

a mind for networks



# NetEnforcer

## AC-6000 Series

Traffic Management Device

### Hardware Guide

(P/N D360016 R1)





# **NetEnforcer AC-6000 Series Hardware Guide**

P/N D360016 R1





## Important Notice

Allot Communications Ltd. ("Allot") is not a party to the purchase agreement under which NetEnforcer was purchased, and will not be liable for any damages of any kind whatsoever caused to the end users using this manual, regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ALLOT OR ANY OF ITS SUBSIDIARIES. ALLOT ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Please read the End User License Agreement and Warranty Certificate provided with this product before using the product. Please note that using the products indicates that you accept the terms of the End User License Agreement and Warranty Certificate.

WITHOUT DEROGATING IN ANY WAY FROM THE AFORESAID, ALLOT WILL NOT BE LIABLE FOR ANY SPECIAL, EXEMPLARY, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, LOSS OF REVENUE OR ANTICIPATED PROFITS, OR LOST BUSINESS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## Copyright

Copyright © 1997-2012 Allot Communications. All rights reserved. No part of this document may be reproduced, photocopied, stored on a retrieval system, transmitted, or translated into any other language without a written permission and specific authorization from Allot Communications Ltd.

## Trademarks

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe. Allot and the Allot Communications logo are registered trademarks of Allot Communications Ltd.

*NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.*

*Changes or modifications not expressly approved by Allot Communication Ltd. could void the user's authority to operate the equipment.*

---

## Version History

Each document has a version and a build number. You can tell the exact version and build of this document by checking the table below. Details of this document version are contained in the top row of the table below.

Document updates are released in electronic form from time to time and the most up to date version of this document will always be found on Allot's online Knowledge Base. To check for more recent versions, login to the support area [www.allot.com/support.html](http://www.allot.com/support.html) and from the knowledgebase tab, enter the title of this document into the search field.

Doc Version	Software Version	Date	Summary of Changes
v1b7	AOS12.3.2 and above	18 December, 2012	Sample Configurations added
v1b6	AOS12.3.2 and above	10 September, 2012	
v1b5	AOS12.3.2 and above	03 September, 2012	
v1b4	AOS12.3.2 and above	29 August, 2012	
v1b3	AOS12.3.2 and above	27 August, 2012	
v1b2	AOS12.3.2 and above	12 July, 2012	
v1b1	AOS12.3.2 and above	5 July, 2012	

---

# TABLE OF CONTENTS

Important Notice .....	v
Version History.....	vi
TABLE OF CONTENTS .....	vii
<b>CHAPTER 1: NETENFORCER HARDWARE .....</b>	<b>1-1</b>
<b>Packing List.....</b>	<b>1-1</b>
<b>Front Panel.....</b>	<b>1-2</b>
Front Panel LEDS Description .....	1-2
Front Panel Connectors.....	1-3
<b>Rear Panel .....</b>	<b>1-4</b>
Power Supply.....	1-4
<b>Interfaces .....</b>	<b>1-5</b>
Modules .....	1-5
Cabling.....	1-6
<b>Bypass Units.....</b>	<b>1-8</b>
<b>CHAPTER 2: CONNECTING THE NETENFORCER .....</b>	<b>2-1</b>
<b>Sample Configurations.....</b>	<b>2-1</b>
Configuration 1 .....	2-2
Configuration 2.....	2-2
Configuration 3.....	2-3
Configuration 4.....	2-3
Configuration 5.....	2-3
<b>Connecting the Bypass Units .....</b>	<b>2-4</b>
<b>Power Connections .....</b>	<b>2-7</b>
Connection to AC Power .....	2-7
Connection to DC Power .....	2-7
Grounding .....	2-8
Powering the NetEnforcer Up and Down .....	2-10
<b>CHAPTER 3: CONFIGURING THE NETENFORCER.....</b>	<b>3-1</b>
<b>Configuring Via a Terminal or Telnet.....</b>	<b>3-1</b>
<b>Changing the Passwords .....</b>	<b>3-3</b>
<b>CHAPTER 4: REDUNDANCY .....</b>	<b>4-1</b>
<b>Active Redundancy.....</b>	<b>4-1</b>
Connections .....	4-2
Configuration.....	4-4
<b>CHAPTER 5: ASYMMETRIC TRAFFIC .....</b>	<b>5-1</b>
<b>Guidelines.....</b>	<b>5-1</b>
<b>Asymmetric Configuration .....</b>	<b>5-2</b>

---

<b>CHAPTER 6: COMMAND LINE INTERFACE.....</b>	<b>6-1</b>
Chassis CLI.....	6-1
<b>CHAPTER 7: SAFETY INFORMATION .....</b>	<b>7-1</b>
General .....	7-1
Chassis Safety .....	7-2
Unpacking.....	7-2
Installation .....	7-3
Rack mounting information .....	7-3
Power Connection Information.....	7-3
Airflow information.....	7-5
Preventing Surge.....	7-5
Laser Safety Requirements.....	7-6
Laser Classification.....	7-6
Laser Information .....	7-6
Laser Safety Statutory Warning.....	7-6
Training for Laser Safety .....	7-6
Laser Device Operating Precautions.....	7-6
<b>CHAPTER 8: TECHNICAL SPECIFICATIONS.....</b>	<b>8-1</b>
AC-6000 Series.....	8-1



---

## TABLE OF FIGURES

Figure 1-1 – AC-6000 Fiber .....	1-1
Figure 1-2 – NetEnforcer Front Panel: AC-6000 Fiber Series .....	1-2
Figure 1-3 – Internal/External Links .....	1-3
Figure 1-4 – NetEnforcer AC Power Feed .....	1-4
Figure 1-5 – NetEnforcer DC Power Feed .....	1-4
Figure 1-6 – Dual LC Connector .....	1-8
Figure 1-7 – Multi-Port Copper Bypass Unit .....	1-9
Figure 1-8 – Multi-Port Fiber Bypass Unit .....	1-9
Figure 2-1 – Possible Port Distribution Schemes .....	2-1
Figure 2-2 – Internal/External Links .....	2-1
Figure 2-3: Connecting the External Bypass .....	2-4
Figure 2-4 – Dual Head Cable .....	2-6
Figure 4-1 – Connecting the NetEnforcer for Active Redundancy .....	4-4
Figure 5-1: Asymmetric Traffic – Network Diagram .....	5-1
Figure 5-2: Asymmetry Configuration dialog .....	5-2
Figure 5-3: Asymmetry Group - New dialog .....	5-3
Figure 5-4: VLans Settings dialog .....	5-4
Figure 5-5: Port Properties dialog .....	5-5



## Chapter 1: NetEnforcer Hardware

---

The Allot NetEnforcer AC-6000 Series is designed to manage Internet traffic on multiple Ethernet links at speeds of up to 16Gbps, utilizing 8 x 10G/1G interfaces and an additional 8 x 1G interfaces. Providing real-time monitoring, policy enforcement and traffic steering, these flexible devices help operators control bandwidth utilization and costs while ensuring quality of experience (QoE) for all network users.



**Figure 1-1 – AC-6000 Fiber**

The NetEnforcer AC-6000 is available with either fiber or copper interfaces.

### Packing List

Verify that the following items are included with NetEnforcer:

- NetEnforcer (hardware with pre-installed software)
- Two mains power cables according to National Electrical Code for AC Models, or two DC power cable for DC Models.
- 1 Serial Console Cable
- 1 Management Cable (Cross)
- Rack Mounting Kit (side mounting brackets, screws, four rubber bumpers)
- Bypass Module (hardware depends upon model and interface type).
- Bypass Cables (in the Bypass Accessory Kit, the number of cables and cables type depends upon model and interface type)
- Bypass Rack Mounting Kit (side mounting brackets, screws)
- Data SFP+/SFP Transceivers (Type and Number of Transceivers depends upon model and interface type)
- CD kit with AOS software and Release Notes

All NetEnforcer models contain a lithium battery on the main board. The recommended battery type is RENATA CR1220.

## Front Panel

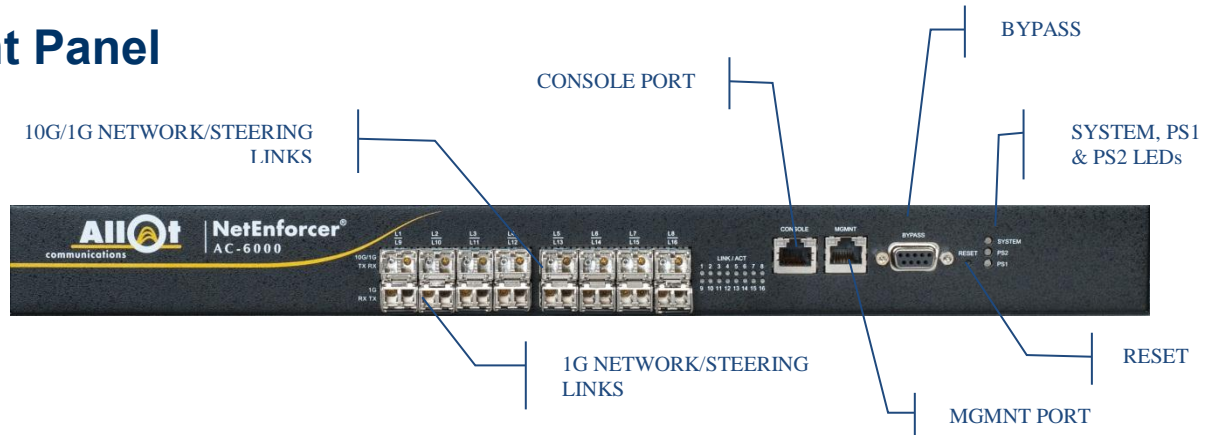


Figure 1-2 – NetEnforcer Front Panel: AC-6000 Fiber Series

## Front Panel LEDs Description

- **SYSTEM** shows the current status of the system. If the LED appears **STEADY GREEN**, the NetEnforcer is functioning normally and if it appears **STEADY RED**, a fatal error has occurred. If the LED is **OFF**, the unit is in Bypass Mode.
- **PS1** indicates the status of Power Supply One. If the LED appears **STEADY GREEN**, the Power Supply is functioning normally, if it is **STEADY RED**, then the Power Supply is in place, but not providing power. If the LED is **OFF**, it means the Power Supply is malfunctioning.

