IBM Security

Intelligence. Integration. Expertise.

IBM® Security Network Active Bypass Open Mic - Wednesday, April 27, 2016

IBM

How to properly deploy, configure and upgrade the NAB

Panelists

- Jeff DiCostanzo, Presenter – AVP Team Lead
- Bill Klauke - Level 2 Product Lead
- Maxime Turlot - Level 2 Product Lead
- Ryan Andersen - Level 2 Senior Engineer
- Edward A Romero - Level 3 Network Security Engineer
- Steven McKinney – Level 2 Support Team Lead

Reminder: You must dial-in to the phone conference to listen to the panelists. The web cast does not include audio.

- **USA toll-free:** 1-866-803-2145
- **USA toll:** 1-210-795-1099
- **Participant passcode:** 1322112
- Slides and additional dial in numbers:

http://bit.ly/OpenMicXGS20160427doc

NOTICE: By participating in this call, you give your irrevocable consent to IBM to record any statements that you may make during the call, as well as to IBM's use of such recording in any and all media, including for video postings on YouTube. If you object, please do not connect to this call.

Agenda

- What is a NAB and when to use it
- How to deploy, configure, and upgrade
- Proactive steps
- Troubleshooting

What is a NAB?

What is a NAB?

- NAB = Network **Active** Bypass unit is an External unit that sits in front of a XGS/GX.

- Its sole purpose is to ensure traffic flows around the appliance if the appliance blocks traffic due to various issues: power loss, link failures, OS crashes, very high latency on IPS, etc.

- **Active** – The NAB actively sends packets through the IPS to ensure the proper flow of traffic.

  Note: The IPS has no idea the bypass is there.

- NABs replace the old passive bypass where the GX would send heartbeats to the bypass through an external USB connection.

- Manufactured by Interface Masters (IM) and installed with IBM custom code.

- Comes in two flavors with multiple NIC configurations:

  1GB supports 4 x 1GB networks

  10GB supports 4 x 10GB networks

When to deploy

Does every GX/XGS model need an external bypass?

GX - GX 4000 - All built-in copper ports have an internal “built-in” bypass →No NAB needed
GX 5000 and up none of the NICS have an internal bypass → NAB recommended

XGS - All built-in copper and built-in Fiber ports have an internal “built-in” bypass→ No NAB needed
All NIMs that do not use SFPs → No NAB needed
All SFP NIMs → NAB recommended

Advantages of deploying NAB

1) Various configurable settings EX: Bypass mode, heartbeat interval, bypass threshold,….
2) Remote alert notifications via SNMP, email, syslog
3) Can place different segments into bypass for any system maintenance on IPS (changing SFPs , RMA replacement, etc) without network disruption
4) NABs maintain link with the connected equipment even if the appliance links change (Prevents spanning tree from blocking traffic for 30 – 60 secs)
5) Provides port statistics

- Note: Based on the above advantages you still may want to deploy a NAB even when your IPS has an internal built-in bypass.

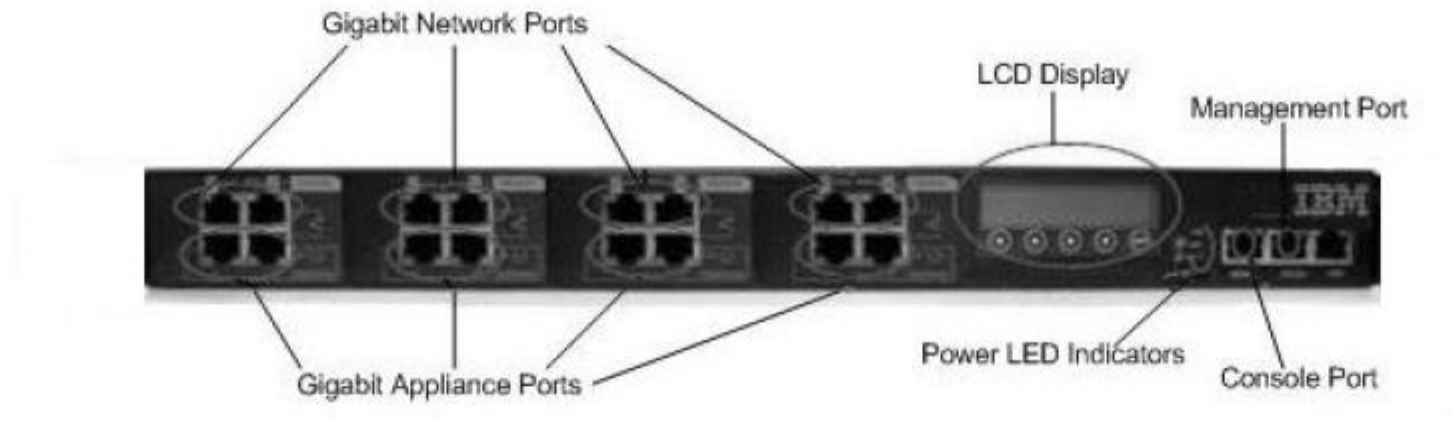
HA Environment

Option 1: Do NOT deploy as the surrounding architecture will fail over to the other path if there is a problem with the IPS so the other security appliance can analyze the traffic. (Recommended)

Option 2 : If deployed the traffic will pass through the appliance uninspected if there is an issue with the IPS and the traffic will not failover to the other path.

- Note: There is a HA service menu in the LMI where if a NAB segment fails it will fail over to another segment however both NAB segments would have to be plugged into the same network equipment and same IPS. Support has never seen this used in the field so this should stay disabled.

Network Active Bypass 1GB



- Segments start from left to right. Seg 1 , Seg 2, Seg3, Seg 4
- Network ports N1 and N2 (SR, LR, Copper)   connect to network
- Appliance ports A1 and A2 (SR, LR, Copper)   connect to the appliance
- Green Led = Inline state
- Red Led = Bypass state

-

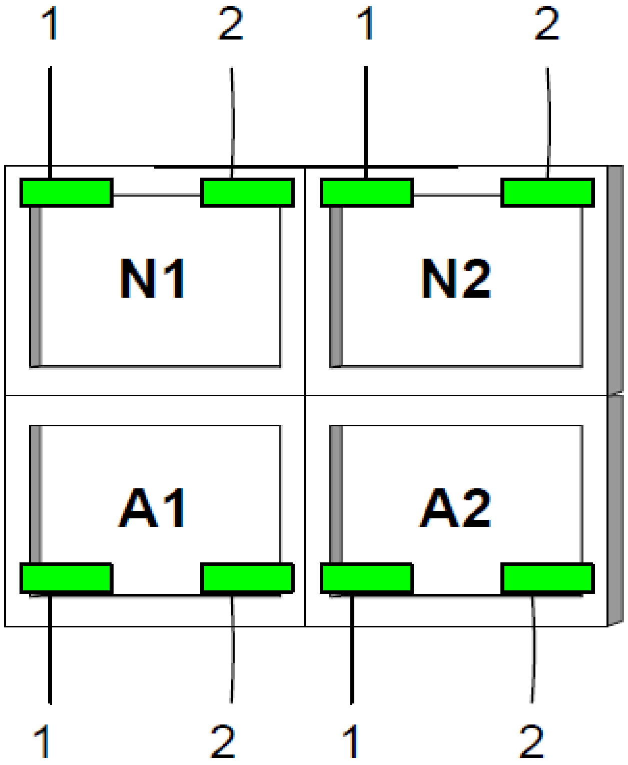
1GB NAB NIC Lights

LED 1 = Link speed of the port

- Green LED on signifies1G
- Green LED off signifies 10M or 100M

LED 2 = Link status of the port

- Green LED on signifies link is stable
- Blinking LED signifies there is traffic on that port
- No LED signifies no link

