Product Information Package

For Units

4210D 1MP / 6210D 2MP

Published: 2019-09-16

Table of Contents

Introduction

Content

About Us

Nimitz is a distributed denial of service (DDoS) mitigation project that is currently in its 5th year of development and making rapid progress from theoretical research to real world testing and product distribution.

We originated out of Grande Prairie, Alberta in early 2014. A location which still serves as our primary headquarters and base of operation. But since then we have also taken on a global presence. Both in terms of clientele as well as contributors. And, currently consist of a small group of international specialists spanning both Canada and Europe. Most of whom have 20+ years of applied/ technical experience in the fields of information research/ technology, cyber-security and computer networking.

Goals

Primary Goal: to develop a protection mechanism that could compete against the continuously evolving DDoS landscape, across all areas. Including performance metrics, such as number of packets per second (pps) mitigated, latency, ease of deployment, upgradeablity and affordability. Through the development of proprietary software that allows for advanced signature detection and high velocity packet processing. We have substantially increased the efficiency of filtering out attacks without compromising a networks normal data/ traffic or integrity. Thus allowing for enhanced levels of pps level mitigation, relative to given hardware specifications.

Secondary Goal: increase the accessiblity to industrial level DDoS mitigation technology for small to enterprise businesses, networks and ISP's for whom traditional solutions from industry leading experts may not have been financialy feasible, effective or scalable. This we achieved through the coupling of our advanced software with standard industry hardware. Allowing Nimitz to be deployed in networks of anysize through nothing more than simple hardware modifications. Delivering revolutionary protection at a reduced cost.

Tertiary Goal: in so doing we have developed a product that is not only more efficient and cost effective than solutions employed by industry leaders. But also liberating in the sense that we have created a security appliance that is essentialy turn-key, easy to deploy and does not rely on 3rd parties managing your data and routing traffic through off site proxys that degrade your network (increase latency) and increase your risk to security vulnerabilities. Thus, giving you back control over your traffic and data.

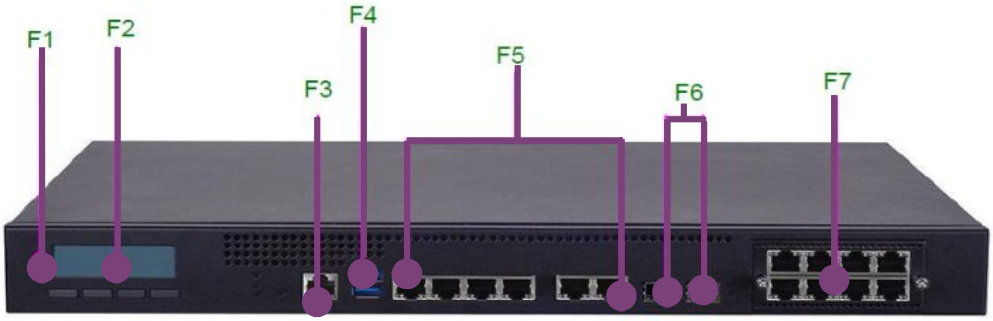
KEY BENEFITS

- **24/7/365 Protection**
- **Automatic Protection**
- **Continuous Development**
- **Low Latency**
- **On-Site Protection**
- **Turn-Key**
- **Universal Protection**

Product Information

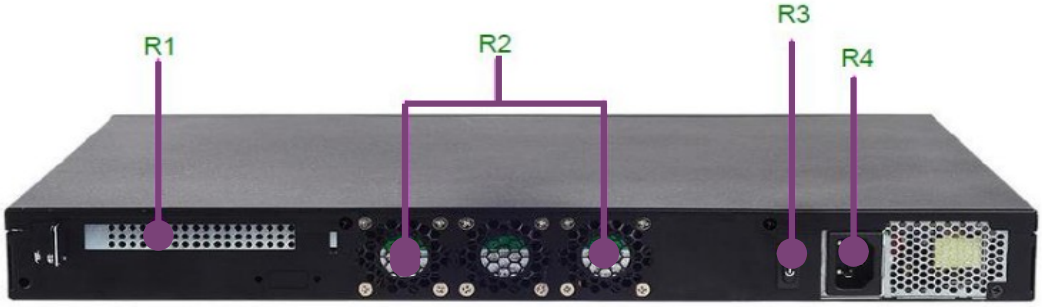
Content

Physical Hardware



Front End	
F1 LED Indicators	Keypad Activated
F2 LCM	LCM with 4 x Keypads
F3 Console	1 x RJ-45 Console Port
F4 USB	2 x USB 3.0 Type-A Ports, in double stacked form
F5 LAN	6 x RJ-45 GbE ports
F6 SFP LAN	2 x SFP LAN ports
F7 Additional Nic Module [1]	1 x NIC Module Space with PCIe Interface

[1] **F7 Additional Nic Module:** Refer to page 8, section “Custom Configurations”. For additional Nic module options. Default Configuration is an empty PCIe slot.



