TOTAL CONTROL™

# Network Management Card

## Version 4.0

## REFERENCE MANUAL

# Table of Contents

# What's New in this Release

This section briefly describes the new features supported by version 4.0 of the Network Management Card. Complete operational information may be found later in this manual, or as referenced.

- **Revised MIB Compilation Procedure**
  *Total Control Manager/SNMP* users who intend to use a MIB Browser must perform MIB compilation through the Novell *Network Management System*. The compilation steps have also been revised to reflect a MIB selection process. See the *Total Control Manager/SNMP Software Guide* for a description of this procedure.
- **ISDN**
  Management release 4.0 of the Total Control Network Management Card and the *Total Control Manager/SNMP* provide support for U.S. Robotics' PRI Access System.
- **New Card Management Support**
  Version 4.0 of the NMC supports additional levels of management for several cards, including the T1/E1 PRI and NETServer PRI gateway cards. New MIBs, includingIDS0 and IDT1, have been added to provide support for the PRI cards.
- **Chassis Awareness**
  The PRI NAC must be aware of the current chassis NAC configuration.

  When the NMC goes through its regular device discovery process, it discovers if a NAC has chassis awareness capability. If the NAC is capable of being chassis aware, the NMC sends it slot availability information. The NAC then knows which slots/entities are available to it.

  The NMC will update the chassis aware NACs only when something important happens (such as a module inserted event or a power up event).

  **NOTE**: The NMC does not store the chassis NAC configuration information in its NVRAM.

- **Call Tracking**
  The NMC supplies the call ID to the Accounting/Event logging server at call establishment and termination or to the trap destination at call termination.

  ISDN cards (T1/E1 PRI, Quad 3.0, and NETServer PRI) generate a unique Call Reference Number when a call enters the chassis through them. They then forward the number to the Quad modem, which in turn provides it to the NMC. The NMC supplies it to the Accounting/Event logging server at call establishment and termination or to the trap destination at call termination.

  Call Reference Number format: 0xSSCCNNNN

  | | |
  |---|---|
  | SS | slot number of the originating NAC |
  | CC | channel number of the originating NAC |
  | NNNN | 16-bit call number assigned by the originating NAC |

- **Full Management of the X.25 PAD**
  Previous Total Control management versions supported the X.25 PAD by recognizing the card in the chassis and supporting basic levels of management on a slot basis. Now, full management is available for version 3.0 of the X.25 PAD, including configuration, fault, and performance management.

- **Additional Modem Features**
  Cellular modem support may be enabled as an added-cost feature and is configurable for your cellular application. Extended 33.6 Kbps V.34 link rates are also supported in this management release.

- **New Auto Response Options**
  Two new module-level response options have been added for response to slot-level events in the Auto Response feature. See the *Total Control Manager/SNMP Software Guide* for a description of the Auto Response feature.

- **Revised Software Download for New Cards**
  Additional .SDL and .NAC files have been developed for easy software download on new cards. See the Software Download Installation Summary that accompanies firmware diskettes for a description of the

# About this Guide

This guide covers the configuration of the Total Control Network Management Card (NMC). Management operations are covered in the *Total Control Manager/SNMP Software Guide*. Hardware information is covered in the *NMC Hardware Install Guide*.

The following material is covered in this guide:

- Internet Addressing
- Local console operator interface description
- Using SNMP
- Accessing a remote NMC / NMC NIC
- Total Control NMC routing overview
- Index

## Documentation Scope

Hardware installation guides are shipped along with components. This manual is a part of the Total Control Reference Library, which is a group of manuals that describe the concepts and procedures for configuring the firmware of all Total Control cards.

## We Welcome Your Suggestions

Every effort has been made to provide useful, accurate information. If you have any comments or suggestions, please let us know.

By voice mail: (847) 933-5200

Via the Internet: sysdocs@usr.com

# Chapter 1
# Internet Protocol (IP) Addressing

Setting IP addresses to route data to and from the Total Control chassis is one of the first things a Network Manager should consider before cabling the chassis to a network.

Default addresses are associated with the NMC NIC ports. These default addresses are *not* appropriate for connection to the Internet. We recommend that default addresses be changed before establishing the network connection for the chassis. This may be accomplished either via the NMC User Interface software or the *Total Control Manager/SNMP* software.

A Network Manager should take into account the size of the network, the number of physical networks, expected growth, and maintenance.

## Internet Naming

TCP/IP had its origins in the U.S. Department of Defense. Naming provides a human-readable, user-friendly scheme by which to refer to hosts and routers. Names administered by the InterNIC Registration Services are organized in a tree structure, under a number of major nodes, called *domains*. The major naming domains include the following:

- COM for commercial organizations
- EDU for education institutions
- GOV for government bodies
- MIL for military organizations
- NET for systems performing network services
- ORG for non-profit organizations
- Country-specific domains

Once a domain has been assigned and registered to an organization, that organization is responsible for maintaining all subunits within the domain.

## IP Address Structure

Each host on a TCP/IP internet is assigned a unique 32-bit address. This address is expressed as four decimal integers separated by decimal points, such as 192.77.203.193. Each integer gives the value of one octet (eight-digit binary number) of the IP address. This number should be thought of as its binary equivalent, with leading 0s inserted to form four 8-bit bytes. The address 192.77.203.193 would therefore be expressed as:

11000000 01001101 11001011 11000001

IP addressing includes a coded reference to the network to which a host attaches, as well as a reference to a unique host on that network. An IP address specifies an attachment to a network rather than an individual machine.

Each address consists of a Net ID and a Host ID. A Net ID may be assigned to a network by the InterNIC Registration Services, and depends on the network size. It is the responsibility of a Network Manager to assign the Host IDs with a view to how the devices must communicate with each other. The proportion of bits devoted to the Net ID and Host ID depends on the address class.

## IP Address Classes

There are three primary classes of IP address: Class A, Class B and Class C. The purpose of the class concept is to distinguish among networks of varying sizes. The following table shows how these classes are divided.

*IP Address Classes*

| Class | Network Size (Number of Hosts) | Net ID Size | Host ID Size |
|---|---|---|---|
| A | Over $2^{16}$ (Over 65,536) | 7 bits | 24 bits |
| B | Between $2^{8}$ and $2^{16}$ (256 to 65,536) | 14 bits | 16 bits |
| C | Under $2^{8}$ (Under 256) | 21 bits | 8 bits |

Figure 1-1 is a graphic representation of this concept. The class of an IP address can be determined from the first two bits.

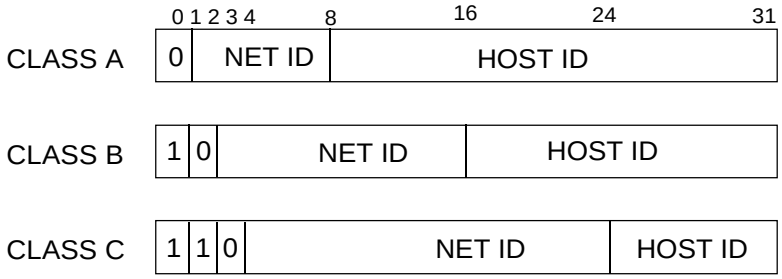



***Figure 1-1. IP Address Classes***

## *Subnet Addressing*

To use subnet addressing, a host computer must be able to identify which bits of the 32-bit internet address correspond to the physical network and which correspond to host identifiers. This information is contained in a 32-bit quantity called the *subnet mask*. Subnet addressing allows a Network Manager to divide the available Host IDs along logical lines that represent the physical connections.

