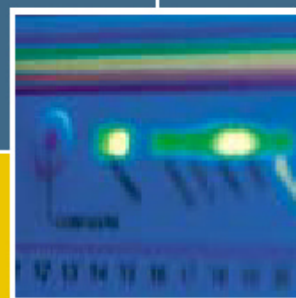
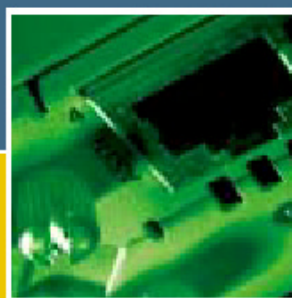
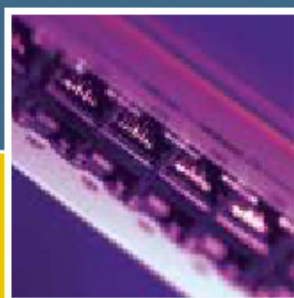
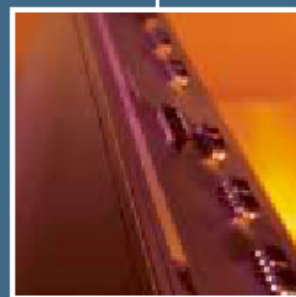


AT-RG213 Residential VoIP Gateway

SIP SOFTWARE REFERENCE MANUAL



AT-RG213 Residential VoIP Gateway - SIP Software Reference Manual
Document Number J613-M0524-00

Copyright © 2002 Allied Telesyn International, Corp.
960 Stewart Drive Suite B, Sunnyvale CA 94086, USA.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn.

Allied Telesyn International, Corp. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn has been advised of, known, or should have known, the possibility of such damages.

All trademarks are the property of their respective owners.

Contents

	Purpose of this Manual	vii
	Intended Audience.....	viii
	Structure of this Manual.....	ix
	Standards and Protocols	ix
	Supported Standards and Protocols.....	ix
	Obtaining Copies of Internet Protocols and Standards.....	x
	Background Reading	xi
	Publicly Accessible Documents	xii
	Conventions.....	xii
CHAPTER 1	Operation	1
	Introduction	1
	Overview of the AT-RG213 Residential VOIP Gateway	1
	Getting Started	2
	Hardware and Software Requirements.....	2
	Command Line Interface	2
	Operating the AT-RG213.....	3
	Logging in	3
	Entering Commands	4
	File Subsystem	4
	Online CLI Help	4
	Configuration Examples	5
	Configuration Script	5
	Saving Configuration Entered with the CLI.....	5
	Loading releases into the AT-RG213	6
	Command Reference	7
CHAPTER 2	IP.....	18
	Introduction	18
	The Internet	18
	Addressing.....	21
	Subnets	23
	Multicasting, IGMP and IGMP snooping.....	24
	What is Multicasting?.....	24
	What is IGMP?	25
	IGMP snooping.....	26
	Configuration Examples	27

	Configuring the IP address	27
	DHCP Client	27
	NTP Protocol	28
	Command Reference	29
CHAPTER 3	DNS	39
	Configuration Examples	39
	Command Reference	40
CHAPTER 4	SIP	43
	Introduction	43
	SIP Protocol	43
	AT-RG213 Call Processes	47
	Calls Involving Another Terminal	47
	Calls Involving a Terminal and a SIP Endpoint	48
	Configuration Examples	50
	Create and configure SIP Port	50
	Command Reference	51
CHAPTER 5	SNMP	57
	Introduction	57
	Simple Network Management Protocol (SNMP)	57
	Communities and Views	58
	Configuration Examples	58
	Command Reference	59
CHAPTER 6	L2TP	62
	L2TP Introduction	62
	Command Reference	63
CHAPTER 7	Phone	67
	Introduction to FXS Ports	67
	PSTN Line management	67
	Ring Generation	70
	Tone Generation	70
	Port Gain	71
	Port Impedance	72
	Buffer Management	72
	Voice Activation and Silence Detection	73
	Digit Collection	73
	Configuration Examples	73
	Command Reference	74
CHAPTER 8	Switch	80
	Introduction	80
	VLAN	80
	Vlan Tagging - 802.1Q	81
	Switch architecture	82
	Configuration Examples	83
	Command Reference	84

List of Figures

Figure 1. Example output from the SHOW CONFIG command.....	14
Figure 2. Example output from the SHOW LOADER command.....	15
Figure 3. Example output from the SHOW SYSTEM command.....	16
Figure 4. IP packet or datagram.....	20
Figure 5. Subdivision of the 32 bits of an Internet address into network and host fields for class A, B and C networks ...	22
Figure 6. IGMP snooping network layers.....	26
Figure 7. Example output from the SHOW IP command.....	35
Figure 8. Example output from the SHOW IP INTERFACE command.....	36
Figure 9. Example output from the SHOW NTP command.....	38
Figure 10. Example output from SHOW DNS command.....	42
Figure 11. Example output from the SHOW IP command.....	42
Figure 12. Phone --> AT-RG213 (A) --> AT-RG213 (B) --> Phone.....	48
Figure 13. Phone --> AT-RG213 (A)--> LAN SIP endpoint.....	49
Figure 14. LAN SIP endpoint --> AT-RG213 --> Phone.....	50
Figure 15. Example output from the SHOW SIP PORT command.....	55
Figure 16. Example output from the SHOW SNMP command.....	60
Figure 17. L2TP network model.....	63
Figure 18. Example output from the SHOW L2TP command.....	66
Figure 19. RING tone diagram.....	69
Figure 20. Tones Frequency/Time graphs.....	71
Figure 21. RTP Packet receive path.....	73
Figure 22. Example output from the SHOW PHONE command.....	77
Figure 23. The VLAN field in the Ethernet file.....	82
Figure 24. Switch architecture.....	82
Figure 25. Example output from the SHOW SWITCH command.....	94
Figure 26. Example output from SHOW SWITCH FDB command.....	95
Figure 27. Example output from SHOW SWITCH PORT command.....	96
Figure 28. Example output from the SHOW SWITCH PORT COUNTER command.....	98
Figure 29. Example output from the SHOW SWITCH QOS command.....	100
Figure 30. Example output from the SHOW VLAN command.....	101

List of Tables

- Table 1. Protocols and standards supported by the AT-RG213 Gateway.ix
- Table 2. Typographic conventions used in this manual. xii
- Table 3. Hardware and Software requirements..... 2
- Table 4. Terminal Emulation Software 2
- Table 5. Parameters for terminal communication..... 3
- Table 6. Command line editing functions and keystrokes 4
- Table 7. Available modules 5
- Table 8. Parameters displayed in the output of the SHOW CONFIG command..... 15
- Table 9. Parameters displayed in the output of the SET LOADER command. 16
- Table 10. Parameters displayed in the output of the SHOW SYSTEM command. 17
- Table 11. Functions of the fields in an IP datagram 20
- Table 12. Internet Protocol address classes and limits on numbers of networks and hosts. 21
- Table 13. Parameters displayed in the output of the SHOW IP IGMP command. 35
- Table 14. Parameters displayed in the output of the SHOW IP INTERFACE command. 37
- Table 15. Parameters displayed in the output of the SHOW IP INTERFACE command. 38
- Table 16. Parameters displayed in the output of the SHOW SIP PORT command. 56
- Table 17. Parameters displayed in the output of the SHOW SNMP command. 61
- Table 18. Parameters displayed in the output of the SHOW L2TP command 66
- Table 19. PSTN Line Management 68
- Table 20. Tone Generation 70
- Table 21. Italian Defaults Tones..... 71
- Table 22. FXS Port equivalent circuits 72
- Table 23. Parameters displayed in the output of the SHOW PHONE command. 78
- Table 24. Parameters displayed in the output of the SHOW SWITCH command..... 94
- Table 25. Parameters displayed in the output of the SHOW SWITCH FDB command. 95
- Table 26. Parameters displayed in the output of the SHOW SWITCH PORT command..... 96
- Table 27. Parameters displayed in the output of the SHOW SWITCH PORT COUNTER command..... 99
- Table 28. Parameters displayed in the output of the SHOW SWITCH QOS command..... 101
- Table 29. Parameters displayed in the output of the SHOW VLAN command. 102

Preface

Purpose of this Manual

This manual is the complete reference to the configuration, management and operation of the AT-RG213 Residential VoIP Gateway, and includes detailed descriptions of all management commands.

The AT-RG213 is a Customer Promise Equipment (CPE) designed to be installed in the customer residence which interfaces with new generation fibre/copper networks designed to support broadband communications.

Using this intelligent equipment, the "residential gateway", the customer can use broadband integrated services for telephony, Internet and Internet Video.

The VoIP residential gateway, fitted with a number of ports for interconnection of the traditional domestic appliances (telephone, fax, personal computer), acts as an adaptor for the conversion and management of all the necessary protocols for using advanced multimedia services:

- *Low cost telephony using internet protocol (VoIP)*
- *Fast navigation in internet*
- *Video on demand*
- *Interactive services*

The main features of the device are listed below:

- *one 10/100 BaseT/Base FX Ethernet port for uplink (WAN port)*
- *three 10/100 Base T Ethernet ports for connecting user equipment (pc, printer, etc.)*
- *Vlan Tagging configuration and management as defined in IEEE 802.1Q*
- *two VoIP ports for connecting two analog telephones or faxes*
- *Connection to PSTN line*
- *Switching function using the same analogue terminal from VoIP to PSTN*
- *Compliant with SIP protocol (RFC 3261)*
- *IGMP snooping configuration and management*
- *TFTP - Trivial File Transfer Protocol support*
- *NTP - Network Time Protocol support*
- *Configuration and management of the device through:*
 - *Serial interface (CLI)*
 - *Telnet*
 - *SNMP*
 - *Zero Touch Configuration*

Intended Audience

This manual is intended for the system administrator, network manager or communications technician who will configure and maintain the AT-RG213, or who manages a network of AT-RG213 Gateways.

It is assumed that the reader is familiar with:

- The topology of the network in which the *AT-RG213 Gateway* is to be used.
- Basic principles of computer networking, routing protocols and interfaces.
- Administration and operation of a computer network.
- This manual is not intended for users who will use the computer network to access network services from their terminal, personal computer or workstation.
- Most of the commands described in this manual require MANAGER privilege and can only be entered from a terminal or port that has been assigned MANAGER privilege.

Structure of this Manual

This manual is organised into the following chapters:

- *Chapter 1, Operation describes general operation, management and support features, including user authentication, down-line loading and installing software releases.*
- *Chapter 2, Internet Protocol (IP) describes the implementation of the Internet Protocol (IP) and all the commands related to IP network configuration management.*
- *Chapter 3, DNS describes the commands related to the internal DNS client implementation*
- *Chapter 4, SIP describes SIP protocol, the related call processes and all the commands related to SIP configuration management.*
- *Chapter 5, Simple Network Management Protocol (SNMP) describes the SNMP service provided by the gateway, and how to configure SNMP interfaces.*
- *Chapter 6, Phone describes the L2TP service provided by the gateway and its configuration and management.*
- *Chapter 7, Phone describes all available settings of the phone and the commands related to the phone interfaces configuration.*
- *Chapter 8, Switch (SW) describes the commands related to the integrated Switch configuration.*
- *Glossary contains definitions of terms and concepts used in this manual.*
- *Index is a master index to topics and commands covered in this manual.*

Standards and Protocols

Supported Standards and Protocols

Table 1 lists the protocols and standards supported by the AT-RG213 Residential Gateway and the references where these protocols and standards are defined.

Table 1. Protocols and standards supported by the AT-RG213 Gateway.

Protocol/standard	Reference
ARP	RFCs 826, 925.
Assigned Numbers	RFC 1700.
DHCP	RFCs 1541, 1542.

H.323	ITU H.323, ITU H.225, ITU H.245
ICMP	RFCs 792, 950.
IEEE 802.2	ANSI/IEEE Std 802.2-1985.
IEEE 802.3	ANSI/IEEE Std 802.3-1985, 802.3a, b, c, e-1988.
IGMP	RFC 3228
IP	RFCs 791, 821, 950, 951, 1009, 1055, 1122, 1144, 1349, 1542, 1812, 1858.
IP addressing	RFC 1597.
L2TP	RFC 2661
NTP	RFCs 958, 1305, 1510.
RTP-RTCP	RFC 1889, ITU G.711, ITU G.723, ITU G.729
SDP	RFC 2327
SIP	RFC 3261
SNMP, MIBs	RFCs 1155, 1157, 1213, 1239, 1315, 1398, 1493, 1514, 1573, 2233.
TCP	RFC 793.
Telnet	RFCs 854–858, 932 1091.
TFTP	RFC 1350.
UDP	RFC 768.
VLAN	IEEE 802.1q

Obtaining Copies of Internet Protocols and Standards

The Internet Protocols are defined in *Requests For Comments* (RFCs). RFCs are developed and published under the auspices of the *Internet Engineering Steering Group* (IESG) of the *Internet Engineering Task Force* (IETF). For more information about the IESG and IETF, visit the IETF web site at <http://www.ietf.org/>.

For more information about RFCs and Internet Drafts (the starting point for RFCs), visit the RFC Editor web site at <http://www.rfc-editor.org/>. This site has information about the RFC standards process, archives of RFCs and current Internet Drafts, links to RFC indexes and search engines, and a list of other RFC repositories.

RFCs can be obtained electronically from many RFC repositories, mail servers, World Wide Web (WWW), Gopher or WAIS sites. A good starting point for finding the nearest RFC repository is to point your Web browser at <http://www.isi.edu/in-notes/rfc-retrieval.txt>.

To obtain a copy of an RFC using FTP, FTP to the host and login as user `anonymous`, and a password of either `guest` or your email address. The FTP server will usually prompt you for one or the other. Use the `get` command to retrieve the desired RFC. Most sites have a file, usually `rfc-index.txt`, which lists the titles and file names of all available RFCs. Most sites have a file, usually `rfc-retrieval.txt`, which gives detailed

information about RFC repositories and how to retrieve RFCs via FTP, mail servers, WWW, Gopher and WAIS.

To learn how to obtain a copy of an RFC via email from a mail server, point your browser at <http://www.isi.edu/in-notes/rfc-editor/rfc-info>.

To obtain a copy of an RFC from a Web site, or to search RFC repositories for a specific RFC or all RFCs relating to a topic, point your Web browser at <http://www.rfc-editor.org/rfc.html>.

Background Reading

For an introduction to the Internet Protocols refer to:

DDN Protocol Handbook, Elizabeth J. Feinler, 1991, DDN Network Information Center, SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025, USA. Email: nic@nic.ddn.mil.

Internetworking with TCP/IP — Volume I: Principles, protocols and architecture (2nd Edition), Douglas E. Comer, 1991, Prentice-Hall International, Inc., New Jersey. ISBN 0-13-474321-0.

Internetworking with TCP/IP — Volume II: Design, implementation, and internals, Douglas E. Comer and David L. Stevens, 1991, Prentice-Hall International, Inc., New Jersey. ISBN 0-13-472242-6.

Internetworking with TCP/IP — Volume III: Client-server programming and applications, Douglas E. Comer and David L. Stevens, 1993, Prentice-Hall International, Inc., New Jersey. ISBN 0-13-474222-2.

For a description of layered protocols refer to:

Computer networks (2nd Edition), Andrew S. Tanenbaum, 1989, Prentice-Hall International, Inc., New Jersey. ISBN 0-13-162959-0.

For an introduction to network management refer to:

The simple book — An introduction to management of TCP/IP-based Internets, Marshall T. Rose, 1991, Prentice-Hall International, Inc. ISBN 013812611-9.

For an introduction to VOIP refer to:

Internet Communications Using SIP, Henry Sinnreich, Alan B. Johnston.

SIP: Understanding the Session Initiation Protocol, Alan B. Johnston.

IP Telephony with H.323: Architectures for Unified Networks and Integrated Services, Vineet Kumar, Markku Korpi, Senthil Sengodan.

Publicly Accessible Documents

Allied Telesyn maintains an online archive of documents and files that customers can access via the World Wide Web or via anonymous FTP. For WWW access, point your Web browser at <http://www.alliedtelesyn.com>.

Conventions

A number of symbols, typographic and stylist conventions are used throughout this manual to aid learning and make information easier to find (see Table 2).

Table 2. Typographic conventions used in this manual.

This typeface	Is used for
<i>Italic</i>	Referring to another section in this manual or another manual, or to introduce and emphasise new terms. For example, "See <i>Chapter 2, IP</i> ".
Monospace	Text as it appears on-screen, or anything you must type.
0xFF	Numbers starting with the 0x prefix are hexadecimal values.
<i>Attention</i>	A special keystroke known as the attention character, which will be either [Break] or [Ctrl/P].



Note. A note like this presents additional information or interesting sidelights.



Warning. A warning alerts you to situations in which you could do something that might result in a loss of data, or cause damage to the equipment.

Screen views show examples of the output resulting from particular commands, or what the screen should look like at a particular time, for instance:

```

01234567890123456789012345678901234567890123456789
Filename           Size      Created
-----
boot.cfg           675      25-Feb-2001  12:01:24
remote.cfg         1987     14-Feb-2001  10:01:24
-----
Boot Configuration Script: boot.cfg
-----

```

Command syntax is defined using these conventions:

This	Is used for
CAPS	Keywords to be typed as shown. In general keywords may be abbreviated to the shortest string that is unambiguous within the current context. The exception is commands with a profound effect, such as RESTART IMMEDIATELY, which must be typed in full.
<i>Italic</i>	A variable placeholder, to be replaced by an actual value in a command.
[]	Square brackets enclose optional items. Enter the item or items required, but do not type the brackets.
	Vertical bars separate choices in a list — choose one of the items.
...	Ellipses indicate that the preceding element may be repeated any number of times
n..m	Defines a range of values from n to m inclusive. n and m are decimal numbers.
<i>interface</i>	An interface type — one of: ETHn for Ethernet interfaces VLANn for Virtual LAN interface. n when defining one of the above interface types. n is a non-negative, zero-based decimal number.
<i>Ipaddr</i>	An IP address in dotted decimal form (e.g. 131.203.9.197). In some situations an address in domain name format.
<i>Macadd</i>	A hardware address (such as an Ethernet address) of the form XXXXXXXXXXXX, where XX is a two-digit hexadecimal number with leading zeros if necessary.

Commands are described under *Command Reference* within the section to which they apply. Each command is described in the following format:

	28	RG203TX Reference Manual
Command The syntax of the command		<p>SET IP INTERFACE</p> <p>Syntax SET IP INTERFACE=<i>name</i> [{CONFIGURATION={DHCP DHCPCONF [SERVERID=<i>id</i>]} [IPADDRESS=<i>ipaddr</i>] [MASK=<i>ipaddr</i>] [GATEWAY=<i>ipaddr</i>]}]</p> <p>Short Syntax S IP INT=<i>name</i> [{CONF={DHCP DHCPCONF [SERVERID=<i>id</i>]} [IPADDRESS=<i>ipaddr</i>] [MASK=<i>ipaddr</i>] [GATEWAY=<i>ipaddr</i>]}]</p> <p>where:</p> <ul style="list-style-type: none"> ▪ <i>name</i> is the interface short name plus the interface number (e.g. eth0, ppp1, ..) ▪ <i>ipaddr</i> is an ip address in dotted decimal notation ▪ <i>id</i> is a string that can contains upper or lower case alphanumeric characters and symbols excluding wildcards (*). The maximum number of characters is 20.
What the command does, and what each of the parameters mean		<p>Description This command configures an IP interface on a specific port. The port can be configured in three ways: manual, DHCP and DHCPCONF. The parameters that can be set manually are address, network mask and default gateway, if any.</p> <p>If the network mask is not given, the default for the class at which the address belongs is taken. For example the address 192.168.0.19 belongs to the class C subnet 192.168.0.x and will have 255.255.255.0 as default network mask.</p> <p>The default configuration for the port is MANUAL.</p> <p>DHCPCONF is a special DHCP configuration to help manage configuration and software upgrade centrally. SERVERID is an identifier of the server that it's supposed to manage the device.</p>
Examples show how the command is used		<p>Examples To set the 192.168.0.10 on the eth0 (Ethernet interface 0):</p> <pre>SET IP INTERFACE=eth0 IPADDRESS=192.168.0.10</pre> <p>That is equivalent to</p> <pre>SET IP INTERFACE=eth0 CONFIGURATION=MANUAL IPADDRESS=192.168.0.10 MASK=255.255.255.0</pre> <p>To set the default gateway to 192.168.0.1:</p> <pre>SET IP INTERFACE=eth0 GATEWAY=192.168.0.1</pre>
Reference to related command		<p>See Also SHOWIP INTERFACE</p>

Software Release 2-1-1
C613-03032-00 REV A

Chapter 1

Operation

Introduction

Overview of the AT-RG213 Residential VOIP Gateway

The AT-RG213 Residential VoIP Gateway is a home-use access device which integrates the services of fast internet, digital video and telephony over Internet (VoIP).

The device has three (3) LAN ports to be connected to PC's or home/office peripherals and one WAN port to connect the CPE (Customer Promise Equipment) to an ISP (Internet Service Provider) network. Through the Line port, the AT-RG213 can be linked to a standard phone/fax analogue (PSTN) line.

