



Masking Shunt

MS-100SC

<http://www.maskingnetworks.com>

Installation Guide

DEVICE OVERVIEW	2
OPERATING ENVIRONMENT	4
INSTALLATION	7
DETAILED OPERATION	15
TROUBLESHOOTING AND MAINTENANCE	18

Section 1

Device Overview

Introduction

This section describes the basic functionality of the masking shunt (hereafter referred to as the MS-100SC) and the items included with the packaging.

About the MS-100SC

The MS-100SC delivers enhanced network security in a reliable security appliance. The MS-100SC has two modes of operation, masking mode and cascade mode as follows:

Masking Mode

In masking mode, the MS-100SC acts by cloaking a firewall and rendering it invisible on the Ethernet level (Layer2 on the ISO stack). As the MS-100SC and the firewall cannot be detected on a network, they are not open to a direct attack. The MS-100SC also performs sanity checks on the firewall, raising an alarm if traffic stops flowing through the firewall.

Cascade Mode

In cascade mode, the device provides a redundancy switch over function, routing traffic to an alternative network. In this mode, one of the device ports can be used for the transparent monitoring of traffic.

Features of the MS-100SC

The MS-100SC has the following key features:

- It provides an extra level of security to help prevent unwanted discovery of local area networks for the purpose of spying or hacking.
- It continuously checks if the firewall is passing traffic correctly and raises an alarm if it is not.
- It is implemented mainly in hardware and it has no operating system. The internal functioning of the device cannot be compromised from the network.
- On firewall or equipment failure, it generates an alarm condition that can be used to prompt the switch over to an alternative network.
- It uses low cost fibre optical interface connectors (Duplex SC connectors).
- It has a universal voltage integrated power supply.

Check Items Included

Check that you have the following items:

- MS-100SC chassis
- Power cord
- OOBM cable
- Manual

Section 2

Operating Environment

Introduction

This section covers safety and compliance, and details of the required operating environment.

Compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. There is no guarantee that interference will not occur in a particular installation. However, if this equipment does cause harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Note: Modifications not expressly approved by Masking Networks Inc. could void the FCC approval and remove your authority to operate this product.

Safety

Please note the following important safety points:

- The socket outlet shall be installed near the equipment and shall be easily accessible.
- Only connect the unit to AC supply voltages in the range 100VAC to 250VAC.
- This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitable ground conductor.
- The cover panel prevents exposure to hazardous voltages and currents. It also shields electromagnetic interference (EMI) that might disrupt other equipment. Do not operate the equipment without the cover in place.
- To avoid electric shock, do not connect the OOBM ports (see diagram in Section 3) to the telephone network. These ports are Safety Extra Low Voltage (SELV) ports and are not suitable for connection to Telephone Network Voltages (TNV).
- Invisible laser radiation is present. Do not stare into the beam or view it directly with optical instruments.

Technical Specification

Table 1 Technical Specification

Parameter	Values
Dimensions	481 x 180 x 44mm (WxDxH)
Weight	2.4 Kg (Net Weight)
Temperature	Operating: 0° to +45°C Storage: 0° to +60°C
Humidity	5-90% non-condensing
Power	Supply voltage: 100 - 250VAC, 50-440Hz Maximum current: 1A Power consumption: 20 Watts
Standards	Ethernet standard: IEEE 802.3u 100Base-FX full duplex. Safety standard: Complies to relevant parts of UL 1950 3 rd Edition and IEC 60950 EMI Standard: FCC Part 15 Class B
Interfaces	Ethernet ports: Four 100Base-FX: SC multi-mode full duplex Management ports: Two OOBM (out of band management) ports- 4-pin RJ type connectors. (Polarity insensitive signaling using the two outer pins only.)
Fibre Optic	1310nm multi-mode fibre

Section 3

Installation

Introduction

This section describes the procedure to follow to install the device in mask or full cascade mode.

