MultiCom

Reference Manual

Version 2.6.1 - 99/7/20

COPYRIGHT

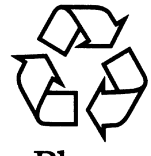
TRADEMARKS

REVISIONS

The information in this document is subject to change without notice. Revisions may be issued at any time. For the latest revision of our manuals, please watch http://www.lightning.ch/support/index_resources.html.

LIGHTNING Instrumentation SA
Avenue des Boveresses 50
1010 Lausanne
SWITZERLAND

Phone: +41 21 654-2000
Fax: +41 21 654-2001
E-mail: info@lightning.ch
Web: http://www.lightning.ch/



Please
Recycle

Warranty

WARRANTY

NO WARRANTIES ARE EXTENDED BY THIS DOCUMENT. The technical information in this document is proprietary to LIGHTNING Instrumentation SA and the recipient has a personal, non–exclusive and non transferable license to use this information solely with the use of LIGHTNING Instrumentation SA products. The only product warranties made by LIGHTNING Instrumentation SA, if any, are set forth in the agreed terms and conditions for the purchase of LIGHTNING Instrumentation SA products. LIGHTNING Instrumentation SA declaims liability for any and all direct and indirect damages that may result from publication or use of this document and/or its contents.

LIGHTNING Instrumentation SA warrants all hardware products of its manufacture to be free from defects in material and workmanship for 12 months from date of delivery.

Upon prompt notification by the purchaser, LIGHTNING Instrumentation SA will correct, within the warranty period, any defects in equipment of its manufacture either by repair at its factory or by supply of replacement parts to the purchaser.

LIGHTNING Instrumentation SA must decide to its own satisfaction that the equipment is defective and has not developed malfunctions as a result of misuse, modification, or abnormal conditions of operation. Damages due to overvoltage (e.g. lightning strokes) or wrong cabling on any interface are expressly excluded from the warranty. Opening the products also voids the warranty. LIGHTNING Instrumentation SA assumes no liability for consequential damages, and its liability shall in no case exceed the original purchase price of the equipment.

The warranties set forth above are the sole warranties applicable to LIGHTNING Instrumentation SA products. THE IMPLIED WARRANTY OF MERCHANTABILITY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ARE EXCLUDED.

LIMITATION OF LIABILITY

UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL LIGHTNING INSTRUMENTATION SA BE LIABLE FOR LOSS OF USE, INTERRUPTION OF BUSINESS, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS) REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT PRODUCT LIABILITY OR OTHERWISE, EVEN IF LIGHTNING HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event shall Lightning be liable for costs of procurement of substitute goods. The potential liability of LIGHTNING arising out of this product is in any case limited to the purchase price paid to Lightning for its products.

SOFTWARE AND DOCUMENTATION LICENSE

The software and documentation included in or with products of Lightning Instrumentation SA is subject to following licence.

License. The software, on any media, including disk, read-only memory, and flash memory and the products related documentation are licensed to you by Lightning. You own the media on which the Lightning software is recorded, but Lightning and/or Lightning's Licensor(s) retain title to the Lightning software and related documentation. The license allows you to use the Lightning software on a single Lightning hardware product. In the case of software on disk, you are allowed to make one copy of Lightning software in machine-readable form for backup purposes only. You must reproduce on such copy the Lightning copyright notice and any other proprietary legends that were on the original copy of the disk containing Lightning software. You may also transfer all your license rights in the Lightning software, together with the associated hardware, the backup copy, the related documentation, and a copy of this license to another party, provided the other party reads and agrees to accept the terms and conditions of this license.

Restrictions. The Lightning software contains copyrighted materials, trade secrets, and other proprietary materials and in order to protect them you may not decompile, reverse engineer, disassemble, or otherwise reduce the Lightning software to a human-perceivable form. You may not modify, network, rent, lease, loan, distribute, or create derivative works based upon the Lightning software in whole or in part. You may not electronically transmit the Lightning software from one computer to another or over a network.

Termination. This license is effective until terminated. You may terminate this license at any time by destroying the Lightning software, the related hardware, related documentation and all copies thereof. The license will terminate immediately without notice from Lightning if you fail to comply with any provision of this license. Upon termination you must destroy the Lightning software, the related hardware, related documentation and all copies thereof.

Limited Warranty on media. Lightning warrants the media on which the software is recorded as its hardware materials, and limits the liability as set for the hardware material.

Disclaimer of warranty on Lightning software. You expressly acknowledge and agree that use of the Lightning software is at your sole risk. The Lightning software and related documentation are provided “AS IS” and without warranty of any kind and Lightning EXPRESSELY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. LIGHTNING DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE LIGHTNING SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE LIGHTNING SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE LIGHTNING SOFTWARE WILL BE CORRECTED. FURTHERMORE, LIGHTNING DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE LIGHTNING SOFTWARE OR RELATED DOCUMENTATION IN THE TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY LIGHTNING OR A LIGHTNING-AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE LIGHTNING SOFTWARE PROVE DEFECTIVE, YOU (AND NOT LIGHTNING OR A LIGHTNING AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL

NECESSARY SERVICING, REPAIR, OR CORRECTION. Some juridictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Limitation of liability. Conforming to the general limitation of liability.

Controlling law and Severability. This license shall be governed by and construded in accordance with the laws of Switzerland and Canton de Vaud, as applied to agreements entered into and to be performed entirely between Canton de Vaud residents. If for any reason a court of competent juridiction finds any provision of this license, or portions thereof, to be unenforceable, that provision of the license shall be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this license shall continue in full force and effect.

Complete agreement. The license constitutes the entire agreement between the parties with respect to the use of the Lightning software and related documentation, and supersedes all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. No amendment to or modification of the License will be binding unless in writing and signed by a duly authorized representative of Lightning.

EXPORT

Some versions and options of Lightning's Software and Hardware, including technical data, may be subject to Swiss, E.U., U.S. (including the U.S. Export Administration Act) or other countries export control laws, and their associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Hardware.

ISDN COSTS

MultiCom bridges and routers can be connected to ISDN networks. The use of these networks is billed to you by your Carrier and is not the responsibility of LIGHTNING Instrumentation SA or your dealer. You are stongly advised to regularly consult ISDN statistics to detect any abnormal usage of your line(s), especially after changing your network configuration.

The billing is usually done for the use of each B-channel, and with a charge **per time** as well as **for each call setup.**

In the automatic mode, the ***MultiCom*** will open a connection whenever it detects traffic that needs to be transmitted to the remote site. This can be seen on a Pocket or Classic ***MultiCom*** when the B1 or B2 LED become green, showing that the channel has been opened (generating a call setup charge for the caller) and staying green for the time needed (generating calling charges for the caller).

The duration a connection remains active in the absence of traffic can be customized to suit your needs (see § 14.18.53, "ISDN IdleCloseTime" on page 181).

The use of the Multi-Point software option can also lead to high telephone bills under certain circumstances.

In no event shall Lightning be liable for costs incurred by a user on its ISDN line. The ***MultiCom*** is designed to open and close ISDN lines automatically, depending on traffic on the Ethernet and ISDN line and on parameters set in the configuration. Front-panel signals and specific commands may indicate the current state and activity of the ISDN line, and the user should keep an eye on those status indications to avoid excessive bills, due to misconfiguration, protocol errors, polling applications, potential software or firmware errors and so forth. **THE USER AND THE USER ONLY IS SOLELY RESPONSIBLE FOR ALL INCURRED ISDN COSTS.**

WARNING

THERE ARE NO OPERATOR SERVICEABLE PARTS INSIDE THIS EQUIPMENT. SERVICE MUST BE PERFORMED BY QUALIFIED SERVICE PERSONNEL. OPENING CASE VOIDS GUARANTEE.

VORSICHT

KEIN TEIL IM GEHÄUSE KANN VOM BENÜTZER SELBST REPARIERT WERDEN. BITTE WENDEN SIE SICH AN QUALIFIZIERTES WARTUNGSPERSONAL. DAS ÖFFNEN DES GERÄTES FÜHRT ZUM VERLUST DER GARANTIE.

ATTENTION

CET APPAREIL NE CONTIENT AUCUN ELEMENT QUE L'UTILISATEUR PUISSE REPARER. CONFIEZ LA MAINTENANCE AU PERSONNEL TECHNIQUE QUALIFIE. L'OUVERTURE DE L'APPAREIL ANNULE LA GARANTIE.

Contents

Contents

Chapter 1

Preface

Let's start by describing what this manual is about …

INTENDED AUDIENCE 1.1

The manual is intended for individuals who are familiar with ISDN and Ethernet concepts, and also with network bridging and routing.

ABOUT THIS MANUAL 1.2

This manual applies to the following hardware:

- ***Pocket** Multi**Com*** (Pocket)
- ***Classic** Multi**Com*** (Classic)
- ***Multi**Com **LAN Access Center*** (LAC)
- ***Multi**Com **Serial IV*** (Serial)
- ***Multi**Com **Access IV*** (Access)
- ***Multi**Com **Backup IV*** (Backup)

With the following firmware options:

- IP Router (IP)
- IPX Router (IPX)
- Bridge (B)
- Multi-point (/M)
- Leased-line support (/V36)
- SNMP (/S)
- Encryption (/E)

The IP and IPX options may be valid for 6, 10 or an infinite number of hosts on the LAN side. That is, a ***Multi**Com* with the option IP6 will only route IP packets from 6 machines on the Ethernet interface (not counting itself).

NEW FEATURES 1.3

The firmware release 2.2.9 introduced:

- Editable Command Line Interface with history using bash-like controls
- Case-sensitive passwords
- Hardware information
- Multiple accounts and keys stored in Flash memory with a security locking mechanism
- ISDN support for USA and DDI mode with static TEI
- PPP encryption with session keys
- Encryption status display (see § 13.6, "Visual Status Display" on page 94)

The firmware release 2.3 introduced:

- Dynamic IP address reception
- DHCP Server, for easy PC configuration
- Port & Address Translation (PAT), to share an Single User Account (SUA)
- AutoConfig™, for a very easy Internet setup
- Simplified troubleshooting and statistics for ISDN and PPP

The firmware release 2.4 introduced:

- Dynamic IP address distribution
- Web Server, for easier configuration
- Multilink PPP (MP), for better throughput via channel bundling
- AutoDNS™, for an even easier Internet setup
- D-channel callback, for cost-free callback
- DES and 3DES support for encryption

The firmware release 2.5 introduced:

- Multiple PAT and multiple NAT (Multi-Internet™)
- `Upgrade` and `Diagnose` via the Web interface

The firmware release 2.6 introduced:

- A complete firewall with IP filtering
- Bigger ISDN history (100 vs. 30 lines)
- More sites on LAC & Series IV (500 vs. 200 sites)
- Better D-Channel display

The firmware release 2.6.1 introduces:

- Active FTP through address translation support
- Better IP filtering with port ranges and router traffic filtering
- Simple RIP broadcaster

For detailed information, please read §14.1 and following.

HOW THIS MANUAL IS ORGANIZED 1.4

APPROPRIATENESS 1.4.1

Each time that an appropriateness to a specific hardware or software option occur, the following table will be displayed:

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket	6,10,∞						
Classic	6,10,∞						
LAC							

The grayed cells indicates in which cases the following text applies. The contents of the cells may indicate further restrictions.

The top left cell indicates the firmware version needed.

In the above example, the text applies only to the ***Pocket*** *Multi****Com*** and ***Classic*** *Multi****Com*** hardware, with the IP router option. It is further valid for IP router with 6, 10 or infinite number of hosts on the LAN site. The minimum software version needed is 2.0.

TYPOGRAPHICAL CONVENTIONS 1.5

The following table describes the typefaces and symbols used in this manual.

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `config` file. Use `help` to get more information.
`AaBbCc123`	What you type, contrasted with on-screen computer output	`Username:` **`manager`** `Password:` **`manager`**
`AaBbCc123`	Command-line parameter: replace with a real name or value	To delete a file, type `rm` *`filename`*.

Table 1. Typographical conventions

A screen output from a ***MultiCom*** console will be displayed like this:

```
MultiCom:Uptime
7 hrs, 53 mins, 45 secs
MultiCom:
```

Bold characters represent user input.

WARNINGS, CAUTIONS, AND NOTES 1.5.1

Be sure that you understand all directions, warnings, and limitations before using this product. In this manual:

WARNING — Presents information or describe conditions which, if not observed, could result in personal injury or product damage.

CAUTION — Reflects conditions which could cause high expenses or data loss.

NOTE - This describes particular features on the use of the equipment or procedures which require the reader's attention.

Chapter 2

Product Description

*Welcome to Lightning's **MultiCom** family!*

*This chapter provides a product description and functional overview of the **MultiCom** family. Included in the description are typical applications, product features, and firmware information.*

OPTIONS 2.1

The ***MultiCom*** family comes with the following options:

- IP Router (IP)

  The IP Router forwards TCP/IP packets. This means that all applications that use this protocol will be remotely available, e.g. FTP, TELNET, NFS, SMTP, DNS, NNTP, etc.

- IPX Router (IPX)

  The IPX Router forwards Novell™ IPX/SPX packets. This means that all applications using this protocol will be available.

- Bridge (B)

  The ***MultiCom*** can also transparently bridge all other protocols.

- Leased-line support (/V36)

  This option allows you to use the serial port(s) available on the ***Classic MultiCom***, ***MultiCom LAN Access Center***, ***MultiCom Access IV***, and ***MultiCom Backup IV*** to connect to a synchronous leased line modem.

- Multi-Point (/M)

  This option allows your ***MultiCom*** to dialog with more than one remote ***MultiCom***.

- SNMP (/S)

  This options lets you manage your ***MultiCom*** through the Simple Network Management Protocol.

- Encryption (/E)

  This options lets you use strong encryption on transmitted data, at link or IP level, to guarantee the integrity and confidentiality of your data.

All Network Management can be done by remote access, or locally with a terminal, without service interruption. A built-in Flash-EPROM™ memory allows for remote firmware upgrades and updates of the available options, without having to physically access the router, using a simple activation key.

TYPICAL APPLICATIONS 2.2

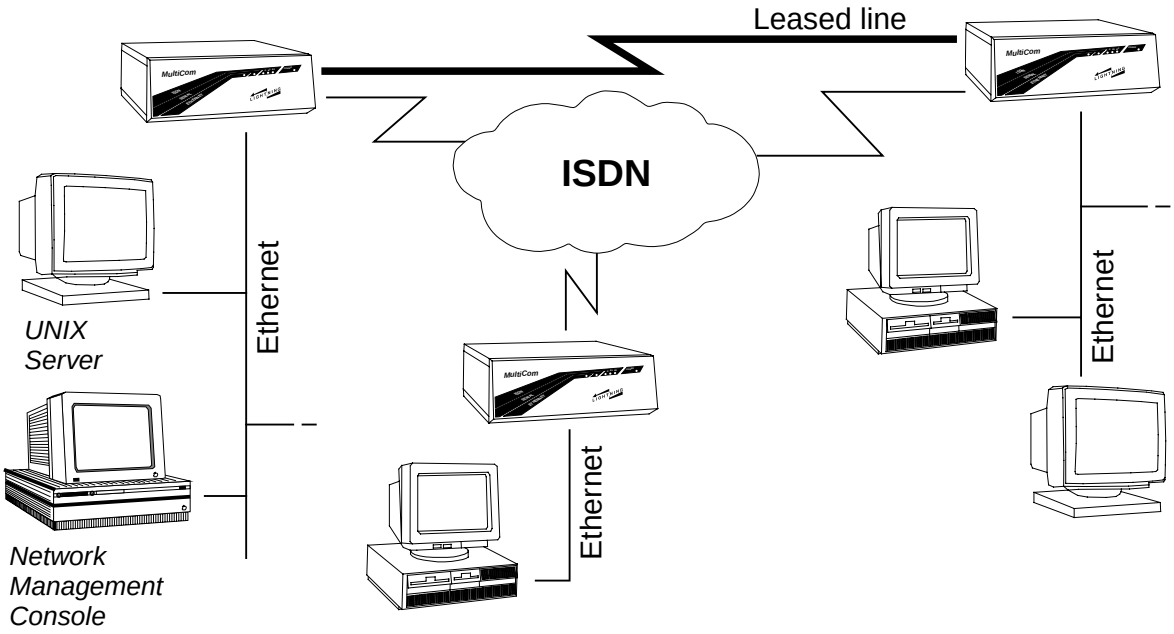


Figure 1 The ***Multi**Com* provides Ethernet connectivity through ISDN as well as through an optional leased line connection.

PRODUCT FEATURES 2.3

- TCP/IP routing with packet filtering
- IPX/SPX routing with spoofing
- Bridging all (or some selected) protocols
- High Security through access control and optional strong encryption
- Exclusive “Never Busy Line” feature, guaranteeing access to your ***Multi**Com*, even when all ISDN B-channels are busy
- Fully uses all ISDN B-channels, at up to 128 Kbps (BRI) or 2 Mbps (PRI)
- Serial port(s) for synchronous leased line modems
- Multi-Point operation
- Very easy installation, management and upgrade

- Support for leased B-Channels
- Stac LZS® compression for improved throughput
- Callback support for security or easier billing
- Easy installation using the EasyConfig™ Windows wizard or the built-in Web-server.
- Supports all major ISDN protocols (EuroISDN, Japan, USA)
- Includes a built-in DHCP server, for easy configuration of you computers
- Allows the sharing of a Single Internet User Account, thanks to Port & Address Translation
- Provides automatic security against intruders thanks to our SecureWall™ feature
- Can be setup for Internet access in a few minutes only, using our very simple AutoConfiguration™
- Provides detailed ISDN logs for billing and troubleshooting, as well as other powerful debugging commands

MULTIPLE PORTS 2.3.1

The ***Classic MultiCom*** has one Ethernet port and two Wide Area Network ports, one for the ISDN public network and one for leased line modems. Both can be used simultaneously for absorbing traffic peaks or as backup.

The ***Pocket MultiCom*** has only two ports, one Ethernet and one ISDN.

The ***MultiCom LAN Access Center*** has one Ethernet port, two leased line ports and four extension slots for PRI or multiple BRI boards.

ADVANCED ROUTING FEATURES 2.3.2

ADVANTAGES OF ROUTING 2.3.2.1

Routing, when possible, is very useful in Wide-Area Networks (WANs), where communication cost is an important factor, because it drastically reduces the number of broadcast packets that bridges would forward.

The ***MultiCom*** IP and IPX routers automatically open and close the ISDN connections, depending on the traffic. Not only does this reduce the overall communications costs, but it gives an unmatched flexibility to your network, thanks to the fast connection setup time of ISDN: you are on-line at off-line cost.

IP ROUTING 2.3.2.2

The ***MultiCom*** fully conforms to the widely-used TCP/IP Standards. Thus, the ***MultiCom*** can be used in multi-vendor environments and is completely independent of the Operating System in use (Windows, MacOS, Unix, ...)

SECURE ROUTING 2.3.2.3

Static routing tables are used for increased security, since network reconfiguration is fully under the control of the Network Manager.

IPX ROUTING 2.3.2.4

The ***MultiCom*** fully conforms to the "IPX router specification" from Novell®. Thus supporting most of the PC compatible networking environments.

ADVANCED BRIDGING FEATURES 2.3.3

PROTOCOL INDEPENDENCE 2.3.3.1

The ***MultiCom*** bridge operates at the Data Link level, filtering and forwarding the traffic according to Ethernet "MAC" addresses and protocols. The operation of the bridge is transparent to all higher level protocols, including NetBIOS® and NetBEUI®, Novell™, AppleTalk™, OSI, XNS™, TCP/IP, etc.

PROTOCOL FILTERING 2.3.3.2

Selectively allowing or denying protocols to transit through the bridge enables the Network Manager to control the use of the communication line.

SOURCE AND DESTINATION ADDRESS FILTERING 2.3.3.3

Traffic can also be filtered depending on its source or destination Ethernet address.

SELF-LEARNING 2.3.3.4

The bridge learns automatically all Ethernet addresses on the Local Area Network, to avoid transmitting local traffic on the (costly) ISDN links.

SERIAL PORTS 2.3.4

V 2.2.6	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

The Serial Ports can be used with synchronous modems at speeds of up to 512 Kbps on the ***Classic*** *Multi****Com*** and at 2 Mbps on the ***Multi****Com* ***LAN Access Center***, ***Multi****Com* ***Serial IV***, and ***Multi****Com* ***Backup IV***.

The ISDN connection can be used in conjunction with the Leased Line during periods of heavy traffic load, providing an overflow function. The ISDN connection can also provide a backup link, should the Leased Line connection fail.

MULTI-POINT 2.3.5

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

The Multi-Point option allows the local ***Multi****Com* to dialog with more than one remote ***Multi****Com*. In this way, more that two Ethernet networks can be interconnected.

EASY TO INSTALL AND OPERATE 2.3.6

INSTALLATION 2.3.6.1

The ***Multi****Com* is very easy to install and operate. It can be configured with its built-in Web-server, through a simple Windows wizard on a PC, or manually from a remote station or a local terminal attached to the serial console port.

ACTIVITY DISPLAY 2.3.6.2

Very clearly designed multicolored status lights provide a continuous display of Ethernet, Serial and ISDN status and activity.

NETWORK MANAGEMENT 2.3.7

PUBLIC NETWORK SECURITY FEATURES 2.3.7.1

Every Local Area Network contains critical data and resources which have to be protected against piracy. This protection has to be very efficient when access to and from public networks like ISDN is possible. Security is a strong feature of the ***MultiCom*** family and has been carefully integrated at every level of its design.

The ***MultiCom*** can use the calling number authentication feature of ISDN (CLI), and does not respond to calls from unauthorized numbers. The ISDN network's Closed User Groups (CLUG) feature is also supported.

The access by the network manager to the configuration features of the ***MultiCom*** is protected by an authentication procedure, preventing unauthorized users from reconfiguring the ***MultiCom***.

In addition, a very strong encryption mechanism, using 128 bits keys, is optionally available. It can encrypt all data on a point-to-point link or only selected packets, to form a secure Virtual Private Network (VPN).

REMOTE MANAGEMENT CAPABILITY 2.3.7.2

The access to the configuration of the ***MultiCom*** can be done with a simple Internet browser, by the EasyConfig™ Windows wizard or manually by Telnet and FTP from the local Ethernet network or from a distant network through ISDN or a leased line, allowing for centralized network management. This can also be done locally, from a terminal attached to the serial console port.

USER-FRIENDLY CONFIGURATION 2.3.7.3

The ***MultiCom*** can be configured on the fly without shutting down the power, allowing for *zero downtime*.

LINK COST CONTROL 2.3.7.4

All B-channels of the ISDN connection can be simultaneously used at full speed. However, a limit can be put on the number of B-channel allowed, on a site-by-site basis. The links are automatically opened and closed during operation, using a load-based algorithm.

FLASH-EPROM ELECTRONIC MEMORY 2.3.7.5

A built-in Flash-EPROM electronic memory allows for easy remote firmware upgrades and updates without having to physically access the router. This memory also permanently stores the ***Multi****Com* configuration.

The absence of moving parts and fan makes the ***Pocket*** *Multi****Com*** a sturdy platform capable of operating in dusty and hostile environments. Its low power consumption makes it also well-suited for use with emergency power supplies.

FUNCTIONAL DESCRIPTION 2.4

HARDWARE 2.4.1

Please refer to the corresponding User's Manual.

FIRMWARE 2.4.2

The ***Multi****Com* resident firmware runs in a multi-tasking environment and consists of a system, a real-time kernel, a File Manager, the protocols stacks, network management, and security components.

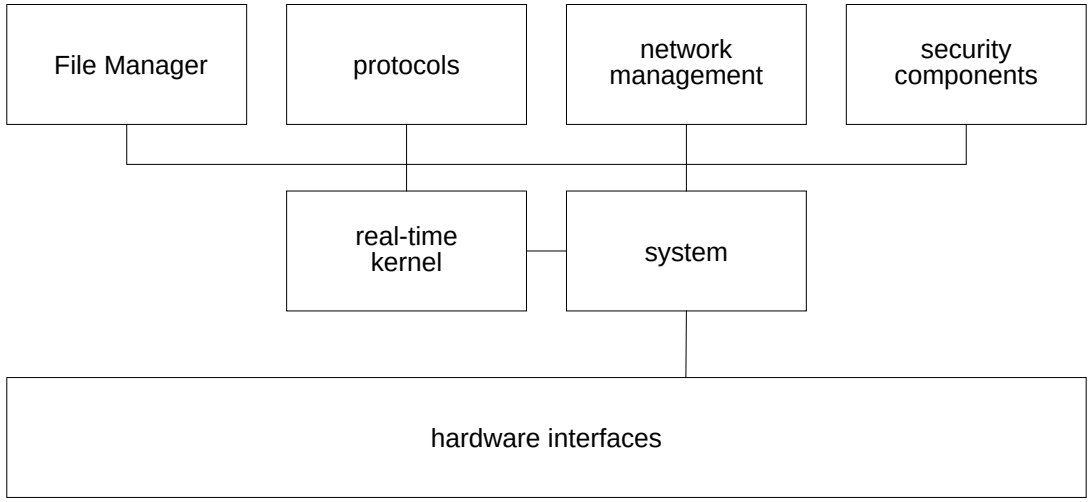


Figure 2 ***MultiCom*** firmware architecture

The current firmware revision is 2.6.1. To be notified of further firmware revisions, register on-line at http://www.lightning.ch/register.html, or return your Warranty Registration Card to LIGHTNING Instrumentation SA.

FLASH-EPROM ELECTRONIC MEMORY CONTENTS 2.4.3

The ***MultiCom*** has Flash-EPROM for storing information that must be kept when power is off. This information is listed below:

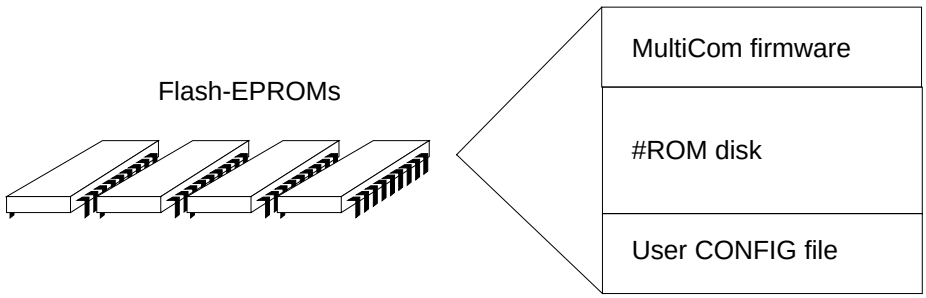


Figure 3 Flash-EPROM electronic memory contents

Specifically, it contains:

- The hardware interface, system, real time kernel and File Manager firmware

- A #ROM disk, where the default CONFIG file is stored
- The user CONFIG file (see § 15, "Configuration" on page 293, for more information).

FILE MANAGER 2.4.4

The ***MultiCom*** is designed to be able to manage files on two virtual disks as shown below in Figure 4:

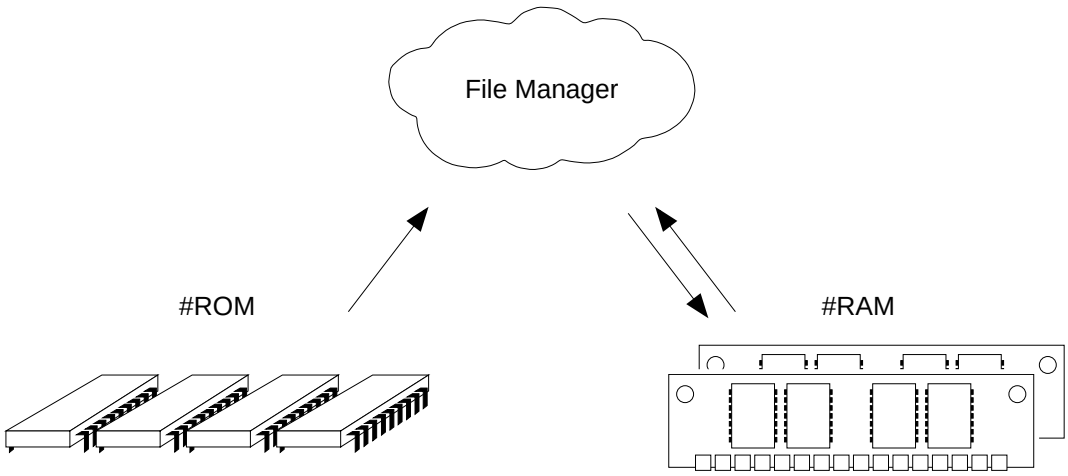


Figure 4 The File Manager interacts with two disks: #ROM and #RAM

- **#ROM**, stored on a Flash Erasable Programmable Read-Only Memory (Flash EPROM), contains the default CONFIG file (see “Configuration” on page 293 for more information about this file). The #ROM disk is read-only.
- **#RAM**, stored on Dynamic Random Access Memories (DRAM), contains run-time files such as the current CONFIG file. You can read and write on the #RAM disk.

The File Manager supports commands, described in § 14, "Commands" on page 97, which allow you to change the default disk, list the content of a disk or of a file, rename a file, remove a file and provide information on disk usage.

Chapter 3

Concepts

All you should know before you start, directly from the R&D laboratory.

FLASH-EPROM 3.1

This is a type of memory that has similarities to both RAM and ROM. Its similarity to RAM is that it can be modified on-line. It acts like a ROM in respect that it retains its contents even if the ***MultiCom*** is switched off.

In the ***MultiCom***, it is used to store both the firmware and the configuration. Unlike a ROM memory, it is possible to download a new release of the firmware and store it in the Flash-EPROM of your ***MultiCom***. See chapter 18 “Upgrading your MultiCom” on page 379 for more details).

THE CONFIGURATION FILE 3.2

The ***MultiCom*** contains a configuration file which is stored in Flash-EPROM. When the ***MultiCom*** boots, it executes the commands that it finds in this file. This file can be edited on the ***MultiCom***, downloaded from another machine using FTP or edited with the EditConfig Windows application.

See chapter 15 “Configuration” on page 293 for details on how to manually create or modify a CONFIG file.

It is also possible to enter commands on-line, however these commands are not automatically stored in the configuration file and their effect will be lost the next time the ***MultiCom*** reboots. This may be useful for debugging purposes.

SITES 3.3

WHAT IS A SITE? 3.3.1

A **Site** in the ***MultiCom*** represents a *path* to a network. The network can be the locally connected Ethernet or a remote Ethernet that is connected to another ***MultiCom***.

Each site has a unique name.

By default, a ***MultiCom*** contains two sites, named **ETH** and **ISDN**, as shown on figure 5.

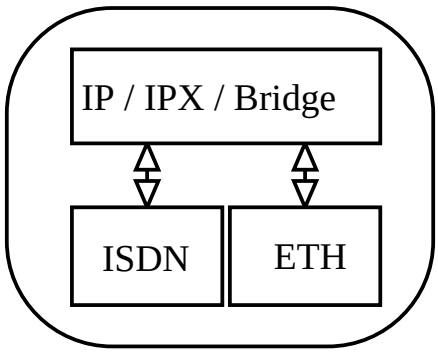


Figure 5 Default sites

The IP Router, IPX Router and the Bridge send and receive packets to and from sites.

For example, the IP Router can be configured to route one range of IP addresses on the ETH site and another range on the ISDN site. Similarly, the bridge can be setup to filter IPX traffic on the ETH site while letting it pass on the ISDN site.

TYPES OF SITES 3.3.2

There are two types of sites: Local Area Network (LAN) sites and Wide Area Network (WAN) sites. Then there are two types of WAN protocols: MHDLC (Lightning's proprietary extension to HDLC) and PPP (standard Point-to-Point Protocol).

There is only be one LAN site per ***MultiCom***, but there may be several WAN sites. Each MHDLC site corresponds to another ***MultiCom***. Each PPP site corresponds to a remote machine that may or may not be a ***MultiCom***.

THE ETH SITE 3.3.3

This is the only LAN site. It must be connected to the local Ethernet network.

THE ISDN SITE 3.3.4

This is the default WAN site. It may be used for ISDN **and** serial connections. Its name was retained for historical reasons.

RENAMING SITES 3.3.5

Sites can be renamed using the command `Site Rename` (see § 14.18.119 on page 267). We strongly advise you to use this feature to give meaningful names to your sites. For example, it may be convenient to rename ETH to Geneva and ISDN to Paris. This makes the ***MultiCom***'s configuration file easier to understand.

MULTI-POINT 3.3.6

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

If you have purchased the Multi-Point option for your ***MultiCom***, it is possible to create more than one WAN site. This allows the local ***MultiCom*** to connect to sev-

eral remote networks. In this way, it is possible to interconnect several remote Ethernet's together, while only having to purchase one ***MultiCom*** per Ethernet.

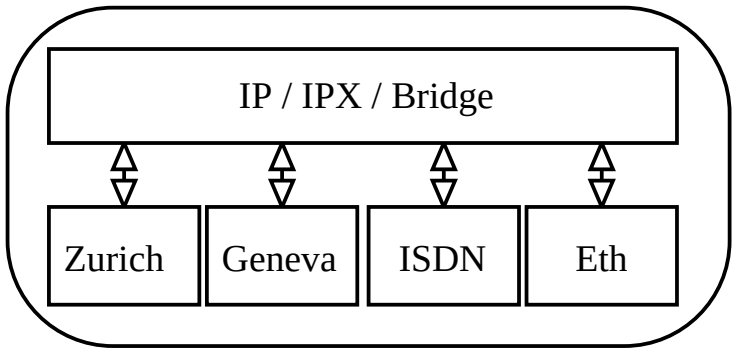


Figure 6 Sites in a Multi-Point ***MultiCom***

The figure 6 shows a multi-point setup where two new WAN sites have been added.

A ***MultiCom*** that does not have the Multi-Point option is said to be a Point-to-Point ***MultiCom***.

CREATING ADDITIONAL SITES 3.3.7

If you have the Multi-Point option, you can create new WAN sites. When creating a site, you must specify its name and protocol using the command `Site Create` (see § 14.18.116 on page 262).

THE SELECTED SITE 3.3.8

Many of the ***MultiCom***'s commands apply to the selected site. The selected site can be changed using the command `Site Select` (see § 14.18.120 on page 268). The command `Site Info` (see § 14.18.117 on page 264) lists all sites and indicates which one is the selected site.

Chapter 4

TCP/IP

*The Internet Protocol. Have a look at how the **MultiCom** connects you to it.*

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

IP ADDRESSES 4.1

WHAT IS AN IP ADDRESS 4.1.1

An IP address is a 32 bit number that uniquely identifies a host on the Internet. IP addresses are written as four decimal bytes separated by dots. For example: `193.5.2.1`.

IP addresses are also referred to as IP numbers.

Each ***MultiCom*** needs a unique IP address for its configuration, even if it is used as a Bridge or IPX Router. Once the ***MultiCom*** has a valid IP address, it can be accessed with Telnet, FTP and WWW.

STRUCTURE OF AN IP ADDRESS 4.1.2

When a company needs to reserve unique IP addresses, it does so by contacting an IP Registration Authority. This authority will allocate a block of consecutive numbers, e.g. `193.5.2.`*x*. The last part of the address (i.e. *x*) can be assigned in any way the company wishes, but the first part (i.e. first three bytes) remains fixed.

IP NETWORKS 4.1.2.1

The first, fixed, part of the address is known as an IP Network, or the network part of the address. The last part (i.e. x) is known as the host address or host part of the address.

The IP standard defines three main classes of IP Networks:

- **Class A** networks: the first byte is fixed by the registration authority and the company is free to assign the last three bytes (e.g. `32.x.x.x`). Class A networks must be in the range `0.x.x.x` to `126.x.x.x`.
- **Class B** networks: the first two bytes are fixed by the authority and the company may set the last two bytes (e.g. `128.172.x.x`). Class B networks must be in the range `128.0.x.x` to `191.255.x.x`.

- **Class C** networks: the first three bytes are fixed by the authority and the company may set the last byte (e.g. `193.172.38.x`). Class C networks must be in the range `192.0.1.x` to `223.255.254.x`.

IP SUBNETS 4.1.2.2

Once a company has reserved an official IP Network number, it is free to assign the host part of the address as it wishes. The simplest way of doing so is to assign the first host the address 1, the second host the address 2 and so on. However, as the number of hosts grows, it will become necessary to assign the addresses in a more structured manner. This is known as **IP Subnetting**.

IP Subnetting consists of sub-dividing the host part of the address into two parts, the subnet part and a (smaller) host part. IP Subnets are typically assigned to individual physical networks (e.g. Ethernet or Token- Rings).

As an example, consider a company that has reserved the IP Network `128.190.x.x`. It might decide to use the third byte (i.e. the first x) as the subnet number and the last byte as the host part of the address. The company has two buildings, each with it's own Ethernet network. The two Ethernets are linked together by an IP Router. Hosts in the first building could be assigned addresses of the form `128.190.1.x` and hosts in the second building `128.190.2.x`. This makes the configuration of the IP router much simpler.

IP SUBNET MASKS 4.1.2.3

In the above example, the subnet part of the address was the third byte and the host part was the last byte. Put a different way, of the 16 available bits, the upper eight were assigned to the subnet part and the lower eight to the host part. It is possible to choose a different boundary between the two. For example, it is possible to assign the upper 4 bits to the subnet part and the lower 12 bits to the host part. This allows for 16 different IP Subnets, each containing a maximum of 4096 machines.

The boundary between the subnet part and the host part of the address is specified by a Subnet Mask. The mask has the bits set to 1 for the network and subnet parts of the address and 0 for the host part. It is up to the Network Manager to decide the size of the subnet mask.

In the above example, where the third byte is the subnet part, the subnet mask is `255.255.255.0`. In the case where there are only 4 bits for the subnet part, the mask would be `255.255.240.0`.

IP BROADCASTS 4.1.3

IP Broadcasts are sent to a group of machines. The number of machines that a broadcast reaches depends on the type of the broadcast. There are three types of broadcast:

- Network broadcasts.
- Subnet broadcasts.
- Cable broadcasts.

NETWORK BROADCASTS 4.1.3.1

These broadcasts are sent to all hosts in the IP Network. These addresses have all the bits in the subnet and host parts of the address set to 1. The above example network has the network broadcast address `128.190.255.255`.

SUBNET BROADCASTS 4.1.3.2

Subnet broadcasts are sent to all hosts in the same subnet. The host part of the address has all its bits set to 1. In the above example, the subnet in the first building would have the subnet broadcast address of `128.190.1.255`.

CABLE BROADCASTS 4.1.3.3

These broadcasts are received by all hosts on the local physical network. The address is `255.255.255.255`.

IP HOST 4.2

The IP host in the ***MultiCom*** is always reachable, since it doesn't use the IP Router. It may be accessed like any other IP machine.

To work properly the IP host needs:

1. An IP address (see § 14.18.27, "IP MyAddr" on page 144)
2. An IP subnet mask (see § 14.18.34, "IP SubnetMask" on page 154)

NOTE - This is also valid in bridging and IPX mode.

PURPOSE 4.2.1

Inside the IP host reside the following software modules:

- DHCP server
- ICMP server/client
- FTP server
- SNMP agent
- SNTP client
- Syslog client
- Telnet server/client
- Web server

These software modules allow you to connect remotely to a ***MultiCom***, to exchange configuration files and to manage the ***MultiCom***.

NOTE - The new default IP address of the ***MultiCom*** since the 2.3 firmware release is **`10.0.0.1`**. It was `1.1.1.1` in older releases.

IP ROUTER 4.3

IP packets are directed through an internetwork using information from a routing table in each ***MultiCom*** IP Router. The routing table indicates on which network a data packet should be forwarded.

IP routing tables can be maintained in two ways :

- Statically, where the routing information is manually entered by the network administrator.
- Dynamically, where the routing information is automatically passed between routing devices using a routing protocol.

The IP Router, in its current release, only supports static routing tables. Since network re-configuration is under the control of the network manager, the use of static routing tables increases security. Another advantage of using static routing over dynamic routing is the reduction of traffic.

For higher availability, we also support a limited RIP broadcaster (see § 14.18.95, "RIP" on page 238).

CONFIGURATION 4.3.1

To configure the IP router you should:

1. Define the ***MultiCom***'s IP address (see § 14.18.27, "IP MyAddr" on page 144).
2. Define the IP range for each site (see § 14.18.28, "IP Range" on page 146).
3. Turn the IP Router On (see § 14.18.30, "IP Router" on page 149).

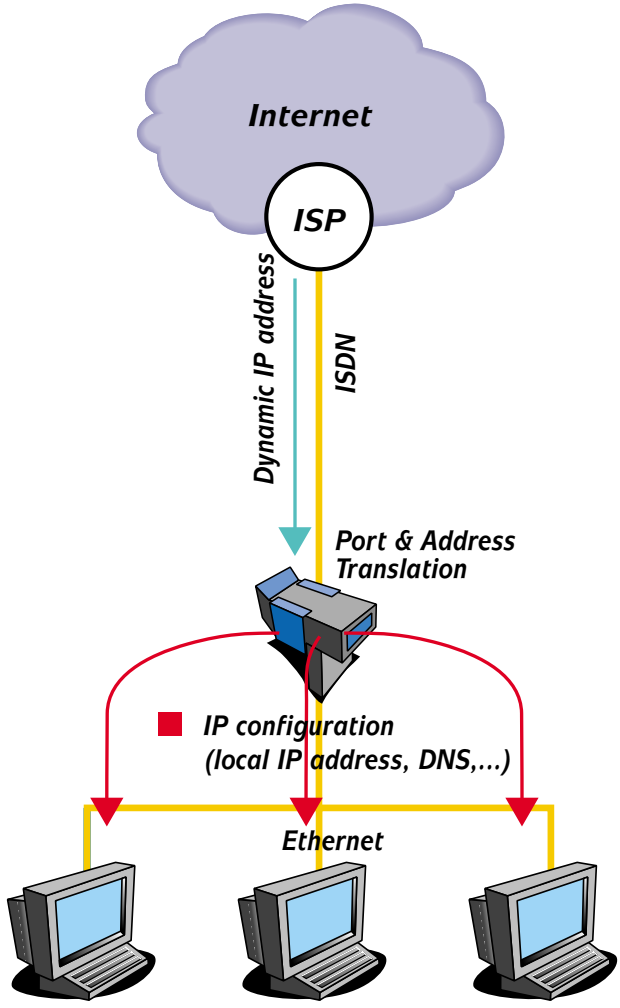
NOTE - Depending on the software option you bought, the number of IP hosts on the LAN site (excluding the router itself) may be limited to 6, 10 or not limited. **If you try to add an IP Range with more IP addresses than you are allowed, the whole range will be rejected!**

IP TRANSLATION 4.4

This feature can dynamically translate private internal IP addresses into legal external Internet addresses. You can disable this feature if you have your own range of legal IP addresses, which you would like to be visible “as is” from remote external sites.

PAT 4.4.1

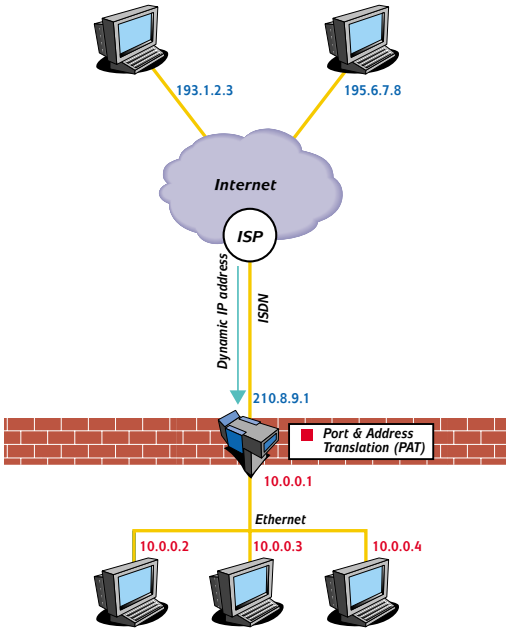
The firmware 2.3 introduced the IP address translation known as Port & Address Translation (PAT) or Single Internet User Account (SUA). This feature allows to share a single IP address among a whole network, thus reducing the cost of Internet connection and simplifying the management of remote networks.

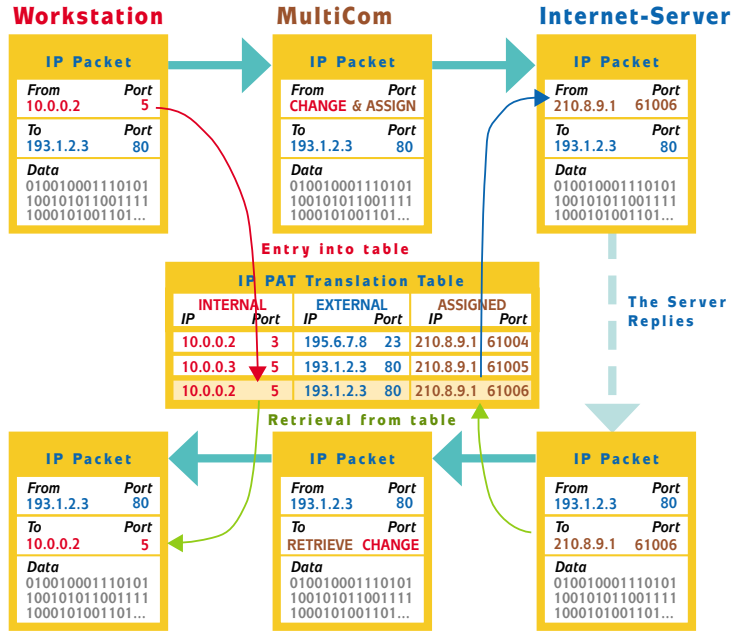


It works by replacing the source address and port number of all outgoing requests, and logging them in an IP Translation table. When the corresponding reply comes, the correct destination and port will be retrieved from the table (see below).

This will hide all your local machines behind a single IP address and, since it records all outgoing requests, this allows to filter and record all unwanted incom-

ing accesses, thus providing a SecureWall™ protection of your network against unsolicited accesses and hacker attacks from the Internet.





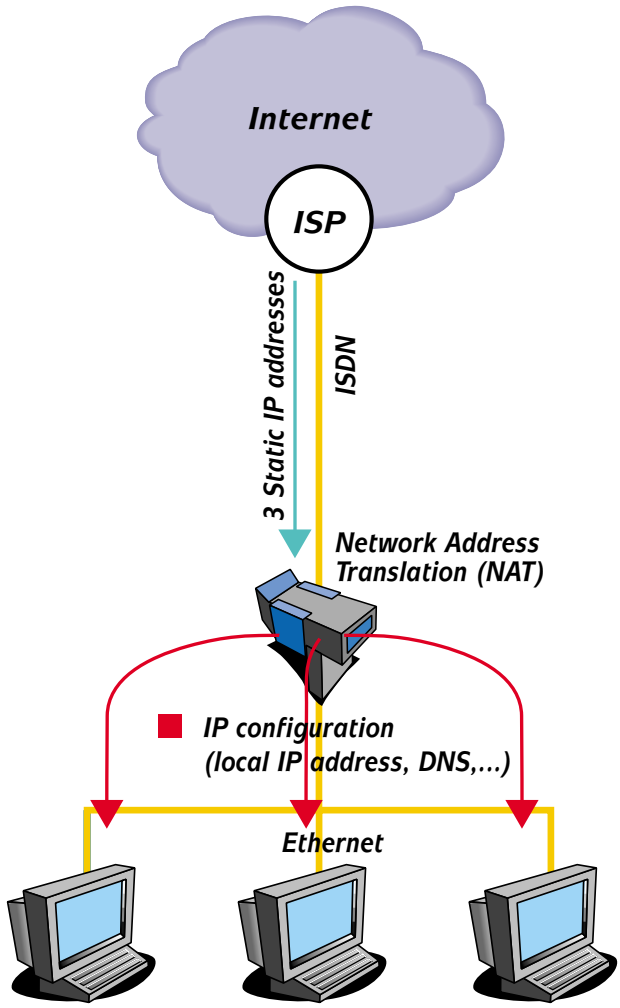
You can statically allow some services (like www, mail, new, telnet, ...) to reach a specific internal machine (and optionally change the destination port as well). In that case, you will probably need a static address. Indeed, if your address changes dynamically, it will be difficult to reach you from the Internet.

