IBM Security Network Active Bypass

User Guide

Publication Date: November 2012

Contents

Homologation statement - regulation notice

This product is not intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks.

Safety, environmental, and electronic emissions notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

DANGER notices

DANGER

To prevent a possible shock from touching two surfaces with different protective ground (earth), use one hand, when possible, to connect or disconnect signal cables. (D001)

DANGER

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device or the power rating label for electrical specifications. (D002)

DANGER

If the receptacle has a metal shell, do not touch the shell until you have completed the voltage and grounding checks. Improper wiring or grounding could place dangerous voltage on the metal shell. If any of the conditions are not as described, STOP. Ensure the improper voltage or impedance conditions are corrected before proceeding. (D003)

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (D004)

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **Connect power to this unit only with the IBM® ISS provided power cord. Do not use the IBM ISS provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

To disconnect:

1. **Turn off everything (unless instructed otherwise).**
2. **Remove the power cords from the outlets.**
3. **Remove the signal cables from the connectors.**
4. **Remove all cables from the devices.**

To connect:

1. **Turn off everything (unless instructed otherwise).**
2. **Attach all cables to the devices.**
3. **Attach the signal cables to the connectors.**
4. **Attach the power cords to the outlets.**
5. **Turn on the devices.**

(D005)

CAUTION notices

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at great than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION:
The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Exchange only with the IBM ISS-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM ISS has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM ISS part number for the battery unit available when you call. (C003)

CAUTION:
For 19" rack mount products:

- **Do not install a unit in a rack where the internal rack ambient temperatures will exceed the manufacturer's recommended ambient temperature for all your rack-mounted devices.**
- **Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.**
- **Consideration should be given to the connection of the equipment to the supply circuit so that overloading the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.**
- *(For sliding drawers)* **Do not pull or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack might become unstable if you pull out more than one drawer at a time.**
- *(For fixed drawers)* **This drawer is a fixed drawer and must not be moved for servicing unless specified by the manufacturer. Attempting to move the drawer partially or completely out of the rack might cause the rack to become unstable or cause the drawer to fall out of the rack.**

(R001 Part 2 of 2)

Product handling information

One of the following two safety notices may apply to this product. Please refer to the specific product specifications to determine the weight of the product to see which applies.

CAUTION:
This part or unit is heavy but has a weight smaller than 18 kg (39.7 lb). Use care when lifting, removing, or installing this part or unit. (C008)

CAUTION:
The weight of this part or unit is between 18 and 32 kg (39.7 and 70.5 lb). It takes two persons to safely lift this part or unit. (C009)

Product safety labels

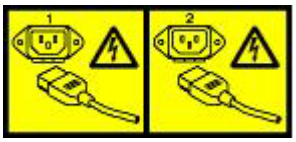
One or more of the following safety labels may apply to this product.

DANGER

Hazardous voltage, current, or energy levels are present inside any component that has this label attached. Do not open any cover or barrier that contains this label. (L001)

DANGER

Multiple power cords. The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords. (L003)



World trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the US English source. Before using a US English publication to install, operate, or service this IBM ISS product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

The following laser safety notices apply to this product:

CAUTION:
This product may contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure. (C026)**

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

Laser compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM ISS product recycling offerings can be found on IBM's Internet site at http:// www.ibm.com/ibm/environment/products/prp.shtml.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM http:// www.ibm.com/ibm/environment/products/prp.shtml.

Notice: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable through the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

注意: このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque: Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'etiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

Battery return program

This product contains a lithium battery. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/ batteryrecycle.shtm or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426- 4333. Please have the IBM part number listed on the battery available prior to your call.

For Taiwan:

Please recycle batteries 廢電池請回收

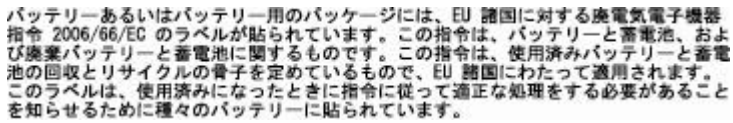
For the European Union:

Notice: This mark applies only to countries within the European Union (EU).

Batteries or packing for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

Les batteries ou emballages pour batteries sont étiquetés conformément aux directives européennes 2006/66/EC, norme relative aux batteries et accumulateurs en usage et aux batteries et accumulateurs usés. Les directives déterminent la marche à suivre en vigueur dans l'Union Européenne pour le retour et

le recyclage des batteries et accumulateurs usés. Cette étiquette est appliquée sur diverses batteries pour indiquer que la batterie ne doit pas être mise au rebut mais plutôt récupérée en fin de cycle de vie selon cette norme.


バッテリーあるいはバッテリー用のパッケージには、EU 諸国に対する廃電気電子機器指令 2006/66/EC のラベルが貼られています。この指令は、バッテリーと蓄電池、および廃棄バッテリーと蓄電池に関するものです。この指令は、使用済みバッテリーと蓄電池の回収とリサイクルの骨子を定めているもので、EU 諸国にわたって適用されます。このラベルは、使用済みになったときに指令に従って適正な処理をする必要があることを知らせるために種々のバッテリーに貼られています。

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a symbol for the metal concerned in the battery (Pb for lead, Hg for the mercury, and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California:

Perchlorate Material - special handling may apply. See http://www.dtsc.ca.gov/ hazardouswaste/ perchlorate.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5, Chapter 33. Best Management Practices for Perchlorate Materials. This product, part, or both may include a lithium manganese dioxide battery which contains a perchlorate substance.

