Network Critical

The Window to your Network™

# Smart Network Access System

## User Guide

Revision 5.0.178

# Contents

# Preface

Welcome to Network Critical's *Smart Network Access System*. The *SmartNA™ System* provides a complete solution for tapping and monitoring your business-critical data traffic, allowing you to safely and securely integrate intrusion detection, analyzers, probes, sniffers, compliance, intrusion prevention, VoIP monitoring, data leakage prevention, content filtering and lawful interception tools into your 1G network infrastructure.

## About this manual

This manual provides a complete reference to the SmartNA System for Network Administrators, Network Security Administrators, and other suitably experienced professionals who need a safe, reliable and non-intrusive way of accessing an Ethernet data network for the purpose of monitoring traffic.

If network tapping is new territory to you, then you may wish to start by reading *About Network Tapping* on page 14, which provides an overview of network tapping and introduces the various TAP modes which you can configure on the SmartNA System to gain access to the traffic on your network.

## Supported firmware

In general, this manual applies to SmartNA Controllers running version 5.0 firmware, and SmartNA TAP Modules running version 4.2 firmware. The web interface, SNMP and 1U backplane filtering are not supported on controllers running firmware earlier than version 4.

If you have earlier firmware, you may like to contact Network Critical to discuss moving forwards with the least disruption to your network.

**Note:** Do not mix TAP firmware versions in a chassis without checking with Network Critical first. See *Contacting Technical Support* on page 53 for contact details.

# Chapter overview

*Chapter 1, The SmartNA System* on page 3 provides a general overview of the SmartNA System, including the various chassis, TAP and Controller modules that comprise the system and provide its inherent flexibility.

*Chapter 2, Getting Started* on page 8 provides information on getting started with the SmartNA System, including information on installing the hardware and connecting to the SmartNA web and command line interfaces.

*Chapter 3, About Network Tapping* on page 14 provides information on placing TAPs and the various TAP modes supported by the SmartNA System.

*Chapter 4, Mapping Ports: Setting up TAP Modes* on page 17 provides details on port mapping and configuring TAP modes.

*Chapter 5, Configuring Ports* on page 25 provides details on how to configure port speed and duplex mode, enable port locks, and view port statistics, including those for byte and packets counters, percentage load, and packet errors.

*Chapter 6, Backplane Filtering* on page 29 provides information relevant to the 1U chassis with Backplane filtering.

*Chapter 7, Using SNMP* on page 33 provides information on using SNMP to alert remote users about conditions that warrant administrative attention.

*Chapter 8, SmartNA Administration* on page 38 provides information on general SmartNA administrative task, such as configuring user, setting the IP address, and updating firmware.

*Appendix A, CLI Commands* on page 43 lists the commands that are available via the SmartNA CLI.

*Appendix B, V-Line DIP Switches* on page 48 describes the DIP switches used to set operating modes on V-Line modules.

*Appendix C, Specifications and Safety* on page 49 provides technical specifications for the SmartNA System.

*Appendix D, Module Features Matrix* on page 51 provides a module features a handy features table for each module that is available for the SmartNA System.

*Appendix E, Hardware Warranty* on page 52 provides details of the SmartNA hardware warranty.

*Appendix F, Contacting Technical Support* on page 53 provides addresses and telephone numbers for contacting Network Critical Technical Support.

# Conventions used in this manual

***Caution:*** *A "Caution" advises the reader about situations that may result in incorrect, poor or no operation of the product, that may cause personal injury or may cause damage to the product or other property.*

**Note:** A "Note" contains essential user information.

**Tip:** A "Tip" contains useful or other interesting information.

# 1 The SmartNA System

The SmartNA System provides a flexible, modular approach to network access. The system is available in a choice of three chassis models — *Portable*, *Aggregating/Filtering 1U* and *High Density 2U*— and over 45 different configurations of TAP modules. Each module can be configured independently of other modules, and each module port can be made to receive *or* send data, providing almost unlimited port mapping flexibility.

## SmartNA chassis types

This section describes the three types of chassis that are available for the SmartNA System:

- Portable chassis
- Aggregating/Filtering 1U chassis
- High Density 2U chassis

### Portable Chassis

The SmartNA Portable Chassis provides power to a single SmartNA module. Administrator access to the unit is via Telnet only via the built-in management port.

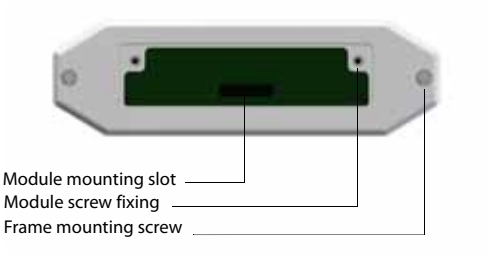



**Figure 1:** Portable Chassis front view

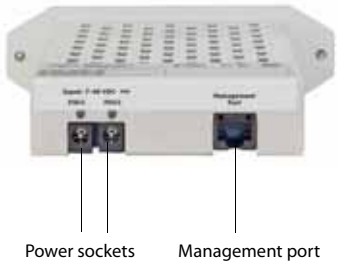



**Figure 2:** Portable Chassis rear view

**Note:** The built-in management port on the portable chassis operates at 10Mbps only, and has an MDI-X pinout.

**Note:** When using the portable chassis with a VLine module the management port is non-operational. Configuration of the module *must* be done with DIP switches.

## Aggregating/Filtering 1U Chassis

The SmartNA 1U Chassis can power up to four modules and has one expansion/Controller module slot. It contains a 20 Gigabit aggregating Backplane, with packet filtering capabilities when used with suitable modules. For safety, the unit has two independent power supplies which may be any combination of AC or DC power. Management access to the system is through a web or command line interface.

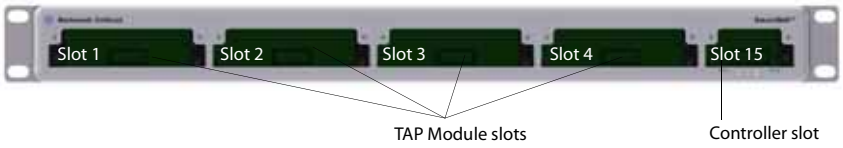



**Figure 3:** 1U chassis front view

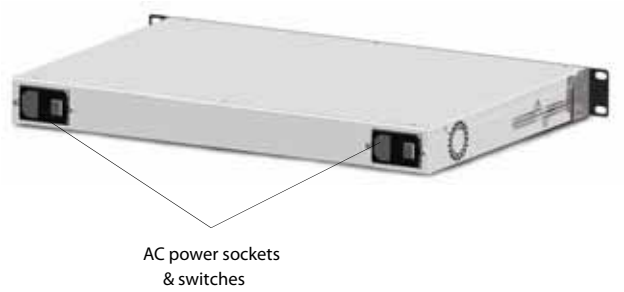



**Figure 4:** 1U AC chassis rear view

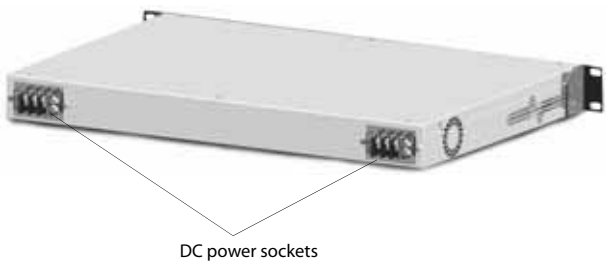



**Figure 5:** 1U DC chassis rear view

## High Density 2U Chassis

The SmartNA High Density 2U Chassis can power up to 12 modules and has three expansion slots. For reliability, the unit has two power sockets, which should be connected to independent power supplies. Management access to the system is through a web or command line interface via a controller module.

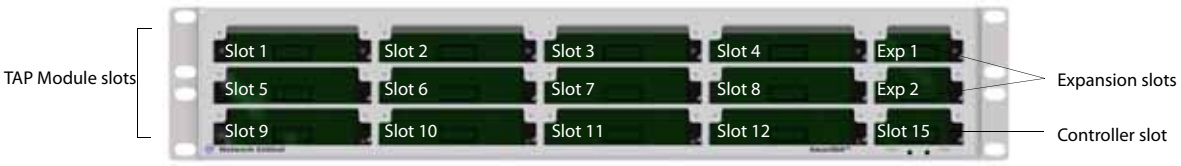



**Figure 6:** 2U chassis front panel

# SmartNA TAP Modules

At the heart of the SmartNA System are the TAP modules; configurable, interchangeable, and hot-swappable cards that are available in four types:

- Breakout/Aggregation/Regeneration Module - a highly flexible individual network access module.
- Backplane Aggregation Module - allows traffic to be aggregated across the 1U chassis backplane.
- Filtering Module - allows traffic to be filtered through the 1U chassis backplane.
- VLine - allows *Virtually Inline* deployment of inline monitoring tools.

Each of these module types is available with a variety of port combinations, including:

- Copper-copper
- Copper-SFP
- Fiber-copper
- Fiber-SFP

In the event of a module or chassis power failure, copper (1000BASE-T) modules have failsafe and autolock mechanisms which automatically maintain the live link throughout (a few milliseconds loss of link may result in failsafe mode).

## Copper–Copper TAP Module

**Features**
TAP link: A&B, C&D
SPAN link: A&B, C&D
Linklock for fiber or 10/100: A&B, C&D
Bi-directional: A&B, C&D
Copper 10/100/1000: A&B, C&D

## Copper–SFP TAP Module

**Features**
TAP link: A&B
SPAN link: A&B, C&D
Linklock for fiber or 10/100: A&B
Bi-directional: A&B, C&D
Copper: 10/100/1000: A&B, C&D (1000 only)
Single mode Gigabit fiber (LC): C&D
Multi-mode Gigabit fiber (LC): C&D

### Fiber–Copper TAP Module

**Features**
TAP link: A&B, C&D
SPAN link: C&D
Linklock for fiber or 10/100: A&B, C&D
Bi-directional: C&D
Copper: 10/100/1000: C&D
Multi-mode Gigabit fiber (LC): A&B

### Fiber–SFP TAP Module

**Features**
TAP link: A&B, C&D
SPAN link: C&D
Linklock for fiber or 10/100: A&B
Bi-directional: C&D
Copper: 10/100/1000: C&D (1000 only)
Single mode Gigabit fiber (LC): C&D
Multi-mode Gigabit fiber (LC): A&B, C&D

## SmartNA System Controller Modules

The SmartNA Backplane Control and Security modules provide administrative access to the SmartNA System. The Control modules are available for both SFP and RJ-45 (copper) connections.

### Secure Copper (RJ-45) Controller

**Features**
1 RJ-45 management port
1 RJ-45 10/100/1000 copper monitoring port
SSH Command-Line Interface
HTTPS Web-Based Interface
SNMP

# Securing your SmartNA System

An unsecured SmartNA System provides an obvious security threat from attackers wanting to gain access to the data on your network. The table below summarizes the measures you can take to protect your SmartNA System against attack and unauthorized use.

| Security measure | Comments |
|---|---|
| Place the SmartNA unit in a secure location | Install the SmartNA chassis in secure server room, preferably housed in a locked cabinet.<br>See *Rack-mounting the chassis* on page 9. |
| Change the default admin login details | The default admin details (by default, **admin** with the password **admin**) should be changed at the earliest opportunity.<br>See *Configuring usernames and passwords* on page 38. |
| Change the SNMP community strings | If SNMP is enabled, you are strongly advised to change the default community strings to prevent access and control of the SmartNA System.<br>See *Configuring SNMP users* on page 34. |
| Disable copper (1000BASE-T) ports | Disable by locking any unused copper ports to prevent them being used by unauthorized persons.<br>See *Locking ports* on page 26. |
| Auto-lock copper ports | Enable auto-locking to disable copper ports when the link is lost.<br>See *Auto-locking ports* on page 26. |
| Enable the SNMP authentication trap | The SNMP authentication trap is triggered whenever access to the system is denied.<br>See *Configuring SNMP system-wide options* on page 33. |

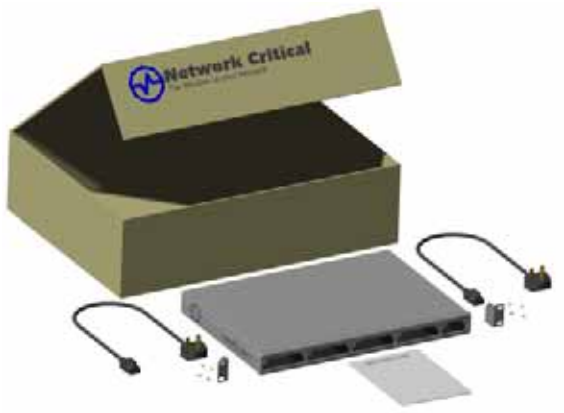
# 2

# Getting Started

This chapter provides details on getting started with the SmartNA System. Before starting, you should check that all the components are present and in good condition. Any issues should be reported immediately to Network Critical. Our contact details can be found in *Appendix F, Contacting Technical Support* on page 53.