NAT

4.4.2

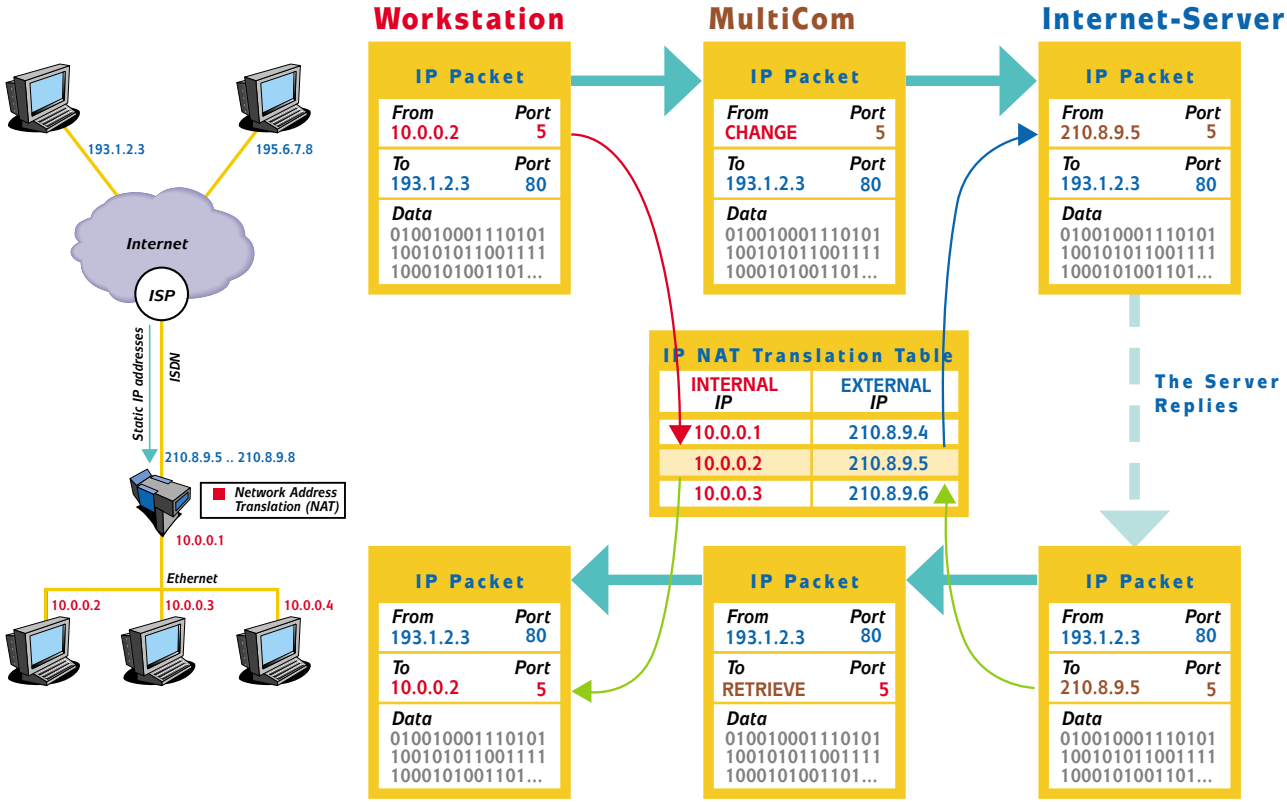
The firmware 2.5 introduces another IP address translation, known as Network Address Translation (NAT). This feature transparently remaps IP addresses in TCP and UDP packets, allowing full external access to internal machines.

A domain with a set of private network addresses can be enabled to communicate with the external network by dynamically mapping to a set of global network addresses. Local nodes allowed to have simultaneous access to the external network are limited by the number of addresses in the global set. In addition, individual local addresses may be statically mapped to specific global addresses to ensure guaranteed access to the outside or to expose a local node for total access from the outside.



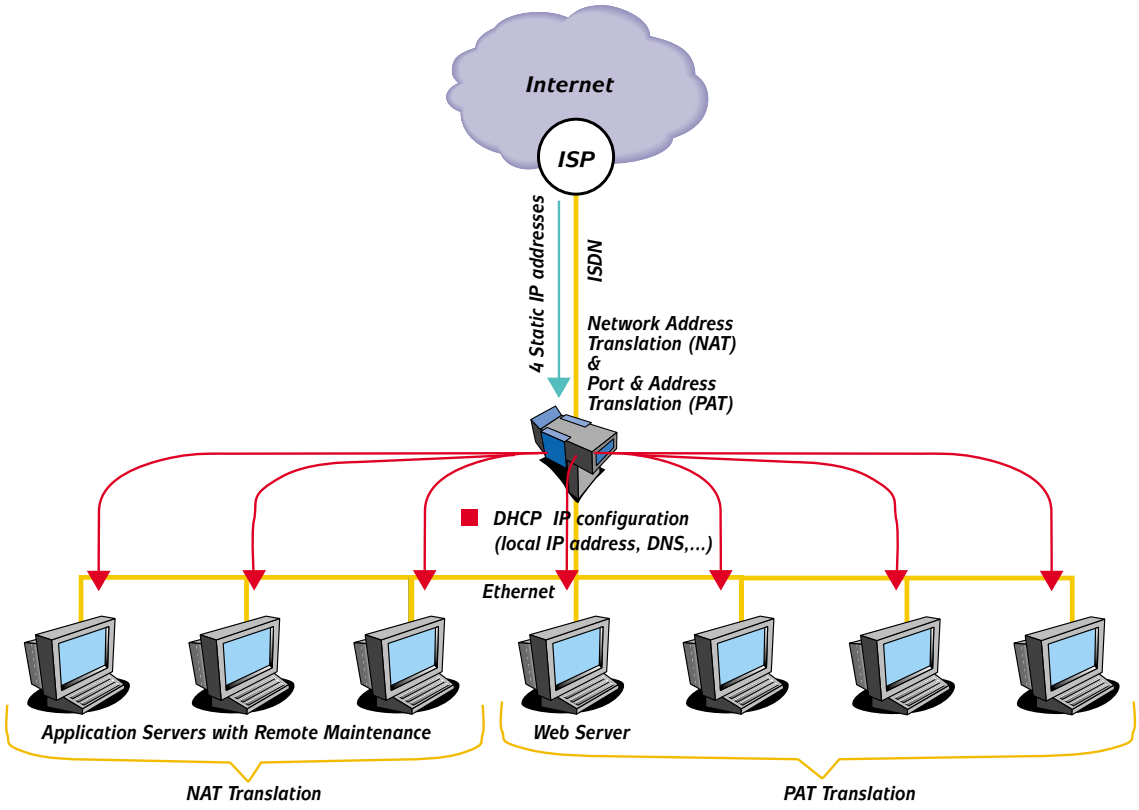
Static addresses are needed if you want to provide services like mail and web to the outside world. Indeed, if your address changes dynamically, it will be difficult to reach you from the Internet.

For each entry in the NAT table, you can specify the External IP Address that is used by NAT: either the address received dynamically from your Internet Service Provider, the global IP address of the MultiCom itself, or a static IP Address, and map this external address to an Internal IP Address.



COMBINATION 4.4.3

These two features can be used simultaneously for maximum flexibility. For example, you can expose three dedicated servers to the outside world, while protecting all your other machines behind the SecureWall™, using only four IP addresses.



LIMITATIONS 4.4.4

The following restrictions apply for the configuration of NAT & PAT:

- A PAT range cannot overlap any other range
- External and Internal IP addresses that are already mapped with PAT can not be mapped with NAT.
- External and Internal IP addresses that are already mapped with NAT can not be mapped with PAT.
- Only one single NAT translation can be specified for a given external or internal address.
- If the default external site address is set and another default external site address was already specified, the old value is replaced.

- The internal destination address of the `IP Translation Map` command has to be included in the range corresponding to the specified external address. If no external address is specified, the internal destination address must be included in a range that is mapped to the default external address, or not included in any range.
- When adding a new range of internal addresses, if an entry already exists in the port mapping table with an internal destination address which is included in the range being added, the entry is removed from the port mapping table.
- Currently, there is no support for translating the data payload, so protocols that transmit IP addresses and ports in the payload may not work, or work only with some limitations. For instance, FTP in the outgoing direction only works in passive (or "firewall") mode, which is the default with Netscape and Internet Explorer. Incoming FTP works in normal active mode.
- If the default site address, or the dynamically allocated address, is equal to an address already specified with an explicit range, all internal addresses that are in the specified range, as well as all addresses that are not explicitly in any range, are mapped to the site address. In the case of a dynamically allocated address this is true only for the duration of the allocation.
- If the dynamically allocated address turns out to be identical to an external address already specified in a NAT entry, or in a port translation mapping for the same port, it is not defined which entry takes precedence (as long as the dynamic allocation lasts).
- Frames encrypted by the MultiCom IP-level encryption cannot be translated.
- IP fragments are recognized and dropped, because there is no way to translate them.

CAUTION — Using NAT will disable the SecureWall™ on some machines, which can open a security hole in your network, from which other machines protected by the SecureWall™ may be attacked. Use it at your own risk!

EXAMPLES 4.4.5

EXAMPLE FOR A STATIC CONFIGURATION 4.4.5.1

If the configuration file contains the following commands:

```
IP SiteAddr 192.168.10.1 For 10.0.0.0 .. 10.0.255.255
IP SiteAddr 192.168.10.2 MapTo 10.1.1.1
IP SiteAddr Global For 10.3.0.0 .. 10.3.255.255
IP SiteAddr 192.168.10.3
IP Translation Map 192.168.10.1:21/tcp To 10.0.0.1:2121
IP Translation Map Global:80/tcp To 10.3.1.1
IP Translation Map 80/tcp To 10.2.2.2:8080
IP Translation On
```

the behavior will be as follows:

• Outgoing packets with a source address between `10.0.0.0` and `10.0.255.255` will be translated with PAT to the external address `192.168.10.1`.

• Outgoing packets with a source address of `10.1.1.1` will be translated with NAT to the external address `192.168.10.2` and incoming packets with a destination address of `192.168.10.2` will be translated with NAT to the internal address of `10.1.1.1`.

• Outgoing packets with a source address between `10.3.0.0` and `10.3.255.255` will be translated with PAT to the global external address (the IP address of the router).

• All outgoing packets with a source address not mentioned in the first three cases will be translated with PAT to the default external address `192.168.10.3`.

• All incoming packets with a destination address of `192.168.10.1` and a destination port of `21/tcp` will be translated with PAT to the port `2121` of the address `10.0.0.1`.

• All incoming packets with the global destination address and a destination port of `80/tcp` will be translated with PAT to the same port (`80/tcp`) of the address `10.3.1.1`.

• All incoming packets with a destination address of `192.168.10.3` and a destination port of `80/tcp` will be translated with PAT to the port `8080` of the address `10.2.2.2`.

• All other incoming packets that are not in reply to a previously outgoing packet will be dropped (and optionally logged with `Syslog`).

EXAMPLE FOR A DYNAMIC CONFIGURATION 4.4.5.2

If the configuration file contains the following commands:

```
IP SiteAddr 192.168.10.1 For 10.0.0.0 .. 10.0.255.255
IP SiteAddr 192.168.10.2 For 10.3.0.0 .. 10.3.255.255
IP SiteAddr Dynamic MapTo 10.1.1.1
IP SiteAddr 192.168.10.3
IP Translation Map 192.168.10.2:23/tcp To 10.3.1.1
IP Translation Map 80/tcp To 10.2.2.2:8080
IP Translation On
```

the behavior will be as follows:

- Outgoing packets with a source address between `10.0.0.0` and `10.0.255.255` will be translated with PAT to the external address `192.168.10.1`.
- Outgoing packets with a source address between `10.3.0.0` and `10.3.255.255` will be translated with PAT to the external address `192.168.10.2`.
- Outgoing packets with a source address of `10.1.1.1` will be translated with NAT to the external address which was allocated dynamically by the ISP, while incoming packets to the dynamically allocated destination address will be translated with NAT to the internal address of `10.1.1.1`.
- All outgoing packets with a source address not mentioned in the first three cases will be translated with PAT to the default external address `192.168.10.3`.
- All incoming packets with a destination address of `192.168.10.2` and a destination port of `23/tcp` will be translated with PAT to the same port of the address `10.3.1.1`.
- All incoming packets with a destination address of `192.168.10.3` and a destination port of `80/tcp` will be translated with PAT to the port `8080` of the address `10.2.2.2`.
- All other incoming packets that are not in reply to a previous outgoing packet will be dropped (and optionally logged with `Syslog`).

IP DISTRIBUTION 4.5

The ***MultiCom*** is able to automatically receive and distribute IP addresses using the PPP protocol. Each site can be allocated its own static IP address. Addresses can also be dynamically allocated to remote clients, from a pool of available IP addresses. This is very useful for Internet Service Providers or for managing big corporate networks.

NOTE - This exclusive feature **is compatible with Dial-On-Demand and PAT**, by trying to re-allocate the same IP address to the same client, whenever possible. This avoids breaking idle connections, unlike many other products!

IP FILTERING 4.6

The ***MultiCom*** is able to filter out IP and ICMP packets, depending on their source and destination addresses and their source and destination ports.

The IP filter is constituted by a global table of packet types and associated actions. Every IP packet going through the router is matched sequentially against each entry of the table, until a matching entry is found. Once it is found, the packet is either allowed through the router, or rejected, according to the action specified in the matching table entry. If no matching entry is found in the table, the packet is rejected. Every time a packet matches a table entry, a counter associated to this entry is incremented. There is also a counter for packets that didn't match any table entry. There is no possibility to send back to the source a notification (ICMP message) that a packet has been rejected. It is possible however to send a syslog notification on every rejected packet, for intrusion detection or statistical purpose.

If IP translation is in place, the filter is applied on the untranslated packet, i.e. before translation on outgoing packets and after reverse translation on incoming

packets. Similarly, the filter is applied before IP-level encryption takes place, i.e. on unencrypted packets.

Only the first packet of a TCP connection is subject to filtering. Subsequent packets are always allowed through. This allows to filter TCP connections differently based on their direction.

The filter table is global to the router. There is no possibility to have different filtering rules for different sites. The number of entries in the table is limited to 64.

IP packets whose higher-level protocol is not one of TCP, UDP, or ICMP are always rejected. Non-IP packets are not subject to filtering and are thus always allowed through. IP fragments with a non-zero fragment offset are always allowed through.

EXAMPLES 4.6.1

- The following configuration is an example of a restrictive configuration, where only explicitly allowed services can go through.

```
# Allow all Web access
IP Filter Allow From Any To Any Port 80/tcp

# Allow outgoing Telnet access
IP Filter Allow From 10.0.0.1 .. 10.255.255.255 To Any Port 23/tcp

# Allow DNS access to our DNS server only (193.247.134.2)
IP Filter Allow From 193.247.134.2 Port 53/udp To 10.0.0.1 .. 10.255.255.255
IP Filter Allow From 10.0.0.1 .. 10.255.255.255 To 193.247.134.2 Port 53/udp

# Allow pings
IP Filter Allow From Any To Any ICMP EchoRequest
IP Filter Allow From Any To Any ICMP EchoReply

# Everything else is denied by default
```

- The following configuration is an example of blocking NetBIOS traffic that can cause unnecessary ISDN connections, while allowing all other traffic.

```
# Block NetBIOS packets
IP Filter Deny From Any To Any Port 137 .. 139/tcp
IP Filter Deny From Any To Any Port 137 .. 139/udp
# All other traffic is allowed
IP Filter Allow From Any To Any
```

- The following configuration is an example of allowing Telnet access only to a specific server (`10.0.0.1`) and denying it to all other machines on the local network (`10.x.x.x`), while still allowing Telnet access from local machines to anywhere.

```
IP Filter Allow From Any To 10.0.0.1 Port 23/tcp
IP Filter Deny  From Any To 10.0.0.2 .. 10.255.255.255 Port 23/tcp
IP Filter Allow From 10.0.0.1 .. 10.255.255.255 To Any Port 23/tcp
```

- The following configuration is an example of allowing **active** outgoing FTP connections.

```
IP Filter Allow From 10.0.0.1 .. 10.255.255.255 To Any Port 21/tcp
IP Filter Allow From Any Port 20/tcp To 10.0.0.1 .. 10.255.255.255 Port 1024 ..
65535/tcp
```

- The following configuration is an example of allowing **passive** outgoing FTP connections.

```
IP Filter Allow From 10.0.0.1 .. 10.255.255.255 To Any Port 21/tcp
IP Filter Allow From 10.0.0.1 .. 10.255.255.255 To Any Port 1024 .. 65535/tcp
```

MORE INFORMATION 4.7

COMMANDS 4.7.1

For more details on commands related to IP routing, see § 14.18.24, "IP DefaultRouter" on page 139 and following paragraphs.

EXAMPLES 4.7.2

- For examples on how to configure the IP router, see § 17.1, "IP: Point-to-Point" on page 314 and § 17.2, "IP: Multi-Point" on page 318.
- For examples of IP translation, see § 17.9, "PPP: Internet Access" on page 353, § 17.11, "IP Translation: Single NAT" on page 361 and § 17.12, "IP Translation: Multiple PAT/NAT" on page 364.
- For an example of dynamic IP distribution, see § 17.10, "PPP: Teleworking" on page 357.

Chapter 5

IPX/SPX

Simple and all automatic : this is the proprietary IPX/SPX from Novell®.

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

INTRODUCTION 5.1

The ***MultiCom*** IPX router follows two different specifications.

For the basic IPX router, it follows the “IPX Router Specification”, Part Number 107-000029-001, Document Version 1.20, Novell®, October 14, 1993.[1], from Novell®.

For the “Demand RIP” protocol used on the ISDN lines to reduce the traffic, it follows Meyer G., “Extensions to RIP to Support Demand Circuits”, RFC 1582, Spider Systems, February 1994.[3].

Please refer to the first document for more information on IPX and the behavior of an IPX router. We will focus here on the configuration and specialities of the ***MultiCom*** IPX router.

IPX SITE TYPES 5.2

When the IPX option is present, an IPX extension is created for each site defined in the ***MultiCom***. See § 3.3, "Sites" on page 19, for details on sites in the ***MultiCom***.

The behavior of the IPX router will slightly differ according to the site type. There are, in the current version, three possible site types:

- LAN
- WAN
- Demand WAN

LAN 5.2.1

The “LAN” IPX site type is bound to an Ethernet interface. It behaves as described in [1]. In addition, it may filter some kind of packets as described in “Spoofing” on page 44. This is the default value for a local site.

WAN 5.2.2

The “WAN” IPX site type is bound to an ISDN or serial interface. It behaves as described in [1].

DEMAND WAN 5.2.3

The “Demand WAN” site type is bound to an ISDN or serial interface. It behaves as described in [3]. In short, the RIP and SAP updates are made only when necessary, in order to keep the ISDN line closed.

As the RIP and SAP updates are no longer periodical, they are acknowledged to avoid losses.

See § 14.18.43, "IPX SiteType" on page 167 for details on how to change the site type.

This is the default value for a remote site.

CAUTION — These spoofing protocols being implemented differently by each manufacturer, **we cannot guarantee that a connection can be made with another router in Demand WAN mode**.

COMMON PARAMETERS 5.3

ETHERNET FRAME TYPE 5.3.1

All the sites may handle various Ethernet formats, but each site may handle only one type of Ethernet frames at a time. Possible types are:

- 802.2
- 802.3
- SNAP

- Ethernet II

The default value for each IPX site, as recommended in [1], is 802.2. See § 14.18.36, "IPX EthType" on page 157, for details on how to change the Ethernet type.

SITE ACTIVITY 5.3.2

Each IPX site may be turned on or off. In a multi-protocol version of the ***MultiCom***, it allows the user to define which site use IPX and which don't.

By default all sites are in the 'off' state. See § 14.18.42, "IPX Site" on page 166, for details on how to change the site state.

SPOOFING 5.4

In order to reduce the amount of traffic and to keep the ISDN line closed on idle conditions, the ***MultiCom*** implements some filtering also known as 'spoofing'.

The following packets are spoofed by the IPX router:

- IPX Watchdog packets
- SPX Watchdog packets
- Serial number packets

See § 14.18.44, "IPX Spoofing" on page 169, for details on how to turn these features on or off.

Some routers implement also spoofing for RIP and SAP broadcast packets. This is not necessary with the ***MultiCom*** since it implements Demand RIP on ISDN connections. See "Demand WAN" on page 43. or [3] for details on Demand RIP. See § 14.18.43, "IPX SiteType" on page 167, for details on how to make a site use demand RIP.

INSTALLATION GUIDE 5.5

For each site you must:

- Select the site
- Set the network number
- Set the Ethernet frame type
- Set the site type
- Set the site on or off

That is:

```
MULTICOM: Site Select my_site
Site “my_site” selected.
MULTICOM: IPX NetNumber 0xabc1
IPX net number for site “my_site” set to 0xabc1.
MULTICOM: IPX EthType 802.2
IPX eth type for site “my_site” is 802.2.
MULTICOM: IPX SiteType WAN
IPX site type for site “my_site” is WAN.
MULTICOM: IPX Site On
IPX protocol for site “my_site” is active.
```

When each site is configured you may turn the router on:

```
MULTICOM: IPX Router On
IPX router is on.
```

MORE INFORMATION 5.6

COMMANDS 5.6.1

For more details on the IPX commands, see § 14.18.36, "IPX EthType" on page 157 and following paragraphs.

EXAMPLES 5.6.2

For examples on how to configure an IPX router, see § 17.3, "IPX: Point-to-Point" on page 323.

REFERENCES 5.6.3

[1] “IPX Router Specification”, Part Number 107-000029-001, Document Version 1.20, Novell®, October 14, 1993.

[2] Meyer G., “Protocol Analysis for Extensions to RIP to Support Demand Circuits”, RFC 1581, Spider Systems, February 1994.

[3] Meyer G., “Extensions to RIP to Support Demand Circuits”, RFC 1582, Spider Systems, February 1994.

Chapter 6

Bridge

Bridging with bridge groups: the simplest and way to connect two networks.

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

INTRODUCTION 6.1

From the firmware release v2.0 on, the ***Multi**Com* contains a new version of the bridge. The main differences between this version and the previous one are as follows:

- A more flexible and powerful filtering system.
- The ability to segment the ***Multi**Com* into several logical bridges (bridge groups).
- A new command interface which is *not* compatible with the previous version.

CAUTION — If you already use a 1.x version of the bridge, you will have to modify the config file when upgrading to 2.x. The bridge commands have been completely redesigned.

STRUCTURE OF BRIDGE 6.2

BRIDGE GROUPS 6.2.1

The new version of the bridge now supports several logical bridges, called *Bridge Groups*. A bridge group consists of several sites that need to be interconnected. A site may be connected to *only one bridge group*.

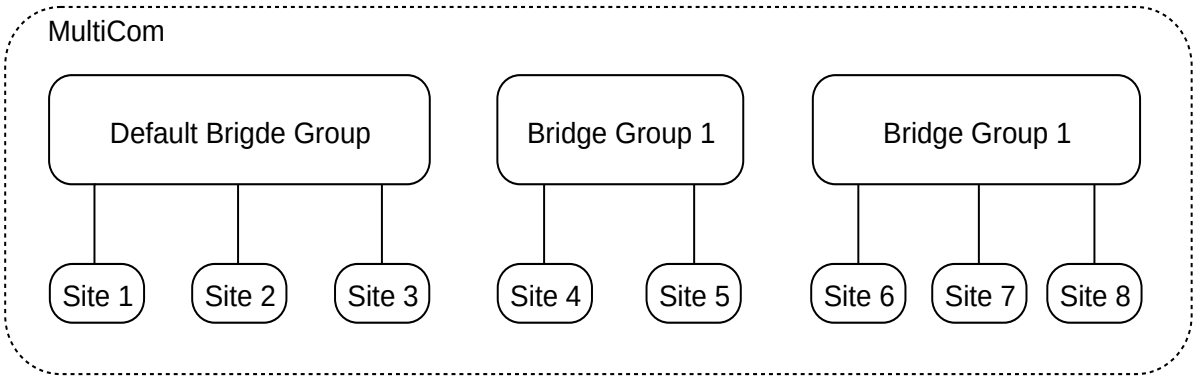


Figure 7 Bridge Groups

The use of bridge groups have several advantages:

- This ability to manage several separate logical bridges within the same ***MultiCom***. Traffic from one group is totally separated from other groups.
- Limiting broadcasts: one of the main problems with a bridge is that unfiltered broadcasts are sent to all sites. By using bridge groups, unfiltered broadcasts are only sent to the sites that are attached to that particular bridge group.
- Scalability: In the ***MultiCom LAN Access Center***, which supports multiple Basic Rate ISDN (BRI) connections or Primary Rate Interfaces (PRI), the maximum number of sites is 200. The cost of bridging broadcasts among so many sites is excessive, however by fragmenting into bridge groups, costs can be reduced.
- Security: traffic from one bridge group is not visible to another bridge group.

THE DEFAULT BRIDGE GROUP 6.2.1.1

By default, all sites are attached to the Default Bridge Group. It is not capable of bridging, it is simply a holding place for unused sites.

FILTERING 6.2.2

The filtering mechanism in the ***MultiCom*** has been modified. There are now three types of filters:

- Input filters
- Output filters
- Group filters

Each site may have its own input and output filter. The group filter belongs to a Bridge Group and is shared by all sites that are attached to that group (see Figure 8).

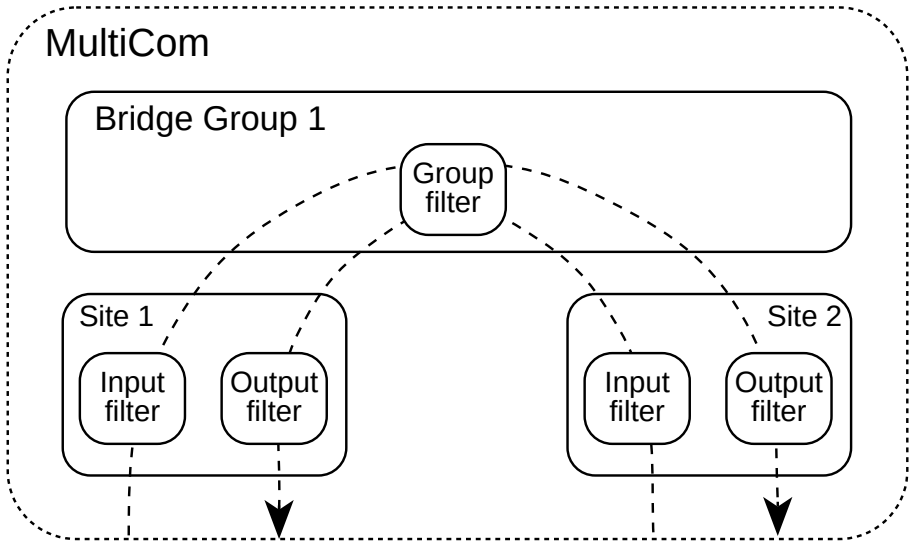


Figure 8 Filtering

A frame first passes through the input filter of the site on which it was received. It then goes through the group filter, and finally the output filter of the destination site. If the frame needs to be sent to several sites (e.g. a broadcast), the frame must pass through the output filter of each destination site.

Each filter contains five filter tables as follows:

- Source address filter table
- Destination address filter table
- Ethernet II protocol filter table
- SAP protocol filter table
- SNAP protocol filter table

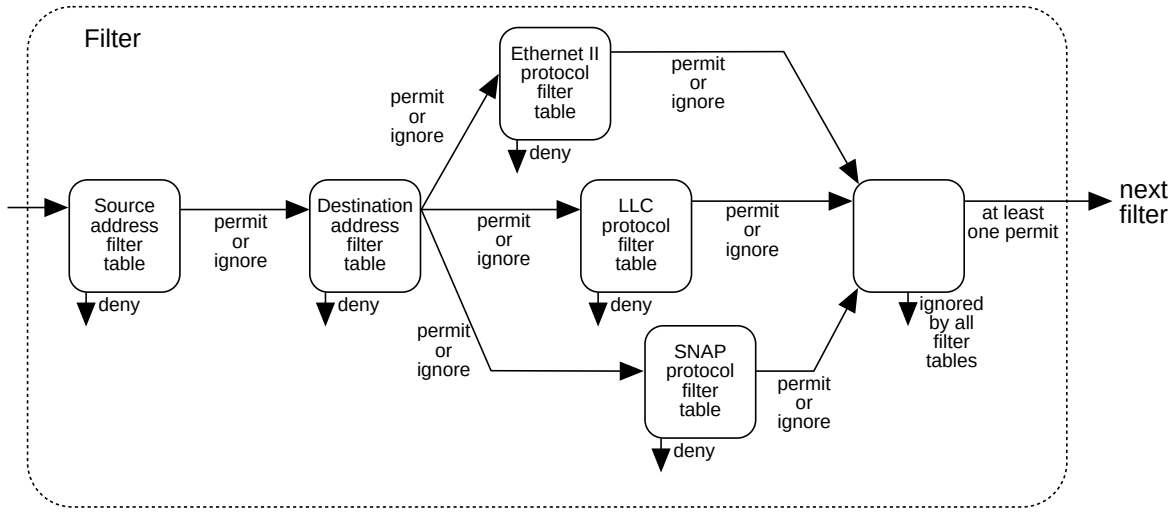


Figure 9 More detailed filtering

As a frame passes though a filter, it first visits the source address filter table, then the destination address filter table and finally one of the three protocol filter tables. It only visits one of the three protocol filter tables because a frame only has one protocol type, which is one of the following:

- Ethernet II frame
- IEEE 802.2 SAP (LLC) frame
- IEEE 802.2 SNAP (extended LLC) frame.

A filter table consists of a list of entries that are either *permit* or *deny.* If a *deny* entry matches a frame, the frame is immediately discarded. If a *permit* entry matches a frame, the frame then passes on the next filter table. If no entry in the table matches the frame, the frame is said to be *ignored*. An *ignored* frame passes to the next filter table in the same way as a *permitted* frame, however, the frame

must be permitted by at least one filter table in order to be forwarded. A frame that is ignored by all filter tables will be discarded.

Filter entries are order dependent, for example:

- deny all
- permit something

will filter all traffic including “something” because the “deny all” entry is given first. But:

- permit something
- deny all

will allow only “something” frames to cross. This is actually equivalent to:

- permit something

alone, because all other frames will not match any filter and will therefore be discarded.

ALIASES 6.2.2.1

It is not easy for everybody to handle filters based on Ethernet frame types and protocol. The bridge commands therefore supply some aliases between common protocol names and their equivalent in filter descriptions:

- All for any type of frames
- AppleTalk for AppleTalk frames
- ARP for ARP frames
- IPX for Novell™ IPX frames
- IPX_802.2 for Novell™ IPX 802.2 frames
- SNMP for SNMP frames
- TCPIP for TCP/IP frames

CONFIGURATION 6.3

At boot time, there are no usable groups or filters existing. Therefore the procedure to configure the bridge is as follows:

1. Create a group
2. Add the desired sites to that group
3. Start over at step 1 for all groups needed
4. Create a filter
5. Configure a filter (for example to allow AppleTalk traffic only)
6. Assign that filter as input or output filter to a site, or as a group filter to a group
7. Start over at step 4 for all filters needed
8. Turn the bridge on

MORE INFORMATION 6.4

COMMANDS 6.4.1

For details on the Bridge commands, see § 14.18.5, "Bridge Cache" on page 111 and following paragraphs.

EXAMPLES 6.4.2

For examples on how to configure a bridge, see § 17.5, "Bridge: Basic" on page 333.

Chapter 7

ISDN

Discover how brilliant our ISDN routing is !

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

ABOUT THE ISDN PROTOCOL 7.1

The current release of Integrated Services Digital Network (ISDN) layer has been established for:

- EuroISDN Net 3 (European Union, Switzerland and other countries) for Basic Rate ISDN
- EuroISDN Net 5 (European Union, Switzerland and other countries) for Primary Rate ISDN
- INS-64 (Japan) for Basic Rate ISDN
- National ISDN 1 (USA) for Basic Rate ISDN

DIAL-UP ISDN 7.2

Dial-Up ISDN is related to WAN sites. It defines all the necessary information to establish an ISDN connection from one site to another.

The needed information for configuration is:

- D-channel protocol (currently, EuroISDN, VN3, Japan or USA)
- Own number and MSN (Multiple Subscriber Number)
- Remote number(s) and remote MSN(s)
- Number of B-channels allowed
- The amount of time an idle connection may stay open

For an example on how to configure an ISDN connection, please refer to § 17.1, "IP: Point-to-Point" on page 314.

For displaying ISDN-related information, please use the following commands:

- § 14.18.54, "ISDN Info" on page 183
- § 14.18.121, "Site Stats" on page 269

CAUTION — Care should be taken when configuring ISDN. If there is regular traffic over the line, the connection may remain open indefinitely, leading to large telephone bills.

LEASED B-CHANNEL 7.3

INTRODUCTION 7.3.1

Leased ISDN B-Channels are similar to analog leased lines. The carrier permanently connects a B-Channel between two points. The user is normally billed a fixed amount per month, like a standard leased line. The advantage of this service is that you do not need synchronous modems and **you can easily upgrade from a dial-up solution to a leased ISDN solution without changing any equipment**!

This service is currently available in Germany and Austria. It may also be available in other countries: contact your local carrier for more information.

SWITZERLAND 7.3.1.1

- The Swiss Telecoms will introduce this feature on the 1st January 1998.

GERMANY 7.3.1.2

Not all PTT exchanges run the same version of ISDN software. As of this writing, there are two versions in existence:

1. *1TR6*:

   The ***MultiCom*** does not support leased B-Channels for this version. It does support dial-up ISDN though.

2. *Euro-ISDN (Net 3, BRI & Net 5, PRI)*:

- *D64S:* One leased B-Channel. The second B-Channel is *not* available.
- *D64S2:* Two leased B-Channels.

In both cases, there is no D-Channel protocol and no ISDN number needs to be assigned.

- *TS01:* One leased B-Channel and one standard dial-up B-Channel.
- *TS02:* Two leased B-Channels.

  In both cases, you can still use the D-Channel.

AUSTRIA 7.3.1.3

- One leased B-Channel, and the second B-Channel can be used as a normal dial-up channel.

NOTE - As of writing, there is a known bug in some of the PTT exchanges software. It occurs if the channel B2 is used as a B-Channel.

CONFIGURATION 7.3.2

ADDING A LEASED B-CHANNEL 7.3.2.1

The ISDN leased line is attached to a specific site. You must also specify which B-Channel is leased. The following is a sample configuration:

```
MultiCom:Select my_site
Site "my_site" selected.
MultiCom:ISDN Leased B1 On
Added leased channel B1 for Site "my_site"
```

If you have a ***Classic*** *Multi****Com*** or a ***Pocket*** *Multi****Com***, the B1 LED will become permanently green. On the ***Multi****Com* ***LAN Access Center***, you must use the command “ISDN Leased” on page 187 to verify your configuration.

It is necessary to repeat the configuration on the remote ***MultiCom*** before the connection will work.

CAUTION — Be careful to specify the correct B-Channel. If you specify the wrong B-Channel, the connection will not function. Also, other devices on the same ISDN connection (e.g. a digital phone) may not work correctly.

REMOVING A LEASED B-CHANNEL 7.3.2.2

A leased B-Channel can be removed as follows:

```
MultiCom:Select my_site
Site "my_site" selected.
MultiCom:ISDN Leased B1 Off
Removed leased channel B1 for Site "my_site"
```

LEASED B-CHANNEL INFO 7.3.2.3

To see the current state of the leased line, type the following:

```
MultiCom:ISDN Leased
Leased B channels:

Channel    Status  User
---------------------------
B1             Ok    Site "my_site"
```

BANDWIDTH ON DEMAND 7.3.2.4

In some countries, it is possible to use the second B-Channel when there is heavy traffic. This is done in the same manner as with the serial leased line. Simply use the command “ISDN Auto” on page 171.

LEASED B-CHANNEL BACKUP 7.3.2.5

The backup of the leased B-Channel works in exactly the same way as the serial leased line (see § 8, "Serial" on page 63). The command “Backup On” on page 110 instructs the ***Multi**Com* to open the other B-Channel if the leased B-Channel is not working (see below).

NOTES 7.3.2.6

- It is possible to use both of the B-Channels as leased B-Channels. They can be connected to the same site or separate sites as required.
- It is possible to use a serial leased line and one (or both) leased B-Channel on the same site if required.

  In other words, there is no limitation on the number of leased lines that can be connected to a site. It is also possible to freely mix dial-up and leased connections as needed.

NOTE - These are the only commands needed to configure the leased B-Channel. The other ISDN commands (e.g. ISDN RemoteNumber) are not needed unless you wish to do bandwidth on demand.

DETECTING ERRORS 7.3.3

LEASED B-CHANNEL ERRORS 7.3.3.1

You will need to use the MHDLC Link Protocol to detect errors on the leased B-Channel. Simply set the MHDLC mode to v3 for the relevant site and enable the alarm as explained in the chapter § 9.3, "Alarm" on page 70.

On the ***Classic** Multi**Com*** and ***Pocket** Multi**Com***, if an error occurs, the corresponding LED will become red. If SNMP has been installed and is correctly configured, a link-down trap will be sent to the management station.

If the error is corrected, the ***Multi**Com* will automatically resume using the connection, just like a normal leased line.

CONFIGURATION ERRORS 7.3.3.2

If you mistakenly configure one channel as a leased B-Channel, while your carrier has setup another B-Channel as the leased connection, the connection will not function. If you have configured the ***MultiCom*** to use the link-protocol v3, the ***MultiCom*** will signal an alarm about 15 seconds after you configure the connection. On the Pocket and Classic, the corresponding LED will turn red.

If the ***MultiCom*** tries to make a dial-up connection and is instructed by the telephone exchange to use the channel B1, it will notice that this is supposed to be a leased B-Channel. In this case, the ***MultiCom*** will consider the leased B-Channel incorrectly configured and will use it anyway as a dial-up channel. It will also set the corresponding alarm. On a Pocket and Classic, the B-Channel LED will turn red and will remain so permanently, whether the channel is open or not.

MORE INFORMATION 7.4

COMMANDS 7.4.1

For details on ISDN commands, see § 14.18.46, "ISDN Auto" on page 171 and following paragraphs.

EXAMPLES 7.4.2

For examples on how to configure ISDN, see § 17, "Examples" on page 313.

REFERENCES 7.4.3

[4] William Stallings, “ISDN and Broadband ISDN”, Macmillan, 1992.

Chapter 8

Serial

You will use it for your synchronous analog leased lines and you will not regret it.

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Classic							
LAC					**V 2.2.6**		

INTRODUCTION 8.1

The serial ports are intended to be used with synchronous leased line modems. Currently, the ***MultiCom*** does not support asynchronous leased line modems or dial-up modems.

In general, synchronous leased line modems offer one of three types of interface: X.21, V.35 or V.36. The ***MultiCom*** can be connected to any of these interfaces provided that you have the appropriate cable. Cables can be purchased from your distributor.

CONFIGURING THE SERIAL PORT 8.2

The standards that describe leased line modems contain a number of options. Not all modem manufacturers implement these options in the same way. As a result, very few leased line modems function in exactly the same way.

To avoid incompatibility problems, the ***MultiCom*** has a highly flexible serial port. It can be configured with a large number of options, and should work with most modems.

To simplify the serial configuration, the command `Serial Mode` can be used to apply the default options for a given interface. For example, `Serial Mode X21` sets the default options for X.21. This configuration should work with most X.21 modems.

SIMPLE SETUP 8.2.1

In most situations the following commands should be sufficient to activate the serial line:

- `Site Select` *`Site`* (Choose the site)
- `Serial Mode X21` (or V35, or V36)
- `Serial On` (Activate the serial line)

MORE INFORMATION 8.3

COMMANDS 8.3.1

For more details on commands related to the serial option see § 14.18.98, "Serial" on page 243 and following paragraphs.

EXAMPLES 8.3.2

For examples on how to configure the serial line for a ***MultiCom***, see § 17.7, "Serial: Basic" on page 345 and § 17.8, "Serial: Backup and Overflow" on page 349.

Chapter 9

MHDLC

Our simple and proprietary link protocol.

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

INTRODUCTION 9.1

The ***MultiCom*** can use a proprietary Bandwidth-on-Demand protocol, called MHDLC, on the ISDN and serial lines.

This protocol has been extended with a link control feature, from the firmware version 2.0 on, in order to better detect errors on leased lines. This link control also prevents packet loss when a dial-up ISDN line is connected or disconnected.

This protocol is now obsolete and should be replaced, when possible, by PPP (see § 10, "PPP/MP" on page 71).

DIFFERENT MODES 9.2

The MHDLC protocol has three different modes:

- v1 - transparent
- v2 - connection-control
- v3 - polling

The mode is set site-by-site, so it is possible to have different values for different sites.

Each mode is a super-set of the previous one, that is v2 includes v1, and v3 includes v2 and v1.

TRANSPARENT MODE (V1) 9.2.1

The transparent mode is compatible with previous releases of the ***MultiCom*** firmware. This mode should only be used when connecting a ***MultiCom*** running

firmware version 2.0 and above with another ***MultiCom*** running an older firmware version.

NOTE - In this mode, no link controls are done.

CONNECTION-CONTROL (V2) 9.2.2

When connecting or disconnecting a link, the two ***MultiCom***'s will perform a handshake before they begin routing/bridging over that link. This insures that the link is fully connected before data is exchanged.

This mode is intended for sites using dial-up ISDN links, where it is possible that one ***MultiCom*** is informed that a B-Channel is opened before the other ***MultiCom***. In transparent mode, the first ***MultiCom*** may start transmitting data too early and some data may be lost. The connection-control mode avoids this risk of data loss.

NOTE - Most high level protocols, like TCP, implement some kind of data integrity checking and will detect and correct a packet loss.

POLLING MODE (V3) 9.2.3

When the polling mode is active, the two ***MultiCom***'s exchange control data on a regular basis. This exchange of data enables the ***MultiCom*** to detect problems on the link. If the link fails, the control data will not get through. After a short delay, the two ***MultiCom***'s will declare the link down and pass to backup mode, if so configured.

This mode also detects loop-backs.

This mode is intended for sites using leased lines. For serial leased lines, it supplements the ***MultiCom***'s ability to detect errors that are indicated by the modem. For ISDN leased B-Channels, this is the only way of detecting link errors.

This mode is an extension of the Connection-Control mode. If a site is using a mix of leased and dial-up links, this mode will work for all link types.

ALARM 9.3

Each site has an alarm associated with it. When activated, the alarm will cause leased-line links (connected to the site) to be declared down, if MHDLC discovers an error on the link. In addition, the serial LED will turn red.

If the SNMP option is present, the SNMP agent will send a “linkDown” trap.

If ISDN backup is enabled for the site, an ISDN B-Channel will be opened (if traffic is present) until the leased-line recovers.

Deactivating the alarm causes the site to ignore link errors. No ISDN backup will be performed if a leased-line fails.

ENCODING 9.4

The physical link encoding on the ISDN channel has been changed from NRZI (on the Classic and Pocket ***MultiCom***) to NRZ (on the LAN Access Center and Serie IV ***MultiCom***). To maintain backward compatibility , the default encoding is still NRZI. If you need to connect a Classic or a Pocket to a LAN Access Center, you will have to use the `MHDLC Encoding NRZ` command for the remote LAC site (cf § 14.18.71, "MHDLC Encoding" on page 208).

MORE INFORMATION 9.5

COMMANDS 9.5.1

See § 14.18.71, "MHDLC Encoding" on page 208 and following paragraphs, for details of the MHDLC commands.

Chapter 10

PPP/MP

The powerful and standard link protocol.

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

INTRODUCTION TO PPP 10.1

ABSTRACT 10.1.1

Most of the text from § 10.1 comes from [5]: Simpson W., “The Point-to-Point Protocol (PPP)”, RFC 1661, Daydreamer, July 1994..

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP is comprised of three main components:

- A method for encapsulating multi-protocol datagrams.
- A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
- A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

The Point-to-Point Protocol is designed for simple links which transport packets between two peers. These links provide full-duplex simultaneous bidirectional operation, and are assumed to deliver packets in order.

ENCAPSULATION 10.1.2

The PPP encapsulation provides for multiplexing of different network-layer protocols simultaneously over the same link. The PPP encapsulation has been carefully designed to retain compatibility with most commonly used supporting hardware.

Only 8 additional octets are necessary to form the encapsulation when used within the default HDLC-like framing.

LINK CONTROL PROTOCOL 10.1.3

In order to be sufficiently versatile to be portable to a wide variety of environments, PPP provides a Link Control Protocol (LCP). The LCP is used to automat-

ically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common misconfiguration errors, and terminate the link. Other optional facilities provided are authentication of the identity of its peer on the link, and determination when a link is functioning properly and when it is failing.

NETWORK CONTROL PROTOCOLS 10.1.4

Point-to-Point links tend to exacerbate many problems with the current family of network protocols. For instance, assignment and management of IP addresses, which is a problem even in LAN environments, is especially difficult over circuit-switched point-to-point links (such as dial-up modem servers). These problems are handled by a family of Network Control Protocols (NCPs), which each manage the specific needs required by their respective network-layer protocols.

CONFIGURATION 10.1.5

It is intended that PPP links be easy to configure. By design, the standard defaults handle all common configurations. The implementor can specify improvements to the default configuration, which are automatically communicated to the peer without operator intervention. Finally, the operator may explicitly configure options for the link which enable the link to operate in environments where it would otherwise be impossible.

This self-configuration is implemented through an extensible option negotiation mechanism, wherein each end of the link describes to the other its capabilities and requirements. Although the option negotiation mechanism described in this document is specified in terms of the Link Control Protocol (LCP), the same facilities are designed to be used by other control protocols, especially the family of NCPs.

For more detailed information on PPP please refer to § 10.3.3, "References" on page 77.

PPP IN THE MULTICOM 10.2

This paragraph describes the particularities of the PPP implementation in the ***MultiCom*** family.