Electronic emissions notices

The following statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

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 instructions contained in the installation 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.

Note: Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, by installation or use of this equipment other than xvi IBM Internet Security Systems as specified in the installation manual, or by any other unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

Note: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité aux normes du ministère des Communications du Canada

Cet appareil numérique de las classe A est conform à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/ EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM ISS cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM ISS option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Warning:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

European Community contact:

IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Telephone: 0049 (0) 711 785 1176
Fax: 0049 (0) 711 785 1283
e-mail: tjahn@de.ibm.com

EC Declaration of Conformity (In German)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EUMitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EGKonformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

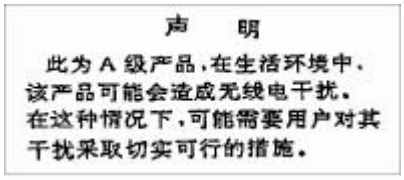
Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A

update: 2004/12/07

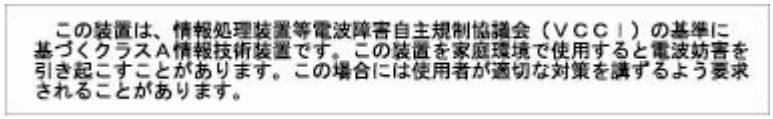
People's Republic of China Class A Compliance Statement:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may need to perform practical actions.

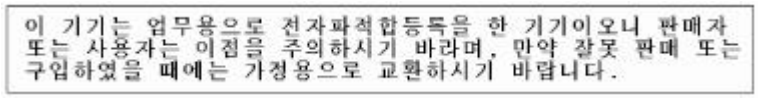


Japan Class A Compliance Statement:

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a xviii IBM Internet Security Systems domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.



Korean Class A Compliance Statement:



About this publication

This guide is designed to help you connect to and configure your Network Active Bypass unit.

Scope

This guide includes basic information and the required procedures for connecting the Network Active Bypass unit to your network and for configuring basic settings.

Audience

This guide is intended for network system administrators responsible for installing and configuring the network and system appliances. A fundamental knowledge of network policies and IP network configuration is helpful.

Latest publications

For the latest documentation, go to the IBM Product Information Center at http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp.

Related publications

See the following documents for more information about the Network IPS appliances supported by the Network Active Bypass unit:

Document	Contents
IBM Proventia GX5000 Series Getting Started Card	Instructions for connecting and configuring a GX5000 Series IPS appliance
IBM Proventia GX6000 Series Getting Started Card	Instructions for connecting and configuring a GX6000 Series IPS appliance
IBM Proventia Network Intrusion Prevention System G and GX Appliance User Guide	Overviews and procedures for creating and managing policies and responses, and maintaining appliance settings.

Contacting IBM Support

IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

Before you contact IBM Support, search for an answer or a solution by using other options first:

- See the Support portfolio topic in the *Software Support Handbook* for information about the types of available support.
- Check IBM Technotes, accessible through the IBM Support Portal.

If you are unable to find an answer or a solution in the Support portfolio or in the IBM Technotes, check to be sure your company or organization has an active IBM maintenance contract, and that you are authorized to submit a problem to IBM, before you contact IBM Support.

Procedure

To contact IBM Support:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - By using IBM Support Assistant (ISA), if the Service Request tool is enabled on your product.
     - Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.
   - Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
   - By telephone for critical, system down, or severity 1 issues. For the telephone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or is about missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a solution is delivered to you. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Chapter 1. Introducing the Network Active Bypass unit

The Network Active Bypass unit is an external device that uses active bypass functions to ensure that network traffic continues to flow if the appliance fails or loses power. The Network Active Bypass unit provides seamless failover, extensive management capabilities, and four independent gigabit Ethernet interface segments with various media combinations. This chapter introduces the features and operating principles for the Network Active Bypass unit.

Package contents

Verify that nothing is missing from the Network Active Bypass unit package contents.

In the box

Check to be sure the following items are in the box:

- One Network Active Bypass unit
- Nine copper cables (green)
- One console cable (blue)
- Two desktop power modules
- Power cords
- One CD

Features

This topic describes the features of the Network Active Bypass unit.

List of features

- Active switching of traffic in case of system failure
- Passive Bypass which is essential during power loss
- Plug and play—no additional drivers required on inline devices
- TAP functions for passive traffic monitoring
- 10/100/1000 TX (Copper), SX (Multi-mode) and LX (Single-mode) support
- Flexible deployment options including Copper, Multi-Mode Fiber, Single-Mode Fiber, and Copper-to-Fiber conversion
- Redundant power supplies for maximum reliability
- Extensive CLI and WEB based management
- SSH and HTTPS for secure management
- E-mail notification on system events
- TACACS+ authentication
- Syslog support
- Full RoHS compliance

Extensive bypass configuration

- Bypass heartbeat custom configurations including:
  - Heartbeat pattern
  - Heartbeat frequency
- Bypass on link loss

- Configuration of the number of link losses before activating bypass
- Configuration of the number of heartbeats before disabling bypass

Secured Web management

The Network Active Bypass unit provides a secured Web management interface that includes the following items:

- Extensive CLI interface
- SSH connectivity over the management port
- SNMP traps on defined events
- E-mail notification on defined events
- TACACS+ authentication
- Syslog support

You can use the management interface to manage and monitor the Network Active Bypass unit from any Web browser. The management port for the Network Active Bypass unit has an assigned IP address. You can retrieve or change the IP address by using command line parameters.

