

SNMP Payload Translation

*By Les Biffle
Network Safety Corporation*

Version 1.0

12 February 1998

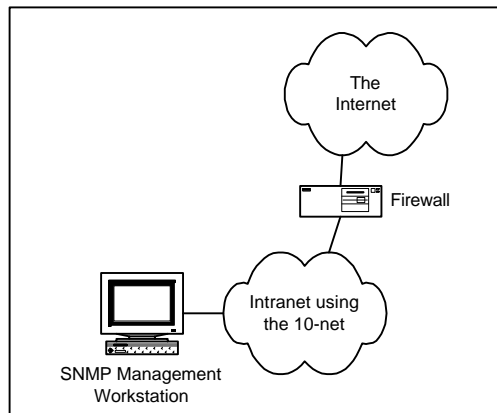
Table of Contents

Section 1	--..... The Problem	1-1
	MANAGEMENT OF A PRIVATE NETWORK.....	1-1
	THIRD PARTY MANAGEMENT.....	1-2
	CUSTOMER-SITE NMS.....	1-3
Section 2	--..... The Solution	2-1
	NETNAT MANAGEMENT.....	2-1
	SINGLE NETNAT FIREWALL.....	2-2
Section 3	--..... The Technology	3-1
	NETWORK ADDRESS TRANSLATION.....	3-1
	THE SNMP PAYLOAD.....	3-1
	<i>Example Object Identifiers</i>	3-1
	NETNAT SNMP RULES.....	3-2
	<i>The at Group</i>	3-2
	<i>The ip Group</i>	3-2
	<i>Other Groups</i>	3-2
	THE SNMPLIST FILE.....	3-3
	OPERATION.....	3-4
	<i>Subnet Mapping Mode 3</i>	3-4
	<i>Public to Private</i>	3-4
	<i>Private to Public</i>	3-4
	<i>Firewall Functionality</i>	3-4

Section 1 -- The Problem

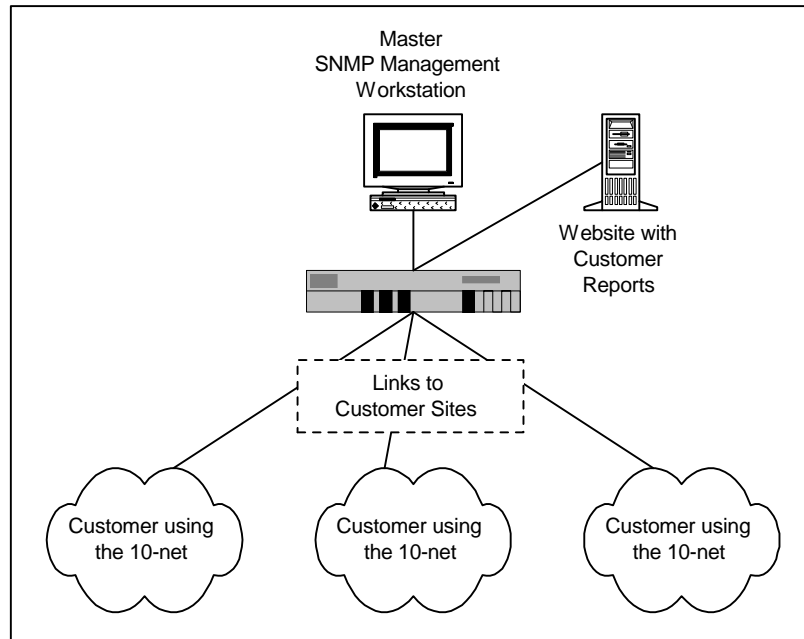
Management of a Private Network

A corporate Intranet using private addressing may be managed from within with a traditional network management station. There is no real difference between managing a network composed of private addresses and one using public addresses. This diagram shows a typical network with this arrangement. The corporate network uses the 10-net instead of registered addresses, although the drawing would be just as accurate with registered public addresses.



Third Party Management

When a third party is contracted to perform complete network management, the issues get more complex. It is very likely that more than one of their customers are using private addressing in their corporate networks. This presents a real problem for the third party manager, since, in IP routing, there cannot be more than one visible network with the same set of addresses.