The subnet mask makes it possible for a Network Manager to partition the Host ID of the IP address into a Physical Network portion and a Host portion. Bits in the subnet mask are set to 1 if the network is to treat the corresponding bit in the IP address as part of the network address, and 0 if it is to treat the bit as part of the host identifier. The IP address and the subnet mask are computed together with a Boolean *and* operation to determine the subnet on which a given IP address resides.

The following example shows both the decimal integer IP address and subnet mask and their binary equivalents.

*IP Address Decimal and Binary Equivalents*

| | **Decimal Integer** | **Binary Equivalent** |
|---|---|---|
| IP Address | 192.77.203.65 | 11000000 01001101 11001011 01000001 |
| Subnet Mask | 255.255.255.192 | 11111111 11111111 11111111 11000000 |

The first three octets of the subnet mask are set to 1; this is the Net ID portion of the IP address. The fourth octet of the subnet mask has 1's in the first two positions; this indicates that the first two digits will be used to indicate physical networks, allowing four subnets: 00, 01, 10 and 11. The remaining six digits in the last octet can be used for the host identifier.

### Subnet Packet Forwarding

The NMC can forward data from one subnet to another. If the NMC has different subnetworks attached to its LAN and WAN ports, then any packets arriving at one port—but targeted at the network on the other port—are forwarded to the other port. This process is analogous to *bridging*, although it is based on IP addresses, which bridges do not typically examine.

## Gateway Addressing

The gateway addressing concept provides a catch-all address for packets that the NMC does not know how to handle. It establishes a default path for data to follow when the destination IP address of a packet is not on the same subnet as either the LAN or WAN port IP address. This allows packets to be forwarded to a bridge or router (or even another NMC).

Figure 1-2 illustrates the gateway concept. The subnet mask is 255.255.255.192, and the gateway address for this NMC is 192.77.203.254, which places the gateway on the same physical network (or subnet) as the LAN port IP address.

**NOTE**: We suggest the NMC be on an isolated LAN segment that does not receive too much traffic; this will prevent the NMC from expending too much time on nonproductive traffic and concentrate its resources on its other real-time management functions.

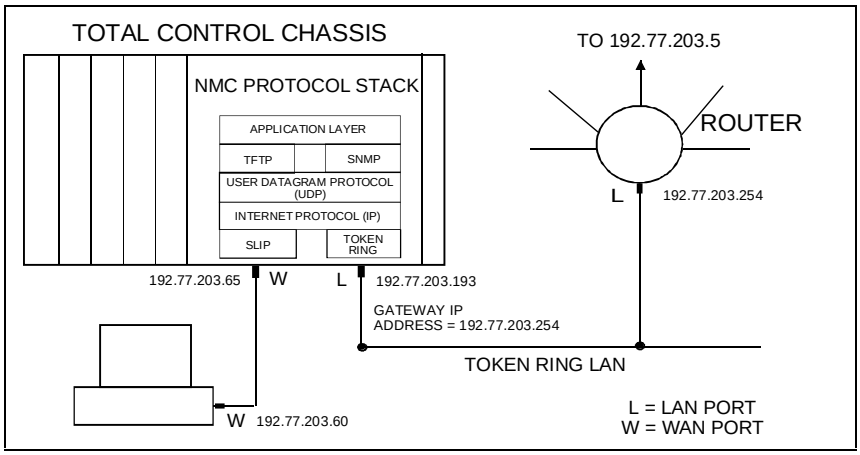



***Figure 1-2. TCP/IP Example, with NMC Protocol Stack***

This example follows this path:

1. A data packet is sent from a PC through the WAN connection, with a destination address of 192.77.203.5.
2. It arrives at the Total Control chassis, which has both LAN and WAN connections. The routing is handled at the IP layer of the protocol stack.

3. The destination address of the packet does not match either the LAN or WAN address, so the packet is routed to the gateway address. The packet is sent through the LAN port to the router, which forwards it to the correct address.

## TCP/IP Reference Material

It is the responsibility of the Network Manager to devise an addressing strategy appropriate for the size and growth potential of the network. We recommend the following reference material for TCP/IP:

Comer, D.E., *Internetworking with TCP/IP Volume I: Principles, Protocols and Architecture*, Prentice-Hall, Englewood Cliffs, New Jersey, 1991.

Comer, D. E. and Stevens, D. L., *Internetworking with TCP/IP Volume II: Implementation and Internals*, Prentice-Hall, Englewood Cliffs, New Jersey, 1991.

IP machines and networks that will be attached to the Internet must obtain registered addresses from the Internet Network Information Center (InterNIC). However, for networks with only a few IP machines, it is probably better to contact your local Internet access provider and let them handle the details. The InterNIC can be contacted at the following address and phone number.

Network Solutions
InterNIC Registration Services
505 Huntmar Park Drive
Herndon, VA 22070

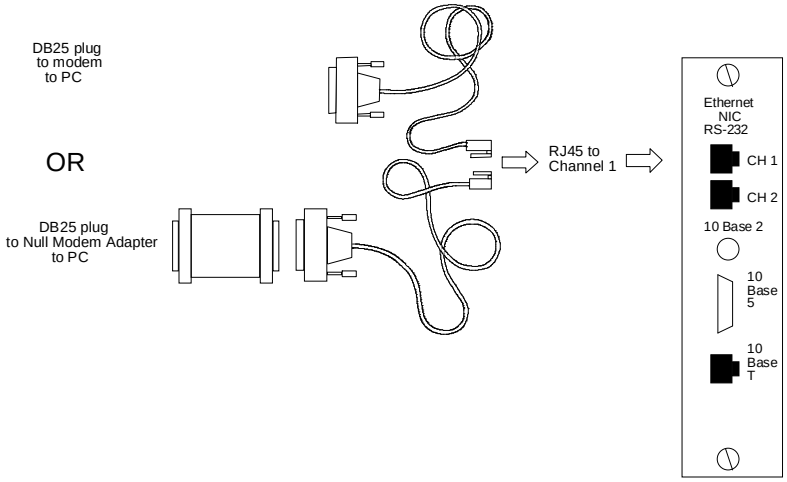
1-703-742-4777

More information may be obtained through ftp from ds.internic.net (U.S. East Coast), nic.nordu.net (Europe), ftp.isi.edu (U.S. West Coast), or munnari.oz.au (Pacific Rim).

# Chapter 2
# NMC Software Configuration

This chapter describes how to use the RS-232 User Interface to configure the NMC. Even if you plan to use the *Total Control Manager/SNMP* software to communicate with the chassis, it is important to understand how to use this interface.