## List of components supplied

The components supplied with each SmartNA System are listed below. If any component is found to be missing, damaged, not working, or otherwise faulty, please report it immediately to Network Critical Technical Support. See *Contacting Technical Support* on page 53.




- 1 x SmartNA chassis (type 1U, 2U, or Portable)
- 1 x Rack mounting kit (brackets and screws)
- 2 x Power leads
- TAP Modules (as per your order)

# Installing the hardware

## Rack-mounting the chassis

This section describes how to mount the SmartNA chassis in a server rack. Due to the obvious security risk of having an unsecured SmartNA device on your network, we recommend installing the SmartNA device in a secure server room in a locked server cabinet.

**To rack mount the SmartNA chassis:**

1. Unpack the SmartNA chassis and place it on a suitable work surface.
2. Attach the two mounting brackets supplied to the side of the chassis.

**Figure 7:** Attaching the rack mount bracket

3. Slide the chassis into your server rack and secure it with screws (not supplied).
4. Attach the power leads to *separate power sources*. The unit is able to work with a single power lead, but two leads connected will help safeguard the device against power failure.

> **Tip:** A fixing kit is also available for the Portable SmartNA unit.

## Installing the TAP and Controller modules

TAP and Controller modules are supplied individually packaged, ready for insertion into the SmartNA chassis. The Controller module must be inserted into the Controller slot (see *Figure 8* for the location of the Controller slot on the 1U and 2U chassis), but the TAP modules can be inserted into any free TAP slot.

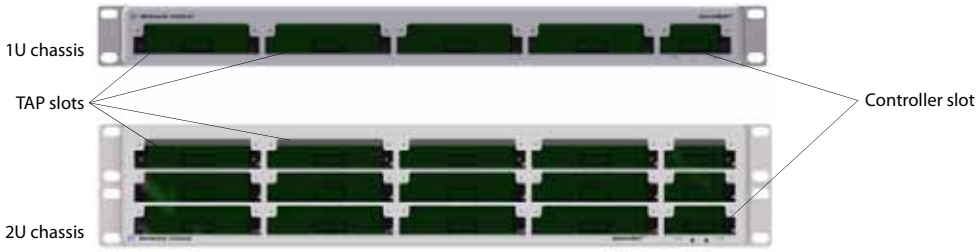



**Figure 8:** Location of the TAP and Controller slot

**To insert modules in the chassis:**

1. To dissipate static electricity, touch a grounded appliance, such as the SmartNA chassis.
2. Being careful not to touch the electronic components, remove the modules from their anti-static bags.
3. Slide the modules into the slots and secure with the locking screws. The locking screws also earth the module, so it is important to do this.
4. Once all the modules are all in place, you can switch on the device by pressing the two power switches located on the rear panel.

**Note:** Modules are hot-swappable. They can be inserted and removed without powering off or disrupting data flow to other modules.

# Attaching power cables

SmartNA System 1U and 2U chassis are equipped with dual power units. Although the chassis will work connected to a single power source, for increased reliability you should attach two cables which are connected to *independent* power sources. If connecting to a DC power supply, you must follow the instructions below to ensure your safety as you wire the unit into an appropriate circuit.

***Caution:*** *Before performing this procedure, ensure that all power is off to the DC circuit of the power supply being added or removed. Locate the circuit breaker on the panel board that services the DC circuit and switch it to the* ***off*** *position. Tape the circuit breaker switch handle in the off position to prevent accidental closing of the circuit.*

**To wire a DC power supply:**

1. Verify that power is **off** to the DC input circuit.
2. Attach the appropriate ring fixings to the DC input wires.

3 From the bottom of the terminal block wire the DC input power supply to the terminal block as follows:

Ground wire to Ground terminal (left)

-48V return to "**+**" terminal (center)

-48V wire to "**-**" terminal (right)

> **Note:** It is recommended that the DC input wires are routed to the bottom of the terminals to reduce undue strain on the cables.

4 Check that all connections are secure.

5 Remove the tape from the circuit breaker switch handle and restore power by moving the circuit breaker switch handle to the on position.

# Management port cable

To access the SmartNA System's user interface, you'll need to attach a network or serial cable to the Controller management port (port B on dual port controllers, see *Figure 9*). On SmartNA Portable units, the management port is located on the rear of the unit and is restricted to 10 Mbps only. Once connected, you can access the web interface and command line interface (CLI) to administer port mappings, filtering options, and other system settings.


**Figure 9:** Location of the Management port

# Accessing the SmartNA System

After connecting to the Management port (see *Management port cable* on page 11), you are ready to access the SmartNA System via the graphical web interface or command line interface using SSH.

## Accessing the web interface

Access to the SmartNA web interface (*Figure 10*) is available using any Java 1.5 (or later) enabled browser. The web interface provides easy access to most of the SmartNA System, including port mappings, Backplane filtering, SNMP configuration, as well as firmware upgrading and other administration tasks. For security, the web interface does not allow you to change the IP address or configure user accounts.

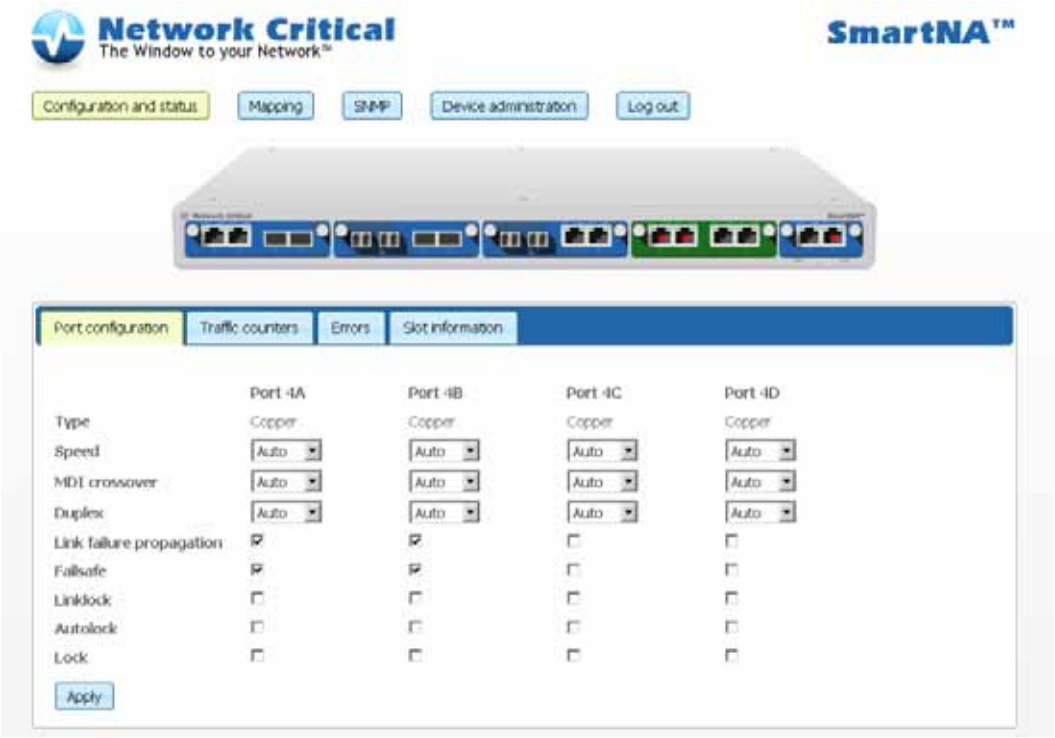



**Figure 10:** The SmartNA graphical web interface

**To access the SmartNA web interface:**

1. Open a web browser and enter the IP address of the SmartNA System. By default the IP address is set to **192.168.254.100**.
2. Login using the administrator account (default settings: username **admin**; password **admin**).
3. After logging in to the SmartNA System, you can:

   - Click on a module to configure ports, inspect statistics, and configure mapping within that module,

   - Click on the chassis to view system details, add filter rules, administer SNMP, and configure mapping between modules,

## Accessing the command line interface (CLI)

SmartNA's command line interface (CLI) provides access to the system from any Secure Shell application. The SmartNA System supports two user accounts:

- *Administrator* – provides full read-write access to the system. Administrators may issue SHOW and SET commands. Default username **admin**; default password **admin**.
- *User* – provides read-only access to the system. Users may only issue SHOW commands. Default username **user**; default password **user**.

See *Appendix A, CLI Commands* on page 43 for the list of available commands.

# About Network Tapping

3

The SmartNA System is a sophisticated device that, simply put, allows data travelling along a computer network to be accessed, or *tapped*. This chapter provides an overview of tapping and describes a few of the many TAP modes that can be employed to collect, aggregate, and distribute data to ports in the SmartNA System. For information on setting up TAP modes on the SmartNA System, see *Chapter 4, Mapping Ports: Setting up TAP Modes* on page 17.

## Placing a Network TAP

A network TAP is simply a device – in this case a SmartNA TAP module – that allows traffic flowing on a live network to be monitored. To achieve this, the network is broken and a TAP is placed across the two open ends, as shown in *Figure 11*. Because the TAP forwards data across the link, the link appears to be intact and functioning normally.

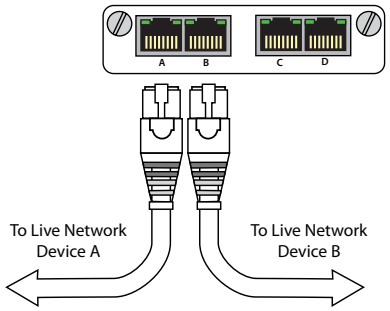



**Figure 11:** Tapping live network traffic

Once traffic has entered the SmartNA System it can be sent, or mapped, to monitoring ports within the SmartNA System. Tools can be attached to the monitoring ports and the traffic analyzed as required, as shown in *Figure 12*.

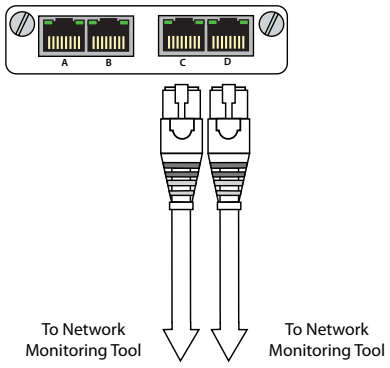



**Figure 12:** Connecting to a monitoring tool

Depending on the type of modules you have, network traffic can be distributed to ports in the system in a variety of configurations, or modes. The next section describes the various modes that are commonly used.

# Tapping modes

The tapping mode determines how network traffic is collated and distributed between ports and modules in the SmartNA System. Depending on the SmartNA System you have, some TAP modes may not be available to you; for example, Breakout TAP modules only support Breakout mode. Other modules allow complete flexibility as to how ports are mapped, and care must be taken to ensure that network traffic is correctly routed so no data is lost.

Several TAP modes, described below, are commonly used:

- Breakout
- Aggregating
- Regenerating
- V-Line/Inline/Bypass

## Breakout TAP

A Breakout TAP copies traffic travelling in one direction (point A to point B) to one monitoring port (port C), and traffic travelling in the other direction (B to A) to another monitoring port (port D).

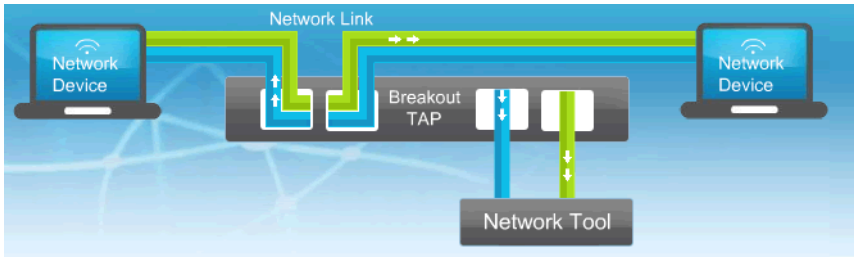



**Figure 13:** A Breakout TAP

Use Breakout TAPs when:

- 100% guaranteed traffic collection is required.
- The network analyzer has dual ports running at the same speed as the live network.

## Aggregating TAP

An Aggregating TAP allows you to take the network traffic from multiple network segments and aggregate the information to a single monitoring port. This enables you to use just one monitoring tool to see all of your network traffic.