The AT-RG213 supports a number of different VoIP protocols - these are factory build options but the unit may be firmware re-loaded to a different VoIP protocol if required:

- *H323*
- *SIP*
- *MGCP and NCS profile*

Getting Started

The AT-RG213 is supplied with default settings that allow it to operate immediately as a Residential Gateway. Even if this is all you want to use the gateway for, you should still gain access to the gateway configuration, if only to change the *manager* password to prevent unauthorised access.

The AT-RG213 is provided with a Command Line Interface (CLI) for configuration and management.

Hardware and Software Requirements

In *Table 3*, the hardware and software requirements are listed.

Table 3. Hardware and Software requirements

Requirement	Description/use	Mandatory
VoIP SERVER	Endpoint registration (Gatekeeper)	NO
Phone/fax	A standard analog telephone or fax	YES
PSTN Line		NO
DHCP Server	This server supplies all network parameters to AT-RG213, if present.	NO
TFTP Server	For remote software updates	NO
Terminal Emulation Software	CLI	YES

Command Line Interface

To use the command line interface (CLI) for configuring the AT-RG213, the first thing you need to do after physically installing the AT-RG213 is to start a terminal session to access the AT-RG213. *Table 4* lists some common names for this software, based on the Operating System you are using.

Table 4. Terminal Emulation Software

Operating System	Software Name
Windows 9X, Windows NT/W2K/XP	HyperTerm (included with Windows software)
Macintosh OS	ProComm, VersaTerm
Linux	Minicom

The terminal emulation software is used to change the settings and communicate through your PC with the AT-RG213.

To start a terminal session, do one of the following:

- Connect a VT100-compatible terminal to the RS-232 Terminal Port, set the communication parameters on the terminal (see Table 5), and press [Enter] a few times until the AT-RG213 login prompt appears; or
- Connect the COM port of a PC running terminal emulation software such as Windows Terminal or HyperTerminal to the RS-232 Terminal Port, set the communications parameters on the emulation software (see Table 5), and press [Enter] a few times until the AT-RG213 login prompt appears.

Table 5. Parameters for terminal communication

Parameter	Value
Baud rate	38400
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware

Operating the AT-RG213

This chapter introduces general operation, management and support features, including user authentication, loading and installing support files, and SNMP MIBs.

Logging in

A user accessing the AT-RG213 from a terminal or PC connected to the side panel RS-232 terminal port, or via a Telnet connection, must enter a login name and password to gain access to the command prompt.

When the AT-RG213 is supplied, it has a *manager* account with an initial password *friend*.

Enter your login name at the login prompt:

```
login: manager
```

Enter the password at the password prompt:

```
password: friend
```

This password should be changed to prevent unauthorized access to the AT-RG213, using the command:

```
SET PASSWORD
```



Make sure you remember the new password you create, as a lost password cannot be retrieved, and would mean losing access for configuring and monitoring the AT-RG213.

Entering Commands

The AT-RG213 is controlled with commands described in this document. While the keywords in commands are not case sensitive, the value entered for some parameters are. The AT-RG213 supports command line editing and recall (*see Table 6*).

Table 6. Command line editing functions and keystrokes

Function	VT100-compatible Keystroke
Move cursors within command line	←, →
Delete character to left of cursor	[Delete] or [Backspace]
Recall previous command	↑
Recal next command	↓

File Subsystem

FLASH memory is structured like a file subsystem. Files can be saved, listed and deleted. Release files, online help files, configuration scripts and other scripts are all stored as files in FLASH memory. Names must have DOS format, with a filename of up to eight characters and an extension of three characters.

To display the files in FLASH, use the command:

```
SHOW CONFIG
```

```
012345678901234567890123456789012345678901234567890123456789
Filename          Size      Created
-----
boot.cfg          675      25-Feb-2001  12:01:24
remote.cfg       1987     14-Feb-2001  10:01:24
-----
Boot Configuration Script: boot.cfg
-----
```

Online CLI Help

Online help is available for all modules in the CLI.

An online help facility provides more detailed help information via the command:

```
HELP [module]
```

If the module is not specified, a list of available modules is displayed (*see Table 7 for available Modules*). The HELP command displays information from the system help file store in FLASH memory.

Table 7. Available modules

Module name	Description
BASIC	Basic device management and configuration
DNS	DNS Client management and configuration
IP	IP network management and configuration
L2TP	L2TP module management and configuration
PHONE	FXS phone interface management
SIP	SIP module management and configuration
SNMP	SNMP version 2 management protocol
SW	Integrated switch management

Configuration Examples

Configuration Script

When powered, the AT-RG213 executes the commands in the boot script in order to obtain the default configuration. A boot script is a sequence of standard commands executed at start-up. A script file (e.g test.cfg) can be defined for the following start-up as the boot script using the command:

```
SET CONFIG=test.cfg
```

A configuration file is a script made up of the same commands as are used in the CLI. This file can be edited manually using the CLI, or uploaded from a terminal that must be a TFTP server.

Saving Configuration Entered with the CLI

Subsequent commands entered from the command line or executed from a script, do not cause any permanent change in the equipment configuration and the setting is effective until the device is power cycled. Changes are not automatically stored in non-volatile memory. When either the AT-RG213 is

restarted or the RESTART REBOOT command is executed, the configuration will be restored to the one defined by the boot script.

To retain any configuration changes made after boot even after a restart or power cycle, save the modified configuration as a script file, according to the following examples.

Example 1: how to create a configuration script

To create the configuration script `sip.cfg` based on the current device configuration:

```
CREATE CONFIG=sip.cfg
```



Note that the filename is case sensitive, that is `sip.cfg` and `SIP.cfg` are considered two distinct files

The script is stored in the indicated filename and can be later used as start-up script with the SET CONFIG command.

The list of scripts present on the flash can be retrieved with the command:

```
SHOW CONFIG
```

Example 2: how to delete a configuration script

To permanently delete a configuration script `sip.cfg` from the flash, use the command:

```
DELETE CONFIG=sip.cfg
```



If the file `sip.cfg` (filename) corresponds to the boot configuration script, automatically the command is aborted.

Example 3: how to save a configuration script on tftp server

To transfer a configuration script from the device flash to a tftp server, for example to save the `script.cfg` to the server `192.168.0.10`:

```
SAVE CONFIG=script.cfg SERVER=192.168.0.10
```

If the server is not specified, the one previously set with the command SET LOADER is used.

Loading releases into the AT-RG213

The LOADER module is responsible for loading and storing releases and other files into FLASH. The LOADER module uses the *Trivial File Transfer Protocol* (TFTP) to retrieve files from a network host.

The loader can be configured with the command:

```
SET LOADER [FILE=filename] [SERVER=ipaddr]
```

This command changes the default parameters used in load command. FILE is the default image file loaded and SERVER the default tftp server.

Example 1: Install Software upgrade for AT-RG213

To download the release file named “rg1-sip-6-0-0.bin” from a TFTP server (es. 192.168.0.50) to the AT-RG213 FLASH memory:

```
LOAD IMAGE FILE= rg1-sip-6-0-0.bin  
SERVER=192.168.0.50
```

If the server or the file is not specified, the one previously set with the command SET LOADER is used.

The process of downloading a release file can take some time. An indicative time for downloading a release over Ethernet is 1 to 2 minutes.

When the download process is completed, the presence of the file in FLASH can be verified through the command:

```
SHOW SYSTEM
```

This command shows the major information relevant to the equipment configuration and status including the ones previously set by SET SYSTEM command.

Command Reference

CREATE CONFIG

Syntax	CREATE CONFIG=filename
Short Syntax	C CONF=filename
	where:
	<ul style="list-style-type: none">■ <i>filename is a file name that can contain up to 20 characters excluding ; , ! @ # \$ () < > / \ " ' ` ~ { } [] = + & ^ <space> <tab>.</i>
Description	This command can be used to create a configuration script based on the device configuration at the time of the command execution. The script is stored in the indicated filename and can be later used as start-up script with the SET CONFIG command.
	Please note that the filename NONE has a special meaning in the SET CONFIG command, so if a NONE configuration is created this will not be usable as boot script.

Examples To create the configuration script `script.cfg` based on the current device configuration:

```
CREATE CONFIG=script.cfg
```

See Also SHOW CONFIG
VIEW CONFIG
SET CONFIG
DELETE CONFIG
SAVE CONFIG
LOAD CONFIG

DELETE CONFIG

Syntax DELETE CONFIG=filename

Short Syntax D CONF=filename

where:

- *filename is a file name that can contains up to 20 characters excluding | ; , ! @ # \$ () < > / \ " ' ` ~ { } [] = + & ^ <space> <tab>.*

Description This command can be used to permanently delete a configuration script from the flash. The list of script present on the flash can be retrieved with the SHOW CONFIG command. If the boot configuration script is the one that is going to be deleted, the command is aborted.

Examples To delete the script `script.cfg`:

```
DELATE CONFIG=script.cfg
```

See Also SHOW CONFIG
VIEW CONFIG
CREATE CONFIG
SET CONFIG
LOAD CONFIG
SAVE CONFIG

EXEC CONFIG

Syntax EXEC CONFIG=filename [FLASH | SERVER [=ipaddr]]

Short Syntax	E CONF= <i>filename</i> [FLASH SERVER [= <i>ipaddr</i>]] where: <ul style="list-style-type: none">■ <i>filename</i> is a file name that can contain up to 20 characters excluding ; , ! @ # \$ () < > / \ " ' ` ~ { } [] = + & ^ <space> <tab>.■ <i>ipaddr</i> is an ip address in dotted decimal notation
Description	This command allows executing a configuration script from a tftp server or internal flash. The default script location is the flash.
Examples	To execute the configuration script <code>script.cfg</code> from the server 192.168.1.10: EXEC CONFIG = script.cfg SERVER=192.168.1.10
See Also	LOAD CONFIG SET LOADER

HELP

Syntax	HELP [module]
Short Syntax	H [module]
Description	This command displays online help for commands. If a module is not specified, a list of available modules is displayed. If a module is specified, and is available, a list of commands relating to the module is displayed.
Examples	To show the list of available topics: >HELp To show the help on the IP module: >HELp IP

LOAD CONFIG

Syntax	LOAD CONFIG= <i>filename</i> [SERVER= <i>ipaddr</i>]
Short Syntax	L CONF= <i>filename</i> [SERVER= <i>ipaddr</i>] where: <ul style="list-style-type: none">■ <i>filename</i> is a file name that can contain up to 20 characters excluding ; , ! @ # \$ () < > / \ " ' ` ~ { } [] = + & ^ <space> <tab>.

- *ipaddr* is an ip address in dotted decimal notation

Description This command allows to load in the device flash a configuration script from a tftp server. If the server is not given the one previously set with the command SET LOADER is used. The name of the configuration script will be the same of the filename and if a script with the same name already exists in the flash, this will be overwritten.

Examples To load the configuration script script.cfg from the server 192.168.1.10:

```
LOAD CONFIG=script.cfg SERVER=192.168.1.10
```

See Also SHOW CONFIG
VIEW CONFIG
CREATE CONFIG
DELETE CONFIG
SET CONFIG
SAVE CONFIG

LOAD IMAGE

Syntax LOAD IMAGE=filename [SERVER=ipaddr]

Short Syntax L IM=filename [SERVER=ipaddr]

where:

- *filename* is a file name that can contain up to 20 characters excluding | ; , ! @ # \$ () < > / \ " ' ` ~ { } [] = + & ^ <space> <tab>.
- *ipaddr* is an ip address in dotted decimal notation

Description This command allows to load in the device flash the application from a tftp server. If the server or the file is not given the one previously set with the command SET LOADER is used.

Examples To load the application image rg1-sip-6-0-0.bin from the server 192.168.1.10:

```
LOAD IMAGE FILE=rg1-sip-6-0-0.bin
SERVER=192.168.1.10
```

See Also SET LOADER

LOGOUT

Syntax	LOGOUT
Description	This command closes the current console or telnet session.
See Also	SHOW SYSTEM

RESTART REBOOT

Syntax	RESTART REBOOT
Description	This command cause a device cold reboot

SAVE CONFIG

Syntax	SAVE CONFIG=filename [SERVER=ipaddr]
Short Syntax	SA CONF=filename [SERVER=ipaddr]
	where:
	<ul style="list-style-type: none">■ <i>filename is a file name that can contain up to 20 characters excluding ; , ! @ # \$ () < > / \ " ' ` ~ { } [] = + & ^ <space> <tab>.</i>■ <i>ipaddr is an ip address in dotted decimal notation</i>
Description	This command allows transferring a configuration script from the device flash to a tftp server. If the server is not given the one previously set with the command SET LOADER is used.
Examples	To SAVE the script.cfg to the server 192.168.1.10: SAVE CONFIG=script.cfg SERVER=192.168.1.10
See Also	SHOW CONFIG VIEW CONFIG CREATE CONFIG DELETE CONFIG SET CONFIG

SET CONFIG

Syntax	SET CONFIG=[<i>filename</i> NONE]
Short Syntax	S CONF=[<i>filename</i> NONE]
	where:
	<ul style="list-style-type: none"> ■ <i>filename</i> is a file name that can contain up to 20 characters excluding ; , ! @ # \$ () < > / \ " ' ` ~ { } [] = + & ^ <space> <tab>.
Description	This command configures the device to execute a specific configuration script starting from the following start-up. The script must exist on the flash when the command is executed. If the NONE parameter is used, the device will not execute any script starting the next boot.
Examples	To set the script <code>boot.cfg</code> as the script executed at the start-up: <pre>SET CONFIG=boot.cfg</pre> <p>To delete the boot script setting</p> <pre>SET CONFIG=NONE</pre>
See Also	SHOW CONFIG VIEW CONFIG CREATE CONFIG DELETE CONFIG LOAD CONFIG SAVE CONFIG

SET LOADER

Syntax	SET LOADER [FILE= <i>filename</i>] [SERVER= <i>ipaddr</i>]
Short Syntax	S LO [FILE= <i>filename</i>] [SERVER= <i>ipaddr</i>]
	where:
	<ul style="list-style-type: none"> ■ <i>filename</i> is a file name that can contain up to 20 characters excluding ; , ! @ # \$ () < > / \ " ' ` ~ { } [] = + & ^ <space> <tab>. ■ <i>ipaddr</i> is an ip address in dotted decimal notation
Description	This command changes the default parameters used in LOAD commands. FILE is the default image file loaded and SERVER the default tftp server.
Examples	To set the device to load the file <code>rg1-sip-6-0-0.bin</code> from the server 192.168.0.10: <pre>SET LOADER FILE= rg1-sip-6-0-0.bin SERVER=192.168.0.10</pre>

See Also LOAD IMAGE
 LOAD CONFIG

SET PASSWORD

Syntax SET PASSWORD

Short Syntax SET PASSWORD

Description This command allows changing login password. Please note that the change can become permanent only after a new CREATE CONFIG. The password length must be between 3 and 15 characters length.

Examples To change the login password

```
SET PASSOWORD
Old Password:
New Password:
Confirm:
```

See Also CREATE CONFIG

SET SYSTEM

Syntax SET SYSTEM [NAME=*name*] [LOCATION=*name*]
 [CONTACT=*name*]

Short Syntax S SYS [N=*name*] [L=*name*] [C=*name*]

where:

- *name* is an string of maximum 30 ASCII characters. If space is included, the string must be enclosed in double quotes.

Description This command allows to set three important variables that are used throughout the system: system name (NAME), system contact (CONTACT) and device location (LOCATION).

Examples To set the above mentioned variables:

```
SET SYSTEM NAME=cpe CONTACT="Bob Kent"
LOCATION="Milan Office, 4th floor"
```

See Also SHOW SYSTEM

SHOW CONFIG

Syntax SHOW CONFIG [FIRST | NEXT | BOOT]

Short Syntax SH CONF [FIRST | NEXT | BOOT]

Description This command shows the list of scripts present on the flash and the script executed at the start-up time, if any.

If FIRST option is given the first script in the list is returned and the internal reference is set to this first script. If the command is then called with NEXT option, all subsequent script names are returned until the last. Any other invocation of SHOW CONFIG NEXT will give an empty string ("").

The command SHOW CONFIG BOOT returns the boot configuration script or an empty string ("") if there isn't one.

The FIRST, NEXT and BOOT options are mainly oriented to the web interface.

Examples To retrieve the scripts present on the flash one by one:

```
>SHOW CONFIG FIRST
```

```
boot.cfg
```

```
>SHOW CONFIG NEXT
```

```
remote.cfg
```

```
>SHOW CONFIG NEXT
```

```
...
```

```
>SHOW CONFIG NEXT
```

To get the boot configuration script:

```
>SHOW CONFIG BOOT
```

```
boot.cfg
```

See Also LOAD CONFIG

VIEW CONFIG

CREATE CONFIG

DELETE CONFIG

Figure 1. Example output from the SHOW CONFIG command.

012345678901234567890123456789012345678901234567890123456789	01234567890123456789012345678901234567890123456789	0123456789012345678901234567890123456789
Filename	Size	Created

```

-----
boot.cfg          675          25-Feb-2001  12:01:24
remote.cfg       1987          14-Feb-2001  10:01:24
-----
Boot Configuration Script: boot.cfg
-----
    
```

Table 8. Parameters displayed in the output of the SHOW CONFIG command.

Parameter	Meaning
FILENAME	The script file name
SIZE	The script file size in bytes
CREATED	When the script has been created. CREATE CONFIG and LOAD CONFIG modify this field even if the a script with that name was already existing.
BOOT CONFIGURATION SCRIPT	This is the script that is executed when the device boots. If there isn't one "(not set)" is written.

SHOW LOADER

- Syntax** SHOW LOADER [FILE | SERVER]
- Short Syntax** SH LO [FILE | SERVER]
- Description** This command shows the default file and server used by LOAD commands. If FILE or SERVER options are given, the associated parameters are returned.
- See Also** LOAD IMAGE
 LOAD CONFIG
 SET LOADER

Figure 2. Example output from the SHOW LOADER command.

```

-----
012345678901234567890123456789012345678901234567890123456789
Loader Information
-----
File:          rg1-sip-6-0-0.bin
Server:        192.168.1.10
-----
    
```

Table 9. Parameters displayed in the output of the SET LOADER command.

Parameter	Meaning
FILE	The default file previously set with SET LOADER FILE=... command
SERVER	The default file previously set with SET LOADER SERVER=... command

SHOW SYSTEM

Syntax	SHOW SYSTEM [NAME CONTACT LOCATION PRODUCT BOOTV APPV HWREV FLASH RAM]
Short Syntax	SH SYS [NAME CONTACT LOCATION PRODUCT BOOTV APPV HWREV FLASH RAM]
Description	This command shows the major information relevant to the equipment configuration and status including the one previously set by SET SYSTEM command. To request a specific parameter, its name must be included in the command. The intent of this option is to allow the access of this information from the web interface.
See Also	SET SYSTEM

Figure 3. Example output from the SHOW SYSTEM command.

```

01234567890123456789012345678901234567890123456789
System Information
-----
General
  Name:          NAME
  Contact:       CONTACT
  Location:      LOCATION
-----
Software
  Protocol:      SIP
  Application File:  rg1-sip-6-0-0.bin
  Application Version: APPV
  Boot Version:   BOOTV
-----
Equipment
  Product Name:   PRODUCT
  Hardware Revision: HWREV
  Platform:       RG213
  Flash Size (Kbytes): FLASH
  RAM Size (Kbytes): RAM

```

Table 10. Parameters displayed in the output of the SHOW SYSTEM command.

Parameter	Meaning
NAME	System name previously set with SET SYSTEM NAME=... command
CONTACT	System contact previously set with SET SYSTEM CONTACT=... command
LOCATION	System location previously set with SET SYSTEM LOCATION=... command
Protocol	VoIP protocol (e.g. SIP)
Application File	The running application file image
APPV	Application version
BOOTV	Boot version
PRODUCT	Product name (e.g. AT-RG213)
HWREV	Hardware revision, usually a letter where A is the first
Platform	Platforms are RG203 or RG213
FLASH	Flash size in Kbytes
RAM	RAM size in Kbytes

VIEW CONFIG

Syntax	VIEW CONFIG= <i>filename</i>
Short Syntax	V CONFIG= <i>filename</i>
	where:
	<ul style="list-style-type: none"> ■ <i>filename</i> is a file name that can contain up to 20 characters excluding ; , ! @ # \$ () < > / \ " ' ~ { } [] = + & ^ <space> <tab>.
Description	This command allows the dumping of the contents of the indicated filename.

Chapter 2

IP

Introduction

This chapter describes the main features of the Internet Protocol (IP) and how to configure and operate the AT-RG213 IP interface.

IP protocols are widely used and available on nearly every hosts and PC systems. They provide a range of services including remote login, file transfer and Email.

The Internet

The Internet (with a capital “I”) is the name given to the large, worldwide network of networks based on the original concepts of the ARPAnet. A large number of government, academic and commercial organisations are connected to the Internet, and use it to exchange traffic such as Email. The Internet uses the TCP/IP protocols for all routing. In recent times the term internet (with a lowercase “i”) has also come to refer to any network (usually a wide area network) which utilises the Internet Protocol. The remainder of this chapter will concentrate on the latter definition, i.e. that of a generalised network which uses IP as the transport protocol.