When the software on the AC-6000 has been shut down, both PS LEDs will appear as **BLINKING GREEN**, indicating the power cable can be removed to fully power down the system. In this event, the system may be restarted by pressing the reset button.

- **PS2** indicates the status of Power Supply Two. If the LED appears **STEADY GREEN**, the Power Supply is functioning normally, if it is **STEADY RED**, then the Power Supply is in place, but not providing power. If the LED is **OFF**, it means the Power Supply is malfunctioning.

When the software on the AC-6000 has been shut down, both PS LEDs will appear as **BLINKING GREEN**, indicating the power cable can be removed to fully power down the system. In this event, the system may be restarted by pressing the reset button.

- **INTERNAL/EXTERNAL LINK LEDs** are located to the right of the Internal/External connections. A single LED is present for each interface and will appear as **STEADY GREEN** indicating the link is connected or **BLINKING GREEN** indicating traffic.

## Front Panel Connectors

- **INTERNAL/EXTERNAL LINKS** There are 8 x 1G/10G Ethernet network interfaces on the top row supporting SFP fiber, SFP+ fiber or SFP copper interfaces. In addition, there are 8 x 1G interfaces on the bottom row supporting SFP fiber or SFP copper. Fiber units use SM Fiber optic cable. Copper units use standard FTP CAT 5e Ethernet cable, and the interface auto-negotiates the connections to be 10BASE-T, 100BASE-T, or 1000BASE-T.



**Figure 1-3 – Internal/External Links**

Ports L1-L8 are on the top row and may be used for either 10G or 1G network or steering interfaces. Ports L9-L16 are located below them and may be used for 1G network or steering interfaces only.

For ports L1-L8 (10G/1G), the TX connection is on the left and the RX connection is on the right. For ports L9-L16 (1G), the RX connection is on the left and the TX is on the right.

LINK/ACT LEDs for each connection are located together to the right of the interfaces.

- **CONSOLE port** (RJ-45 connector). The serial RS232 port is implemented as an RJ-45 connection.
- **MGMNT** is the System's management port with a 1G Ethernet interface (RJ-45 connectors) and should be used for system monitoring and maintenance. This port allows connections to external management devices. The port auto negotiates the connections to be 10BASE-T, 100BASE-T, or 1000BASE-T.
- **BYPASS** (D-Type connector) should only be used to connect the NetEnforcer to the Bypass unit.

**CAUTION** The Bypass connector should **ONLY** be connected to the Allot Multiport Bypass Unit. The Bypass connector should always be connected to the bypass unit. When not in use, the Bypass connector should be kept covered.

The bypass cable should only be connected/disconnected when the system is powered down.

## Resetting the NetEnforcer

The reset button is located in a small recessed hole set on the NetEnforcer faceplate. Pressing the reset button will restart the system in the event of shutdown, indicated by both PS1 and PS2 LEDs BLINKING GREEN.

## Rear Panel

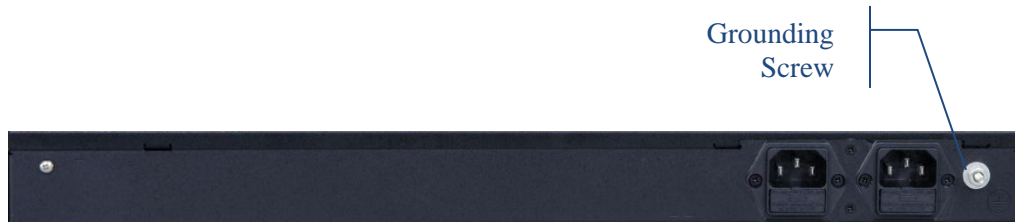
The rear panel of the NetEnforcer contains the following:

- Grounding Screw
- Two Power Inlets

## Power Supply

The NetEnforcer contains two built in power supply modules and a dual line feed for Redundancy purposes. Each line feed drives one power supply. It is possible for the unit to operate normally with only one of the two power supplies active.

**NOTE**      **The AC power supply automatically adapts to voltages between 100 V and 240 V, 50/60 Hz.**



**Figure 1-4 – NetEnforcer AC Power Feed**



**Figure 1-5 – NetEnforcer DC Power Feed**

## Interfaces

### Modules

#### Supported 10G module types

The AC-6000 supports the following 10G module types:

MODULE	MEDIA TYPE	RANGE
<b>10G-BASE-SR</b>	Multi mode	400m
<b>10G-BASE-LR</b>	Single mode	10km
<b>10G-BASE-ER</b>	Single mode	40km

10G modules fit SFP+ ports

#### Supported 1G module types

The AC-6000 supports the following 1G module types:

MODULE	MEDIA TYPE	RANGE
<b>1000Base-SX</b>	Multi mode	220m
<b>1000Base-LX</b>	Single mode	10km
<b>1000Base-LX</b>	Single mode	40km
<b>1000Base-ZX</b>	Single mode	80km
<b>10/100/1000Base-T</b>	Copper	100m

1G modules fit both SFP & SFP+ ports

## Cabling

### 1G Ethernet Copper Interface

**NOTE** Ethernet Cables for connecting the NetEnforcer to Network may be Straight or Cross, the Copper interface will automatically match your network connection.

Shielded CAT 5 or higher cables must be used in order to insure compliance.

CONNECTIONS	CABLE TYPE	CONNECTOR TYPE
<b>Management Port</b>	Ethernet (CAT 6) (Included, P/N C411011)	RJ-45
<b>Console Port</b>	Serial (Included, P/N C002005B)	RJ-45
<b>Bypass (Internal/External)</b>	Ethernet (CAT 6) (Included, P/N C411008)	RJ-45
<b>NetEnforcer's Bypass Connector to Bypass Unit</b>	Bypass Cable (Included, P/N C351036)	D-Type 9-Pin
<b>Between Bypass Unit Internal/External to Network</b>	Ethernet (CAT 6)	RJ-45

### Multi Mode Fiber Interface

CONNECTIONS	CABLE TYPE	CONNECTOR TYPE
<b>Management Port</b>	Ethernet (CAT 6) (Included, P/N C411011)	RJ-45
<b>Console Port</b>	Serial (Included, P/N C002005B)	RJ-45
<b>Bypass (Internal/External)</b>	62.5/125 MM fiber optic straight cable (Included, P/N C411014)	Dual LC
<b>NetEnforcer's Bypass Connector to Bypass Unit</b>	Bypass Cable (Included, P/N C702001)	D-Type 9-Pin



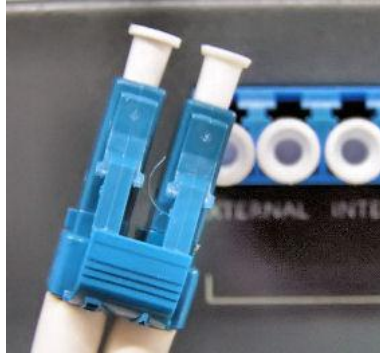
CONNECTIONS	CABLE TYPE	CONNECTOR TYPE
<b>Between Bypass Unit Internal/External to Network</b>	Standard 62.5/125 or 50/125 MM fiber optic cross cable	Dual LC

### Single Mode Fiber Interface

CONNECTIONS	CABLE TYPE	CONNECTOR TYPE
<b>Management Port</b>	Ethernet (CAT 6) (Included, P/N C411011)	RJ-45
<b>Console Port</b>	Serial (Included, P/N C002005B)	RJ-45
<b>Bypass (Internal/External)</b>	9/125 SM fiber optic straight cable (Included, P/N C411015)	Dual LC
<b>NetEnforcer's Bypass Connector to Bypass Unit</b>	Bypass Cable (Included, P/N C702001)	D-Type 9-Pin
<b>Between Bypass Unit Internal/External to Network</b>	Standard 9/125 SM fiber optic cross cable	Dual LC

## Connectors

NetEnforcer Multi-Port Bypass Units using Multi Mode fiber (MM) or Single Mode fiber (SM) utilize dual LC Connectors.



**Figure 1-6 – Dual LC Connector**

**NOTE** Color and appearance of actual connectors may vary.

## Bypass Units

The NetEnforcer operates with an external Bypass Unit. The Bypass Unit is a mission-critical subsystem designed to ensure network connectivity at all times. The Bypass mechanism provides "connectivity insurance" in the event of a NetEnforcer subsystems failure.

When the system moves to bypass mode, the bypass unit internally cross connects between its internal and external ports so all traffic entering the bypass unit is forwarded directly through the bypass unit without passing through the in-line platform.

The following bypass units are supported by the AC-6000:

PRODUCT NUMBER	DESCRIPTION
A102052F	BP Fiber MM Dual Line SC ports
A102059F	BP Fiber SM Dual Line SC
A102087F	BP Copper Dual Line
A102086F	BP Fiber SM Dual Line LC ports
A102002F	BP Fiber MM Dual Line LC ports
A102004F	BP Copper Dual Line (SP)
A102059F	BP Fiber SM Dual Line SC Ports

**CAUTION** A NetEnforcer unit must be connected to an appropriate Bypass Unit. This is to ensure continuous service in the event of failure.

A separate NetEnforcer Bypass package is included with your NetEnforcer shipment.

**NOTE** The total distance of the link between the External and Internal is defined by the interface type. The maximum range remains the same despite the presence of the NetEnforcer. For example if a 1000BaseT interface is used, the total allowed distance between the router and the switch is still limited to 100 meters, despite the inclusion of the NetEnforcer.

**CAUTION** The Bypass connector should ONLY be connected to the Allot Multiport Bypass Unit. The Bypass connector should always be connected to the bypass unit. When not in use, the Bypass connector should be kept covered.

## Multi-Port Copper Bypass Unit

The Multi-port Copper Bypass Unit works in conjunction with the NetEnforcer Copper.



**Figure 1-7 – Multi-Port Copper Bypass Unit**

**NOTE** Use the supplied UTP CAT-6 straight Ethernet cables to connect link connections marked with Internal and External labels.

The Copper Bypass Unit includes RJ-45 connectors for Ethernet cables and D-type 9-pin connectors for connection to the Bypass port on the NetEnforcer.

## Multi-Port Fiber Bypass Unit

The Multi-Port Fiber Bypass Unit works in conjunction with the NetEnforcer Fiber.