The user interface port on the NMC NIC is designated as CH1. This port can drive an RS-232 compatible, TTY-like device, and is implemented as a DTE port (Data Terminal Equipment, or computer side). Either a dumb terminal or a PC running terminal emulation software can access this port using the RS-232 cable and null modem adapter provided with the NIC.




The User Interface is a simple, menu-driven application with three levels. Options at each level lead to a menu at the next lower level. After making choices at the first and second levels, the third level implements the selection made.

An explicit Save option must be selected before exiting. Changes do not take effect until the NMC is rebooted; upon power-up, the NMC reads the new settings from EEPROM.

## Accessing the User Interface

1. Use the RS-232 cable and null modem adapter provided with the NIC to connect a dumb terminal or PC to the user interface port. The default port speed is 9600 bps; it can be changed with DIP switches 1 and 2 on the NMC.
2. Press Return. The Main Menu appears.

```
U.S. Robotics

Network Management Card Revision 4.0.2
Boot Code Linked Date: Dec 12 1995 at 12:00:00
Operation Code Linked Date: Jan 8 1996 at 12:00:00

Main Menu

1 Configuration
2 Command
3 Feature Enable

Enter menu selection and press Return.

Menu Selection (1-3):
```

# Configuration Menu Options

This section assumes that the Network Manager has a good working knowledge of TCP/IP, and has an addressing strategy in mind. We suggest the NMC be on an isolated LAN segment that does not receive too much traffic; this will prevent the NMC from expending too much time on nonproductive traffic and concentrate its resources on its other real-time management functions. For more information on IP addressing, refer to Chapter 1.

The NMC NIC ports are both configured to default to Class C IP addresses.

| | **Default IP Address** |
|---|---|
| LAN Port | 192.77.203.193 |
| WAN Port | 192.77.203.65 |
| Subnet Mask | 255.255.255.192 |
| Gateway | 192.77.203.126 |

## *Setting IP Addresses*

1. When the Main Menu is displayed, type **1** and press Return. The Configuration Menu appears.

```
Configuration

1 Local LAN IP Address
2 Local WAN IP Address
3 Local Gateway IP Address
4 Local Token Ring IEEE Address
5 Local SNMP Community Strings
6 Local Lan Enable/Disable on Power-up
7 RADIUS Security Secret Key
8 Reset Authorized Access List
9 Save Configuration To Non-Volatile Memory

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-9): 1
```

**NOTE:** Keep in mind that no configuration changes will take effect until you have saved changes to nonvolatile RAM, and reset or reboot the NMC.

## Local LAN IP Address

1. To change the IP address at the NMC NIC's LAN port, type **1** at the Menu Selection prompt on the Configuration Menu and press Return.
2. The LAN IP Address Menu appears. This menu offers a choice between LAN IP Address and LAN IP Subnet Mask. You may also press either Return or Esc to exit back one screen level.

### LAN IP Address

1. To change the LAN IP address, type **1** at the Menu Selection prompt on the LAN IP Address Menu and press Return.

```
LAN IP Address

 1 LAN IP Address
 2 LAN IP Subnet Mask

 Enter menu selection and press Return or press Esc to exit.

 Menu Selection (1-2): 1
```

2. The current IP address at the LAN port is displayed. You may press either Return or Esc to accept this address and exit back one screen level.

```
 LAN IP Address

 Current LAN IP Address = 192.77.203.193

  Press Return or press Esc to exit.

 Enter New LAN IP Address:
```

3. To change the LAN IP address, enter a new address at the prompt and press Return.

### LAN IP Subnet Mask

1. To change the LAN IP subnet mask, type **2** at the Menu Selection prompt on the LAN IP Address Menu and press Return.

```
LAN IP Address

1 LAN IP Address
2 LAN IP Subnet Mask

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-2): 2
```

2. The current IP subnet mask at the LAN port is displayed. You may press either Return or Esc to accept this subnet mask and exit back one screen level.

```
LAN IP Subnet Mask

Current LAN IP Subnet Mask = 255.255.255.192

Press Return or press Esc to exit.

Enter New LAN IP Subnet Mask:
```

3. To change the LAN IP subnet mask, enter a new address at the prompt and press Return.

## Local WAN IP Address

Even if the chassis is only connected to the LAN, a WAN IP address must be assigned. IP address 0.0.0.0 is **NOT** valid.

1. To change the IP address at the NMC NIC's WAN port, type **2** at the Menu Selection prompt on the Configuration Menu and press Return.

```
Configuration

1 Local LAN IP Address
2 Local WAN IP Address
3 Local Gateway IP Address
4 Local Token Ring IEEE Address
5 Local SNMP Community Strings
6 Local Lan Enable/Disable on Power-up
7 RADIUS Security Secret Key
8 Reset Authorized Access List
9 Save Configuration To Non-Volatile Memory

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-9): 2
```

2. The WAN IP Address Menu appears. This menu offers a choice between WAN IP Address and WAN IP Subnet Mask. You may also press either Return or Esc to exit back one screen level.

### WAN IP Address

1. To change the WAN IP address, type **1** at the Menu Selection prompt on the WAN IP Address Menu and press Return.

```
WAN IP Address

1 WAN IP Address
2 WAN IP Subnet Mask

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-2): 1
```

2. The current IP address at the WAN port is displayed. You may press either Return or Esc to accept this address and exit back one screen level.

```
WAN IP Address

Current WAN IP Address = 192.77.203.65

 Press Return or press Esc to exit.

Enter New WAN IP Address:
```

3. To change the WAN IP address, enter a new address at the prompt and press Return.

### WAN IP Subnet Mask

1. To change the WAN IP subnet mask, type **2** at the Menu Selection prompt on the WAN IP Address Menu and press Return.

```
WAN IP Address

1 WAN IP Address
2 WAN IP Subnet Mask

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-2): 2
```

2. The current IP Subnet Mask at the WAN port is displayed. You may press either Return or Esc to accept this subnet mask and exit back one screen level.

```
WAN IP Subnet Mask

Current WAN IP Subnet Mask = 255.255.255.192

 Press Return or press Esc to exit.

Enter New WAN IP Subnet Mask:
```

3. To change the WAN IP subnet mask, enter a new address at the prompt and press Return.

## Local Gateway IP Address

1. The NMC NIC uses the Gateway IP address to route data packets that are not destined for either the LAN or WAN ports. To change the Gateway IP address, type **3** at the Menu Selection prompt on the Configuration Menu and press Return.

```
Configuration

1 Local LAN IP Address
2 Local WAN IP Address
3 Local Gateway IP Address
4 Local Token Ring IEEE Address
5 Local SNMP Community Strings
6 Local Lan Enable/Disable on Power-up
7 RADIUS Security Secret Key
8 Reset Authorized Access List
9 Save Configuration To Non-Volatile Memory

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-9): 3
```

2. The current Gateway IP address is displayed. You may press either Return or Esc to accept this address and exit back one screen level.

```
Gateway IP Address

Current Gateway IP Address = 192.77.203.126

 Press Return or press Esc to exit.

Enter New Gateway IP Address:
```

3. To change the IP address, enter a new address at the prompt and press Return.

**NOTE**: You cannot Save to NVRAM (option 9 on the Configuration Menu) unless the Gateway address points to either the LAN or the WAN port subnet.

