contains both static entries and entries dynamically updated based on information in received ARP frames.
- Routing Table Object, responsible for maintaining the common routing table used by all registered routing protocols.

You can then activate RIP or OSPF, used by routers to exchange route information, on top of IP Routing. RIP is more often used in smaller networks, while OSPF was designed for larger and more complex topologies.

The following figure shows a Layer 3 switch configured for port routing. It connects three different subnets, each connected to a different port.



Figure 7. Layer 3 switch configured for port routing

Enable Routing for the Switch

The example is shown as CLI commands and as a Web interface procedure.

CLI: Enable Routing for the Switch

The following script shows the commands that you would use to configure a M4100 Managed Switch to provide the port routing support shown in *Figure 7, Layer 3 switch configured for port routing* on page 59.

Use the following command to enable routing for the switch. Execution of the command enables IP forwarding by default.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Web Interface: Enable Routing for the Switch

1. Select Routing > IP > Basic > IP Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS Si	curily.	Monitoring	Maintenance	Help	Index
Routing Table	IP VIAN	ARP RIP O	SPF Router Disc	covery I V	RRP. /			l D
* Bankt • IP Configuration • Statistics	IP Co	Onfiguration Configuration				0		
Advanced	Defau	It Time to Live 19 Node	30 C Disable	e (@ Enabl	0			
	IP For Maxim	warding Node sum Next Hops	C Disable 2	e 🗷 Enabl	•			

- 2. For Routing Mode, select the Enable radio button.
- 3. Click Apply to save the settings.

Enable Routing for Ports on the Switch

Use the following commands or the web interface to enable routing for ports on the switch. The default link-level encapsulation format is Ethernet. Configure the IP addresses and subnet masks for the ports. Network-directed broadcast frames will be dropped. The maximum transmission unit (MTU) size is 1500 bytes.

CLI: Enable Routing for Ports on the Switch

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#routing
(Netgear Switch) (Interface 1/0/5)#routing
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Interface 1/0/5)#exit
```

Web Interface: Enable Routing for Ports on the Switch

- 1. Assign IP address 192.150.2.1/24 to interface 1/0/2.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

A screen similar to the following displays.

System	Switching	Routin	g GoS	Security	Monitorin	g Maintenance	Help	Index
Routing Table)	P VIAN	ARP RI	P OSPF Route	e Discovery	VRRP			
Basic	IP	Interface	Configuration	1				
» IP Configuratio	n 📑	Configuratio	n.					
Statistics	1	RA.			00			
Contiguration > Secondary IP		Interface	Description	VLAN 1D	IP Address	Subnet Mask	Routing Mode	Administrative
		1/0/2			192.150.2.1	255.255.255.0	Enable 💌	Enable 💌
		1/0/1			0.0.0.0	0.0.0.0	Disable	Enable
	5	1/0/2		1	0.0.0.0	0.0.0.0	Disable	Enable
		1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
	10	1/0/4			0.0.0.0	0.0.0.0	Disable	Enable

b. Scroll down and select the interface 1/0/2 check box.

Now 1/0/2 appears in the Interface field at the top.

- c. Under the IP Interface Configuration, enter the following information:
 - In the IP Address field, enter 192.150.2.1.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Routing Mode field, select Enable.
- d. Click Apply to save the settings.
- **2.** Assign IP address 192.150.3.1/24 to interface 1/0/3.
 - a. Select Routing > IP> Advanced > IP Interface Configuration.

A screen similar to the following displays.

System	Switchin	a Routin	g QoS	Security	Monitoring	Maintenance	Help	Index
Booting Table 1	P I VIA	N ARP RI	P OSPF Route	ar Discovery	VERP			
Basic	I	P Interface	Configuration	89				
> IP Configuratio	n: 1	Configuratio	m					
+ Statistics	1	All				So To Interface	00	
• Secondary IP		Interface	Description	VLAN ID	IP Address	Subnet Hask	Routing Mode	Administrative Mode
		1/0/3			192.150.3.1	255.255.255.0	Enable 💌	Enable -
	T	1/0/1	_		0.0.0.0	0.0.0.0	Disable	Enable
	i.	1/0/2			192.150.2.1	255.255.255.0	Enable	Enable
		2 1/0/3			0.0.0.0	0.0.0.0	Disable	Enable
	1	1/0/4			0.0.0.0	0.0.0	Disable	Enable
	ſ	1/0/5			0.0.0.0	0.0.0.0	Disable	Enable

b. Scroll down and select the interface **1/0/3** check box.

Now 1/0/3 appears in the Interface field at the top.

- c. Enter the following information:
 - In the IP Address field, enter 192.150.3.1.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the **Routing Mode** field, select **Enable**.
- d. Click Apply to save the settings.
- **3.** Assign IP address 192.150.5.1/24 to interface 1/0/5.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

A screen similar to the following displays.

System 5	witching	Routin	G QoS	Security	Monitoring	Maintenance	Help	Index	
Routing Table	PII VLAT	ARP RIP	OSPF Rou	ter Discovery	VRRP				
Basic	IP	Interface	Configuratio	en :					
 IP Configuration 		Configuratio	n.						
 Statistics 		All				to To Interface	00		
* Secondary 1P		Interface	Description	VLAN TD	IP Address	Subnet Mask	Routing Mode	Administrative Piode	aspr Admin Node
	E	1/0/5			192.150.5.1	255.255.255.0	Enable 💽	Enable 🖃	Disable
		1/0/1	1		0.0.0.0	0.0.0.0	Disable	Enable	Disable
	10	1/0/2			192.150.2.1	255.255.255.0	Enable	Enable	Disable
		1/0/3			192.150.3.1	255.255.255.0	Enable	Enable	Disable
	E	1/0/4			0.0.0.0	0.0.0.0	Disable	Enable	Disable
	P	1/0/5			0.0.0.0	0.0.0.0	Enable	Enable	Disable

b. Scroll down and select the interface **1/0/5** check box.

Now 1/0/5 appears in the Interface field at the top.

- c. Enter the following information:
 - In the IP Address field, enter 192.150.5.1.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Routing Mode field, select Enable.
- d. Click Apply to save the settings.

Add a Default Route

When IP routing takes place on a switch, a routing table is needed for the switch to forward the packet based on the destination IP address. The route entry in the routing table can either be created dynamically through routing protocols like RIP and OSPF, or be manually created by the network administrator. The route created manually is called the static or default route.

A default route is used for forwarding the packet when the switch cannot find a match in the routing table for an IP packet. The following example shows how to create a default route.

CLI: Add a Default Route

(FSM7338S) (Config) #ip route default? <nexthopip> Enter the IP Address of the next router. (FSM7328S) (Config)#ip route default 10.10.10.2

Note: IP subnet 10.10.10.0 should be configured using either port routing (see *Enable Routing for Ports on the Switch* on page 60) or VLAN routing (see *Set Up VLAN Routing for the VLANs and the Switch* on page 72).

Web Interface: Add a Default Route

1. Select Routing > Routing Table > Basic > Route Configuration.

The Route Configuration screen displays.

System	Switchin	g Routing	QoS	Security	Monitor	ring Mai	intenance	Help
Routing Table	IP VLA	N ARP RIP C	SPF Rout	er Discovery	VRRP			
Harak.	R	oute Configura	tion					
	5	Configure Routes						1
Advanced		Route Type	Network	Address S	iubnet mask	Rext Hop I Address	P Pr	eference
		DefaultRoute V				10.10.10.	2	
		Static						
	1	Learned Routes				_		0
		toute Network Sol	metmask	Protocol	Next Hop Interface	Next Hop 1P Address	Preference	Hetric

- 2. In the Route Type list, select DefaultRoute.
- 3. In the Next Hop IP Address field, enter one of the routing interface's IP addresses.
 - The **Network Address** and **Subnet Mask** fields will not accept input as they are not needed.
 - The **Preference** field is optional. A value of 1 (highest) will be assigned by default if not specified.
- 4. Click the Add button on the bottom of the screen.

This creates the default route entry in the routing table.

Add a Static Route

When the switch performs IP routing, it forwards the packet to the default route for a destination that is not in the same subnet as the source address. However, you can set a path (static route) that is different than the default route if you prefer. The following procedure shows how to add a static route to the switch routing table.

CLI: Add a Static Route

The following commands assume that the switch already has a defined a routing interface with a network address of 10.10.10.0, and is configured so that all packets destined for network 10.10.100.0 take the path of routing port.

To delete the static route, simply add "no" keyword in the front of the "ip route" command.

Web Interface: Add a Static Route

1. Select **Routing > Routing Table > Basic > Route Configuration** to display the Route Configuration screen.

System	Şŵi	tching	Routing		QoS	Security	1	Monitori	ng	Main	lenance	He	p.	Index
Rooting Table	12	VIAN I	ARP RIP	OS	PF Rout	er Discovery	1 VR	RP C						
Bartis:		Rout	te Config	uratie	on									
Configuration		0	onfigure Ro	utes									0	
Advanced			Route Type		Network	Address	Subo	et mask	No.	nt Hop I Mess	•	Preferen		
			Static	2	10.10.2	0.0	255.	255.255.0	1	92.168.1	.1			
		D	Etatic DefaultRou	/te	0.0.0.0		0.0.0	.0	10	0.10.10.2	6	1		
		L.	earned Rou	tes						_			(2)	
		Rout	Address	Subm	et maak.	Protocol		Next Hop Interface	Next I Addre	lop IP 1	Drefere	nce Met	ric	

- 2. In the Route Type list, select Static.
- 3. Fill in the Network Address field.

Note that this field should have a network IP address, not a host IP address. Do not enter something like *10,100.100.1*. The last number should always be 0 (zero).

- 4. In the **Subnet Mask** field, enter a value that matches the subnet range that you want to use.
- 5. The **Preference** field is optional. A value of 1 is entered by default if you do not enter a number.
- 6. Click the **Add** button on the bottom of the screen. The screen is updated with the static route shown in the routing table.
- 7. To remove a route entry, either static or default, select the check box to the left of the entry, and click the **Delete** button on the bottom of the screen.

VLAN Routing

VLAN routing for a VLAN and for the switch

5

This chapter includes the following sections:

- VLAN Routing Concepts
- Create Two VLANs
- Set Up VLAN Routing for the VLANs and the Switch

VLAN Routing Concepts

You can configure the ProSAFE M4100 Managed Switches with some ports supporting VLANs and some supporting routing. You can also configure it to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (the default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC destination address (DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, and also to the internal bridge-router interface if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when more segmentation or security is required.

The next section shows you how to configure the ProSAFE M4100 Managed Switches to support VLAN routing and how to use RIP and OSPF. A port can be either a VLAN port or a router port, but not both. However, a VLAN port can be part of a VLAN that is itself a router port.

Create Two VLANs

This section provides an example of how to configure the M4100 Managed Switch to support VLAN routing. The configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN has been created, you must use the *show ip vlan* command to determine the VLAN's interface ID so that you can use it in the router configuration commands.

The diagram in this section shows a Layer 3 switch configured for port routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script shows the commands that you would use to configure a M4100 Managed Switch to provide the VLAN routing support shown in the diagram.



Figure 8. Layer 3 switch configured for port routing

CLI: Create Two VLANs

The following code sequence shows an example of creating two VLANs with egress frame tagging enabled.

(Netgear	Switch)	#vlan data
(Netgear	Switch)	(Vlan)#vlan 10
(Netgear	Switch)	(Vlan)#vlan 20
(Netgear	Switch)	(Vlan)#exit
(Netgear	Switch)	#conf
(Netgear	Switch)	(Config)#interface range 1/0/1-1/0/2
(Netgear	Switch)	(conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear	Switch)	(conf-if-range-1/0/1-1/0/2)#vlan pvid 10
(Netgear	Switch)	(conf-if-range-1/0/1-1/0/2)#exit
(Netgear	Switch)	(Config)#interface 1/0/3
(Netgear	Switch)	(Interface 1/0/3)#vlan participation include 20
(Netgear	Switch)	(Interface 1/0/3)#vlan pvid 20
(Netgear	Switch)	(Interface 1/0/3)#exit
(Netgear	Switch)	(Config)#exit

Web Interface: Create Two VLANs

- 1. Create VLAN 10 and VLAN20.
 - a. Select Switching > VLAN > Advanced > VLAN Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Mointenance	Help	Index
VEAN STP	Multicost	Address Tuble	North LAG					
Basic Advanced	VL	AN Configur	ation					
ALL ALL	1.1	Reset				(2)		
Configuration	Re	set Configuration	S	E	Í.			
VLAN Membe VLAN Status	ersmip							
MAC Based V	/LAN	VLAN Configur	ation			ŵ		
» Port PVID	8	VLAN ID	VLAN Name		VLAN TYP			
· Port OVLAN		10	VLAN10	1	Static			
Configuration	· ·	1 1	Default		Default			
» Protocol Base	ed	61.5s	- and an		o en suite			

- b. In the VLAN ID field, enter 10.
- c. In the VLAN Name field, enter VLAN10.
- d. In the VLAN Type list, select Static.
- e. Click Add.
- f. Select Switching > VLAN > Advanced > VLAN Configuration.

System 5	witching	Routing	QoS	5ecurity	Monitoring	Maintenance	Help	Index
VUAN STP. M	ulticast Ac	idress Toble	Ports LAG				· · · · · ·	
Basic	VLAN	Configura	ation					
+ VLAY	Res	et				(D)		
Configuration	Reset (onfiguration		E				
 VLAN Status 	P							
> MAC Based VLAM	VLA	N Configur	ation			100		
Port PVID Configuration		IAN ID	VLAN Name		VLAN TY	ae -		
* Port DVLAN		20.	VLAN20	1	Static	a		
Configuration	C 1		Default		Default			
 Protocol Based VLAN Group 	F 3	0	VLAN10		Static			

- g. In the VLAN ID field, enter 20.
- h. In the VLAN Name field, enter VLAN20.
- i. In the VLAN Type list, select Static.
- j. Click Add.
- 2. Add ports to the VLAN10 and VLAN20.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

System Swit	iching Routing QoS Security Monitoring Maintenance Help Ind
VUAN STP Mult	icost Address Table Ports LAG
Bastc Advanced	VLAN Membership
Configuration	VLAN TO 10 Crossp Operation Unitag All
VLAN Status MAC Based VLAN	VEAN Type Static TACGED PORT MEMBERS
Port PVID Configuration Port DVLAN	Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 T T
Configuration Protocol Based	25 26 27 20

- b. In the VLAN ID field, select 10.
- c. Click the Unit 1. The ports display.
- d. Click the gray boxes under ports 1 and 2 until T displays.

The T specifies that the egress packet is tagged for the port.

e. Click Apply.

f. Select Switching > VLAN > Advanced > VLAN Membership.

A screen similar to the following displays.

System S	witching		Re	outin	0		205		5	incu	rity		M	nito	ring	1	M	inter	anc	8		Help	Index
VIAN STP A	Aulticost	Add		Tobl	• 1.	Ports	I. P	AG.															
Basic	VL/		ler	nbe	ersi	nip																	
+ VLAN		/LAN	Me	mb	ersh	ip																0	
Configuration	VL	NN 10	t.			20 •								Group	a Ope	ratio	m.	Unt	ag A	11			
 VLAK Hamiltonsh 	VL.	NN Na	me			VLAN	20							UNIT,	AGGE	0.001	IT ME	MOCRE					
 MAC Based VLA 	. VL	LN TY	pe			Static	8							TA	ogep	FOR	MEN	MERS					
* Port PVID	1	the																					
Configuration > Port DVLAN	Port	1	2	3	4	5 6	7	8	9	10	11	12	19	14 1	5 16	17	18	19 20	0 21	22	23	24	
Configuration	_	- 20	£.0		£0																	-	

- g. In the VLAN ID list, select 20.
- h. Click Unit 1. The ports display.
- i. Click the gray box under port **3** until **T** displays.

The T specifies that the egress packet is tagged for the port.

- j. Click Apply.
- 3. Assign PVID to VLAN10 and VLAN20.
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration.

System Swi	tching	Routing	QeS Secu	rity Monitor	ing Main	tenance Help	Index
VLANE STP Mult	icest Ac	idress Table Por	h LAG				
lasic	Port	VLAN Id Con	figuration				
VLAN	PV	ID Configuration	1			0	
Configuration		2	All	Go To Int	terface 👘	00	
VLAN Membership		Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)	
Fort PVIC			101				
Castignetion	R	1/0/1	1	Admit All	Disable	0	
Port DVLAN	R	1/0/2	1	Admit All	Disable	0	
Protocol Based	C	1/0/3	1	Admit All	Disable	0	
VLAN Group	E.	1/0/4	1	Admit All	Disable	0	
Configuration	П	1/0/5	1	Admit All	Disable	0	
Protocol Based	Г	1/0/6	1	Admit All	Disable	0	
VLAN Group	E .	1/0/7	1	Admit All	Disable	0	

- b. Scroll down and select 1/0/1 and 1/0/2 check boxes.
- c. In the PVID (1 to 4093) field, enter 10.
- d. Click Apply to save the settings.
- e. Select Switching > VLAN > Advanced > Port PVID Configuration.

System	Switching	Routing	QoS Secu	rity Monitor	ing Main	tenance	Help	Index
VIAN STP	Multicost A	ddress Table Por	N LAG					
Dasic	Port	VLAN Id Con	figuration					
VLAN	PV	ID Configuration	1				1	
Configuration		2	A11	Go To Int	orface 📃 🧔	00		
 VLAN Members VLAN Status MAC Based Music 	hip .	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priorit (0 to 7)	Y	
Hart PVID		1/0/3	20	Admit All 💽	Disable 💌	0		
Conferences	1	1/0/1	10	Admit All	Disable	0		
Port DVLAN Configuration	Г	1/0/2	10	Admit All	Disable	0		
 Protocol Based 	1	1/0/3	1	Admit All	Disable	0		
VLAN Group	n -	1/0/4	1	Admit All	Disable	0		
Configuration	E	1/0/5	1	Admit All	Disable	0		
Protocol Based	5	1/0/6	1	Admit All	Distable	8		
VLAN Group		1/0/7	1	Admit All	Disable	0		

- f. Scroll down and select the 1/0/3 check box.
- g. In the PVID (1 to 4093) field, enter 20.
- h. Click Apply to save the settings.

Set Up VLAN Routing for the VLANs and the Switch

The example is shown as CLI commands and as a Web interface procedure.

CLI: Set Up VLAN Routing for the VLANs and the Switch

1. The following code sequence shows how to enable routing for the VLANs:

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
```

This returns the logical interface IDs that will be used instead of the slot/port in subsequent routing commands. Assume that VLAN 10 is assigned the ID 3/1, and VLAN 20 is assigned the ID 3/2.

2. Enable routing for the switch.

(Netgear Switch) #config (Netgear Switch) (Config)#ip routing (Netgear Switch) (Config)#exit

3. The next sequence shows an example of configuring the IP addresses and subnet masks for the virtual router ports.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface-vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface-vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface-vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface-vlan 20)#exit
(Netgear Switch) (Config)#exit
```
Web Interface: Set Up VLAN Routing for the VLANs and the Switch

1. Select Routing > VLAN > VLAN Routing.

System	Swi	tching	Ro	oting	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	P	VLAN	ARP	RIP	OSPE	touter Discovery	VRRP			
VLAN Routing Wizard		VLA	N Rou	ting (Configur	ation		6		
The second			VLAN ID (1 to 4093)	Port	MAC Address	IP Address	Subnet Mask			
			10 -			192,150.3,1	255.255.255.0			

- 2. Enter the following information:
 - In the VLAN ID (1 to 4093) list, select 10.
 - In the IP Address field, enter 192.150.3.1.
 - In the Subnet Mask field, enter 255.255.255.0.
- 3. Click Add to save the settings.
- 4. Select Routing > VLAN > VLAN Routing. A screen similar to the following displays.



- **5.** Enter the following information:
 - Select **10** in the **VLAN ID** (1 to 4093) field.
 - In the IP Address field, enter 192.150.4.1.
 - In the Subnet Mask field, enter 255.255.255.0.
- 6. Click Add to save the settings.

Proxy ARP

Proxy Address Resolution Protocol

6

This chapter includes the following sections:

- Proxy ARP Concepts
- Proxy ARP Examples

Proxy ARP Concepts

Proxy ARP allows a router to answer ARP requests when the target IP address is not that of the router itself but a destination that the router can reach. If a host does not know the default gateway, proxy ARP can learn the first hop. Machines in one physical network appear to be part of another logical network. Without proxy ARP, a router responds to an ARP request only if the target IP address is an address configured on the interface where the ARP request arrived.

Proxy ARP Examples

The following are examples of the commands used in the proxy ARP feature.

CLI: show ip interface

(Netgear Switch) #show	ip interface ?					
<slot port=""> brief</slot>	Enter an interface in s Display summary informa settings for all ports.	slot/port format. ation about IP configuration				
(Netgear Switch) #show ip interface 0/24						
Routing Mode		Disable				
Administrative Mode		Enable				
Forward Net Directed Br	padcasts	Disable				
Proxy ARP		Disable				
Active State		Inactive				
Link Speed Data Rate		Inactive				
MAC Address		08:00:17:05:05:02				
Encapsulation Type		Ethernet				
IP MTU 1500						

CLI: ip proxy-arp

(Netgear Switch)	(Interface 0/24)#ip	proxy-arp ?
<cr></cr>	Press Enter	to execute the command.
(Netgear Switch)	(Interface 0/24)#ip	proxy-arp

Web Interface: Configure Proxy ARP on a Port

1. Select Routing > IP > Advanced > IP Interface Configuration.

System	Switchi	ng Routi	ng QoS	Security	Monitorin	g Maintenance	Help	Index	
Routing Table	P W	AN ARP R	IP OSPF Route	r Discovery	VREP				
Basic	1	P Interface	Configuration						
> 1P Configuratio	n. 1	Configurati	on						
+ Statistics		L AI	1			Go To Interface	ao I		
* Secondary IP		Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode	
							2		
		1/0/1	1	19	0.0.0.0	0.0.0.0	Disable	Enable	
	- 1	1/0/2			0.0.0.0	0.0.0.0	Disable	Eneble	
		1/0/3			0.0.0.0	0.0.0.0	Disable	Enable	

- 2. Under Configuration, scroll down and select the Interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.
- 3. In the Proxy Arp field, select Enable.
- 4. Click Apply to save the settings.

ACLs

7

Access Control Lists

This chapter includes the following sections:

- ACL Concepts
- Set Up an IP ACL with Two Rules
- One-Way Access Using a TCP Flag in an ACL
- Use ACLs to Configure Isolated VLANs on a Layer 3 Switch
- Set up a MAC ACL with Two Rules
- ACL Mirroring
- ACL Redirection
- Configure IPv6 ACLs

ACL Concepts

Access control lists (ACLs) can control the traffic entering a network. Normally ACLs reside in a firewall router or in a router connecting two internal networks. When you configure ACLs, you can selectively admit or reject inbound traffic, thereby controlling access to your network or to specific resources on your network.

You can set up ACLs to control traffic at Layer 2-, or Layer 3. MAC ACLs are used for Layer 2. IP ACLs are used for Layer 3. Each ACL contains a set of rules that apply to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the fields within a packet.

The following limitations apply to ACLs. These limitations are platform dependent.

- The maximum of number of ACLs is 100.
- The maximum number of rules per ACL is 8–10.
- Stacking systems do not support redirection.
- The system does not support MAC ACLs and IP ACLs on the same interface.
- The system supports ACLs set up for inbound traffic only.

MAC ACLs

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect the following fields of a packet (limited by platform):

- Source MAC address with mask.
- Destination MAC address with mask.
- VLAN ID (or range of IDs).
- Class of Service (CoS) (802.1p).
- EtherType:
 - Secondary CoS (802.1p).
 - Secondary VLAN (or range of IDs).
- L2 ACLs can apply to one or more interfaces.
- Multiple access lists can be applied to a single interface: the sequence number determines the order of execution.
- You cannot configure a MAC ACL and an IP ACL on the same interface.
- You can assign packets to queues using the assign queue option.
- You can redirect packets using the redirect option.

IP ACLs

IP ACLs classify for Layer 3. Each ACL is a set of up to 10 rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and can apply to one or more of the following fields within a packet:

- Source IP address
- Destination IP address
- Source Layer 4 port
- Destination Layer 4 port
- ToS byte
- Protocol number

Note that the order of the rules is important: When a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL is denied access.

ACL Configuration

To configure ACLs:

- 1. Create an ACL by specifying a name (MAC ACL) or a number (IP ACL).
- 2. Add new rules to the ACL.
- 3. Configure the match criteria for the rules.
- 4. Apply the ACL to one or more interfaces.

Set Up an IP ACL with Two Rules

This section shows you how to set up an IP ACL with two rules, one applicable to TCP traffic and one to UDP traffic. The content of the two rules is the same. TCP and UDP packets will be accepted by the M4100 Managed Switch only if the source and destination stations have IP addresses within the defined sets.



Figure 9. IP ACL with rules for TCP traffic and UDP traffic

CLI: Set Up an IP ACL with Two Rules

The following is an example of configuring ACL support on a 7000 Series Managed Switch.

Create ACL 101. Define the first rule: The ACL will permit packets that match the specified source IP address (after the mask has been applied), that are carrying TCP traffic, and that are sent to the specified destination IP address.

1. Enter these commands:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#access-list 101 permit tcp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255
```

2. Define the second rule for ACL 101 to set conditions for UDP traffic similar to those for TCP traffic.

```
(Netgear Switch) (Config)#access-list 101 permit udp 192.168.77.0 0.0.0.255 192.178.77.0 0.0.0.255
```

3. Apply the rule to inbound traffic on port 1/0/2. Only traffic matching the criteria will be accepted.

(Netgear Switch) (Config)#interface 1/0/2 (Netgear Switch) (Interface 1/0/2)#ip access-group 101 in (Netgear Switch) (Interface 1/0/2)#exit (Netgear Switch) (Config)#exit

Web Interface: Set Up an IP ACL with Two Rules

- 1. Create IP ACL 101 on the switch.
 - a. Select Security > ACL > IP ACL.

A screen similar to the following displays.

System	Swite	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
Management	Security	Access	Port Authentic	ation Tra	fic Control AC	Ļ	2	11			
MAC ACL	1	IP ACL									
IF ALL		IP A	CL				٢				
IP Rules		Current	Number of ACL	0							
IP Extended	d Rules	Maximu	m ACL	100							
Configuratio	00										
» Binding Table	le	IP A	CL Table				1				
		IP	ACL ID		Rules	Туре					
		10	11	L.							
		Second Descent	<u> </u>			<u>k</u>	11				

- b. In the IP ACL ID field, enter 101.
- c. Click Add to create ACL 101.
- 2. Create a new rule associated with ACL 101.
 - a. Select Security > ACL > IP ACL > IP Extended Rules.

System S	Switching	R	auting	QoS		Security	Mo	nîtorîng	Moir	lenonce	Help	Index
Management Secu	rity Acce	en 1 Pe	ort Authent	ication 1	Troffic C	ontrol AC	ļ					
MAC ACL	IP E	xten	ded Ru	les								
. IP ACL	1	P Exter	nded Rul	es								
> IP Rules	ACL	ID		1	01 💌							
> IP Binding Configuration		xtende	d ACL R	ule Table	U.							0
 Dinding Table 	-	Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination TP Address	Destination IP Mask

- b. For ACL ID, select 101.
- c. Click Add to create a new rule.
- 3. Create a new ACL rule and add it to ACL 101.
 - **a.** After you click the Add button in step 2.

System Swit	ching Routing GoS	Security Monitoring Maintenance Help Ind						
Monogement Security	Access Port Authentication Traff	c Control ACL						
MAC ACL	Extended ACL Rule Configure	tion(100-199)						
IP ACL	ACLID	101						
+ IP Rules	Rule 10 (1 to 23)	1						
· IF Estenden Rutes	Action	@ Permit Egress Queue (0 to 6)						
 IF Binding Configuration 		C Deny						
> Binding Table	Match Every	false 💌						
	Protocol Type	TCP - (0 to 255)						
	TCP Flag	FIN Ignore - SYN Ignore - RST Ignore -						
		PSH Ignore · ACK Ignore · URG Ignore ·						
	Source IP Address	192.168.77.0						
	Source IP Mask	0.0.0.255						
	Source L4 Port	(0 to 65535)						
	Destination IP Address	192.178.77.0						
	Destination IP Hask	0.0.255						
	Destination L4 Port	(0 to 65535)						
	Service Type	○ IF DSCP = (0 to 63)						

- **a.** In the Extended ACL Rule Configuration, enter the following information:
 - In the Rule ID (1 to 23) field, enter 1.
 - For Action, select the **Permit** radio button.
 - In the Protocol Type list, select TCP.
 - In the Source IP Address field, enter 192.168.77.0.
 - In the Source IP Mask field, enter 0.0.0.255.
 - In the Destination IP Address field, enter 192.178.77.0.
 - In the **Destination IP Mask** field, enter **0.0.0.255**.
- b. Click Apply to save the settings.
- 4. Create another ACL rule and add it to the ACL 101.
 - **a.** After you click the Add button in step 3, a screen similar to the following displays.

System	Swite	hing	Routing	QoS	Security	Mor	itoring	Maint	enanci	e Help	Index	
Monogement S	Security	Access	Port Authentic	otion Traf	lic Control	ACI						
HAC ACL		Extens	ded ACL R	ule Configu	puration ation(100	-199)				Ţ		
> IP Rules	Diles	ACL ID			101							
+ IF Binding	a transfer	Rule 1D	(1 to 21)		22							
Configuratio	ne	Action			G P	ermit		Egress Queue (0 to 6)				
+ Dinding Tab	ile:				C Deny							
		Hatch E	very		False +							
		Protoco	Type		UDP		(0 to 25	a 255)				
		TCP Flag			FIN	Ignore 🖃	SYN	Ignore -	RST	Ignore -		
					PSH	Ignore -	ACK	Ignore -	URG	Ignore -		
		Source)	(P Address		192.	168.77.0						
		Source 2	IP Mask		0.0.0	.255						
		Source I	L4 Port		× (0 to			0 to 65533)				
		Destina	tion IP Addres		192.178.77.0							
		Destina	tion IP Mask		0.0.0	0.0.0.255						

- **b.** Under Extended ACL Rule Configuration, enter the following information:
 - In the Rule ID (1 to 23) field, enter 22.
 - For Action, select the **Permit** radio button.
 - In the **Protocol Type** list, select **UDP**.
 - In the Source IP Address field, enter 192.168.77.0.
 - In the Source IP Mask field, enter 0.0.0.255.
 - In the Destination IP Address field, enter 192.178.77.0.
 - In the Destination IP Mask field, enter 0.0.0.255.
- c. Click Apply to save the settings.
- 5. Apply ACL 101 to port 2.
 - a. Select Security > ACL > IP ACL > IP Binding Configuration.

System 5	iwitching	Routing	QoS	Security	Monitoring	Maintenance	Help Ind
Monogement Secu	rity Access I	fort Authenti	cation Traf	lic Control ACI			
MAC ACL	IP Bindi	ng Confi	guration				
P ACL	Bindin	g Configur	ation				(7).
= IP Rules	ACL ID		101 -	D	rection	Inbound 💌	
IP Extended Ru	les Seguence	Number	1	0	to 4294967295)		
Carobourstore	Port Selec	tion Table					
* Binding Table	· Onit.	b.					
	Port 1	2 3 4	5678	9 10 11 13	13 14 15 16 1	7 10 19 20 21 22	23 24
	25 1	6 27 28					
	15	PERMIT					12
	Interf	ice Bindin	g Status		-		w_{0}
	Interface	Dire	ction	ACL Type	ACL ID	Sequence Num	ber

- **b.** Under IP Binding Configuration, enter the following information:
 - In the ACL ID list, select 10.
 - In the **Sequence Number** field, enter **1**.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 2. A check mark displays in the box.
- e. Click Apply to save the settings.

One-Way Access Using a TCP Flag in an ACL

This example shows how to set up one-way Web access using a TCP flag in an ACL. PC 1 can access FTP server 1 and FTP server 2, but PC 2 can access only FTP server 2.



Figure 10. One-Way Web access using a TCP flag in an ACL

CLI: Configure One-Way Access Using a TCP Flag in an ACL

This configuration consists of two step:

- Step 1: Configure the Switch on page 85
- Step 2: Configure the GSM7352S on page 86

Step 1: Configure the Switch

1. Create VLAN 30 with port 0/35 and assign IP address 192.168.30.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 30
(Netgear Switch) (Vlan)#vlan routing 30
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/35
(Netgear Switch) (Interface 0/35)#vlan pvid 30
(Netgear Switch) (Interface 0/35)#vlan participation include 30
(Netgear Switch) (Interface 0/35)#exit
(Netgear Switch) (Interface 0/35)#exit
(Netgear Switch) (Config)#interface vlan 30
(Netgear Switch) (Interface-vlan 30)#routing
(Netgear Switch) (Interface-vlan 30)#ip address 192.168.30.1 255.255.255.0
(Netgear Switch) (Interface-vlan 30)#exit
(Netgear Switch) (Interface-vlan 30)#exit
```

2. Create VLAN 100 with port 0/13 and assign IP address 192.168.100.1/24.

(Netgear	Switch)	#vlan database
(Netgear	Switch)	(Vlan)#vlan 100
(Netgear	Switch)	(Vlan)#vlan routing 100
(Netgear	Switch)	(Vlan)#exit
(Netgear	Switch)	#configure
(Netgear	Switch)	(Config)#interface 0/13
(Netgear	Switch)	(Interface 0/13)#vlan pvid 100
(Netgear	Switch)	(Interface 0/13)#vlan participation include 100
(Netgear	Switch)	(Interface 0/13)#exit
(Netgear	Switch)	(Config)#interface vlan 100
(Netgear	Switch)	(Interface-vlan 100)#routing
(Netgear	Switch)	(Interface-vlan 100)#ip address 192.168.100.1 255.255.255.0
(Netgear	Switch)	(Interface-vlan 100)#exit
(Netgear	Switch)	(Config)#exit

3. Create VLAN 200 with port 0/44 and assign IP address 192.168.200.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/44
(Netgear Switch) (Interface 0/44)#vlan pvid 200
(Netgear Switch) (Interface 0/44)#vlan participation include 200
(Netgear Switch) (Interface 0/44)#vlan participation include 200
(Netgear Switch) (Interface 0/44)#exit
(Netgear Switch) (Interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.200.1 255.255.255.0
(Netgear Switch) (Interface-vlan 200)#exit
```

 Add two static routes so that the switch forwards the packets for which the destinations are 192.168.40.0/24 and 192.168.50.0/24 to the correct next hops.

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip route 192.168.40.0 255.255.255.0 192.168.200.2
(Netgear Switch) (Config)#ip route 192.168.50.0 255.255.255.0 192.168.200.2
```

5. Create an ACL that denies all the packets with TCP flags +syn-ack.

(Netgear Switch) (Config)#access-list 101 deny tcp any flag +syn -ack

6. Create an ACL that permits all the IP packets.

(Netgear Switch) (Config)#access-list 102 permit ip any

7. Apply ACLs 101 and 102 to port 0/44; the sequence of 101 is 1 and of 102 is 2.

Step 2: Configure the GSM7352S

1. Enter the following commands.

```
(Netgear Switch) (Config)#interface 0/44
(Netgear Switch) (Interface 0/44)#ip access-group 101 in 1
(Netgear Switch) (Interface 0/44)#ip access-group 102 in 2
(Netgear Switch) (Interface 0/44)#exit
```

```
86
```

2. Create VLAN 40 with port 1/0/24 and assign IP address 192.168.40.1/24.

(Netgear Switch)	#vlan database
(Netgear Switch)	(Vlan)#vlan 40
(Netgear Switch)	(Vlan)#vlan routing 40
(Netgear Switch)	#configure
(Netgear Switch)	(Config)#interface 1/0/24
(Netgear Switch)	(Interface 1/0/24)#vlan pvid 40
(Netgear Switch)	(Interface 1/0/24)#vlan participation include 40
(Netgear Switch)	(Interface 1/0/24)#exit
(Netgear Switch)	(Config)#interface vlan 40
(Netgear Switch)	(Interface-vlan 40)#routing
(Netgear Switch)	(Interface-vlan 40)#ip address 192.168.40.1 255.255.255.0
(Netgear Switch)	(Interface-vlan 40)#exit

3. Create VLAN 50 with port 1/0/25 and assign IP address 192.168.50.1/24.

(Netgear	Switch)	(Config)#exit
(Netgear	Switch)	#vlan database
(Netgear	Switch)	(Vlan)#vlan 50
(Netgear	Switch)	(Vlan)#vlan routing 50
(Netgear	Switch)	(Vlan)#exit
(Netgear	Switch)	#configure
(Netgear	Switch)	(Config)#interface 1/0/25
(Netgear	Switch)	(Interface 1/0/25)#vlan pvid 50
(Netgear	Switch)	(Interface 1/0/25)#vlan participation include 50
(Netgear	Switch)	(Interface 1/0/25)#exit
(Netgear	Switch)	(Config)#interface vlan 50
(Netgear	Switch)	(Interface-vlan 50)#routing
(Netgear	Switch)	(Interface-vlan 50)#ip address 192.168.50.1 255.255.255.0
(Netgear	Switch)	(Interface-vlan 50)#exit
(Netgear	Switch)	(Config)#exit

4. Create VLAN 200 with port 1/0/48 and assign IP address 192.168.200.1/24.

(Netgear Switch)	#vlan database
(Netgear Switch)	(Vlan)#vlan 200
(Netgear Switch)	(Vlan)#vlan routing 200
(Netgear Switch)	(Config)#interface 1/0/48
(Netgear Switch)	(Interface 1/0/48)#vlan pvid 200
(Netgear Switch)	(Interface 1/0/48)#vlan participation include 200
(Netgear Switch)	(Interface 1/0/48)#exit
(Netgear Switch)	#interface vlan 200
(Netgear Switch)	(Interface-vlan 200)#routing
(Netgear Switch)	(Interface-vlan 200)#ip address 192.168.200.2 255.255.255.0
(Netgear Switch)	(Interface-vlan 200)#exit

5. Add two static routes so that the switch forwards the packets with destinations 192.168.100.0/24 and 192.168.30.0/24 to the correct next hops.

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip route 192.168.100.0 255.255.255.0 192.168.200.1
(Netgear Switch) (Config)#ip route 192.168.30.0 255.255.255.0 192.168.200.1
```

Web Interface: Configure One-Way Access Using a TCP Flag in an ACL

This configuration consists of two steps:

- Configure the Switch on page 88
- Configure the GSM7342S Switch on page 96

Configure the Switch

- 1. Create VLAN 30 with IP address 192.168.30.1/24.
 - a. Select Routing > VLAN > VLAN Routing Wizard.

System	Swite	hing	T	Ro	utin	g		Q	oS		S	ecuri	ty	Г	Mo	tinc	orin	g		Mo	int	ena	inc	e		ł	lelp	,	
Management S	Security	Acces	55	Por	Au	hent	licat	ion	T	affi	c Co	ntrol	A	CL															
MAC ACL		IP B	linc	ling	C	onf	igu	irat	tior	ı																			
» IP ACL		В	indi	ing (Con	figu	rat	ion																			(?)		
» IP Rules		ACL	ID					101	. 💌					Dire	ectio	n				Ir	nbou	Jund	-						
» IP Extended	d Rules	Sequ	Jenc	e Nu	mbe	er i		1						(11	io 42	949	6729	5)											
> IP Binding	00	Port	Sele	ctio	n Tal	ble																							
» Binding Tab	ole	-	Uni	t 1																									
	1	Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	12	2 3	23	24		
		-	25	26	27	28								-			1-1-1-								1.	-			
		: I	nter	face	Bi	ndir	ng S	stat	us																		(?)		
		Inte	erfa	ce		Dire	ecti	on			ACI	Тур	e		A	CL	ID			S	equ	end	ce	Nu	mb	er			

A screen similar to the following displays.n the VLAN Routing Wizard,

- b. In the VLAN Routing Wizard, enter the following information:
 - In the Vlan ID field, enter 30.
 - In the IP Address field, enter 192.168.30.1.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 35 twice until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply to save VLAN 30.
- 2. Create VLAN 100 with IP address 192.168.100.1/24.
 - a. Select Routing > VLAN > VLAN Routing Wizard.

				_		_																				
System	Swit	ching		Re	outin	ŋg		Q	oS		S	ecui	ity		N	loni	tori	ng	1	М	lain	tend	ance	11	4	Hel
Routing Table	IP	VLAN	AR	P																						
VLAN Routi Wizard VLAN Routi	ng ng	VLA	LAN		utir outi	ng \ ng \	Wiz Niz	ard	d																	(2
		Vlan	ID					10	0																	
			12.3.4											LP	IG EI	nabli	ed			-9						
		IP A	ddre	:55				19	2.16	68.10	00.1			Ne	two	rk M	ask	ý.		_1	255	.255	.255	i.0		
		-	Unit	1																						
						104.0	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		Port	1	2	3	4	a minist		diam.	, in the second	Tornin (i nan	i nin		Design	o transfer	E NASSAGE	E training	10000	I NINDE	R Intel	a since	a Think	inist.	Contract of	i nini

- **b.** Enter the following information:
 - In the Vlan ID field, enter 100.
 - In the IP Address field, enter 192.168.100.1.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 13 twice until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply to save VLAN 100.
- 3. Create VLAN 200 with IP address 192.168.200.1/24.
 - a. Select Routing > VLAN > VLAN Routing Wizard.

A screen similar to the following displays.

						_	1																		
System	Swite	hing		Ro	utir	ng		Q	oS		S	ecur	ity	ľ	N	loni	torin	ng	1	Mo	inte	nanc	е	Y i	Hel
Routing Table	a IP ℓ	VLAN	AR	P																					
VLAN Routi Wizard	ng	VLA V		l Ro	uti	ng \	Wiz	zar ard	d																(2
	9 3	Vlan	ID					20	0																
		_												LÆ	G E	nable	ed								
		IP A	ddre	-55				19	2.16	68.20	00.1			Ne	etwo	rk M	ask			2	55.2	55.25	5.0		
		-	Uni	t 1																					
		Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	192	0 21	22	23	24
								14 (100)				-					20							1000	11
			25	26	27	28	29	30	31	32	33	34	35	36	31	38	39	40	41	4Z -	13 4	4 45	46	47	48

- **b.** Enter the following information:
 - In the Vian ID field, enter 200.
 - In the IP Address field, enter 192.168.200.1.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 44 twice until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply to save VLAN 200.
- 4. Enable IP routing.
 - a. Select Routing > IP > Basic > IP Configuration.

System	Switching	Routing	QoS 5	ecurity	Monitoring	Maintenance	Help	Index
Routing Table	🕑 VIAN AR	P RIP OS	PF Router Dis	covery V	KRP			
Basis	IP Conf	iguration						
Configuration	IP Cor	ofiguration				30		
Statistics	Default Ti	me to Live	30					
Advanced	Routing M	ode	C Disable	Enable				
	IP Forwar	ding Mode	C Disable	(* Enable				
	Maximum	Next Boos	2					

- **b.** Under IP Configuration, make the following selections:
 - For Routing Mode, select the **Enable** radio button.
 - For IP Forwarding Mode, select the **Enable** radio button.
- c. Click Apply to enable IP routing.
- 5. Add a static route with IP address 192.268.40.0/24:
 - a. Select Routing > Routing Table > Basic > Route Configuration.

med with troover	an"						48-Port Gige Switz
System	Switching	Routing	QoS Securit	hy Monitoring	Mointenad	ce Help	Index
Routing Table	IP VLAN	ARP					
Base	Rou	ite Configurat	ion				
- America		onfigure Routes					80
Advanced		Boute Type	Network Address	Subnet mask	Next Hop IP Add	ress Preferenc	
		Static 💼	192.168.40.0	255.255.255.0	192.168.200.2		

- **b.** Under Configure Routes, make the following selection and enter the following information:
 - In the Route Type list, select **Static**.
 - In the Network Address field, enter 192.168.40.0.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Next Hop IP Address field, enter 192.168.200.2.
- c. Click Add.
- 6. Create a static route with IP address 192.168.50.0/24:
 - a. Select Routing > Routing Table > Basic > Route Configuration.

System	Swit	ching	Routing	QoS	Security	Monitor	ing Mai	ntenance	Help	Index
Routing Table	IP	VIAN	ARP							
Baste		Rout	te Configurat	tion						
		C	onfigure Routes							
Advanced			Route Type	Network	Address S	ubnet mask	Next Hop	IP Address	Preference	
			Static 📃	192.168	.50.0	255.255.255.0	192.168.	200.2		
		Г	Static	192.168.	40.0 2	55.255.255.0	192.168.2	00.2	1	
		Le	arned Routes							
		Rout	e Network Address	Subn	et mask 1	Protocol	Next Hop Interface	Next Ho	p IP Address	Preferenc
		Dyna	mic 192.168.10	0.0 255.	255.255.0	Local	Vian 100	192.16	.100.1	0

- **b.** Under Configure Routes, make the following selection and enter the following information:
 - In the Route Type list, select Static.
 - In the Network Address field, enter 192.168.50.0.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Next Hop IP Address field, enter 192.168.200.2.
- c. Click Add.
- 7. Create an ACL with ID 101.
 - a. Select Security > ACL > Advanced > IP ACL.

System Swi	tching Routing	QoS Se	curity	Monitoring	Maintenance	Help
Management Security	Access Port Authenticatio	on Traffic Cont	trol ACL			
Basic	IP ACL					
. IP ACL	IP ACL				1	
> IP Rules	Current Number of ACL	0				
> IP Extended Rules	Maximum ACL	100				
> IP Binding Configuration						
> Binding Table	IP ACL Table				0	
	IP ACL ID	R	tules	Туре		
	101					
	Array Because and	_				

- b. In the IP ACL Table, in the IP ACL ID field, enter 101.
- c. Click Add.
- 8. Create an ACL with ID 102.
 - a. Select Security > ACL > Advanced > IP ACL.

System	Swite	hing	Routing	QoS	Security	Monitoring	Maintenance	Help
Monogement S	ecurity	Access	Port Authentic	cation Traf	fic Control AC	L		
Basic		IP AC	L					
> IF ACL		IP /	ACL				1	
» IP Rules	-	Current	t Number of AC	L 1				
> IP Extended > IP Binding	Rules	Maxim	am ACL	100		- N -		
Configuratio	n	2257						
» Binding Tab	e:	IP /	ACL Table				(D)	
		16	P ACL ID		Rules	Туре		
		1	02					
		F 10	1		0	Extended		

- b. In the IP ACL Table, in the IP ACL ID field, enter 102.
- c. Click Add.
- 9. Add and configure an IP extended rule that is associated with ACL 101.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

System	Switchi	ng Ro	outing	QoS	Se	scurity	Mor	itoring	Maint	enance	Help	Index	100
Monogement	Security	Access Po	rt Authonti	cotion 1	Traffic Cor	strol ACL							
Basic		IP Exten	ded Ru	les									
> IP ACL		IP Exter	nded Rul	es									
> IP Rules		ACL ID		1	• 201								
> IP Binding													
Configuratio	n	Extende	d ACL R	ule Table			_		_			-	
> Binding Tab	le	Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port

- b. Under IP Extended Rules, in the ACL ID list, select 10.
- c. Click Add.

The Extended ACL Rule Configuration screen displays.

System	Swite	hing	Routing	QoS	Security	Mor	itoring	Maint	lenance	Help	Index
Management S	ocurity	Access	Port Authenti	ication Tra	fic Control	ACL					
Basic		Exten	ded ACL F	Rule Confi	guration						
IP ACL		Exte	ended ACL R	ule Configu	ration(100-	199)				(7)	
IP Rules		ACLID			101		-1				
IP Binding		Rule ID	(1 to 24)		1		1				
Configuration Binding Table	n e	Action			CP	ermit		Egress Qu	eue (0 to 7}	
	60				@ D	eny					
		Match E	very		False	•					
		Protoco	l Type		TCP	-	(0 to 255))			
		TCP Flag	9		FIN	Ignore 💌	SYN	Set 🔹	RST 1	Ignore 💌	
		Founda	ID Address		PSH	Ignore _	ACK	Clear •	URG []	Ignore •	
		Source	IP Mask								
		Source	L4 Port				(0 to	65535)			
		Destina	tion IP Addre	55	Ĩ.						
		Destina	tion IP Mask		1	1.000	1				
		Destina	tion L4 Port				(0 to	65535)			
		Femilee	10 mm		C 10	0.000			0 4- 2.03		

- **d.** Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:
 - In the Rule ID field, enter 1.
 - For Action mode, select the **Deny** radio button.
 - In the Match Every field, select False.
 - In the Protocol Type list, select TCP.
 - For TCP Flag, in the SYN field, select Set, and in the ACK field, select Clear.
- e. Click Apply to save the settings.
- **10.** Add and configure an IP extended rule that is associated with ACL 102.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

System Swite	hing	Routing	QoS	S	ecurity	Mor	itoring	Maint	lenance	Help	Index	100
Management Security	Access	Port Authent	ication	Traffic Co	ntrol ACL							
Basic	IP Ext	ended Ru	lles									
> IP ACL	IP E	tended Ru	les									
> IP Rules	ACL ID		[102 •								
 IP Extended Fullet IP Binding 												
Configuration	Exte	nded ACL R	tule Table	e	_	_		_				_
> Binding Table		le Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port

- b. Under IP Extended Rules, in the ACL ID list, select 102.
- c. Click Add.

The Extended ACL Rule Configuration screen displays.

System Swite	ching Routing G	loS Security	Monitoring	Maintenance	Help	Index
Management Security	Access Port Authentication	Troffic Control ACL	ŕ			
Basic Advanced > IP ACL	Extended ACL Rule	Configuration onfiguration(100-199))		0	
 IP Rules IP Extended Rules IP Binding Configuration Binding Table 	ACL ID Rule ID (1 to 24) Action	102 1 © Permi	t.	Egress Queue 🦲 (0) to 7)	
	Natch Every Protocol Type TCP Flag	False • IP • FIN 10 PSH 10	(0 to 255) hore SYN	Ignore + RST I	anore 💌	
	Source IP Address Source IP Mask Source L4 Port Destination IP Address Destination IP Mask](0 to 65	5335)		
	Destination L4 Port	C 18 05	(0 to 65	535)		

- **d.** Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:
 - In the Rule ID field, enter 1.
 - For Action, select the **Permit** radio button.
 - In the Match Every field, select False.
 - In the Protocol Type list, select IP.
- e. Click Apply to save the settings.

11. Apply ACL 101 to port 44.

a. Select Security > ACL > Advanced > IP Binding Configuration.

Management	Security	Acces	a 1	Por	1 AL	thent	icat	ion	1 10	offic	: Co	ntrol		ACL													
Basic		IP B	lind	lin	g C	onf	igı	ıra	tio	n																	
IP ACL		В	indi	ing	Cor	nfigu	rat	ion																		0	
> IP Rules		ACL	ID					10	1 💌					Dj	rect	ion					Inbo	und	•				
IP Extende	d Rules	Sequ	Jenc	ie N	umb	er		1						(1	to 4	294	967	295)									
		Port	Sele	ctic	n Ta	able																					
» Binding Tal	ble	*	Uni	t I																							
		Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
			25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	
							113	100						1 25 1					110	111		V			110	112.0	
		I	nter	fac	e B	indir	10 5	Stat	us																	0	
		Inte	rfa	ce	DI	recti	ion			A	о с. т	VPE			A	CL 1	D			s	equ	enc	e Ni	umt	er		

- **b.** Under Binding Configuration, specify the following:
 - In the ACL ID list, select 101.
 - In the **Sequence Number** field, enter **1**.

- c. Click Unit 1. The ports display.
- d. Click the gray box under port 44. A check mark displays in the box.
- e. Click Apply to save the settings.

12. Apply ACL 102 to port 44.

a. Select Security > ACL > Advanced > IP Binding Configuration.

A screen similar to the following displays.

System	Switch	ing	Т	Ro	utir	ng l	Т	Q	oS		S	ocur	ity	Т	N	loni	itori	ng	Т	Μ	ainten	anc	e		Help	Т
Management Sec	curity	Acces	n 1	Po	t Au	thent	icati	on	T	raffic	Co	ntrol	Ľ	ACL	Ł											
lasic		IP B	Bind	din	g C	onf	igu	ira	tio	n																
IP ACL		B	ind	ing	Con	figu	rat	ion																	(1)	
IP Rules		ACL	ID					10	2 .					Di	nect	ion					Inboun	d •				
» IP Extended R	tules	Sequ	ueno	se N	umb	er		2						(1	to 4	294	967	295)								
F Binding		Port	Sele	ectio	n Ta	ble																				
 Binding Table 			Uni	é i																						
Contrast (Sector		Port	1	2	3	4	\$	6	7	8	9	10	11	12	13	14	15	16	17	18	19 20	21	22	23	24	
			25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43 44	45	46	47	48	
		-	10				23	115	127		1								111		~			253		
		I	nter	fac	e Bi	indi	ng S	stat	us																1	
		Inte	erfa	ce	Dir	recti	on		ACI	Ту	pe		A	U I)						Sequ	enc	e Ni	imb	er	
		0/4	42		Int	oun	d	1	IP #	CL			10	1							1					

- **b.** Under Binding Configuration, make the following selection and enter the following information:
 - In the ACL ID list, select 102.
 - In the Sequence Number field, enter 2.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 44.

A check mark displays in the box.

e. Click Apply to save the settings.

Configure the GSM7342S Switch

- 1. Create VLAN 40 with IP address 192.168.40.1/24.
 - a. Select Routing > VLAN > VLAN Routing Wizard.

PF Router zard ard 40	Disco	overy	VR	RP										(7)
eard ard 40			124		_									٢
ard 40			ĽÀ											1
40			14											
			1 A											
				NG EN	abled									
192.168.40).1		Ne	two	ik Mas	¢.			255	.255	.255	5.0	_	
678	9 1	10 11	12	13	14 1	5 16	17	18	19	20	21	22	23	24
30 31 32	33 3	34 35	36	37	38 39	40	41	42	43	44	45	46	47	48
	111115				110					1011		1104	3	
	6 7 8 30 31 32	6 7 8 9 30 31 32 33	6 7 8 9 10 11 30 31 32 33 34 35	6 7 8 9 10 11 12 30 31 32 33 34 35 36	6 7 8 9 10 11 12 13 30 31 32 33 34 35 36 37	6 7 8 9 10 11 12 13 14 15 30 31 32 33 34 35 36 37 38 35	6 7 8 9 10 11 12 13 14 15 16 30 31 32 33 34 35 36 37 38 39 40	6 7 8 9 10 11 12 13 14 15 16 17 30 31 32 33 34 35 36 37 38 39 40 41	6 7 8 9 10 11 12 13 14 15 16 17 18 30 31 32 33 34 35 36 37 38 39 40 41 42	6 7 8 9 10 11 12 13 14 15 16 17 18 19 30 31 32 33 34 35 36 37 38 39 40 41 42 43	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47

- **b.** Enter the following information:
 - In the Vlan ID field, enter 40.
 - In the IP Address field, enter 192.168.40.1.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 24 twice until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply to save VLAN 40.
- 2. Create VLAN 50 with IP address 192.168.50.1/24:
 - a. Select Routing > VLAN > VLAN Routing Wizard.