**Figure 1-8 – Multi-Port Fiber Bypass Unit**

**NOTE** Use 62.5/125 or 50/125 or 9/125 fiber optic cables with dual LC connectors (not provided) to connect 1 Gbps fiber ports of the switch and the router.

The Multi-Port Fiber Bypass Unit includes connectors for connecting to up to 4 links on the NetEnforcer. The Link Connectors area includes two quad LC connectors for each link. In addition, the Multi-Port Fiber Bypass Unit includes D-type 9-pin connectors for connection to the Bypass port on the NetEnforcer.



## Chapter 2: Connecting the NetEnforcer

### Sample Configurations

The 16 ports (8 1G and 8 1G/10G) of the AC-6000 may be connected in different combinations of network ports and steering ports, as well as different combinations of 1G and 10G connections, depending on your requirements.

The table below outlines several typical configurations which are described in more depth below. These are intended as examples only.

**NOTE**      **The total bandwidth of the AC-6000 may never exceed 16GB**

Network Ports		Steering Ports		BW Distribution Example		# Bypass	Network Description
10G	1G	10G	1G	Network	Steering		
-	8	-	-	8G	-	1	Small 1G network with growth option
-	12	-	4	12G	4G	2	Medium 1G network with 1G steering
2	-	-	4	12G	4G	1	Typical 10G network with 1G steering
4	-	2	-	12G	4G	1	10G Network with steering
8 (4X2)	-	-	-	16G	-	-	Large 10G Network with active redundancy

**Figure 2-1 – Possible Port Distribution Schemes**

Ports L1-L8 are on the top row and may be used for either 10G or 1G network or steering interfaces. Ports L9-L16 are located below them and may be used for 1G network or steering interfaces only.

**NOTE**      **For ports L1-L8 (10G/1G), the TX connection is on the left and the RX connection is on the right. For ports L9-L16 (1G), the RX connection is on the left and the TX is on the right.**



**Figure 2-2 – Internal/External Links**

## Example 1: 1GE Network Ports

This configuration is designed for a small network that currently utilizes 1G links only. The eight 1G ports along the bottom row are being used for network traffic only. This configuration allows for a great deal of expansion via the available 1G/10G interfaces on the top row which can be used for either network or steering purposes.

L1	L2	L3	L4	L5	L6	L7	L8
Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected
L9	L10	L11	L12	L13	L14	L15	L16
Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G

## Example 2: 1GE Network and Steering Ports

This configuration is designed for a medium sized network that utilizes 1G links only. All sixteen ports are being used with 1G interfaces. Twelve ports are being used for network traffic while four are reserved for steering.

L1	L2	L3	L4	L5	L6	L7	L8
Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G
L9	L10	L11	L12	L13	L14	L15	L16
Network Link 1G	Network Link 1G	Network Link 1G	Network Link 1G	Steering 1G	Steering 1G	Steering 1G	Steering 1G

### Example 3: 10GE Network with 1GE Steering Ports

This configuration is designed for a larger network that requires a 10G link. Two 10G interfaces are being used for network traffic while four 1G interfaces are being used for steering.

L1	L2	L3	L4	L5	L6	L7	L8
Network Link 10G	Network Link 10G	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected
L9	L10	L11	L12	L13	L14	L15	L16
Not Connected	Not Connected	Not Connected	Not Connected	Steering 1G	Steering 1G	Steering 1G	Steering 1G

### Example 4: 10GE Network and Steering Ports

This configuration is designed for a larger network that utilizes 10G links only. Four 10G ports are being used for network traffic and two 10G ports are being used for steering.

L1	L2	L3	L4	L5	L6	L7	L8
Network Link 10G	Network Link 10G	Network Link 10G	Network Link 10G	Not Connected	Not Connected	Steering 10G	Steering 10G
L9	L10	L11	L12	L13	L14	L15	L16
Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected

### Example 5: 10GE Network with Active Redundancy

This configuration is designed for a large network that requires Active Redundancy and utilizes all eight 10G ports for network traffic.

L1	L2	L3	L4	L5	L6	L7	L8
Network Link 10G	Network Link 10G	Network Link 10G	Network Link 10G	Network Link 10G	Network Link 10G	Network Link 10G	Network Link 10G
L9	L10	L11	L12	L13	L14	L15	L16
Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected	Not Connected

## Connecting the Bypass Units

The NetEnforcer operates with external Bypass Units. The Bypass Unit is a mission-critical subsystem designed to ensure network connectivity at all times. The Bypass mechanism provides ‘connectivity insurance’ in the event of a NetEnforcer subsystems failure. NetEnforcer Copper units operate with a Copper Bypass and NetEnforcer Fiber units operate with a Fiber Bypass. Bypass Units are connected to NetEnforcer by a series of leads and cables.

Each Bypass unit can handle between 1 and 4 network links. When connecting more than 4 network links, you will need two bypass units connected by the dual-head cable described below.

**CAUTION** The bypass cable should only be connected/disconnected when the system is powered down.

### External Bypass Unit Connections

**NOTES** The total distance of the link between the External and Internal is defined by the interface type. The maximum range remains the same despite the presence of the NetEnforcer. For example if a 1000BaseT interface is used, the total allowed distance between the router and the switch is still limited to 100 meters, despite the inclusion of the NetEnforcer.

In each connection to the Bypass unit, the Tx port is on the left-hand side and the Rx port is on the right-hand side.

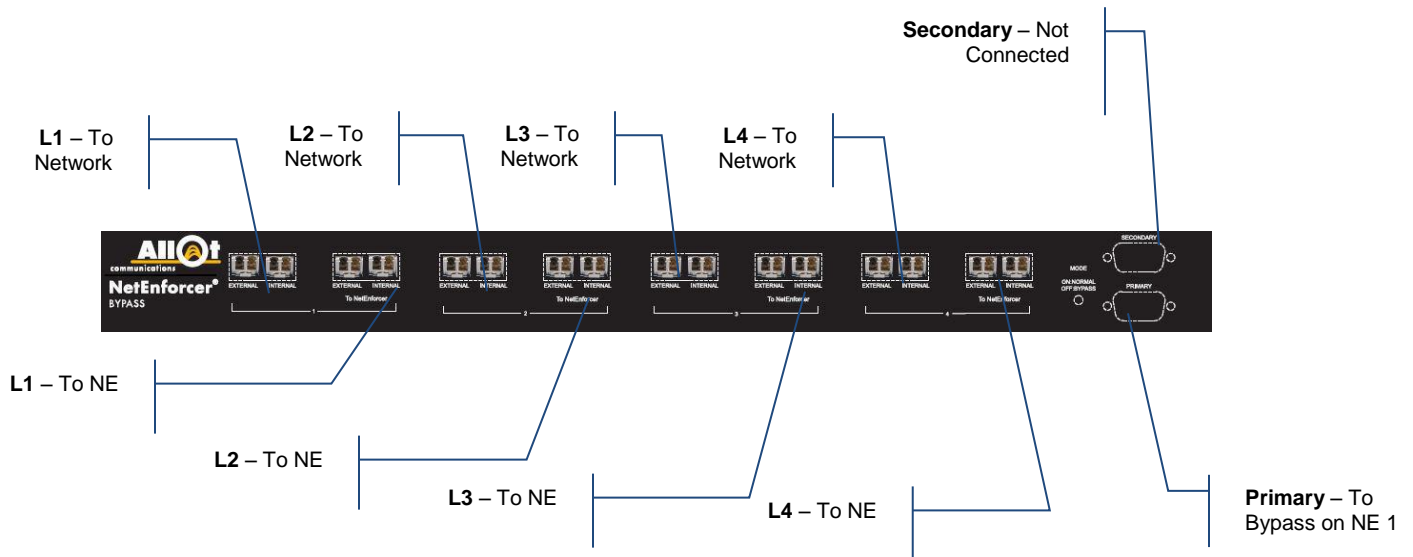


Figure 2-3: Connecting the External Bypass



## Connecting one External Bypass Units

**CAUTION** The bypass cable should only be connected/disconnected when the system is powered down.

1. Connect Network links to the external bypass unit(s); Verify (ping) that traffic runs via bypass unit
2. Connect fiber ports on the NE to a Bypass unit.

Connect one side of the Bypass Control cable to the PRIMARY port on the External Bypass unit and the other side to the Bypass connection on the NE.

3. Power up the chassis
4. Verify connectivity (ping) & use the following CLI commands (for more information, see page 6-1) to confirm that traffic is running via the NetEnforcer:

```
acmon  
acstat
```

## Connecting Two External Bypass Units using a Dual Head Cable

**CAUTION** The bypass cable should only be connected/disconnected when the system is powered down.

Two bypass units are connected and managed by the same AC-6000 device via a Dual Head cable.

Each Dual Head cable can utilize any of the following combinations of external bypass units:

- 2 Fiber bypass units
- 2 Copper bypass units
- 1 Copper bypass unit and 1 Fiber bypass unit

Remember that the bypass units must have the same interfaces (Single-Mode Fiber, Multi-Mode Fiber or Copper) that are utilized by the AC-6000.

**NOTE** The Dual Head cable may be used ONLY with AC-6000 units.



**Figure 2-4 – Dual Head Cable**

**NOTE**      **If one branch of the Dual-Head cable is disconnected from the bypass or the connection fails, the system will go into Bypass.**

1. Log into the AC-6000 and enter the following CLI command to enable use of the Dual Head cable:  
**go config bypass -unit 1:update:external:1:2**
2. Connect Network links to two external bypass units; Verify that traffic runs via bypass unit (ping).
3. Connect NetEnforcer network ports to the Bypass units. Ports may be connected to any available ports on any of the Bypass Units as long as EXTERNAL is matched with odd numbered ports and INTERNAL with even numbered ports.
4. Connect the special Dual Head Control Cable directly from the Bypass port on the NetEnforcer PRIMARY connections on the 1st and 2nd External Bypass units.
5. Power up the chassis
6. Verify connectivity (ping) & use the following CLI commands (for more information, see page 6-1) to confirm that traffic is running via the NetEnforcer:  
**acmon**  
**acstat**

## Power Connections

### Connection to AC Power

Make sure the wall socket outlet is installed near the equipment and that the socket is easy to access. The wall socket outlet must be connected to the building installation protection.

When connecting NetEnforcer to 100-240 VAC supply, plug into 10A service receptacles, type N5/10 or NEMA 5-10R. Ensure that each site has a suitable ground. Ground all metal racks, enclosures, boxes and raceways. The NetEnforcer equipment should be reliably grounded through the power supply cord.