## *Additional Port Configuration*

### Local IEEE Address

Both Token Ring and Ethernet NICs have a unique IEEE address burned in at the factory. The Ethernet NIC IEEE address cannot be changed. USR does allow the IEEE address on Token Ring NICs to be changed in order to permit compatibility with some older Token Ring equipment. In most cases, however, the IEEE address should not require a change.

1. The unique default here should be fine for most installations. To override the default IEEE address, type **4** at the Menu Selection prompt on the Configuration Menu and press Return.

```
Configuration

1 Local LAN IP Address
2 Local WAN IP Address
3 Local Gateway IP Address
4 Local Token Ring IEEE Address
5 Local SNMP Community Strings
6 Local Lan Enable/Disable on Power-up
7 RADIUS Security Secret Key
8 Reset Authorized Access List
9 Save Configuration To Non-Volatile Memory

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-9): 4
```

2. The current Token Ring IEEE address is displayed. You may press either Return or Esc to accept this address and exit back one screen level.

```
Local Token Ring IEEE Address

Physical Address = 38393a3b3c3d (Default NIC address)

 Press Return or press Esc to exit.

Enter New Local Address:
```

3. To change the IEEE address, enter a new address at the prompt and press Return. If you change the address and later want to change back to the burned-in default, set the Local Token Ring IEEE address to all zeros.

## Local SNMP Community Strings

1. The SNMP community string permits operator access to SNMP set commands. Type **5** at the Menu Selection prompt on the Configuration Menu and press Return.

```
Configuration

1 Local LAN IP Address
2 Local WAN IP Address
3 Local Gateway IP Address
4 Local Token Ring IEEE Address
5 Local SNMP Community Strings
6 Local Lan Enable/Disable on Power-up
7 RADIUS Security Secret Key
8 Reset Authorized Access List
9 Save Configuration To Non-Volatile Memory

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-9): 5
```

2. The SNMP Community Strings submenu displays. You may use this screen to access the read-only or read-write SNMP Community Strings. Type either 1 or 2 at the prompt to access the SNMP Community Strings.

```
SNMP Community Strings

1 SNMP Read-Only (Public) Community String
2 SNMP Read-Write (Private) Community String

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-2):
```

3. The current SNMP Community String is displayed (defaults are “public” for read-only and “private” for read-write). To change the SNMP community string, enter a new string at the prompt and press Return. You may also press Esc to accept this address and exit back one level.

## Enable/Disable Lan on Power-Up

This option is provided due to current functionality of Token Ring LANs. If the Token Ring is not currently available, the NMC will wait for two minutes before detecting the LAN. Use this option to disable the NMC from looking for the Token Ring LAN, possibly shortening start-up time by two minutes.

1. To enable or disable your LAN on chassis power-up, type **6** at the Menu Selection prompt on the Configuration Menu and press Return.

```
Configuration

1 Local LAN IP Address
2 Local WAN IP Address
3 Local Gateway IP Address
4 Local Token Ring IEEE Address
5 Local SNMP Community Strings
6 Local Lan Enable/Disable on Power-up
7 RADIUS Security Secret Key
8 Reset Authorized Access List
9 Save Configuration To Non-Volatile Memory

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-9): 6
```

2. The current status of this setting (Enable / Disable) is displayed. Type either 1 or 2 to change the status and press Return, or press Esc to exit this screen, maintain the current status, and exit back one level.

## RADIUS Security Secret Key

The RADIUS Security Secret Key is a series of up to 64 keystrokes known only to the NMC client and RADIUS Security server. These keystrokes are used to encrypt data sent between the server and client. The secret key is never displayed, so you must remember what it is, note it, and keep the information in a secure place.

1. To create a secret key for the RADIUS security database, type **7** at the Menu Selection prompt on the Configuration Menu and press Return.

```
Configuration

1 Local LAN IP Address
2 Local WAN IP Address
3 Local Gateway IP Address
4 Local Token Ring IEEE Address
5 Local SNMP Community Strings
6 Local Lan Enable/Disable on Power-up
7 RADIUS Security Secret Key
8 Reset Authorized Access List
9 Save Configuration To Non-Volatile Memory

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-9): 7
```

2. The following screen appears, allowing you to enter a secret key. The Secret Key is a shared secret known only to the NMC client and the RADIUS security server. Press Esc when done.

```
RADIUS Security Secret Key

Press Esc to exit.

Enter New Secret Key:
```

## Reset Authorized Access List

1. To clear the list of IP addresses allowed to communicate with the NMC (usually required when the NMC is being redefined), type **8** at the Menu Selection prompt on the Configuration Menu and press Return.

```
Configuration

1 Local LAN IP Address
2 Local WAN IP Address
3 Local Gateway IP Address
4 Local Token Ring IEEE Address
5 Local SNMP Community Strings
6 Local Lan Enable/Disable on Power-up
7 RADIUS Security Secret Key
8 Reset Authorized Access List
9 Save Configuration To Non-Volatile Memory

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-9): 8
```

2. The list of IP addresses of users with authorized access is cleared. This permits any IP address to access the NMC until a restricted set of user addresses is once again defined.

## Save Configuration to Nonvolatile Memory

1. To save the changes that you have made to the chassis configuration to nonvolatile memory, type **9** at the Menu Selection prompt on the Configuration Menu and press Return.

```
Configuration

1 Local LAN IP Address
2 Local WAN IP Address
3 Local Gateway IP Address
4 Local Tpoken Ring IEEE Address
5 Local SNMP Community Strings
6 Local Lan Enable/Disable on Power-up
7 RADIUS Security Secret Key
8 Reset Authorized Access List
9 Save Configuration To Non-Volatile Memory

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-9): 9
```

2. A screen is displayed to indicate that your configuration has been saved. Press Esc to exit.

## Command Menu Options

Currently, one command, Reset, is available on the Command Menu.

1. To reset the NMC, type **2** at the Menu Selection prompt on the Main Menu.

```
U.S. Robotics

Network Management Card Revision 4.0.2
Boot Code Linked Date: Dec 12 1995 at 12:00:00
Operation Code Linked Date: Jan 8 1996 at 12:00:00

Main Menu

1 Configuration
2 Command
3 Feature Enable

Enter menu selection and press Return.

Menu Selection (1-3):
```

   The Command Menu displays.

```
Command

1 Reset

Enter menu selection and press Return or press Esc to exit.

Menu Selection (1-1): 1
```

2. Type **1** and press Return. A Reset Confirmation message appears. Type **Y** to reset the NMC.

## Feature Enable

Several features are available at an additional cost. These features must be enabled in the NMC, and some require an additional feature enable operation in TCM.