Front Panel Description

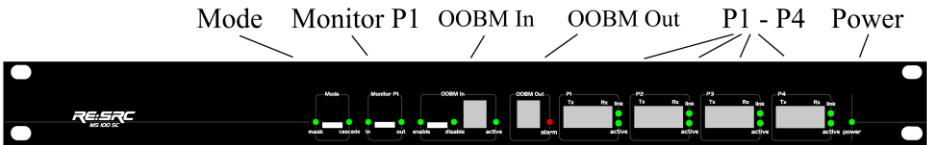


Figure 1 - Front Panel

Table 2 - Front Panel Description

Panel Part	Description	Notes
Mode switch	This switch selects whether the MS-100SC is in mask mode or cascade mode. The LEDs indicate which mode has been selected.	Care should be exercised with this switch as the firewall can be bypassed if it is in the wrong state.
Monitor P1	In cascade mode (only) this switch selects the Port 1 traffic direction to monitor. This data stream is then replicated out to Port 2.	The LEDs indicate which direction has been selected.

OOBM In	<p>In cascade mode (only) this switch enables or disables the Out Of Band Monitoring (OOBM) input. Two LEDs indicate whether OOBM is enabled or disabled.</p> <p>The OOBM In connector is a 4 pin RJ-14* type socket used to transport alarms into the unit.</p>	<p>In cascade mode a signal on the OOBM In port will cause the MS-100SC to switch to the back up network, and the active LED to illuminate.</p>
OOBM Out	<p>The OOBM Out connector is a 4-pin RJ-14 type socket used to transport alarms out of the unit.</p>	
P1-P4	<p>These are optical fibre interfaces running at 100Mbit/s (IEEE802 -100Base-FX). They use Low Cost Fibre Optical Interface Connectors (Duplex SC connectors) with 1300nm multimode fiber. Only full duplex mode is supported.</p>	<p>The link LED illuminates when the port has a valid optical connection.</p> <p>The active LED is on whenever there is data on transmit or receive fibres.</p>
Power	<p>This LED illuminates when the unit is turned on and is receiving power.</p>	

*RJ-14 - Telephone **handset** connector plug

Before Installation

Before installation, check that you have the required number of optical leads (four for mask mode and ten for cascade mode). The MS-100SC optical ports use SC connectors.

Notes:

1. Connecting the masking shunt into a network requires the network to be taken off line briefly, so this should be done at a time of minimal traffic.
2. For the device to be effective the firewall must not reveal its MAC address to higher-level queries

Single Unit in Mask Mode

A single unit in mask mode is used for networks with a single firewall and no redundancy. If the network uses UPS devices to ensure continuous power, then the masking shunt should be powered from the same UPS as the firewall.