**NOTE**      **The Power supply cords are intended to serve as the disconnect device. The user can power down the device only by removing all power cords from the power source or the NetEnforcer itself.**

Connect one end of the AC power cord to the power connector on the switch rear panel. As the NetEnforcer powers on it begins the power-on self-test, a series of tests that run automatically to ensure that the NetEnforcer functions properly.

**NOTE**      **If the NetEnforcer is powered through a DC power supply, see Connection to DC Power, below.**

Connect the other end of the power cable to a grounded AC outlet. In addition, a grounding wire may also be connected to the Grounding Screw located on the rear panel of the NetEnforcer.

**CAUTION**      **This unit is intended for RESTRICTED ACCESS LOCATIONS in accordance with NEC (National Electric Code) or the authority having jurisdiction. The power supply cable is comprised of three sets of 2x14 AWG copper wires; use UL-listed cable only.**

### Connection to DC Power

**NOTE**      **The Power supply cords are intended to serve as the disconnect device. The user can power down the device only by removing all power cords from the power source or the NetEnforcer itself.**

**CAUTION**      **Use a UL listed 10A Dual Pole circuit breaker between a centralized DC power system and the NetEnforcer power entry module.**

1. Before performing the following procedure, ensure that power is removed from DC circuit.
2. Verify that power is off to the DC-input circuit.
3. Wire the DC-input power supply to the terminal block, ensuring that all wire connections are secure. Suggested minimum DC-input wires are 14-AWG. Two power cables are supplied by Allot in the accessory kit.

Use Copper UL recognized conductors:

- Connect the ground wire to the ground connector (you should always connect the ground wire first and disconnect it last).
  - Connect the power source 48V to the ‘-’ connector of the NetEnforcer
  - Connect the power source ‘Return’ to the ‘+’ connector of the NetEnforcer.
4. Restore power to the DC circuit by turning the circuit breaker on (I). Do not restore power until you are ready to boot the NetEnforcer system.

When connecting NetEnforcer to 48V, use a UL-Listed 10A Dual Pole circuit breaker between the centralized DC power system and NetEnforcer power entry module as the disconnect device incorporated in the fixed wiring. The circuit breaker must be close to the NetEnforcer and easily accessible.

The DC supply source is to be located within the same premises as this equipment. There shall be no switching or disconnecting devices in the grounded circuit conductor between the DC source and the point of connection of the grounding electrode conductor.

## Grounding

All NetEnforcer equipment has a connection between the grounded conductor of the DC supply circuit and the grounding conductor.

Connect to a reliably grounded SELV source. Grounding is achieved through connection of the power entry module grounding terminal to one power port of the terminal block by min. No. 12 AWG green/yellow conductor.

This equipment shall be connected directly to the DC supply system grounding electrode conductor or to a bonding jumper from grounding terminal bar or bus to which the DC supply system grounding electrode is connected. When connecting the supply wires to the DC main supply, the earth conductor will be connected first and disconnected last.

This equipment shall be located in the same immediate area such as adjacent cabinets or any other equipment that has a connection between the grounded conductor of the same DC supply circuit and the grounding conductor, and also the point of grounding of the DC system. The DC system shall not be grounded elsewhere.

**CAUTION** **DC Unit Grounding:** Before connecting the product to the power line, make sure that the protective ground terminal of the device is connected to the safety ground conductor of the mains power cord.

The mains plug should only be inserted in a socket outlet provided with a connected safety ground. The protective action must not be negated by use of an extension cord (power cable) without a protective conductor (grounding). Any interruption of the protective (grounding) conductor or disconnection of the protective ground terminal can make the device unsafe to use. Intentional interruption is prohibited.

This equipment has a connection between the earthed conductor of the DC supply circuit and the earthing conductor.

## Powering the NetEnforcer Up and Down

### To power up the NetEnforcer:

**NOTE** It is recommended to connect the two power line feeds to separate power sources to have full power redundancy.

1. Connect Power Supply 1 and Power Supply 2 to a power source.
2. The **PS1** and **PS2** LEDs on the front panel of the NetEnforcer appears STEADY GREEN indicating that both power cables are in place and providing power.
3. The **SYSTEM** LED on the front panel of the NetEnforcer appears STEADY GREEN indicating that the NetEnforcer is performing normally.

**NOTE** Should one of the power supplies fail during start up, power will be shut down to the entire system and the **SYSTEM LED** will appear **STEADY RED** to indicate a fatal error. If case one of the power supplies fails after the system is up and running no shutdown will occur.

### To power down the NetEnforcer:

1. Halt the NetEnforcer via the CLI Command Line:

```
sysadmin@host-prc:~#: ac_halt
```

The **PS1** and **PS2** LEDs will turn OFF. To protect the NetEnforcer from inadvertent heat damage, the fans will continue to run until the power cables are disconnected from the unit.

2. Disconnect both power cables from the NetEnforcer.

## Chapter 3: Configuring the NetEnforcer

---

In order to manage and configure NetEnforcer policies remotely from your Web browser, several basic parameters must be configured on NetEnforcer. You can configure these basic parameters using a terminal connected to NetEnforcer.

### Configuring Via a Terminal or Telnet

You can use a standard terminal /PC running terminal emulation software connected to the Console port, or Telnet via the internet to configure a NetEnforcer. If you choose to connect via the Console port, most standard windows-based PC systems have a terminal emulation program called *HyperTerminal* that can be used for this purpose. Configure the terminal to run VT100 terminal emulation with the following parameters:

- Baud rate 19200
- Data: 8 bits
- No parity
- Stop bits 1
- No flow control

### To connect a terminal to the NetEnforcer:

1. Use the supplied serial cable to connect the terminal to the Console Connector on the front panel of the NetEnforcer.
2. Connect the power cables and power up the NetEnforcer.
3. At the terminal, select **Start > Programs > Accessories** and click on the **HyperTerminal** icon. Enter a name for the session and then to set the com port and the parameters (see above). The system boots up and you are prompted for a login and a password.
4. Enter **sysadmin** for the login and **sysadmin** (by default) for the password.
5. Press **<Enter>**.

### To connect to a NetEnforcer via Telnet:

1. Open a Microsoft DOS window on a PC and at the C:\ prompt, enter **Telnet** (IP address of NetEnforcer). Press **<Enter>**. The system boots up and you are prompted for a login and a password.
2. Enter **sysadmin** for the login and **sysadmin** (by default) for the password.
3. Press **<Enter>**.

### Configuring the NetEnforcer:

Use the **go config ips** command to configure the IP address, gateway IP, DNS and NTP servers for the NetEnforcer.

Command: **go config ips**

Usage: **go config ips <-OPTION> <VALUE>...**

Options:

-h	Hostname	set host name of NE
-d	Domain	set domain name of NE
-g	<type:ip>	set gateway IP address
-dns	<dns1:dns2> none	set DNS IP addresses
-ts	<ntp1:ntp2:ntp3> none	set NTP time server IP addresses
-ip	<type:ip:mask[:vlan]>	set IP/netmask/VLAN ID of interface



Examples:

**To set the IP address of the NetEnforcer:**

```
sysadmin@host-prc:~#: go config ips -ip <NE IP ADDRESS> :<SUBNET MASK>
```

**To set the gateway IP:**

```
sysadmin@host-prc:~$ go config ips -g <GATEWAY IP ADDRESS>
```

**To set the DNS server:**

```
sysadmin@host-prc:~$ go config ips -dns <DNS IP ADDRESS>
```

**To set the NTP server:**

```
sysadmin@host-prc:~$ go config ips -ts <NTP IP ADDRESS>
```

## Changing the Passwords

Allot provides end-users with CLI access to the system via a user privilege called “**sysadmin**”. The sysadmin user can access all of the CLI commands outlined in Chapter 6 below. The default password for the sysadmin user is **sysadmin**.

In addition, each NetEnforcer has an “**admin**” password, which is used to enable secure communication between the NetXplorer and the NetEnforcer. Whenever a NetXplorer Operator wishes to add a new NetEnforcer to the NetXplorer the admin password of that NetEnforcer must be entered. In addition, no policy changes can be saved without the correct NetEnforcer admin password. The default admin password is **allot**.

**NOTE** Allot **STRONGLY** recommends that the default passwords are changed to ensure a minimum level of security.

**To change the sysadmin password:**

1. Use the supplied serial cable to connect the terminal to the Console Connector on the front panel of the NetEnforcer.

OR

Enable SSH and open an SSH session to the NetEnforcer.

2. Enter **sysadmin** for the login and the sysadmin password (default is **sysadmin**), and then press **<Enter>**.
3. Enter **passwd** and then press **<Enter>**.
4. Enter a new password and press **<Enter>**. The password must be between 5 and 8 characters. You can use a combination of upper and lower case letters and numbers.

5. Re-enter the new password and press **<Enter>**.

**TIP**            **You can further protect access to the NetEnforcer by limiting the hosts that are allowed to manage the unit. For more information see the NetXplorer Operation Guide.**

**To change the admin password:**

1. Use the supplied serial cable to connect the terminal to the Console Connector on the front panel of the NetEnforcer.

OR

Enable SSH and open an SSH session to the NetEnforcer.

2. Enter **sysadmin** for the login and the sysadmin password (default is **sysadmin**), and then press **<Enter>**.
3. Enter **change\_admin\_pass** and then press **<Enter>** to run the script to change the admin password.
4. Enter a new admin password and press **<Enter>**.
5. Re-enter the new password and press **<Enter>**.

## Chapter 4: Redundancy

---

### Active Redundancy

Active redundancy is recommended for network topologies where at least two network links are active in load-balancing mode. It requires two NetEnforcers and typically, no bypass units.

In the Active Redundancy configuration, each NetEnforcer manages a single link while duplicating the link's traffic to the other NetEnforcer. Both NetEnforcers are active. Each unit shapes the traffic of one link only, but the shaping algorithm considers traffic of both links.

In the event that one of the links fails due to router, switch or line malfunction, the network redundancy mechanism (for example, spanning tree) will ensure that traffic is routed or switched via the other link and managed by the second NetEnforcer. Since both NetEnforcers maintain a constant view of the two links, there will be no loss of flow's state and other information required for correct shaping and application classification.

In the Active Redundancy configuration, the two NetEnforcers should share the same policy configuration.