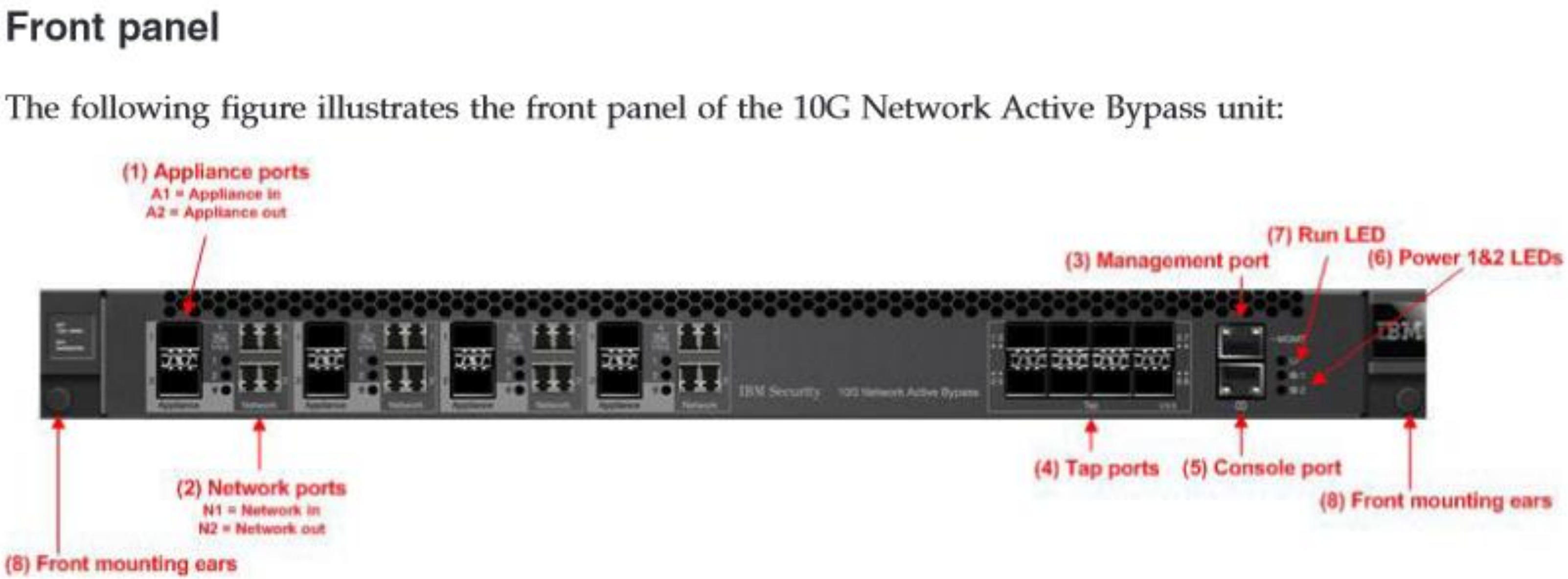


1 GB NAB Models

Model	Supported 1 GbE segments
ABYP-4T-0S-0L	4 TX copper
ABYP-0T-4S-0L	4 SX fiber
ABYP-0T-0S-4L	4 LX fiber
ABYP-2T-2S-0L	2 copper + 2 SX fiber
ABYP-2T-0S-2L	2 copper + 2 LX fiber
ABYP-2T-1S-1L	2 copper + 1 SX fiber and 1 LX fiber
ABYP-0T-2S-2L	2 SX fiber + 2 LX fiber

- SX = Multi-Mode Fiber (Short range)
- LX = Single-Mode Fiber (Long range)

Network Active Bypass 10GB



Front panel

The following figure illustrates the front panel of the 10G Network Active Bypass unit:

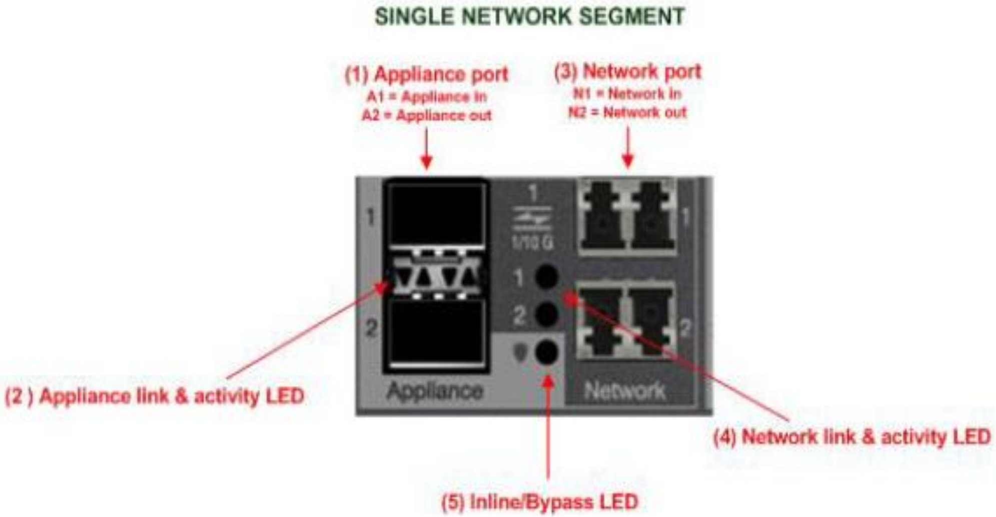
- Run LEDS

Blinking green = System is booting
Solid green = Normal operations

- Power LEDS

Solid green = Connected
Solid red = Not connected

NAB 10GB LEDs



- **10G = Orange LED** Solid LED = Traffic Link
  Blinking orange = Traffic activity (blinks only when receiving traffic, not when transmitting traffic)

- **1G = Yellow LED** Solid LED= Traffic Link
  Blinking yellow = Traffic activity

- **10M/100M Green LED** Solid LED = Traffic Link
  Blinking green = Traffic activity

10 GB NAB Models

Model	**Supported 10 GbE segments**
ABYP-10G-2SR-2LR	2 SR fiber + 2 LR fiber
ABYP-10G-4LR	4 LR fiber
ABYP-10G-4SR	4 SR fiber

- SR = Multi-Mode Fiber (Short range)
- LR = Single-Mode Fiber (Long range)

SFP / SFP+ NICs

Transceiver kit options – 2 transceivers in a kit

- TX – 1 Gigabit copper
- SX – 1 Gigabit short range fiber
- LX – 1 Gigabit long range fiber
- SR – 10 Gigabit short range fiber
- LR – 10 Gigabit long range fiber

Note: Do not forget to order kits for the bypass if your XGS or GX has SFPs.

Example : If you have a 4 x1GbE (SX) SFP NIM you need two 1GbE (SX) SFP transceiver kits for the NAB.