The basic unit of data sent through an internet is a packet or datagram. An IP network functions by moving packets between routers and/or hosts. A packet consists of a header followed by the data (*see Figure 4*). The header

contains the information necessary to move the packet across the internet. It must be able to cope with missing and duplicated packets as well as possible fragmentation (and reassembly) of the original packet.

Packets are sent using a connectionless transport mechanism. A connection is not maintained between the source and destination addresses; rather, the destination address is placed in the header and the packet is transmitted on a best effort basis. It is up to the intermediate systems (routers and gateways) to deliver the packet to the correct address, using the information in the header.

Successive packets may take different routes through the network to the destination. There is a strong analogy with the postal delivery system in that letters are placed in individually addressed envelopes and put into the system in the 'hope' that they will arrive. Like an internet, the postal system is very reliable. In an internet, higher layers (such as TCP and Telnet) are responsible for ensuring that packets are delivered in a reliable and sequenced way.

In contrast to a connectionless transport mechanism, a connection-oriented transport mechanism requires a connection to be maintained between the source and destination for as long as necessary to complete the exchange of packets between source and destination. X.25 is an example of a connection-oriented protocol. A good analogy to X.25 would be a telephone call, in which both parties verify that they are talking to the correct person before exchanging highly sequenced data (if both talk at once then nothing intelligible results!), and the connection is maintained until both parties have finished talking. Its not hard to imagine the chaos if the telephone system delivered words in the wrong order.

Figure 4. IP packet or datagram

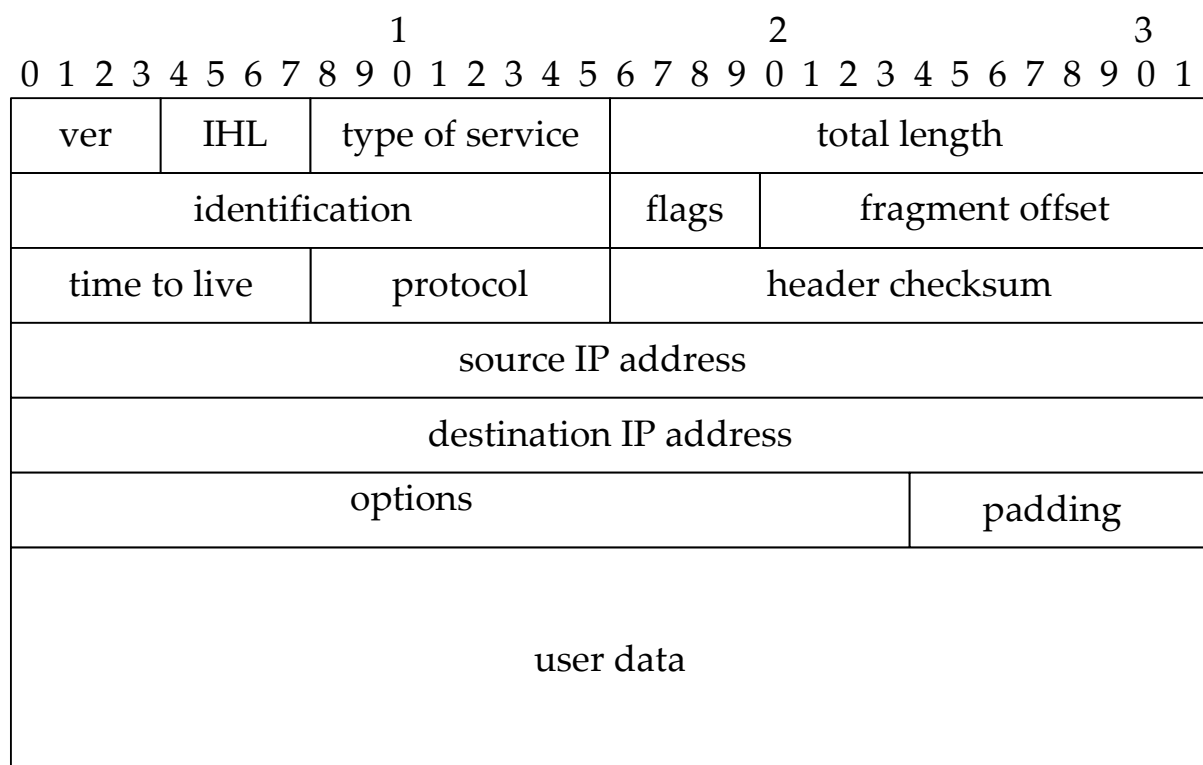


Table 11. Functions of the fields in an IP datagram

Field	Function
ver	The version of the IP protocol that created the datagram.
IHL	The length of the IP header in 32-bit words (the minimum value is 5).
Type of service	The quality of service (precedence, delay, throughput, and reliability) desired for the datagram.
Total length	The length of the datagram (both header and user data), in octets.
Identification	A 16-bit value assigned by the originator of the datagram, used during reassembly
Flags	Control bits indicating whether the datagram may be fragmented, and if so, whether other later fragments exist
Fragment offset	The offset in the original datagram of the data being carried in this datagram, for fragmented datagrams
Time to live	The time in seconds the datagram is allowed to remain in the internet system

Protocol	The high level protocol used to create the message (analogous to the type field in an Ethernet packet)
Header checksum	A checksum of the header
Source IP address	32-bit IP address of the sender
Destination IP address	32-bit IP address of the recipient
Options	An optional field primarily used for network testing or Debugging.
Padding	All bits set to zero—used to pad the datagram header to a length that is a multiple of 32 bits.
User data	The actual data being sent.

Addressing

Internet addresses are fundamental to the operation of the TCP/IP internet. Each packet must contain an internet address to determine where to send the packet. Most packets also require a source address so that the sender of the packet is known. Addresses are 32-bit quantities which are logically divided into fields. They must not be confused with physical addresses (such as an Ethernet address); they serve only to address Internet Protocol packets.

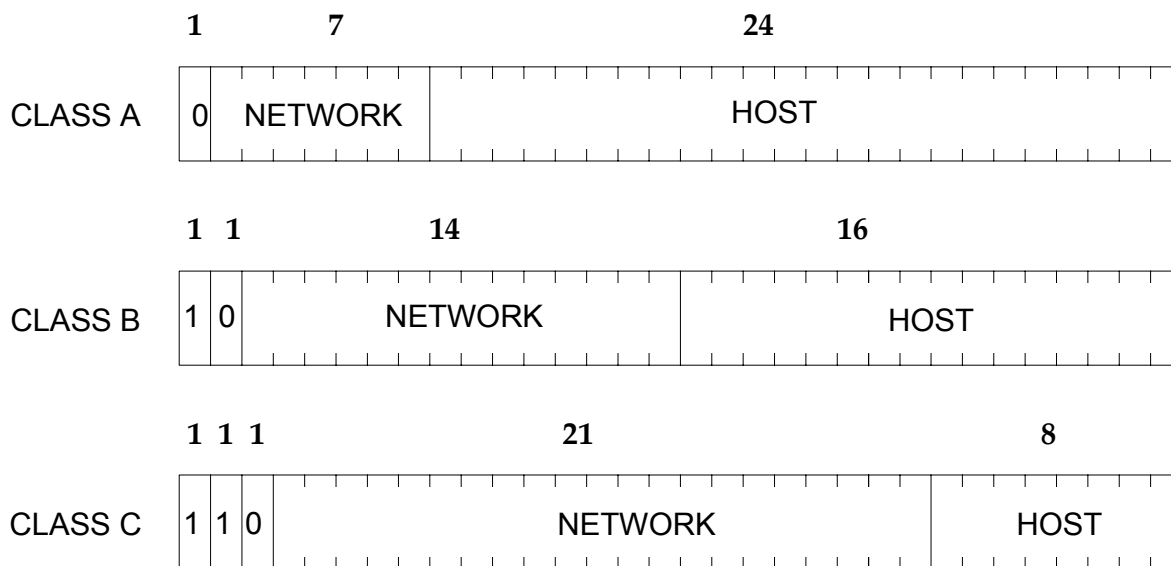
Addresses are organised into five classes (*see Table 12*).

Table 12. Internet Protocol address classes and limits on numbers of networks and hosts.

Class	Maximum number of possible networks	Maximum number of hosts per network
A	127	16,777,216
B	16,384	65,536
C	2,097,152	255
D	Reserved Class	
E	Reserved Class	

Each class differs in the number of bits assigned to the host and network portions of the address (*see Figure 5*).

Figure 5. Subdivision of the 32 bits of an Internet address into network and host fields for class A, B and C networks



The addressing scheme is designed to allow routers to efficiently extract the host and network portions of an address. In general a router is only interested in the network portion of an address.

Class A sets the Most Significant Bit (MSB) to 0 and allocates the next 7 bits to define the network and the remaining 24 bits to define the host. Class B sets the two MSBs to 10 and allocates the next 14 bits to designate the network while the remaining 16 refer to the host. Class C sets the three MSBs to '110' and allocates the next 21 bits to designate the network while the remaining 8 are left to the user to assign as host or subnet numbers.

The term host refers to any attached device on a subnet, including PCs, mainframes and routers. Most hosts are connected to only one network. In other words they have a single IP address. Routers are connected to more than one network and can have multiple IP addresses. The IP address is expressed in dotted decimal notation by taking the 32 binary bits and forming 4 groups of 8 bits, each separated by a dot.

For example:

10.4.8.2 is a class A address

10 is the DDN assigned network number

.4.8 are (possibly) user assigned subnet numbers

.2 is the user assigned host number

172.16.9.190 is a class B address

- 172 . 16 is the DDN assigned network number
- . 9 is the user assigned subnet number
- . 190 is the user assigned host number

The value 0.0.0.0 is used to define the default address, while a value of all ones in any host portion (i.e. 255) is reserved as the broadcast address. Some older versions of UNIX use a broadcast value of all zeros, therefore both the value '0' and the value '255' are reserved within any user assigned host portion. The address 172.16.0.0 refers to any host (not every host) on any subnet within the class B address 172.16. Similarly 172.16.9.0 refers to any host on subnet 9, whereas 172.16.9.255 is a packet addressed to every host on subnet 9. The router uses this terminology to indicate where packets are to be sent.

An address with '0' in the host portion refers to 'this particular host' while an address with '0' in the network portion refers to 'this particular network'. As mentioned above a value of all '1' (255) is a broadcast. To reduce loading, IP consciously tries to limit broadcasts to the smallest possible set of hosts, hence most broadcasts are 'directed'. For example 172.16.56.255 is a broadcast to subnet 56 of network 172.16. A major problem with the IP type of addressing is that it defines connections not hosts. A particular address, although it is unique, defines a host by its connection to a particular network. Therefore if the host is moved to another network the address must also change. The situation is analogous to the postal system. A related problem can occur when an organization that has a class C address finds that they need to upgrade to class B. This involves a total change of every address for all hosts and routers. Thus the addressing system is not scalable.

Subnets

Related to the two issues discussed above, the rapid growth of the Internet has meant a proliferation in the number of addresses which must be handled by the core routers. More addresses means more loading and tends to slow the system down. This is overcome by minimising the number of network addresses by sharing the same IP prefix (the assigned network number) with multiple physical networks. Generally these would all be within the same organisation, although this is not a requirement. There are two main ways of achieving this; Proxy ARP and subnetting. Proxy ARP will be discussed later in this section.

A subnet is formed by taking the host portion of the assigned address and dividing it into two parts. The first part is the 'set of subnets' while the second refers to the hosts on each subnet. For example the DDN may assign a class B address as 172.16.0.0. The system manager would then assign the lower two octets in some way which makes sense for this particular network. A common method for class B is to simply use the higher octet to refer to the subnet. Thus there are 254 subnets (0 and 255 are reserved) each with 254 hosts. These subnets need not be physically on the same media.

Generally they would be allocated geographically with subnet 2 being one site, subnet 3 another and so on. Some sites may have a requirement for multiple subnets on the same LAN.

This could be to increase the number of hosts or simply to make administration easier. In this case it is normal (but not required) that the subnets be assigned contiguously for this site. This makes the allocation of a subnet mask easier.

This mask is needed by the routers to ascertain which subnets are available at each site. Bits in the mask are set to '1' if the router is to treat the corresponding bit in the IP address as belonging to the network portion or set to '0' if it belongs to the host portion. This allows a simple bit-wise logical AND to determine if the address should be forwarded or not. Although the standard does not require that the subnet mask must select contiguous bits, it is normal practice to do so. To do otherwise can make the allocation of numbers rather difficult and prone to errors. Some example masks are:

11111111.11111111.11111111.00000000 = 255.255.255.0
 <----network-----> <subnet> <host>

This would give 254 subnets on a class B network, each with 254 hosts.

11111111.11111111.11111111.11110000 = 255.255.255.240
 <-----network-----> <----subnet----><host>

This would give 4094 subnets on a class B network, each with 14 hosts or, 14 subnets on a class C network each with 14 hosts.

Multicasting, IGMP and IGMP snooping

What is Multicasting?

Multicasting is a technique developed to send packets from one location in the Internet to many other locations, without any unnecessary packet duplication. In multicasting, one packet is sent from a source and is replicated as needed in the network to reach as many end-users as necessary.

The concept of a group is crucial to multicasting. Every multicast requires a multicast group; the sender (or source) transmits to the group address, and only members of the group can receive the multicast data. A group is defined by a Class D address.

Multicasting is not the same as broadcasting on the Internet or on a LAN. In networking jargon, broadcast data are sent to *every* possible receiver, while multicast packets are sent only to receivers that want them.

The multicast approach uses up a LOT less bandwidth. Not only does it make better use of available bandwidth it means that there is no limit to the number of hosts that can 'tune in'. Consider the case of sending video on a LAN using the 'multiple-unicast' approach. For full-motion, full-screen viewing, a video stream requires approximately 1.5 Mbps of server-to-client bandwidth.

In a unicast environment, the server must send a separate video stream to the network for each client (this consumes $1.5 \times n$ Mbps of link bandwidth where n = number of client viewers). With a 10-Mbps Ethernet interface on the server, it takes only six or seven server-to-client streams to completely saturate the network interface. With the multicast approach, there is no limit to the number of recipient hosts – as the server never has to send more than one stream, whether there is one recipient or 1000 recipients.

Of course, multicasting has to be a connectionless process. The server simply sends out its multicast UDP packets, with no idea who will be receiving them, and whether they get received. It would be quite impossible for the server to have to wait for ACKs from all the recipients, and remember to retransmissions to those recipients from whom it does not receive ACKs. Apart from anything else – the server does not know who the recipients are, or how many there are.

What is IGMP?

IGMP (Internet Group Management Protocol) is the protocol whereby hosts indicate that they are interested in receiving a particular multicast stream. When a host wants to receive a stream (in multicast jargon, this is called 'joining a group') it sends to its local router an IGMP packet containing the address of the group it wants to join – this is called an IGMP Membership report (sometimes called a Join packet).

Now – the local router generally going to be a long way from the server that is generating the stream. So, having received the IGMP join packet, the router then knows that it has to forward the multicast stream onto its LAN (if it is not doing so already). However, if the router is not already receiving the multicast stream from the server (probably many hops away) what does the router do next in order to ensure that the multicast stream gets to it?

Does it just forward the IGMP packet on up the chain back up to the server? No, it does not, because it does not necessarily know the correct path to get to the server. There is a far more elaborate process involving multicast routing protocols like PIM, DVMRP, MOSPF, etc. However, the operation of these protocols is well beyond the scope of this manual. All we need to understand here is that once the router has received the IGMP join message,

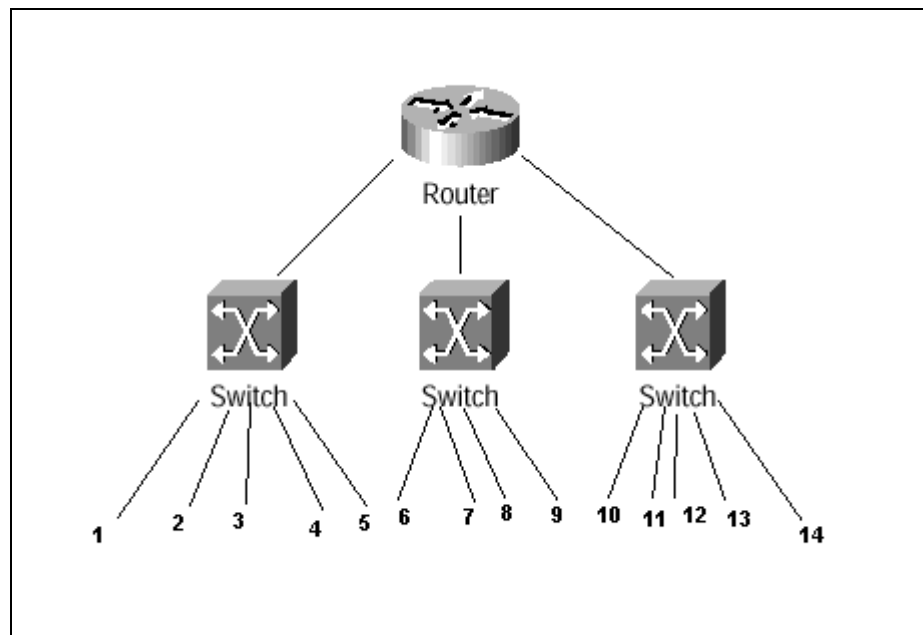
there is a process whereby all the routers back up the chain to the server now know to forward the stream to this router – ie the router has joined onto ('grafted to') the tree through which this stream is flowing.

IGMP snooping

IGMP snooping is something that layer-2 switches do to reduce the amount of multicast traffic on a LAN.

IGMP snooping is a solution to a particular problem. To get an idea of what the problem is, consider a LAN containing some layer-2 switches, and with a router as a gateway (see Figure 6):

Figure 6. IGMP snooping network layers



If individual hosts on the LAN (ie host connected to ports on the switches) wish to receive multicast streams, then they will send out IGMP joins, which will get up to the router; and the router will join into the appropriate multicast trees; and the multicast flows will then reach the router, and it will forward them into the LAN. OK, so far so good.

But, lets think what happens when the multicast flows are forwarded into the LAN. By default, when a switch receives a multicast packet, it must forward it out all its ports (except the port upon which it was received). So, if, say, ONLY host number 1 actually requests to join a particular multicast group, what will happen is that ALL the hosts on the LAN will start receiving the multicast packets, as all the switches will forward the multicast packets to all their ports.

This is rather a waste of bandwidth, and the purpose of multicasting is to make efficient use of bandwidth.

The solution to this problem is to make the layer-2 switches aware of the IGMP packets that are being passed around. That is, although the IGMP packets are destined for the router, the layer-2 switches need to 'snoop' them as they go past. Then the layer-2 switches can be aware which hosts have asked to join which multicast groups, and so will only forward the multicast data to the places where it really needs to go.

Configuration Examples

Configuring the IP address

To configure an IP interface for the Ethernet LAN connection:

```
SET IP INTERFACE=ETH0 IPADDRESS=192.168.10.5  
    MASK=255.255.255.0 GATEWAY=192.168.10.1
```

To see the IP interface configuration:

```
SHOW IP INTERFACE
```

This command shows the major information relevant to IP interface configuration. To request a specific parameter, its name must be included in the command.

DHCP Client

An IP interface can be configured either with a static IP address, or with a dynamic IP address assigned by DHCP (Dynamic Host Configuration Protocol).

To configure an IP interface to use an address assigned by DHCP, set the CONFIGURATION parameter of the interface to DHCP.

When the CONFIGURATION parameter of an IP interface is set to DHCP rather than to a static IP address, the AT-RG213's DHCP client will obtain the IP address and subnet mask for the interface, and other IP configuration parameters, from a DHCP server.

Example

To configure the interface eth0 in order to automatically obtain its IP address and subnet mask from DHCP, use the command:

```
SET IP INTERFACE=eth0 CONFIGURATION=DHCP
```

To test the interface configuration:

```
SHOW IP INTERFACE
```

This command shows the major information related to IP interface configuration. To request a specific parameter, its name must be included in the command:

```
SHOW IP INTERFACE=eth0
```

NTP Protocol

The device does not have any backup real time clock (RTC), so the NTP protocol is implemented to retrieve at every power-up the actual time from a server.

One or more NTP servers can be used, but only the first available one is taken as reference for the internal software RTC.

The above-mentioned server is then polled every 12 hours to resynchronize the local RTC.

Example 1: how to configure the NTP Server

To enable the NTP module:

```
ENABLE NTP
```



This must be called before any other command of this module.

To set the 194.35.252.7 as NTP server:

```
ADD NTP SERVER=194.35.252.7
```

This command adds a NTP server to the internal list that contains maximum 10 entries.

Exemple 2: how to configure the time zone as hours offset from the GMT.