**NOTE** Users should be aware that a NetEnforcer working in Active Redundancy mode duplicates all traffic passing through it. Therefore, the overall throughput of each NetEnforcer in Active Redundancy will be half of the throughput enabled by the current license key.

## Connections

**L1/L2, L5/L6, L9/L10 & L13/L14** are used to pass actual traffic – these interfaces will be used to connect the NetEnforcers to the corresponding switches or routers.

**L3/L4, L7/L8, L11/L12 & L15/L16** are used to duplicate traffic and pass it to the second NetEnforcer. Traffic that is passed between NetEnforcers is not sent to adjacent network devices – it is only used for monitoring and classification purposes.

**NOTE** If the NetEnforcer Active Redundancy mechanism is implemented a bypass unit should not be used. This ensures that the network is made aware of any failure and is able to smoothly transfer traffic to the secondary link.

## Connection Matrix

The Connection Matrix Tables below are designed to simplify the procedure of connecting the NetEnforcer in Active Redundancy mode.

NetEnforcer A:

<b>L1</b>	<b>L2</b>	<b>L3</b>	<b>L4</b>	<b>L5</b>	<b>L6</b>	<b>L7</b>	<b>L8</b>
Network Link 1 (10G/1G)	Network Link 1 (10G/1G)	NetEnforcer B L3 (10G/1G)	NetEnforcer B L4 (10G/1G)	Network Link 2 (10G/1G)	Network Link 2 (10G/1G)	NetEnforcer B L7 (10G/1G)	NetEnforcer B L8 (10G/1G)
<b>L9</b>	<b>L10</b>	<b>L11</b>	<b>L12</b>	<b>L13</b>	<b>L14</b>	<b>L15</b>	<b>L16</b>
Network Link 3	Network Link 3	NetEnforcer B L11 (1G)	NetEnforcer B L12 (1G)	Network Link 4	Network Link 4	NetEnforcer B L15 (1G)	NetEnforcer B L16 (1G)

NetEnforcer B:

<b>L1</b>	<b>L2</b>	<b>L3</b>	<b>L4</b>	<b>L5</b>	<b>L6</b>	<b>L7</b>	<b>L8</b>
Network Link 1 (10G/1G)	Network Link 1 (10G/1G)	NetEnforcer A L3 (10G/1G)	NetEnforcer A L4 (10G/1G)	Network Link 2 (10G/1G)	Network Link 2 (10G/1G)	NetEnforcer A L7 (10G/1G)	NetEnforcer A L8 (10G/1G)
<b>L9</b>	<b>L10</b>	<b>L11</b>	<b>L12</b>	<b>L13</b>	<b>L14</b>	<b>L15</b>	<b>L16</b>
Network Link 3	Network Link 3	NetEnforcer A L11 (1G)	NetEnforcer A L12 (1G)	Network Link 4	Network Link 4	NetEnforcer A L15 (1G)	NetEnforcer A L16 (1G)

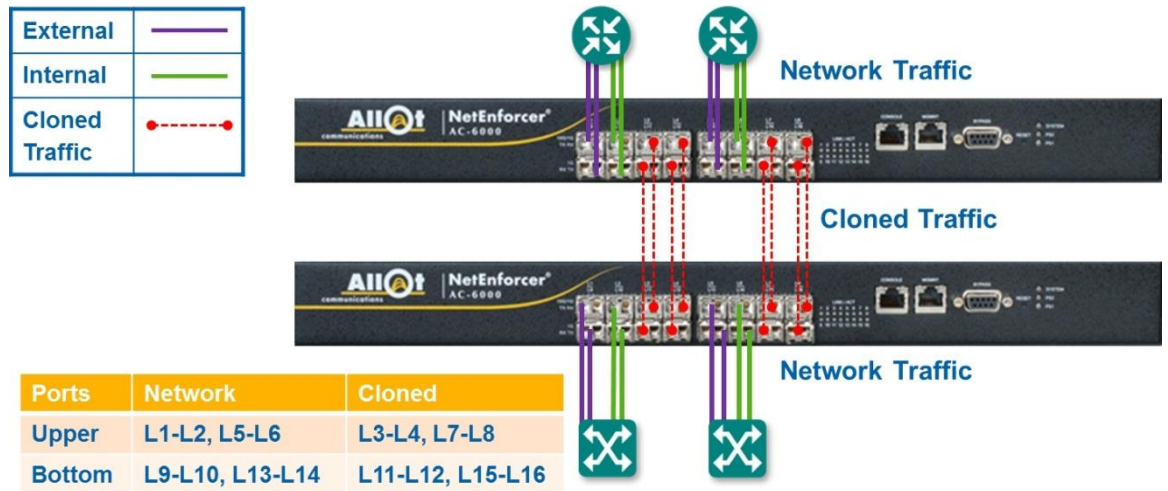


Figure 4-1 – Connecting the NetEnforcer for Active Redundancy

## Configuration

Active redundancy can be configured on the AC-6000 either via the NetXplorer GUI or via NetEnforcer CLI.

### Via NetXplorer GUI

#### To configure Active Redundancy:

1. Log into NetXplorer
2. Select the NetEnforcer you wish to configure in the Navigation Pane.
3. Right-click the NetEnforcer and select **Configuration** from the drop down menu.

OR

Click the **Configuration** button in the Toolbar.

4. Open the **NIC** tab and in the *Action on Failure* field, set L1, L2, L5, L6, L9, L10, L13 and L14 to **fail paired port**.
5. Set L3, L4, L7, L8, L11, L12, L15 and L16 to **No Action** in the *Action on Failure* field.
6. Open the **Networking** tab and set the *Redundancy Mode* to **Active**. This will automatically change the Port Usage of the relevant ports to **Cloned**.

7. Confirm that the **Enable Bypass Unit** checkbox is not selected.
8. Click **Save**. The system will reboot.

After rebooting, you can view the changes from the Configuration tab.

For more information concerning NetEnforcer configuration via NetXplorer, see the **NetXplorer Operation Guide**.

## Via NetEnforcer CLI

### To configure Active Redundancy:

1. Log into the NetEnforcer via Telnet (see page 3-1).

OR

Open a console connection to the NetEnforcer and use the following CLI commands:

#### *To disable the bypass unit:*

**go config network -bypass\_unit disable**

#### *To set redundancy mode:*

**go config network -redund\_mode active**

**NOTE** There is no need to change the port usage settings after running the previous command for enabling active-redundancy the port usage for the cloned ports will be set automatically.

#### *To change NIC settings:*

**go config nic {<Label:Mode:Speed[:FailureAction:PortUsage]}**

Acceptable Labels are: L1, L2, L3, L4, L5, L6, L7, L8, L9, L10, L11, L12, L13, L14, L15, L16, MGMNT

Acceptable values for Mode are: full, auto

Acceptable values for Speed are: 10, 100, 1000, 10000, auto

Acceptable values for Failure Action are: none, fail\_pair, fail\_all, bypass

#### **Examples:**

**go config nic L1:auto:auto:fail\_pair**

**go config nic L2:auto:auto:fail\_pair**

**go config nic L3:auto:auto:none**

**go config nic L4:auto:auto:none**

```
go config nic L5:auto:auto:fail_pair
go config nic L6:auto:auto:fail_pair
go config nic L7:auto:auto:none
go config nic L8:auto:auto:none
go config nic L9:auto:auto:fail_pair
go config nic L10:auto:auto:fail_pair
go config nic L11:auto:auto:none
go config nic L12:auto:auto:none
go config nic L13:auto:auto:fail_pair
go config nic L14:auto:auto:fail_pair
go config nic L15:auto:auto:none
go config nic L16:auto:auto:none
```

*To view redundancy mode:*

```
go config view network
```

*To view NIC settings:*

```
go config view nic
```



## Chapter 5: Asymmetric Traffic

In some network topologies the traffic flows of a single connection can take different paths in the upstream and the downstream directions. This can lead to a situation where one NetEnforcer on the network sees one flow of the connection while another NetEnforcer that is located remotely sees the complementary flow of the same connection. Since DPI should inspect both flows of the connection, this may lead to reduced accuracy when identifying the applications running in the network.

Asymmetric Traffic is designed to significantly increase DPI accuracy by allowing NetEnforcer devices to share information concerning connections. This will ensure that two different flows may be identified as part of the same connection, even when their traffic is handled by different NetEnforcers. Ideally, using Asymmetric Traffic should provide the same percentage of DPI accuracy with remotely located NetEnforcers as is found when a single NetEnforcer sees both sides of the connection.

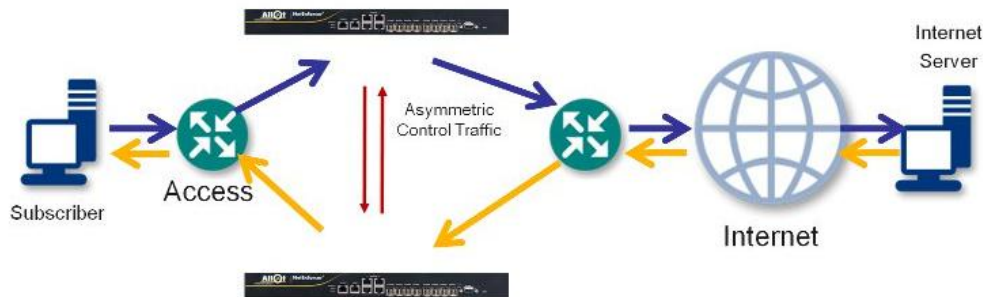


Figure 5-1: Asymmetric Traffic – Network Diagram

### Guidelines

Asymmetric Traffic information is synched between all devices that belong to the same Asymmetric Device Group (ADG) which is configured via NetXplorer using the NetXplorer GUI. All devices in an ADG must be assigned to the same NetXplorer installation and each NetXplorer may support up to eight ADGs.

An ADG can include co-located devices (e.g. NE1 & NE2, NE3 & NE4) and remotely located devices (devices in POP1 and devices in POP2). Co-located devices are connected with intra-site asymmetric control link. This link passes control information between the co-located devices to sync the DPI information while remotely located devices are connected over an L2/L3 network.

Each ADG may be configured with up to eight devices and has a group ID of 0 through 7. Each device configured to an ADG has a local ID of 0 through 7. Therefore a NetEnforcer may have a local ID of 1 in ADG 0.