1. To enable a feature on the NMC, first contact U.S. Robotics Customer Service. Have your NMC serial number ready, as it will be required. The Customer Service representative will provide a Feature Enable String.
2. Type **3** at the Menu Selection prompt on the Main Menu and press Return.

```
U.S. Robotics

Network Management Card Revision 4.0.2
Boot Code Linked Date: Dec 12 1995 at 12:00:00
Operation Code Linked Date: Jan 8 1996 at 12:00:00

Main Menu

1 Configuration
2 Command
3 Feature Enable

Enter menu selection and press Return.

Menu Selection (1-3):
```

The Feature Enable screen appears.

```
Feature Enable

Current Features Enabled = XXXXXXXXXXXX

Press Return or press Esc to exit.

Enter New Feature Enable String:
```

3. Enter the string provided by Customer Service at the prompt and press Return.
4. Once the Feature Enable String has been entered into your system, you must save your configuration and reset or reboot the NMC before the new feature can be used.

## Exiting from the User Interface

1. Press Esc to back out of the RS-232 User Interface screens. Remember to Save to NVRAM if you have made any configuration changes (option 9 on the Configuration Menu).
2. Reboot the NMC for any modifications to take effect (if you didn't reset it before exiting).
3. Disconnect the RS-232 cable from the user interface port if you intend to use it to cable the WAN port.

**NOTE:** You may leave this port cabled if you want a means of future access. Additional RS-232 cables are available from U.S. Robotics.

# Chapter 3
# Using SNMP

The NMC communicates with the Management Station (MS) via the Simple Network Management Protocol (SNMP). SNMP defines a structure for management information, as well as an approach to configuring and monitoring that information.

The NMC serves as an SNMP proxy agent. The NMC receives management data via SNMP, and then passes the data to all the other cards in the chassis via the Management Bus Protocol. The management data is formatted to address MIB objects (described in the next section), which enables any SNMP-compliant management console to manage the chassis.

## Management Information Base (MIB)

Management of a device by SNMP requires the definition of a set of managed objects or variables that can be written to, read from, or both. A collection of managed objects resides in a virtual store, or database, referred to as a Management Information Base (MIB).

In order to manage the assignment of unique names to managed objects, a tree-like structure is defined. The branches of the tree are used to divide up the objects into related groups, with the managed objects represented as nodes in the structure. Every node is labeled with an integer and a brief text definition.

The International Standards Organization (ISO) has issued a standard for defining a MIB called Abstract Syntax Notation 1, (or ASN.1). ASN.1 defines the following kinds of information to be used in the MIB.

- Syntax—indicates the data type.
- Access—indicates read-only or read-write.
- Status—indicates whether implementation of the MIB is mandatory, optional or obsolete.
- Description—provides a complete value explanation.
- Identifier—indicates where the MIB fits in the tree.

## *SNMP Commands*

SNMP has five basic Protocol Data Units (PDUs) that it uses to manage devices.

| Command | Operation |
|---|---|
| Get-Request | Retrieves current MIB values for a specified list of data types. |
| Get-Next-Request | Retrieves management information by moving sequentially through the MIB tree. |
| Set-Request | Sets the specified MIB items to the enclosed values. |
| Get-Response | Replies to any of the three commands above, with a response or error message. |
| Trap | Reports extraordinary events. |

As an SNMP proxy agent, the NMC has the ability to handle all SNMP requests from the MS for any of the cards in the chassis. The NMC carries out these requests using the Management Bus Protocol, and can be programmed so that when it detects that a specified event has occurred on a card, the NMC sends a trap to the appropriate MS.

## *Supported MIBs*

There are two types of MIBs handled by the *Total Control Manager/SNMP* software: standard MIBs and proprietary MIBs. The *Total Control SNMP MIB Reference Manual* provides a discussion of how the U.S. Robotics chassis implements MIBs.

### Standard MIBs

Standard MIBs are those that have been assigned one of the following classifications by the Internet Engineering Task Force (IETF):

- Full Standard
- Draft Standard
- Proposed Standard
- Experimental
- Working Draft

*Total Control Manager/SNMP* supports two standard MIBs:

| MIB Filename | Function |
|---|---|
| DS1.MIB | Provides management of T1 interfaces (based on RFC 1232). |
| MIB2.MIB | Defines various protocol and administrative information (Full Standard). |

### Proprietary MIBs

Proprietary MIBs are those that have been developed by U.S. Robotics to define the managed objects for the devices that are installed in the chassis. For example, there is no approved standard MIB for modems, so U.S. Robotics has defined a proprietary MIB for its modems. An example of a managed object in this MIB would be the error control setting, corresponding to the AT command &M*n*.

The following proprietary MIBs, which use ASN.1 structure, are supported by the NMC:

| MIB Filename | Function |
|---|---|
| NMC.MIB | Contains NMC-specific information. |
| DT1.MIB | Contains parameters that affect the hardware operation of a T1 Card. |
| DS0.MIB | Contains parameters that affect the operation of each timeslot on a Dual T1 Card. |
| UDS1.MIB | Contains DS1-specific parameters not supported in the standard DS1 MIB. |
| CHS.MIB | Provides tables that describe the devices in the chassis, and allows the Network Manager to take generic actions on cards on the chassis, such as resetting a card or downloading software to a card. |
| MDM.MIB | Defines all objects for a USR modem. |
| CHS_TRAP.MIB | Defines SNMP traps for Fault Management. Must be compiled and integrated in order to use traps and alarms, as well as Auto Response. |
| USRTRAPS.MIB | Defines SNMP traps for Fault Management. Included for compatibility with NMCs running older versions of software. |
| ANIC.MIB | Contains parameters used for basic management of the analog NIC. |
| PB.MIB | Contains parameters used for configuring Packet Bus sessions. |
| PBDG.MIB | Contains parameters used for monitoring Packet Bus performance. |
| IDS0.MIB | Contains parameters that affect the operation of each timeslot on a Primary Rate ISDN Card. |
| IDT1.MIB | Contains parameters used for basic management of the Primary Rate ISDN Card. |
| UX25.MIB | Contains parameters used for Packet Level Protocol management on the X.25 PAD. |
| UX25G.MIB | Contains parameters used for basic management of the X.25 PAD Gateway Card. |
| ULPB.MIB | Contains parameters used for LAPB management on the X.25 PAD, |
| UX25W.MIB | Contains parameters used for WAN management on the X.25 PAD. |

# Chapter 4
# Accessing a Remote NMC / NMC NIC

This chapter describes how to connect the Management Station to a remote NMC. The instructions are for a dial-up connection between two USRobotics or compatible modems, including laptop modems.

The *calling* modem is connected to the Management Station. The *answering* modem must be connected to an NMC NIC in the remote system. You can use one of the Total Control modems in the system, or a separate U.S. Robotics or compatible modem.

The following steps describe how to configure the modems at both ends of the connection, enabling the NMC to receive incoming calls. You'll need the RS-232-to-RJ45 cable that came with the NMC NIC to cable it to an external modem, and another standard RS-232 cable to connect a modem to the Management Station.

## Local Connection

1. Designate a rack modem or standalone modem to be dedicated as the local Management Station-connected modem. This must be done for each planned operator connection, in the event that you want to equip more than one Management Station with the ability to dial in to a chassis.
2. Cable the modem to the Management Station PC with an RS-232 cable.
3. Configure the local, or calling modem, according to the following table.