To set the device to operate in CET (Central European Time) time zone:

```
SET NTP UTCOFFSET=+1
```

To shows the major information relevant to NTP client protocol:

```
SHOW NTP
```

Command Reference

ADD NTP SERVER

Syntax	ADD NTP SERVER=ipaddr [DEFAULT]
Short Syntax	A NTP SERVER=ipaddr [DEFAULT] where: <ul style="list-style-type: none">▪ <i>ipaddr is an ip address in dotted decimal notation</i>
Description	This command adds a NTP server to the internal list that contains maximum 10 entries. If the DEFAULT option is used, this will be the preferred server and the others will be used only on the default server failure. The first server added to the list will be always the DEFAULT even if the option is not used.
Examples	To set the 194.35.252.7 as NTP server: ADD NTP SERVER=194.35.252.7
See Also	DELETE NTP SERVER SHOW NTP

DELETE NTP SERVER

Syntax	DELETE NTP SERVER=ipaddr
Short Syntax	DEL NTP SERVER=ipaddr where: <ul style="list-style-type: none">▪ <i>ipaddr is an ip address in dotted decimal notation</i>
Description	This command deletes an NTP server from the internal list that contains maximum 10 entries.
Examples	To delete the 194.35.252.7 as NTP server: DELETE NTP SERVER=194.35.252.7
See Also	ADD NTP SERVER

DISABLE IP IGMP

Syntax	DISABLE IP IGMP
Short Syntax	DIS IP IGMP
Description	This command disables IGMP snooping support.
Examples	To disable the IGMP support: DISABLE IP IGMP
See Also	ENABLE IP IGMP SET IP IGMP SHOW IP IGMP

ENABLE IP IGMP

Syntax	ENABLE IP IGMP
Short Syntax	EN IP IGMP
Description	<p>This command enables IGMP snooping to run. Multicast traffic will be isolated per VLAN.</p> <p>The switch provides the following services for each VLAN:</p> <ul style="list-style-type: none">■ <i>IGMP Snooping</i>■ <i>IGMP proxying to present all members attached to switch as would be connected together.</i>■ <i>Supports till eight membership groups; specific multicast path are defined for each one to minimize the LAN bandwidth use.</i> <p>Remarks:</p> <p>The multicast traffic is transfered in broadcast either the IGMP module is disabled or the packets belongs not handle groups because membership group number exceeds the maximum allowed entries.</p> <p>Only IGMP v1 and v2 are supported.</p>
Examples	To enable the IGMP module: ENABLE IP IGMP
See Also	DISABLE IP IGMP SET IP IGMP SHOW IP IGMP

ENABLE NTP

Syntax	ENABLE NTP
Short Syntax	EN NTP
Description	This command enables the NTP module. This must be called before any other command of this module.
Examples	To enable the NTP module: ENABLE NTP

ENABLE TELNET

Syntax	ENABLE TELNET
Short Syntax	EN TELNET
Description	This command enables the TELNET module and allows to access CLI remotely with telnet protocol
Examples	To enable the TELNET module: ENABLE TELNET

PING

Syntax	PING ipaddr where: <ul style="list-style-type: none">▪ <i>ipaddr is an ip address in dotted decimal notation</i>
Description	This command sends IP echo request packets to the given ip address (ipaddr).
Examples	To ping 192.168.1.10: PING 192.168.1.10

SET IP IGMP

Syntax	SET IP IGMP [QUERYINTERVAL=1..65535] [LEAVETIME=0..65535] [TIMEOUT=1..65535]
---------------	---

Short Syntax	<code>S IP IGMP [QI=1..65535] [LT=0..65535] [TO=1..65535]</code>
Description	<p>This command sets operational timers for IGMP.</p> <p>The default values for these timers will suit most networks. Changing them to inappropriate values can cause IGMP to function in undesirable ways. A system administrator should only change these timer values based on a sound understanding of their interaction with other devices in the network.</p> <p>The QUERYINTERVAL parameter specifies the time interval, in seconds, at which IGMP Host Membership Queries are sent . The default is 125.</p> <p>The LEAVETIME parameter sets the duration of the Leave Period timer for the IGMP proxy application in deciseconds. The timer controls the maximum allowed time before hosts send a response to Query message issue by proxy router.</p> <p>In Proxy Router application when a Leave message is received on a port it will be catch and a Query message is sent to check if other members are present on the attached LAN. To keep valid the multicast path towards the port a subsequent Report message must be received, otherwise the multicast path will be purged and a Leave message will be forwarded either towards the port where the Router was picked out or to each other ports.</p> <p>The Query Response Interval (QRI) used in proxied Query message takes values reflecting the following scenarios:</p> <ul style="list-style-type: none"> ■ <i>No Multicast Routers are present - QRI will be equal to the LEAVETIME value.</i> ■ <i>Multicast Routers are present - QRI will take LEAVETIME value if it has been provisioned, otherwise it will be equal to the value read in last received Query message.</i> ■ <i>LEAVETIME=0 is used for fast member pruning (Fast Leaving procedure). A received Leave message will be forward at once and the multicast path will be cut.</i> <p>The TIMEOUT parameter specifies the longest interval, in seconds, for which a group will remain in the local multicast group database without the router (designated router or not) receiving a Host Membership Report for this multicast group.</p> <p>All IGMP routers to maintain their group membership databases use this TIMEOUT parameter. The default is 270. If a value is specified for QUERYINTERVAL without specifying a value for TIMEOUT, TIMEOUT is calculated as $2 * (\text{QUERYINTERVAL} + \text{QRI})$.</p> <p>The QRI added</p> <p>is the variation that hosts use when sending Host Membership Reports.</p> <p>If a timeout interval is specified, it will override any calculated value.</p>
Examples	<p>To set the IGMP query interval to 180s (3 minutes), use:</p> <pre>SET IP IGMP QUERYINTERVAL=180</pre>

See Also DISABLE IP IGMP
 ENABLE IP IGMP
 SHOW IP IGMP

SET IP INTERFACE

Syntax SET IP INTERFACE=*name* [{CONFIGURATION={DHCP | DHCPCONF [SERVERID=*id*]} | [IPADDRESS=*ipaddr*] [MASK=*ipaddr*] [GATEWAY=*ipaddr*]}]

Short Syntax S IP INT=*name* [{CONF={DHCP | DHCPCONF [SERVERID=*id*]} | [IPADDRESS=*ipaddr*] [MASK=*ipaddr*] [GATEWAY=*ipaddr*]}]

where:

- *name* is the interface short name plus the interface number (e.g. eth0, ppp1, ..)
- *ipaddr* is an ip address in dotted decimal notation
- *id* is a string that can contain upper or lower case alphanumeric characters and symbols excluding wildcards (*). The maximum number of characters is 20.

Description This command configures an IP interface on a specific port. The port can be configured in three ways: manual, DHCP and DHCPCONF. The parameters that can be set manually are address, network mask and default gateway, if any.

If the network mask is not given, the default for the class at which the address belongs is taken. For example the address 192.168.0.19 belongs to the class C subnet 192.168.0.x and will have 255.255.255.0 as default network mask.

The default configuration for the port is MANUAL.

DHCPCONF is a special DHCP configuration to help manage configuration and software upgrade centrally. SERVERID is an identifier of the server that it's supposed to manage the device.

Examples To set the 192.168.0.10 on the eth0 (Ethernet interface 0):

```
SET IP INTERFACE=eth0 IPADDRESS=192.168.0.10
```

That is equivalent to

```
SET IP INTERFACE=eth0 CONFIGURATION=MANUAL
IPADDRESS=192.168.0.10 MASK=255.255.255.0
```

To set the default gateway to 192.168.0.1:

See Also SET IP INTERFACE=eth0 GATEWAY=192.168.0.1
 SHOW IP INTERFACE

SET NTP

Syntax SET NTP UTCOFFSET=[+, -] *offset*
Short Syntax S NTP UTCOFFSET=[+, -] *offset*

where:

- *offset is the offset in hours from the GMT so must be between -12 and +12.*

Description This command configures the time zone as hours offset from the GMT.

Examples To set the device to operate in CET (Central European Time) time zone:

 SET NTP UTCOFFSET=+1

SHOW IP IGMP

Syntax	SHOW IP IGMP
Short Syntax	SH IP IGMP
Description	This command displays information about IGMP, and multicast group members for each VLAN.
See Also	DISABLE IP IGMP ENABLE IP IGMP SET IP IGMP

Figure 7. Example output from the SHOW IP command.

```

0123456789012345678901234567890123456789012345678901234567890123456789
IGMP protocol
-----
Leave Time                10.0 Sec.
Query Interval           125 Sec.
Timeout Interval        120 Sec.

Interface Name           default VLAN
Multicast Router
  Port:  WAN              Last Adv: 10.17.39.1      Refresh time: 48 Sec.

Group List
Group: 230.20.20.25
  Port:  WAN              Last Adv: Multicast Filter Refresh time: 44 Sec.
  Port:  LAN2            Last Adv: 10.17.39.3      Refresh time: 72 Sec.
Group: 230.20.20.26
  Port:  WAN              Last Adv: Multicast Filter Refresh time: 44 Sec.
  Port:  LAN2            Last Adv: 10.17.39.3      Refresh time: 72 Sec.
Group: 230.20.20.28
  Port:  LAN1            Last Adv: 10.17.39.4      Refresh time: 12 Sec.
  Port:  LAN3            Last Adv: 10.17.39.8      Refresh time: 75 Sec.
  Port:  LAN2            Last Adv: 10.17.39.231   Refresh time: 92 Sec.
Group: 230.20.20.21
  Port:  WAN              Last Adv: Multicast Filter Refresh time: 53 Sec.
  Port:  LAN1            Last Adv: 10.17.39.2      Refresh time: 68 Sec.
Group: 230.20.20.22
  Port:  LAN1            Last Adv: 10.17.39.2      Refresh time: 68 Sec.
Group: 230.20.20.24
  Port:  LAN2            Last Adv: 10.17.39.3      Refresh time: 72 Sec.
-----

```

Table 13. Parameters displayed in the output of the SHOW IP IGMP command.

Parameter	Meaning
Leave Time	Duration of the Leave Period timer.

Query Interval	Interval at which Host Membership Queries are sent.
Timeout Interval	Interval after which entries will be removed from the group database.
Interface Name	VLAN reference.
Multicast Router	Recognized Multicast route.
Group List	Membership list for this VLAN.
Group	The group multicast address. "Multicast Filter" highlights members useful to stop
Port	Port where the member is attached.
Last Adv.	The last host to advertise the membership report or query.
Refresh time	The time interval (in seconds) until the membership group will be deleted .

SHOW IP INTERFACE

Syntax	SHOW IP INTERFACE [=name {IPADDRESS MASK GATEWAY CONFIGURATION DHCPSEVER LEASE LEASESTART}]
Short Syntax	SH IP INT [=name {CONFIGURATION IPADDRESS MASK GATEWAY DHCPSEVER LEASE LEASESTART}]
	where:
	<ul style="list-style-type: none"> name is the interface short name plus the interface number (e.g. eth0, ppp1, ..)
Description	This command shows the major information relevant to IP interface configuration. To request a specific parameter, its name must be included in the command. The intent of this option is to allow the access of this information from the web interface.
See Also	SET IP INTERFACE

Figure 8. Example output from the SHOW IP INTERFACE command.

```

01234567890123456789012345678901234567890123456789
IP Interface Information
-----
Iface   IP Address   Network Mask   Def Gateway
Config DHCP Server  Lease Obtained
-----
eth0    192.168.0.1  255.255.255.0  192.168.0.1
DHCP    192.168.0.1  7200 from 1/2/01 17:56

```

Table 14. Parameters displayed in the output of the SHOW IP INTERFACE command.

Parameter	Meaning
CONFIGURATION	Manual of DHCP
IPADDRESS	Interface IP address
MASK	Network mask
GATEWAY	Default gateway
DHCPSEVER	DHCP Server, (valid only if configuration is DHCP)
LEASE	Lease time obtained in seconds (valid only if configuration is DHCP)
LEASESTART	When offer has been accepted, (valid only if configuration is DHCP)

SHOW NTP

Syntax	SHOW NTP [TIME UTCOFFSET LASTUPDATE LASTDELTA SERVERIP=servernum SERVERSTATE=servernum]
Short Syntax	SH NTP [TIME UTCOFFSET LASTUPDATE LASTDELTA SERVERIP=servernum SERVERSTATE=servernum]
	where:
	<ul style="list-style-type: none"> ■ <i>servernum is the a number between 1 and 10.</i>
Description	This command shows the major information relevant to NTP client protocol.
See Also	ADD NTP SERVER DELETE NTP SERVER

Figure 9. Example output from the SHOW NTP command.

```

01234567890123456789012345678901234567890123456789
NTP Module Information
-----
General
  Current Time:      CURRENT
  UTC Offset:       OFFSET
  Last Update:      UPDATE
  Last Delta:       DELTA
-----
Configured Servers      State
SERVER1
SERVER2                 DEFAULT
SERVER3
-----

```

Table 15. Parameters displayed in the output of the SHOW IP INTERFACE command.

Parameter	Meaning
CURRENT	Current time as reported by RTC
OFFSET	The offset in hours from the GMT time zone
UPDATE	When the internal RTC has been synchronized with the NTP server
DELTA	
SERVER	NTP Server IP addresses. The one with DEFAULT state is the currently used.

Chapter 3

DNS

The AT-AR215 Residential VoIP gateway provides a DNS client module. A primary and secondary name server can be set; a static table can be configured and also an nslookup utility is provided

Configuration Examples

To configure a primary and a secondary DNS servers in the AT-RG213 use the commands:

```
SET IP NAMESERVER=ipaddr
SET IP SECONDARYNAMESERVER=ipaddr
```

To retrieve the IP address of a certain host given its name (e.g. www.google.com) use the command:

```
NSLOOKUP HOST=www.google.com
```

To statically set in the DNS table the IP address and related host name use the command:

```
SET DNS IP HOST=hostname IPADDRESS=ipaddr
```

Command Reference

SET DNS IP

Syntax	SET DNS IP HOST=hostname IPADDRESS=ipaddress
Short Syntax	S DNS IP HOST=hostname IPADDRESS=ipaddress
	where:
	<ul style="list-style-type: none"> ■ <i>hostname is a domain name as defined in "IETF RFC-1034, 'Domain Names – Concepts and facilities'". It must be less or equal than 256 characters.</i> ■ <i>ipaddress is an ip address in dotted decimal notation</i>
Description	This command adds or modifies a static entry in the host name table.
Examples	To add the IP address for host name "Zaphod" to the host name table, use: SET DNS IP HOST= Zaphod IPADDRESS=172.16.8.3
See Also	SHOW IP HOST

SET DOMAIN

Syntax	SET DOMAIN=hostname
Short Syntax	S DO=hostname
	where:
	<ul style="list-style-type: none"> ■ <i>hostname is a domain name as defined in "IETF RFC-1034, 'Domain Names – Concepts and facilities'". It must be less or equal than 256 characters.</i>
Description	This command specifies the host domain.
Examples	To set the domain as ati.com, use: SET DOMAIN=ati.com
See Also	SET IP NAMESERVER SET IP SECONDARYNAMESERVER

SET IP NAMESERVER

Syntax	SET IP NAMESERVER=ipaddress
---------------	-----------------------------

Short Syntax	<pre>S IP NS=ipaddress</pre> <p>where:</p> <ul style="list-style-type: none">▪ <i>ipaddress is an ip address in dotted decimal notation.</i>
Description	This command specifies the IP address of a host able to act as the primary name server.
Examples	To specify the host with IP address 172.16.1.5 as a name server, use: <pre>SET IP NAMESERVER=172.16.1.5</pre>
See Also	<pre>SET IP SECONDARYNAMESERVER</pre>

SET IP SECONDARYNAMESERVER

Syntax	<pre>SET IP SECONDARYNAMESERVER=ipaddress</pre>
Short Syntax	<pre>S IP SNS=ipaddress</pre> <p>where:</p> <ul style="list-style-type: none">▪ <i>ipaddress is an ip address in dotted decimal notation.</i>
Description	This command specifies the IP address of a host able to act as the secondary name server. The request is sent to the primary name server and if a response is not received it is sent to the secondary name server.
Examples	To specify the host with IP address 172.16.1.6 as a secondary name server, use: <pre>SET IP SECONDARYNAMESERVER=172.16.1.6</pre>
See Also	<pre>SET IP NAMESERVER</pre>

SHOW DNS

Syntax	<pre>SHOW DNS [PRIP SECIP DOMAIN]</pre>
Short Syntax	<pre>SH DNS [PRIP SECIP DOMAIN]</pre> <p>where:</p> <ul style="list-style-type: none">▪ <i>PRIP is primary name server IP address.</i>▪ <i>SECIP is secondary name server IP address.</i>▪ <i>DOMAIN is domain name.</i>
Description	This command shows the DNS configuration. To get information about primary, secondary name server and domain, the command must be used without any option. To get a specific configuration the command must be used with the relative

option. The parameter value is returned as is, since this command invocation is designed for web interface.

Examples

To show only the primary name server IP address, type:

```
SHOW DNS PRIP
```

To show the entire configuration (Primary Name Server, Secondary Name Server and Domain) use:

```
SHOW DNS
```

See Also

SET DNS IP

Figure 10. Example output from SHOW DNS command.

```
01234567890123456789012345678901234567890123456789
DNS Information
-----
Primary Name Server IP      172.16.8.2 [MANUAL]
Secondary Name Server IP   172.16.8.3 [DHCP]
Domain name                 ati.com [MANUAL]
-----
```

SHOW IP HOST

Syntax SHOW IP HOST

Short Syntax SH IP HOST

Description This command displays the IP host name table.

Figure 11. Example output from the SHOW IP command.

```
012345678901234567890123456789012345678901234567890123456789
IP Address      Host Name      Alias
-----
172.16.8.2     ip4            ipaddress4
172.16.8.3     Zaphod
172.29.2.8     Admin
-----
```

NSLOOKUP HOST

Syntax NSLOOKUP HOST

Short Syntax

Description This command displays the IP address of a certain host name.

Chapter 4

SIP

Introduction

This chapter describes the main features of the SIP standard, the protocols supported, the implementation of the call processes in the AT-RG213 and how to configure and operate the AT-RG213 to provide, or connect to, a VoIP Network.

SIP Protocol

SIP (Session Initiation Protocol) is a protocol developed to assist in providing advanced telephony services across the Internet. Internet telephony is evolving from its use as a "cheap" (but low quality) way to make international phone calls to a serious business telephony capability. SIP is one of a group of protocols required to ensure that this evolution can occur.

SIP is part of the IETF standards process and is modeled upon other Internet protocols such as SMTP (Simple Mail Transfer Protocol) and HTTP (Hypertext Transfer Protocol.) It is used to establish, change and tear down (end) calls between one or more users in an IP-based network. In order to provide telephony services there is a need for a number of different standards and protocols to come together - specifically to ensure transport (RTP), signalling inter-working with today's telephony network, to be able to guarantee voice quality (RSVP, YESSIR), to be able to provide directories

(LDAP), to authenticate users (RADIUS, DIAMETER), and to scale to meet the anticipated growth curves.

SIP is described as a control protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet multimedia conferences, Internet (or any IP Network) telephone calls and multimedia distribution. Members in a session can communicate via multicast or via a mesh of unicast relations, or via a combination of these. SIP supports session descriptions that allow participants to agree on a set of compatible media types. It also supports user mobility by proxying and redirecting requests to the user's current location. SIP is not tied to any particular conference control protocol.

In essence, SIP has to provide or enable the following functions:

Name Translation and User Location

Ensuring that the call reaches the called party wherever they are located. Carrying out any mapping of descriptive information to location information. Ensuring that details of the nature of the call (Session) are supported.

Feature Negotiation

This allows the group involved in a call (this may be a multi-party call) to agree on the features supported – recognizing that not all the parties can support the same level of features. For example video may or may not be supported; as any form of MIME type is supported by SIP, there is plenty of scope for negotiation.

Call Participant Management

During a call a participant can bring other users onto the call or cancel connections to other users. In addition, users could be transferred or placed on hold.

Call feature changes

A user should be able to change the call characteristics during the course of the call. For example, a call may have been set up as 'voice-only', but in the course of the call, the users may need to enable a video function. A third party joining a call may require different features to be enabled in order to participate in the call

Protocol Components

There are two components within SIP. The SIP User Agent and the SIP Network Server. The User Agent is effectively the end system component for the call and the SIP Server is the network device that handles the signaling associated with multiple calls.

The User agent itself has a client element, the User Agent Client (UAC) and a server element, the User Agent Server (UAS.) The client element initiates the calls and the server element answers the calls. This allows peer-to-peer calls to be made using a client-server protocol.

The SIP Server element also provides for more than one type of server. There are effectively three forms of server that can exist in the network - the SIP stateful proxy server, the SIP stateless proxy server and the SIP re-direct server. The main function of the SIP servers is to provide name resolution and user location, since the caller is unlikely to know the IP address or host name of the called party. What will be available is perhaps an email-like address or a telephone number associated with the called party. Using this information, the caller's user agent can identify with a specific server to "resolve" the address information - it is likely that this will involve many servers in the network.

A SIP proxy server receives requests, determines where to send these, and passes them onto the next server (using next hop routing principals). There can be many server hops in the network.