To access the management interface, open a Web browser and type `https://` followed by the management port IP address. The default IP address for the management port is 192.168.0.111. The default management port Web address is https://192.168.0.111.

The management interface is documented in Chapter 3, "Configuring the Network Active Bypass unit in the management interface," on page 11.

Power fail protection

The Network Active Bypass unit uses two redundant power supplies for maximum reliability.

If the power fails, two optical switches remove the Network Active Bypass unit from the network and the Network Active Bypass unit functions as two straight cables.

About the unit

Familiarize yourself with the features of the Network Active Bypass unit before you add the unit to your network.

Front panel diagram

The following figure illustrates the front panel of the Network Active Bypass unit Your unit's front panel may vary depending on the model:

Note: Segments are arranged right-to-left, in the following order: Segment 4, Segment 3, Segment 2, Segment 1.

1. Network ports: 1G (SR, LR, or Copper) N1 and N2 ports connecting to an Ingress network and Egress network
2. Appliance ports: 1G (SR, LR, or Copper) A1 and A2 ports connecting to an IPS appliance
3. LCD display

   Note: LCD buttons are not active.
4. LED indicators (position of LED indicators varies depending on the model)
   - Link/Active LEDs for 1 G ports: lights indicate if a connection exists and the general amount of traffic
   - Existing connection
     - Green indicates a connection
     - Amber indicates a collision
     - No light indicates no connection
   - Amount of traffic
     - Rapid blinking indicates heavy traffic
     - Slow blinking indicates light traffic
     - No blinking indicates no traffic
5. Console port serial
6. Management port Ethernet
7. Tap port

Power adapter

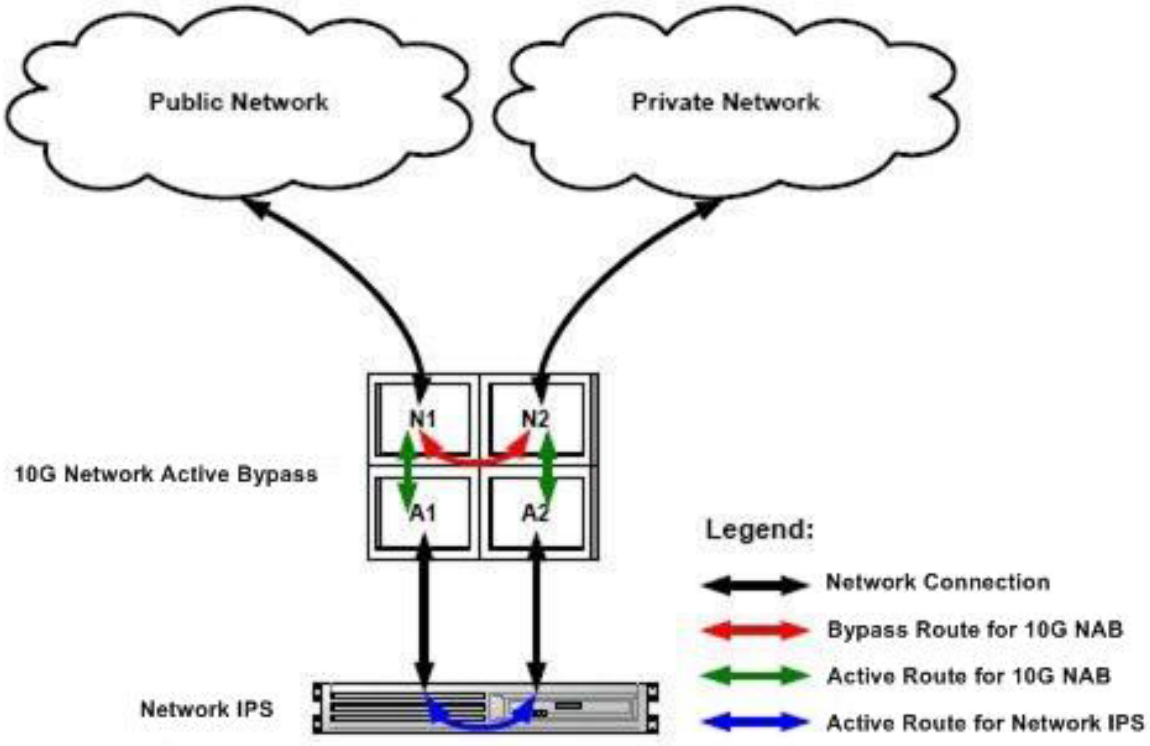
You must use a UL listed power supply with a rated output of 12 VDC, 5 A, marked LPS or NEC Class 2.

Basic operation

This topic describes the basic operating principles of the Network Active Bypass unit.