*Calling Modem Configuration*

| Setting | Command/Switch Equivalent |
|---|---|
| AT command set recognition enabled | DIP switch 8 ON |
| Normal CD operation | AT&C1 |
| Normal DTR operation | AT&D2 |
| CTS flow control | AT&H1 |
| Fixed DTE rate | AT&B1 |
| RTS flow control | AT&R2 |
| DSR override | AT&S0 |
| Online echo off | ATF1 |

## Chassis Connection

1. Be sure that the NMC NIC's out-of-band management port speed is set to the same speed the modems will use. If set above 9600 bps, hardware flow control must be enabled on the modem.

   The NMC NIC's out-of-band management port is set at the factory to 9600 bps. Depending on your modem, you may have to adjust two of the DIP switches, which are located on the NMC. DIP switches 3 and 4 are used to select the port speed.

   The NMC DIP switches are all shipped OFF, or up. The following table shows how to set DIP switches 3 and 4 to select the serial port speed.

   *Selecting the Out-of-Band Management Port Speed*

| DIP 3 | DIP 4 | Speed |
|---|---|---|
| ON | ON | 57,600 bps |
| ON | OFF | 38,400 bps |
| OFF | ON | 19200 bps |
| OFF | OFF | 9600 bps* |

   *Factory setting

   Use the USRobotics screwdriver or a similar tool to adjust the DIP switches.

2. Cable the out-of-band management port on the NMC NIC (CH2) to the answering modem with an RS-232 cable.

3. Configure the answering modem according to the following table.

*Answering Modem Configuration*

| Setting | Command/Switch Equivalent |
|---|---|
| Auto Answer enabled | DIP switch 5 OFF |
| AT command set disabled | DIP switch 8 OFF |
| DTR normal | AT&D2 (or DIP switch 1 OFF) |
| CTS flow control | AT&H1 |
| Fixed DTE rate | AT&B1 |
| RTS flow control | AT&R2 |
| DSR override | AT&S0 |
| Handshake options | ATB0 |
| Local command mode echo off | ATE0 |
| Online echo off | ATF1 |
| Suppress result codes | ATQ1 |

## Manual Software Connection

The following procedure describes how to manually dial up the remote chassis through software.

1. From Windows, launch the NetWare Management System.
2. From the File Menu, select *New U.S.R. Device.* The New Device window appears.
3. Enter the IP address of the remote NMC's out-of-band management port.
4. Select *Options* at the bottom of the window to display additional fields.
5. Under *Remote Serial Communications,* fill in the phone number of the line to which the remote modem is connected.
6. Select *OK* at the bottom of the window. The modem connected to the Management Station goes off hook and dials the remote chassis.
7. When the connection is established, select *Save* from the File Menu. This will save a description of how the Management Station communicates with the chassis, as well as what cards are installed in what slots, with an identifier of the chassis name and address. You can select this in the future to dial the chassis.

   **NOTE:** Configuration data is not saved with this option.

## Automatic Software Connection

The following procedure describes how to dial a remote chassis automatically when the Management Station is rebooted.

1. Add dosdialr.exe to your autoexec.bat. This should be installed after other TSRs to guarantee correct operation, and may be loaded high.

   The example below shows the loading order of the TSRs for a SLIP connection including the dosdialr program.

   LSL
   SLIP_PPP
   TCPIP
   DOSDIALR

2. Edit your net.cfg to include dialing instructions for the port to which you have connected a modem. The following statement is an example for a port configured with SLIP to dial a remote chassis. (Do not use the square brackets when you insert your phone number.)

   **NOTE:** Set the same speed here as your modem configuration. See the table on the next page for port and interrupt information.

   Link Driver SLIP_PPP
   DIRECT YES
   DIAL [*remote chassis number*]
   BAUD 9600
   OPEN ACTIVE
   TCPIPCOMP VJ
   PCOMP YES
   ACCOMP YES
   PORT 2F8
   INT 3
   FRAME SLIP

*COM Port Addressing*

| COM Port | Interrupt | Hex Address |
|---|---|---|
| 1 | 4 | 3F8 |
| 2 | 3 | 2F8 |
| 3 | 4 | 3E8 |
| 4 | 3 | 2E8 |

3. After you have edited and saved your files, reboot the Management Station.

# Appendix A
# Frequent Questions—NMC Routing

This chapter describes configuration of the Total Control NMC to enable local and remote network management from *TCM/SNMP* or other management systems. It addresses IP network configuration issues for the Total Control NMC and answers some frequently asked questions.

## How does the NMC physically connect to management systems?

The Network Management Card (NMC) connects to the outside world via ports on its Network Interface Card. The NMC can be used with Ethernet or Token Ring interface cards. Each type of interface card has LAN interface port(s) as well as a serial port for hard-wired or dial-up serial communications.

## What are the WAN/LAN addresses for the NMC? How are they used?

The NMC uses IP networking to support protocols such as SNMP and FTP. Since the NMC NIC has both serial and LAN ports, it needs two addresses; the serial port's address is called a WAN address to differentiate it from the LAN address. The WAN port is often called the SLIP port, since remote IP communications uses the SLIP (Serial Line IP) protocol.

## How Much Traffic is too Much Traffic on the NMC?

The NMC has many real-time responsibilities. Too much MAC (Medium Access Control) layer broadcast data may slow the NMC down as it uses its resources to discard nonproductive traffic. For this reason, we suggest the NMC be on an isolated LAN segment that does not receive too many MAC layer broadcasts; this will prevent the NMC from expending too much time on nonproductive traffic and concentrate its resources on its other real-time management functions.

## How Many Traps are Too Many Traps?

The NMC is capable of generating all the traps that occur in the chassis, though an inundation of MAC layer broadcast messages (see previous question) may affect trap generation time.

If, however, you discover Novell NMS is not logging in all your traps, NMS may be overwhelmed by too many traps per second. This is a limitation of NMS version 1.15B, which is required to run with TCM; other versions of NMS or other SNMP Host programs may not have this limitation. A good estimate to use is that NMS 1.15B comfortably handles two traps per second, but may start to drop traps when more than four are sent per second.

There is no way of configuring the NMC to send only so many *traps per second*, but we recommend you set up traps in a conservative fashion when you begin, then build slowly to determine your system's reliability threshold.

## How does TCM connect to an NMC?

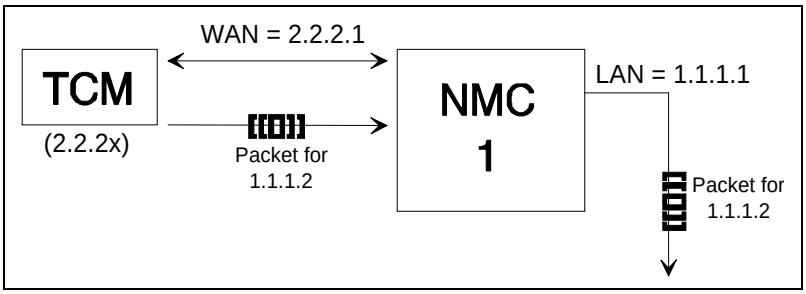
Management software such as TCM can be used at a Network Operation Center to manage either local or remote sites. Local management can be through hard-wired serial lines, or over an Ethernet or Token Ring LAN. When using a local LAN, it is possible to run multiple TCM consoles and manage multiple USR chassis (each with an NMC). Any installation of TCM could talk to any NMC by opening the NMC's IP address from the "File->Open" menu option. In the hard-wired serial line scenario, generally only one NMC talks to one chassis since the connection is physical and point-to-point, although this chassis might serve as a bridge to a local LAN of NMC.