The difference between a stateful and stateless proxy server is that a stateful proxy server remembers the incoming requests it receives, along with the responses it sends back and the outgoing requests it sends on. A stateless proxy server forgets all information once it has sent on a request. This allows a stateful proxy server to fork requests to try multiple possible user locations in parallel and only send the best responses back. Stateless Proxy servers are most likely to be the fast, backbone of the SIP infrastructure. Stateful proxy servers are then most likely to be the local devices close to the User Agents, controlling domains of users and becoming the prime platform for the application services.

A re-direct server receives requests, but rather than passing these onto the next server it sends a response to the caller indicating the address for the called user. This provides the address for the caller to contact the called party at the next server directly.

SIP addresses users by an email-like address. Each user is identified through a hierarchical URL that is built around elements such as a user's phone number or host name (for example, SIP:user@company.com). Because of this similarity, SIP URLs are easy to associate with a user's e-mail address.

SIP provides its own reliability mechanism and is therefore independent of the packet layer and only requires an unreliable datagram service. SIP is typically used over UDP or TCP.

SIP provides the necessary protocol mechanisms so that end systems and proxy servers can provide services:

- User location
- User capabilities
- User availability
- Call set-up
- Call handling
- Call forwarding, including
 - The equivalent of 700-, 800- and 900- type calls
 - Call-forwarding no answer
 - Call-forwarding busy
 - Call-forwarding unconditional
 - Other address-translation services

- Callee and calling "number" delivery, where numbers can be any (preferably unique) naming scheme
- Personal mobility, i.e., the ability to reach a called party under a single, location-independent address even when the user changes terminals
- Terminal-type negotiation and selection: a caller can be given a choice how to reach the party, e.g., via Internet telephony, mobile phone, an answering service, etc.
- Terminal capability negotiation
- Caller and callee authentication
- Blind and supervised call transfer
- Invitations to multicast conferences

When a user wants to call another user, the caller initiates the call with an invite request. The request contains enough information for the called party to join the session. If the client knows the location of the other party it can send the request directly to their IP address. If not the client can send it to a locally configured SIP network server. If that server is a proxy server it will attempt to resolve the called user's location and send the request to them. There are many ways it can do this, such as searching the DNS or accessing databases. Alternatively, the server may be a redirect server that may return the called user location to the calling client for it to try directly. During the course of locating a user, one SIP network server can, of course, proxy or redirect the call to additional servers until it arrives at one that definitely knows the IP address where the called user can be found.

Once found, the request is sent to the user, and from there several options arise. In the simplest case, the user's telephony client receives the request—that is, the user's phone rings. If the user takes the call, the client responds to the invitation with the designated capabilities* of the client software and a connection is established. If the user declines the call, the session can be redirected to a voice mail server or to another user.

"Designated capabilities" refers to the functions that the user wants to invoke. The client software might support videoconferencing, for example, but the user may only want to use audio conferencing. Regardless, the user can always add functions—such as videoconferencing, white-boarding, or a third user—by issuing another invite request to other users on the link.

SIP has two additional significant features. The first is a stateful SIP proxy server's ability to split or "fork" an incoming call so that several extensions can be rung at once. The first extension to answer takes the call. This feature is handy if a user is working between two locations (a lab and an office, for example), or where someone is ringing both a boss and their secretary.

The second significant feature is SIP's unique ability to return different media types. Take the example of a user contacting a company. When the SIP server receives the client's connection request, it can return to the customer's phone client via a Web Interactive Voice Response page (IVR or could use the term Interactive Web Response or IWR), with the extensions of the available departments or users provided on the list. Clicking the appropriate link sends an invitation to that user to set up a call.

SIP Messages

A SIP request message consists of three elements:

- Request Line
- Header
- Message Body

A SIP response message consists of three elements:

- Status Line
- Header
- Message Body

The Request line and header field define the nature of the call in terms of services, addresses and protocol features. The message body is independent of the SIP protocol and can contain anything.

SIP defines the following methods (SIP uses the term 'method' to describe the specification areas):

- Invite – invites a user to join a call.
- Bye – terminates the call between two of the users on a call
- Options – requests information on the capabilities of a server
- Ack – confirms that a client has received a final response to an INVITE
- Register – provides the map for address resolution, letting a server know the location of other users.
- Cancel – ends a pending request, but does not end the call

The INFO method, for mid-session signalling, is also being added
Related Standards Activity.

AT-RG213 Call Processes

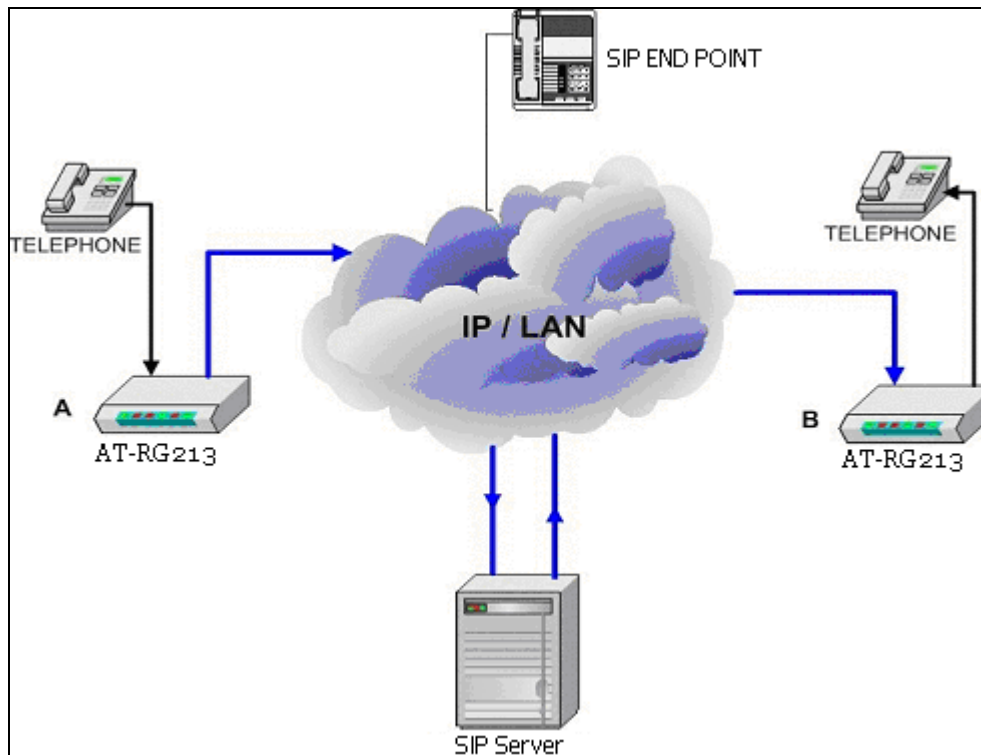
The AT-RG213 can communicate with the following devices:

- *Another terminal on the IP network such as the AT-RG213.*
- *Any LAN SIP endpoint on the IP network, for instance:*
 - *a Soft Phone*
 - *an IP phone directly connected to the IP network*
- *A PSTN phone or fax. However, the AT-RG213 would need to contact a PSTN gateway*

Calls Involving Another Terminal

The following example described in Figure 12 illustrates how to reach a phone or fax on another AT-RG213 terminal.

Figure 12. Phone --> AT-RG213 (A) --> AT-RG213 (B) --> Phone



A user makes a call with the phone connected to an AT-RG213, which in turn contacts another AT-RG213, then reaches the corresponding phone.

Calls Involving a Terminal and a SIP Endpoint

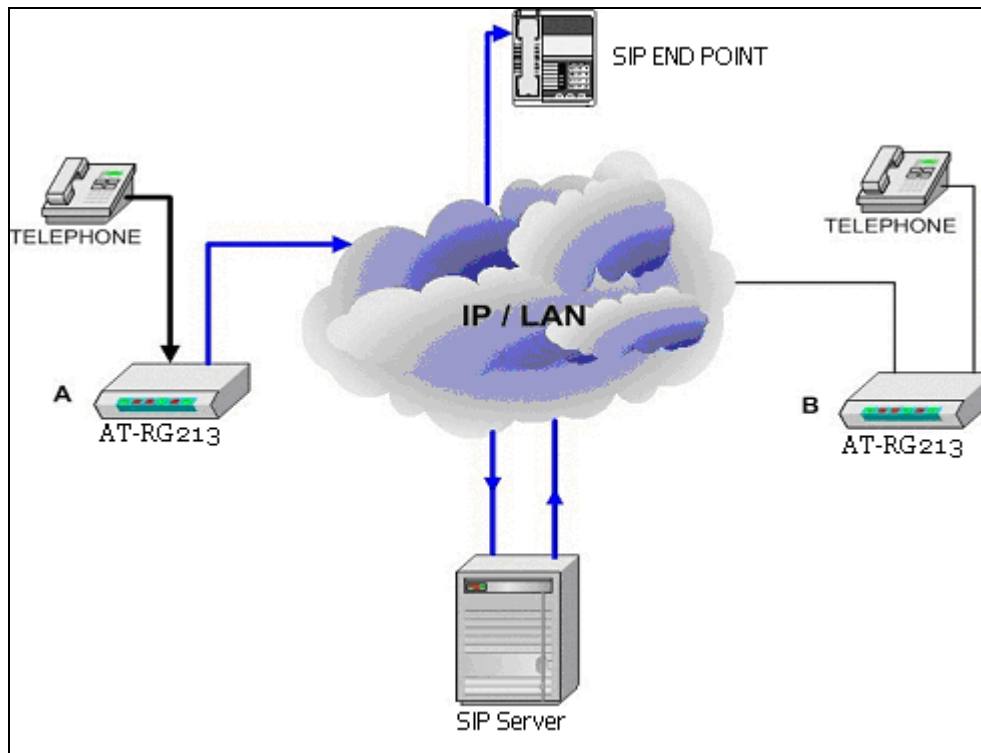
The following examples illustrate how a phone connected to an AT-RG213 terminal can communicate with a LAN SIP endpoint on the IP network. Such endpoints could be:

- *a Soft Phone*
- *an IP phone directly connected to the IP network*

Exemple 1: Phone --> AT-RG213 (A)--> LAN SIP endpoint

A user makes a call with the phone connected to an AT-RG213, which reaches the corresponding LAN SIP endpoint on the IP network (*see Figure 13*).

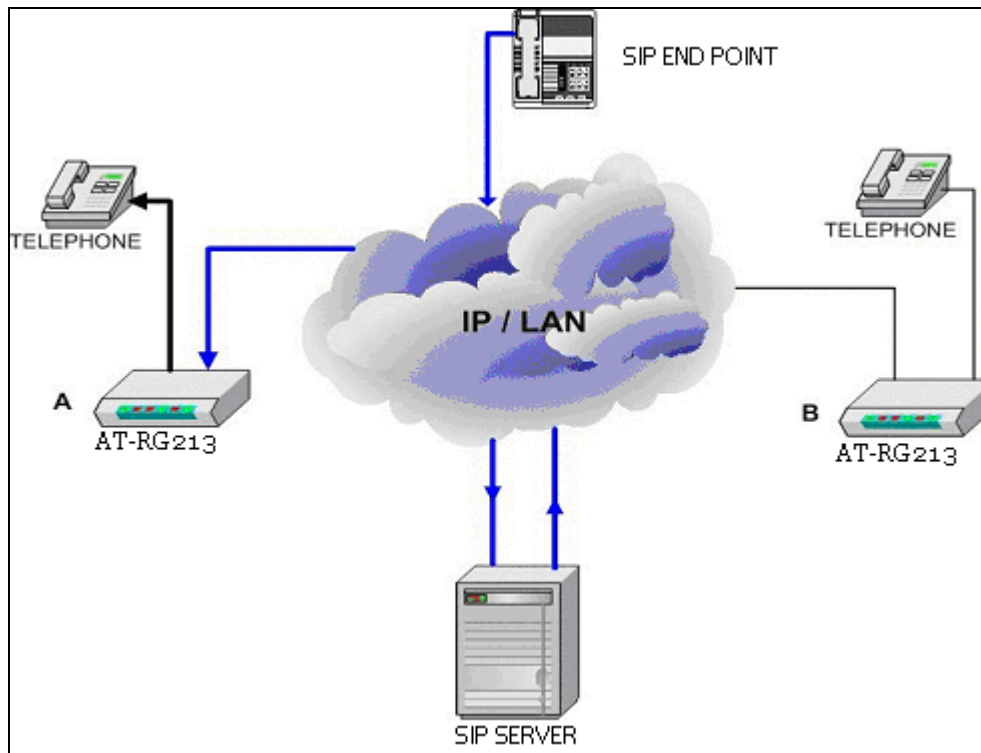
Figure 13. Phone --> AT-RG213 (A)--> LAN SIP endpoint



Exemple 2: LAN SIP endpoint --> AT-RG213 --> Phone

A LAN SIP endpoint contacts the AT-RG213, which reaches the corresponding phone connected to the AT-RG213 terminal (see Figure 14).

Figure 14. LAN SIP endpoint --> AT-RG213 --> Phone



Configuration Examples

Create and configure SIP Port

To create and configure a SIP port, follow the steps below:

Step 1: Enable SIP module:

```
ENABLE SIP
```



This command must be executed before any other command concerning this session

Step 2: Create and configure the SIP protocol on a specific voice port and assign the telephone number.

For example, to assign the telephone number 1000 to the port tel1 (physical port 0) and enable all allowed coding methods, using the IP Address 192.168.0.10 as Location and Proxy server and alliedtelesyn.com as Domain use:


```
CREATE SIP PORT=0 PHONENUMBER=1000
      LOCATIONSERVER=192.168.0.10
      PROXYSERVER=192.168.0.10
      DOMAIN=alliedtelesyn.com CAPABILITY=ALL
```

With CAPABILITY=ALL all supported voice codec are allowed (PCMU, PCMA and G723).

Step 3: Test the correct configuration of the SIP ports:

```
SHOW SIP PORT
```

Step 4: Save the configuration for example in SIP.cfg:

```
CREATE CONFIG=SIP.cfg
```

Command Reference

CREATE SIP PORT

Syntax

```
CREATE SIP PORT=port PHONENUMBER=number
      DOMAIN=domain
      PROXYSERVER=ipadd[:ippport] [;ipadd[:ippport]]
      [AUTH-USERNAME={NONE|username}] [AUTH
      PASSWD={NONE|password}]
      [LOCATIONSERVER=ipadd[:ippport] [;ipadd[:ippport]]]
      [CAPABILITY=capability[;capability]]
      [RTPPORT=ippport] [DSCP=dscppriority|TOS=tospriority]
```

Short Syntax

```
C SIP PORT=port PHNO=number DO=domain
PS=ipadd[:ippport] [;ipadd[:ippport]]
[A-USR={NONE|username}] [A-PWD={NONE|password}]
[LS=ipadd[:ippport] [;ipadd[:ippport]]] [CAP=
capability[;capability]] [RP=ippport] [DSCP=dscppriori
ty|TOS=tospriority]
```

where:

- *port* is the physical port number (can be 0 or 1)
- *ippport* is the IP port number within 1..65535 range
- *number* is the phone number of 20 digits maximum
- *domain* can either be an ip address in dotted decimal notation or a number of words in lower case alphanumeric characters (a-z) and (0-9) separated by a dot (.).

- *ipadd* is an ip address in dotted decimal notation
- *capability* is the coding methods used when setting up a call. Currently PCMU, PCMA and G723 are supported. Use ALL to indicate all the above.
- *username* is a max 128 chars string used to authenticate the AT-RG213 with a proxy server that requires SIP authentication.
- *password* is a max 16 chars used to authenticate the AT-RG213 with a proxy server that requires SIP authentication.
- *rtpport* is the port number that will be used for listen the RTP messages. This value is the range 5061..49151. Only an even number can be assigned. This is because the odd numbers are reserved for RTCP protocol. If not set the *rtpport* will be assigned dynamically.
- *tospriority* is a number from 0 to 7
- *dscppriority* is a number from 0 to 63

Description

This command enables the SIP protocol on a specific physical phone port. The port URI is:

PHONENUMBER@DOMAIN

The port will be register to LOCATIONSERVER with the above-mentioned URI, if at least LOCATIONSERVER is given.

When a number is dialled, the invite message is sent to the PROXYSERVER.

When making a call, the preferred coding methods for the voice will be the list given with the CAPABILITY option or G711 u-law (PCMU).

The available coding algorithms are:

- *G711 u-law (PCMU)*
- *G711 a-law (PCMA)*
- *G723.1 (G723)*
- *All the above (ALL)*

As described in the SIP standard (RFC 2544) every SIP user can be requested to authenticate on a proxy server in order to use its services. For this purpose the parameters AUTH-USERNAME and AUTH-PASSWD are used. This command enables the SIP protocol on a specific physical phone port. The PHONENUMBER and PORT are the only required options.

Examples

To enable the SIP protocol on the first VoIP port with the 000555 phone number in the alliedtelesyn.com domain using 192.168.0.10 as both location and proxy servers. The preferred coding algorithm will be G723. Username and password set for the SIP port are eurord@alliedtelesyn.com and "welcome"

```
C SIP PORT=0 PHNO=000555 AUTH-
```

```
USR=eurord@alliedtelesyn.com A-PWD=welcome  
PS=192.168.0.10 DO=alliedtelesyn.com  
LS=192.168.0.10 CAP=G723; PCMU
```

DELETE SIP PORT

Syntax	DELETE SIP PORT= <i>port</i>
Short Syntax	D SIP PORT= <i>port</i>
	where:
	▪ <i>port is the physical port number (can be 0 or 1)</i>
Description	This command allows deleting a port from the SIP stack. Any ongoing call will be terminated as effect of command execution.
Examples	To delete the port 0: DELETE SIP PORT=0

DISABLE SIP

Syntax	DISABLE SIP
Short Syntax	DIS SIP
Description	This command disables the SIP module and frees all the allocated resources. Please note that this command terminates any ongoing call.
Examples	To delete enable the SIP module: DISABLE SIP

ENABLE SIP

Syntax	ENABLE SIP [DEFAULTPORT= <i>port</i>] [NATIP= <i>ipaddr</i>]
Short Syntax	EN SIP [DP= <i>port</i>] [NI= <i>ipaddr</i>]
Description	This command enables the SIP module. This must be called before any other command of this section. If the AT-RG213 is behind a NAT it is possible to SET the NAT IP address

and the PORT number that the SIP protocol will use for signalling.

Examples To enable the SIP module behind a NAT with IP address 10.10.1.10 using 5050 as the signalling port:

```
ENABLE SIP NATIP=10.10.1.10 DEFAULTPORT=5050
```

SET SIP PORT

Syntax

```
SET SIP PORT=port PHONENUMBER=number DOMAIN=domain
PROXYSERVER=ipadd[:ippport] [;ipadd[:ippport]]
[AUTH-USERNAME={NONE|username}]
[AUTH-PASSWD={NONE|password}]
[LOCATIONSERVER=ipadd[:ippport] [;ipadd[:ippport]]]
[CAPABILITY=capability[;capability]]
[RTPPORT=ippport] [DSCP=dscppriority|TOS=tospriority]
```

Short Syntax

```
SET SIP PORT=port PHNO=number DO=domain
PS= ipadd[:ippport] [;ipadd[:ippport]]
[A-USR={NONE|username}] [A-PWD={NONE|password}]
[LS=ipadd[:ippport] [;ipadd[:ippport]]]
[CAP=capability[;capability]] [RP=ippport]
[DSCP=dscppriority|TOS=tospriority]
```

where:

- *port is the physical port number (can be 0 or 1)*
- *ippport is the IP port number within 1..65535 range.*
- *number is the phone number of 20 digits maximum*
- *domain can either be an ip address in dotted decimal notation or a number of words in lower case alphanumeric characters (a-z) and (0-9) separated by a dot (.) up to 30 characters.*
- *ipadd is an ip address in dotted decimal notation*
- *capability is the coding methods used when setting up a call. Currently PCMU, PCMA G723 and G729 are supported*
- *username is a max 128 chars string used to authenticate the AT-RG213 with a proxy server that requires SIP authentication.*
- *password is a max 16 chars used to authenticate the AT-RG213 with a proxy server that requires SIP authentication.*
- *rtpport is the port number that will be used for listen the RTP messages. This value is the range 5061..49151. Only an even number can be assigned. This is because the odd numbers are reserved for RTCP protocol. If not set the rtpport*

will be assigned dynamically.

- *tospriority is a number from 0 to 7*
- *dscppriority is a number from 0 to 63*

Description This command allows to set different parameters of an already created port. For the option meaning please refer to the CREATE SIP PORT command.

Examples To change a port 1 phone number:

```
SET SIP PORT=0 PHONENUMBER=000888
```

SHOW SIP PORT

Syntax SHOW SIP [DEFAULTPORT] | [NATIP] | [PORT=port
[PHONENUMBER | DOMAIN | AUTHORIZATION
LOCATIONSERVER | PROXYSERVER | REGISTERED |
CAPABILITY | RTPPORT | TOS | DSCP]]

Short Syntax SH SIP [DP] | [NI] | [PORT=port [PHONENUMBER |
DOMAIN | AUTHORIZATION LOCATIONSERVER | PROXYSERVER
| REGISTERED | CAPABILITY | RTPPORT | TOS | DSCP]]

Description This commands shows the SIP ports configuration. To get information on all the ports the command must be used without any option. To get a specific parameter, like PHONENUMBER, the port must be indicated along with the required filed. The parameter is returned as is, since this command invocation is designed for web interface.