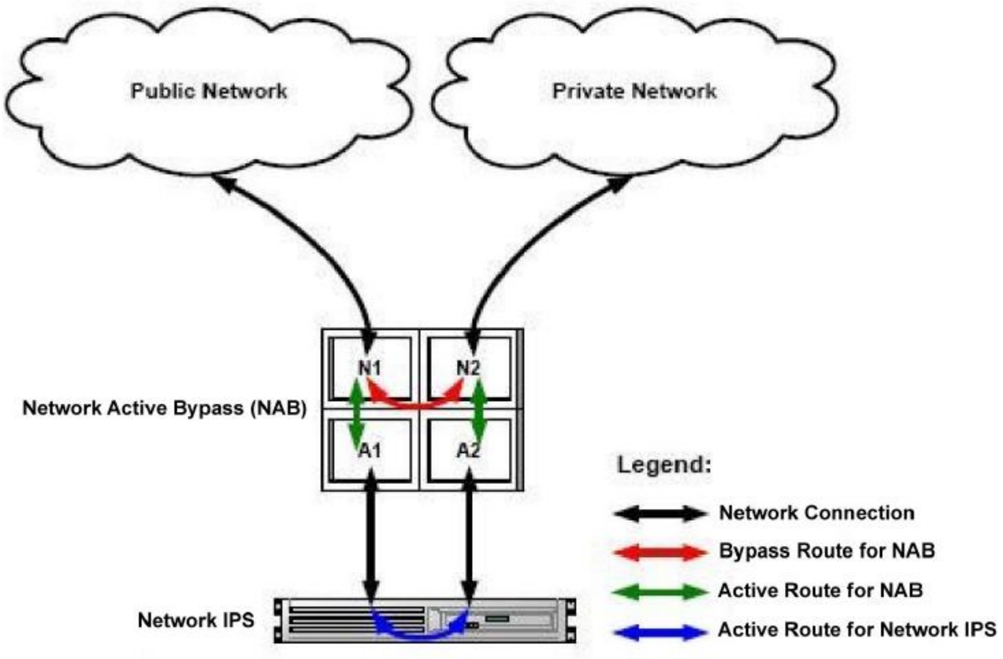
IBM Security

Intelligence. Integration. Expertise.

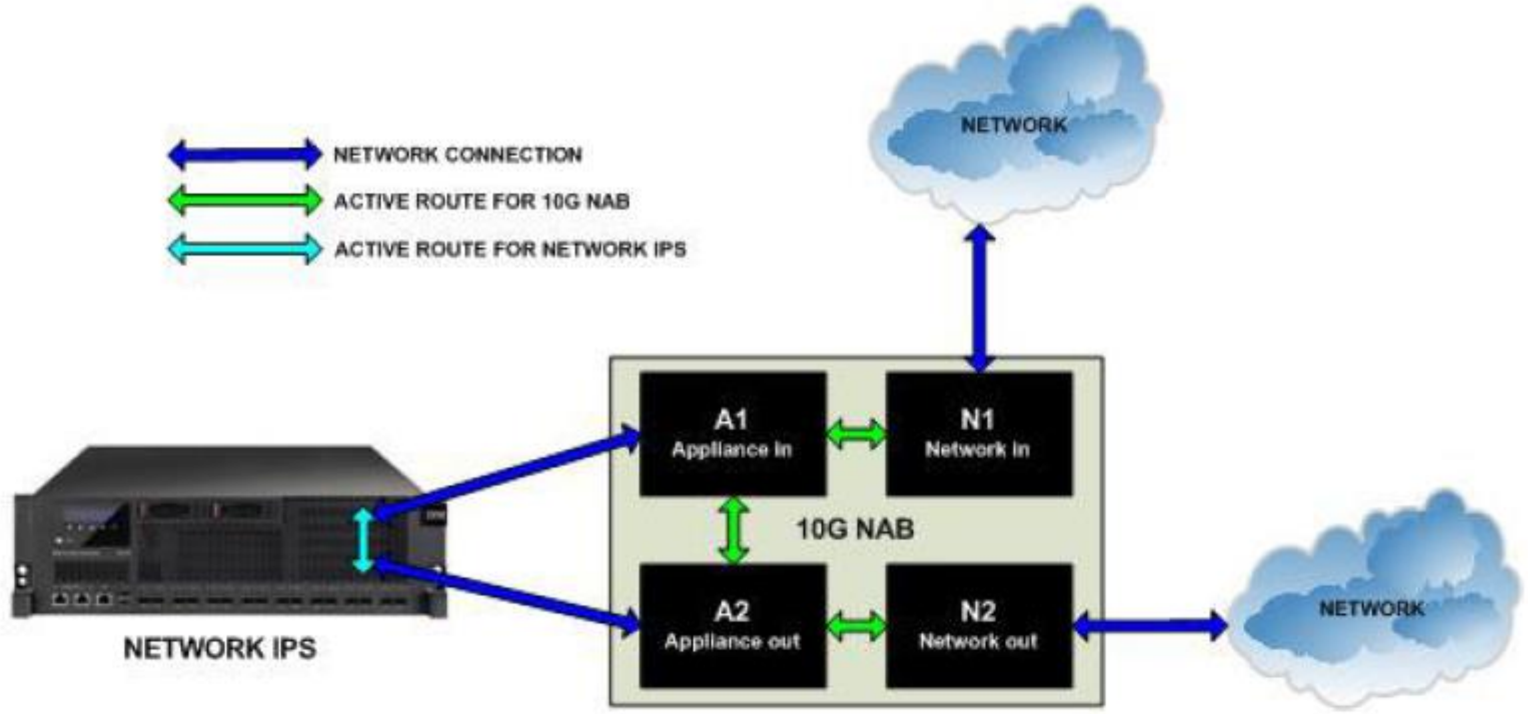
IBM

Deployment, Configuration and Upgrade procedures

1 GB NAB Deployment



10 GB NAB Deployment



Deployment - Cabling

- **Copper:** All equipment ports need the speed/duplex to be hard coded to minimize link issues. Proper cabling is a must.
- EX Scenario: firewall, switch, NAB, and IPS

  Hard code all interfaces to desired speed

  Connect firewall to NAB (N1) using a crossover cable

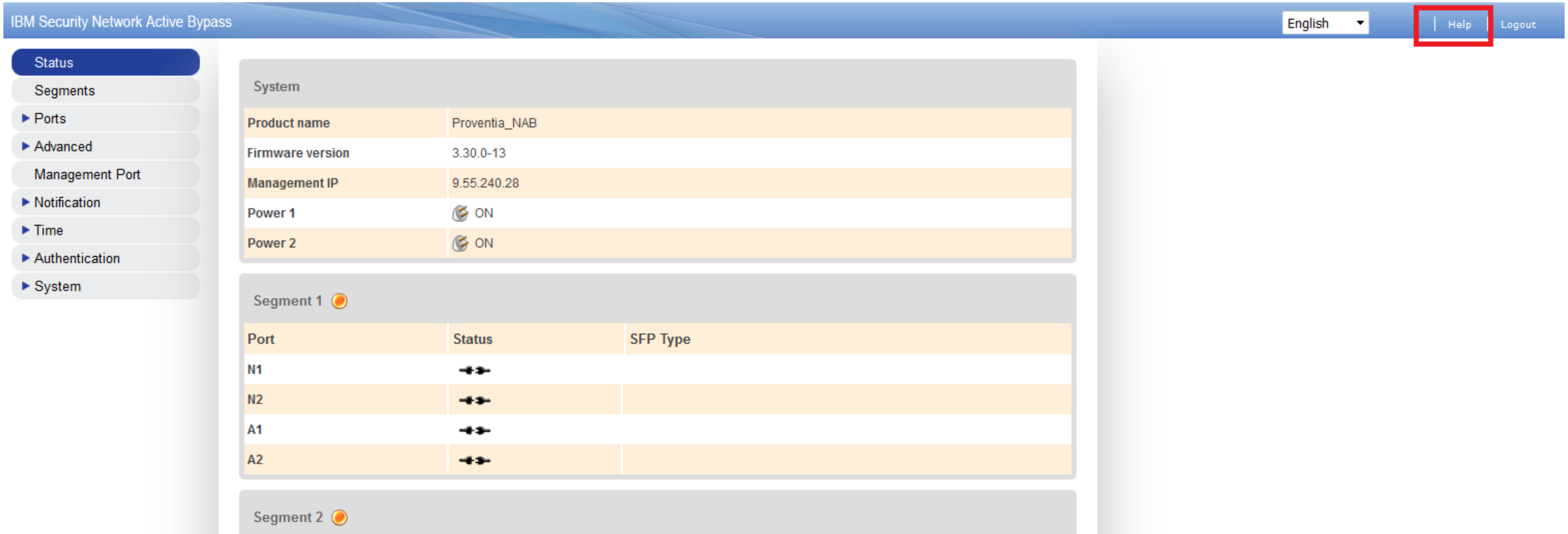
  Connect switch to NAB (N2) using a straight cable