Using TCM to dial into a modem at the remote site allows remote site management. The remote modem is attached to an NMC, which might be on a LAN with other NMCs. These other NMCs can be managed as well, using techniques described below. It is also possible to involve routers.

## Can an NMC forward packets from one IP network to another?

Yes, in a limited fashion. If an NMC has different networks assigned for its LAN and WAN IP addresses, then any packets arriving on one port—but targeted at the network on the other port—are forwarded to that port. This behavior is analogous to *bridging* although it occurs based on the IP address, which true bridges usually do not examine.

**Example:** If an NMC is set up with LAN address 1.1.1.1 and WAN address 2.2.2.1, and the network mask indicates that the first three bytes of the address define the network, and a packet arrives on the WAN port with a destination of 1.1.1.2, the packet will be forwarded (sent out) on the LAN.




## What is the Gateway IP Address?

This is a catch-all address for packets an NMC does not know what to do with; it allows packets to be forwarded to a bridge or router (or even an NMC that is set up to forward).

We alluded earlier to remote site management. Suppose that we have two chassis (each with an NMC) on a LAN at a remote site.

Chassis 1, which is also attached to a modem, has:

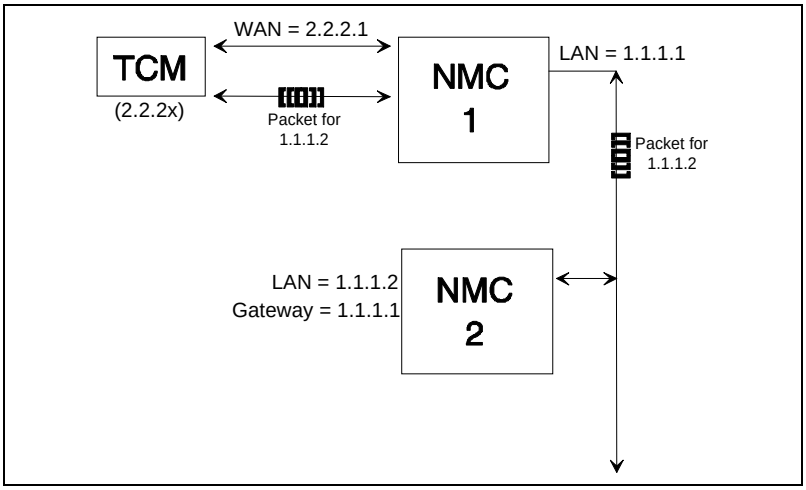
- WAN IP 2.2.2.1 (On modem)
- LAN IP 1.1.1.1 (On local LAN)

Chassis 2 has:

- WAN IP 3.3.3.1 (WAN port not used)
- LAN IP 1.1.1.2 (On local LAN)
- GW IP 1.1.1.1 (Points to chassis 1)

Now, any traffic chassis 2 wants to send to network 2.2.2 will automatically go to chassis 1. So if chassis 2 is configured to send traps to TCM at IP 2.2.2.5, for example, chassis 2 will send the traps out the port matching the gateway address 1.1.1.1 (i.e., the local LAN). The traps will be addressed to 2.2.2.5 so they reach the right end system, but will be sent out on the LAN so that chassis 1 will see and forward them.

What should chassis 1's gateway address be set to? If it has a router or similar device on the WAN port, it could specify that device's address (2.2.2.x) so that any packets it does not know how to handle are sent there. We assume there is no router on the LAN side, because otherwise chassis 2 would probably be sending its traffic there, too.




If there is no router, it is best to ensure that the gateway address is pointed at a nonexistent host on the WAN network (e.g., 2.2.2.253, if there is no host with this address). This will then cause the NMC to ignore packets that it doesn't know how to route. Setting a gateway address that matches neither the WAN nor LAN is not permitted.

**NOTE:** An implementation peculiarity requires that the WAN side be chosen for the gateway address, if you want chassis 1 to forward incoming WAN packets onto the LAN. Any address on the WAN should work.

### How does the NMC know which port to use for a packet it originates (such as a Trap or SNMP response)?

The NMC knows what IP address it is sending to, for example, from the trap destination table internal to the NMC, or from the IP address in a request it is responding to. This is the destination IP address.

- If the destination address matches its own LAN IP address using the network mask (i.e., it is on the NMC's LAN network), the NMC sends the packet on the LAN port.
- If the destination address matches its own WAN IP address using the network mask (i.e., it is on the NMC's WAN network), the NMC sends the packet on the WAN port.
- If the address is not on either the LAN or WAN network of the NMC, and the NMC's gateway address is valid (i.e., the gateway address is on the NMC's LAN or WAN network), it sends the packet on the LAN or WAN port as appropriate so the packet will reach the gateway.
- Otherwise, it doesn't send the packet at all.

### How does the NMC decide what to do with a packet it receives?

- If the destination address is exactly the same as its own LAN or WAN IP address, it processes the packet. E.g., it might be receiving and fielding an SNMP request.
- If the packet arrives on the WAN port, but the destination address is on the NMC's LAN network, it forwards the packet out the LAN port.
- If the packet arrives on the LAN port, but the destination address is on the NMC's WAN network, it forwards the packet out the WAN port. In other words, the NMC forwards a packet when it crosses NMC networks.
- If the destination address is not on either the WAN or LAN networks, the NMC consults its gateway address.

- If the gateway is valid (i.e., on the same WAN or LAN network as the NMC), and if the packet is from the same network as the gateway, the NMC allows the gateway to see it and process it, then issues a Re-Direct to the originator so the traffic is not set to the NMC in future.
- If the gateway is valid, and if the packet must cross NMC networks to reach the gateway, the NMC forwards the packet out the port associated with the gateway so that the gateway will see it. (This might happen in scenario 2 (described below) where NMC 2 sent something to a remote address like 4.4.4.4.)
- If the gateway address is invalid (matches neither WAN nor LAN network), the NMC ignores the packet.

## What are some reasonable scenarios for remote site management?

Assuming there is only one remote link to the site, there are at least three reasonable scenarios. Having multiple links opens up a range of possibilities not addressable here.