Figure 15. Example output from the SHOW SIP PORT command.

```
01234567890123456789012345678901234567890123456789
SIP Port information
-----
Default port          5050
NAT IP Address       10.10.1.10

Port 0
  Phone Number       000555
  Authorization      UserName: "eurord@alliedtelesyn.com"
                    Password: "welcome"
  Domain             alliedtelesyn.com
  Location Server    192.168.0.5
  Proxy Server       192.168.0.5
  TOS                 0
  Registered         YES
  Capability          PCMU
                    G723
```

RTP port	dynamic assignment

Table 16. Parameters displayed in the output of the SHOW SIP PORT command.

Parameter	Meaning
DEFAULTPORT	The SIP signalling port number
NAT IP	The NAT IP address
PHONE NUMBER	The port phone number
DOMAIN	The port assigned SIP domain
LOCATION SERVER	The server where the port register itself
PROXY SERVER	The server where the port sends invites
TOS	The TOS value
REGISTERED	YES if the port is successfully registered to the location servers
CAPABILITY	The list of capabilities used during call setup. The first one has the highest priority
RTP PORT	The set RTP port

Chapter 5

SNMP

Introduction

Simple Network Management Protocol (SNMP)

The device can be monitored/configured with SNMP protocol via private mibs.

The Simple Network Management Protocol (SNMP) is the network management protocol of choice for the Internet and IP-based internetworks.

The SNMP protocol provides a mechanism for management entities, or stations, to extract information from the Management Information Base (MIB) of a managed device.

The standard way of accessing information contained in a MIB file is to use a Network Management Station (NMS), typically a PC or workstation, to send commands to the managed device using the SNMP protocol.

SNMP can use a number of different protocols as its underlying transport mechanism, but the most common transport protocol, and the only one supported by AT-RG213, is UDP. SNMP trap messages are sent to UDP port 162; all other SNMP messages are sent to UDP port 161.

Communities and Views

A community is a relationship between an NMS and an agent. The community name is used like a password for a trivial authentication scheme.

An SNMP MIB view is a arbitrary subset of objects in the MIB. Objects in the view may be from any part of the object name space, and not necessarily the same sub-tree.

An SNMP community profile is the pairing of an SNMP access mode (read-only or read-write) with the access mode defined by the MIB for each object in the view. A pairing of an SNMP community and an SNMP community profile determines the level of access that the agent affords to an NMS that is a member of the specified community. When an agent receives an SNMP message it checks the community name encoded in the message. If the agent knows the community name, the message is deemed to be an authentic SNMP message and the sending SNMP entity is accepted as a member of the community.

The community profile associated with the community name then determines the sender's view of the MIB and the operations that can be performed on objects in the view.

Configuration Examples

The following example illustrates the steps required to configure the SNMP agent.

In this example, the management station "NMS" (IP address 192.168.10.5) will be used to both monitor and manage devices on the network using SNMP set messages.



The IP module must be enabled and correctly configured in order to allow the remote access to the SNMP agent, since the IP module handles the UDP datagrams used to transport SNMP messages.

Example 1: configure SNMP

Step 1: Enable the SNMP agent:

```
ENABLE SNMP
```

Step 2: Create a community with write access for the central NMS.

To create a community called "private", with write access for use only by the central network management station at 192.168.0.11:

```
SET SNMP COMMUNITY SET=private
SET SNMP MANAGER=192.168.0.11
```


Step 3: Check the configuration.

To check that the current configuration of the SNMP communities matches the desired configuration:

```
SHOW SNMP
```

Command Reference

DISABLE SNMP

Syntax	DISABLE SNMP
Short Syntax	DIS SNMP
Description	This command disables the SNMP module and frees all the allocated resources.
Examples	To disable the SNMP module: DISABLE SNMP

ENABLE SNMP

Syntax	ENABLE SNMP
Short Syntax	EN SNMP
Description	This command enables the SNMP module. This must be called before any other command of this section.
Examples	To enable the SNMP module: ENABLE SNMP

SET SNMP COMMUNITY

Syntax	SET SNMP COMMUNITY {SET GET TRAP}=name
Short Syntax	S SNMP COMM {SET GET TRAP}=name

where:

- *name* is the name of specified community (can be any alphanumeric string) which serves as a password for either retrieving (GET), modifying (SET) or accepting trap messages (TRAP). The maximum number of characters is 200.

Description This command sets one COMMUNITY name at time. If these community names are not defined, SNMP module cannot work, being unable to manage SNMP command. Widely used names are “public” for GET and TRAP community, and “private” for SET community.

Examples To modify COMMUNITY SET name:

```
SET SNMP COMMUNITY SET=private
```

SET SNMP MANAGER

Syntax SET SNMP MANAGER=ipaddress

Short Syntax S SNMP MAN=ipaddress

where:

- *ipaddress* is the an ip address in dotted decimal notation, of TRAP manager server

Description This command sets the ip address of the machine SNMP agent sends trap messages to.

Examples To set snmp MANAGER:

```
SET SNMP MANAGER=192.160.0.11
```

SHOW SNMP

Syntax SHOW SNMP [COMMUNITY = {SET | GET | TRAP}] | [MANAGER]

Short Syntax SH SNMP [COMMUNITY = {SET | GET | TRAP}] | [MANAGER]

Description This commands shows SNMP module configuration.

Figure 16. Example output from the SHOW SNMP command.

```
01234567890123456789012345678901234567890123456789
```

SNMP Information	
Set Community	private
Get Community	public
Trap Community	public
Manager	192.160.0.11

Table 17. Parameters displayed in the output of the SHOW SNMP command.

Parameter	Meaning
STATUS	The module can be in the ENABLED or DISABLED state
SET	Set community name, e.g. private
GET	Get community get name, e.g. public
TRAP	Trap community name e.g. public
MANAGER	Trap manager ip address: ip where snmp agent send any trap

Chapter 6

L2TP

L2TP Introduction

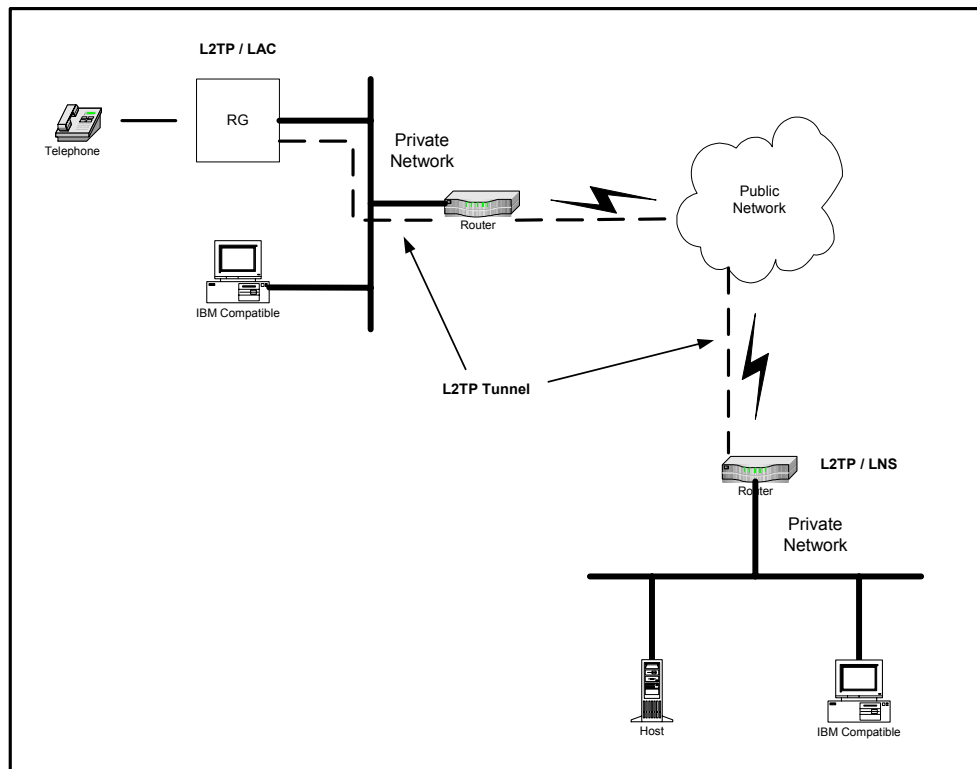
L2TP is a real tunneling protocol, much more elaborate protocol than other tunneling protocols i.e. GRE. There are multiple levels of negotiation at the connection setup time – a tunnel is negotiated, and then a call is negotiated within the tunnel, and then a PPP link is negotiated within the call.

Basically, the purpose of L2TP is to tunnel a PPP link across the Internet. So, a remote user can have a PPP connection to a central site, or two offices can have a PPP connection to each other. This PPP connection, although across the Internet, can be treated as though it were a direct connection over a leased line, and all the richness of the PPP protocol can be used. This provides a simple model for the setup at each end – all the complexity is confined to the protocol implementation in the end-point routers.

The AT-RG213 provides the tunneling of PPP packets across an IP Network in a transparent way to both end-points.

The AT-RG213 acts as an L2TP Access Concentrator (LAC) creating a tunnel across the IP infrastructure from itself (LAC) and the L2TP Network Server (LNS), enabling Point-to-Point Protocol layer frames to be encapsulated and carried across the Internet. *Figure 17* shows the related network model.

Figure 17. L2TP network model



Command Reference

ENABLE L2TP

Syntax	ENABLE L2TP
Short Syntax	EN L2TP
Description	This command enables the L2TP module. This must be called before any other command of this section.
Examples	To enable the L2TP module, use the command: ENABLE L2TP
See also	DISABLE L2TP CREATE L2TP DELETE L2TP SHOW L2TP

DISABLE L2TP

Syntax	DISABLE L2TP
Short Syntax	DIS L2TP
Description	This command disables the L2TP module, closes session and tunnel active and release all the allocated resources.
Examples	To disable the L2TP tunnel, use the command: DISABLE L2TP
See also	ENABLE L2TP CREATE L2TP DELETE L2TP SHOW L2TP

CREATE L2TP

Syntax	CREATE L2TP LNSIP= <i>ipaddr</i> LOCALTUNNELIP= <i>ipaddr</i> [PASSWD= <i>passwd</i>]
	where:
	<ul style="list-style-type: none"> ■ <i>ipaddr</i> : is an IP address in dotted decimal notation. ■ <i>passwd</i> : is a character string, 1 to 20 characters in length, in either lower or upper case. Valid characters are letters (a ÷ z, A ÷ Z) and digits (0 ÷ 9). The string cannot contain any spaces.
Short Syntax	C L2TP LNSIP= <i>ipaddr</i> LTUNIP= <i>ipaddr</i> [PASSWD= <i>passwd</i>]
Description	<p>This command creates a L2TP tunnel between the RG and the LNS server specified into the command line.</p> <p>If an error occurs during the tunnel establishment, this procedure is repeated every 30 seconds until the tunnel establishment process is complete.</p> <p>If one of Call Disconnect Notify or Stop Control Connection Notification message is received the session and the tunnel will be closed; after 30 seconds the RG will start retrying to establish a new tunnel session.</p> <p>The LNSIP parameter specifies the IP address of the remote L2TP server. The LOCALTUNNELIP parameter specifies the IP address of the local L2TP LAC. The PASSWD parameter specifies a password to be used to authenticate the tunnel creation with the remote L2TP server (encrypted using MD5 method).</p> <p>This is the password that LNS is receiving from RG.</p>
Examples	To create a L2TP tunnel between the local L2TP LAC with IP address

20.20.20.1 and the remote L2TP server with IP address 20.20.20.2, using the authentication password "test", use the command:

```
CREATE L2TP LNSIP=20.20.20.2
LOCALTUNNELIP=20.20.20.1 PASSWD=test
```

See also

- ENABLE L2TP
- DISABLE L2TP
- DELETE L2TP
- SHOW L2TP

DELETE L2TP

Syntax DELETE L2TP LNSIP=*ipaddr* LOCALTUNNELIP=*ipaddr*
[PASSWD=*passwd*]

where:

- *ipaddr* : is an IP address in dotted decimal notation.

Short Syntax D L2TP LNSIP=*ipaddr* LTUNIP=*ipaddr* [PASSWD=*passwd*]

Description This command deletes a L2TP tunnel between the RG and the LNS server specified into the command line.

The LNSIP parameter specifies the IP address of the remote L2TP server. The LOCALTUNNELIP parameter specifies the IP address of the local L2TP LAC.

Examples To delete a L2TP tunnel between the local L2TP LAC with IP address 20.20.20.1 and the remote L2TP server with IP address 20.20.20.2, use the command:

```
DELETE L2TP LNSIP=20.20.20.2
LOCALTUNNELIP=20.20.20.1
```

See also

- ENABLE L2TP
- DISABLE L2TP
- CREATE L2TP
- SHOW L2TP

SHOW L2TP

Syntax SHOW L2TP

Short Syntax SH L2TP

Description This command shows the L2TP tunnel configuration and its status.

Examples To see the L2TP tunnel configuration and its status, use the command:

```
SHOW L2TP
```

See also ENABLE L2TP
DISABLE L2TP

Figure 18. Example output from the SHOW L2TP command

```
L2TP Configuration
-----
Enabled
  Session              Created
  LNS IP               20.20.20.2
  Configured Tunnel IP 20.20.20.1
  Negotiated Tunnel IP 20.20.20.1
  Remote Tunnel IP     20.20.20.2
  Password             test
  Tunnel Status        Active
  Tunnel ID            1234
  Session ID           5678
  Call Serial Num.     10
  LCP Mru               1500
  LCP Magic Num.       14234
-----
```

Table 18. Parameters displayed in the output of the SHOW L2TP command

Parameter	Meaning
LNS IP	IP Address of remote L2TP server.
CONF. TUNNEL IP	IP Address of local L2TP tunnel.
NEGOT. TUNNEL IP	Negotiated IP Address of local L2TP tunnel.
REMOTE TUNNEL IP	IP Address of remote L2TP tunnel.
PASSWORD	Password used to authenticate the tunnel.
TUNNEL STATUS	Actual L2TP tunnel state.
TUNNEL ID	L2TP Tunnel ID.
SESSION ID	L2TP Session ID.
CALL SERIAL NUM.	L2TP Call Serial Number.
LCP MRU	Maximum Receive Unit of the PPP session.
LCP MAGIC NUM.	Magic Number of the PPP session.

Chapter 7

Phone

Introduction to FXS Ports

A Foreign Exchange Station (FXS) interface connects directly to a standard analog telephone, fax machine or similar device and supplies ring, voltage and dial tone. In AT-RG213, FXS ports are assigned to tel1 and tel2, that correspond respectively to physical port 0 and 1 and support only analog telephones.

In the next paragraphs, the main functions and features of FXS analogue interface and the specification of the PSTN line management in AT-RG213 device are described.

PSTN Line management

Table 19 shows how the PSTN line is managed in the various cases. Note that if a port is not created, then no tone will be provided.

Table 19. PSTN Line Management

SUPPLY POWER	VoIP Port 0 STATUS	VoIP Port 1 STATUS	VoIP Port 0 VoIP Call Status	VoIP Port 1 VoIP Call Status	PSTN line management
OFF	Not created Not registred	Not created Not registred	N/A	N/A	PSTN line will be available on both ports both for incoming and outgoing calls
ON and VoIP module Disabled	Not created Not registred	Not created Not registred	N/A	N/A	PSTN line will be available on both ports both for incoming and outgoing calls
ON and VoIP module Enabled	Not created Not registred	Not created Not registred	N/A	N/A	PSTN line will be NOT available on both ports both for incoming and outgoing calls
ON	Created Not registred	Not created Not registred	N/A	N/A	PSTN line will be available only on Port 0 both for incoming and outgoing calls
ON	Created Registred	Not created Not registred	No VoIP call running	N/A	PSTN line will be available only on Port 0 both for incoming and outgoing calls
ON	Created Registred	Not created Not registred	VoIP call is running	N/A	PSTN line will be available only on Port 0 both for incoming and outgoing calls (Note 1)
ON	Not created Not registred	Created Not registred	N/A	N/A	PSTN line will be available only on Port 1 both for incoming and outgoing calls
ON	Not created Not registred	Created Registred	N/A	No VoIP call running	PSTN line will be available only on Port 1 both for incoming and outgoing calls
ON	Not created Not registred	Created Registred	N/A	VoIP call is running	PSTN line will be available only on Port 1 both for incoming and outgoing calls (Note 1)
ON	Created Not registred	Created Not registred	N/A	N/A	PSTN line will be available on both ports both for incoming and outgoing calls (Note 2)
ON	Created Registred	Created Not registred	No VoIP call running	N/A	PSTN line will be available on both ports both for incoming and outgoing calls (Note 2)
ON	Created Registred	Created Not registred	VoIP call is running	N/A	PSTN line will be available on both ports both for incoming and outgoing calls (Note 3)
ON	Created Not registred	Created Registred	N/A	No VoIP call running	PSTN line will be available on both ports both for incoming and outgoing calls (Note 2)
ON	Created Not registred	Created Registred	N/A	VoIP call running	PSTN line will be available on both ports both for incoming and outgoing calls (Note 4)
ON	Created Registred	Created Registred	No VoIP call is running	No VoIP call is running	PSTN line will be available on both ports both for incoming and outgoing calls (Note 2)
ON	Created Registred	Created Registred	VoIP call is running	No VoIP call is running	PSTN line will be available on both ports both for incoming and outgoing calls (Note 3)
ON	Created Registred	Created Registred	No VoIP call running	VoIP call is running	PSTN line will be available on both ports both for incoming and outgoing calls (Note 4)
ON	Created Registred	Created Registred	VoIP call is running	VoIP call is running	PSTN line will be available on both ports both for incoming and outgoing calls (Note 5)

Note 0

If the PSTN line is the default mode and PSTN line is used by one port, then off hooking the other phone the user will hear a busy tone. In order to make a VoIP call it will be needed to digit the set prefix.

Note 1

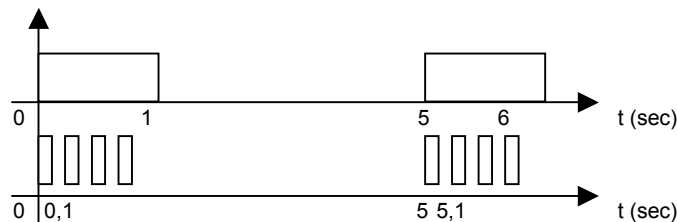
In this case, if the AT-RG213 has an incoming PSTN call, it will signal the incoming PSTN call using a tone that is ON by default (a parameter in the SET phone command will permit to modify this default CWAITT from ON to OFF).

This tone has:

- the same periodicity of RING provided by the PSTN
- a fixed frequency (425 Hz) and duration (see diagram below)
- this tone will be provided by default for 30 secs (if the caller from PSTN hang up the phone before 30 secs the tone will be stopped); a parameter in the SET phone command will permit to modify this default CWAITD from 0 to 60 secs)
- if the user closes the running VoIP call hanging up the phone, then the phone will RING and it will be able to answer to the incoming PSTN call.

As an example *Figure 19* shows, in the upper diagram the RING tone provided in Italy from the PSTN, and in the lower diagram the tone that will be generated by the AT-RG213.

Figure 19. RING tone diagram

**Note 2**

In case of an incoming PSTN call port 0 will ring.

Note 3

In case of an incoming PSTN call, port 1 will ring.

Note 4

In case of an incoming PSTN call, port 0 will ring.

Note 5

In this case, if the AT-RG213 has an incoming PSTN call, it will signal to the both ports the PSTN incoming call with a tone, that is ON by default (a

parameter in the SET phone command will permit to modify this default CWAITT from ON to OFF).

This tone has:

- the same periodicity of RING provided by the PSTN,
- a fixed frequency (425 Hz) and duration (see diagram)
- this tone will be provided by default for 30 secs (if the caller from PSTN hang up the phone before 30 secs the tone will be stopped); a parameter in the SET phone command will permit to modify this default CWAITD from 0 to 60 secs)
- if the port 0 closes the running VoIP call hanging up the phone, then the related phone will RING (at the same time the tone will be stopped on the other phone) and the user will be able to answer to the incoming PSTN call,.
- if the port 1 closes the running VoIP call hanging up the phone, then the related phone will RING (at the same time the tone will be stopped on the other phone) and the user will be able to answer to the incoming PSTN call.

Ring Generation

The ring waveform is the one generated on the FXS port when a call is received and the phone is on-hook. The ring waveform is specific to the country and can be customized by changing the following parameters:

- *OnRing time in milliseconds (0-5000) default is 1000*
- *OffRing time in milliseconds (0-5000) default is 4000*
- *Frequency in Hertz (16-70) default is 25*

Tone Generation

Tone is the audible sound used to signal to the phone user a specific state. In *Table 20*, are listed the tone names and their corresponding meanings.