  Connect NAB to A1 and A2 using straight cable
- **Fiber:** For 1 GB Fiber you can use Auto however for any 10 GB SFP+ hard coding to 1 GB or 10 GB is recommended.

Important: 1) Always connect the NAB to the network with the power off to verify traffic flow to ensure proper cabling.

2) Ensure to use the correct Fiber types (SX , LX , etc) that match your GX/XGS. You can NOT mix Fiber types on the same network connection.

Initial Setup Configuration



System

Product name	Proventia_NAB
Firmware version	3.30.0-13
Management IP	9.55.240.28
Power 1	ON
Power 2	ON

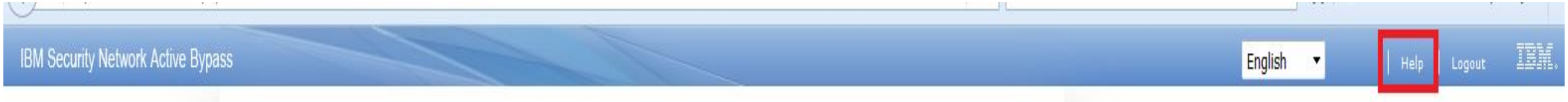
Segment 1 ●

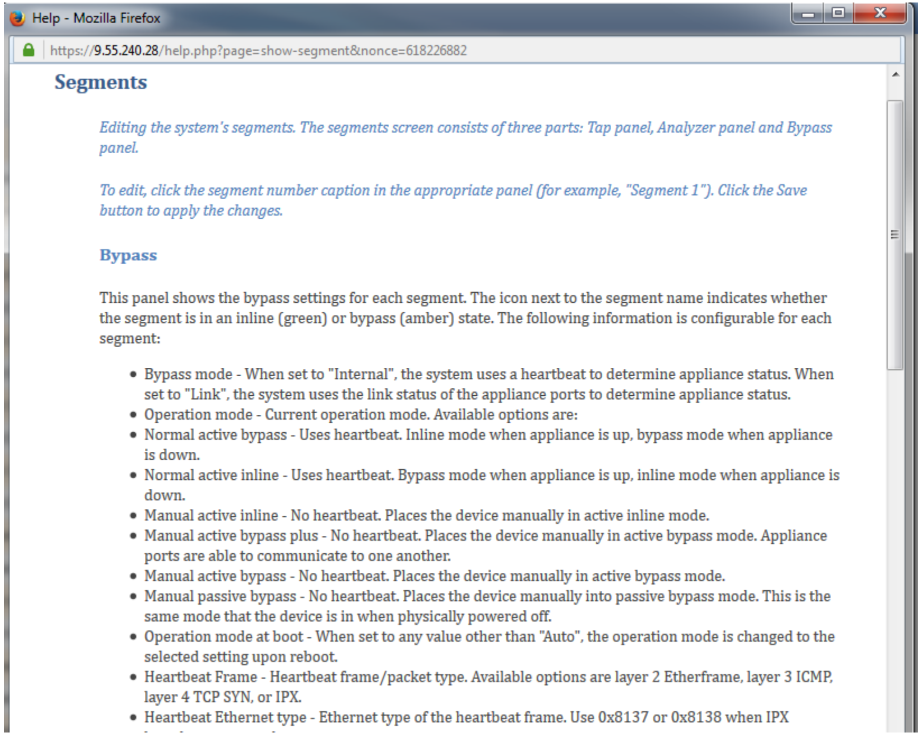
Port	Status	SFP Type
N1		
N2		
A1		
A2		

Segment 2 ●

Green - not in bypass mode (traffic is routed to the IPS)
Amber – bypass mode (traffic is bypassing the IPS)

Initial Setup - Help




Help - Mozilla Firefox
https://9.55.240.28/help.php?page=show-segment&nonce=618226882

Segments

Editing the system's segments. The segments screen consists of three parts: Tap panel, Analyzer panel and Bypass panel.

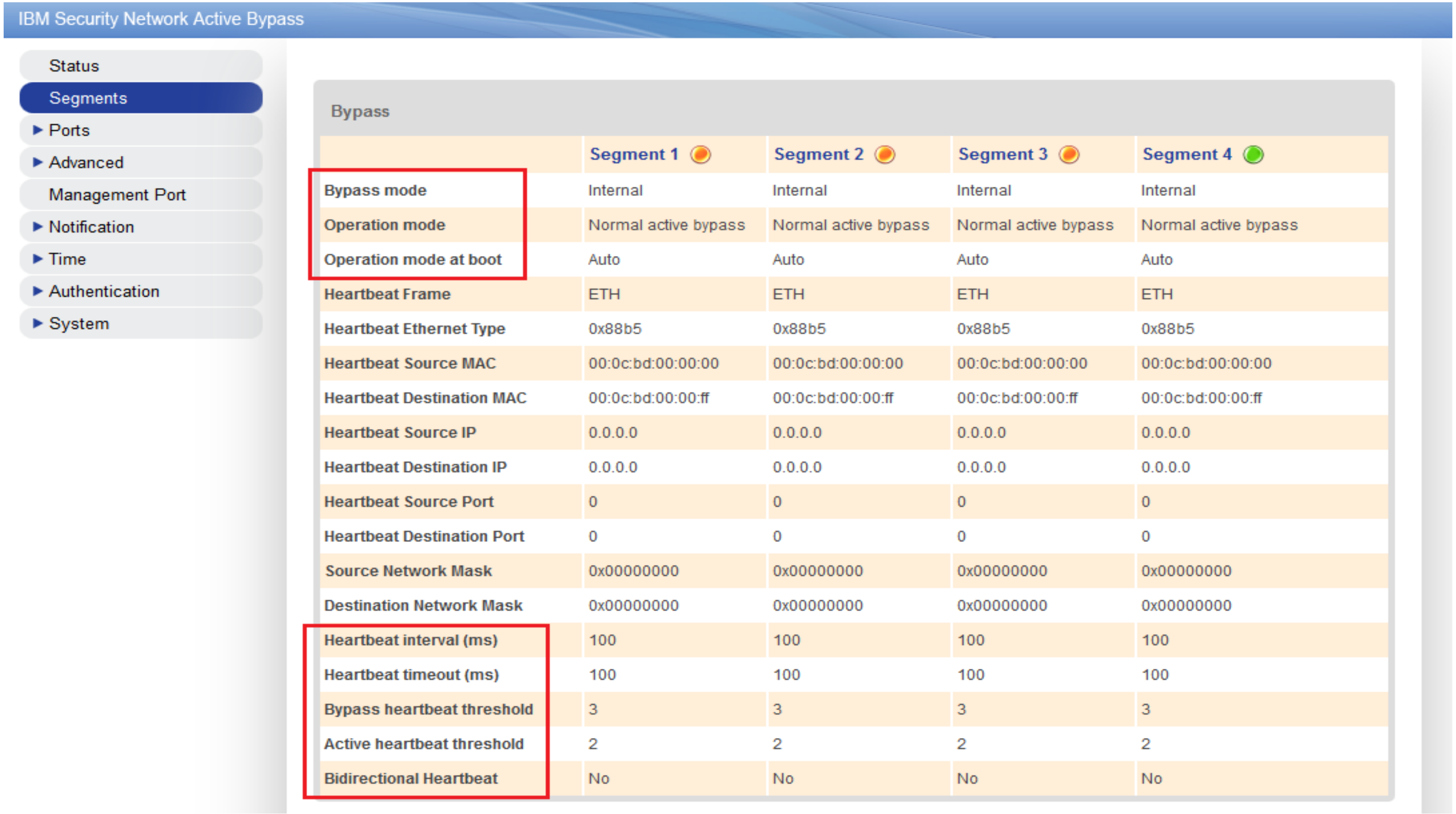
To edit, click the segment number caption in the appropriate panel (for example, "Segment 1"). Click the Save button to apply the changes.