COPYRIGHTS 10.2.1

Part of the software uses the MD5 message-digest algorithm by RSA Data Security, Inc. Here is the copyright notice for this portion of code:

```
**********************************************************************
** Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.  **
**                                                                   **
** License to copy and use this software is granted provided that    **
** it is identified as the "RSA Data Security, Inc. MD5 Message-     **
** Digest Algorithm" in all material mentioning or referencing this  **
** software or this function.                                        **
**                                                                   **
** License is also granted to make and use derivative works          **
** provided that such works are identified as "derived from the RSA  **
** Data Security, Inc. MD5 Message-Digest Algorithm" in all          **
** material mentioning or referencing the derived work.              **
**                                                                   **
** RSA Data Security, Inc. makes no representations concerning       **
** either the merchantability of this software or the suitability    **
** of this software for any particular purpose.  It is provided "as  **
** is" without express or implied warranty of any kind.              **
**                                                                   **
** These notices must be retained in any copies of any part of this  **
** documentation and/or software.                                    **
**********************************************************************
```

IMPLEMENTATION 10.2.2

The implementation of PPP strictly follows [5]. The differences reside in the configuration commands described in § 14.18.79, "PPP Callback" on page 217 and following paragraphs, and as described below.

AUTHENTICATION FAILURES 10.2.2.1

On authentication failures, the ***MultiCom*** will close the ISDN lines if in dial-up mode, and this forbids further channel opening to the same location. For the channel to be used again, the user must change the configuration to correct the authentication problem. The connection must then be manually forced open again (see § 14.18.49, "ISDN Conn" on page 177).

For more details on authentication configuration see the following commands:

- § 14.18.84, "PPP Local Authentication" on page 226
- § 14.18.87, "PPP Remote Authentication" on page 229
- § 14.18.88, "PPP Stats" on page 231
- § 14.18.86, "PPP Password" on page 228

LCP OPTIONS 10.2.2.2

Only the local and remote PPP authentication protocol can be configured by the user.

The ***MultiCom***'s PPP implementation negotiates the MRU (Maximum Receiver Unit), set to 1500, and the Magic Number.

All other options are set to their default values:

- Asynchronous Control Character Map set to 0
- Quality Protocol set to none
- Protocol Field Compression set to none
- Address and Control Field Compression set to none.

CCP OPTIONS 10.2.2.3

By default, the ***MultiCom*** will try to negotiate Stac LZS® compression with the remote peer. If it fails, it will fall back to normal uncompressed transmission. See § 14.18.80, "PPP Compression" on page 219 for more details.

ECP OPTIONS 10.2.2.4

The ***MultiCom*** will try to negotiate IDEA™ encryption, if turned on. If it fails, the connection will be aborted, for security reasons. See § 14.18.82, "PPP Encryption" on page 222 for more details.

IPCP OPTIONS 10.2.2.5

The user has no IP options to set.

The ***MultiCom*** negotiates only the IP Address. All other options are set to the default value:

- IP Addresses -> deprecated -> not managed by the ***MultiCom***
- IP Compression Protocol set to none.

IPXCP OPTIONS 10.2.2.6

The user has no IPX options to set.

The ***MultiCom*** negotiates the IPX Network Number, the IPX Node Number and the IPX Routing Protocol (RIP/SAP). The other options are set to the default value:

- IPX Compression Protocol set to none
- IPX Router Name set to ““ (empty string)
- IPX Configuration Complete -> not managed.

BCP OPTIONS 10.2.2.7

The user has no BCP options to set.

The ***MultiCom*** negotiates the MAC Support option (advisory only), set to IEEE 802.3, the MAC Address option and the Spanning Tree Protocol, set to none.

The other options are not treated (and rejected if received), except the Tinygram Compression one, set to none by default.

MORE INFORMATION 10.3

COMMANDS 10.3.1

For details on PPP commands, see § 14.18.79, "PPP Callback" on page 217 and following paragraphs.

EXAMPLES 10.3.2

For examples of using PPP with the ***MultiCom*** and other machines, see § 17.9, "PPP: Internet Access" on page 353 and § 17.10, "PPP: Teleworking" on page 357. For compatibility examples, see `http://www.lightning.ch/support`.

REFERENCES 10.3.3

[5] Simpson W., “The Point-to-Point Protocol (PPP)”, RFC 1661, Daydreamer, July 1994.

[6] Perkins, D., “Requirements for an Internet Standard Point-to-Point Protocol”, RFC 1547, Carnegie Mellon University, December 1993.

[7] Reynolds, J., and Postel, J., “Assigned Numbers”, STD 2, RFC 1340, USC/Information Sciences Institute, July 1992.

Chapter 11

DNS

Would you like to use "www.lightning.ch" instead of "193.247.134.2"? Then you need the Domain Name Service!

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

INTRODUCTION 11.1

DNS is the network protocol used for transforming machine names into IP addresses. For example, if you type "`telnet fido.cs.mit.edu`", the DNS software will find the associated IP address.

In order to use DNS on a ***MultiCom***, you must have access to a DNS server. Ask your Network Manager or Internet Service Provider if you don't know where are your DNS servers. If you don't have access to one, you will have to specify IP addresses manually (i.e. "`telnet 128.136.34.25`").

DNS IN THE MULTICOM 11.2

FEATURES 11.2.1

- Standard DNS operation: it allows you to use "Telnet", "Ping" and "Traceroute" with names instead of IP numbers.
- The DNS configuration can be automatically retrieved or provided using PPP. This allows a very simple configuration for Internet access, if your ISP supports this feature.
- The local domain name of the ***MultiCom*** may be set. This allows to type only the name of local machines, without the full domain (i.e. "`telnet fido`" instead of "`telnet fido.cs.mit.edu`").
- Records statistics on DNS traffic issued by the ***MultiCom***.
- The local DNS cache may be enabled or disabled.

MORE INFORMATION 11.3

COMMANDS 11.3.1

For details on DNS commands, see § 14.18.18, "DNS" on page 129.

EXAMPLES 11.3.2

For an example of how to configure DNS, see § 17.17, "DNS" on page 386. For an exemple of how to receive automatically a DNS configuration, see § 17.9, "PPP: Internet Access" on page 353.

REFERENCES 11.3.3

[8] Mockapetris P., “Domain Implementation and Specification”, RFC 1035, ISI, November 1987.

[9] Paul Albitz & Cricket Liu, “DNS and BIND, 2nd Edition”, O’Reilly, December 1996.

[10] Cobb S., “PPP Internet Protocol Control Protocol Extensions for Name Server Addresses”, RFC 1877, Microsoft, December 1995.

Chapter 12

SNMP

*The Simple Network Management Protocol or the other easy way to manage your **MultiCom**.*

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

INTRODUCTION 12.1

WHAT IS SNMP 12.1.1

SNMP (Simple Network Management Protocol) is a network management protocol. It allows a managing station to consult information tables and counters belonging to a network station through an SNMP agent. These counters and tables are located in a Management Information Base (MIB), which is organized as a tree.

There are two versions of SNMP, version 1 (SNMPv1) and 2 (SNMPv2). The version 2 is a superset of version 1, adding mainly security, in the form of authentication and encryption, and information sharing, in the form of the manager-to-manager MIB.

The current firmware revision implements an SNMPv1 agent only.

Both SNMP and the MIB are defined in RFC's (Request for comments) as follows:

- RFC 1155 to 1157: SNMP version 1
- RFC 1212, 1213: MIB-II
- RFC 1441 to 1452: SNMP version 2

Please refer to the different RFC's described above and to § 12.6.3, "References" on page 89, for a more detailed information on SNMP and the behavior of an SNMP agent. We will focus here on the particularities of the agent's implementation in the ***MultiCom***, as well as the restrictions and proprietary adjunctions.

FEATURES 12.1.2

- Full SNMPv1 Agent
- Support of MIB-II
- Multiple communities
- Multiple trapping hosts

RESTRICTIONS 12.1.3

- Some restrictions in the MIB-II tree.
- No dynamic row creation in tables.

COMMUNITIES 12.2

To be able to access the agent with a manager you need to have a community name, which is a sort of password.

As communities management is not described in the SNMPv1 RFC's, the ***Multi-Com*** implements a command that allows the user to set the community names that will be accepted by the agent: '`SNMP Community'`. Two access types are defined in this command: '`Read`' or '`Write`'. It determines the type of SNMP requests the manager may issue to the agent. These are:

- For 'Read': GetRequest and GetNextRequest.
- For 'Write': GetRequest, GetNextRequest and SetRequest.

COMMAND USAGE 12.2.1

- To display the allowed community names type:

```
MULTICOM: SNMP Community
SNMP Community names
     Name     Rights
     ----     ------
     public   Read
```

- To add a community name with 'Read' permission type:

```
MULTICOM: SNMP Community toto Read
SNMP Community names
     Name     Rights
     ----     ------
     public   Read
     toto     Read
```

- To add a community name with ‘Write’ permission type:

```
MULTICOM: SNMP Community toto Write
SNMP Community names
     Name     Rights
     ----     ------
     public   Read
     toto     Write
```

- To remove a community name type:

```
MULTICOM: SNMP Community toto Remove
SNMP Community names
     Name     Rights
     ----     ------
     public   Read
```

The community name ‘toto’ has been removed. The community names that are left are shown.

NOTE - Be aware that unlike commands, the community names are case-sensitive, that is ‘toto’ is not the same as ‘Toto’ or ‘toTo’.

TRAPS 12.3

INTRODUCTION 12.3.1

The SNMP agent is capable of sending unsolicited informations to a managing station in order to report unusual events. These packets, called ‘traps’, may report these following events:

- coldStart (0)
- warmStart (1)
- linkDown (2)
- linkUp (3)

- authenticationFailure (4): When an inappropriate community name is used.
- enterpriseSpecific (5)

For a ***MultiCom*** to send one of these traps, at least one manager must be specified.

For a ***MultiCom*** to send authenticationFailure traps, the authentication failure traps must be enabled.

SETTING MANAGERS 12.3.2

- To add a manager type:

```
MULTICOM: SNMP Manager 193.5.2.16
SNMP Manager
     Address       Port
     -------       -----
     193.5.2.16   162
```

- The port number is optional. By default it is set to 162, which is the reserved SNMP trap port in UDP. You may specify another port by typing:

```
MULTICOM: SNMP Manager 193.5.2.16 8000
SNMP Manager
     Address       Port
     -------       -----
     193.5.2.16    162
     193.5.2.16   8000
```

Where 8000 is the port number on which your SNMP manager is listening.

- To remove a manager type:

```
MULTICOM: SNMP Manager 193.5.2.162 8000 remove
SNMP Manager
     Address       Port
     -------       -----
     193.5.2.162   162
```

In this case you must specify the port number. The display will show the managers that are left after the remove command.

AUTHENTICATION FAILURE TRAPS 12.3.3

When authentication traps are enabled, the agent will send an authenticationFailure trap to each defined manager, each time an invalid community name is used.

- To enable authentication failure traps, type:

```
MULTICOM: SNMP AuthTrap enable
SNMP authentication failure traps enabled
```

- To disable authentication failure traps, type:

```
MULTICOM: SNMP AuthTrap disable
SNMP authentication failure traps disabled
```

You may also enable and disable authentication failure traps through SNMP by setting then following MIB object:

iso.org.dod.internet.mgmt.mib-2.snmp.snmpEnableAuthenTraps.0

to

enabled(1) or disabled(2).

OTHER COMMANDS 12.4

Other commands are:

- SNMP Stats: display SNMP counters.
- SNMP Info: gives the managers, community names and state of the authentication failure traps.
- SNMP Help: displays help.
- SNMP Restart: abort current operation, reset all variables and send warm start trap.

For more details on SNMP commands, see § 14.18.123, "SNMP AuthTrap" on page 273.

MANAGEMENT INFORMATION BASE (MIB) 12.5

The SNMP counters and tables are located in a Management Information Base (MIB), which is organized as a tree.

The ***MultiCom*** agent implements the full MIB-2, as defined in RFC 1213, with the following restrictions.

RESTRICTIONS 12.5.1

- ip.ipForwarding is writable but has no effect.

  This will be corrected in a future firmware release.
- You may not create new rows in a table through a SNMP manager.
- The ipAddrTable and the ipRouteTable are not implemented since the ***MultiCom*** uses range routing and not subnet routing as defined in these tables.

MORE INFORMATION 12.6

COMMANDS 12.6.1

For details on SNMP commands, see § 14.18.123, "SNMP AuthTrap" on page 273 and following paragraphs.

EXAMPLES 12.6.2

For examples on how to configure SNMP, see § 17.16, "SNMP" on page 384.

REFERENCES 12.6.3

[11] M. Rose & K. McCloghrie, “Structure and Identification of Management

Information for TCP/IP-based Internets", RFC 1155, Performance Systems International & Hughes LAN Systems, May 1990.

[12] K. McCloghrie & M. Rose, "Management Information Base for Network Management of TCP/IP-based internets", RFC 1156, Hughes LAN Systems & Performance Systems International, May 1990.

[13] J. Case & M. Fedor & M. Schoffstall & J. Davin, "A Simple Network Management Protocol", RFC 1157, SNMP Research & Performance Systems International & MIT Laboratory for Computer Science, May 1990.

[14] M. Rose & K. McCloghrie, "Concise MIB Definitions", RFC 1212, Performance Systems International & Hughes LAN Systems, May 1990.

[15] K. McCloghrie & M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", RFC 1213, Hughes LAN Systems & Performance Systems International, May 1990.

[16] Tobias Oetiker and Dave Rand, "Multi Router Traffic Grapher", available at http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html

[17] Jürgen Schönwälder, "Scotty - Tcl Extensions for Network Management Applications", available at http://wwwhome.cs.utwente.nl/~schoenw/scotty/ and http://www.ibr.cs.tu-bs.de/cgi-bin/sbrowser.cgi, TU Braunschweig

Chapter 13

Security

Encryption, the key to security!

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

INTRODUCTION 13.1

Lightning's ***MultiCom*** software release 2.1 introduced a powerful and proven 128 bits encryption technology: the IDEA™ algorithm.

Lightning's ***MultiCom*** software release 2.4 introduces a standard encryption technology: the DES and 3DES algorithms with 40, 56 and 112 bits keys.

NOTE - IDEA is a trademark of Ascom Systec.

LINK ENCRYPTION 13.2

The link encryption is used to encrypt all data in point-to-point configurations, using ISDN or leased lines. All data, bridged or routed, is encrypted independently of the protocol type. This can be done with MHDLC or PPP, but PPP allows you to use random session keys, for even more security.

CAUTION — The link encryption in version 2.2.3 and above is not compatible with version 2.2.2 and below!

IP-LEVEL ENCRYPTION 13.3

The IP-level encryption is used for a secure transmission over IP networks, like the Internet, Intranets and Extranets. The difference between IP-level encryption and link-level encryption is that data going through a site can be encrypted or not, depending on its destination. This enables you, for example, to build your own

Virtual Private Data Network (VPDN) using the Internet, to provide low-cost secure international connections.

CAUTION — Only IP data are encrypted, not IPX data. The IP-level encryption can be used over MHDLC and PPP. IP broadcasts are never encrypted.

KEYS 13.4

IDEA (International Data Encryption Algorithm) is an algorithm which uses symmetric secret keys. It means that you must use exactly the same key for encoding and decoding. You can share the same key between multiple sites, or use a different key for each bilateral communication, for improved security.

IDEA is a well-known algorithm which is considered by many people as the most secure public algorithm for symmetric encryption (see [21]). It is still unbroken after years of public use, unlike DES, the Data Encryption Standard of the US government. It uses long keys of 128 bits instead of the standard 40 or 56 bits used by DES. This means that it is 2^{72} (not 2.3) times more secure than DES!

CAUTION — All the secret of your communication depends on the secrecy of your keys. Keep them secret very carefully!

CONFIGURATION 13.5

To use encryption, the following procedure must be used:

- Create all needed encryption keys with their corresponding key id’s.
- Save the keys you will use in Flash memory

- Assign each key to an IP range or to a site.
- Enable the corresponding encryption (using `MHDLC Encryption`, `PPP Encryption` or `IP Router Encryption`)
- If you want additional protection, lock the keys in memory with the `Security` command.

If this procedure is not respected, errors will occur, and in some extreme cases, the remote ***Multi**Com* may become unreachable.

VISUAL STATUS DISPLAY 13.6

When the encryption option is not installed, the Power LED remains green after boot time (except when modifying the Flash memory). But when the encryption option is installed, the Power LED displays the current status of the encryption:

- Green

  - When using link encryption and all remote sites are encrypted
  - When transmitting encrypted packets in IP-level encryption

  This means that your data are securely protected against listeners and intruders.

- Orange

  - When not all remote sites are encrypted in link encryption
  - When transmitting unencrypted packets in IP-level encryption

  This means that some of your data may be listened to or tampered with. You should check your configuration to make sure that it is what you really want.

MORE INFORMATION 13.7

COMMANDS 13.7.1

For more details on the security-related commands, read these paragraphs:

- § 14.18.65, "Key Create" on page 201
- § 14.18.68, "Key Save" on page 205
- § 14.18.28, "IP Range" on page 146
- § 14.18.31, "IP Router Encryption" on page 150
- § 14.18.72, "MHDLC Encryption" on page 209
- § 14.18.73, "MHDLC EncryptionKeyId" on page 211
- § 14.18.82, "PPP Encryption" on page 222
- § 14.18.97, "Security" on page 241

EXAMPLES 13.7.2

For examples on how to configure the encryption, see § 17.13, "Encryption: Link-level" on page 368, § 17.14, "Encryption: IP-level" on page 372 and § 17.15, "Encryption: Ethernet-Ethernet" on page 377.

REFERENCES 13.7.3

[18] T. Brüggemann, H. Bütk, “Damit Geheimdaten vertraulich bleiben, Verschlüsselungsalgorithmus IDEA löst DES ab”, Elektronik, Sonderdruck aus Heft 10/1993, München, 1993.

[19] Bruce Schneier, “The IDEA Encryption Algorithm, an advanced block-cipher approach to encryption”, Dr. Dobb’s Journal, December 1993.

[20] “IDEA™ - der zukünftige Standard der Datenverschlüsselung von Ascom”, Ascom Systec.

[21] Bruce Schneier, “Applied Cryptography, Second Edition”, John Wiley &

Sons, 1996.

[22] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, “Handbook of applied cryptography”, CRC Press, 1996.

Chapter 14

Commands

*This chapter describes all the commands that are available in the **MultiCom** firmware.*

INTRODUCTION 14.1

GENERAL 14.1.1

The commands are not case sensitive.

The command prompt shows the name of the ***MultiCom*** that is defined by the `MyName` command in the `config` file (see §14.18.77, "MyName" on page 215).

The command line can be edited with bash-like control characters, including standard VT-100 arrows:

^A	Goto start of line
^B, Left	Backward char
^C	Break
^D	Delete forward character
^E	Goto end of line
^F, Right	Forward character
^H, Del	Backspace
^K	Kill end of line
^L	Refresh
^M	Enter
^N, Down	History next
^P, Up	History previous
^T	Transpose characters
^U	Kill line

TYPOGRAPHICAL CONVENTIONS

14.1.2

Each command will be presented in the following manner:

Type

`{Global | Site-specific | Interactive}`

Commands may be grouped in different categories:

- Interactive commands that **should only be used in command-line mode**
- Global commands that apply to the ***MultiCom*** in general
- Site-specific commands that apply only to the currently selected site (see §3.3, "Sites" on page 19, to understand what is a site)

Format

`Command Keyword1 {Keyword2 [`*`parameter_1`*`] | Keyword3}`

This is the overall format of the command.

- `Keywords` are written in a mono-space plain font.
- *`parameters`* are written in a mono-space italic font.
- Keywords or arguments between [] are optional.
- Different possibilities are inside {}, separated by a |.
- The default value is underlined.

Parameters

- `argument_1 argument_2 [`*`parameter_1`*`]`

Each possible argument or parameter are described separately, if relevant.

A console output is given if relevant:

```
MultiCom:Command argument_1 argument_2 my_parameter
Command is OK.
```

The typed command is in a mono-space **`bold`** font.

Default value

`Empty`

The default value is described when available.

GETTING ON-LINE HELP ON COMMANDS 14.2

Format
`Help [command]`

Parameters
- `none`

  Generates a list of all valid command names, depending on the installed firmware options and hardware configuration.

- *`command`*

  Displays the on-line help on a specific command.

  The alternate format "*`command`* `Help`" is also available.

GETTING INFORMATION 14.3

Format
`Info [topic]`

Parameters
- *`none`*

  Displays the list of valid information topics.

- *`topic`*

  Displays detailed information and statistics about the specified topic.

  The alternate format "*`topic`* `Info`" is also available.

  The "`Info`" command is further described in the paragraphs related to specific parts of the firmware. For example the "Info Bridge" command is described in §14.18.12, "Bridge Info" on page 120.

NEW 2.2 COMMANDS 14.4

These commands have been introduced in the 2.2 firmware revision:

MODIFIED 2.2 COMMANDS 14.5

These commands have been modified in the 2.2 firmware revision:

NEW 2.2.9 COMMANDS 14.6

These commands have been introduced in the 2.2.9 firmware revision:

- §14.18.21, "Hardware" on page 135
- §14.18.55, "ISDN Interface" on page 186
- §14.18.82, "PPP Encryption" on page 222
- §14.18.97, "Security" on page 241
- §14.18.136, "User" on page 288

MODIFIED 2.2.9 COMMANDS 14.7

These commands have been modified in the 2.2.9 firmware revision:

- §14.18.50, "ISDN DChannelProtocol" on page 178
- §14.18.68, "Key Save" on page 205

NEW 2.3 COMMANDS 14.8

These commands have been introduced in the 2.3 firmware revision:

- §14.18.16, "DHCP" on page 124
- §14.18.17, "Diagnose" on page 128
- §14.18.33, "IP SiteAddr" on page 152
- §14.18.35, "IP Translation" on page 155
- §14.18.88, "PPP Stats" on page 231
- §14.18.115, "Setup" on page 261
- §14.18.130, "Syslog" on page 282

MODIFIED 2.3 COMMANDS 14.9

These commands have been modified in the 2.3 firmware revision:

- §14.18.54, "ISDN Info" on page 183
- §14.18.79, "PPP Callback" on page 217
- §14.18.83, "PPP Info" on page 224
- §14.18.117, "Site Info" on page 264

NEW 2.4 COMMANDS 14.10

These commands have been introduced in the 2.4 firmware revision:

- §14.18.19, "DNS GetFrom" on page 132
- §14.18.25, "IP DynamicRange" on page 140
- §14.18.29, "IP RemoteAddr" on page 148
- §14.18.48, "ISDN Callback" on page 175
- §14.18.52, "ISDN ErrorResetTime" on page 180
- §14.18.61, "ISDN NeverBusy" on page 196
- §14.18.81, "PPP EchoRequest" on page 221
- §14.18.85, "PPP Multilink" on page 227

MODIFIED 2.4 COMMANDS 14.11

These commands have been modified in the 2.4 firmware revision:

- §14.18.47, "ISDN BChannel" on page 173
- §14.18.65, "Key Create" on page 201
- §14.18.66, "Key Info" on page 203

- §14.18.79, "PPP Callback" on page 217
- §14.18.115, "Setup" on page 261

MODIFIED 2.4.2 COMMAND 14.12

This command has been modified in the 2.4.2 firmware revision:

- §14.18.65, "Key Create" on page 201

MODIFIED 2.5 COMMANDS 14.13

These commands have been modified in the 2.5 firmware revision:

- §14.18.33, "IP SiteAddr" on page 152
- §14.18.35, "IP Translation" on page 155

NEW 2.6 COMMAND 14.14

This command has been introduced in the 2.6 firmware revision:

- §14.18.26, "IP Filter" on page 141

NEW 2.6.1 COMMAND 14.15

This command has been introduced in the 2.6.1 firmware revision:

- §14.18.95, "RIP" on page 238

MODIFIED 2.6.1 COMMAND 14.16

This command has been modified in the 2.6.1 firmware revision:

- §14.18.26, "IP Filter" on page 141

OBSOLETE COMMANDS 14.17

All other commands not described in this manual are obsolete and **should not be used anymore**, however some are maintained for backward compatibility.

ALL THE COMMANDS 14.18

They are all here, one by one, in alphabetical order.

# #

14.18.1

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This is not really a command. It marks the beginning of a comment in the `config` file.

Type

`Global`

Format

`#`

The comment starts at the # and continues to the end of the line.

```
# This entire line is a comment
IP Router On    # The second half of this line is a comment
```

NOTE - When the '#' or ' ' characters appears in a password, they must be escaped, as well as the '\' character, by a '\', i.e. "PPP Authentication Local Password 1#2 3\4" should be "PPP Authentication Local Password 1\#2\ 3\\4".

ACCOUNT

14.18.2

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is used to create management user accounts on the ***MultiCom***.

Type
`Global`

Format
`Account` *`username password`*

Parameters
- *`username password`*

  Creates a username with an associated password.
  This command is obsolete: it has been replaced by the `User` command. It is maintained for backward compatibility.

NOTE - Multiple accounts may be created by repeating this command.

NOTE - When no accounts are defined (which is the case in the default configuration file), there is no check at all to access the ***MultiCom***. This is to simplify the initial configuration only. **We strongly advise you to create an account to protect the access to your *MultiCom*.**

ARP

14.18.3

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is used to configure the Address Resolution Protocol (ARP).

Type

`Global`

Format

`ARP [Delete` *`x.x.x.x`* `| Proxy [{On | Off}] | Info]`

Parameters

- *none*

  Displays the ARP lookup tables.

```
MultiCom:ARP

Contents of ARP Table
---------------------
193.5.1.1 --> 08:00:20:19:97:72, Time to Live  18, Clean
193.5.1.2 --> 08:00:20:10:62:26, Time to Live 343, Stale
```

- `Proxy [{On|Off}]`

  Allows or forbids the ***MultiCom*** to respond to ARP lookup requests on behalf of the remote sites. On a network with a single router, this should be On, but on a network with many routers, it is better to disable this feature and program an explicit Default Gateway on all connected machines. Without parameters, this command displays the current state of the ARP proxy.

```
MultiCom:ARP Proxy On
Proxy ARP enabled
MultiCom:ARP Proxy
Proxy ARP enabled
MultiCom:ARP Proxy Off
Proxy ARP disabled
MultiCom:ARP Proxy
Proxy ARP disabled
```

- `Delete` *`x.x.x.x`*

  Deletes an entry from the ARP lookup tables. This is very useful when you replace a machine by another, which has the same IP address.

```
MultiCom:ARP Delete 193.5.1.1
arp: 193.5.1.1 deleted
```

- `Info`

  Displays statistics on ARP lookup requests.

```
MultiCom:ARP Info


ARP Configuration
-----------------
DefaultIPRouter = 193.5.1.1
SubNetMask      = 255.255.255.0

Statistics for ARP
------------------
Nbr Successfull Lookups                   = 23
Nbr Lookups Sent                          = 23
Nbr Replies Received                      = 26
Nbr Lookups Received                      = 23
Nbr Replies Sent                          = 23
Nbr Expired Entries                       = 8
Nbr IP_Frames Buffered                    = 9
Errors: Failed Lookup                     = 0
Errors: Nobody Responding To ARP Request  = 0
Errors: IP-Frames Unresolved              = 0
Errors: ARP Not Ready                     = 0
Errors: No More Entries In ARP Table      = 0
Errors: Unsupported Protocol or Hardware  = 0
Errors: Reply Not Sent                    = 0

Contents of ARP Table
---------------------
193.5.1.1 --> 08:00:20:19:97:72, Time to Live  16, Clean
193.5.1.2 --> 08:00:20:10:62:26, Time to Live 341, Stale
```

Default value

`Proxy On`

BACKUP

14.18.4

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the leased-line backup feature.

Type

```
Site-specific
```

Format

```
Backup [{On | Off}]
```

Parameters

- *none*

  Display the status of the backup function.

- `On`

  Turns the backup feature on.

  This means that if an analog or ISDN leased-line fails, the ***MultiCom*** will use a dial-up ISDN connection to backup the link.

- `Off`

  Turns the backup feature off.

Default value

```
Off
```

BRIDGE CACHE

14.18.5

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the cache of MAC addresses used by the bridge.

Type

`Global`

Format

`Bridge Cache [{On | Off | Flush}]`

Parameters

- *none*

  Without parameter, this command displays the current status of this feature.

- `{On | Off}`

  Enables or disables the bridge cache.

- `Flush`

  Empties the bridge cache.

Default value

`On`

BRIDGE CLEAR-FILTER

14.18.6

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command removes a filter from a group or from a site, for input or output traffic.

Type

`Global`

Format

`Bridge Clear-filter` *`filter_name`* `{Group` *`group_name`* `| Site-input` *`site_name`* `| Site-output` *`site_name`*`}`

Parameters

- *`filter_name`* `Group` *`group_name`*

  Clears the global filter of the group "*`group_name`*"

- *`filter_name`* `Site-input` *`site_name`*

  Clears the input filter of the site "*`site_name`*"

- *`filter_name`* `Site-output` *`site_name`*

  Clears the output filter of the site "*`site_name`*"

BRIDGE CREATE

14.18.7

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command creates new filters and new groups for bridge control.

Type

`Global`

Format

`Bridge Create {Filter` *`filter_name`* `| Group` *`group_name`*`}`

Parameters

- `Filter` *`filter_name`*

  Creates a filter with the name "*`filter_name`*"

- `Group` *`group_name`*

  Creates a group with the name "*`group_name`*"

BRIDGE DELETE

14.18.8

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command deletes a bridge filter.

Type

`Global`

Format

`Bridge Delete Filter` *`filter_name`*

Parameters

- *`filter_name`*

  Deletes the specified filter.

BRIDGE FILTER (ASSIGNING ENTRY)

14.18.9

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

There are two extensions to this command, one that fills an entry in a named filter table (§14.18.10, "Bridge Filter (entry filling)" on page 116) and another that assigns a filter to a group or to a site, for input or output traffic (this command).

Type

`Global`

Format

`Bridge Filter` *`filter_name`* `Assign {Group` *`group_name`* `| Site-input` *`site_name`* `| Site-output` *`site_name`*`}`

Parameters

- *`filter_name`* `Assign Group` *`group_name`*

  Sets "*`filter_name`*" as the group filter for the group "*`group_name`*".

- *`filter_name`* `Assign Site-input` *`site_name`*

  Sets "*`filter_name`*" as the input filter for the site "*`site_name`*".

- *`filter_name`* `Assign Site-output` *`site_name`*

  Sets "*`filter_name`*" as the output filter for the site "*`site_name`*".

For more information on how filters are used, see §6.2.2, "Filtering" on page 50.

NOTE - Before assigning a filter, you must create it (§14.18.7, "Bridge Create" on page 113) and fill it (§14.18.10, "Bridge Filter (entry filling)" on page 116).

BRIDGE FILTER (ENTRY FILLING)

14.18.10

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

There are two extensions to this command, one that fills an entry in a named filter table (this command), and another that assigns a filter to a group or to a site, for input or output traffic (§14.18.9, "Bridge Filter (assigning entry)" on page 115).

Type

`Global`

Format

`Bridge Filter {`*`filter_name`* `{Permit | Deny} {src_addr` *`src_addr addr_mask`* `| dst_addr` *`dst_addr addr_mask`* `| llc_lsap` *`dsap_lsap lsap_mask`* `| ethII` *`prot_type type_mask`* `| snap` *`snap_addr snap_mask`* `| All | Tcpip | Ipx | AppleTalk}}`

Parameters

- *`filter_name`* `Permit src_addr` *`src_addr addr_mask`*

  Allows frames with source address "*`src_addr`*" masked with "*`addr_mask`*" to cross the filter.

`MUL:` **`bridge filter test permit src_addr 0102.0304.0506 ffff.ffff.ffff`**

- *`filter_name`* `Permit dst_addr` *`dst_addr addr_mask`*

  Allows frames with destination address "*`dst_addr`*" masked with "*`addr_mask`*" to cross the filter.

- *`filter_name`* `Permit llc_lsap` *`dsap_lsap lsap_mask`*

  Allows frames with llc field of a 802.3 Ethernet header matching the "*`dsap_lsap`*" value masked with the "*`lsap_mask`*" value to cross the filter.

- *`filter_name`* `Permit ethII` *`prot_type type_mask`*

  Allows frames with the protocol field of a Ethernet II header matching the "*`prot_type`*" value masked with the "*`type_mask`*" value to cross the filter.

- *filter_name* `Permit snap` *snap_addr snap_mask*

  Allows frames with the snap address field of a SNAP Ethernet header matching the "*snap_addr*" value masked with the "*snap_mask*" value to cross the filter.

- *filter_name* `Permit All`

  Allows all frames to cross the filter.

- *filter_name* `Permit Tcpip`

  Allows IP (and TCP, and UDP, etc...) frames to cross the filter. This is an alias that sets the proper values for the corresponding Ethernet II frames.

- *filter_name* `Permit Ipx`

  Allows IPX frames to cross the filter. This is an alias that sets the proper values for the corresponding Ethernet II, 802.2, 802.3 Ethernet and SNAP Ethernet frames.

- *filter_name* `Permit AppleTalk`

  Allows AppleTalk frames to cross the filter. This is an alias that sets the proper values for the corresponding Ethernet SNAP frames.

- *filter_name* `Deny src_addr` *src_addr addr_mask*

  Forbids frames with source address "*src_addr*" masked with "*addr_mask*" to cross the filter.

`MULTI:` **`bridge filter test deny src_addr 0102.0304.0506 ffff.ffff.ffff`**

- *filter_name* `Deny dst_addr` *dst_addr addr_mask*

  Forbids frames with destination address "*dst_addr*" masked with "*addr_mask*" to cross the filter.

- *filter_name* `Deny llc_lsap` *dsap_lsap lsap_mask*

  Forbids frames with llc field of a 802.3 Ethernet header matching the "*dsap_lsap*" value masked with the "*lsap_mask*" value to cross the filter.

- *filter_name* `Deny ethII` *prot_type type_mask*

  Forbids frames with the protocol field of a Ethernet II header matching the "*prot_type*" value masked with the "*type_mask*" value to cross the filter.

- *filter_name* Deny snap *snap_addr snap_mask*

  Forbids frames with the snap address field of a SNAP Ethernet header matching the "*snap_addr*" value masked with the "*snap_mask*" value to cross the filter.

- *filter_name* Deny All

  Forbids all frames to cross the filter.

- *filter_name* Deny Tcpip

  Forbids IP (and TCP, and UDP, etc...) frames to cross the filter. This is an alias that sets the proper values for the corresponding Ethernet II frames.

- *filter_name* Deny Ipx

  Forbids IPX frames to cross the filter. This is an alias that sets the proper values for the corresponding Ethernet II, 802.2, 802.3 Ethernet and SNAP Ethernet frames.

- *filter_name* Deny AppleTalk

  Forbids AppleTalk frames to cross the filter. This is an alias that sets the proper values for the corresponding Ethernet SNAP frames.

NOTE - You should not use "deny all" and then "allow something". The line "allow something" is sufficient to deny the rest of the traffic.

NOTE - Before filling a filter, you must create one (§14.18.7, "Bridge Create" on page 113). After filling it, you may assign it (§14.18.9, "Bridge Filter (assigning entry)" on page 115).

BRIDGE GROUP

14.18.11

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Global`

Format

`Bridge Group` *`group_name`* `{{On | Off} | {Assign-site | Remove-site}` *`site_name`*`}}`

Parameters

- *`group_name`* `{On | Off}`

  Enables or disables a group.

- *`group_name`* `Assign-site` *`site_name`*

  Assigns the site *`site_name`* to the group *`group_name`*.

- *`group_name`* `Remove-site` *`site_name`*

  Removes the site *`site_name`* from the group *`group_name`*.

BRIDGE INFO

14.18.12

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Gives information on the bridge configuration.

Type

`Interactive`

Format

`Bridge Info [All | Groups | Group` *`group_name`* `| Filters | Filter` *`filter_name`* `| Sites | Site [`*`site_name`*`]]`

Parameters

- *`none`*

  Lists global statistics of bridging traffic.

- `All`

  Gives all the information available with the following commands.

- `Groups`

  Lists the available bridge groups.

- `Group` *`group_name`*

  Lists the sites belonging to the group "*`group_name`*".

- `Filters`

  Lists the available filters.

- `Filter` *`filter_name`*

  Lists the parameters of the filter "*`filter_name`*", including where it is used.

- `Sites`

  Lists all sites involved in bridging. For each site, the bridge group it belongs to is listed.

- `Site [`*`site_name`*`]`

  Lists information about the "*`site_name`*" site's filters. If no site name is specified, the currently selected site is used.

BRIDGE ON & OFF

14.18.13

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Enables or disables the bridge.

Type

`Global`

Format

`Bridge {On | Off}`

Parameters

- `On`

  Turns the bridge on.

- `Off`

  Turns the bridge off.

Default value

`Off`

CAT

14.18.14

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command allows to display the content of a file.

Type

`Interactive`

Format

`Cat` *`filename`*

Parameters

- *`filename`*

  Displays the contents of the file *`filename`*. This is very useful to get a quick look at the `config` file or to check for errors in the `boot.rpt` file.

CAUTION — This command only displays the first 8 Kb of the target file. If you want to see the rest, use FTP or the Web interface.

CD

14.18.15

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Sets the default path to the ROM disk or to the RAM disk.

Type
Global

Format
Cd {#ROM | #RAM}

Parameters
- #ROM

```
MultiCom:Cd #ROM
#ROM: is the new directory
MultiCom:Pwd
#ROM:
```

- #RAM

```
MultiCom:Cd #RAM
#RAM: is the new directory
MultiCom:Pwd
#RAM:
```

DHCP

14.18.16

V 2.3	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command configures the Dynamic Host Configuration Protocol server, which provides configuration parameters to local machines, including: the IP address, the SubnetMask, the Gateway Address (the ***Multi**Com* itself) and the DNS configuration (if known).

Type

```
Global
```

Format

```
DHCP {On | Off | LeaseTime minutes | Range from .. to {Add
| Remove} | Add {client | xx:xx:xx:xx:xx:xx} IP_addr |
Remove {client | xx:xx:xx:xx:xx:xx} | Info}
```

Parameters

- `LeaseTime` *`minutes`*

  This is the delay a DHCP client is authorized to keep an allocated IP address. Before that time, it must renew its allocation. If you have portable computers used on your network and at home, you may need a short time here.

- `Range` *`from`* `..` *`to`* `{Add | Remove}`

  This defines the range of IP addresses, which form a pool of available addresses for dynamic allocation. Be careful to also include these addresses in the local IP range.

- `Add {`*`client`* `|` *`xx:xx:xx:xx:xx:xx`*`}` *`IP_addr`*

  This defines a static binding between a client machine (defined by its name or Ethernet address) and a fixed IP address. This is needed for servers which must be accessed locally or remotely, using a fixed IP address. This may also be used to centralize the network management of PCs.

NOTE - This IP address will be reserved for this machine, even if it is in the address pool for dynamic allocation.

- `Remove {client | xx:xx:xx:xx:xx:xx}`

  This removes an entry from the static IP allocation table. This will not release the address, if allocated, until the LeaseTime expires.

- `Info`

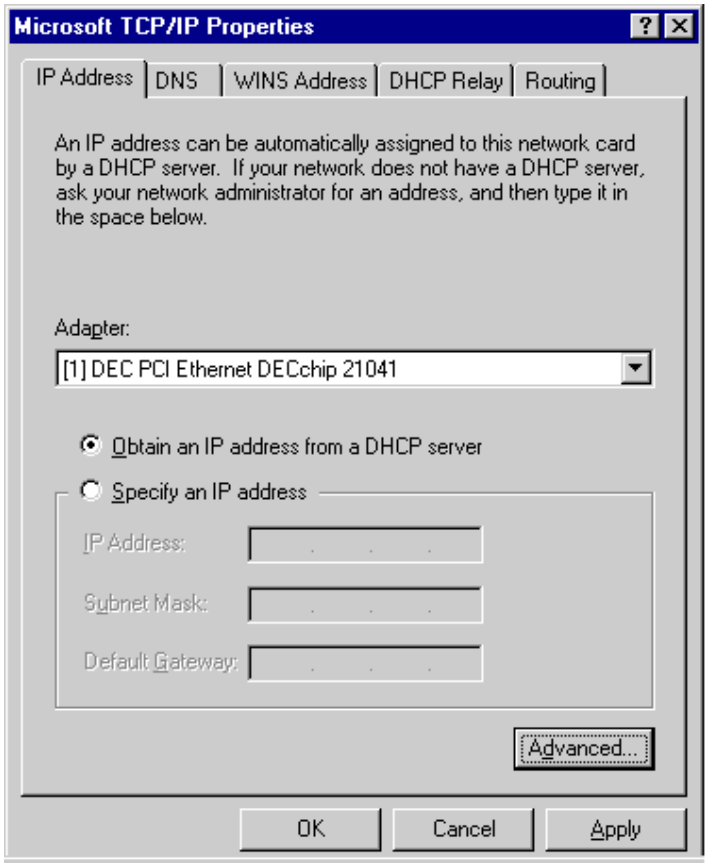
  This gives detailed information about the status and configuration of the DHCP server.

```
MultiCom:DHCP Info

DHCP server is running.

Configuration :
Lease time     : 12 minutes
Renewal time   : 6 minutes
Rebinding time : 10 minutes
Netmask        : 255.255.255.0
Gateway        : 193.5.2.180
DNS            : 193.5.2.161, 193.246.108.10
Domain name    : lightning.ch

Static allocation clients :
10.0.0.2 : www

Dynamic allocation ranges :
10.0.0.2 .. 10.255.255.255

Current clients list :
```

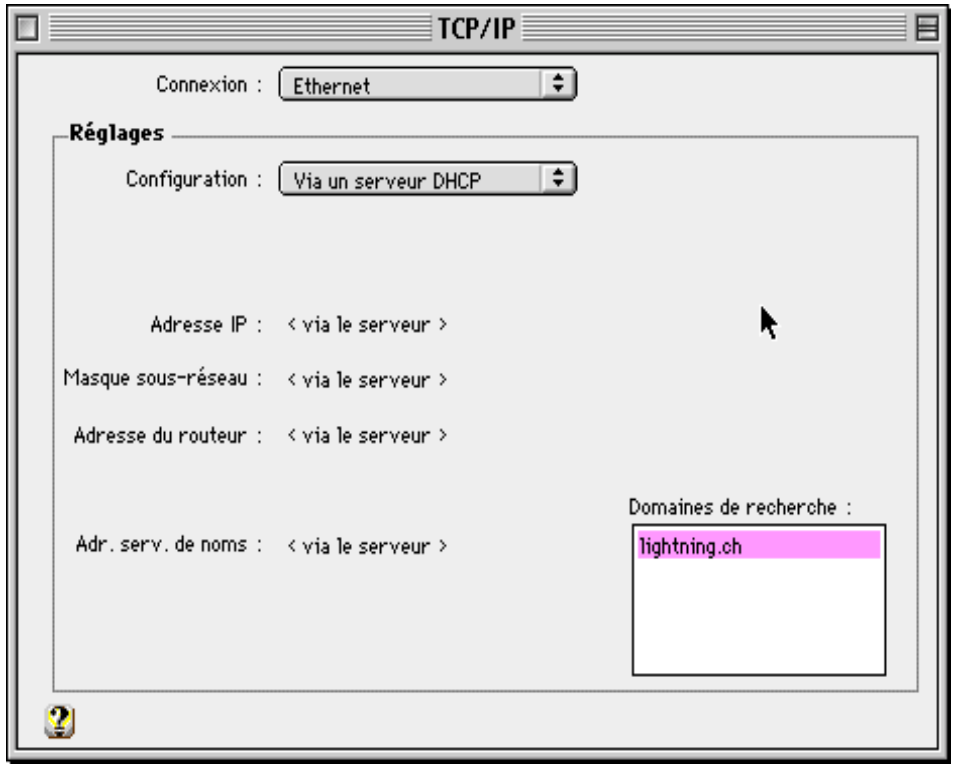
- on

  Enables the DHCP server. All machines on the Local Area Network (LAN) can be auto-configured by the ***MultiCom***. They must be set as “DHCP clients” to receive this information.

  Under Windows 95/98/NT, you have to use the TCP/IP setup inside the “Network” control panel:



Under MacOS, you have to use the “TCP/IP” control panel:



- `Off`

  Disables the DHCP server immediately. Clients with an allocated IP address will lose it after the LeaseTime expires.

Default value

```
DHCP Off
LeaseTime 12 min.
```

DIAGNOSE

14.18.17

V 2.3	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Displays advanced diagnostics about your ***Multi**Com*. This is the first command you should use in case of problems.

Type

`Interactive`

Format

`Diagnose`

Parameters

- *none*

  This command analyzes some internal counters and status variables and displays warnings about possible problems, along with suggestions for correction and the command to use for detailed troubleshooting.

```
MultiCom:Diagnose

Welcome to advanced diagnostics

No ethernet packets have been routed.
-> type "Info IProuter" for more info

Site: Lockeed
PPP authentication failed.
-> check PPP username and password

Site: Test
No packets are received on the PPP connection
-> check the PPP sites parameters
or try to make a connection
```

DNS

14.18.18

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command allows the management of the built-in Domain Name Service client.

Type

`Global`

Format

`DNS {Primary` *`IP-address`* `| Secondary` *`IP-address`* `| DomainName` *`domain`* `| Cache [{Enable | Disable}] | Info}`

Parameters

- `Primary` *`IP-address`*

  Sets the address of the primary DNS server.

```
MultiCom:DNS primary 196.4.2.34
Primary DNS server address : 196.4.2.34
```

- `Secondary` *`IP-address`*

  Sets the address of the secondary DNS server. The secondary server will be used if the primary server does not respond to name lookups.

```
MultiCom:DNS secondary 196.4.2.35
Secondary DNS server address : 196.4.2.35
```

- `DomainName` *`the_name`*

  Sets the default domain name.

  When doing a Telnet to a machine, you can specify the machine's complete name (e.g. "*telnet fido.cs.mit.edu*"), which is known as a fully qualified name, or you can use an unqualified name (e.g. a name without dots: "*telnet fido*"). If you use an unqualified name, the ***MultiCom*** will automatically append this default domain name.

```
MultiCom:DNS DomainName lightning.ch
The domain name is << .lightning.ch >>
```

- `Cache`

  Displays the current state of the cache. By default, it is enabled.

```
MultiCom:DNS Cache
Cache management is ENABLED.
```

- `Cache Enable`

  Enables the DNS cache.

  This will keep in memory recent DNS queries, to speed-up further requests to the same names.

```
MultiCom:DNS Cache Enable
Cache management is ENABLED.
```

- `Cache Disable`

  Disables the DNS cache.

  This may be used to save memory when DNS is not used.

```
MultiCom:DNS Cache Disable
Cache management is DISABLED.
```

- `Info`

  Displays the current DNS configuration and related statistics.

```
MultiCom:DNS info
Primary DNS server address : 196.4.2.20
Secondary DNS server address : 196.4.2.21
Cache management is ENABLED.
Domain name : .cs.mit.edu

Statistics for DNS
------------------
Nbr Requests Received                    = 2
```

```
Nbr Requests Rejected                    = 0
Nbr Requests Resolved By Cache           = 0
Nbr Requests Unresolved By Cache         = 2
Nbr Requests Resolved By Primary DNS     = 2
Nbr Requests Unresolved By Primary DNS   = 0
Nbr Requests Resolved By Secondary DNS   = 0
Nbr Requests Unresolved By Secondary DNS = 0
Nbr Packets Sent                         = 2
Nbr Packets Received                     = 13
Nbr Packets Rejected                     = 11
```

DNS GETFROM

14.18.19

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the AutoDNS feature.