System	Swite	hing	ſ	Ro	outin	9		Q	٥5		S	scur	ity		N	loni	itori	ng		Ν	ain	tend	ince	i		Hel
Routing Table	IP	VLAN	A	RP	RI	P	os	PF	R	outer	Dise	ove	y ⊥	VR	RP											
VLAN Routing	1	VLA	NI	Roi	utin	ıg \	Wiz	are	d																	
VLAN Routing		V	LAN	NR	outi	ng \	Niz	ard																		Ē
		Vlan	ID					50		[
														Ľ/	IG E	nabl	ed			E						
		IP A	ıddr	255	1			19	2.16	68.50	0.1			Ne	two	nk M	lask				255	.255	.255	.0		
			Uni	t 1																						
		Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
			49	50	51	52	1					1		1211	15				223	1.2		1203	1		13	1
						111																				

- **b.** Enter the following information:
 - In the Vlan ID field, enter 50.
 - In the IP Address field, enter 192.168.50.1.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display.

- d. Click the gray box under port 25 twice until U displays.The U specifies that the egress packet is untagged for the port.
- e. Click Apply to save VLAN 50.
- 3. Create VLAN 200 with IP address 192.168.200.2/24.
 - a. Select Routing > VLAN > VLAN Routing Wizard.

OSPF /izard izard 200
izard izard 200
izard 200
200
192
6 7
9 30 3
1

- **b.** Enter the following information:
 - In the Vlan ID field, enter 200.
 - In the IP Address field, enter 192.168.200.2.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 48 twice until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply to save VLAN 200.
- 4. Create a static route with IP address 192.168.100.0/24:
 - a. Select Routing > Routing Table > Basic > Route Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP VLAN	ARP RIP C	SPF Rout	er Discovery	VRRP			
Basic	Rout	te Configura	tion					
	C	onfigure Routes						
Advanced		Route Type	Netwo	rk Address	Subnetmask	Next Hop IP	Address	Pref
		Static	192.1	68.100.0	255.255.255.0	192.168.200	.1	
	Le	arned Routes				- 18	n=	
	Rout	e Network				Next Hop		
	Type	Address	Subr	netmask	Protocol	Interface	Next Hop IP	Address
	Type	Address mic 192.168.4	0.0 255	255.255.0	Protocol	Interface Vian 40	Next Hop IP 192.168.40.	Address
	Dyna Dyna	Address imic 192.168.4 imic 192.168.5	0.0 255 0.0 255	255.255.0 .255.255.0	Protocol Local Local	Interface Vlan 40 Vlan 50	Next Hop IP 192.168.40. 192.168.50.	Address 1

- **b.** Under Configure Routes, make the following selections and enter the following information:
 - Select **Static** in the **Route Type** field.
 - In the Network Address field, enter 192.168.100.0.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Next Hop IP Address field, enter 192.168.200.1.
- c. Click Add.
- 5. Create a static route with IP address 192.168.30.0/24:
 - a. Select Routing > Routing Table > Basic > Route Configuration.

System	Switching	Routing G	oS Security	Monitoring	Maintenance	Help	Index
Routing Table	IP VLAN AR	P RIP OSPF	Router Discovery	VRRP			
Desic	Route 0	Configuration	(
Centigeration	Confi	gure Routes					
Advanced	The second se	toute Type	Network Address	Subnet mask	Next Hop IP A	ddress	Prefe
		Static 💽	192.168.30.0	255.255.255.0	192.168.200	1	
	E s	itatic	192.168.100.0	255.255.255.0	192.168.200.	1	1
	Learn	ed Routes					
	Route Type	Network Address	Subnet mask	Protocol	Next Hop Interface	Next Hop II	Address
	Dynamic	192.168.40.0	255.255.255.0	Local	Vlan 40	192.168.40	1
	Dynamic	192.168.50.0	255.255.255.0	Local	Vlan 50	192.168.50	.1
	Dynamic	192.168.200.0	255.255.255.0	Local	Vlan 200	192.168.20	0.2

- **b.** Under Configure Routes, make the following selection and enter the following information:
 - In the Route Type field, select Static.
 - In the Network Address field, enter 192.168.30.0.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Next Hop IP Address field, enter 192.168.200.1.
- c. Click Add.

Use ACLs to Configure Isolated VLANs on a Layer 3 Switch

This example shows how to isolate VLANs on a Layer 3 switch by using ACLs. In this example, PC 1 is in VLAN 24, PC 2 is in VLAN 48, and the server is in VLAN 38. PC 1 and PC 2 are isolated by an ACL but can both access the server. The example is shown as CLI commands and as a Web interface procedure.



Figure 11. Using ACLs to isolate VLANs on a Layer 3 switch

CLI: Configure One-Way Access Using a TCP Flag in ACL Commands

1. Enter the following CLI commands.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 24
(Netgear Switch) (Vlan)#vlan routing 24
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 24
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Config)#interface vlan 24
(Netgear Switch) (Interface-vlan 24)#routing
(Netgear Switch) (Interface-vlan 24)#ip address 192.168.24.1 255.255.255.0
(Netgear Switch) (Interface-vlan 24)#exit
(Netgear Switch) (Interface-vlan 24)#exit
```

2. Create VLAN 48, add port 1/0/48 to it, and assign IP address 192.168.48.1 to it.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 48
(Netgear Switch) (Vlan)#vlan routing 48
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 48
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) (Interface -vlan 48)#routing
(Netgear Switch) (Interface-vlan 48)#ip address 192.168.48.1 255.255.255.0
(Netgear Switch) (Interface-vlan 48)#exit
(Netgear Switch) (Interface-vlan 48)#exit
(Netgear Switch) (Interface-vlan 48)#exit
(Netgear Switch) (Interface-vlan 48)#exit
```

3. Create VLAN 38, add port 1/0/38 to it, and assign IP address 10.100.5.34 to it.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 38
(Netgear Switch) (Vlan)#vlan routing
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/38
(Netgear Switch) (Interface 1/0/38)#vlan participation include 38
(Netgear Switch) (Interface 1/0/38)#vlan pvid 38
(Netgear Switch) (Interface 1/0/38)#vlan pvid 38
(Netgear Switch) (Interface 1/0/38)#exit
(Netgear Switch) (Config)#interface vlan 38
(Netgear Switch) (Interface-vlan 38)#routing
(Netgear Switch) (Interface-vlan 38)#ip address 10.100.5.34 255.255.255.0
(Netgear Switch) (Interface-vlan 38)#exit
```

4. Enable IP routing on the switch.

(Netgear Switch) (Config)#ip routing

5. Add a default route so that all the traffic without a destination is forwarded according to this default route.

(Netgear Switch) (Config) #ip route default 10.100.5.252

6. Create ACL 101 to deny all traffic that has the destination IP address 192.168.24.0/24.

(Netgear Switch) (Config)#access-list 101 deny ip any 192.168.24.0 0.0.0.255

7. Create ACL 102 to deny all traffic that has the destination IP address 192.168.48.0/24.

(Netgear Switch) (Config)#access-list 102 deny ip any 192.168.48.0 0.0.0.255

8. Create ACL 103 to permit all other traffic.

(Netgear Switch) (Config)#access-list 103 permit ip any any

9. Deny all traffic with the destination IP address 192.168.48.0/24, and permit all other traffic.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip access-group 102 in 1
(Netgear Switch) (Interface 1/0/24)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/24)#exit
```

10. Deny all traffic with the destination IP address 192.168.24.0/24, and permit all other traffic.

```
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#ip access-group 101 in 1
(Netgear Switch) (Interface 1/0/48)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/48)#exit
```

Web Interface: Configure One-Way Access Using a TCP Flag in an ACL

- 1. Create VLAN 24 with IP address 192.168.24.1.
 - a. Select Routing > VLAN > VLAN Routing Wizard.

A screen similar to the following displays.



- **b.** Enter the following information:
 - In the Vlan ID field, enter 24.
 - In the IP Address field, enter 192.168.24.1.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 24 twice until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply to save VLAN 24.
- 2. Create VLAN 48 with IP address 192.168.48.1.

a. Select Routing > VLAN > VLAN Routing Wizard.

A screen similar to the following displays.

System	Swite	hing	ſ	Ro	utir	g		Q	oS		S	ecu	rity		N	Noni	tori	ng		N	lain	tend	ince	3		Hel
Routing Table	I IP I I	VLAN	A	RP	RI	P	os	PF	R	oute	Dis	cove	ny I	VR	RP											
YLAN Routin	0	VLA	NI	Roi	utir	ŋ	Wiz	ar	d																	
VLAN Routing	a	۷	LAN	N Ro	outi	ng '	Wiz	ard																		C
		Vlan	ID					48																		
														L/	G E	nabl	ed									
		IP A	ddr	e55				19	2.16	8.4	8.1		- 1	Ne	two	irk M	lask				255	.255	.255	5.0		
		-	Uni	t 1																						
		Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
			49	50	51	52		_	-	-	_		_	-	_	_	-			_	_	-	_	_	_	CH I

- **b.** Enter the following information:
 - In the Vlan ID field, enter 48.
 - In the IP Address field, enter 192.168.48.1.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 48 twice until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply to save VLAN 48.
- 3. Create VLAN 38 with IP address 10.100.5.34.
 - a. Select Routing > VLAN > VLAN Routing Wizard.

System	Swite	ching	ſ	Ro	outin	g	Ľ	Q	٥S		S	scur	ity		h	loni	tori	ng		Μ	ain	tenc	ance	2		Help
Routing Table	IP. I	VIAN	A	RP	RI	PI	os	PF	R	outer	Dis	ove	γI	VR	RP											
VLAN Routing	6	VLA	NI	Roi	utir	ıg '	Wiz	ar	d																	
VLAN Routing		. V	LAN	N R	outi	ng \	Wiz	ard																		Ō
	M	Vian	ID	2				38	8																	
														LA	GE	nabl	ed									
		IP A	ddr	e55			- 1	10	.100).5.3	4			Ne	two	nik M	lask				255	.255	.255	5.0		
		۰.	Uni	t 1																						
		Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
			49	50	51	52			_		-	-	-	-		0	-	_	-		_		-	_		_
					- () 																					

- **b.** Enter the following information in the VLAN Routing Wizard:
 - In the Vlan ID field, enter 38.
 - In the IP Address field, enter 10.100.5.34.

- In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display.
- **d.** Click the gray box under port **38** twice until **U** displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply to save VLAN 38.
- 4. Enable IP routing:
 - a. Select Routing > IP > Basic > IP Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Routing Table	🕑 VLAN	ARP RIP O	OSPF Route	ar Discovery VR	RP	
Basic	attan	IP Config	guration			
Statistics	auon	IP Conf	figuration			۲
Advanced		Default Tim	e to Live	30		
		Routing Mo	de	🔿 Disable	Enable	
		IP Forward	ing Mode	O Disable	Enable	
		Maximum N	lext Hops	2		

- **b.** Under IP Configuration, make the following selections:
 - For Routing Mode, select the **Enable** radio button.
 - For IP Forwarding Mode, select the **Enable** radio button.
- c. Click Apply to enable IP routing.
- 5. Create an ACL with ID 101.
 - a. Select Security > ACL > Advanced > IP ACL.

System	Swite	hing	Routing	QoS	Security	Monitoring	Maintenance	Help
Management	Security	Access	Port Authentic	ation Tra	fic Control AC	L		
Basic Advanced		IP AC					•	
 IP Rules IP Extender IP Binding 	d Rules	Curren Maxim	t Number of AC um ACL	L 0)			
Configurati	on sle	IP .	ACL Table				0	
		1	P ACL ID		Rules	Туре		
			P ACL ID		Rules	Туре		

- **b.** In the IP ACL Table, in the **IP ACL ID** field, enter **101**.
- c. Click Add.
- 6. Create an ACL with ID 102.
 - a. Select Security > ACL > Advanced > IP ACL.

Management Security Basic	Access Port Auther	ntication Tral	fic Control AC	L		
Basic	IP ACL					
a 1P ACL	IP ACL				•	
> IP Rules	Current Number of	ACL 1				
 IP Extended Rules IP Binding Configuration 	Maximum ACL	100)			
» Binding Table	IP ACL Table				(1)	
	IP ACL ID		Rules	Туре		
	102					
	F 101		0	Extended		

- b. In the IP ACL Table, in the IP ACL ID field, enter 102.
- c. Click Add.
- 7. Create an ACL with ID 103.
 - a. Select Security > ACL > Advanced > IP ACL.

System	Swite	hing	Routing	QoS	Security	Monitoring	Maintenance					
Management	Security	Access	Port Authentic	ation Traf	fic Control AC	Ĺ						
MAC ACL	1	IP ACL										
IP ACL		IP		0								
> IP Rules		Curren	nt Number of ACI	L 2								
> IP Extende	d Rules	Maxim	num ACL	100	1							
> IP Binding	0.0											
» Binding Ta	ble	IP	ACL Table									
		1	P ACL ID		Rules	Туре						
			103									
		101			0	Extended						
			02		0	Extended						

- b. In the IP ACL ID field of the IP ACL Table, enter 103.
- c. Click Add.
- 8. Add and configure an IP extended rule that is associated with ACL 101:
 - a. Select Security > ACL > Advanced > IP Extended Rules.

System Swite	hing	Ro	gnitud	QoS	S	ecurity	Mor	itoring	Maint	enance	Help	Index	LOOD	sit)
Management Security	Acces	s Por	rt Authenti	cation 1	Iraffic Co	introl ACL	<u> </u>							
Basic	IP E	xten	ded Ru	les										
> IP ACL	н	P Exter	nded Rul	es										
> IP Rules	ACL	ID		[]	.01 •									
IP Extended Rules														
Configuration	E	xtende	d ACL R	ule Table	1									
> Binding Table	-	Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port	Se Ty

- b. Under IP Extended Rules, in the ACL ID field, select 101.
- c. Click Add. The Extended ACL Rule Configuration screen displays.

System Switch	ing Routing QoS	Security Monitoring Maintenance Help Ind
Management Security	Access Port Authentication Traff	ic Control ACL
MAC ACL	Extended ACL Rul	e Configuration
> IP ACL	Extended ACL Rule	Configuration(100-199)
 IP Rules IP Extended Rules 	ACL ID	101
IP Binding Configura	tion Rule ID (1 to 23)	1
» Binding Table	Action	O Permit Egress Queue (0 to 6)
		Deny
	Match Every	False 💌
	Protocol Type	IP 💉 (0 to 255)
	TCP Flag	FIN Ignore SYN Ignore RST Ignore
		PSH Ignore 👻 ACK Ignore 👻 URG Ignore 👻
	Source IP Address	
	Source IP Mask	
	Source L4 Port	(0 to 65535)
	Destination IP Address	192.168.24.0
	Destination IP Mask	0.0.0.255
	Destination L4 Port	(0 to 65535)
	Service Type	O 18 DSCR (0 to 63)

- **d.** Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:
 - In the **Rule ID** field, enter **1**.
 - For Action, select the **Deny** radio button.
 - In the Match Every field, select False.
 - In the **Destination IP Address** field, enter **192.168.24.0**.
 - In the Destination IP Mask field, enter 0.0.0.255.
- e. Click Apply to save the settings.
- 9. Add and configure an IP extended rule that is associated with ACL 102.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

Management Security	Acces	e Po	Authenti	cation	Iroffic Co	atrol ACL							
	TOF		de d Du	las									
Basic	IP E	xten	aed Ru	les									
* IP ACL	IP Extended Rules												
> IP Rules	ACL	ID		[1	• 201								
- IF Extended Fulles	1												
Configuration	E	xtende	d ACL R	ule Table									
» Binding Table		Rule ID	Action	Assign Queue	Match Every	Protocol Keyword	TCP Flag	Source IP	Source IP	Source L4	Destination IP Address	Destination IP Mask	Destinatio L4 Port

- b. Under IP Extended Rules, in the ACL ID field, select 102.
- c. Click Add. The Extended ACL Rule Configuration screen displays.

System	Switching	Routing QoS	Security	Monitoring	Maintenance	Help Index						
Management	Security Access	Port Authentication Tra	fic Control AC									
MAC ACL		Extended ACL Ru	le Configura	tion								
> IP ACL		Extended ACL Rule Configuration(100-199)										
> IP Rules	ed Bakes	ACL ID		102								
> IP Binding	Configuration	Rule ID (1 to 23)		1								
> Binding T	able	Action		O Permit	Egress Qu	s Queue (0 to 6)						
				O Deny								
		Match Every		False 💌								
		Protocol Type		1P (0 to 255)								
		TCP Flag		FIN Ignore	SYN Ignore	RST Ignore 🗸						
				PSH Ignore	ACK Ignore 😒	URG Ignore 💚						
		Source IP Address										
		Source IP Mask										
		Source L4 Port		~	(0 to 65535)							
		Destination IP Address		192.168.48.0								
		Destination IP Mask		0.0.0.255								
		Destination L4 Port		~	(0 to 65535)							
		Service Type		O IP DSCP		(0 to 63)						

- **d.** Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:
 - In the Rule ID field, enter 1.
 - For Action mode, select the **Deny** radio button.
 - In the Match Every field, select False.
 - In the Destination IP Address field, enter 192.168.48.0.
 - In the Destination IP Mask field, enter 0.0.0.255.
- e. Click Apply to save the settings.
- **10.** Add and configure an IP extended rule that is associated with ACL 103:
 - a. Select Security > ACL > Advanced > IP Extended Rules.
| System Switching | ROUTI | 18 1 | 305 5 | econity | Monito | ring | Maini | enance | rteip | Index | | _ |
|------------------------------|---------|---------------|----------------|----------------|---------------------|-------------|-------------------------|----------------------|----------------------|---------------------------|------------------------|-----------------------|
| Management Security Access | Port Au | thentication | n Troffic Co | ntrol Al | cit. | | | | | | | |
| MAC ACL | IP E | ktended | l Rules | | | | | | | | | |
| > IP ACL | IP | Extende | d Rules | | | | | | | | | |
| > IP Rules | ACLI | D | | 103 💌 | | | | | | | | |
| > IP Binding Configuration | | | | | | | | | | | | |
| * Binding Table | Ex | tended A | CL Rule Tab | le | | | | | | | | |
| | | Rule
ID Ac | tion Assign | Match
Every | Protocol
Keyword | TCP
Flag | Source
IP
Address | Source
IP
Mask | Source
L4
Port | Destination
IP Address | Destination
IP Mask | Destinatio
L4 Port |

- b. Under IP Extended Rules, in the ACL ID field, select 103.
- c. Click Add. The Extended ACL Rule Configuration screen displays.

System	Switching	Routing QoS	Security	Monitoring	Maintenance	Help Inde
Managemen	Security Access	Port Authentication Traffic	Control AC	i -		
MAC ACL		Extended ACL Rule	e Configura	ition		
> IP ACL		Extended ACL Rule	Configuratio	(100-199)		(1)
> IP Rules	led Rules	ACLID		103		
> IP Bindin	g Configuration	Rule ID (1 to 23)		1		
> Binding T	able	Action		O Permit	Egress Qu	ieue (0 to 6)
				O Deny		
		Match Every		False 💙		
		Protocol Type		1P 💌	(0 to 255)	
		TCP Flag		FIN Ignore	SYN Ignore 9	RST Ignore
				PSH Ignore ~	ACK Ignore 😒	URG Ignore
		Source IP Address				
		Source IP Mask				
		Source L4 Port		~	(0 to 65535)	
		Destination IP Address				
		Destination IP Mask				
		Destination L4 Port		~	(0 to 65535)	
		Service Type		O IP DSCP	- International	(0 to 63)

- **d.** Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:
 - In the Rule ID field, enter 1.
 - For Action mode, select the **Permit** radio button.
 - In the Match Every field, select False.
 - In the Protocol Type field, select IP.
- e. Click Apply to save the settings.
- 11. Apply ACL 102 to port 24:
 - a. Select Security > ACL > Advanced > IP Binding Configuration.

System	Swite	hing		Ro	uting		Q	oS		S	ecur	ity		٨	Aoni	itori	ng		Ν	ain	ten	anci	e		Help
Management	Security	Acces	s I	Por	t Authe	ntical	ion	1	roffic	Co	ntrol	I.	ACL												
MAC ACL		IP E	Bind	ling	g Cor	nfig	ura	tio	n																
IP ACL		B	indi	ng	Config	jura	tion																		0
IP Rules		ACL	ID				10	2 🔹					Di	nect	lion					Inb	ound				
> IP Extende	d Rules	Seq	uenc	e N	umber		1						(1	to	1294	967	295)	<u> </u>	_						
 IP Einding Configuration 		Port	Sele	ctio	n Table																				
» Binding Tal	ble	*	Uni	t 1																					
		Port	1	2	3 4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			25	26	27 28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
			49	50	51 52	2					-					11		1		1.000					-
		I	nter	fac	e Binc	ling	Stat	tus																	0
		Inte	erfa	ce	Dire	tion	h		A	CL T	уре			A	CL 1	D			5	equ	ienc	e N	uml	ber	

- **b.** Under Binding Configuration, make the following selection and enter the following information:
 - In the ACL ID field, select 102.
 - In the Sequence Number field, enter 1.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 24.

A check mark displays in the box.

- e. Click Apply to save the settings.
- **12.** Apply ACL 101 to port 48:
 - a. Select Security > ACL > Advanced > IP Binding Configuration.

System	Swite	hing	T	Ro	utin	9	í.	QoS	E.	S	ecu	rity	T	N	Non	itori	ng	Υ	Μ	ain	ten	anc	8		Help
Management	Security	Acces	us I	Por	t Au	thenti	catio	n	Troff	ic Co	ntrol	el M	ACL	e.											
MAC ACL		IP E	Bind	ling	g C	onfi	igur	ati	on																
IP ACL		в	indi	ng	Con	figu	ratio	n																	Ð
> IP Rules		ACL	ID					101	-				Di	rect	ion					Inbo	oune	•			
» IP Extende	d Rules	Seq	uenc	e Ni	umb	er		1					(1	to -	1294	967	295)								
> IP Binding		Port	Sele	ctio	n Ta	ble																			
» Binding Ta	ble		Unit	11																					
		Port	1	2	3	4	5 6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			25	26	27	28	29 3	0 3	1 33	: 33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
			49	50	51	52			_					-		-	-		-						~
					100																				
		1	nter	fac	e Bi	ndin	ig St	atu	\$																٢
		Inte	erfa	ce	Dir	ecti	on	A	CL T	pe		AC	L II	6						Se	qu	inci	N	ımb	er
		1/0	/24		Inb	ound	ł	IP	ACL			10	2							1					

- **b.** Under Binding Configuration, make the following selection and enter the following information:
 - In he ACL ID field, select 101.
 - In the Sequence Number field, enter 1.
- c. Click Unit 1. The ports display.
- d. Click the gray box under port 48.

A check mark displays in the box.

- e. Click Apply to save the settings.
- **13.** Apply ACL 103 to port 24 and port 48:
 - a. Select Security > ACL > Advanced > IP Binding Configuration.

A screen similar to the following displays.

System Swite	hing	T	Ro	outin	ŋg	Υ	Q	oS		S	ecui	ity		N	١on	itori	ng	η	Ν	ain	ten	anc	8		Help
Management Security	Acces	8 I	Po	rt Au	then	ticat	ion	IT	roffi	: Co	ntrol	10	ACL												
MAC ACL	IP B	Bind	din	g C Cor	on	figu	ira	tio	n																(7)
> IP Rules	ACL	ID					10	3•	1				Di	nect	ion					Inb	ound	•			
> IP Extended Rules	Sequ	Jeno	ce N	umb	er		2		2				(1	to 4	1294	967	295)			-					
Configuration	Port	Sele	ectio	n Ta	ble																				
> Binding Table	•	Uni	it 1																						
	Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
		49	50	51	52		-										_			_		_			V
	I	nter	rfac	e B	indi	ing s	Stat	us																	1
	Inte	rfa	ce	Di	rect	ion	Т	ACI	Ту	pe		A	L II	0						Se	que	ence	e Ni	ımb	er
	1/0/	24		Ini	bour	hd	1	IP /	CL			10	2							1					
	1/0/	48		Ini	bour	nd		IP A	CL			10	1							1					

- **b.** Under Binding Configuration, make the following selection and enter the following information:
 - In the ACL ID field, select 103.
 - In the Sequence Number field, enter 2.
- c. Click Unit 1. The ports display.

Configure the following ports:

- Click the gray box under port 24. A check mark displays in the box.
- Click the gray box under port **48**. A check mark displays in the box.
- d. Click Apply to save the settings.

Set up a MAC ACL with Two Rules

The example is shown as CLI commands and as a Web interface procedure.

CLI: Set up a MAC ACL with Two Rules

1. Create a new MAC ACL acl_bpdu.

```
(Netgear Switch) #
(Netgear Switch) #config
(Netgear Switch) (Config)#mac access-list extended acl_bpdu
```

2. Deny all the traffic that has destination MAC 01:80:c2:xx:xx:xx.

```
(Netgear Switch) (Config-mac-access-list)#deny any 01:80:c2:00:00:
00:00:00:ff:ff:ff
```

3. Permit all the other traffic.

```
(Netgear Switch) (Config-mac-access-list)#permit any
(Netgear Switch) (Config-mac-access-list)#exit
```

4. Apply the MAC ACL acl_bpdu to port 1/0/2.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#mac access-group acl_bpdu in
```

Web Interface: Set up a MAC ACL with Two Rules

- 1. Create MAC ACL 101 on the switch.
 - a. Select Security > ACL > MAC ACL.

System Sw	tching Routing (QoS Security	Monitoring	Mointenance	Help	Index
Management Security	Access Port Authentication	1 Troffic Control ACI				
MAC AGE	MAC ACL					
. MAC Rules	MAC ACL			00		
MAC Binding	Current Number of ACL	0				
Configuration Disiding Table	Maximum ACL	100				
IP ACL						
10001040	MAC ACL Table			0		
	Name	Rules	Direction			
	acl_bpdu					

- **b.** In the **Name** field, enter **acl_bpdu**.
- c. Click Add to create ACL acl_bpdu.
- 2. Create a new rule associated with the ACL acl_bpdu.
 - a. Select Security > ACL > MAC ACL > MAC Rules.

System 5	witching	Rooting	405 5	ecurity	Monit	oring Maintena	nce Help	Index
Management Secur	ity Access	Port Authentication	Traffic Co	introl AC	Ŀ			
MAC ACL	MAC R	ules						
a MAC Roles	Rule	\$				10		
MAC binding Configuration Binding Table	AELN	ime acl_bpdu	1					
IP ACL	Rule	Table				-		
	10	Action	Assign Queue Id	Match Every	CoS	Destination MAC	Destination MAC Mask	Eth
		Deny 3				01:00:c2:00:00:00	00:00:00:#:#:#	

- a. In the ACL Name field, select acl_bpdu.
- **b.** In the **Action** field, select **Deny**.
- c. Enter the following information in the Rule Table.
 - In the ID field, enter 1.
 - In the **Destination MAC** field, enter **01:80:c2:00:00:00**.
 - In the Destination MAC Mask field, enter 00:00:00:ff:ff:ff.
- d. Click the Add button.
- 3. Create a another rule associated with the ACL acl_bpdu.
 - a. Select Security > ACL > MAC ACL > MAC Rules.

System Sw	itching	Re	Q gnitur	oS S	ecurity	Monit	oring Maintena	nce Help	Index
Monogement Security	y I Acce	na i Po	rt Authentication	Troffic Co	introl ACL				{
MAC ACL	MA	C Rule	s						
A MAC ALL	100	tules					10		
· MAC Binding	A	L. Name	aci_bpdu •						
Binding Table									
IP ACL		Rule Tal	ale						
		TD	Action	Assign Queue Id	Match Every	CoS	Destination MAC	Destination NAC Nask	Eth
		2	Permit 👻		- 2				
		1	Deny		False	-	01:80:C2:00:00:00	00:00:00:FF:FF:FF	

- a. Select acl_bpdu in the ACL Name field.
- **b.** Enter the following information in the Rule Table.
 - In the ID field, enter 2.
 - In he Action field, select the Permit.
- **c.** Click the **Add** button.
- **4.** Apply the ACL acl_bpdu to port 2.
 - a. Select Security > ACL > MAC ACL > MAC Binding Configuration.

System	Swite	hing	1	Routi	ng	6	05		Se	curity		Moi	literi	°8	N	lainten	ance	: 10	Help
Monogement 5	iecurity:	Acces	61	Port A	thent	ication	1	roffi	c Con	trol	ACL								
HAL ACL		MAC	Bi	nding	Co	nfigu	rat	ion											
* MAC Rules		B	indi	ng Cor	figu	ration													D.
- HAC TINUE		ACL	ю			ac	j_bp	du 🔹			Di	metion				Inbound	*		
Currigerate	22	Sequ		Numb	er.	1					(I	to 829	49672	15)					
IP ACL	er.	Port	Selec	tion Ta	ble														
105.004		1	Unit	4															
		Port	1	2 3	-4	5 6	7	8	9	10 1	1 12	13 1	4 15	16 1	17 11	19 20	1 21	22 23	24
		1	25	26 27	28		-			1000		1000				1.000		-	100
		I	iteri	ace B	indir	ng Sta	tus												100
		Inte	rfac	e -	Dire	ection			ACL	Туре		AC	L 10			Sequen	ice N	umber	

- **b.** Enter the following information in the MAC Binding Configuration.
 - IN the ACL ID field, select acl_bpdu.
 - In the Sequence Number field, enter 1.
- c. Click the Unit 1. The ports display.
- d. Click the gray box under port 2. A check mark displays in the box.
- e. Click Apply to save the settings.

ACL Mirroring

This feature extends the existing port mirroring functionality by allowing you to mirror a designated traffic stream in an interface using ACL rules. Define an ACL rule matching the desired traffic with the option mirror to an interface. Any traffic matching this rule will be copied to the specified mirrored interface.



Figure 12. ACL mirroring

CLI: Configure ACL Mirroring

The script in this section shows how to mirror the traffic stream received from a host in an interface. These examples mirror the traffic from the host 10.0.0.1 connected to the interface 1/0/1.

1. Create an IP access control list with the name monitorHost.

```
(Netgear Switch) (Config)# ip access-list monitorHost
```

2. Define the rules to match host 10.0.0.1 and to permit all others.

```
(Netgear Switch) (Config-ipv4-acl)# permit ip 10.0.0.1 0.0.0.0 any mirror 1/0/19
(Netgear Switch) (Config-ipv4-acl)# permit every
```

3. Bind the ACL with interface 1/0/1.

(Netgear Switch) (Interface 1/0/1)#ip access-group monitorHost in 1

4. View the configuration.

```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1 Maximum number of ACLs: 100
ACL ID/Name
           Rules Direction
                        Interface(s)
                                    VLAN(s)
_____ ____
                        _____
                                     _____
monitorHost
           2
                inbound
                        1/0/1
(Netgear Switch) #show ip access-lists monitorHost
 ACL Name: monitorHost
 Inbound Interface(s): 1/0/1
 Rule Number: 1
 Action..... permit
 Match All..... FALSE
 Source IP Address..... 10.0.0.1
 Source IP Mask..... 0.0.0.0
 Mirror Interface..... 1/0/19
 Rule Number: 2
 Action..... permit
 Match All..... TRUE
```

Web Interface: Configure ACL Mirroring

- 1. Create an IP access control list with the name monitorHost on the switch.
 - a. Select Security > ACL > Advanced > IP ACL.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management S	Security Access	Port Authentic	ation Traffi	c Control Cor	itrol ACL			
Basic Advanced	I	P ACL	ation					7
 > IP Rules > IP Extended > IPv6 ACL 	i Rules	Current Number Maximum ACL	of ACL		0			
> IPv6 Rules > IP Binding	6	IP ACL Tabl	e				(D
Configuratio	n l	IP ACL		Rules		Туре		
 Binding Tab Vlan Binding 	le g Table	monitorH	ost					

- b. In the IP ACL ID field, enter monitorHost.
- c. Click Add to create ACL monitorHost, and the following screen displays:

System Swite	hing Routing QoS	Security	Monitoring	Maintenance	Help Index
Management Security	Access Port Authentication	Traffic Control Co	ntrol ACL		
Basic Advanced s IP ACL IP Rules IP Extended Rules IP 6 ACL	IP ACL IP Configuration Current Number of ACL Maximum ACL		100		۲
» IPv6 Rules » IP Binding	IP ACL Table		-6		۲
Configuration > Binding Table	IP ACL	Rules	Туре		
Vlan Binding Table	monitorHost	0	Named I	P ACL	

- 2. Create a rule to match host 10.0.0.1 in the ACL monitorHost.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

System	Switchin	ng l	Routin	97 3	QoS.	Security	Monitor	ring N	Aainteria	nce l	Help	Index
Monogement	Security /	locess]	Port Aut	hentication	. [. Traffic	Control Co	ntrol ACL					
Basic		Ext	ende	d ACL	Rules							
Advanced		1	IP Rule	rs :							(D)	
+ IP Rules		AC	LID/N	NHE			monitori	fost +				
. IPv6 ACL	d Hoder.	6.0	Extend	ed ACL F	Rule Table							
 IPv6 Rules IP Binding Configuration 	on		Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Addres
> Binding Tat	ble	No 22	des have	been config	ured for thu A	CL.						

b. Click **Add**, and the Extended ACL Rule Configuration screen displays.

System	Switching	Routing	QoS	Security	Monitoring N	laintenance	Help	Index
Manogement	Security Acce	as Port Authentication	m Traffi	e Control Co	entrol ACL			
Basic Advanced > IP ACL		Extended ACL	Rule Con	onfiguratio	n 00-199)			
* IP Rules		ACL ID/Name	monitorHe	fac				
- IF extends	d Puler	Rule ID	1		1			
IFV6 ALL		Action	· Perm	e	Egress Queue	0 • (0-6)		
IP Binding	i.		C Deny					
Configurati	on	Logging	. Disab	le	Enable			
Binding Tal	ble	Hirror Interface	1/0/19	-				
Vian Bindin	g Table	Redirect Interface		2				
		Hatch Every	False +					
		Protocol Type	Other .		(1 to 255)			
		TCP Flag	URG		Ignore -	ACK	Igours -	PSH Innore
			RST		Janore -	SYN	Ignane -	FIN Ignore
		Sec IP Address	10.0.0.1					
		Sec IP Mask	0.0.0.0					
		Sec L4 Poet	Other	•	(0 to 65535)			
		Dst IP Address						
		Dst IP Mask	L					
		Dat L4 Port	Other		(0 to 65535)			
		Service Type	IP DS	CP	other -	(0-63)		
			C IP Pro	ecedence	0 = (0-7)			
			C IP TO	S		(00-ff)		

- c. In the Rule ID field, enter 1.
- d. For Action, select the **Permit** radio button.
- e. In the Mirror Interface list, select 1/0/19.
- f. In the Src IP Address field, enter 10.0.0.1.
- g. In the Src IP Mask field, enter 0.0.0.0.
- h. Click Apply.
- 3. Create a rule to match every other traffic.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

System S	witching	Routin		QoS 6	Security	Monito	ring N	laintena	nce I	felp	Index	
Management Securi	ty Access	Port Aut	hentication	1 Traffic (Control Co	ntrol ACL						
Basic	E	tende	d ACL I	Rules								
Advanced	6	IP Rule	s							1		
> IP Rules	٨	CL ID/NA	ME			monitor	Host +					
. IPv6 ACL		Extend	ed ACL F	Rule Table								
 IPv6 Rules IP Binding Configuration 		Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Natch Every	Protocol Keyword	TCP Flag	Source IP Address	Source Mask
> Binding Table	en E	1	Permit	Disable	0	1/0/19		False			10.0.0.1	0.0.0.0

b. Click Add, and a screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Monogement	Security Acces	Port Authentication	on Traffic	Control Co	ACL	
Basic		Extended ACL	Rule Co	nfiguratio	n	
+ IP ACL		Extended ACL	Rule Confi	guration(10	0-199)	
> 1P Rules		ACL ID/Name	monitorHos	ŧ		
A TRUCK A CL	d Ruben	Rule 1D	2			
> IPV6 Rules		Action	· Permit		Egress Queue	0 • (0-6)
+ IP Binding			Deny			
Configurati	on	Logging	Disable	t:	C Enable	
* Binding Tal	ble	Hirror Interface	+			
Vien Bindin	g Table	Redirect Interface				
		Match Every	True +			

- c. In the Rule ID field, enter 2.
- d. Select the Permit radio button.
- e. In the Match Every field, select True.
- f. Click Apply.

At the end of this configuration a screen similar to the following displays.

System Switchi	ing I	Routing	Q	oS	Security	Monitori	ing Mi	aintenar	H H	elp l	ndex	
Management Security	Access P	ort Auth	entication	Traffic C	iontrol Cor	Hol ACL						
Basic	Exte	ended	ACL P	ules								
Advanced		P Rules								171		
. IP Rules	ACL	ID/NA	46			monitorH	ost •					
> 19 Extended Roles												
+ IPv6 Rules	E	xtende	d ACL R	ule Table						_		
 IP Binding Configuration Binding Table 		Rule 1D	Action	Logging	Assign Queue ID	Nirrror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source I Mask
+ Vian Binding Table	B	4	Permit	Disable	0	1/0/19		False		1	10.0.0.1	0.0.0.0
		2	Permit	Disable	0			True				

- 4. Bind the ACL with interface 1/0/1.
 - a. Select Security > ACL > Advanced > IP Binding Configuration.

System	Switz	hing	R	outing		G	loS	8		Sec	orit	ÿ		Mo	nite	ring		1	Aaini	lena	nce		Н	elp	
Management	Security	Access	Po	rt Auth	ontic	ation	Į.	Traf	fic (Cont	rol	G	antro	U	AC	Ļ									
Basic		IJ	P Bi	ndin	g C	onfi	igu	ira	tio	n															
IP ACL		. 6	B	nding	Cor	nfigu	rati	ion																	
IP Rules				D.				mo	nite	rHo	st 🔹			D	nect	ion				Inb	ound	•			
 IP Extende 	d Rules		iequ	ence N	umb	er		1			-			¢	uto 4	294	9672	95)							
IPv6 ACL		P	ort S	electi	in Ta	able																			
the kules			100	their 1																					
Configurate		P	ort	1 2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	7 1	8 19	20	21	22	23	2
Binding Tal	ble		1211	1			1	10	101	111			1					1		1	111	100			
a Man Bindin	n Table		10	25 26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	11 43	2 43	44	45	46	47	4

- b. In the Sequence Number field, enter 1.
- c. In the Port Selection Table, click **Unit 1** to display all the ports for the device.
- d. Select the Port 1 check box.
- e. Click Apply.

	a				
Management Security A	ccess Port Authentication	Traffic Control C	iontrol ACL		
Basic	IP Binding Confi	guration			
Advanced + IP ACL	Binding Configu	ration			
* IP Rules	ACLID	monitorHost	Direction	Inbound -	F.
» IP Extended Rules	Sequence Number	0	(1 to 42949672	95)	
> IPv6 ACL	Port Selection Table				
- UP Continue	+ Unit 1				
Cashger stoph					
Binding Table	Interface Bindin	g Status			
e aven denning i adre	Interface Direction	on ACL Type	ACL ID/Name	Sequenc	e Numbr
	1/0/1 Inhound	t IP ACL	monitoittost	1	

ACL Redirection

This feature redirects a specified traffic stream to a specified interface.



Figure 13. ACL Redirect

CLI: Redirect a Traffic Stream

The script in this section shows how to redirect an HTTP traffic stream received in an interface to the specified interface. This example redirects the HTTP traffic stream received in port 1/0/1 to port 1/0/19.

1. Create an IP access control list with the name redirectHTTP.

(Netgear Switch) (Config) #ip access-list redirectHTTP

2. Define a rule to match the HTTP stream and define a rule to permit all others.

(Netgear Switch) (Config-ipv4-acl)# permit tcp any any eq http redirect 1/0/19 (Netgear Switch) (Config-ipv4-acl)# permit every

3. Bind the ACL with interface 1/0/1.

(Netgear Switch) (Interface 1/0/1)#ip access-group redirectHTTP in 1

4. View the configuration.

(Netgear Switch) # show ip	access-	lists		
Current number of ACLs: 1	Maximum	number of AC	Ls: 100	
ACL ID/Name	Rules	Direction	<pre>Interface(s)</pre>	VLAN(s)
redirectHTTP	2	inbound	1/0/1	
(Netgear Switch) #show ip	access-	lists redirec	tHTTP	
ACL Name: redirectHTTP				
Indound Interface(s): 1/0/.	L			
Pule Number: 1				
Action			permit	
Match All			FALSE	
Protocol			6(tcp)	
Destination L4 Port Keyword	1		80(www/http)	
Redirect Interface			1/0/19	
Rule Number: 2				
Action			permit	
Match All			TRUE	

Web Interface: Redirect a Traffic Stream

This example redirects the HTTP traffic stream received in port 1/0/1 to port 1/0/19.

- 1. Create an IP access control list with the name redirectHTTP.
 - a. Select Security > ACL > Advanced > IP ACL.

A screen similar to the following displays.

System	Switching	Routing	QoS Securit	y Monitoring	Maintenance	Help
Management	Security Access	Port Authenti	cation Traffic Control	Control ACL		
Basic	1	IP ACL				
= IP ACL		IP Configu	ration			- (
> IP Rules		Current Numbe	r of ACL	0		
> IP Extende	d Rules	Maximum ACL		100		
> IPv6 Rules		IP ACL Tab	ale			(
Configurat	ion	IP ACL	Rules		Туре	
 Binding Ta Vlan Bindir 	ble ng Table	redirecti	нттр			

- b. In the IP ACL field, enter redirectHTTP.
- c. Click Add to create the IP ACL redirectHTTP.

A screen similar to the following displays.

System	Switching	Routing	GoS	Security	Monitoring	Maintenance	Help
Management Se	curity Acce	a Port Authentic	cation Traffic (Control Con	nol ACL		
Basic		IP ACL					
A IP ACL		IP Configur	ation				()
• IP Rules	n de la	Current Number	of ACL		3		
+ IPv6 ACL	n unes	Maximum ACL			1997		
 IPv6 Rules IP Binding 		IP ACL Tab	le				
Configuration	n	IP ACL		Rules	Туре		
Binding Table	e and a second						
* Vian Binding	Table	III redirecter	CTP.	0	Named I	PACL	

- 2. Create a rule to redirect HTTP traffic.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

System	Switching		Routin	g (QuS	Security	Monitor	ring A	laîntena	nce I	Help	Index
Management	Security Acce	an 1	Port Aut	hentication	a Troffic	Control Co	mtrol ACL					
Basic		Ext	ende	d ACL	Rules							
Advanced		1	P Rule	5							1	
» IP Rules		ACI	ID/NJ	.HE			redirecti	HTTP +				
> IPV6 ACL	d Bules		xtend	ed ACL F	Rule Table							
 IPv6 Rules IP Binding Configuration 	an.		Rule 1D	Action	Logging	Assign Queue ID	Nirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Sourc IP Addre
» Binding Tab	de	Nom	les have l	wen config	used for this A	CL.			-		_	

b. Click **Add**, and the Extended ACL Rule Configuration screen displays.

System	Switz	hing Routing	Qo5	Security	Monitoring	Maintenance	Help	Index
Management	Security	Access Port Authenticati	on Traffic C	ontrol Co	ntial ACL			
Basic Advanced		Extended ACL	Rule Con	figuration	n			
IP ACL		Extended ACL	Rule Config	uration(10	00-199)			
IP Rules		ACL ID/Name	redirectHTTP	9				
TRUE ACT	d. A Lifes	Rule ID	1					
IPv6 Rules		Action	Permit		Egress Queue	0 🖝 (0-6)		
IP Binding			O Deny					
Configurati	ion	Logging	@ Disable		Enable			
Binding Tal	ble	Hirror Interface						
Vian Bindin	ng Table	Redirect Interface	1/0/19 -					
		Match Every	False -					
		Protocol Type	Other -		(1 to 295)			
		TCP Flag	URG		Ignore -	ACK	Ignore -	PSH Ignore
			RST		Ignore -	SYN	tanare -	FIN Ignore
		Sec IP Address						
		Sec IP Mask						
		Src L4 Port	Other •		(0 to 655	35)		
		Dst IP Address	-					
		Dst IP Mask	1.11	_				
		Dst L4 Port	neto •		[[0 to 655]	20)		
		Service Type	· IP DSCP	and the second s	outer -	(0-43)		
			IP Prece	dence	0 - (0.3)	14 mm		
			IP TOS			(08-#)		

- c. In the Rule ID field, enter 1.
- d. For Action, select the Permit radio button.
- e. In the Redirect Interface list, select 1/0/19.
- f. In the Dst L4 Port list, select http.
- **g.** Click **Apply**. The Extended ACL Rules screen displays, as described in the next step in this procedure.
- 3. Create a rule to match every other traffic.
 - a. Select Security > ACL > Advanced > IP Extended Rules.

System Switc	hing	Routin	g (QoS 6	Security	Monito	ring A	Aaintena	ince i	Help	Index					(LUBOOW)
Management Security	Access	Port Aut	hentication	1 Traffic	Control Co	ACL					-					
Basic	Ex	tende	d ACL	Rules												
- Advanced	63	IP Rule	IS.							O						
> IP Rules	A	L 10/N/	INE			redirect	нттр 🛨									
 IP Foliatided hules IPv6 ACL 	0	Extend	ed ACL F	Rule Table												
 IPv6 Rules IP Binding Configuration 	-	Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destina L4 Port
 Binding Table Vlan Binding Table 	E	1	Permit	Disable	0		1/0/19	False	62 - B	7	0	<i>n</i>	/// ·····		v	http

b. Click **Add**, and the Extended ACL Rule Configuration screen displays.

System	Switching	Routing	Qo5	Security	Monitoring /	Aaintenance	Help	Index
Management	Security Acce	as Port Authenticatio	an Troffic	Control Co	entrol ACL			
Basic Advanced > IP ACL		Extended ACL Extended ACL	Rule Co	nfiguratio	n 00-199)			
> IP Rules		ACL ID/Name	redirectHT	TP				
· P Echande	C. Pullen	Rule ID	2		1			
* IPv6 Rules	1	Action	Permit		Egress Queue	0 • (0-6)		
+ IP Binding			Deny					
Configuration	on	Logging	💌 Disabl	e	🗇 Enable			
» Binding Tab	ble Table 1	Hirror Interface	•					
* Vian bindin	d radie	Redirect Interface						
		Match Every	True +					
		Protocol Type	Other +		(1 to 255)			
		TCP Flag	URG		Johore -	ACK	Ignore +	PSH Ignore -
		2.0222.222	RST		[Ignore +]	SYN	Ignore +	FIN Ignore -
		Sec IP Address						
		Sec LA Bout	Zithar		1 (D to 65515			
		Ost IP Address						
		Dot IP Mask						
		Dot L4 Port	Other -		(0 to 65535	·		
		Service Type	IP DS	CP	other -	(0-63)		
			IP Pre	cedence	0.7 (0.7)			
			C IP TOS	5		(00-#)		

- c. In the Rule ID field, enter 2.
- d. For Action, select the **Permit** radio button.
- e. In the Match Every field, select True.
- f. Click Apply. A screen similar to the following displays.

Management Security / A	Access P	ort Auth	entication	Troffic C	ontrol Con	trol ACL	ng m	unnenur	ce a	eth 1	IDEX.				-	(000)
> Basic = Advanced	Exte	ended	ACL R	ules												
. IP ACL	- 1	Rule	\$2							(0)						
* IP.Rules	ACL	ID/NA	ME			redirectH	TTP -									
+ IPv6 ACL	E	xtende	d ACL R	ule Table									1			
1P Binding Configuration Binding Table		Rule ID	Action	Logging	Assign Queue ID	Mirrror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destin L4 Port
+ Vian Binding Table	10	1	Permit	Disable	0		1/0/19	False								http
	100	2	Permit	Disable	0			True								

- 4. Bind the ACL with interface 1/0/1.
 - a. Select Security > ACL > Advanced > IP Binding Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
Management	Security Acce	as Port Auth	entication [1	roffic Control	Control ACL		
Basic		IP Bindin	g Configu	ration			
+ IP ACL		Binding	Configuratio	n			
> IP Rules		ACL ID		redirectHTTP -	Direction	Inbound -	
> IP Extende	d Rules	Sequence N	umber	0	(1 to 4294967	295)	
> IPv6 ACL		Port Selectio	n Table	74	1991 - C		
· IP Funding		+ Unit 1					
Cumperat	om						
> Binding Tal	ble va Table	Interfac	e Binding St	tatus			
- There being a	19 10010	Interface	Direction	ACL Type	ACL 1D/Name	Sequen	ce Number
		1/0/1	Inbound	IF ACL	redirectHTTP	1	

b. In the Sequence Number field, enter 1.

- c. In the Port Selection Table, click **Unit 1** to display all the ports.
- **d.** Select the check box below Port 1.
- e. Click Apply.

At the end of this configuration a screen similar to the following displays.

System	Switching	Routing	GoS	Security	Monitoring	Maintenance	Help
Management S	curity Acces	a Port Auth	entication 1	Iraflic Control C	Control ACL		
Basic		IP Bindin	g Configur	ration			
Advantant > IP ACI		Binding	Configuratio	on			
> IP Rules		ALL 10	1	redirectHTTP .	Direction	Inbound	-
> IP Extended	Rules	Sequence N	umber	0	(1 to 42949872	•5)	
> IPv6 ACL		Port Selectio	in Table				
> 1P Sinding		· Unit 1					
	6 - C						
> Binding Tabl	0	Interfac	e Binding St	tatus			
 Vian binding 	Table	Interface	Direction	ALL Type	ACL ID/Name	Sequen	ce Number
		100,204010		1000000000			

Configure IPv6 ACLs

This feature extends the existing IPv4 ACL by providing support for IPv6 packet classification. Each ACL is a set of up to 12 rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and can apply to one or more of the following fields within a packet:

- Source IPv6 prefix
- Destination IPv6 prefix
- Protocol number
- Source Layer 4 port
- Destination Layer 4 port
- DSCP value
- Flow label

Note that the order of the rules is important: When a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL is denied access.



Figure 14. IPv6 ACLs

The script in this section shows you how to set up an IPv6 ACL with the following three rules:

- Rule-1. Permits every traffic to the destination network 2001:DB8:C0AB:AC14::/64.
- **Rule-2**. Permits IPv6 TELNET traffic to the destination network 2001:DB8:C0AB:AC13::/64.
- **Rule-3**. Permits IPv6 HTTP traffic to any destination.

CLI: Configure an IPv6 ACL

1. Create the access control list with the name ipv6-acl.

(Netgear Switch) (Config)# ipv6 access-list ipv6-acl

- 2. Define three rules to:
 - Permit *any* IPv6 traffic to the destination network 2001:DB8:C0AB:AC14::/64 from the source network 2001:DB8:C0AB:AC11::/64.
 - Permit IPv6 *Telnet* traffic to the destination network 2001:DB8:C0AB:AC13::/64 from the source network 2001:DB8:C0AB:AC11::/64.

• Permit IPv6 HTTP traffic to *any* destination network from the source network 2001:DB8:C0AB:AC11::/64.

```
(Netgear Switch) (Config-ipv6-acl)# permit ipv6 2001:DB8:COAB:AC11::/64
2001:DB8:COAB:AC14::/64
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:COAB:AC11::/64
2001:DB8:COAB:AC13::/64 eq telnet
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:COAB:AC11::/64 any eq http
```

3. Apply the rules to inbound traffic on port 1/0/1. Only traffic matching the criteria will be accepted.

(Netgear Switch) (Config)#interface 1/0/1 (Netgear Switch) (Interface 1/0/1)# ipv6 traffic-filter ipv6-acl in (Netgear Switch) (Interface 1/0/1)# exit (Netgear Switch) (Config)#exit

4. View the configuration.

