

AXXESSMARINE



PEPLINK MEDIAFAST 500

AXXESS MARINE

support@axxess-marine.com

Phone: +1 954 354 2077

www.axxess-marine.com



SUMMARY

Peplink MEDIAFAST 500	3
Network Settings	3
Grouped Networks	4
Outbound Policy	5
Access Rules	7
Content Blocking	8
Bandwidth Control	9
Usage Reports	10

PEPLINK MEDIAFAST 500

To access the Peplink MediaFast 500 dashboard, type the Gateway on your browser and fill user/password to access the Peplink's main page.

The screenshot shows the Peplink MediaFast 500 dashboard. The top navigation bar includes 'Dashboard', 'Network', 'AP', 'System', and 'Status', with 'Apply Changes' on the right. The main content area is divided into several sections:

- WAN 1 - 4G SIM1:** IP Address: [Details...], Status: Connected (green dot), Disconnect button.
- WAN 2 - 4G SIM2:** IP Address: [Details...], Status: Connected (green dot), Disconnect button.
- WAN 3 - VSAT Data:** IP Address: [Details...], Status: Connected (green dot), Disconnect button.
- WAN 4 - GSM Data:** IP Address: (none), Status: No Cable Detected (red dot).
- LAN Interface:** Router IP Address: [Input field]
- Device Information:**
 - Model: Peplink MediaFast 500
 - Firmware: 8.0.2 build 2721
 - Uptime: 10 days 11 hours 20 minutes
 - CPU Load: [Progress bar] 15%
 - Fan Speed: 7458 rpm
 - Temperature: 49.0 °C / 120.2 °F
 - Throughput: ↓ 168.0 kbps ↑ 466.0 kbps

Network Settings

In this session, you can create and manage your Virtual LANs to define some settings and controls within your network.

Go to your Peplink's webpage, click on **Network**, **Network Settings** and you can see your Virtual LANs.

The screenshot shows the Peplink MediaFast 500 Network Settings page. The top navigation bar includes 'Dashboard', 'Network', 'AP', 'System', and 'Status', with 'Apply Changes' on the right. The left sidebar shows a tree view with 'WAN' selected. The main content area is divided into several sections:

- WAN:** A table showing the configuration for each WAN connection.
- IPv6:** A toggle switch set to 'Disabled'.
- WAN Quality Monitoring:** A dropdown menu set to 'Auto'.

Connection Name	Method	Routing Mode	Type
1. WAN 1 - 4G SIM1	DHCP	NAT	Always-on
2. WAN 2 - 4G SIM2	DHCP	NAT	Always-on
3. WAN 3 - VSAT Data	DHCP	NAT	Always-on
4. WAN 4 - GSM Data	DHCP	NAT	Always-on
5. WAN 5 - Not Used	PPPoE	NAT	Always-on
6. Mobile Internet - Not Used	PPP	-	Backup (Priority 2)

peplink Dashboard **Network** AP System Status Apply Changes

WAN

LAN

- Network Settings
- Port Settings

VPN

- SpeedFusion
- IPsec VPN
- GRE Tunnel

Outbound Policy

Inbound Access

- Servers
- Services
- DNS Settings

NAT Mappings

MediaFast

- Cache Settings
- Prefetch Schedule

ContentHub

Docker

MDM Settings

Captive Portal

LAN

IP Settings

IP Address (/24)

Network Settings

Name

VLAN ID

Inter-VLAN routing

DHCP Server

DHCP Server Enable

DHCP Server Logging

IP Range - (/24)

Lease Time Days Hours Mins

DNS Servers Assign DNS server automatically

WINS Servers Assign WINS server

BOOTP

Extended DHCP Option

Option	Value
No Extended DHCP Option	

Add

All changes must be **saved** and **applied**.