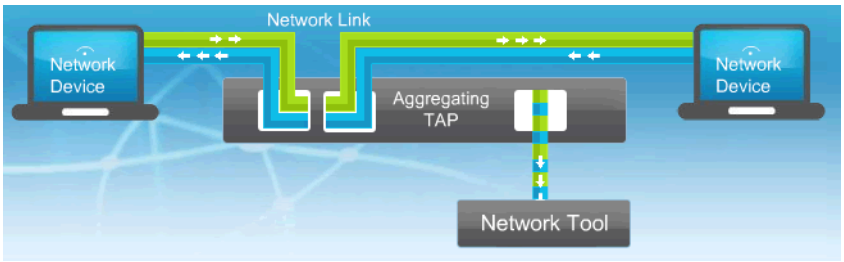



**Figure 14:** An Aggregating TAP

Use Aggregating TAPs when:

- 100% guaranteed traffic collection is *not* required. If the aggregated traffic rate exceeds the inbound network bandwidth of the network tool then excess packets will be dropped at the Monitor Port.
- The network tool has only a single interface.

## Regenerating TAP

A Regeneration TAP allows you to take traffic from one network segment and send it to multiple monitoring tools. This enables you to send a single traffic stream to a range of different monitoring tools, each serving a different purpose, whilst taking traffic from the network only once.

## V-Line (Inline or Bypass) TAP

V-Line TAPs (also known as Inline or Bypass TAPs) allow you to place a network tool "Virtually Inline". These TAPs are used where monitoring devices need to be placed in-line on the network to be effective, but when putting these devices inline will compromise the integrity of a critical network. By placing a V-Line TAP in its place and connecting the monitoring tool to the V-Line TAP, you can guarantee that the network will continue to flow and the device will not create a failure point in the network.

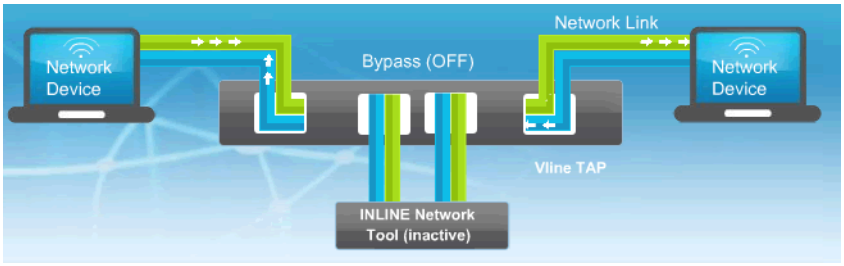



**Figure 15:** A Vline (Bypass) TAP

Use V-Line TAPs when:

- Complete failsafe protection for an inline tool is required. If the tool goes offline, the TAP automatically bypasses it and traffic is directed straight through to the network devices.

# 4

# Mapping Ports: Setting up TAP Modes

This chapter describes how to configure TAP modes by mapping ports. Port mapping is available on Fully Configurable, Aggregating, and V-Line modules. Breakout modules do not support port mapping. For information tapping a network and the various TAP modes that can be employed, see *Chapter 3, About Network Tapping* on page 14.

## About port mapping

Port mapping allows you to specify how live traffic entering the SmartNA System gets distributed to other ports in the system. The flexibility of the SmartNA System enables you to map any combination of ports, some of which may not be valid. Thus, when mapping ports, care must be taken to ensure that data is correctly routed so as not to overload ports or direct traffic away from the tapped devices, which will cause packets to be lost on the network.

**Note:** Customized port mapping is not available on V-Line Modules. Instead you will need to set the correct DIP switches (see sections below for details) or select one of the predefined operating modes through CLI.

# Port schematic

The port schematic below shows how ports are numbered and arranged in a typical SmartNA System. It may help to refer to this diagram when setting up port mappings.

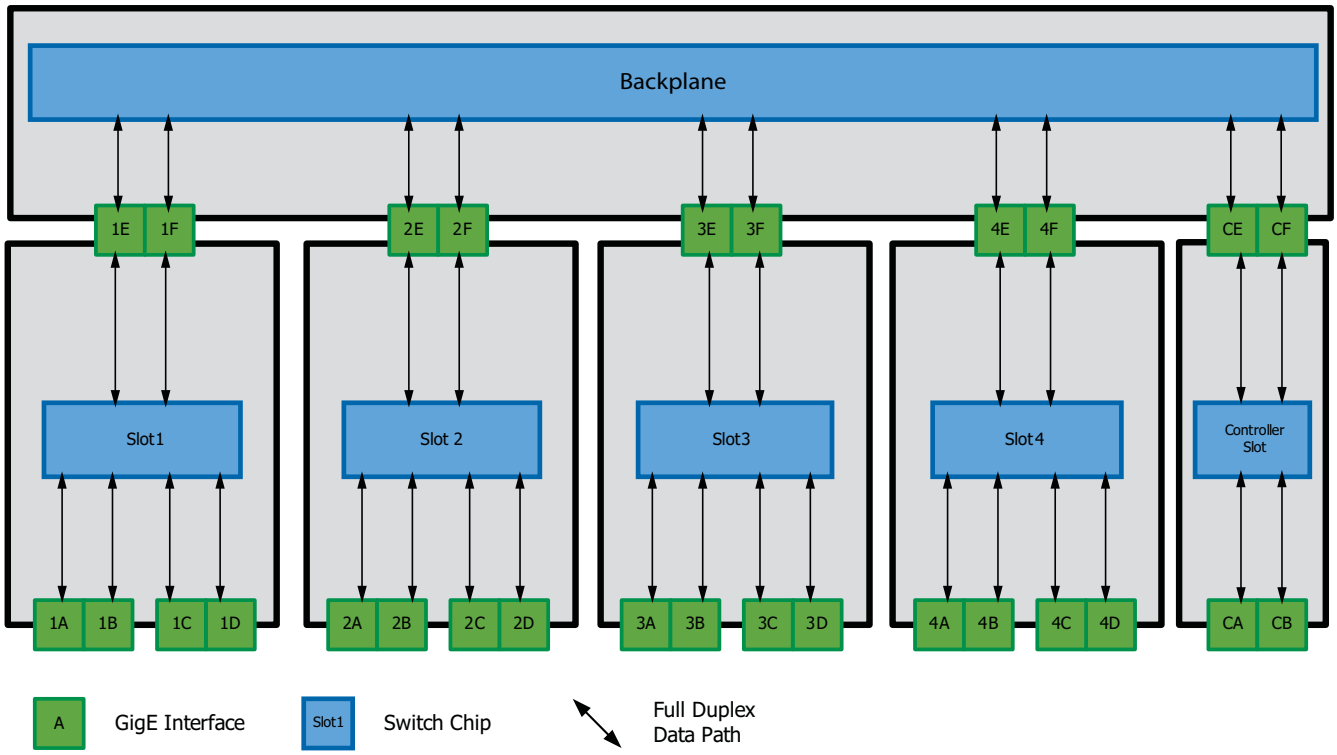



**Figure 16:** SmartNA System: Port Nomenclature & Connections

# Setting up a TAP pair

A TAP pair is a simple mapping configuration used to ensure live traffic continues to flow across a tapped network segment. It does this by copying traffic from A to B and B to A, as shown in *Figure 17*. A failsafe device in the port can also be enabled to ensure that traffic will still flow even when the module is not powered.

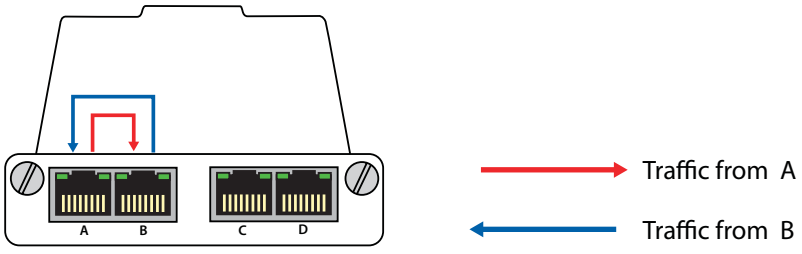


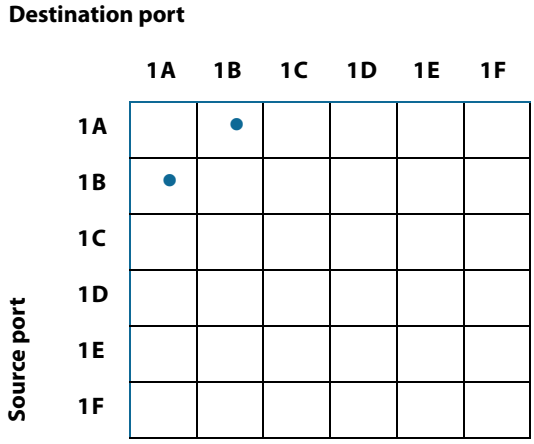

**Figure 17:** A TAP pair

After setting up a TAP pair, you'll also need to set the extra destinations for the traffic to the backplane or other monitoring ports (A to E, B to D, for example) as required.

> **Note:** TAP pairs are set up by default on ports A & B. Unless you have changed the mappings for these ports, you shouldn't need to configure these ports to support TAP pairs. Failsafe is also enabled by default.

**To set up a TAP pair via the web interface:**

1. Connect to the web interface and login.
2. Click **Mapping** to open the mapping page.
3. Click the module that you want to map. The module is highlighted in green and the mapping page updates to show the currently mapped configuration.
4. To set a TAP pair on ports A&B, select the ports shown below.




5. Click **Apply** to implement your mapping changes. Don't forget you'll also need to set destinations for the live traffic; for example, A to E, B to D.
6. To enable failsafe mode, click the **Configuration and Status** button, select the module that you want to configure, and then select the **Failsafe** checkbox. Before deploying a module with failsafe enabled, you may want to perform a test to ensure failsafe is working properly. See *Locking ports* on page 26.
7. Click **Apply** to implement your port configuration changes.
8. To save your changes so they are available after a restart, select **Device administration** and click **Make Permanent**.

# Setting up a port SPAN: Port mirroring

A port SPAN allows data to be mirrored to another port. Unlike a TAP pair, a SPAN is not part of a pair and therefore does not need to failsafe with its partner (the port failsafe options can be turned off). LFP (Link Failure Propagation) should also be disabled, as enabling it will make the port's up/down status dependant on its partner.

# Configuring TAP modes

This section describes how to configure ports for several of the most commonly implemented TAP modes:

- Breakout
- Aggregating
- Backplane aggregating
- V-Line (Bypass)

Other port mappings may also be available, depending on the card type installed. For information about tapping modes, see *Tapping modes* on page 15.

Port mapping can be performed using the web interface, using commands in the CLI, or, for V-Line TAPs, using DIP switches.

## Configuring Breakout mode

Breakout mode is available on Fully Configurable, Aggregating, Breakout, and V-Line modules. Breakout mode allows for an analyzer tool with dual ports to monitor traffic from devices A to B on one port, and traffic from devices B to A on another port. For information, see *Breakout TAP* on page 15.

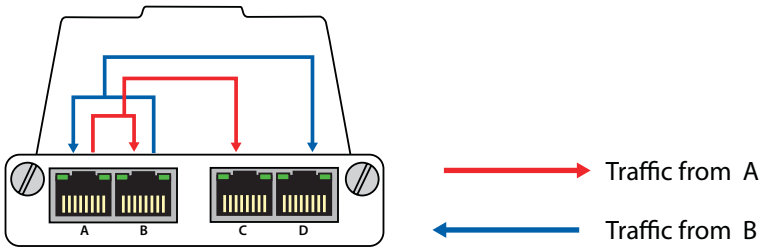



**Figure 18:** Breakout mode

**To configure Breakout mode via the web interface:**

1. Connect to the web interface and login.
2. Click **Mapping** to open the mapping page.
3. Click the module that you want to map. The module is highlighted in green and the mapping page updates to show the currently mapped configuration.
4. To set Breakout mode, select the ports shown below.

**Destination port**

| Source port | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|
| 1A | | ● | ● | | | |
| 1B | ● | | | ● | | |
| 1C | | | | | | |
| 1D | | | | | | |
| 1E | | | | | | |
| 1F | | | | | | |

5. Click **Apply** to implement your changes.
6. To save your changes so they are available after a restart, select **Device administration** and click **Make Permanent**.