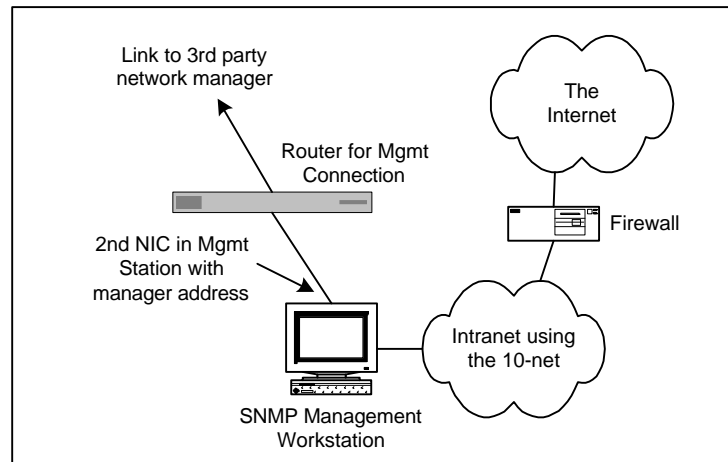


This drawing shows a network that **can't work**. The third party management firm's router cannot have links to more than one independent network with the same addresses being used in each. Traditional Network Address Translation can be used to hide the network addresses that the three example customer nets are using, except that the contents of SNMP packets will reveal those network addresses and result in confusion within the Master NMS and associated reporting systems.

The next section discusses the techniques normally employed to handle this network situation.

Customer-Site NMS

In order that the customer addresses be hidden from the network of the third party manager, a network management station must be placed at each customer's site to deal with that customer network. A second network card must be installed in the NMS and a new network created with addresses from the third party manager's network. A router with a link to the manager's network completes the connection, allowing the manager to access the information gathered by the customer-site NMS.



In this configuration, the customer-site-located NMS will handle all network discovery functions, gather SNMP traps, and perform network management duties via a remote-control utility run from the third party manager's site. Information will be retrieved from the NMS for report preparation via FTP or another file transfer mechanism.

This certainly handles the network management requirements, but it really complicates the job, and runs up the costs for hardware and licenses. It would be far more natural to have a Master NMS at the third party manager's site, let it handle all customers' networks and eliminate the network management stations from the customers' sites with the associated complication and costs.

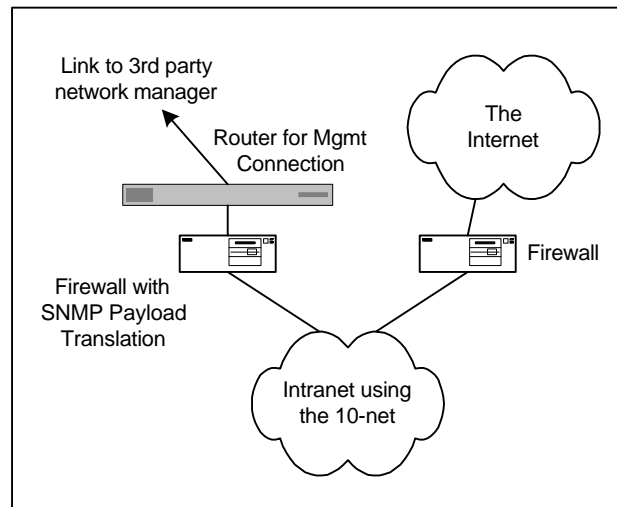
Section 2 -- The Solution

NetNAT Management

A NetNAT Firewall with SNMP Payload Translation at each customer site provides a number of useful solutions. First, it completely translates the customers' addresses into other sets of addresses, so that a Master NMS may be used to manage the sites directly. All NMS functions, including network discovery would be possible. Reports that are prepared for the customers are translated back into the customers' addresses by the reporting system.

The second benefit is that a powerful firewall is now between the customers' sites and the third party network, limiting access by the third party manager to just the network management functions.

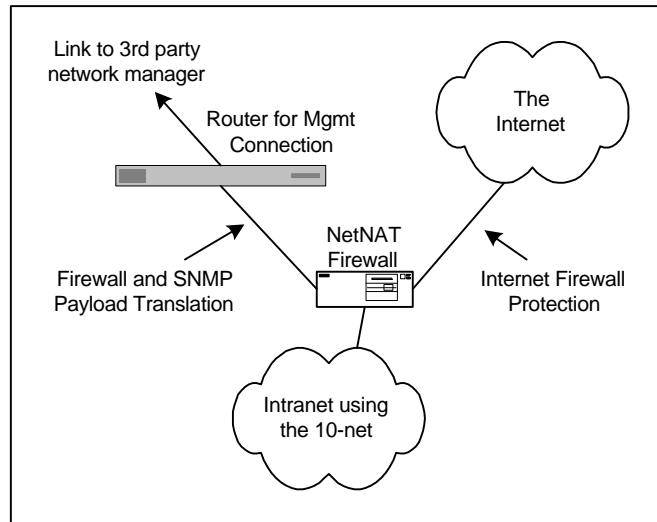
The customer network is now visible to the third party NMS, but just for management functions, and as a different network number than the actual private network. The third party network is now visible to the customer for Web access to reports prepared on their behalf.