## Asymmetric Configuration

**NOTE** The physical port that may be used for Asymmetry is the Service1 port on the front of the device.

Asymmetric traffic is configured from the NetXplorer User Interface.

### To define an Asymmetric Device Group (ADG).

1. Right click on the Network in the Navigation pane and select **Asymmetry Configuration**.

OR

Highlight the Network in the Navigation pane and select **Asymmetry Configuration** from the View menu.

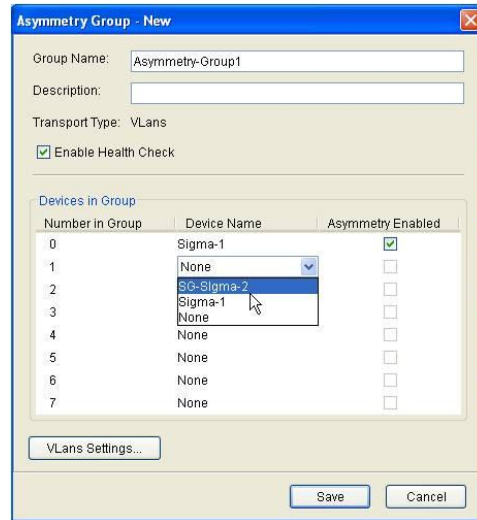
The Asymmetry Configuration dialog appears.



**Figure 5-2: Asymmetry Configuration dialog**

2. In the Asymmetry Groups field you see any ADGs currently configured on the NetXplorer. Select an ADG and click **Edit** to alter the configuration, or add/remove devices from an existing ADG.
3. To create a new ADG, click **Add**.

The Asymmetry Group – New dialog appears.



**Figure 5-3: Asymmetry Group - New dialog**

4. Enter a **Group Name** and **Description** in the appropriate fields.
5. Select the **Enable Health Check** checkbox if you wish NetXplorer to automatically confirm the health of all devices in the ADG.

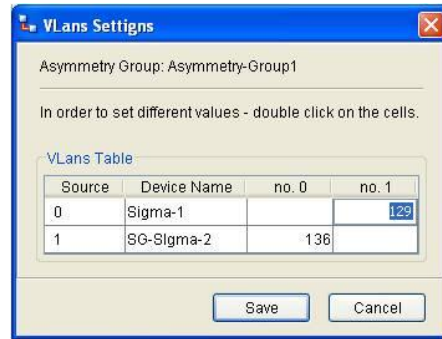
#### To assign devices to the ADG:

1. Assign up to eight devices to the ADG. This will automatically define a local ID for each device you add.
2. Select the devices to add to the group from the drop down menus in the Asymmetry Group – New dialog box. The Device ID will be established based on the order you place them in inside the ADG. For example, if the Sigma 1 selected as Number in Group 0 will have a Device ID of 0 for the purposes of Asymmetry.
3. Select the **Asymmetry Enabled** checkbox for each device.

#### To create VLAN IDs:

1. Create a VLAN ID for each point to point link in each direction. A mesh configuration is required between all devices.
2. Click the **VLANs Settings** button to edit the VLAN configuration.

The Vlan Settings dialog appears.

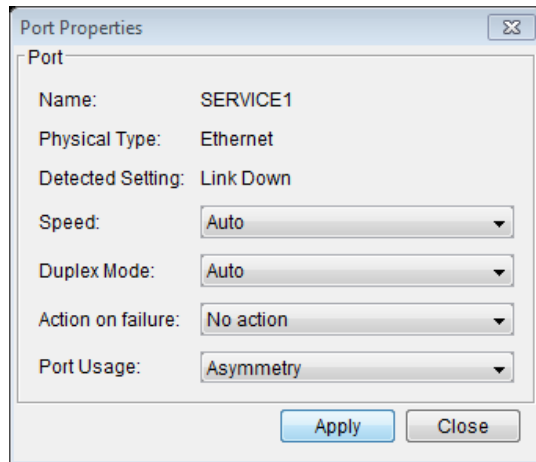


**Figure 5-4: VLans Settings dialog**

3. A VLAN must be set for each connection between any two devices in the group. Each direction must have a VLAN to be used for Asymmetric control messages (however the same number can be used for both directions)
4. Double click in a field to enter a new VLAN number.
5. Click **Save** to save the information and return to the Asymmetry Group – New dialog.
6. Click **Save** to save the new ADG.

**To configure the NetEnforcer:**

1. Open the Configuration screen for the selected NetEnforcer and click on the NIC tab.
2. Select the appropriate NIC from the available Ports and click Edit to open the Port Properties dialog for the selected link.
3. Select Asymmetry in the Port Usage field.



**Figure 5-5: Port Properties dialog**

4. Click Apply to save your changes.
5. Verify that this has been configured correctly by using the NetXplorer GUI or the following CLI commands:

**go config view asymmetry**

**go config view asymmetry\_remote\_device**



## Chapter 6: Command Line Interface

### Chassis CLI

The following CLI (Command Line Interface) commands can be used to troubleshoot the AOS based NetEnforcer. To access the CLI commands, enable SSH and open an SSH session to the NetEnforcer and login using: user: **sysadmin** password: **sysadmin**.

Each of the commands in the table below has several possible options. In the table below, for each command we give examples of the most common options together with the command syntax.

**NOTE** Specific parameters for each command may be found by using the **HELP** function after logging into the system via SSH or by entering the command without flags or parameters. Follow the onscreen instructions.

COMMAND	FLAG	ENABLES YOU TO
acmon	<none>	Display total throughput of the system
	-l <LINE>	Monitor a specific line rate
	-p <PIPE>	Monitor a specific Pipe rate
	-v <VC>	Monitor a specific VC rate
	-d	Monitor packet distribution
	-a	Monitor detailed asymmetric traffic stats
	-y	Monitor total asymmetric traffic stats
	-c	Run acmon limited count number
	-r	Monitor octet rx
	-t <SECONDS>	Set the time to wait between samples in seconds
ac_reboot	<none>	Reboot the system
acstat	<none>	Display the number of open connections.
	-I <LINE>,<PIPE>,<VC>	Display the hierarchy of all connections on line, pipe or vc
	-c	Display connection establishment rate

COMMAND	FLAG	ENABLES YOU TO
	-e	Display Service name and connection flag
	-t	Display TCP connections
	-u	Display UDP connections
	-n	Don't resolve policyId and show statistic handles
	-i	Display all connections
	-f	Display extended view
	-x	Display internal/external
	-m <NUMBER>	Display up to NUMBER of sessions
	-N	Don't resolve names
	-B	Dump binary data to file
	-r	Display number of active rules.
actype	<none>	View software version
boxkey	<none>	View the box key. The box key should be sent to Allot in order to purchase a system activation key.
dsAdmin	<NONE>	View total number of hosts
	-v	View all hosts (Host ID, service group, IP).
	-i <IP>	Show IP data
	-o <HOST>	Show host data
	-g <GROUP>	Show all hosts in group.
go add	line	Add a line to the system.
	pipe	Add a Pipe to the system.
	vc	Add a VC to the system.
	prule	Add a rule to a Pipe on the system.
	vcrule	Add a rule to a VC on the system.



COMMAND	FLAG	ENABLES YOU TO
	service_entry	Add a Service Catalog entry on the system.
	service_gr_entry	Add a Service Group Catalog entry on the system.
	time_entry	Add a Time Catalog entry on the system.
	tos_entry	Add a ToS Catalog entry on the system.
	qos_entry	Add a QoS Catalog entry on the system.
	dos_entry	Add a DoS Catalog entry on the system.
	host_entry	Add a Host Catalog entry on the system.
	host_gr_entry	Add a Host Group Catalog entry on the system.
	vlan_entry	Add a VLAN Catalog entry on the system.
go delete	line	Delete a line from the system.
	pipe	Delete a Pipe from the system.
	vc	Delete a VC from the system.
	prule	Delete a rule from a Pipe on the system.
	vcrule	Delete a rule from a VC on the system.
	service_entry	Delete a Service Catalog entry from the system.
	service_gr_entry	Delete a Service Group Catalog entry from the system.
	time_entry	Delete a Time Catalog entry from the system.
	tos_entry	Delete a ToS Catalog entry from the system.

COMMAND	FLAG	ENABLES YOU TO
	qos_entry	Delete a QoS Catalog entry from the system.
	dos_entry	Delete a DoS Catalog entry from the system.
	host_entry	Delete a Host Catalog entry from the system.
	host_gr_entry	Delete a Host Group Catalog entry from the system.
	vlan_entry	Delete a VLAN Catalog entry from the system.
go change	line	Change a line on the system.
	pipe	Change a Pipe on the system.
	vc	Change a VC on the system.
	prule	Change a rule to a Pipe on the system.
	vcrule	Change a rule to a VC on the system.
	service_entry	Change a Service Catalog entry on the system.
	service_gr_entry	Change a Service Group Catalog entry on the system.
	time_entry	Change a Time Catalog entry on the system.
	tos_entry	Change a ToS Catalog entry on the system.
	qos_entry	Change a QoS Catalog entry on the system.
	dos_entry	Change a DoS Catalog entry on the system.
	host_entry	Change a Host Catalog entry on the system.
	host_gr_entry	Change a Host Group Catalog entry on the system.

COMMAND	FLAG	ENABLES YOU TO
	vlan_entry	Change a VLAN Catalog entry on the system.
go rename	line	Rename a line on the system.
	pipe	Rename a Pipe on the system.
	vc	Rename a VC on the system.
	service_entry	Rename a Service Catalog entry on the system.
	service_gr_entry	Rename a Service Group Catalog entry on the system.
	time_entry	Rename a Time Catalog entry on the system.
	tos_entry	Rename a ToS Catalog entry on the system.
	qos_entry	Rename a QoS Catalog entry on the system.
	dos_entry	Rename a DoS Catalog entry on the system.
	host_entry	Rename a Host Catalog entry on the system.
	host_gr_entry	Rename a Host Group Catalog entry on the system.
	vlan_entry	Rename a VLAN Catalog entry on the system.
go list	lines	List the Lines on the system.
	linedata <LINE_NAME>	List the configuration details on a specific Line.
	pipes	List the Pipes on the system.
	pipedata <PIPE_NAME>	List the configuration details on a specific Pipe.
	vc <VC_NAME:PIPE_NAME: LINE_NAME>	List the configuration details of a specific Virtual Channel on the system.