**To configure Breakout mode from a command line:**

1. Connect to the CLI and login as the administrator.

2 Select the slot number, enter:

**select slot<number>**

3 Enable Breakout mode, enter:

**set tap1**

4 Write your changes to NVR, enter:

**save**

**To configure Breakout mode on V-Line (Bypass) modules:**

- To set Breakout mode on V-Line (Bypass) modules in a portable chassis, set the DIP switches as shown in *Figure 19*. See *Appendix B, V-Line DIP Switches* on page 48 for switch key.

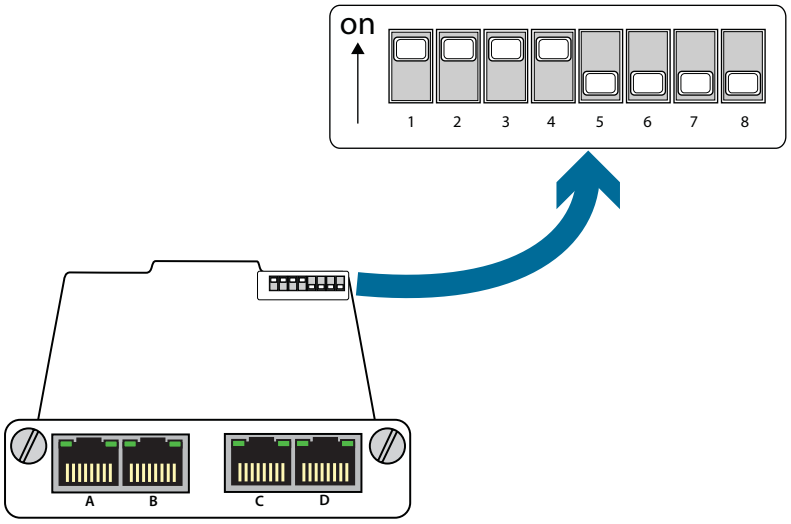



**Figure 19:** V-Line Breakout mode

## Configuring Aggregating mode

Aggregating mode is available on Fully Configurable, Aggregating, and V-Line modules. Aggregating mode allows an analyser tool with a single port to monitor traffic flowing in each direction between live network devices A and B. For more information, see *Aggregating TAP* on page 15.

> ***Caution:*** *Aggregating mode should only be considered when network utilization is low to moderate. Anything over 50% utilization may saturate the monitoring port and cause packets to be missed at that port. However, it is important to note that live traffic will not be affected in the event of port saturation.*

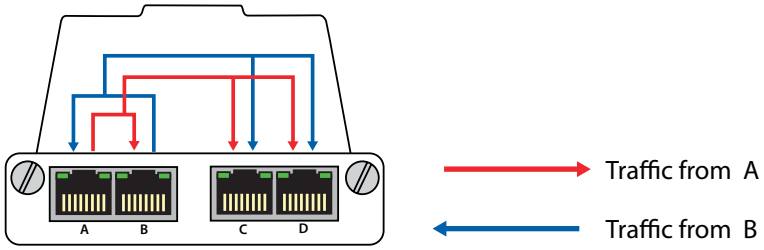



**Figure 20:** Aggregating mode

**To set Aggregating mode via the web interface:**

1. Connect to the web interface and login.
2. Click **Mapping** to access the mapping page.
3. Click on the module you wish to map. The selected module is highlighted in green and the mapping page updates to show the current mapped configuration.
4. To set Aggregating mode, select the ports shown below.

**Destination port**

| Source port | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|
| 1A | | ● | ● | ● | | |
| 1B | ● | | ● | ● | | |
| 1C | | | | | | |
| 1D | | | | | | |
| 1E | | | | | | |
| 1F | | | | | | |

5. Click **Apply** to implement your changes.
6. To save your changes so they are available after a restart, select **Device administration** and click **Make Permanent**.

**To configure Aggregating mode via the command line:**

1. Connect to the CLI and login as the administrator.
2. Select the slot number, enter:

   **select slot<number>**

3. Enable Aggregating mode, enter:

**Set tap2**

4 Write your changes to NVR, enter:

**save**

**To configure Aggregate mode on V-Line (Bypass) modules:**

- To set Aggregate mode on V-Line (Bypass) modules in a portable chassis, set the DIP switches as shown in *Figure 21*. See *Appendix B, V-Line DIP Switches* on page 48 for switch key.

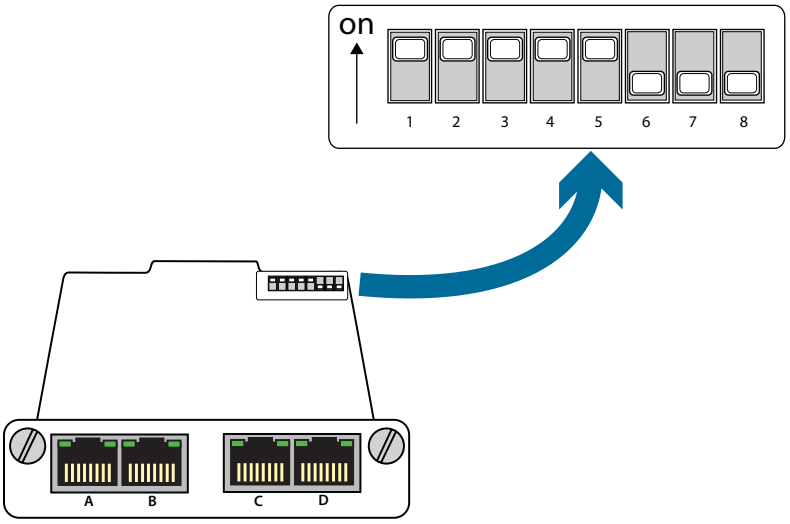



**Figure 21:** V-Line Aggregate mode

## Configuring Backplane Aggregating mode

Backplane Aggregating (BPA) provides a flexible solution for tapping, aggregating, regenerating and distributing live traffic to numerous network tools simultaneously. BPA is a configurable option that allows the administrator to decide which modules send and receive traffic to and from the Backplane.

**Note:** It is important to note that traffic reaching the Backplane will be dropped unless a matching filter rule has been set up to allow the packets to pass through. Initially, no filter rules are set up for the Backplane, so any traffic directed to the Backplane will be dropped. See, *Backplane Filtering* on page 29.

There are a multitude of Backplane configurations that can be set. In the configuration below (*Figure 22*), traffic from ports A and B is sent to the Backplane, where it is aggregated and output to port C and D.

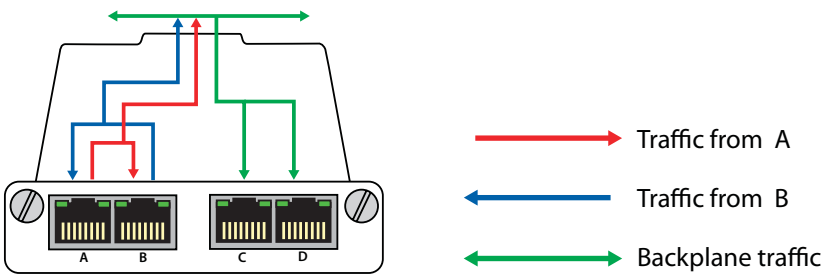



**Figure 22:** Backplane Aggregating mode

**To configure the example BPA mode from the web interface:**

1 Connect to the web interface and login.

2 Click **Mapping** to access the mapping page.

3 Click on the module you wish to map. The selected module is highlighted in green and the mapping page updates to show the current mapped configuration.

4 To set BPA mode, select the ports shown below.

**Destination port**

| Source port | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|
| 1A | | ● | | | ● | |
| 1B | ● | | | | ● | |
| 1C | | | | | | |
| 1D | | | | | | |
| 1E | | | ● | ● | | |
| 1F | | | | | | |

5 Click **Apply** to implement your changes.

6 To save your changes so they are available after a restart, select **Device administration** and click **Make Permanent**.

**To configure the example BPA mode from the command line:**

1 Connect to the CLI and login as the administrator.

2 Select the slot number, enter:

**select slot<number>**

3 Enable BPA mode as per the example, enter:

**Set bpa2e**

4 Write your changes to NVR, enter:

**save**

# Configuring Ports

5

You can configure module and Controller port properties to match the speed, duplex mode and MDI crossover type supported by your network (copper ports only). You can also select failsafe and linklock port options to ensure live traffic continue to flow during a power outage or TAP module disconnection.

## Configuring port settings

You can configure port settings in the TAP and Controller modules to suit your network requirements. For example, for copper connections you can specify the link speed, duplex mode, and MDI crossover settings. From the port options, you can specify settings for link failure propagation, failsafe, and other options to ensure the live link remains unaffected in the event of a power outage or module failure.

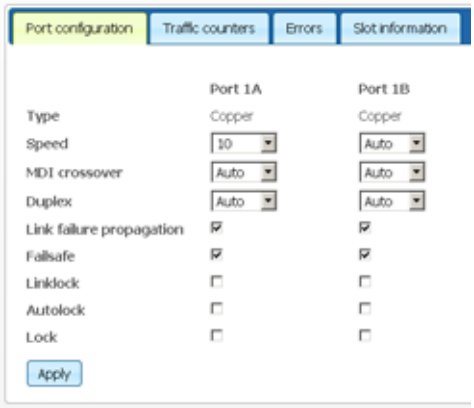



**Figure 23:** Port options for copper ports

**To configure ports using the web interface:**

1. Login to the web interface as an administrator or user.
2. Click **Configuration and Status**.
3. On the graphic, click on the module that you want to configure.
4. If it's not already selected, select the **Port configuration** tab.
5. Enter and specify the port settings required:

   **Speed** Determines the port communication speed. Choose from **Auto** (the default setting), **10**, **100**, or **1000** Mbps. **Auto** allows the port to negotiate the best speed with the link partner. Anything else fixes the part at that speed, whether it is supported by the partner or not. This option is available for Copper connections only.

   **MDI crossover** MDI (Medium Dependent Interface) provides the physical and electrical connection to the cabling medium. Choose from **Auto** (the default setting), **MDI** or **MDI-X** for MDI crossover. Crossover cables must be used for MDI–MDI and MDIX–MDIX connections; straight-through cables must be used for MDI–MDIX connections. This option is available for Copper connections only.

   **Duplex** Determines the duplex (data flow) mode. Choose from **Auto** (the default setting), **Full** or **Half** duplex. **Auto** allows the port to negotiate the duplex mode with the link partner. This option is available for Copper connections only.

**Link failure propagation** This feature is used primarily in high availability networks. It allows the attached network devices to detect if a failure occurs on the adjacent network interface(s). When one side of a link is lost, LFP brings down the rest of the link automatically, allowing the network to identify the failure. This is done by continually monitoring the link status of each port of a port pair (for example, ports A & B). If a connection is lost, SmartNA continues to monitor both ports and will immediately bring both ports back online when the connection has been re-established. LFP is available for all port types. This option is available for Copper connections only, and is enabled by default on ports A&B.

**Failsafe** In the event of a power outage, ports with failsafe enabled will continue passing live network traffic, with just a short break in transmission as the failsafe relay is activated (no monitoring is possible if power is lost). Failsafe is available for copper connections only, and is enabled by default on ports A&B. See *Locking ports* on page 26.

**Linklock** When enabled, relays are closed creating a physical connection between the tap ports. If power is lost or the module is pulled (removed) from the chassis, data will continue to flow across the live link without any loss of data. Linklock is available on copper ports operating at 100 Mbps or less. Linklock is disabled by default.

**Autolock** When enabled, Available on copper ports. Once enabled, autolock closes the port if the network cable is removed. Autolock is disabled by default.

**Lock** Available on copper ports. Once Lock is enabled, the port cannot be used. This option is available for Copper connections only, and is disabled by default.

6 Click **Apply** to implement your changes.

# Locking ports

For security, you may wish to lock copper ports (V-Line modules excluded) that aren't being used to TAP or monitor data. Once locked, the port is disabled and cannot be used without removing the lock first, thus securing the port from unauthorized usage. Port locking is not enabled by default. See also, *Auto-locking ports* on page 26.

**To lock ports from the web interface:**

1 Login to the web interface as an administrator or user.

2 Click **Configuration and Status**.

3 On the SmartNA graphic, select the module you want to configure.

4 In the **Port configuration** tab, select the **Lock** checkbox for the port(s) you want to disable.

5 Click **Apply** to implement your changes.

**To lock ports from the command line:**

❖ Enter the following commands:

**select slot<*slot_number*>**

**set lock <*port_letter*> on**

**save**

# Auto-locking ports

You can configure copper (1000BASE-T) ports so they auto-lock whenever the link is lost, such as if someone removes the network cable. Auto-lock is not enabled by default, and is only available for copper ports. See also, *Locking ports* on page 26.