Rear End	
R1 PCIe Expansion	1 x PCIe Expansion slot (Optional)
R2 Fans	2 x Cooling Fans
R3 Power Switch	1 x Power ON / OFF Switch
R4 Power Jack	1 x Power Jack, for connection with power adapter

Product Matrix			
Model	**Nimitz 4210D-1MP**	**Nimitz 6210D-2MP**	**Nimitz 8210D-5MP[1]**
Network Grade			
Network Category Recommended	Small <5Gbps	Business / ISP <10Gbps	Enterprise >10Gbps
Performance Characteristics			
DDoS Threshold[2] (pps)	1 000 000	2 000 000	5 000 000
Peak Mitigation[3] (pps)	~1 500 000	~3 500 000	**PENDING**
Ingress/ Egress Mitigation	Ingress	Ingress	Ingress
DDoS Attack Vector[4]	DNS / HTTP / ICMP / IP Fragmentation / Memcached / NTP / SSDP / TCP / UDP / HTTP3		
DDoS Attack Method	Amplification / Reflection / Flood / Multi-Vector		
Protected Layers	Network / Transport / Application		
Response Type[5]	Automatic		
Time to Mitigation	<200 microseconds (<0.2 milliseconds)		
Additional Latency	<200 microseconds (<0.2 milliseconds)		
Management			
Configuration	Telnet / Console (Serial to USB)		
Live attack Notification	SMS / Email		
Logging	Full History Logs 60s Intervals 1hr Windows		
Software as a Service[6]	Software Fee $ 100.00 USD / Monthly $ 1 000.00 USD / Annualy		
Platform			
CPU	Intel® Core™ i3 2C/4T	Intel® Core™ i7 4C/8T	
Chipset	Intel® H110 or C236		
BIOS	AMI SPI Flash BIOS		
Memory Technology	DDR4 2400MHz		
Memory Socket	2 x 288-pin DIMM		
Core Memory (RAM)	2 x 4GB		
SATA Storage	32GB		
Default Configuration I/O			
Ethernet controller	Intel i210 / i210-IS		
Default LAN	6 x GbE RJ45		

Bypass	2 Pairs Gen3		
Console	1 x RJ45		
USB 3.0	2 x Type A		
Additional NIC Modules	+ 1		
Bandwidth (Total)	6Gbps		
Bandwidth (In/Out)	3 / 3 Gbps		
Custom Configurations[7] [8]			
Max Bandwidth (Total)	46 Gpbs	46 Gbps	
Max Bandwidth (In/Out)	23 /23 Gbps	23 / 23 Gbps	
RJ45 NIC CARDS **-NCS2-IGM428A** **-Intel i350-AM4, 4 ports GbE G3 Bypass, 2 pairs**	+ 1 module(s) $ 177.00 USD	+ 1 module(s) $ 177.00 USD	
RJ45 NIC CARDS **-NCS2-IGM808A** **-Intel i210-AT + PEX8608, 8x GbE G3 Bypass, 4 pairs**	+ 1 module(s) $ 384.00 USD	+ 1 module(s) $ 384.00 USD	
SFP+ NIC CARDS **-NCS2-IXM204A** **-Intel 82599EB ,2 ports 10Gb SFP+, No bypass**	+ 1 module(s) $ 265.00 USD	+ 1 module(s) $ 265.00 USD	
SFP+ NIC CARDS **-NCS2-IXM407A** **-Intel XL710 4x10Gb, 4 ports 10G SFP+, No bypass**	+ 1 module(s) $ 386.00 USD	+ 1 module(s) $ 386.00 USD	
Power and Mechanical			
Power input	AC 90~264V @47~63 Hz		
Type/Watt	220W ATX Single PSU		
Expansion	1 x PCIE*8 Default, 2 x PCIE*4 Optional		
Reset	Reset Button x 1		
Processor cooling	Passive CPU Heatsink		
System cooling	2 x Cooling Fans with Smart Fan		
Physical Specifications			
Dimensions (W x H x D)	438 mm x 44 mm x 321 mm (17.24" x 1.73" x 12.64") 1U		
Weight	7.5 kg (16.5 lbs)		
Mounting	Rack Mount		
1U Slide Rail Kit	Optional		
Environmental			