Typical deployment

The following diagram shows how the data is transferred from the network to the Network IPS through the Network Active Bypass unit, and highlights the associated functions handled at each stage of bypass switching.



Switching modes

The Network Active Bypass unit provides two switching modes:

Switching mode	Description
Active	Active mode channels Ethernet frames between the public network and the private network through the Network IPS appliance. Typically, data flows from the public network to port N1 (network in). The Network Active Bypass unit transfers the data to port A1 (appliance in) and then routes the data through the Network IPS appliance to port A2 (appliance out). Active switching then routes the data through port N2 and out to the private network. Active mode also operates in reverse, routing data from a private network to a public network.

Switching mode	Description
Bypass	Bypass mode channels Ethernet frames from the public network to port N1 (network in). Data is routed through a closed loop from port N1 (network in) to port N2 (network out) and bypasses the Network IPS appliance so that frames go directly from the public network to the private network. Bypass mode also operates in reverse, routing data from a private network to a public network.

Heartbeat modes

The Network Active Bypass unit can continually monitor the health of Network IPS appliances by sending and receiving heartbeat pulses. This ensures real-time safety and accuracy of the data stream. You use a set time defined in the Timeout value (see “Command line parameters” on page 25 for timeout values) to configure heartbeat frames that are sent from the Network Active Bypass unit on one appliance port and received on the other port.

Network Active Bypass unit provides the following heartbeat modes :

Heartbeat mode	Description
Internal Heartbeat Frame Loopback Mode	A user-defined Ethernet heartbeat frame that is generated by the Network Active Bypass unit. and sent from port A1.The Network Active Bypass unit Ethernet port A2 must receive the same heartbeat frame from the Network IPS appliance. **Note:** The heartbeat is sent every 100 milliseconds (ms) by default and can be increased up to 25500 ms. This mode is designed for Network IPS appliances that act as a bridge. Make sure appliances are properly configured so that the device does not filter out the heartbeat frame. This mode does not require a driver for Network IPS appliances. Default: 1
Link Status Heartbeat Mode	The heartbeat signal acts as a link status indicator for Network Active Bypass unit Ethernet port A1 and A2. If port A1 or port A2 loses the link, theNetwork Active Bypass unit stops the heartbeat transmissions and activates bypass mode.

Operation modes

The Network Active Bypass unit uses the following operation modes:

Operation mode	Description
Mode 0: Normal Active Inline	The bypass unit passes traffic to the Network IPS appliance. If the unit does not receive a heartbeat, then it bypasses the Network IPS appliance and forwards the traffic to the network.

Operation mode	Description
Mode 1: Normal Inline	The bypass unit passes traffic to the network, bypassing the Network IPS appliance. If the unit does not receive a heartbeat, then it passes traffic to the Network IPS appliance.
Mode 2: Manual Active Inline	The bypass unit always passes traffic to the Network IPS appliance, whether it receives a heartbeat or not. Another description for this mode is that the bypass unit always works in Active Switching mode.
Mode 3: Manual Active Bypass	The bypass unit always passes traffic to the network, bypassing the Network IPS appliance, whether it receives a heartbeat or not. Another description for this mode is that the bypass unit always works in Bypass Switching mode. This operation mode is useful for maintenance tasks, such as updating firmware, installing patches, or replacing appliances.
Mode 4: Manual Passive Bypass	The bypass unit does not pass any traffic, either to the Network IPS appliance or to the network. This operation mode is useful for testing high availability scenarios.

Chapter 2. Setting up the Network Active Bypass unit

This chapter contains information you need to connect and configure the Network Active Bypass unit.

Configuring and deploying the Proventia Network Active Bypass unit

This topic contains detailed steps for configuring and deploying the Network Active Bypass unit.

About this task

The following process is required to configure and deploy the Network Active Bypass unit.

Procedure

1. Place the Network Active Bypass unit and the Network IPS appliances on a rack.
2. Connect the cable to and configure the Network IPS appliances using the instructions provided in the *Proventia GX Getting Started Guide*.
3. Connect the power cables to the Network Active Bypass unit and to two different power sources (for added redundancy).
4. Use a browser to access the management interface and log in.
5. Verify that the Network Active Bypass unit is passing traffic.
6. Use the management interface to set the segment configuration. (This process maps the ports on the appliance and sets bypass tolerances.)

Placing the Network Active Bypass unit and the Network IPS appliances

Procedure

1. Decide where to place the Network Active Bypass unit and the Network IPS appliances.
2. Add the Network Active Bypass unit and the Network IPS appliances to the rack.
3. Connect the cable to the Network IPS appliances using the instructions provided in the *Proventia GX Getting Started Guide*.

   Note: The Network Active Bypass unit uses four 1 Gb segments.

Connecting the power cables

Procedure

1. Plug the DC connector of each AC adapter into the Network Active Bypass unit.
2. Plug one of the power cables into an AC outlet. Plug the other power cable into an AC outlet serviced by a different AC feed.

   Tip: Use independent AC power sources to maximize power redundancy in the event of AC power loss from a single source.
3. Check the power LEDs to confirm that the Network Active Bypass unit is receiving power.

Logging into the management interface

Procedure

1. Use the management cable (labeled "CAT5E") to connect a computer to the management port on the Network Active Bypass unit.