```
(Netgear Switch) #show ipv6 access-lists
Current number of all ACLs: 1 Maximum number of all ACLs: 100
IPv6 ACL Name
       Rules Direction Interface(s) VLAN(s)
----- -----
                     _____
                             _____
ipv6-acl
            3
              inbound
                      1/0/1
(Netgear Switch) #show ipv6 access-lists ipv6-acl
ACL Name: ipv6-acl
Inbound Interface(s): 1/0/1
Rule Number: 1
Action..... permit
Destination IP Address...... 2001:DB8:COAB:AC14::/64
Rule Number: 2
Action..... permit
Destination L4 Port Keyword..... 23(telnet)
```

```
Rule Number: 3Action.....Protocol......6(tcp)Source IP Address.....2001:DB8:C0AB:AC11::/64Destination L4 Port Keyword......80(www/http)
```

Web Interface: Configure an IPv6 ACL

- 1. Create the access control list with the name ipv6-acl
 - a. Select Security > ACL > Advanced > IPv6 ACL.
 - b. In the IPv6 ACL Table, in the IPv6 ACL field, enter ipv6-acl.

A screen similar to the following displays.

System	Swite	hing	Routing	QoS	Security	Monitoring	Maintenance	Help
Monogement	Security 1	Access	Port Authentic	cation Tru	flic Control Cor	itiol ACL		
Basic		1	Pv6 ACL					
. IP ACL			IPv6 Config	guration				(Ø
IP Rules IP Extends	d Rules		Current Number taximum ACL	of ACL		0 100		
+ IPv6 Rules + IP Binding	1		IPV6 ACL T	able				
Configurati	ion		IPv6 ACI		Rules	Th Th	/p-g	
 Binding Ta Ulan Einder 	bie In Table		ipv6-ad			1P	V6 ACL	

c. Click Add. A screen similar to the following displays.

System Swit	ching	Routing	QoS	Security	Monitoring	Maintenance	Help
Management Security	Access	Port Authentia	cation Tra	flic Control Co	ntrol ACL		
Basic	IP	V6 ACL					
+ IP ACL		IPv6 Confi	guration				0
* IP Rules	0	urrent Numbe	s of ACL		11		
IP Extended Rules Pro-ACL	н	aximum ACL			100	2	
= IPv6 Rules = IP Bindion	6	IPv6 ACL T	able				Ű
Configuration		IPV6 AC	E.	Rules		ype	
- Binding Table					1	PV6 ACL	
 vian binding Table 		ipv6-ad		0	13	PV6 ACL	

- 2. Define the first rule (1 of 3).
 - a. Select Security > ACL > Advanced > IPv6 Rules.

System	Switch	ing	Routing	G	105	Security	Monitori	ing Mi	aintenan	ice ł	telp
Management	Security	Access	Port Auth	entication	Traffic C	ontrol Con	erol ACL				
Basic Advanced	1	IPv	6 Rul	es							
* IP ACL		-1	IPv6 Ru	iles						0	0
+ IP Rules	00.000	AC	Name				ipv6-acl +				
 IP Extende IPv6 ACL 	d Rules		IPv6 AC	1. Rule T	able	ò	e diversa e la				
 IP Binding Configuration 	on	-	Rule ID	Action	Logging	Assign Queue ID	Mirrror Interface	Redirect Interface	Hatch Every	Protocol	Source
 Vian Bindin 	g Table	Nor	des have b	en configu	ed for this Af	I					

- b. In the ACL Name list, select ipv6-acl.
- c. Click Add.
- d. In the Rule ID field, enter 1.
- e. For Action, select the Permit radio button.
- f. In the Source Prefix field, enter 2001:DB8:C0AB:AC11:..
- g. In the Source Prefix Length field, enter 64.
- h. In the Destination Prefix field, enter 2001:DB8:C0AB:AC14:..
- i. In the Destination Prefix Length field, enter 64.

System Sw	tching Routing QoS	Security Monitoring	Maintenance Help Index
Management Security	Access Port Authentication Tra	flic Control Control ACL	
Basic Advine od FIP ACL	IPv6 ACL Rule Config IPv6 ACL Rule Config	guration uration	Ū
P Rules IP Rules IP Extended Rules IPv6 ACL IPv6 ACL IPv6 ACL IPv6 Rules IP Binding Configuration Binding Table Vlan Binding Table	ACL Name Rule ID Action Logging Mirror Interface	ipv6-ad 1 Permit Deny Disable	Egress Queue (0-6)
	Redirect Interface Match Every Protocol Type Source Prefix/PrefixLength Source L4 Port Destination Prefix/PrefixLe Destination L4 Port How Label IP DSCP Service	Disable Other Dool:DB8:C0AB:AC11:: Other Conter Cother Cother Cother (0 the	© Enable (1 to 255) 64 (0 to 65535) 64 (0 to 65535) 1048375)

- j. Click Apply.
- 3. Add Rule 2.
 - a. In the Rule ID field, enter 2.
 - **b.** For Action, select the **Permit** radio button.
 - c. In the Protocol Type list, select TCP.
 - d. In the Source Prefix field, enter 2001:DB8:C0AB:AC11::.
 - e. In the Source Prefix Length field, enter 64.
 - f. In the Destination Prefix field, enter 2001:DB8:C0AB:AC13:..
 - g. In the Destination Prefix Length field, enter 64.
 - h. In the Destination L4 Port list, select telnet.

System Switchin	g Routing QoS	Security Monitoring	Maintenance Help Index
Monogement Security A	ccess Port Authentication Traffic C	ontrol Control ACL	
Basic Advanced + IF ACL	IPv6 ACL Rule Configur IPv6 ACL Rule Configurati	ation	
IP Rules IP Extended Rules IPv6.ACL	ACL Name Rule 10	ipv6-ad 2	
+ IP-Binding	Action	 Permit Deny 	Egress Queue • (0-6)
Configuration = Binding Table = Vian Binding Table	Logging Mirror Interface	Disable	C Enable
	Redirect Interface Match Every	Disable	© Enable
	Source Prefix/PrefixLength	2001:DB8:C0AB:AC11::	64
	Destination Prefix/PrefixLength	2001:D88:C0AB:AC13:	64 (0 to 45528)
	Flow Label	(0.1a	1046373)

- i. Click Apply.
- 4. Add Rule 3.
 - a. In the Rule ID field, enter 3.
 - b. For Action, select the Permit radio button.
 - c. In the Protocol Type list, select TCP.
 - d. In the Source Prefix field, enter 2001:DB8:C0AB:AC11::.
 - e. In the Source Prefix Length field, enter 64.
 - f. In the Destination L4 Port list, select http.

A screen similar to the following displays.

System Switc	hing Routing QoS	Security Monitoring	g Maintenance	Help Index
Management Security	Access Port Authentication Traffic	Control Control ACL		
Basic Advanced • IP ACL	IPv6 ACL Rule Configu IPv6 ACL Rule Configura	ration tion		Q
+ IP Rules + IP Extended Rules	ACL Name Rule ID	ipv6-ad 3		
IP Binding	Action	 Permit. Deny 	Egress Ques	• (0-6)
Configuration • Binding Table	Logging Mirror Interface	Disable	🕑 Enable	
* vian binding racie	Redirect Interface Match Every	Disable	🕤 Enable	
	Protocol Type Source Prefix/PrefixLength	TCP - 2001:D68:C0AB:AC11::	(1 to	255)
	Source L4 Port Destination Prefix/PrefixLengt	http •	10	to 65523)
	Destination L4 Port Flow Label	Other •	0 te 1048375)	to 65535)
	IP DSCP Service			

- g. Click Apply.
- 5. Apply the rules to inbound traffic on port 1/0/1.

Only traffic matching the criteria will be accepted.

a. Select Security > ACL > Advanced > IP Binding Configuration.

- b. In the ACL ID list, select ipv6-acl.
- c. In the Sequence Number list, select 1.
- d. Click Unit 1.
- e. Select Port 1.

System	Switchin	g 1	Routin	9		QoS	È.		Sec	urit	Y I		Mo	nitor	ing	E	Mai	nten	ance		1	telp	g -
Management	Security I A	ccesa P	ort Aut	hentic	ofio	n 1	Tro	fic C	iont	ol	G	nho	Ú.	ACL	-								
Basic		IP E	lindi	ng C	on	fig	ıra	tio	n														
+ IP ACL		B	inding	Cor	nfig	urat	ion			_											_		
+ IP Rules	1000	ACL	10				ipv	6-8	d •				D	rectio				1	nbou	sd .			
+ IP Extende	d Rules	Seq	uence	Numl	HT		1						(1	to 47	94967	295	6						
+ IPV6 ACL		Port	Select	ion Ti	able	į N	-			-	1												
* IPvo Kules			Unit I																				
Cathorne	6m.	Port	1 2	з	4	5	6	7	8	9	10	11	12	13 1	4 15	16	17	18	19 2	0 21	1 22	23	2
. Binding Tab	ale	1200	4	5.5	120		13			13	2		1.1		10.5	10	110	128		1.	振行	112	93
+ Vlan Bindin	g Table	- C	25 2	6 27	28	29	30	31	32	33	34	35	36	37 1	18 39	40	41	42 /	43 4	4 43	5 44	47	- 4

f. Click Apply.

A screen similar to the following displays.

System	Switchin	ng Routing	QoS	Security	Monitoring	Maintenance	Help
Management	Security A	ccess Port Auth	intication Tri	affic Control Co	ntrol ACL		
Basic	-	IP Binding	Configura	ation			
• IP ACL		Binding	Configuration	1			
+ 1P Rules		ACL ID	ip	w6-adl +	Direction	Inbound +	
 IP Extende 	d Rules	Sequence N	mber 0		(1 to 42949672	95)	
· IPV6 ACL		Port Selectio	n Table				
* IPV6 KUNES		· Dolt 5					
	-						
 Binding Ta Vian Bindu 	ble va Table	Interfac	e Binding Sta	tus			
- vient contain	A LOUGH	Interface	Direction	ACL Type	ACL ID/Name	Sequenc	e Numbe
		1/0/1	Inbound	IPV6 ACL	iov6-ad	1	

6. View the binding table.

Select Security > ACL > Advanced > Binding Table.

Management Secu	rity Access	Port Authentication	n Troffic Control	Control ACL		
Basic Advanced	п	P ACL Binding	Table			
- IP ACL		IP ACL Binding	Table		200	
* IP Extended Ru	les	Interface	Direction	ACL Type	ID/Name	Number
+ IPV6 ACL		1/0/1	In Bound	IPV6 ACL	ipv6-acl	10

CoS Queuing

8

Class of Service Queuing

This chapter includes the following sections:

- QoS Queuing Concepts
- Show classofservice Trust
- Set classofservice Trust Mode
- Show classofservice IP-Precedence Mapping
- Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode
- Set CoS Trust Mode for an Interface
- Configure Traffic Shaping

QoS Queuing Concepts

This chapter describes Class of Service (CoS) queue mapping, CoS Configuration, and traffic shaping features. Each port has one or more queues for packet transmission. During configuration, you can determine the mapping and configuration of these queues.

Based on the service rate and other criteria you configure, queues provide preference to specified packets. If a delay is necessary, the system holds packets until the scheduler authorizes transmission. As queues become full, packets are dropped. Packet drop precedence indicates the packet's sensitivity to being dropped during queue congestion.

Select per interface configuration scheme:

You can configure CoS mapping, queue parameters, and queue management are configurable per interface.

Queue management is configurable per interface.

Some hardware implementations allow queue depth management using tail dropping or weighted random early discard (WRED).

Some hardware implementations allow queue depth management using tail dropping.

The operation of CoS queuing involves queue mapping and queue configuration.

CoS Queue Mapping

CoS queue mapping uses trusted and untrusted ports.

Trusted Ports

- The system takes at face value certain priority designations for arriving packets.
- Trust applies only to packets that have that trust information.
- There can be only one trust field at a time per port.
 - 802.1p user priority (This is the default trust mode and is managed through switching configuration.)
 - IP precedence
 - IP DiffServ Code Point (DSCP)

The system can assign the service level based upon the 802.1p priority field of the L2 header. You configure this by mapping the 802.1p priorities to one of three traffic class queues. These queues are:

- **Queue 2**. Minimum of 50 percent of available bandwidth
- Queue 1. Minimum of 33 percent of available bandwidth
- **Queue 0**. Lowest priority, minimum of 17 percent of available bandwidth

For untagged traffic, you can specify the default 802.1p priority on a per-port basis.

Untrusted Ports

- No incoming packet priority designation is trusted; therefore, the default priority value for the port is used.
- All ingress packets from untrusted ports, where the packet is classified by an ACL or a DiffServ policy, are directed to specific CoS queues on the appropriate egress port. That specific CoS queue is determined by either the default priority of the port or a DiffServ or ACL-assigned queue attribute.
- Used when trusted port mapping is unable to be honored for instance, when a non-IP DSCP packet arrives at a port configured to trust IP DSCP.

CoS Queue Configuration

CoS queue configuration involves port egress queue configuration and drop precedence configuration (per queue). The design of these on a per-queue, per-drop precedence basis allows you to create the service characteristics that you want for different types of traffic.

Port egress queue configuration:

- Scheduler type, strict vs. weighted
- Minimum guaranteed bandwidth
- Maximum allowed bandwidth per-queue shaping
- Queue management type, tail drop vs. WRED

Drop precedence configuration (per queue):

- WRED parameters
 - Minimum threshold
 - Maximum threshold
 - Drop probability
 - Scale factor
- Tail drop parameters, threshold

Per-interface basis:

• Queue management type, rail Drop vs. WRED

Only if per-queue configuration is not supported

- WRED decay exponent
- Traffic shaping for an entire interface

Show classofservice Trust

The example is shown as CLI commands and as a Web interface procedure.

CLI: Show classofservice Trust

To use the CLI to show CoS trust mode, use these commands:

```
(Netgear Switch) #show classofservice trust?
<cr> Press Enter to execute the command.
(Netgear Switch) #show classofservice trust
Class of Service Trust Mode: DotlP
```

Web Interface: Show classofservice Trust

Select **QoS > CoS > Basic > CoS Configuration**. A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSe	rv							
* Basic	CoS (Configura	ation					
Configuratio	m Co	S Configur	ation					
Advanced	ି କ	obal	ALL 💌	Global Trust Mode	trust dot1p			
	Ĉ In	terface	1/0/1 💌	Interface Trust Mode	Untrusted	<u>.</u>		

Set classofservice Trust Mode

The example is shown as CLI commands and as a Web interface procedure.

CLI: Set classofservice Trust Mode

(Netgear Switch)	(Config)#classofservice?
dot1p-mapping	Configure dotlp priority mapping.
ip-dscp-mapping	Maps an IP DSCP value to an internal traffic class.
trust	Sets the Class of Service Trust Mode of an Interface.
(Netgear Switch)	(Config)#classofservice trust?
dot1p	Sets the Class of Service Trust Mode of an Interface
	to 802.1p.
ip-dscp	Sets the Class of Service Trust Mode of an Interface
	to IP DSCP.
(Netgear Switch)	(Config)#classofservice trust dot1p?
<cr></cr>	Press Enter to execute the command.
(Netgear Switch)	(Config)#classofservice trust dot1p

Web Interface: Set classofservice Trust Mode

1. Select QoS > CoS > Basic > CoS Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Cos DiffSer	W (
- Daniel	CoS	Configura	ation					
Cambalanata	Co	S Configura	ation			121		
Advanced	@ G	obal	ALL .	Global Trust Mode	trust dot1p	-		
	C 10	terface	1/0/1 -	Interface Trust Mode	Untrusted	-		

- 2. Select the Global radio button.
- 3. In the Global Trust Mode list, select trust dot1p.
- 4. Click **Apply** to save the settings.

Show classofservice IP-Precedence Mapping

The example is shown as CLI commands and as a Web interface procedure.

CLI: Show classofservice IP-Precedence Mapping

(Netgear Switch) IP Precedence	#show classofservice ip-precedence-mapping Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Web Interface: Show classofservice ip-precedence Mapping

1. Select QoS > CoS > Advanced > IP Precedence Queue Mapping.

System Sy	vitching Rout	ing	QoS	Sec	urity -	Monito	ring	Mainte	nance	Help	Index
Ce5 DiffServ			<u> </u>								
Dasic	IP Precede	nce to	Queue	Mappir	ig						
CoS	Interface	Selectio	n						ġ		
Configuration	Interface	Al									
Mapping											
EP Precedence	IP Preced	ence to l	Queue M	apping					Q.		
IP DSCP Queue	IP Precedence		x	2	2	4	5		2		
Mapping Cold Interface	Queue	1 -	0 +	0. 💌	1 -	2 3	2 2	3 -	3 💌		
Configuration Interface Queue Configuration											

2. In the Interface list, select All.

The global IP precedence to queue mapping is displayed.

3. In the Interface list, select the specific interface (such as 1/0/1).

The IP precedence to queue mapping of the interface is displayed.

Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

(Netgear Switch)	(Config)#cos-queue min-bandwidth?
<bw-0></bw-0>	Enter the minimum bandwidth percentage for Queue 0.
(Netgear Switch)	(Config)#cos-queue min-bandwidth 15
Incorrect input!	Use 'cos-queue min-bandwidth <bw-0><bw-7>.</bw-7></bw-0>
(Netgear Switch)	(Config)#cos-queue min-bandwidth 15 25 10 5 5 20 10 10
(Netgear Switch)	(Config)#cos-queue strict?
<queue-id></queue-id>	Enter a Queue Id from 0 to 7.
(Netgear Switch)	(Config)#cos-queue strict 1?
<cr></cr>	Press Enter to execute the command.
<queue-id></queue-id>	Enter an additional Queue Id from 0 to 7.
(Netgear Switch)	(Config)#cos-queue strict 1

Web Interface: Configure CoS-queue Min-bandwidth and Strict Priority Scheduler Mode

- 1. For Interface 1/0/2, set the minimum bandwidth to 15 for queue 0.
 - a. Select QoS > CoS > Advanced > Interface Queue Configuration.

A screen similar to the following displays.

System	Switching	Routin	19	QoS Se	curity Mon	itoring	Maintenance	Help	Index			
CoS DiffSer	W I											
Basic	Int	erface Qu	ieue Co	onfiguration	12							
· CoS	177	Interface Queue Configuration ()										
Configuration	•	All		Go To In	terface	00						
Mapping > IP Preceden	ce	Interface	Queue ID	Ninimum Bandwidth	Scheduler Type	Queue Managemen Type	t					
+ IP DSCP Qu	eue	1/0/2	0 📃	15	Weighted -	taildrop						
Mapping		1/0/1	0	0	weighted	taildrop						
+ CoS Interfai	ce 🔽	1/0/2	0	0	velobted	taildrop						
Configuartion	° –	1/0/3	0	0	weighted	taildrop						
Configuration	Г	1/0/4	0	0	weighted	taildrop						
	- C	1/0/5	0	0	weighted	taildrop						

- b. In the Queue ID list, select 0.
- **c.** Under Interface Queue Configuration, scroll down and select the interface **1/0/2** check box.

Now 1/0/2 appears in the Interface field at the top.

- d. Enter the following information:
 - In the Minimum Bandwidth field, enter 15.
 - In the Scheduler Type list, select Weighted.
- e. Click Apply to save the settings.
- 2. For interface 1/0/2, set the minimum bandwidth 25 for queue 1, and set the scheduler type to strict.
 - a. Select QoS > CoS > Advanced > Interface Queue Configuration.

System Swi	tching	Routin	18	GoS Se	curity Mon	itoring	Maintenance	Help	Index
CoS DiffServ				100					
Dasic	Int	ertace Qu	ieue Co	onfiguration	0				
* CoS	111	interface Q	ueue Co	nfiguration			1		
Configuration	3	IA		Go To Int	orfaco	00			
Mapping • IP Precedence		Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Managemer Type	it.		
IP DSCP Queue		1/9/2	1 .	25	Strict 💌	taildrop			
Mapping		1/0/1	1	0	veighted	taildrop			
 CoS Interface Configuration 	R	1/0/2	1	0	weighted	talldrop			
		1/0/3	1	0	weighted	taildrop			
Configuration		1/0/4	1	0	reighted	taildrop			
		1/0/5	1	0	weighted	taildrop			

- b. In the Queue ID list, select 1.
- **c.** Under Interface Queue Configuration, scroll down and select the interface **1/0/2** check box.

Now 1/0/2 appears in the Interface field at the top.

- d. Enter the following information:
 - In the Minimum Bandwidth field, enter 25.
 - In the **Scheduler Type** list, select **Strict**.
- e. Click Apply to save the settings.

Set CoS Trust Mode for an Interface

The example is shown as CLI commands and as a Web interface procedure.

CLI: Set CoS Trust Mode for an Interface

(Netgear	Switch)	(Interface 1/0/3)#classofservice trust?
dot1p		Sets the Class of Service Trust Mode of an Interface
		to 802.1p.
ip-dscp		Sets the Class of Service Trust Mode of an Interface
		to IP DSCP.
(Netgear	Switch)	(Interface 1/0/3)#classofservice trust dot1p?
<cr></cr>		Press Enter to execute the command.
(Netgear	Switch)	(Interface 1/0/3)#classofservice trust dot1p

Note: The traffic class value range is 0–-6 instead of 0–-7 because queue 7 is reserved in a stacking build for stack control, and therefore you cannot configure it.

Web Interface: Set CoS Trust Mode for an Interface

1. Select QoS > CoS > Advanced > CoS Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	11	Maintenance	Help	index.
CoS DiffServ	6								
Basic.	CoS	Configura	tion						
+ CaS	Co	S Configura	ation			.0			
> 902.1p Queue	0.4	ledo	ALL -	Global Trust Hode	Untrusted	4			
Mepping > IP Precedence	(i ta	terface	1/0/3 💌	Interface Trust Hode	trust dottp				
Queue Mappir + IP DSCP Que	ue.								
Mepping + CoS Interface									
Configuartion	6								
Configuration	oue.								

- 2. Under CoS Configuration, select the Interface radio button.
- 3. In the Interface list, select 1/0/3.
- 4. In the Interface Trust Mode list, select trust dot1p.
- 5. Click Apply to save the settings.

Configure Traffic Shaping

Traffic shaping controls the amount and volume of traffic transmitted through a network. This has the effect of smoothing temporary traffic bursts over time. Use the traffic-shape command to enable traffic shaping by specifying the maximum transmission bandwidth limit for all interfaces (Global Config) or for a single interface (Interface Config).

The <bw> value is a percentage that ranges from 0 to 100 in increments of 5. The default bandwidth value is 0, meaning no upper limit is enforced, which allows the interface to transmit up to its maximum line rate.

The bw value is independent of any per-queue maximum bandwidth values in effect for the interface and should be considered as a second-level transmission rate control mechanism that regulates the output of the entire interface regardless of which queues originate the outbound traffic.

CLI: Configure traffic-shape

(Netgear	Switch)	(Config)#traffic-shape?
<bw></bw>		Enter the shaping bandwidth percentage from 0 to 100
		in increments of 5.
(Netgear	Switch)	(Config)#traffic-shape 70?
<cr></cr>		Press Enter to execute the command.
(Netgear	Switch)	(Config)#traffic-shape 70
(Netgear	Switch)	(Config)#

Web Interface: Configure Traffic Shaping

- 1. Set the shaping bandwidth percentage to 70 percent.
 - a. Select QoS > CoS > Advanced > CoS Interface Configuration.

A screen similar to the following displays.

System 5	witching	Routin	GoS	Security Moni	itoring	Maintenance	Help	Index	
CoS DiffServ			AR MI					Ξ.	
Basic Advanced Cos Configuration e02.1p Queue Mapping IP Precedence Queue Mapping IP DSCP Queue Mapping DSCP Queue Mapping DSCP Queue Configuration Configuration	Cof	CoS Interface Configuration							
		CoS Interface Configuration							
	3	01	Go To Interface		00				
		Interface	Interface Trust Piode	Interface Shapin to 100)	g Rate (O				
		1/0/3	Dottp 🕑	70					
	Г	1/0/1	Dotlp	0		1			
	Г	1/0/2	Dotip	0					
	12	1/0/0	Dotto	0					
	: Г	1/0/4	Dotap	0					
	Г	1/0/5	Dettp	0					

b. Under CoS Interface Configuration, scroll down and select the interface **1/0/3** check box.

Now 1/0/3 appears in the Interface field at the top.

- c. In the Interface Shaping Rate (0 to 100) field, enter 70.
- d. Click Apply to save the settings.

DiffServ

Differentiated Services

This chapter includes the following sections:

- DiffServ Concepts
- Configure DiffServ
- DiffServ for VoIP
- Auto VoIP
- DiffServ for IPv6
- Color Conform Policy



DiffServ Concepts

Differentiated services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol. This section explains how to configure the ProSAFE M4100 Managed Switches to identify which traffic class a packet belongs to, and how it should be handled to provide the quality of service you want. As implemented on the M4100 Managed Switch, DiffServ allows you to control what traffic is accepted and what traffic is discarded.

How you configure DiffServ support on a M4100 Managed Switch varies depending on the role of the switch in your network:

- Edge device. An edge device handles ingress traffic, flowing toward the core of the network, and egress traffic, flowing away from the core. An edge device segregates inbound traffic into a small set of traffic classes, and is responsible for determining a packet's classification. Classification is based primarily on the contents of the Layer 3 and Layer 4 headers, and is recorded in the Differentiated Services Code Point (DSCP) added to a packet's IP header.
- Interior node. A switch in the core of the network is responsible for forwarding packets, rather than for classifying them. It decodes the DSCP code point in an incoming packet, and provides buffering and forwarding services using the appropriate queue management algorithms.

Before configuring DiffServ on a particular M4100 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.

Configure DiffServ

This example shows how a network administrator can provide equal access to the Internet (or other external network) to different departments within a company. Each of four departments has its own Class B subnet that is allocated 25 percent of the available bandwidth on the port accessing the Internet.



Figure 15. Class B subnet with differentiated services

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure DiffServ

1. Ensure that the DiffServ operation is enabled for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#diffserv
```
Create a DiffServ class of type all for each of the departments, and name them. Define the match criteria of source IP address for the new classes.

```
(Netgear Switch) (Config)#class-map match-all finance_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.10.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit
(Netgear Switch) (Config class-map)#match srcip 172.16.20.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit
(Netgear Switch) (Config class-map)#exit
(Netgear Switch) (Config class-map)#match srcip 172.16.30.0 255.255.255.0
(Netgear Switch) (Config class-map)#match srcip 172.16.30.0 255.255.255.0
(Netgear Switch) (Config class-map)#match srcip 172.16.30.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit
(Netgear Switch) (Config class-map)#exit
```

3. Create a DiffServ policy for inbound traffic named 'internet_access', adding the previously created department classes as instances within this policy.

This policy uses the assign-queue attribute to put each department's traffic on a different egress queue. This is how the DiffServ inbound policy connects to the CoS queue settings established in the following example.

```
(Netgear Switch) (Config)#policy-map internet_access in
(Netgear Switch) (Config policy-map)#class finance_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 1
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class marketing_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 2
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class test_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 3
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-class-map)#assign-queue 4
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-class-map)#exit
```

4. Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the inbound direction.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/3)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/3)#service-policy in internet_access
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/4)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/4)#service-policy in internet_access
```

5. Set the CoS queue configuration for the (presumed) egress interface 1/0/5 such that each of queues 1, 2, 3, and 4 gets a minimum guaranteed bandwidth of 25 percent. All queues for this interface use weighted round robin scheduling by default. The DiffServ inbound policy designates that these queues are to be used for the departmental traffic through the assign-queue attribute. It is presumed that the switch will forward this traffic to interface 1/0/5 based on a normal destination address lookup for Internet traffic.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#cos-queue min-bandwidth 0 25 25 25 25 0 0 0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure DiffServ

- 1. Enable Diffserv.
 - a. Select QoS > DiffServ > Basic > DiffServ Configuration.

System	Switching	Routing	QoS	Se	curity	Monitoring	Maintenance	Help	Index
CoS DiliSen				-					
Diffserv Wize	ard Diffse	erv configura	ation						
* Diffuerx	Dif	fServ Config					1		
Configuration • Advanced	Diffse	rv Admin Hode	Ć P	isable	(F Enable				

- b. For Diffserv Admin Mode, select the Enable radio button.
- c. Click Apply to save the settings.

- 2. Create the class finance_dept.
 - a. Select QoS > DiffServ > Advanced > Class Configuration.

System Sw	itching	Routing	Go5	Security	Monitoring	Maintenance	Help	Index
CoS DillServ								
 Diffserv Wizard Basic Advanced 	Class	Configurat	ion			Ø.		
DiffServ Configuration Configuration		lass Name inance_dept		Elass T All	уре			
Configuration * Policy Configuration								
Service Configuration Service Statistics								

- **b.** Enter the following information:
 - In the Class Name field, enter finance_dept.
 - In the Class Type list, select All.
- c. Click Add to create a new class finance_dept.
- d. Click the finance_dept to configure this class.

System Swit	thing Routing	QoS Security	Monitoring	Maintenance	Help	Index
CoS DiffSerr						
Diffsery Wizard	Class Information				00	
Basic Advanced	Class Type	finance_d	ept			
Configuration	Diffserv Class Config	uration			Ð	
Configuration > Policy Configuration > Service Service Statistics	Match Every Reference Class Class of Service VLAN Ethernot Type Source MAC Source MAC Source MAC Mask Destination MAC Destination MAC Mask		α.4 Σ	093) (0600 - 1777)		
	Source IP Address	172.16.10	.0 (0 + 255)			
	Source L4 Port Destination IP Address	255.255.2	. 0 (0.4	65535)		

- e. Under Diffserv Class Configuration, enter the following information:
 - In the Source IP Address field, enter 172.16.10.0.
 - In the Source Mask field, enter 255.255.255.0.
- f. Click Apply.
- **3.** Create the class marketing_dept:
 - a. Select QoS > DiffServ > Advanced >Class Configuration.

System Swi	tching Routing	QoS	Security	Monitoring	Mointenance	Help	Index
CoS DiffServ		- Sin					
Diffserv Wizard Basic Advanced	Class Configura	ation		^a			
DiffServ Configuration	Class Name marketing_de	pt	Class T	ype			
Configuration Policy Configuration	Finance_dept		All				
Service Configuration Service Statistics							

- **b.** Enter the following information:
 - In the Class Name field, enter marketing_dept.
 - In the Class Type list, select All.
- c. Click Add to create a new class marketing_dept.
- d. Click marketing_dept to configure this class.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DillServ								
Diffsery Wizar	d Cl	ass Informatio	n				00	
Basic Advanced	Class Class	Name Туре		marketin All	p_dept			
Configuration	D	ffserv Class Co	onfiguration	6			0	
Policy Configuration Service	Hatch Refer Class	Every ence Class of Service						
Configuration + Service Statis	VLAN Ethur	net Type • MAC			0-4	093) (0600 - 19977)		
	Sourc	e MAC Mask						
	Proto	nation MAC Hask col Type		-	0 (0 - 255)			
	Sourc	e IP Address e Mask		255.255.2	1.0			
	Sourc	e L4 Port nation IP Addres			≥ 0 (0.4	\$5533)		

- e. Under Diffserv Class Configuration, enter the following information:
 - In the Source IP Address field, enter 172.16.20.0.
 - In the Source Mask field, enter 255.255.255.0.
- f. Click Apply.
- 4. Create the class test_dept:
 - a. Select QoS > DiffServ > Advanced >Class Configuration.

System Swi	tebing	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ		- 1						
Diffserv Wizard Basic Advanced	Class C	Configurat i Table	ion			0.		
> DiffServ	Class Name			Class T	ype)			
Configuration	Te:	test_dept						
Currenter attent	T fina	nce_dept		All		- 20		
> Policy	E ma	electing_dept		15A				
Configuration > Service Configuration > Service Statistics								

- **b.** Enter the following information:
 - In the Class Name field, enter test_dept.
 - In the Class Type list, select All.
- c. Click Add to create a new class test_dept.
- d. Click test_dept to configure this class.

System 5	witching	Routing	GoS	Security	Monitor	ing Mo	aintenance	Help	Index
Co5 DiffServ									
Diffsory Wizard	ci	ass Informatio	n					0	
Basic Advanced	Class	Name Type		test_dept All			3		
Configuration	Di	ffserv Class Co	onfiguration					۲	
Configuration • Policy Configuration • Service Configuration • Service Statistic	Configuration Service Service Service	Every ence (lass of service net Type e MAC			J J	(1 - 4093)	1777)		
	Destin Destin Proto Sourc	e HAL Haar nation HAC nation NAC Mask col Type e IP Address		172-16-30	0 (0 0	- 255)			
	Sourc	n Mask n L4 Port		255.255.25	• 0	(0 - 65535)			
	Destin	nation IP Addres							

- e. Under Diffserv Class Configuration, enter the following information:
 - In the Source IP Address field, enter 172.16.30.0.
 - In the Source Mask field, enter 255.255.255.0.
- f. Click Apply.
- 5. Create class development_dept.
 - a. Select QoS > DiffServ > Advanced > Class Configuration.

System Swi	tching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS Diffânry					і <u> </u>			
Diffserv Wizard Basic Advanced > DiffServ	Clar	ss Configurat Class Table	ion			0)		
 DiffServ 	Class Name			Class T	YPE.			
Configuration		development		Al W				
Confrigue alson	r	finance_dept		All				
Policy	Γ.	marketing_dept		IIA.		1		
Configuration	r	test_dept		All				
Configuration								

- **b.** Enter the following information:
 - In the Class Name field, enter development_dept.
 - In the Class Type list, select All.
- c. Click the Add to create a new class development_dept.
- d. Click development_dept to configure this class.

System Swit	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DIRSorv		-				G		- 1
Diffserv Wizard	Cla	ss Informatio	0				0	
Basic Advanced > DiffServ	Class N Class T	ame Ype		developm All	ent []]			
Configuration	Dif	fserv Class Co	ofiguration				(O)	
Configuration > Policy Configuration > Service Configuration > Service Statistics	Hatch Refere Class o VLAN Ethern Source Source Destin Destin	Every nce Class F Service NAE NAE Hask atton NAC atton NAC		3	2 2	093) (0600 - 7777)		
	Protoc	ol Type		172.16.40	0 (0 - 255)			
	Source	Mask L4 Port		255.255.2	55.0 + 0 00-0	02223		
	Destin	ation IP Address				an a		

- e. Under Diffserv Class Configuration, enter the following information:
 - In the Source IP Address field, enter 172.16.40.0.
 - In the Source Mask field, enter 255.255.255.0.
- f. Click Apply.
- 6. Create a policy named internet_access and add the class finance_dept to it.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System Swit	tching Routing	QoS	Socurity	Monitoring	Maintenance	Help	Index
CoS DiffServ							
Diffserv Wizard Hasic Advanced	Policy Configurat	tion tion			2)		
DiffServ Configuration	Policy Selector	8	Policy Type	Member Class			
Class Configuration	internet_access	n.		finance_dept			
Service Configuration Service Statistics							

- **b.** Enter the following information:
 - In the **Policy Selector** field, enter **internet_access**.
 - In the Member Class list, select the finance_dept.
- c. Click Add to create a new policy internet_access.
- 7. Add the class marketing_dept into the policy internet_access.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System 5	witching	Routing	GoS	Security	Monitoring	Maintenance	Help	Index	
CoS DiffSory									
Diffserv Wizard Basic Advanced	Policy	y Configura	tion tion			0			
DiffServ Configuration		olicy Selector		Policy Type	Nember Class				
 Class Configuration 		internet_access	12	In	marketing_del				
Configuration	2	iternet access		în	finance_slept				
 Service Configuration Service Statistic 	\$								

- **b.** Under Policy Configuration, scroll down and select the **internet_access** check box. internet_access now appears in the Policy Selector field at the top.
- c. In the Member Class list, select marketing_dept.
- d. Click Apply to add the class marketing_dept to the policy internet_access.
- 8. Add the class test_dept into the policy internet_access.
 - a. Select QoS > DiffServ > Advanced >Policy Configuration.

System Swi	tching	Routing	QoS	Security	Monitoring	Maintenance	Help.	Index
CoS DiffServ								
Diffserv Wizard	Pol	icy Configurat	tion					
Basic Advanced	199	Policy Configurat	tion			2)		
DiffServ Configuration		Policy Selector	ł	Policy Type	Member Class			
Class Configuration		internet_access		In	test_dept.	1		
A Palezz	E	internet_access		In	finance_dept			
Configuration	12	Interest_Atress		to	marketing_dept			
Service Configuration Service Statistics								

- **b.** Under Policy Configuration, scroll down and select the **internet_access** check box. Internet_access now appears in the Policy Selector field at the top.
- c. In the Member Class list, select test_dept.
- d. Click Apply to add the class test_dept to the policy internet_access.
- 9. Add the class development_dept into the policy internet_access.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

A screen similar to the following displays.

System S	witching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
Diffserv Wizard Basic Advanced	Polic	y Configura	tion			D)		
* DiffServ Configuration		Policy Selector		Policy Type	Member Class			
 Class Configuration 		internet_access	П.,	In	development .	1		
s tuicz	E 1	nternet_access		In	finance_dept			
Configuration.	F 4	nternet_access		tn	marketing_dept	2		
Service Configuration Service Statistic	×	nternet_access		In	test_dept			

- **b.** Under Policy Configuration, scroll down and select the **internet_access** check box. Now internet_access appears in the Policy Selector field at the top.
- c. In the Member Class list, select development_dept.
- d. Click Apply to add the class development_dept to the policy internet_access.

10. Assign queue 1 to finance_dept.

a. Select QoS > DiffServ > Advanced > Policy Configuration.

System Swi	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
Diffserv Wizard	Pol	icy Configura	tion					
Basic Advanced	128	Policy Configura	tion			13		
 DiffServ Configuration 	Policy Selector			Policy Type	Member Class			
* Class					finance_dept 🔄	1		
Configuration		internet_access		In	finance_dept			
Configuration	Γ.	internet_access		In	marketing_dept			
» Service	E	internet_access		In	test_dept			
Configuration • Service Statistics	1	Internet_access		10	development	1		

b. Click the $internet_access$ check box for the member class finance_dept.

System	Switching	Routing	QoS	Security	Monitoring	Mainfenance	Help	Index
CoS DiffServ								
Diffserv Wizar Basic	d Polic	y Class Con ass Informatio	figuration				æ	
DiffServ Configuration Class Configuration	Palicy Policy Hemb	Name Type er Class Name		internet_ In finance_s	access lept			
Configuration	Policy	licy Attribute n Queue 1. Abvibute C	Drop				0	
* service statut	5.5.1	с с с	Mark COS Mark IP Proc Mark IP DSC Police Simple	odonce 0 p af	9 11 9			
		· ·	Calar No Calar No Calar Ca	de Ci nform Class 🗍	oloralind 💽			
			Committ	ed Rate				

- c. In the Assign Queue list, select 1.
- d. Click Apply.
- **11.** Assign queue 2 to marketing_dept.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System Swi	tching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DillServ								
Diffserv Wizard	Polic	y Configura	tion					
Basic	P	alicy Configura	tion		.0	0		
> DiffServ Configuration		Policy Selector		Policy Type	Member Class			
a Class					finance_dept 💌	1		
Configuration		internet_access		In	finance_dept			
Configuration	Γ.	internet_access		In	marketing_dept			
» Service	E	internet_access		In	test_dept			
Configuration * Service Statistics	r i	internet_access		In .	development	1		

b. Click the **internet_access** check box for marketing_dept.

A screen similar to the following displays.

System Swit	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiRServ								
Diffserv Wizard Basic	Policy C	æ						
DiffServ Configuration Class Crafterentian	Policy Nan Policy Typ Member C	ne e Lass Name		internet_i In marketing	access a_dept			
Configuration • Tonss Configuration • Service Service Statistics	Policy Assign Qu Policy Abr	Attribute eue 2 2 mbute C) Drop Hark COS	0	a.		C D	
		с с с	Hark IP Pres Hark IP DSC Police Simple	odence 0 p af:		1		
			Color Ho Color Car Color Car	de Co nform Class	lorBlind 🖻			

- c. In the Assign Queue list, select 2.
- d. Click Apply.

12. Assign queue 3 to test_dept.

a. Select QoS > DiffServ > Advanced > Policy Configuration.

System Swil	iching.	Routing	QoS	Security	Monitoring	Maintenance.	Help	Index
CoS DiffServ								
Diffserv Wizard	Poli	cy Configura	tion					
Basic	p	olicy Configura	tion		.9	9		
> DiffServ Configuration		Policy Selector	8	Policy Type	Member Class			
. Class					finance_dept 💌	1		
Configuration		internet_access		In	finance_dept			
Configuration	C	internet_access		In	marketing_dept			
- Service	E	internet_access		In	test_dept			
Configuration	Г	internet_access		1h	development	l.		

b. Click the internet_access check mark for test_dept.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
CoS DiffServ				Ŧ						
Diffserv Wizard Basic Advanced > DiffServ Configuration • Class Configuration • Class Configuration • Class Configuration • Service Configuration • Service Statistics	4 Policy Cla	Policy Class Configuration Class Information Policy Name								
	Policy	Policy Type In Hernber Class Name test_dept								
	P0 Assign Policy	Policy Attribute Policy Attribute C Drop								
		0000	Mark COS Mark IP Pro Mark IP DSC Police Simpl	codence 0 p af:	9 11 11 12	1				
			Color Me Color Co Color Co	nform Class	ilorBlind 💽					
			Commit	ted Rate		1				

- c. In the Assign Queue list, select 3.
- d. Click Apply.

13. Assign queue 4 to development_dept.

a. Select QoS > DiffServ > Advanced > Policy Configuration.

System Swi	tching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
Diffserv Wizard	Pol	icy Configura	tion					
Basic		Policy Configura	tion		.0	8		
 DiffServ Configuration 		Policy Selector	8	Policy Type	Member Class			
a Class					finance_dept 💌	1		
Configuration		internet_access		In	finance_dept			
Configuration	C	internet_access		In	marketing_dept			
» Service	E	internet_access		In	test_dept			
Configuration • Service Statistics	1	Internet_access		10	development	E.		

b. Click the **internet_access** check mark for development_dept.

System Swi	tching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DillServ								
Diffserv Wizerd Basic Advanced > DiffServ Configuration > Class Configuration > Service Configuration > Service	Policy Class							
	Policy No Policy Ty Hember							
	Polic Assign Q Policy At	y Attribute Juenne 4] Drop				(T)	
		0000	Mark COS Mark IP Prec Mark IP DSCI Police Simple	edence 0 e af:	1 .	1		
			Color Mon Color Cor Color Cor	le Co form Class	lorBind 🔳			

- c. In the Assign Queue list, select 4.
- d. Click Apply.
- **14.** Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the inbound direction.
 - a. Select QoS > DiffServ > Advanced > Service Configuration.

System Swit	ching	Routing	GoS S	ecurity	Monitoring	Maintenance	Help	Index
CoS DiffSore								
Diffserv Wizard Basic Advanced	Diff	Serv Serv	ice Configuration e Config	n		2		
DiffServ		All	Go To Int	erfoce				
> Class		Interface	Policy In	Direction	Operational Status			
* Policy		-	internet_access					
Configuration	P	1/0/1		1				
	9	1/0/2						
Service Statistics	×.	1/0/3						
Service States	9	1/0/4						
	1	1/0/5						

- b. Scroll down and select the check boxes for interfaces 1/0/1, 1/0/2, 1/0/3, and 1/0/4.
- c. In the Policy In list, select internet_access.
- d. Click Apply.
- **15.** Set the CoS queue 1 configuration for interface 1/0/5.
 - a. Select QoS > CoS > Advanced > Interface Queue Configuration.

A screen similar to the following displays.

System	Switching	Routin	19.	QoS Se	curity Mon	illoring	Maintenance	Help	Index
CoS DiffServ	¢		- 10			e e			
Dasic Advanced	Int	erface Qu	ieue Co	onfiguration	1	8	ñ		
Configuration	1	All		Go To Int	erface	60			
 902.1p Queue Mapping IP Precedence 		Interface	Queue 1D	Minimum Bandwidth	Scheduler Type	Queue Managemen Type			
IP DSCP Que	10	1/0/5	1	25	Weighted -	taildrop			
Mapping	E	1/0/1	0	0	weighted.	taildrop			
CoS Interface	_	1/0/2	0	0	veighted	taildrop.			
Configuartion	C	1/0/3	0	0	weighted	talldrop			
Cathgaratan	C	1/0/4	0	0	weighted	taddrop			
	P	3/0/5	0	9	valohted	talidrop			

b. Scroll down and select the Interface 1/0/5 check box.

Now 1/0/5 appears in the Interface field at the top.

- c. In the Queue ID list, select 1.
- d. In the Minimum Bandwidth field, enter 25.
- e. Click Apply.
- **16.** Set the CoS queue 2 configuration for interface 1/0/5.
 - a. Select QoS > CoS > Advanced > Interface Queue Configuration.

System Swit	ching	Routin	19	QoS Se	curity Mon	itoring	Maintenance	Help	Index
CoS DiffServ									
Basic	Int	erface Qu	ieue Co	onfiguration	E.				
* CoS	103	Interface Q	ueue Co	figuration			D		
Configuration	×.	All		Ge To Int	erface	00	0		
 802.1p Qumue Mapping IP Precedence 		Interface	Queue ID	Ninimum Bandwidth	Scheduler Type	Queue Managemen Type	it.		
Queue Mapping IP DSCP Queue		1/0/5	2	25	Weighted 💌	taildrop			
Mapping	E	1/0/1	1	0	weighted	taildrop			
» CoS Interface	C	1/0/2	1	0	weighted	talldrop			
Configuation		1/0/0	1	0	weighted	taildrop			
Configurations	1	1/0/4	1	0	weighted	taildrop			
	1	1/0/5	4	23	veighted	taildrop			

b. Under Interface Queue Configuration, scroll down and select the interface **1/0/5** check box.

Now 1/0/5 appears in the Interface field at the top.

- c. In the Queue ID list, select 2.
- d. In the Minimum Bandwidth field, enter 25.
- e. Click Apply.
- **17.** Set the CoS queue 3 configuration for interface 1/0/5.
 - a. Select QoS > CoS > Advanced > Interface Queue Configuration.

A screen similar to the following displays.

System	Switching	Routin	1g.	QoS Se	curity Mon	itoring	Maintenance	Help	Index
CoS DiffServ			90						
Basic Advanced + CoS	Int	erface Qu Interface Q	ieue Ca	onfiguration afiguration	1	1	8		
Configuration	× .	All		Go To Int	erface	90	3		
 902.1p Queue Mapping IP Precedence 		Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Managemen Type	it		
 IP DSCP Queu 		1/0/5	3 .	25	Weighted -	taildrop			
Mapping	C	1/0/1	2	0	weighted	taildrop			
* CoS Interface	F	1/0/2	2	0	veighted	taildrop			
Configuation		1/0/3	2	0	weighted	taildrop			
Configuration	E .	1/0/4	4	0	weighted .	taildrop			
	R	1/0/8	2	28	veighted	talideop			
		1/0/6	2	0	weighted	taildrop			
	C	1/0/7	2	0	weighted	taildrop			

b. Under Interface Queue Configuration, scroll down and select the interface **1/0/5** check box.

Now 1/0/5 appears in the Interface field at the top.

c. In the Queue ID list, select 3.

- d. In the Minimum Bandwidth field, enter 25.
- e. Click Apply.
- **18.** Set the CoS queue 4 configuration for interface 1/0/5.
 - a. Select QoS > CoS > Advanced > Interface Queue Configuration.

System	Switching	Routir	10	QoS Se	curity Mon	itoring	Maintenance	Help	Index
CoS DiffServ									
Rasic Advanced > CoS	Int	erface Qu Interface Q	ieue Co	onfiguration	6		D		
Configuration		-		Go To Int	erface	00			
 B02.1p Queue Mapping IP Precedence 		Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Manageme Type	nt		
 IP DSCP Queu 		1/0/5	4 💌	25	Weighted 🕥	taildrop			
Mapping	E	1/0/1	э	0	weighted	-taildrop			
CoS Interface	-	1/0/2	3.	٥	weighted	talldrop			
Configuartion	- C	1/0/3	3	0	weighted	taildrop			
	-	1/0/4	9	0	weighted	taildrop			
	1	1/0/3	a	25	weighted	talldrop			
		1/0/6	3	0	weighted	taildrop			
	C	1/0/7	3	0	weighted	taildrop			

b. Under Interface Queue Configuration, scroll down and select the Interface **1/0/5** check box.

Now 1/0/5 appears in the Interface field at the top.

- c. In the Queue ID list, select 4.
- d. In the Minimum Bandwidth field, enter 25.
- e. Click Apply.

DiffServ for VolP

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time sensitive: For a network to provide acceptable service, a guaranteed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: A similar script should be applied to Router 2.



Figure 16. Diffserv for VoIP in Router 1

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure DiffServ for VolP

1. Enter Global configuration mode. Set queue 5 on all ports to use strict priority mode. This queue will be used for all VoIP packets. Activate DiffServ for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#cos-queue strict 5
(Netgear Switch) (Config)#diffserv
```

2. Create a DiffServ classifier named class_voip and define a single match criterion to detect UDP packets. The class type match-all indicates that all match criteria defined for the class must be satisfied in order for a packet to be considered a match.

```
(Netgear Switch) (Config)#class-map match-all class_voip
(Netgear Switch) (Config class-map)#match protocol udp
(Netgear Switch) (Config class-map)#exit
```

3. Create a second DiffServ classifier named class_ef and define a single match criterion to detect a DiffServ code point (DSCP) of EF (expedited forwarding). This handles incoming traffic that was previously marked as expedited somewhere in the network.

```
(Netgear Switch) (Config)#class-map match-all class_ef
(Netgear Switch) (Config class-map)#match ip dscp ef
(Netgear Switch) (Config class-map)#exit
```

4. Create a DiffServ policy for inbound traffic named pol_voip, then add the previously created classes class_ef and class_voip as instances within this policy.

This policy handles incoming packets already marked with a DSCP value of **EF** (according to the **class_ef** definition), or marks UDP packets according to the **class_voip** definition) with a DSCP value of **EF**. In each case, the matching packets are assigned internally to use queue 5 of the egress port to which they are forwarded.

```
(Netgear Switch) (Config)#policy-map pol_voip in
(Netgear Switch) (Config policy-map)#class class_ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class class_voip
(Netgear Switch) (Config policy-class-map)#mark ip-dscp ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-class-map)#exit
```

5. Attach the defined policy to an inbound service interface.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in pol_voip
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Diffserv for VoIP

- 1. Set queue 5 on all interfaces to use strict mode.
 - a. Select QoS > CoS > Advanced > CoS Interface Configuration.

System 5	witching	Routin	18	GoS Se	curity Mor	itoring	Maintenance	Help	Index
CoS* DiffServ									
Dasic	Int	erlace Qu	ieue Co	onfiguration	e.				
+ CoS	100	Interface Q	ueue Co	figuration					
Configuration	1	All		Go To Int	erface	00			
Mapping + IP Precedence		Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Managemen Type	t.		
IP DSCP Queue		1/0/2	5 .	0	Strict .	taildrop			
Mapping		1/0/1	0	0	veighted	taildrop			
> CoS Interface	57	1/0/2	0	0	weighted	talldrop			
Configuartion	Г	1/0/3	0	0	weighted	taildrop			
Configuration	_	1/0/4	0	o	veighted	taildrop			

- b. Under Interface Queue Configuration, select all the interfaces.
- c. In the Queue ID list, select 5.
- d. In the Scheduler Type list, select Strict.
- e. Click Apply to save the settings.
- 2. Enable DiffServ.
 - a. Select QoS > DiffServ > Basic > DiffServ Configuration.

A screen similar to the following displays.

System Swi	tching Routing	QoS	Security	Monitoring	Mointenonce	Help	Index
CoS DiffServ						6	
Diffserv Wizard	Diffserv configur	ation					
* Diffsore	DiffServ Config				00		
•Configuration > Advanced	Diffsery Admin Mode	C Disa	ble 🕜 Enabl				

- b. For Diffserv Admin Mode, select the Enable radio button.
- c. Click Apply to save the settings.
- **3.** Create a class class_voip.
 - a. Select QoS > DiffServ > Advanced > DiffServ Configuration.

System 5w	tching	Routing	GoS	Security	Monitoring	Maintenance	Help	Index
CoS DIESON		8		12				
 Diffserv Wizard Basic Advanced 	Class	Configurat	ion			2		
DiffServ Configuration Class Configuration		lass Name dass_voip		Class T All In	ype			
Policy Configuration Service Configuration Configuration								

- b. In the Class Name field, enter class_voip.
- c. In the Class Type list, select All.
- d. Click Add to create a new class.
- e. Click class_voip.

System Sw	tching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ								
Diffserv Wizard	Cla	ss Informatio	n				.0	
Basic Advanced > DiffServ	Class 7	iame ype		class_voi All	•			
Configuration .	Dif	fserv Class Co	onfiguration	ř.			1.00	
Configuration • Policy Configuration • Service Configuration • Service Statistics	Match Refere Class o VLAN Ethern	Every nice Class of Service et Type			(1-4 2	293) (0600 - 17777)		
	Source Destin	MAC Mask MAC Mask ation MAC						
	Protoc	ol Type		UDP .	0 (0 - 255)			

- f. In the Protocol Type list, select UDP.
- g. Click Apply to create a new class.
- 4. Create a class class_ef:
 - a. Select QoS > DiffServ > Advanced > DiffServ Configuration.

System Swi	tching Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ							
Diffserv Wizard Basic Advanced	Class Configur	ation			2		
DiffServ Configuration	Class Name		Class T	Abs.			
Configuration	C class_voip		All				
Configuration Service Configuration							
> Service Statistics							

- b. In the Class Name field, enter class_ef.
- c. In the Class Type list, select All.
- d. Click Add to create a new class.
- e. Click class_ef.

System 5wit	ching Routing QoS	Security Monitoring Maintenance Help Inc	dex
CoS DiffServ			
Diffserv Wizard Basic Advanced • DiffServ Configuration • Clear Configuration • Policy Configuration	Diffserv Class Configurat Match Every Reference Class Class of Service VLAN Ethemot Type Source MAC	ion (1 - 4093)	
 Service Configuration Service Statistics 	Source MAC Hask Destination MAC Destination MAC Hask Protocol Type Source IP Address Source Mask	(0 - 355)	
	Source L4 Port Destination TP Address Destination Hask	· 0 (0 - 65535)	
	Destination L4 Port IP DSCP		

- f. In the IP DSCP list, select ef.
- g. Click Apply to create a new class.
- 5. Create a policy pol_voip. and add class_voip to this policy.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System Swi	tching	Routing	GoS	Security	Monitoring	Maintenance	Help	Index
CoS DillServ								
Diffserv Wizard Basic	Policy	Configurat	tion tion		3	D.		
> DiffServ Configuration	P	olicy Selector	8	Policy Type	Member Class			
Class Configuration Policy Configuration Service		ail_vois			class_voip_	2		
Configuration Service Statistics								

- **b.** In the **Policy Selector** field, enter **pol_voip**.
- c. In the Member Class list, select class_voip.
- d. Click Add to create a new policy.
- e. Click the pol_voip whose class member is class_voip.

ang koona	0 000	Security	Monitoring	Maintenance	Help	Index
Class Inform	nation				0	
Policy Name		pol_voip				
Policy Type		In	1			
Member Class Na	me	class_voir	p			
Policy Attrib	ute				49	
Assign Queue	5 -					
Policy Atmbute	C Drop					
	C Mark COS	0	-1			
	C Hart 10 Dance	adapter 0	1			
	C much in pres			1		
	nank IP DSLP	Lar.	. 21			
	Class Inform Policy Name Policy Type Mamber Class Na Policy Attrib Assign Queue Policy Attribute	Class Information Policy Name Policy Type Mamber Class Name Policy Attribute Assign Queue 5 Policy Attribute C Drop C Mark COS C Mark IP Proc C Mark IP DSCS C Police Simple	Policy Name Policy Type In Mamber Class Name class_voir Policy Attribute class_voir Policy Attribute C C Mark COS C Mark IP Decedence C Mark IP DECP C Police Simple	Class Information Policy Name pol_voip Policy Type In Mamber Class Name class_voip Policy Attribute class_voip Policy Attribute 5	Class Information Policy Name pol_voip Policy Type In Mamber Class Name dass_voip Policy Attribute dass_voip Policy Attribute Drop C Hark EOS 0 = C Hark IP Precedence 0 = C Mark IP DSCP at11 #	Class Information

- f. In the Assign Queue list, select 5.
- g. For Policy Attribute, select the Mark IP DSCP radio button, and select ef.
- h. Click Apply to create a new policy.
- 6. Add class_ef to the policy pol_voip.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System S	witching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ				90- 				_
Diffserv Wizard Basic	Polic	y Configura	tion tion			0		
DiffServ Configuration	1	Policy Selector		Policy Type	Hember Class			
» Class		pol_voip		10	class_ef	2		
Configuration	÷.,	and_write		In	class_wnip			
Configuration								
Service Configuration Service Statistic								

- b. Under Policy Configuration, scroll down and select the pol_voip check box.
 Pol_voip now appears in the Policy Selector field at the top.
- c. In the Member Class list, select class_ef in.
- d. Click Apply to add the class class_ef to the policy pol_voip.
- e. Click the pol_voip whose class member is class_ef.

System Swit	ching Routing	Qo5	Security	Monitoring	Maintenance	Help	Index
CoS DiffServ							
Diffserv Wizard	Policy Class C	onfiguration					
Basic	Class Informa	stion				(1)	
> DiffServ	Policy Name		pol_voip				
Configuration	Policy Type		In				
Configuration	Hember Class Nam		dass_ef	14			
· Faller	Policy Attribu	te				C	
Configuration	Assign Queue	5 🛞					
Configuration	Policy Atmibute	C Drup					
Service Statistics	0	Mark EDS	0	-			
		C Mark IP Prec	edence 0				
		Mark IP DSC	e lef	1.	t		

- f. In the Assign Queue list, select 5.
- g. Click Apply to create a new policy.
- 7. Attach the defined policy to interface 1/0/2 in the inbound direction.
 - a. Select QoS > DiffServ > Advanced > Service Configuration.

A screen similar to the following displays.

System Switt	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
CoS DiffServ										
Diffserv Wizard	Diff	Serv Servic	e Configurat	ion						
Basic	Policy Service Config (2)									
DiffServ		A	Go To	Interface	00					
Class Configuration		Interface	Policy In	Direction	Operational Status					
Policy		1/0/2	pol_voip							
Configuration	Γ.	1/0/1								
Carrier.	12	1/0/2								
Service Statistics	Γ.	1/0/3								
North Contraction of the		1/0/4								

b. Scroll down and select the Interface **1/0/2** check box.

Now 1/0/2 appears in the Interface field at the top.

- c. In the Policy In list, select pol_voip.
- d. Click Apply to create a new policy.

Auto VolP

The Auto-VoIP feature makes it easy to set up VoIP for IP phones on a switch. This functionality copies VoIP signaling packets to the CPU to get the source and destination IP address and Layer 4 port of the current session. Based on these parameters a filter is installed to assign the highest priority to VOIP data packets. As soon as the call ends, the filters are removed.



Figure 17. Auto VoIP

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Auto VoIP

This script in this section shows how to set up auto VoIP system-wide.