Bypass

This panel shows the bypass settings for each segment. The icon next to the segment name indicates whether the segment is in an inline (green) or bypass (amber) state. The following information is configurable for each segment:

- Bypass mode - When set to "Internal", the system uses a heartbeat to determine appliance status. When set to "Link", the system uses the link status of the appliance ports to determine appliance status.
- Operation mode - Current operation mode. Available options are:
- Normal active bypass - Uses heartbeat. Inline mode when appliance is up, bypass mode when appliance is down.
- Normal active inline - Uses heartbeat. Bypass mode when appliance is up, inline mode when appliance is down.
- Manual active inline - No heartbeat. Places the device manually in active inline mode.
- Manual active bypass plus - No heartbeat. Places the device manually in active bypass mode. Appliance ports are able to communicate to one another.
- Manual active bypass - No heartbeat. Places the device manually in active bypass mode.
- Manual passive bypass - No heartbeat. Places the device manually into passive bypass mode. This is the same mode that the device is in when physically powered off.
- Operation mode at boot - When set to any value other than "Auto", the operation mode is changed to the selected setting upon reboot.
- Heartbeat Frame - Heartbeat frame/packet type. Available options are layer 2 Etherframe, layer 3 ICMP, layer 4 TCP SYN, or IPX.
- Heartbeat Ethernet type - Ethernet type of the heartbeat frame. Use 0x8137 or 0x8138 when IPX

Initial Setup - Segments



IBM Security Network Active Bypass

Bypass

	Segment 1 ●	Segment 2 ●	Segment 3 ●	Segment 4 ●
Bypass mode	Internal	Internal	Internal	Internal
Operation mode	Normal active bypass	Normal active bypass	Normal active bypass	Normal active bypass
Operation mode at boot	Auto	Auto	Auto	Auto
Heartbeat Frame	ETH	ETH	ETH	ETH
Heartbeat Ethernet Type	0x88b5	0x88b5	0x88b5	0x88b5
Heartbeat Source MAC	00:0c:bd:00:00:00	00:0c:bd:00:00:00	00:0c:bd:00:00:00	00:0c:bd:00:00:00
Heartbeat Destination MAC	00:0c:bd:00:00:ff	00:0c:bd:00:00:ff	00:0c:bd:00:00:ff	00:0c:bd:00:00:ff
Heartbeat Source IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Heartbeat Destination IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Heartbeat Source Port	0	0	0	0
Heartbeat Destination Port	0	0	0	0
Source Network Mask	0x00000000	0x00000000	0x00000000	0x00000000
Destination Network Mask	0x00000000	0x00000000	0x00000000	0x00000000
Heartbeat interval (ms)	100	100	100	100
Heartbeat timeout (ms)	100	100	100	100
Bypass heartbeat threshold	3	3	3	3
Active heartbeat threshold	2	2	2	2
Bidirectional Heartbeat	No	No	No	No

Initial Setup - Segments Menu

- Bypass mode

  Internal (Default) - heartbeat packets sent through the appliance

  Link – bypass only engaged if link down is detected

- Operational mode

  Normal Active Bypass (Default) – traffic sent to IPS if heartbeat flows through IPS

  Manual Active Bypass – actively bypasses the IPS (no heartbeat sent)

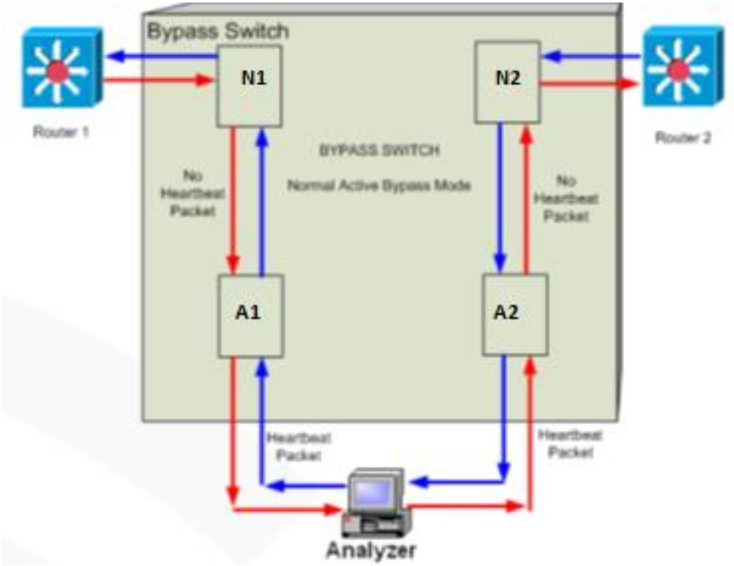
  Manual Passive Bypass – bypasses IPS (acts like NAB is powered off)

  * causes link state change on the network side*

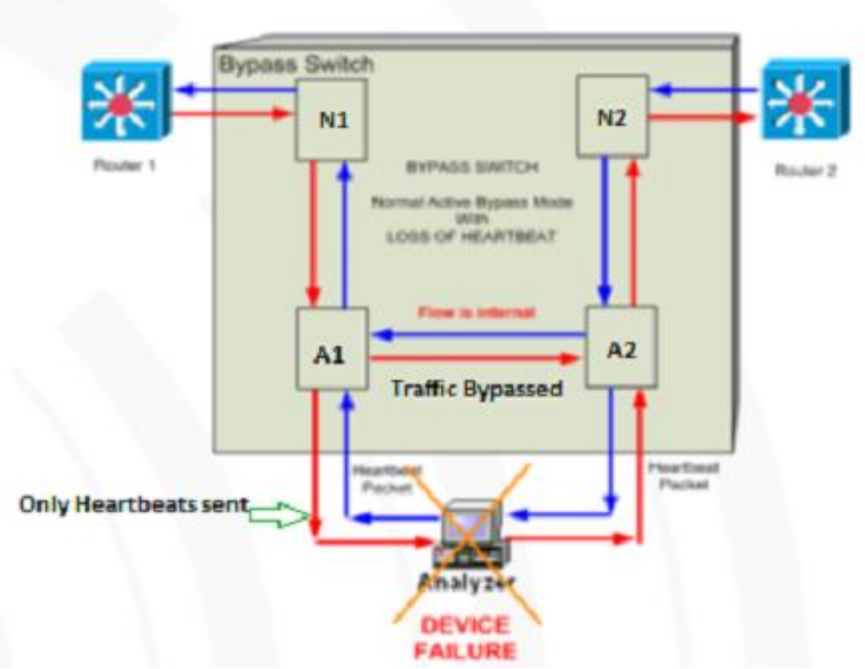
Normal Active Bypass

Traffic will flow between the network and appliance ports as shown in the following diagram.