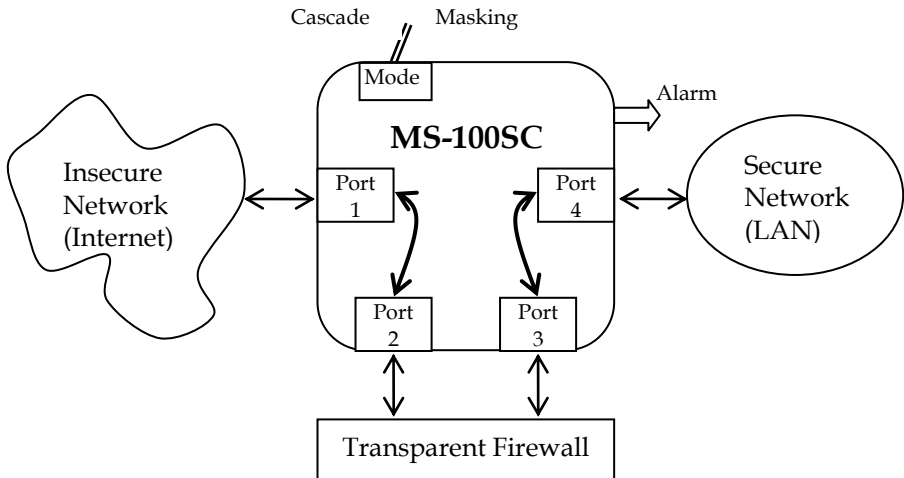


Figure 2 - Mask Mode Configuration

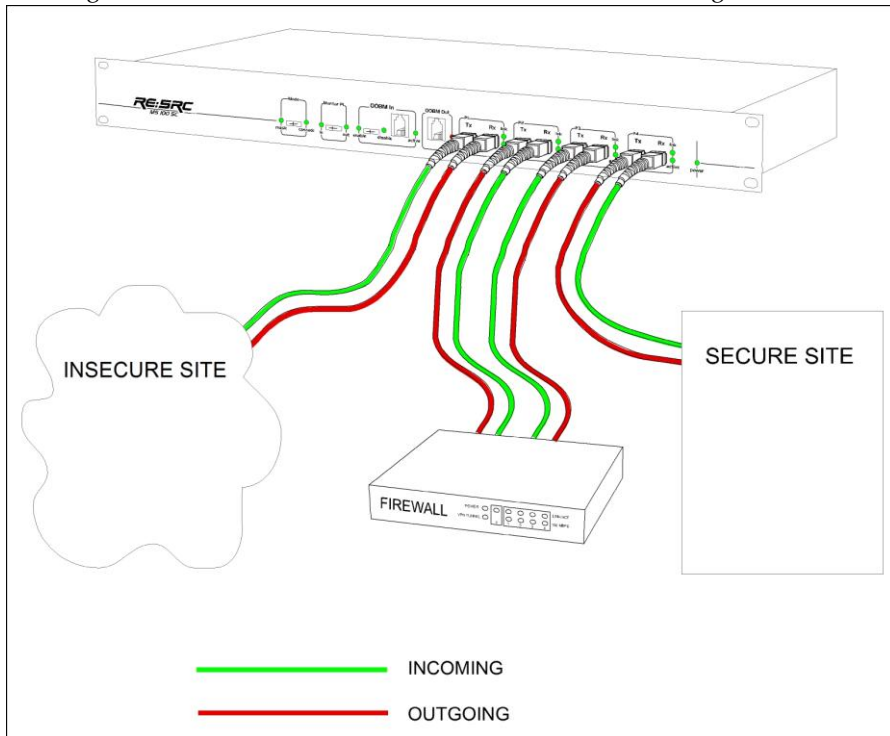


Figure 3 - Mask Mode Configuration

Table 3 Mask Mode Installation

Step	Action
1.	Connect the unit up as in Figure 2 with: <ul style="list-style-type: none"> • The insecure (Internet) connection going to Port 1 of the MS-100SC. • Port 2 connected to the insecure side of the firewall • Port 3 connected to the secure side of the firewall. • Port 4 connected to the protected network.
2.	Ensure the mode switch is in mask mode by checking that the mask mode LED is on.
3.	Configure the firewall to pass the ICMP sanity check packet from IP address 10.0.1.1 to 10.0.0.1. This is for a packet from port 3 to port 2. This is required so that the MS-100SC can send check packets through the firewall if needed. Refer to your firewall's setup guide for help on configuring this.
4.	Configure the firewall so that it does not give out the MAC address to higher-level queries. Refer to your firewall's technical set up instructions for this procedure.
5.	Turn the power on to the device and send some traffic through the system in both directions, for example a ping command from each direction. The first packet in each direction is discarded- it is used by the device to learn the MAC addresses of connected devices.
6.	When a continuous stream of traffic is present, all the port LEDs should be on. When no traffic is present after the device has been running traffic through ports 1, 2 & 3, active LEDs will flash every second as the device checks that the firewall is still passing traffic.
7.	The alarm LED should be off initially. Unplug a Tx connection on port 2 or 3 to simulate a dead firewall condition. The alarm LED will illuminate.

Note:

The MS-100SC must learn the MAC address of the firewall so it is able to send monitoring packets through the attached firewall. This is done by sending traffic through the firewall in both directions. If the firewall, network cards or other security devices are changed or repaired, step 5 must be repeated to ensure that the MS-100SC has the correct MAC address.

A Full Cascade

A full cascade can be used for networks with two or more firewalls in a redundant configuration. Two MS-100SCs are used to mask the two firewalls. A third MSC100SC is used to route traffic to a backup firewall if there is a failure to the primary firewall. Loss of power to one of the MS-100SC devices in mask mode will generate an alarm, causing the unit in cascade mode to switch to the redundant network.

Note: For this functionality to be effective, the masking shunts should be connected to a UPS supply. A unit in cascade mode will not pass traffic if it loses power.

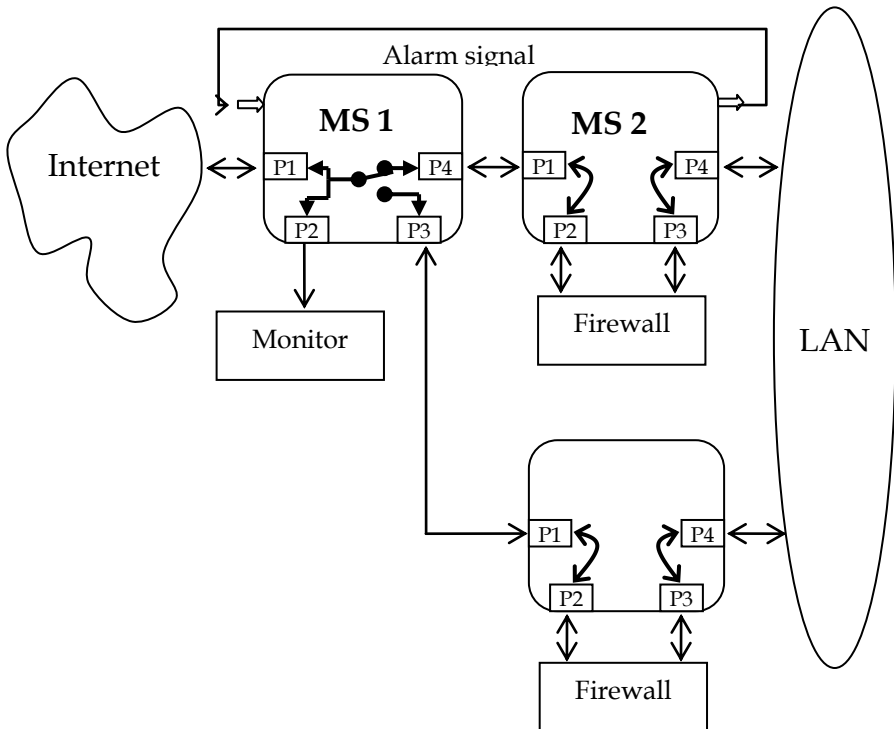


Figure 4 - Full Cascade System Diagram

Table 4 Cascade Mode Installation

Step	Action
1.	Connect up and configure the two units around the firewalls in mask mode (MS 2 and MS 3 in Figure 4). Follow the same procedure as for a single unit in mask mode. Check that each unit passes traffic and generates an alarm if a firewall connection is broken.
2.	When MS 2 and MS 3 are working in mask mode, connect in the cascade unit (MS 1). Port 4 of the cascade unit is the default port. Connect the primary network MS 2, Port 1 to Port 4 of MS 1. Port 3 of the cascade unit is the backup port. Connect the backup network MS 3, Port 1 to Port 3 of MS 1. Port 1 of the cascade unit is connected to the insecure network (internet).
3.	Ensure that the cascade unit is in cascade mode and that the OOBM In is disabled, by checking the front panel LEDs of the cascade device MS 1.
4.	Turn the power on and send some traffic through the cascade unit from the primary network.
5.	Switch the OOBM In switch to enable and check that the alternative network is on line. (The OOBM In active LED will also be on.)
6.	Connect the OOBM cable from the primary network device OOBM Out to the cascade device OOBM In . (This will extinguish the OOBM In active LED and divert traffic back to the primary network.) The system is now functional.
7.	To monitor the traffic, connect a monitoring device to Port 2 of MS 1 and configure the Monitor P1 switch to the direction to be monitored. The In and Out LEDs indicate the direction of the traffic from Port 1 to the monitor port, Port 2. The interface on the monitoring device must be set to promiscuous mode.

Section 4

Detailed Operation

Introduction

This section provides further detail on the mask and cascade modes of operation. The current mode of operation for a device is indicated by the LEDs on the front panel.

Mask Mode

The MS-100SC can be used to hide other network devices which are connected to it. It does this by ensuring that each outgoing Ethernet frame has a MAC originating address consistent with the MAC originating address of the corresponding received frame. Any monitoring equipment or firewall that inserts its own originating MAC address has it substituted with one of the set of valid MAC addresses from the originating area, making the equipment invisible at the data link layer (MAC level).

If there is no traffic out of a connected firewall (towards the Internet) in a period of 500ms, the MS-100SC sends a packet through the firewall (from Port 3 to Port 2). If nothing is received in the next 100ms period, the device sends a second packet. This is repeated five times at 100ms intervals. If there has been no traffic or test packet through the firewall for one second, then the alarm is raised. If three first attempt pings are received in a row, the firewall is considered to be functioning. Successfully detected test packets are corrupted and are discarded by the network devices. To prevent rapid toggling of the alarm, it is prevented from changing state within a period of five seconds.

Note: The device does not check traffic from the opposite direction.

The format of the test packet is a standard ICMP ping (protocol 1, type 8) with a random payload. The payload is constructed once for each burst (i.e. each of the 5 attempts will be the same). The address fields used in the ping are as follows:

- The destination MAC address is set to the most recent source address received on Port 3.
- The source MAC address is set to the most recent destination MAC address received on Port 3. (This may be the broadcast address.)
- The source IP address is set to 10.0.1.1 for the Port 3 to Port 2 direction.
- The destination IP address is set to 10.0.0.1 for the Port 3 Port 2 direction.

The test packet from Port 3 to Port 2 is an ICMP ping from 10.0.1.1 to 10.0.0.1. For firewall detection to work, the firewall must be configured in such a way to allow this packet to pass. Also, the MS-100SC must have first learned the MAC address of the firewall as per Step 5 of Mask Mode Installation.

Three LAN Network

A routing firewall in a three LAN network can be masked with the use of two MS-100SCs as detailed in Figure 6 below. The Masking Shunts will continue to hide the firewall's MAC address at the Ethernet frame level. From the point of view of the "world", all frames appear to come from LAN2 because shunt2 will modify the source MAC addresses in addition to shunt1. Both masking shunts check the firewall's sanity as per normal. During initialization all three LANs must transmit a packet toward the shunts before traffic will be allowed to flow.

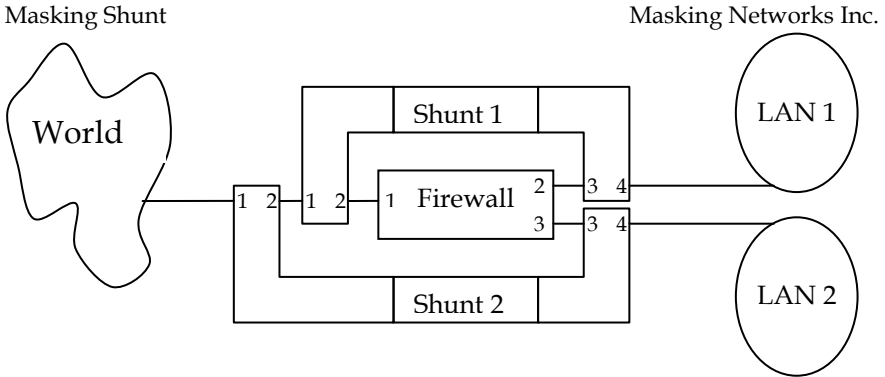


Figure 6 - Three LAN Topology

Cascade Mode

In cascade mode the routing of the traffic is performed in hardware, resulting in a very small traffic delay (less than 20ns). A switch over to an alternate network occurs if the Port 3 link is up and:

- The primary firewall stops passing traffic.
- The OOBM cable becomes disconnected.
- The primary firewall and associated shunt lose power.
- A primary firewall shunt optical Rx port connection is broken.

For the change over to occur the OOBM In switch must be set to disable. (This will cause a switch over independent of the state of the Port 3 link.)

Note: The switch over between networks is performed asynchronously, so a packet may be truncated during the switch over.

The monitor port has a traffic delay, but this is inconsequential, as the monitor port is not timing critical. The monitor port is designed to be unidirectional (out traffic only) so that there is no indication to users that they are being monitored.

Section 5

Troubleshooting and Maintenance

Introduction

This section provides information on troubleshooting the MS-100SC device. It also provides details on maintaining the device and running regular health checks.

Troubleshooting

Mask Mode

To check that a shunt device is operating correctly in mask mode, proceed as follows:

Table 5 Troubleshooting - Mask Mode

Step	Action
1.	Bypass the firewall by connecting Port 3 to Port 2 with a crossover cable.
2.	If it is possible to send through a ping from Port 1 to Port 4 or from Port 4 to Port 1, then the device is working correctly.
3.	With no traffic passing through, the firewall sanity check will cause the active LEDs on Ports 1, 2 and 3 to flash every 0.5 seconds.
4.	With the firewall present again (the crossover cable in 1. removed), look at Ports 1 and 4 using an Ethernet frame viewer to check that the MAC source address of the firewall does not appear as part of the Ethernet frame source address.

Cascade Mode

To check that a shunt is operating correctly in cascade mode, proceed as follows:

Table 6 Troubleshooting - Cascade Mode

Step	Action
1.	Send a ping through the device from Port 1 to Port 4 (or Port 3), using the OOBM In switch to control the path as follows: <ul style="list-style-type: none"> - Disable connects Port 1 to Port 4 - Enable connects Port 1 to Port 3, with no OOBM cable present.
2.	To check the monitor port: <ul style="list-style-type: none"> - Switch the Monitor P1 switch to Out - Take the Tx cable from Port 1 and plug it into Port 2. - Supply Port 2 with a valid Rx signal - Send a ping from Port 4 to Port 1 and check that it comes out of Port 2.

General Maintenance

In general this unit does not require maintenance and it has no batteries. However, it is suggested that the configuration settings are periodically checked, as part of routine network maintenance, to ensure that they are correct. A simulated firewall failure can be achieved by unplugging one of the primary firewall connections and checking that the switch over to the back up network works successfully.

Customer Support

For support with any aspect of the Masking shunt, please refer to the Masking Networks Masking Shunt website – <http://www.maskingnetworks.com>

Please check your question in the Frequently Asked Questions (FAQ) section on our website, before contact Masking Networks at +1 703-738-4550, or email inquiries@maskingnetworks.com

For sales enquiries, please call Masking Networks Inc., +1 703-738-4550.

Disclaimer

The specifications and information regarding the product in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of this product.

In no event shall Masking Networks or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation lost profits or loss or damage to data arising out of the use or inability to use this manual, even in a case where Masking Networks or its suppliers have been advised of the possibility of such damages.

The information contained in this document is proprietary to Masking Networks Inc., The information contained in this document shall not be reproduced, shown or disclosed without written permission.

Copyright

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalised. Masking Networks Inc. cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Revision History and Authorisation

Document Title	Masking Shunt Quick Start Guide
Author	Ian Howat
Authorised for Revision by	Masking Networks Inc.
File Name	MS100SC Installation Guide

Revision Number	Section	Date	Author	Remarks
1.0			Teltest	Initial release
1.1	2	10-12-03	Teltest	Changed power rating to match PSU CB certificate.
1.1	2	10-12-03	Teltest	Changed to FCC Class B.
1.1	4	10-12-03	Teltest	Added masking of a routing firewall in a 3 LAN topology.
1.2	5	01-08-05	Masking Networks	Contact detail update
1.3		01-03-08	Masking Networks	Contact detail update
1.4		20-01-10	Masking Networks	Contact detail update