Grouped Networks

In this session you can Add, Set and Edit your network groups to improve your management inside the internet in your Yacht. To do this, go to **Network**, scroll down and click on **Grouped Networks**, choose a name and the IP addresses that will participate in that group.

peplink Dashboard **Network** AP System Status Apply Changes

WAN

LAN

- Network Settings
- Port Settings

VPN

- SpeedFusion
- IPsec VPN
- GRE Tunnel

Service Passthrough

Grouped Networks

Grouped Networks

Name	Networks
All Networks	<input type="checkbox"/>
AV	<input type="checkbox"/>
User WIFI Networks	<input type="checkbox"/>
Crew & Officer	<input type="checkbox"/>
owner and guest	<input type="checkbox"/>

Add Group

All changes must be **saved** and **applied**.

Outbound Policy

You can define customized rules to manage the outbound traffic behavior. The rule Default will be applied to traffic that does not match with any higher precedence rules.

The screenshot shows the Peplink Outbound Policy configuration interface. The sidebar on the left contains navigation links for WAN, LAN, VPN, Inbound Access, NAT Mappings, MediaFast, ContentHub, Docker, MDM Settings, and Captive Portal. The main content area is titled "Outbound Policy" and shows a table of rules. The table has columns for Service, Algorithm, Source, Destination, and Protocol / Port. The "Default" rule is highlighted, and an "Add Rule" button is visible at the bottom.

Service	Algorithm	Source	Destination	Protocol / Port	
			Any	Any	X
			Any	Any	X
			Any	Any	X
			Any	Any	X
			Any	Any	X
			IP Network	Any	X
			Any	Any	X
			Any	TCP 443	X
Default			(Auto)		

This table allows you to fine tune how the outbound traffic should be distributed to the WAN connections.

Click the Add Rule button to add a new rule or the existent rule to make changes.

The screenshot shows the Peplink Outbound Policy configuration interface with the "Edit Custom Rule" dialog box open. The dialog box has fields for Service Name, Enable, Source, Destination, Protocol, Algorithm, and Enforced Connection. The "Enforced Connection" field is highlighted, and the "Save" and "Cancel" buttons are visible.

Service	Algorithm	Source	Destination	Protocol / Port	
All Networks	Enforced WAN: WAN 3 - VS...	Grouped Network All Networks	Any	Any	X
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	X
Default			(Auto)		

This field allows you to choose the WAN selection algorithm.

Weighted Balance - Traffic will be proportionally distributed among available WAN connections according to the specified load distribution weight;

Persistence - Traffic coming from the same machine will be persistently routed through the same WAN connection;

Enforced - Traffic will be routed through the specified connection regardless of the connection's health status;

Priority - Traffic will be routed through the healthy connection that has the highest priority;

Overflow - Traffic will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load;

Least Used - Traffic will be routed through the healthy WAN connection that is selected in the field Connection and has the most available downlink bandwidth;

Lowest Latency - Latency checking packets will be periodically sent to all selected healthy connections. Latency will then be determined by the response time of the second and third hops. New traffic will then be routed to a healthy connection with the lowest average latency during that detection period;

Fastest Response Time - Traffic will be duplicated and sent to all selected healthy connections. The connection with the earliest response will be used to send all further traffic from the session for the fastest possible response time. If there are any slower responses received from other connection afterwards, they will be discarded. As a result, this algorithm selects the most responsive connection on a per session basis.

The screenshot displays the Peplink management interface. The left sidebar contains navigation menus for WAN, LAN, VPN, Outbound Policy, Inbound Access, NAT Mappings, MediaFast, ContentHub, Docker, MDM Settings, Captive Portal, and QoS. The main area shows the 'Outbound Policy' configuration page with a table of rules. An 'Edit Custom Rule' dialog is open, allowing configuration of a new rule. The 'Enforced Connection' dropdown menu is expanded, showing a list of WAN connections, with 'WAN: WAN 3' highlighted. The background table shows existing rules like 'All Networks' and 'HTTPS Persistence'.

This setting means all the users in Grouped Network XYZ will be **enforced** to use the WAN 3. This forces Crew/Officer networks to use VSAT connections (for example).