**To lock ports from the web interface:**

1. Login to the web interface as an administrator or user.
2. Click **Configuration and Status**.
3. On the SmartNA graphic, select the module you want to configure.
4. In the **Port configuration** tab, select the **Auto-lock** checkbox for the port(s) you want to disable.
5. Click **Apply** to implement your changes.

**To auto-lock ports from the command line:**

- Enter the following commands:

  **select slot<*slot_number*>**

  **set autolock <*port_letter*> on**

  **save**

# Viewing port statistics

## Traffic counters

For each network interface (port), the SmartNA System maintains a set of traffic counters which show the accumulated number of bytes and packets sent and received since the module was last rebooted (see *Rebooting the Controller and TAP modules* on page 40). Port utilization as a percentage is also shown.

**To view traffic counters via the web interface:**

1. Login to the web interface as an administrator or user.
2. On the image of the SmartNA System, click on the module you want to inspect.
3. Click **Configuration and Status**, and then select the **Traffic counters** tab (*Figure 24*).

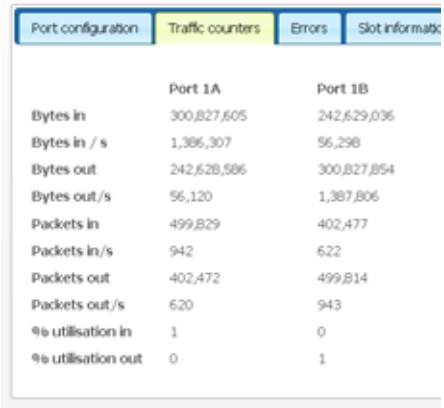



**Figure 24:** Traffic counters for Ports 1A & 1B

**To view traffic counters from the command line:**

- Enter the following commands:

  **select slot<*slot_number*>**

**show counters**

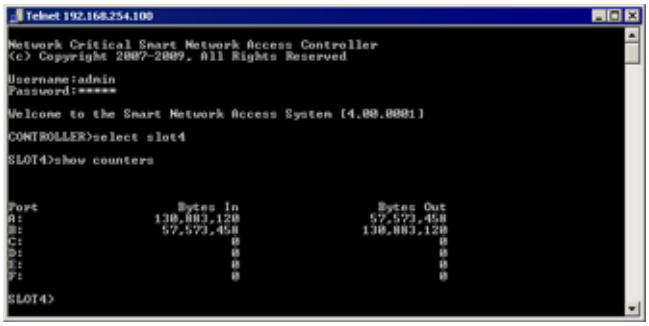



**Figure 25:** CLI showing counters for slot 4

## Packet errors

For each network interface, the SmartNA System maintains statistics for the number of error packets received since the module was last rebooted. A large number of packet errors often indicates a port configuration issue, and administrators are advised to check the error statistics periodically and reconfigure the port settings if required. See *Configuring port settings* on page 25.

### To view packet errors via the web interface:

1. Login to the web interface as an administrator or user.
2. On the image of the SmartNA System, click on the module you wish to view.
3. Click **Configuration and Status**, and then select the **Errors** tab.

### To view traffic counters from the command line:

- Enter the following commands:

  **select slot<*slot_number*>**

  **show errors**

# 6

# Backplane Filtering

When the Aggregating/Filtering 1U chassis is used in conjunction with Filtering Modules, it can apply a set of filter rules to selectively pass data based on various criteria, including TAP port, VLAN identity, MAC address, plus a host of other parameters. This chapter describes how Backplane filtering works, and explains why you might want to use it.

**Note:** Backplane filtering is not available in systems with pre- v4.*x* firmware installed.

## About Backplane filtering

Backplane filtering provides a powerful and flexible approach for providing access to a useful subset of full line rate 1Gbps traffic. For example, a laptop running packet analysis software can be connected to a 1G link and a filter can be set to duplicate only relevant packets for debug (say ICMP packets with a particular payload), and instead of receiving the entire 1G link, the laptop receives only the relevant packets.

When you create a filter, you specify a rule that governs the data flow to the output port. The rules you define specify whether the system should permit or deny access to the output port, based on the packet header details and the criteria you have specified. To pass traffic that matches several rules, you can add several rules, each with its own set of criteria.

Some important points about filtering:

- Filters are applied to the Backplane ports only (Ports E&F)
- The first matching rule found applies the associated action (see *Arranging Backplane rules* on page 31)
- The policy match counters count packets that match a particular rule

It is important to note that traffic reaching the Backplane will be dropped unless a matching filter rule has been set up to allow the packets to pass through. Initially, no filter rules are set up for the Backplane, so any traffic directed to the Backplane will be dropped.

***Caution:*** *Backplane filtering is only compatible with Filtering Modules. If any other type of module is inserted into the chassis all filtering capabilities will be immediately disabled until removed.*

# Adding filter rules

The SmartNA System supports a maximum of 512 rules and 32 counters, which increment each time a rule is matched (the rules effectively count packets). Multiple rules are able to share the counters, enabling you to count rules in groups. This approach can be helpful when designing complex filter rules.

**To add a filter rule:**

1. Using a web browser, connect to the SmartNA web interface.
2. Click **Mapping**.
3. On the diagram of the SmartNA System, click the top of the unit, as shown in the diagram.


4. On the Filter Rules panel, click **Add +** to add a new rule.
5. Enter the rule options and filter criteria using the following fields (all fields are optional):

   **Name** Specifies a name for the filter. Enter a name which describes the filter, for example "1A to 4F (HTTP)".

   **Source** Specifies the inbound source port(s) to which the filter is applied. To disable a rule, you can select **Rule disabled** from the list.

   **VLAN** Filters traffic with the specified VLAN ID. The field accepts decimal or a 12-bit binary value.

   **MAC Source** Filters traffic with the specified source MAC address. Use hexadecimal notation with or without colon separators.

   **MAC Destination** Filters traffic with the specified destination MAC address. Use hexadecimal notation with or without colon separators. You may also use a mask ("*") to specify a range.

   **Is IP?** Filters traffic according to if the packet type is IP, not IP, or don't care.

   **Protocol** Filters traffic with the specified protocol. The Layer 4 protocol id (0–255) may also be entered in the text box.

   **DSCP** Filters traffic with the specified Differentiated Services Code Point (DSCP) identity. The field accepts decimal or binary data.

   **IP source** Filters traffic with the specified IP source address. Specify a single IP address in dotted decimal notation; optionally use a mask to specify a range; for example: 192.168.0.0/255.255.255.0.

   **IP destination** Filters traffic with the specified IP destination address. Specify a single IP address in dotted decimal notation; optionally use a mask to specify a range; for example: 192.168.0.0/255.255.255.0.

   **L4 source** Filters packets with the specified source TCP/UDP Port number.

   **L4 destination** Filters packets with the specified destination TCP/UDP Port number.
6. Using the **Send to** checkboxes, specify at least one destination port for the filtered traffic.

> **Note:** You must select at least one destination port to avoid dropping data.

7. If required, enter a counter number between 0 and 31. The counter is incremented each time a rule is matched (the rule effectively counts packets). Rules can also share the same counter, so you can easily count rules in groups, this can be helpful when designing complex filter rules.

8 Click **Add +** to add more rules, or click **Apply all rules** to apply your rules.

9 If necessary, drag your filter rules up or down to organise them into the correct order. As has already been noted, the first matching rule found applies the associated action, so it is important to make sure the filter order is correct. See, *Designing complex rules* on page 32 an example of a complex rule where order is important.

10 To save your filter rules, click **Device Administration**, **NVR**, and click **Make permanent**.

# Arranging Backplane rules

When setting up Backplane filters, keep in mind that the *first* matching rule found in the list applies the associated action. Backplane rules are read from top to bottom; once a match is found, no further rules will be checked.

You can arrange Backplane rules simply by dragging the rule to a new position in the list. To do this, click and hold on the rule's name and then drag, as shown in *Figure 26*.

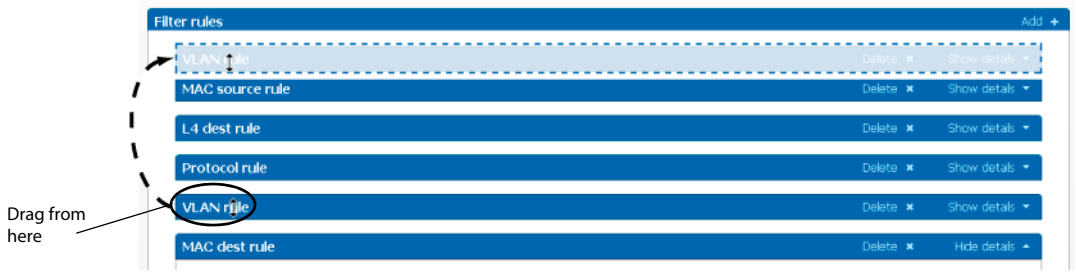



**Figure 26:** Dragging a rule to a new position

# Example rules

## Adding a simple rule

An easy rule to add might be a rule to send all HTTP traffic from port 1E to 4F.

1 Click **Add +** to add a blank rule at the bottom of the list.

2 Name the rule "1A to 4F (HTTP)", or whatever makes sense to you.

3 For Source port select **1A**.

4 For Protocol select **TCP**.

5 For L4 source enter **80**.

6 For Send To check **4F**.

7 If you wish you can also set a counter for this rule.

8 Click **Apply all rules** to make your changes happen.

## Designing complex rules

Since rules are processed in list order and only the first matching rule is actioned, whenever you are filtering a single inbound stream to multiple destinations you must think carefully about your rules. Consider the following rules:

- Rule 1: Send all HTTP traffic from port 1E to 4F.
- Rule 2: Send all IP traffic from host 192.168.0.1 from port 1E to 3E.

If these two separate rules exist in this order then port 3E will not receive ALL the correct traffic. It will actually receive all IP traffic for host 192.168.0.1 *except* HTTP packets.

To make sure that 3E receives all the correct packets we must add another rule. The rule must specifically match the overlap between the existing two rules, it must have BOTH ports set as the destination, and it must be placed higher in the list:

- Rule 1: Send all HTTP traffic from host 192.168.0.1 from port 1E to ports 3E and 4F.
- Rule 2: Send all HTTP traffic from port 1E to 4F.
- Rule 3: Send all IP traffic from host 192.168.0.1 from port 1E to port 3E.

Rules can be dragged into order by their title bar.

**Tip:** Save your filter rules to NVR (memory) if you want them to be available after a restart. See, *Saving changes to NVR* on page 41.

# 7

# Using SNMP

SmartNA Systems with v.4.x firmware support Simple Network Management Protocol (SNMP). You can use SNMP to monitor the SmartNA System for conditions that warrant administrative attention, such as removal of a module or changes to the link up/link down status.

> **Note:** SNMP is not available in systems with pre- v4.*x* firmware installed.

The following sections explain how to enable SNMP, define who may access the system, who may receive traps, which ones, and define the conditions for triggering some of those traps.

The following sections do not offer a tutorial in SNMP, which the user should be familiar with, nor does it discuss the data objects supported by the system. You should refer to the Management Information Bases (MIBs) relevant to this product:

- RFC1213-MIB — Standard MIB-2 items
- NCProductIDs.mib — Unique IDs for Network Critical products
- NCSystem.mib — System items for Network Critical products
- NCTap.mib — Items specific to TAPs

## Configuring SNMP system-wide options

The SNMP system-wide options can be used to enable or disable SNMP itself, SNMP traps, and whether any IP address or a fixed address must be used (called zero (0.0.0.0) IP address or allow all).

> **Note:** SNMP is a powerful tool that provides remote access to the system from anywhere on the net. For security therefore, SNMP and traps are disabled by default and must be enabled before they can be used.

**To configure SNMP system-wide options:**

1. Connect to the web interface and login as an administrator or user.
2. Click **SNMP** and select the **System-wide** tab.
3. Select the required settings from the following options:

**SNMP enabled** Select this checkbox to enable SNMP. Once enabled, you can access the system from any IP address using the default user account: read community string **public**; write community string **private**. This option is not selected by default.

> ***Caution:*** *The default SNMP community strings (**public** and **private**) are not secure. You are strongly advised to set up users with different community strings at the earliest opportunity.*

SNMP may also be enabled from the command line, by entering **set snmp on** on the Controller module.

**Trap enabled** Select this checkbox to enable traps to be sent. Note that traps are not sent where the entry IP address is zero (0.0.0.0). This option is not selected by default.

> **Note:** Traps are not sent where the user entry IP address is zero (0.0.0.0).