1. Enable auto VoIP on all the interfaces in the device.

```
(Netgear Switch) (Config)# auto-voip all
```

2. View the auto VoIP information:

(Netgear	Switch) #	show auto-voip	interface all
	Interface	Auto VoIP Mode	Traffic Class
	1/0/1	Enabled	6
	1/0/2	Enabled	6
	1/0/3	Enabled	6
	1/0/4	Enabled	6
	1/0/5	Enabled	6
	1/0/6	Enabled	6
	1/0/7	Enabled	6
	1/0/8	Enabled	6
	1/0/9	Enabled	6
	1/0/10	Enabled	6
	1/0/11	Enabled	6
	1/0/12	Enabled	б
	1/0/13	Enabled	6
	1/0/14	Enabled	6
	1/0/15	Enabled	6
	1/0/16	Enabled	б
	1/0/17	Enabled	6
	1/0/18	Enabled	6
	1/0/19	Enabled	6
	1/0/20	Enabled	б
	More o	r (q)uit	
	Interface	Auto VoIP Mode	Traffic Class
	1/0/21	Enabled	6
	1/0/22	Enabled	6
	1/0/23	Enabled	6
	1/0/24	Enabled	6
	1/0/25	Enabled	6
	1/0/26	Enabled	6
	1/0/27	Enabled	6
	1/0/28	Enabled	6

Auto VoIP classifies and prioritizes the packets and places only the packets in the higher-priority queue. In the previous example, the packets are placed in queue 6. You can override the egress queue setting using the cos-queue strict or cos-queue min-bandwidth command.

Web Interface: Configure Auto-VoIP

- 1. Enable auto VoIP for all the interfaces in the device.
 - a. Select QoS > DiffServ > Auto VoIP.

A screen similar to the following displays.

System Sy	witching	Routing	QoS	Security	Monitoring	Maintenance	Help				
Co5 DiffSory					<u>а</u> А						
Diffserv Wizard	1	Auto VoIP Configuration									
Basic	-	Auto VoIP Co	nfiguratio	n Co To Interfa	Go To Interface						
Advanced		Interface	Auto	OIP Mode		Traffic Class					
		1/0/1	Disable	£		6					
		1/0/2	Disable			6					

- **b.** Select the check box in the first row to select all the interfaces.
- c. In the Auto VoIP Mode field, select Enable.

A screen similar to the following displays.

System Switch	ing Kouting	Gos Security Monito	iring Maintenance Help							
CoS DillServ										
Diffsery Wizard	Auto VoIP Cor	nfiguration								
Auto Volt	Auto VolP Co	Auto VoIP Configuration								
Advanced			10000							
	Au	Le le Interface								
	Interface	Auto VoIP Mode	Traffic Class							
	12	Enable +								
	2 1/0/1	Disable	6							
	1/0/2	Disable	6.							
	1/0/3	Disable	6							
	9 1/0/4	Disable	6							
	2 1/0/5	Disable								
	1/0/6	Disable	1. The second se							
	2 1/0/7	Disable	6							
	1/0/8	Disable	6							
	2 1/0/9	Disable								
	2 1/0/10	Disable								
	97 1/0/11	Disable	6							
	07 1/0/12	Disable	6.							
	0 1/0/13	Disable	6							
	9 1/0/14	Disable	6							
	9 1/0/15	Disable	6							
	1/0/16	Disable	6							
	1/0/17	Disable	6							
	1/0/18	Disable:	6							
	1/0/19	Disable	6							
	2 1/0/20	Disable	6							

d. Click Apply.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help		
CoS Dillis	brv						j		
Diffserv Wi	zard	Auto VoIP Co	onfigura	tion					
Basic		Auto VoIP Configuration							
Advanced		I All		Go To Interface					
		Interface	Auto	VoIP Mode		Traffic Class	3		
		2/0/1	Enab	19		6			

DiffServ for IPv6

This feature extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification.



Figure 18. DiffServ for IPv6

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure DiffServ for IPv6

The script in this section shows how to prioritize ICMPv6 traffic over other IPv6 traffic.

1. Create the IPv6 class classicmpv6.

```
(Netgear Switch) (Config)# class-map match-all classicmpv6 ipv6
```

2. Define matching criteria as protocol ICMPv6.

```
(Netgear Switch) (Config-classmap) # match protocol 58
(Netgear Switch) (Config-classmap) # exit
```

3. Create the policy policyicmpv6.

(Netgear Switch) (Config)# policy-map policyicmpv6 in

4. Associate the previously created class classicmpv6.

(Netgear Switch) (Config-policy-map)# class classicmpv6

5. Set the attribute as assign queue 6.

(Netgear Switch) (Config-policy-classmap)# assign-queue 6
(Netgear Switch) (Config-policy-map)# exit

6. Attach the policy policy_icmpv6 to interfaces 1/0/1,1/0/2 and 1/0/3:

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/1)# exit
(Netgear Switch) (Config)# interface 1/0/2
(Netgear Switch) (Interface 1/0/2)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/2)# exit
(Netgear Switch) (Config)# interface 1/0/3
(Netgear Switch) (Interface 1/0/3)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/3)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/3)# service-policy in policyicmpv6
```

Web Interface: Configure DiffServ for IPv6

- 1. Create the IPv6 class classicmpv6.
 - a. Select QoS > DiffServ > Advanced > IPv6 Class Configuration.

A screen similar to the following displays.

System Swite	ching Routing	QoS	Security	Monitoring	Maintenance	Help	
CoS DiffSorv		- 14 .				o 1960.	
Diffserv Wizard Auto VoIP	IPv6 Clas	s Name					
Advanced	Class?	lame	Class Type				
* DiffServ				•			
Configuration			100				
> Class Configuration							
+ JPr4 Class							
* Policy Configuration							

- b. In the Class Name field, enter classicmpv6.
- c. In the Class Type list, select All.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help				
CoS Diffs	erv	1									
Diffserv Wi	zard	IPv6 Class	Name								
Auto VoIP Basic		IPv6 Class Name									
Advanced		Class Na	tlass Type								
> DiffServ Configurati	ion	Classicm	pv6		All 👻						
> Class											
Configurati	ion										
a Policy											

d. Click Add to create the IPv6 class.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help		
CoS DiffSen									
Diffserv Wize Auto VoIP	urd	IPv6 Class	Name						
Basic		Class Name							
Advanced		Class Na	me Class	Туре					
 DiffServ Configuration 	i i								
» Class	2	Classionp	IIA BY	3					
Configuration	Ř.								
· If you Chees									
a Polica									

- 2. Define matching criteria as protocol ICMPv6.
 - a. Select QoS > DiffServ > Advanced > IPv6 Class Configuration.

System Sv	itching	Routing	QoS	Security	Monitoring	Maintenance	Help
CoS DiffServ							
Diffserv Wizard Auto VoIP Basic	I	Pv6 Class N Class Name	ame				
* DiffServ		Class Nan	ne Class	Туре			
Class Configuration Pre-Class Configuration Configuration		C classionay	E All				

b. Click the class classicmpv6.

A screen similar to the following displays.

System	Switching	Routing	GoS	Security	Monitoring	g Maintenance	Help				
CoS DillSen	£					100					
Diffserv Wize Auto VoIP	ard	IPv6 Class Configuration IPv6 Class Information									
Advanced > DiffServ Configuration	1	Class Name Class Type	rit								
 Class Configuration 	6) 17	IPv6 DiffServ Class Configuration									
 Origination Carifiquentian Policy 		Match Every Reference (lass 1ass		Any •						
Configuration • Service Inter Configuration	face	 Source Pref Source L4 P 	ix/Length ort	de	domain + (0 to 65535)						
> Service Stati	stics	 Destination Destination 	Prefix/Long L4 Port	ete 🗌	domain + (0 to 63538)						
		Flow Label (6 to 1048375) (9 DSCP (0 to 63)									

c. Select the Protocol Type radio button, select Other, and enter 58.A screen similar to the following displays.

System Switchi	ng Routing QoS	Security M	onitoring l	Maintenance	Help	Index			
CoS DillServ									
Diffserv Wizard	Class Configuration								
Basic	Class Information	Class Information							
Advanced DiffServ Configuration	Class Name Class Type			All +					
Class Configuration	DiffServ Class Configuration								
· Dres Chart	Match Every	Any -							
Policy Configuration Saturday Interface	Reference class Protocol Type Supera Prefer (Japath	Other •	-	58		0 to 255)			
Service Interface Configuration Service Statistics	Source L4 Port	domain 🚽			10	0 to 65525)			
	 Destination L4 Port Flow Label 	domain ~	(8 to 104857		(0 to 65535)	1		
	TP DSCP	+ 106	Tribul proofs			(0 to 63)			

d. Click Apply.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help			
CoS Diffs	iv:									
Diffserv Wi	zard	IPv6 Class	Configura	ition						
Auto VoIP	a la cara	IPv6 Class	Informatio	n			۷			
* Advanced > DiffServ Configurate	00	Class Name Class Type								
Class		IPv6 DiffServ Class Configuration								
Service Interface Configuration Service Interface Configuration Service Statistics	on on ierface on atistics	 Natch Every Reference 0 Protocol Tyy Source Preficience Source L4 P Destination Destination Flow Label 1P DSEP 	r Jass je ix/Langth ort Prefix/Lang L4 Port	An IC do	ÿ + main + 11 +	(0 to 255) (0 to 45535) (0 to 45535) (0 to 45535) (0 to 1048575) 0 to 51)				

- 3. Create the policy policyicmpv6, and associate the previously created class classicmpv6.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

A screen similar to the following displays.

System Switch	hing Routing	QoS	Security	Monitoring	Maintenance	Help			
CoS DiffSerr						840 - 308 			
Diffserv Wizard Auto YoIP	Policy Confie Policy Conf	guration							
Basic Policy		me	Policy Type	e Member Class					
Differv Configuration Class Configuration Prv6 Class Configuration Class Configuration Service Interface Service Interface									

- b. In the Policy Name field, enter policyicmpv6.
- c. In the Policy Type list, select In.
- d. In the Member Class list, select classicmpv6.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help		
CoS DiffSer	e.								
Diffserv Wize	ard P	olicy Confi	guration						
Auto VoIP Basic	1	Policy Conf	iguration						
* Advalued		Policy No	me	Policy Type		Nember Class			
> DiffServ Configuration		policyicm	ipiv6	In 🝝		classicmpvé 💌			
+ Class					196-				
Configuration	P.								
* IPvo Class Configuration									
a sping (
Califyratio									
> Service Inter	rface								

e. Click Add.

- 4. Set the attribute as assign queue 6.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

Systum Swite	hing Routing	QoS	Security	Monitoring	Maintenance	Help			
CoS DillSere									
Diffserv Wizard	Policy Confi	guration							
Auto YoIP Basic	Policy Con	figuration							
Advanced	Policy N	ame	Policy Type		Member Class				
Configuration			•		*				
» Class	E selicyion	ave	In		tassicmpvil				
Configuration + IPv6 Class									
Configuration									
a Palicy									
* Service Interface									
Configuration									

b. Click the policy **policyicmpv6**.

Systum Switch	ing Routing	g QoS	Security	Monitoring	Maintenance	Help
CoS DillServ						
Diffserv Wizard	Policy Co	nfiguration				
Auto YoIP Basic	Palicy	Configuration				
Advanced	Polic	y Name	Policy Type		lember Class	
> DiffServ Configuration			•		*	
» Class	E policy	icmové	In	1	assicmpy#	
Configuration						
Configuration						
e Paler						
* Service Interface						
Configuration						

c. In the Assign Queue list, select 6.

Diffserv Wizard Auto YoIP Basic	Policy Class	c f				
Diffserv Wizard Auto YoIP Basic Advanced + Diffserv Configuration + Class	Class Inform Policy Name Policy Type Member Class Na	nation		Eviliationa(6		
Class Configuration TRv6 Class	Policy Attrit	oute				
Configuration • Palar Configuration • Service Interface Configuration • Service Statistics	Policy Atrybute	Assign Queue Drop Mark IP COS Mark IP Precedence Mark IP DSCP Simple Policy	6 • 0 • af11 - Color Hode Consitted Rate	Color Blind		
			Conform Action	 G send C Drop C Mark Cos C Mark LP Precedence 	<u>D =</u> <u>D =</u>	
			Violate Action	C Mark IP DSCP C Send C Drop C Mark CoS C Mark IP Precedence	[0] + [10]	

- d. Click Apply.
- 5. Attach the policy policyicmpv6 to interfaces 1/0/1,1/0/2 and 1/0/3.
 - a. Select QoS > DiffServ > Advanced > Service Interface Configuration.

System Sw	itching	Routing	QoS	Security	Monitoring	Mointenance	Help
CoS DillServ							
Diffserv Wizard	s	ervice Inte	erface Co	nfiguration			
Auto VoIP	1.5	Service Int	erface Con	figuration			
Advanced	1.1	All		Go To Interfac	•	00	
> DiffServ		Interface		Policy Name	Directio	n Operational	Status
Configuration		1			-		
Configuration		1/0/1			In		
+ IPv6 Class	12	1/0/2			In		
Configuration	1	1/0/3			In		
* Policy	12	1/0/4			In		
Configuration	1	1/0/5			in		
	1	1/0/6			In		
» Service Statistics	1	1/0/7			In		
	- 1	1/0/8			In		

- b. In the Policy Name list, select policyicmpv6.
- c. Select the Interface 1/0/1, 1/0/2, and 1/0/3 check boxes.

System	Switching	R	outing	QoS	Security	Monit	toring	Maintenance	Help
CoS DillSer	6						98 AU		
Diffserv Wiza	und	Serv	ice Inter	face Cor	nfiguration				
Auto VoIP Basic		Se	rvice Inte	rface Conf	iguration				
* DiffServ	All		0						
Configuration	(Interface	8	Policy Nam	e l	Direction	Operational	Status
* Class Confiduration			-		policyicmpy	6 •		i i	
* IPv6 Class			1/0/1				In		
Configuration	>	-	1/0/2				In		
Configuration		-	1/0/3				In		
	face:	121	1/0/4				In		
· Service Stati	stics	12	1/0/5				In		
		10000	a lan ba						

d. Click Apply.

A screen similar to the following displays.

System Sw	itching	Routing	QoS	Security	Monitoring	Maintenance	Help
CoS DiliServ							
Diffserv Wizard	Se	rvice Inte	rface Co	nfiguration			
Auto VoIP Basic	100	Service Int	erface Com	figuration			
* DiffServ		All		Go To Inter	rface 👘	00	
Configuration		Interface		Policy Nam	e Direct	tion Operational	Status
 Class Configuration 					-		
> IPv6 Class	E	1/0/1		policyicmpvt	5 In	Up	
Configuration	35	1/0/2		policyicmpv6	i In	Up .	
Configuration	1	1/0/3		policyicmpvé	5 In	Up	
· Service Interfece	12	1/0/4			In		
· Service Statistics	R.	1/0/5			En		
TRANSPORT OF TRANSPORT	- 12	1/0/6			In		

Color Conform Policy

This example shows how to create a policy to police the traffic to a committed rate. The packets with IP precedence value of 7 are colored green to ensure that these packets are the last to be dropped when there is congestion. The example is shown as CLI commands and as a web interface procedure.

CLI: Configure a Color Conform Policy

1. Create a VLAN 5 and configure ports 1/0/13 and 1/0/25 as its members.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#vlan participation include 5
(Netgear Switch) (Interface 1/0/13)#vlan tagging 5
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Interface 1/0/25)
(Netgear Switch) (Interface 1/0/25)#vlan participation include 5
(Netgear Switch) (Interface 1/0/25)#vlan tagging 5
(Netgear Switch) (Interface 1/0/25)#vlan tagging 5
(Netgear Switch) (Interface 1/0/25)#vlan tagging 5
```

2. Create classes class_vlan and class_color.

Note: DiffServ service is enabled by default.

```
(Netgear Switch) (Config)#class-map match-all class_vlan
(Netgear Switch) (Config-classmap)#match vlan 5
(Netgear Switch) (Config-classmap)#exit
(Netgear Switch) (Config)#class-map match-all class_color
(Netgear Switch) (Config-classmap)#match ip precedence 7
(Netgear Switch) (Config-classmap)#exit
```

3. Create a policy to police the traffic to a rate of 1000 kbps with an allowed burst size of 64 KB. Furthermore, the packets with IP precedence value of 7 will be colored green. That means these packets will be the last packets to be dropped in the event of congestion beyond the policed rate.

(Netgear	Switch)	(Config)#policy-map policy_vlan in
(Netgear	Switch)	(Config-policy-map)#class class_vlan
(Netgear transmit	Switch) violate-	(Config-policy-classmap)#police-simple 1000 64 conform-action action drop
(Netgear	Switch)	(Config-policy-classmap)#conform-color class_color
(Netgear	Switch)	(Config-policy-classmap)#exit
(Netgear	Switch)	(Config-policy-map)#exit

4. Apply this policy to port 1/0/13.

```
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#service-policy in policy_vlan
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure a Color Conform Policy

- 1. Create a VLAN.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays.

System	Switching	Routin	g QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP	Multicost	Address Toble	Ports LAG	8				
Basic	VLA	N Config	uration					
> VLAN	R	eset					(2)	
Advanced	Rese	et Configurat	ion					
10.0007-005-0.00	(C 1)	oternal VI 4	N Configuratio	D			(7)	
	Inte	mal VLAN A	location Base		4093	×.		
	Inte	mal VLAN Al	Descending					
	v	LAN Config	uration				1	
		VLAN ID	LAN Name	v	LAN Type	Make Static		
		5				Disable 💌		
		1 1	Default	D	efault	Disable		

- b. In the VLAN ID field, enter 5.
- c. Click Add.
- 2. Add ports 1/0/13 and 1/0/25 to VLAN 5.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

A screen similar to the following displays.

System Swi	tching		Re	outin	ng		Qo	s	1	S	ecur	ity	T)	N	loni	tori	ng		Mo	int	end	ance	3		Help	
VLAN STP Mul	ticost (Add	ress	Tabl	•	Port	s	LAG	G																	
Basic	VLA	NN	/ler	nb	ers	nip																				
Advanced » VLAN	v	LAN	I Me	mb	erst	ip																			1	
Configuration	VLA	NID	i.			5 🔻									Gre	oup (Oper	atio	n	ι	Inta	g Al	I	-		
» VLAN Membership	VLA	N Na	me		Ţ										U	NTAC	GEE	POP	T ME	MBE	RS	l				
» VLAN Status	VLA	N Ty	pe.			Stat	ic									TAG	GED	POR	MEN	BER	s	1				
Configuration		Unit	t 1		-																					
» MAC Based VLAN	Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
» IP Subnet Based														Т												
VLAN		25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	
» Port DVLAN		1										122														
Configuration		49	50	51	52																					
» Protocol Based	10	121												_											-	

b. In the VLAN ID list, select 5.

- c. Click Unit 1. The ports display.
- d. Click the gray boxes under ports 13 and 25 until T displays.The T specifies that the egress packet is tagged for the port.
- e. Click Apply.
- 3. Create a class class_vlan:
 - a. Select QoS > DiffServ > Advanced > Class Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSer	e.		G L 2					
 Diffserv Wiza Auto VoIP Basic Advanced DiffServ Configuration Cless Configuration IPv6 Class Configuration Policy Configuration Service Intel Configuration 	Class Class	Name Iss Name Iass Name dass_vlan		Class T All	уре		•	

- **b.** Enter the following information:
 - In the Class Name field, enter class_vlan.
 - In the Class Type list, select All.
- c. Click Add to create a new class class_vlan.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
CoS DiffServ	1								
Diffserv Wizar	d Class	Class Name							
Auto VoIP	Cla	Class Name					۲		
Basic		Class Name			Class Type				
» DiffServ									
Configuration		Class vlan			All				
Configuration									
» IPv6 Class									
Configuration									
* Policy Configuration									
» Service Interfa	ice								
Configuration									
» Service Statist	ics								

d. Click class_vlan to configure this class.
System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSo	rv _		61 D-					
Diffserv Wiz	ard Class	Configurat	ion					
Auto VoIP	Cla	ss Informatio	n				(7)	
Advanced	Class	Name			class_vlan			
» DiffServ	Class	Туре			All			
Configuratio	on Dif	fServ Class Co	onfiguration				(7)	
Configuration > IPv6 Class Configuration > Policy Configuration	C Mat C Ref C Clas C Clas C Clas C Eth	ch Every erence Class IS Of Service IN emet Type	Any O S (0 Annietali	to 4095)	(600 to ffff b	evi		
 Service Inte Configuration 	erface on C Sou	rce MAC	Address		Mask	50)		
» Service Sta	tistics C Des	tination MAC	Address		Mask			

- e. Under Diffserv Class Configuration, in the VLAN field, enter 5.
- f. Click Apply.
- 4. Create a class class_color.
 - a. Select QoS > DiffServ > Advanced > Class Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSe	arv	111						
Diffserv Wi Auto VoIP	zard Class	s Name					0	
Basic Advanced » DiffServ Configurati	on E d	class Name		Class T	ype			
 Class Configurati IPv6 Class Configurati 	on							
 Policy Configurati Service Int Configurati 	on terface							
» Service Sta	atistics							

- **b.** Enter the following information:
 - In the Class Name field, enter class_color.
 - In the Class Type list, select All.

c. Click Add to create a new class class_color.

System	Switc	hing	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSe	ary .								
Diffserv Wi Auto VoIP	zard	Class Class	Name ss Name					۲	
Advanced > DiffServ		CI	ass Name		Class T	ype			
Configurati	on		ass vlan		All				
 Class Configurati IPv6 Class Configurati 	on		ass color		All				

d. Click class_color to configure this class.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSer	V					N.	11 II.	
 Diffserv Wiz Auto VoIP 	ard Class	Name Type						
> Basic	Di	ffServ Class Co		۲				
 » DiffServ Configuratio » Class Configuratio » IPv6 Class Configuratio » Policy Configuratio » Service Inte Configuratio » Service Stat 	n C Ma C Cla n C VL C Eth n C Sou rface C Pro n C Sou istics C Sou C De C De C De C De	tch Every ference Class ss Df Service AN memet Type urce MAC stination MAC otocol Type urce IP urce L4 Port stination IP stination L4 Port DSCP scedence Value	Any v class_vlar 0 v (0 v Appletalk Address Address ICMP v Address domain afi1 v 7 v (0 t	n 💌	(600 to ffff h Mask Mask 0 to 255) Mask (0 to 65535) Mask (0 to 65535) to 63)	ex)		
	C 1P	ToS	Bit Value		Bit Mask			

- e. Under Diffserv Class Configuration, in the Precedence Value list, select 7.
- f. Click Apply.
- 5. Create a policy policy_vlan.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffS	9FY							
Diffserv Wi	zard Polic	y Configurat	ion					
Auto VoIP	Po	licy Configurat	ion				(2)	
Basic	1	olicy Name	Pol	ісу Туре	Memb	er Class		
» DiffServ		policy_vlan	In					
Configurati	ion							
 Class Configurati 	ion							
» IPv6 Class								
Configurati	ion							
Confidurati	on							
» Service Int	terface							
Configurati	ion							
» Service St	atistics							

- b. In the Policy Name field, enter policy_vlan.
- c. In the Policy Type list, select In.
- d. Click Add.
- 6. Associate policy_vlan with class_vlan.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
CoS DiffSor	N.					й. -		
Diffserv Wiz	ard Polic	y Configura	tion					
Auto VoIP	P	olicy Configura	tion				(?)	
Advanced		Policy Name	Pol	ісу Туре	Membo	er Class		
» DiffServ		policy_vlan	In		class	vlan 💌		
Configuratio	n 🔽	policy vlan	In					
» Class								
Configuratio	'n							
> IPv6 Class	D.							
> Policy								
Configuratio	n.							
» Service Inte	rface							
Configuratio	n							
> Service Stat	tistics							

- **b.** Under Policy Configuration, scroll down and select the **policy_vlan** check box.
- c. In the Member Class field, enter class_vlan.
- d. Click Apply.
- 7. Configure policy_vlan.
 - a. Select QoS > DiffServ > Advanced > Policy Configuration.
 - b. Click policy_vlan.

System Switch	ing Routing	QoS	Security Mon	itoring Mainten	ance He	lp Index	
CoS DiffServ				2			
 Diffserv Wizard Auto VoIP Paste 	Policy Class Con Class Informatio	figuration n					0
 Basic Advanced DiffServ Configuration Class 	Policy Name Policy Type Member Class Name			policy_vlan In class_vlan			
Configuration > IPv6 Class Configuration = Policy Configuration > Service Interface Configuration > Service Statistics	Policy Attribute C As Policy Attribute C As C Dr C Ma C Ma C Ma G Sir	sign Queue op urk IP COS urk IP Precedence urk IP DSCP nple Policy	0 0 af11 Color Conform Class Comitted Rate Comitted Burst Size Conform Action	class_color v 1000 64 © Send © Drop © Mark CoS	Color Mode	Color Aware 💌	0

- c. Select the **Simple Policy** radio button.
- d. In the Color Mode list, select Color Aware.
- e. In the Color Conform Class list, select class_color.
- f. In the Committed Rates field, enter 1000.
- g. In the Committed Burst Size field, enter 64.
- h. For Conform Action, select the Send radio button.
- i. For Violate Action, select the **Drop** radio button.
- j. Click Apply.
- 8. Apply policy_vlan to interface 1/0/13.
 - a. Select QoS > DiffServ > Advanced > Service Interface Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
CoS DiffServ	ĸ									
Diffserv Wiza Auto VoIP	rd Sei	Service Interface Configuration								
Basic	1	All		Go To Interface	- 6	GO				
> DiffServ		Interface	Po	licy Name	Direction	Operational Status				
Configuration		1/0/13	P	olicy_vlan 💌	In					
* Class		1/0/1		-	In					
> IPv6 Class		1/0/2			In					
Configuration		1/0/3			In					
» Policy		1/0/4			In					
Configuration		1/0/5			In					
	tace []	1/0/6			In					
» Service Stati-	stics	1/0/7			In					
		1/0/8			In					
		1/0/9			In					
		1/0/10			In					
		1/0/11			In					
	Г	1/0/12			In		_			
		1/0/13			In					

- **b.** Under Service Interface Configuration, scroll down and select the Interface **1/0/13** check box.
- c. In the Policy Name list, select policy_vlan.
- d. Click Apply to save the settings.

IGMP Snooping and Querier

Internet Group Management Protocol features

10

This chapter includes the following sections:

- Internet Group Management Protocol Concepts
- IGMP Snooping
- Show igmpsnooping
- Show mac-address-table igmpsnooping
- External Multicast Router
- Multicast Router Using VLAN
- IGMP Querier
- Enable IGMP Querier
- Show IGMP Querier Status

Internet Group Management Protocol Concepts

NETGEAR implements Internet Group Management Protocol (IGMP) in the following way:

- IGMP uses version 1, version 2, or version 3.
- IGMP includes snooping.
- You can enable IGMP snooping on a per-VLAN basis.

IGMP Snooping

The following are examples of the commands used in the IGMP snooping feature.

CLI: Enable IGMP Snooping

The following example shows how to enable IGMP snooping.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#set igmp
(Netgear Switch) (Config)# set igmp unknown-multicast filter
(Netgear Switch) (Config)#exit
```

Web Interface: Enable IGMP Snooping

Configure IGMP snooping:

1. Select Switching > Multicast > IGMP Snooping Configuration.

System Sv	vitching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP M	ulticast A	ddress Table 1	Ports LAG					
MEDB		IGMP Sno	oping Co	nfiguration				
IGMP Sneeping		IGMP Sn	ooping Con	figuration				.str
a Interface Config	unation	Admin Mode			C Disable	Enable		
> IGMP VLAN Cont	figuration	Unknown Hul	ticast Filterin	ng .	C Disable	Enable		
Multicest Router	arteste arteste a	Multicast Con	trol Frame C	ount	11			
Configuration	100.000	Interfaces E	nabled for IG	MP Snooping				
 Multicast Router Configuration 	VLAN	Data Frames	Forwarded b	y the CPU	Ø			
> Querier Configu	ration							-
> Querier VLAN		VLAN ID	s Enabled to	or IGMP Shoop	ing			(1992) (1992)
Configuration MLD Snooping								

- 2. For Admin Mode select the Enable radio button.
- 3. For Unknown Multicast Filtering, select the **Enable** radio button.
- 4. Click Apply.

Show igmpsnooping

The example is shown as CLI commands and as a Web interface procedure.

CLI: Show igmpsnooping

(Netgear Switch) #show igmpsnooping	
Admin Mode	Disable
Unknown Multicast Filtering	Disable
Multicast Control Frame Count	0
Interfaces Enabled for IGMP Snooping	None
VLANs enabled for IGMP snooping	None

Web Interface: Show igmpsnooping

Select **Switching > Multicast > IGMP Snooping Configuration**. A screen similar to the following displays.

System Switchi	ng Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP Multicon	Address Table	Ports LAG					
MFDB	IGMP Sno	ooping Co	nfiguration				
· tortP Sneeping	IGMP St	nooping Con	figuration				3
> Interface Configuratio	Admin Hode	N		C Disable	Enable		
IGMP VLAN Configuration	unknown Hu	liticast Filteri	-9	C Disable	🐨 Enable		
Multicast Router	Multicast Co	ntrol Frame C	ount	11			
Configuration	Interfaces (nabled for 10	MP Snooping	0/1			
 Multicast Router VLAN Configuration 	Data Frame	s Forwarded I	by the CPU	0			
Querier Configuration Ouerier VLAN	VLAN ID	s Enabled f	or IGMP Snoop	ing			(1)
Configuration	1			999			
MLD Snooping							

Show mac-address-table igmpsnooping

The example is shown as CLI commands and as a Web interface procedure.

CLI: Show mac-address-table igmpsnooping

(Netgear Switch) #show mac	-address-ta	able igmpsnooping ?						
<cr> Press Enter to execute the command.</cr>								
(Netgear Switch) #show mac	-address-ta	able igmpsnooping						
	Туре	Description	Interfaces					
00:01:01:00:5E:00:01:16	Dynamic	Network Assist	Fwd: 1/0/47					
00:01:01:00:5E:00:01:18	Dynamic	Network Assist	Fwd: 1/0/47					
00:01:01:00:5E:37:96:D0	Dynamic	Network Assist	Fwd: 1/0/47					
00:01:01:00:5E:7F:FF:FA	Dynamic	Network Assist	Fwd: 1/0/47					
00:01:01:00:5E:7F:FF:FE	Dynamic	Network Assist	Fwd: 1/0/47					

Web Interface: Show mac-address-table igmpsnooping

Select Switching > Multicast > IGMP Snooping Table.

System	Switching	Routing Qos	5 Se	curity M	onitoring	Mointenance	Help				
VIAN STP	Multicast A	ddress Table Ports	AG								
NEDA		MFDB Table									
· MEDB Table		MFD8 Table 🛞									
Statistics		Search By MAC Addre			60						
IGMP Snoopin MLD Snooping	3	MAC Address VLAN Componen			Туре	Description	Forwarding Interfaces				
		01:00:5#:01:02:03	999	IGMP	DYNAMIC	Network Assist	0/1				

External Multicast Router

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure the Switch with an External Multicast Router

This example configures the interface as the one the multicast router is attached to. All IGMP packets snooped by the switch is forwarded to the multicast router reachable from this interface.

```
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter interface
```

Web Interface: Configure the Switch with an External Multicast Router

1. Select Switching > Multicast > Multicast Router Configuration.

MFDB	IG	MP Shoop	ing Interfa	ce Configurat	ion					
LEMP Snooping	63	IGMP Snooping Interface Configuration								
 Configuration Interface Configuration 	4	3 All		Go To Interfac	•	00				
IGMP VLAN Configuration Multicast Router Configuration Multicast Router VLAN		Interface	Admin Mode	Group Membership Interval(secs)	Max Response Time(secs)	Present Expiration Time(secs)	Fast Leave Admin Mode			
Configuration		1/0/3	Enable 💌	260	10	0	Disable -			
Querier Configuration	17	1/0/1	Disable	260	10	0	Disable			
Configuration		1/0/2	Disable	260	10	0	Disable			
MLD Snooping	R	1/0/3	Disable	260	10	0	Disable			
		1/0/4	Disable	260	10	0	Disable			
		1/0/5	Disable	260	10	0	Disable			

- Under Multicast Router Configuration, scroll down and select the Interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.
- 3. In the Admin Mode field, select Enable.
- 4. Click Apply.

Multicast Router Using VLAN

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure the Switch with a Multicast Router Using VLAN

This example configures the interface to forward only the snooped IGMP packets that come from VLAN ID (<VLAN Id>) to the multicast router attached to this interface.

```
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter 2
```

Web Interface: Configure the Switch with a Multicast Router Using VLAN

1. Select Switching > Multicast > Multicast Router VLAN Configuration.

System Switching	Routing	QoS Security	Monitoring	Maintenance	Help Index					
VLAN STP Multicost	Address Toble Port	LAG								
MFDB	Multicast Ro	Multicast Router VLAN Configuration								
Title Support	Multicast Router VLAN Configuration									
> Configuration > Interface Configuration	Interface		1/0/3 .							
IGMP VLAN Configuration Multicast Router	Multicast Router VLAN Configuration									
Configuration	VLAN ID Multicast Router									
Canfidur share	Enable -									
> Querier Configuration										
> Querier VLAN										
Configuration										
MLD Snooping										

- 2. Under Multicast Router VLAN Configuration, scroll down and select the Interface 1/0/3 check box.
- 3. Enter the following information in the Multicast Router VLAN Configuration.
 - In the VLAN ID field, enter 2.
 - In the Multicast Router field, select Enable.
- 4. Click Apply.

IGMP Querier

When the switch is used in network applications where video services such as IPTV, video streaming, and gaming are deployed, the video traffic is normally flooded to all connected ports because such traffic packets usually have multicast Ethernet addresses. IGMP snooping can be enabled to create a multicast group to direct that traffic only to those users that require it.

However, the IGMP snooping operation usually requires an extra network device—usually a router—that can generate an IGMP membership query and solicit interested nodes to respond. With the built-in IGMP querier feature inside the switch, such an external device is no longer needed.





Since the IGMP querier is designed to work with IGMP snooping, it is necessary to enable IGMP snooping when using it. The following figure shows a network application for video streaming service using the IGMP querier feature.

Enable IGMP Querier

The example is shown as CLI commands and as a Web interface procedure.

CLI: Enable IGMP Querier

Use the following CLI commands to set up the switch to generate an IGMP querier packet for a designated VLAN. The IGMP packet will be transmitted to every port on the VLAN. The following example enables the querier for VLAN 1 and uses 10.10.10.1 as the source IP address in querier packets. See the *Command Line Reference* for more details about other IGMP querier command options.

```
(Netgear switch) #vlan database
(Netgear switch) (vlan)#set igmp 1
(Netgear switch) (vlan)#set igmp querier 1
(Netgear switch) (vlan)#exit
(Netgear switch) #config
(Netgear switch) (config)#set igmp querier
(Netgear switch) (config)#set igmp querier address 10.10.10.1
(Netgear switch) (config)#exit
```

Web Interface: Enable IGMP Querier

1. Select Switching > Multicast > IGMP VLAN Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
VLAN STP	Multicast	Address Table F	Ports LAG			lu.	
MFDB	IGM	IP Snooping (Configura	ition			
 IGMP Snoop 	ping E I	GMP Snooping (Configuratio	on			(1)
 Contigurat Totorface 	Adn	nin Mode			C Disable 💽 Enab	le	
Configurati	ion Unk	nown Multicast Filt	tering		O Disable C Enable	ole	
* IGMP VLAN	V Mult	icast Control Fram	e Count		0		
Configurati	ion Inte	rfaces Enabled for	r IGMP Snoop	ping			
» Multicast R Configuration	outer Dat	a Frames Forward	ed by the CP	U	0		
» Multicast R VLAN	outer	LAN IDs Enable	d for IGMP	Snooping			0
Configurati	ion						

- 2. Enable IGMP snooping on VLAN 1.
 - a. Select Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration.

System	Switching	Routi	ing Q	oS Sec	urity Moni	toring Maint	enance Help			
VLAN STP	Multicast	Address Tob	ole Ports	LAG						
MFDB	IGM	IP VLAN	Configur	ation						
* IGMP Snoopi	ng 🗍 🗄 I	IGMP VLAN Configuration								
Configuration Interface Configuration IGMP VLAN	1	VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time			
 Configuration Multicast Rou Configuration 	uter	1	Enable							

- **b.** Enter the following information:
 - In the VLAN ID field, enter 1.
 - In the Admin Mode field, select Enable.
- c. Click Add.
- 3. Enable the IGMP snooping querier globally.
 - a. Select Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help		
VLAN STP	Multicost	Address Table F	Ports LAG	8 8	44.5. 	A1			
> MFDB	IG	MP Snooping	Querier (Configuratio	n				
* IGMP Snoop	ing (E)	IGMP Snooping Querier Configuration							
 Configuration Interface 	on Qu	ierier Admin Mode			C Disable 🖲 Enal	ble			
Configuratio	on Qu	erier IP Address			10.10.10.1				
> IGMP VLAN	16	MP Version			2				
Configuratio	on Qu	ery Interval(secs)			60	(1 to 1800)			
> Multicast Ro	outer Qu	ierier Expiry Interva	al(secs)		60	(60 to 300)			
> Multicast Ro VLAN Configuratio	on outer	VLAN Ids Enabled for IGMP Snooping Querier							
 Querier Configuration 	an.								

- **b.** Enter the following information:
 - For Querier Admin Mode, select the **Enable** radio button.
 - In the Querier IP Address field, enter 10.10.10.1.
- c. Click Apply.
- 4. Enable the IGMP snooping querier on VLAN 1.
 - a. Select Switching > Multicast > IGMP Snooping Querier VLAN Configuration.

System	Switching	Rout	ing Go5	5 Security	Monitori	ng Main	tenance	Help	Todex
VLAN STP	Malticont	Address Tob	de Ports L	AG					
MEDB	IG	MP Snoo	ping Querie	r VLAN Conf	iguration				
These Balancests	1 12	IGMP Snoo	ping Querier	VLAN Configure	tion				
 Configuration Interface Configuration IGMP VLAN 		VLAN ID	Querier Election Participate Mode	Querier VLAN Address	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Nax Response Time
Configuration • Multicast Rout Configuration • Multicast Rout VLAN Configuration • Querier Configuration	er 🔳	1	2						

- b. In the VLAN ID field, enter 1.
- 5. Click Add.

Show IGMP Querier Status

The example is shown as CLI commands and as a Web interface procedure.

CLI: Show IGMP Querier Status

To see the IGMP querier status, use the following command.

```
(Netgear Switch) #show igmpsnooping querier vlan 1
VLAN 1 : IGMP Snooping querier status
------
IGMP Snooping Querier VLAN Mode..... Enable
Querier Election Participate Mode..... Disable
Querier VLAN Address..... 0.0.0.0
Operational State.... Disabled
Operational version..... 2
```

The command shows that the IGMP admin mode is Active. The mode is controlled by the **set igmp** command. If the mode is inactive, no query packet is sent.

Web Interface: Show IGMP Querier Status

1. Select Switching > Multicast > IGMP Snooping Configuration.

System Sv	vitching	Routing QoS	Security Monitoring	Maintenance	Help	Index	lippoir
YIAN STP M	ulticast. /	Addrese Table Ports LACI					
ICHI Incoming	IGM	P Snooping Configural	ion				
IGMP Snooping	10	MP Snooping Configuration	i -		0		
Interface Configuration	Admi	in Made	Obsat	ie 💿 Enable			
IGHP Snooping	Unkn	own Multicast Filtering	🛞 Disab	ie O Enable			
MFD8 Table	Quer	ier IP Address	10.10.10	.1			
GMRP Table	Multi	cast Control Frame Count	0				
MFD8 Statistics	Inter	faces Enabled for IGHP Snoopi	ng (176/10)				
Configuration	Data	Frames Forwarded by the CPU	·				
Multicast Router	1				_		
Configuration Hulticast Router	V	LAN Ids Enabled for IGMP 5	mooping		140		
VLAN		- N.					
Configuration							
	V	LAN Ids Enabled for IGMP 5	incoping Querier		0		
						tioning and	T. There
						STREEP CANE	AL APPLY

2. Click Refresh.

MVR

Multicast VLAN Registration

11

This chapter includes the following sections:

- MVR Concepts
- Configure MVR in Compatible Mode
- Configure MVR in Dynamic Mode

MVR Concepts

The IGMP Layer 3 protocol is widely used for IPv4 network multicasting. In Layer 2 networks, the IGMP protocol uses resources inefficiently. For example, a Layer 2 switch multicast traffic to all ports even if there are receivers connected to only a few ports.

To address this problem, the IGMP Snooping protocol was developed. But the problem reappears when receivers are in different VLANs. Multicast VLAN registration (MVR) is intended to solve the problem of receivers in different VLANs. It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.

MVR, like the IGMP Snooping protocol, allows a Layer 2 switch to snoop on the IGMP control protocol. Both protocols operate independently of each other. Both protocols can be enabled on the switch interfaces at the same time. In such a case, MVR listens to the join and report messages only for groups configured statically. All other groups are managed by IGMP snooping.

There are two types of MVR ports: source and receiver.

- The source port is the port to which the multicast traffic flows using the multicast VLAN.
- The receiver port is the port where a listening host is connected to the switch. It can utilize any (or no) VLAN, except the multicast VLAN. This implies that the MVR switch performs VLAN tag substitution from the multicast VLAN source port to the VLAN tag used by the receiver port.

The Multicast VLAN is the VLAN that is configured in the specific network for MVR purposes. It has to be manually specified by the operator for all source ports in the network. It is a VLAN that is used to transfer multicast traffic over the network to avoid duplication of multicast streams for clients in different VLANs. A diagram of a network configured for MVR is shown in the following illustration. SP is the source port and RP is the receiver port.



Figure 20. Network configured for MVR

Note: The following examples show how to configure the MVR on the MVR switch (GSM7212P in this case).

Configure MVR in Compatible Mode

In compatible mode, the MVR switch does not learn multicast groups; the groups have to be configured by the operator as the MVR does not forward IGMP reports from the hosts (RP port) to the IGMP router (SP port). To operate in this mode, the IGMP router has to be statically configured to transmit all required multicast streams to the MVR switch.

CLI: Configure MVR in Compatible Mode

1. Create mVlan, VLAN1, VLAN2, and VLAN3.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
(Netgear Switch) (Vlan)#vlan name 999 mVlan
(Netgear Switch) (Vlan)#vlan name 1001 Vlan1
(Netgear Switch) (Vlan)#vlan name 1002 Vlan2
(Netgear Switch) (Vlan)#vlan name 1003 Vlan3
(Netgear Switch) (Vlan)#exit
```

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#mvr
(Netgear Switch) (Config)#mvr vlan 999
(Netgear Switch) (Config)#mvr group 224.1.2.3
```

3. Configure multicast VLAN on the source port.

```
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#vlan participation include 999
(Netgear Switch) (Interface 0/9)#vlan tagging 999
(Netgear Switch) (Interface 0/9)#mvr
(Netgear Switch) (Interface 0/9)#mvr type source
(Netgear Switch) (Interface 0/9)#exit
```

4. Configure the receive ports.

Note: The receive port can participate in only one VLAN.

```
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 1001
(Netgear Switch) (Interface 0/1) #vlan pvid 1001
(Netgear Switch) (Interface 0/1) #vlan participation exclude 1
(Netgear Switch) (Interface 0/1)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/1)#exit
(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5)#vlan pvid 1002
(Netgear Switch) (Interface 0/5) #vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr stype receiver
(Netgear Switch) (Interface 0/5)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/5)#exit
(Netgear Switch) (Config)#interface 0/7
(Netgear Switch) (Interface 0/7)#vlan participation include1003
(Netgear Switch) (Interface 0/7)#vlan pvid 1003
(Netgear Switch) (Interface 0/7) #vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/7)#exit
```

5. Show mvr status.

```
(Netgear Switch) #show mvr
MVR Running..... TRUE
MVR multicast VLAN..... 999
MVR Max Multicast Groups..... 256
MVR Current multicast groups..... 1
MVR Global query response time.... 5 (tenths of sec)
MVR Mode..... compatible
(Netgear Switch) #show mvr interface
Port
          Type
                     Status
                                         Immediate Leave
                               _____
_____
           _____
_____
0/1
        RECEIVER
                       ACTIVE/InVLAN
                                        DISABLED
0/5
        RECEIVER
                       ACTIVE/InVLAN
                                        DISABLED
0/7
        RECEIVER
                       ACTIVE/InVLAN
                                         DISABLED
0/9
        SOURCE
                       ACTIVE/InVLAN
                                        DISABLED
```

Web Interface: Configure MVR in Compatible Mode

- 1. Create MVLAN 999, VLAN1 1001, VLAN2 1002 and VLAN3 1003.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays:

System Switch	ing Routing	QoS Security	Manitoring	Maintenance	Help Index			
MAN STP Multicon	A MVE Address	Table Ports LAG						
CANE.	VLAN Config	puration						
Conference and	Reset	Reset						
Advanced	Reset Configure	Reset Configuration						
	VLAN Confi	guration						
	VLAN ID	VLAN Name	YLAN TYPE	Make Sta	tic			
	999	miVian		Disable				
	F 1	default	Default	Disable				

- b. In the VLAN ID field, enter 999, and in the VLAN Name field, enter mVlan.
- c. Click Add.
- d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.
- 2. Add port 9 into MVLAN 999 with tagged mode.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

System Switching	Routing	QoS Security	Monitoria	ng Maintenance	Help Inde
VLAN STP Multicost	MVR Address	Table Ports LAG			
Basic Advanced	VLAN Memb	ership			
VLAN Configuration	VLAN Memb	ership			
A PLACE PLANNING	VLAN TO	999 💌		Group Operation U	intag All 📃
* VLAN Status	VLAN Nome	mVian		UNTAGGED FORT MEMAL	11.
= Port PVID Configuration	VLAN Type	Static		I TADGED POST MEMBER	15
· Protocol Based VLAN	· DOM: 1	- 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10			
Group Configuration	Port 1 2	3 4 5	6 7 8	9 10 11 12	
+ Protocol Based VLAN	and the second second				
Group Membership = IP Subpet Based VLAN	* TEAG				

- b. In the VLAN ID list, select 999.
- c. Click Unit 1. The ports display.
- **d.** Click the gray box under port 9 until T displays. The T specifies that the egress packet is tagged for the ports.
- e. Click Apply to save the settings.
- f. Repeat steps from b to e, add port 0/1 to VLAN1 1001, add port 0/5 to VLAN2 1002, and add port 0/7 to VLAN3 1003.
- 3. Enable MVR and multicast VLAN.

a. Select Switching > MVR > Basic > MVR Configuration. A screen similar to the following displays:

System Switching	Routing QoS Security	Manitoring Maintenance P	ielp Index	
Baser a Wel Carlanaum	MVR Configuration			
MVR Group Comparation MVR Interface Configuration	HVR Running HVR Hullscast Vian	Enable 💌 999 (2 to 4094)		
Advanced	HVR. Hax Hulticast Groups HVR. Corrent Hulticast Groups	256 0		
	NVR Global query response time NVR Node	5 (1 to 100)		

- b. For MVR Running, select Enable.
- c. In the MVR Multicast VLAN field, enter 999.
- d. Click Apply.
- 4. Add multicast group 224.1.2.3 to MVR.
 - a. Select Switching > MVR > Basic > MVR Group Configuration. A screen similar to the following displays:

System	Switching	Routi	ng QoS	5	ecurity	Manitoring	Mainh	nonce	Help	Index
VLAN STP	Multicost	MVE	Address Table	Porte	MG					
Multi Confu	nuration	MVR	Group Confi	igurati	ion					
		MVR Group Configuration								
+ HVR Interf	ace	HVR Group 1P					Status	Members		
Configuration	ion .		24.1.2.3					=		
Advanced										

- b. In the MVR Group IP field, enter 224.1.2.3.
- c. Click Add.
- 5. Configure a receiver on interface 0/1, 0/5, and 0/7.
 - a. Select Switching > MVR > Basic > MVR Interface Configuration. A screen similar to the following displays:

System Switching VLAN STP Multicent	Routing MVE Addr	QoS Security	Monitoring	Maintenance	Help Index
HVR Configuration HVR Configuration	MVR Inte	rface Configuration			1
a Helt Lanathian	I All	Go To Ini	terface		
Sector and the sector of the s	Interfa	ace Admin Mode	Туре	Immediate Leave	Status
Advances		Enable -	receiver +		
	P 0/1	Disable	none	Disable	ACTIVE/InVLAN
	F 0/2	Disable	none	Disable	INACTIVE/InVLAN
	E 0/3	Disable	none	Disable	INACTIVE/InVLAN
	F 0,4	Disable	none	Disable	INACTIVE/InVLAN
	🔛 0/5	Disable	none	Disable	ACTIVE/INVLAN
	F 0/6	Disable	none	Disable	INACTIVE/InVLAN
	R 0/7	Disable	none	Disable	ACTIVE/INVLAN
	F 0/0	Disable	none	Disable	INACTIVE/InVLAN
	F 0/9	Disable	0004	Disable	ACTIVE/InVLAN
	F 0/10	Disable	none	Disable	INACTIVE/INVLAN
	F 0/11	Disable	none	Disable	INACTIVE/InVLAN
	F 0/12	Disable	hone	Disable	ACTIVE/INVLAN
	I All	Ge To Int	leeface	00	

- b. Under MVR Interface Configuration, scroll down and select the Interface 0/1, 0/5 and 0/7 check boxes.
- c. Enter the following information:
 - In the Admin Mode list, select **Enable**.
 - In the Type list, select **Receiver**.
- d. Click Apply to save the settings.
- 6. Configure source interface.
 - a. Select Switching > MVR > Basic > MVR Interface Configuration. A screen similar to the following displays:

System Switching	Routing	QoS Security	Manitoring	Maintenance	Help Index
MVR Configuration MVR Configuration	MVR Inte	rface Configuration			0
A Hys brieflage	I All	Go To I	interface	00	
Contract of the second	Interf	ace Admin No	de Type	Immediate Leave	Status
Advanced	0/9	Enable :	source .	Disable .	ACTIVE/INVLAN
	□ 0/1	Enable	receiver	Disable	ACTIVE/InVLAN
	F 0/2	Disable	none	Disable	INACTIVE/INVLAN
	E 0/3	Disable	none	Disable	INACTIVE/INVLAN
	F 0/4	Disable	hone	Disable	INACTIVE/INVLAN
	F 0/5	Enable	receiver	Disable	ACTIVE/InVLAN
	F 0/6	Disable	none	Disable	INACTIVE/INVLAN
	E 0/7	Enable	receiver	Disable	ACTIVE/InVLAN
	F 0/0	Disable	none	Disable	INACTIVE/INVLAN
	P 0/9	Disable	nome	Disable	ACTIVE/INVLAN
	F 0/10	Disable	none	Disable	INACTIVE/INVLAN
	F 0/11	Disable	none	Disable	INACTIVE/InVLAN
	F 0/12	Disable	hone	Disable	ACTIVE/InVLAN
	II.A.I	Go To I	Interface	00	

- **b.** Under MVR Interface Configuration, scroll down and select the Interface **0/9** check box.
- c. Enter the following information:
 - In the Admin Mode list, select **Enable**.
 - In the Type list, select **source**.
- d. Click Apply to save the settings.
- 7. Configure MVR Group Membership.
 - a. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays:

System	Switching	Rout	ing	Q	oS	S	scurity	6	Mor	itorin	9	Ma	intenan	ce	Help	Inde
VLAN STP	Multicost	MYR	Addr	ess Tab	le	Ports	LAG									
Basic		MVR	Grou	p Me	mb	ershi	p									
Advanced MVR Group:		MVR Group Membership								Ð						
Hunbership	÷ .	Group	IP.			224.1	2.3 *									
* MVR Statisti	25	- 1	mit 1													
		Port	1	2	3	- 4	5	6	7	8	9	10	11	12		
			17.00				1.225		1200		- C.F					

- b. In the Group IP list, select 224.1.2.3.
- c. Click Unit 1. The ports display.

- **d.** Click the gray boxes under ports **1**, **5**, and **7**. (Port 9 is already in MVR group 224.1.2.3 because it is configured as the source port.)
- e. Click Apply to save the settings.

Configure MVR in Dynamic Mode

CLI: Configure MVR in Dynamic Mode

In dynamic mode, the MVR switch learns existing multicast groups by snooping the IGMP queries from router on source ports and forwarding the IGMP reports from the hosts to the IGMP router on the Multicast VLAN (with appropriate translation of the VLAN ID).

1. Create MVLAN, VLAN1, VLAN2, and VLAN3.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
(Netgear Switch) (Vlan)#vlan name 999 mVlan
(Netgear Switch) (Vlan)#vlan name 1001 Vlan1
(Netgear Switch) (Vlan)#vlan name 1002 Vlan2
(Netgear Switch) (Vlan)#vlan name 1003 Vlan3
(Netgear Switch) (Vlan)#exit
```

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#mvr
(Netgear Switch) (Config)#mvr vlan 999
(Netgear Switch) (Config)#mvr group 224.1.2.3
```

3. Configure MVR in dynamic mode.

(Netgear Switch) (Config) #mvr mode dynamic

4. Configure multicast VLAN on the source port.

```
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#vlan participation include 999
(Netgear Switch) (Interface 0/9)#vlan tagging 999
(Netgear Switch) (Interface 0/9)#mvr
(Netgear Switch) (Interface 0/9)#mvr type source
(Netgear Switch) (Interface 0/9)#exit
```

5. Configure the receive ports.

Note: A receive port can participate in only one VLAN.

```
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 1001
(Netgear Switch) (Interface 0/1)#vlan pvid 1001
(Netgear Switch) (Interface 0/1) #vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#exit
(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5)#vlan pvid 1002
(Netgear Switch) (Interface 0/5) #vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr stype receiver
(Netgear Switch) (Interface 0/5)#exit
(Netgear Switch) (Config)#interface 0/7
(Netgear Switch) (Interface 0/7)#vlan participation include1003
(Netgear Switch) (Interface 0/7) #vlan pvid 1003
(Netgear Switch) (Interface 0/7)#vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#exit
```

6. Show the MVR status.

```
(Netgear Switch) #show mvr
MVR Running..... TRUE
MVR Max Multicast Groups..... 256
MVR Current multicast groups..... 1
MVR Global query response time.... 5 (tenths of sec)
MVR Mode..... compatible
(Netgear Switch) #show mvr interface
                  Status
         Туре
Port
                                       Immediate Leave
_____
           _____
                             _____
_____
        RECEIVER
                     ACTIVE/InVLAN
0/1
                                      DISABLED
0/5
       RECEIVER
                     ACTIVE/InVLAN
                                      DISABLED
0/7
        RECEIVER
                     ACTIVE/InVLAN
                                      DISABLED
0/9
       SOURCE
                     ACTIVE/InVLAN
                                      DISABLED
```

```
206
```

7. After port 0/1 receive IGMP report for Multicast Group 224.1.2.3, it will be added to the MVR Group 224.1.2.3.

(Netgear Switch) #s	show mvr members	
MVR Group IP	Status	Members
224.1.2.3	ACTIVE	0/1(d)

Web Interface: Configure MVR in Dynamic Mode

- 1. Create MVLAN 999, VLAN1 1001, VLAN2 1002, and VLAN3 1003.
 - a. Select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays:

System Switching	Routing	QoS Security	Manitoring	Maintenance Hel	p Index
Education in the local division of the	VLAN Confi	guration			
	Reset				-00-
Advanced	Reset Configur	ation	E		
	VLAN Conf	iguration			
	VLAN ID	VLAN Name	YLAN Type	Make Static	
	999	million		Disable -	
	F 1	default	Default	Disable	-

- b. In the VLAN ID field, enter 999, and in the VLAN Name field, enter mVlan.
- c. Click Add.
- d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.
- e. Add port 9 into MVLAN 999 with tagged mode.
- f. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays:

System Switching	Routing	QoS	Security	Ma	nitoring	Maint	snance	Help	Inde
IAN STP Multicent	MVR Address	Table Pr	m LAG)					
Basic Advanced	VLAN Memb	ership							
VLAN Configuration	VLAN Mem	pership	_		_				100
	VLAN ID	999 -	k		64	rup Operatio	in Unta	ig All 💽	
VLAN Status	VLAN Name	million				NTAGGED PD	T MEMALET		
Port PVID Configuration	VLAN Type	Static				TADGED NOT	MEMBERS		
Protocol Based VLAN	· DINK &								
Group Configuration	Port 1	2 3	4 5	6 7	8 9	10 1	1 12		
Fratocol Based VLAN	100000000000000				10000	and is the	12.45		
Group Membership	* LAG								

- g. In the VLAN ID list, select 999.
- h. Click Unit 1. The ports display.
- i. Click the gray boxes under port **9** until T displays. The T specifies that the egress packet is tagged for the ports.
- j. Click Apply to save the settings.