COMMAND	FLAG	ENABLES YOU TO
	vlan_entry	List the entries in the VLAN Catalog.
	service_entry	List the entries in the Service Catalog.
	time_entry	List the entries in the Time Catalog.
	tos_entry	List the entries in the ToS Catalog.
	qos_entry	List the entries in the QoS Catalog.
	host_entry	List the entries in the Host Catalog.
	dos_entry	List the entries in the DoS Catalog.
	host_gr_entry	List the Host Groups in the Host Catalog.
	service_gr_entry	List the Service Groups in the Service Catalog.
	appl_entry	Lists the applications or content entries in the Service catalog.
go config	ips	Configure the IP Addresses.
	key	Enter the product key for the device.
	network	Configure the network parameters.
	network -bypass_unit enable	Enable the bypass unit. To be used if the bypass unit has been previously disabled.
	network -bypass_unit disable	Disable the bypass unit. To be used only if you wish to use the product without a bypass unit.
	network -dev_mode system:mode	Move a device into active mode, bypass mode or reboot <ul style="list-style-type: none"> <li>mode = active, bypass, reboot</li> </ul>
	network -redund_mode active	Enable Active Redundancy
	nic	Configure the NIC speeds and modes.
	access_control	Designate who may access the device.
	time	Set the time on the device for syncing purposes.

COMMAND	FLAG	ENABLES YOU TO
	view	Display all information concerning the configuration.
	view asymmetry	Displays if asymmetric traffic is enabled.
	view asymmetry_remote_device	Displays the remote device configured for asymmetric traffic.
	view web_update	Displays the current Protocol Pack.
	security	Configure the security parameters.
	data_collect	Configure the data collection parameters.
	snmp	Configure the SNMP settings.
	device_bw_limits	Configure the bandwidth of the device.
	password_security	Configure the password security settings (e.g: expiration days, warning days, length, character enforcement etc)
	uds enable	Enable User Defined Signatures.
	uds disable	Disable User Defined Signatures.
	web_update	Display the Protocol Pack currently installed.
	web_safe	Configure WebSafe
	bypass	Configure the bypass unit.
	next_hop_router	When steering to a “proxy based” service, the NetEnforcer will occasionally need to make routing decisions. Use this command to configure the NE to work as a next hop router (gateway).

COMMAND	FLAG	ENABLES YOU TO
	cer -value -action	Drop sessions over a specified CER <ul style="list-style-type: none"> <li>value = number of “frames per second”. The default is <b>maximum</b>.</li> <li>Action = Bypass or Drop. The default is <b>bypass</b></li> </ul>
	hairpin enable	Enables support for hanging routers in devices shipped in 2011 or after.
	hairpin disable	Disables support for hanging routers in devices shipped in 2011 or after.
snapshot	<none>	Create a snapshot of the status & logs of the system.
change_admin_pass	<none>	Runs a script that allows a user signed in as sysadmin to change the default admin password on the NetEnforcer.

## Examples

COMMAND	OUTPUT
<b>acstat</b> Displays the connection allocation summary	<pre> ----- Protocol type  Connections ----- TCP           : 183077 UDP           : 128685 anyIP        : 23674 nonIP        : 5 ----- TOTAL         : 335441           </pre>
<b>acstat -i</b> Displays all current connections	<pre> ----- Protocol      Client           Server           VC ----- HTTP   :IP:6   22.19.157.213:80  22.18.157.214:80  Fallback_Jumbo_Http_TrafficLin HTTP   :IP:6   22.20.17.169:80   22.19.17.170:80   Fallback_Jumbo_Http_TrafficLin QNext  :IP:17  181.0.55.138:1024 192.0.0.1:5237    1062782_VCSPI_SMP_TrafficLine HTTP   :IP:6   22.19.196.111:80  22.18.196.112:80  Fallback_Jumbo_Http_TrafficLin QNext  :IP:17  181.0.94.67:1024  192.0.0.1:5237    1072695_vcsp2_a_SMP_TrafficLin           </pre>

COMMAND	OUTPUT
<p><b>acstat -if -m 20</b></p> <p>Displays an extended view of all connections, but limits the number of displayed lines to the first 20.</p>	<pre> sysadmin@AC5k:/opt/allot/logs\$ acstat -if -m 20 ----- Protocol          Client          Server          VC          State AppId  ConFl  DpiInf  AuthSt  TTL ----- HTTP      :IP:6  22.19.157.213:80  22.18.157.214:80  Fallback_Jumbo_Http_Traff WIRE4EVER 0      RAW      1e8030000 0      4294967196  HTTP      :IP:6  22.20.17.169:80  22.19.17.170:80  Fallback_Jumbo_Http_Traff WIRE4EVER 0      RAW      1e8030000 0      4294967284  HTTP      :IP:6  22.20.134.164:80  22.19.134.165:80  Fallback_Jumbo_Http_Traff WIRE4EVER 0      RAW      1e8030000 0      4294967212  HTTP      :IP:6  22.20.76.31:80  22.19.76.32:80  Fallback_Jumbo_Http_Traff WIRE4EVER 0      RAW      1e8030000 0      32 </pre>
<p><b>acstat -l pipe or acstat -l vc</b></p> <p>This command can be used to show the QID of a Pipe/VC. The QID is used in other commands to identify the details of a certain Pipe/VC.</p>	<pre> sysadmin@AC5k:/opt/allot/logs\$ acstat -l pipe ----- Rule QID      Rule name          Live connections  Accepted conn  Drop connections ----- 1.1.0         1                  1                1              0 52.20.0      14606             14606            14606          0 52.21.0      25619             25619            25619          0 55.10.0      64                64               64             0 52.25.0      13000000          13000000         13000000       0 </pre>
<p><b>acstat -l 4.1357254463.1.0 -f</b></p> <p>Displays an extended view of the connections to a specific VC</p>	<pre> ----- Protocol Client          Server          State  VC          Client Timeout Vlan ----- IP:TCP  80.230.15.63:54322  216.66.74.145:80  WIRE4EVER  Fallback_80.230.15.63_Test-T IP:TCP  80.230.15.63:62020  216.239.37.104:80  WIRE4EVER  Fallback_80.230.15.63_Test-T IP:TCP  213.30.74.49:3728  80.230.15.63:1214  WIRE4EVER  Fallback_80.230.15.63_Test-T IP:UDP  81.7.112.66:32769  80.230.53.162:137  QUEUE      Fallback_80.230.15.63_Test-T </pre>
<p><b>acstat -iN</b></p> <p>Shows output without resolving VC names</p>	<pre> ac-pri:~# acstat -iN  less ----- Protocol Client          Server          VC ----- 0      199.203.223.3:9903  64.14.90.231:80  0.0.0.0 23a    199.203.223.3:27848  64.233.161.19:80  4.0.2.0 0      199.203.223.3:27936  213.252.152.56:25  0.0.0.0 23a    199.203.223.3:24352  64.14.90.231:80  4.0.2.0 23a    199.203.223.3:28207  212.143.162.134:80  4.0.2.0 23a    199.203.223.3:10084  212.143.162.134:80  4.0.2.0 23a    199.203.223.3:29178  212.143.162.134:80  4.0.2.0 23a    199.203.223.3:21320  62.189.244.254:80  4.0.2.0 23a    199.203.223.3:17716  212.143.162.134:80  4.0.2.0 23a    199.203.223.3:30926  192.114.71.245:80  4.0.2.0 23a    199.203.223.3:15784  212.143.162.200:80  4.0.2.0 23a    199.203.223.3:7349  66.161.36.110:80  4.0.2.0 </pre>

COMMAND	OUTPUT
<p><b>acstat -ifx</b> - The x shows internal/external instead of client/server</p> <p><b>AC:~# acstat -ifx  less</b></p>	<pre> DPIIC:~# acstat -ifx ConFl(=Connection Flags): [flags:flags2] ----- NP Service      Internal      External      VC              State  Vlanb Cl-IF ConFl ----- 0  Other UD:IP:17  1.57.71.0:208  170.4.56.100:184  Other UDP_Fallback  WIRE4EVER 7d0  0 205 raw 0  Other UD:IP:17  1.113.183.0:23  170.5.246.101:50  Other UDP_Fallback  WIRE4EVER 7d0  1 201 raw 0  Other TC:IP:6   1.80.142.0:203  170.27.128.100:184  Other TCP_Fallback  WIRE4EVER 7d1  0 204 raw 0  Other UD:IP:17  1.31.82.0:224   170.9.131.100:184  Other UDP_Fallback  WIRE4EVER 7d0  0 205 raw 0  Other UD:IP:17  1.101.132.0:23  170.32.211.101:59  Other UDP_Fallback  WIRE4EVER 7d0  1 201 raw 0  Other UD:IP:17  1.58.98.0:23   170.13.33.101:57  Other UDP_Fallback  WIRE4EVER 7d0  1 201 raw 0  Other TC:IP:6   1.40.75.0:194   170.34.29.100:184  Other TCP_Fallback  WIRE4EVER 7d1  0 204 raw                     </pre>



## Chapter 7: Safety Information

---

### General

**NOTE** Before installing or using the NetEnforcer, please read all Safety Information carefully.

**Product intended only for installation in a Restricted Access Area.**

---

#### CAUTION



Indicate potential damage to hardware and tells you how to avoid the problem.



---

#### WARNING



Indicates potential for bodily harm and tells you how to avoid the problem.



---

#### Danger of electrostatic discharge



The Shelf contains static sensitive devices. To prevent static damage wear an ESD wrist strap.



---

**CAUTION RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS**

### Regulatory Compliance Statements

This section provides the FCC compliance statement for Class A devices and describes how to keep the system CE compliant.

#### FCC Compliance Statement for Class A Devices

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

---

WARNING



This is a Class A product. If not installed in a properly shielded enclosure and used in accordance with this Hardware Guide, this product may cause radio interference in which case users may need to take additional measures at their own expense.



---

## Chassis Safety

### Unpacking

---

CAUTION



To minimize any possibility of physical damage to equipment, ensure that floor space at the installation site is neat and uncluttered.



---

WARNING



All poly strap-shipping bands that secure the Shelf packaging are stretched tight and are under tension. Wear eye protection to prevent possible eye injury when cutting the strap, as the strap tension is released, and strap ends recoil outward.