**Authentication trap enabled** If this checkbox is selected, authentication traps will be sent to warn when a bad SNMP request is made, such as with an invalid community string. Unauthorised access traps are only sent for invalid attempts to access the system through SNMP (invalid attempts to access the TAP through the Web interface or CLI do NOT generate traps). This option is not selected by default.

> **Note:** To receive authentication traps it is essential to enable both traps and authentication traps.

**Zero IP address = allow all** When selected (the default), entries with a zero IP address (0.0.0.0) are recognised and any request fulfilling the other criteria (for example, community string) will be allowed from *any* address; this does, however, remove a level of verification and thus security. This facility allows for systems where DHCP is used to allocate IP addresses, but it is strongly urged that fixed IP addresses are used where possible. Traps are not sent where the IP address is zero. This option is selected by default.

4 Click **Apply** to implement your changes.

# Configuring SNMP users

The SmartNA System allows up to 16 SNMP access entries to be set up. They are designated "users" since, effectively, this is what they are; although in SNMP architecture they are an NMS (Network Management Station). Each entry has the access details of some "user" device or program that will access the system for information or to request changes in operation. These entries have an IP address, port number, community strings, access type, an OID pointing into the SNMP tree, and a number of trap enable flags.

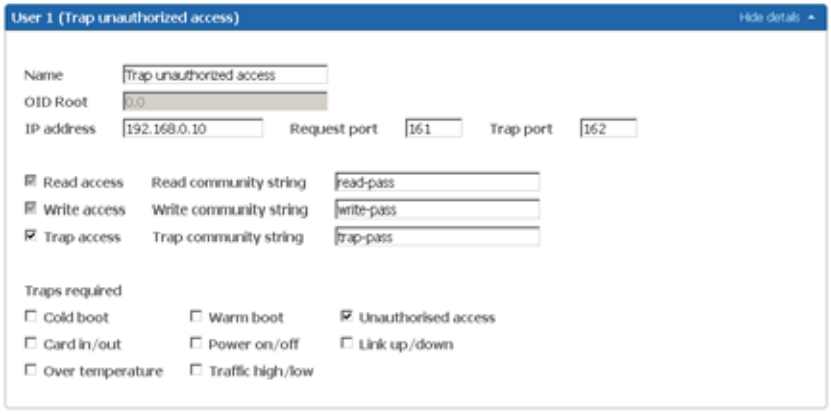



**Figure 27:** Example SNMP user

**To configure SNMP users:**

1 Connect to the web interface and login as an administrator or user.

2 Click **SNMP**, and then select the **Users** tab to list the user entries.

3 Click **Show details** to expand an entry, or click **Clear details** to remove details.

4 To add or configure a user, enter information into the fields as follows:

**Name** The name field is provided for identification purposes only and is not used by the system for access. Names are limited to 32 characters and may contain spaces.

**OID Root** The OID root value limits the view of the SNMP tree. If set to 0.0 then any OID value can be accessed. If set to a point in the OID tree then only those values "below" the OID root can be seen. For example, if set to 1.3.6.1.2.1.2 (the Interface part of the MIB-2 mib), only the Interface OIDs would be visible to this user entry.

**IP address** The IP address indicates which IP address will be used by this user to make requests. If traps are enabled for this user, this is the address they will be sent to. All broadcast requests are ignored even if the IP address entered is valid for that broadcast. If the IP address is a broadcast address then a broadcast trap will be sent.

**Tip:** When power is removed from the tap, it will attempt to send a "Cold Boot" trap, with appropriate data (Varbinds), to any users configured to receive this trap. The tap only has a short period in which to send this trap before the power fails. A broadcast will be quicker than one or more individual messages so consider using a broadcast address in this case. See *Combining SNMP values for greater access control* on page 37.

If the **AllowZeroIPAddress** flag is enabled, then entries with a zero IP address (0.0.0.0) are recognised and any request fulfilling the other criteria (e.g. community string) will be allowed from *any* address; this does, however, remove a level of verification and thus security. This facility allows for systems where DHCP is used to allocate IP addresses but it is strongly urged that fixed IP addresses are used where possible. Traps are not sent where the IP address is zero (0.0.0.0).

**Request port** The request port is the software port on the system the user will make SNMP requests to. Any port value may be used except zero. Entering zero signifies that the port should be set to the standard port for SNMP for requests (161).

**Trap port** The trap port is the port for the user device to which traps are sent. Any port value may be used except zero. Entering zero signifies that the port should be set to the standard port for SNMP traps (162).

**Note:** It is the administrator's responsibility to ensure that the ports used are valid and not used by other processes or blocked by firewalls. A maximum of four different ports may be used to receive SNMP requests on.

**Read community string** This is the SNMP Community String (or password) that is used when read (GET/GET NEXT) requests are made. Entries are case sensitive, are limited to 32 characters, and may include spaces.

**Write community string** This is the SNMP Community String (or password) that is used when write (SET) requests are made. Entries are case sensitive, are limited to 32 characters and may include spaces.

**Tip:** The Write community string is only valid for write requests (SETs). This provides compatibility with SNMP tools that use the Write community string for write operations but still use the Read community string for read operations. Setting the Read and Write community strings to the same value will achieve standard read/write behaviour.

**Trap community string** The trap community string is included with any trap to verify that the system generated the trap. Entries are case sensitive, are limited to 32 characters and may include spaces.

**Read/Write/Trap access** Indicates if read and/or write access is allowed for this user and if traps are to be sent to the user.

**Traps required** The trap flags indicate which types of traps are to be sent to the IP address indicated by this entry. Note if the IP address is zero (0.0.0.0), no trap is sent. The following traps are available:

- Cold boot

- Warm boot
- Unauthorized access
- Card in/out
- Power on/off
- Link up/down
- Over temperature (see *Setting thresholds for temperature and traffic traps* on page 36)
- Traffic high/low (see *Setting thresholds for temperature and traffic traps* on page 36)

**Note:** To send traps, the **Traps enabled** option in SNMP system-wide settings must be selected. See *Configuring SNMP system-wide options* on page 33. Unauthorized access traps *also* require **Authentication Trap enabled** to be selected (**System-wide > Authentication trap enabled**). Unauthorized access traps are only sent for invalid attempts to access the system through SNMP; invalid attempts through the web interface or the CLI do *not* generate traps.

# Setting thresholds for temperature and traffic traps

Thresholds at which temperature and traffic trap are triggered can be specified for each slot or port, respectively. When a threshold is exceeded, a trap will be generated. A clear trap is generated as soon as the temperature falls 1° C below the specified threshold, or when traffic falls below the lower threshold. Traps are sent to users who have the **Over temperature** or **Traffic high/low** flags selected (see *Configuring SNMP users* on page 34).

**Note:** If you transfer a Controller to another SmartNA System of a different size (1U to 2U, say) thresholds for traffic and temperature will need reviewing.

**To configure temperature and traffic thresholds:**

1. Connect to the web interface and login as an administrator or user.
2. Click **SNMP**.
3. Select the **Temperature thresholds** tab and enter temperature thresholds, in degrees Celsius, for each slot. The default threshold is 70° C.
4. Select the **Traffic thresholds** tab and enter traffic thresholds, as a percentage of total capacity, for each port. The 'high' value must be greater than the 'low' value. Setting the high to 100% or the low to 0% will inhibit the appropriate trap. The limits are set to 100% and 0%, respectively.
5. Click **Apply** to implement your changes.

# Combining SNMP values for greater access control

Combined, SNMP values allows greater control over access to the system. Depending on individual settings a request must be made from a known IP address, to a known port with the correct community string and access and a view of the OID concerned. Using more than one entry, different access can be given to different parts of the MIB tree. For example, read access can be given for all OID but write access to only part of the tree. If Zero IP addresses are allowed then this level of verification is removed but the community string is still required and access may be further restricted by the read/write/trap access flags and the OID view.

For example, in the first three entries below, the first allows Fred to read any OID using the community string "GoReadIt", the second to write Tap OIDs (for instance, starting 1.3.6.1.2.2) using the community string "WriteThatOID", the third to write MIB2 OIDs using the community string "Write Away". This means that they do not have write access for NC system OIDs. Fred would be unable to alter the access table (1.3.6.1.4.1.31645.2.1).

Traps are sent to Fred at 100.150.10.5 with the community string "Traps2" because of entry 2. If the access field in Entry 1 were changed to read-trap then a second set of traps would be sent to Fred with the community string "Traps1".

| | **Entry 1** | **Entry 2** | **Entry 3** | **Entry 4** |
|---|---|---|---|---|
| **Name** | Fred - Read All | Fred - Write tap | Fred - Write MIB2 | Cold Boot Trap |
| **IP address** | 100.150.10.5 | 100.150.10.5 | 100.150.10.5 | 100.150.10.255 |
| **Request port** | 161 | 161 | 161 | <Could be anything> |
| **Trap port** | 162 | 162 | 162 | 162 |
| **Read community string** | GoReadIt | <Could be anything> | <Could be anything> | <Could be anything> |
| **Write community string** | <Could be anything> | WriteThatOID | Write Away | <Could be anything> |
| **Trap community string** | Traps1 | Traps2 | <Could be anything> | BcastTrap |
| **Access** | read-only | write-trap | write-only | trap-only |
| **OID root** | 0.0 | 1.3.6.1.4.1.31645.2.2 | 1.3.6.1.2.1 | <Could be anything> |
| **Traps** | All enabled | All enabled | <Could be anything> | Cold boot only |

The fourth entry uses a broadcast address to broadcast a cold boot trap with the community string "BcastTrap" to all devices on the subnet 100.150.10.0. This is quicker than sending individual traps, which is particularly useful when a cold boot trap is sent to indicate the system has lost power. Note that this means a broadcast trap will also be sent when power is applied to the system (when it is switched on).

This also demonstrates the ability to select which users receive which traps. Here, all users on a subnet receive one specific trap. Equally, the system can be set so that, say, all users receive notification of a particular type of event such a card being removed but only certain users are told if a card is too hot.

# SmartNA Administration

8

This chapter describes setting up user accounts, configuring the network address, updating firmware, and performing other general SmartNA administration tasks.

## Configuring usernames and passwords

The system supports two user accounts: administrator and standard user. Administrators have full read-write access to the system via the CLI; standard users have read access only via the CLI. Both accounts have full access to the web GUI.

By default, the administrator and user accounts have the following login settings:

| User | Login Details |
|---|---|
| Administrator | username: admin<br>password: admin |
| Standard user | username: user<br>password: user |

To prevent unauthorized access to the SmartNA System, you are strongly advised to change the default user names and passwords at the first opportunity. For security, accounts can only be changed from the command line interface after logging in as the administrator.

**To configure usernames and passwords:**

1. Login to the SmartNA command line interface as the administrator. See *Accessing the command line interface (CLI)* on page 13.
2. Select the Controller module:

   **select controller**
3. To change the administrator account, enter these commands:

   **set admin password**

   (you will then be prompted for the new password)

   Passwords are case sensitive and may not contain spaces.

   **set admin username**

   (you will then be prompted for the new username)
4. To change the standard account, enter these commands:

   **set user password** (you will then be prompted for the new password)

   **set user username** (you will then be prompted for the new username)
5. There is no need to save or reboot the system, the account changes will take effect immediately.

# Configuring the IP address

By default, the SmartNA System is configured with the IP address **192.168.254.100**. You can use this address to access the SmartNA web interface and to SSH to the system. When first setting up the system, you may need to manually set an IP address from the 192.168.254.x subnet on the workstation you are using to configure the system.

**To set the IP address via the CLI:**

1. Login to the SmartNA CLI. See *Accessing the command line interface (CLI)* on page 13.
2. Depending on if you are using static or DHCP IP address allocation:
   - For DHCP allocation, enter the following command:

     **set address dhcp**
   - For static IP address allocation, enter the following commands:

     **set ip <*address*>**

     **set netmask <*netmask*>**

     **set gateway <*address*>**
3. To write your changes to NVR, enter:

   **save**
4. Reboot the SmartNA System to activate the new IP address.

> **Note:** After changing the IP address, you must reboot the Controller for the new IP to become active.

# Updating system firmware

Network Critical periodically issues firmware updates for the SmartNA System, including updates for the Controller and TAP modules. As described below, updates can be applied from the command line, the web interface, or by using the SmartNA Locator software.

> ***Caution:*** *Updating the Controller SmartNA firmware resets the SmartNA System back to factory defaults, deleting all port settings, mappings, users and user passwords in the process.*

> **Tip:** Before updating firmware, note down the port setting and port mappings for each module so you can return them to their pre-update status.