The drawing above shows the NetNAT Firewall along side a customer Internet Firewall, which may be a NetNAT as well. The alternative, when the customer does not as yet have an Internet Firewall, is shown in the next section.

Single NetNAT Firewall

When the customer does not have a firewall, or is dissatisfied with an existing firewall, our NetNAT Firewall can solve both problems at a price far less than any competitive solution, and with fewer boxes to administer. Configured with two public interfaces, a single NetNAT may perform SNMP Payload Translation for the third party management link and powerful Internet Firewall duty for the Internet link.



This configuration needs a bit of explanation, as no other Firewall product offers a similar set of options.

The various service mapping options of the NetNAT are associated with a specific public interface, so configuring subnet mapping mode 3 on the first public interface (that looks toward the third party network manager) does not weaken the firewall functions on the public interface that looks toward the Internet. The NetNAT has a default route toward the Internet via the second public interface, and a static route to the third party network manager's network via the first.

Section 3 -- The Technology

Network Address Translation

Network Address Translation (NAT) and the concept of Private Addressing were invented by Network Safety Corporation in 1993 and submitted as an RFC in October of 1993, but the RFC was declined as frivolous and useless. Needless to say, things have changed since then.

NAT is comprised of a number of mechanisms that conceal the internal IP Addressing policies, the number of internal computers and the topology of the internal network. Depending upon the application, the NAT mechanism may be very simple or very tricky. The simple mechanisms involve simply modifying the IP Addresses in the IP header. The more-difficult ones involve the interpretation of the data in the IP packet: the “payload” of the packet. Of the protocols that require payload translation, SNMP is one of the most tricky.

The SNMP Payload

The data carried in an SNMP packet is defined in RFC 1155. The information consists of combinations of items of various types, including items nested within structures that may in turn be nested within other structures. The data items are defined in a formal language called ASN.1 (for Abstract Syntax Notation 1) and encoded using BER (Basic Encoding Rules), which are discussed in Chapter 8 of *The Open Book: A Practical Perspective on OSI*, by Marshall T. Rose (Prentice-Hall, 1990).

The NetNAT parses the BER-encoded SNMP data and searches for IP Address information in it. Some IP Address information is clearly labeled (like the “IpAddress” data type). Others are hidden as part of the name structure of an Object Identifier. To help the NetNAT locate these hidden addresses, a set of rules were defined to control the detection mechanism. These rules are contained in a user-modifiable file that the NetNAT processes on startup, to permit the addition of new rules without the need for programming changes.

Example Object Identifiers

The “object identifiers” are hierarchical strings that detail the path from the top of this defined structure to the actual data in the MIB (Management Information Base, see RFC 1213). The path is described by a sequence of decimal numbers separated by periods. A “1” implies the left-most path from a given spot, a “2” is the next to the right, etc. Each branch in this upside-down tree is also given a textual name. The MIB is actually six levels down the tree, starting at:

1.3.6.1.2.1, or iso.org.dod.internet.mgmt.mib.

Example object identifiers that contain hidden IP Address information are:

**1.3.6.1.2.1.3.2.1.1.207.86.17.101 -or-
1.3.6.1.2.1.6.13.1.1.207.86.17.101.110.192.168.31.31.2392**

Where the 207.86.17.101 and 192.168.31.31 are actually IP Addresses. Note the occurrence of two IP Addresses in the second example.

NetNAT SNMP Rules

The NetNAT's SNMP Payload Translation process uses a set of rules that detect parsed object identifiers that contain embedded IP Addresses. These rules use a combination of object length and content to detect items to be translated. Once a to-be-modified object is detected, the rules specify the start offsets for up to three embedded IP Addresses. These are isolated and translated using the NetNAT's normal translation mechanisms.

