

VIP-NET-2804PP-1G VIP-NET-4804PP-1G VIP-NET-0424-1G

Multicast Configuration Guide

L2+

'Media Hub' Managed Switch Note: There may be slight variations of web user interface between the network switch models listed above. If you have any questions, please contact support@purelinkav.com.

IGMP Overview

Internet Group Management Protocol (IGMP) allows devices to establish multicast group memberships. The routes between transmitters (sources) and receivers (outputs) is maintained by a table on each switch or router on the multicast network. The master route table is maintained by an IGMP Querier that is either statically or dynamically assigned (*Querier Election). An IGMP aware switch is crucial in sending large amounts of data through a network for time sensitive data like video or audio. IGMP aware switches are capable of treating multicast data packets as directed traffic rather than blindly broadcasting the data packets to every port of the switch. Only devices that have elected to join a multicast group will receive multicast data packets allowing for more efficient network routing.

With Querier Election, each switch starts off assuming it is the IGMP Querier and builds a table of all locally connected multicast devices. After it has identified each multicast device, and the associated groups, it looks for a Router Port (switch-to-switch interconnect). An IGMP Query is sent out each Router Port and the switches begin to elect a single switch as the IGMP Querier (the switch responsible for building the master route table between transmitters and receivers). This is repeated until the switch with the lowest management IP address is located and selected as the IGMP Querier.

Proper configuration allows this process to complete the routing table necessary for connecting transmitters and receivers across VIP-NET.

**Note*: Querier Election is not supported by IGMPv1 devices.

IGMP Snooping

IGMP Snooping is passive and can take 1-2 minutes to build out the routing table when switches are first started up, particularly with a large deployment of multicast devices.

- 1. Login to the VIP-NET switch
- 2. On the left-hand menu, select Multicast \rightarrow IGMP Snooping \rightarrow Basic Configuration

VIP-NET-4804PP-1G × ← → C ▲ Not secure 192	+ 2.168.1.1/ipmc_ign	nps.htm	7 24 31 33 35 37 34 41 41	1.45.47.49.51		- 🛛 * 🏤 * 🙆	× 1					
PureLink	IGMP Snooping Basic Configuration Intere > Multicat > 16MP Snooping											
Switch DMS	Global Con	figuration										
 Port Management PoE Management VLAN Management 	Unregistere	d IPMCv4 Flooding Enabled										
 QoS Spanning Tree MAC Address Tables 	Leave Proxy Proxy Enabl	r Enabled										
Multicast Y IGMP Snooping Sasic Configuration	Port Related Configuration											
> VLAN Configuration	Port	Router Port	Fast Le	eave	Throttling	Filtering Profile						
> Status	•				• •	\$ V						
Groups Information IGMP SFM Information	1				unlimited 🗸	- V Preview						
» MLD Snooping < » MVR <	2				unlimited 🗸	- V Preview						
» Multicast Filtering Profile <	3				unlimited 🖌	- V Preview						
DHCP Security	4				unlimited 🗸	Preview						

- a. Global Configuration
 - i. Snooping Enabled \rightarrow Checked
 - ii. Unregistered IPMCv4 Flooding Enabled \rightarrow Unchecked
 - iii. IGMP SSM Range \rightarrow Default Value
 - iv. Leave Proxy Enabled \rightarrow Unchecked
 - v. Proxy Enabled \rightarrow Unchecked
- b. Port Related Configuration
 - i. Any port that has an Encoder (Transmitter) connected needs to have the Fast Leave box checked.

VIP-NET-4804PP-1G ×	+			
← → C ▲ Not secure 19	2.168.1.1/ipmc_igmps.	htm		* 🎰 🗯 🕲
	39		unlimited ~	- V Preview
	40		unlimited ~	Preview
	41		unlimited V	Preview
	42		unlimited V	-
	43		unlimited V	-
	44		unlimited	- V Preview
	45		unlimited 🗸	Preview
	46		unlimited 🗸	- V Preview
	47		unlimited 🗸	Preview
	48		unlimited 🗸	- V Preview
	49		unlimited 🗸	- V Preview
	50		unlimited V	- V Preview
	51		unlimited 🗸	- V Preview
	52		unlimited 🗸	- V Preview
	Apply Reset]		

ii. Ports 49-52 are used for SFP+ 10Gb switch interconnects. Any port that is connected to another switch should have Router Port checked