- **k.** Repeat steps from b to e, add port 0/1 to VLAN1 1001, add port 0/5 to VLAN2 1002, and add port 0/7 to VLAN3 1003.
- 2. Enable MVR and multicast VLAN.
 - a. Select Switching > MVR > Basic > MVR Configuration. A screen similar to the following displays:

System Switching	Routing QoS Security	Monitoring Maintenance	Help Index
daan - Nak Contaction	MVR Configuration		-
MVR Group Configuration MVR Interface	HYR Running	Enable 💌	
Configuration	NVR Hulbcast Vian	999 (1 to 4073)	
Advanced	HVR Hax Hulticast Groups	256	
	HVR Current Hubbcast Groups	1	
	MYR Global quary response time	5 (1.to 107)	
	NVR Node	dynamic -	

- **b.** From the MVR Running list, select **Enable**.
- c. In the MVR Multicast Vlan field, enter 999.
- d. From the MVR mode list, select dynamic.
- e. Click Apply.
- 3. Add multicast group 224.1.2.3 to the MVR.
 - a. Select Switching > MVR > Basic > MVR Group Configuration. A screen similar to the following displays:

System	Switching	Rout	ing G	105	Security	Manitoring	Mainte	nonce	Help	Index
VLAN STP	Multicost	MVE	Address Tob	de Porte	I LAG					
+ MVR Config	uration	MVR	Group Co	enfigura Infigurati	tion m					0
+ HVR Interfa	108	2	WR Group 1	P .		1	status	Nemi	ierii —	
Configuration Advanced	1		224 1 2 3							

- **b.** In the MVR Group IP field, enter **224.1.2.3**.
- c. Click Add.
- 4. Configure a receiver on interface 0/1, 0/5 and 0/7.

a. Select Switching > MVR > Basic > MVR Interface Configuration. A screen similar to the following displays:

System	Switching	Re	outing	QoS	Security	Monitoring	Maintenance	Help Inde
VLAN STP	Multicent	MVE	Adda	nn Toble	Ports LAG			
• HVR Config	uration Configuration	MV	R Inter	face Co	onfiguration			4
a Hot, Laborer	1.1	1	All		Go To Intr	erface	00	
Advanced			Interfa	ce	Admin Mode	Туре	Immediate Leave	Status
HUVHOLEN					Enable -	receiver		
		12	0/1		Disable	000e	Disable	ACTIVE/INVLAN
		r	0/2		Disable	none	Disable	INACTIVE/InVLAN
		1	0/3		Disable	none	Disable	INACTIVE/InVLAN
		1	0,44		Disable	none	Disable	INACTIVE/InVLAN
		1	0/5		Disable	none	Disable	ACTIVE/INVLAN
		Γ.	0/6		Disable	none	Disable	INACTIVE/InVLAN
		12	0/7		Disable	none	Disable	ACTIVE/INVLAN
		-	9/0		Disable	none	Disable	INACTIVE/InVLAN
		17	0/19		Disable	0004	Disable	ACTIVE/InVLAN
		1	0/10		Disable	none	Disable	INACTIVE/INVLAN
			0/11		Disable	none.	Disable	INACTIVE/InVLAN
		1	10/12		Disable	none	Disable	ACTIVE/INVLAN
		10	All		Ge To Inte	orface .	00	

- Under MVR Interface Configuration, scroll down and select the Interface 0/1, 0/5 and 0/7 check boxes
- c. Enter the following information:
 - In the Admin Mode list, select **Enable**.
 - In the Type list, select Receiver.
- d. Click Apply to save the settings.
- 5. Configure a source interface.
 - a. Select Switching > MVR > Basic > MVR Interface Configuration. A screen similar to the following displays:

System	Switching	Ro	gnitud	QoS	Security	Maniloring	Maintenance	Help Ind
YLAN STP	Multicent	MYR	Adde	ess Table	Ports LAG			
- HVR Config	uration Configuration	MV	R Inte	rface Co	onfiguration nfiguration			- 0
A HUR DISATI	1.1	1	A11		Go To Inb	erface	00	
Advanced			Interfa	ce	Admin Node	Туре	Immediate Leave	Status
NUVINCEU			0/9		Enable 💌	source .	Disable .	ACTIVE/INVLAN
		17	0/1		Enable	receiver	Disable	ACTIVE/InVLAN
		1	0/2		Disable	none	Disable	INACTIVE/InVLA
		[1]	0/3		Disable	none	Disable	INACTIVE/INVLAN
			0/4		Disable	hone	Disable	INACTIVE/INVLAT
		17	0/5		Enable	receiver	Disable	ACTIVE/InVLAN
			9/6		Disable	none	Disable	INACTIVE/INVLAN
		17	0/7		Enable	receiver	Disable	ACTIVE/InVLAN
		F	0/6		Disable	none	Disable	INACTIVE/INVLAT
		P	0/9		Overable	none	Disable	ACTIVE/INVLAN
		5	0/10		Disable	none	Disable	DIACTIVE/INVLAT
		Γ.	0/11		Disable	none	Disable	INACTIVE/INVLAN
		1	0/12		Disable	hone	Disable	ACTIVE/InVLAN
			All		Go To Inte	orface	1.90	

b. Under MVR Interface Configuration, scroll down and select the Interface **0/9** check box.

- **c.** Enter the following information:
 - In the Admin Mode list, select **Enable**.
 - In the Type list, select **source**.
- d. Click Apply to save the settings.
- 6. After port 1 receives an IGMP report for multicast group 224.1.2.3, it is added into MVR group 224.1.2.3.
 - a. Select Switching > MVR > Advanced > MVR Group Membership. A screen similar to the following displays:

System	Switching	Rout	ing	QoS	5	ecurit	Y.	Mor	itorin		Mai	inteno	ince	Help	Inde
YLAN STP	Multicost	MYR	Address	Table	Porte	LAG									
Basic Advanced		MVR	Group	Mem	bershi	P									_
	3	MV	R Group	Memb	ership		_								
+ MVR Statistic	s .	- 0	hait 1			1.52	-								_
		Port	1	2 3		5	6	7	8	9	10	11	12		

Security Management

Port security features

This chapter includes the following sections:

- Port Security
- Set the Dynamic and Static Limit on Port 1/0/1
- Convert the Dynamic Address Learned from 1/0/1 to a Static Address

12

- Create a Static Address
- Protected Ports
- 802.1x Port Security
- Create a Guest VLAN
- Assign VLANs Using RADIUS
- Dynamic ARP Inspection
- Static Mapping
- DHCP Snooping
- Enter Static Binding into the Binding Database
- Maximum Rate of DHCP Messages
- IP Source Guard

211

Port Security

Port Security helps secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits:

- You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.
- You can enable port security on a per port basis.

Port security implements two traffic filtering methods, dynamic locking and static locking. These methods can be used concurrently.

• **Dynamic locking**. You can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is given in the software Release Notes. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC addresses are forwarded.

Note: If you want to set a specific MAC address for a port, set the dynamic entries to 0, then allow only packets with a MAC address matching the MAC address in the static list.

Dynamically locked addresses can be converted to statically locked addresses. Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. You can set the time out value. Dynamically locked MAC addresses are eligible to be learned by another port. Static MAC addresses are not eligible for aging.

• **Static locking**. You can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

Set the Dynamic and Static Limit on Port 1/0/1

The example is shown as CLI commands and as a Web interface procedure.

CLI: Set the Dynamic and Static Limit on Port 1/0/1

(Netgear Switch)	(Config)#po	rt-security		
Enable port-secu	urity globall	У		
(Netgear Switch)	(Config)#in	terface 1/0/1		
(Netgear Switch)	(Interface	1/0/1)#port-secur	ity	
Enable port-secu	arity on port	1/0/1		
(Netgear Switch)	(Interface	1/0/1)#port-secur	ity max-dynamic 1	0
Set the dynamic	limit to 10			
(Netgear Switch)	(Interface	1/0/1)#port-secur	ity max-static 3	
Set the static l	imit to 3			
(Netgear Switch)	(Interface	1/0/1)#ex		
(Netgear Switch)	(Config)#ex			
(Netgear Switch)	#show port-	security 1/0/1		
Adn	nin	Dynamic	Static	Violation
Intf Mod	le	Limit	Limit	Trap Mode
1/0/1 Disa	abled	10	3	Disabled

Web Interface: Set the Dynamic and Static Limit on Port 1/0/1

1. Select Security > Traffic Control > Port Security >Port Administrator.

System Swi	tching Ro	outing QoS	Security	Monitoring	Maintenance	Help	Index
Monogement Security	Access Po	rt Authentication Tra	file Control ACL				
MAC Filter	Port Secu	rity Configurati	on				
- Port Sectority	Port Sec	urity Settings			0		
Adminutration	Part Securit	y Mode C (Disable 🕅 Enable				
Configuration	Port Sec	urity Violations			(1)		
 Dynamic MAC Address Static MAC Address 	Port	Lest Violation	HAC	VLAN ID			
Protected Port							

- **b.** Under Port Security Configuration, next to Port Security Mode, select the **Enable** radio button.
- c. Click Apply to save the settings.
- 2. Set the dynamic and static limit on the port 1/0/1:
 - a. Select Security > Traffic Control > Port Security > Interface Configuration.

System Swi	tching	Ro	uting QoS	Security	Monitoring	Maintenance Help	Index			
Management Security	I Acce	ss Por	Authentication	Traffic Control A	ci.					
MAC Filter	Port Security Interface Configuration									
Storm Control	Interface Configuration (9)									
Port	1 AI			Go To Interface						
Bidenieux Configue anno Dynamic MAC Address Static MAC Address Protected Part		Port	Port Security	Max Allowed Dynamically	Max Allowed Statically Locked NAC	Enable Violation Traps				
		1/0/1	Enable 💌	10	3	No 💌				
	P	1/0/1	Disable	600	48	He .				
	1	1/0/2	Dirable	600	40	No				
	E .	1/0/3	Disable	600	45	Ne				

- b. Scroll down and select the Interface 1/0/1 check box.
 Now 1/0/1 appears in the Interface field at the top.
- c. Enter the following information:
 - In the Port Security field, select Enable.
 - In the Max Allowed Dynamically Learned MAC field, enter 10.
 - In the Max Allowed Statically Locked MAC field, enter 3.
- d. Click Apply to save the settings.

Convert the Dynamic Address Learned from 1/0/1 to a Static Address

The example is shown as CLI commands and as a Web interface procedure.

CLI: Convert the Dynamic Address Learned from 1/0/1 to the Static Address

Web Interface: Convert the Dynamic Address Learned from 1/0/1 to the Static Address

1. Select Security > Traffic Control > Port Security > Dynamic MAC Address.

A screen similar to the following displays.

System 5	witching 1	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Monogement Securi	ity Access P	Port Authentic	ation Tra	ffic Control AC				
MAC Filter	Dynamie	MAC Ad	dress T	able				
Storm Control	Port S	ecurity Set	(1)					
Port Administration Interface	Conver Numbe	rt Dynamic A ar of Dynami	ddress to 5 c MAC Addr	itatic resses Learned:	5			
Configuration	Dynam	ic MAC Ad	iress Tabl	G 1				
· Dynamic HAC	Port List		1/	0/1				
> Static MAC	VLAN ID		MA	C Address				
Address	1		00:	0e:45:30:15:f3				
Protected Port	1		:00	13146:ec:2f:62				
	1		80	19:5b:e9:51:20				
	1		00	19:5b:e9:51:45				
	1		00:	1b:2fib3:15:89				

- 2. Under Port Security Configuration, in the Port List field, select 1/0/1.
- 3. Select the Convert Dynamic Address to Static check box.
- 4. Click **Apply** to save the settings.

Create a Static Address

The example is shown as CLI commands and as a Web interface procedure.

CLI: Create a Static Address

(Netgear Switch) (Interface 1/0/1) #port-security mac-address 00:13:00:01:02:03

Web Interface: Create a Static Address

1. Select Security > Traffic Control > Port Security > Static MAC address.

A screen similar to the following displays.

System 5	Switching	Routing	Qo5	Security	Monitoring	Maintenance	Help	Index
Monogement Secu	rity Access	Port Authentic	ation Traf	le Control AC	i			
MAC Filter	Static	MAC Addro	ess Confi	iguration				
Part Security	Port	List				TD-		
* Port	Interfac	e 1/0/1	-					
Administration								
Configuration	Stati	Static MAC Address						
Dynamic MAC	St	Static MAC Address			Vian ID			
Address Mac		00:13:00:01:02:03			3 💌			
Address	F 00	00:0E:45:30:15:F3						
Protected Port	F 00	00113146:EC12F162			1			
	E 00	D 00:14:6C:E0:01:20						

- 2. Under Port List, in the Interface list, select 1/0/1.
- 3. In the Static MAC Address section of the screen, enter the following information:
 - In the Static MAC Address field, enter 00:13:00:01:02:03.
 - In the Vlan ID list, select 3.
- 4. Click Add.

Protected Ports

This section describes how to set up protected ports on the switch. Some situations might require that traffic is prevented from being forwarded between any ports at Layer 2 so that one user cannot see the traffic of another user on the same switch. Protected ports can:

- Prevent traffic from being forwarded between protected ports.
- Allow traffic to be forwarded between a protected port and a non-protected port.

In following example, PC 1 and PC 2 can access the Internet as usual, but PC 1 cannot see the traffic that is generated by PC 2, that is, no traffic is forwarded between PC 1 and PC 2.




CLI: Configure a Protected Port to Isolate Ports on the Switch

1. Create one VLAN 192 including PC 1 and PC 2.

(Netgear	Switch)	#vlan database
(Netgear	Switch)	#vlan 192
(Netgear	Switch)	#vlan routing 192
(Netgear	Switch)	#exit
(Netgear	Switch)	#configure
(Netgear	Switch)	(Config)#interface 1/0/23
(Netgear	Switch)	(Interface 1/0/23)#vlan pvid 192
(Netgear	Switch)	(Interface 1/0/23)#vlan participation include 192
(Netgear	Switch)	(Interface 1/0/23)#exit
(Netgear	Switch)	(Config)#interface 1/0/24
(Netgear	Switch)	(Interface 1/0/24)#vlan pvid 192
(Netgear	Switch)	(Interface 1/0/24)#vlan participation include 192
(Netgear	Switch)	(Interface 1/0/24)#exit
(Netgear	Switch)	(Interface-vlan 192)#interface vlan 192
(Netgear	Switch)	(Interface-vlan 192)#routing
(Netgear	Switch)	(Interface-vlan 192)#ip address 192.168.1.254 255.255.255.0
(Netgear	Switch)	(Interface-vlan 192)#exit

2. Create one VLAN 202 connected to the Internet.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 202
(Netgear Switch) (Vlan)#vlan routing 202
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 202
(Netgear Switch) (Interface 1/0/48)#vlan participation include 202
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) (Interface vlan 202
(Netgear Switch) (Interface-vlan 202)#routing
(Netgear Switch) (Interface-vlan 202)ip address 10.100.5.34 255.255.255.0
(Netgear Switch) (Interface-vlan 202)#exit
```

3. Create a DHCP pool to allocated IP addresses to PCs.

```
(Netgear Switch) (config)#service dhcp
(Netgear Switch) (config)#ip dhcp pool pool-a
(Netgear Switch) (Config-dhcp-pool)#dns-server 12.7.210.170
(Netgear Switch) (Config-dhcp-pool)#default-router 192.168.1.254
(Netgear Switch) (Config-dhcp-pool)#network 192.168.1.0 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#exit
```

4. Enable IP routing and configure a default route.

```
(Netgear Switch)(config)#ip routing
(Netgear Switch)(config)#ip route 0.0.0.0 0.0.0.0 10.100.5.252
```

5. Enable a protected port on 1/0/23 and 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#switchport protected
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#switchport protected
(Netgear Switch) (Interface 1/0/24)#exit
```

Web Interface: Configure a Protected Port to Isolate Ports on the Switch

1. Create a DHCP pool:

Note: This example assumes that the DHCP service is enabled. For information about how to enable the DHCP service, see the Web interface procedure in *Configure a DHCP Server in Dynamic Mode* on page 305.

a. Select System > Services > DHCP Server > DHCP Server Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Management	Device View	Services Star	king SN/	MP		
 DHCP Serve DHCP Serve Configurati DHCP Pool DHCP Pool 	er on Configuration Options	DHCP Po DHCP F Pool Name	ol Config Iool Config	uration uration	pool_a V	Ð
 > DHCP Serv > DHCP Bind Information > DHCP Conline > DHCP Relay > UDP Relay 	er Statistics ings ilicts i	Pool Name Type of Bin Network Nu Network Ma Network Ma Client Name Hardware A Client ID Host Numbe Host Numbe	ding Imber Isk efix Length I uddress Uddress Type er		Dynamic 192.168.1.0 255.255.255.0 ethernet	(0-32)
		Lease Time Days Hours Minutes			Specified Duration 💌 1 0 0	(0 to 59) (0 to 1439) (0 to 86399)
		- Default	Router Addi	esses	192.168.1.254	
		- DNS Ser	ver Address	es		4
					12.7.210.170	

- **b.** Under DHCP Pool Configuration, enter the following information:
 - In the **Pool Name** field, select **Create**.
 - In the **Pool Name** field, enter **pool-a**.
 - In the **Type of Binding** field, select **Dynamic**.

- In the Network Number field, enter 192.168.1.0.
- In the Network Mask field, enter 255.255.255.0.
- In the **Days** field, enter **1**.
- Click **Default Router Addresses**. The DNS server address fields display. In the first **Router Address** field, enter **192.168.1.254**.
- Click DNS Server Addresses. The router address fields display. In the first DNS Server Address field, enter 12.7.210.170.
- c. Click Add.
- 2. Configure a VLAN and include ports 1/0/23 and 1/0/24 in the VLAN:
 - a. Select Routing > VLAN > VLAN Routing Wizard.

System	Switching		Re	outir	g	Т	Q	٥S	1	S	ecur	ity	Π	N	lon	itori	ng	T	Ν	lain	tend	ance			Hel
Routing Table	I IP I VLAN	4	RP.	RI	P	os	PF	R	outer	Dis	cove	ry	VR	RP											
VLAN Routin	a VL		Ro	utir	ıg	Wiz	ar	d																	
VLAN Routin	a 🗐	VLA	NR	outi	ng 1	Wiz	ard																		0
	VI.	n ID					19	2																	
													- 1.4	G E	nabl	ed									
	IP	Addr	ess	ł.			19	2.16	8.1	254		- 7	Ne	two	eric M	lask				255	.255	.255	0.0		
	-	Uni	it t																						
	Por	t 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23 U	24
		25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
		49	50	51	52		-			_				-	_		_		-	-			_	1000	_
		9	111																						

- **b.** Enter the following information:
 - In the Vlan ID field, enter 192.
 - In the IP Address field, enter 192.168.1.254.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display:
 - Click the gray box under port 23 twice until U displays.
 - Click the gray box under port 24 twice until U displays.

The U specifies that the egress packet is untagged for the port.

- d. Click Apply to save the VLAN that includes ports 23 and 24.
- 3. Configure a VLAN and include port 1/0/48 in the VLAN:
 - a. Select Routing > VLAN > VLAN Routing Wizard.

System	Swit	ching		Ro	utin	ng	T	Q	oS		S	ocur	ity		N	۱oni	itori	ng		N	lain	fenc	nce	1		Hel
Routing Table	IP	VLAN	A	RP	RI	P	os	PF	R	outer	Dise	cove	y I	VR	RP											
VLAN Routing		VLA	NI	Rou	utir	ng	Wiz	ar	d																	
VLAN Routing	r	V	LA	NRO	outi	ng	Wiz	ard																		Q
		Vlan	ID					20	2																	
														U	IG E	nabl	ed									
		IP A	ddr	e 55				10	.100).5.3	4			N	two	ark N	task	ð –			255	255	,255	0,0		
		*	Uni	it I																						
		Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
			49	50	51	52	-	4		12-1		(10)				1.923	(1	1 1121	1	100	-		1993	1	U
			E	1200	E																					

- **b.** Enter the following information:
 - In the Vian ID field, enter 202.
 - In the IP Address field, enter 10.100.5.34.
 - In the Network Mask field, enter 255.255.255.0.
- c. Click Unit 1. The ports display:
- **d.** Click the gray box under port **48** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
- e. Click Apply to save the VLAN that includes port 48.
- 4. Enable IP routing:

a. Select Routing > IP > Basic > IP Configuration.

System	Switch	ing Routing	QoS	Security	Monitoring	Maintenance
Routing Table	(P) VI	AN ARP RIP	OSPF Route	ar Discovery VR	RP	
Basic	shap	IP Confi	guration			
Statistics		IP Con	figuration			۲
Advanced		Default Tin	ne to Live	30		
		Routing Mo	de	🔿 Disable	Enable	
		IP Forward	ling Mode	O Disable	Enable	
		Maximum M	Next Hops	2		

- **b.** Under IP Configuration, make the following selections:
 - For Routing Mode, select the **Enable** radio button.
 - For IP Forwarding Mode, select the **Enable** radio button.
- c. Click Apply to enable IP routing.
- 5. Configure default route for VLAN 202:
 - a. Select Routing > Routing Table > Basic > Route Configuration.

							48-Port Gigs Switz
System Se	vitching	Routing	QoS Securit	y Monitoring	Maintenance	Help	Index
Routing Table 1P	VIAN I	ARP					
Basir	Rout	te Configurati	on				
Cardiperson	C	onfigure Routes					
Advanced		Route Type	Network Address	Subnotmask	Sext Hop 1P Address	Proference	1
		Static 🛌	192.168.40.0	255.255.255.0	192.168.200.2		

- **b.** Under Configure Routes, in the **Route Type** list, select **Default Route**.
- c. In the Next Hop IP Address field, enter 10.100.5.252.
- **d.** Click **Add** to add the route that is associated to VLAN 202 to the Learned Routes table.
- 6. Configure port 23 and port 24 as protected ports:
 - a. Select Security > Traffic Control > Protected Port.

A screen similar to the following displays.

System	Swite	hing	Υ	Ro	outir	g	Υ	Q	50	T	S	scur	ity	Т	N	loni	torin	9	N	lain	tenc	ince			Help
Management	Security	Acces	s	Por	rt Au	thent	licati	ion	Ţ	offic	Co	ntrol	17	ACL											
MAC Filter		Prot	tec	teo	d Pe	orts	s M	len	nbe	ers	hip														
 Storm Conti Port Securit 	rol Y	P	rot	ecte	ed P	ort	Mei	mbe	rsh	ip															۲
· Protected P	ort		Uni	t 1																					
		Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16 1	7 18	19	20	21	22	23	24
																								1	1
		1	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40 4	42	43	44	45	46	47	48
			49	50	51	52			1123			1201		1.023			1000			1999			1128		1000

- **b.** Under Protected Ports Configuration, click **Unit 1**. The ports display.
 - Click the gray box under port 23. A check mark displays in the box.
 - Click the gray box under port 24. A check mark displays in the box.
- c. Click Apply to activate ports 23 and 24 as protected ports.

802.1x Port Security

This section describes how to configure the 802.1x port security feature on a switch port. IEEE 802.1x authentication prevents unauthorized clients from connecting to a VLAN unless these clients are authorized by the server. 802.1x port security prevent unauthorized clients from connecting to a VLAN. It can be configured on a per-port basis.



Figure 22. Using 802.1x port security

The following example shows how to authenticate the dot1x users by a RADIUS server. The management IP address is 10.100.5.33/24. The example is shown as CLI commands and as a Web interface procedure.

CLI: Authenticating dot1x Users by a RADIUS Server

1. Assign an IP address to 1/0/19, and set force authorized mode to this port, and create a user name list dot1xList.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Config)#dot1x system-auth-control
(Netgear Switch) (Config)#interface 1/0/19
(Netgear Switch) (Interface 1/0/19)#routing
(Netgear Switch) (Interface 1/0/19)#ip address 10.100.5.33 255.255.0
(Netgear Switch) (Interface 1/0/19)#dot1x port-control force-authorized
```

2. Use RADIUS to authenticate the dot1x users.

(Netgear Switch) (Config)#aaa authentication dot1x default radius

3. Configure a RADIUS authentication server.

(Netgear Switch) (Config) #radius server host auth 10.100.5.17

4. Configure the shared secret between the RADIUS client and the server.

```
Netgear Switch) (Config)#radius server key auth 10.100.5.17
Enter secret (16 characters max):123456
Re-enter secret:123456
```

5. Set the RADIUS server as a primary server.

```
(Netgear Switch) (Config)#radius server msgauth 10.100.5.17
(Netgear Switch) (Config)# radius server primary 10.100.5.17
```

6. Configure an accounting server.

```
(Netgear Switch) (Config)#radius accounting mode
(Netgear Switch) (Config)#radius server host acct 10.100.5.17
```

7. Configure the shared secret between the accounting server and the client.

```
(Netgear Switch) (Config)#radius server key acct 10.100.5.17
Enter secret (16 characters max):123456
Re-enter secret:123456
```

Web Interface: Authenticating dot1x Users by a RADIUS Server

- **1.** Enable routing for the switch.
 - a. Select Routing > Basic > IP Configuration.

System	Switching	Routing	QoS Sno	surity.	Monitoring	Maintenance	Help	Index
Routing Table (IP VLAN	ARP RIP C	DSPF Router Disco	wery I VR	RP ()			
• Basic • IP Continuent	IP Co	onfiguration Configuration				0		
Advanced	Defaul Routin IP For Maxim	lt Time to Live 19 Mode warding Mode 14 Next Nops	30 C Diseble C Diseble 2	@ Enable @ Enable				

- **b.** For Routing Mode, select the **Enable** radio button.
- c. Click Apply to save the settings.

- 2. Assign IP address 192.168.1.1/24 to the interface 1/0/1.
 - a. Select Routing > Advanced > IP Interface Configuration.

System 3	Switchin	Routi	ng QoS	Security	Monitorin	g Maintenance	Help	Index
Routing Table	P I VV	NI ARP R	IP OSPF Rout	er Discovery	VRRP			
Basic	I	P Interface	Configuration	0				
» IP Configuratio	40 1	Configuratio	n					
» Statistics	1					Gn To Interface	60	
• Secondary IP		Interface	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Hode
	Ē	1/0/1			192.168.1.1	255.255.255.0	Enable i.	Enable 💽
		1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

b. Under IP Interface Configuration, scroll down and select the Interface **1/0/1** check box.

Now 1/0/1 appears in the Interface field at the top.

- **c.** Enter the following information:
 - In the IP Address field, enter 192.168.1.1.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Routing Mode field, select Enable.
- d. Click Apply to save the settings.
- 3. Assign IP address 10.100.5.33/24 to interface 1/0/19:
 - a. Select Routing > Advanced > IP Interface Configuration.

A screen similar to the following displays.

System S	witching	Routin	0 Qo5	Security	Monitorin	g Maintenance	Help	Index
Routing Table 1	VEAN	ARP RU	OSPF Route	r Discovery	VRRP			
a Basic	IP	Interface	Configuration					
+ IP Configuration		Configuratio	n					
 Statistics 		All				Go To Interface	00	
 Secondary IP 		Interface	Description	VLAN 10	IP Address	Subnet Mask	Routing Mode	Administrative Mode
		1/0/19			10,100.5.33	255.255.255.0	Enable 🖻	Enable -
	E	1/0/1			0.0.0.0	0.0.0.0	Disable	Enable

b. Scroll down and select the interface **1/0/19** check box.

Now 1/0/19 appears in the Interface field at the top.

- c. Enter the following information:
 - In the IP Address field, enter 10.100.5.33.
 - In the Subnet Mask field, enter 255.255.255.0.
 - In the Routing Mode field, select Enable.
- d. Click Apply to save the settings.

- 4. Create an authentication name list.
 - a. Select Security > Management Security > Login > Authentication List.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Seco	ally Access	Port Authentic	ation Tra	fic Control AC	í.			
Dier Configuration H Dier	Autho	Intication Li	st				ŵ	
Hanagement		ist Name	1		2	а		
RADIUS TACACS+		dot1xList	R	adius 💌	Undefined 3	Undefin	ed 🔄	
Login	E 4	lefaultList	Lo	cal	Undefined	Undefine	d.	
» Authenticatio List » Login Sessio	ns							

- **b.** Select the check box before **dot1xList**.
- c. In the 1 list, select Radius.
- d. Click Apply.
- 5. Set port 1/0/19 to force authorized mode. (In this case, the RADIUS server is connected to this interface.)
 - a. Select Security > Port Authentication > Advanced > Port Authentication.

System Sw	itching	Rout	ing Qos	5 Secu	rity	Monitoring	Moint	snance	Help	Index
Monogement Security	Acces	1 Port A	offention	Traffic Contro	ACL					
Basic	Port	Authen	tication							
* 802.18	Pu	rt Auther	itication							
Configuration										Ge
> Port Summary		ort	Control Mo	de	Quiet Period	Transmit Period	Supplicant Timeout	Server Timeout	Naximum Requests	Periodic Reauthentication
and the second		1/0/19	Force Author	e bezne	60	30	30	30	2	Disable 💽
	E 1	/0/1	Auto		60.	39	30	30	2	Disable
	Γ :	/0/2	Auto		60	30	10	30	2	Disable

- **b.** Scroll down and select the Interface **1/0/19** check box. Now 1/0/19 appears in the Interface field at the top.
- c. In the Control Mode list, select Force Authorized.
- d. Click Apply to save the settings.
- 6. Enable dot1x on the switch.
 - a. Select Security > Port Authentication > Server Configuration.

System 51	vitching	Routing	QoS Security	Monitoring	Maintenance	Help	Index
Monogement Securi	ly Access	Port Authenticatio	an: Troffic Control A	ci			
Ranit	802.1X	Configurati	on				
Cilifiguration	Mode			4			
Advanced	Administra VLAN Assis	ative Mode gnment Mode	ale ale				
	802.1	X Configuratio	0	0	D.		
	Users	Non-config	ured use				
	Login	dottxLest	-				

- **b.** For Administrative Mode, select the **Enable** radio button.
- c. In the Login list, select dot1xList.
- d. Click Apply to save settings.
- 7. Configure the RADIUS authentication server.
 - a. Select Security > Management Security > Server Configuration.

System St	witching	Routing	QeS	Security	Manito	ring	Maintenance	e Help	index	10801
Monogement Securi	ly Access	Port Autho	nticotion	Traffic Control Al	ck					
User	Server	Configu	ration							
- RADTUS	Serve	r Configu	ration							
* Redus		erver Ad	Idress	Por	t Se	cret Confi	gured Se	ecret	P	imary Server
Configuration		10,100.5,1	7	10	12 1	5 🔺				es
Accounting	Statis	lics				0				
Configuration Login	Server Address	Round Trip Time	Access Requests	Access Retransmission	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticator	s Pending Requests

- b. In the Server Address field, enter 10.100.5.17.
- c. In the Secret Configured field, select Yes.
- d. In the Secret field, enter 123456.
- e. In the Primary Server field, select Yes.
- f. In the Message Authenticator field, select Enable.
- g. Click Add.
- 8. Enable accounting.
 - a. Select Security > Management Security > RADIUS > Radius Configuration.

System S	witching Routing Qo	S Security	Monitoring	Maintenance	Help	Index
Monogement Secur	Ity Access Port Authentication	Traffic Control ACL				
User Configuration	Radius Configuration Radius Configuration			Ū		
• Radims Configuration	Current Server Address Number of Configured Servers	10.100.5.17 1				
Configuration - Accounting Server	Max Number of Retransmits Timeout Duration (secs) Accounting Mode	4 5 Enable	(1 to 15) (1 to 30)			
Configuration	RADIUS Attribute 4	@ Disable C Enable				

- b. In the Server Address field, enter 10.100.5.17.
- c. In the Accounting Mode field, select Enable.
- d. Click Apply.
- 9. Configure the accounting server.
 - a. Select Security > Management Security > RADIUS > Radius Accounting Server Configuration.

A screen similar to the following displays.

System 5w	itching Routing Q	oS Security	Monitoring	Maintenance	Help	Index
Management Security	y Access Port Authentication	Truffic Control AC	1			
User Configuration	Accounting Server Co	onfiguration				
RADIUS	Accounting Server Con	figuration	0	0		
* Radius	Accounting Server Address	10.100.5.17				
Configuration	Port	1813				
Configuration	Secret Configured	Yes	•			
a Accounting	Secret	*******				
Server	Accounting Hode	Enable				

- b. In the Accounting Server Address field, enter 10.100.5.17.
- c. In the Accounting Mode field, select Enable.
- d. Click Apply.

Create a Guest VLAN

The guest VLAN feature allows a switch to provide a distinguished service to dot1x unaware clients (not rogue users who fail authentication). This feature provides a mechanism to allow visitors and contractors to have network access to reach an external network with no ability to surf the internal LAN.



Figure 23. Guest VLAN

If a port is in port-based mode, and a client that does not support 802.1X is connected to an unauthorized port that has 802.1X enabled, the client does not respond to the 802.1X requests from the switch. The port remains in the unauthorized state, and the client is not granted access to the network. If the guest VLAN is configured for that port, then the port is placed in the configured guest VLAN and the port is moved to the authorized state, allowing access to the client after a certain amount of time (determined by the guest VLAN period). If the client attached is 802.1x aware, then this allows the client to respond to 802.1X requests from the switch.

For a port in MAC-based mode, if traffic from a unauthenticated client is noticed on a port then, if guest VLAN has been configured on the port, the guest VLAN timer is started for that client. If the client is 802.1x unaware and does not respond to any 802.1x requests, when the guest VLAN timer expires, the client is authenticated and associated with the guest VLAN. This ensures that traffic from the client is accepted and switched through the guest VLAN.

In this example, dot1x is enabled on all the ports so that all the hosts that are authorized are assigned to VLAN 1. On ports 1/0/1 and 1/0/24, guest VLAN is enabled. If guests connect to the port, they are assigned to VLAN 2000, so that guests cannot access the internal VLAN, but can access each other in the guest VLAN.

CLI: Create a Guest VLAN

1. Enter the following commands:

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2000
(Netgear Switch) (Vlan)#exit
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 2000
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 2000
(Netgear Switch) (Interface 1/0/24)#exit
```

2. Create VLAN 2000, and have 1/0/1 and 1/0/24 as members of VLAN 2000.

(Netgear	Switch)	(Config)#aaa authentication dot1x default radius
(Netgear	Switch)	(Config)#dot1x system-auth-control
(Netgear	Switch)	(Config)#radius server host auth 192.168.0.1
(Netgear	Switch)	(Config)#radius server key auth 192.168.0.1
Enter sea	cret (16	characters max):12345
Re-enter	secret:1	2345
(Netgear	Switch)	(Config)#interface 1/0/6
(Netgear	Switch)	(Interface 1/0/6)#dot1x port-control force-authorized
(Netgear	Switch)	(Interface 1/0/6)#exit
(Netgear	Switch)	(Config)#interface 1/0/12
(Netgear	Switch)	(Interface 1/0/12)#dot1x port-control force-authorized
(Netgear	Switch)	(Interface 1/0/12)#exit

3. Enable dot1x and RADIUS on the switch.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#dot1x guest-vlan 2000
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#dot1x guest-vlan 2000
(Netgear Switch) (Interface 1/0/24)#exit
```

4. Enable the guest VLAN on ports 1/0/1 and 1/0/24.

(Netgear Switch) #show dot1x detail 1/0/1	
Protocol Version	1
PAE Capabilities	Authenticator
Control Mode	auto
Authenticator PAE State	Authenticated
Backend Authentication State	Idle
Quiet Period (secs)	60
Transmit Period (secs)	30
Guest VLAN ID	2000
Guest VLAN Period (secs)	90
Supplicant Timeout (secs)	30
Server Timeout (secs)	30
Maximum Requests	2
VLAN Id	2000
VLAN Assigned Reason	Guest
Reauthentication Period (secs)	3600
Reauthentication Enabled	FALSE
Key Transmission Enabled	FALSE
Control Direction	both
Maximum Users	16
Unauthenticated VLAN ID	0
Session Timeout	0
Session Termination Action	Default

Web Interface: Create a Guest VLAN

- 1. Create VLAN 2000.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP	Multicost	Address Table	Ports LAG					
• Basic	VLA	N Configurat	tion					
 VLAN Configuration 	R	eset					۲	
Advanced	Rese	et Configuration						
	Ir	nternal VLAN C	onfiguration	1			(1)	
	Inte	mal VLAN Allocat	ion Base		4093			
	Inte	mal VLAN Allocat	ion Policy		C Asce	ending 🖲 Descending		
	v	LAN Configurat	tion				۲	
		VLAN ID	VLA	N Name	v	LAN Type		
		2000				*		
		1	Defa	ult	D	efault		

b. In the VLAN ID field, enter 2000.

- c. In the VLAN Type field, select Static.
- d. Click Add.
- 2. Add ports to VLAN 2000.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

System	Switchi	ng	ſ	Ro	utir	ng		QoS		S	ecur	îty		Mo	nitor	ing	Y	Μ	aint	ena	ince	8		Hel	lp	Ind
VLAN STP	Multicas	117	Addr	ess	Tabl	•	Ports	ΙL	AG																	
Basic	٧	VLAN Membership																								
> VLAN	1	VL	AN	Me	mb	ersh	ip																	1		
Configuration	9 I	VLAN	ID				2000	-						į	Group	Ope	ratio	a	U	Inta	g Al	1	F			
VLAN Membe	rship	VLAN	Nar	ne											UNTA	GGE	D POI	IM TS	EMBER	RS	ľ.			T		
Port PVID		VLAN	Typ	e			Statio								TA	GGED	POR	T ME	MBER	5	l.					
Configuration		•	Unit	1																						
MAC Based V	LAN P	ort	1	2	3	4	56	7	8	9	10	11	12	13 1	4 15	5 16	17	18	19	20	21	22	23	24		
 IP Subnet Ba VLAN Port DVIan 	sed		25	26	27	28				13		3 - 31.			IJ								81	U	l E	

- b. In the VLAN ID list, select 2000.
- c. Click Unit 1. The ports display.
- d. Click the gray boxes under ports 1 and 24 until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply.
- 3. Set force authorized mode on ports 1/0/6 and 1/0/12.
 - a. Select Security > Port Authentication > Advanced > Port Authentication.

System	Swite	hing	Ro	outing	QoS	Security	Monitoring	Maintena	nce Help	Index
Management	Security	Acce	ss Por	rt Authentica	tion Traffi	Control Con	trol ACL		6.ML	
Basic	1	Port	Auth	enticatio	on					
Advanced > 802.1X		р	ort Auti	henticatio	n					
Configurati	on	I A	1							
* Port Authenticat * Port Summ	ton		Port	Control	Mode	Quiet Period	Transmit Period	Guest ¥LAN ID	Guest ¥LAN Period	Unauthenticated VLAN ID
» Client Sum	mary		1/0/6	Force A	uthorized	• 60	30	0	90	0
		Г	1/0/1	Auto		60	30	2000	90	0
		Г	1/0/2	Auto		60	30	0	90	0
		Г	1/0/3	Auto		60	30	0	90	0
		Г	1/0/4	Auto		60	30	0	90	0
			1/0/5	Auto		60	30	0	90	0
		V	1/0/6	Auto		60	30	0	90	0

- b. Scroll down and select the Interface 1/0/6 and 1/0/12, check boxes.
- c. In the Control Mode list, select Force Authorized.
- d. Click Apply to save settings.
- **4.** Enable dot1x on the switch.

Make sure that 1/0/12 and 1/0/6 are configured as force authorized before you do this step; otherwise you cannot access the switch through the Web Interface.

a. Select Security > Port Authentication > Basic > 802.1x Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Security Access	Port Authenti	cation Tra	fic Control Co	ntrol ACL		100	
Basic	802.1	LX Configur	ation					
Configurat	ion 803	2.1X Configur	ation				(7)	
Advanced	Admin	istrative Mode			C Disabl	e 🖲 Enable		
	VLAN .	Assignment Mod	ie		Disabl	e C Enable		
	Users				admin			
	Login				defaultLis	tt +		
	Authe	ntication List			defaultList			

- **b.** For Administrative Mode, select the **Enable** radio button.
- c. Click Apply to save settings.
- 5. Configure the dot1x authentication list.
 - a. Select Security > Management Security > Authentication List > Dot1x Authentication List.

System	Switching	Routing	QoS Security	Monitoring	Maintenance	Help	Index
Management Sec	urity Access	Port Authenticati	on Traffic Control Co	ontrol ACL			
Local User	Dot1	x Authenticat	ion List				
TACACS+	Do	t1x Authenticatio	in List			(7)	
Authentication	1 T	List Name	1	2	3		
List » Login	ম	defaultList	RADIUS 💌	LOCAL 💌	LOCAL 💽		
Authentication List » Enable Authentication	on						
List » Dot1x Authenticatio	on						

- b. Select the defaultList check box.
- c. In the 1 list, select RADIUS.
- d. Click Add.
- 6. Configure the RADIUS authentication server.
 - a. Select Security > Management Security > Radius > Server Configuration.

System	Switching	Routin	g Qos	5 Security	Monit	loring	Maintenan	ce Help	Index	
Monogement Secu	rity Acces	Port Aut	hentication	Traffic Control Co	ntrol AC	1				
Local User	Serv	e <mark>r Confi</mark> g	juration							
» Radius	Se	rver Confi	guration							
Configuration		Radius Ser Address	ver IP	Radius Server	Radius Server Name Curren		Port	Secret Configu re d	Secret	
 Configuration Accounting Ser 	ver 🔲	192.168.0.	1					Yes 💌	****	
Configuration	St	atistics								
Authentication List » Login	Radi Serv	rs Round Er Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pendi Reque

- b. In the Radius Server IP Address field, enter 192.168.0.1.
- c. In the Secret Configured field, select Yes.
- d. In the Secret field, enter 12345.
- e. Click Add.
- 7. Configure the guest VLAN.
 - a. Select Security > Port Authentication > Advanced > Port Authentication.
 A screen similar to the following displays.

System	Swit	ching	Ro	uting	QoS	Security	Monitoring	Maintenar	nce Help	Index
Management	Security	Acce	ss Por	t Authenticat	lion Troff	ic Control Cor	ntrol ACL		(240) 	
Basic		Port	Auth	enticatio	'n					
* 802.1X		P	ort Aut	nentication	1					
Configurati	ion	1 A	u					Transmit Guest YLAN Guest YLAN Unauthentica		
Authenticat » Port Summ	tion hary		Port	Control N	tode	Quiet Period	Transmit Period	Guest ¥LAN ID	Guest VLAN Period	Unauthenticated VLAN ID
» Client Sum	mary		[]			•		2000		
			1/0/1	Auto		60	30	0	90	0
		Г	1/0/2	Auto		60	30	0	90	0

- **b.** Scroll down and select the port 1/0/1 and 1/0/24 check boxes.
- c. In the Guest VLAN ID field, enter 2000.
- d. Click Apply to save your settings.

Assign VLANs Using RADIUS

This feature allows the client to connect from any port and be assigned to the appropriate VLAN assigned by the RADIUS server. This gives flexibility for the clients to move around the network without requiring the administrator to do static VLAN configuration. When multiple hosts are connected to the switch on the same port, only one host uses authentication. If any VLAN information is applied on the port based on the authenticated host, the VLAN applies that information to all the hosts that are connected to that port.

- After a port is in an authorized state, if any client initiates dot1x authentication, the port clears authenticated clients' states, and in the process clears the VLAN assigned to the port (if any). Then the port continues with the new client authentication and authorization process.
- When a client authenticates itself initially on the network, the switch acts as the authenticator to the clients on the network and forwards the authentication request to the RADIUS server in the network.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = VLANID where VLANID is 12 bits, with a value between 1 and 4094.



Figure 24. VLAN assignment using RADIUS

In the previous figure, the switch has placed the host in the VLAN (vlan2000) based on the user details of the clients.

The configuration on a RADIUS server for a user logged in as admin is:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = 2000

CLI: Assign VLANS Using RADIUS

1. Create VLAN 2000.

```
(Netgear Switch) #network protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y
(Netgear Switch) #network parms 192.168.0.5 255.255.255.0
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2000
(Netgear Switch) #exit
```

2. Enable dot1x authentication on the switch

(Netgear Switch) (Config)#dot1x system-auth-control

3. Use the RADIUS as the authenticator.

(Netgear Switch) (Config)#aaa authentication dot1x default radius

4. Enable the switch to accept VLAN assignment by the RADIUS server.

(Netgear Switch) (Config) #authorization network radius

5. Set the RADIUS server IP address.

(Netgear Switch) (Config) #radius server host auth 192.168.0.1

6. Set the NAS-IP address for the RADIUS server.

```
(Netgear Switch) (Config)#radius server key auth 192.168.0.1
Enter secret (16 characters max):12345
Re-enter secret:12345
Set the radius server key.
(Netgear Switch) (Config)#radius server attribute 4 192.168.0.1
```

7. Force 1/0/6 to be authorized for it to connect to the RADIUS server.

(Netgear Switch) (Config)#interface 1/0/6 (Netgear Switch) (Interface 1/0/6)#dot1x port-control force-authorized (Netgear Switch) (Interface 1/0/6)#exit 8. Show the dot1x detail for 1/0/5.

(Netgear Switch) #show dot1x detail 1/0/5	
Port	1/0/5
Protocol Version	1
PAE Capabilities	Authenticator
Control Mode	auto
Authenticator PAE State	Authenticated
Backend Authentication State	Idle
Quiet Period (secs)	60
Transmit Period (secs)	30
Guest VLAN ID	0
Guest VLAN Period (secs)	90
Supplicant Timeout (secs)	30
Server Timeout (secs)	30
Maximum Requests	2
VLAN Id	2000
VLAN Assigned Reason	RADIUS
Reauthentication Period (secs)	3600
Reauthentication Enabled	FALSE
Key Transmission Enabled	FALSE
Control Direction	both
Maximum Users	16
Unauthenticated VLAN ID	0
Session Timeout	0
Session Termination Action	Default

Web Interface: Assign VLANS Using RADIUS

- 1. Assign the IP address for the Web Management Interface.
 - a. Select System > Management > Network Interface > IPv4 Network Configuration.

System Sw	itching R	Routing QoS	Security	Monitoring	Maintenance	Help	Index
Management Dev	vice View Serv	rices Stacking S	NMP LLDP I	SDP	10	4) .	
System Information	IPv4 Net	work Interface	e Configuratio	n			
Switch Statistics	IPv4 Ne	etwork Interface (Configuration			۲	
System Resource	IP Address			192.168.0	.5		
Slot Information	Subnet Mas	k		255.255.2	55.0		
Loopback	Default Gat	teway					
Interface	Burned In M	AC Address		00:1E:2A:	D9:24:99		
Interface	Locally Adm	ninistered MAC Addre	55	00:00:00:	00:00:00		
* IPv4 Network	MAC Addres	ss Type		@ Burned	In		
Configuration				C Locally	Administered		
» IPv6 Network	Current Net	twork Configuration P	rotocol	€ None (Bootp C DHCP		
Configuration	DHCP Vende	or Class Identifier		Disable	C Enable		
Neighbor	DHCP Vend	or Class Identifier St	ring				
Time	Managemer	nt VLAN ID		1			

- b. For Current Network Configuration Protocol, select the None radio button.
- c. In the IP Address field, enter 192.168.0.5.
- d. In the Subnet Mask field, enter 255.255.255.0.
- e. Click Apply.
- 2. Create VLAN 2000.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP	Multicost	Address Table 1	Ports LAG					
Basic	VLA	N Configurat	tion					
 VLAN Configuration 	R	eset					(1)	
Advanced	Rese	et Configuration						
	. 1	nternal VLAN Co	onfiguration	I.			(1)	
	Inte	mal VLAN Allocat	ion Base		4093			
	Inte	mal VLAN Allocat	ion Policy		O Asc	ending 🖲 Descending		
	v	LAN Configurat	ion				۲	
		VLAN ID	¥LA	N Name	v	LAN Type		
		2000						
		1	Defa	ult	C	efault		

- b. In the VLAN ID field, enter 2000.
- c. In the VLAN Type field, select Static.
- d. Click Add.
- 3. Set force authorized mode on ports 1/0/6 and 1/0/12.
 - a. Select Security > Port Authentication > Advanced > Port Authentication.

System	Swit	ching	Ro	outing QoS	Security	Monitoring	Maintenar	ice Help	Index		
Management	Security	Acce	ss Por	t Authentication Traffi	c Control Con	trol ACL		-236			
Basic Advanced		Port	Auth	entication							
≥ 802.1X		- P	ort Auti	hentication							
Configurat	ion	1 All									
Authentica » Port Sumn	tion harv:		Port	Control Mode	Quiet Period	Transmit Period	Guest ¥LAN ID	Guest VLAN Period	Unauthenticated VLAN ID		
» Client Sum	mary		1/0/6	Force Authorized	• 60	30	0	90	0		
		П	1/0/1	Auto	60	30	2000	90	0		
		Г	1/0/2	Auto	60	30	0	90	0		
		Г	1/0/3	Auto	60	30	0	90	0		
		Г	1/0/4	Auto	60	30	0	90	0		
			1/0/5	Auto	60	30	0	90	0		
		V	1/0/6	Auto	60	30	0	90	0		

- **b.** Under Port Authentication, scroll down and select the 1/0/6 and 1/0/12 check boxes.
- c. In the Control Mode list, select Force Authorized.
- d. Click Apply to save settings.
- **4.** Enable dot1x on the switch.

Make sure that 1/0/12 and 1/0/6 are configured as force authorized before you do this step; otherwise, you cannot access the switch through the Web Management Interface.

a. Select Security > Port Authentication > Basic > 802.1x Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Security Access	Port Authentic	ation Tro	ffic Control Co	ntrol ACL	Hr.		
* Basic * 802.1X	802.1	X Configur	ation					
Configurati	on 802	1X Configura	ation		<u> </u>	6	(7)	
Auvanceu	VLAN A	strative Mode Assignment Mod	e		C Disabl	e 🤨 Enable e 🖸 Enable		
	Users				admin			
	Login				defaultLis	* *		
	Auther	tication List			defaultList			

- b. For Administrative Mode, select the Enable radio button.
- c. For VLAN Assignment Mode, select the Enable radio button.
- d. Click Apply to save settings.
- 5. Configure the dot1x authentication list.
 - a. Select Security > Management Security > Authentication List > Dot1x Authentication List.

System	Swite	hing	Routing	QoS Security	Monitoring	Maintenance	Help	Index
Management	Security	Access	Port Authenticat	ion Troffic Control	Control ACL			
Local User		Dot1x	Authenticat	ion List				
TACACS+		Dot	Lx Authenticati	on List			(7)	
Authentica	tion		List Name	1	2	3		
List		V	defaultList	RADIUS 💌	LOCAL 💽	LOCAL 💽		
Authentic List » Enable Authentic List » Dot1x Authentic	ation ation ation							

- **b.** Select the **defaultList** check box.
- c. In the 1 list, select RADIUS.
- d. Click Add.
- 6. Configure the RADIUS authentication server.
 - a. Select Security > Management Security > Radius > Server Configuration.

A screen similar to the following displays.

System	Switz	ching	Routing	g QoS	Security	Monit	loring	Maintenan	ce Help	Index	
Monogement	Security	Access	Port Aut	entication	Traffic Control Co	ntrol AC	1				
Local User	2	Server	Config	uration							
» Radius		Serve	er Config	juration							
Configurat	on	Ra Ad	dius Ser dress	ver IP	Radius Server	Name	Current	Port	Secret Configured	Secret	
 Accounting 	Server	19	2.168.0.1						Yes 💌	****	
Configurat	on	Statis	stics								
Authentica List > Login	tion	Radius Server	Round Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pendii Reque

- b. In the Radius Server IP Address field, enter 192.168.0.1.
- c. In the Secret Configured field, select Yes.
- d. In the Secret field, enter 12345.
- e. Click Add.

Dynamic ARP Inspection

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface).

When DAI is enabled, the switch drops ARP packet if the sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. However, it can be overcome through static mappings. Static mappings are useful when hosts configure static IP addresses, DHCP snooping cannot be run, or other switches in the network do not run dynamic ARP inspection. A static mapping associates an IP address to a MAC address on a VLAN.





CLI: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

(Netgear Switch) (Config)# ip dhcp snooping

2. Enable DHCP snooping in a VLAN.

(Netgear Switch) (Config)# ip dhcp snooping vlan 1

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

5. Enable ARP inspection in VLAN 1.

```
(Netgear Switch) (Config)# ip arp inspection vlan 1
```

Now all ARP packets received on ports that are members of the VLAN are copied to the CPU for ARP inspection. If there are trusted ports, you can configure them as trusted in the next step. ARP packets received on trusted ports are not copied to the CPU.

6. Configure port 1/0/1 as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip arp inspection trust
```

Now ARP packets from the DHCP client go through because there is a DHCP snooping entry; however ARP packets from the static client are dropped. It can be overcome by static configuration as described in *Static Mapping* on page 246.

Web Interface: Configure Dynamic ARP Inspection

- 1. Enable DHCP snooping globally.
 - a. Select Security > Control > DHCP Snooping Global Configuration.

System	Switching	Routing	QoS Security	Monitoring	Maintenance	Help	Index
Monogement	Security Access	Port Authentication	Traffic Control Co	ntrol ACL			
DHEP Shoup	-	DHCP Snooping	Global Configura	ition			
+ Clobal		DHCP Snooping	Global Configuration	6		ġ	
* Interface		DHCP Snooping Mod	•	🧧 Disable 🔘) Enable		
Configuratio	an a	HAC Address Valida	tion	🕤 Disable 🦉	Enable		
Configuratio		VLAN Configure	ation			đ	6
 Persistent Configuration 	an	VLAN ID	DHCP Snoo	ping Mode			
> Statistics				01490			

- **b.** For DHCP Snooping Mode, select the **Enable** radio button.
- c. Click Apply.
- 2. Enable DHCP snooping in a VLAN.
 - a. Select Security > Control > DHCP Snooping Global Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Security Acc	ess Port Authenti	cation Tra	ffic Control Co	ind (ACL		10	
DHEP Sucop	100	DHCP Snoo	ping Glob	al Configura	tion			
Configuration	in Cine	DHCP Snot	ping Globa	Configuration				0
> Interface		DHCP Snooping	Mode		Oisable	Enable		
Contiguration	on	MAC Address V	alidation		🗇 Disable 🍯	Enable		
Configuratio	on	ULAN Conf	louration					
 Persistent Configuration 	on.	VEAN COM	DUCD Sec	oping blode				-
» Statistics	Region Region		Chickette	apping mode.				
IP Source G	uard							
Dynamic AR	UP (
Captive Por	tal							

- b. In the VLAN ID field, enter 1.
- c. In the DHCP Snooping Mode field, select Enable.