The at Group

The first example is the "at" group, which contains the address translation information used in mapping network card hardware address to IP Address. This is the table that the ARP process manipulates. All objects in this group that contain IP Addresses are 15 levels deep, start with 1.3.6.1.2.1.3, and have a single IP Address starting at level 12. The NetNAT SNMP rule for this group is therefore:

15,6,12,0,0,43,6,1,2,1,3

Where:

15	is the length of the entire object.
6	is the length of the initial, detectable contents.
12	is the level of the first embedded IP Address.
0	specifies the absence of a second embedded IP Address.
0	specifies the absence of a third embedded IP Address.
43	is a combination representing the initial 1.3 of the object identifier.
6,1,2,1,3	represents the 6-byte-long string (counting the previous byte of 43) that uniquely specifies this group of objects.

The ip Group

There are three branches of the ip group that have embedded IP Addresses. These are:

1.3.6.1.2.1.4.20.1	ip.ipAddrTable.ipAddrEntry
1.3.6.1.2.1.4.21.1	ip.ipRouteTable.ipRouteEntry
1.3.6.1.2.1.4.22.1	ip.ipNetToMediaTable.ipNetToMediaEntry

The first two are 13 levels in depth with an IP Address at level 10, while the third one is 14 levels deep with an IP Address at level 11. The rules that relate to these three objects are shown here. Refer to the field interpretation above when decoding these.

13,8,10,0,0,43,6,1,2,1,4,20,1

13,8,10,0,0,43,6,1,2,1,4,21,1

14,8,11,0,0,43,6,1,2,1,4,22,1

Other Groups

There are many other rules in the snmplist file, with more to be added in the future. Users that discover new objects with embedded IP Addresses where no rules exist in the standard rule set are encouraged to email this information to us. We are happy to assist you in the preparation of new rules.

The *SNMPLIST* File

Here is the content of the **snmplist** file that accompanies the NetNAT release as of 11 February 1998.

```
# Top of file
# All "at" group members
15,6,12,0,0,43,6,1,2,1,3
#
# ip.ipAddrTable.ipAddrEntry
13,8,10,0,0,43,6,1,2,1,4,20,1
#
# ip.ipRouteTable.ipRouteEntry
13,8,10,0,0,43,6,1,2,1,4,21,1
#
# ip.ipNetToMediaTable.ipNetToMediaEntry
14,8,11,0,0,43,6,1,2,1,4,22,1
#
# tcp.tcpConnTable.tcpConnEntry (Note two embedded addresses)
19,8,10,15,0,43,6,1,2,1,6,13,1
#
# udp.udpTable.udpEntry
14,8,10,0,0,43,6,1,2,1,7,5,1
#
# Cisco-specific 14.7.1, 14.8.1, 14.10.1
14,8,10,0,0,43,6,1,2,1,14,7,1
14,8,10,0,0,43,6,1,2,1,14,8,1
14,8,10,0,0,43,6,1,2,1,14,10,1
#
# Bottom of file
```

Operation

As in any NetNAT configuration, there is at least one Private Interface and at least one Public Interface. The "Private" side addresses are concealed from the view of computers on the "Public" side. Treatment of messages depends on the direction of travel of the message: public-to-private or private-to-public.

Subnet Mapping Mode 3

SNMP Payload Translation is enabled only in NetNAT Subnet Mapping Mode 3. See the NetNAT Product Guide for information on this configuration option. Mode 3 maps a private subnet into a same-sized public subnet, and enables two types of inbound accesses that are normally blocked by the firewall facility: inbound ping and SNMP messages for the purposes of network discovery and management. No other inbound messages are permitted, except those that are part of a client session initiated from the private side.

Public to Private

Messages travelling from the public to the private side are frequently referred to as "inbound" messages in our documentation. Subnet Mapping Mode 3 enables inbound ping requests, to permit network discovery by an SNMP management station on the public side. Also permitted are inbound SNMP requests. The SNMP requests are processed with our Payload Translation facility before being forwarded into the private network.

Private to Public

Messages from the private network are permitted to flow to the public side. Almost any Internet application will work from a client on the private side to a server in the public network. SNMP traps and replies are processed and translated with our Payload Translation facility.

Firewall Functionality

All NetNAT Firewall functionality is in operation in Subnet Mapping Mode 3, with the ping and SNMP exceptions described above. Please see the NetNAT Product Guide for additional configuration details.