Storage temperature	-20°C to 70°C	
Operating temperature	0°C to 40°C 32°F to 104°F	
Operating humidity	5% to 90% (non-condensing)	
Certifications		
Certifications	RoHS CE/FCC Class A UL	
Warranty		
Warranty	1 year	
Custom Designs		
[9]	For clients with very large networks or special requirements e.g. Carriers	

[1] **Nimitz 8210D-5MP:** is currently undergoing design optimizations related to heat dissipation, hardware and performance characteristics will be provided soon. We are currently expecting an absolute minimum performance capability of 5mpps DDoS mitigation.
[2] **DDoS Threshold (pps):** guaranteed level of protection across all DDoS taxonomies and attack variants.
[3] **Peak Mitigation (pps):** is a lab metric of Nimitz products tested under maximum load. It is an absolute maximum performance capacity that allows for overhead mitigation in cases of large spikes in pps during an attack. It is not recommended to be viewed as a guaranteed metric for sustained continuous load and may vary depending on networks and type of DDoS attack profile.
[4] **Attack Vector:** TCP includes attacks such as {Syn}, {Syn, Ack} floods etc...
[5] **Response Type:** Nimitz default configuration is for automatic detection. Clients are provided with the option to enable/disable Nimitz via cloud interface.
[6] **Software as a Service (SaaS):** Nimitz physical hardware comes with a monthly subscription, required for the software. Which carry a software license.
[7] **Custom Configurations:** additional NIC modules will add to final cost of product.
[8] **Custom Configurations:** refer to page 6. Indicator (F7) represents customizable module.
[9] **Custom Designs:** Nimitz offers consultation for designing and implementing custom products for clients with very large networks or special requirements. Please contact directly.

Additional Package Content		
Short Ear Rack mount kit w/ screws	+ 1	
Power cable	+ 1	
Console Cable (Serial to usb)	+ 1	
Lan Cable (grey)	+ 1	
1U Slide Rail Kit [1]	Optional	

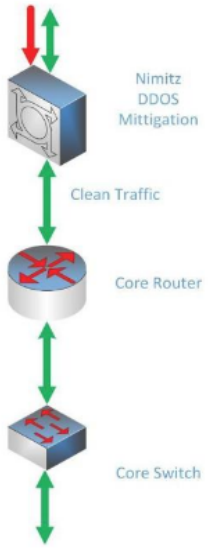
[1] **1U Slide Rail Kit:** Please mention directly. During the ordering process, in order to receive with shipment.

General Setup

Content

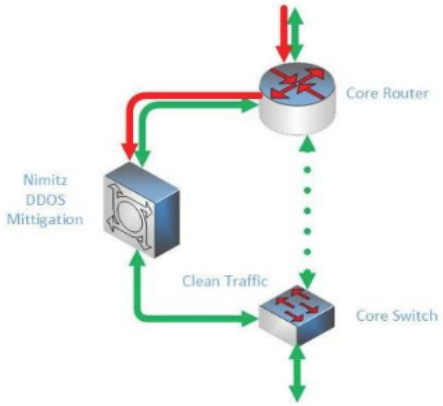
Network Schematics[1]	
Pass Through 1	Note: Configuration will allow automatic detection/mitigation.
Pass Through 2	Note: Configuration will allow automatic detection/mitigation.
Bypass	Note: Must manually switch over during an attack for mitigation to take effect.