Table 20. Tone Generation

Tone Name	Description
Ring	A number has been dialled and the called party phone is ringing
Dial	The phone is off-hook and the device is ready to collect digits to make a call
Busy	The called party is busy
Disconnect	The device is not able to complete the placed call

Each tone can and must be customized for the specific country. The parameters that can be used to define the above-mentioned tones are:

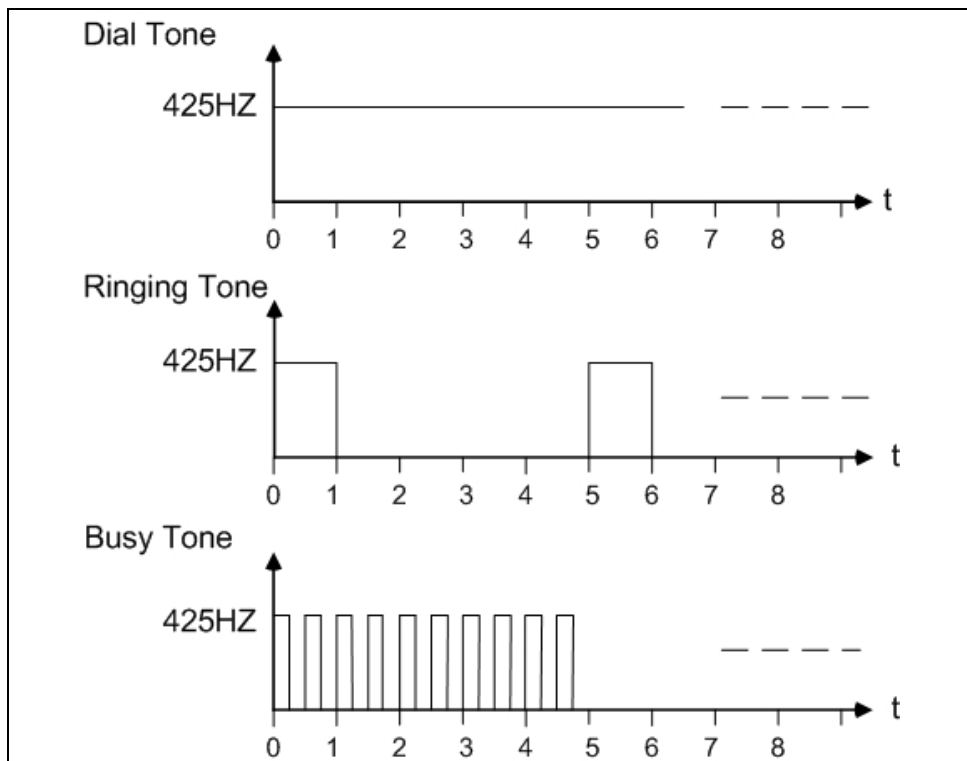
- *On time in milliseconds (0-5000)*
- *Off time in milliseconds (0-5000)*
- *Frequency in Hertz (20-1000)*

The default values used for each tones in Italy are shown in *Table 21* while *Figure 20* shows the respective Frequency/Time graphs.

Table 21. Italian Defaults Tones

Tone Name	On Time (msec)	Off Time (msec)	Frequency (Hz)
Ring	1000	4000	425
Dial	1000	0	425
Busy	500	500	425
Disconnect	500	500	425

Figure 20. Tones Frequency/Time graphs



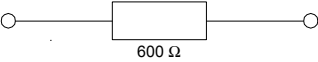
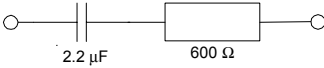

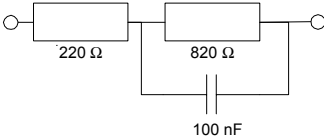
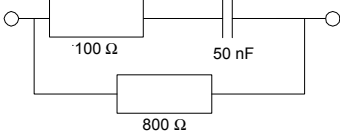
Port Gain

For each FXS port a gain/attenuation can be specified for each direction (receive and transmit). The minimum increment/decrement is 3 dB and the value must be included in the -24, +24 dB range.

Port Impedance

The FXS port impedance must match the phone one to guarantee the maximum quality and avoid annoying echo. The *Table 22* shows the equivalent circuits that can be configured for the FXS ports and their corresponding name.

Table 22. FXS Port equivalent circuits

Tone Name	Description
600r	
600c	
900c	
cplx1	
cplx2	

Buffer Management

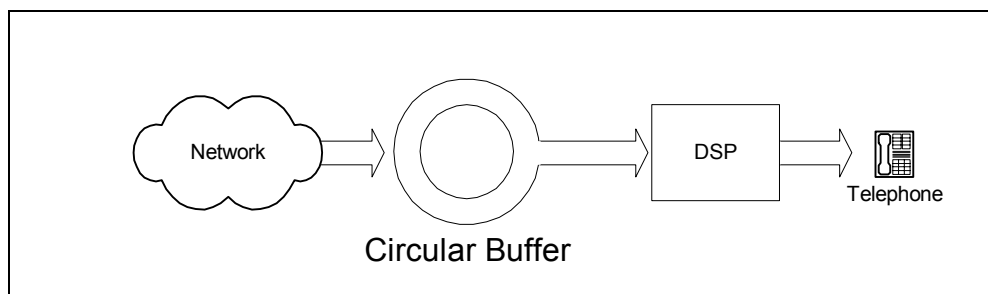
As show in *Figure 21*, the RTP packet coming from the network, before being played back, goes in a circular buffer. The frames are passed from this buffer to the DSP only when a number of frames are accumulated.

The dimensioning of these two parameters: length of the buffer and its threshold can be configured and must be chosen to guarantee a tradeoff between immunity to packet arrival time and introduced delay.

Their default values are:

- *Buffer Length 120 msec*
- *Threshold 0 msec*

Figure 21. RTP Packet receive path



Voice Activation and Silence Detection

The DSP can detect silence and avoid sending packets to the network when the phone user is not talking. This minimizes network traffic but a comfort noise must be generated on the remote end to make the remote party understand that the call is ongoing.

This feature can be disable/enabled.

Digit Collection

The dialed digits are collected until a configurable (DigitTout) between 1 and 255 seconds timeout occurs or the hash “#” key is pressed.

Configuration Examples

Example 1

To configure the phone settings if the AT-RG213 location is in Italy:

```
SET PHONE PORT=0 DIALFREQ=425 TDIAL=1000
SET PHONE PORT=0 RINGFREQ=425 TRING=1000 ;4000
SET PHONE PORT=0 BUSYFREQ=425 TBUSY=1000
```

Example 2

To change the tel1 (physical port 0) default network the call is routed to, from PSTN to VOIP, type the command:

```
SET PHONE PORT=0 DEFAULTCALL=VOIP
```

Example 3

To modify the prefix used to change from the set network to the other one (in this example from VOIP to PSTN), type the command:

```
SET PHONE PORT=0 PREFIX=#
```

After the execution of this command, to make a PSTN call when VOIP is set as default, simply type the #. key on the phone.

To see the setting of the modified port:

```
SHOW PHONE PORT=0
```

Command Reference

SET PHONE

Syntax SET PHONE PORT=*port* [RING=*ton;toff* 3* [;*ton;toff*]]
 [RINGFREQ=*rfreq*] [TRING=*ton;toff* 3* [;*ton;toff*]]
 [TRINGFREQ=*tfreq*] [TDIAL=*ton;toff* 3* [;*ton;toff*]]
 [TDIALFREQ=*tfreq*] [TBUSY=*ton;toff* 3* [;*ton;toff*]]
 [TBUSYFREQ=*tfreq*] [TDISC=*ton;toff* 3* [;*ton;toff*]]
 [TDISCFREQ=*tfreq*] [TWAIT=*ton;toff* 3* [;*ton;toff*]]
 [TWAITFREQ=*tfreq*] [TXGAIN=*gain*] [RXGAIN=*gain*]
 [IMPEDANCE=*impedance*] [BUFFLEN=*blen*] [BUFFTHR=*bthr*]
 [VAD={ON|OFF}] [DIGITOUT=*dtout*] [LEC=*lecframe*]
 [DEFAULTCALL={PSTN|VOIP}] [PREFIX=*digit*]
 [CWAITT={ON|OFF}] [CWAITD=*duration*]

Short Syntax S PHONE PORT=*port* [R=*ton;toff* 3* [;*ton;toff*]]
 [RF=*rfreq*] [TR=*ton;toff* 3* [;*ton;toff*]] [TRF=*tfreq*]
 [TD=*ton;toff* 3* [;*ton;toff*]] [TDF=*tfreq*]
 [TB=*ton;toff* 3* [;*ton;toff*]] [TBF=*tfreq*]
 [TDI=*ton;toff* 3* [;*ton;toff*]] [TDIF=*tfreq*]
 [TW=*ton;toff* 3* [;*ton;toff*]] [TWF=*tfreq*] [TXG=*gain*]
 [RXG=*gain*] [IMP=*impedance*] [BLEN=*blen*] [BTHR=*bthr*]
 [VAD={ON|OFF}] [DT=*dtout*] [LEC=*lecframe*]
 [DEFAULTCALL={PSTN|VOIP}] [PREFIX=*digit*]
 [CWAITT={ON|OFF}] [CWAITD=*duration*]

where:

- *port* is the physical port number (can be 0 or 1)
- *ton* a time interval expressed in msec within 0,5000 range

- *toff* a time interval expressed in msec within 0,5000 range
- *rfreq* a frequency expressed in Hz within 16-70 range
- *tfreq* a frequency expressed in Hz within 20,1000 range
- *gain* expressed in dB within -12,+12 range with 3 dB steps.
- *impedance* is the name of the interface equivalent circuit. The possible values are 600R, 600C, 900C, CPLX1 and CPLX2.
- *blen* input circular buffer length in milliseconds within 0,500 range
- *bthr* input circular buffer threshold in milliseconds within 0, blen range
- *dtout* timeout in seconds within 1, 255 range
- *lecf* number of frames in 0, 63 range
- *digit* can be a phone keypad valid digit, i.e. 0-9 * and #.
- *duration* is expressed in seconds in 0,60 range.

Description

This command sets different parameters for FXS port configuration.

A signal/tone cadence can be specified with a series of on and off time interval. This waveform is then repeated as long as the signal or tone is active.

RING and RINGFREQ set the ring signal, its cadence and its frequency when there is an incoming call. The default values are (1000, 4000) and 25 respectively.

TRING and TRINGFREQ set the ring tone cadence and its frequency when the called party phone is ringing. The default values are (1000, 4000) and 425 respectively.

TDIAL and TDIALFREQ set the dial tone cadence and its frequency when the system is ready to collect the digits for making a call. The default values are (1000, 0) and 425 respectively.

TBUSY and TBUSYFREQ set the busy tone cadence and its frequency when the called party phone is busy. The default values are (500, 500) and 425 respectively.

TDISC and TDISCFREQ set the disconnect tone cadence and its frequency when the called party phone or the VoIP server cannot be reached. The default values are (500, 500) and 425 respectively.

TWAIT and TWAITFREQ set the busy tone cadence and its frequency

when a call is already in progress and there is a new incoming call. The default values are (300, 5000) and 425 respectively.

TXGAIN and RXGAIN are respectively the gain applied to the audio signal to and from the network. The default values are 0 dB.

IMPEDANCE changes the FXS equivalent circuit that should match the connected phone one to guarantee the maximum quality and lowest line echo. The default value is 600R.

Between the network and the FXS interface there is a circular buffer where BUFLen is its total length while BUFTHR is the accumulated voice frame length before they start to be transferred to the FXS interface. This default value for BUFLen and BUFTHR are respectively 120 and 60 msec.

VAD enable or disable the feature to detect silence period and avoid sending corresponding frames on the network. By default this parameter is ON.

The digit collection terminates after a timeout of DIGITOUT seconds. The default value is 3 seconds. This timeout can be skipped if the # key is pressed.

The device can cancel line echo up to 8 msec. The value given is expressed in 0.125 usec frames so the value 64 corresponds to the longest echo that can be cancelled.

If a call is placed this can be routed by default to PSTN or to the VOIP network based on DEFAULTCALL parameters value. The default is PSTN. If the call must be routed to the not default network, a prefix must be dialled. The prefix is a one digit corresponding to PREFIX parameter that has its default value set to "*".

If there is an incoming call from the PSTN and all the configured phone ports are engaged in a VoIP call an audible tone is played for CWAITD seconds, with the same ring cadence.

SHOW PHONE

Syntax SHOW PHONE [PORT=*port* | RING | RINGFREQ | TRING | TRINGFREQ | TDIAL | TDIALFREQ | TBUSY | TBUSYFREQ | TDISC | TDISCFREQ | TWAIT | TWAITFREQ | TXGAIN | RXGAIN | IMPEDENCE | BUFLen | BUFFTHR | VAD | DIGITOUT | LEC | DEFAULTCALL | PREFIX | CWAITT | CWAITD]

Short Syntax SH PHONE [PORT=*port* | RING | RINGFREQ | TRING | TRINGFREQ | TDIAL | TDIALFREQ | TBUSY | TBUSYFREQ | TDISC | TDISCFREQ | TWAIT | TWAITFREQ | TXGAIN | RXGAIN | IMPEDENCE | BUFFLEN | BUFFTHR | VAD | DIGITOUT | LEC | DEFAULTCALL | PREFIX | CWAITT | CWAITD]

where:

- *port* is the physical port number (can be 0 or 1)

Description This command shows the phone ports configuration. To get information on all the ports the command must be used without any option.

To get a specific parameter, like RING, the port must be indicated along with the required parameter. The parameter is returned as is, since this command invocation is designed for web interface.

Figure 22. Example output from the SHOW PHONE command.

```

01234567890123456789012345678901234567890123456789
FXS Ports Configuration
-----
Phone 0
-----
Ring      Freq (Hz)  Cadence (msec)
-----
          25      1000 4000
-----
Tone      Freq (Hz)  Cadence (msec)
-----
Ring      425        1000 4000
Dial      425        1000  0
Busy      425         500 500
Disc      425         500 500
Wait      425         500 500
-----
Gain
Tx (dB)           0
Rx (dB)           0
-----
Input Buffer
Length (msec)     120
Threshold (msec)  0
-----
Impedence
Impedence        600R
-----
General
VAD              ON
Digit Tout (sec) 3
Lec Length (nframe) 64
Default Call     PSTN
Prefix           *
Call Wait Tone   ON

```

```

Call Wait Dur. (sec)    30
-----
Phone 1
-----
Ring   Freq (Hz)  Cadence (msec)
-----
      25      1000 4000
-----
Tone   Freq (Hz)  Cadence (msec)
-----
Ring   425      1000 4000
Dial   425      1000  0
Busy   425      500  500
Disc   425      500  500
Wait   425      500  500
-----
Gain
Tx (dB)                0
Rx (dB)                0
-----
Input Buffer
Length (msec)          120
Threshold (msec)      0
-----
Impedence
Impedence              600R
-----
General
VAD                    ON
Digit Tout (sec)      3
Lec Length (nframe)   64
Default Call           PSTN
Prefix                 *
Call Wait Tone         ON
Call Wait Dur. (sec)  30
-----

```

Table 23. Parameters displayed in the output of the SHOW PHONE command.

Parameter	Meaning
RING	Ring parameters RING cadence and RINGFREQ
TONE	Tone parameters for Ring, Busy, Dial, Disconnect and Wait
GAIN	Gain applied to audio signal. TXGAIN is to the network, RXGAIN is from the network
INPUT BUFFER	Input buffer parameters BUFLen and BUFTHR
IMPEDENCE	Interface equivalent circuit
VAD	If ON means that Voice Activation and silence Detection is active
DIGIT TOUT	Timeout before call send

LEC LENGTH	Line echo cancellation expressed in frames. Each frame is 0.125 usec.
DEFAULT CALL	If PSTN a call without prefix is routed to PSTN, otherwise to VOIP
PREFIX	This digit must be dialed before the number to route the call to the not standard one.

Chapter 8

Switch

Introduction

VLAN

A Virtual LAN is a software-defined broadcast domain. The switch's VLAN feature allows the network to be segmented by software management, improving network performance. Workstations, servers, and other network equipment connected to the switch can be grouped according to similar data and security requirements.

By default the switch is configured to include all ports as untagged members of a single default VLAN, with no VLAN tagging required on incoming frames, or added to outgoing frames.

One port on the switch can be configured as an uplink to another 802.1Q compatible switch. By using VLAN tagging, this one port can carry traffic from all VLANs on the switch.

VLANs can consist of simple logical groupings of untagged ports, in which the ports receive and transmit untagged packets. Alternatively, VLANs can include tagged ports, which add VLAN tags to packets they transmit.

VLAN tagging

VLAN tagging provides the advantages of more efficient and flexible use of switch ports and network resources, while maintaining the level of security given by port-based VLANs. With VLAN tagging, a port can belong to several VLANs.

A VLAN Identifier (VID) is defined for each VLAN, and this VID is used to switch traffic through a VLAN aware network so that frames are only transmitted on ports belonging to the VLAN.

Vlan Tagging - 802.1Q

The 802.1Q standard recommends the use of the 802.1Q VLAN tags for Ethernet frames traffic prioritization. VLAN tags are 4-byte headers in which three bits are reserved for priority indication.

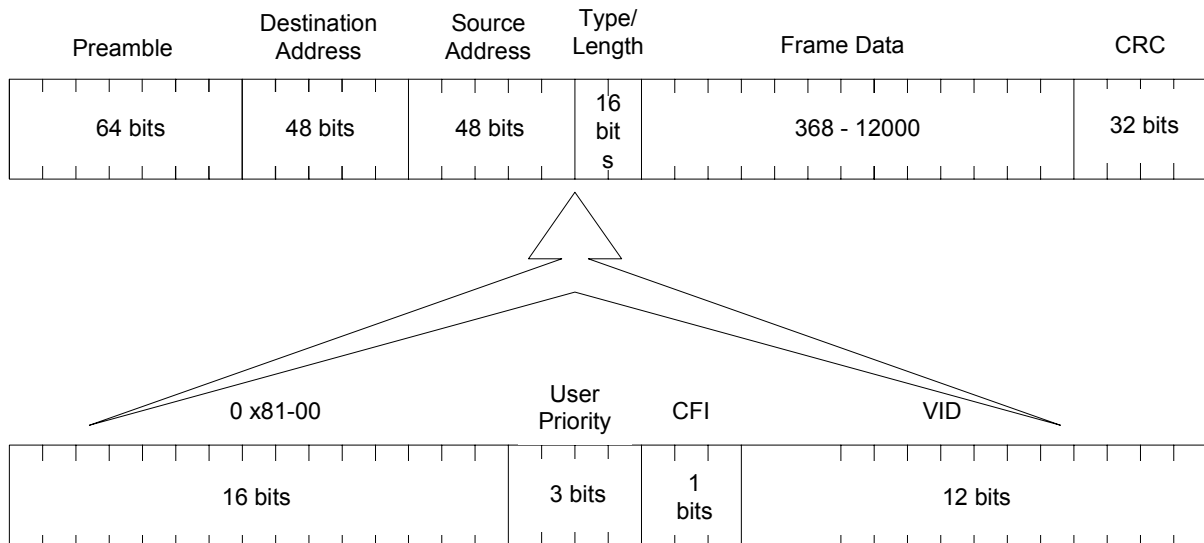
VLANs are created with standard Layer 2 Ethernet. A VLAN Identifier (VID) is associated with each VLAN. VLANs aim to offer the following benefits:

- *VLANs are supported over all IEEE 802 LAN MAC protocols, and over shared media LANs as well as point-to-point LANs.*
- *VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of moves, adds, and changes in members of these groups.*
- *Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.*
- *As far as possible, VLANs maintain compatibility with existing bridges and end stations.*

The VLAN field in the Ethernet frame is located after both destination and source as detailed in *Figure 23*.

For both signaling and media packets, the VLAN priority section is configurable independently.

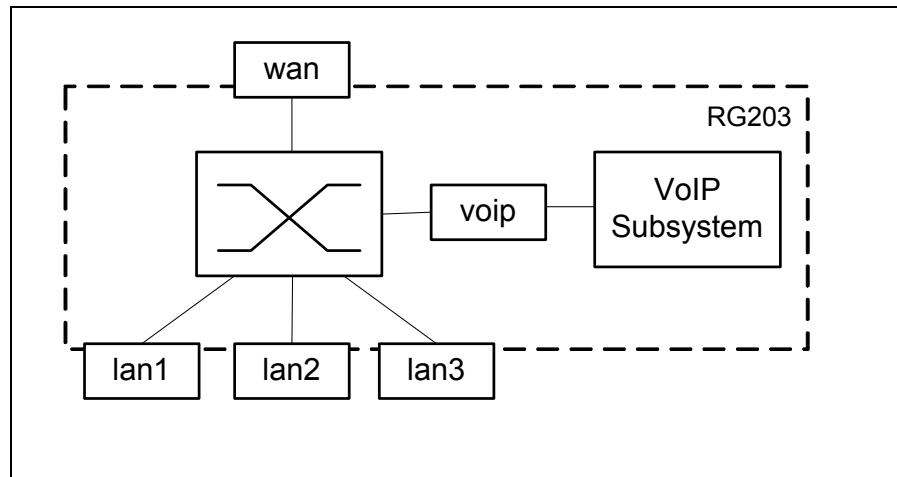
Figure 23. The VLAN field in the Ethernet file



Switch architecture

The integrated Switch relays Ethernet packets among the three LAN ports (lan1, lan2 and lan3), WAN port (wan) and VoIP subsystem port (voip), as shown in *Figure 24*.