   Important: Make sure you follow industry best practices for securing your critical network infrastructure. Do not connect the management port to any network that is open to external traffic. The management port should be connected only to a restricted network that is dedicated to managing the Network Active Bypass unit and the Network IPS appliances.
2. Start Internet Explorer.
3. Type `https://192.168.0.111`.

   Note: The default IP address for the management port is 192.168.0.111. If you change the management port IP address, the Web address to access the management port is changed to include the new IP address.
4. Log in to the management interface. Use the default user name and password the first time you connect to the management interface.

Field	Default setting
User Name	`admin`
Password	`admin`

Note: If you change the default log on settings on the Users page of the management interface, the values you set are in effect for future log on attempts.

Setting up e-mail notification

About this task

Configure e-mail notification to receive a status e-mail when the state of the Network Active Bypass unit changes. You must set up e-mail notification *before* you configure your segments.

Setting up segments

Procedure

1. In the management interface, select theSegment page for the Segment you want to configure.
2. Type or select the appropriate settings, and then click **Save**

Chapter 3. Configuring the Network Active Bypass unit in the management interface

You can use either the management interface or the command line interface to set most of the configuration options for the Network Active Bypass unit. This chapter lists the configuration options available through the user interface, and describes how to set them.

About the management interface

The Network Active Bypass unit provides a secured Web management interface.

Management pages

The management interface consists of a series of pages, as indicated in the following table:

Management Page	Description
Status	Status information about the Network Active Bypass unit
Management Port	IP settings for the management port
Segment 1	Port settings and heartbeat settings to activate bypass or get into active mode, for appliances on this segment.
Segment 2	Port settings and heartbeat settings to activate bypass or get into active mode, for appliances on this segment.
Segment 3	Port settings and heartbeat settings to activate bypass or get into active mode, for appliances on this segment.
Segment 4	Port settings and heartbeat settings to activate bypass or get into active mode, for appliances on this segment.
Email Notifications	Settings required for e-mail notification, such as e-mail accounts and mail server information
SNMP Settings	Settings for sending SNMP traps to an SNMP trap server
NTP Settings	Settings that enable the network time protocol (NTP) to synchronize the Network Active Bypass unit time with a network time server
Time Settings	Time zone settings for the Network Active Bypass unit
Backup/Restore	Backup, restore, and reset to factory default functions
Firmware Update	Upload firmware update files to the Network Active Bypass unit
Log Settings	Settings for the system log files
Reboot	Reboot the Network Active Bypass unit
Users	Change the admin password
Remote Authentication	Settings that allow a remote access server to communicate with an authentication server in order to determine if the user has access to the network

Accessing the management interface

You can manage and monitor the Network Active Bypass unit from any Web browser.

Prerequisite

Make sure that the Ethernet management port for the Network Active Bypass unit is connected to the local network or to the host computer.

Default management port IP address and Web address

The Network Active Bypass unit has a default IP address assigned to the management port. The default IP address and URL are shown in the following table:

Item	Default value
Management port IP address	192.168.0.111
Management port Web address	https://192.168.0.111

These default values remain in effect until you change them. You can use command line parameters or use the Management Port page of the management interface to change the the IP address for the management port.

Important: Changes to the management port can interrupt the management interface connection. Make sure that the new IP address is accessible before you make any changes. When you change the IP address, the management port Web address changes also.

Management interface Web address

You can access the management interface using a Web address that consists of https:// followed by the management port's IP address. The Web address format is as follows:

https://*xxx.xxx.xxx.xxx*

When you type the Web address, replace xxx.xxx.xxx.xxx with the IP address assigned to the management port.

For example, the default Web address is https://192.168.0.111

Note: When you enter the Web address, you will see a message regarding the Web site's security certificate. Click “Continue to this website (not recommended)” to proceed.

Logging in

When you enter the management Web site, you see the log in screen. Complete the fields as indicated in the following table.

Field	Description
User	Type the user name **Note:** The default user is `admin`.
Password	Type the password **Note:** The default password is `admin`.

The default values remain in effect until you change them. If you need to change the user name or password, you can use the Users page of the management interface or the command line interface.

Monitoring the status of the Network Active Bypass unit

This topic provides information about using the management interface to monitor the status of the Network Active Bypass unit.

Checking overall status

The Status page is the first page you see when you log in to the management interface. Use the Status page to view information for the Network Active Bypass unit. The Status page provides information in sections, as indicated in the following table.

Section	Description
System	Provides general information about the Network Active Bypass unit
Power Supply	Indicates whether power supplies are present or not present
Segment 1	Shows the active/bypass status for segment 1
Segment 2	Shows the active/bypass status for segment 2
Segment 3	Shows the active/bypass status for segment 3
Segment 4	Shows the active/bypass status for segment 4
Tap Settings	Shows current port configurations

Viewing system status

The System section provides general system status, as indicated in the following table.