Network Schematic Pass Through 1

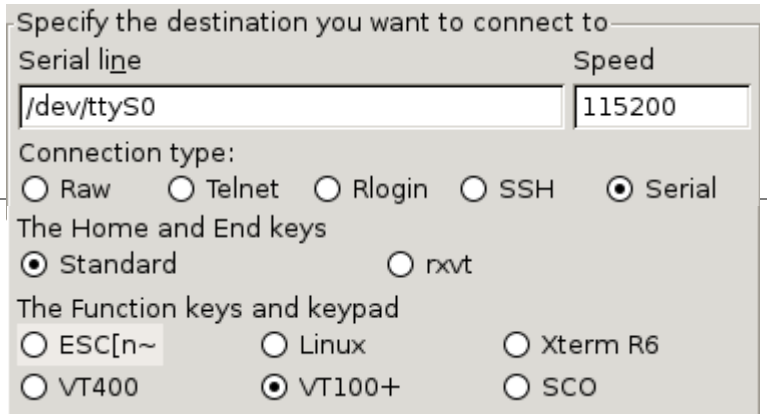
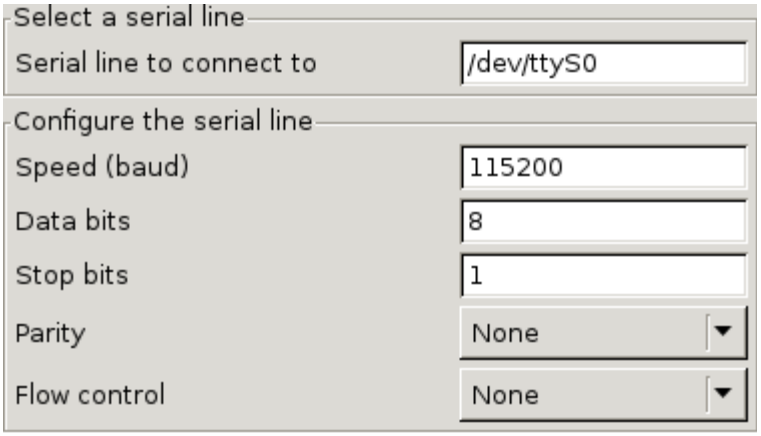


Network Schematic Pass Through 2

Network Schematic Bypass



[1] **Network Schematics:** sample setup topologies.

Serial Cable Login	
Client	PuTTY
Session	
Terminal **-- Keyboard**	
Connection **-- Serial**	 *Microsoft Windows: COM(n) *Linux: /dev/ttys(n) *Serial line will vary with Operating System, check kernel device pages for more information.

Console Settings			
Terminal Type	vt100+	**Stop Bits**	1
Bits Per Second	115200	**Flow Control**	none
Data Bits	8	**Putty KeyPad**	VT100
Parity	none	**Recorder Mode**	disabled
VT-UTF8 Combo Key Support		enabled	

Telnet Settings	
Telnet	telnet 10.30.0.33 2601
Password (default)	nimitz

Change Default Password	
Login	$telnet 10.30.0.33 2601 Trying ::1... Trying 10.30.0.33 Connected to 10.30.0.33 Escape character is '^]'. Hello, this is Quagga (version 1.1.1). Copyright 1996-2005 Kunihiro Ishiguro, et al. User Access Verification Password: <nimitz>
enable	Nimitz> enable Password: <nimitz> Nimitz#
configure terminal	Nimitz# configure terminal Nimitz(config)#
password	Nimitz(config)# password <enter new password> Nimitz(config)#

Enable IP-Forwarding	
enable	Nimitz> enable Password: <password> Nimitz#
Configure terminal	Nimitz# configure terminal Nimitz(config)#
ip forwarding	Nimitz(config)# ip forwarding Nimitz(config)#

Adding Static Routes	
enable	Nimitz> enable Password: <password> Nimitz#
configure terminal	Nimitz# configure terminal Nimitz(config)#
ip route <gateway - address>	Nimitz(config)# ip route A.B.C.D/xx A.B.C.D Nimitz(config)#
ip route <interface - address>	Nimitz(config)# ip route A.B.C.D/xx <interface-name> Nimitz(config)#
Using <?> for clarity	
ip route ?	Nimitz(config)# ip route ? A.B.C.D IP destination prefix A.B.C.D/M IP destination prefix (e.g. 10.0.0.0/8)
ip route A.B.C.D/24 ?	Nimitz(config)# ip route A.B.C.D/xx ? A.B.C.D IP gateway address INTERFACE IP gateway interface name
ip route A.B.C.D/24 A.B.C.D ?	Nimitz(config)# ip route A.B.C.D/xx A.B.C.D ? <1-255> Distance value for this route *Directly connected routes carry a default route metric of 0

Show Running Configuration <sample>	
enable	Nimitz> enable Password: <password> Nimitz#
show running-config	Nimitz# show running-config Current configuration: ! hostname Nimitz password nimitz ! interface enp1s0 description "WAN" ip address A.B.C.D/xx ! interface enp2s1 description "LAN" ip address A.B.C.D/xx ! interface lo ! ip route A.B.C.D/xx A.B.C.D ip route A.B.C.D/xx A.B.C.D ! ip forwarding ! ! line vty ! end #Nimitz