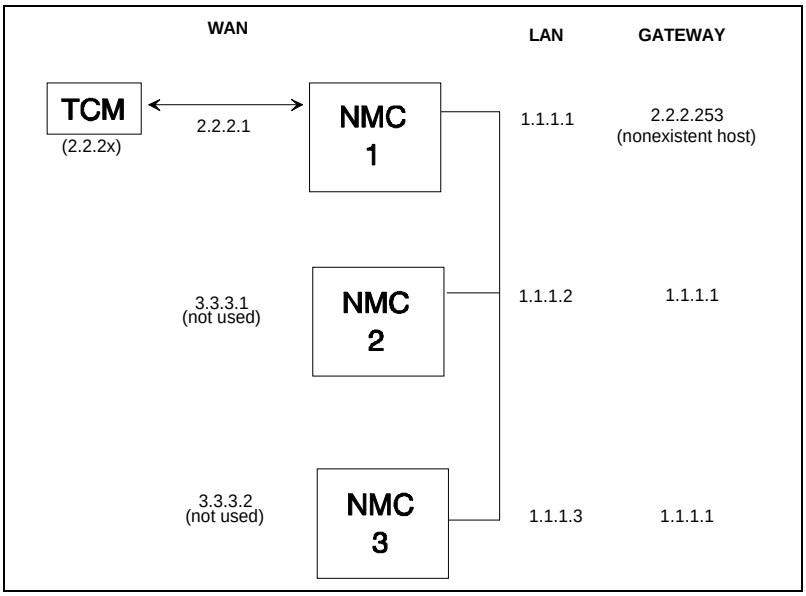
For simplicity we assume we have three networks distinguished by their first three bytes. This could be implemented with a class B address with a network mask of 255.255.255.0.

**NOTE**: It might be more efficient to use a class C address with subnetting that allows at least three networks. This could be done using the network mask 255.255.255.192 (0xFFFFFFC0), since the two bits in the fourth byte allow four distinct networks within the three-byte class C address.

### Scenario 1—NMCs on a LAN, one NMC with direct SLIP connection to TCM or other manager

Here, the NMC with a SLIP connection to TCM through its WAN port must serve as a gateway for the others. The gateway address for the SLIP NMC should be set to a nonexistent host address on either of the LANs, so that packets for strange destinations are ignored. (The gateway address must be on either the LAN or WAN network; TCM's software will not allow other addresses such as all 0's.)

The non-SLIP NMCs must ensure packets meant for SLIP are not mistakenly sent to their WAN ports. This means the SLIP and WAN networks must not match. It is a good convention to set up a common WAN network for all the non-SLIP NMCs; this reduces confusion and facilitates local serial management (e.g., over hard-wired lines) by using a "valid" but non-colliding IP address.

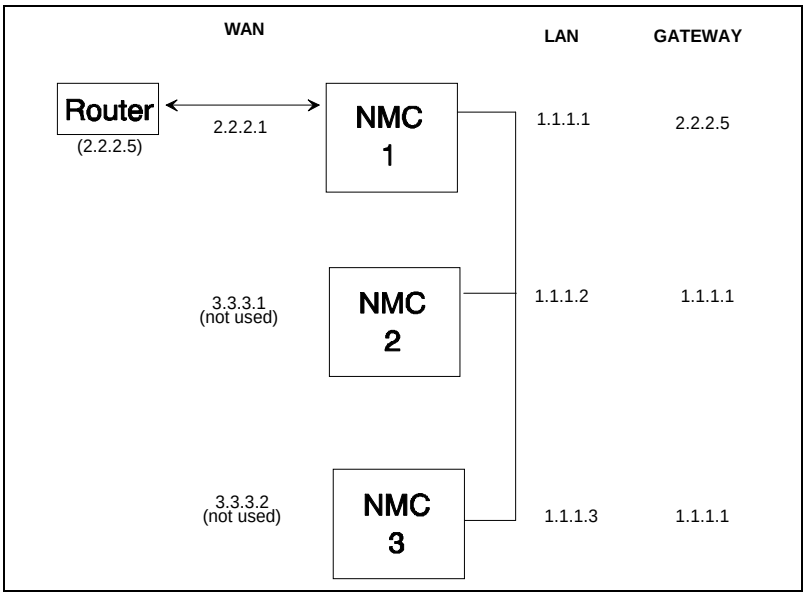



Here, WAN packets (such as SNMP requests) addressed to 1.1.1.2 or 1.1.1.3 will be forwarded by NMC 1 to NMC 2 or 3, respectively.

Outgoing packets (e.g., traps or SNMP responses) sent by NMC 2 or 3 will be noticed by NMC 1 and forwarded over the LAN port, provided they are for network 2.2.2. Any other packets will be ignored since there is no host at gateway address 2.2.2.253.

### Scenario 2—NMCs on a LAN, one with a direct SLIP connection to a router

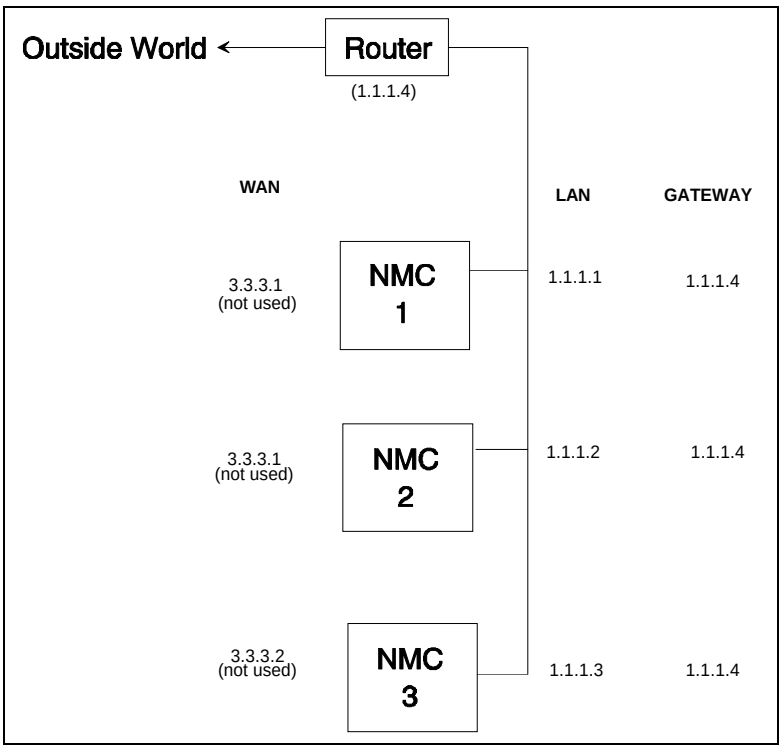
As in scenario 1, the NMC with SLIP serves as a gateway to the remote management center. However, the NMC with SLIP can specify the router as the gateway, allowing it to handle packets with unknown IP addresses.




The only difference from scenario 1 is that now, outgoing NMC packets destined for external networks (e.g., addressed to 4.4.4.1) will be sent to the router, for any and all NMCs. The only configuration change is that NMC 1's gateway IP address is now the router's IP address, 2.2.2.5. NMC 1 forwards both ways for NMC 2 and 3, and external outgoing packets are forwarded further by the router.

### Scenario 3—NMCs on a LAN, router also on the LAN

In this situation, all NMCs should specify the router's IP address as the gateway. No NMC forwarding is necessary; the router handles all forwarding.



# Index