Access Rules

You can create rules to deny an internet group or a specifically person. To do this, go to Network, Access Rules, Internal Network Firewall Rules and click on Add Rule.

The screenshot shows the PepiLink web interface with the following sections:

- WAN**
- LAN**
 - Network Settings
 - Port Settings
- VPN**
 - SpeedFusion
 - IPsec VPN
 - GRE Tunnel
- Outbound Policy**
- Inbound Access**
 - Servers
 - Services
 - DNS Settings
- NAT Mappings**
- MediaFast**
 - Cache Settings
 - Prefetch Schedule
- ContentHub**
- Docker**
- MDM Settings**
- Captive Portal**
- QoS**

The main content area displays several rule tables:

- Outbound Firewall Rules:** Table with columns: Rule, Protocol, Source, Destination, Action. Row: Default, Any, Any, Any, [Green Checkmark].
- Inbound Firewall Rules:** Table with columns: Rule, Protocol, WAN, Source, Destination, Action. Row: Default, Any, Any, Any, Any, [Green Checkmark].
- Internal Network Firewall Rules:** Table with columns: Rule, Protocol, Source, Destination, Action. Row: Block Users to Ship, Any, User WIFI Networks, [Empty], [Red X]. A red arrow points to this row.
- Intrusion Detection and DoS Prevention:** Disabled.
- Local Service Firewall Rules:** Table with columns: Rule, Service, WAN, Source, Action. Row: Default, Any, Any, Any, [Green Checkmark].

The 'Edit a Firewall Rule' dialog box shows the following configuration:

- Rule Name:** Block Users to Ship
- Enable:**
- Protocol:** Any
- Source:** Grouped Network, User WIFI Networks
- Destination:** Network, IP: [Empty], Mask: 255.255.255.0 (/24)
- Action:** Allow, Deny
- Event Logging:** Enable. A blue arrow points to this checkbox.

Buttons: Save, Cancel

This rule example means when its allowed, all users tagged with User WIFI Networks into the Grouped Networks will be unable to use internet.

Content Blocking

Choose applications to be blocked from LAN/PPTP/PepVPN peer clients' access, except for those on the Exempted User Groups or Exempted Subnets defined below.

You can block Audio/Video Streaming, Pornography, Database, Email, File Sharing and others applications into the Pepwave. To do this, click on **Network, Content Blocking**, mark the applications and categories, mark or unmark the exempted users and/or groups.

To Block a specifically website, you should click on **Customized Domains**, fill with the domain. Examples: **facebook.* youtube.*** and click on .

All changes must be **saved** and **applied**.

Example: How to block **Netflix** to **Crew Network**:

Go to 10.0.8.1 **Network, Content Blocking** and in the session **Customized Domains**, type:

nflximg.*

netflix.*

nflxext.com

nflxvideo.net

nflxext.com

Mark **Manager** and **Guest** as **Exempted User Groups**, **Save** and click on **Apply Changes**.

The screenshot shows the Pepwave web interface with the following sections:

- Navigation:** Dashboard, Network (selected), AP, System, Status, Apply Changes.
- Left Sidebar:** WAN, LAN (Network Settings, Port Settings), VPN (SpeedFusion, IPsec VPN, GRE Tunnel), Outbound Policy, Inbound Access (Servers, Services, DNS Settings), NAT Mappings, MediaFast (Cache Settings, Prefetch Schedule), ContentHub, Docker, MDM Settings, Captive Portal, QoS (User Groups, Bandwidth Control, Application), Firewall (Access Rules, Content Blocking), Routing Protocols.
- Application Blocking:** Please Select Application...
- Web Blocking:**
 - Preset Category: High, Moderate, Low, Custom
 - Selected Categories: Adware, P2P/File sharing, Malware, Social Networking, Violence, Aggressive, Drugs, Gambling, Pornography, Contraband, Weapons, Audio-Video, File Hosting, Games, Proxy/Anonymizer, Update Sites
 - Content Filtering Database Auto Update:
 - Customized Domains:

nflximg.*	<input type="button" value="X"/>
netflix.*	<input type="button" value="X"/>
nflxext.com	<input type="button" value="X"/>
nflxvideo.net	<input type="button" value="X"/>
nflxext.com	<input type="button" value="+"/>
 - Exempted Domains from Web Blocking:
- Exempted User Groups:**