Adding Interface Descriptors <sample>	
enable	Nimitz> enable Password: <password> Nimitz#
configure terminal	Nimitz# configure terminal Nimitz(config)#
interface <if-name>	Nimitz(config)#interface <if-name> Nimitz(config-if)# description “WAN Interface” Nimitz(config-if)# show running-config Current Configuration: ...truncated for clarity ! interface <if-name> description "WAN Interface" ip address A.B.C.D/xx Nimitz(config-if)#

Negating commands <sample>	
no	Prepend <no> to an existing command to negate its effect e.g. Nimitz(config)# no ip route A.B.C.D/xx A.B.C.D Nimitz(config)#

Maneuvering Zebra commands with <?>

Nimitz> ?

```
The <?> command has 4 primary uses
1. Show current available commands
Nimitz> ?
  echo      Echo a message back to the vty
  enable    Turn on privileged mode command
  exit      Exit current mode and down to previous mode
  help      Description of the interactive help system
  list      Print command list
  quit      Exit current mode and down to previous mode
  show      Show running system information
  terminal  Set terminal line parameters
  who       Display who is on vty
```

Nimitz> show?

```
2, Show a commands <definition>
   *no space following command
Nimitz> show?
  show  Show running system information
```

Nimitz> show ?

```
3. Show a commands <options>
   *space following command
Nimitz> show ?
 commandtree  Show command tree
  debugging    Debugging information
  history      Display the session command history
  interface    Interface status and configuration
  ip           IP information
  ipv6         IPv6 information
  logging      Show current logging configuration
  memory       Memory statistics
  table        default routing table to use for all clients
  thread       Thread information
  version      Displays zebra version
  work-queues  Work Queue information
```

Nimitz> show ip ?

```
4. Show a commands <options><suboptions><suboptions>
Nimitz> show ip ?
  forwarding   IP forwarding status
  nht          IP nexthop tracking table
  prefix-list  Build a prefix list
  protocol     IP protocol filtering status
  route        IP routing table
```

Nested Privileges While Maneuvering Zebra <sample>

Nimitz>

Nimitz#

Nimitz(config)#

Nimitz(config-if)#

```
Nimitz>
Nimitz> enable
Password: <password>
Nimitz#
Nimitz# configure terminal
Nimitz(config)#
Nimitz(config)# interface <interface-name>
Nimitz(config-if)#
```

Returning to Previous Levels <sample>

exit

```
The <exit> command returns you to the previous level of privilige e.g.
Nimitz(config-if)# exit
Nimitz(config)#
```

end

```
The <end> command returns you to the initial enable level of privilige e.g.
Nimitz(config-if)# end
Nimitz#
```

Common Questions and Answers	
Does Nimitz operate in Bridge Mode or Routing Mode?	Nimitz is required to run in **Routing Mode** for it's **WAN** facing interface, in order to operate and perform **Ingress** filtering. You may bridge the **LAN** facing interface if that meets your networks requirements.
Does Nimitz operate in kernel or user mode.	**User mode.**
How does Nimitz Work?	Nimitz operates at layers 3/4 (OSI Model) of the protocol stack to eliminate DDoS attacks at layers 3/4/7. It achieves this via our proprietary software that uses a **novel** form of **signature detection** that is **unique to our product**.Without violating a packets integrity or security.
Does Nimitz perform both ingress and egress filtering?	**No**, Currently Nimitz **only performs Ingress filtering**, due to additional complexities. Egress filtering is something that we may consider deploying in the future on a case by case basis.
Am I required to purchase both the hardware and software or can I assemble my own hardware?	**Yes**, you are required to purchase the hardware configured with Nimitz proprietary software.
Can I make my own custom configurations to the hardware?	**No.** Any custom modifications to the hardware outside of purchase void all warranties. In addition to this clients are provided access to a restricted environment via telnet/console cable in which to configure Nimitz. Allowing only for basic routing operations.
How are you able to keep the costs of your security appliances so low? When compared to industry leaders.	We couple our software with **commodity hardware.** Commodity hardware opens us up to the opportunity of using relatively powerful components (e.g. CPU's) that are readily available. That would normally be utilized for multiple, non-related tasks. Instead we repurpose that hardware and optimize it for a single dedicated purpose.
What happens if I am hit with a DDoS attack that you have not identified?	If any client is hit with a DDoS attack that Nimitz has not identified or a new one has been developed then we will simply require a **Packet Capture** of that attack. Following which point we will analyze it and update all clients units via cloud. Thus allowing for continuous upgrades.
Why do you provide protection in packets per second (pps) rather than Gbps?	The simple answer to that is that modern networks are relatively high bandwidth. This makes it difficult for most malicious agents to launch an attack against a network or organization that will overwhelm their pipe and result in down time. For example ~81% of DDoS attacks in 2018 were under 1G with ~86% under <5G, according to research done by Corero Network Security. So if you have a network that is capable of handling 10G of throughput but is operating at 40% capacity, you can still handle 6G of traffic between endpoints. But still experience performance degredation at endpoints, due to the number and contents of those packets reaching your endpoint that fall within that <6G range. This is because not all bandwidths are made equal. Eventually a packet has to reach a point where it is processed. Attackers can craft packets by modifying their sizes and flags to attack endpoints/ nodes along a path regardless of bandwidth. Preferring to tie up system resources through greater CPU hardware utilization. e.g. A 2mpps = 1G Syn Flood can be more devastating to a networks hardware than a 1mpps = 2G Syn Flood.
Further Questions?	Please email us at **info@nimitz.ca**