Type
`Global`

Format
`DNS GetFrom site`

Parameters
- `site`

  This specify the site from which DNS configuration should be retrieved. At start-up, if no DNS is configured, the ***MultiCom*** will retrieve this information from the remote site and store it in the config file for further reference. If DNS servers are manually configured anyway, they will be used until a connection takes place and a new configuration is given by PPP.

NOTE - The chosen site must be a PPP WAN site.

NOTE - The ***MultiCom*** is, of course, also capable to provide this information to clients requesting it ...

EDIT

14.18.20

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command activates a very simple line text editor, for the initial configuration of your ***MultiCom***.

Type
`Interactive`

Format
`Edit [filename]`

Parameters

- *none*

  Opens the current configuration file in `#RAM:config` for edition.

- *filename*

  Open a specified file, for example the default configuration file in `#ROM:config`.

```
MultiCom:Edit #ROM:config
-------- EDIT --------
Current file name is : #ROM:CONFIG
? to get this help
I to insert a line
M to modify a line
D to delete a line
S to save the file
W to save the file as ..
SPACE to go forward in the file
Q or  CTRL-] to quit without saving
```

CAUTION — With this command, **you can only edit configuration files smaller than 4096 bytes** (typically the default configuration). Afterwards, you are strongly advised to use the EditConfig Windows application or FTP and a full-fledged text editor on your computer.

Default value

```
#RAM:config
```

HARDWARE

14.18.21

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Displays hardware information.

Type
`Interactive`

Format
`Hardware Info`

Parameters
- *none*

  Displays hardware information about your ***Multi**Com*. This includes the type of motherboard, the optional extension cards, the physical RAM and Flash memory size. Please use this command **before** any call to Customer Support.

```
MultiCom:Hardware Info

Type of machine: MultiCom Lan Access Center, Motherboard version 1.1

Extension slots:
Slot 1 = <Empty>
Slot 2 = <Empty>
Slot 3 = <Empty>
Slot 4 = LACx4BRI

RAM size [kbytes]: 4096

Flash size [kbytes]
bank 1: 4096
bank 2: 0
```

HELP

14.18.22

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Our simple on-line help system.

Type

`Interactive`

Format

`Help [`*`command`*`]`

Parameters

- *none*

  Displays the list of recognized commands.

```
MultiCom:Help

The following commands are recognized:
Account   ARP       Backup    Bridge    cat       cd        DNS       Edit
Hardware  IP        IPX       ISDN      Key       ls        Mem       MHDLC
MyName    Ping      PPP       pwd       Quit      Reboot    Rename    rm
Security  Serial    Site      Sleep     SNMP      SNTP      Syslog    Telnet
Time      Traceroute          Upgrade   Uptime    User      Version
WriteConfig

For more information, please consult the Reference Manual.
```

- *command*

  Entering `Help` followed by a command name generates specific help text for that command.

  The alternate format *`Command`* `Help` is also available.

INFO

14.18.23

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

To get detailed information about your ***MultiCom***.

Type

`Interactive`

Format

`Info [topic]`

Parameters

- *none*

  Without parameter, this command displays the list of valid topics.

```
MultiCom:Info

Usage: Info topic
Valid topics...
ARP             displays ARP statistics and the contents of its cache
Bridge          bridge statistics
DNS             statistics on DNS requests
Hardware        displays information about the hardware platform
IP              IP config, IP Router tables and statistics on IP traffic
IPX             status of the IPX router
ISDN            general ISDN information
Key             displays the encryption keys currently defined
Mem             displays the amount of free memory
PPP             information on PPP negotiations & statistics on PPP traffic
Site            lists all site names or the config of a given site
SNMP            displays SNMP managers and communities
SNTP            displays information about SNTP
Time            Sets or displays the RTC time and date
Version         displays the software versions and options
```

- *topic*

  Displays detailed information and statistics about the specified topic.

  The alternate format *Topic* `Info` is also available.

  The `Info` command is further described in the paragraphs related to specific parts of the firmware. For example the “Info Bridge” command is described in §14.18.12, "Bridge Info" on page 120.

IP DEFAULTROUTER

14.18.24

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command specifies the default gateway used by the internal IP host. **It does not apply to routed traffic.**

Type
`Global`

Format
`IP DefaultRouter` *`IP_Address`*

Parameters

- *`none`*

  Without parameter, this command displays the current default router.

```
MultiCom:IP DefaultRouter
Default IP router set to <NIL>
```

- *`IP_Address`*

  Set the address of the default IP router. This is only used by the IP host, not for packets in transit. Those must be explicitly routed with the command "`IP Range`" (see page 146).

```
MultiCom:IP DefaultRouter 128.178.149.1
Default IP router set to 128.178.149.1
```

NOTE - The default router must be on the local Ethernet site.

IP DYNAMICRANGE

14.18.25

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the pool of dynamic IP addresses distributed by PPP. See also §14.18.29, "IP RemoteAddr" on page 148.

Type

`Global`

Format

`IP DynamicRange {Info | x.x.x.x .. y.y.y.y {Add | Remove}}`

Parameters

- *none* or `Info`

  Displays the current address pool, the list of allocated addresses and the list of used addresses.

- `x.x.x.x .. y.y.y.y Add`

  Inserts a new range into the dynamic address pool.

- *x.x.x.x .. y.y.y.y* `Remove`

  Removes a range from the dynamic address pool.

NOTE - The ***MultiCom*** tries to re-allocate the same IP address to the same remote site, if possible, to avoid disrupting idle sessions.

IP FILTER

14.18.26

V 2.6.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the filtering of IP packets. See §4.6, "IP Filtering" on page 37 for more information on filtering and firewalls.

Type

`Global`

Format

```
IP Filter {Allow | Deny} From src_addresses [Port
src_ports/{TCP|UDP}] To dst_addresses [Port dst_ports/
{TCP|UDP}] [Log]
IP Filter {Allow | Deny} From src_addresses To
dst_addresses ICMP type [Log]
IP Filter {On | Off | Clear | Info}
IP Filter RouterFrames {On | Off}

addresses = [x.x.x.x .. ]y.y.y.y
ports = [n .. ]m/{TCP|UDP}
```

- `{Allow | Deny} From src_addresses [Port src_ports/{TCP|UDP}] To dst_addresses [Port dst_ports/{TCP|UDP}] [Log]`

  This command adds an entry in the filtering table to allow or deny packets whose parameters are within the specified address ranges and port numbers. *src_addresses*, *dst_addresses*, *src_ports* and *dst_ports* can be a single address or port, or a range (two addresses or ports separated by ‘ .. ’). The source and/or destination port(s) can be omitted, in which case all ports are allowed or denied. The special keyword `Any` can be used to replace the full range of all possible IP addresses (`0.0.0.0 .. 255.255.255.255`). See §4.6.1, "Examples" on page 38 for detailed examples.

- `{Allow | Deny} From src_addresses To dst_addresses ICMP type [Log]`

  These commands add an entry in the filtering table to allow or deny ICMP packets within the specified source and destination address ranges. *type* is an integer corresponding to specific ICMP message types. The following key-

words can be used as *type* instead of a numeric value: `EchoRequest`, `EchoReply`, `DestUnreachable`, `Redirect`, and `TimeExceeded`.

If the optional `Log` parameter is given, all packets matching this entry generate a syslog notification message. The text of the message is similar to the syslog message sent by PAT (see §14.18.35, "IP Translation" on page 155), and contains the source and destination addresses of the packet, as well as the port numbers, if applicable.

NOTE - The syslog client must be correctly configured for this option to work. See §14.18.130, "Syslog" on page 282.

- `On | Off`

  These commands turn the IP filter on or off. When the IP filter is off, the filtering table is ignored and all packets are allowed through the router.

- `Clear`

  This command clears the filtering table. After this command is executed, the filtering table is completely empty, and thus all packets are rejected (except packets to/from the router itself, depending on the `IP Filter RouterFrames` setup).

- `Info`

  This command displays the content of the filtering table as well as the packet counter associated to each entry of the table.

- `RouterFrames On`

  This command turns on the filtering of the IP frames coming from or going to the router itself. This allows additional security by controlling access to the router (for example, by only allowing a single machine to manage the ***MultiCom***) but, if misused, it can result in an unreachable ***MultiCom***, in which case only the console connection or a reboot in default configuration can help you regain control to it.

- `RouterFrames Off`

  This command turns off the filtering of the IP frames coming from or going to the router itself, so that the ***MultiCom*** is always reachable, independently of the filtering entries. This is the (safe) default.

Default value

```
IP Filter RouterFrames Off
```

By default, **all packets not explicitly allowed are rejected** ("`IP Filter Deny From Any To Any`"). If the "`IP Filter Allow From Any To Any`" command is added last, all packets, including ICMP packets, which have not been explicitly denied will be allowed through the router.

IP MYADDR

14.18.27

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command allows to dynamically modify the global IP address of the ***MultiCom***.

Type

`Global`

Format

`IP MyAddr [`*`IP_Address`*`]`

Parameters

- *none*

  Without parameter, this command displays the current global IP address of the ***MultiCom***.

```
MultiCom:IP MyAddr
My IP Address is 193.5.2.180
```

- *IP_Address*

  Defines the address of the ***MultiCom*** IP host, in standard dotted decimal notation (see §4.1, "IP Addresses" on page 24). If you choose an address which was already used, you may get ARP problems. In that case, flush ARP tables (i.e. by rebooting) on all client machines.

```
MultiCom:IP MyAddr 193.5.2.180
My IP Address set to 193.5.2.180
```

Default value

`10.0.0.1` after firmware 2.3
`1.1.1.1` before firmware 2.3

NOTE - If you cannot change this address using the **console** connection, you can temporarily change the address of your computer to `10.0.0.2` and connect it directly to your ***MultiCom***, to be able to configure it using a **network** connection.

IP RANGE

14.18.28

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the static routing table for IP.

Type

`Site-specific`

Format

`IP Range [`*`from`* `..` *`to`* `{Add | RoutedOn` *`site`* `| RoutedTo` *`gateway`* `| Remove} [Encrypted KeyID` *`key_name`*`]]`

Parameters

- *none*

  Displays all existing IP ranges in the routing table.

```
MultiCom:IP Range
IP Range 1.1.1.1 .. 193.5.1.254 routed on "Internet"
IP Range 193.5.2.1 .. 193.5.2.200 routed on "Headquarters"
IP Range 193.5.2.201 .. 193.5.2.220 routed on "Subsidiary"
IP Range 193.5.2.221 .. 193.5.2.254 routed to 193.5.2.1
IP Range 193.5.3.1 .. 255.255.255.254 routed on "Internet"
```

- `Range` *`from`* `..` *`to`* `Add`

  This command instructs the router that the specified IP range belongs to the currently selected site.

```
MultiCom:Site Select Local
Site "Local" selected.

MultiCom:IP Range 193.5.2.1 .. 193.5.2.254 Add
IP Range 193.5.2.1 .. 193.5.2.254 routed on "Local" inserted
```

- `Range` *`from`* `..` *`to`* `RoutedOn` *`site`*

  This command is used to indicate that the specified IP range belongs to the specified site.

```
MultiCom:IP Range 10.0.0.2 .. 10.255.255.254 RoutedOn Local
IP Range 10.0.0.2 .. 10.255.255.254 routed on "local" inserted
```

- Range *from* .. *to* RoutedTo *gateway*

  This command is used to indicate that the specified IP range is behind another local router. This command is required if the other router does not do proxy ARP. The other router must be on the same Ethernet as the ***MultiCom***.

```
MultiCom:IP Range 1.1.1.1 .. 2.2.2.2 RoutedTo 3.3.3.3
IP Range 1.1.1.1 .. 2.2.2.2 routed to 3.3.3.3 inserted
```

- Range *from* .. *to* Remove

  Deletes an IP range from the routing table.

```
MultiCom:IP Range 193.5.2.1 .. 193.5.2.254 Remove
IP Range 193.5.2.1 .. 193.5.2.254 deleted.
```

NOTE - Only an existing line in the router table may be deleted.

- … Encrypted KeyID *key_name*

  Sets the encryption key for the specified IP range. This allows to create Virtual Private Networks (see §13.3, "IP-level Encryption" on page 92).

```
MultiCom:IP Range 1.1.1.1 .. 2.2.2.2 Add Encrypted KeyID my_key
IP Range 1.1.1.1 .. 2.2.2.2 routed on “Secure” inserted
```

NOTE - The encryption option (/E) is needed to use this command.

IP REMOTEADDR

14.18.29

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the distribution of IP addresses through PPP.

Type

`Site-specific`

Format

`IP RemoteAddr [{None | x.x.x.x | Dynamic | Info}]`

Parameters

- *none* or `Info`

  Displays the current configuration of this feature.

- `None`

  Do not send an IP address to the remote site, even if requested.

- *x.x.x.x*

  Sends a static IP address to the remote site, if requested.

- `Dynamic`

  Sends a dynamic IP address from the address pool defined by "`IP DynamicRange`" (see page 140), when requested.

NOTE - IP addresses distributed either statically or dynamically are dynamically routed, independently of the defined IP ranges.

Default value

`None`

IP ROUTER

14.18.30

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is mainly useful for debugging, to enable or disable the IP routing function of your ***Multi**Com*.

Type
`Global`

Format
`IP Router [{On | Off}]`

Parameters

- *none*

  Displays the current state of the IP router.

```
MultiCom:IP Router
IP Router is off.
```

- `On`

  Turns the IP router on.

```
MultiCom:IP Router On
IP Router is on.
```

- `Off`

  Turns the IP router off.

```
MultiCom:IP Router Off
IP Router is off.
```

Default value
`Off`

IP ROUTER ENCRYPTION

14.18.31

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

Global

Format

```
IP Router Encryption [{On | Off}]
```

Parameters

- *none*

  Without parameter, this command tells if the IP-level encryption is enabled or disabled.

```
MultiCom:IP Router Encryption
IP Data encryption is enabled.
```

- On

  Enables the IP-level encryption.

```
MultiCom:IP Router Encryption On
IP Data encryption enabled.
```

- Off

  Disables the IP-level encryption.

```
MultiCom:IP Router Encryption Off
IP Data encryption disabled.
```

Default value

Off

IP SENDNETBROADCAST

14.18.32

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the routing of IP network broadcasts.

Type

```
Site-specific
```

Format

```
IP SendNetBroadcast {On | Off}
```

Parameters

- `On`

  Enables the sending of IP network broadcasts to the selected site. The ***MultiCom*** will only send IP network broadcasts to remote sites if they contain any hosts that belong to the same IP network.

- `Off`

  Disables the sending of IP network broadcasts to the selected site.

Default value

```
Off
```

CAUTION — Use this feature with precautions, as it may keep your ISDN line up.

IP SITEADDR

14.18.33

V 2.3	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command allows to set the external IP addresses of the selected site, statically or dynamically.

Type

```
Site-specific
```

Format

```
IP SiteAddr [Info]
IP SiteAddr {Dynamic | None | ext_addr}
IP SiteAddr {Dynamic | Global | ext_addr} For low .. high
IP SiteAddr {Dynamic | Global | ext_addr} MapTo addr
IP SiteAddr {Dynamic | Global | ext_addr} Remove
```

Parameters

- *none* or Info

  Displays the current site address configuration of the selected site.

- Dynamic

  Requests an IP address from the remote site, using standard PPP commands. See §14.18.25, "IP DynamicRange" on page 140 and §14.18.29, "IP RemoteAddr" on page 148 to learn how to **distribute** dynamic addresses.

- None

  This site has no own IP address, it will share the global ***MultiCom*** address. This is backward-compatible with older versions.

- *ext_addr*

  Use a statically defined IP address. This is needed if you want to provide local services to the Internet, so that the DNS knows where to direct incoming requests to your servers. It is generally provided by your Internet Service Provider.

- For *low .. high*

  Specifies that this local address range will use PAT to translate all included addresses to the given external address (either the global address of the router,

the dynamically allocated address received by PPP or a statically specified address). This command can be used many times for the same external address, to specify disjoint local address ranges.

- `MapTo` *addr*

  Specifies that this local address will use NAT to translate it to the given external address (either the global address of the router, the dynamically allocated address received by PPP or a statically specified address). This command is exclusive with another `MapTo` or `For` command using the same external address.

- `Remove`

  Removes an entry from the IP mapping table.

Default value
`None`

CAUTION — Using NAT will disable the SecureWall™ on some machines, which can open a security hole in your network, from which other machines protected by the SecureWall™ may be attacked. Use it at your own risk!

For more information about NAT and PAT, and for detailed examples, please see §14.18.35, "IP Translation" on page 155 and §4.4, "IP Translation" on page 28.

IP SUBNETMASK

14.18.34

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command defines the SubnetMask used on the LAN side.

Type

`Global`

Format

`IP SubnetMask` *`x.x.x.x`*

Parameters

- `SubnetMask` *`x.x.x.x`*

  Sets the IP Subnet Mask for the local Ethernet. Standard values are `255.0.0.0` for an A-class network, `255.255.0.0` for a B-class network and `255.255.255.0` for a C-class network.

```
MultiCom:IP SubnetMask 255.255.255.0
Subnet mask set to 255.255.255.0
```

Default value

`255.255.255.255`

NOTE - See §4.1.2.3, "IP Subnet Masks" on page 25 for details on how to use a Subnet Mask.

IP TRANSLATION

14.18.35

V 2.3	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the NAT and PAT features. With it, you can share a Single Internet User Account with an unlimited number of machines on your LAN (depending on your options), hide all your machines behind a simple firewall and translate private internal addresses into valid Internet addresses.

Type

```
Site-specific
```

Format

```
IP Translation [{On | Off | Info}]
IP Translation Map [{Dynamic | Global | ext_addr}:]port/
protocol To addr[:dest_port]
IP Translation Unmap [{Dynamic | Global |
ext_addr}:]port/protocol
```

Parameters

- *none*

  Without parameter, this command displays the current status of this feature.

- On

  Enables the IP address translation for the currently selected site. All outgoing IP packets will use one of the current site addresses (see §14.18.33, "IP SiteAddr" on page 152) as source address. The reverse translation will be done on reply packets.

- Off

  Disables the IP address translation for the currently selected site.

- Info

  Gives detailed information about NAT and PAT, as well as the content of the static services mapping table.

- `Map [{Dynamic | Global | ext_addr}:]port/protocol To addr[:dest_port]`

  Allows to statically map some services (like www, mail, news, telnet, ...) to a specific internal server (and optionally change the destination port as well). You must specify these services by using their port number and protocol (`tcp` or `udp`). You can define up to 64 services in this table.

  Optionally, you can specify for which external address this translation is valid, either the global address of the router, the dynamically allocated address received by PPP or a statically specified address.

  To fully use these services, you need a statically assigned IP address from your Internet Service Provider (ISP), so that the DNS knows where to find your services. You should also statically configure the IP address of your servers, either on the servers themselves or by using static DHCP mapping (see §14.18.16, "DHCP" on page 124).

  All other incoming requests are dropped and optionally logged with "`Syslog`" (see page 282) as break-in attempts, providing SecureWall™ protection.

- `Unmap [{Dynamic | Global | ext_addr}:]port/protocol`

  Allows to remove an entry from the static services mapping table.

Default value
`Off`

CAUTION — Using NAT will disable the SecureWall™ on some machines, which can open a security hole in your network, from which other machines protected by the SecureWall™ may be attacked. Use it at your own risk!

For more information about NAT and PAT, and for detailed examples, please see §14.18.33, "IP SiteAddr" on page 152 and §4.4, "IP Translation" on page 28.

IPX ETHTYPE

14.18.36

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Sets the Ethernet frame type for the currently selected site.

Type
`Site-specific`

Format
`IPX EthType [{802.2 | 802.3 | eth2 | SNAP}]`

Parameters

- *none*

  Displays the currently selected Ethernet frame type

```
MultiCom:IPX EthType
IPX eth type for site Local is 802.2
```

- `802.2`

  Changes the Ethernet frame type accepted on the currently selected site to 802.2

```
MultiCom:IPX EthType 802.2
IPX eth type for site Local is 802.2
```

- `802.3`

  Changes the Ethernet frame type accepted on the currently selected site to 802.3

```
MultiCom:IPX EthType 802.3
IPX eth type for site Local is 802.3
```

- `eth2`

  Changes the Ethernet frame type accepted on the currently selected site to Ethernet II.

```
MultiCom:IPX EthType eth2
IPX eth type for site Local is eth2
```

- SNAP

  Changes the Ethernet frame type accepted on the currently selected site to SNAP

```
MultiCom:IPX EthType SNAP
IPX eth type for site Local is SNAP.
```

Default value

802.2

NOTE - Currently, it must be done even for remote sites.

CAUTION — You may use different Ethernet frame types on different sites, but you may only use one type on each site. That is, all your servers on a site should use the same Ethernet frame type. In fact, this is also recommended by Novell®.

IPX INFO

14.18.37

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command displays general information on IPX.

Type
`Interactive`

Format
`IPX Info`

Parameters
- *none*

```
MultiCom:IPX Info
Internal network
IPX: off

Site: Basel
IPX: on          Type:     LAN          Protocol: 802.3   Net id:   0x00000002
RIP info: 4      SAP info: 18

Site: Koeln
IPX: on          Type:     Demand WAN   Protocol: 802.3   Net id:   Not Set
RIP info: 2      SAP info: 5

Site: Berlin
IPX: on          Type:     Demand WAN   Protocol: 802.3   Net id:   Not Set
RIP info: 2      SAP info: 6

Site: LISA
IPX: off

RIP cache is on

IPX router is on
```

IPX INTERNALNETNUMBER

14.18.38

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command allows you to set the Internal NetNumber. The Internal NetNumber is the address of the virtual IPX LAN present inside the ***MultiCom***. It will be used in future firmware releases to support our own services like SNMP over IPX.

Type

`Global`

Format

`IPX InternalNetNumber` *`number`*

Parameters

- *`number`*

  Sets the Internal NetNumber to *`number`*.

```
MultiCom:IPX InternalNetNumber 0xaabcd1
IPX internal net number set to 0xaabcd1
```

NOTE - You must use the hexadecimal format with a leading `0x` (i.e. `0xa` for “a” hexadecimal = “16” decimal).

IPX NETNUMBER

14.18.39

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Sets the Cable NetNumber for the currently selected site.

Type

`Site-specific`

Format

`IPX NetNumber` *`number`*

Parameters

- *`number`*

  Sets the Cable NetNumber to *`number`*.

```
MultiCom:IPX NetNumber 0xabc1
IPX net number for site my_site set to 0xabc1.
```

Default value

`Not Set`

NOTE - You must use the hexadecimal format with a leading “0x” (i.e. 0xa for “a” hexadecimal = “10” decimal).

CAUTION — When configuring the NetNumber do not confuse the Internal NetNumber of your Novell® server and the Cable or Ethernet interface network number. **You must use the Cable network number**.

IPX RESET

14.18.40

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command allows you to reset the contents of RIP & SAP tables.

Type

```
Global
```

Format

```
IPX Reset [{RIP | SAP}]
```

Parameters

- *none*

  Reset both RIP and SAP tables.

```
MultiCom:IPX reset
RIP & SAP tables have been reset.
```

- RIP

  Empties the RIP tables.

```
MultiCom:IPX reset RIP
RIP tables have been reset.
```

- SAP

  Empties the SAP tables.

```
MultiCom:IPX reset SAP
SAP tables have been reset.
```

CAUTION — If you use **Demand RIP** and you reset the RIP or SAP tables, the remote sites will not be updated. You must turn the router OFF and ON for this to happen. But be aware that turning the router ON and OFF may cause a lot or traffic on routers with many remote sites.

IPX ROUTER

14.18.41

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This is the main switch for IPX.

Type

`Global`

Format

`IPX Router [{On | Off}]`

Parameters

- *none*

  Without arguments returns the current state:

```
MultiCom:IPX Router
IPX router is off.
```

- `On`

  Turns the IPX router on.

```
MultiCom:IPX Router On
IPX router is on.
```

- `Off`

  Turns the IPX router off.

```
MultiCom:IPX Router Off
IPX router is off.
```

Default value
`Off`

CAUTION — Turning the router off then on in interactive mode may cause a lot of traffic due to power-down and power-up IPX sequences. If you have remote IPX sites on ISDN, it will open your lines to these sites.

IPX SITE

14.18.42

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Enables or disables the IPX routing for the currently selected site.

Type

Site-specific

Format

```
IPX Site [{On | Off}]
```

Parameters

- *none*

  Without parameter, this command displays the current status of this feature on the current site.

```
MultiCom:IPX Site
IPX protocol for site Internet is inactive.
```

- On

  Turns IPX routing on, for the current site.

```
MultiCom:IPX Site On
IPX protocol for site Headquarters is active.
```

- Off

  Turns IPX routing off, for the current site.

```
MultiCom:IPX Site Off
IPX protocol for site Internet is inactive.
```

Default value

Off

IPX SITETYPE

14.18.43

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Allows you to change the IPX type of a site.

Type

```
Site-specific
```

Format

```
IPX SiteType [{LAN | WAN | DemandWAN}]
```

Parameters

- *none*

  Displays the IPX site type for the currently selected site.

- `LAN`

  Change the site type to LAN.

NOTE - LAN sites may not be changed.

- `WAN`

  Change the site type to WAN.

NOTE - You can use the WAN type for permanent connections.

- `DemandWAN`

  Change the site type to DemandWAN. This includes spoofing of the RIP and SAP traffic, to avoid unneeded connections. It is best suited for dial-up connections.

CAUTION — These spoofing protocols being implemented differently by each manufacturer, **we cannot guarantee that a connection can be made with another router in DemandWAN mode**.

NOTE - See §5.2, "IPX Site Types" on page 42 for details on the differences between LAN, WAN and DemandWAN.

Default value

```
LAN (on LAN sites)
DemandWAN (on WAN sites)
```

CAUTION — For your router to work properly, you must configure both sides of an ISDN link to use the same type, i.e. a WAN site will work only with another WAN site and a DemandWAN site with another DemandWAN site.

CAUTION — If you change the site type while the router is running, you must turn the router OFF and ON for the other site to be updated. But be aware that turning the router ON and OFF may cause a lot or traffic on routers with many remote IPX sites.

IPX SPOOFING

14.18.44

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command allows you to control the IPX spoofing.

Type

```
Site-specific
```

Format

```
IPX Spoofing [{IPXwatchdog | SPXwatchdog | Serial |
netBIOS | netBIOSprop} {On | Off}]
```

Parameters

- *none*

  Displays the state of IPX spoofing on the current site

- `IPXwatchdog {On | Off}`

  Turn the spoofing of IPX watchdog packets on or off.

- `SPXwatchdog {On | Off}`

  Turn the spoofing of SPX watchdog packets on or off.

- `Serial {On | Off}`

  Turn the spoofing of Serial number packets on or off.

- `netBIOS {On | Off}`

  Turn the spoofing of all netBIOS packets on or off.

- `netBIOSprop {On | Off}`

  Turn the spoofing of netBIOS propagation packets on or off.

Default value

```
All On
```

CAUTION — Spoofing is currently available only on LAN sites. You must therefore select a LAN site for this command to work.

IPX STATS

14.18.45

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command will display some statistics on incoming and outgoing packets.

Type

```
Interactive
```

Format

```
IPX Stats
```

Parameters

- *none*

  Display statistics.

```
MultiCom:IPX Stats
ipxBasicSysInReceives: 68    ipxBasicSysOutPackets: 9041
ipxBasicSysInDelivers: 0     ipxBasicSysOutRequests: 9041
ipxBasicSysInDiscards: 0     ipxBasicSysOutDiscards: 0
ipxBasicSysInHdrErrors: 0    ipxBasicSysOutMalformedRequests: 0
ipxBasicSysInBadChecksums: 0 ipxBasicSysInUnknownSockets: 0
ipxBasicSysNoRoutes: 0

ipxAdvSysForwPackets: 0      ipxAdvSysNETBIOSPackets: 0
ipxAdvSysInFiltered: 0       ipxAdvSysOutFiltered: 0
ipxAdvSysInTooManyHops: 0
```

NOTE - These counters are in the IPX MIB, which is located at the following place:
enterprise.novell.mibDoc.ipx.ipxSystem.ipxBasicSysTable.ipxBasicSysEntry

For more information on MIB and SNMP see §12, "SNMP" on page 83.

ISDN AUTO

14.18.46

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the automatic Dial-on-Demand feature.

Type

`Site-specific`

Format

`ISDN Auto [{On | Off}]`

Parameters

- *none*

  Without parameter, this command displays the current state of this feature.

```
MultiCom:ISDN Auto
Automatic use of the ISDN lines Disabled for site "Lausanne".
```

- `On`

  Configure the ***MultiCom*** so that it automatically opens a connection when packets need to be forwarded. Further channels will be automatically opened if sufficient traffic is detected. The maximum number of used B-channels is set by "`ISDN BChannel`" (see page 173).

```
MultiCom:Select Geneva
Site “Geneva” selected.
MultiCom:ISDN Auto On
Automatic use of the ISDN lines Enabled for site “Geneva”
```

- `Off`

  Setting this option to `Off` means that the connection has to be opened manually using "`ISDN Conn`" (see page 177). This is useful for dail-in sites.

  This command causes all B-channels that are open for the selected site to be closed immediately and prevents them from being re-opened automatically.

Default value
`Off`

NOTE - The ***MultiCom*** will close the B-channels automatically, regardless of the value of `ISDN Auto`. The B-channel will be closed if there is no traffic on the connection for a specified time (see §14.18.53, "ISDN IdleCloseTime" on page 181). You can also manually close a B-channel (see §14.18.51, "ISDN Disc" on page 179).

NOTE - The `ISDN Auto` command only applies to the ***MultiCom***'s ability to initiate outgoing calls. It does not prevent incoming connections (for that purpose, see §14.18.62, "ISDN NumberEnabled" on page 197).

CAUTION — Care should be taken when `ISDN Auto` is set to `On`. If there is regular traffic over the line, the connection may remain open indefinitely, leading to large telephone bills.

ISDN BCHANNEL

14.18.47

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command sets the maximum number of B-channels that the selected site is allowed to use simultaneously.

Type

`Site-specific`

Format

`ISDN BChannel [`*n*`]`

Parameters

- *none*

  Without parameter, this command displays the number of allowed B-channels on the current site.

- *n*

  Specify the maximum number of B-channels that the selected site is allowed to use concurrently when using Channel Bundling with MHDLC or PPP. A Bandwidth-on-Demand (BoD) algorithm will be used to decide how many channels are really needed. These channels can also be bundled together with a serial or ISDN leased line, to provide dynamic Overflow on ISDN.

  n must be between 1 and 60, depending on your ISDN configuration.

```
MultiCom:Select Geneva
Site “Geneva” selected.
MultiCom:ISDN BChannel 10
Max number of B-channels for site “Geneva” set to 10.
```

Default value

1

NOTE - Of course, the number of physically available B-channels will prevail over the desired maximum number of B-channels, i.e. you cannot get more than 2 B-channels on a Pocket or Classic ***MultiCom***.

ISDN CALLBACK

14.18.48

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the D-channel callback. This type of callback allows cost-free callback. It is mainly used for convenience and by ISP clients who want dail-in as well as dial-out. See also §14.18.79, "PPP Callback" on page 217.

Type

```
Site-specific
```

Format

```
ISDN Callback [{On | Off | Expect}]
```

Parameters

- `none`

  Without parameter, this command displays the current configuration of this feature.

- `On`

  When a call comes for the currently selected site, the ***MultiCom*** will reject it and call back the predefined number corresponding to that site.

- `Off`

  Accept incoming calls. Do not call back. This does not prevent B-channel callback.

- `Expect`

  Wait for a callback when a call is rejected. This is recommended when the remote site is in callback mode.

Default value

`Off`

CAUTION — Unlike the B-channel callback, there is no authentication check for the identity of the caller. A malicious person could force you to open the line as much as it wants, without paying anything.
Also, do not mix D-channel callback with B-channel callback!

ISDN CONN

14.18.49

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command allows to manually open a B-channel. It is useful for ISDN troubleshooting.

Type
`Interactive`

Format
`ISDN Conn`

Parameters
- `none`

  Opens an ISDN connection for the selected site using the phone number that was set with `"ISDN RemoteNumber"` (see page 199).

  This command must be used to open a connection if `"ISDN Auto"` (see page 171) is `Off`.

```
MultiCom:Select Zurich
Site “Zurich” selected
MultiCom:ISDN Conn
Site “Zurich” connected
```

The connection will be automatically closed if there is no traffic on the link (see §14.18.53, "ISDN IdleCloseTime" on page 181).

Each further command will open an additional B-channel, which can be closed by a matching disconnection command. See §14.18.51, "ISDN Disc" on page 179 for manually closing a B-channel.

CAUTION — Care should be taken when an ISDN line is opened. If there is regular traffic over the line, the connection may remain open indefinitely, leading to large telephone bills.

ISDN DCHANNELPROTOCOL

14.18.50

V 2.2.9	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command specifies the protocol used on the ISDN D-channel. The type of D-channel protocol depends on the type of telephone exchange to which the ***Multi-Com*** is connected.

Type

`Global`

Format

```
ISDN DChannelProtocol {Info | {EuroISDN | Japan | USA |
VN3}
```

Parameters

- `Info`

  Displays the current protocol used on the D-channel.

- `EuroISDN`

  Selects the European protocol. It is currently available in most countries, including Asia and Africa.

- `Japan`

  Selects the INS-64 protocol. This is a modified version of EuroISDN which is mainly available in Japan.

- `USA`

  Selects the National ISDN 1 protocol used in the United States of America. In addition, you may need to specify your SPID using "`ISDN Interface`" (see page 186).

- `VN3`

  Selects the VN3 protocol. This is an old French standard, supported only for backward compatibility. Nowadays, only EuroISDN should be used in France.

Default value

`EuroISDN`

ISDN DISC

14.18.51

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command allows to manually close a B-channel. This is useful for ISDN troubleshooting.

Type

```
Interactive
```

Format

```
ISDN Disc
```

Parameters

- *none*

  Close one ISDN B-channel used by the selected site. The "`ISDN Auto`" (see page 171) command can be used to close all B-channels for the selected site.

  Each further command will close an additional B-channel. See §14.18.49, "ISDN Conn" on page 177 for manually opening a B-channel.

NOTE - `ISDN Disc` causes one B-channel to close but does not prevent it from re-opening automatically. `ISDN Auto Off` closes all open B-channels for the selected site and prevents them from re-opening.

ISDN ERRORRESETTIME

14.18.52

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command defines the delay after which a permanent error condition (such as repeated ISDN and authentication errors) is reset. It avoids rebooting the ***MultiCom*** to try again a bad connection.

Type

`Global`

Format

`ISDN ErrorResetTime [`*`minutes`*`]`

Parameters

- *`none`*

  Without parameter, this command displays the current configuration of this feature.

- `0`

  Specifies that the permanent error should not be cleared automatically. In that case, a manual intervention is needed to retry a connection. This is the same comportment as before version 2.4.

- *`minutes`*

  Specifies the time after which all errors are automatically cleared.

Default value

`60` minutes

ISDN IDLECLOSETIME

14.18.53

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Specifies the time after which an idle connection should be closed.

Type

`Site-specific`

Format

`ISDN IdleCloseTime [`*`seconds`*`]`

Parameters

- *none*

  Without parameter, this command displays the current amount of time after which an idle connection is closed.

- *seconds*

  Sets the time after which an **outgoing** connection with no traffic in on it is closed to *seconds*. This parameter should be set carefully depending on the initial connection cost, the cost of the communication and the type of transfers (bursty or bulky).

```
MultiCom:Select Zurich
Site “Zurich” selected
MultiCom:ISDN IdleCloseTime 20
Idle Close Time for site “Zurich” set to 20 seconds
```

Default value

```
60 (1 minute)
```

NOTE - The minimum value for `IdleCloseTime` is 10 seconds.

NOTE - Normally, this is the calling machine which decides when to end a call. But for safety reasons, we will also close an idle **incoming** call after 10 times the `IdleCloseTime`.

ISDN INFO

14.18.54

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

```
Interactive
```

Format

```
ISDN Info [{Enabled | History | Current}]
```

Parameters

- *none*

  Displays general ISDN informations.

```
MultiCom:ISDN Info
MyNumber             = 9
MySubAddress         = *** NONE ***
Total calls made     = 1
Total calls received = 0
Total failed calls   = 0
NbrConnected         = 1
NbrToCloseForICC     = 0
NbrToCloseForOther   = 0
```

- `History`

  Displays the log of all successful and unsuccessful ISDN connections. For successful connections, the duration and cost of the call is shown. For unsuccessful connections, the reason is shown instead. This can be very useful for troubleshooting.

```
MultiCom:ISDN Info History

Call history:
 Time ago  Kind Local number     <-> Remote number       Duration    Tax
-------------------------------------------------------------------------------
   00:02:15 Dat 1                ->| 91                **user busy**
   00:02:07 Dat 1                ->| 92                **call rejected**
```

```
00:00:12 Dat 1              ->| 93               **incompatible dest**
00:20:24 Dat 1              --> 94               00:00:39      0
00:00:04 Dat 1              ->| 0216542003       **no route to dest**
00:01:07 Dat 1              --> 00216542003          00:00:25   0.30
```

NOTE - This command also displays the ignored calls made to the same number but to a different MSN.

- `Enabled`

  Displays enabled ISDN numbers and their associated site.

```
MultiCom:ISDN Info Enabled
Number 'data/*' enabled for Site "Remote"
Number 'data/0216542003' enabled for Site "Lightning"
```

- `Current`

  Displays the current incoming and outgoing ISDN calls.

```
MultiCom:ISDN Info Current
Total free B channels: 29

Current calls:
Time ago  Kind Local number     <-> Remote number     B  D    Tax User
-------------------------------------------------------------------------------
00:00:11 Dat 0216542003         --> 94                1  0      0 Site "Lockeed"
```

The meaning of the connection indicator is as follows:

- `-->`

  Successful outgoing call

- `->|`

  Unsuccessful outgoing call

- `<--`

  Successful incoming call

- `|<-`

Unsuccessful incoming call

- ???

  Establishing/disconnecting (transient)

ISDN INTERFACE

14.18.55

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command defines low-level properties for each ISDN interface. If you don't understand what it does, don't use it!

Type

`Global`

Format

`ISDN Interface [Slot` *`i`*`] [D`*`j`*`] {Mode {DDI | MSN} | TEI` *`n`* `| SPID` *`spid`* `| Info}`

Parameters

- `ISDN Interface [Slot` *`i`*`] [D`*`j`*`] Mode {DDI | MSN}`

  Sets the mode of an ISDN connection to Point-to-Point Direct Dial-In (DDI) or Point-to-Multipoint Multiple Subscriber Number (MSN).

- `ISDN Interface [Slot` *`i`*`] [D`*`j`*`] TEI` *`n`*

  Sets the Terminal Endpoint Identifier (TEI) statically to *n* (between 0 and 63). Normally, it is dynamically assigned by the central switch, to something between 64 and 127. Some switches and PBX may require TEI=0.

- `ISDN Interface [Slot` *`i`*`] [D`*`j`*`] SPID` *`spid`*

  Specifies the Service Profile Identifier (SPID), provided by your carrier, for the "USA" D-channel protocol (see "ISDN DChannelProtocol" on page 178).

- `ISDN Interface [Slot` *`i`*`] [D`*`j`*`] Info`

  Returns information on all ISDN interfaces or a specific one.

Default value

```
DDI on PRI interfaces
MSN on BRI interfaces
Dynamic TEI
```

ISDN LEASED

14.18.56

V 2.2.6	IP	IPX	Bridge	M	V36	S	E
Pocket							
Classic							
LAC							

This commands attaches a Leased-ISDN (also called Semi-permanent) B-channel to the currently selected site.

Type
`Site-specific`

Format
`ISDN Leased [[Slot i] [Dj] Bk {On | Off}]`

Parameters

- *none*

  Displays the status of all leased B-channels

```
MultiCom:ISDN Leased
Leased B channels:

Channel    Status  User
---------------------------
B1             Ok    Site "Permanent"
```

- `[Slot i] [Dj] Bk On`

  This records the B-channel k of D-channel j of slot i as leased.

```
MultiCom:ISDN Leased B1 On
Added leased channel B1 for Site "Permanent"
```

- `[Slot i] [Dj] Bk Off`

  This records the B-channel k of D-channel j of slot i as dial-up.

```
MultiCom:ISDN Leased B1 Off
Removed leased channel B1 for Site "Dialup"
```

NOTE - The slot number and D-channel need to be specified only if you have multiple ISDN cards or multiple ISDN ports on one card.

NOTE - The backup of the leased B-channel works in exactly the same way as the serial leased-line. The command "`Backup On`" (see §14.18.4, "Backup" on page 110) instructs the ***Multi**Com* to open the other B-channel if the leased B-channel is not working.

NOTE - It is possible to add dial-up B-channels when there is heavy traffic. This is done in the same manner as with the serial leased-line. Use the command "ISDN Auto On" (see page 171). It is possible to use many B-channels as leased B-channels. They can be connected to the same site or different sites, as required. It is possible to use a serial leased and one (or both) leased B-channel on the same site, if needed. In other words, there is no limitation on the number of leased-lines that can be connected to a site. It is also possible to freely mix dial-up and leased connections.

Default value

```
All Off
```

ISDN MAXBACKOFF

14.18.57

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

The MaxTries parameter (see §14.18.58, "ISDN MaxTries" on page 191) is used to limit the number of times that a ***Multi**Com* attempts to contact a remote ***Multi**Com*, when the connection fails. The MaxBackoff parameter is used to control the duration between each successive attempt.

Type

```
Site-specific
```

Format

```
ISDN MaxBackoff [seconds]
```

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

- *seconds*

  Sets the MaxBackoff parameter for the current site.

Default value

```
86400 seconds (24 hours)
```

The ***Multi**Com* uses a backoff method if it experiences an error when connecting to a remote ***Multi**Com*. A backoff method consists of waiting a period of time before retrying. For each successive time that the connection fails, the time period is increased.

The ***Multi**Com* uses an initial time period of 3 seconds and doubles it for each successive failure. This gives the sequence 3, 6, 12, 24, 48… seconds. MaxBackoff limits the size to which the delay can grow. A MaxBackoff of 15 seconds would give the following sequence: 3, 6, 12, 15, 15, 15… seconds. The number of times

that the ***MultiCom*** will retry the connection is limited by the `MaxTries` parameter (see page 191).

NOTE - Once the ***MultiCom*** successfully connects to the remote ***MultiCom***, the backoff time period is reset to 3 seconds.

ISDN MAXTRIES

14.18.58

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

If the ***MultiCom*** experiences an error when it tries to connect to a remote ***MultiCom***, it will try again after a delay. This parameter limits the number of consecutive times that a ***MultiCom*** retries the connection.

Type

`Site-specific`

Format

`ISDN MaxTries [limit]`

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

- *limit*

  Sets the maximum number of retries to *limit*.

Default value

`20`

In some countries, the telephone companies charge the user for attempting to make a phone call, even if the attempt fails. This policy normally only applies to ISDN equipment. MaxTries limits the number of failed call attempts to help prevent excessive phone bills. In Switzerland, you only pay after the 10th failed attempt.

Some countries also set limits on the number of automatic attempts and the duration between these attempts.

ISDN MYNUMBER

14.18.59

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This commands sets the own ISDN number of your ***MultiCom***.

Type
`Global`

Format
`ISDN MyNumber [`*`msn`*`]`

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

- *msn*

  Set the ISDN phone number (see note below) of the local ***MultiCom***.

```
MultiCom:ISDN MyNumber 1
MyNumber set to 1
```

`MyNumber` is not defined by default. **In that configuration, the *MultiCom* will answer ALL incoming DATA calls on its S_0 bus.** This is useful for the initial configuration, but you will have to change this for proper operation, if you have other equipments on the same bus.

NOTE - The structure of an ISDN number is somewhat complicated. Please read the following description before setting the `MyNumber` parameter.

NUMBERS AND MSN

14.18.59.1

Some ISDN numbers contain a Multiple Subscriber Number (MSN). This is typically the last digit, or possibly the last several digits of the number.

For example, in Switzerland, the PTT allocates a block of five consecutive numbers for each ISDN line (e.g. 021712123**x**, where x is the MSN). This is for Swissnet 2 and 3. For Swissnet 3, the MSN is seven digits long. In France, the MSN is four digits long and in Germany seven.

NOTE - Please check the MSN length with your Telecom operator.

The MSN can be assigned by the user. It is typically used to distinguish between different devices on the same ISDN line. For example, the FAX could be assigned the number 0217121123**1**, the telephone the number 0217121123**2** and the ***MultiCom*** the number 0217121123**3**. In this way, it is possible to ring the FAX while not ringing the ***MultiCom***, even though they are on the same ISDN line.

To put it in another way, the MSN behaves like the extension number for a device.

It is possible that a number has no MSN. This is a detail that is typically discussed when the ISDN line is ordered from the PTT.

NOTE - If you are connected to a PABX, the MSN could be from one to four digits long. Some PABX translate the destination number of incoming calls. Please ask your telecom specialist about your PABX configuration.

NUMBERS AND THE MULTICOM 14.18.59.2

On the ***MultiCom***, the MyNumber parameter should be set to the MSN. If there is no MSN then the MyNumber should be left empty.

The ***MultiCom*** uses the MyNumber in two situations:

1. When making an outgoing call, the ***MultiCom*** transmits the MyNumber parameter to the telephone exchange. This enables the telephone exchange to identify the caller.

   In some cases it is possible to send the entire telephone number of the ***MultiCom*** to the telephone exchange. It will figure out for itself which part of it corresponds to the MSN. If this is the case, MyNumber can be set to the entire telephone number. Otherwise, only the MSN should be used.

2. When there is an incoming call, the telephone exchange transmits the MSN to all devices on the ISDN line. The ***MultiCom*** will answer the incoming call if the MSN corresponds to its MyNumber. The ***MultiCom*** will also answer the call if the MyNumber is empty.

   To be more precise, the ***MultiCom*** compares the MSN with the end of its MyNumber. If the MSN is one digit long, the ***MultiCom*** will compare it with the last digit of MyNumber. If the MSN is two digits long, it will be compared with the last two digits of MyNumber and so on. Thus, if the MyNumber is set to the complete telephone number, instead of just the MSN, the ***MultiCom*** will still answer the call correctly.

NOTE - On some PABX, data calls are blocked by default. You may need to reconfigure your PABX to use an ISDN connection in data mode.

ISDN MYSUBADDRESS

14.18.60

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command defines the ISDN subaddress.

Type

`Global`

Format

`ISDN MySubaddress [[<NSAP>]`*`string`*`]`

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

- `[<NSAP>]`*`string`*

  This commands sets the ISDN subaddress of the ***MultiCom***. A subaddress is a string that can be used in addition to the phone number to address an ISDN terminal more precisely. It is typically used when several ISDN devices share the same phone number. The ***MultiCom*** can accept sub-addresses of up to 20 characters, but many telephone exchanges restrict the subaddress to a shorter length.

  The use of this command is optional.

```
MultiCom:ISDN MySubaddress FooBar
MySubaddress set to 1:FooBar
```

NOTE - The subaddress is “User-defined” by default. Prefixing it with `<NSAP>` sets the subaddress to the “NSAP” type.

ISDN NEVERBUSY

14.18.61

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the Never Busy Line feature.

Type

`Site-specific`

Format

`ISDN NeverBusy [{On | Off}]`

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

- `On`

  Allows the current site to be temporarily disconnected to make space for an incoming call.

- `Off`

  Forbids to disconnect the current site when all B-channels are busy, to allow an incoming call. This must be used for stupid Terminal Adapters which don't know how to reconnect automatically when disconnected. It may also be used to guarantee access to privileged users over standard users or to reduce the costs associated with each call setup, if you don't need this feature.

Default value

`On`

ISDN NUMBERENABLED

14.18.62

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is used to specify which remote machines are authorized to call this ***MultiCom***.

Type

```
Site-specific
```

Format

```
ISDN NumberEnabled {[<UNSURE>]number | *}
```

Parameters

- *number*

  Sets the authorized remote number for the currently selected site to *number*.

  When the ***MultiCom*** is called, the telephone exchange indicates the phone number of the calling device. The ***MultiCom*** uses this information to decide whether or not it is willing to accept the call.

  On a Multi-point ***MultiCom***, this command has a second function: it is used to associate incoming calls with the correct site.

```
MultiCom:Select Bern
Site “Bern” selected.
MultiCom:ISDN NumberEnabled 0187654338
ISDN Number '0187654338' enabled for Site 'BERN'
```

NOTE - If you wish to authorize connections from more than one ISDN number, simply define multiple `NumberEnabled` on different lines.

- <UNSURE>*number*

  Under certain circumstances, the telephone exchange may consider that the authenticity of the caller’s number is unsure. This usually happens if the calling ***MultiCom*** is connected to a private PABX. In this case, the telephone exchange informs the called ***MultiCom*** that the caller’s number is “*insecure*”.

The ***MultiCom*** will only accept unsure calls if it has been explicitly configured to do so. This is done as follows:

```
MultiCom:ISDN numberEnabled <UNSURE>0223458796
ISDN Number '<UNSURE>0223458796' enabled for Site 'GENEVA'
```

- *

  This allows all ISDN numbers to initiate a connection to the currently selected site.

```
MultiCom:ISDN NumberEnabled *
ISDN Number '*' enabled for Site 'BERN'
```

CAUTION - Currently, you must not use this command on more than one site!

Default value

The default configuration permits all incoming calls, to allow remote installation and troubleshooting.

NOTE - The command `ISDN Info Enabled` (see “ISDN Info” on page 183) displays the list of currently enabled numbers.

ISDN REMOTENUMBER

14.18.63

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This commands sets the phone number of a remote site.

Type

Site-specific

Format

ISDN RemoteNumber [*number*]

Parameters

- *none*

  Without parameter, this command unsets the current remote number, thus disabling outgoing calls.

```
MultiCom:ISDN RemoteNumber
Remote number set to "*** NONE ***" for site "Lockeed"
```

- *number*

  The remote ISDN *number* is the phone number that will be used to call the remote ***MultiCom*** that corresponds to the selected site.

```
MultiCom:Select Lightning
Site “Lightning” selected.
MultiCom:ISDN RemoteNumber 0216542003
Remote number set to "0216542003" for site "Lightning"
```

Default value

The remote ISDN number is not defined by default. You have to set it for proper operation.

NOTE - If you are connected to an internal PBX, you may have to add an extra access code to reach the public ISDN network (this is typically ‘0’).

ISDN REMOTESUBADDRESS

14.18.64

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Sets the remote subaddress.

Type

`Site-specific`

Format

`ISDN RemoteSubaddress [[<NSAP>]`*`string`*`]`

Parameters

- *none*

  Without parameter, this command unsets the current remote subaddress.

- `[<NSAP>]`*`string`*

  The remote ISDN subaddress will be used when calling a remote ***MultiCom***. It will be passed to the telephone exchange at the same time as the remote ISDN number. It should only be used if the remote ***MultiCom*** has been programmed to have a subaddress (see §14.18.60, "ISDN MySubaddress" on page 195).

```
MultiCom:Select Zurich
Site “Zurich” selected.
MultiCom:ISDN RemoteSubaddress FooBar
RemoteSubaddress set to “FooBar” for Site “Zurich”
```

NOTE - The subaddress is “User-defined” by default. Prefixing it with `<NSAP>` sets the subaddress to the “NSAP” type.

KEY CREATE

14.18.65

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

In order to use the encryption, you need to create encryption keys first.

Type

`Global`

Format

`Key Create` *`key_id`* `[IDEA [128] [Rounds` *`n`*`]| DES [{40 | 56}] | 3DES [112]]` *`secret`*

Parameters

- *`key_id`*

  Each key is associated with a key id. A key id has a maximum of 8 characters. It is used to manipulate keys without seeing them.

- *`secret`*

  The key itself has a minimum of 6 (DES), 13 (IDEA) or 18 (3DES) characters, and a maximum of 7 (DES 40), 10 (DES 56), 19 (3DES 112) or 21 (IDEA) characters, including a to z, A to Z, 0 to 9, '-' (minus) and '_' (underscore).

- `IDEA [128] [Rounds` *`n`*`]`

  Selects the International Data Exchange Algorithm from Ascom Systec to encrypt data using this key. This is a well-known and proven algorithm used for high-security applications. It is still unbroken yet and quite fast to compute. This is currently the only algorithm available for link encryption. By default, it uses the standard 8 rounds algorithm, although you can choose fewer rounds for faster but WEAKER encryption.

- `DES [{40 | 56}]`

  Selects the Data Encryption Standard from the U.S. government. This is a standard algorithm which has been broken recently by brute-force attacks in 22 hours, but is still widely used. Currently, it can only be used for IP-level encryption.

- `3DES [112]`

  Selects the Triple DES algorithm, which is a much better version of DES, still unbroken. Currently, it can only be used for IP-level encryption.

```
MultiCom:Key Create Unsure DES 40 not_very_safe
Selected : DES 40 bit key.
Encryption Key "Unsure" registered.
MultiCom:Key Create Secure this_is_very_safe
Encryption Key “Secure” registered.
MultiCom:Key Create Weak 3DES aaaaaaaaaaaaaaaaaaaaaaaa
Selected : DES 112 bit key.

WARNING : This key or one part of the Triple-DES key
          is a DES weak key. For security reasons, you
          should change this key..

Encryption Key "Weak" registered.
```

NOTE - A warning will be issued when trying to create so-called “weak” keys, which are less secure than normal keys. You should never use these keys!

Default value

IDEA algorithm
128 bits for IDEA
56 bits for DES
112 bits for 3DES

KEY INFO

14.18.66

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Displays the list of defined keys.

Type

`Interactive`

Format

`Key Info`

Parameters

- *none*

  Lists all currently defined keys, the algorithm and key size which will be used, the fingerprint of the secret part, and whether they are saved in Flash memory or not.

```
MultiCom:Key Info

Name       Algorithm   Key Size     Checksum   Saved
-----------------------------------------------------
Unsure     DES          40 bits     606D       No
Weak       3DES        112 bits     2E76       No
Secure     IDEA        128 bits     88C8       Yes
```

KEY REMOVE

14.18.67

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is used to erase a key.

Type

`Global`

Format

`Key Remove` *`key_id`*

Parameters

- *`key_id`*

  Deletes the key whose name is key_id.

```
MultiCom:Key Remove my_key
Encryption Key “my_key” removed.
```

KEY SAVE

14.18.68

V 2.2.6	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command saves a precedently created key into Flash memory, where it will persist across reboots.

Type
`Global`

Format
`Key Save` *`key_id`*

Parameters
- *`key_id`*

  Store in Flash memory the key whose name is key_id. This key can then be used like a standard key, but its secret can not be recovered in any way, for security reasons.

```
MultiCom:Key Save my_key
Key “my_key” saved in Flash-EPROM.
```

Ls

14.18.69

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Lists the contents of a directory.

Type

`Interactive`

Format

```
Ls [{#ROM: | #RAM:}]
```

Parameters

- `None`

  Lists the current directory.

- `#RAM:`

  Lists the content of the read/write memory partition.

```
MultiCom:ls #RAM:
CONFIG
BOOT.RPT
```

- `#ROM:`

  Lists the content of the read-only memory partition.

```
MultiCom:ls #ROM:
CONFIG
```

MEM

14.18.70

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Gives memory statistics.

Type
`Interactive`

Format
`Mem Info`

Parameters
- `Info`

  Displays the amount of free memory.

```
MultiCom:Mem Info
Total free: 1054K
```

MHDLC ENCODING

14.18.71

V 2.1.3	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Selects the binary encoding type on a MHDLC link.

Type

Site-specific

Format

MHDLC Encoding {NRZ | NRZI}

Parameters

- Encoding NRZ

  Selects the “Non Return to Zero” encoding scheme for the currently selected site. This is needed if you want to connect to a ***MultiCom LAN Access Center***, a ***MultiCom Serial IV***, a ***MultiCom Access IV*** or a ***MultiCom Backup IV***.

```
MultiCom:MHDLC Encoding NRZ
Encoding set to ‘NRZ’ for site “ISDN”.
```

- Encoding NRZI

  Selects the “Non Return to Zero Inverted” encoding scheme for the currently selected site. This is the default for the ***Classic MultiCom*** and the ***Pocket MultiCom***. It must be used to ensure backward compatibility.

```
MultiCom:MHDLC Encoding NRZI
Encoding set to ‘NRZI’ for site “ISDN”.
```

Default value

NRZI on the ***Classic MultiCom*** and the ***Pocket MultiCom***
NRZ on newer models

NOTE - This does not affect PPP connections, which use NRZ.

MHDLC ENCRYPTION

14.18.72

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Controls the MHDLC link encryption. See also §14.18.82, "PPP Encryption" on page 222.

Type

Site-specific

Format

```
MHDLC Encryption [{On | Off}]
```

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

```
MultiCom:MHDLC Encryption
Data encryption is enabled for site "Secure".
```

- Off

  Disables the MHDLC encryption for the selected WAN site.

```
MultiCom:MHDLC Encryption Off
Data encryption disabled for site "Unsecure".
```

- On

  Enables the MHDLC encryption for the selected WAN site. Before enabling the encryption, a key must have been created and assigned to this site. See §14.18.65, "Key Create" on page 201 and §14.18.73, "MHDLC Encryption-KeyId" on page 211).

```
MultiCom:MHDLC Encryption On
Data encryption enabled for site "Secure".
```

Default value

`Off`

MHDLC ENCRYPTIONKEYID

14.18.73

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Assigns an encryption key to an MHDLC link.

Type

`Site-specific`

Format

`MHDLC EncryptionKeyId` *`key_id`*

Parameters

- *`key_id`*

  Sets the encryption key, using the associated key id, for the current site.

  Before this, you must create a key (see §14.18.65, "Key Create" on page 201) and afterwards, you must enable the encryption (see §14.18.72, "MHDLC Encryption" on page 209).

```
MultiCom:MHDLC EncryptionKeyId my_key
Encryption Key ID set to "my_key".
```

MHDLC MODE

14.18.74

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Changes the link mode of an MHDLC connection.

Type

`Site-specific`

Format

`MHDLC Mode {v1 | v2 | v3}`

Parameters

- `Mode {v1 | Transparent}`

  Sets the MHDLC mode to “Transparent”. This can be used for backward compatibility with very old firmware, but should be avoided.

```
MultiCom:MHDLC Mode Transparent
Mode set to ‘transparent’ for site site_name
```

- `Mode {v2 | ConnectionControl}`

  Sets the MHDLC mode to “Connection Control”. This is specially designed for ISDN connections.

```
MultiCom:MHDLC Mode ConnectionControl
Mode set to ‘connection-control’ for site site_name
```

- `Mode {v3 | Polling}`

  Sets the MHDLC mode to “Polling”. This is best for leased-lines.

```
MultiCom:MHDLC Mode Polling
Mode set to ‘polling’ for site site_name
```

Default value

`v2` for ISDN links
`v3` for Serial links

MHDLC MODIFYIPFORMAT

14.18.75

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Changes the IP format of an MHDLC connection.

Type

`Site-specific`

Format

`MHDLC ModifyIPFormat {Routed | Bridged}`

Parameters

- `ModifyIPFormat {Routed | Bridged}`

  Specifies if the IP traffic on the WAN connections is routed or bridged.

  Routed is the most efficient method, as it sends the frames without Ethernet headers. *Bridged* sends the frames with Ethernet headers. However, Routed can only be used if both ***MultiCom*** have the IP Router software option. The current WAN protocol format can be seen with the command “Site Info” on page 264.

Default value

`Routed`

MHDLC PADDING

14.18.76

V 2.2.6	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Change the padding mode of an MHDLC connection.

Type

`Site-specific`

Format

`MHDLC Padding {On | Off}`

Parameters

- `Padding On`

  Sets the MHDLC padding to an even number of bytes. This solves a rare but annoying bug.

```
MultiCom:MHDLC Padding On
Padding set to ‘On’ for site “ISDN”.
```

- `Padding Off`

  Resets the MHDLC padding. This is provided for backward compatibility.

```
MultiCom:MHDLC Padding Off
Padding set to ‘Off’ for site “ISDN”.
```

Default value

`On`

MYNAME

14.18.77

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Changes the name of your ***MultiCom***.

Type
`Global`

Format
`MyName [`*`name`*`]`

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

- *name*

  This command redefines the name of the ***MultiCom***. The name will be displayed as a prompt when you log in, for informational purpose only.

```
MultiCom:MyName Test
Test:
```

Default value
`MultiCom`

PING

14.18.78

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Check the reachability and liveliness of a remote host by using ICMP. This is very useful for IP routing troubleshooting.

Type

`Interactive`

Format

`Ping` *`host`*

Parameters

- *`host`*

  The name (if DNS is correctly configured) or the IP address of a remote machine you want to check for liveliness.

```
MultiCom:ping www.lightning.ch
Ping: “www.lightning.ch” (193.5.2.161) is alive !
MultiCom:ping 1.2.3.4
Ping: no answer from 1.2.3.4
```

PPP CALLBACK

14.18.79

V 2.2.6	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the B-channel callback. This type of callback allows authentication of the remote caller before calling back. It is mainly used for security.

Type

```
Site-specific
```

Format

```
PPP Callback [{Reject | Require [WithNumber [number]]|
Accept | Force}]
```

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

```
MultiCom:PPP Callback
Callback is in REJECT mode
```

- `Accept`

  Accepts to call back, if required by the peer.

- `Force`

  Always call back, even if not required. This is useful for security reasons.

- `Require`

  Ask peer to call back to the usual `RemoteNumber` for that site. This is useful for simpler cost control and billing, but see §14.18.48, "ISDN Callback" on page 175 for a better way to do that.

- `Require WithNumber`

  Ask peer to call back to the local `MyNumber`.

- `Require WithNumber` *number*

  Ask peer to call back to the provided number. This is useful when travelling.

- `Reject`

  Refuses to call back.

Default value
`Reject`

PPP COMPRESSION

14.18.80

V 2.2.6	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the standard Stac LZS® compression from Hi/Fn™.

Type
`Site-specific`

Format
`PPP Compression [{On | Off | Stats}]`

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

```
MultiCom:PPP Compression
PPP Compression is enabled for site "ISDN".
```

  This does not mean that it **is** using compression now, just that it **may** use compression, if the remote site supports it. If you want to know the **current** state, check the CCP status with §14.18.83, "PPP Info" on page 224.

- `On`

  This enables the negotiation of the compression option with CCP. If the remote site does not use the same compression, the ***MultiCom*** will fall back to normal uncompressed transmission.

- `Off`

  This is for the rare cases where the compression is not desired or incorrectly implemented on the remote site. If such a case occurred to you, please inform us.

- `Stats`

  Gives detailed statistics about the compression on the current link.

```
MultiCom:PPP Compression Stats

Compression statistics
----------------------
Frames sent compressed       : 177
Frames sent uncompressed     : 0
Frames received compressed   : 172
Frames received uncompressed : 0
Frames discarded             : 0
Bytes sent                   : 3926 / 7530
Average compression ratio    : 1.91
Bytes received               : 4172 / 7814
Average compression ratio    : 1.87
CCP Renegotiations           : 0
CCP Resets                   : 0
```

Default value

On

PPP ECHOREQUEST

14.18.81

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls low-level LCP options. Do not use it, unless advised to by technical people.

Type
`Site-specific`

Format
`PPP EchoRequest [{On | Off}]`

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

- `On`

  Allows the ***MultiCom*** to send “Echo-Request” frames to check the liveliness of a PPP connection. This is desirable, but may cause problems with brain-dead implementations of PPP which consider this as traffic and therefore never close the line.

- `Off`

  Forbids the ***MultiCom*** to send “Echo-Request” frames.

Default value
`On`

NOTE - This command can be used only if the selected site is a PPP one. See §14.18.116, "Site Create" on page 262 for details on how to create a PPP site.

PPP ENCRYPTION

14.18.82

V 2.2.9	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Configures the PPP link encryption.

Type

`Site-specific`

Format

`PPP Encryption [{On | Off | Key` *`key_id`* `| Session [{On | Off | MaxDuration` *`hours`* `| MaxTraffic` *`gigabytes`*`}]}]`

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

```
MultiCom:PPP Encryption
Encryption is enabled for site "ISDN".
```

- `{On | Off}`

  This enables or disables the negotiation of the encryption using ECP. Unlike CCP, if the remote side refuses to use the same algorithm, the ***MultiCom*** **will NOT fall back to normal plain transmission**, for security reasons.

- `Key` *`key_id`*

  Sets the MasterKey to use on that link. This will automatically enable the encryption and select the encryption algorithm depending on the provided key. Currently, only the IDEA algorithm is available for link encryption.

- `Session {On | Off}`

  This enables or disables the negotiation of sessions keys on that link. When disabled, the MasterKey will be directly used to encrypt data. When enabled, each new connection will negotiate a new random SessionKey to encrypt data, so that the MasterKey is not exposed.

- `Session MaxDuration` *`hours`*

  Sets the maximum time a SessionKey is valid. After that time has expired, a new random SessionKey will be negotiated with the remote peer. By default, this is `0` (unlimited time).

- `Session MaxTraffic` *`gigabytes`*

  Sets the maximum amount of data that a SessionKey will encrypt. After that amount is reached, a new random SessionKey will be negotiated with the remote peer. By default, this is `0` (unlimited amount).

PPP INFO

14.18.83

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Displays useful PPP information.

Type

```
Interactive
```

Format

```
PPP Info [{LCP [Options] | PAP | CHAP | All}]
```

Parameters

- *none*

  Displays the PPP configuration and negotiation results in a synthetic format.

```
MultiCom:PPP Info

PPP information on site "Lockeed"

Authentication  Protocol  UserID           Password
Local           CHAP      test             light
Remote          Either    test             light

PPP Callback    Reject
Compression     On
Encryption      Off
Multilink       On

Protocol  Status    Message
------------------------------------------------------------
IPCP      On
IPXCP     Off
BCP       Off
CCP       On
ECP       Off
MP        Off

Local rejected protocols : 8031 (BCP)
Remote rejected protocols :
```

- `LCP`

  Displays the statistics on received or sent packets, for the Link Control Protocol.

- `LCP Option`

  Displays the negotiated Link Control Protocol options that have been accepted, refused and rejected by the remote peer (Local options) and the remote peer's options accepted, refused and rejected by the ***Multi**Com* (Remote options).

- `PAP`

  Displays the statistics on received or sent packets, for the Password Authentication Protocol.

- `CHAP`

  Displays the statistics on received or sent packets, for the Challenge Handshake Authentication Protocol.

- `All`

  Displays all statistics informations on PPP data traffic, LCP, PAP, CHAP, and the selected NCPs (IPCP, BCP, and IPXCP). It's not recommended to use this command due to the amount of information displayed.

PPP LOCAL AUTHENTICATION

14.18.84

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

Site-specific

Format

```
PPP [Local] Authentication {None | PAP | CHAP}
```

Parameters

- None

  Do not ask the remote peer to authenticate itself.

- PAP

  Sets the authentication protocol that will be asked by the ***MultiCom*** to the remote peer to PAP.

```
MultiCom:PPP Authentication PAP
PPP Authentication protocol: PAP
```

- CHAP

  Sets the authentication protocol that will be asked by the ***MultiCom*** to the remote peer to CHAP.

```
MultiCom:PPP Local Authentication CHAP
PPP Authentication protocol: CHAP
```

Default value

None

NOTE - This command can be used only if the selected site is a PPP one. See §14.18.116, "Site Create" on page 262 for details on how to create a PPP site.

PPP MULTILINK

14.18.85

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the negotiation of the Multilink PPP (MP) option.

Type

```
Site-specific
```

Format

```
PPP Multilink [{On | Off}]
```

Parameters

- *none*

  Without parameter, this command displays the current setting of this feature.

- `On`

  Allows the ***MultiCom*** to negotiate this option. It will only be used if the remote party accepts it. A second link will only be used if allowed by the command “ISDN BChannel” on page 173 and there is enough traffic. Some ISPs will only provide one link, even when MP was successfully negotiated and authorized by `ISDN BChannel 2`.

- `Off`

  Forbids the ***MultiCom*** to ask for and accept this option. This can solve compatibility problems with some manufacturers which do not use MP correctly.

Default value

```
On
```

NOTE - This command can be used only if the selected site is a PPP one. See §14.18.116, "Site Create" on page 262 for details on how to create a PPP site.

PPP PASSWORD

14.18.86

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Sets the local or remote password for PPP authentication.

Type

`Site-specific`

Format

`PPP Authentication {Local | Remote} Password` *`password`*

Parameters

- `Authentication Local Password` *`password`*

  Sets the local password for authentication to *`password`*

```
MultiCom:PPP Authentication Local Password MANAGER
Local Password registered
```

- `Authentication Remote Password` *`password`*

  Sets the remote password for authentication to *`password`*

```
MultiCom:PPP Authentication Remote Password TEST_PASSWORD
Remote Password registered
```

NOTE - This command can be used only if the selected site is a PPP one. See §14.18.116, "Site Create" on page 262 and §14.18.118, "Site Modify" on page 266 for details on how to create a PPP site.

NOTE - When the '#' or ' ' characters appears in a password, they must be escaped, as well as the '\' character, by a '\', i.e. "PPP Authentication Local Password 1#2 3\4" should be "PPP Authentication Local Password 1\#2\ 3\\4".

PPP REMOTE AUTHENTICATION

14.18.87

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Sets the authentication protocol that the ***Multi**Com* will accept from the remote peer.

Type

`Site-specific`

Format

`PPP Remote Authentication {None | PAP | CHAP | Either}`

Parameters

- `None`

  No authentication protocol is accepted from the remote peer.

NOTE - This is the lowest security level. Some PPP products will consider this as a security hole and refuse the connection.

- `PAP`

  Sets the authentication protocol that the ***Multi**Com* should accept from the remote peer to PAP.

```
MultiCom:PPP Remote Authentication PAP
PAP Authentication requests will be accepted for site “ascend”.
```

- `CHAP`

  Sets the authentication protocol that the ***Multi**Com* should accept from the remote peer to CHAP.

- `Either`

  Sets the authentication protocol that the ***Multi**Com* should accept from the remote peer to CHAP or PAP. In this case, both will be accepted.

```
MultiCom:PPP Remote Authentication Either
Both PAP and CHAP Authentication requests will be accepted for
site “Internet”.
```

Default value

```
Either
```

NOTE - This command can be used only if the selected site is a PPP one. See §14.18.116, "Site Create" on page 262 for details on how to create a PPP site.

PPP STATS

14.18.88

V 2.3	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Display PPP statistics.

Type

`Interactive`

Format

```
PPP [{IPCP|IPXCP|BCP|CCP|ECP|Compression|Encryption}]
Stats
```

Parameters

- `none`

  Display general PPP statistics.

- `IPCP`

  Displays IP negotiation statistics.

- `IPXCP`

  Displays IP negotiation statistics.

- `BCP`

  Displays Bridge negotiation statistics.

- `CCP`

  Displays Compression negotiation statistics.

- `ECP`

  Displays Encryption negotiation statistics.

- `Compression`

  Displays Compression statistics.

- `Encryption`

  Displays Encryption statistics.

PPP USERID

14.18.89

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Sets the local or remote user id for PPP authentication.

Type

`Site-specific`

Format

`PPP Authentication {Local | Remote} UserID` *`userid`*

Parameters

- `Authentication Local UserID` *`userid`*

  Sets the local user id for authentication to *`userid`*

```
MultiCom:PPP Authentication Local UserID LIGHTNING
Local UserId registered
```

- `Authentication Remote UserID` *`userid`*

  Sets the remote user id for authentication to *`userid`*

```
MultiCom:PPP Authentication Remote UserID TEST
Remote UserId registered
```

NOTE - This command can be used only if the selected site is a PPP one. See §14.18.116, "Site Create" on page 262 for details on how to create a PPP site.

PWD

14.18.90

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Displays the current path.

Type

Interactive

Format

Pwd

```
MultiCom:Cd #ROM
#ROM: is the new directory
MultiCom:Pwd
#ROM:
MultiCom:Cd #RAM
#RAM: is the new directory
MultiCom:Pwd
#RAM:
```

QUIT

14.18.91

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Leaves an interactive Telnet or Console session.

Type

```
Interactive
```

Format

```
Quit
```

This closes an active management session. You will need to identify yourself again to gain access to the ***MultiCom***. It is recommended, for security reasons, to use it if you leave your computer or terminal unattended.

NOTE - All parameters of the ***MultiCom*** remain unchanged until the next session.

READCONFIG

14.18.92

This command is obsolete and has been removed for security reasons.

REBOOT

14.18.93

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Interactive`

Format

`Reboot`

Force the system to reboot to the configuration saved into Flash memory with the "`WriteConfig`" command.

NOTE - See your User's Manual for information on how to reset to the default configuration file.

CAUTION — Rebooting the system interrupts all data flow through the ***Multi****Com* and discards all interactive modifications to the configuration. Inform users before doing this.

RENAME

14.18.94

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Interactive`

Format

`Rename` *`source destination`*

Parameters

- *`source destination`*

  Renames the file named *`source`* to *`destination`*.

```
MultiCom:ls
CONFIG
FOO
MultiCom:rename foo bar
#RAM:FOO -> #RAM:BAR file renamed
MultiCom:ls
CONFIG
BAR
```

RIP

14.18.95

V 2.6.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the limited RIP broadcaster.

Type

```
Global
```

Format

```
RIP netaddr Netmask mask Metric metric {Add | Remove}
RIP Broadcast {On | Off | ISDN}
RIP Info
```

A send-only RIP broadcaster is supported. It can send out RIP-2 frames according to the format defined in RFC 1723. The routing information that is broadcasted is defined by this command, and has nothing to do with the actual IP router configuration.

CAUTION — Even though the frames are in RIP-2 format, they are sent as broadcast according to the RIP-1 protocol (RFC 1058), instead of being sent as multicast. This may not work with all RIP-2 implementations. Incoming RIP-2 frames are ignored, except for RIP-2 requests that are processed according to the RFC. RIP-2 authentication and next hop fields are not supported.

Parameters

- `netaddr Netmask mask Metric metric {Add | Remove}`

  This command adds or removes an entry in the RIP broadcast table. *netaddr* and *mask* are in the standard IP address format; metric is an integer between 0 and 15 (included).

  The *netaddr* must contain all zeros bits in the host part, according to the specified *mask*. An attempt to enter the same *netaddr*/*mask* pair twice is rejected.

  The broadcast table is limited to 25 entries.

- `Broadcast {On | Off | ISDN}`

  This command turns the RIP broadcaster on or off.
  If the value is `ISDN`, the broadcaster is active when at least one ISDN interface is working. Broadcasts stop when all ISDN interfaces are out of order. There is no support for sending triggered updates, or infinity metrics, when the ISDN interfaces go down; thus the behavior in this case is the same as if the router had been completely disconnected from the LAN. Serial interfaces are not taken into account at all.

- `Info`

  This command displays the content of the broadcast table.

Default value

```
Broadcast Off
```

RM

14.18.96

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Interactive`

Format

`Rm` *`filename`*

Parameters

- *`filename`*

  Removes the file *`filename`* from disk. Note that only files stored on the #RAM disk can be deleted.

```
MultiCom:Rm foobar
#RAM:FOOBAR file deleted
```

SECURITY

14.18.97

V 2.2.9	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is used to lock/unlock the ***Multi**Com* into high-security mode.

Type

`Interactive`

Format

`Security {Info | {Lock | Unlock} [`*`password`*`]}`

Parameters

- `Info`

  Displays the current security mode: either “transparent”, which allows all commands to be used, or “locked”, which forbids to modify users and keys.

```
MultiCom:Security Info

Mode transparent.
```

- `Lock [`*`password`*`]`

  Locks the ***Multi**Com* in high-security mode where users and keys can only be listed, not modified. This allows a Security Manager to configure secret keys and management users, which cannot be modified or read back by a Network Manager.

```
MultiCom:Security Lock verysecret

Mode high security locked.
```

- `Unlock [`*`password`*`]`

  Unlocks temporarily the ***Multi**Com* in transparent, low-security mode where all commands can be used. After reboot, the ***Multi**Com* will be in high-security mode again.

```
MultiCom:Security Unlock verysecret

Mode high security unlocked.
```

NOTE - To unlock it permanently, you have to lock it with a null password.

```
MultiCom:Security Lock

password:<return>

WARNING: A null password set the transparent mode.

password confirm:<return>

WARNING: Transparent mode is set.
```

CAUTION — Rebooting in default configuration puts you in transparent mode. This allows to recover from a lost password situation, but for security reasons, if any user or key is saved while in this mode, ALL stored users and keys are deleted and the transparent mode is set.

SERIAL

14.18.98

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is used to configure the serial port(s). It takes a number of options, each of which is detailed further.

NOTE - On the ***MultiCom LAN Access Center***, ***MultiCom Serial IV***, ***MultiCom Backup IV*** and ***MultiCom Access IV***, the `Serial` command takes an additional parameter, to specify which serial port to consider (1 or 2).

SERIAL ALARM

14.18.99

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

The ***Multi**Com* is capable of detecting when the serial line is not working correctly and switches to ISDN backup if configured so.

Type

```
Global
```

Format

```
Serial [{1 | 2}] Alarm {All | CD | DSR | Clocks | Flags}
{On | Off}
```

Parameters

- `Alarm All {On | Off}`

  Off: disables the detection of errors on the serial line.
  On: enables the detection of errors on all appropriate events.

- `Alarm CD {On | Off}`

  Turn Carrier Detect alarm on or off.

  CD (carrier detect 109): When this signal is active, it indicates that the modem has detected that there is a carrier on the leased-line. If CD is inactive, this indicates that either the leased-line has been disconnected or the modem on the other end of the line is not switched on.

- `Alarm DSR {On | Off}`

  Turn DSR alarm on or off.

  DSR (data set ready 107): This signal should be activated by the Modem when it is switched on.

- `Alarm Clocks {On | Off}`

  Turn Clocks alarm on or off.

  Under normal circumstances, the serial port will be configured so that it takes its clock(s) from the modem. If is possible to monitor the clock(s). If it (they) are absent then the ***Multi**Com* considers the serial line to be down.

- `Alarm Flags {On | Off}`

  Turn Flags alarm on or off.

  By default, the ***MultiCom*** transmits flags on the serial line when it is idle. The absence of these flags indicates either that data is not transiting the serial line correctly, or that the transmission of flags was disabled on the other ***MultiCom***.

Default value
`All On`

The ***MultiCom*** is capable of detecting when the serial line is not working correctly. If it detects that the serial line is down (not working) and the ***MultiCom*** is configured to do serial line backup (see §14.18.4, "Backup" on page 110), the ISDN line will be used to replace the serial line, as long as the erroneous condition remains

The ***MultiCom*** monitors certain events to decide if the serial line is up or down. The command `Serial Alarm` can be used to configure which events should be monitored. The command `Serial Mode` (page 252) will set the default values. In most cases it should not be necessary to change the alarm settings.

Switching an alarm event off tells the ***MultiCom*** to ignore the event. Switching the alarm event on tells the ***MultiCom*** that it should monitor the event *if it exists*. It may not be possible to monitor certain events. For example, if the serial port is configured as X.21, then the signal DSR does not exist, thus it makes no sense to monitor it.

THE DTR SIGNAL 14.18.99.1

NOTE - The ***MultiCom*** conforms to the V.36 standard, which does not require the use of the DTR signal. With some V.35 modems, it may be necessary to configure the modem to ignore DTR.

SERIAL AUTORTS

14.18.100

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Global`

Format

`Serial [{1 | 2}] AutoRTS {On | Off}`

Parameters

- `AutoRTS On`

  Turns autoRTS on. When on, the ***MultiCom*** activates RTS (signal 105) every time that it needs to transmit something. It will only transmit when the modem replies by activating the CTS (signal 106).

- `AutoRTS Off`

  Turns autoRTS off. When off, the RTS signal takes the value specified by the `Serial RTS` (page 257) command. The CTS signal from the modem is ignored.

Default value

`Off`

NOTE - When autoRTS is on and flags are on, the ***MultiCom*** will activate the RTS signal permanently, since it always has something to transmit.

SERIAL BRG

14.18.101

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Chooses the source for the Baud-Rate-Generator (BRG) driving the data streams clocks.

Type
`Global`

Format
`Serial [{1 | 2}] BRG {Internal | External}`

Parameters

- `BRG Internal`

  `Internal` uses the ***MultiCom***'s system clock divided to give the correct speed.

- `BRG External`

  `External` corresponds to the TCLK that is provided by the modem (signal 114).

Default value
`External`

The rate is specified by the `Serial Speed` (page 258) command, when BRG is internal.

The output of the BRG is driven onto the signals 113 (TCLK from ***MultiCom*** to Modem) and 128 (RCLK from ***MultiCom*** to Modem).

SERIAL FLAGS

14.18.102

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Used to turn on or off the transmission of serial flags.

Type

`Global`

Format

`Serial [{1 | 2}] Flags {On | Off}`

Parameters

- `Flags On`

  Turns flags sending on.

- `Flags Off`

  Turns flags sending off.

Default value

`On`

The ***MultiCom*** normally sends flags (eight bit markers) on the serial line when the line is idle (i.e. Between frames). These flags are used by the receiving ***MultiCom*** to detect if the serial line is working correctly.

NOTE - When serial flags are being sent, the transmit and receive LEDs on the modem will remain permanently lit.

SERIAL INFO

14.18.103

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command displays the current status of the serial line(s).

Type

`Interactive`

Format

```
Serial [{1 | 2}] Info
```

Parameters

- `Info`

  The first block of text describes how the serial port has been configured and the second block gives the alarm details. A typical example is given below:

```
MultiCom:Info Serial
Serial Info
-----------
Serial is Connected
Site      = Internet
Mode      = X21
Clk speed = 128Kbit/s
BRG       = External
RCLK      = External
TCLK      = RCLK
RTS mode  = OFF
Flags     = ON

Alarm Details
-------------
CD   - 109: Alarm Disabled
DSR  - 107: OK
TCLK - 114: Alarm Disabled
RCLK - 115: OK
BRG  - 114: Alarm Disabled
flags- RxD: OK
Link -    : OK
```

SERIAL LLB

14.18.104

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is for test purposes only. Switching LLB on puts the modem in local loop-back mode.

Type

```
Global
```

Format

```
Serial [{1 | 2}] LLB {On | Off}
```

Default value

```
Off
```

SERIAL LMT

14.18.105

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is for test purposes only. Switching LMT on puts the modem in maintenance mode.

Type

`Global`

Format

`Serial [{1 | 2}] LMT {On | Off}`

Default value

`Off`

SERIAL MODE

14.18.106

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command applies the default configuration for a given type of modem.

Type

`Global`

Format

`Serial [{1 | 2}] Mode {X21 | V35 | V36 | NM}`

Parameters

- `Mode X21`

  Sets the configuration to use a X21 interface.

- `Mode V35`

  Sets the configuration to use a V35 interface.

- `Mode V36`

  Sets the configuration to use a V36 interface.

- `Mode NM`

  Sets the configuration to use a null-modem cable. This mode is for test purposes only.

Default value

`X21`

SERIAL NS

14.18.107

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is for test purposes only.

Type

```
Global
```

Format

```
Serial NS {On | Off}
```

Default value

```
Off
```

SERIAL ON & OFF

14.18.108

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This commands activates or de-activates the serial port. It attaches the serial line to the currently selected site.

Type

`Site-specific`

Format

`Serial [{1 | 2}] {On | Off}`

Parameters

- `On`

  Activates the serial port.

```
MultiCom:Serial On
Serial mode on for site “Bern”
```

- `Off`

  De-activates the serial port.

Default value

`Off`

SERIAL PINS

14.18.109

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Displays the status of the control signals on the serial port.

Type

```
Interactive
```

Format

```
Serial [{1 | 2}] Pins
```

Parameters

- *none*

```
MultiCom:Serial Pins
RTS  (o) = ON
SRS  (o) = OFF
NS   (o) = OFF
LMT  (o) = OFF
LLB  (o) = OFF
CTS  (i) = OFF
CD   (i) = OFF
DSR  (i) = OFF
TI   (i) = OFF
CI   (i) = ON
BRG      = TCLK
RCLK (i) = OFF
TCLK (i) = OFF
```

The signal names followed by the text (o) are output signals (***MultiCom*** -> Modem), (i) indicates input signals (Modem -> ***MultiCom***).

SERIAL RCLK

14.18.110

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Chooses the source of the Receive Clock.

Type

Global

Format

```
Serial [{1 | 2}] RCLK {Internal | External}
```

Parameters

- `RCLK Internal`

  `Internal corresponds to the internal Bit Rate Generator (BRG).`

- `RCLK External`

  `External corresponds to the RCLK generated by the modem (signal 115).`

Default value

External

NOTE - It is also possible to derive the RCLK from the modems's TCLK by configuring the BRG as external and the RCLK as internal.

SERIAL RTS

14.18.111

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Global`

Format

`Serial [{1 | 2}] RTS {On | Off}`

Parameters

- `RTS On`

  Sets the state of the RTS signal to on, if AutoRTS (page 246) is off.

- `RTS Off`

  Sets the state of the RTS signal to off, if AutoRTS (page 246) is off.

Default value

`Off`

SERIAL SPEED

14.18.112

V 2.2.6	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Specifies the speed of the serial line. This information is used for two purposes: if the ***MultiCom*** is generating the clock for the line, then this specifies the clock speed. The bandwidth-on-demand option needs to know the serial line speed so that it can decide when the serial line is saturated.

Type

`Global`

Format

`Serial [{1 | 2}] Speed` *`rate`*`[{K|M}]`

Parameters

- *`rate`*

  Specifies the speed of the serial line (measured in bits/s).

- *`rate`*`K`

  Specifies the speed of the serial line (measured in Kbits/s).

- *`rate`*`M`

  Specifies the speed of the serial line (measured in Mbits/s).

Default value

`64 Kbits/s`

NOTE - Under normal circumstances the modem generates the clock, however it is possible to configure the ***MultiCom*** to generate one or both clocks. The default modes that are selected by the `Serial Mode` (page 252) command, always assume that the clock comes from the modem.

SERIAL SRS

14.18.113

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is for test purposes only.

Type

`Global`

Format

`Serial SRS {On | Off}`

Default value

`Off`

SERIAL TCLK

14.18.114

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Chooses the source of the Transmit Clock.

Type

`Global`

Format

`Serial [{1 | 2}] TCLK {Internal | External | RCLK}`

Parameters

- `TCLK Internal`

  `Internal` corresponds to the BRG.

- `TCLK External`

  `External` corresponds to the TCLK generated by the modem (signal 114).

- `TCLK RCLK`

  `RCLK` configures the ***MultiCom*** so that it takes its TCLK from the RCLK that is provided by the modem (signal 115).

Default value

`RCLK`

SETUP

14.18.115

V 2.3	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Allows you to use the EasySetup™ feature from an interactive session.

Type

`Interactive`

Format

`Setup`

Parameters

- `none`

  This command allows you to use the Easy Internet Access Setup from the console port or from a remote Telnet session. It requires that:

  - All your local machines are configured with TCP/IP as DHCP clients (see §14.18.16, "DHCP" on page 124)

  - No other DHCP server is active in your Local Area Network

  - Your Internet Service Provider use standard PAP or CHAP for PPP

  - You get a dynamic IP address from your ISP

  - You have a Single Internet User Account with ***username*** and ***password***

  - You know the nearest ***phone number*** of your ISP

  You can then run the setup command and simply follow the instructions.

  For more complex setup, you may use the EasyConfig™ Windows wizard.

  For really complex setup and fine tuning, you can directly edit the Configuration file (see §15, "Configuration" on page 293) using the EditConfig™ Windows application, the built-in Web-server, Telnet or FTP.

NOTE - You may have to know the DNS configuration of your ISP, if it doesn't provide it using PPP.

SITE CREATE

14.18.116

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

The following command is used to create a site.

Type

`Global`

Format

`Site Create` *`site_name`* `[{PPP | MHDLC}]`

Parameters

- `Create` *`site_name`* `[MHDLC]`

  Creates a new WAN site that will use MHDLC as the link protocol. If the site already exists, an error message is displayed.

  See §14.18.71, "MHDLC Encoding" on page 208 and following paragraphs for detailed MHDLC commands.

- `Create` *`site_name`* `PPP`

  Creates a new WAN site that will use PPP as the link protocol. If the site already exists, an error message is displayed.

  See §14.18.79, "PPP Callback" on page 217 and following paragraphs for detailed PPP commands.

WARNING FOR POCKET AND CLASSIC MULTICOM

14.18.116.1

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Care should be taken when using the Multi-Point option in the Pocket and Classic ***Multi****Com*. There are only two B-channels (and possibly one leased-line connection with a ***Classic*** *Multi****Com***). If a situation arises where there is traffic for more sites than there are WAN links, the ***Multi****Com* will juggle the available B-channels among the sites.

Juggling the B-channels means giving a B-channel to a site for 5 seconds before taking it back to give to another site. This continues until the number of sites needing to transmit data no longer exceeds the number of WAN links.

If this situation arises regularly or for long periods, *telephone bills can become very costly* since juggling the B-channels means connecting and disconnecting the B-channels frequently.

This situation can typically arise because of frequent broadcasts on the Ethernet, but may come from other sources. It can be avoided if the ***MultiCom*** is correctly configured to avoid these situations. This is done by filtering all unnecessary traffic. This is especially important if the number of sites exceeds the number of channels.

NOTE - There are many other commands that modify the individual parameters of the selected site. They are given in the other sections of this chapter.

SITE INFO

14.18.117

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Interactive`

Format

`Site Info [`*`site`* `[{Frames | Frame` *`n`*`}]]`

Parameters

- `none`

  Displays the list of all available sites.

- *`site`*

  Displays specific information about one site.

```
MultiCom:Info Site lightning
Name                  = lightning
Type                  = WAN
Send IP Broadcasts    = OFF
WAN Protocol          = Proprietary MHDLC (ROUTED)
MHDLC mode            = Polling (v3)
MHDLC Encryption      = OFF
MHDLC encoding        = NRZI
Site Protocol Alarm   = ON
Leased Line Backup    = OFF
ISDN RemoteNumber     = *** NONE ***
ISDN RemoteSubAddress = *** NONE ***
ISDN BChannels (max)  = 1
ISDN Auto             = OFF
ISDN MaxTries         = 20
ISDN MaxBackoff       = 86400s
ISDN IdleCloseTime    = 60s


Callback mode         = REJECT
Callback status       = Idle
```

- *site* Frames

  Displays information about frames which caused openings of the ISDN line. This is very useful to find a misconfigured computer or application which causes a lot of unneeded traffic.

  Each packet of the same type (same source, same destination and same destination port) is only recorded once, with an associated counter. If this counter is high, you can suspect a configuration problem.

- *site* Frame *n*

  This command displays detailed information about a suspect packet.

SITE MODIFY

14.18.118

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Changes the link protocol of a site to PPP or MHDLC.

Type

`Global`

Format

`Site Modify` *`site_name`* `WANProtocol {MHDLC | PPP}`

Parameters

- `Modify` *`site_name`* `WANProtocol MHDLC`

  Sets the link protocol for site *`site_name`* to MHDLC.

- `Modify` *`site_name`* `WANProtocol PPP`

  Sets the link protocol for site *`site_name`* to PPP.

NOTE - The link must be closed and reopen, for the change to take effect.

SITE RENAME

14.18.119

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

The following command is used to rename a site.

Type

`Global`

Format

`Site Rename` *`old_site_name new_site_name`*

Parameters

- `Rename` *`old_site_name new_site_name`*

  Renames the site "*`old_site_name`*" to "*`new_site_name`*".

  This command is useful for renaming the two default site names (`ETH` and `ISDN`) to something more meaningful. It may also be used to rename new sites that are added with the "`Site Create`" command.

NOTE - There are many other commands that modify the individual parameters of the selected site. They are given in the other sections of this chapter.

SITE SELECT

14.18.120

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

The following command is used to select the current site.

Type

`Global`

Format

`Site Select [site_name]`

Parameters

- `Select`

  The name of the currently selected site is displayed.

- `Select site_name`

  Makes *site_name* the selected site.

NOTE - There are many other commands that modify the individual parameters of the selected site. They are given in the other sections of this chapter.

SITE STATS

14.18.121

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

The following command is used to display the status of a site.

Type

Interactive

Format

Site Stats [*site_name*]

Parameters

- Stats

  Displays traffic and ISDN statistics for the currently selected site.

- Stats *site_name*

  Displays traffic and ISDN statistics for the named site.

```
MultiCom:Site Stats werner
TRAFFIC STATISTICS (Site Werner):
Total Packets Sent     = 67797
Total Packets Received = 65264
Total Bytes Sent       = 44496920
Total Bytes Received   = 5058860
Total Rx Discards      = 0
Total Tx Discards      = 76
Total Rx Bad Protocol  = 0
IP Packets Sent        = 67797
IP Packets Received    = 65264
IP Bytes Sent          = 43547762
IP Bytes Received      = 4145164

ISDN STATISTICS (Site Werner)
Number of outgoing calls              = 0
Number of outgoing calls for callback = 0
Number of incoming calls              = 108
Nbr failed outgoing calls             = 0
Total Cost                            =       0
Callback Cost                         =       0
Total Site Connection time            = 48660s
Incoming B-Channel total time         = 48658s
```

```
Outgoing B-Channel total time         = 0s
Outgoing B-Channel for callback time   = 0s
Current cost                           =       0
Current connection time                = 123s
B-Channels in use                      = tx=1 rx=1
Currently doing callback               = NO
```

NOTE - There are many other commands that modify the individual parameters of the selected site. They are given in the other sections of this chapter.

SLEEP

14.18.122

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Suspends the command interpreter.

Type
`Interactive`

Format
`Sleep` *`delay`*

Parameters
- *`delay`*

  Causes the command interpreter to delay a specified number of seconds before executing the next command.

  This is useful for testing the ability of a remote site to call back the local site. The following example shows how this can be done.

```
Local:Select RemoteSite
Site 'RemoteSite' selected.

Local:ISDN IdleCloseTime 10
Idle Close Time for site “RemoteSite” set to 10 seconds.

Local:Telnet RemoteMultiCom
TELNET V1.02    Hit CTRL-] to quit
connection open

Lightning MultiCom release 2.4 ready.

Remote:Sleep 30
ls
...
```

  On the local machine the IdleCloseTime is set to 10 seconds. On the remote site the machine is to sleep for 30 seconds and the `ls` command is typed immediately, before the prompt is displayed. Supposing that it took 5 seconds to type the `ls` command, the output will not be displayed for another 25 seconds. Since it was the local machine that opened to connection and its Idle-

CloseTime is 10 seconds, the local machine will close the ISDN before the output of the `ls` command has been displayed. Several seconds later, the remote machine will try to display the results of the `ls` command. Since there is no ISDN connection open, it will automatically try to open one.

If the connection is opened, this means that the remote site has been correctly configured. If it is not opened, the remote site has been incorrectly configured (e.g. wrong `ISDN RemoteNumber`). To recontact the remote site, simply hit any key (remember, you are still in Telnet). This will cause the local machine to re-open the connection.

SNMP AUTHTRAP

14.18.123

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

When authentication traps are enabled, the agent will send an authenticationFailure trap to each defined manager, each time an invalid community name is used.

Type
Global

Format
SNMP AuthTrap {Enable | Disable}

Parameters

- AuthTrap Enable

  Enables SNMP authentication failure traps.

```
MultiCom:SNMP AuthTrap Enable
SNMP authentication failure traps enabled
```

- AuthTrap Disable

  Disables SNMP authentication failure traps.

```
MultiCom:SNMP AuthTrap Disable
SNMP authentication failure traps disabled
```

Default value
Enabled

NOTE - You may also enable and disable authentication failure traps through SNMP by setting the following MIB object:
iso.org.dod.internet.mgmt.mib-2.snmp.snmpEnableAuthenTraps.0
to enabled(1) or disabled(2).

SNMP COMMUNITY

14.18.124

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

To be able to access the agent with a manager you need to have a community name, which is a sort of password. This command allows you the set the community names that will be accepted by the agent.

Type
`Global`

Format
`SNMP Community [`*`community_name`* `{Read | Write | Remove}]`

Parameters

- `Community`

  Displays the defined community names.

```
MultiCom:SNMP Community
SNMP Community names
     Name     Rights
     ----     ------
     public   Read
```

- `Community` *`community_name`* `Read`

  Adds the community name *`community_name`* with “Read” permission.

```
MultiCom:SNMP Community toto Read
SNMP Community names
     Name     Rights
     ----     ------
     public   Read
     toto     Read
```

  All existing community names are shown.

- `Community` *`community_name`* `Write`

  Adds the community name *`community_name`* with “Write” permission.

```
MultiCom:SNMP Community toto Write
SNMP Community names
     Name     Rights
     ----     ------
     public   Read
     toto     Write
```

- `Community` *`community_name`* `Remove`

  Removes the community name *`community_name`*.

```
MultiCom:SNMP Community toto Remove
SNMP Community names
     Name     Rights
     ----     ------
     public   Read
```

The community name ‘toto’ has been removed. The community names that are left are shown.

NOTES 14.18.124.1

The access type, ‘Read’ or ‘Write’ determines the type of SNMP requests the manager may issue to the agent. These are:

- For ‘Read’: GetRequest and GetNextRequest.
- For ‘Write’: GetRequest, GetNextRequest and SetRequest.

The community ‘public’ with ‘Read’ permission exists by default.

CAUTION — Be aware that the community name are case-sensitive, that is ‘toto’ is not the same as ‘Toto’ or ‘toTo’.

SNMP INFO

14.18.125

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Interactive`

Format

`SNMP Info`

Parameters

- `Info`

  Gives the managers, community names and state of the authentication failure traps.

```
MultiCom:Snmp Info
Managers:
Address         Port
-------         ----
193.5.2.1       162

Communities:
Name            Rights
----            ------
manager         Write
public          Read

Authentification failure traps enabled.
```

SNMP MANAGER

14.18.126

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command sets the SNMP managing stations.

Type

`Global`

Format

`SNMP Manager [`*`IP_Address`* `[`*`port_number`* `[Remove]]]`

Parameters

- `SNMP Manager` *`IP_Address`*

  Adds a managing station to the manager list.

```
MultiCom:SNMP Manager 193.5.2.162
SNMP Manager
     Address       Port
     -------       -----
     193.5.2.162   162
```

- `SNMP Manager` *`IP_Address port_number`*

  The port number is optional. By default it is set to 162, which is the reserved SNMP trap port in UDP. You may specify another port .

```
MultiCom:SNMP Manager 193.5.2.162 8000
SNMP Manager
     Address       Port
     -------       -----
     193.5.2.162   162
     193.5.2.162   8000
```

  Where 8000 is the port number on which your SNMP manager is listening.

- `SNMP Manager` *`IP_Address port_number`* `Remove`

  Removes a manager from the manager list.

```
MultiCom:SNMP Manager 193.5.2.162 8000 Remove
SNMP Manager
     Address       Port
     -------       -----
     193.5.2.162   162
```

In this case you must specify the port number. The display will show the managers that are left after the command.

NOTES 14.18.126.1

The SNMP agent is capable of sending unsolicited information to a managing station in order to report unusual events. These packets, called ‘traps’, may report the following events:

- coldStart (0)
- warmStart (1)
- linkDown (2)
- linkUp (3)
- authenticationFailure (4) : When an inappropriate community name is used.
- enterpriseSpecific (5)

For a ***MultiCom*** to send one of these traps, at least one manager must be specified.

For a ***MultiCom*** to send authenticationFailure traps, the authentication failure traps must be enabled.

SNMP RESTART

14.18.127

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Interactive`

Format

```
SNMP Restart
```

Parameters

- `Restart`

  Abort current operation, reset all variables and send warm start trap.

SNMP STATS

14.18.128

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Interactive`

Format

```
SNMP Stats
```

Parameters

- `Stats`

  Displays SNMP counters.

SNTP

14.18.129

V 2.2.6	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command controls the Simple Network Time Protocol client.

Type

`Global`

Format

```
SNTP Server {hostname | IP_number}
SNTP Offset [+|-]hh:mm
SNTP Period hours
SNTP Timeout seconds
```

Parameters

- `Server {hostname | IP_number}`

  Sets the SNTP server. To set the server by name, a DNS must be defined.

- `Offset [+|-]hh:mm`

  Sets the offset between UTC and your local time. If your timezone is GMT+1, set the offset to 1. For Daylight Savings Time, add one to the offset.

- `Period hours`

  Sets the time interval at which the SNTP server will be polled for time updates. It must be in the range [1..744].

- `Timeout seconds`

  Sets the maximum time SNTP will wait for a reply.

- `Info`

  Displays information on the SNTP configuration.

SYSLOG

14.18.130

V 2.2	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Configures the built-in syslog client.

Type

```
Global
```

Format

```
Syslog {LogHost [IP_Address] | Facility [code] |
Priority [level]}
```

Parameters

- `LogHost` *`IP_Address`*

  Defines the address of the machine hosting the syslog daemon. This daemon will receive notifications from the ***MultiCom***, including:

  - SecureWall™ break-in attempts (see “IP Translation” on page 155)

  - Failed logins

  - Leased Line failure and recovery (see “Backup” on page 110)

- `Facility`

  Displays the facility currently used by the syslog client.

- `Facility` *`code`*

  Changes the facility used by the syslog client.

- `Priority`

  Displays the priority currently used by the syslog client.

- `Priority` *`level`*

  Changes the priority used by the syslog client.

Default value

```
Facility = user
Priority = info
```

TELNET

14.18.131

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Invokes the interactive Telnet client.

Type

`Interactive`

Format

`Telnet {`*`IP_Address`* `|` *`hostname`*`} [`*`port_number`*`]`

Parameters

- *`IP_Address`*

  Opens a Telnet connection to the host specified by the address *`IP_Address`*.

```
MultiCom:Telnet remote
TELNET V1.02
connection open
REMOTE Server Telnet 1.1 ready.
UserName :
```

- *`hostname`*

  If the DNS client is properly configured, then *`hostname`* can be an Internet machine name (See §14.18.16, "DHCP" on page 124).

- *`port_number`*

  TCP port number to connect to. By default: 23.

TIME

14.18.132

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Displays and configure the system clock.

Type

`Interactive`

Format

`Time [Set hh:mm:ss | Set Date date month year]`

Parameters

- `None`

  Displays the current date and time.

- `Set hh:mm:ss`

  Configures the system time.

- `Set Date date month year`

  Configures the system date.

NOTE - On the ***MultiCom LAN Access Center***, ***MultiCom Access IV*** and ***MultiCom Backup IV***, the time and date are saved inside a Real-Time Clock (RTC) across reboots.

TRACEROUTE

14.18.133

V 2.2.6	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command displays all routers between you and a remote machine.

Type

`Interactive`

Format

`Traceroute` *`machine`*

Parameters

- *`machine`*

  The name or IP address of the remote machine you want to test.

```
MultiCom:Traceroute www.lightning.ch
traceroute to www.lightning.ch (193.5.2.161), 64 hops max
1 (193.5.2.161) 80 ms * 20 ms
-- Traceroute completed successfully
```

UPGRADE

14.18.134

V 2.2.6	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Installs additional firmware options.

Type

`Interactive`

Format

`Upgrade Key` *`UpgradeKey`*

Parameters

- *`UpgradeKey`*

  This command installs additional firmware options, like multi-point (/M) or encryption (/E), without fully reprogramming your ***MultiCom***, using an activation key provided by your distributor.

  You can check the currently installed options with the "`Version`" command.

NOTE - Your ***MultiCom*** will be rebooted after successful installation of the new options, to activated them.

WARNING — While all the lights on the front panel are red, you **must not** switch off the ***MultiCom***. Doing so may cause the ***MultiCom*** to malfunction.

UPTIME

14.18.135

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Type

`Interactive`

Format

`Uptime`

Displays the time duration for which the ***MultiCom*** has been running. This time is reset to zero when the ***MultiCom*** is switched on or reboots.

```
MultiCom:Uptime
25 days, 5 hrs, 15 mins, 41 secs
```

USER

14.18.136

V 2.2.9	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This command is used to manage user accounts on the ***MultiCom***. It replaces the obsolete "`Account`" command.

Type

`Interactive`

Format

`User {Create` *`username password`* `| Save` *`username`* `| Remove` *`username`* `| Info}`

Parameters

- `Create` *`username password`*

  Creates a temporary user account with a name and an associated password.

NOTE - Multiple user accounts may be created by repeating this command.

```
MultiCom:User Create toto secret_password
User "toto" created.
```

NOTE - When no user is defined (which is the case in the default configuration file), there is no check at all to access the ***MultiCom***. This is to simplify the initial configuration only. **We strongly advise you to create user accounts to protect the access to your *MultiCom*.**

- `Save` *`username`*

  Saves a user account into permanent Flash-EPROM memory.

- `Remove` *`username`*

  Permanently removes a user account from memory.

- `Info`

  Displays the list of currently defined user accounts and their state (unsaved or saved to Flash-EPROM).

```
MultiCom:User Info
Username        Saved
---------------------
toto             Yes
titi             No
```

NOTE - This is the only option is available in high-security mode (see §14.18.97, "Security" on page 241).

VERSION

14.18.137

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Displays version information.

Type

`Interactive`

Format

`Version Info`

Parameters

- `Info`

  Displays the current firmware revision, serial number and installed options. Please use this command **before** any call to Customer Support.

```
MultiCom:Version Info


Software Release 2.2.9

ISDN Layer2 : version 2.0
ISDN Layer3 : version 2.0
ISAC Driver : version 2.0

Serial Number = LI-MU1-CH-2167

Software Options
---------------
IP Router   : INSTALLED
IPX Router  : INSTALLED
Bridge      : INSTALLED
Serial Line : INSTALLED
Multi-point : INSTALLED
SNMP        : INSTALLED     (SNMPv1)
Encryption  : INSTALLED
```

WRITECONFIG

14.18.138

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Copy (and overwrite) the current config file from the `#RAM` disk to Flash memory. The system will use this config file for all further boots.

Type
`Interactive`

Format
`WriteConfig`

Parameters
- `none`

```
MultiCom:WriteConfig
#RAM:CONFIG file stored in the Flash-EPROM.
```

NOTE - During the programming of the Flash-EPROM (typically a few seconds), all LEDs on the front panel become red and the Power LED becomes orange, indicating that all other functions of the ***MultiCom*** are suspended.

NOTE - You must reboot (see §14.18.93, "Reboot" on page 236) the ***MultiCom*** to use the new config file.

WARNING — While all the lights on the front panel are red, you **must not** switch off the ***MultiCom***. Doing so may cause the ***MultiCom*** to malfunction.

Chapter 15

Configuration

This describes how to create your own configuration file.

INTRODUCTION 15.1

Normally, the configuration commands of the ***MultiCom*** are stored in Flash EPROM. When the ***MultiCom*** boots, it creates a file named CONFIG in the `#RAM:` disk and copies the configuration commands from the Flash EPROM into this file. The ***MultiCom*** then executes the commands from this file. See figure 10 “CONFIG file mechanism” on page 295.

NOTE - As the ***MultiCom*** executes the commands in the CONFIG file, it keeps a trace in a file called “BOOT.RPT”. Any errors that are encountered in the CONFIG file will be recorded in this file. This file can be viewed with the `Cat` command. It is a very useful way of finding syntax errors.

However, when you receive a new ***MultiCom***, there is no configuration in the Flash EPROM. In this case the ***MultiCom*** executes the contents of the default configuration file, which is found in the `#ROM:` disk. Note that the `#ROM:` disk is read-only, so you can not modify the default configuration file.

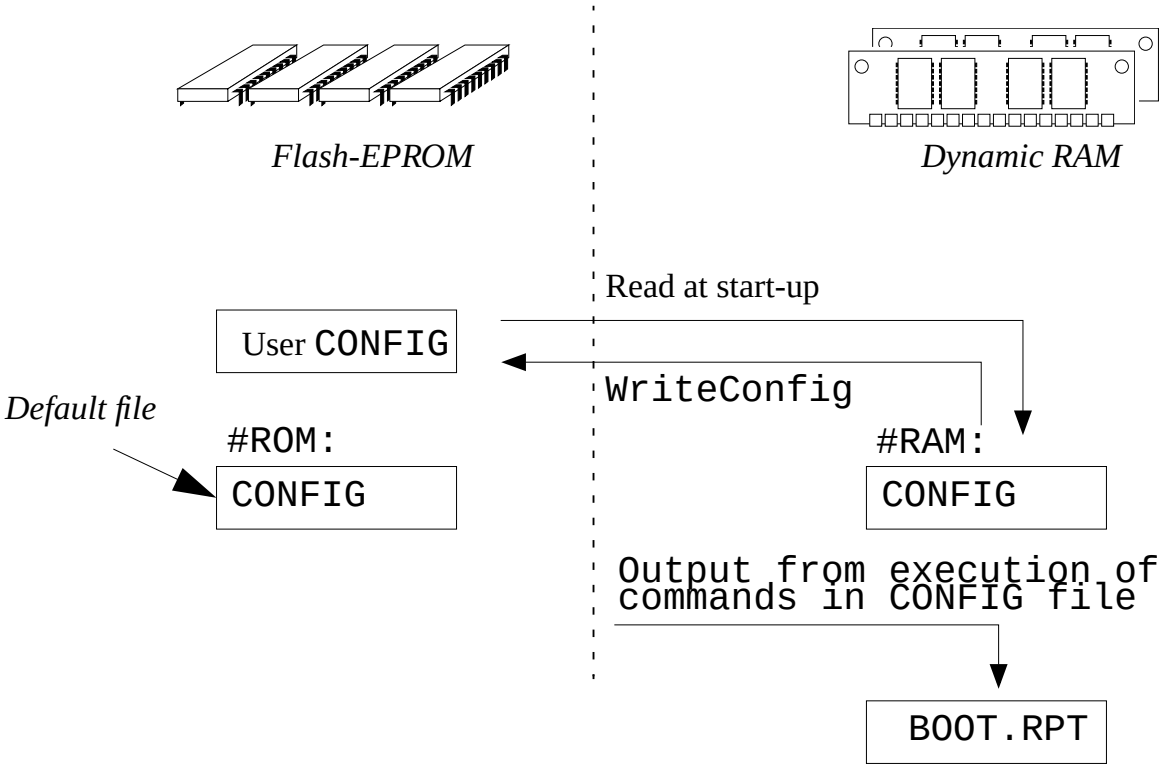


Figure 10 CONFIG file mechanism

The easiest way to create a new configuration file is to copy the default configuration file from the #ROM: disk to the #RAM: disk. Once in the #RAM: disk, the file can be modified. The ***MultiCom*** does not have a command to copy files, but it is possible to do the equivalent of this using the editor: simply edit #ROM:CONFIG and save it as #RAM:CONFIG (use the "`W`" command to save a file under a new name).

Once the configuration file has been modified, it should be written to the Flash EPROM. Otherwise, the modifications will be lost the next time that the ***MultiCom*** is rebooted. The `WriteConfig` command must be used to store the configuration file in Flash EPROM.

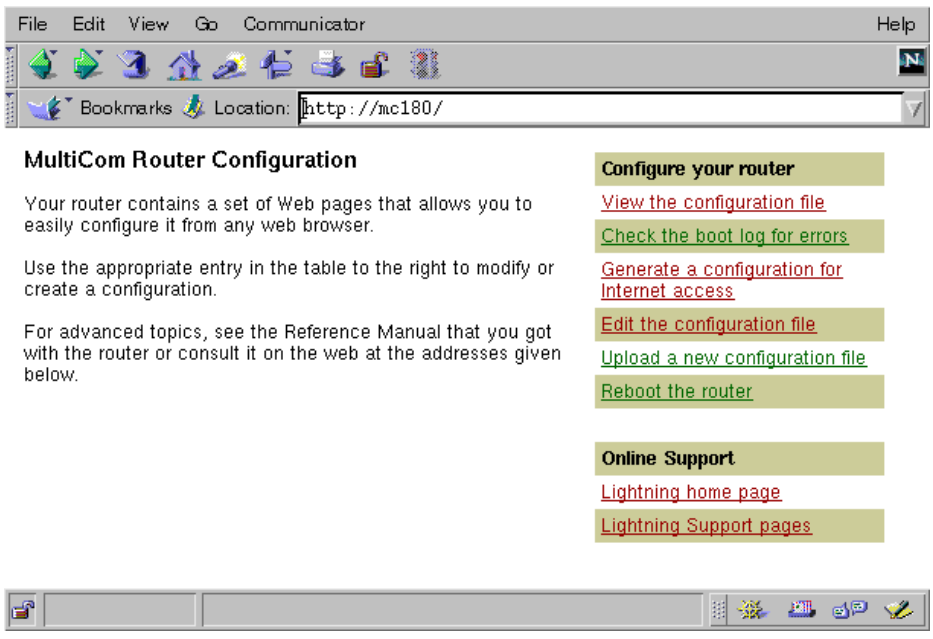
ACCESSING THE MULTICOM 15.2

In order to modify the configuration file, it is necessary to log into the ***MultiCom***. There are six ways of doing this:

- Use a browser to connect to the built-in Web-server.
- Use the EasyConfig Windows wizard.
- Use the EditConfig Windows application.
- Log in using TELNET.
- Use FTP to copy files to and from the ***MultiCom***.
- Log in through the CONSOLE port as described in your User's Manual.

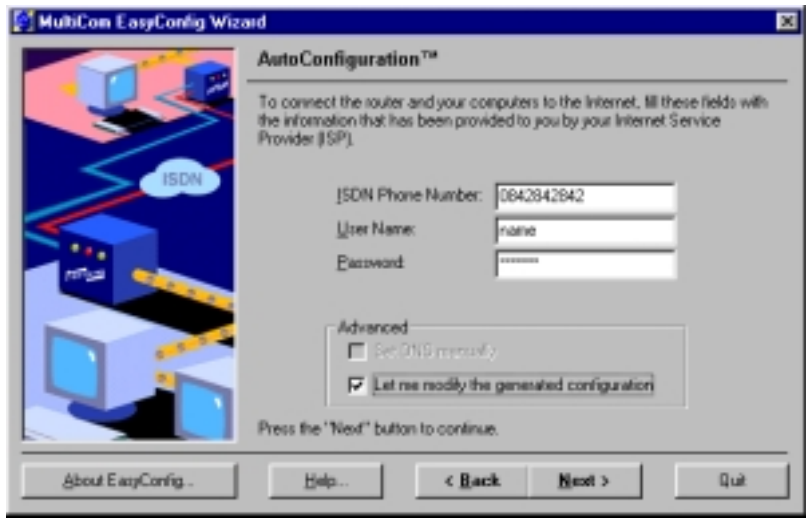
ACCESSING THE MULTICOM WITH A BROWSER 15.2.1

There is a built-in Web-server inside your ***MultiCom*** (which is by default at the URL http://10.0.0.1/). You can access it using any Internet browser (like Netscape or Internet Explorer). It allows currently to view, edit and upload the configuration file and to automatically generate a configuration for a very easy Internet access.



ACCESSING THE MULTICOM WITH EASYCONFIG 15.2.2

On the CD-ROM delivered with your ***MultiCom***, there is an installer for a Windows wizard that let you configure your router with a simple graphical interface.



ACCESSING THE MULTICOM WITH TELNET 15.2.3

If you have a host on your network that supports TELNET, you can log in to the ***MultiCom*** remotely. You may be prompted for a username and password. Once logged in, the connection behaves in a similar manner as when you are logged in on the CONSOLE port.

ACCESSING THE MULTICOM WITH FTP 15.2.4

If you have a host on the internetwork that supports FTP, you can copy files to and from the ***MultiCom***. Each time that you connect to the ***MultiCom***, you will be prompted for a username and password.

NOTE - Once a new configuration file has been downloaded to the ***MultiCom***, it is still necessary to login through the console or Telnet to execute the `WriteConfig` command.

NOTE - The name of the downloaded file must be `CONFIG`

NOTE - Download MUST be done in text mode (ASCII).

MODIFYING THE CONFIGURATION 15.3

To modify the ***MultiCom*** configuration, you need to create a new CONFIG file. There are several ways of doing this:

1. Connect to the built-in Web-server (by default http://10.0.0.1/).
2. Use the `EasyConfig` Windows wizard or the `EditConfig` Windows application (available on the provided CD-ROM or at http://www.lightning.ch/support/index_upgrades.html).
3. Local modification of the default CONFIG file: Log in to the ***MultiCom*** and use the `Edit` command to modify the default CONFIG file (#ROM:CONFIG). Save the result in #RAM:CONFIG. This is the approach that is explained in your User's Manual.
4. Local modification of an existing configuration: Log in to the ***MultiCom***. The file can then be modified using `Edit`.

5. Remote modification of the default CONFIG file: From another host on the internetwork, use FTP to copy #ROM:CONFIG from the ***MultiCom***. Edit the file on the host. Use FTP again to copy the file back to the ***MultiCom*** and store the file as #RAM:CONFIG. (Note: the #ROM disk is read-only).
6. Remote modification of an existing configuration: From another host on the internetwork, use FTP to copy #RAM:CONFIG from the ***MultiCom***. Edit the file on the host. Use FTP again to copy the file back to the ***MultiCom***.

NOTE - When using FTP to transfer the configuration file, it is essential to do it in ASCII mode.

USING THE NEW CONFIG FILE 15.4

Once you have completed one of the above steps, you should have the new configuration stored in #RAM:CONFIG. The following steps are then necessary before the new configuration is taken into account:

1. If you are not already logged in to the ***MultiCom***, do so.
2. Issue the `WriteConfig` command to copy #RAM:CONFIG to Flash-EPROM.
3. Reboot the ***MultiCom*** (see § 14.18.93, "Reboot" on page 236).

NOTE - The ***MultiCom*** will default to the #RAM: disk if no path name is specified. The file names CONFIG and #RAM:CONFIG are equivalent.

Chapter 16

Trouble Shooting

Something went wrong?
Please go through our check-list!

CONFIG CHECK-LIST 16.1

This check-list describe the steps you should take to verify that your ***MultiCom*** is properly configured.

This is not an exhaustive list, since the number of possible configurations is nearly infinite.

You will find in § 18.1, "Config check-list" on page 390, an empty check-list with only the check-box titles that you may use for checking your ***MultiCom*** configuration, once you are familiar with the following detailed list.

BASICS 16.1.1

☐ ***Advanced Diagnostics***

If you can connect to the *MultiCom*, use the built-in `Diagnose` command (see §14.18.17), which will help you find the problem, otherwise follow the steps below:

☐ *Power LED*

At the beginning of the start-up procedure the power LED should turn orange. At the end of the start-up procedure the power LED should turn green, unless you have the encryption option.

- Is the power cable connected as described in the User's Manual ?
- Is the ***MultiCom*** inside the operating temperature range ?

☐ *Terminal*

If you have connected a terminal or terminal emulation software, you should see a power-up message appear on the screen when powering the ***MultiCom*** on.

- Are the terminal settings correct (Baud rate, parity, etc...), as specified in the User's Manual ?
- Is the terminal cable correctly connected at both ends ?

- Are you using the supplied terminal cable ? (See the package contents in your User's Manual)

You can see the power-up message but cannot type any characters.

- Make sure that the terminal settings are correct (Baud rate, parity, etc...), as specified in the User's Manual.

☐ *Cables*

All cables for the desired configuration should be connected, as specified in the User's Manual:

- Power cable
- ISDN cable(s)
- Ethernet cable(s)
- Serial cable(s)

☐ *Ethernet LED*

The Ethernet LED should turn green near the end of the start-up procedure.

- Is the Ethernet cable correctly connected ?
- Do you use the correct cable for this ? (See § 16.2.2, "Pocket MultiCom" on page 308).

☐ *ISDN D LED*

The ISDN D LED(s) (D-channel indication) should be green or off after power-on or restart. If red, there is an ISDN connection problem.

- Is the ISDN cable correctly connected ?
- Is the D-channel protocol correct (see § 14.18.50, "ISDN DChannelProtocol" on page 178) ?
- Is your local PABX (if there is one) properly configured for data calls (see § 16.2.3, "PABX" on page 308) ?
- Is your ISDN connection in function ? Try it with an ISDN phone or ask your telecom operator.

CONFIGURATION: BASICS

16.1.2

☐ *IP Number*

- The IP number of the ***MultiCom*** must be defined. The default value is **10.0.0.1** (see § 14.18.27, "IP MyAddr" on page 144).
- If you wish to connect to the ***MultiCom*** via FTP, Telnet or WWW, this IP address must be a valid address on your network. This should be done with a console connection as described in your User's Manual, and before connecting the ***MultiCom*** to the LAN.

☐ *Config file*

The default config file allows the ***MultiCom*** to start-up in a generic manner. You must configure the ***MultiCom*** for your specific usage by changing the config file.

- When changed on the ***MultiCom*** the config file must be:

1. Saved (§ 14.18.20, "Edit" on page 133) with the name CONFIG
2. Copied to Flash-EPROM (§ 14.18.138, "WriteConfig" on page 291)
3. The ***MultiCom*** should be rebooted to use the new CONFIG file.

- When changed on a PC, the `config` file must be:

1. Downloaded in ASCII mode to the ***MultiCom*** using a FTP software.
2. Copied to Flash-EPROM (§ 14.18.138, "WriteConfig" on page 291) using a console connection or a Telnet connection.
3. The ***MultiCom*** should be rebooted to use the new CONFIG file.

☐ *Boot.rpt*

The "`boot.rpt`" file contains the commands used in the config file and their results.

- There should be no errors in the "`boot.rpt`" file. You may view this file by using the "`cat boot.rpt`" command (§ 14.18.14, "Cat" on page 122).

The "`boot.rpt`" file shows an error on each line although the commands seem correct.

- If you have downloaded the CONFIG file, make sure that the editor you have used does not add special characters at the end of each line.
- Use the local editor to edit the CONFIG file (§ 14.18.20, "Edit" on page 133).

CONFIGURATION: ISDN

16.1.3

☐ *Length of MSN*

The ***MultiCom*** uses the MSN part of the ISDN number to identify itself (See § 14.18.59, "ISDN MyNumber" on page 192). To determine the length of the MSN on your connection, try the following:

1. Ask your Telecom operator.
2. Do an “ISDN loop back (external)” on page 305 and look at the ISDN history (§ 14.18.54, "ISDN Info" on page 183) to determine the number.

☐ *Enabled ISDN numbers*

Some numbers may be truncated or changed by the Telecom switch or your local PABX. When you specify allowed remote numbers (§ 14.18.62, "ISDN Number-Enabled" on page 197) you must use the number as delivered by the switch.

To determine how the numbers are truncated or changed:

1. Call the ***MultiCom*** from an external number.
2. Look at the ISDN history (§ 14.18.54, "ISDN Info" on page 183) to determine the number.

Your connection opens shortly then closes down right after.

- Make sure you use only one “*” as an enabled remote number (§ 14.18.62, "ISDN NumberEnabled" on page 197).
- Verify the PPP parameters

☐ *ISDN loop back (external)*

The same as “*ISDN loop back (internal)*” (see below) but with the full ***MultiCom*** number as the remote number in step 2.

☐ *ISDN loop back (internal)*

Only applies if you are connected to a local PABX.

To verify the ISDN connection you may open a loop back connection from the ***MultiCom*** to itself through your PABX. To do so use the following steps:

1. Select a WAN site:

`Site Select ISDN` (or your site name) (§ 14.18.120, "Site Select" on page 268)

2. Set the remote number to the ***MultiCom*** number:

   `ISDN RemoteNumber` ***`msn`*** (§ 14.18.63, "ISDN RemoteNumber" on page 199)

3. Open manually the connection:

   `ISDN Conn` (§ 14.18.49, "ISDN Conn" on page 177)

   Two B-channel LEDs should turn green.

   If not, use the command **`Info Site ISDN`** (or your site name) (§ 14.18.117, "Site Info" on page 264). It will give you the error on the previous outgoing call, returned by the PABX or telecom operator switch.

4. Close the connection:

   `ISDN Disc` (§ 14.18.51, "ISDN Disc" on page 179)

☐ *Site Select + Site Info*

The ***MultiCom*** uses a “site” philosophy and not a “port” philosophy (see § 3.3.1, "What is a Site?" on page 19). That means you should configure all the parameters for each different site.

1. Select a WAN site:

   `Site Select ISDN` (§ 14.18.120, "Site Select" on page 268)

2. Look at the site information:

   `Site Info` (§ 14.18.117, "Site Info" on page 264)

   Check whether all the displayed information corresponds to the desired configuration.

☐ *ISDN Info*

Check whether the ***MultiCom*** MSN and other parameters are corresponding to the desired configuration by typing:

- **`Info ISDN`** (see § 14.18.54, "ISDN Info" on page 183)
- **`Info ISDN Enabled`**
- **`Info ISDN History`**

☐ *PPP Info*

Check whether the PPP parameters are corresponding to the desired configuration by typing:

PPP Info (see § 14.18.83, "PPP Info" on page 224)

CONFIGURATION: IP HOST 16.1.4

☐ *Ping*

To check whether the IP Host part of the ***MultiCom*** is properly configured:

- Use a “PING” application to “ping” the ***MultiCom***’s IP address.

  If this is not working, check that the host’s IP address and the ***MultiCom***’s IP address are in the same subnet and that the subnet mask is properly configured on the PC. See § 4.1.2, "Structure of an IP Address" on page 24, for details on IP addresses and subnet masks.

☐ *Telnet*

If the “Ping” step is working you may now use a “Telnet” application to connect to a local ***MultiCom***.

For further testing of the IP options see § 16.2.6, "IP" on page 310.

CONFIGURATION: OTHER SOFTWARE OPTIONS 16.1.5

For the other software options, use the info command to display the current settings. Check whether these settings are corresponding to the desired configuration.

☐ *Info Bridge*

☐ *Info IP*

☐ *Info IP Router*

☐ *Info IPX*

FREQUENT PROBLEMS 16.2

These are some more explanations on some frequently encountered problems.

MULTICOM 16.2.1

The ***MultiCom*** reboots endlessly at start-up.

- There may be some important errors in the CONFIG file. Go back to the default CONFIG file (see your User's Manual), and start over.

POCKET MULTICOM 16.2.2

V 2.1	IP	IPX	Bridge	MP	V36	SNMP	E
Pocket							
Classic							
LAC							

The ***Pocket MultiCom*** may reboot endlessly or in default configuration if a wrong cable is used to connect it to a Hub. If so try to use a 4-wires cable :

- Use the crossed Ethernet cable to connect your router directly to a PC.
- Use the straight Ethernet cable to connect your router to a Hub.

PABX 16.2.3

- Make sure that your PABX is configured to support data communications and the correct D-channel protocol for this port.
- There is a software bug in an early software version of the Siemens HICOM PABX. Check with your PABX distributor if you use such a PABX.
- Verify if you need to provide a prefix to dial out (usually '0' or '9') and what is the format of incoming CLI.

  These problems can be verified using the "ISDN loop back (external)" test on page 305.

ETHERNET 16.2.4

- Do not forget to configure the IP number of the ***MultiCom*** (§ 14.18.27, "IP MyAddr" on page 144).
- Be careful with the cables, you may have: AUI (***Classic MultiCom*** and ***MultiCom LAN Access Center***), 10-Base-2 (***Classic MultiCom***) or 10-Base-T (***MultiCom LAN Access Center*** and ***Pocket MultiCom***).

  See also § 16.2.2, "Pocket MultiCom" on page 308.
- Make sure that the default gateway of the local PC(s) is set to the local's ***MultiCom*** IP address.

BRIDGE 16.2.5

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

- All the following steps must be completed for a bridge to work:

1. Create a group (§ 14.18.7, "Bridge Create" on page 113).
2. Add desired sites to that group (§ 14.18.11, "Bridge Group" on page 119).
3. Start over at step 1 for all group needed.
4. Create a filter (§ 14.18.7, "Bridge Create" on page 113)
5. Configure filter (§ 14.18.10, "Bridge Filter (entry filling)" on page 116).
6. Assign that filter as input or output filter to a site, or as a group filter to a group (§ 14.18.9, "Bridge Filter (assigning entry)" on page 115).
7. Start over at step 4 for all filter needed
8. Turn the Bridge on (§ 14.18.13, "Bridge On & Off" on page 121).

- Do not use "deny all" combined with "allow something" (See § 14.18.10, "Bridge Filter (entry filling)" on page 116).

IP 16.2.6

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

- Be careful with routing tables, always use planning work-sheets (§ 18.1, "Config check-list" on page 390) and refer to the examples (§ 17.1, "IP: Point-to-Point" on page 314 & § 17.2, "IP: Multi-Point" on page 318).
- Check your connections using:

1. Ping to the local ***MultiCom***
2. Ping to the remote ***MultiCom***
3. Telnet to the local ***MultiCom***
4. Telnet from the local ***MultiCom*** to the remote ***MultiCom***
5. Telnet from the remote ***MultiCom*** to a remote host, if possible.
6. Telnet from a local host to a remote host via the ***MultiCom*** connection, if possible.

If steps 1 to 5 work and not step 6, check the following:

- The ***MultiCom*** routing table (use `Info Ip Router`)
- The PC's default gateway address
- The ARP tables of the remote equipment or other intermediate network devices

IPX 16.2.7

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

- The login procedure to a distant server is very long.

  Usually the login program resides on the distant server and is transferred to the host before being executed. With a 64 kbits/s connection this may take several minutes.

Try to copy the login program to all the client's local disks. Refer to your Novell specialist for the procedure.

PPP 16.2.8

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

- Connection from a ***MultiCom*** to another machine from another vendor in PPP mode does not work.

1. Try connecting two ***MultiCom***'s if possible, in MHDLC mode. Use this check-list to ensure the connection is working properly.
2. Once the connection is working change the link mode to PPP using the `Site Modify` command (§ 14.18.118, "Site Modify" on page 266).
3. Once the connection is working replace the remote ***MultiCom*** with the other vendor's machine.
4. If a connection problem still remains, try the `PPP info` command on the ***MultiCom*** (§ 14.18.83, "PPP Info" on page 224).

NOTE - Lighting may supply PPP configuration files for the main router vendor's machines. Check our web pages: http://www.lightning.ch/support/

Chapter 17

Examples

*This chapter is intended to help you setup the **MultiCom**'s configuration file. Several typical configurations are presented and explained in detail.*

IP: POINT-TO-POINT 17.1

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

The following is an example of a simple point-to-point configuration for TCP/IP.

DESCRIPTION 17.1.1

A company has two offices in Geneva and Bern. It wishes to connect their Local Area Networks (LANs) in routing mode.

- Each site uses the TCP/IP protocol.
- The link will be allowed 2 B-channels (128 kbits/s).

Following is the network layout and the configuration file for each site.

NETWORK DIAGRAM 17.1.2

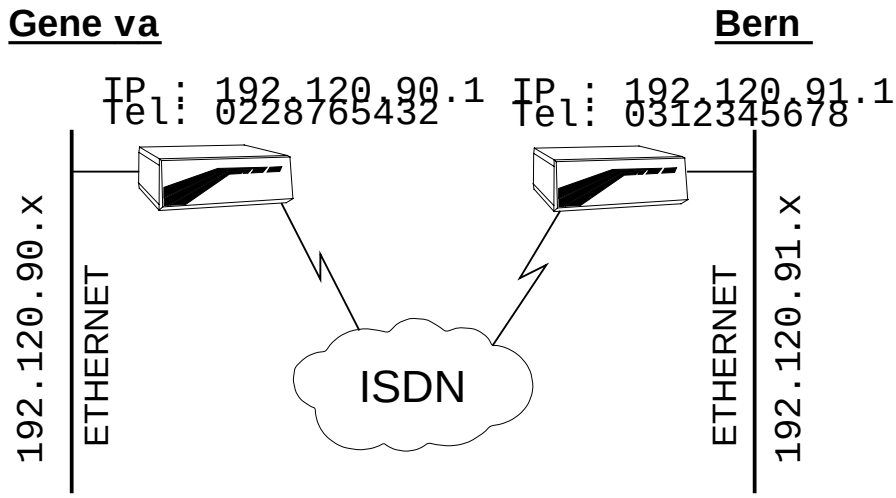


Figure 11 IP: Point-to-Point configuration

CONFIG FILES

17.1.3

On the following pages you will find the config files.

In *Italic*, the sections corresponding to the ISDN options.
In **bold**, the section corresponding to the IP options.

- Geneva config file: page 316
- Bern config file: page 317

```
# Geneva config for IP point to point example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Geneva
Site Select Geneva
IP Range 192.120.90.1 .. 192.120.90.254 Add

# --- Remote site
Site Rename ISDN Bern
Site Modify Bern WanProtocol PPP
Site Select Bern
ISDN Auto On
ISDN BChannel 2
ISDN IdleCloseTime 90
ISDN RemoteNumber 0312345678
ISDN NumberEnabled 0312345678
IP Range 192.120.91.1 .. 192.120.91.254 Add


# --- Bridge and Routers activation
IP Router On
```

```
# Bern config for IP point to point example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern
Site Select Bern
IP Range 192.120.91.1 .. 192.120.91.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 2
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IP Range 192.120.90.1 .. 192.120.90.254 Add


# --- Bridge and Routers activation
IP Router On
```

IP: MULTI-POINT 17.2

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket				Geneva MultiCom only			
Classic							
LAC							

This is a more advanced example using multi-point.

DESCRIPTION 17.2.1

A company has a central office in Geneva and two branches in Bern and Zurich. It wishes to connect their Local Area Networks (LANs) in routing mode.

- All sites use the TCP/IP protocol.
- Each link will be allowed 1 B-channel (64 kbits/s).

Following is the network layout and the configuration files for each site.

NETWORK DIAGRAM

17.2.2

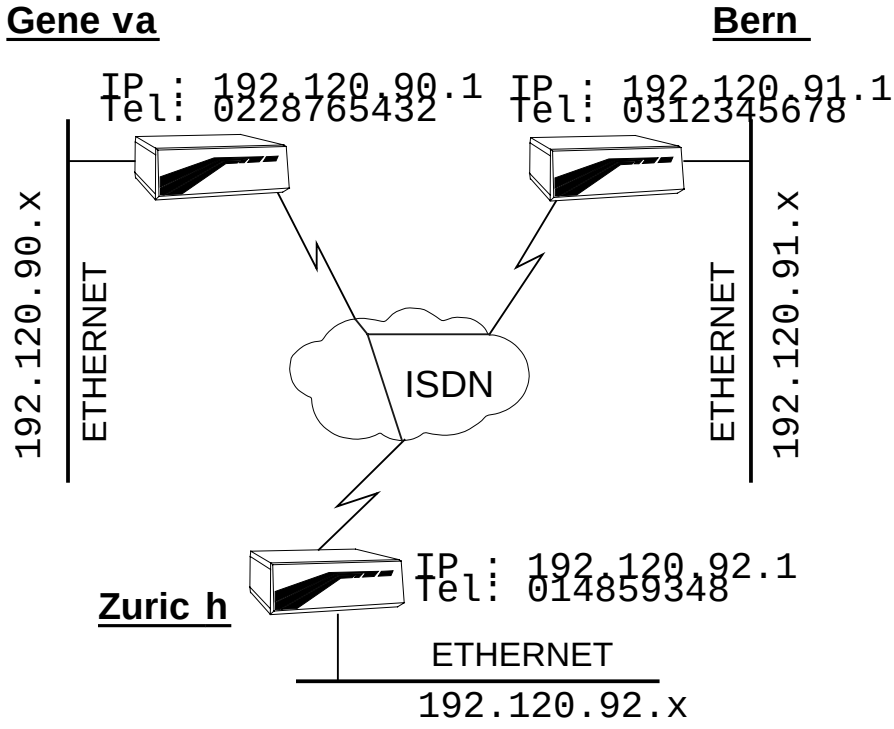


Figure 12 IP: Multi-point configuration

CONFIG FILES

17.2.3

On the following pages you will find the config files.

In **`bold,`** the section corresponding to the multi-point option.

- Geneva config file: page 320
- Bern config file: page 321
- Zurich config file: page 322

NOTES

17.2.3.1

- The traffic between Bern and Zurich goes through Geneva, which may cause high telephone bills. You can avoid this by having three Multi-point ***Multi-Com***s, each configured to route directly to the remote site.

```
# Geneva config for IP multi-point example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Geneva
Site Select Geneva
IP Range 192.120.90.1 .. 192.120.90.254 Add

# --- Remote site Bern
Site Rename ISDN Bern
Site Modify Bern WanProtocol PPP
Site Select Bern
ISDN Auto On
ISDN BChannel 1
ISDN IdleCloseTime 90
ISDN RemoteNumber 0312345678
ISDN NumberEnabled 0312345678
IP Range 192.120.91.1 .. 192.120.91.254 Add

# --- Remote site Zurich
Site Create Zurich PPP
Site Select Zurich
ISDN Auto On
ISDN BChannel 1
ISDN IdleCloseTime 90
ISDN RemoteNumber 014859348
ISDN NumberEnabled 014859348
IP Range 192.120.92.1 .. 192.120.92.254 Add


# --- Bridge and Routers activation
IP Router On
```

```
# Bern config for IP multi-point example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern
Site Select Bern
IP Range 192.120.91.1 .. 192.120.91.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 1
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IP Range 192.120.90.1 .. 192.120.90.254 Add
IP Range 192.120.92.1 .. 192.120.92.254 Add


# --- Bridge and Routers activation
IP Router On
```

```
# Zurich config for IP multi-point example.

# --- General information
MyName Zurich
IP MyAddr 192.120.92.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 014859348
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Zurich
Site Select Zurich
IP Range 192.120.92.1 .. 192.120.92.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 1
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IP Range 192.120.90.1 .. 192.120.91.254 Add


# --- Bridge and Routers activation
IP Router On
```

IPX: POINT-TO-POINT 17.3

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

DESCRIPTION 17.3.1

A company has two offices in Geneva and Bern. It wishes to connect their local area networks in routing mode.

- Each side uses the Novell™ IPX protocol.
- The link will be allowed 2 B-Channels (128 kbits/s).

Following is the network layout and the configuration files for each site.

NETWORK DIAGRAM 17.3.2

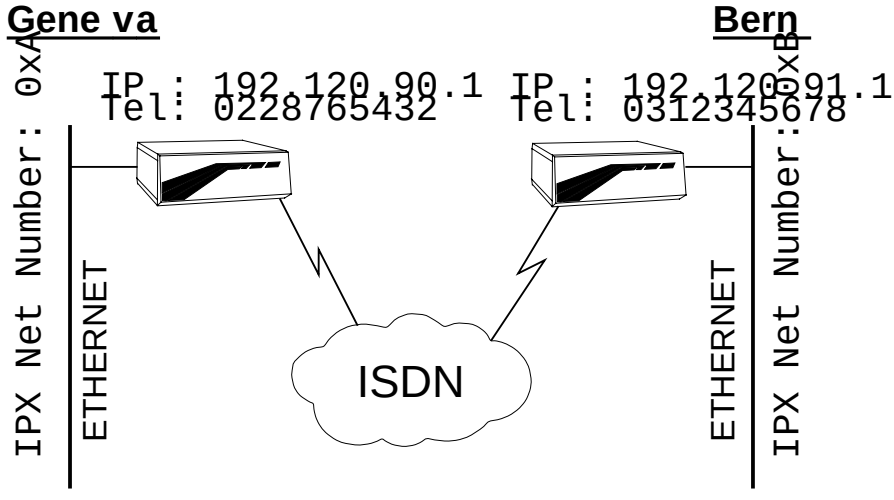


Figure 13 IPX: Point-to-Point configuration.

CONFIG FILES 17.3.3

On the following pages you will find the config files.

In **bold,** the section corresponding to the IPX options.

- Geneva config file: page 325
- Bern config file: page 326

NOTES 17.3.3.1

- The NetNumber must be given in hexadecimal format with a leading “0x” (zero-x) (i.e. 0xA is the “a” hexadecimal value = “10” in decimal). See § 14.18.39, "IPX NetNumber" on page 161 for more details.
- The “DemandWAN” site type is not explicitly set because it is the default value (see § 14.18.43, "IPX SiteType" on page 167).
- The Ethernet frame type is not set to 802.2 because it is the default value (see § 14.18.36, "IPX EthType" on page 157).
- All spoofing features are `On` by default (see § 14.18.44, "IPX Spoofing" on page 169).
- An IP number is assigned to the ***MultiCom*** because it is mandatory and to allow remote management through TCP/IP.

CAUTION — When configuring the NetNumber, do not confuse the Internal Net Number of your Novell™ server and the Cable or Ethernet Network Number. You must use the Cable Network Number! This number may be found in the server configuration.

```
# Geneva config for IPX point to point example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Geneva
Site Select Geneva
IPX NetNumber 0xA
IPX Site On

# --- Remote site
Site Rename ISDN Bern
Site Modify Bern WanProtocol PPP
Site Select Bern
ISDN Auto On
ISDN BChannel 1
ISDN IdleCloseTime 90
ISDN RemoteNumber 0312345678
ISDN NumberEnabled 0312345678
IPX NetNumber 0xB
IPX Site On


# --- Bridge and Routers activation
IPX Router On
```

```
# Bern config for IPX point to point example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern
Site Select Bern
IPX NetNumber 0xB
IPX Site On

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 1
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IPX NetNumber 0xA
IPX Site On


# --- Bridge and Routers activation
IPX Router On
```

IPX: MULTI-POINT 17.4

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

DESCRIPTION 17.4.1

A company has three offices in Geneva, Bern and Zurich. It wishes to connect their local area networks in routing mode.

- All sites use the Novell™ IPX protocol.
- Each link will be allowed 1 B-channel (64 kbits/s).
- The Zurich office uses the 802.3 Ethernet frame type.
- The Geneva-Bern link is considered by the company as more critical, it will be allowed 2 B-channels (128 kbits/s).

Following is the network layout and the configuration files for each site.

NETWORK DIAGRAM

17.4.2

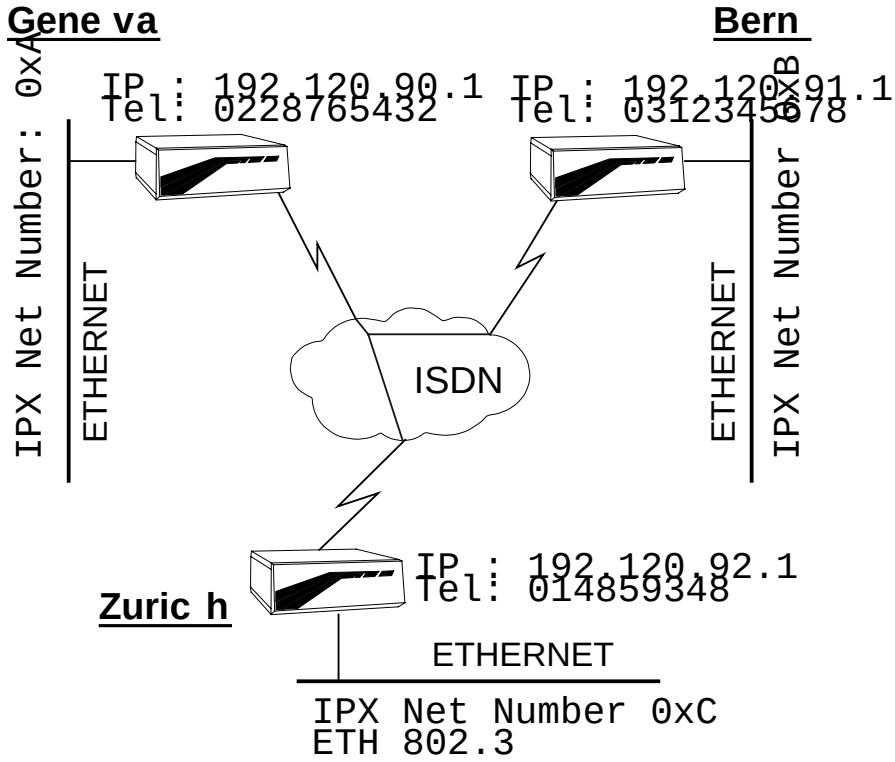


Figure 14 IPX: Multi-point configuration

CONFIG FILES

17.4.3

On the following pages you will find the config files.

In **`bold,`** the section corresponding to the IPX options.

- Geneva config file: page 330
- Bern config file: page 331
- Zurich config file: page 332

NOTES

17.4.3.1

- IPX supports looped networks.
- The NetNumber must be given in hexadecimal format with a leading “0x” (zero-x) (i.e. 0xA is the “a” hexadecimal value = “10” in decimal). See § 14.18.39, "IPX NetNumber" on page 161 for more details.

- The “DemandWAN” site type is not explicitly set because it is the default value (see § 14.18.43, "IPX SiteType" on page 167).
- The Ethernet frame type is not set to 802.2 because it is the default value (see § 14.18.36, "IPX EthType" on page 157).
- All spoofing features are `On` by default (see § 14.18.44, "IPX Spoofing" on page 169).
- An IP number is assigned to the ***MultiCom*** because it is mandatory and to allow remote management through TCP/IP.

CAUTION — When configuring the NetNumber, do not confuse the Internal Net Number of your Novell™ server and the Cable or Ethernet Network Number. You must use the Cable Network Number! This number may be found in the server configuration.

```
# Geneva config for IPX multi-point example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Geneva
Site Select Geneva
IPX NetNumber 0xA
IPX Site On

# --- Remote site Bern
Site Rename ISDN Bern
Site Modify Bern WanProtocol PPP
Site Select Bern
ISDN Auto On
ISDN BChannel 2
ISDN IdleCloseTime 90
ISDN RemoteNumber 0312345678
ISDN NumberEnabled 0312345678
IPX NetNumber 0xB
IPX Site On

# --- Remote site Zurich
Site Create Zurich PPP
Site Select Zurich
ISDN Auto On
ISDN BChannel 1
ISDN IdleCloseTime 90
ISDN RemoteNumber 014859348
ISDN NumberEnabled 014859348
ISDN BChannel 1
ISDN Auto On
ISDN IdleCloseTime 300
IPX NetNumber 0xC
IPX Site On

# --- Bridge and Routers activation
IPX Router On
```

```
# Bern config for IPX multi-point example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern
Site Select Bern
IPX NetNumber 0xB
IPX Site On

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 2
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IPX NetNumber 0xA
IPX Site On


# --- Bridge and Routers activation
IPX Router On
```

```
# Zurich config for IPX multi-point example.

# --- General information
MyName Zurich
IP MyAddr 192.120.92.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 014859348
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Zurich
Site Select Zurich
IPX NetNumber 0xC
IPX EthType 802.3
IPX Site On

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 1
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IPX NetNumber 0xA
IPX Site On


# --- Bridge and Routers activation
IPX Router On
```

BRIDGE: BASIC 17.5

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This examples describes how to configure a simple LAN to LAN bridge for an AppleTalk network.

DESCRIPTION 17.5.1

A company has two offices in Geneva and Bern. It wishes to connect their local area networks in bridging mode for the AppleTalk™ protocol.

Following is the network layout and the configuration files for each site.

CAUTION — Using a bridge in a dial-up ISDN configuration may lead to high telephone bills due to broadcast traffic. Therefore, a semipermanent line will be used (see § 14.18.56, "ISDN Leased" on page 187)

NETWORK DIAGRAM

17.5.2

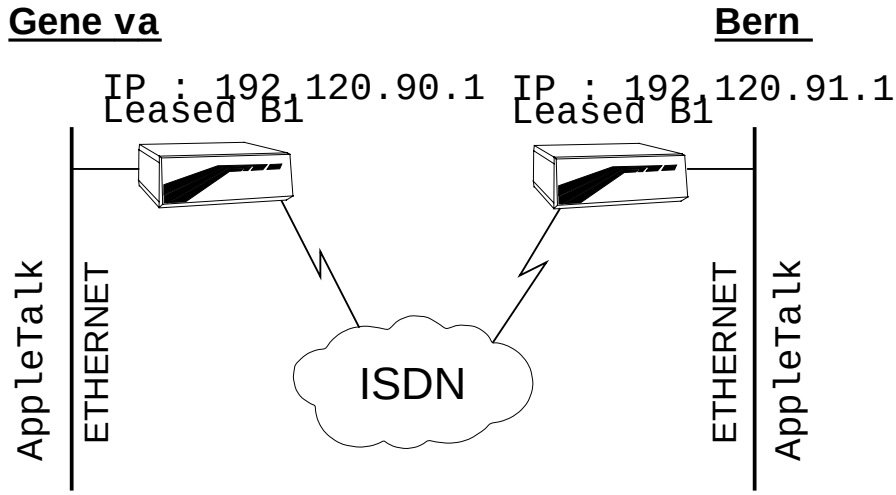


Figure 15 Bridging: Basic configuration

CONFIG FILES 17.5.3

On the following pages you will find the config files.

In *italic*, the sections corresponding to the Leased-ISDN option.
In **bold,** the section corresponding to the bridge.

- Geneva config file: page 336
- Bern config file: page 337

NOTES 17.5.3.1

- There is no “deny all” and then “allow something”. The line “allow something” is sufficient to deny the rest of the traffic.

```
# Geneva config for Basic bridging example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Geneva

# --- Remote site
Site Rename ISDN Bern
Site Modify Bern WanProtocol PPP
Site Select Bern
ISDN Leased B1


# --- Bridge
Bridge Create Group AppleGroup
Bridge Group AppleGroup Assign-site Geneva
Bridge Group AppleGroup Assign-site Bern

Bridge Create Filter AppleFilter
Bridge Filter AppleFilter Permit AppleTalk
Bridge Filter AppleFilter Assign Group AppleGroup


# --- Bridge and Routers activation
Bridge On
```

```
# Bern config for Basic bridging example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Leased B1


# --- Bridge
Bridge Create Group AppleGroup
Bridge Group AppleGroup Assign-site Geneva
Bridge Group AppleGroup Assign-site Bern

Bridge Create Filter AppleFilter
Bridge Filter AppleFilter Permit AppleTalk
Bridge Filter AppleFilter Assign Group AppleGroup


# --- Bridge and Routers activation
Bridge On
```

BRIDGE: ADVANCED 17.6

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket				Geneva MultiCom only			
Classic							
LAC							

This examples describes how to configure a LAN to LAN bridge for two AppleTalk networks and two IPX networks.

DESCRIPTION 17.6.1

A company has a central offices in Geneva, and two branches in Bern and Zurich. It wishes to connect their Local Area Networks in bridging mode.

- Geneva uses the Novell™ IPX protocol and the AppleTalk™ protocol.
- One machine in Geneva with Ethernet address `01:02:03:04:05:06` should not be seen on the other networks.
- Bern uses the AppleTalk™ protocol.
- Zurich uses the Novell™ IPX protocol.
- Each link will be allowed 1 B-Channel (64 kbits/s).

Following is the network layout, then the configuration tables that you need for configuring the ***MultiCom***s and finally the configuration files for each site.

NOTE - You will find empty tables for you own configurations in § 18.1, "Config check-list" on page 390.

CAUTION — Using a Bridge in a dial-up ISDN configuration may lead to high telephone bills due to the broadcast traffic.

NETWORK DIAGRAM

17.6.2

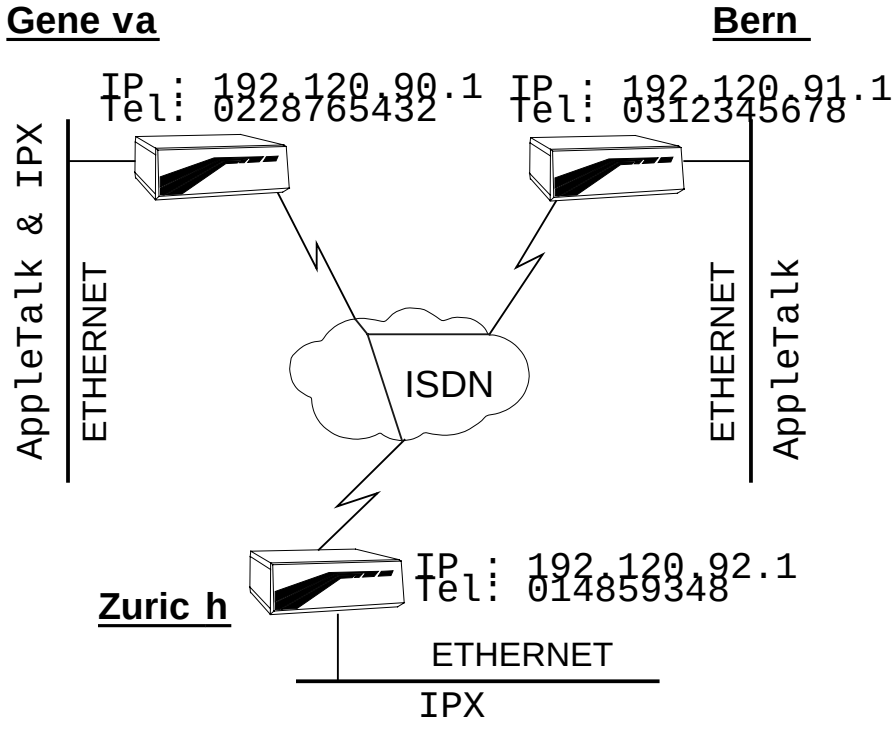


Figure 16 Bridging: Multi-Point configuration

CONFIG FILES

17.6.3

On the following pages you will find the config files.

In **bold,** the section corresponding to the bridge.

- Geneva config file: page 341
- Bern config file: page 343
- Zurich config file: page 344

```
# Geneva config for Advanced bridging example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Geneva

# --- Remote sites
Site Rename ISDN Bern
Site Select Bern
ISDN RemoteNumber 0312345678
ISDN NumberEnabled 0312345678
ISDN BChannel 1
ISDN Auto On
ISDN IdleCloseTime 300

Site Create Zurich
Site Select Zurich
ISDN RemoteNumber 014859348
ISDN NumberEnabled 014859348
ISDN BChannel 1
ISDN Auto On
ISDN IdleCloseTime 300
MHDLC Mode Polling

# --- Bridge
Bridge create group ApIpxGroup
Bridge group ApIpxGroup assign-site Geneva
Bridge group ApIpxGroup assign-site Bern
Bridge group ApIpxGroup assign-site Zurich

Bridge create filter GenevaFilter
Bridge filter GenevaFilter permit AppleTalk
Bridge filter GenevaFilter permit ipx
Bridge filter GenevaFilter assign site-input Geneva

Bridge create filter BernFilter
Bridge filter BernFilter permit AppleTalk
Bridge filter BernFilter deny src_addr 0102.0304.0506 ffff.ffff.ffff
Bridge filter BernFilter assign site-output Bern
```

```
Bridge create filter ZurichFilter
Bridge filter ZurichFilter permit ipx
Bridge filter ZurichFilter assign site-output Zurich


# --- Bridge and Routers activation
Bridge On
```

```
# Bern config for Advanced bridging example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern

# --- Remote site
Site Rename ISDN Geneva
Site Select Geneva
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
ISDN BChannel 2
ISDN Auto On
ISDN IdleCloseTime 300


# --- Bridge
Bridge create group AppleGroup
Bridge group AppleGroup assign-site Geneva
Bridge group AppleGroup assign-site Bern

Bridge create filter AppleFilter
Bridge filter AppleFilter permit AppleTalk
Bridge filter AppleFilter assign group AppleGroup


# --- Bridge and Routers activation
Bridge On
```

```
# Zurich config for Advanced bridging example.

# --- General information
MyName Zurich
IP MyAddr 192.120.92.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Zurich

# --- Remote site
Site Rename ISDN Geneva
Site Select Geneva
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
ISDN BChannel 2
ISDN Auto On
ISDN IdleCloseTime 300


# --- Bridge
Bridge create group IpxGroup
Bridge group IpxGroup assign-site Zurich
Bridge group IpxGroup assign-site Geneva

Bridge create filter IpxFilter
Bridge filter IpxFilter permit ipx
Bridge filter IpxFilter assign group IpxGroup


# --- Bridge and Routers activation
Bridge On
```

SERIAL: BASIC 17.7

V 1.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

DESCRIPTION 17.7.1

A company has two offices in Geneva and Bern. It wishes to connect their Local Area Networks in routing mode with a permanent leased line.

- Each side uses the TCP/IP protocol.
- The link is a 128 Kbits/s synchronous leased line.
- The modems use a V.35 interface.
- For security, CHAP authentication is used.

Following is the network layout and the configuration files for each site.

NETWORK DIAGRAM 17.7.2

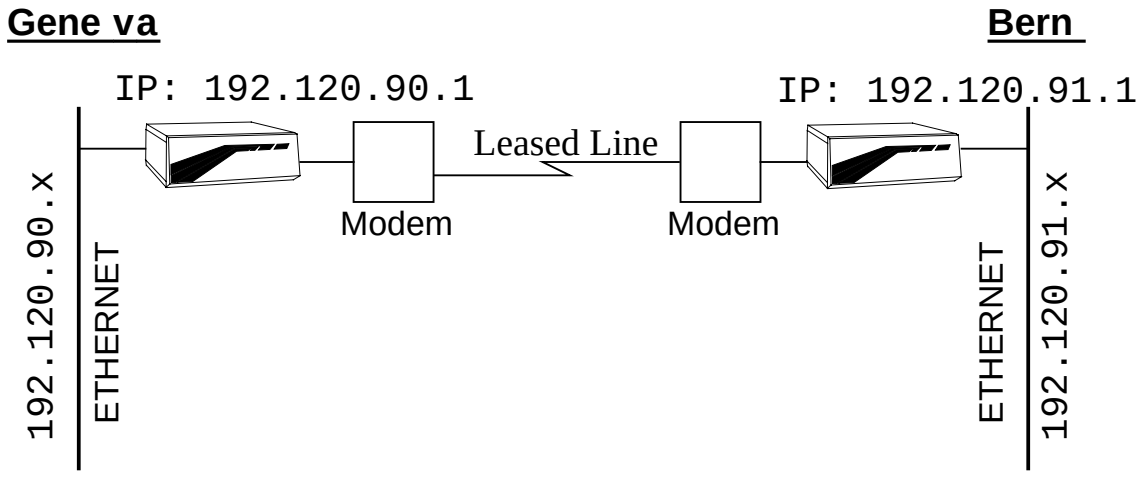


Figure 17 Serial: Point-to-point leased line.

CONFIG FILES

17.7.3

On the following pages you will find the config files.

In *italic*, the section corresponding to the authentication.
In **bold**, the section corresponding to the Serial options.

- Geneva config file: page 347
- Bern config file: page 348

```
# Geneva config for Serial example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0


# --- Local site
Site Rename ETH Geneva
Site Select Geneva
IP Range 192.120.90.1 .. 192.120.90.254 Add

# --- Remote site
Site Rename ISDN Bern
Site Modify Bern WanProtocol PPP
Site Select Bern
Serial Mode V35
Serial Speed 128K
Serial On
PPP Authentication CHAP
PPP Local Authentication UserID Geneva
PPP Local Authentication Password toto
PPP Remote Authentication UserID Bern
PPP Remote Authentication Password titi
IP Range 192.120.91.1 .. 192.120.91.254 Add


# --- Bridge and Routers activation
IP Router On
```

```
# Bern config for Serial example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0


# --- Local site
Site Rename ETH Bern
Site Select Bern
IP Range 192.120.91.1 .. 192.120.91.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
Serial Mode V35
Serial Speed 128K
Serial On
PPP Authentication CHAP
PPP Local Authentication UserID Bern
PPP Local Authentication Password titi
PPP Remote Authentication UserID Geneva
PPP Remote Authentication Password toto
IP Range 192.120.90.1 .. 192.120.90.254 Add


# --- Bridge and Routers activation
IP Router On
```

SERIAL: BACKUP AND OVERFLOW 17.8

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

DESCRIPTION 17.8.1

A company has two offices in Geneva and Bern. It wishes to connect reliably their Local Area Networks in routing mode.

- Each site uses the TCP/IP protocol.
- The link is a 128 Kbits/s analog leased line.
- The modems use a V.35 interface.
- Backup and overflow will be done on the ISDN line.

Following is the network layout and the configuration files for each site.

NETWORK DIAGRAM 17.8.2

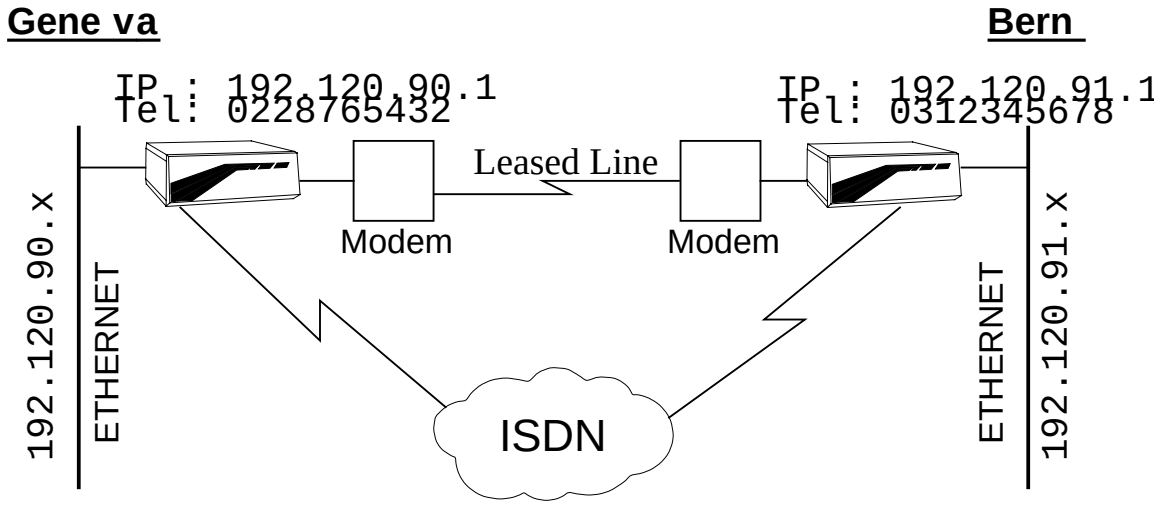


Figure 18 Serial: Point-to-point leased line with backup and overflow on ISDN.

CONFIG FILES 17.8.3

On the following pages you will find the config files.

In **bold,** the section corresponding to the Serial options.

- Geneva config file: page 351
- Bern config file: page 352

NOTES 17.8.3.1

- The overflow is allowed by the `ISDN Auto On` command which allows Bandwidth-on-Demand (BoD).
- Overflow means that if the traffic load is higher than 128 kbits/s, an ISDN line will be open. If the load is thereafter higher than 192 kbits/s (128 + 64), a second line will be opened.
- The backup is allowed by the `Backup On` command.
- Backup is activated as soon as an error is detected on the leased line link, either by the modem or by the link control protocol. Activation means opening one ISDN B-channel.

```
# Geneva config for Serial with backup & overflow example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Geneva
Site Select Geneva
IP Range 192.120.90.1 .. 192.120.90.254 Add

# --- Remote site
Site Rename ISDN Bern
Site Modify Bern WanProtocol PPP
Site Select Bern
ISDN Auto On
ISDN BChannel 2
ISDN IdleCloseTime 90
ISDN RemoteNumber 0312345678
ISDN NumberEnabled 0312345678
Serial Mode V35
Serial Speed 128K
Serial On
Backup On
IP Range 192.120.91.1 .. 192.120.91.254 Add


# --- Bridge and Routers activation
IP Router On
```

```
# Bern config for Serial with backup & overflow example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern
Site Select Bern
IP Range 192.120.91.1 .. 192.120.91.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 2
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
Serial Mode V35
Serial Speed 128K
Serial On
Backup On
IP Range 192.120.90.1 .. 192.120.90.254 Add


# --- Bridge and Routers activation
IP Router On
```

PPP: INTERNET ACCESS 17.9

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Basic Internet Access using PAT, DHCP, AutoDNS, MP and IP filtering.

DESCRIPTION 17.9.1

A company wishes to connect their Local Area Network to the Internet, using a Single Internet User Account provided by an Internet Service Provider.

Following is the network layout and the configuration file.

NETWORK DIAGRAM 17.9.2

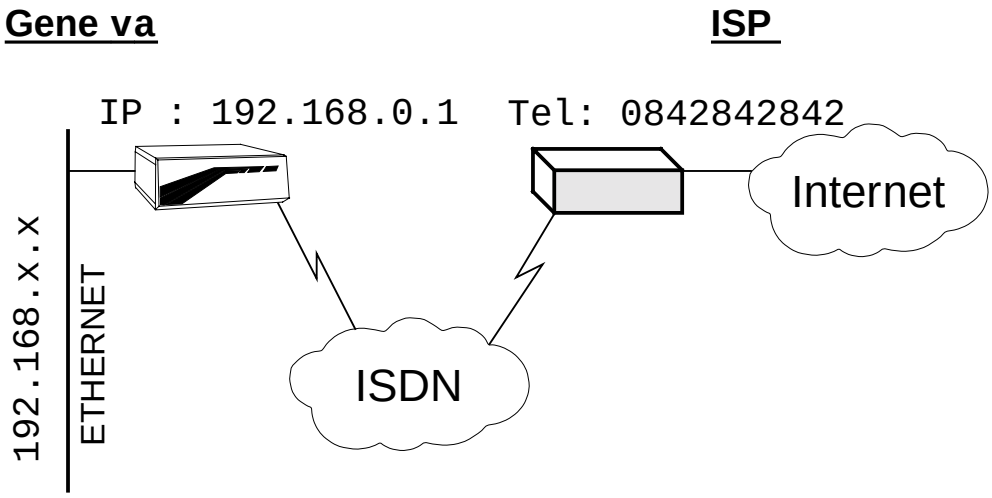


Figure 19 Internet Access using PAT, DHCP and AutoDNS

CONFIG FILES

17.9.3

On the following page you will find the config file.

In **`bold`**, the section corresponding to the new IP filtering and remapping.

- Geneva config file: page 355

NOTE - This configuration can be automatically generated by the built-in `Setup` command, the built-in Web-server or the EasyConfig Windows wizard.

NOTES

17.9.3.1

- All your computers must be in DHCP client mode
- If your Internet Service Provider (ISP) doesn't support DNS configuration through PPP, you'll have to specify them manually
- NetBIOS traffic will be filtered, to avoid unneeded ISDN connections
- The `ident` service (port 113) will be redirected to the ***MultiCom***, to avoid strange mail and ftp problems (see the FAQs on `http://www.lightning.ch/support/`)

```
# Geneva config for the Internet Access example.

# --- General information
MyName MultiCom
IP MyAddr 192.168.0.1
IP SubnetMask 255.255.0.0
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Local
Site Select Local
DHCP On
DHCP Range 192.168.0.2 .. 192.168.0.7 Add       # IP6
IP Range 192.168.0.2 .. 192.168.0.7 Add
#DHCP Range 192.168.0.2 .. 192.168.0.11 Add     # IP10
#IP Range 192.168.0.2 .. 192.168.0.11 Add
#DHCP Range 192.168.0.2 .. 192.168.255.254 Add  # unlimited IP
#IP Range 192.168.0.2 .. 192.168.255.254 Add

# --- Remote Site
Site Rename ISDN Internet
Site Select Internet
Site Modify Internet WANProtocol PPP
ISDN Auto On
#ISDN BChannel 2                          # If you want 128 Kbps
ISDN IdleCloseTime 90
ISDN RemoteNumber 0842842842
PPP Local Authentication None
PPP Remote Authentication Either
PPP Authentication Local UserID toto
PPP Authentication Local Password secret
PPP Authentication Remote UserID toto
PPP Authentication Remote Password secret
IP SiteAddr Dynamic
IP Translation Map 113/tcp to 192.168.0.1
IP Translation On
IP Range  1.0.0.0 ..   192.167.255.255 Add
IP Range 192.169.0.1 .. 255.255.255.254 Add

# --- NETBIOS Filter Configuration
IP Filter Deny from Any to Any Port 137 .. 139/udp
IP Filter Deny from Any to Any Port 137 .. 139/tcp
IP Filter Allow from Any to Any
IP Filter On
```

```
# --- Router activation
IP Router On


# --- DNS Section
DNS GetFrom Internet
#DNS Primary x.x.x.x                    # If AutoDNS is not
#DNS Secondary y.y.y.y                   # supported by your ISP
```

PPP: TELEWORKING 17.10

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This is another example using new PPP features.

DESCRIPTION 17.10.1

A company wishes to connect its employees to their Local Area Networks, so that they can work from home.

- All sites use the TCP/IP protocol.
- Callback will be used to centralize costs at the headquarters.
- Laptops in DHCP configuration will be able to move between home and work (this is possible thanks to the short DHCP LeaseTime).
- The range `192.120.90.200 .. 192.120.90.254` is reserved for these DHCP clients.

Following is the network layout and the configuration files for each site.

NETWORK DIAGRAM

17.10.2

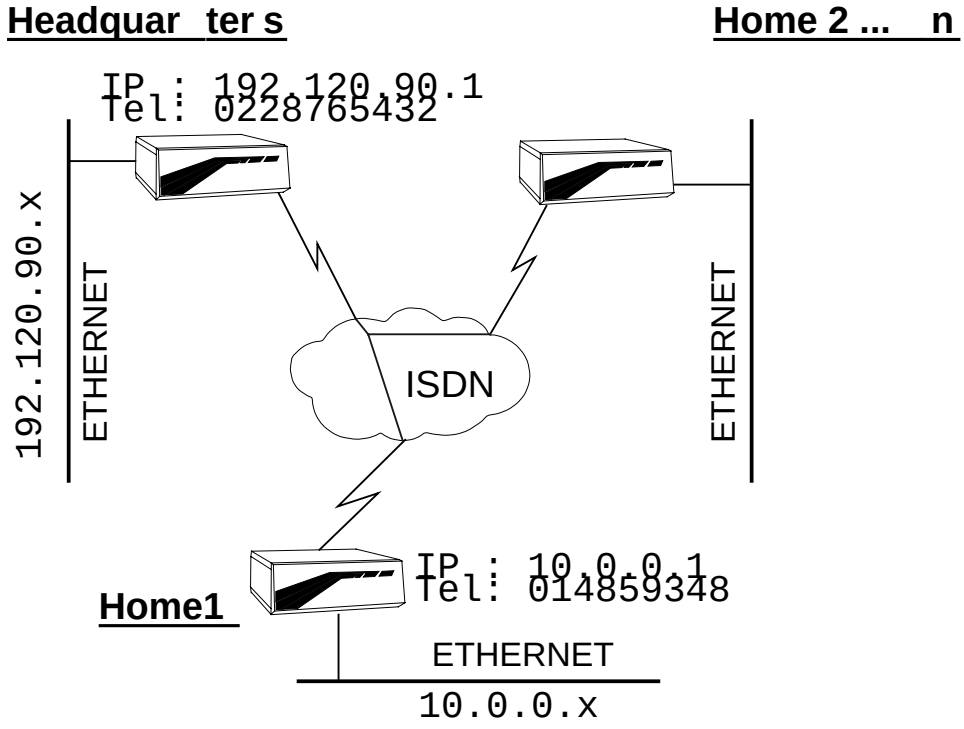


Figure 20 Teleworking example

CONFIG FILES

17.10.3

On the following pages you will find the config files.

In **bold** the section corresponding to the dynamic IP distribution.

- Headquarters: page 359
- Home: page 360

```
# Headquarters config for Teleworking example.

# --- General information
MyName Headquarters
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
IP DynamicRange 192.168.0.1 .. 192.168.0.254 Add
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Headquarters
Site Select Headquarters
DHCP On
DHCP Range 192.120.90.200 .. 192.120.90.254 Add
IP Range 192.120.90.1 .. 192.120.90.254 Add

# --- Remote site 1
Site Create Home1 PPP
Site Select Home1
ISDN BChannel 1
ISDN Callback On
ISDN IdleCloseTime 90
ISDN RemoteNumber 0312345678
ISDN NumberEnabled 0312345678
IP RemoteAddr Dynamic

# --- Remote site 2 .. n
# [...]


# --- Bridge and Routers activation
IP Router On
```

```
# Home config for Teleworking example.

# --- General information
MyName Home1
IP MyAddr 10.0.0.1
IP SubnetMask 255.0.0.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Home1
Site Select Home1
DHCP On
DHCP Range 10.0.0.2 .. 10.255.255.254 Add
IP Range 10.0.0.2 .. 10.255.255.254 Add

# --- Remote site
Site Create Headquarters PPP
Site Select Headquarters
ISDN Auto On
ISDN Callback Expect
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IP SiteAddr Dynamic
IP Translation On
IP Range  1.0.0.0 ..   9.255.255.255 Add
IP Range 11.0.0.0 .. 255.255.255.255 Add


# --- Bridge and Routers activation
IP Router On
```

IP TRANSLATION: SINGLE NAT 17.11

V 2.5	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

Internet access for a single machine without SecureWall™.

DESCRIPTION 17.11.1

A user wants to connect his single machine to the Internet, without SecureWall™ protection.

NETWORK DIAGRAM 17.11.2

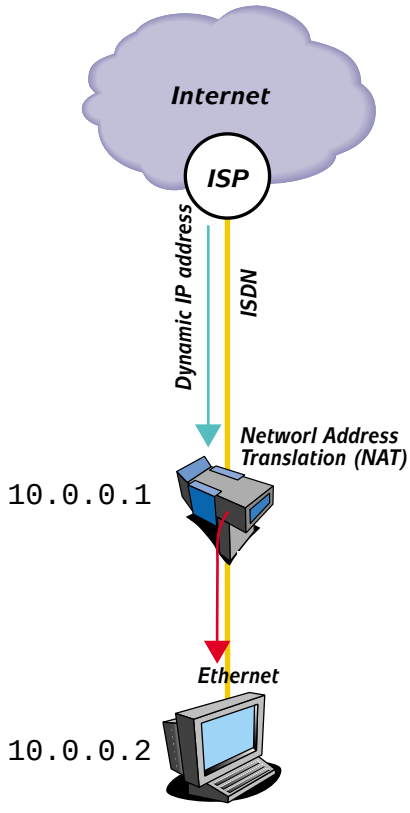


Figure 21 Internet access for a single machine without SecureWall™

CONFIG FILES

17.11.3

On the following page you will find the config file.

In **bold**, the section corresponding to the new IP Translation options.

• Geneva config file: page 363

CAUTION — Using NAT will disable the SecureWall™ on some machines, which can open a security hole in your network, from which other machines protected by the SecureWall™ may be attacked. Use it at your own risk!

```
# Geneva config for the single NAT example.

# --- General information
MyName MultiCom
IP MyAddr 10.0.0.1
IP SubnetMask 255.0.0.0
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Local
Site Select Local
IP Range 10.0.0.2 .. 10.0.0.2 Add

# --- Remote Site
Site Rename ISDN Internet
Site Select Internet
Site Modify Internet WANProtocol PPP
ISDN Auto On
ISDN RemoteNumber 0842842842
PPP Authentication Local UserID toto
PPP Authentication Local Password secret
PPP Authentication Remote UserID toto
PPP Authentication Remote Password secret
IP Range  1.0.0.0 ..   9.255.255.255 Add
IP Range 11.0.0.1 .. 255.255.255.254 Add
IP SiteAddr Dynamic MapTo 10.0.0.2
IP Translation On


# --- Bridge and Routers activation
IP Router On
```

IP TRANSLATION: MULTIPLE PAT/NAT 17.12

V 2.4	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This describes a complex configuration with two subnets and two servers accessing the Internet, using only four static IP addresses.

DESCRIPTION 17.12.1

A company wishes to connect their Local Area Networks to the Internet, using only four IP addresses given by their Internet Service Provider.

They have two separate subnets, whose machines they want to protect from Internet intruders and two dedicated servers, which they want to be fully accessible from the Internet.

Following is the network layout and the configuration file.

CAUTION — Using NAT will disable the SecureWall™ on some machines, which can open a security hole in your network, from which other machines protected by the SecureWall™ may be attacked. Use it at your own risk!

NETWORK DIAGRAM

17.12.2

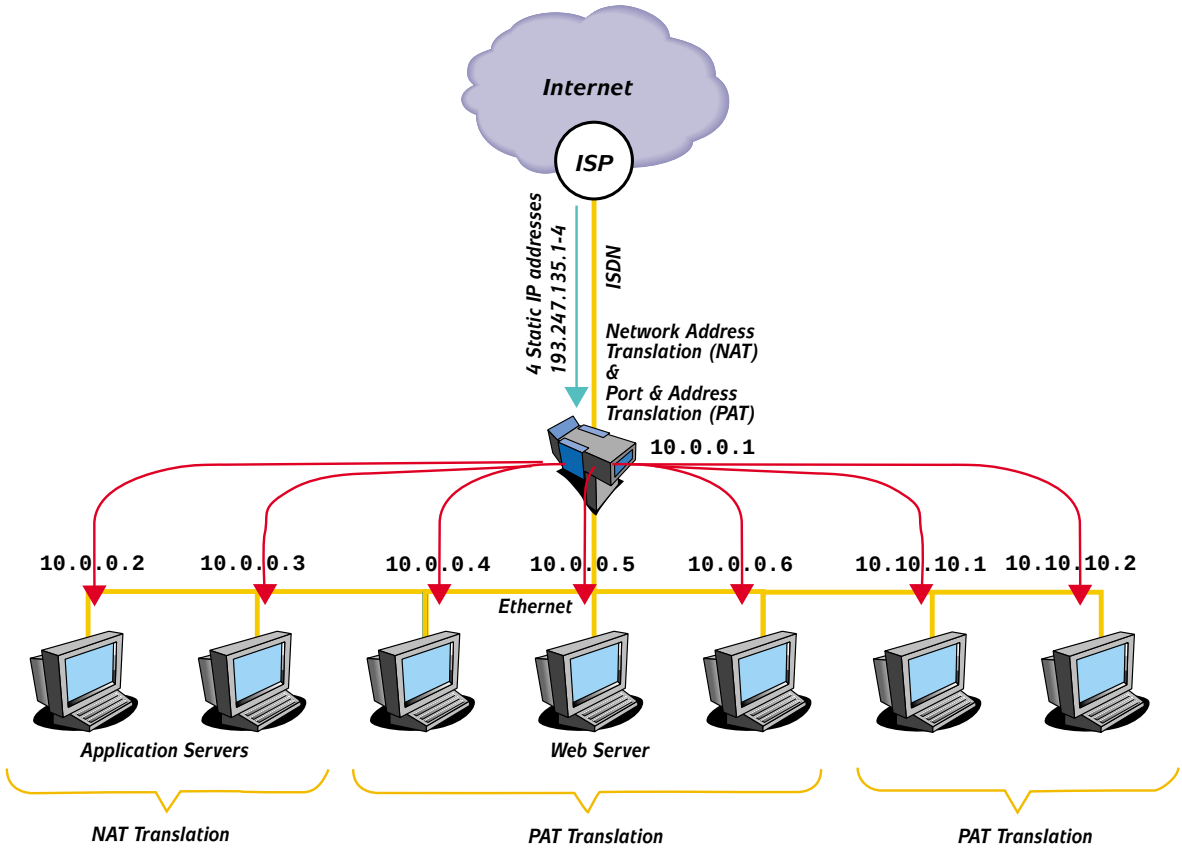


Figure 22 Internet Access using PAT, DHCP and AutoDNS

CONFIG FILES

17.12.3

On the following page you will find the config file.

In **bold**, the section corresponding to the new IP Translation options.

• Geneva config file: page 367

```
# Geneva config for the multiple PAT/NAT example.

# --- General information
MyName MultiCom
IP MyAddr 10.0.0.1
IP SubnetMask 255.0.0.0
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Local
Site Select Local
IP Range 10.0.0.2 .. 10.255.255.255 Add

# --- Remote Site
Site Rename ISDN Internet
Site Select Internet
Site Modify Internet WANProtocol PPP
ISDN Auto On
ISDN RemoteNumber 0842842842
PPP Authentication Local UserID toto
PPP Authentication Local Password secret
PPP Authentication Remote UserID toto
PPP Authentication Remote Password secret
IP Range  1.0.0.0 ..   9.255.255.255 Add
IP Range 11.0.0.1 .. 255.255.255.254 Add
IP SiteAddr 193.247.135.1 MapTo 10.0.0.2
IP SiteAddr 193.247.135.2 MapTo 10.0.0.3
IP SiteAddr 193.247.135.3 For 10.0.0.4 .. 10.0.0.6
IP SiteAddr 193.247.135.4 For 10.10.10.1 .. 10.10.10.2
IP Translation Map 193.247.135.3:80/tcp To 10.0.0.5
IP Translation On


# --- Bridge and Routers activation
IP Router On
```

ENCRYPTION: LINK-LEVEL 17.13

V 2.3	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This is an example using link-level encryption.

DESCRIPTION 17.13.1

A company has two offices in Geneva and Lausanne. It wishes to connect their Local Area Networks in routing mode, using link-level encryption, in order to transmit and receive data securely.

- All sites use the TCP/IP protocol.
- All sites transmit confidential data using the IDEA algorithm.
- The secret encryption key has already been introduced in both ***MultiCom*** with an interactive connection:

```
MultiCom:Key Create Secret Geneva_Lausanne_secret
Standard IDEA 128 bit key.
Encryption Key "Secret" registered.

MultiCom:Key Save Secret
Key "Secret" saved in Flash-EPROM.
```

Following is the network layout and the configuration files for each site.

NETWORK DIAGRAM

17.13.2

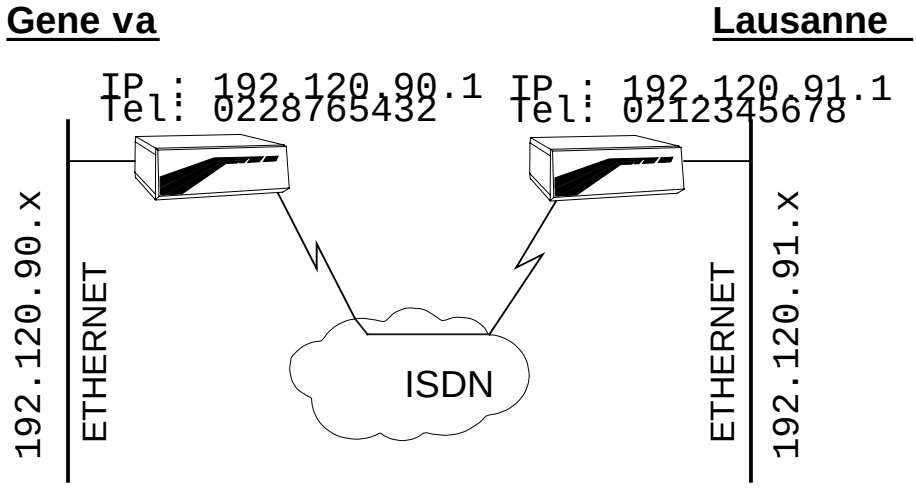


Figure 23 Link-level encryption

CONFIG FILES

17.13.3

On the following pages you will find the config files.

In **bold,** the section corresponding to the encryption options.

- Geneva config file: page 370
- Lausanne config file: page 371

```
# Geneva config for link encryption example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Geneva
Site Select Geneva
IP Range 192.120.90.1 .. 192.120.90.254 Add

# --- Remote site Bern
Site Rename ISDN Lausanne
Site Modify Lausanne WANProtocol PPP
Site Select Lausanne
ISDN Auto On
ISDN IdleCloseTime 90
ISDN RemoteNumber 0212345678
ISDN NumberEnabled 0212345678
PPP Encryption Key Secret
IP Range 192.120.91.1 .. 192.120.91.254 Add


# --- Bridge and Routers activation
IP Router On
```

```
# Lausanne config for link encryption example.

# --- General information
MyName Lausanne
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0212345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Lausanne
Site Select Lausanne
IP Range 192.120.91.1 .. 192.120.91.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WANProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
PPP Encryption Key Secret
IP Range 192.120.90.1 .. 192.120.90.254 Add


# --- Bridge and Routers activation
IP Router On
```

ENCRYPTION: IP-LEVEL 17.14

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

This is an example using multi-point and IP-level encryption.

DESCRIPTION 17.14.1

A company has three offices in Geneva, Bern and Zurich. It wishes to connect their Local Area Networks in routing mode, using IP-level encryption, in order to transmit and receive data securely.

- All sites use the TCP/IP protocol.
- Each link will be allowed 1 B-Channel (64 kbits/s).
- All sites transmit confidential data using the IDEA algorithm.
- The secret encryption keys have already been introduced in the corresponding ***MultiCom*** with an interactive connection:

```
MultiCom:Key Create KeyGE_BE Geneva_Bern_secret
Standard IDEA 128 bit key.
Encryption Key "KeyGE_BE" registered.

MultiCom:Key Save KeyGE_BE
Key "KeyGE_BE" saved in Flash-EPROM.
```

```
MultiCom:Key Create KeyGE_ZH Geneva_Zuerich_secret
Standard IDEA 128 bit key.
Encryption Key "KeyGE_ZH" registered.

MultiCom:Key Save KeyGE_ZH
Key "KeyGE_ZH" saved in Flash-EPROM.
```

Following is the network layout and the configuration files for each site.

NETWORK DIAGRAM 17.14.2

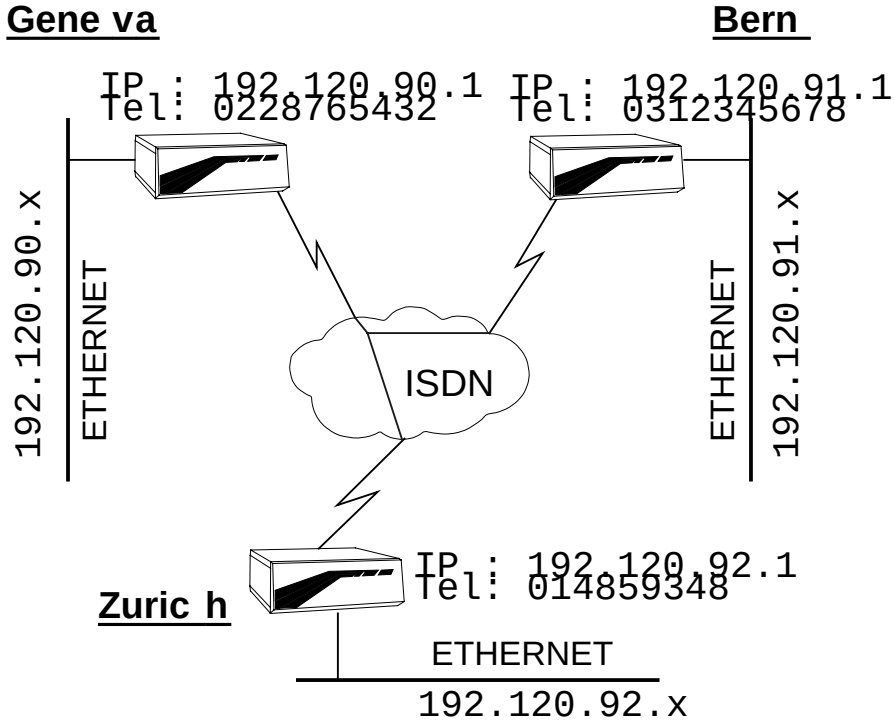


Figure 24 IP-level encryption

CONFIG FILES 17.14.3

On the following pages you will find the config files.

In **bold,** the section corresponding to the encryption options.

```
# Geneva config for Encryption multi-point example.

# --- General information
MyName Geneva
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Geneva
Site Select Geneva
IP Range 192.120.90.1 .. 192.120.90.254 Add

# --- Remote site Bern
Site Create Bern PPP
Site Select Bern
ISDN Auto On
ISDN IdleCloseTime 90
ISDN RemoteNumber 0312345678
ISDN NumberEnabled 0312345678
IP Range 192.120.91.1 .. 192.120.91.254 Add Encrypted KeyID KeyGE_BE

# --- Remote site Zurich
Site Create Zurich PPP
Site Select Zurich
ISDN Auto On
ISDN IdleCloseTime 90
ISDN RemoteNumber 014859348
ISDN NumberEnabled 014859348
IP Range 192.120.92.1 .. 192.120.92.254 Add Encrypted KeyID KeyGE_ZH


# --- Bridge and Routers activation
IP Router On
IP Router Encryption On
```

```
# Bern config for Encryption multi-point example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern
Site Select Bern
IP Range 192.120.91.1 .. 192.120.91.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WANProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IP Range 192.120.90.1 .. 192.120.90.254 Add Encrypted KeyID keyGE_BE


# --- Bridge and Routers activation
IP Router On
IP Router Encryption On
```

```
# Zurich config for Encryption multi-point example.

# --- General information
MyName Zurich
IP MyAddr 192.120.92.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 014859348
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Zurich
Site Select Zurich
IP Range 192.120.92.1 .. 192.120.92.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WANProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IP Range 192.120.90.1 .. 192.120.90.254 Add Encrypted KeyID keyGE_ZU


# --- Bridge and Routers activation
IP Router On
IP Router Encryption On
```

ENCRYPTION: ETHERNET-ETHERNET 17.15

V 2.1	IP	IPX	Bridge	MP	V36	SNMP	E
Pocket							
Classic							
LAC							

DESCRIPTION 17.15.1

A company has two offices linked like in the example § 17.1, "IP: Point-to-Point" on page 314. This company would like to encrypt the communication over their Wide-Area Network. But the manager don’t want to change the current network layout and the legacy routers can’t provide data encryption.