Manager	<input checked="" type="checkbox"/> Exempt
Staff	<input type="checkbox"/> Exempt
Guest	<input type="checkbox"/> Exempt
- Exempted Subnets:**

Network	Subnet Mask
<input type="text"/>	255.255.255.0 (/24) <input type="button" value="+"/>
- URL Logging:**

Bandwidth Control

Using the Peplink you can define how much minimum bandwidth will be reserved to each user group when a WAN connection is in full load **or/and** you can define a maximum download speed will be reserved for each WAN connection to Guest/Crew (owner no limit).

To do this, you need to know your VLANs and IP Addresses and go to **Network, User Groups, Add** and in **Grouped by** mark **Subnet** and fill the IP Address from Owner/Crew/Guest and mark as **Manager/Staff/Guest** respectively. Example:

These settings mean the IP addresses 0.0.0.0/24 will follow the bandwidth rules as **Manager** (Normally Owner - no limit by default).

After to defining all groups, click on **Bandwidth Control** and check the best option for you and change the settings according to your needs. Example:

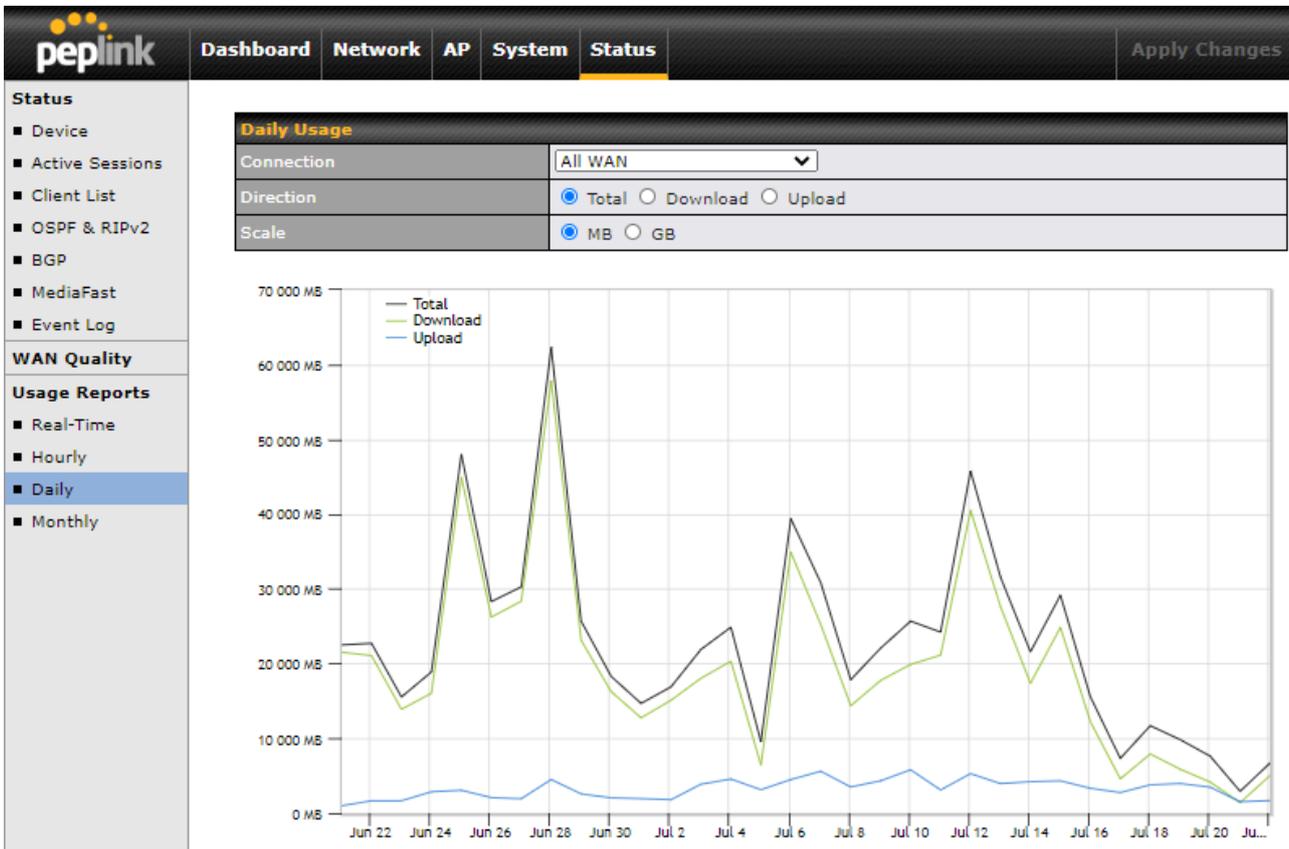
User Bandwidth Limit		Download	Upload
Manager:	Unlimited	Unlimited	Unlimited
Staff:	0	0	0
Guest:	0	0	0