- iii. All other settings can be left as default values.
- c. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner.
- 3. On the left hand menu, select Multicast \rightarrow VLAN Configuration

VIP-NET-4804PP-1G	× +											
← → C ▲ Not secure	192.168.1.1/ipmo	_igmps_vlan.htm								1	* 🍈 *	•
PureLink										H (9 🕞	r
VIP-NET-4804PP-1G	IGMP S	nooping VLAN Con	figuration						& Home >	Multicast > IGMP Snooping	> VLAN Config	guration
Switch DMS												
System	< VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (se	ec)
Port Management	< 1			0.0.0.0	IGMP-Auto 🗸	0 🗸	2	125	100	10	1	
PoE Management	<											
VLAN Management	< Apply	Reset										
QoS	<											
Spanning Tree	<											
MAC Address Tables	<											
Multicast	×											
» IGMP Snooping	*											
> Basic Configuration												
> VLAN Configuration												
> Status												
> Groups Information												
> IGMP SFM Information												
» MLD Snooping	<											
» MVR	<											
» Multicast Filtering Profile	<											
DHCP	<											
Security	<											

- a. If there is no VLAN defined, click "Add New IGMP VLAN"
 - i. VLAN ID \rightarrow 1
 - ii. Snooping Enabled \rightarrow Checked
 - iii. Querier Election \rightarrow Checked

- iv. Querier Address \rightarrow Blank or default
- v. Compatibility \rightarrow IGMP-Auto
- vi. PRI \rightarrow Default Value
- vii. RV \rightarrow Default Value
- viii. QI (sec) \rightarrow Default Value
- ix. QRI (0.1 sec) \rightarrow Default Value
- x. LLQI (0.1 sec) \rightarrow Default Value
- xi. URI (sec) \rightarrow Default Value
- b. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner.

Link Aggregation – LACP

Link Aggregation Control Protocol allows for automatic determination, configuration, and monitoring of Link Aggregation Group members. LACP will automatically discover any duplicate routes between any two switches and aggregate them into a single connection so long as LACP is enabled on each port utilized on both switches. Any two switches that are connected via two or more 10G switch-to-switch interconnects should utilize LACP to maximize available bandwidth.

- 1. Login to the VIP-NET switch
- 2. On the left hand menu, select Port Management \rightarrow Link Aggregation \rightarrow LACP Configuration

VIP-NET-4804PP-1G		LACF	Port Confi <mark>g</mark> ura	ation	Home - Port Management - Unik Aggregation - LACP Configu				
Switch	DMS	Port	LACP Enabled	Key	Pole	Timeout	Prio		
System	<	Port	Ener Enabled		Note	Thireout	- 110		
Port Manage	ement 👻			< v	< v	0 V	32768		
> Port Configu	uration	1		Auto 👻	Active 🛩	Fast 🗸	32768		
> Port Statisti	C5								
> SFP Port Info	io.	2		Auto 👻	Active 👻	Fast 👻	32768		
> Energy Effici	lent Ethernet	3		Auto 👻	Activa	Fast ¥	32768		
» Link Aggregi	ation ~	- C				1.222.00	1.000,000		
> Static Conf	figuration	4		Auto 👻	Active 👻	Fast 🗸	32768		
> LACP Confi	lguration	-							
> System Sta	atus	5		Auto 👻	Active Y	Fast 💙	32768		
> Port Status		6		Auto 👻	Active 👻	Fast 🗸	32768		

 Locate the 10G ports that are connected switch-to-switch and check the checkbox for LACP Enabled

45	Auto 👻	Active 🛩	Fast 🗸	32768
46	Auto 🛩	Active 👻	Fast 🗸	32758
47	Auto 😽	Active 🛩	Fast 💙	32768
48	Auto 🛩	Active 👻	Fast 🛩	32768
49	Auto 🛩	Active 👻	Fast 🗸	32768
50	Auto 👻	Active 👻	Fast 👻	32758
51	Auto 🗸	Active 🛩	Fast 🗸	32768
52	Auto 🗸	Active 👻	Fast 🗸	32768

4. Set the **Key value** to a number e.g. 1 for each port that is connected to a second switch. You will need to follow the same guidelines for the second switch. If there is a third switch, you will

need to set a key value for the aggregated ports interlinked to that switch to a different Key value e.g. 2.