The purpose of this example is to add one ***MultiCom*** on each site and use them to encrypt and forward the data to the existing routers.

This solution allows data encryption on the WAN with a small modification of the network’s layout. Only a few changes in the configuration of the legacy routers and the modification of the gateway address of every client computers.

NETWORK DIAGRAM

17.15.2

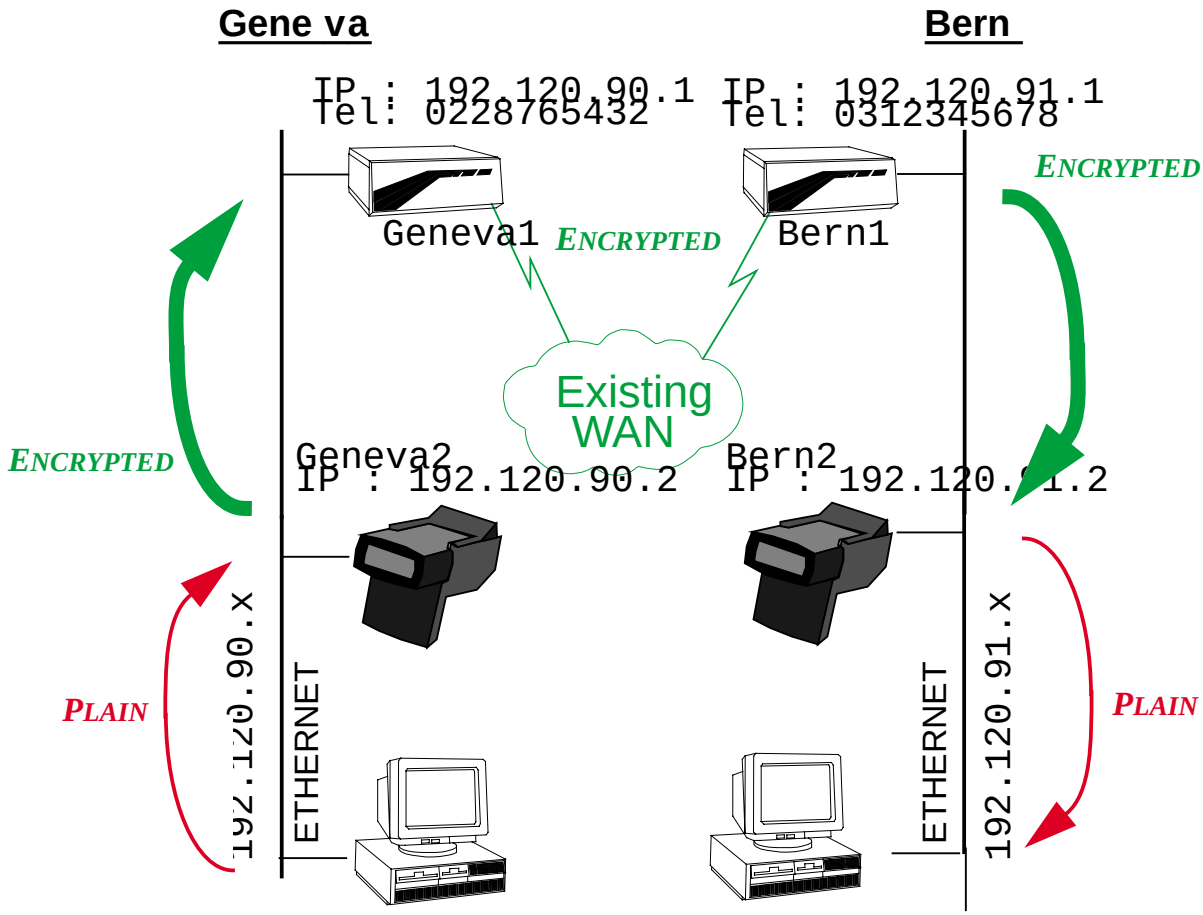


Figure 25 Encryption: Ethernet-Ethernet

PERFORMANCE

17.15.3

The Ethernet to Ethernet encryption may affect your bandwidth because of the two added routers. The next table show you the rate in Kbyte/s of an FTP transfer between the two sites with two channels opened (available bandwidth: 128 Kbps = 16 KByte/s) with a ***Pocket*** *Multi****Com*** or ***Classic*** *Multi****Com***. With a ***Multi****Com* ***LAN Access Center,*** the total performance is around 64 KByte/s = 512 Kbps.

Layout of the network	Rate [KByte/s]
2 *MultiCom*s without encryption	15
2 *MultiCom*s with encryption	14
4 *MultiCom*s without encryption	15
4 *MultiCom*s with encryption	14

It is interesting to see that Ethernet-Ethernet encryption is as efficient as direct encryption, for a 128 Kbps WAN link.

CONFIG FILES 17.15.4

On the following pages you will find the config files.

In **bold**, the sections corresponding to the changed part of the config (only for Geneva1 and Bern1).

- Geneva1 config file: page 380
- Geneva2 config file: page 381
- Bern1 config file: page 382
- Bern2 config file: page 383

```
# Geneva1 config for Ethernet-Ethernet encryption

# --- General information
MyName Geneva1
IP MyAddr 192.120.90.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0228765432
ISDN DChannelProtocol EuroISDN


# --- Sites
Site Select ETH
IP Range 192.120.90.2 .. 192.120.90.2 Add
IP Range 192.120.90.3 .. 192.120.90.254 RoutedTo 192.120.90.2


# --- Remote sites
Site Rename ISDN Bern
Site Modify Bern WANProtocol PPP
Site Select Bern
ISDN Auto On
ISDN BChannel 2
ISDN CloseTime 90
ISDN RemoteNumber 0312345678
ISDN NumberEnabled 0312345678
IP Range 192.120.91.1 .. 192.120.91.254 Add


# --- Bride and routers activation
IP Router On
```

```
# Geneva2 config for Ethernet-Ethernet encryption

# --- Required information
MyName Geneva2
IP MyAddr 192.120.90.2
IP SubnetMask 255.255.255.0


# --- Sites
Site Select ETH
IP Range 192.120.90.1 .. 192.120.90.254 Add
IP Range 192.120.91.1 .. 192.120.91.254 RoutedTo 192.120.90.1 Encrypted KeyID key


# --- Bride and routers activation
IP Router On
IP Router Encryption On
```

```
# Bern1 config for Ethernet-Ethernet encryption

# --- General information
MyName Bern1
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Sites
Site Select ETH
IP Range 192.120.91.2 .. 192.120.91.2 Add
IP Range 192.120.91.3 .. 192.120.91.254 RoutedTo 192.120.91.2


# --- Remote sites
Site Rename ISDN Geneva
Site Modify Geneva WANProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 2
ISDN CloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IP Range 192.120.90.1 .. 192.120.90.254 Add


# --- Bride and routers activation
IP Router On
```

```
# Bern2 config for Ethernet-Ethernet encryption

# --- Required information
MyName Bern2
IP MyAddr 192.120.91.2
IP SubnetMask 255.255.255.0


# --- Sites
Site Select ETH
IP Range 192.120.91.1 .. 192.120.91.254 Add
IP Range 192.120.90.1 .. 192.120.90.254 RoutedTo 192.120.91.1 Encrypted KeyID key


# --- Bride and routers activation
IP Router On
IP Router Encryption On
```

SNMP 17.16

V 2.1	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

DESCRIPTION 17.16.1

The same configuration as § 17.1, "IP: Point-to-Point" on page 314 is used.

A manager in Bern wants to manage the ***MultiCom*** on his network.

- The managing station is at address 192.120.92.7

CONFIG FILE 17.16.2

- Modified Bern config file: page 385.

NOTES 17.16.3

- You may also change the access rights of the “public” community by using:
  `SNMP Community public Write` (See § 14.18.124, "SNMP Community" on page 274)
- or remove the “public” community by using:
  `SNMP Community public Remove`
- You may add more managers by using several times the `SNMP Manager` command (See § 14.18.126, "SNMP Manager" on page 277).

```
# Bern config for SNMP example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern
Site Select Bern
IP Range 192.120.91.1 .. 192.120.91.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 2
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IP Range 192.120.90.1 .. 192.120.90.254 Add


# --- Bridge and Routers activation
IP Router On


# --- SNMP
SNMP Community Manager Write
SNMP Manager 192.120.91.7
```

DNS 17.17

V 2.0	IP	IPX	B	/M	/V36	/S	/E
Pocket							
Classic							
LAC							

DESCRIPTION 17.17.1

The same configuration as § 17.1, "IP: Point-to-Point" on page 314 is used.

A manager in Bern wants to be able to use Telnet from the Bern ***Multi**Com* with machine names. He must therefore configure DNS in this ***Multi**Com*.

- The DNS primary server is at address 193.5.2.161
- The DNS secondary server is at address 193.5.2.170

CONFIG FILE 17.17.2

- Modified Bern config file: page 387.

```
# Bern config for DNS example.

# --- General information
MyName Bern
IP MyAddr 192.120.91.1
IP SubnetMask 255.255.255.0
ISDN MyNumber 0312345678
ISDN DChannelProtocol EuroISDN


# --- Local site
Site Rename ETH Bern
Site Select Bern
IP Range 192.120.91.1 .. 192.120.91.254 Add

# --- Remote site
Site Rename ISDN Geneva
Site Modify Geneva WanProtocol PPP
Site Select Geneva
ISDN Auto On
ISDN BChannel 2
ISDN IdleCloseTime 90
ISDN RemoteNumber 0228765432
ISDN NumberEnabled 0228765432
IP Range 192.120.90.1 .. 192.120.90.254 Add


# --- Bridge and Routers activation
IP Router On


# --- DNS
DNS DomainName lightning.ch
DNS Primary 193.5.2.161
DNS Secondary 193.5.2.17
```

Chapter 18

Appendix

CONFIG CHECK-LIST 18.1

- ☐ *"Diagnose" command*
- ☐ *Power LED*
- ☐ *Terminal*
- ☐ *Cables*
- ☐ *Ethernet LED*
- ☐ *ISDN D LED*

CONFIGURATION: BASICS 18.1.1

- ☐ *IP Number*
- ☐ *Config file*
- ☐ *Boot.rpt*

CONFIGURATION: ISDN 18.1.2

- ☐ *Length of MSN*
- ☐ *Remote numbers*
- ☐ *Use of PBX*
- ☐ *ISDN loop back (internal)*
- ☐ *ISDN loop back (external)*
- ☐ *Site Select + Site Info*

- ☐ *ISDN Info*
- ☐ *PPP Info*

CONFIGURATION: IP HOST 18.1.3

- ☐ *Ping*
- ☐ *Telnet*

CONFIGURATION: OTHER SOFTWARE OPTIONS 18.1.4

- ☐ *Info Bridge*
- ☐ *Info IP*
- ☐ *Info IP Router*
- ☐ *Info IPX*

ISDN ERRORS 18.2

NORMAL CLASS 18.2.1

- **Cause #1 “unallocated (unassigned) number “**

  This cause indicates that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned (allocated)

- **Cause #2 “no route to specifies transit network”**

  This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognise. the equipment sending this cause does not recognise the transit network either because the transit network does not exist or because that particular transit network, while it does exist, dose not service the equipment which is sending this cause. This cause is supported on a network-dependent basis.

- **Cause #3 “no route to destination”**

  This cause indicates that the called user cannot be reached because the network through which the call has been routed does not serve the destination desired. This cause is supported on a network-dependent basis.

- **Cause #6 “channel unacceptable”**

  This cause indicates the channel most recently identified is not acceptable to the sending entity for use in this call.

- **Cause #7 “call awarded and being delivered in an established channel”**

  This cause indicates that the user has been awarded the incoming call, and that the incoming call is being connected to a channel already established to that user for a similar calls (e.g. packet-mode X.25 virtual calls).

- **Cause #10 “no channel available”**

  Indicates that the connection could not be established because there were no B-channels available. This is probably a temporary situation that will be resolved when one of the current calls is completed. (protocol 1TR6 only).

- **Cause #16 “normal call clearing”**

  This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared. Under normal situations, the source of this cause is not the network.

- **Cause #17 “user busy”**

  This cause is used when the called user has indicated the inability to accept another call. It is noted that the user equipment is compatible with the call.

- **Cause #18 “no user responding”**

  This cause is used when a user does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated (defined in ETS 300 102-1 by the expiry of either timer T303 or T310).

- **Cause #19 “no answer from user (user alerted)”**

  This cause is used when a user has provided an alerting indication but has not provided a connect indication within a prescribed period of time. Note: This cause is not necessarily generated by ETS 300 102-1 procedures but may be generated by internal network timers.

- **Cause #20 “Subscriber absent”**

  This cause indicates that the remote subscriber is absent. (protocol SwissNet only ?).

- **Cause #21 “call rejected”**

  This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible.

- **Cause #22 “number changed”**

  This cause is returned to a calling user when the called party number indicated by the calling user is no longer assigned. The new called party number may optionally be included in the diagnostic field. if a network does not support this capability cause #1 “unallocated (unassigned) number” shall be used.

- **Cause #26 “non selected user clearing”**

  This cause indicates that the user has not been awarded the incoming call.

- **Cause #27 “destination out of order”**

  This cause indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly.

The term “not functioning correctly” indicates that a signalling message was unable to be delivered to the remote user; e.g. a physical layer or data link layer failure at the remote user, user equipment off-line, etc.

- **Cause #28 “invalid format (address incomplete)”**

  This cause indicates that he called user cannot be reached because the called party number is not in a valid format or is not complete.

- **Cause #29 “facility rejected”**

  This cause is returned when a facility requested by the user cannot be provided by the network.

- **Cause #30 “response to status enquiry”**

  This cause is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message.

- **Cause #31 “normal, unspecified”**

  This cause is used to report a normal event only when no other cause in the normal class applies.

- **Cause #32 “Outgoing calls barred”**

  Indicates that the network is unable to handle outgoing calls. This may be a switch configuration problem. (protocol 1TR6 only).

- **Cause #33 “User access busy”**

  Indicates that the destination was unable to accept or acknowledge the call because the access was in use. (protocol 1TR6 only).

RESOURCE UNAVAILABLE CLASS 18.2.2

- **Cause #34 “no circuit/channel available”**

  This cause indicates that there is no appropriate circuit/channel presently available to handle the call.

- **Cause #35 “Non existent Closed User Groug”**

  Indicates that the network rejected a connection request from a non-existent closed user group (CUG). (protocol 1TR6 only).

- **Cause #36 “(user) out of order”**

  Indicates that the user is out of order. (protocol ??? only).

- **Cause #37 “Communication relation as semi-permanent connection not alowed”**

  Indicates that the network refused a request to open a “semi-permanent” connection. (protocol 1TR6 only).

- **Cause #38 “network out of order”**

  This cause indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time; e.g. immediately reattempting the call is not likely to be successful.

- **Cause #41 “temporary failure”**

  This cause indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time; e.g. the user may wish to try another call attempt almost immediately.

- **Cause #42 “switching equipment congestion”**

  This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.

- **Cause #43 “access information discarded”**

  This cause indicates that the network could not deliver access information to the remote user as requested; i.e. a user-to-user information, low layer compatibility, high layer compatibility, or subaddress as indicated in the diagnostic. It is noted that the particular type of access information discarded is optionally included in the diagnostic.

- **Cause #44 “requested circuit/channel not available”**

  This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.

- **Cause #47 “resource unavailable, unspecified”**

  This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.

- **Cause #49 “quality of service not available”**

  This cause is used to report that the requested quality of service, as defined in CCITT Recommendation X.213, cannot be provided, (e.g. throughput or transit delay cannot be supported).

- **Cause #50 “requested facility not subscribed”**

  This cause indicates that the requested supplementary service could not be provided by the network because the user has not completed the necessary administrative arrangements with its supporting network.

- **Cause #52 “Outgoing calls barred”**

  This cause indicated that the network is unable to handle outgoing calls. This may be a switch configuration problem. (protocol AT&T 5ESS 5e5 only).

- **Cause #53 “Destination not obtainable”**

  Indicates that the destination could not be reached for an unspecified reason. This may be a configuration or a subscription problem. (protocol 1TR6 only).

- **Cause #54 “Incoming calls barred”**

  This cause indicated that the network is unable to handle incoming calls. This may be a switch configuration problem. (protocol AT&T 5ESS 5e5 only).

- **Cause #56 “Number changed”**

  Indicates that the ISDN number used to set up the call is no longer assigned to any system. If an alternate address has been assigned to the called equipment, this may be returned in the diagnostic field of this message. (protocol 1TR6 only).

- **Cause #57 “bearer capability not authorised”**

  This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but the user is not authorised to use.

- **Cause #58 “bearer capability not presently available”**

  This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but which is not available at this time.

- **Cause #59 “user busy”**

  Indicates that the called system has acknowledged the connection request, but is unable to accept the call because the B-channels are currently in use. (protocol 1TR6 only).

- **Cause #61 “incoming calls barred”**

  Indicates that the network is unable to handle incoming calls. This may be a switch configuration problem. (protocol 1TR6 only).

- **Cause #62 “call rejected”**

  Indicates that the destination was capable of accepting the call (was neither busy nor incompatible) but rejected the call for some other reason. (protocol 1TR6 only).

- **Cause #63 “service or option not available “unspecified”**

  This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.

SERVICE OR OPTION NOT IMPLEMENTED CLASS 18.2.3

- **Cause #65 “bearer capability not implemented”**

  This cause indicates that the equipment sending this cause does not support the bearer capability requested.

- **Cause #66 “channel type not implemented”**

  This cause indicates that the equipment sending this cause does not support the channel type requested.

- **Cause #69 “requested facility not implemented”**

  This cause indicates that the equipment sending this cause does not support the requested supplementary service.

- **Cause #70 “only restricted digital information bearer capability is available”**

  This cause indicates that one equipment has requested an unrestricted bearer service but that the equipment sending this cause only supports the restricted version of the requested bearer capability.

- **Cause #79 “service opinion not implemented, unspecified”**

  This cause is used to report a service or option not implemented event only when no other cause in the service or option not implemented class applies.

INVALID MESSAGE CLASS 18.2.4

- **Cause #81 “invalid call reference value”**

  This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user- network interface.

- **Cause #82 “identified channel does not exist”**

  This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if a user has subscribed to those channels on a primary rate interface num-

bered from 1 to 12 and the user equipment or the network attempts to use channels 13 through 23, this cause is generated.

- **Cause #83 “a suspended call exists, but this call identity does not”**

  This cause indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).

- **Cause #84 “call identity in use”**

  This cause indicates that the network has received a call suspend request. The call suspend request contained a call identity (including the null call identity) which is already in use for a suspended call within the domain of interfaces over which the call might be resumed.

- **Cause #85 “no call suspended”**

  This cause indicates that the network has received a call resume request. The call resume request contained a Call identity information element which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed. This cause may also indicate “invalid digit value for number”: Indicates that the connection could not be established because the destination address was presented in an unrecognized format or because the destination address was incomplete. (this meaning in protocol AT&T 5ESS 5e5 only).

- **Cause #86 “call having the requested call identity has been cleared”**

  This cause indicates that the network has received a call resume request. The call resume request contained a Call identity information element which once indicated a suspended call; however, that suspended call was cleared while suspended (either by network timeout or by the remote user).

- **Cause #87 “user not member of closed user group”**

  This cause indicates that the caller is not member of the closed user group (CUG) of the called party. (protocol SwissNet only ?).

- **Cause #88 “incompatible destination”**

  This cause indicates that the equipment sending this cause has received a request to establish a call which has low layer compatibility, high layer compatibility, or other compatibility attributes (e.g. data rate which cannot be accommodated.

- **Cause #89 “Network congestion”**

  Indicates that the destination could not be reached because the network switching equipment was temporarily overloaded. This is a transient problem that will be resolved after successive retries. (protocol 1TR6 only).

- **Cause #90 “Destination address missing or incomplete”**

  Indicates that destination address is missing or incomplete. (protocol ??? only). Cause #91 “invalid transit network selection” This cause indicates that a transit network identification was received which is of an incorrect format as defined in Annex C.

- **Cause #93 “Mandatory information element is missing”**

  Indicates that a mandatory information element is missing in a received frame.

- **Cause #95 “invalid message, unspecified”**

  This cause is used to report an invalid message event only when no other cause in the invalid message class applies.

PROTOCOL ERROR CLASS 18.2.5

- **Cause #96 “mandatory information element is missing”**

  This cause indicates that the equipment sending this cause has received a message which is missing an information element which must be present in the message before that message ca be processed.

- **Cause #97 “message type non-existent or not implemented”**

  This cause indicates that the equipment sending this cause has received a message with a message type it does recognise either because this is a message not defined or defined but not implemented by the equipment sending this cause.

- **Cause #98 “message not compatible with call state or message TYPE NON-EXISTENT OR NOT IMPLEMENTED”**

  This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.

- **Cause #99 “information element non-existent or not implemented”**

  This cause indicates that the equipment sending this cause has received a message which includes information elements not recognised because the information element identifier is not defined or it is defined but not implemented by the equipment sending the cause. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

- **Cause #100 “invalid information element contents”**

  This cause indicates that the equipment sending this cause has received an information element which it has implemented; however, one or more of the fields in the information element are coded in such a way which has not been implemented by the equipment sending this cause.

- **Cause #101 “message not compatible with call start”**

  This cause indicates that a message has been received which is incompatible with the call state.

- **Cause #102 “recovery on timer expiry”**

  This cause indicates that a procedure has been initiated by the expiry of a timer in association with ETS 300 102-1 error handling procedures.

- **Cause #103 “mandatory information element of uncorrect length”**

  This cause indicates that an information element was received with an invalid or urecognized length. D-channel error. (protocol VN3 only).

- **Cause #111 “protocol error, unspecified”**

  This cause is used to report a protocol error event only when no other cause in the protocol error class applies.

- **Cause #112 “local procedure error”**

  Indicates the occurrence of an unspecified error at the local end. D-channel error. If this error is returned sytematically, please report the occurrence to your authorized service provider. (protocol 1TR6 only).

- **Cause #113 “remote procedure error”**

  Indicates the occurrence of an unspecified error at the remote end. D-channel error. If this error is returned sytematically, please report the occurrence to your authorized service provider. (protocol 1TR6 only).

INTERWORKING CLASS 18.2.6

- **Cause #127 “interworking, unspecified”**

  This cause indicates that there has been interworking with a network which does not provide causes for actions it takes; thus, the precise cause for a message which is being sent cannot be ascertained.

INTERNAL LAYER 1 CLASS 18.2.7

- **Cause #200 “deactivation received”**

  This cause indicates a deactivated ISDN physical layer. This may be caused by a hardware cause, including an unpluged ISDN cord or a defective NT or missing termination resistors on the S bus.

ETHERNET NUMBERS 18.3

RFC 1700 Assigned Numbers October 1994

ETHER TYPES

The following list of EtherTypes is contributed unverified information from various sources.

Assignments:

Ethernet decimal	Hex	Exp. Ethernet decimal	octal	Description	References
000	0000-05DC	-	-	IEEE802.3 Length Field	[XEROX]
257	0101-01FF	-	-	Experimental	[XEROX]
512	0200	512	1000	XEROX PUP (see 0A00)	[8,XEROX]
513	0201	-	-	PUP Addr Trans (see 0A01)	[XEROX]
	0400			Nixdorf	[XEROX]
1536	0600	1536	3000	XEROX NS IDP	[133,XEROX]
	0660			DLOG	[XEROX]
	0661			DLOG	[XEROX]
2048	0800	513	1001	Internet IP (IPv4)	[105,JBP]
2049	0801	-	-	X.75 Internet	[XEROX]
2050	0802	-	-	NBS Internet	[XEROX]
2051	0803	-	-	ECMA Internet	[XEROX]
2052	0804	-	-	Chaosnet	[XEROX]
2053	0805	-	-	X.25 Level 3	[XEROX]
2054	0806	-	-	ARP	[88,JBP]
2055	0807	-	-	XNS Compatability	[XEROX]
2076	081C	-	-	Symbolics Private	[DCP1]
2184	0888-088A	-	-	Xyplex	[XEROX]
2304	0900	-	-	Ungermann-Bass net debugr	[XEROX]
2560	0A00	-	-	Xerox IEEE802.3 PUP	[XEROX]
2561	0A01	-	-	PUP Addr Trans	[XEROX]
2989	0BAD	-	-	Banyan Systems	[XEROX]
4096	1000	-	-	Berkeley Trailer nego	[XEROX]
4097	1001-100F	-	-	Berkeley Trailer encap/IP	[XEROX]
5632	1600	-	-	Valid Systems	[XEROX]
16962	4242	-	-	PCS Basic Block Protocol	[XEROX]
21000	5208	-	-	BBN Simnet	[XEROX]
24576	6000	-	-	DEC Unassigned (Exp.)	[XEROX]
24577	6001	-	-	DEC MOP Dump/Load	[XEROX]
24578	6002	-	-	DEC MOP Remote Console	[XEROX]
24579	6003	-	-	DEC DECNET Phase IV Route	[XEROX]
24580	6004	-	-	DEC LAT	[XEROX]
24581	6005	-	-	DEC Diagnostic Protocol	[XEROX]
24582	6006	-	-	DEC Customer Protocol	[XEROX]
24583	6007	-	-	DEC LAVC, SCA	[XEROX]
24584	6008-6009	-	-	DEC Unassigned	[XEROX]
24586	6010-6014	-	-	3Com Corporation	[XEROX]
28672	7000	-	-	Ungermann-Bass download	[XEROX]
28674	7002	-	-	Ungermann-Bass dia/loop	[XEROX]

28704	7020-7029	-	-	LRT	[XEROX]
28720	7030	-	-	Proteon	[XEROX]
28724	7034	-	-	Cabletron	[XEROX]
32771	8003	-	-	Cronus VLN	[131,DT15]
32772	8004	-	-	Cronus Direct	[131,DT15]
32773	8005	-	-	HP Probe	[XEROX]
32774	8006	-	-	Nestar	[XEROX]
32776	8008	-	-	AT&T	[XEROX]
32784	8010	-	-	Excelan	[XEROX]
32787	8013	-	-	SGI diagnostics	[AXC]
32788	8014	-	-	SGI network games	[AXC]
32789	8015	-	-	SGI reserved	[AXC]
32790	8016	-	-	SGI bounce server	[AXC]
32793	8019	-	-	Apollo Computers	[XEROX]
32815	802E	-	-	Tymshare	[XEROX]
32816	802F	-	-	Tigan, Inc.	[XEROX]
32821	8035	-	-	Reverse ARP	[48,JXM]
32822	8036	-	-	Aeonic Systems	[XEROX]
32824	8038	-	-	DEC LANBridge	[XEROX]
32825	8039-803C	-	-	DEC Unassigned	[XEROX]
32829	803D	-	-	DEC Ethernet Encryption	[XEROX]
32830	803E	-	-	DEC Unassigned	[XEROX]
32831	803F	-	-	DEC LAN Traffic Monitor	[XEROX]
32832	8040-8042	-	-	DEC Unassigned	[XEROX]
32836	8044	-	-	Planning Research Corp.	[XEROX]
32838	8046	-	-	AT&T	[XEROX]
32839	8047	-	-	AT&T	[XEROX]
32841	8049	-	-	ExperData	[XEROX]
32859	805B	-	-	Stanford V Kernel exp.	[XEROX]
32860	805C	-	-	Stanford V Kernel prod.	[XEROX]
32861	805D	-	-	Evans & Sutherland	[XEROX]
32864	8060	-	-	Little Machines	[XEROX]
32866	8062	-	-	Counterpoint Computers	[XEROX]
32869	8065	-	-	Univ. of Mass. @ Amherst	[XEROX]
32870	8066	-	-	Univ. of Mass. @ Amherst	[XEROX]
32871	8067	-	-	Veeco Integrated Auto.	[XEROX]
32872	8068	-	-	General Dynamics	[XEROX]
32873	8069	-	-	AT&T	[XEROX]
32874	806A	-	-	Autophon	[XEROX]
32876	806C	-	-	ComDesign	[XEROX]
32877	806D	-	-	Computgraphic Corp.	[XEROX]
32878	806E-8077	-	-	Landmark Graphics Corp.	[XEROX]
32890	807A	-	-	Matra	[XEROX]
32891	807B	-	-	Dansk Data Elektronik	[XEROX]
32892	807C	-	-	Merit Internodal	[HWB]
32893	807D-807F	-	-	Vitalink Communications	[XEROX]
32896	8080	-	-	Vitalink TransLAN III	[XEROX]
32897	8081-8083	-	-	Counterpoint Computers	[XEROX]
32923	809B	-	-	Appletalk	[XEROX]
32924	809C-809E	-	-	Datability	[XEROX]
32927	809F	-	-	Spider Systems Ltd.	[XEROX]
32931	80A3	-	-	Nixdorf Computers	[XEROX]
32932	80A4-80B3	-	-	Siemens Gammasonics Inc.	[XEROX]
32960	80C0-80C3	-	-	DCA Data Exchange Cluster	[XEROX]
	80C4			Banyan Systems	[XEROX]
	80C5			Banyan Systems	[XEROX]
32966	80C6	-	-	Pacer Software	[XEROX]
32967	80C7	-	-	Applitek Corporation	[XEROX]
32968	80C8-80CC	-	-	Intergraph Corporation	[XEROX]
32973	80CD-80CE	-	-	Harris Corporation	[XEROX]

32975	80CF-80D2	-	-	Taylor Instrument	[XEROX]
32979	80D3-80D4	-	-	Rosemount Corporation	[XEROX]
32981	80D5	-	-	IBM SNA Service on Ether	[XEROX]
32989	80DD	-	-	Varian Associates	[XEROX]
32990	80DE-80DF	-	-	Integrated Solutions TRFS	[XEROX]
32992	80E0-80E3	-	-	Allen-Bradley	[XEROX]
32996	80E4-80F0	-	-	Datability	[XEROX]
33010	80F2	-	-	Retix	[XEROX]
33011	80F3	-	-	AppleTalk AARP (Kinetics)	[XEROX]
33012	80F4-80F5	-	-	Kinetics	[XEROX]
33015	80F7	-	-	Apollo Computer	[XEROX]
33023	80FF-8103	-	-	Wellfleet Communications	[XEROX]
33031	8107-8109	-	-	Symbolics Private	[XEROX]
33072	8130	-	-	Hayes Microcomputers	[XEROX]
33073	8131	-	-	VG Laboratory Systems	[XEROX]
	8132-8136			Bridge Communications	[XEROX]
33079	8137-8138	-	-	Novell, Inc.	[XEROX]
33081	8139-813D	-	-	KTI	[XEROX]
	8148			Logicraft	[XEROX]
	8149			Network Computing Devices	[XEROX]
	814A			Alpha Micro	[XEROX]
33100	814C	-	-	SNMP	[JKR1]
	814D			BIIN	[XEROX]
	814E			BIIN	[XEROX]
	814F			Technically Elite Concept	[XEROX]
	8150			Rational Corp	[XEROX]
	8151-8153			Qualcomm	[XEROX]
	815C-815E			Computer Protocol Pty Ltd	[XEROX]
	8164-8166			Charles River Data System	[XEROX]
	817D-818C			Protocol Engines	[XEROX]
	818D			Motorola Computer	[XEROX]
	819A-81A3			Qualcomm	[XEROX]
	81A4			ARAI Bunkichi	[XEROX]
	81A5-81AE			RAD Network Devices	[XEROX]
	81B7-81B9			Xyplex	[XEROX]
	81CC-81D5			Apricot Computers	[XEROX]
	81D6-81DD			Artisoft	[XEROX]
	81E6-81EF			Polygon	[XEROX]
	81F0-81F2			Comsat Labs	[XEROX]
	81F3-81F5			SAIC	[XEROX]
	81F6-81F8			VG Analytical	[XEROX]
	8203-8205			Quantum Software	[XEROX]
	8221-8222			Ascom Banking Systems	[XEROX]
	823E-8240			Advanced Encryption Syste	[XEROX]
	827F-8282			Athena Programming	[XEROX]
	8263-826A			Charles River Data System	[XEROX]
	829A-829B			Inst Ind Info Tech	[XEROX]
	829C-82AB			Taurus Controls	[XEROX]
	82AC-8693			Walker Richer & Quinn	[XEROX]
	8694-869D			Idea Courier	[XEROX]
	869E-86A1			Computer Network Tech	[XEROX]
	86A3-86AC			Gateway Communications	[XEROX]
	86DB			SECTRA	[XEROX]
	86DE			Delta Controls	[XEROX]
34543	86DF	-	-	ATOMIC	[JBP]
	86E0-86EF			Landis & Gyr Powers	[XEROX]
	8700-8710			Motorola	[XEROX]
	8A96-8A97			Invisible Software	[XEROX]
36864	9000	-	-	Loopback	[XEROX]
36865	9001	-	-	3Com(Bridge) XNS Sys Mgmt	[XEROX]

```
36866   9002        -       -     3Com(Bridge) TCP-IP Sys  [XEROX]
36867   9003        -       -     3Com(Bridge) loop detect [XEROX]
65280   FF00        -       -     BBN VITAL-LanBridge cache[XEROX]
        FF00-FF0F                 ISC Bunker Ramo          [XEROX]
```

PLANNING WORK-SHEETS 18.4

On the following pages you will find empty planning work-sheets. These are the same work-sheets that are used in the examples.

NETWORK DIAGRAM

18.4.1

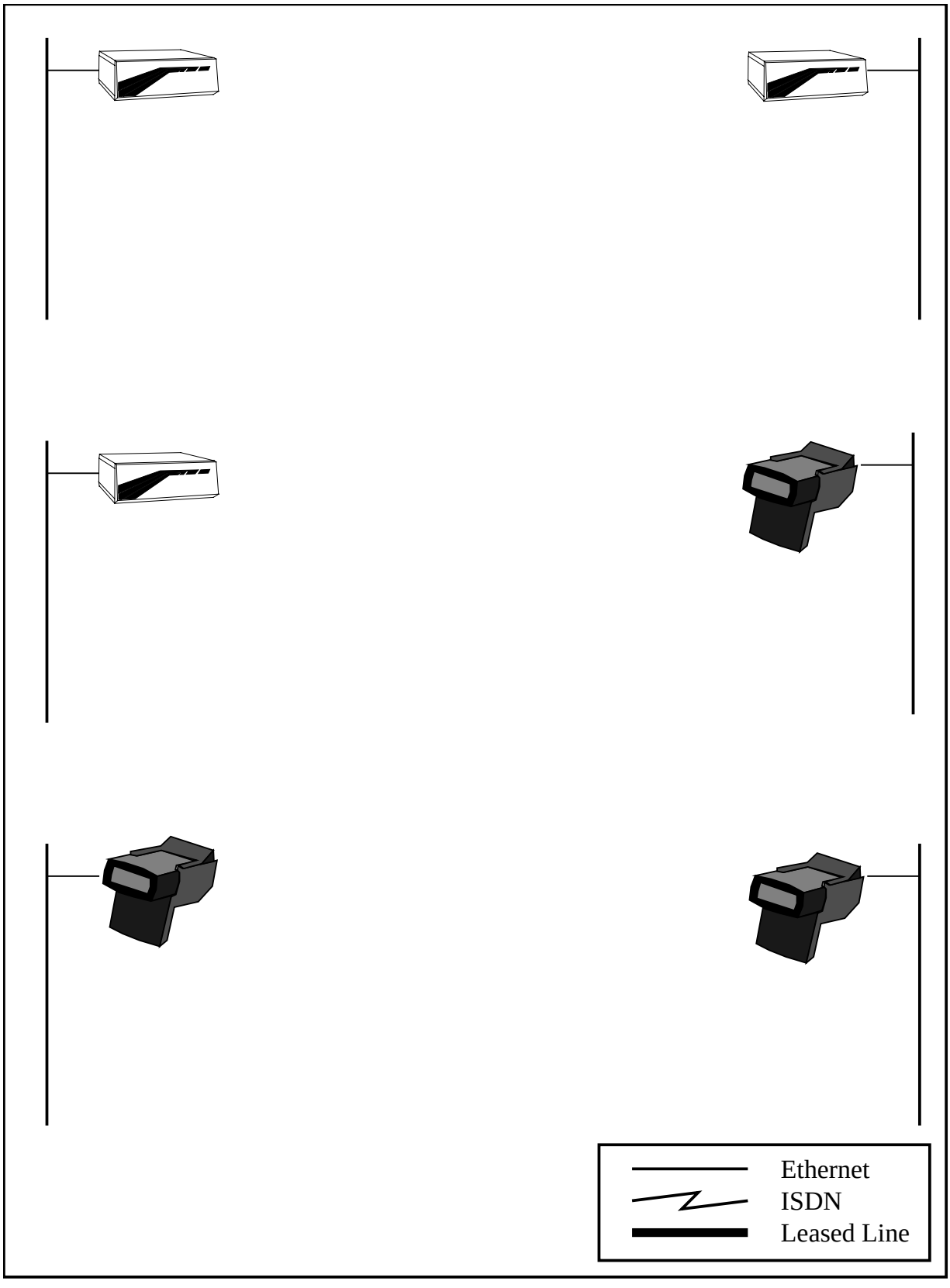
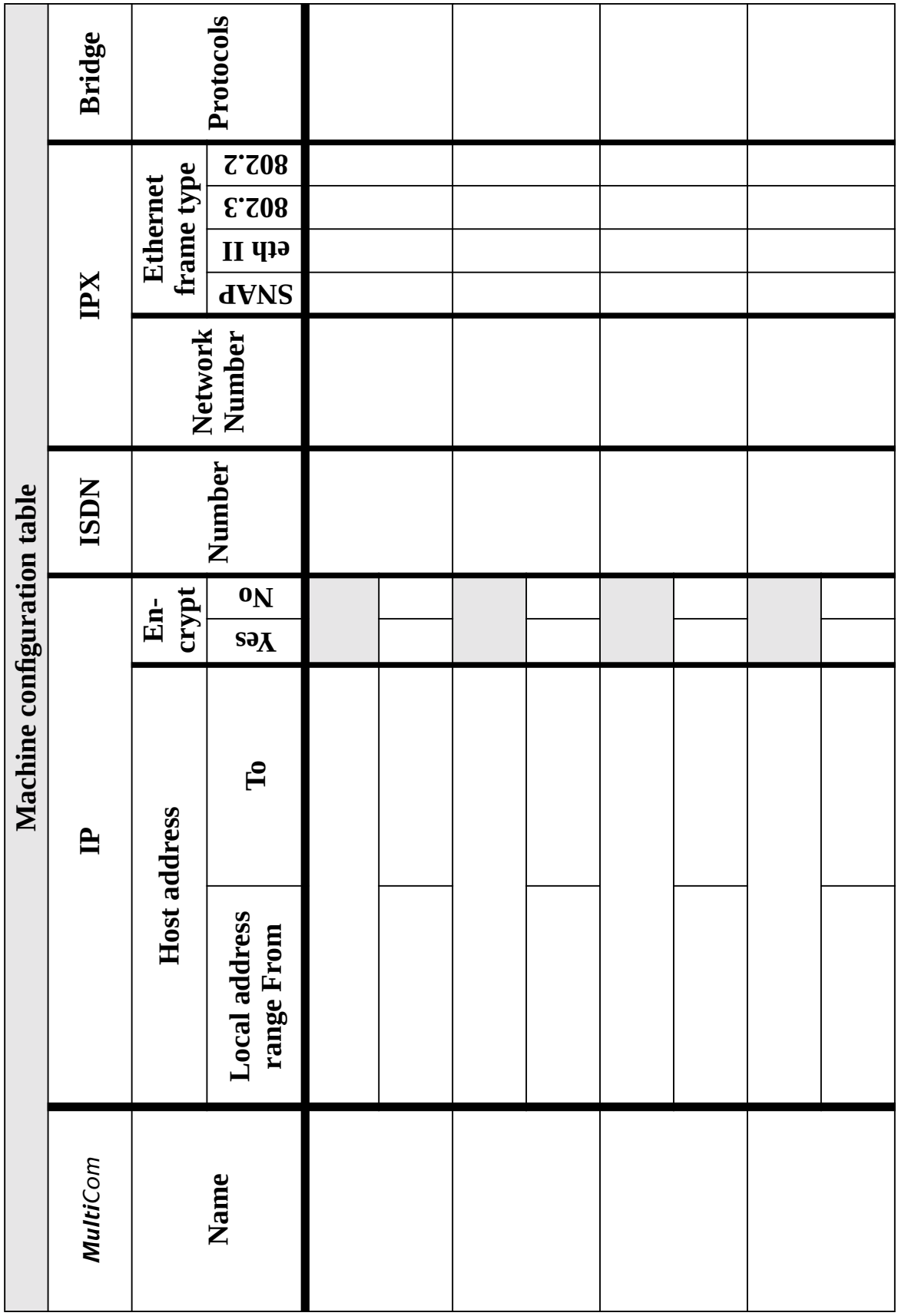


Figure 26 Blank Network diagram

MACHINES

18.4.2



LINKS

18.4.3

Links configuration table

Link		Type								Backup		ISDN		IPX		Serial		En-crypted	
			WAN																
			MHDLC																
						IP													
From	To	LAN	Polling	Connection Control	Transparent	Routed	Bridged	PPP		Yes	No	Dial-up	Leased	WAN	Demand WAN	Yes	No	Yes	No

SITES & ISDN

18.4.4

ISDN configuration table					
MultiCom	B Channels	Auto		RemoteNumber	IdleCloseTime
Site Name		On	Off	NumberEnabled	

BRIDGE GROUPS

18.4.5

Bridge groups configuration table

MultiCom	Group name	Group filter name	Site name	Input filter name
				Output filter name

BRIDGE FILTERS

18.4.6

Bridge filters configuration table												
MultiCom	**Filter Name**	**Type**		**Addres s**		**Ethernet**			**Aliases**			
		Permit	**Deny**	**Source Address**	**Destination Address**	**LLC**	**Ethernet II**	**SNAP**	**TCP/IP**	**IPX**	**AppleTalk**	**All**
				Value								
				Mask								

PPP

PPP Configuration table										
MultiCom	Site Name	Local Authentication (Required incoming authentication)				Remote Authentication (Desired outgoing authentication)				
		User ID / Password	CHAP	PAP	None	User ID / Password	Either	CHAP	PAP	None
Required							***Optional***			

```
# Configuration file for version 2.3 on Pocket and Classic MultiComs.
# Please refer to your Reference Manual for more information.


# --- General information
MyName MultiCom
IP MyAddr 10.0.0.1
IP SubnetMask 255.0.0.0
#ISDN MyNumber 1
ISDN DChannelProtocol EuroISDN
#Account Manager Manager
#ARP Proxy Off


# --- Sites
# - Local site
Site Rename ETH Local
Site Select Local
#IP Range 10.0.0.2 .. 10.255.255.255 Add
DHCP Range 10.0.0.2 .. 10.255.255.255 Add
DHCP On
#IPX NetNumber 0xABCD
#IPX Site On

# - Remote site
Site Rename ISDN Remote
Site Select Remote
Site Modify Remote WANProtocol PPP
ISDN Auto On
ISDN IdleCloseTime 90
#ISDN RemoteNumber 0041216542002
ISDN NumberEnabled *
PPP Authentication NONE
#Serial Mode V35
#Serial Speed 128K
#Serial On
#Backup On
#IP Range  1.0.0.0 ..   9.255.255.255 Add
#IP Range 11.0.0.0 .. 255.255.255.255 Add
#IPX Site On

# - Another site (requires the Multi-Point option)
#Site Create Lightning PPP
#Site Select Lightning
#ISDN Auto On
#ISDN IdleCloseTime 90
#ISDN RemoteNumber 0041216542003
#ISDN NumberEnabled 0041216542003
#PPP Authentication CHAP
#PPP Authentication Local  Userid   ppp_test
#PPP Authentication Local  Password lightning
#PPP Authentication Remote Userid   ppp_test
#PPP Authentication Remote Password lightning
#PPP Compression Off
#PPP Callback Accept
#IP Range 193.247.134.2 .. 193.247.134.2 Add


# --- Bridge
#Bridge Create Group example_group
#Bridge Group example_group Assign-site Local
#Bridge Group example_group Assign-site Remote
#Bridge Create Filter example_filter
#Bridge Filter example_filter permit All
#Bridge Filter example_filter Assign Group example_group


# --- Bridge and Routers activation
Bridge Off
IP Router Off
IPX Router Off


# --- DNS client
#DNS Primary 1.2.3.4
#DNS Secondary 1.2.3.5
#DNS DomainName yourdomain.com
```

```
# Configuration file for version 2.3 on LAN Access Center MultiComs.
# Please refer to your Reference Manual for more information.


# --- General information
MyName MultiCom
IP MyAddr 10.0.0.1
IP SubnetMask 255.0.0.0
#ISDN MyNumber 1
ISDN DChannelProtocol EuroISDN
#Account Manager Manager
#ARP Proxy Off


# --- Sites
# - Local site
Site Rename ETH Local
Site Select Local
#IP Range 10.0.0.2 .. 10.255.255.255 Add
DHCP Range 10.0.0.2 .. 10.255.255.255 Add
DHCP On
#IPX NetNumber 0xABCD
#IPX Site On

# - Remote site
Site Rename ISDN Remote
Site Select Remote
Site Modify Remote WANProtocol PPP
ISDN Auto On
ISDN IdleCloseTime 90
#ISDN RemoteNumber 0041216542002
ISDN NumberEnabled *
PPP Authentication NONE
#Serial 1 Mode V35
#Serial 1 Speed 256K
#Serial 1 On
#Backup On
#IP Range  1.0.0.0 ..   9.255.255.255 Add
#IP Range 11.0.0.0 .. 255.255.255.255 Add
#IPX Site On

# - Another site
#Site Create Lightning PPP
#Site Select Lightning
#ISDN Auto On
#ISDN IdleCloseTime 90
#ISDN RemoteNumber 0041216542003
#ISDN NumberEnabled 0041216542003
#Serial 2 Mode V36
#Serial 2 Speed 2M
#Serial 2 On
#Backup On
#PPP Authentication CHAP
#PPP Authentication Local  Userid   ppp_test
#PPP Authentication Local  Password lightning
#PPP Authentication Remote Userid   ppp_test
#PPP Authentication Remote Password lightning
#PPP Compression Off
#PPP Callback Accept
#IP Range 193.5.2.228 .. 193.5.2.228 Add


# --- Bridge
#Bridge Create Group example_group
#Bridge Group example_group Assign-site Local
#Bridge Group example_group Assign-site Remote
#Bridge Create Filter example_filter
#Bridge Filter example_filter permit All
#Bridge Filter example_filter Assign Group example_group


# --- Bridge and Routers activation
Bridge Off
IP Router Off
IPX Router Off


# --- DNS client
#DNS Primary 1.2.3.4
#DNS Secondary 1.2.3.5
#DNS DomainName yourdomain.com
```

Index

Chapter 19

C

D

E

F

H

I

J

K

L

M

N

P

T

U

V

W