**To update firmware from the web interface:**

1. Login to the SmartNA web interface.
2. Click **Device Administration**, and select the **Firmware Upload** tab.
3. Browse to the firmware file and upload it to the Controller and modules. Note that after updating the Controller firmware, the system will be reset to factory default settings, erasing any user names, passwords, port mappings and port configuration details that have been configured.

# Rebooting the Controller and TAP modules

The SmartNA System allows you to reboot the Controller and TAP modules independently of each other without interfering with data monitoring on other ports. A reboot of the Controller module is required following a change in the IP address configuration or after uploading new firmware. Modules can be rebooted to reset their counters, as well as following a firmware update.

**To reboot the Controller or TAP modules from the web interface:**

1. Login to the SmartNA web interface.
2. Click **Device Administration**.
3. Select the **Reboot** tab.
4. Enter the slot number that you want to reboot. See *Figure 3* on page 4 and *Figure 6* on page 4 for details of the slot numbers.
5. Click **Reboot slot**. Rebooting the Controller may disable web access for up to one minute.


**Figure 28:** The Controller/TAP module reboot screen

**To reboot the Controller or TAP modules from the command line interface:**

1. SSH to the SmartNA System and login as the administrator.
2. To reboot the Controller module, enter the following command:

   **select controller**

   **reboot**

   To reboot a module, enter:

   **select slot <*slot_number*>**

   **reboot**

   Following a reboot of the Controller access to the web interface may be disabled for up to one minute.

# Resetting to factory defaults

If necessary, you can reset the Controller module to its factory default settings. Resetting the controller should not be done lightly as the following settings are affected:

- Erases 1U Backplane Filter Rules
- Resets Controller mappings and port settings

**To reset to factory defaults:**

1. Login to the SmartNA web interface.
2. Click **Device Administration**.
3. Select the **Factory Reset** tab.
4. Click **Set Defaults**.


**Figure 29:** The factory reset screen

# Saving changes to NVR

SmartNA NVR, or non-volatile RAM, stores user names, passwords, port mappings, and port configuration settings. Any changes you make to these settings must be saved to NVR to make them available after a system restart or reboot.

**To save changes to NVR from the web interface:**

1. Login to the SmartNA web interface.
2. Click **Device Administration**.
3. Select the **NVR** tab.
4. Click **Make Permanent**.

**To save changes to NVR from the command line:**

1. From the command line, login to the SmartNA System as an administrator.
2. To save changes to NVR, enter:

   **save**

# Viewing slot information

Slot information contains details of the module's firmware version, model number, and serial number, as well as its current operating temperature and uptime. Slot information can be displayed in the CLI by entering the module Show

commands, as described in *TAP module: SHOW commands* on page 45, or more easily from the SmartNA web interface, as described below.

**To view slot information from the web interface:**

1. Login to the web interface as an administrator or user.
2. On the image of the SmartNA System, click on the module you wish to view.
3. Click **Configuration and Status**, and then select the **Slot information** tab to display the slot details (*Figure 30*).

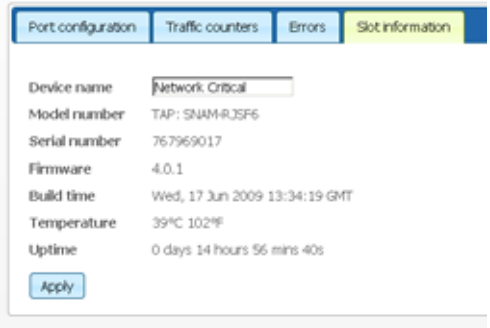



**Figure 30:** Slot information details

4. If you want to change the device name, enter a new name and then click **Apply**.

# CLI Commands

A

This section lists the CLI command that are available for SmartNA Controller and TAP modules. The commands enable you to view and set module settings. To access the CLI, SSH to the SmartNA System and login as the administrator or user, depending on the access level required.

> **Note:** CLI commands are executed on the current selected module only. Commands that are executed on the Controller affect only the Controller, while commands executed on a module affect only that module.

In this chapter, the commands are organized in the following sections:



## General (system-wide) commands

The following general commands are available from any slot in the SmartNA System.

| Command | Meaning |
|---|---|
| **Help \| ?** | Displays the command summary. |
| **Select Slot <#>** | Select slot# to manage a module. |
| **Select Controller** | Return to controller to manage system. |
| **Show <*Feature*>** | Show the current feature value/state. |
| **Set <*Function*>** | Set a system function or attribute. |
| **Save** | Make any changes permanent. |
| **Reset \| Reboot** | Resets selected Module/System to last saved state. |
| **Clear Counters** | Clear port based byte counters. |
| **Exit \| Quit** | Terminates the telnet session. |

# Controller: SHOW commands

The following read-only commands are available for the Controller module. Ensure the Controller module has been selected (**select controller**) before entering these commands.

| Command | Meaning |
|---|---|
| **Show System** | Display an overview of the current system configuration. View settings for IP address, management interfaces, and PSU state, along with a summary of the module present in each slot. |
| **Show Config** | Display the hardware configuration and list the current settings for each network interface on the controller. |
| **Show map** | Display the internal port mapping of the controller, and of the backplane.<br><br>The table indicates the currently mapped egress settings for each ingress port. |
| **Show counters** | Display the inbound/outbound byte counters for each network interface on the controller.<br>Optional integer will refresh the display every [#] seconds.<br>Use Ctrl+C to stop refreshing the display. |
| **Show errors** | Display the error counters every for each interface on the controller, including backplane interfaces.<br>Optional integer will refresh the display every [#] seconds.<br>Use Ctrl+C to stop refreshing the display. |
| **Show port** | Display the current status & settings of the port(s) selected. |
| **Show SN** | Display the Controller Serial Number and MAC. |
| **Show ver** | Display the Controller firmware version. |

# Controller: SET commands

The following 'Set' commands are available for the Controller module. Before enter these commands, make sure you have selected the Controller module by entering the following command:

**select controller**

To make any changes you make available after a system restart or reboot, enter the following command:

**save**

| Command | Meaning |
|---|---|
| **Set Defaults** | Set all features to factory defaults. |
| **Set Device Name** | Set the device name seen in Locator. |
| **Set Echo** | Toggles whether text is echoed during the CLI session. |
| **Set IP <*address*>** | Set the IP Address. |
| **Set Netmask <*address*>** | Set the Netmask. |

| Command | Meaning |
|---|---|
| **Set Gateway <*address*>** | Set Gateway address |
| **Set Resolver <*address*>** | Set DNS Resolver address |
| **Set Address Static\|DHCP** | Set the IP address mode: Static, DHCP |
| **Set HTTP on\|off** | Turn HTTP(S) interface on or off. |
| **Set map *ports* on\|off** | Map traffic between ports |
| **Set snmp on\|off** | Turn SNMP interface on or off |
| **Set <*account*> password** | Set the account password |
| **Set port <*attribute*>** | Set the port attribute |
| **Set <*account*> username** | Set the account login name |

# TAP module: SHOW commands

The table below lists the module 'show', read-only, commands. Show commands are available to all user accounts. Before entering the commands, make sure the correct module slot has been selected with the following command:

**select slot #** (where # is the slot number)

| Command | Meaning |
|---|---|
| **Show system** | Display an overview of the current system configuration.<br><br>View settings for IP address, management interfaces, and PSU state, along with a summary of the module present in each slot. |
| **Show config** | Display the hardware configuration and list the current settings for each network interface on the current module. |
| **Show map** | Display the internal port mapping of the module controller.<br><br>The table indicates the currently mapped egress settings for each ingress port. |
| **Show mode** | Display the module mode setting. |
| **Show counters** | Display the inbound/outbound byte counters for each network interface on the module. |
| **Show errors** | Display the error counters every for each interface on the controller, including backplane interfaces. |
| **Show port** | Display the current status & settings of the port(s) selected. |
| **Show SN** | Display the Controller Serial Number and MAC. |
| **Show ver** | Display the Controller firmware version. |

# TAP module: SET commands

The following 'Set' commands are available for TAP modules. Before entering commands, make sure the correct module slot has been selected with the following command:

**select slot #** (where # is the slot number)

To make any changes you make available following a system restart or reboot, enter the following command:

**save**

| Command | Meaning |
|---|---|
| **Set autolock <*port_list*> <*state*>** | Set Auto Locking of Port(s) when Link Lost. |
| **Set BI <*monitor_port*> <On\|Off>** | Set Bidirectional (BI) on or off for C or D. |
| **Set BPA1E** | Set A,B TAP, C Local Aggregate & Backplane E Aggregate to D. |
| **Set BPA1F** | Set A,B TAP, C Local Aggregate & Backplane F Aggregate to D. |
| **Set BPA2E** | Set A,B TAP and Backplane E Aggregate to C,D. |
| **Set BPA2F** | Set A,B TAP and Backplane F Aggregate to C,D. |
| **Set BPA3E** | Set A,B SPAN, C Local Aggregate & Backplane E Aggregate to D. |
| **Set BPA3F** | Set A,B SPAN, C Local Aggregate & Backplane F Aggregate to D. |
| **Set BPA4E** | Set A,B SPAN and Backplane E to C,D. |
| **Set BPA4F** | Set A,B SPAN and Backplane F to C,D. |
| **Set BPA5E** | Set A SPAN to B,C,D,E. |
| **Set BPA5F** | Set A SPAN to B,C,D,F. |
| **Set BPA6E** | Set E Backplane to A,B,C,D. |
| **Set BPA6F** | Set F Backplane to A,B,C,D. |
| **Set BPA7E** | Set A,B TAP, Backplane E Aggregate to C & Local. |
| **Set BPA7F** | Set A,B TAP, Backplane E Aggregate to C & Local. |
| **Set Bypass <State>** | Set the V-Line bypass mode. |
| **Set Defaults** | Set all features to factory defaults. |
| **Set Duplex Auto\|Full** | Set the duplex mode on V-Line modules. |
| **Set Failsafe <*port_pair*> <*state*>** | Turn AB or CD Failsafe on or off. |
| **Set FE-AGG** | Set basic config to Fast Ethernet Aggregation. |
| **Set FE-BRE** | Set basic config to Fast Ethernet Breakout. |
| **Set GE-AGG** | Set basic config to Gigabit Ethernet Aggregation. |
| **Set GE-BRE** | Set basic config to Gigabit Ethernet Breakout. |
| **Set LFP <port_pair> <On\|Off>** | Set Link Failure Propagation (LFP) on or off. |

| Command | Meaning |
|---|---|
| **Set LinkLock <port_pair> <On\|Off>** | Set LinkLock on or off. |
| **Set Lock <port_list> <On\|Off>** | Enable/disable port locking for the specified ports. |
| **Set Map <port> <port_list> <*state*>** | Map traffic between ports. |
| **Set Packet-Slicing <Enable\|Disable>** | Enable/disable packet slicing on V-Line modules. |
| **Set Port <*port_list*> <*attribute*>** | Set the port attribute. |
| **Set Reverse Bypass <Enable\|Disable>** | Enable/disable Reverse Bypass on V-Line modules. |
| **Set Slicing Size #** | Set the Packet Slicing size (64 to 4096 bytes). |
| **Set SPAN1** | Set A,B SPAN Inputs to C,D Monitor. |
| **Set SPAN2** | Set A SPAN Input to B,C,D Monitor. |
| **Set SPAN3** | Set A SPAN Input, B LAN and C,D Monitor. |
| **Set SPAN4** | Set A,B,C SPAN Inputs to D Monitor. |
| **Set Speed 100\|1000** | Set the data rate on V-Line modules. |
| **Set TAP1** | Breakout TAP Mode. |
| **Set TAP2** | Aggregating TAP Mode. |
| **Set TAP3** | Set V-Line TAP Mode on V-Line modules. |
| **Set TAPSPAN** | Set A,B TAP, C SPAN Input all to D Monitor. |

## CLI Legend

The following general commands are available from any slot in the SmartNA System.

| Notation | Meaning |
|---|---|
| **[#]** | denotes a number value. For example, entering the command 'Show Counters 30' would display the port byte counters every 30 seconds |
| **<ACCOUNT>** | denotes the user account. For example, entering the command 'Set user Username' would then prompt for a new username |
| **<ATTRIBUTES>** | 100, 1000, AUTO, HALF, FULL, AUTO DUPLEX, MDI, MDIX, AUTO MDI |
| **<PORT>** | denotes any of the ports A B C D E or F |
| **<PORT LIST>** | denotes any combination of ports separated by commas and without spaces. For example, entering the command 'Show Port A,C,D' would display the current state of ports A,C and D but would not display port B status. |
| **<PORT PAIR>** | denotes a pair of ports. For example AB or CD or ABCD |
| **<STATE>** | denotes either:<br>ON, ENABLE or 1<br>OFF, DISABLE or 0 |
| **<STRING>** | denotes any combination of alpha or numeric characters |

# V-Line DIP Switches

B

For V-Line (Bypass) modules in a portable chassis, or when no controller module is present, the onboard DIP switches *must* be used to set the operating mode, port speed, duplex mode, and other options because the management port on the rear of the chassis is non-functional. *Figure 31* shows the location of the DIP switches on the V-Line module. Refer to *Table 1* for the switch legend.