All changes must be **saved** and **applied**.

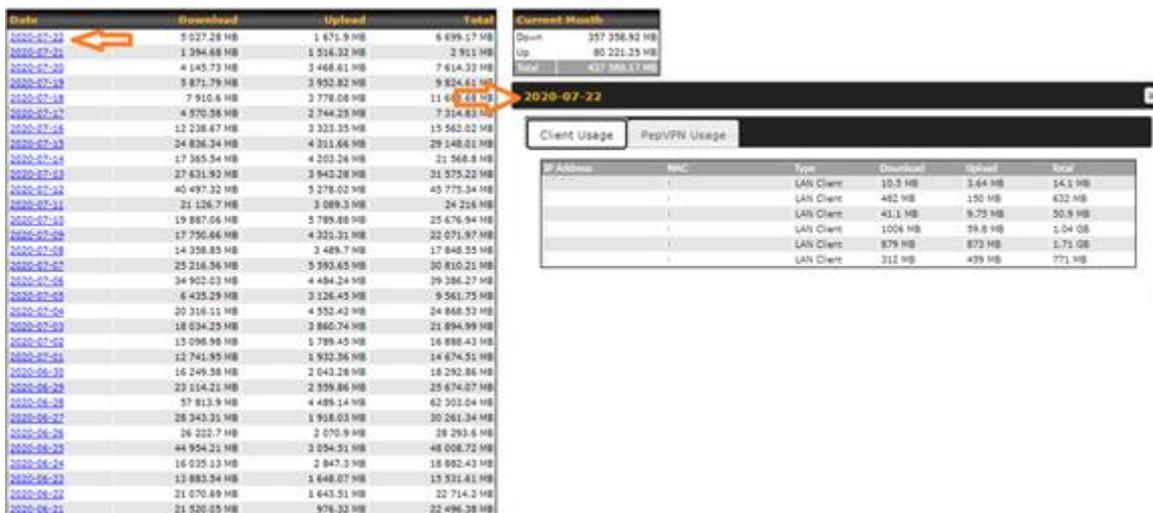
Usage Reports

Your Peplink is able to show you all the internet usage in different times (Real time, Hourly, Daily and Monthly). You can see how much download each user made in these different times. To see these informations, go to **Status** and click on **Real time**, **Hourly**, **Daily** or **Monthly**.

Example: You click in **Daily** and see a usage graph:



Scrolling down and you see the usage total per day (figure below left), clicking in a day, you can see details about this day (figure below right):



** If you want to make changes, we are here (Support Phone and Portal) to help if you have problems. But also if you want to change something, you can always ask us and we can do it remotely.*