If heartbeat signals are not received within the timeout period, traffic will bypass the IPS and go directly from A1 to A2 however the Heartbeat packets will continue to be sent out the Appliance port. This allows the module to automatically route traffic back through the appliance once it is repaired, or placed back into service.

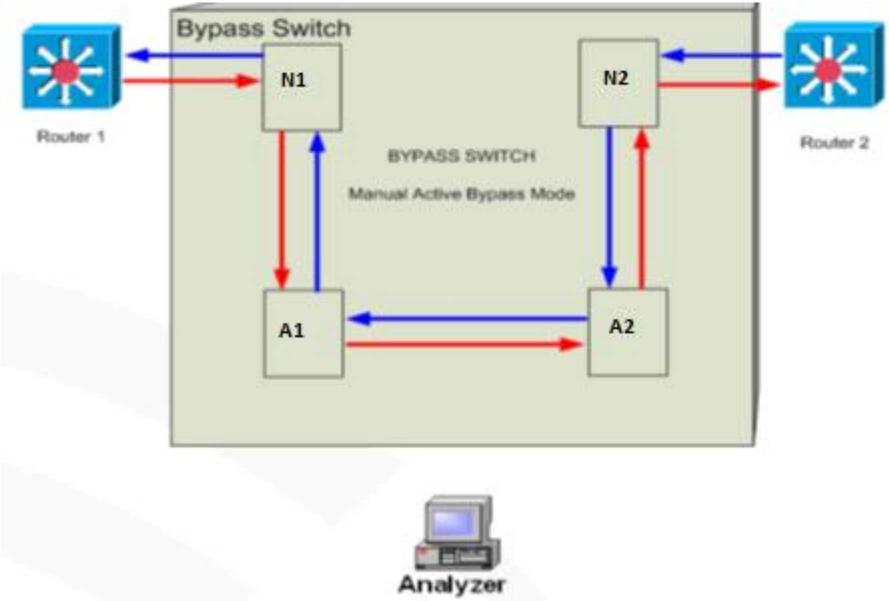


Normal Active Bypass



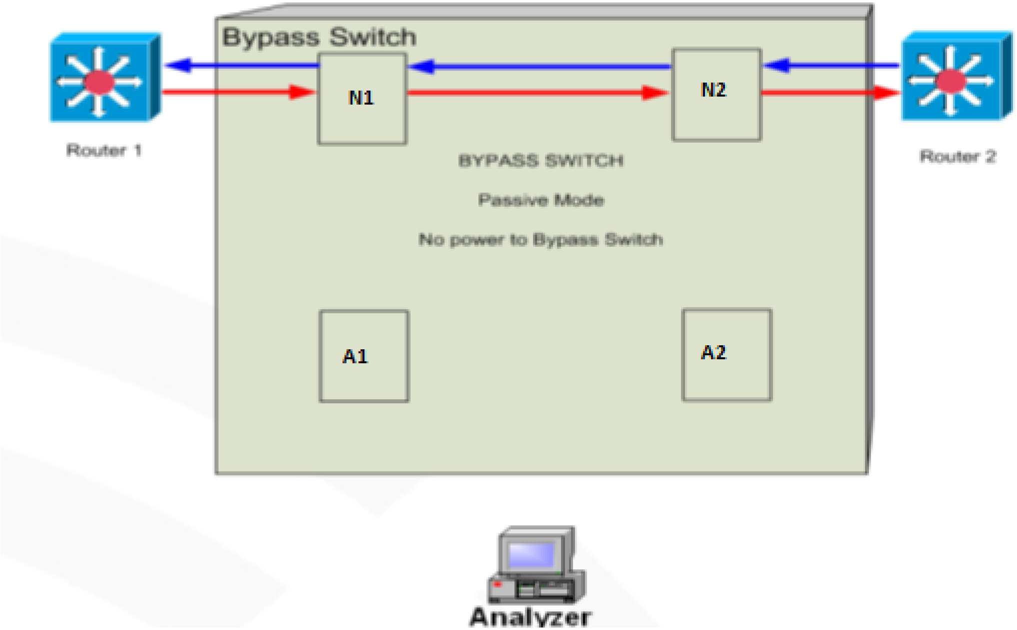
Manual Active Bypass

Traffic flows between N1 and N2 via A1 and A2. No heartbeat packets are sent, and the device will remain in this mode until changed.



Manual Passive Bypass

This mode forces connectivity directly between N1 and N2. If the Bypass Switch loses power from both of its redundant power supplies, this mode will automatically occur, to maintain the network link. Note that switching to this mode will cause a brief interruption of the network link, which may force routing and link protocol algorithms (STP) to recalculate and renegotiate.
This may cause link downtime.



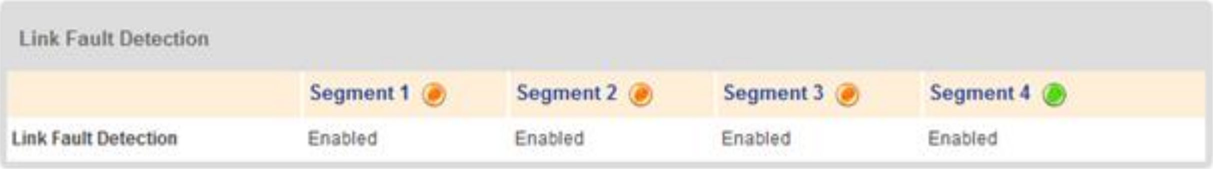
Initial Setup - Segments (continued)

- Heartbeat Interval – sent every 100ms
- Heartbeat timeout – 100ms, after that time its considered lost
- Bypass Heartbeat threshold – 3 (Once 3 heartbeats are missed , NAB switches to bypass)
- Active Heartbeat threshold – 2 (Once 2 heartbeats are received, NAB switches out of bypass)
- Bidirectional Heartbeat- No (NAB will only send heartbeats in one direction)

Most of the time the default values work effectively. However, customers might need to tweak some of these settings based on network conditions to achieve optimal performance.

Note: There is a software bypass procedure on the GX where it will go into software bypass if a packet is held up longer then 300 ms, so you might want to tweak the Bypass threshold to 4 to account for this so the NAB does not go in and out of bypass if there is some latency.