Compliance and Certifications

Content

Acknowledgments

- Intel, Pentium and Celeron are registered trademarks of Intel Corp.
- Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.
- All other product names or trademarks are properties of their respective owners.

Compliances and Certifications

CE Certification

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A Certification

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.

EMC Notice

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 users will be required to correct the interference at their own expense.

Safety Guidelines

Follow these Guidelines to ensure general safety:

- Keep the chassis area clear and dust-free before, during and after installation.
- Do not wear loose clothing or jewelry that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
- Wear safety glasses/goggles if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Disconnect all power by turning off the power and unplugging the power cord before installing or removing a chassis or working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit; always check the circuit.

Lithium Battery Caution

- Risk of explosion could occur if battery is replaced by an incorrect type. Please dispose of used batteries according to the recycling instructions of your country.
- Installation only by a trained electrician or only by an electrically trained person who knows all the applied or related installation and device specifications.
- Do not carry the handle of power supplies when moving to other place.
- The machine can only be used in a fixed location such as labs or computer facilities.

Operating Safety

- Electrical equipment generates heat. Ambient air temperature may not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Be sure that the room in which you choose to operate your system has adequate air circulation.
- Ensure that the chassis cover is secure. The chassis design allows cooling air to circulate effectively. An open chassis permits air leaks, which may interrupt and redirect the flow of cooling air from internal components.
- Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD damage occurs when electronic components are improperly handled and can result in complete or intermittent failures. Be sure to follow ESD-prevention procedures when removing and replacing components to avoid these problems.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. If no wrist strap is available, ground yourself by touching the metal part of the chassis.
- Periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms (Mohms).

Precautions

1. Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
2. Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
3. Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
4. Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
5. Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Terms and Conditions

Content

Warranty Policy

1. All products are under warranty against defects in materials and workmanship for a period of one year from the date of purchase.
2. The buyer will bear the return freight charges for goods returned for repair within the warranty period; whereas the manufacturer will bear the after service freight charges for goods returned to the user.
3. The buyer will pay for repair (for replaced components plus service time) and transportation charges (both ways) for items after the expiration of the warranty period.
4. If the RMA Service Request Form does not meet the stated requirement as listed on “RMA Service,” RMA goods will be returned at customer’s expense.
5. The following conditions are excluded from this warranty:

- Improper or inadequate maintenance by the customer.
- Unauthorized modification, misuse, or reversed engineering of the product Operation outside of the environmental specifications for the product.

Contact & Additional Resources

Content

Contact	
Days of Operation:	Monday , Tuesday, Wednesday, Thursday, Friday
Hours of Operation:	MDT 9:00AM to 5:00PM UTC 15:00 to 23:00
Phone:	Office: 587-771-2284
Email:	info@nimitz.ca sales@nimitz.ca
Appointments:	Schedule an appointment via info@nimitz.ca or through our commercial website nimitz.ca.

Additional Resources	
Commercial Website:	Nimitz.ca
Wiki:	Nimitz.wiki

Partnered With	
GPNetworks	GPNetworks GPN WIRELESS NETWORK SOLUTIONS LTD.
Lanner	Lanner