System Switch	ing Routing QoS	Security	Monitoring	Maintenance	Help	Index
Monogement Security	Access Port Authentication Tr	affic Control Co	ACL			
· DHEP Severging	DHCP Snooping Glo	bal Configura	tion			
Carifiguration	DHCP Snooping Glot	al Configuration			1.3	
> Interface	DHCP Snooping Mode		🕤 Disable 🕯	Enable		
Configuration > Binding	MAT Address Validation		🗇 Disable 🔮	Enable		
 Persistent 	VLAN Configuration				3.0	
Configuration	VLAN ID DHCP St	ooping Node				
» Statistics		•				
IP Source Guard	117 . Enable				_	
Inspection	El a Enable					

- Configure the port through which the DHCP server is reached as trusted. Here interface 1/0/1 is trusted.
 - a. Select Security > Control > DHCP Snooping Interface Configuration.

System Swit	ching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Monogement Security	Access	Port Authentic	ation Traffic C	ontrol Control	ACE				
DITEP Seconing	DH	ICP Snoop	ing Interfa	ce Configura	ation				
Global DHCP Snooping Interface Configuration									
* Interface	1	Z All		Go To Interface		60			
Configuration Configuration		Interface	Trust Mode	Logging Invalid Packets	Rate Limit(p	ps) Burst Inter	rval(secs)		
 Persistent Configuration 									
> Statistics		1/0/1	Disable	Disable	15	1			

- **b.** Select the check box for Interface **1/0/1**.
- c. For Interface 1/0/1, set the Trust Mode as Enable.
- d. Click Apply. A screen similar to the following displays.

System	Switching	Routi	ng QoS	Security	Monitoring	Maintenance Help
Monogement	Security Access	Port A	nhentication Tra	fic Control Cont	rel ACL	
- DHLP Same	ping	DHCP S	nooping Inte	rface Configu	iration	
 Global Configurati 	ion	DHCP	Snooping Inter	face Configurati	on	
 Interface Certifiquesti 	201	-		Go To Inter	face 🦳 🕼	
 Binding Configuration 	ion	Int	erface Trust M	Logging ode Invalid	Rate Limit(pp	a) Burst Interval(secs)
> Persistent	on.		The set of the set of the	Packets	200000 0000000000	
* Statistics	1991)			-	•	
IP Source (Guard	1/0	1 Enable	Disable	15	1
Dynamic Al	RP.	-	in alasti	- Alexandre		

- 4. View the DHCP Snooping Binding table.
 - a. Select Security > Control > DHCP Snooping Binding Configuration.

System	Swite	hing	Routing	QoS	Security	Monitor	ing	Maintenar	nce Help	
Management	Security	Access	Port Authenti	cotion Tra	ffic Control 🥵	ntrol ACL				
OHCP Snoop Slobal Configurati	ping	D	HCP Snoo	ping Bind	ing Configur	ation				(7)
 Interface Configurati Einding 	on		Interfac	e MAC Ad	dress	VL/	AN ID	IP Addres	5	
Configuration > Persistent	ón To	1	Dynamic B	inding Conf	iguration					
Configuration	on	1	nterface	MAC Addr	ess	VLAN ID	IP A	ddress	Lease Time	
> IP Source 0	iuard	1	/0/2	00:18:8B:5	56:FD:35	1	192.	168.10.94	86394	

- 5. Enable ARP Inspection in VLAN 1.
 - a. Select Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration.

System S	Switching	Routing	GoS	Security	Monitoring	Maintenance	Help	Index
Monogement Secu	rity Access	Port Auth	entication Tra	flic Control Gar	HOL ACL			
DHCP Snooping IP Source Guar	d Di	namic VLAN C	ARP Inspect	tion Configu	ration		4	D.
DAI Configurati CAI (CAN)	ion:	VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Nam	•	Static Flag	
> DAI Interface	-			·			•	
* DAI ACL Configuration								
 DAI ACL Rule Configuration 								
DAI Statistics Captive Portal								

- b. In the VLAN ID field, enter 1.
- c. In the Dynamic ARP Inspection field, select Enable.

A screen similar to the following displays.

System Swi	itching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Security	Access	Port Auth	entication Tra	file Control Co	abol ACL			
DHCP Snooping	D	ynamic	ARP Inspe	ction Configu	uration			
1P Source Guard	6	VLAN C	onfiguration					1
> DAI Configuration		VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP AEL Nam	e Fl	atic ag	
Configuration	C (1 -	Enable 👻				•	
DAI Interface Configuration DAI ACL Configuration DAI ACL Rule Configuration DAI ACL Rule Configuration DAI Statistics Captive Portal								

d. Click Apply.

A screen similar to the following displays.

System	Swite	hing	Routing	QoS	Security	Monitoring N	laintenance Help
Management	Security	Access	Port Auth	entication Tra	fic Control Con	HILL ACL	
DHCP Snoop IP Source C	ping iuard	Dy		ARP Inspect	tion Configu	ration	
> DAI Config	uration		VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
> DAI Interfe	ice	C	-	Enable	Enable		Disable

Now all the ARP packets received on the ports that are member of the VLAN are copied to the CPU for ARP inspection. If there are trusted ports, you can configure them as trusted in the next step. ARP packets received on the trusted ports are not copied to the CPU.

Note: Make sure the administrator PC has a DHCP snooping entry or can access the device through the trusted port for ARP. Otherwise, you might get disconnected from the device.

- 6. Configure port 1/0/1 as trusted.
 - a. Select Security > Control > Dynamic ARP Inspection > DAI Interface Configuration.
 - b. Select the Interface 1/0/1 check box.
 - c. For the Trust Mode, select Enable.
 - d. Click Apply.

A screen similar to the following displays.

System	Switch	ing	Routing	GoS Se	curity Monitorin	g Maintenance Help
Monogement	Security	Access	Port Authentica	tion Traffic Con	trol Control ACL	
DHCP Snoo	ping juard	Dy	namic ARF	P Inspection	Interface Configu	ration
Dynamic Al		8.0	DAI Interfac	e Configuration	ł.	
> DAI Config	uration :	4	All		Go To Interface	00
B DAI VLAN	124		Interface	Trust Mode	Rate Limit(pps)	Burst Interval(secs)
+ DAL Universit	on					
Configuratio	der i		1/0/1	Enable	15	1
> DAI ACL		1024	10000	Disable	- Areas	

Now ARP packets from the DHCP client will go through; however ARP packets from the static client are dropped, since it does have a DHCP snooping entry. It can be overcome by static configuration as described in the following section, *Static Mapping* on page 246.

Static Mapping

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Static Mapping

1. Create an ARP ACL.

(Netgear Switch) (Config)# arp access-list ArpFilter

2. Configure the rule to allow the static client.

```
(Netgear Switch) (Config-arp-access-list)# permit ip host 192.168.10.2
  mac host 00:11:85:ee:54:e9
```

3. Configure ARP ACL used for VLAN 1.

```
(Netgear Switch) (Config)# ip arp inspection filter ArpFilter vlan 1
```

4. Now the ARP packets from the static client will go through since it has an entry in the ARP. ACL ARP packets from the DHCP client is also through since it has a DHCP snooping entry.

This command can include the optional static keyword. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings. In this example, ARP packets from the DHCP client are dropped since it does not have a matching rule, though it has a DHCP snooping entry.

Web Interface: Configure Static Mapping

- 1. Create an ARP ACL.
 - a. Select Security > Control > Dynamic ARP Inspection > DAI ACL Configuration.
 - b. In the Name field, enter ArpFilter.
 - c. Click Add.

System	Switching	Routing	Qo5	Security	Monitoring	Maintenance	Help
Management Secu	rity Access	Port Authentic	cation Traffi	e Control Car	HIGH ACL		
DHCP Snooping IP Source Guar Densmin APP	a	ynamic AP	Inspect	tion ACL Co	nfiguration		.0
DAI Configurat DAI VLAN	ion		Name	1			
Configuration > DAI Interface Configuration < CAI ACL Configuration > DAI ACL Rule			AraFilter				

- 2. Configure a rule to allow the static client.
 - a. Select Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration.
 - b. In the ACL Name list, select ArpFilter.
 - c. In the Source IP Address field, enter 192.168.10.2.
 - d. In the Source MAC Address field, enter 00:11:85:EE:54:E9.
 - e. Click Add.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
Monogement S	ecurity Access	Port Authentic	ation Traff	lic Control Co	and ACL		
DHCP Snoop	ing C	ynamic AR	P Inspec	tion ACL Ru	les Configurat	tion	
IP Source Gu	Jard	Rules					
Inspection	-	ACL Name			ArpFilter +		
DAI VLAN	ration	DAI Rule Te	ible				
> DAI Interfac	*	Source I	P Address	Source MA	C Address		
Configuratio	n:						
Configuratio	n	192.168.1	0.2	00:11:85:EF	::54:E9		
· DALACLEIA Configuration	e. 6						
* DAI Statistic	5						

- 3. Configure the ARP ACL used for VLAN 1.
 - a. Select Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration.
 - b. In the ARP ACL Name field, enter ArpFilter.
 - c. Click Apply.

A screen similar to the following displays.

System	Switch	ing	Couting	Qo5	Security	Monitoring	Maintenance	Help
Management	Security	Access F	ort Auther	ntication Traff	ic Control Con	nol ACL		
DHCP Snoo	ping	Dyn	amic A	RP Inspec	tion Configu	ration		
Dynamic Al	uaru.	V	LAN Cor	figuration				
 DAI Config DAI VLAN 	puration		VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Nam	•	latic lag
DAI Interf	ace							
Configurat	ion	10	1	Enable	Enable	ArpFilter	D	sable

DHCP Snooping

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP message and to build a bindings database of (MAC address, IP address, VLAN ID, port) tuples that are considered authorized. The network administrator enables DHCP snooping globally and on specific VLANs and configures ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.



Figure 26. DHCP Snooping

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure DHCP Snooping

1. Enable DHCP snooping globally.

(Netgear Switch) (Config)# ip dhcp snooping

2. Enable DHCP snooping in a VLAN.

(Netgear Switch) (Config)# ip dhcp snooping vlan 1

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

```
(GSM7328S) #show ip dhcp snooping binding
Total number of bindings: 1
MAC Address
                IP Address
                              VLAN Interface
                                               Туре
                                                      Lease (Secs)
                _____
                                    _____
-----
                               ____
                                               _____
                                                      _____
00:16:76:A7:88:CC 192.168.10.89
                               1
                                    1/0/2
                                               DYNAMIC 86400
```

Web Interface: Configure DHCP Snooping

- 1. Enable DHCP snooping globally:
 - a. Select Security > Control > DHCP Snooping Global Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Monogement	Security Access	Port Authentical	tion Trail	ic Control Cor	nol ACL			
-	ning (HCP Snoopi	ng Globa	al Configura	tion			
* Clobal		DHCP Snoop	ing Global	Configuration			ġ.	
* Interface		DHCP Snooping M	ode		😐 Disable 🐔	Enable		
Configurati	on	HAC Address Vab	dation		🕙 Disable 🧐	Enable		
 Binding Configuration 	on	VLAN Config	uration				đ	6
Configurati	on	VLAN ID	CONCERCISION OF	DHCP Snoop	ing Mode			
> Statistics			_					

- **b.** For DHCP Snooping Mode, select **Enable**.
- c. Click Apply.

A screen similar to the following displays:.

System S	witching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Monogement Securi	ty Access	Port Authentic	ation Tra	ffic Control Co	Hol ACL			
· DHCP Security	D	HCP Snoot	oing Glob	al Configura	tion			
Configuration	1	DHCP Snoo	ping Globa	al Configuration	1	7 (ANRA) (A	(<u>1</u>
 Interface Configuration 		DHCP Snooping HAC Address Vi	Mode alidation		 Disable Disable 	Enable Enable		
 Binding Configuration 		VLAN Confi	guration					6
 Persistent Configuration 		VLAN ID	1	DHCP Snoot	oing Mode			
> Statistics								

- 2. Enable DHCP snooping in a VLAN.
 - a. Select Security > Control > DHCP Snooping Global Configuration.

System	Switchi	ng Routing	QoS Security	Monitoring	Maintenance	Help	Index
Monogement :	Security /	Access Port Authenticatio	n Traffic Control Co	ntrol ACL			
· DHCF Snoup	ing.	DHCP Snoopine	g Global Configura	tion			
+ Ciccal		DHCP Snoopin	g Global Configuration			ğ	
* Interface		DHCP Snooping Mod	le i	🤒 Disable 🔘	Enable		
Configuration	an a	HAC Address Valida	tion	🕙 Disable 🧐	Enable		
Configuratio	80	VLAN Configur	ation			đ	6
Configuratio	an	VLAN ID	DHCP Snoop	ning Mode			1
Statistics			•				

- b. In the VLAN ID list, select 1.
- c. For DHCP Snooping Mode, select the **Enable** radio button.

System	Switching	Routing	2o5 Security	Monitoring	Maintenance	Help	Index
Monogement	Security Acces	Port Authentication	Traffic Control	ACL			
DHCP finans	pine .	DHCP Snooping	Global Configura	ition			
Cardigurate		DHCP Snooping	Global Configuration	i		00	8
» Interface		DHCP Snooping Mode	•	🔿 Disable 🔹	Enable		
> Binding	on .	MAC Address Validat	ion	🗇 Disable 🕯	Enable		
Configuration Persistent	ion	VLAN Configure	tion				2
Configuratio	ion	VLAN ID DH	CP Snooping Mode				
Statistics IP Source G	hand		•				
Dynamic AF	RP	🗐 1 En	ble				3

- d. Click Apply.
- 3. Configure the port through which DHCP server is reached as trusted.
 - a. Select Security > Control > DHCP Snooping Interface Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	
Monogement S	ecurity Access	Port Authentic	ation Traffic C	Control Control	ACE				
- DHEP Smoopl	mg C	HCP Snoop	oing Interfa	ce Configura	ation				
 Global Configuration 		DHCP Snooping Interface Configuration							
* Interface		Z All		Go To Interface	10	60		1	
* Binding Configuration	n.)	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pp	s) Burst Inter	val(secs)		
 Persistent Configuration 				•					
> Statistics	2/1 1	1/0/1	Disable	Disable	15	1			

- **b.** Select the Interface **1/0/1** check box.
- c. For Interface 1/01/, in the Trust Mode field, select Enable.
- d. Click Apply.

A screen similar to the following displays.

System	Switching	Routing	QoS S	iecurity	Monitoring A	Aaintenance Help	
Monogement	Security Acces	Port Authentic	ation Traffic Co	ontrol Contro	ACL		
DHLP Same	ping	DHCP Snoot	oing Interfac	e Configur	ation		
 Global Configurati 	Iobal DHCP Snooping Interface Configuration						
e Interface Certifiqueste	All Go To Interface					2	
 Binding Configurati Persistent 	on	Interfact	e Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)	
Configuration	on		-				
IP Source G	luard	1/0/1	Enable	Disable	15	1	
Dynamic AF	en e	1/0/2	Disable	Disable	15	14	

4. Select Security > Control > DHCP Snooping Binding Configuration.

System	Switching	Routing	QoS Security	Monitoria	ng Maintena	ince Help	
Management S	ecurity Access	Port Authentic	otion Traffic Control	Control ACL			
DHCP Snoop » Global	ng C	HCP Snoop	oing Binding Config	uration			
Configuration > Interface		Static Bindi	MAC address	VI AL	10 10 Address		
Configuration				-			
Configuratio » Persistent	•	Dynamic Bi	nding Configuration				
Configuration		Interface	MAC Address	VLAN ID	IP Address	Lease Time	
> Statistics IP Source Gi	lard	1/0/2	00:18:8B:56:FD:35	1	192.168.10.94	86394	

Enter Static Binding into the Binding Database

You can also enter the static binding into the binding database.

CLI: Enter Static Binding into the Binding Database

1. Enter the DHCP snooping static binding.

(Netgear Switch) (Config)# ip dhcp snooping binding 00:11:11:11:11:11
vlan 1 192.168.10 .1 interface 1/0/2

2. Check to make sure the binding database has the static entry.
Web Interface: Enter Static Binding into the Binding Database

1. Select Security > Control > DHCP Snooping > Binding Configuration.

A screen similar to the following displays.

Monogement Security	Access Port Auther	ticotion Troffic Co	ntrol Control	11.00		
				ACL		
OHEP Second	DHCP Sno	oping Binding (Configurat	ion		
 Global Configuration 	Static Bin	ding Configuration	n			
* Interface	Interfe	ce MAC Address	60	VLAN ID	IP Addres	ś.
Configuration	1/0/2	. 00:11:11:11:	11:11	1 -	192.168.10	1.1
Configuration	10 - 10		10			
» Persistent	Dynamic	Binding Configura	ition			
Configuration	Interface	MAC Address	VI.	LAN ID IP	Address	Lease Time
P Source Guard	1/0/2	00:18:88:56:FD:	:35 1	193	168.10.94	86394

- 2. Fill in the fields for the static binding and click **Apply**.
- **3.** Check to make sure that the binding database shows the entry in the Static Binding Configuration table.

System	Swite	hing	Routing	Qo\$	Security	Monitori	ng	Maintenan	ce Help
Management	Security	Access	Port Authenti	cation Traf	lic Control 🔞	steel ACL			
DHCP Search	ang.	DH	ICP Snoo	ping Bindi	ng Configu	ration			
 Global Configuration 	on	5	Static Bind	ing Configu	ration				
> Interface	5775 952		Interfac	e MAC Ad	Iress	VLA	N 10	IP Address	
Configurati	on			•	opcover a				
Curringen	ok.	E	1/0/2	00:11:11	11/11/11	1		192.168.10.3	1
 Persistent Configuration 	on	C	Dynamic B	inding Confi	guration				
IP Source (uard	In	terface	MAC Addr	055	VLAN ID	IP A	ddress	Lease Time
Dynamic Al Inspection	4P	1/	0/2	00:18:8B:5	6:FD:35	1	192.1	68.10.94	86210

Maximum Rate of DHCP Messages

To prevent DHCP packets being used as DoS attachments when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit, DHCP snooping brings down the interface. The user must specify "no shutdown" on this interface to further work with that port.

CLI: Configure the Maximum Rate of DHCP Messages

1. Control the maximum rate of DHCP messages.

```
(Netgear Switch) (Interface 1/0/2)# ip dhcp snooping limit rate 5
```

2. View the rate configured.

(GSM7328S)	#show ip dhcp sno	ooping interfaces	s 1/0/2
Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
1/0/2	No	5	1

Web Interface: Configure the Maximum Rate of DHCP Messages

1. Select Security > Control > DHCP Snooping > Interface Configuration.

A screen similar to the following displays:

System	Swite	hing	Routing	Qo5	security	Monitoring	Maintenance He	lρ.
Monogement	Security	Access	Port Authentica	tion Traffic C	ontrol Contr	ACL		
DHEP Sname	ping	DH	CP Snoopi	ng Interfac	e Configu	ration		
 Global Configurati 	00		HCP Snoop	ing Interface	Configuratio	n		
Configurate		. *	All		Go To Interf	ACE 0		
 Binding Configurati Persistent 	on		Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pp	s) Burst Interval(se	cs)
 Configuration Statistics 	on		1/0/2	Disable -	Disable -	5	1	
IP Source G	iuard	13	1/0/1	Enable	Disable	15	1	
Dynamic Al	UP ::	2	1/0/2	Disable	Disable	15	4	
Captive Por	tal		1/0/3	Disable	Disable	15	1	

2. Select the interface, fill in the **Rate Limit (pps)** field, and then click **Apply**. The screen shows the new rate limit for the interface.

System	Switching	N .	Routing	QoS S	ecurity	Monitoring M	aintenance Help
Management Se	curity Acc	1058	Port Authentica	tion Traffic Co	introl Contro	ACL	
Ditt.P Sanapin	G	DH	CP Snoopi	ng Interfac	e Configur	ation	
 Global Configuration 	6	-	DHCP Snoop	ing Interface	Configuration	n	14
· Interface Configuration		1	All		Go To Interfa	Ke 00	
 Binding Configuration 	E.		Interface	Trust Mode	Logging Invalid	Rate Limit(pps)	Burst Interval(secs)
 Persistent Configuration 	e.	_			Packets		
. Statistics							
IP Source Gu	ard	13	1/0/1	Enable	Disable	15	1
Dynamic ARP	10 C	1000	1 10 10	Dirable	minute		1.63

IP Source Guard

IP Source Guard uses the DHCP snooping bindings database. When IP Source Guard is enabled, the switch drops incoming packets that do not match a binding in the bindings database. IP Source Guard can be configured to enforce just the source IP address or both the source IP address and source MAC address.





The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

(Netgear Switch) (Config) # ip dhcp snooping

2. Enable DHCP snooping in a VLAN.

(Netgear Switch) (Config)# ip dhcp snooping vlan 1

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

If the entry does not exist in the DHCP Snooping Binding table, you can add it statically through the **ip verify binding** mac-address **vlan** vlan id ip address **interface** interface id command in global configuration mode.

5. Enable IP Source Guard in interface 1/0/2.

(GSM7352Sv2) (Interface 1/0/2)#ip verify source port-security

With this configuration, the device verifies both the source IP address and the source MAC address. If the port-security option is skipped, the device verifies only the source IP address.

Web Interface: Configure Dynamic ARP Inspection

- 1. Enable DHCP snooping globally.
 - a. Select Security > Control > DHCP Snooping Global Configuration.

System	Switching	Routing Qe	oS Security	Monitoring	Maintenance	Help	Index
Monogement :	Security Aco	ess Port Authentication	Traffic Control	the ACL			
· DHE F Snoup	-	DHCP Snooping	Global Configura	tion			
* Clobal		DHCP Snooping (Global Configuration			(2
* Interface		DHCP Snooping Hode		🧧 Disable 🔮	Enable		
Configuratio	ań	MAC Address Validatio	n	🕙 Disable 🦉	Enable		
 Binding Configuration 	20	VI AN Configurati	ion				8
> Persistent		YLAN ID	DHCP Snool	ning Mode			
> Statistics	an .			1966			

- **b.** For DHCP Snooping Mode, select the **Enable** radio button.
- c. Click Apply.
- **2.** Enable DHCP snooping in a VLAN.
 - a. Select Security > Control > DHCP Snooping Global Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Monogement S	Security Acces	Port Authentic	ation Tro	ffic Control Co	HILL ACT			
DHEP Shoop	100	DHCP Snoot	oing Glob	al Configura	tion			
Configuration	ni:	DHCP Snoo	ping Globa	Configuration				5
> Interface		DHCP Snooping	Mode		Oisable	Enable		
Configuration	on	HAC Address V	alidation		🗇 Disable 🏾	Enable		
Configuratio	on.							3
» Persistent		VLAN Confi	guration				12	1
Configuratio	pn (VLAN ID	DHCP Sec	oping Node				
P Statistics	1000		5	-				
Dynamic AR	P							
Inspection								
Captive Port	tal							

- **b.** In the VLAN Configuration table, in the **VLAN ID** list, select **1**.
- c. In the DHCP Snooping Mode field, select Enable.

A screen similar to the following displays.

System	Switching	Routing	Qo5	Security	Monitoring	Maintenance	Help	Index
Monogement	Security Access	Port Authentic	otion Troffi	e Control Co	dial ACL			
* DHEP Sinuag	ini) i i	DHCP Snoop	ing Globa	l Configu r a	tion			
Cardigurate	6n)	DHCP Snoo	ping Global	Configuration			10	
» Interface		DHCP Snooping	Node		🕤 Disable 🕯	Enable		
> Binding	on.:	MAC Address Va	lidation		🗇 Disable 🕯	Enable		
Configuration	on	VLAN Confi	guration					
Configuration	on	VLAN ID	DHCP Shoe	ping Mode				
 Statistics IP Source G 	uard		•					
Dynamic AP	1P	四 1	Enable					

d. Click Apply.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Monogement	Security Acce	is Port Authentic	cation Traf	fic Control Go	diol ACL			
Y DHEP Same	pinds -	DHCP Snoot	ping Glob	al Configura	tion			
· Circled	Sent C	DHCP Snot	ping Globa	I Configuration				
» Interface		DHCP Snooping	Mode		🔘 Disable 🕯	Enable		
Configurati	ion	MAC Address V	alidation		🗇 Disable 🤘	Enable		
* Binding Configurat	ion	VLAN Confi	iguration					DE .
 Persistent Configuration 	00	VLAN ID	· · · · · · · · · · · · · · · · · · ·	DHCP Snoop	ing Mode			
» Statistics		1		Enable •				
IP Source (Juard	12 12						1.1

- **3.** Configure the port through which the DHCP server is reached as trusted. Here interface 1/0/1 is trusted.
 - a. Select Security > Control > DHCP Snooping Interface Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Monogement Sec	urity Access	Port Authentic	ation Traffic C	Control Control	ACE			
DILP Superior	DI	ICP Snoop	ing Interfa	ce Configura	ation			
 Global Configuration 		DHCP Snoo	ping Interface	Configuration			Q	
* Interface	1	2 All		Go To Interface		60		
Binding Configuration	2	Interface	Trust Mode	Logging Invalid Packets	Rate Limit(p	pps) Burst Inter	rval(secs)	
» Persistent								
Chaburber	- E	1/0/1	Disable	Disable	15	1		

- **b.** Select Interface **1/0/1** check box.
- c. For interface 1/0/1, in the Trust Mode field, select Enable.
- d. Click Apply.

A screen similar to the following displays.

System	Switching	Routing	QoS S	iecurity	Monitoring	Maintenance	Help
Management S	ecurity Access	Port Authentic	ation Traffic Co	ontrol Contro	ACL		
- DHLP Sanapi		HCP Snoot	oing Interfac	e Configur	ation		
 Global Configuration 	n (DHCP Snoo	ping Interface	Configuratio	n		
Carfiguration		I AII		Go To Interf	ace (9	2	
 Binding Configuration Persistent 	n	Interface	Trust Mode	Logging Invalid	Rate Limit(pp	s) Burst Inter	val(secs)
Configuratio	R. S	200		Packets			
 Statistics IP Source Gu 	ard	1/0/1	Enable	Disable	15		
Dynamic ARI	2	1/0/2	Disable	Disable	15	12	

4. View the DHCP Snooping Binding table.

Select Security > Control > DHCP Snooping Binding Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintena	ance Help
Monogement	Security Ac	cess Port Authent	ication Traf	ic Control 🥵	ntrol ACL		
• OHCP Shop	ping	DHCP Snoo	ping Bindi	ng Configur	ation		
Configurat	ion	Static Bind	ling Configu	ration			(1)
> Interface		Interfa	e MAC Ad	Iress	VLAN I	D IP Addres	55
Configurat	ion		•		-		
Configurat	ion	Dynamic P	Linding Confi	guration			- 0
Configurat	ion	Interface	MAC Addr	gardaon	VI AN TO	IP Address	Lease Time
» Statistics IP Source (Guard	1/0/2	00:18:8B:5	6:FD:35	1 1	192.168.10.94	86394

- 5. Enable IP source guard in the interface 1/0/2.
 - a. Select Security > Control > IP Source Guard > Interface Configuration.
 - **b.** Select the Interface **1/0/2** check box.
 - c. For the IPSG mode, select Enable.
 - d. Click Apply.

System Swit	ching 1	Routing	Qo5 Sec	urity Monitori	ing Maintenance	Help
Management Security	Access F	ort Authentico	tion Traffic Contro	al Control ACL		
DHCP Snooping	IP S	Source Gu	ard Interface	Configuration		
+ Distarf eta		P Source Gu	and Interface Co	nfiguration		
 Binding 	4	All	6	o To Interface	60.0	
Configuration		Interface	IPSG Mode	IPSG P	ort Security	
Inspection					•	
Captive Portal	10	1/0/1	Disable	Disable		-

- 6. Set up IP source guard static binding.
 - a. Select Security > Control > IP Source Guard > Binding Configuration.
 - **b.** Select the Interface **1/0/2** check box.
 - c. In the MAC Address field, enter 00:05:05:05:05:05.
 - d. In the VLAN ID field, enter 1.
 - e. In the IP Address field, enter 192.168.10.80.
 - f. Click Add. A screen similar to the following displays.

System	Switch	ing F	gnituo	QoS Security	Monitor	ing Maintena	nce Help
Management	Security 1	Access P	ort Authentic	ation Traffic Control (Control ACL		
DHCP Snoo	ping	IP S	ource G	uard Binding Config	juration		
> Interface	111940 A	5	tatic Bindi	ng Configuration			
Configurati	on		Interface	MAC Address	VLAN ID	IP Address	Filter Type
	an.		· · · · ·				
Dynamic Al	uP.	四	1/0/2	00:05:05:05:05:05	1	192.168.10.80	ip
Inspection Captive Por	tal	D	ynamic Bi	nding Configuration			
		Inte	rface	MAC Address	VLAN ID	IP Address	Filter Type
		1/0/	2	00:18:88:56:FD:35	65536	192.168.10.94	(p

SNTP

Simple Network Time Protocol

This chapter includes the following sections:

- SNTP Concepts
- Show SNTP
- Configure SNTP
- Set the Time Zone
- Set the Named SNTP Server

13

SNTP Concepts

Simple Network Time Protocol (SNTP) can provide the following benefits:

- It can be used to synchronize network resources and for adaptation of NTP.
- SNTP provides synchronized network timestamp.
- It can be used in broadcast or unicast mode.
- It supports SNTP client implemented over UDP, which listens on port 123.

Show SNTP

The following are examples of the commands used in the SNTP feature. These examples are provided for thew CLI only.

show sntp

```
(Netgear Switch Routing) #show sntp?
<cr> Press Enter to execute the command.
client Display SNTP Client Information.
server Display SNTP Server Information.
```

show sntp client

```
(Netgear Switch Routing) #show sntp client
Client Supported Modes: unicast broadcast
SNTP Version: 4
Port: 123
Client Mode: unicast
Unicast Poll Interval: 6
Poll Timeout (seconds): 5
Poll Retry: 1
```

show sntp server

```
(Netgear Switch Routing) #show sntp server
                         81.169.155.234
Server IP Address:
Server Type:
                          ipv4
Server Stratum:
                          З
Server Reference Id:
                         NTP Srv: 212.186.110.32
Server Mode:
                          Server
Server Maximum Entries:
                         3
Server Current Entries:
                          1
SNTP Servers
_____
                          81.169.155.234
IP Address:
Address Type:
                          TPV4
Priority:
                           1
Version:
                           4
Port:
                           123
Last Update Time:
                         MAY 18 04:59:13 2005
Last Attempt Time:
                          MAY 18 11:59:33 2005
                          Other
Last Update Status:
Total Unicast Requests:
                          1111
Failed Unicast Requests:
                           361
```

Configure SNTP

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure SNTP

NETGEAR switches do not have a built-in real-time clock. However, it is possible to use SNTP to get the time from a public SNTP/NTP server over the Internet. You may need permission from those public time servers. The following steps configure SNTP on the switch:

1. Configure the SNTP server IP address. The IP address can be either from the public NTP server or your own. You can search the Internet to locate the public server. The servers available could be listed in domain-name format instead of address format. In that case, use the ping command on the PC to find the server's IP address. The following example configures the SNTP server IP address to 208.14.208.19.

(Netgear Switch) (Config)#sntp server 208.14.208.19

2. After configuring the IP address, enable SNTP client mode. The client mode can be either broadcast mode or unicast mode. If the NTP server is not your own, you must use unicast mode.

(Netgear Switch) (Config)#sntp client mode unicast

3. Once SNTP client mode is enabled, the client waits for the polling interval to send the query to the server. The default value is approximately 1 minute. After this period, issue the **show** command to confirm that the time has been received. The time will be used in all logging messages.

(Netgear Switch) #show sntp server	
Server IP Address:	208.14.208.19
Server Type:	ipv4
Server Stratum:	4
Server Reference Id:	NTP Srv: 208.14.208.3
Server Mode:	Server
Server Maximum Entries:	3
Server Current Entries:	1
SNTP Servers	
IP Address: 208.14.208.19	
Address Type: IPV4	
Priority: 1	
Version: 4	
Port: 123	
Last Update Time: Mar 26 03:36:09	2006
Last Attempt Time: Mar 26 03:36:09	2006
Last Update Status: Success	
Total Unicast Requests: 2	
Failed Unicast Requests: 0	

Web Interface: Configure SNTP

- 1. Configure the SNTP server.
 - a. Select System > Management > Time > SNTP Server Configuration.

System	Switchi	ing	Routing	GoS	5	ecurity	Monitor	ring	Maintenance	Help	Index
Monogement C	levice V	lew	Services 5	tocking	SNMP						
System	1	SNT	P. Server C	onfigura	ation						
witch Statistic	8	52	NTP Server C	onfigurat	ion			10	h.		
System Resour IP Configuratio	ce n		Server Type	ddress		Port	Priority	Version			
ilot Informatio	0		IPV4 ·	200.14:200	19	123	1	4			
SNTP Global Configuration		П	DNS 0	me-d.netg	ar.com	129	1	•			
Configurabile		S	NTP Server S	tatus				-9	8		
DNS Configurat	bon	Adde	***	Last Update Time	Last Attempt Time	t Attempt Statue	Requests	Failed Requests			
		time	-d.netgear.com	6	JAN 01 00:00:0 1970	Request 0 Timed Out	0	70			

- **b.** Enter the following information:
 - In the Server Type field, select IPV4.
 - In the Address field, enter 208.14.208.19.
 - In the **Port** field, enter **123**.
 - In the **Priority** field, enter **1**.
 - In the Version field, enter 4.
- c. Click Add.
- 2. Configure SNTP globally.
 - a. Select System > Management > Time > SNTP Global Configuration.

System Sw	itching Routing	QoS Sec	urity M	gnitoring	Maintenance	Help	Index
Monogement Dev	ice View Services Stocking	g SNMP					
System Information	SNTP Global Config	uration					
Switch Statistics	SNTP Global Config	uration		1	0		
System Resource	Client Hode	C Disable	@ Unicast	C Broadcast			
IP Configuration	Port	123	(1 to 65535)				
Slot Information	Unicast Poll Interval	6	(6 to 10 and	10 10 16204)			
A CITD Control	Broadcast Poll Interval	6	(6 to 10.and	16 to 16284)			
Canbour Atom	Unicast Poll Timeout	5	(1 to 30)				
⇒ SNTP Server	Unicast Poll Retry	1	(0 to 10)				
Configuration	Time Zone Name	PST					
DNS	Offset Hours	-8	(-24 to 24)				
 Host Configuration 	Offset Minutes	0	(9 to 39)				

- **b.** Enter the following information:
 - For Client Mode, Select the **Unicast** radio button.
 - In the Time Zone Name field, enter PST.
 - In the Offset Hours field, enter -8.
- c. Click Apply.

Set the Time Zone

This example is provided for the CLI only.

The SNTP/NTP server is set to Coordinated Universal Time (UTC) by default. The following example shows how to set the time zone to Pacific Standard Time (PST), which is 8 hours behind GMT/UTC.

```
(Netgear switch)(config)#clock timezone PST -8
```

Set the Named SNTP Server

The example is shown as CLI commands and as a Web interface procedure.

CLI: Set the Named SNTP Server

NETGEAR provides SNTP servers accessible by NETGEAR devices. Because NETGEAR might change IP addresses assigned to its time servers, it is best to access an SNTP server by DNS name instead of using a hard-coded IP address. The public time servers available are time-a, time-b, and time-c.

Enable a DNS name server and access a time server with the following commands:

```
(Netgear switch) (config)#ip domain-lookup
(Netgear switch) (config)#ip name-server 192.168.1.1
(Netgear switch) (config)#sntp server time-a.netgear.com
```

where 192.168.1.1 is the public network gateway IP address for your device.

This method of setting DNS name look-up can be used for any other applications that require a public IP address, for example, a RADIUS server.

Web Interface: Set the Named SNTP Server

- 1. Configure the SNTP server.
 - a. Select System > Management > Time > SNTP Server Configuration.

System 5	witching	Routin	ig Gos	5 5-6	curity	Monitor	ring	Maintenance	Help	Index
Management D	evice View	Services	Stocking	SNMP						
System Information Switch Statistic	SN	IP Server	r Configura	ation				R		
System Resource IP Configuration	n	Server Type	Address	1	Port	Priority	Version			
Slot Informatio	•	DNS .	time-f.netic	ear.cor	123	1	4			
SNTP Global		DNS	time-d.netg	sar.com 3	127	1.	4			
Configuration	5	1PV4	208.14.208	19 1	173	1	+			
DNS	1.53	SNTP Serve	r Status					Z)		
 DNS Configurat Host Configurat 	ion Ad	dress	Last Update	Last Attempt	Last Attempt Status	Requests	Failed Request			

- **b.** Enter the following information:
 - In the Server Type list, select DNS.
 - In the Address field, enter time-f.netgear.com
 - In the **Port** field, enter **123**.
 - In the **Priority** field, enter **1**.
 - In the Version field, enter 4.
- c. Click Add.
- **2.** Configure the DNS server.
 - a. Select System > Management > DNS > DNS Configuration.

System Swit	ching Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Devic	e View Services Stor	king SNA	AP				
• System	DNS Configuratio	on					
• Switch Statistics	DNS Configuratio	in			00		
System Resource IP Configuration Slot Information Time	DNS Status DNS Default Name (0 t characters)	w 255	C Disable @	Enable			
* SNTP Global Configuration	DNS Server Conf	iguration			2		
SNTP Server	Serial No		DN5 Ser	ver			
- Dris			192.168	4.4			
Host Configuration							

- **b.** Enter the following information:
 - For DNS Status, select the **Enable** radio button
 - In the DNS Server field, enter 192.168.1.1.
- c. Click Add.

Tools

14

Tools to manage, monitor, and personalize the switch and network

This chapter includes the following sections:

- Traceroute
- Configuration Scripting
- Pre-Login Banner
- Port Mirroring
- Dual Image
- Outbound Telnet

Traceroute

This section describes the traceroute feature. Use traceroute to discover routes that packets take when traveling on a hop-by-hop basis to their destination through the network.

- Traceroute maps network routes by sending packets with small time-to-live (TTL) values and watches the ICMP time-out announcements.
- The traceroute command displays all L3 devices.
- It can be used to detect issues on the network.
- Traceroute tracks up to 20 hops.
- The default UPD port is used 33343 unless you specify otherwise in the traceroute command.

The following shows an example of using the traceroute command to determine how many hops there are to the destination. The command output shows each IP address the packet passes through and how long it takes to get there. In this example, the packet takes 16 hops to reach its destination.

CLI: Traceroute

```
(Netgear Switch) #traceroute?
<ipaddr>
             Enter IP address.
(Netgear Switch) #traceroute 216.109.118.74 ?
<cr>
       Press Enter to execute the command.
<port>
             Enter port no.
(Netgear Switch) #traceroute 216.109.118.74
tracing route over a maximum of 20 hops
1 10.254.24.1
                     40 ms
                                  9 ms
                                            10 ms
2 10.254.253.1
                      30 ms
                                 49 ms
                                             21 ms
3 63.237.23.33
                      29 ms
                                 10 ms
                                             10 ms
4 63.144.4.1
                      39 ms
                                  63 ms
                                             67 ms
5 63.144.1.141
                      70 ms
                                 50 ms
                                             50 ms
6 205.171.21.89
                      39 ms
                                  70 ms
                                             50 ms
7 205.171.8.154
                      70 ms
                                  50 ms
                                             70 ms
8 205.171.8.222
                      70 ms
                                  50 ms
                                             80 ms
9 205.171.251.34
                      60 ms
                                  90 ms
                                             50 ms
10 209.244.219.181
                      60 ms
                                  70 ms
                                             70 ms
11 209.244.11.9
                       60 ms
                                  60 ms
                                             50 ms
12 4.68.121.146
                      50 ms
                                  70 ms
                                             60 ms
13 4.79.228.2
                      60 ms
                                  60 ms
                                             60 ms
14 216.115.96.185
                                             70 ms
                     110 ms
                                  59 ms
                      70 ms
15 216.109.120.203
                                  66 ms
                                             95 ms
16 216.109.118.74
                      78 ms
                                 121 ms
                                             69 ms
```

Web Interface: Traceroute

1. Select Maintenance > Troubleshooting > Traceroute.

A screen similar to the following displays.

System	Switz	hing	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	1000
Save Config	Reset	Upload	Download	File Manag	mart Troubl	mbooring)		3 		
Ping		Tracel	Route							
Concernation .		Tra	etoute				100			
		trac	crouce							
		() 3P A	abdenna	1	216.109.110.74	10				
		OW		1						
		Rest	ults				14			
		1			*					
		2	14	•	*	•				
		3	1		*					
		(4)				*				
		5	1		×.	*				
		4		-						
		7								
		4				•				
		9				*				
		10								

Use this screen to tell the switch to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Once you click the Apply button, the switch will send three traceroute packets each hop, and the results will be displayed in the result table.

- 2. In the IP Address field, enter 216.109.118.74.
- 3. Click Apply.

Configuration Scripting

This section provides the following examples:

- script on page 270
- script list and script delete on page 270
- script apply running-config.scr on page 271
- Create a Configuration Script on page 271
- Upload a Configuration Script on page 271

Configuration scripting:

- Allows you to generate text-formatted files.
- Provides scripts that can be uploaded and downloaded to the system.
- Provides flexibility to create command configuration scripts.
- Can be applied to several switches.
- Can save up to 10 scripts or 500 K of memory.
- Provides script format of one CLI command per line.

Here are some considerations:

- The total number of scripts stored is limited by the NVRAM/FLASH size.
- Application of scripts is partial if a script fails. For example, if the script executes 5 of 10 commands and the script fails, the script stops at 5.
- Scripts cannot be modified or deleted while being applied.
- Validation of scripts checks for syntax errors only. It does not validate that the script will run successfully.

script

(Netgear S	Switch) #script ?
apply	Applies configuration script to the switch.
delete	Deletes a configuration script file from the switch.
list	Lists all configuration script files present on the switch.
show	Displays the contents of configuration script.
validate	Validate the commands of configuration script.

script list and script delete

script apply running-config.scr

(Netgear Switch) #script apply running-config.scr Are you sure you want to apply the configuration script? (y/n) y The system has unsaved changes. Would you like to save them now? (y/n) y Configuration Saved!

Create a Configuration Script

```
(Netgear Switch) #show running-config running-config.scr
Config script created successfully.
(Netgear Switch) #script list
Configuration Script Name Size(Bytes)
------
running-config.scr 3201
1 configuration script(s) found.
1020799 bytes free.
```

Upload a Configuration Script

```
(Netgear Switch) #copy nvram: script running-config.scr
tftp://192.168.77.52/running-config.scr
Mode....
                             TFTP
Set TFTP Server IP.....
                             192.168.77.52
TFTP Path....
                             ./
TFTP Filename.....
                             running-config.scr
Data Type....
                            Config Script
Source Filename.....
                             running-config.scr
Are you sure you want to start? (y/n) y
File transfer operation completed successfully.
```

Pre-Login Banner

Pre-login banner:

- Allows you to create message screens that display when a user logs in to the CLI.
- By default, no banner file exists.
- You can upload or download.
- File size cannot be larger than 2 K.

The Pre-Login Banner feature is only for the CLI interface.

Create a Pre-Login Banner

This command is provided for the CLI only.

1. On your PC, using Notepad create a banner.txt file that contains the banner to be displayed.

Login Banner - Unauthorized access is punishable by law.

2. Transfer the file from the PC to the switch using TFTP.

Note: The no clibanner command removes the banner from the switch.

Port Mirroring

The port mirroring feature:

- Allows you to monitor network traffic with an external network analyzer.
- Forwards a copy of each incoming and outgoing packet to a specific port.
- Is used as a diagnostic tool, debugging feature, or means of fending off attacks.
- Assigns a specific port to copy all packets to.
- Allows inbound or outbound packets to switch to their destination and to be copied to the mirrored port.

The example is shown as CLI commands and as a Web interface procedure.

CLI: Specify the Source (Mirrored) Ports and Destination (Probe)

(Netgear Switch)#config
(Netgear Switch)(Config)#monitor session 1 mode
Enable mirror
(Netgear Switch)(Config)#monitor session 1 source interface 1/0/2
Specify the source interface.
(Netgear Switch)(Config)#monitor session 1 destination interface 1/0/3
Specify the destination interface.
(Netgear Switch)(Config)#exit
(Netgear Switch)#show monitor session 1
Session ID Admin Mode Probe Port Mirrored Port
1 Enable 1/0/3 1/0/2

Web Interface: Specify the Source (Mirrored) Ports and Destination (Probe)

1. Select Monitoring > Mirroring > Port Mirroring.

System	Swi	tching	Routing	QoS Securi	y Moni	toring	Maintenance	Help	Index
Porte Loge	1 Min	oring							
- Part Streama	9	Mul	tiple Port Mir	roring					
			Status Table						
		1	AB	Go To Interfac					
			Source Port	Destination Port	Session Hode	Mirroring Port			
			1/0/2	1/0/3	Enable 💽				
		1	1/0/1		Disable				
		2	1/0/2		Disable				
		-	1/0/3		Disable				

- 2. Scroll down and select the Source Port 1/0/2 check box. The value 1/0/2 now appears in the Interface field at the top.
- 3. Enter the following information:
 - In the **Destination Port** field, enter 1/0/3.
 - In the Session Mode field, select Enable.
- 4. Click Apply.

Dual Image

Traditionally switches contain a single image in the permanent storage. This image is loaded into memory every time there is a reboot. The dual image feature allows switches to have two images in permanent storage. You can denote one of these images as an active image that will be loaded in subsequent reboots and the other image as a backup image. This feature provides for reduced down time for the switches, when the firmware is being upgraded or downgraded.

The images are stored in the file system with the file names image1 and image2. These names are used in the CLI, Web, and SNMP interfaces. Each of the images can be associated with a textual description. The switch provides commands to associate and retrieve the text description for an image. A switch also provides commands to activate the backup image such that it is loaded in subsequent reboots. This activation command makes the current active image as the backup image for subsequent reboots.

On three successive errors executing the **active-image**, the switch attempts to execute the **backup-image**. If there are errors executing the **backup-image** as well, the bootloader will invoke the boot menu.

The Dual Image feature works seamlessly with the stacking feature. All members in the stack must be uniform in their support for the dual Image feature. The Dual Image feature works in the following way in a Stack.

- When an image is activated, the Management node notifies all the participating nodes. All nodes activate the specified image.
- When any node is unable to execute the **active-image** successfully, it attempts to execute the **backup-image**, as mentioned in the section above. Such cases will require user intervention to correct the problem, by using appropriate stacking commands.

CLI: Download a Back up an Image and Make It Active

```
(Netgear Switch) #copy tftp://192.168.0.1/gsm73xxseps.stk image2
Mode..... TFTP
Set Server IP..... 192.168.0.1
Path...../
Filename..... gsm73xxseps.stk
Data Type..... Code
Destination Filename..... image2
Management access will be blocked for the duration of the transfer Are you sure you
want to start? (y/n) y
TFTP code transfer starting
101888 bytes transferred...277504 bytes transferred...410112 bytes
transferred....628224 bytes transferred....803328 bytes transferred....978944 bytes
transferred...1154560 bytes transferred...1330176 bytes transferred...1505280 bytes
transferred...1680896 bytes transferred...1861632 bytes transferred...2040320 bytes
transferred...2215936 bytes transferred...2391040 bytes transferred...2566656 bytes
transferred...2741760 bytes transferred...2916864 bytes transferred...3092992 bytes
transferred....3268096 bytes transferred....3443712 bytes transferred....3619328 bytes
transferred...3794432 bytes transferred...3970048 bytes transferred...4145152 bytes
transferred...4320768 bytes transferred...4496384 bytes transferred...4669952 bytes
transferred...4849152 bytes transferred...5027840 bytes transferred...5202944 bytes
transferred...5378560 bytes transferred...5554176 bytes transferred...5729280 bytes
transferred...5904896 bytes transferred...6078976 bytes transferred...6255616 bytes
transferred...6423040 bytes transferred...6606336 bytes transferred...6781952 bytes
transferred...6957056 bytes transferred...7111168 bytes transferred...7307776 bytes
transferred...7483392 bytes transferred...7658496 bytes transferred...
Verifying CRC of file in Flash File System
Distributing the code to the members of the stack!
File transfer operation completed successfully.
(Netgear Switch) #
(Netgear Switch) #show bootvar
Image Descriptions
 image1 : default image
 image2 :
 Images currently available on Flash
```

	image	 1 image2	current-active	next-active
1 5.11	.2.51	8.0.0.2	imagel	image1
(Netgear	Switch)	#boot system i	lmage2	
Activati	ng image	image2		
(Netgear	Switch)	#show bootvar		
Image De	scription	ns		
imagel :	default	image		
image2 :				
Images c	urrently	available on H	flash	
unit	imagel	image2	current-active	next-active
			· · ·	
1 5.11	.2.51	8.0.0.2	image1	image2
			Image2 will k	be executed after reboot.

Web Interface: Download a Backup Image and Make It Active

- 1. Download a backup image using tftp.
 - a. Select Maintenance > Download > File Download.

System	Switch	ning	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Save Config	Reset	Upload	Download	File Manag	ement Trouble:	shooting	7 6	A	
v File Downloa	ađ	File Do	wnload						
Download		File	Download					1	
		File Typ	e			Archive			
		Image	Name		1	mage2 💌			
		Transfe	r Mode			TFTP			
		Server	Address Type			Pv4 -			
		Server	Address		1	0.100.5.17			
		Remote	File Name		n	73xxse-r8v0m0b3.s	tk		

- b. In the File Type list, select Archive.
- c. In the Image Name list, select image2.
- d. In the Transfer Mode list, select TFTP.
- e. In the Server Address Type list, select IPv4.
- f. In the Server Address field, enter 10.100.5.17(tftp server IP address).
- g. In the Remote File Name, enter gsm73xxse-r8v0m0b3.stk.
- h. Click Apply.
- **2.** Activate image2.
 - a. Select Maintenance > File Management > Dual Image Configuration.

System	Swite	ching	R	louting	QoS	Security	Monitoring	Mair	ntenance	Help	Index
Save Config	Reset	Uplo	od [Download	File Manager	nent Trouble	shooting				
Сору		Dua	Ima	ige Confi	iguration						
Eonfiguratio	n	Dual Image Configuration							(7)		
			Unit	Image Name	Active Image	Descri	ption	Version	Update Boo Code	t	
			1	image2	TRUE			8.0.0.3	Disable 💌		
			1	image1	TRUE	default	image	8.0.0.4	Disable		
		V	1	image2	FALSE		<u>ji</u>	8.0.0.3	Disable		

- **b.** Under Dual Image Configuration, scroll down and select the **Image 2** check box. The image2 now appears in the Image name field at the top.
- c. In the Active Image field, select TRUE.
- d. Click Apply.

Outbound Telnet

In this section, the following examples are provided:

- CLI: show network on page 278
- CLI: transport output telnet on page 279
- Web Interface: Configure Telnet on page 279
- CLI: Configure the session-limit and session-timeout on page 280
- Web Interface: Configure the Session Timeout on page 280

Outbound Telnet:

- Establishes an outbound Telnet connection between a device and a remote host.
- A Telnet connection is initiated, each side of the connection is assumed to originate and terminate at a network virtual terminal (NVT).
- Server and user hosts do not maintain information about the characteristics of each other's terminals and terminal handling conventions.
- Must use a valid IP address.

CLI: show network

```
(Netgear Switch Routing) >telnet 192.168.77.151
Trying 192.168.77.151...
(Netgear Switch Routing)
User:admin
Password:
(Netgear Switch Routing)
                  >en
Password:
(Netgear Switch Routing)
                  #show network
IP Address..... 192.168.77.151
Subnet Mask..... 255.255.255.0
Default Gateway...... 192.168.77.127
Locally Administered MAC Address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Network Configuration Protocol Current... DHCP
Management VLAN ID..... 1
Web Mode..... Enable
Java Mode ..... Disable
```

CLI: show telnet

(Netgear Switch Routing)#show telnet Outbound Telnet Login Timeout (minutes)...... 5 Maximum Number of Outbound Telnet Sessions..... 5 Allow New Outbound Telnet Sessions...... Yes

CLI: transport output telnet

(Netgear	Switch	Routing)	(Config)#lineconfig ?
<cr></cr>			Press Enter to execute the command.
(Netgear	Switch	Routing)	(Config)#lineconfig
(Netgear	Switch	Routing)	(Line)#transport ?
input			Displays the protocols to use to connect to a
output			Displays the protocols to use for outgoing connections from a line.
(Netgear	Switch	Routing)	(Line)#transport output ?
telnet			Allow or disallow new telnet sessions.
(Netgear	Switch	Routing)	(Line)#transport output telnet ?
<cr></cr>			Press Enter to execute the command.
(Netgear	Switch	Routing)	(Line)#transport output telnet
(Netgear	Switch	Routing)	(Line)#

Web Interface: Configure Telnet

1. Select Security > Access > Telnet.

System	Switching	Routing Qe	S Security	Monitoring	Maintenance	Help	Index	1000/
Monogement Sec	willy Acces	E Port Authentication	Treffic Control AC					
HTTP HTTPS SSH	TEL	NET Configuration	n		0			
aon Felant Console Port	Alley Sessi Haxi Curre	v new talket sessions ion Timeout mum number of session ent number of sessions	O Disable S Enable S S S	• 				
	0	utbound Teinet			(1)			
	Adm Seas Maxi Curre	in Mode ion Timeout mum number of session ent number of sessions	C Disable © Enable 5 5	minutes				
-							REFRESH CON	CEL APPLY

- 2. Under Outbound Telnet, for Admin Mode, select the Enable radio button.
- 3. Click Apply.

CLI: Configure the session-limit and session-timeout

```
(Netgear Switch Routing) (Line)#session-limit ?
<0-5> Configure the maximum number of outbound telnet sessions
allowed.
(Netgear Switch Routing) (Line)#session-limit 5
(Netgear Switch Routing) (Line)#session-timeout ?
<1-160> Enter time in minutes.
(Netgear Switch Routing) (Line)#session-timeout 15
```

Web Interface: Configure the Session Timeout

1. Select Security > Access > Telnet.

System	5witching	Routing G	205 5	iocurity	Monitoring	Maintenance	Help	Index	Lineur.)
Management Se	certly Access	Port Authentication	Troffic Co	introl ACI					
HTTP HTTPS SSH	TELM	IET Configuratio	ж			(III)			
Allow new tehet sessions Console Port Kassion Timeout Haximum number of sessions Current number of sessions		5 5	le 🛞 Enable	minutes .					
	0	atbound Telnet				10			
	Admi Sessi Maxir Curre	n Mode on Timeaut num number of sessio nt number of sessions	© Disəb 15 ms 5	ie 🛞 Enable					
							l	MHEM CORE	U. APPO

- 2. Enter the following information:
 - In the Session Timeout field, enter 15.
 - In the Maximum number of sessions field, enter 5.
- 3. Click Apply.

Syslog

System logging

This chapter includes the following sections:

- Syslog Concepts
- Show Logging
- Show Logging Buffered
- Show Logging Traplogs
- Show Logging Hosts
- Configure Logging for a Port
- Email Alerting

15

Syslog Concepts

The syslog feature:

- Allows you to store system messages and errors.
- Can store to local files on the switch or a remote server running a syslog daemon.
- Provides a method of collecting message logs from many systems.

The following illustration explains how to interpret log files.





Show Logging

The example is shown as CLI commands and as a Web interface procedure.

