



Key Features

- Layer 2 network masking
- Masks a single device or network segment
- Wire speed processing
- Easy Installation and configuration
- Full Network Compatibility

Masking Shunt MS-100SC



Securing your network in a borderless world:

Masking Networks offers hardware and software products that uniquely protect organizations from cyber-attacks at network Layers 2 and 3. These attacks include network mapping, traffic analysis across segments, denial of service, and spoofing. Network technology trends, such as cross-domain interoperability, switch-oriented topologies, virtualization, and cloud computing, are exposing organizations to Layer 2 threats throughout networks as they become “borderless.”

Do you need Network Masking?

The most urgent customer demand for network masking is driven by requirements to isolate and segment networks. Examples include government-contractor interfaces, industrial and IT networks, and places of converging network traffic. Business enterprise networks have similar segmentation compliance requirements, particularly for energy, finance and healthcare markets. Network masking prevents or greatly hinders node hopping, traffic analysis, and other vulnerabilities in these situations.

Layer 2 network masking includes masking the MAC address and network hop of the protected device at wire speed. The masked device operates as before without network reconfiguration.

The MS-100SC hides the Layer 2 identity and presence of an individual firewall, server or LAN segments. It maintains full network interoperability and performance and is easy to install and maintain. The MS-100SC is a quick-impact and cost effective response to current network security threats and policy mandates.

MS-100SC Operational Examples

Method of Attack	Attack Objective	MS-100SC Counter Measure
Nmap	Map network devices	Confuse results and prevents disclosure of MAC address / vendor ID
Man-in-Middle	Pose as key device	Foils attack & exposes attacker to detection
ARP Poisoning	Device spoofing	Creates additional layer of translation & exposes attacker to detection
Traceroute	Node map to target	MS-100SC and sub-net remain invisible

Network Operation and Compatibility:

The MS-100SC employs several proprietary techniques to mask devices while remaining invisible itself. It processes only address-related information without changing the data content part of the packet. The MS-100SC:

- Installs in-line with the firewall, critical host or other device it is masking.
- Dynamically generates proxy MAC addresses and ARP responses.
- Operates at the electrical signal level with virtually no latency.
- Does not have a MAC address and is not detectable on the network.
- Is compatible with encrypted communication because it does not process encrypted packet content.
- Is compatible with IPv4 and IPv6.