Initial Setup – Segments – Link Fault Detection

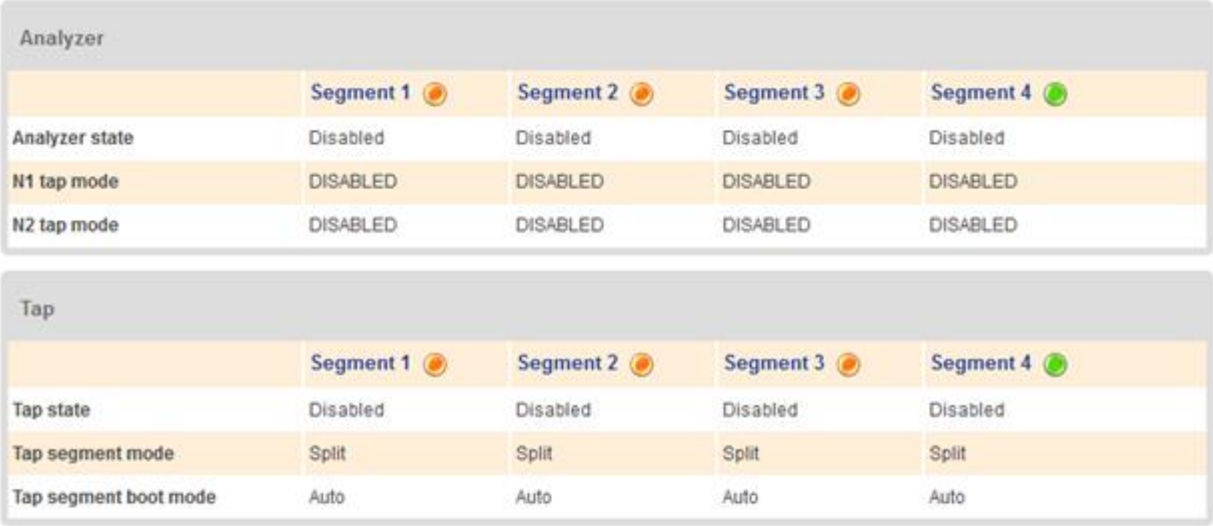


Link Fault Detection

	Segment 1 ●	Segment 2 ●	Segment 3 ●	Segment 4 ●
Link Fault Detection	Enabled	Enabled	Enabled	Enabled

- Link Fault Detection - Propagates link status between the network ports.

Initial Setup – Segments – Analyzer and Tap



Analyzer

	Segment 1 🟠	Segment 2 🟠	Segment 3 🟠	Segment 4 🟢
Analyzer state	Disabled	Disabled	Disabled	Disabled
N1 tap mode	DISABLED	DISABLED	DISABLED	DISABLED
N2 tap mode	DISABLED	DISABLED	DISABLED	DISABLED

Tap

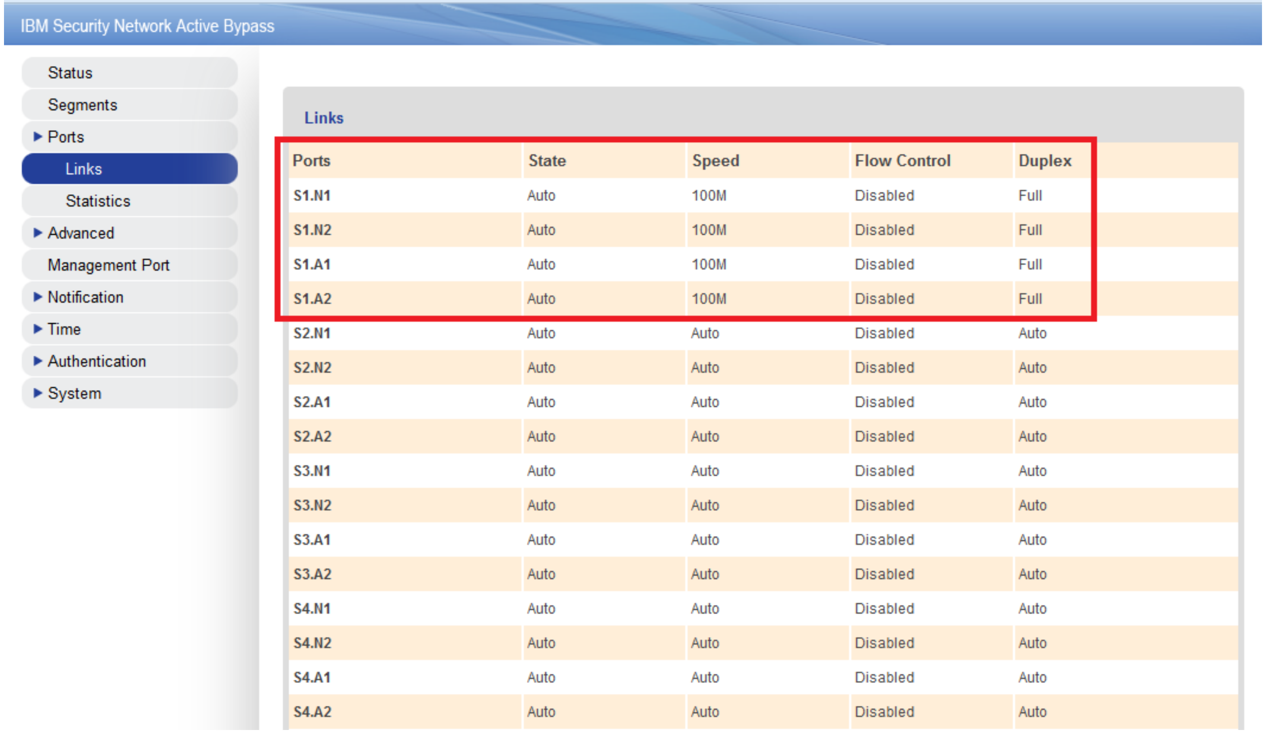
	Segment 1 🟠	Segment 2 🟠	Segment 3 🟠	Segment 4 🟢
Tap state	Disabled	Disabled	Disabled	Disabled
Tap segment mode	Split	Split	Split	Split
Tap segment boot mode	Auto	Auto	Auto	Auto

- Analyzer menu - never used (due to our custom code); always leave **Disabled**
- Tap menu – if you want to mirror the traffic to the tap port/ports (rarely used)