Field	Description
Product Name	Displays the name of the Network Active Bypass unit: "Proventia® NAB"
Product ID	Displays the product ID of the Network Active Bypass unit: "Proventia NAB rev 1"
Hardware Revision	Displays the hardware version of the Network Active Bypass unit
Firmware Version	Displays the current firmware version of the Network Active Bypass unit
Management IP	Displays the IP address for the management port **Tip:** Use the Management Port page if you want to change IP settings for the management port. Default: 192.168.0.111
Email Notifications	Indicates whether e-mail notifications are enabled or disabled **Tip:** Use the Email Notification page if you want to change e-mail settings. Default: Disable (Don't send)

Managing settings for the Network Active Bypass unit

Use the management interface to view or change settings for the Network Active Bypass unit.

Setting up segment configurations

Procedure

1. In the management interface, select the Segment Configuration page.
2. Complete the fields for each of the four segments (A - D) that best fits your specific network environment:

Field	Description
Max time allowed between heartbeat acceptance (100 ms - 25500 ms)	Specifies the user-defined Ethernet heartbeat frame generated by the Network Active Bypass unit. The heartbeat frames are sent from the Network Active Bypass unit Ethernet port A1 every 100 milliseconds (ms), and the Network Active Bypass unit Ethernet port A2 must receive the same heartbeat frame from the Network IPS appliance.
Number of HB lost to activate bypass (1–10)	Specifies the heartbeat signal that acts as a link up status indicator for the Network Active Bypass unit Ethernet ports A1 and A2. If port A1 or A2 loses the link, Network Active Bypass unit stops the heartbeat transmission and activates bypass mode.
Number of accepted HB to get into active mode (1–10)	Specifies the user-defined Ethernet heartbeat frame that is generated by the Network IPS appliance. This is the number of heartbeats the Network Active Bypass unit must receive in order for the unit to change from bypass to active. Default: 1

Field	Description
Operation Mode	Specifies the operation mode of the Network Active Bypass unit: • Mode 0: Normal Active Bypass (Default mode) - If Network Active Bypass unit receives heartbeat signals within the Timeout period, the switching mode remains or is changed to Active Switching mode. If Network Active Bypass unit does not receive heartbeat signals within the Timeout period, it will change to or remain in Bypass Switching mode. By default (without a heartbeat), Network Active Bypass unit remains in Bypass Switching mode. • Mode 1: Normal Active Inline - If Network Active Bypass unit receives heartbeat signals within the Timeout period, the switching mode remains or is changed to Bypass Switching mode. If Network Active Bypass unit does not receive heartbeat signals within the Timeout period, it will change to or remain in Active Switching mode. By default (without a heartbeat), Network Active Bypass unit remains in Active Switching mode. • Mode 2: Manual Active - Network Active Bypass unit is always in Active Switching mode. • Mode 3: Manual Active Bypass - Network Active Bypass unit is always in Bypass Switching mode. • Mode 4: Manual Passive Bypass - Network Active Bypass unit is in passive bypass, in which the optical switch is “Close” in bypass mode.
Link fault detection	Generates an SNMP trap if a network port stops functioning: • 0: disables the system from detecting Link Fault Detection • 1: enables the system to detect and activate Link Fault Detection Default: Enabled
Tap Setting	Specifies the ports on the Network Active Bypass unit for data flow during Bypass Switching mode and Active Switching mode: • Port N1: Network in • Port N2: Network out • Port A1: Appliance in • Port A2: Appliance out Options for Tap setting are: • RX • TX • RX/TX

Configuring Management Port settings

Procedure

Use the Management Port page to configure IP settings for the management port.

Field	Description
IP Address	IP address of the management port Default: 192.168.0.111
Network Mask	IP address of the network or subnet mask Default: 255.255.255.0
Gateway	IP address of the network gateway Default: 192.168.0.1
DNS 1	IP address of the primary domain name system server Default: 192.168.0.1
DNS 2	IP address of the secondary domain name system server Default: 0.0.0.0

Setting up e-mail notifications

About this task

TheNetwork Active Bypass unit provides an e-mail notification function that you can configure to send an e-mail message when the switching mode of a segment has changed. Use the Email Notification page to configure e-mail servers and accounts, and to enable or disable notifications.

Procedure

Set the values as indicated in the following table.

Field	Description
Email Notification	Enable or disable e-mail notification Default: Disabled (Don't send)
Outgoing Mail Server (SMTP)	Address of the appropriate outgoing SMTP mail server
Outgoing Mail Server (SMTP) Port	Port number of the outgoing SMTP mail server Default: 25
SMTP Username	User name for the outgoing SMTP mail server
SMTP Password	Password for the outgoing SMTP mail server (if applicable)
Outgoing Server (SMTP) Security	SSL encryption used between the SMTP mail server and mail client Default: Enable (Secured)
From (Sender's email address)	Name or address that should be displayed in the **From** field of an outgoing e-mail message
To (List of recipients, comma separated)	List of e-mail addresses to whom the notification should be sent

Field	Description
Subject	Subject to be displayed in the subject line of the outgoing e-mail message Example: “Proventia NAB status report”

Configuring SNMP traps

About this task

The Network Active Bypass unit provides an SNMP trap function that can send messages to a trap server when the segment status or power supply status changes. Use the SNMP Settings page to configure the SNMP destination IP and SNMPv2 community name, and to enable or disable the SNMP trap function.

Procedure

Complete the fields as indicated in the following table.