48		Active 🗸	Fast 🗸	32768
49	1	Active 🗸	Fast 🗸	32768
50	1	Active 🗸	Fast 🗸	32768
51		Active 🗸	Fast 🗸	32768
52		Active 🗸	Fast 🗸	32768

You can check the success of the settings in the Port Management>Internal Status and Port Management>Neighbor Status pages

=																			
1	LACP Int	ACP Internal Port Status																	
,	uto-refresh Tom Refresh																		
	Port	State	Key	Priority	(Activity	Timeout	Agg	regation	Synchr	onization	Collec	cting	Distributing	Defa	ulted	Expired	4	
	49	Active	1	32768		Active	Fast	Yes		Yes		Yes		Yes	No		No		
	50	Active	1	32768		Active	Fast	Yes		Yes	Yes			Yes No			No		
F	Pure	Link	≡														н	0 (•
	VIP-NET-48	804PP-1G	LACP	leighbor F	Port Statu	us									BHome -	fort Management + Link Agg	pegation -	Neighbor Sta	tus
-	Switch	DMS	Auto-refr	esh O off	Refresh														
•	System Port Management		Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchroni	zation	Collecting	Distributing	Defaulted	Exp	pired	
5	Port Statistic	5	49	Active	1	1	49	32768	Active	Fast	Yes	Yes		Yes	Yes	No	No	0	
>	SFP Port Info		50	Active	1	1	50	32768	Active	Fast	Yes	Yes		Yes	Yes	No	No	9	

5. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner

In a two-switch configuration where switch 1 port 49-50 are connected to switch 2 port 49-50, only ports 49 and 50 on both switches will require the LACP Enabled checkbox to be checked.

In a configuration containing more than 2 switches connected in a series (S1 \leftarrow \rightarrow S2 \leftarrow \rightarrow S3), you may either enable LACP on all interconnect ports (49-52) or enable only ports 49-50 on the first and last switch in the series while enabling ports 49-52 on all intermediary switches between the first and last switch.

IPMC Profile

Port Filtering Profiles allow you to assign a filtering profile to a port for blocking or accepting traffic for specific multicast groups on a per port basis. IGMP Snooping should block multicast traffic to ports that have not elected to join a multicast group, but here you can define additional rules, or block multicast packets explicitly, rather than implicitly through IGMP Snooping built routing tables.

1. Login to the VIP-NET switch

2. On the left hand menu, select Multicast \rightarrow Multicast Filtering Profile \rightarrow Filtering Address Entry

VIP-NET-4804PP-1G ×	+						
← → C ▲ Not secure 1	92.168.1.1/ipmc_lib_e	ntry_table.htm?&DynDisplayNum=2	20&DynChannelGrp=		1	* 🏤 🕯	F 🕑 E
PureLink					н	0 🕞	F
VIP-NET-4804PP-1G	Multicast F	iltering Profile Addres	s Configuration	8 Home > Multicast	> Multicast Filtering Profile >	Filtering Addre	iss Entry
Switch DMS	Refresh Ei	ret Entry Next Entry					
▶ System <	Navigate Addre	ass Entry Setting in IBMC Profi	le by 20 entries per page				
▶ Port Management <	Mavigate Addre	as they setting in the rion	entries per page.				_
▶ PoE Management <	Delete	Entry Name	Start Address	End Address			
► VLAN Management <		NoMulticast	224.0.0.0	239.255.255.254			
► QoS <							
▶ Spanning Tree 〈	Add New Add	ress (Range) Entry					
► MAC Address Tables <	Apply Rese	et					
▶ Multicast ×							
» IGMP Snooping <							
» MLD Snooping <							
» MVR (
Filtering Profile Table							
> Filtering Address Entry							
► DHCP <							
 Security < 							
Access Control <							
► SNMP <							
Event Notification <							

- a. To block all Multicast traffic
 - i. Select "Add New Address (Range) Entry"
 - ii. Entry Name \rightarrow NoMulticast
 - iii. Start Address \rightarrow 224.0.0.0
 - iv. End Address → 239.255.255.254
- b. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner

3. On the left-hand menu, select Multicast \rightarrow Multicast Filtering Profile \rightarrow Filtering Profile Table

VIP-NET-4804PP-1G	× +				- 🗆 X					
← → C ▲ Not secure 1	192.168.1.1/ipmc_	lib_profile_table.htm			🖈 🎰 🗯 🕑 🗄					
PureLink										
VIP-NET-4804PP-1G	Multica	st Filtering Profile	e Configuration	Home > Multicast >	Multicast Filtering Profile > Filtering Profile Table					
Switch DMS	Multicas	t Filtering Profile Glo	bal Setting							
System Port Management System PoF Management	Multicast	Ist Filtering Profile Mode								
 VLAN Management 	Multicas	t Filtering Profile Tak	ole Setting							
► QoS <	Delete	Profile Name	Profile Description		Rule					
Spanning Tree MAC Address Tables		NoMulticast	blocks multicast traffice		Preview					
 Multicast » IGMP Snooping « MLD Snooping « MVR 	Add New Apply	Filtering Profile								
» Multicast Filtering Profile · Filtering Profile Table Filtering Address Entry										
► DHCP <										
▶ Security <										
► Access Control <										
▶ SNMP <										
Event Notification Construction										
5105105105										

- a. IPMC Profile Global Setting
 - i. Multicast Filtering Profile Mode \rightarrow Enabled
- b. IPMC Profile Table Setting
 - i. If no profiles exist, click Add New IPMC Profile
 - 1. Profile Name \rightarrow NoMulticast
 - 2. Profile Description \rightarrow Blocks multicast traffic

c. Once a profile exists, click the edit icon under Rule on the right side of the IPMC Profile Table Setting table.

VIP-NET-4804PP-1G	× +					- 🗆 ×
← → C ▲ Not secure	192.168.1.1/ipmc_lib_rule_table.htm?CurSidV=0&Dc	PdxOp=1&DynBgnPdx=0x4e0x6f0x	4d0x750x6c0x740x690x630x610x730>	(74	☆	🏤 🗯 😰 🗄
Pure Link VIP-NET-4804PP-1G	■	Multicast] Rule Settin	gs (In Precedence Orde	r) æHome > Multica	st > Multicast Filtering Profile > Filt	tering Profile Table
Switch DMS	Profile Name & Index	Entry Name	Address Range	Action	Log	
System Port Management	< NoMulticast 1	· •	~	Deny 🗸	Disable 🗸	⊕© ⊗©
 PoE Management VLAN Management 	< Add Last Rule Commit Reset	Ba NoMulticast ion				
▶ QoS <	<					
▶ Spanning Tree <	<					
MAC Address Tables	<					
Multicast	~					
» IGMP Snooping <	<					
» MLD Snooping <	<					
» MVR <	<					
» Multicast Filtering Profile ~	~					
> Filtering Profile Table						
> Filtering Address Entry						
▶ DHCP <	<					
▶ Security <	<					
Access Control	<					
▶ SNMP <	<					
Event Notification	<					
 Diagnostics 	<					

- 1. Click Add Last Rule
- 2. Under Entry Name, select NoMulticast.
- 3. Address Range will populate.
- 4. Action \rightarrow Deny
- 5. Log \rightarrow Disable
- 6. Click Commit
- 4. Apply the filtering profile to a specific port.

- VIP-NET-4804PP-1G × + ← → C ▲ Not secure | 192.168.1.1/ipmc_igmps.htm 🖈 🚓 🏞 😰 : PureLink = H 0 C P VIP-NET-4804PP-1G IGMP Snooping Basic Configuration Home > Multicast > IGMP Snooping > Basic Configuration Switch DMS Global Configuration System < on ▶ Port Management < Snooping Enabled PoE Management <</p> Unregistered IPMCv4 Flooding Enabled VLAN Management < IGMP SSM Range 8 \ 232.0.0.0 < ▶ QoS < Leave Proxy Enabled Spanning Tree MAC Address Tables < Proxy Enabled ~ Multicast Port Related Configuration » IGMP Snooping > Basic Configuration Router Port Fast Leave Throttling Filtering Profile Port > VLAN Configuration 0 ~ > Status \diamond ~ > Groups Information 1 unlimited 🗸 ~ > IGMP SFM Information » MLD Snooping < 2 unlimited 🗸 » MVR » Multicast Filtering Profile < unlimited 🗸 3 < ▶ DHCP unlimited V 4 < Security < 5 unlimited 🗸 ~ Access Control < ▶ SNMP unlimited 🗸 ✓ Preview 6
- 5. On the left-hand menu, select Multicast \rightarrow IGMP Snooping \rightarrow Basic Configuration

- i. Locate the port number you would like to assign a filtering profile.
- ii. Using the drop-down menu on the right side of the table, select the IPMC Profile for the port.
- iii. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner.