

## Masking Shunt MS-100SC Frequently Asked Questions

---

### 1. What exactly does the Masking Shunt MS-100SC do?

The MS-100SC is a network masking device that makes another network device “invisible” from detection at Layer 2. It operates by replacing the source MAC address with a proxy and masking the segment hop associated with the device. It is typically used to mask a network’s host, firewall, critical node, or subnet LAN. Defense in Depth is achieved by limiting session and network segment information from discovery by hackers and intruders seeking to map and exploit networks.

NAT (Network Address Translation) for IP addresses is an analogous Layer 3 network masking technique. The new MS 200 product family will deploy an advanced NAT technique for Layer 3 level protection.

### 2. Aren’t firewalls sufficient without Masking Shunt?

Firewalls today need added protection because the intruders’ techniques have advanced. Firewalls block only some methods intruders use to get into your network and they do not block intruders from attacking the firewall itself. Masking Shunt provides faulty intelligence to prevent intruders from identifying the firewall thus making it difficult for them to attack it. Intruders will generally be forced to apply techniques that take much longer to succeed or are more prone to detection.

### 3. How can Masking Shunt operate without breaking any protocols?

Masking Shunt deploys several proprietary techniques to mask devices it is protecting and to remain invisible itself. It only processes address related information without changing the data content part of the packet. The process has a precedent in how NAT allowed for more Internet addresses under IPv4.

### 4. What about ARP, NetBIOS, and other protocols that gain access to MAC address and IP address through higher protocol or encapsulated protocols?

Masking Shunt processes all ARP, NetBIOS packets to replace their source MAC address and processes all packet headers and content for source IP addresses. Masking Shunt does not process any encrypted packet contents and will not interfere with encrypted communication.

### 5. How do I know intruders won’t be able to get around the MS-100SC?

There is no known way to discover or detect a Masking Shunt MS-100SC. It is a programmable ASIC-based device with very minimal configuration. It can only be reprogrammed through the console port/switch and cannot be discovered or addressed over the network.

## 6. Why do I need MAC address (OSI layer 2) protection?

The MAC address can be decoded to reveal the hardware vendor code and model related information. Knowing this reveals hardware and possible software application information for hackers and intruders to exploit.

## 7. Why do I need Masking Shunt when I have NAT, PAT in place?

Masking Shunt provides MAC address protection and various added security benefits. With the introduction of IPv6, NAT/PAT will no longer be needed as there will be more than enough IP addresses available. Masking Shunt provides far greater protection than simply relying on NAT/PAT.

## 8. What about IPv6?

The new MS 200 product line is designed to work with IPv4 to offer additional functionality with IPv6. Some DHCP IPv6 addresses are generated based on MAC addresses and with Masking Shunt this would not contain any original MAC address on the IPv6 address. Because some random IP address generation (DHCP) is assigned based on MAC addresses, MS 200 generated proxy MAC addresses will reduce the slight chance of being able to identify a device via its IP address directly. Also, because under IPv6 there will not be a need for Network Address Translation (NAT) the specialized NAT provided by the MS 200 will be an added value.

## 9. My network is switch based so I'm OK.

It is a mistake to think that switched networks are immune from these attack methodologies which plague older networks. For more information, refer to the SANS Institute document "Intrusion Detection FAQ - Why Your Switched Network Isn't Secure," which may be obtained from the [www.sans.org](http://www.sans.org) website. The author examines attack methodologies such as ARP Spoofing, MAC Spoofing and MAC Duplicating and concludes:

*"I believe this examination provides another justification for 'defense-in-depth'. Networks are an infrastructure enabler for us to perform our daily functions. The general networks we use were never meant to be used as a security feature; although, they continue to be used in this manner. Providing a managed network infrastructure is a key component of any good defensive position. While compromising a single host may gain the attacker access to a few systems, the ability to sniff userids and passwords for several machines will effectively give away the keys to the kingdom. Network managers must be aware that they have 2 realistic options. They can either manage the network appropriately in order be part of the team trying to protect the environment, or they can configure the environment so that it is 'hands-off' or 'self-maintaining' which, traditionally, translates into lax security."*

*Continued on following page:*

---

## 10. Does the Masking Shunt break IPSEC?

Masking Shunt technology deals with the IP header and the Ethernet frame. The Masking Shunt never examines the payload where IPSEC functions. From RFC2402:

*"AH provides authentication for as much of the IP header as possible, as well as for next level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus the protection provided to the IP header by AH is piecemeal."*

This is where such information as the destination address, MAC address of the sender, TTL, Hop and CRC are kept. Information relating to the "real" purpose of the packet is encrypted in the IPSEC protocol and accordingly will not be affected by Masking Shunt.

## 11. Can the Masking Shunt be used with a VPN?

Yes. The Generic Route Encapsulation (GRE) protocol is used in conjunction with Point-to-Point Tunneling Protocol (PPTP) to create virtual private networks (VPNs) between clients or between clients and servers.

According to RFC2784, as GRE still requires the normal frame structure, it is encapsulated in a region not even examined by the Masking Shunt.

*"Structure of a GRE Encapsulated Packet*

*A GRE encapsulated packet has the form:*

*Delivery Header - GRE Header - Payload packet*

*This specification is generally concerned with the structure of the GRE header, although special consideration is given to some of the issues surrounding IPv4 payloads."*

Accordingly the delivery header containing the destination, MAC address, hop, TTL, and CRC are left intact by GRE.