CLI: Show Logging

(Netgear Switch Routing) #show	loggi	ng
Logging Client Local Port	:	514
CLI Command Logging	:	disabled
Console Logging	:	disabled
Console Logging Severity Filter	:	alert
Buffered Logging	:	enabled
Syslog Logging	:	enabled
Log Messages Received	:	66
Log Messages Dropped	:	0
Log Messages Relayed	:	0
Log Messages Ignored	:	0

Web Interface: Show Logging

- **1.** Configure the syslog.
 - a. From the main menu, select **Monitoring > Logs > Sys Log Configuration**.

Buffered Logs Command Log	Syslog Configurat	ion on			a	
Console Log Configuration	Admin Status Local UDP Part	O Disable	(1.10 43333)			
Trap Logs Event Logs	Hessages Ralayed Hessages Ignored	0	3			
	Hest Configuration	i i				
	Heat Address	Status	Port (1 to 65535)	Severity Filter		
					~	

- **b.** In the Syslog Configuration, next to the Admin Status, select the **Enable** radio button.
- c. Click Apply.
- 2. Configure the command log.
 - a. Select Monitoring > Logs > Command Log.

Ports Logs Mir	todag kouning		Maintenance	Help Index	Theory
Buffered Logs	Command Log	Configuration	-0		
Console Log Configuration Style Log Configuration Trap Logs Event Logs	Admin	⊙Daable ⊙trable			
					n amr

- **b.** Under Command Log, for Admin Status, select the **Disable** radio button.
- c. Click Apply.

- **3.** Configure the console log.
 - a. Select Monitoring > Logs > Console Log.

System Sw	itching Routing	QoS Security	Monitoring	Maintenance	Help.	Index Lopour
Ports Logs Mir	roring :			17		
Buffered Logs Command Log	Console Log Con	figuration		0		
Configuration Sys Log Configuration Trap Logs Event Logs	Admin Status Severity Filter	C Daable C Enable				
			_		_	CANCEL APPLE

- **b.** Under Console Log Configuration, for Admin Status, select the **Disable** radio button.
- c. Click Apply.
- 4. Configure the buffer logs.
 - a. Select Monitoring > Logs > Buffer Logs.

System Swi	tching Routing G	loS Security	Monitoring	Maintenance	Help	Index	Luisiou
Ports Logi Min	roring		-				
Buffered Logs	Buffered Logs						
Command Log	Buffered Logs		1.07				
Console Log Configuration Sys Log Configuration Trap Logs Event Logs	Admin Status Rehavior	O Disable 🛞 Eriet Wrep 🔗	fe.				
	Message Log						
	Total number of Hessages	369 (displaying only	the last 128 messa	(jes)			
	Description						
	<14> 3an 1 02:14:37 0.0.0 371 Ne% DNS Client: Config	0-1 UtxX[774669480] ured DNS server 192.16	dra_client_tors.c() 8.10.1 unreachable	(58			
	<34> Jan 1 02:13:26 0.0.0 370 %% DNS Clant: Carfig	0-1 UNKN(774669480) ured DNS server 192.16	dna_client_turc.e() 0.10.1 unreachable	88)			
	414> Jan 1 02:12:15 0.0.0 369 Yefs DRS Client: Config	0-1 UNKN(774669400) ured DND server 192-16	dna_client_ture.c[1 8.10.1 unreachable	95)			
	-4> Jan 1 02-11-04 0.0.0.1	-1 UNIN(774669400)-	dra_allant_tors.a(2)	a)			
					CILAL	MUNER CAN	CD APPLY

- b. Under Buffer Logs, for Admin Status, select the Enable radio button.
- c. Click Apply.

Show Logging Buffered

The example is shown as CLI commands and as a Web interface procedure.

CLI: Show Logging Buffered

```
(Netgear Switch Routing) #show logging buffered ?
        Press Enter to execute the command.
<cr>
(Netgear Switch Routing) #show logging buffered
Buffered (In-Memory) Logging
                                     :
                                           enabled
Buffered Logging Wrapping Behavior
                                           On
                                   :
Buffered Log Count
                                      :
                                           66
<1> JAN 01 00:00:02 0.0.0.0-0 UNKN[268434944]: usmdb_sim.c(1205) 1 %% Error 0 (0x0)
<2> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(487) 2 %% Event
(Oxaaaaaaaa)
<6> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(531) 3 %% Starting code...
<6> JAN 01 00:00:16 0.0.0.0-3 UNKN[251627904]: cda_cnfgr.c(383) 4 %% CDA: Creating
new STK file.
<6> JAN 01 00:00:39 0.0.0.0-3 UNKN[233025712]: edb.c(360) 5 %% EDB Callback: Unit
Join: 3.
<6> JAN 01 00:00:40 0.0.0.0-3 UNKN[251627904]: sysapi.c(1864) 6 %% File
user_mgr_cfg: same version (6) but the sizes (2312->7988) differ
```

Web Interface: Show Logging Buffered

Select Monitoring > Logs > Buffer Logs. A screen similar to the following displays.

System Sw	itching Routing Q	a5 Security	Monitoring	Maintenance	Help	Index	looevt
Porte Logie Mil	roring	تعسكته					
· Buffered Logs	Buffered Logs						
Command Log	Buffered Logs			. (8)			
 Console Log Configuration Sys Log Configuration 	Admin Status Behavior	O Disable 🛞 Enab	he i				
* Trap Logs * Event Logs	Message Log			an-			
	Total number of Hessages	369 (displaying only	the last 120 messa	ges)			
	Description						
	<14> Jan 1 02:14:37 0.0.0. 371 %% DNS Client: Config.	0-1 UNKN[774669480] ired DNS server 192.16	dis_dient_txx.c(1 8.10.1 unreachable	95)			
	<14> Jan 1 02:13:26 0.0.0. 370 Yels DNB Client: Canfig	0-1 LINKN(774669480) red DNR server 192.16	ez)				
	<14> Jan 1 02:12:15 0.0.0 369 544 DBS Client: Config	0-1 UNKN(774669480)) red DNS server 192-16	93)				
	44> 3an 1 02:11:04 0.0.0.0	1 UNKN[774669400]1	dna_cliant_tons.c(19	5)			
					CIEAR	REFERENCE CANE	APPLY

Show Logging Traplogs

The example is shown as CLI commands and as a Web interface procedure.

CLI: Show Logging Traplogs

(Netgear Switch Routing)		#show logging	traplogs	?				
<pre><cr> Press Enter to exe</cr></pre>	cute the command.							
(Netgear Switch Routing)		#show logging	traplogs					
Number of Traps Since Last	Reset	6						
Trap Log Capacity								
Number of Traps Since Log	Number of Traps Since Log Last Viewed 6							
Log System Up Time	Trap							
0 0 days 00:00:46	Link Up: Unit: 3	Slot: 0 Port:	2					
1 0 days 00:01:01	Cold Start: Unit:	0						
2 0 days 00:21:33	Failed User Login	: Unit: 1 User	ID: admin					
3 0 days 18:33:31	Failed User Login	: Unit: 1 User	ID: \					
4 0 days 19:27:05	Multiple Users: U	nit: 0 Slo	t: 3 Port: 1					
5 0 days 19:29:57	Multiple Users: U	nit: 0 Slo	t: 3 Port: 1					

Web Interface: Show Logging Trap Logs

Select Monitoring > Logs > Trap Logs.

System Swi	tching	Routing C	265 Security Monitorin	Mointenance	Help	Index	100001
Ports Logs Mir	roring						
Buffered Logs Command Log Configuration Console Log Configuration Sys Log Configuration Two Logs	Tra	p Logs					
	1	rap Logs		0			
	Num Trap Num	ber of Trape Since Last Log Capacity ber of Trape Since Log I	Reat 23 256 Last Viewed 55				
	Trap Logs						
	Log	System Up Time	Тгар				
	0	0.days 01:33:44	Link Up: Unit: 0 Slot: 2 Port: 1				
	1	0 days 01:31:56	Link Up: Unit: 1 Slat: 0 Port: 7				
	2	0.days 01:31:54	Link Up: Unit: I Slot: 0 Port: I				
	3	0 days 01:31:49	Last or default VLAN deleted: VLAN	1.3			
	4	0 days 01:31:49	Last or default VLAN deleted: VLAN	11			
	5	0 days 01/31/48	Link Dawn: Unit: 1 Slot: 0 Port: 7				
			the second se				

Show Logging Hosts

The example is shown as CLI commands and as a Web interface procedure.

CLI: Show Logging Hosts

(Netgea	r Switch Routing)	#show loggin	g host	s ?
<cr></cr>		Press Enter	to exe	cute the command.
(Netgea	r Switch Routing)	#show loggin	g host	S
Index	IP Address	Severity	Port	Status
1	192.168.21.253	critical	514	Active

Web Interface: Show Logging Hosts

Select Monitoring > Logs > Sys Log Configuration.

Buffered Logs	Syslog Configuratio	0/2				
Configuration Console Log Configuration	Syslog Configuration		D			
	Admie Status	ODisabi	e 💿 Inable			
	Local UDP Port	514	(1 to 65325	0		
Configuration	Messages Relayed	0				
Trap Logs Event Logs	Messages Ignored	0				
	Host Configuration				30	
	Host Address	Status	Port (1 to 65535)	Severity Filter		
				Critical	2	
	192.168.31.533	Addivie	514	Official		

Configure Logging for a Port

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Logging for the Port

(Netgear Switch	Routing) #config
(Netgear Switch	Routing) (Config)#logging ?
buffered	Buffered (In-Memory) Logging Configuration.
cli-command	CLI Command Logging Configuration.
console	Console Logging Configuration.
host	Enter IP Address for Logging Host
syslog	Syslog Configuration.
(Netgear Switch	Routing) (Config)#logging host ?
<hostaddress></hostaddress>	Enter Logging Host IP Address
reconfigure	Logging Host Reconfiguration
remove	Logging Host Removal
(Netgear Switch	Routing) (Config)#logging host 192.168.21.253 ?
<cr></cr>	Press Enter to execute the command.
<port></port>	Enter Port Id

```
(Netgear Switch Routing) (Config) #logging host 192.168.21.253 4 ?
               Press Enter to execute the command.
<cr>
<severitylevel> Enter Logging Severity Level (emergency|0, alert|1, critical|2,
error 3, warning 4, notice 5, info 6, debug 7).
(Netgear Switch Routing) (Config) #logging host 192.168.21.253 4 1 ?
               Press Enter to execute the command.
<cr>
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1
(Netgear Switch Routing) #show logging hosts
Index
       IP Address
                       Severity Port
                                         Status
     _____ ____
1
      192.168.21.253
                     alert
                                  4 Active
```
Web Interface: Configure Logging for the Port

1. Select Monitoring > Logs > Sys Log Configuration.

A screen similar to the following displays.

Norte Logs Minoring Buffered Logs Syslog Configuration Command Log Syslog Configuration								
Buffered Logs Command Log Configuration Syslog Configuration								
			(0)					
Configuration Local UDP Port Set Log Messages Relayed Trap Logs Messages Ignored Event Logs	C Disable 🛞 Briable 514 0	(1 ta 68533)						
Host Configuration	Host Configuration							
Host Address Status	Port (1 b	Alert						
192.160.21.250 Active	+	Alert						

- 2. Enter the following information:
 - In the Host Address field, enter your host address 192.168.21.253.
 - In the **Port** field, enter **4**.
 - In the Severity Filter list, select Alert.
- 3. Click Add.

Email Alerting

Email Alerting is an extension of the logging system. The logging system allows you to configure a set of destinations for log messages. This feature adds the email configuration, through which the log message are sent to a configured SMTP server such that an administrator may receive the log in an email account of their choice.

This feature is enabled globally. When email alerting is enabled, selected log messages are sent to an SMTP server. Log messages are divided into three groups by severity level: urgent, non-urgent, and never.



Figure 29. Log message severity levels

The network administrator can adjust the urgent and non-urgent severity levels. These levels are global and apply to all destination email addresses. Log messages in the urgent group are sent immediately to the SMTP server with each log message in a separate mail. Log messages in the non-urgent group are batched into a single email message and after a configurable delay.

Email alerting also provides a configuration option that allows the network administrator to specify the severity level at which SNMP traps are logged. Using this option, the administrator can put traps in the urgent group, the non-urgent group, or the never group for emailing. Traps are not emailed by default. For traps to be emailed, the network administrator has to either increase the severity at which traps are logged, or lower the severity level of log messages that are emailed.

The network administrator can configure multiple destination email addresses, and for each email address, specify whether to deliver urgent log messages, non-urgent log messages, or both.

There is an exception to the sending of the messages periodically to the SMTP server. When the log buffer is completely full before the expiry of the periodic timer sending of the log messages to the SMTP server does not until the expiry of the timer. When the log buffer is full, a connection is opened immediately with the SMTP server, and all the messages that have not previously been emailed are sent to it.

CLI: Send Log Messages to admin@switch.com Using Account aaaa@netgear.com

1. Configure an SMTP server, for example, smtp.netgear.com. Before you configure the SMTP server, you need to have an account on SMTP server.

```
(Netgear Switch) (Config)#mail-server "smtp.netgear.com" port 465
(Netgear Switch) (Mail-Server)#security tlsv1
(Netgear Switch) (Mail-Server)# username aaaa
(Netgear Switch) (Mail-Server)# password xxxxxx
(Netgear Switch) (Mail-Server)#exit
```

2. Configure logging mail. From-addr is the source address of email and to-addr is the destination address of email.

(Netgear Switch) (Config)#logging email (Netgear Switch) (Config)#logging email from-addr aaaa@netgear.com (Netgear Switch) (Config)#logging email message-type urgent to-addr admin@switch.com (Netgear Switch) (Config)#logging email message-type non-urgent to-addr admin@switch.com

3. Increase the severity of traps to 3 (error). By default, it is 6 (informational).

(Netgear Switch) (Config)#logging traps 3

SNMP

Simple Network Management Protocol

16

This chapter includes the following sections:

- Add a New Community
- Enable SNMP Trap
- SNMPv3
- sFlow
- Time-Based Sampling of Counters with sFlow

Add a New Community

The example is shown as CLI commands and as a Web interface procedure.

CLI: Add a New Community

```
(Netgear switch) #config
(Netgear switch) (Config)#snmp-server community rw public@4
```

Web Interface: Add a New Community

1. Select System > SNMP > SNMP V1/V2 > Community Configuration. A screen similar to the following displays.

System S	witching	Routing (20S Security	Monitoring	Maintenan	ce Help	Inde				
Monogement D	evice View	View Services Stacking SNMP									
soore V1/V2 * Convenientler Configuration	Co	Community Configuration									
Trap Configurat Trap Flags	ion	Community Name	Client Address	Client IP Mask	Access Mode	Status					
· Sopported MIES		public@4	0.0.0.0	0.0.0.0	Read/Vite 💌	Enable 💌					
South An	- 6	public	0.0.0.0	0.0.0.0	ReadOnly	Enable					
	E.	private	0.0.0.0	0.0.0.0	ReadWrite	Enable					
		public@1	0.0.0.0	0.0.0.0	ReadOnly	tnable					
		public@2	0.0.0	0.0.6.6	ReadOnly	Enable					
		publicgra	0.0.0.0	0.0.0.0	ReadOnly	Enable					

- 2. In the Community Name field, enter public@4.
- 3. In the Client Address field, enter 0.0.0.0.
- 4. In the Client IP Mask field, enter 0.0.0.0.
- 5. In the Access Mode field, select Read/Write.
- 6. In the Status field, select Enable.
- 7. Click Add.

Enable SNMP Trap

The example is shown as CLI commands and as a Web interface procedure.

CLI: Enable SNMP Trap

This example shows how to send SNMP trap to the SNMP server.

Web Interface: Enable SNMP Trap

- 1. Enable SNMP trap for the server 10.100.5.17.
 - a. Select System > SNMP > SNMP V1/V2 > Trap Configuration. A screen similar to the following displays.



- b. In the Community Name field, enter public.
- c. In the Version list, select SNMPv1.
- d. In the Address field, enter 10.100.5.17.
- e. In the Status field, select Enable.
- f. Click the Add button.
- 2. Set the Link Up/Down flag.

a. Select System > SNMP > SNMP V1/V2 > Trap Flags. A screen similar to the following displays.

System Swi	tching Routing	Qo5 Se	curity	Monitoring	Maintenance	Help	Index
Monogement Devi	ce View / Services 5k	cking SNMP					
SHIP V1/V2-	Trap Flags						
Configuration	Trap Flags				3		
Trap Configuration	Authentication	C Disable	(R Enable				
a Train Plaga	Link Up/Down	C Disable	Enable Enable				
> Supported MIBS SNNP V3	Hultiple Users	C Disable	& Enable				
	Spanning Tree	C Disable	€ Enable				
	OSPF Trape	(Disable	C Enable				

- **b.** For Link Up/Down, select the **Enable** radio button.
- c. Click Apply.

SNMPv3

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure SNMPv3

```
(Netgear Switch) #config
(Netgear Switch) (Config)#users passwd admin
Enter old password:
Enter new password:12345678
Confirm new password:12345678
Password Changed!
change the password to "12345678"
(Netgear Switch) (Config)#users snmpv3 authentication admin md5
Set the authentication mode to md5
(Netgear Switch) (Config)#users snmpv3 encryption admin des 12345678
Set the encryption mode to des and the key is "12345678"
```

Web Interface: Configure SNMPv3

1. Change the user password.

If you set the authentication mode to MD5, you must make the length of password longer than 8 characters.

a. Select Security > Management Security > User Configuration > User Management. A screen similar to the following displays.



- **b.** Under User Management, scroll down and select the User Name **admin** check box. Now admin appears in the User Name field at the top.
- c. In the Password field, enter 12345678.
- d. In the Confirm Password field, enter 12345678.
- e. Click Apply to save the settings.
- **2.** Configure the SNMP V3 user.
 - a. Select System > Management > User Configuration. A screen similar to the following displays.

System 5w Management Dev	itching Routing C Ice View Services Stocking	DoS Security	Monitoring	Maintenance	Help	Index
 SNHP V1/V2 SNHP V3 User Carificantion 	SNMP V3 User Confi User User Name admin •	iguration		2		
	SNMP v3 Access Mode Authentication Protocol Encryption Protocol Encryption Key	Read/Write C None @ MDS C None @ DES	() SHA			

- b. In the User Name field, select the admin.
- c. For Authentication Protocol, select the MD5 radio button.
- **d.** For Encryption Protocol, select the **DES** radio button.
- e. In the Encryption Key field, enter 12345678.
- f. Click Apply to save the settings.

sFlow

sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

The sFlow monitoring system consists of an sFlow agent (embedded in a switch or router or in a standalone probe) and a central sFlow collector. The sFlow agent uses sampling

technology to capture traffic statistics from the device it is monitoring. The sFlow datagrams are used to immediately forward the sampled traffic statistics to an sFlow collector for analysis.

The sFlow agent uses two forms of sampling: statistical packet-based sampling of switched or routed packet flows, and time-based sampling of counters.



Figure 30. sFlow

CLI: Configure Statistical Packet-Based Sampling of Packet Flows with sFlow

1. Configure the sFlow receiver (sFlow collector) IP address. In this example, sFlow samples will be sent to the destination address 192.168.10.2.

(Netgear Switch) (Config)# sflow receiver 1 ip 192.168.10.2

2. Configure the sFlow receiver timeout. Here sFlow samples will be sent to this receiver for the duration of 31536000 seconds. That is approximately 1 year.

(Netgear Switch) (Config) # sflow receiver 1 owner NetMonitor timeout 31536000

3. Here the default maximum datagram size is 1400. It can be modified to a value between 200 and 9116 using the command sflow receiver 1 maxdatagram <size>.

```
(GSM7328S) #show sflow receivers
Receiver Owner Time out Max Datagram Port IP Address
Index String
                     Size
_____ ____
           NetMonit 31535988 1400
                                   6343 192.168.10.2
     1
                                 63430.0.0.063430.0.0.063430.0.0.063430.0.0.0
     2
                 0
                        1400
                         1400
1400
1400
1400
1400
1400
                  0
     3
     4
                  0
     5
                  0
                                   63430.0.0.063430.0.0.0
                  0
     6
     7
                  0
                  0
                                   6343 0.0.0.0
     8
(GSM7328S) #
```

4. Configure the sampling port sFlow receiver index, sampling rate, and sampling maximum header size. You need to repeat these for all the ports to be sampled.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# sflow sampler 1
(Netgear Switch) (Interface 1/0/1)# sflow sampler rate 1024
(Netgear Switch) (Interface 1/0/1)# sflow sampler maxheadersize 64
```

5. View the sampling port configurations.

(GSM7328S) #show s	flow samplers		
Sampler	Receiver	Packet	Max Header
Data Source	Index	Sampling Rate	Size
1/0/1	1	1024	64

Web Interface: Configure Statistical Packet-based Sampling with sFlow

- 1. Configure the sFlow receiver IP address.
 - a. Select Monitoring > sFlow > Advanced > sFlow Receiver Configuration.
 - b. Select the 1 check box.
 - c. In the Receiver Owner field, enter NetMonitor.
 - d. In the Receiver Timeout field, enter 31536000.

e. In the **Receiver Address** field, enter **192.168.10.2**. A screen similar to the following displays.

System 5	witching	Routi	ng	QoS Secur	ity Monitoring	Maintenance H	elp Index					
Ports Logs A	Nirroring	sflow										
Basic		sFlow F	teceiv	er Configuratio	n							
+ sFlow Agent		sFlow Receiver Configuration										
• sitter Galarier Geofesitetier		Rei	ceiver lex	Receiver Owner	Receiver	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version			
 sFlow Interface Configuration 		1		NetMonitor	31536000	1400	192.168.10.2	6545	5			
	_	12 1			0	1400	0.0.0.0	6343	5			
		F 2			0	1400	0.0.0.0	6343	5			

f. Click Apply. A screen similar to the following displays.

System	Switching	1	Routing	QoS Securi	ty Monitoring	Maintenance	Help Index		
Ports Logs	Mirroring	sHow							
Basic		sFlo	w Receiv	ver Configuration	1				
= sFlow Agent		5	Flow Recei	ver Configuration					Q
Conformation			Receiver Index	Receiver Owner	Receiver	Haximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
 show Interfact Configuration 									
	-	- E1	1	NetMonitor	31535999	1400	192.168.10.2	6343	5
		門	2		0	1400	0.0.0.0	6343	5

- 2. Configure the sampling ports sFlow receiver index, sampling rate, and sampling maximum header size.
 - a. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuration**. A screen similar to the following displays.

System Swite	thing	Routing	Qo5 Secu	rity Monitoring	Maintenance h	telp Index	
Ports Logs Mirro	ring sHow	í –					
Basic	sFl	ow Interfa	ice Configurati	ion			
Advisored • sFlow Agent • sFlow Receiver Configuration Configuration		sFlow Interf	ace Configuration				
	1	All		6	o To Interface	00	
				Poller		Sampler	
	1	Interface	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
		1/0/1	0	0	1	1024	64
	10	1/0/1	0	0	0	G	128

- **b.** Select the Interface **1/0/1** check box.
- c. In the Sampling Rate field, enter 1024.
- d. In the Maximum Header Size field, enter 64.
- e. Click Apply. A screen similar to the following displays.

System Swite	hing J	Routing	QoS Security	Monitoring	Maintenance H	ielp Index	
Ports Logs Mirroring Basic Advanced + sFlow Agent + sFlow Receiver	sFlo	w Interfa Flow Interfa	ce Configuration	6	o To Interface	1 (co.)	
- office provides	1			Poller		1	
Configuration		Interface	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Haximum Header Size

Time-Based Sampling of Counters with sFlow

CLI: Configure Time-Based Sampling of Counters with sFlow

1. Configure the sampling port sFlow receiver index, and polling interval. You need to repeat this for all the ports to be polled.

(Netgear Switch) (Config)# interface 1/0/1 (Netgear Switch) (Interface 1/0/1)# sflow poller 1 (Netgear Switch) (Interface 1/0/1)# sflow poller interval 300

2. View the polling port configurations.

(GSM7328S) #show	sflow pollers	
Poller	Receiver	Poller
Data Source	Index	Interval
1/0/1	1	300

Web Interface: Configure Time-Based Sampling of Counters with sFlow

Configure the sampling ports sFlow receiver index, and polling interval:

- 3. Select Monitoring > sFlow > Advanced > sFlow Interface Configuration.
- 4. Select the Interface 1/0/1 check box.
- 5. In the Poller Interval field, enter 300.

A screen similar to the following displays.

System	Switching	, P	louting	QoS Secu	mity Monitoring	Maintenance	Help Index				
Ports Logs	Mirroring	sRow									
Basic	1	sFlo	w Interfa	ce Configurat	ion						
sFlow Agent		: 51	How Interfa	ce Configuration	6						
 sflow Receiver Configuration 	n .		All			Go To Interface					
- pillow Scientise					Poller		Sampler				
Cantigoration			Interface	Receiver Index	Poller Interval	Receiver	Sampling Rate	Maximum Header Size			
				1							
		0	1/0/1	1	300	1	1024	64			
		121	1/0/2	0	0	0	0	128			

6. Click Apply.

DNS

Domain Name System

This chapter includes the following sections:

- DNS Concepts
- Specify Two DNS Servers
- Manually Add a Host Name and an IP Address

17

DNS Concepts

This section describes the Domain Name System (DNS) feature. The DNS protocol maps a host name to an IP address, allowing you to replace the IP address with the host name for IP commands such as a ping and a traceroute, and for features such as RADIUS, DHCP relay, SNTP, SNMP, TFTP, SYSLOG, and UDP relay.

You can obtain the DNS server IP address from your ISP or public DNS server list. DNS is used to resolve the host's IP address. It enables a static host name entry to be used to resolve the IP address. The following are examples of how the DNS feature is used.

Specify Two DNS Servers

The following example shows how to specify two DNS servers (that is, two IP addresses for DNS servers) and to resolve an IP address using the DNS server. The example is shown as CLI commands and as a Web interface procedure.

CLI: Specify Two DNS Servers

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip name-server 12.7.210.170 219.141.140.10
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#exit
(Netgear Switch)#ping www.netgear.com
Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface: Specify Two DNS Servers

1. Select System > Management > DNS > DNS Configuration.

A screen similar to the following displays.

System Sv	vitching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index	100001
Management De	vice View	Services Sto	cking SN/	MP					
System Information Switch Statistics	DNS	Configuration	n			2)			
 System Resource IP Configuration Slot Information Time 	DNS S DNS D charae	tatus lefault Name (0 to cters)	255	O Disable 🕥					
Y DNS	DN	IS Server Confi	guration			0			
Configuration		Serial No		DNS Ser	/er				
Configuration		1		12.7.210.	170				
		2		219.141.1	40.10				
	<								18
						5_A	DD DEU	TE CANCEL	APPLY

- 2. Under DNS Server Configuration, in the DNS Server field, enter 12.7.210.170.
- 3. Click Add.
- 4. In the DNS Server field, enter 219.141.140.10.
- 5. Click Add.

Both DNS servers now show in the DNS Server Configuration table.

Manually Add a Host Name and an IP Address

The following example shows commands to add a static host name entry to the switch so that you can use this entry to resolve the IP address. The example is shown as CLI commands and as a Web interface procedure.

CLI: Manually Add a Host Name and an IP Address

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip host www.netgear.com 206.82.202.46
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#ping www.netgear.com
Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface: Manually Add a Host Name and an IP Address

1. Select System > Management > DNS > Host Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenanc
Monogement	Device View	Services Sta	cking SNN	AP		
System	1	DNS Hos	st Configu	ration		
Information Switch Statis	stics	DNS H	ost Configur	ration		(7)
System	April 6	Host	Name (1-158	characters)	IP Address	
Resource IP Configura	tion					
Slot Informa	ition	- www.	netgear.com		206.82.202.46	
Time DNS						
DNS		Dynam	ic Host Map	ping		0
Configuratio	n	Host Tota	al Elapsed		Туре	Addresses
# Host						

- 2. Under DNS Host Configuration, enter the following information:
 - In the Host Name field, enter www.netgear.com.
 - In the IP Address field, enter 206.82.202.46.
- 3. Click Add.

The host name and IP address now show in the DNS Host Configuration table.

DHCP Server

Dynamic Host Configuration Protocol Server

18

This chapter includes the following sections:

- DHCP Server Concepts
- Configure a DHCP Server in Dynamic Mode
- Configure a DHCP Server that Assigns a Fixed IP Address

DHCP Server Concepts

When a client sends a request to a DHCP server, the DHCP server assigns the IP address from address pools that are specified on the switch. The network in the DHCP pool must belong to the same subnet.

DHCP server allows the switch to dynamically assign an IP address to a DHCP client that is attached to the switch. It also enables the IP address to be assigned based on the client's MAC address. The following are examples of how the DHCP Server feature is used.

Configure a DHCP Server in Dynamic Mode

The following example shows how to create a DHCP server with a dynamic pool. The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure a DHCP Server in Dynamic Mode

(Netgear	Switch)	#vlan database
(Netgear	Switch)	(Vlan)#vlan 200
(Netgear	Switch)	(Vlan)#vlan routing 200
(Netgear	Switch)	(Vlan)#exit
(Netgear	Switch)	(Config)#interface 1/0/1
(Netgear	Switch)	(Interface 1/0/1)#vlan participation include 200
(Netgear	Switch)	(Interface 1/0/1)#vlan pvid 200
(Netgear	Switch)	(Interface 1/0/1)#exit
(Netgear	Switch)	(Config)#interface vlan 200
(Netgear	Switch)	(Interface-vlan 200)#routing
(Netgear	Switch)	(Interface-vlan 200)#ip address 192.168.100.1 255.255.255.0
(Netgear	Switch)	#config
(Netgear	Switch)	(Config)#service dhcp
(Netgear	Switch)	(Config)#ip dhcp pool pool_dynamic
(Netgear	Switch)	(Config)#network 192.168.100.0 255.255.255.0

Note: If there is no DHCP L3 relay between client PC and DHCP server, there must be an active route whose subnet is the same as the DHCP dynamic pool's subnet.

Web Interface: Configure a DHCP Server in Dynamic Mode

- 1. Create VLAN 200.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Inde
VUAN STP	Melticost Ac	Idress Toble	Ports LAG					
- Dash	VLAN	Configura	tion					
TIDAN	Res	et					10	
Advanced	Reset	Configuration			E			
	Inte	ernal VLAN C	onfiguration				(9)	
	Intern	al VLAN Alloca	Son Vare		4093			
	Intern	al VLAN Alloca	tion Policy		C Ascending @ D	escending		
	VU	AN Configura	tion				(1)	
	v	LAN ID YEAP	N Name		LAN Type	Make Static		
		00				Disable 👱	,	
	F 1	Defa	ult	D	efault	Disable		

- b. Under VLAN Configuration, in the VLAN ID field, enter 200.
- c. Click Add.
- 2. Add port 1/0/1 to VLAN 200.
 - a. Select Switching > VLAN >Advanced > VLAN Membership.

A screen similar to the following displays.

System Sy	witching		Ro	outin	g	8	QoS	1	S	ecui	rity		N	loni	tori	ng		Mo	inten	anc	е		Help
TAN STP M	ulticast	Add	ress	Table		Ports	L	١G															
isic	VLA	NN	/ler	nbe	ersh	ip																	
dvanced VLAN	v	LAN	I Me	mbe	ershi	p																	۲
Configuration	VLA	N ID	<u>.</u>		2	00	-							Gro	oup (Jper	atio	n	Unt	ag A	H) —	-	
VLAN Membershi	VLA	N Na	me											U	NTAG	GED	POR	T ME	ABERS				
VLAN Status	VLA	N Ty	pe		5	Statio	Ċ.								TAG	GED F	PORT	MEM	BERS				
Configuration	*	Unit	E 1																				
MAC Based VLAN	Port	1	2	3	4 !	56	57	8	9	10	11	12	13	14	15	16	17	18	19 20	21	22	23	24
IP Subnet Based		U																					
VLAN	-	25	26	27	28 2	29 3	30 3	32	33	34	35	36	37	38	39	40	41	42	13 44	45	46	47	48
Port DVLAN Configuration		49	50	51	52		_												11.5				
Protocol Bacad				· ····																			7

- b. In the VLAN ID field, select 200.
- c. Click Unit 1. The ports display.
- d. Click the gray boxes under ports 1 and 24 until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply.
- 3. Assign PVID to the VLAN 200.
 - a. Select Switching > VLAN> Advanced > Port PVID Configuration.

A screen similar to the following displays.

System S	witching	Routi	ng (QoS Security	Monitoring	Maintenance	Help	Index
VLAN STP A	Aulticast 🕴	Address Tab	le Ports	LAG				
Basic	Por	t PVID C	onfigura	ation				
Advanced	(1)	VID Config	juration				1	
» VLAN Configuration	1	All		Go To Interface	GO			
 » VLAN Membersh » VLAN Status 	ip	Interface	PVID	Acceptable Frame Types	Ingress Filtering	Port Priori	ty	
> Port PVID		1/0/1	200	Admit All	Disable 💌	0		
Configuration		1/0/1	1	Admit All	Disable	0		
» IP Subnet Based		1/0/2	1	Admit All	Disable	0		
VLAN		1/0/3	1	Admit All	Disable	0		
» Port DVLAN		1/0/4	1	Admit All	Disable	0		
Configuration		1/0/5	1	Admit All	Disable	0		

- **b.** Under Port PVID Configuration, scroll down and select the **1/0/1** check box.
- c. In the PVID (1 to 4093) field, enter 200.
- d. Click Apply to save the settings.
- 4. Create a new DHCP pool.
 - a. Select System > Services > DHCP Server > DHCP Server Configuration.

A screen similar to the following displays.

System S	witching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management D	evice View	Services Stac	king SN/	AP LLDP I	SDP			
· DHEP Server	DHCP	Server Co	nfiguratio	on				
» DHCP Server	DH	CP Server Co	nfiguration				(7)	
» DHCP Pool	Admin	Mode			O Disable 🕑 Enab	le		
Configuration	Ping P	acket Count			2	(0, 2 to 10)		
» DHCP Pool Optic	ons Conflic	t Logging Mode			C Disable 🖲 Enab	le		
» DHCP Server Statistics	Bootp	Automatic Mode	B		Oisable C Enable	le		
» DHCP Bindings	Exc	luded Addres	s				1	
» DHCP Conflicts	10	PRange From	IP	Range To				
Information								

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply to enable the DHCP service.
- d. Select System > Services > DHCP Server > DHCP Pool Configuration.

A screen similar to the following displays.

System Swit	ching Routing QoS	Security	Monitoring	Maintenance	Help	Index
Management Devic	e View Services Stacking S	NMP LLDP ISD	P	10		
DHCP Server	DHCP Pool Configuration	on				
» DHCP Server	DHCP Pool Configuration				(7)	
> DHCP Pool	Pool Name	Create 💌	1			
Configuration	Pool Name	pool_dyna	mic (1 t	o 31 Alphanumeric Cha	racters)	
» DHCP Pool Options	Type of Binding	Dynamic				
» DHCP Server	Network Address	192.168.10	0.0			
Statistics	Network Mask	255.255.25	5.0			
» DHCP Bindings	Network Prefix Length		(0 t	o 32)		
» DHCP Conflicts	Client Name					
Information	Hardware Address	00:00:00:0	00:00:00			
DHCP Relay	Hardware Address Type	Ethernet	*			
DHCP L2 Relay	Client ID					
UDP Relay	Host Number	0.0.0.0				
DHCPv6 Server	Host Mask	0.0.0.0				
DHLPV6 Relay	Host Prefix Length		(8 t	o 32)		

- e. Under DHCP Pool Configuration, enter the following information:
 - In the **Pool Name** list, select **Create**.
 - In the **Pool Name** field, enter **pool_dynamic**.
 - In the Type of Binding list, select Dynamic.
 - In the Network Number field, enter 192.168.100.0.
 - In the Network Mask field, enter 255.255.255.0. As an alternate, you can enter 24 in the Network Prefix Length field. Do not fill in both the Network Mask field and Network Prefix Length fields.
 - In the **Days** field, enter **1**.
- f. Click Add.

The pool_dynamic name is now added to the Pool Name drop-down list.

Configure a DHCP Server that Assigns a Fixed IP Address

The following example shows how to set up a DHCP server with an IP address pool and let the DHCP server assign a fixed IP address based on a MAC address. The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure a DHCP Server that a Assigns Fixed IP Address

(Netgear	Switch)	tconfig
(Netgear	Switch)	(Config)#service dhcp
(Netgear	Switch)	(Config)#ip dhcp pool pool_manual
(Netgear	Switch)	(Config)#client-name dhcpclient
(Netgear	Switch)	(Config)#hardware-address 00:01:02:03:04:05
(Netgear	Switch)	(Config)#host 192.168.200.1 255.255.255.0
(Netgear	Switch)	(Config)#client-identifier 01:00:01:02:03:04:05

Note: The unique identifier is a concatenation of the media type and MAC addresses. For example, the Microsoft client identifier for Ethernet address c8:19:24:88:f1:77 is 01:c8:19:24:88:f1:77, where 01 represents the Ethernet media type. For more information, see the "Address Resolution Protocol Parameters" section of RFC 1700.

Web Interface: Configure a DHCP Server that Assigns a Fixed IP Address

1. Select System > Services > DHCP Server > DHCP Server Configuration.

A screen similar to the following displays.

Switching	Routing	QoS	Security	Monitor	ring N	laintenanc
Device View	Services Stackin	g SNMP				
er ver	DHCP Serv	er Config ver Configu	uration ration			۲
Configuration Options ver Statistics lings n flicts	Admin Mode Ping Packet Co Conflict Loggir Bootp Automa	ount ng Mode ntic Mode	 ○ Disable 2 ○ Disable ③ Disable 	⊙ Enable ⊙ Enable ○ Enable	(0, 2 to 10)	
n	Excluded	Addresses e From		IP Range T	0	(3)
	Switching Dovice View Configuration Options ver Statistics lings n flicts n	Switching Routing Device View Services Stockin DHCP Services DHCP Servic	Switching Routing QoS Dovice View Services Stocking SNMP DHCP Server Config DHCP Server Config Options DHCP Server Config Ver Statistics DHCP Server Config Ings DHCP Server Config Dhcp Server Config DHCP Server Config Statistics DHCP Server Config Dhcp Server Config DHCP Server Config Description Statistics Dhcp Server Config DHCP Server Config Dhcp Server Config DHCP Server Config Dhcp Server Config DHCP Server Config Description Statistics Dhcp Server Config DHCP Server Config Description Statistics Description Statistics	Switching Routing QoS Security Device View Services Stocking SNMP DHCP Server Configuration DHCP Server Configuration Configuration DHCP Server Configuration Options DHCP Server Configuration Admin Mode Disable Ping Packet Count 2 Conflict Logging Mode Disable Bootp Automatic Mode Disable Excluded Addresses 1P Range From	Switching Routing QoS Security Monitor Dovice View Services Stacking SNMP DHCP Server Configuration DHCP Server Configuration Configuration DHCP Server Configuration Options Admin Mode Disable Ping Packet Count 2 Conflict Logging Mode Disable Enable Bootp Automatic Mode Disable Enable IP Range From IP Range T	Switching Routing QoS Security Monitoring N Device View Services Stocking SNMP DHCP Server Configuration DHCP Server Configuration Configuration DHCP Server Configuration Options DHCP Server Configuration Image: Statistics Object Image: Statistics Object Image: Statistics Disable Im

- 2. For Admin Mode, select the Enable radio button.
- 3. Click Apply to enable the DHCP service.
- 4. Select System > Services > DHCP Server > DHCP Pool Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Management	Device View	Services Stat	king SNA	AP		
DHCP Serve » DHCP Serve Configurati	er on	DHCP Po	ol Config	uration uration		0
> DHCP Pool > DHCP Pool	Configuration Options	Pool Name Pool Name			pool_manual 💌	
 » DHCP Serv » DHCP Bind Information » DHCP Conf Information 	er Statistics ings i licts	Type of Bin Network Nu Network Ma	ding mber isk		Manual 💌]
DHCP Relay UDP Relay		Client Name Hardware A	enx cengur address		dhcpclient 00:01:02:03:04:05]
		Hardware A Client ID	ddress Type		ethernet 🔽	1
		Host Numbe Host Mask	ar		192.168.200.1 255.255.255.0	
		Host Prefix Lease Time	Length		Specified Duration 💌	(0-32)
		Days Hours			1	(0 to 59) (0 to 1439)
		Minutes			0	(0 to 86399)

- **5.** Under DHCP Pool Configuration, enter the following information:
 - In the **Pool Name** list, select **Create**.
 - In the **Pool Name** field, enter **pool_manual**.
 - In the Type of Binding list, select Manual.
 - In the Client Name field, enter dhcpclient.
 - In the Hardware Address field, enter 00:01:02:03:04:05.
 - In the Hardware Type list, select ethernet.
 - In the Host Number field, enter 192.168.200.1.
 - In the **Network Mask** field, enter **255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field.
 - In the **Days** field, enter **1**.
- 6. Click Add. The pool_manual name is now added to the Pool Name drop-down list.

DVLANs and Private VLANs



Double VLANS and private VLAN groups

This chapter includes the following sections:

- Double VLANs
- Private VLAN Groups on page 316

Double VLANs

This section describes how to enable the double DVLAN feature. Double VLANs pass traffic from one customer domain to another through the metro core. Custom VLAN IDs are preserved and a provider service VLAN ID is added to the traffic so the traffic can pass the metro core in a simple and cost-effective manner. You can use VLANs to specify customer ports and a service provider port. In this example, the switches have the same configuration.



Figure 31. Double VLANS

The following example shows how to configure the NETGEAR switch shown in the preceding figure to add a double VLAN tag for traffic going from the subnet domain connected to port 1/0/24. This example assumes there is a Layer 2 switch connecting all these devices in your domain. The Layer 2 switch tags the packet going to the NETGEAR switch port 1/0/24. The example is shown as CLI commands and as a Web interface procedure.

CLI: Enable a Double VLAN

```
Create a VLAN 200.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit
Add interface 1/0/24 to VLAN 200, add pvid 200 to port.
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24) #vlan pvid 200
(Netgear Switch) (Interface 1/0/24)#vlan participation include 200
(Netgear Switch) (Interface 1/0/24)#exit
Add interface 1/0/48 to the VLAN 200 in a tagging mode.
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#vlan tagging 200
(Netgear Switch) (Interface 1/0/48)#exit
Select interface 1/0/48 as the provider port.
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#mode dvlan-tunnel
(Netgear Switch) (Interface 1/0/48)#exit
```

Web Interface: Enable a Double VLAN

- 1. Create static VLAN 200:
 - Select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays.

Switching	Routing	QoS	Security	Monitoring	Maintenance
Multicost A	ddress Table F	orts LAG			
	VLAN Co	nfiguratio	on		
	Reset				Û
	Reset Confi	guration			
	1				4.
	VLAN C	onfiguratio	n		
	VLAN	ID	VLAN Name		VLAN Type
	200		vlan200		Static 🔽
	1		Default		Default
	100				Static
	Switching Multicost Ar	Switching Routing Multicost Address Toble P VLAN Co Reset Reset Confi VLAN C VLAN C VLAN C 1 200 1	Switching Routing QoS Multicost Address Table Ports LAG VLAN Configuration Reset Reset Configuration VLAN Configuration VLAN 1D 200 1 1	Switching Routing QoS Security Multicost Address Table Ports LAG VLAN Configuration Reset Reset Reset Configuration VLAN Configuration VLAN Configuration VLAN Name 200 VIAN Name 1 Default	Switching Routing QoS Security Monitoring Multicost Address Table Ports LAG VLAN Configuration Reset Reset VLAN Configuration Image: Configuration Image: Configuration VLAN Configuration Image: Configuration Image: Configuration VLAN 1D VLAN Name Image: Configuration Image: Configuration Image: Configuration Image: Configuration

- **b.** Under VLAN Configuration, enter the following information:
 - In the VLAN ID field, enter 200.
 - In the VLAN Name field, enter vlan200.
 - In the VLAN Type field, select Static.
- c. Click Add.
- 2. Add ports 24 and 48 to VLAN 200.
 - a. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays.

System	Switc	hing		Ro	uti	ng	T	Q	oS	Υ	S	ocur	ity	T	N	Noni	tori	ng	Ĩ	Ν	lain	ten	ance	ġ		Help
VLAN STP	Multic	ast .	Add	ross	Tob		Por	ts	LA	G																
Basic Advanced		VLA	NI	Me	eml	bers	ship hip	>																		Ð
Configuratio	on	VLA	N 10)			20	0								Gr	oup	Oper	ati	on (Unta	ag A	1	·	
VLAN Memb	renship.	VLA	N Na	ime	į.		vla	n20	0							U	NTA	GGED	PO	RT M	EMB	ERS				
VLAN Statu	5	VLA	N Ty	pe			St	atic									TAG	GED	POR	TME	MBE	RS				
Port PVID	VLAN	-	Uni	t I																						
Configuratio	on	Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Port DVLAN Configuratio	i on		25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Protocol Ba VLAN Group	sed		49	50	51	52																				1
Protocol Ba VLAN Group Membership	sed																									
GARP Switc Configuratio	h on																									
GARP Port Configuratio	on																									

- b. Under VLAN Membership, in the VLAN ID field, select 200.
- c. Click Unit 1. The ports display:
 - Click the gray box under port **24** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
 - Click the gray box under port **48** once until **T** displays. The T specifies that the egress packet is tagged for the port.
- d. Click Apply to save the settings.
- 3. Change the port VLAN ID (PVID) of port 24 to 200:
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration. A screen similar to the following displays.

Basic	Port	VLAN Id Co	nfiguration			
Advanced	C. NEW CO.					
> VLAN	P	VID Configurati	on			(P
Configuration		All		Go To Inter	face GO	
VLAN Status MAC Based VLAN		Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
Configuration		1/0/24	200	Admit All 💌	Disable 💌	0
> Port DVLAN		1/0/1	100	Admit All	Disable	0
Configuration		1/0/2	1	Admit All	Disable	0
VI AN Group		1/0/3	1	Admit All	Disable	0
Configuration		1/0/4	1	Admit All	Disable	0
Protocol Based		1/0/5	1	Admit All	Disable	0
VLAN Group		1/0/6	1	Admit All	Disable	0
> GARP Switch		1/0/7	1	Admit All	Disable	0
Configuration		1/0/8	1	Admit All	Disable	0
GARP Port		1/0/9	1	Admit All	Disable	0
Configuration		1/0/10	1	Admit All	Disable	0
		1/0/11	1	Admit All	Disable	0
		1/0/12	1	Admit All	Disable	0
		1/0/13	1	Admit All	Disable	0
		1/0/14	1	Admit All	Disable	0
		1/0/15	1	Admit All	Disable	0
		1/0/16	1	Admit All	Disable	0

- **b.** Scroll down and select the Interface **1/0/24** check box. Now 1/0/24 appears in the Interface field at the top.
- c. In the PVID (1 to 4093) field, enter 200.
- d. Click Apply to save the settings.
- 4. Configure port 48 as the provider service port:
 - a. Select Switching > VLAN > Advanced > Port DVLAN Configuration. A screen similar to the following displays.

System	Switching	Routing	QoS Security	Monitoring	Maintenance	Help
VLAN STP	Multicost A	ddress Table Port	LAG			
Basic Advanced > VLAN	Port	DVLAN Config /LAN Configuration	guration			۲
Configuration	100	All		Go To Interface	GO	
> VLAN Member > VLAN Status	ship	Interface	Admin Mode	EtherType	Custom Va	ue
» MAC Based VI	LAN 📃	1/0/48	Enable 💌	802.1Q Tag		
> Port PVID	0	1/0/1	Disable	802.1Q Tag		
# Port DVLAN	Г	1/0/2	Disable	802.1Q Tag		
Configuration	E	1/0/3	Disable	802.1Q Tag		
» Protocol Baser VLAN Group	۵ ۲	1/0/4	Disable	802.1Q Tag		
Configuration	E	1/0/5	Disable	802.1Q Tag		
Protocol Baser VLAN Group	d F	1/0/6	Disable	802.1Q Tag		
Membership	E .	1/0/7	Disable	802.1Q Tag		
> GARP Switch	Г	1/0/8	Disable	802.1Q Tag		
> GARP Port	E	1/0/9	Disable	802.1Q Tag		
Configuration	- F	1/0/10	Disable	802.1Q Tag		
	Ē	1/0/11	Disable	802.10 Tag		

- **b.** Scroll down and select the Interface **1/0/48** check box. Now 1/0/48 appears in the Interface field at the top.
- c. In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.

Private VLAN Groups

The private VLAN group allows you to create groups of users within a VLAN that cannot communicate with members in different groups but only within the same group. There are two modes for the private group. The mode can be either isolated or community. When in isolated mode, the member port in the group cannot forward its egress traffic to any other members in the same group. the default mode is community, in which each member port can forward traffic to other members in the same group, but not to members in other groups. The following examples shows how to create a private group.

The following example creates two groups. Group 1 is in community mode, and Group 2 is in isolated mode.



Figure 32. Private VLAN groups in community mode and isolated mode

CLI: Create a Private VLAN Group

1. Enter the following commands.

```
(Netgear Switch) #
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#vlan participation include 200
(Netgear Switch) (Interface 1/0/6)#vlan pvid 200
(Netgear Switch) (Interface 1/0/6)#exit
(Netgear Switch) (Config)#interface 1/0/7
(Netgear Switch) (Interface 1/0/7)#vlan participation include 200
(Netgear Switch) (Interface 1/0/7)#vlan pvid 200
(Netgear Switch) (Interface 1/0/7)#exit
(Netgear Switch) (Config)#interface 1/0/16
(Netgear Switch) (Interface 1/0/16)#vlan participation include 200
(Netgear Switch) (Interface 1/0/16)#vlan participation pvid 200
(Netgear Switch) (Interface 1/0/16)#exit
(Netgear Switch) (Config)#interface 1/0/17
(Netgear Switch) (Interface 1/0/17)#vlan participation include 200
(Netgear Switch) (Interface 1/0/17)#vlan pvid 200
(Netgear Switch) (Interface 1/0/17) #exit
```

2. Create a VLAN 200 and include 1/0/6,1/0/7, 1/0/16, and 1/0/17.

(Netgear Switch) (Config)#
(Netgear Switch) (Config)#private-group name group1 1 mode community

3. Create a private group in community mode.

(Netgear Switch) (Config) #private-group name group2 2 mode isolated

4. Create a private group in isolated mode.

```
(Netgear Switch) (Config)#interface range 1/0/6-1/0/7
(Netgear Switch) (conf-if-range-1/0/6-1/0/7)#switchport private-group 1
(Netgear Switch) (conf-if-range-1/0/6-1/0/7)#exit
```

5. Add 1/0/16 and 1/0/7 to the private group 1.

```
(Netgear Switch) (Config)#interface range 1/0/16-1/0/17
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#switchport private-group 2
```

6. Add 1/0/16 and 1/0/7 to the private group 2.