Field	Description
Send SNMP Traps	Enable or disable the sending of SNMP traps Default: Disabled
SNMP traps destination IP	Destination IP of the SNMP trap server Default: localhost
SNMPv2 community	Community name of the SNMP trap server Default: public

Synchronizing time and setting time zones

Procedure

Use the NTP Setting page to enable the network time protocol (NTP) to synchronize the Network Active Bypass unit time with a network time server. Use the Time Setting page to set the time zone for the Network Active Bypass unit. Set the values as described in the following table.

Field	Description
NTP	Protocol that synchronizes the Network Active Bypass unit time with a network time server Default: Disabled
NTP Server	Public domain of a collection of computers that provide time using NTP
Time Zone	Time zone used by the Network Active Bypass unit Default: America\New York

Managing User Account settings

Procedure

Use the Users page to change the user name and password required to access the Web management interface.

Field	Description
Password	Password required to access the management interface from a Web browser
Confirm Password	Confirmation for the password required to access the management interface from a Web browser

Backing up or restoring settings

Procedure

Use the Backup/Restore page to make a backup file or to return the Network Active Bypass unit to its default settings. Complete the fields as indicated in the following table.

Field	Description
Backup	Saves a copy of current settings on the Network Active Bypass unit in a file named `config.txt`
Restore From	Location of a stored backup file. Type the file location or navigate to the file, and click **Restore From**.
Restore to Factory Default Configuration	Restores the Network Active Bypass unit to the default configuration and then restarts it **Important:** The IP address for the management interface is not reset.

Applying firmware updates

About this task

Use the Firmware Update page to manually upload firmware updates to theNetwork Active Bypass unit. Browse to the update file location, and click **Upload Firmware**.

Note: It can take up to 5 minutes for the process to finish.
Check the Status page to verify that the new firmware version has been installed.

Enabling system logging

About this task

Use the Log Setting page to enable the consolidation of log data from various systems into a central repository. System logs contain important information about actions the Network Active Bypass unit has taken, due to user interaction, such as a system restart or manual feature configuration, or due to a system action, such as an automatic restart after firmware update.

Procedure

Complete the fields as indicated in the following table.

Field	Description
Logging	Set up consolidation of log data Default: Disabled
Syslog Server Host	IP address of the central repository of log data Default: localhost
Syslog Server Port	Port number on which the syslog server is monitoring Default: 514
Syslog Server Identification	Host name of the syslog server Default: NAB

Restarting the Network Active Bypass unit

About this task

Use the Restart page to restart the Network Active Bypass unit.

Configuring Remote Authentication

About this task

Use the Remote Authentication page to configure settings for the TACACS+ protocol. The TACACS+ (Terminal Access Controller Access Control System Plus) protocol provides access control (separate authentication, authorization, and accounting services) for Network Active Bypass unit from one or more servers.

Procedure

Complete the fields as indicated in the following table.

Field	Description
TACACS+	Allows TACACS+ protocol for access control Default: Disabled
Server	IP address of the server providing access services Default: 0.0.0.0
Encrypt	Encrypts the body of the TACACS+ packets for more secure communications Default: No
Secret	Shared secret value for encryption that is known to both the client and the daemon Default: None
Service	Services that are requesting authentication Default: All

Chapter 4. Configuring the Network Active Bypass unit using the command line interface

You can use either the management interface or the command line interface to set most of the configuration options for the Network Active Bypass unit. This chapter lists the command line parameters, and describes how to set up configuration options through the command line interface.

Accessing the command line interface

This topic contains the information you need to access the command line interface.

Connection types

You can access the command line interface for the Network Active Bypass unit in one of two ways:

- Through a serial terminal emulator
- Through an SSH remote shell emulator

Connection requirements

The requirements for both connection types are shown in the following table.

Connection type	Port on Network Active Bypass unit	Cable
Serial terminal emulator	Console port	Console cable
SSH remote shell emulator	Management port	Management cable

Serial terminal settings

Use a serial terminal emulator and the following terminal settings:

Setting	Value
Communications Port	Typically COM1 (depending on computer setup)
Emulation	VT100
Bits per second	115,200
Data bits	8
Parity	None
Stop	1
Flow Control	None

SSH port

The Network Active Bypass unit SSH server uses the standard port 22.

User name and password

Use the administrator account to configure parameters and to monitor the status of the Network Active Bypass unit. The default user name and password are listed in the following table.

Field	Description
User	Type the user name **Note:** The default user is `admin`.
Password	Type the password **Note:** The default user is `admin`.

Note: You can change the password through the command line interface or through the management interface.

Syntax for command line parameters

This topic outlines the syntax required to set or to retrieve values using the command line parameters.

Permissions required

Only the Admin account has permissions to set and to retrieve system parameters.

Command line syntax

Use the following command line syntax to set or to retrieve values for parameters.

Command	Action
cli get |more	Outputs values for all parameters
cli get *parameter_ name*	Specifies a value for the parameter **Example:** Typing `cli get timeout` displays the timeout value in decimal form
cli set *parameter_name parameter_value*	Sets a value for the parameter you specify **Example:** Typing `cli set timeout 20` sets the timeout value to 20

Command line parameters

This topic lists the command line parameters available for the Network Active Bypass unit.