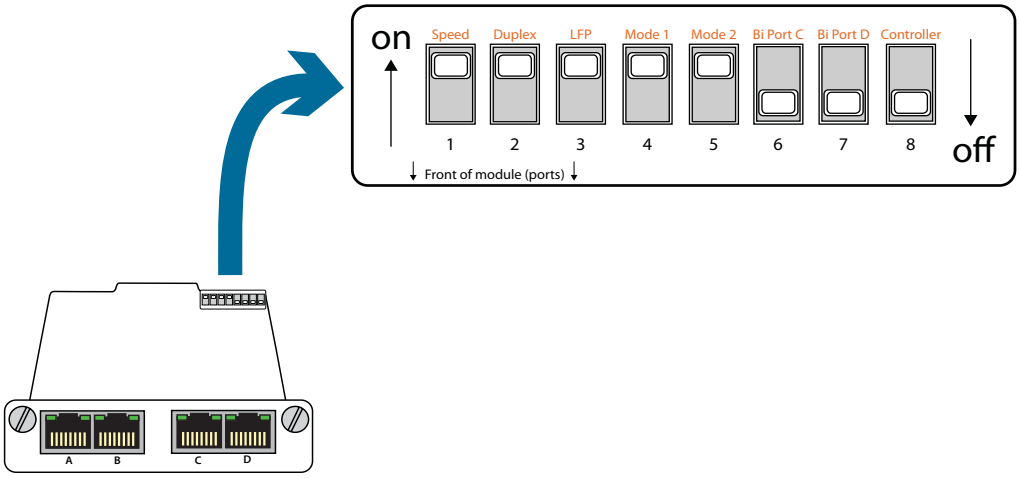



**Figure 31:** Location of DIP switches on the V-Line TAP

| Switch | | On Setting | Off Setting |
|---|---|---|---|
| 1. | Speed | 1000 Mbps | 100 Mbps |
| 2. | Duplex | Auto | Full Duplex |
| 3. | LFP (Link Failure Propagation) | Enabled | Disabled |
| 4. | Mode 1 | Use mode 2 | V - Line mode |
| 5. | Mode 2 | Aggregate mode | Breakout mode |
| 6. | Bidirectional allowed for port C | Enabled | Disabled |
| 7. | Bidirectional allowed for port D | Enabled | Disabled |
| 8. | Controller Module Present | Yes (Controller Managed) | No (Portable Only) |

**Table 1:** Switch Legend

**Note:** The power LEDs on the rear of the Portable chassis will NOT light when power applied. This is a known issue in the VLine module but does not affect operation.

# Specifications and Safety

C

| |  Portable Chassis |  1U Chassis |  2U Chassis |
|---|---|---|---|
| **Module slots** | 1 | 4 | 12 |
| **Expansion slots** | 0 | 1 | 3 |
| **Dimensions (W x H x D)** | 5.8in x 1.8in x 7.5in<br>14.7cm x 4.6cm x 19.1cm | 17.33in x 1.73in x 12.44in<br>44.05cm x 4.4cm x 31.63cm | 17.33in x 3.46in x 12.44in<br>44.02cm x 8.80cm x 31.60cm |
| **Weight** | 1.4 lbs<br>0.6 kg | 7.0 lbs<br>3.2 kg | 8.7 lbs<br>3.9 kg |
| **Operating temperature** | +32°F to +104°F<br>0°C to +40°C | +32°F to +104°F<br>0°C to +40°C | +32°F to +104°F<br>0°C to +40°C |
| **Storage temperature** | -4°C to +158°F<br>-20°C to +70°C | -4°C to +158°F<br>-20°C to +70°C | -4°C to +158°F<br>-20°C to +70°C |
| **Voltage (AC/DC)** | 85V – 264V AC<br>7V – 60V DC | 85V – 264V AC<br>36V – 72V DC | 85V – 264V AC<br>36V – 72V DC |
| **Current (nominal)** | 1.25 @ 12VDC | 0.22 A @ 230 VAC<br>0.44A @ 110 VAC<br>1.5A @ 50 VDC | 6A @ 115 VAC<br>3A @ 230 VAC<br>1.5A @ 50 VDC |
| **Max power consumption** | 7 Watts | 50 Watts | 100 Watts |
| **Mean time between failure (MTBF)** | 465,000+ hours | 465,000+ hours | 465,000+ hours |

Specifications are subject to change without notice.

## Safety information

Document reference symbol. If the product is marked with this symbol, refer to the product documentation to get more information about the product.

| | |
|---|---|
| WARNING | A WARNING in the documentation denoted a hazard that can cause injury or death. |
| CAUTION | A CAUTION in the documentation denotes a hazard that can damage equipment. |

Do not proceed beyond WARNING or CAUTION notices until the hazardous conditions are understood and appropriate steps have been taken.

### Grounding

There must be an interruptible safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that protection has been impaired, disconnect the power cord until the ground has been restored.

### Servicing

There are no user-serviceable parts inside this product. Any servicing, adjustment, maintenance or repair must be performed only by service-trained personnel.

# D

# Module Features Matrix

Network Critical provide three module types for the SmartNA System: Breakout/Aggregation/Regeneration Modules, Backplane Aggregation Modules and Filtering Modules. Each type supports a variety of physical interfaces and therefore has various capabilities and limitations due to the hardware. The following table lists the models (port combinations) that are available for each module type and shows the features each supports.

| | | A&B Ports | | | C&D Ports | | Port Role Capabilities | | | | | | Module Capabilities | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 10/100/1000Base-T | 1000Base-SX | 1000Base-LX | 10/100/1000Base-T | SFP Slot | A&B TAP Pair | A/B SPAN Input | A/B Monitor | C&D TAP Pair | C/D SPAN Input | C/D Monitor | Custom Port Maps | Backplane Aggregation | Backplane Filtering | VLine Bypass |
| Bre/Agg/Reg Modules | SNAM-RJRJ2 | ● | | | ● | | ● | ● | ● | ● | ● | ● | ● | | | |
| | SNAM-RJSF2 | ● | | | | ● | ● | | | | ● | ● | ● | | | |
| | SNAM-MCRJ2 | | ● | | ● | | ● | | | ● | ● | ● | ● | | | |
| | SNAM-MCSF2 | | ● | | | ● | ● | | | | ● | ● | ● | | | |
| | SNAM-SCRJ2 | | | ● | ● | | ● | | | ● | ● | ● | ● | | | |
| | SNAM-SCSF2 | | | ● | | ● | ● | | | | ● | ● | ● | | | |
| Backplane Aggregation Modules | SNAM-RJRJ4 | ● | | | ● | | ● | ● | ● | ● | ● | ● | ● | ● | | |
| | SNAM-RJSF4 | ● | | | | ● | ● | ● | ● | | ● | ● | ● | ● | | |
| | SNAM-MCRJ4 | | ● | | ● | | ● | | | ● | ● | ● | ● | ● | | |
| | SNAM-MCSF4 | | ● | | | ● | ● | | | | ● | ● | ● | ● | | |
| | SNAM-MPRJ4 | | ● | | ● | | | ● | ● | ● | ● | ● | ● | ● | | |
| | SNAM-MPSF4 | | ● | | | ● | | ● | ● | | ● | ● | ● | ● | | |
| | SNAM-SCRJ4 | | | ● | ● | | ● | | | ● | ● | ● | ● | ● | | |
| | SNAM-SCSF4 | | | ● | | ● | ● | | | | ● | ● | ● | ● | | |
| | SNAM-SPRJ4 | | | ● | ● | | | ● | ● | ● | ● | ● | ● | ● | | |
| | SNAM-SPSF4 | | | ● | | ● | | ● | ● | | ● | ● | ● | ● | | |
| Backplane Filtering Modules | SNAM-RJRJ6 | ● | | | ● | | ● | ● | ● | ● | ● | ● | ● | ● | ● | |
| | SNAM-RJSF6 | ● | | | | ● | ● | ● | ● | | ● | ● | ● | ● | ● | |
| | SNAM-MCRJ6 | | ● | | ● | | ● | | | ● | ● | ● | ● | ● | ● | |
| | SNAM-MCSF6 | | ● | | | ● | ● | | | | ● | ● | ● | ● | ● | |
| | SNAM-MPRJ6 | | ● | | ● | | | ● | ● | ● | ● | ● | ● | ● | ● | |
| | SNAM-MPSF6 | | ● | | | ● | | ● | ● | | ● | ● | ● | ● | ● | |
| | SNAM-SCRJ6 | | | ● | ● | | ● | | | ● | ● | ● | ● | ● | ● | |
| | SNAM-SCSF6 | | | ● | | ● | ● | | | | ● | ● | ● | ● | ● | |
| | SNAM-SPRJ6 | | | ● | ● | | | ● | ● | ● | ● | ● | ● | ● | ● | |
| | SNAM-SPSF6 | | | ● | | ● | | ● | ● | | ● | ● | ● | ● | ● | |
| VLine Modules | SNAM-RJRJV | ● | | | ● | | ● | | ● | | | ● | | | | ● |
| | SNAM-RJSFV | ● | | | | ● | ● | | ● | | | ● | | | | ● |
| | SNAM-MSRJV | | ● | | ● | | ● | | ● | | | ● | | | | ● |
| | SNAM-MSSFV | | ● | | | ● | ● | | ● | | | ● | | | | ● |
| | SNAM-SSRJV | | | ● | ● | | ● | | ● | | | ● | | | | ● |
| | SNAM-SSSFV | | | ● | | ● | ● | | ● | | | ● | | | | ● |

# Hardware Warranty

E

Subject to the provisions described below, this NETWORK CRITICAL SOLUTIONS product is protected for one (1) year from date of purchase against defect in material and workmanship.

Should a product fail to perform as described above within the warranted period, it will be repaired or replaced with the same or functionally equivalent product by NETWORK CRITICAL SOLUTIONS, at its discretion, free of charge provided you: (1) return the product to a NETWORK CRITICAL SOLUTIONS designated repair facility with shipping charge prepaid, and (2) provide NETWORK CRITICAL SOLUTIONS with proof of the original date of purchase. Repaired or replacement products will be returned to you with shipping charges prepaid.

Replacement products may be refurbished or contain refurbished materials. If NETWORK CRITICAL SOLUTIONS, by its sole determination, is unable to repair or replace the defective product, it will refund the depreciated purchase price of the product.

This warranty does not apply if, in the judgement of NETWORK CRITICAL SOLUTIONS, the product fails due to damage from shipment, handling, storage, accident, abuse or misuse, or if it has been used or maintained in a manner not conforming to the product manual instructions, has been modified in any way, or has had any serial number removed or defaced. Repair by anyone other than NETWORK CRITICAL SOLUTIONS or an approved agent will void this warranty. The maximum liability of NETWORK CRITICAL SOLUTIONS under this warranty is limited to the purchase price of the product covered by the warranty.

Prior to returning any defective product, the end customer or the reseller from whom the end customer originally purchased the product must obtain a Return Materials Authorisation (RMA) number from NETWORK CRITICAL SOLUTIONS. All defective products should be returned to NETWORK CRITICAL SOLUTIONS with shipping charges prepaid. NETWORK CRITICAL SOLUTIONS will not accept collect shipments.

Except as specifically provided in this agreement or as required by law, the warranties and remedies stated above are exclusive and in lieu of all others, oral or written, express or implied. Any or all other warranties, including implied warranties of merchantability, fitness for a particular purpose and non-infringement of third party rights are expressly excluded. NETWORK CRITICAL SOLUTIONS shall not under any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use or malfunction of the product, loss of profits or revenues or costs of replacement goods, even if NETWORK CRITICAL SOLUTIONS is informed in advance of the possibility of such damages.

# Contacting Technical Support

F

For additional assistance with the Smart Network Access System, please contact one of our Technical Customer Support Centers:

| **European Support Center** | |
|---|---|
| **Phone** | +44 (0)118 954 3210 |

| **North and South American Support Center** | |
|---|---|
| **Phone** | (716) 558-7280 |

| **On the web** |
|---|
| http://www.networkcritical.com/support |