```
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#exit
```

Web Interface: Create a Private VLAN Group

- 1. Create VLAN 200.
 - a. Select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays.

System	Switching Routi	ng QoS	Security	Monitoring	Maintenance	Help	Index
VIAN STP	Multicost Address Tob	e Forts LAG					
Basse	VLAN Config	uration					
Cilificiani	Reset				(U)		
Advanced	Reset Configura	tion					
	VLAN Confi	guration			00		
	VLAN ID	WEAN Nam		VLAN TY	pe		
	200	VLAN200		Static			
	[] 1	Default		Default			

- **b.** Enter the following information:
 - In the VLAN ID field, enter 200.
 - In the VLAN Name field, enter VLAN200.
 - In the VLAN Type field, select Static.
- c. Click Add.
- **2.** Add ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17 to VLAN 200.
 - a. Select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays.

System	Switchin	D	R	outir	9	0	o\$	\$	ecurity	/	Mo	nitorin	0	Mai	nteno	nce	10	Help	Index
VIAN STP	Melficest	A	Idres	Tabl	(I.)	Ports	LAG												
* Basic	V	AN	Me	mb	ers	hip													
+ VLAN	1	VLA	IN M	lemb	erst	ip .												22	
Configuration		LAN	ID .		4	200 -					_5	Group C	iperatis	an 🛛	Unte	g All	1		
 VLAN Member 	1998	LAND	Same			VLAN2	00				- 1	UNTAD	GED PO	ET MEN	HERS				
> VLAN Status	4.14	LAN	V PH	ļ.		Static					1	TADO	SED POR	T MEMI	ER3				
> Port PVID	1778 C	. 0	-																
Configuration	Po	ort 1	2	э	4	56	7 (0 9	10 1	1 12	13	14 15	16 17	10 1	9 20	21 2	2 23	24	
Port DVLAN Configuration Protocol Base		2	5 Z	6 27	28	U	U					1.11.121	0 0		-x-1-3				

- **b.** Under VLAN Membership, in the **VLAN ID** list, select **200**.
- c. Click Unit 1. The ports display.
- **d.** Click the gray boxes under ports **6**, **7**, **16** and **17** until **U** displays. The U specifies that the egress packet is untagged for the port.
- e. Click Apply.
- 3. Specify the PVID on ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17.
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration. A screen similar to the following displays.

System System System Stream	witching Witcost	Routing Address Table P	GioS S orth LAG	ecurity Monitori	ng Mainter	nonce Help	Index
• Basic • Advanced • VLAN	Por	t VLAN Id Co VID Configurati	nfiguration on			đ	
Configuration		AR		Go To Interf	ace 00	1	
VLAN Membersh VLAN Status MAC Based VLAN	4	Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)	
Configuration			200	<u> </u>			
* Port DVLAN		1/0/1	1.	Admit All	Disable	0	
Configuration	C	1/0/2	1	Admit All	Disable	Ø	
* Protocol Based	17	1/0/3	1	Admit All	Disable	0	
Configuration	Г	1/0/4	1	Admit All	Disable	0	
+ Protocol Based		1/0/5	1	Admit All	Disable	0	
VLAN Group	1	1/0/6	1	Admit All	Disable	0	
Membership	P	1/0/7	1	Admit All	Disable	0	

- **b.** Under PVID Configuration, scroll down and select the Interface **1/0/6**,**1/0/7**,**1/0/16**, and **1/0/17** check boxes.
- c. In the PVID (1 to 4093) field, enter 200.
- d. In the Acceptable Frame Type list, select Admit All.
- e. Click Apply to save the settings.
- 4. Create a private group, group1.
 - a. Select Security > Traffic Control > Private Group VLAN > Private Group VLAN > Private Group Configuration. A screen similar to the following displays.

System S	witching Routing G	loS Security	Monitoring	Maintenance	Help	Index
Monogement Secur	ity Access Port Authentication	Traffic Control ACL				Ī
MAC Filter Port Security	Private Group Config Private Group Config	juration aration	3	8		
T Privana Group	Group Name	Group 10	Group Mode			
 Private Group Membership Storm Control Protected Port 	a capa					

- b. In the Group Name field, enter group1.
- c. In the Group ID field, enter 1.
- d. In the Group Mode list, select community.

- e. Click Add.
- 5. Add port 6 and 7 to group1.
 - a. Select Security > Traffic Control > Private Group VLAN >Private Group Membership. A screen similar to the following displays.

System	Switching	8	Re	nifua	8:	0	205		5	scurit	y.	1	Aonit	lorin	9:	N	ainte	nond	e.	111	Help	In	dex
Management Sec	urity Acc	055	Po	et Au	heni	cation	i n	ntiic	Co	strol.	AC	i.											
MAC Filter Port Security	Pri	vate	e G	Gree	p M	lemb	ershi	hip P	•												11		
* Private Group	64 64	oup 1 oup M	n Iode			1 con	nmun	ity		1	Gran	gr Na	ne.	_	_	grout	4						
firrer Group formberong Storm Control	Par	Ues t 1 25	2	3	4 28	5 6	1	8	9	10 1		2 13	14	15	16 1	7 18	19 2	0 2	1 22	2 23	24		

- b. In the Group ID list, select 1.
- c. Click Unit 1. The ports display.
- d. Click the gray boxes under ports 6 and 7. A check mark displays in each box.
- e. Click Apply.
- 6. Create a private group, group2.
 - a. Select Security > Traffic Control > Private Group VLAN > Private Group Configuration. A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Manugement Sec	urity Acces	Port Authentic	otion Tra	fic Gentrel ACI	i .			
MAC Filter Port Security	Prive	ate Group Co rivate Group Co	onfiguration	ion		æ		
YLAN		Group Name		Group ID	Group Mode			
Surfaced at the		group2		. 2	isplated			
 Private Group Membership Storm Control Protected Port 		group1		1	community			

- b. In the Group Name field, enter group2.
- c. In the Group ID field, enter 2.
- d. In the Group Mode field, select isolated.
- e. Click Add.
- 7. Add ports 16 and 17 to group2.

a. Select Security > Traffic Control > Private Group VLAN > Private Group VLAN > Private Group Membership. A screen similar to the following displays.



- b. In the Group ID list, select 2.
- c. Click Unit 2. The ports display.
- d. Click the gray boxes under ports 16 and 17, and a check mark displays in each box.
- e. Click Apply.

STP

Spanning Tree Protocol

20

This chapter includes the following sections:

- SPT Concepts
- Configure Classic STP (802.1d)
- Configure Rapid STP (802.1w)
- Configure Multiple STP (802.1s)

SPT Concepts

The purpose of Spanning Tree is to eliminate loops in the switch system. There are three STPs: Classic STP (802.1d), Rapid STP (RSTP, 802.1w), and Multiple STP (MSTP, 802.1s).

While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a few seconds. RSTP can revert back to 802.1d in order to interoperate with legacy bridges on a per-port basis. This drops the benefits it introduces.

In Multiple Spanning Tree Protocol (MSTP), each Spanning Tree instance can contain several VLANs. Each Spanning Tree instance is independent of other instances. This approach provides multiple forwarding paths for data traffic, enabling load balancing, and reducing the number of Spanning Tree instances required to support a large number of VLANs.

Configure Classic STP (802.1d)

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Classic STP (802.1d)

(Netgear Switch) (Config)# spanning-tree (Netgear Switch) (Config)# spanning-tree forceversion 802.1d (Netgear switch) (Interface 1/0/3)# spanning-tree port mode

Web Interface: Configure Classic STP (802.1d)

- 1. Enable 802.1d on the switch.
 - a. Select Switching > STP > STP Configuration.

A screen similar to the following displays.

TTP Carlingson	STP Configuration			
Idvanced	STP Configuration			
	Spanning Tree Admin Hode Force Protocol Version	O Disable () Enable () IEEE 802.1d () IEE	e E 802.1w () 1555 802.1s	
	Configuration Name Configuration Revision Level	00-14-6C-53-62-8E	(2 14 62228)	
	Forward BPOU while STP Disabled Configuration Digest Key	Disable O Enable Oxar3617/930283e646	e 83821.69x6266x62	
	STP States			
	PIST 10 V10	1 110		

- **b.** Enter the following information:
 - For Spanning Tree Admin Mode, select the **Enable** radio button.
 - For Force Protocol Version, select the IEEE 802.1d radio button.
- c. Click Apply.
- 2. Configure the CST port.
 - a. Select Switching > STP > CST Port Configuration.

A screen similar to the following displays.

ad Information Information	G	Port Co ST Pert Co LADS	nfique al atique ati ati	-		As to interferen							
art Danse Schaperation art Danse		Intertaire	Part .	Admin Dige Dige	Pert Park Cont	Auto Calculated Part Park Cost	***	Caternal Part Path Cost	Auto Calculated External Fort Fath Cost	241 11	Part Harts	Part Particular Basta	
		100/0	1.210	-	1	and the second s	No Carry press	1	Conceptual de la concep	-	maire in	The setting	
	13	1/01	1.00	144	. 8	India	Box Configuration	al -	Statial .	41749	Buelle	TAKEN	
	11	4103	1.09	240		Brallin	Ad Defigured	81	Average	70170	Bustin	Distance	
	1	AND -	129	110	1	2mailte -	the Configuration	1114	Distant .	10.171		Distanting	
	0	104	129	114		theire 7	Sectored.	8	Bratine	34714	Branks.	Dantest 1.5	
	10	6/6/8	128	1944	1.8	diam'r	Set Configuration	*	Anativad	34778	Stable	Disting	
	0	1.04	128	740		bratte.	Sil Delgord	4	Brailing.	32774	Brance .	Bastreet	
	63	6/67	108	1944	14	biette	No Contactor	4	8-stilled	34778	Brable	During	
	03	1.04	128	Tree		Date 1	All Deligent	4	bratilar	32776	Prairs	Basives :	
	E3	LU18	128	this .	14	State:	no Contgood	4	Analised	22717	Evalte	Desired	
	0	1999	128 -	The .		Diale .	Ad Delgard		brutter.	12179	Sec.	Bastrad	
	E3	6/0196	100	51.4	14	diverse	ne limbural	4	anatived	10119	Statta	Destront	
	0	10012	125 -	See		diama.	Ad Grippet	*	States.	12740	E-salia	Daawad	
	24	A MARK -	1.04	51.0	14	i databia	And Distances	(a.)	Revenue.	denais.	Distant.	Reading.	

- **b.** Under CST Port Configuration, scroll down and select the Interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
- c. In the Port Mode field, select Enable.
- d. Click Apply.

Configure Rapid STP (802.1w)

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Rapid STP (802.1w)

```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree forceversion 802.1w
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

Web Interface: Configure Rapid STP (802.1w)

- 1. Enable 802.1w on the switch:
 - a. Select Switching > STP > STP Configuration.
| System | Switching | Routing | GoS | Security | Monitoring | Mainten | ance Help | Ind |
|-------------------------|----------------|--------------------------|------------------------------|----------|----------------------|--------------------------------|---------------------------|----------|
| YIAN STP | Multicost Ad | dress Toble | Porte LAG | i. | | | | |
| Notes
• 217 Contagos | - | STP Con | figuration | | | | | |
| Advanced | | STP C | onfiguration | | | | | 0 |
| | | Spanning T
Force Prot | ree Admin Mo
ocal Version | de | 01 | Disable 🛞 Eria
EEE 802.1d 💽 | ible
IEEE 002.1w 🔿 IEE | E 802.1s |
| | | Configurat | ton Name | | 00 | 14-6C-53-62-8 | E | |
| | | Configurat | ion Revision L | evel | 0 | | (0 Sp 65538) | |
| | | Forward Bi | PDU while STP | Disabled | 01 | Disable 💿 Ena | ible | |
| | | Configurat | iun Digest Ke | e | 0 H B | 36177/5028366 | 14683821d8a626de | 62 |
| | | STP St | atus | | | | | |
| | | MST ID | | VID | | FID | | |
| | | CIT | | 123 | 4 10 20 90 40 50 100 | 111 1.23 | 8 4 10 20 30 40 50 100 | 111 |

- **b.** Enter the following information:
 - For Spanning Tree Admin Mode, select the **Enable** radio button.
 - For Force Protocol Version, select the **IEEE 802.1w** radio button.
- c. Click Apply.
- **2.** Configure the CST port.

a. Select Switching > STP > CST Port Configuration.

dette:	CST	Port Co	nfigurat	ion								
STE Configuration	-	ST Purt Ca	eligeratio	-								
CET Configuration		LASE					Sin Te da	narface (1.00			
CET for Solution CET Fort Solution HST Fort Status HST Fort Status STP Statustics		Interface	Port. Priority	Admin Trige Port	Port Path Cost	Auto Colculated Port Path Cost	Madla Tinter	External Port Path Cost	Auto Colcolated External Part Path Cost	1 91	Port Hode	Port Porsearching State
		1/1/1	428	×	8	Illegate	Not Configured	1	(Deskind)	10771	Anatia (M.	Distanting
	13	1/8/3	128	The	4	Inable	Not Carrigonal		tratial .	32769	Double .	Disabled .
		APRCE.	125	714		Stalla	Ref Configured		Habled .	82778	Brail/a	Disabled
		1.02	529	250		Dance	Ant Carefigured	1	Saured.	82778	Brane .	Describer
	0	134	138	Test.	*	Tratia	Not Carligand	*	Enabled :	82772	Brable	Desitied
	0	1/6/9	600	714		biable	Not Configured		Stabled	34773	Brable	Destied
	11	1/3/6	1.2.0	210	4.7	Brable	the Configured	#C	braklad .	\$2774	brable	Disabled
	13	1/9/7	125	The		Statis	Int Caringwed		trains!	31778	trate	Disabled .
	10	1004	128	250	4	Braile	Aut Cardigured	*	Statist .	32776	Braile	Destind
	63	1/2/8	138	The		Instin	Not Cardiguest		Enabled .	32779	Stable .	Disabled :
	0	101/18	133	240		Draffe	Not Configurad	*	Diabled 1	84778	E-able .	Deskind
	0	1/8/11	124	1140		6nable	that Configured		tradied.	82778	(making	Dashied
	115	1/1/18	124	True		Stalia .	Inte Configurated	P.7	Statist.	22790	Bratin	Destind

- b. Under CST Port Configuration, scroll down and select the Interface 1/0/3 check box.
 Now 1/0/3 appears in the Interface field at the top.
- c. In the Port Mode field, select Enable.
- d. Click Apply.

Configure Multiple STP (802.1s)

The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure Multiple STP (802.1s)

```
(Netgear switch) (Config) # spanning-tree
(Netgear switch) (Config) # spanning-tree forceversion 802.1s
(Netgear switch) (Config) # spanning-tree mst instance 1
Create a mst instance 1
(Netgear switch) (Config) # spanning-tree mst priority 1 4096
(Netgear switch) (Config) # spanning-tree mst vlan 1 2
(Netgear switch) (Config) # spanning-tree mst vlan 1 3
Associate the mst instance 1 with the VLAN 2 and 3
(Netgear switch) (Config) # spanning-tree mst instance 2
Create a mst instance 2
(Netgear switch) (Config) # spanning-tree mst priority 2 4096
(Netgear switch) (Config) # spanning-tree mst vlan 2 11
(Netgear switch) (Config) # spanning-tree mst vlan 2 12
Associate the mst instance 2 with the VLAN 11 and 12
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 port-priority 128
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 cost 0
```

Web Interface: Configure Multiple STP (802.1s)

- 1. Enable 802.1s on the switch.
 - a. Select Switching > STP > STP Configuration.

System Swite VIAN STP Awbs	thing Routing	CoS Acris 1AG	Security	Monitoring	Maintenance	Halp	Index	(special
* Basic * Advanced - 111* Configuration	STP Configurat	ion				æ		_
Configuration Configuration COT Port Configuration COT Port Status HOT Configuration HOT Port Status STP Statustors	Spanning Tree Admin Force Protocol Versis Configuration Name Configuration Revisis Forward BPDU while Configuration Digest	: Hode on In Level STP On abled Key		○ Disable ④ ○ 1855 802.1d 00-14-6C-53-63 0 ④ Disable ◎ Disable ◎	Inable 0 1888 802,1w @ 188 0 188 (12 10 02233) Inable 0x01734/f6a12/f7494	€ 802.1s		
	STP Status					đ		
	HST TD CST 1 2		1 23 11.12		10 13 1122			
						i i i	CANCE HITH	LEN APPLY

- **b.** Enter the following information:
 - For Spanning Tree Admin Mode, select the **Enable** radio button.
 - For Force Protocol Version, select the IEEE 802.1s radio button.
- c. Click Apply.
- 2. Configure MST.
 - a. Select Switching > STP > MST Configuration.

Advanced • STE Configuration	MO	MST Com	ofiguration						
CST Configuration CST Port Configuration CST Port Status		MST ID	Priority	Vian Id	Oridge Identifier	Time Since Topology Change	Topology Change Count	Topology Change	Designated Roo
+ HST Part Status				1					
- STF Statistics	-	2	4096	2, 3	10-01-00-14-5c:51-62-8+ 10-02-00:14-6c:53-62-8+	0 day 2 hr 45 min 35 sec 0 day 2 hr 45 min 35 sec	0	Palee Palee	10102100114-6c15

- **b.** Configure MST ID 1.
 - In the **MST ID** field, enter **1**.
 - In the **Priority** field, enter **4096**.
 - In the VLAN Id field, enter 2.
 - Click Add.
 - In the VLAN Id field, enter 3.
 - Click Apply.
- c. Configure MST ID 2.
 - In the **MST ID** field, enter 2.
 - In the **Priority** field, enter **4096**.
 - In the VLAN Id field, enter 11.
 - Click Add.
 - In the VLAN Id field, enter 12.
 - Click Apply.
- 3. Configure the MST port.
 - a. Select Switching > STP > MST Port Status.

A	screen	similar	to	the	following	displays.
---	--------	---------	----	-----	-----------	-----------

		-						with the second			
Basic STP Configuration CST Configuration CST Fast Configuration CST Fast		Interface	Port Priority	Port Path Cost	Auto Calculated Port Path Cost	Port- TD	Port Uplime Since Last Clear Counters	Port Hode	Port Forwarding State	Port Role	Des
- CGT Port Status		1/0/3	128	0	traffe	ann	O'day Ohr 3 min 14 set:	Enabled	Disabled	Disabled	-
MST Configuration		1/0/1	128	200000	trable	32769	G day 0 hr 3 min 13 sec	trabled	Forwarding	Designated	10/1
. STP Statistics		1/0/2	178	0	Enable	32770	0 day 0 hr 3 min 14 sec	Enabled	Duabled	Disabled	80-0
	2	1/0/3	128	•	Enable	32771	Gidey II for 3 min 14 eec	Institut	Deabled	Destind	
		1/6/4	128	8	Enable	32772	0 day 0 hr 3 min 14 sec	Enabled	Disabled	Disabled	40-
		1/0/5	128	0	Knable	32773	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	80.0
		1/0/6	128	8	Enable	32774	0 day 0 hr 3 min 15 sec	Enabled	Disabled	Disabled	801
		1/8/7	128	200000	Inable	32775	Q day Q hr 3 min 24 and	Enabled	Forwarding	Designated	1.01
		1/9/8	128	0	Enable	32776	G day 0 to 3 min 13 sec	snabled	Duabled	Disabled	801
	0	1/0/9	128	\$	Broable .	32777	0 day 0 hr 3 min 15 sec.	Enabled.	Disabled	Disabled	80.0

- Under MST Port Configuration, scroll down and select the Interface 1/0/3 check box. Now 1/0/3 appears in the Interface field at the top.
- **5.** Enter the following information:
 - In the **Port Priority** field, enter **128**.
 - In the **Port Path Cost** field, enter **0**.
- 6. Click Apply.

DHCP L2 Relay and L3 Relay



Dynamic Host Configuration Protocol Relays

This chapter includes the following sections:

- DHCP L2 Relay
- DHCP L3 Relay

DHCP L2 Relay

DHCP relay agents eliminate the need to have a DHCP server on each physical network. Relay agents populate the giaddr field and also append the Relay Agent Information option to the DHCP messages. DHCP servers use this option for IP addresses and other parameter assignment policies. These DHCP relay agents are typically IP routing-aware devices and are referred to as Layer 3 relay agents.

In some network configurations, there is a need for Layer 2 devices to append the relay agent Information option as they are closer to the end hosts.



Host #2

Figure 33. DHCP L2 Relay

These Layer 2 devices typically operate only as bridges for the network and might not have an IPv4 address on the network. Lacking a valid IPv4 source address, they cannot relay packets directly to a DHCP server located on another network. These Layer 2 devices append the Relay agent information option and broadcast the DHCP message. This section provides information about where a Layer 2 relay agent fits in and how it is used.

CLI: Enable DHCP L2 Relay

1. Enter the following commands:

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 200
(Netgear Switch)(Vlan)#exit
```

2. Enable the DHCP L2 relay on the switch.

```
(Netgear Switch) (Config)#dhcp l2relay
(Netgear Switch) (Config)#dhcp l2relay vlan 200
```

3. Enable the Option 82 Circuit ID field.

(Netgear Switch) (Config)#dhcp l2relay circuit-id vlan 200

4. Enable the Option 82 Remote ID field.

(Netgear Switch) (Config)#dhcp l2relay remote-id rem_id vlan 200

5. Enable DHCP L2 relay on port 1/0/4.

(Netgear Switch) (Config)#interface 1/0/4 (Netgear Switch) (Interface 1/0/4)# dhcp 12relay

```
(Netgear Switch) (Interface 1/0/4)# vlan pvid 200
(Netgear Switch) (Interface 1/0/4)# vlan participation include 200
(Netgear Switch) (Interface 1/0/4)# exit
```

6. Enable DHCP L2 relay on port 1/0/5.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)# dhcp l2relay
(Netgear Switch) (Interface 1/0/5)# vlan pvid 200
(Netgear Switch) (Interface 1/0/5)# vlan participation include 200
(Netgear Switch) (Interface 1/0/5)# exit
```

7. Enable DHCP L2 relay on port 1/0/6.

(Netgear Switch) (Config)#interface 1/0/6 (Netgear Switch) (Interface 1/0/6)# dhcp 12relay

8. Trust packets with option 82 received on port 1/0/6.

```
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay trust
(Netgear Switch) (Interface 1/0/6)# vlan pvid 200
(Netgear Switch) (Interface 1/0/6)# vlan participation include 200
(Netgear Switch) (Interface 1/0/6)# exit
```

Web Interface: Enable DHCP L2 Relay

- 1. Create VLAN 200.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP	Multicost	Address Table P	Ports LAG					Î
v Basic	VLA	N Configurat	tion					
Configuration	R	eset					1	
Advanced	Rese	et Configuration			Γ			
	I	nternal VLAN Co	onfiguration	1			(?)	
	Inte	mal VLAN Allocati	ion Base		4093			
	Inte	mal VLAN Allocati	ion Policy		C Asce	nding 🖲 Descending		
	v	LAN Configurati	ion				1	
		VLAN ID	VLA	N Name	×	LAN Type		
		200		1				
	П	1	Defa	ult	D	efault		

- b. In the VLAN ID field, enter 200.
- c. In the VLAN Type field, select Static.
- d. Click Add.
- 2. Add ports to VLAN 200.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

A screen similar to the following displays.

System	Switching	Re	auting	Qu	s	Security	Monito	aring	Maintenan	ce	Help	Index
VEAN STP	Multicost	Address	Table	Ports.	LAG							
Basic	VLA	N Mei	nber	ship								
* VLAN	VI	AN MI	mber	ship							:20	
Configuration	VLA	TD		200 💌			Gros	ip Operatio	untag	All 📃		
- Vide Methods	VLA	Name		-			UN	TAGGED POR	T MEMBERS			
VLAN Status Port PUID	VLA	Type		Static				AGGED PORT	MEMBERS			
Configuration		Unit 1										
> MAC Based VL	AN Port	1 2	3 4	56	7 0 1	9 10 11	12 13 14 1	15 16 17	18 19 20 2	1 22 23	24	
> IP Subnet Base VLAN	ed	25 26	27 21	100	2433	9999	59353531	-12313				

- b. In the VLAN ID field, select 200.
- c. Click Unit 1. The ports display.
- d. Click the gray boxes under ports 4, 5, and 6 until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply.
- 3. Specify the PVID on ports 1/0/4, 1/0/5 and 1/0/6.
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration.

System Swit	ching	Routin	g QaS	Security N	anitoring	Maintenance	Help	Index
VLAN STP Mult	cost	Address Table	Ports LA	5				
Dasic	Port	PVID Co	nfiguration					
VLAN	P	VID Configu	aration				100	
Configuration	1 A	н		Go To Interface	60			
VLAN Membership VLAN Status		Interface	PVID (1 to 4093)	Acceptable Frame Types	Ingress Filtering	Part Priority to 7)	(0	
Configuration			200					
HAC Based VLAN	E	1/0/1	1	AdmitAll	Disable	0		
VLAN	Г	1/0/2	1	AdmitAll	Disable	0		
Port DVIan	5	1/0/3	1	AdmitAll	Disable	0		
Configuration	F	1/0/4	1	AdmitAll	Disable	0		
Protocol Based VLAN Group	F	1/0/5	1	AdmitAll	Disable	0		
Configuration	F	1/0/6	1	AdmitAll	Disable	0		

- b. Scroll down and select the Interface 1/0/4, 1/0/5, and 1/0/6 check boxes.
- c. In the PVID (1 to 4093) field, enter 200.
- d. Click Apply to save the settings.
- 4. Enable DHCP L2 relay on VLAN 200.
 - a. Select System > Services > DHCP L2 Relay > DHCP L2 Relay Configuration.

System	Switching	Routing	Qo5	Security	Monitoring	Maintenance	Help	Index
Management	Device View	Services ;	Stocking SNMP	LLDP ISDP				
DHCP Server	DH	CP L2 Rela	y Configurati	on				
DHCP LT Pete	× 100	DHCP L2 Rela	y Global Configu	uration			.97	
A DHCHLERAD	Ad	min Mode			C Disal	ble 🗭 Enable		
Clobel	Land Contract	a productiva de la					_	
Cutifi jur diete	V 24	DHCP L2 Relay VLAN Configuration						
> DHCP L2 Reli	NX I	VLAN ID	Admin Mode	Circuit II	Hode	Remote ID String		
Configuration		200	Enable 🖃	Enable	•	rmt_id		
> DHCP L2 Rel	ay [1	Disable	Disable				
Interface Sta	tistics 🔽	200	Disable	Desable				
DHCPv6 Serve DHCPv6 Relay	er							

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Scroll down and select the VLAN ID 200 check box.
- **d.** Enter the following information:
 - In the Admin Mode field, select Enable.
 - In the Circuit ID Mode field, select Enable.
 - In the Remote ID String field, enter rmt_id.
- e. Click Apply to save the settings.
- 5. Enable DHCP L2 Relay on interfaces 1/0/4,1/0/5, and 1/0/6.
 - a. Select System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration.

System :	Switching	Routing	QoS Security	Monitoring	Maintenance	Help	Index
Management 0	Device View	Services Stor	king SNMP LLDP	ISOP			
DHCP Server	DHO	CP L2 Relay C	onfiguration				
DHCP Relay		HCP L2 Relay C	onfiguration			1	
· OHCP L2 Relay	1 4	.11	Go To Interfa	KB 00			
Configuration		Interface	Admin Mode	82 Option Tru	ist Mode		
			Enable 💌				
and the second second	Г	1/0/1	Disable	Disable			
· DHCF L2 Relay	Г	1/0/2	Disable	Disable			
Interface	E	1/0/3	Disable	Disable			
Statistics	1	1/0/4	Disable	Disable			
DHCPv6 Server		1/0/5	Disable	Disable			
DHCPv6 Relay	P	1/0/6	Disable	Disable			

- b. Scroll down and select the 1/0/4, 1/0/5, and 1/0/6 check boxes.
- c. In the Admin Mode field, select Enable.
- d. Click Apply to save the settings.
- 6. Enable DHCP L2 relay trust on interface 1/0/6.
 - a. Select System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration.

System	Switching	Routing	Qu5 Security	Monitoring	Maintenance	Help	Index
Monogement	Device View	Services Stoc	king SNMP LLDP	ISDP			
DHCP Server	DHO	CP L2 Relay C	onfiguration				
DHCP Relay		HCP L2 Relay C	onfiguration			0	
+ DHCP L2 Rela	1 1 1		Go To Inter	lace 00			
Configuration		Interface	Admin Mode	82 Option Tri	ist Node		
· DHEP LEAND		1/0/6	Enable 🖃	Enable -			
Interface.		1/0/1	Disable	Disable		1	
+ DHCP L2 Rela	γ Γ	1/0/2	Disable	Disable			
Interface		1/0/3	Disable	Disable			
Statistics.	F	1/0/4	Enable	Disable			
DHCPv6 Serve	e E	1/0/5	Enable	Disable			
DHCPv6 Relay	9	1/0/6	Enable	Disable			

- **b.** Under DHCP L2 Relay Configuration, scroll down and select the Interface **1/0/6** check box.
- c. In the 82 Option Trust Mode field, select Enable.
- d. Click Apply to save the settings.

DHCP L3 Relay

This case has two steps, DHCP server configuration and DHCP L3 relay configuration. This example shows how to configure a DHCP L3 relay on a NETGEAR switch and how to configure DHCP pool to assign IP addresses to DHCP clients using DHCP L3 relay.



Figure 34. DHCP L3 relay

Configure the DHCP Server Switch

CLI: Configure a DHCP Server

1. Enable routing on the switch.

(Netgear Switch) #config (Netgear Switch) (Config)#ip routing (Netgear Switch) (Config)# 2. Create a routing interface and enable RIP on it so that the DHCP server learns the route 10.200.1.0/24 from the DHCP L3 relay.

```
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 10.100.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#ip rip
(Netgear Switch) (Interface 1/0/3)#exit
```

3. Create a DHCP pool.

(Netgear	Switch)	(Config)#ip dhcp pool dhcp_server
(Netgear	Switch)	(Config-dhcp-pool)#network 10.200.1.0 255.255.255.0
(Netgear	Switch)	(Config-dhcp-pool)#exit
(Netgear	Switch)	(Config)#ip dhcp pool dhcp_server_second
(Netgear	Switch)	(Config-dhcp-pool)#network 10.200.2.0 255.255.255.0
(Netgear	Switch)	(Config-dhcp-pool)#exit
(Netgear	Switch)	(Config)#service dhcp
(Netgear	Switch)	(Config)#exit

4. Exclude the IP address 10.200.1.1 and 10.200.2.1 from the DHCP pool because it has been used on the DHCP L3 relay.

```
(Netgear Switch) (Config)#ip dhcp excluded-address 10.200.1.1
(Netgear Switch) (Config)#ip dhcp excluded-address 10.200.2.1
```

Web Interface: Configure a DHCP Server

- 1. Enable routing mode on the switch.
 - a. Select Routing > IP > Basic > IP Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP IPv6	VLAN ARP	RIP OS	PF OSPFv3	Router Discovery	VRRP Multicost	IPv6 Multicast	
w Basic	IP Co	nfiguration						
* IP Configuration	IP IP	Configuration					(7)	
Advanced	Defau	It Time to Live			64			
- Havancea	Routin	g Mode			🕑 Enable 🔿 Disa	ble		
	ICMP	Echo Replies			€ Enable C Disa	ble		
	ICMP	Redirects			€ Enable C Disa	ble		
	ICMP	Rate Limit Inter	val		1000	(0 to 21474836	47 ms)	
	ICMP	Rate Limit Burst	Size		100	(1 to 200)		
	Maxim	um Next Hops			4			

- **b.** For Routing Mode, select the **Enable** radio button.
- c. Click Apply.

- 2. Create a routing interface and assign 10.100.1.1/24 to it.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System Sw	ritching	R	outing	QoS	Se	curity	Monitoring	Ma	intenance	Help	Index		10000	
Routing Table IP	I IPv6	VLAN	ARP	RIP O	SPF C	DSPFv3 1	Router Discovery	VRRP	Multicost	IPv6 Multic	ast			
Basic	IP	Interf	ace Co	nfigurat	ion									
Advanced	103	IP Interface Configuration												
 > IP Configuration > Statistics 	4	I All Go To Interface												
 IP Interface Configuration Secondary IP 		Port	Descri	ption	VLAN ID	IP Addres	s Masi	iet (Routi Mode	ng Ad Ma	lministrative ode	OSPF Admin Mode	Forward Net Directed Broadcast	
		1/0/3				10.100.	1.1 255.	255.255.	0 Enat	le 🔹 E	nable 💽	Disable	Disable 💌	
		1/0/1	1	2		0.0.0.0	0.0.0	.0	Disabl	e En	able	Disable	Disable	
	Г	1/0/2				0.0.0.0	0.0.0	.0	Disabl	e En	able	Disable	Disable	
	V	1/0/3				0.0.0.0	0.0.0	.0	Disabl	e En	able	Disable	Disable	

- **b.** Scroll down and select the **1/0/3** check box.
- c. In the IP Address field, enter 10.100.1.1.
- d. In the Subnet Mask field, enter 255.255.255.0.
- e. In the Routing Mode field, select Enable.
- f. Click Apply to save the settings.
- **3.** Enable RIP on interface 1/0/3.
 - a. Select Routing > RIP > Advanced > Interface Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	IP IPv6	VLAN ARP	RIP OSI	PF OSPFv3	Router Discovery	VRRP Multicost	IPv6 Multicast	
Basic	Inter	face Config	guration					
• Advanced	Int	erface Config	juration				(D
 » RIP Configura » Interface 	Interf	ace			1/0/3 🔹			
Configuration	Send V	ersion			RIP-2 ·			
» Route	Receiv	e Version			RIP-2 ·			
Redistribution	RIP A	dmin Mode			O Disable 🙆	Enable		
	Authe	ntication Type			None	2		

- b. In the Interface field, select 1/0/3.
- c. For RIP Admin Mode, select the Enable radio button.
- d. Click Apply to save the settings.
- 4. Set up the DHCP global configuration.
 - a. Select System > Services > DHCP Server > DHCP Server Configuration.

System Sv	witching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management De	vice View	Services Stack	king SNA	AP LLDP IS	DP			
DHCP Server	DHCP	Server Cor	ofiguratio	on				
> DHCP Server	DHO	P Server Con	figuration				(?)	
» DHCP Pool	Admin	Mode			C Disable 🖲 Enab	le		
Configuration	Ping Pa	icket Count			2	(0, 2 to 10)		
» DHCP Pool Optio	ns Conflic	t Logging Mode			C Disable 🖲 Enab	le		
» DHCP Server Statistics	Bootp	Automatic Mode				le		
» DHCP Bindings	Exc	luded Address					1	
» DHCP Conflicts	IP	Range From	IP	Range To				
Information DHCP Relay	1	0.200.1.1	10	.200,1,1	P	11-11-11-11-11-11-11-11-11-11-11-11-11-		

- **b.** For Admin Mode, select the **Enable** radio button.
- c. In the IP Range From field, enter 10.200.1.1.
- d. In the IP Range To field, enter 10.200.1.1.
- e. Click Add.
- 5. Exclude 10.200.2.1 from the DHCP pool.
 - a. Select System > Services > DHCP Server > DHCP Server Configuration.

System	Switching	Routing	QoS	Security	Manitoring	Maintenance	Help	Index
Monogement	Device View	License Senio	III Stocking	I SNMP	LLDP I ISDP			
UNCP Serve		DHCP Serv	er Config	uration				
- Dech Sale		DHCP Ser	ver Configu	iration				(0)
+ DHCP Pool	Continuation	Admin Hode			(F Disable (C Enable		
+ DHCP Pool	Options	Ping Packet G			2	(0, 2 m	3.03	
+ DHCP Serv	er Statistics	Conflict Loggin	g Hode		C Disable (F Enable		
* DHCP Bind Information	nos	Booty Automa	Nic Mode		(Disable)	C Enable		
DHCP Conf Information	licts	Excluded	Address		1001			0
DHCP Relay		IP Range	From	TP Rang	e To			
DHCP LZ Re	lay	10.200.2	1	10.200.	2.1			
UDP Relay DHCPv6 Ser	ver	L0.200.1	i	10.200.1	1			

- b. In the IP Range From field, enter 10.200.2.1.
- c. In the IP Range To field, enter 10.200.2.1.
- d. Click Add.
- 6. Create a DHCP pool named dhcp_server.
 - a. Select System > Services > DHCP Server > DHCP Pool Configuration.

System Switc	hing Routing QoS	Security Monito	ring Maintenance	Help	Index				
Management Device	View Services Stacking St	NMP LLDP ISDP							
DHCP Server	DHCP Pool Configuratio	n							
» DHCP Server	DHCP Pool Configuration								
> DHCP Pool	Pool Name	Create 💌							
Configuration	Pool Name	dhcp_server	(1 to 31 Alphanumeric Ch	aracters)					
» DHCP Pool Options	Type of Binding	Dynamic 💌							
» DHCP Server	Network Address	10.200.1.1							
Statistics	Network Mask	255.255.255.0							
» DHCP Bindings	Network Prefix Length		(0 to 32)						
» DHCP Conflicts	Client Name								
Information	Hardware Address	00:00:00:00:00:00							
DHCP Relay	Hardware Address Type	Ethernet 💌							
DHCP L2 Relay	Client ID								
UDP Relay	Host Number	0.0.0							
DHCPv6 Server	Host Mask	0.0.0							
price to Kelay		1	The second second						

- **b.** Under DHCP Pool Configuration, enter the following information:
 - In the **Pool Name** list, select **Create**.
 - In the **Pool Name** field, enter **dhcp_server**.
 - In the Type of Binding list, select Dynamic.
 - In the Network Number field, enter 10.200.1.0.
 - In the Network Mask field, enter 255.255.255.0. As an alternate, you can enter 24 in the Network Prefix Length field.

Note: Do not fill in the Network Mask field and Network Prefix Length field at the same time.

- c. Click Add. The pool_dynamic name is now added to the Pool Name drop-down list.
- 7. Create a DHCP pool named dhcp_server_second.
 - a. Select System > Services > DHCP Server > DHCP Pool Configuration.

System	Switching	Routing	QoS	Security	Ma	gnitotin	Maintenance	Help	Index
Monogement	Device Year	License Sinis	ces Stocking	SNMP	LLDP	ISDP			
MILE Arrest	-	DHCP Poo	l Configura	tion					
+ DHCP Serv	er.	DHCP Po	ol Configurat	ion					(2)
Configuratio	Conditionation	Pool Name		1	Create	-			
+ DHCP Pool	Options	Pool Name		1	dhcp_ser	ver_second	Ek to 11 alphanur	neric character	10
+ DHCP Serv	er Statistics	Type of Binds			Dynamic				
+ DHCP bind	nge	Network Add	lemon .	1	10 200 2	.0			
Information	2017	Network Has	A	1	255-255	255.0			
Information	ices.	Network Pret	fix Length	1			(0 to 22)		
DHCP Relay		Client Name		I					
DHCP L2 Rel	lay	Hardmare Ad	dream	1	00:00:00	00:00:00			
UDP Relay		Hardstare Ad	dress Type	1	Ethernet	14			
DHEPV6 Ser	ver	(Sent ID		1					
DUICE VS 1021	ey:	Host Number		1	0.0.0.0				
		Host Hask		1	0.0.0.0				
		Hest Prefix L	ength	1			[# 10 22]		

- **b.** Under DHCP Pool Configuration, enter the following information:
 - In the Pool Name list, select Create.
 - In the Pool Name field, enter **dhcp_server_second**.
 - In the Type of Binding list, select **Dynamic**.
 - In the Network Number field, enter 10.200.2.0.
 - In the Network Mask field, enter **255.255.255.0**. As an alternate, you can enter **24** in the Network Prefix Length field.
- c. Click Add. The dhcp_server_second name is now added to the Pool Name drop-down list.

Configure a DHCP L3 Switch

CLI: Configure a DHCP L3 Relay

1. Enable routing on the switch.

(Netgear Switch) #config (Netgear Switch) (Config)#ip routing (Netgear Switch) (Config)#

2. Create a routing interface and enable RIP on it.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 10.100.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#ip rip
(Netgear Switch) (Interface 1/0/4)#exit
```

3. Create a routing interface connecting to the client.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/16
(Netgear Switch) (Interface 1/0/16)#routing
(Netgear Switch) (Interface 1/0/16)#ip address 10.200.2.1 255.255.0
(Netgear Switch) (Interface 1/0/16)#exit
```

4. Configure the DHCP Server IP address and enable the DHCP L3 relay.

```
(Netgear Switch) (Config)#ip helper-address 10.100.1.1 dhcp
(Netgear Switch) (Config)#ip helper enable
```

5. Redistribute 10.200.1.0/24 and 10.200.2.0/24 to the RIP such that RIP advertises this route to the DHCP server.

(Netgear Switch) (Config)# (Netgear Switch) (Config)#router rip (Netgear Switch) (Config-router)#redistribute connected (Netgear Switch) (Config-router)#exit

Web Interface: Configure a DHCP L3 Relay

- 1. Enable routing mode on the switch.
 - a. Select Routing > IP > Basic > IP Configuration.

A screen similar to the following displays.

System S	witching Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
Routing Table	IPv6 VLAN ARP	RIP OS	PF OSPFv3	Router Discovery	VRRP Multicast	IPvó Multicast			
* Basic	IP Configuration	n							
* IP Configuration	IP Configuration	i.				(1)			
» Statistics Advanced	Default Time to Live			64					
	Routing Mode			💽 Enable 🔿 Disa	ble				
	ICMP Echo Replies			€ Enable C Disa	ble				
	ICMP Redirects			€ Enable C Disa	ble				
	ICMP Rate Limit Inter	rval		1000	(0 to 21474836	47 ms)			
	ICMP Rate Limit Burs	t Size		100 (1 to 200)					
	Maximum Next Hops			4					

- **b.** For Routing Mode, select the **Enable** radio button.
- c. Click Apply.
- 2. Create a routing interface and assign 10.100.1.2/24 to it.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System Sw	itching	R	outing Qo	S Se	curity Mo	nitoring Main	tenance	Help Index		LOGO				
Routing Table IP	IPv6	VLAN	ARP RIP	OSPF O	SPFv3 Router D	iscovery VRRP A	Aulticast IPv6	Multicost						
Basic	IP	Interf	ace Configur	ation						1				
Advanced	(ER	IP Interface Configuration												
 IP Configuration Statistics DF Interface Configuration Secondary IP 	1	1 All Go To Interface												
		Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode	OSPF Admin Mode	Forward Net Directed Broadcas				
		1/0/4			10.100.1.2	255,255,255.0	Enable .	Enable 💌	Disable	Disable				
		1/0/1			0.0.0	0.0.0	Disable	Enable	Disable	Disable				
	Г	1/0/2			0.0.0	0.0.0	Disable	Enable	Disable	Disable				
	Г	1/0/3			0.0.0.0	0.0.0	Disable	Enable	Disable	Disable				
	R	1/0/4			0.0.0	0.0.0	Disable	Enable	Disable	Disable				
		1/0/5			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable				

- b. Scroll down and select the Port 1/0/4 check box.
- c. In the IP Address field, enter 10.100.1.2.
- d. In the Subnet Mask field, enter 255.255.255.0.

- e. In the Routing Mode field, select Enable.
- f. Click Apply to save the settings.
- **3.** Enable RIP on interface 1/0/4.
 - a. Select Routing > RIP > Advanced > Interface Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Routing Table	P IPv6	VLAN ARP	RIP OSF	PF OSPFv3	Router Discovery	VRRP Multicast	IPv6 Multicast	
> Basic	Inter	face Config	uration					
 Advanced DID Configuration 	Int	erface Config	uration				(D
> Interface	Interf	ace			1/0/4 💽			
Configuration	Send V	ersion			RIP-2 ·			
» Route	Receiv	ve Version			RIP-2 -			
Redistribution	RIP A	dmin Mode			O Disable 💽	Enable		
-	Authe	ntication Type			None -	1		

- b. In the Interface list, select 1/0/4.
- c. For RIP Admin Mode, select the Enable radio button.
- d. Click Apply to save the settings.
- 4. Create a routing interface and assign 10.200.1.1/24 to it.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

Rooting Table 1 (Pr. 1946	T VLAN	T AIP	BIP COSH	004-3	Rooter Decovery	VEP Hote	- Pristant									
and the second s	IP Interface Configuration IP Interface Configuration IP Interface Configuration															
+ Thefacture	1.0	I 2 YLANS AR														
California California Secondary IP		P == 1	P == 1	Pai1	Pair	P == 1	Pair	Pre-1	Description	NLAN SP	IF Address Configuration Pathod	5	Nobeet . Hash	Realing:	Administrative Nude	Link Spreid Data Rate
		1/5/15			Mahual y	14,299 1.5	255.255.255.8	Readly (w)	triable in	Dekeption						
	E	1/9/1			None	9.0.0.0	0.0.0.0	Disable	Bheble	Unknown						
	1	1.00			Store .	8.8.8.6	1000	Disable	Enable	Linksoner.						
	FT	1/9/7			Rene	9.8.6.6	43.8.8	Positie	Brieble .	Spansee						
	1	1.64			Henn	0.0.0.0	8.0.0.0	Disalife	diventa .	100 mprox						
	10	1/9/5			None	0.0.0.0	0.0.0.0	Detable	Enable	Unknown						
	100	1.0.9			here	3.8.4.8	3333	Disable	Englise .	Abdroom .						
	1	\$/9/7			time	3.8.6.0	14444	Double	E146/e	10kium						
	10	1.0/9			None	0.0.6.0	6.0.0.0	Disable	dinable	Websont						
	- F	1.000			#1111			Publishing	Raikia	Niel State						

- **b.** Under IP Interface Configuration, scroll down and select the Port **1/0/15** check box.
- c. In the IP Address Configuration Method field, enter Manual.
- d. In the IP Address field, enter 10.200.1.1.
- e. In the Subnet Mask field, enter 255.255.255.0.
- f. In the Routing Mode field, select Enable.
- g. Click Apply to save the settings.
- 5. Create a routing interface and assign 10.200.2.1/24 to it.
 - a. Select Routing > IP > Advanced > IP Interface Configuration.

System	Switching	Re	outing	QoS	Security	Monitoring	Maistenano	e Help	Index						
Routing Table	P ING	VLAN	AIP	RP OSPF	OSHV3	Router Discovery	VERP Multicest	Pv6 Multicent							
Basic		IP.	Interfa	ce Configur	ation										
Advanced		100	IP Interf	ace Coofigura	tien										
 IP Configur Statistics 	rbion.	1	1 2 VIANS All												
• IP Interface Configuration • Secondary II			Port	Description	YLAN 10	IP Address Configuration Nethod	sp Address	Subset Nask	Routing Hode	Administrative Hode	Link Speed Data Rate				
			1/0/24			Hatual in	10.200.2.3	285.255.255.0	Enable in	Enable (#	Unknown				
			1/9/1		1	None	0.0.0.0	0.0.0.0	Dinable	Enable	Unknown				
		101	1/6/2			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown				
		E	1/5/3			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown				
		10	1/0/4			None	0.8.0.0	0.0.0.0	Disable	Enable	Unknown				
		C	1/0/5			Note	0.0.0.0	0.0.0.0	Disable	Enable	Unknown				
		10	1/0/5			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown				
		C	1/6/7			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown				
		10	1/5/9			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown				
		E	1/6/9			None	0.0.0.0	0.0.0.0	Disable	Enable	Unknown				

- **b.** Under IP Interface Configuration, scroll down and select the Port **1/0/16** check box.
- c. In the IP Address Configuration Method field, enter Manual.
- d. In the IP Address field, enter 10.200.2.1.
- e. In the Subnet Mask field, enter 255.255.255.0.
- f. In the Routing Mode field, select Enable.
- g. Click Apply to save the settings.
- 6. Redistribute the connected routes to RIP.
 - a. Select Routing > RIP > Advanced > Route Redistribution.

System Swit	ching	Routing	QoS	Security	Monitoring	Maintena	ince	Help	Index	LOGOUT
Routing Table IP	IPv6	VLAN ARP	RIP OSPF	OSPFv3	Router Discovery	VRRP Multie	ast IPv6	Multicast		
Basic	Rout	e Redistrib	ution							
» RIP Configuration	Co	nfiguration								
> Interface	Source	e							Connected -	
Configuration	Redist	bibute Mode							Enable 💌	
> Route .	Metric								0	(0 to 15, 0
Redistribution	Distri	bute List							0	(0 to 199,

- **b.** In the **Source** field, select **Connected**.
- c. In the Redistribute Mode field, select Enable.
- d. Click Apply to save the settings.
- 7. Enable DHCP L3 relay.
 - a. Select System > Services > DHCP Relay.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index						
Management	Device View	Services Star	cking SN/	AP LLDP I	SDP									
DHCP Server	DHCF	DHCP Relay												
DHCP Relay DHCP L2 Relay	DH	DHCP Relay												
	Maxim	num Hop Count			4	(1 to 16)								
DHCPv6 Serve	r Admir	n Mode			O Disable 🕑 Enat									
DHCPv6 Relay	Minim	um Wait Time (s	ecs)		0	(0 to 100)								
	Circuit	t ID Option Mode	•		Oisable C Enable									
	DH	CP Status					۲							
	Reque	sts Received			364									
	Reque	sts Relayed			8									
	Packe	ts Discarded			0									

- **b.** For Admin Mode, select the **Enable** radio button.
- c. Click Apply to save the settings.
- 8. Configure the DHCP server IP address.
 - a. Select System > Services > UDP Relay.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Inde					
Management	Device View	Services Stac	king SNA	AP LLDP IS	DP								
DHCP Server	UDF	Relay											
DHCP Relay	100	IDP Relay Confi	guration				(2)						
UDP Relay	y Adn	Admin Mode C Disable © Enable											
> UDP Relay Gi Configuration	iobal I I I I I I I I I I I I I I I I I I I	IDP Relay Globa	l Configura	ition			0						
» UDP Relay Interface		Server Address	UD	P Port	UDP Port Other Value		Hit Count						
Configuration		10.100.1.1	(d	ncp 💽	67								
DHCPv6 Relay	/												

- b. In the Server Address field, enter 10.100.1.1.
- c. In the UDP Port field, enter dhcp.
- d. Click Add to save the settings.

MLD Snooping

Multicast Listener Discovery

22

This chapter includes the following sections:

- Multicast Listener Discovery Concepts
- MLD Snooping Concepts
- CLI: Configure MLD Snooping
- Web Interface: Configure MLD Snooping

Multicast Listener Discovery Concepts

Multicast Listener Discovery (MLD) protocol enables IPv6 routers to discover multicast listeners, the nodes that are configured to receive multicast data packets, on its directly attached interfaces. The protocol specifically discovers which multicast addresses are of interest to its neighboring nodes and provides this information to the active multicast routing protocol that makes decisions on the flow of multicast data packets.

Periodically, the multicast router sends general queries requesting multicast address listener information from systems on an attached networks. These queries are used to build and refresh the multicast address listener state on the attached networks. In response to the queries, multicast listeners reply with membership reports. These membership reports specify their multicast addresses listener state and their desired set of sources with current-state multicast address records.

The multicast router also processes unsolicited filter- mode-change records and source-list-change records from systems that want to indicate interest in receiving or not receiving traffic from particular sources.

MLD Snooping Concepts

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes configured to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2, and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

CLI: Configure MLD Snooping

1. Enter the following commands.

```
(Netgear Switch) #vlan da
(Netgear Switch) (Vlan)#vlan 300
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 300
(Netgear Switch) (Interface 1/0/1)#vlan pvid 300
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 300
(Netgear Switch) (Interface 1/0/24) #vlan pvid 300
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) (Config) #set mld
(Netgear Switch) (Config)#exit
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#set mld 300
(Netgear Switch) (Vlan)#exit
```

2. Enable MLD snooping on VLAN 300.

```
(Netgear Switch) #show mldsnooping
Admin Mode..... Enable
Multicast Control Frame Count..... 0
Interfaces Enabled for MLD Snooping..... None
VLANs enabled for MLD snooping..... 300
(Netgear Switch) #
```

Web Interface: Configure MLD Snooping

- 1. Create VLAN 300.
 - a. Select Switching > VLAN > Basic > VLAN Configuration.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index					
VLAN STP	Multicast A	ddress Table	Ports LAG	N.		- 10	40						
Basic	VLAN	VLAN Configuration											
* VLAN Configuration	Res	et					۲						
Advanced	Reset	Configuration											
	Inte	ernal VLAN C	onfiguration				1						
	Intern	al VLAN Allocat	ion Base		4093								
	Intern	al VLAN Allocat	ion Policy		C Ascending 🖲 De	escending							
	VLA	N Configurat	ion				(1)						
		LAN ID VLA	N Name		VLAN TY	pe							
		300				· ·							
	L 1	Defa	ult		Default								

- b. In the VLAN ID field, enter 300.
- c. Click Add.
- 2. Assign all of the ports to VLAN 300.
 - a. Select Switching > VLAN > Advanced > VLAN Membership.

A screen similar to the following displays.

System	Switch	hing		Ro	outir	g	12	Qo	5		S	ecu	rity		N	oni	lori	ng		N	ainter	ance	e	T	Hel	Р	In	de
VLAN STP	Multico	ast	Add	ress	Tabl	e	Ports	j.	LAC	G																		
Basic	1	VLA	NN	1er	nbe	ersl	nip																					
» VLAN		VLAN Membership																		۲	li -							
Configuratio	on	VLAN ID					300 💌						Group Operation Untag All															
* VLAN Monst	bership	VLAN Name					1						UNTAGGED PORT MEMBERS															
> VLAN Statu	s	VLA	N Tyj	pe			Stati	c									TAG	GED	POR	T ME	MBERS							
Configuratio	on	-	Unit	: 1																								
» MAC Based	VLAN	Port	1	2	3	4	5 (5	7	8	9	10	11	12	13	14	15	16	17	18	19 20	21	22	23	24			
» IP Subnet B	Based		U							:	_			-						-				; I	U			
VLAN		_	25	26	27	28																				6		
» Port DWI AN	1					1																				-		_

- b. In the VLAN ID list, select 300.
- c. Click Unit 1. The ports display.
- d. Click the gray boxes under ports 1 and 24 until U displays.

The U specifies that the egress packet is untagged for the port.

- e. Click Apply.
- 3. Assign PVID to ports 1/0/1 and 1/0/24.
 - a. Select Switching > VLAN > Advanced > Port PVID Configuration.

System	witching	Routin	g G	oS Security	Monitoring	Maintenance	Help	Index						
VLAN STP	Multicast	Address Table	e Ports	LAG										
Basic	Por	Port PVID Configuration												
» VLAN	P	VID Configu	uration				1							
Configuration	1 A	п		Go To Interface GO										
 VLAN Membersi VLAN Status Port PVID 	qir	Interface	P¥ID	Acceptable Fram Types	e Ingress Filtering	Port Prior	ity							
Configuration			300											
» MAC Based VLA		1/0/1	1	Admit All	Disable	0								
VLAN	Г	1/0/2	1	Admit All	Disable	0								
> Port DVLAN		1/0/3	1	Admit All	Disable	0								

- **b.** Scroll down and select the interface **1/0/1** and 1/0/24 check boxes.
- c. In the PVID (1 to 4093) field, enter 300.
- d. Click Apply to save the settings.
- 4. Enable MLD snooping on the switch.
 - a. Select Routing > Multicast > MLD Snooping > Configuration.

A screen similar to the following displays.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN STP	Multicast Ad	ddress Table 📋 I	Ports LAG					
MFDB	MLD S	Snooping Co	onfigurat	ion				
IGMP Snooping MLD Snooping	ML	Snooping Co	onfiguration	1 -			۲	
· Configuration	MLD Sr	nooping Admin M	le					
 Interface Configuration 	Multica Interfa	st Control Fram aces Enabled for	e Count · MLD Snoopii	ng	0			
> MLD VLAN Configuration	Data F	rames Forwarde	ed by the CPI	1	0			
» Multicast Route Configuration » Multicast Poute	r VLA	N IDs Enable	d for MLD S	Snooping			0	

- b. For MLD Snooping Admin Mode, select the Enable radio button.
- c. Click Apply.
- 5. Enable MLD snooping on the VLAN 300.
 - a. Select Routing > Multicast > MLD Snooping > MLD VLAN Configuration.

System	Switching	Routi	ng Qo	S Sec	urity Monite	oring Mainte	nance Help	Index						
VLAN STP	Multicast	Address Tab	le Ports	LAG										
MFDB	MLE		onfigurat	tion										
> IGMP Snooping > MLD Snooping	ng N	MLD VLAN Configuration ()												
 Configuration Interface Configuration MLD VLAN 		VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time							
Configuration	ter 🗖	300	Enable 💽											

- **b.** Enter the following information:
 - In the VLAN ID field, enter 300.
 - In the Admin Mode field, select Enable.
- 6. Click Add.

Index

Numerics

802.1d (STP) 802.1s (MSTP) 802.1w (RSTP) 802.1x port security

Α

ACLs (access control lists), configuring 77 active image 274 aggregation, links 51 alerting, emails 289 ARP (Address Resolution Protocol) configuring 74 dynamic inspection 240 auto VoIP 167

B

backup image 274 banner, pre-login 272 bindings, static 252 buffered logging 285

С

class of service (CoS) queuing 133 class, QoS 143 classic STP (802.1d) 323 color conform policy, CoS 177 community port 42 community VLAN 41 compatible mode, MVR 199 configuration scripting 269 CoS (class of service) queuing 133

D

default routes, adding 62 default VLAN 21 DHCP messages, maximum rate 253, 254 DHCP relays, L2 and L3 329 DHCP servers, configuring DHCP snooping Differentiated Services Code Point (DSCP) DiffServ, configuring DNS (domain name system), configuring double VLANs (DVLANs) DSCP (Differentiated Services Code Point) dual image DVLANs (double VLANs) dynamic ARP inspection dynamic locking, port security dynamic mode DHCP servers MVR **205**

E

edge device, DiffServ 143 email alerting 289 external multicast router 190

F

fixed IP address, assigning 308

G

gaming **192** groups, private VLANs **316** guest VLAN **228**

IGMP (Internet Group Management Protocol) snooping and querying 187 IGMP snooping 192 images 274 interior node, DiffServ 143 interpreting log files 282 IP ACLs 79 IP precedence 136 IP routing, configuring 57 IP source guard 254

IPTV 192 IPv6 ACLs 125 DiffServ 170 isolated port 42 isolated VLAN 41

L

L2 and L3 relays, DHCP **329** LAGs (link aggregation groups) **51** logging **282**

Μ

MAC ACLs 78, 112 MAC-based VLANs 22 mapping CoS queues 133 static, ARP ACLs 246 mirroring ACLs 115 ports 273 MLD (multicast listener discovery), configuring 345 MSTP (802.1s) 326 multicast router, external 190 MVR (multicast VLAN registration), configuring 197

Ν

NVT (network virtual terminal) 277

0

outbound, telnet 277

Ρ

policy, QoS 143 port mirroring 273 port routing, configuring 57 port security (802.1x) 222 precedence, IP 136 primary VLAN 41 priority, strict, CoS 137 private edge VLANs 14 private VLAN groups 316 promiscuous port 42 protected ports 216 protocol-based VLANs 25 proxy ARP 74

Q

querier, IGMP **192** queues, CoS **133**

R

RADIUS, assigning VLANs 234 rapid STP (802.1w) 324 redirection, ACLs 120 relays, DHCP 329 routes, adding 62 routing VLANs 66

S

sampling, sFLow 300 scheduler, CoS 137 scripting, configuration 269 security levels, alerts 289 service, QoS 143 sFlow 296 SNMP (Simple Network Management Protocol) 292 snooping DHCP 248 IGMP 187 MLD 346 SNTP (Simple Network Time Protocol), configuring 261 source guard 254 spanning tree protocol 323 static bindings 252 static host name 302 static IP address, assigning 308 static locking, port security 212 static MAC address, port security 215 static mapping 246 static routes, adding 64 strict priority, CoS 137 syslog 282

Т

TCP flags 84 technical support 2 telnet, outbound 277 time zones 265 traceroute 268, 269 trademarks 2 traffic shaping, CoS 140 traplogs 286 traps, SNMP 294 trust mode, CoS 139 trusted ports, CoS 133

U

untrusted ports, CoS 134

V

```
video streaming 192
VLAN routing 66
VLANs 14
configuring 13
double 311
guest 228
multicast router 191
private groups 316
VoIP
auto 167
DiffServ 159
```

W

WRED (weighted random early discard) 133