  Note: 1GB has 1 Tap port

  10 GB has 7 tap ports

Initial Setup

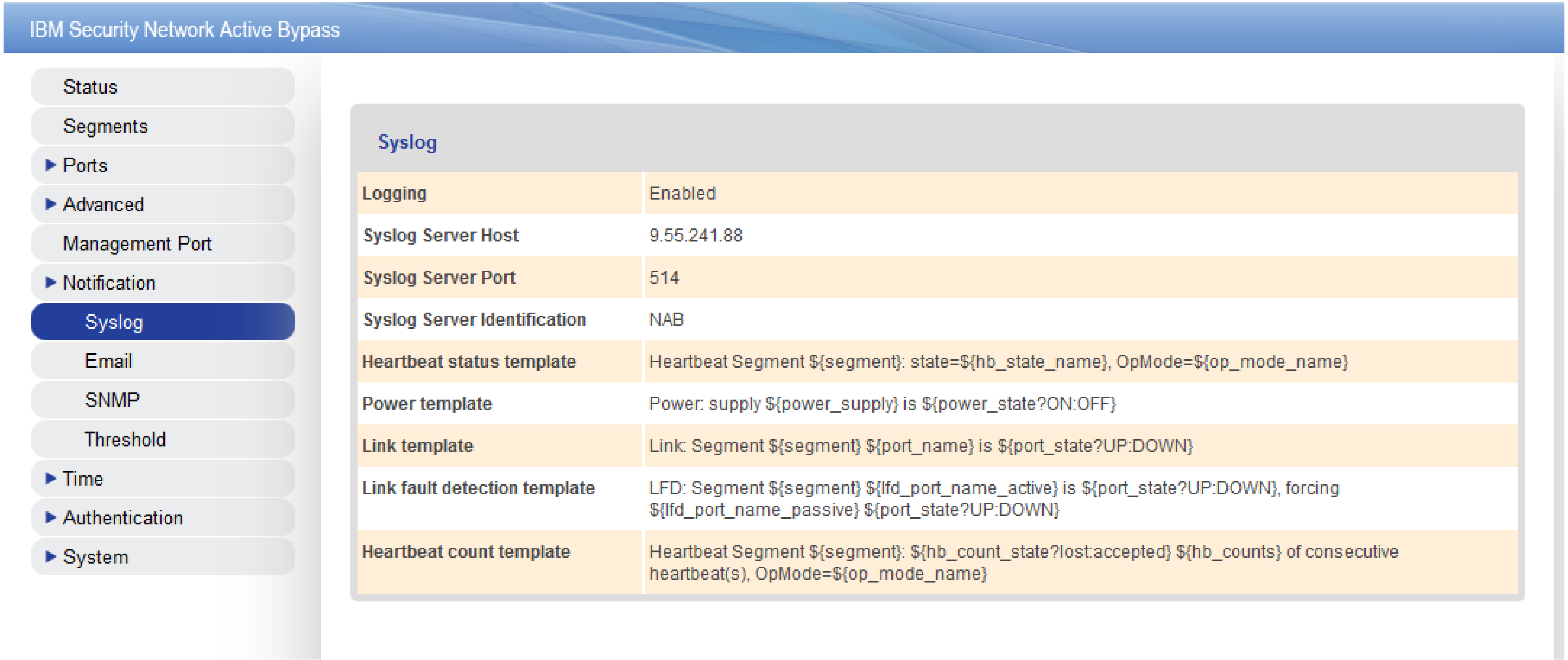


Links

Ports	State	Speed	Flow Control	Duplex
S1.N1	Auto	100M	Disabled	Full
S1.N2	Auto	100M	Disabled	Full
S1.A1	Auto	100M	Disabled	Full
S1.A2	Auto	100M	Disabled	Full
S2.N1	Auto	Auto	Disabled	Auto
S2.N2	Auto	Auto	Disabled	Auto
S2.A1	Auto	Auto	Disabled	Auto
S2.A2	Auto	Auto	Disabled	Auto
S3.N1	Auto	Auto	Disabled	Auto
S3.N2	Auto	Auto	Disabled	Auto
S3.A1	Auto	Auto	Disabled	Auto
S3.A2	Auto	Auto	Disabled	Auto
S4.N1	Auto	Auto	Disabled	Auto
S4.N2	Auto	Auto	Disabled	Auto
S4.A1	Auto	Auto	Disabled	Auto
S4.A2	Auto	Auto	Disabled	Auto

Always hard code the **Speed/Duplex** for Copper NICs as well as all connected equipment. Disable **Flow Control** as there is currently a known issue with this causing latency.

Initial Setup - Notifications



Syslog

Logging	Enabled
Syslog Server Host	9.55.241.88
Syslog Server Port	514
Syslog Server Identification	NAB
Heartbeat status template	Heartbeat Segment ${segment}: state=${hb_state_name}, OpMode=${op_mode_name}
Power template	Power: supply ${power_supply} is ${power_state?ON:OFF}
Link template	Link: Segment ${segment} ${port_name} is ${port_state?UP:DOWN}
Link fault detection template	LFD: Segment ${segment} ${lfd_port_name_active} is ${port_state?UP:DOWN}, forcing ${lfd_port_name_passive} ${port_state?UP:DOWN}
Heartbeat count template	Heartbeat Segment ${segment}: ${hb_count_state?lost:accepted} ${hb_counts} of consecutive heartbeat(s), OpMode=${op_mode_name}

Initial Setup - Notifications

Events that will trigger a notification via **E-mail, Syslog, and SNMP**
1. Active/Bypass state
2. Power status

Events that will trigger a notification via **Syslog** and **SNMP** only.
1. Link Fault Detection notification
2. Operation Mode

Events will be triggered via **SNMP** and **E-mail**.
1. Warm boot trap
2. Cold boot trap

Events will be triggered specifically for **Syslog**.
1. Heartbeat counts
2. SSH
3. TACACS+
4. Web UI login → only logs failures; defect is open with IM
5. Console login → logs failed and successful logins but only on the newest FW

Note: Each Notification sends messages for different items therefore enable all of the types.

Upgrade

Two ways you can upgrade:

1) **Remote upgrade:** Download latest .pkg and use LMI to upgrade.
   If on 1.x → go to 2.18 → 3.x
   If on 2.x → 3.x
   If on 3.x (below 3.18) → 3.18 → latest 3.x

For the 1 GB NAB once update completes you must pull the power cords on the NAB.

Note: 3.x FW are on FixCentral, 2.18 must be obtained from Support

Keep in mind: If there are any issues that cause the NAB to fail to boot, you will have to get someone local to the appliance or have a remote serial connection.

Local Upgrade

2) Local Upgrade:

1) Use the latest FW .pkg (currently 3.30) and upgrade from the LMI
2) Go to System → Settings→ restore to factory default
3) Using the serial port, log in locally and set the ip address
4) Power Cycle the appliance by unplugging the power cords
5) Complete the configuration process

Note: There is a re-image process. However, it’s not published, so contact Support.

Proactive steps

Proactive Steps

1) Setup syslog/snmp/email notifications

   The NAB does not have a hard drive so it does not keep any logs. Without notifications there is no history saved on the NAB.

2) Disable Flow control on all Ports

   http://www.ibm.com/support/docview.wss?uid=swg21967430

3) Install the get-NAB-logs script for future troubleshooting

   http://www.ibm.com/support/docview.wss?uid=swg21678374

   Note: Copy the script to the /flash dir so it does not get deleted when you reboot.

IBM Security

Intelligence. Integration. Expertise.

Troubleshooting

Troubleshooting

Perform the following steps before you reboot or route around the NAB

1) Run top and ps commands and send screen output

2) Run ./get-NAB-logs script and send output file

3) Send in remote syslog file, snmp traps, or emails from NAB

4) Send in output file from the telnet command to NAB on port 10000 **(if requested by Level 3)*

    Example: telnet ip_address_NAB 1000

    Note: If using Putty:

        A) Go to logging, enable all session output
        B) Go to Terminal, enable ‘Implicit CR in every LF’
        C) Save to file

Where can I get more information?

- **Cabling the NAB to Network IPS sensors at 100Mb/s**
  http://www.ibm.com/support/docview.wss?uid=swg21567902

- **Upgrading Network Active Bypass from 1.x to 3.x firmware version**
  http://www.ibm.com/support/docview.wss?uid=swg21694811

- **Lost password recovery procedure on the Network Active Bypass**
  http://www.ibm.com/support/docview.wss?uid=swg21437286

- **IBM Knowledge Center:**
  http://www.ibm.com/support/knowledgecenter/SSB2MG_4.6.2/com.ibm.ips.doc/concepts/nab_pdf_library.htm

- **Useful links:** **Get started with IBM Security Support**
  IBM Support Portal | Sign up for "My Notifications"

Follow us: You Tube t f

Questions for the panel?

Now is your opportunity to ask questions of our panelists.

To ask a question now:

Press *1 to ask a question over the phone

or

Type your question into the SmartCloud Meetings chat

To ask a question after this presentation:

You are encouraged to participate in this
dWAnswers forum topic: OpenMic WebCast Announcement for 27 April 2016: How to properly deploy, configure, and upgrade the Network Active Bypass unit

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM Security

Intelligence. Integration. Expertise.