---

Follow these recommendations while unpacking:

- After the equipment arrives at the installation site, carefully inspect each carton for signs of shipping damage. If the package is damaged, document the damage with photographs and contact the transport carrier immediately.

---

CAUTION



Always cut any shrink wrapping material away from the packing carton; do not physically pull and tear the fabric. Physically pulling the shrink wrapping from the shipping carton without cutting it first may create an electrostatic charge that could damage electronic equipment.



- 
- Remove all items from the box. If any items listed on the purchase order are missing, notify Allot customer service immediately.
  - Inspect the product for damage. If there is damage, notify Allot customer service immediately.
  - Save the box and packing material for possible future shipment.

## Installation

This unit is intended for stationary rack mounting.

---

### IMPORTANT



Before installing the Rack Mount Kit, ensure there will be adequate vertical space to install the Shelf in addition to other equipment installed.



- 
- Keep tools and chassis components off the floor and away from foot traffic.
  - Clear the area of possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.
  - Keep the area around the chassis free from dust and foreign conductive material.

## Rack mounting information

---

### CAUTION



Mount your system in a way that ensures even loading of the rack. Uneven weight distribution can result in a hazardous condition. Secure all mounting bolts when rack mounting the enclosure.



### CAUTION

Do NOT stack the unit on top of any other equipment. If the Shelf falls, it can cause severe bodily injury and damage the equipment.



- 
- Ensure that the rack is constructed to support the weight and dimensions of the Shelf.
  - Install any stabilizers or shelf to the rack before mounting or servicing the system in the rack.
  - Load the rack from the bottom to the top, with the heaviest system at the bottom, avoid uneven mechanical loading of the rack.

## Power Connection Information

- In AC installations, the system relies on the protective devices in the building installation for protection against short-circuit, overcurrent, and earth (grounding) fault. Ensure that the protective devices in the building installation are properly rated to protect the system, and the power lines have to be protected on rack level with dual pole 10A breakers when using DC power.
- The unit can be powered using a regular telecommunication power supply of -48 VDC. The specified voltage range is from -40.5 VDC to 60 VDC. The unit supports redundant power supplies but the two supplies should be independently powered.

- The Unit must be properly grounded via the Ground Terminal. The unit provides a Shelf Ground Terminal at the right rear view.

---

**WARNING**



Protective ground must be connected to the unit before connecting any external power.



**DANGER!—HIGH VOLTAGE HAZARD** if not connected

---

---

**WARNING**

Do not open the unit under any circumstances.



---

**WARNING**



Verify power cord and outlet compatibility: Use the appropriate power cords for your power outlet configurations.



---

**WARNING**



Avoid electric overload, heat, shock, or fire hazard: Only connect the system to a properly rated supply circuit as specified in the product user manual. See the product user manual for correct connections.



---

**CAUTION**



All input power and return wiring should be specified, configure, and installed by a qualified electrician in order to prevent damage to the equipment.

The wiring should be limited to recommendation in order to prevent damage to the shelf.



---

WARNING



Ensure that each power domain supply (feeding) circuit breaker is switched *OFF* while completing the power connection procedure. Failure to comply can result in personal injury.



---

**NOTE** In a typical telecommunications environment, the VRTN path of the -48 VDC supply is grounded to protective earth (PE) of the building.

### Airflow information

- Install the system in an open rack whenever possible. If installation in an enclosed rack is unavoidable, ensure that the rack has adequate ventilation.
- Maintain ambient airflow to ensure normal operation. If the airflow is blocked or restricted, or if the intake air is too warm, an over temperature condition can occur.
- Ensure that cables from other equipment do not obstruct the airflow through the shelf.

### Preventing Surge

---

WARNING



This product is design to meet Intra building surge signals, other location are required additional protective elements to needed to be add.



---

WARNING



The intra-building port(s) of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly **MUST NOT** be metallicly connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallicly to OSP wiring.



## Laser Safety Requirements

### Laser Classification

Allot Equipment and components equipped with laser devices described in this manual comply with IEC 60825-1: 2007 and FDA CDRH 21CFR - Safety of Laser Products. They also comply with UL / IEC 60950-1 2<sup>nd</sup> Edition

All the SFP, SFP+ and XFP modules that are used in the equipment are Class 1 Laser Products.

As long as the Equipment is operated in accordance with the applicable safety instructions, the Hazard Level in Equipment access locations is inherently Class 1.

Allot provides product and installation information in order that the products may be installed and serviced safely.

### Laser Information

See the System Specifications for information regarding the laser transmitters of the various optical cards available for the platform.

### Laser Safety Statutory Warning

All personnel involved in Equipment installation, operation, and maintenance must be aware that laser radiation is invisible. Therefore, although protective devices generally prevent direct exposure to the beam, personnel must strictly observe the applicable safety precautions and, in particular, must avoid staring into optical connectors, either directly or using optical instruments.

Remember that observing safety precautions is not a matter of personal choice: ignoring safety puts all the people within line of sight in danger!

### Training for Laser Safety

Personnel must be trained for safety before being authorized to operate, install, and/or maintain laser products. The IEC 60825 standards require organizations to appoint a laser safety officer who is responsible for training personnel, establishing safe operational procedures, and supervising the implementation of these procedures during routine work.

Untrained personnel must not be allowed to operate, install, and/or maintain laser products.

### Laser Device Operating Precautions

In addition to the general precautions described in this section, be sure to observe the following warning when operating a product equipped with a laser device. Failure to observe this warning could result in bodily injury and damage to equipment.



**Warning:** Invisible laser radiation may be emitted from the aperture of optical ports when no fiber cable is connected. Avoid exposure and do not stare into open apertures.

**Advarsel:** Der kan forekomme usynlige laserstråler fra de optiske portes åbninger, når der ikke er tilsluttet et lyslederkabel. Undgå at blive udsat for disse stråler, og kig ikke ind i åbninger.

**Waarschuwing:** Er kan onzichtbare laserstraling uit de opening van de optische poorten komen wanneer er geen fiberkabel is aangesloten. Vermijd blootstelling aan straling en kijk niet in de openingen.

**Varoitus:** Optisten porttien aukoista saattaa säteillä näkymätöntä lasersäteilyä silloin, kun niissä ei ole kuitukaapeleita kiinni. Vältä altistumista ja älä tuijota näihin avoimiin aukkoihin.

**Attention:** Un rayonnement laser invisible peut être émis à partir de l'ouverture des ports optiques lorsque aucun câble à fibres optiques n'est connecté. Évitez de vous y exposer et ne fixez pas les ouvertures.

**Warnung:** Wenn kein Faserkabel angeschlossen ist, können aus der Öffnung der optischen Anschlüsse Laserstrahlen austreten. Vermeiden Sie Bestrahlungen und schauen Sie nicht in diese Öffnungen.

**Avvertenza:** Le aperture delle porte ottiche possono emettere radiazioni laser invisibili quando i cavi in fibra non sono collegati. Evitare lunghe esposizioni davanti alle aperture.

**Aviso:** Podem ser emitidas radiações invisíveis de laser a partir das aberturas das portas ópticas se não estiver ligado qualquer cabo de fibra óptica. Evitar a exposição e não olhar directamente pelas aberturas aparentes.

**Advertencia:** Es posible que la radiación láser invisible se emita desde la apertura de puertos ópticos cuando no haya ningún cable de fibra conectado. Evite la exposición y no mire fijamente a las aberturas.

**Warning:** Osynlig laserstrålning kan spridas från öppningen på optiska portar om ingen fiberoptikkabel är ansluten. Undvik exponering och stirra inte in i öppningarna.





## Chapter 8: Technical Specifications

### AC-6000 Series

CAPACITY	
Number of Connections/Flows	5,000,000
Throughput	16 Gbps (8 Gbps, Full Duplex)
Lines/Pipes/Virtual Channels	512 / 125,000 / 250,000
No. of Subscribers	400,000
INTERFACES AND CONNECTIONS	
Management Interface	10/100/1000BASE-T
Network Interfaces (Internal / External)	8 x 1GE ports 8 x 10GE / 1GE ports (dual mode) 10GBase-SR/LR/ER or 1000BASE-SX/LX/ZX or 10/100/1000BASE-T (Auto-Negotiation)
Console Port	Serial, RJ-45 Connector
PRODUCT OPTIONS	
Monitoring	Yes
QoS Enforcement Levels	2Gbps, 4Gbps, 8Gbps (full duplex)
MANAGEMENT	
NetXplorer Centralized Management	Yes
NetXplorer Long-term Reporter	Yes
NetXplorer Real-time Reporter	Add-on license
NETENFORCER UNIT	
Size	Standard 1U by 19" rack mount,
Dimensions	350mm x 440mm x 44mm (L x W x H)
Weight	7 kg (15.4 lb)
Operating Temp	0°C to 50°C
EXTERNAL BYPASS UNIT	
Size	Standard, 1U, 19" rack mount
Dimensions	130mm x 440mm x 44mm (L x W x H)
Weight	2.4 Kg (5.3 lbs)

POWER	
Input (AC)	100 - 240 VAC, 50/60Hz, 4A max
Input (DC)	-48V DC, 7.5A max
Power Supply Units	2 (Load Sharing)
Redundancy for PSUs	1 + 1
Power Consumption	300W
Heat Dissipation	1,025 BTU/hour
SAFETY AND CERTIFICATIONS	
<b>Emissions:</b>	
Conducted & Radiated Emissions	EN 55022: 2006 + A1:2007 FCC CFR 47 Part 15B Class A ICES-003 Issue 4; C108.8-M1983 CISPR 22: 2009 AS/NZS CISPR 22: 2009
Power-line Harmonics Power-line Flicker ETSI	EN 61000-3-2: 2006 + A1:2009 + A2:2009 EN 61000-3-3: 2008 EN 300 386 V1.4.1:2008-04 for use in telecommunication canterers
<b>Immunity:</b> ETSI	EN 55024: 1998 + A1:2001 + A2:2003 EN 300 386 V1.4.1:2008-04
<b>Safety:</b>	EN 60950-1: 2006 + A11:2009 UL 60950-1: 2007 CAN/CSA-C22.2 No. 60950-1-07
<b>RoHS:</b>	EN 50581: 2012
<b>CE Mark:</b>	Product is compliant with the essential requirements of the following Directives: 2004/108/EC Electromagnetic Compatibility directive 2006/95/EC Low Voltage Equipment directive 2011/65/EU RoHS