The parameters are divided into the following categories:

- Management port
- Communication
- E-mail notification
- SNMP
- Operational

Use parameters with care

Use these command line parameters carefully, because they control the behavior of the Network Active Bypass unit. Do not change a default value unless you are sure of the effect the change will have on your network. Some parameters should not be changed unless you are instructed to do so by a representative from IBM ISS Customer Support.

Management port parameters

The parameters in the following table control the IP settings for the management port.

Parameter	Description
ip	Current IP address for the management port for Network Active Bypass unit Default: 172.16.124.17
mask	Subnet mask for the management port Default: 255.255.255.0

Parameter	Description
gw	Gateway IP address for the management port Default: 172.16.124.1
current_ip	Current IP address for the management port **Note:** The current_ip parameter is read only.

Communication parameters

The parameters in the following table control the communication features of the Network Active Bypass unit. Use `cli get` to retrieve the current value for a parameter. Use `cli set`, plus the new value to change the value of the parameter. For example, `cli set ip` 127.0.0.1.

Parameter	Description
dns	DNS server IP address **Note:** This parameter corresponds to DNS 1 in the user interface.
dns2	Second DNS server IP address
domain	Domain name for the local host Default: local
dhcp	DHCP client dhcp: Set this parameter to dhcp to enable the DHCP client on the Network Active Bypass unit management port. Static: Set this parameter to static to disable the DHCP client on the Network Active Bypass unit management port
host	Host name for the unit This parameter is read-only. Default: Proventia_NAB
username	Administrator account name Default: admin
password	Administrator password Default: admin
https	Enables or disables the HTTPS server • 0: disables the secure Web management interface • 1: enables access to the secure Web management interface Default: 1 (enabled)

E-mail notification parameters

The parameters in the following table control the e-mail notification feature.

Parameter	Description
email	Enables or disables the e-mail notification feature • 0: disables e-mail notification • 1: enables e-mail notification Default: 1
email_from	Name or e-mail address that is displayed in the "From" field on the e-mail notification
email_security	Enables or disables the e-mail security feature • 0: disables e-mail security feature • 1: enables e-mail security feature Default: 1
email_username	User name for the e-mail account used to send e-mail notifications from the Network Active Bypass unit
email_password	Password for the e-mail account used to send e-mail notifications from the Network Active Bypass unit
email_server	SMTP server address for the mail server
email_subject	Text to be displayed in the subject line of notification e-mail messages Sample: "Notice: PNAB segment(s) have switched modes"
email_to	List of e-mail addresses to which the notification should be sent

SNMP parameters

The parameters in the following table control the sending of SNMP traps.

Parameter	Description
snmp	Enables or disables the SNMP function • 0: disables SNMP function • 1: enables SNMP function Default: 0 (disabled)
snmp_community	SNMP community name Default: public
snmp_destination	SNMP destination Default: localhost
LFD	Link Fault Detection generated if a network port goes down • 0: disables the system from detecting Link Fault Detection • 1: enables the system to detect and activate Link Fault Detection Default: Enabled

Operational parameters

The parameters in the following table control the behavior of the Network Active Bypass unit.

Parameter	Description
timeout	Timeout value for Network Active Bypass unit Each timeout unit is 100 ms. (Timeout range is 100 milliseconds to 25.5 seconds.) In default bypass operation mode, if the Network Active Bypass unit does not detect a heartbeat frame within the set timeout value, the segment will switch from active to bypass. Default: 1
force	Force (debug) mode for each I/O unit • 0: Disables force (debug) mode • 2: Forces segment to Active Switch mode • 4: Forces segment to Bypass Switch mode Default: 0 (Disable)
op_mode	Default operation mode for the Network Active Bypass unit • 0: Normal Active Bypass If heartbeat is received, system will be inline. • 1: Normal Inline If heartbeat is received, system will be in bypass. • 2: Always Inline • 4: Always Active Bypass • 5: Manual Passive Bypass (Bypass Switch is closed in bypass mode) Default: 0 (Normal Active Bypass)
hb_mode	Heartbeat mode for the Network Active Bypass unit • hb_mode 1: system is generating heartbeat • hb_mode 2: external source is generating heartbeat • hb_mode 3: system activates bypass depending on link detection on the appliance Default: hb_mode 1
state	State of the Network Active Bypass unit This parameter is read-only. • 0: Bypass Switch state • 1: Active/Inline Switch state
active_hb_cnt	Stores the active heartbeat signal count The segment switches to Active Switch mode only if it receives active_hb_cnt number for a consecutive heartbeat. Default: 2 (Range: 1 - 10)

Parameter	Description
bypass_hb_cnt	Stores the bypass heartbeat signal count The segment will switch to Bypass Switch mode only if it loses bypass_hb_cnt heartbeat signal number. Default: 3 (Range: 1 - 10)

TACACS+ parameters

Use the following parameters to configure TACACS+ from the CLI:

Parameter	Description
tacacs	Values: • 0: disabled • 1: enabled
tacacs_encryption	Values: • 0: disabled • 1: enabled
tacacs_protocol	TACACS+ protocol Default: all
tacacs_secret	TACACS+ secret Default: None
tacacs_server	IP number of TACACS+ server
tacacs_service	TACACS+ service Default: all

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Index

Printed in USA