Figure 24. Switch architecture



For each port it's possible to enable 802.1P/Q Tag insertion/stripping and two receive queues (high and low priority). Each 802.1Q user priority value can be defined as HIGH and LOW priority.

Tagged based VLAN are supported

A tagged based VLAN switch determines the membership of a data frame by examining the tagged info in the packet received. A four-byte field in the header is used to identify the VLAN. This VLAN identification indicates what VLAN the frame belongs to.

The AT-RG213 switch can use VLAN functionality both in upstreaming and downstream communication.

Configuration Examples

Example 1

Let's suppose that the AT-RG213 is inserted into a VoIP network where three Vlan are defined:

- VLAN1 used for VoIP traffic
- VLAN2 used for Video traffic (Multicast Stream)
- VLAN3 used for Internet browsing traffic

VLAN1 is created by default; VLAN2 and VLAN3 have to be created using the commands:

```
CREATE VLAN=VLAN2 VID=2
CREATE VLAN=VLAN3 VID=3
```

VLAN1 configuration

The VoIP and WAN ports must belong to VLAN1.

WAN port must be tagged because it is shared with other VLANs. VoIP port cannot be tagged. This VLAN is needed to allow VoIP traffic to reach the network and VoIP port.

```
ADD VLAN=1 PORT=WAN FRAME=TAGGED
```

VLAN2 configuration

LAN1, LAN2 and WAN ports must belong to VLAN2. WAN port must be tagged because it is shared with other VLANs. LAN1 and LAN2 are untagged ports to allow the Set Top Boxes to receive the packets. This VLAN is needed to allow Video traffic coming from the network (WAN) to reach two Set Top Boxes connected to LAN1 and LAN2 ports.

```
ADD VLAN=2 PORT=LAN1, LAN2 FRAME=UNTAGGED
ADD VLAN=2 PORT=WAN FRAME=TAGGED
```

VLAN3 configuration

LAN3 and WAN ports must belong to VLAN3. WAN port must be tagged because it is shared with other VLANs. LAN3 port is untagged to allow the

PC to receive the packets. This VLAN is needed to allow traffic incoming and outgoing from PC to reach the network and vice versa.

```
ADD VLAN=3 PORT=LAN3 FRAME=UNTAGGED
```

```
ADD VLAN=3 PORT=WAN FRAME=TAGGED
```

Command Reference

ADD VLAN PORT

Syntax `ADD VLAN={vlaname | 1..4094} PORT={port-list | ALL}
 [FRAME={TAGGED | UNTAGGED}]`

Short Syntax `A VLAN={vlaname | 1..4094} PORT={port-list | ALL}
 [FRAME={TAG | UTAG}]`

where:

- *vlaname* is a unique name for the VLAN, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9) the underscore character (" _"), and the hyphen character (-). The *vlaname* cannot be a number or ALL.
- *port-list* is an identifier or a comma separated list of port identifiers. Port identifier could be: VOIP, WAN, LAN1, LAN2 and LAN3.

Description This command adds ports to the specified VLAN.
The VLAN parameter specifies the name or numerical VLAN Identifier of the VLAN. The name is case insensitive, although the case is preserved for display purposes. The VLAN must already exist. By default, all ports belong to the default VLAN, with a numerical VLAN Identifier (VID) of 1.

The PORT parameter specifies the ports.

The FRAME parameter specifies whether a VLAN tag header is included in each frame transmitted on the specified ports. If TAGGED is specified, a VLAN tag is added to frames prior to transmission. The port is then called a tagged port for this VLAN. If UNTAGGED is specified, the frame is transmitted without a VLAN tag. The port is then called an untagged port for this VLAN.

The following constrain are assumed:

- *A port can be untagged for one and only one of the VLANs to which it belongs, or for none of the VLANs to which it belongs.*

- A port can be tagged for zero or more VLANs to which it belongs.
- A port cannot be tagged or untagged at the same time: the choice is exclusive. If you assign a port to a VLAN as untagged, only untagged setting will be permitted and if you assign a port to VLAN as tagged, only tagged setting will be permitted.

The default setting is UNTAGGED.

Examples

To add WAN port to the port-based *corporateA* VLAN, use:
ADD VLAN=*corporateA* PORT=WAN

To add LAN1 port to the *corporateB* VLAN as a tagged port, use:
ADD VLAN=*corporateB* PORT=LAN1 FRAME=TAGGED

See Also

CREATE VLAN

Syntax

```
CREATE VLAN=vlanname VID=2..4094
```

Short Syntax

```
C VLAN=vlanname VID=2..4094
```

where:

- *vlanname* is a unique name for the VLAN, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9) the underscore character (“_”), and the hyphen character (-). The *vlanname* cannot be a number or ALL.

Description

This command creates a VLAN with a unique name and VLAN Identifier (VID). To change the VID of an existing VLAN, that VLAN must be destroyed and created again with the modified VID. A maximum of 16 VLANs can be created with any VID in the range 2 to 4094.

The VLAN parameter specifies a unique name for the VLAN. This name can be more meaningful than the VID, to make administration easier. The VLAN name is only used within the switch; it is not transmitted to other VLAN-aware devices, or used in the Forwarding Process or stored in the Forwarding Database. If the VLAN name begins with “vlan” and ends with a number, for instance “vlan1” or “vlan234”, then the number must be the same as the VID specified. This avoids confusion when identifying which VLAN subsequent commands refer to.

The VID parameter specifies a unique VLAN Identifier for the VLAN. If tagged ports are added to this VLAN, the specified VID is used in the VID field of the tag in outgoing frames. If untagged ports are added to this VLAN, the specified VID only acts as an identifier for the VLAN in the Forwarding Database. The default port based VLAN has a VID of 1.

Examples

To create a VLAN named *marketing* with a VLAN Identifier of 2, use:
CREATE VLAN=*marketing* VID=2

To create a VLAN named *vlan42*, which must have a VID of 42, use:
CREATE VLAN=*vlan42* VID=42

See Also

DELETE VLAN PORT

Syntax DELETE VLAN={*vlanname* | 1..4094} PORT={*port-list* | ALL}
Short Syntax D VLAN={*vlanname* | 1..4094} PORT={*port-list* | ALL}

where:

- *vlanname* is a unique name for the VLAN, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9) the underscore character (" _"), and the hyphen character (-). The *vlanname* cannot be a number or ALL.
- *port-list* is an identifier or a comma separated list of port identifiers. Port identifier could be: VOIP, WAN, LAN1, LAN2 and LAN3.

Description This command deletes ports from the specified VLAN. An untagged port can be deleted from a VLAN if the port is still a member of a VLAN after the deletion has occurred. If the port does not belong to any VLAN as a tagged port then the port is implicitly added to the default VLAN as an untagged port. It is not possible to delete a port that belongs only to the default VLAN as an untagged port.

The VLAN parameter specifies the name or numerical VLAN Identifier of the VLAN. The name is case insensitive. The VLAN must already exist.

The PORT parameter specifies the ports to be deleted from the VLAN. If ALL is specified, then all ports belonging to the VLAN are deleted. If the command would succeed on a subset of the ports specified, but cause an error on the others, then the command as a whole will fail and have no effect.

Examples To delete port 3 from the *marketing* VLAN, use the command:
DELETE VLAN=marketing PORT=3

See Also

DESTROY VLAN

Syntax DESTROY VLAN={*vlanname* | 2..4094 | ALL}
Short Syntax DES VLAN={*vlanname* | 2..4094 | ALL}

Where:

- *vlanname* is a unique name for the VLAN, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9) the underscore character (" _"), and the hyphen character (-).


The *vlanname* cannot be a number or ALL.

- Description** This command destroys the specified VLAN or all VLANs in the switch. The default VLAN, which has a numerical VLAN Identifier (VID) of 1, cannot be destroyed. If ALL is specified then all VLANs except the default VLAN are destroyed. A VLAN cannot be destroyed if ports still belong to it.
- Examples** To destroy the VLAN with the VLAN Identifier of 1234, use the command:
DESTROY VLAN=1234
- To remove all user created VLANs from the switch, none of which have any member ports, use the command:
DESTROY VLAN=ALL
- See Also**

DISABLE SWITCH AGEINGTIMER

- Syntax** DISABLE SWITCH AGEINGTIMER
- Short Syntax** DIS SWITCH AGET
- Description** This command disables the ageing timer from ageing out dynamically learned entries in the Forwarding Database. The default setting for the ageing timer is enabled.
- Examples** To disable the ageing out of learned MAC addresses, use the command:
DISABLE SWITCH AGEINGTIMER
- See Also**


DISABLE SWITCH LEARNING

- Syntax** DISABLE SWITCH LEARNING
- Short Syntax** DIS SWITCH LEARN
- Description** This command disables the dynamic learning and updating of the Forwarding Database. The default setting for the learning function is enabled.
-  *If switch learning is disabled and the ageing timer has aged out all dynamically learned entries. If the switch finds no matching entries in the Forwarding Database during the Forwarding Process, then all switch ports in the VLAN will be flooded with the packet, except the port on which the packet was received.*
- Examples** To disable the switch learning function, use the command:
DISABLE SWITCH LEARNING
- See Also**

DISABLE SWITCH PORT

Syntax	<code>DISABLE SWITCH PORT={<i>port-list</i> ALL} [FLOW={JAMMING PAUSE} [, {PAUSE JAMMING}]]</code>
Short Syntax	<code>DIS SWITCH PORT={<i>port-list</i> ALL} [FLOW={JAM PAUSE} [, {PAUSE JAM}]]</code>
	where:
	<ul style="list-style-type: none"> ▪ <i>port-list</i> is an identifier or a comma separated list of port identifiers. Port identifier could be: WAN, LAN1, LAN2 and LAN3.
Description	<p>This command disables a port or group of ports on the switch, or disables one or both of the flow control mechanisms. If the port is disabled, it will no longer send or receive packets. Ports should be disabled if there faulty wiring or equipment attached to the ports, or as a security measure to stop access from intruders. Switch ports are enabled by default.</p> <p>The PORT parameter specifies the port or ports to be disabled, or which are to have flow control methods disabled.</p> <p>The FLOW parameter specifies the types of flow control to be disabled for the port. One or both types may be disabled with this command. If JAMMING is specified, flow control for half duplex ports by asserting the jamming signal will be disabled. If PAUSE is specified, flow control for full duplex ports by sending PAUSE frames will be disabled. Both these forms of flow control are enabled by default.</p>
Examples	<p>To disable ports LAN1 and LAN2 use the command:</p> <pre>DISABLE SWITCH PORT=LAN1,LAN2</pre>
See Also	

ENABLE SWITCH AGEINGTIMER

Syntax	<code>ENABLE SWITCH AGEINGTIMER</code>
Short Syntax	<code>EN SWITCH AGET</code>
Description	<p>This command enables the ageing timer to age out dynamically learned entries in the Forwarding Database. The default setting for the ageing timer is enabled.</p> <p> <i>If the ageing timer ages out all dynamically learned filter entries, the switch finds no matching entries in the Forwarding Database during the Forwarding Process, then all switch ports in the VLAN will be flooded with the packet, except the port on which the packet was received.</i></p>
Examples	<p>To enable the ageing out of learned MAC addresses, use the command:</p> <pre>ENABLE SWITCH AGEINGTIMER</pre>

See Also

ENABLE SWITCH LEARNING

Syntax	ENABLE SWITCH LEARNING
Short Syntax	EN SWITCH LEARN
Description	This command enables the dynamic learning and updating of the Forwarding Database. The default setting for the learning function is enabled.
Examples	To enable the switch learning function, use the command: ENABLE SWITCH LEARNING
See Also	

ENABLE SWITCH PORT

Syntax	ENABLE SWITCH PORT={ <i>port-list</i> ALL} [FLOW={JAMMING PAUSE} [, {PAUSE JAMMING}]]
Short Syntax	EN SWITCH PORT={ <i>port-list</i> ALL} [FLOW={JAM PAUSE} [, {PAUSE JAM}]]
	where:
	<ul style="list-style-type: none"> ▪ <i>port-list</i> is an identifier or a comma separated list of port identifiers. Port identifier could be: WAN, LAN1, LAN2 and LAN3.
Description	<p>This command enables a port or group of ports on the switch, or enables one or both of the flow control mechanisms. Switch ports are enabled by default.</p> <p>Use the SET SWITCH PORT command to enable a port which has been disabled by the Port Security function, rather than this command.</p> <p>The PORT parameter specifies the port or ports to be enabled, or which are to have flow control methods enabled.</p> <p>The FLOW parameter specifies the types of flow control to be enabled for the port. One or both types may be enabled with this command. If JAMMING is specified, flow control for half duplex ports by asserting the jamming signal will be enabled. If PAUSE is specified, flow control for full duplex ports by sending PAUSE frames will be enabled. Both these forms of flow control are enabled by default.</p>
Examples	To enable ports LAN1 and LAN2, use the command: ENABLE SWITCH PORT=LAN1, LAN2
See Also	

RESET SWITCH

Syntax	RESET SWITCH
Short Syntax	RES SWITCH
Description	This command resets the switch module. All dynamic switch information is cleared. All ports are reset. All counters and timers are reset to zero.
Examples	To reset the switch module, use the command: RESET SWITCH
See Also	

RESET SWITCH PORT

Syntax	RESET SWITCH PORT={ <i>port-list</i> ALL} [COUNTER]
Short Syntax	RES SWITCH PORT={ <i>port-list</i> ALL} [CNT]
	Where:
	<ul style="list-style-type: none"> ▪ <i>port-list</i> is an identifier or a comma separated list of port identifiers. Port identifier could be: VOIP, WAN, LAN1, LAN2 and LAN3.
Description	This command resets a port or group of ports on the switch. All packets queued for reception or transmissions on the port are discarded, the port is reset at the hardware level and autonegotiation of speed and duplex mode is activated. Switch port counters are reset to zero. This command can be used to try to ensure that packets stuck in a queue are cleared, perhaps after a packet storm of some nature. The PORT parameter specifies the ports to be reset. The COUNTER parameter specifies that only switch port counters are reset. If the COUNTER parameter is not used the switch port is fully reset.
Examples	To reset port 3, use the command: RESET SWITCH PORT=LAN3
See Also	

SET SWITCH AGEINGTIMER

Syntax	SET SWITCH AGEINGTIMER={FAST NORMAL}
Short Syntax	S SWITCH AGET={FAST NORMAL}

Description	This command sets the threshold value of the ageing timer, after which a dynamic entry in the Forwarding Database is automatically removed. FAST corresponds to 800 μ Sec., while NORMAL is equal to 300 Sec.. The default value is 300 seconds (5 minutes).
Examples	To set the ageing timer to 300 seconds (5 minutes), use the command: SET SWITCH AGEINGTIMER=NORMAL
See Also	

SET SWITCH PORT

Syntax	<pre>SET SWITCH PORT={port-list ALL} [BCLIMIT={NONE limit}] [DESCRIPTION=description] [INFILTERING={OFF ON}] [MCLIMIT={NONE limit}] [RCVLIMIT={NONE limit}] [SPEED={AUTONEGOTIATE 10MHALF 10MFULL 100MHALF 100MFULL 1000MHALF 1000MFULL}]</pre>
Short Syntax	<pre>S SWITCH PORT={port-list ALL} [BCL={NONE limit}] [DES=description] [IFLT={OFF ON}] [MCL={NONE limit}] [RCVL= {NONE limit}] [SPEED={AUTO 10MH 10MF 100MH 100MF 1000MH 1000MF}]</pre>

where:

- *description* is a string, 1 to 47 characters in length. Valid characters are any printable characters.
- *limit* is a decimal number, from 0 to the maximum value of the limit variable based on the particular switch hardware. The maximum packet storm protection limit is 262143.
- *port-list* is an identifier or a comma separated list of port identifiers. Port identifier could be: WAN, LAN1, LAN2 and LAN3.

Description	This command modifies the value of parameters for switch ports.
--------------------	---

The PORT parameter specifies the ports for which parameters are modified. If the command would succeed on a subset of the ports specified, but cause an error on the others, then the command as a whole will fail and have no effect. Reference in the descriptions below to an individual port should be taken as a reference to all ports selected by the PORT parameter. If packet storm protection limits are set on the switch, the PORT parameter must specify complete processing blocks (see the note after the BCLIMIT parameter description).

The BCLIMIT parameter specifies a limit on the rate of reception of broadcast packets for the port(s). The value of this parameter represents a per second rate of packet reception above which packets will be discarded, for broadcast packets. If the value NONE or 0 is specified, then packet rate limiting for broadcast packets is turned off. If any other value is specified, the reception of broadcast packets will be limited to that number of packets

per second. See the note below for important information about packet rate limiting. The default value for this parameter is NONE.



The ability of the switch to limit packet reception rates for different classes of packets is dependent on the particular switch hardware. In particular, groups of ports may have to have the same limits set, and the same limit may be set for the different types of packets, depending on the hardware. Whenever packet rate limits are set on switches, which have this type of constraint, the latest parameter values entered will supersede earlier values. When a command entered for specified ports changes the parameters for other ports, a message will indicate these changes

The BCLIMIT parameter accepts only values multiples of 2000 so if any other value is specified, the BCLIMIT parameter will be set to the largest multiple of 2000 inferior to the specified value

see Examples.

The INFILTERING parameter enables or disables Ingress Filtering of frames admitted on the specified ports. Each port on the switch belongs to one or more VLANs. If INFILTERING is set to ON, Ingress Filtering is enabled: any frame received on a specified port is only admitted if the port belongs to the VLAN with which the frame is associated. Conversely, any frame received on the port is discarded if the port does not belong to the VLAN with which the frame is associated. Untagged frames are admitted, since they have the numerical VLAN Identifier (VID) of the VLAN for which the port is an untagged member. If OFF is specified, Ingress Filtering is disabled, and no frames are discarded by this part of the Ingress Rules. The default setting is OFF.

The MCLIMIT parameter specifies a limit on the rate of reception of multicast packets for the port. The value of this parameter represents a per second rate of packet reception above which packets will be discarded, for multicast packets. If the value NONE or 0 is specified, then packet rate limiting for multicast packets is turned off. If any other value is specified, the reception of multicast packets will be limited to that number of packets per second. See the note after the BCLIMIT parameter description for important information about packet rate limiting. The default value for this parameter is NONE. If packet storm protection limits are set on the switch, the PORT parameter must specify complete processing blocks.

For the RG213 switches the setting is applied also to BCLIMIT parameter.



see Examples.

The RCVLIMIT parameter specifies a rate limiting on reception bandwidth for the port. The value of this parameter represents a per second rate of Kbit reception above which the incoming data will be discarded. If the value NONE or 0 is specified, then rate limiting is turned off. If any other value is specified, the reception of will be limited to that bandwidth. The default value for this parameter is NONE.



The RCVLIMIT parameter accepts only values multiples of 32 so if

any other value is specified, the RCVLIMIT parameter will be set to the largest multiple of 32 inferior to the specified value

The SPEED parameter specifies the configured line speed and duplex mode of the port(s). If AUTONEGOTIATE is specified, the port(s) will autonegotiate the line speed and duplex mode with the device attached to the port if the port does not belong to a trunk group. If any other option is specified, the port(s) will be forced to the speed and duplex mode given. If the port(s) are a member of a trunk group, the speed setting specified with this command will be saved, but ignored. The speed will be set to the speed of the trunk group and the duplex mode will be set to full duplex. The default for this parameter is AUTONEGOTIATE. The gigabit uplink ports can only operate at 1000MFULL.

Examples

To set the speed of port LAN2 to 10Mbps, half duplex, use the command:
SET SWITCH PORT=LAN2 SPEED=10MHALF

Setting the broadcast rate limit to 7000 packets/s, using the command
SET SWITCH PORT=LAN2 BCLIMIT=7000, the broadcast rate limit will be set to 6000 packets/s

Setting the multicast rate limit to 8000 packets/s, using the command
SET SWITCH PORT=LAN2 MCLIMIT=8000, also the broadcast rate limit will be set to the same limit

Setting the receive rate limit to 10000 kbps for LAN2, using the command
SET SWITCH PORT=LAN2 RCVLIMIT=10000, the receive rate limit will be set to 9984 kbps

See Also

SET SWITCH QOS

Syntax	SET SWITCH QOS DSCP= <i>dscpcode-list</i> PRIORITY={HIGH LOW}
Short Syntax	S SWITCH QOS DSCP= <i>dscpcode-list</i> PRI={HIGH LOW}
	Where:
	<ul style="list-style-type: none"> ▪ <i>dscpcode-list</i> is a comma-separate list of numbers in the range 0-63 which represent the DSCP (Differentiated Service Code Point) in the most significant 6 bits of the TOS field in IPv4 header.
Description	This command maps the priority levels for Quality of Service. The six bits TOS field in the IP header is decoded in 64 entries and for each one it is possible to specify the priority.
Examples	To set the high priority for TOS 24 and 37, use the command:

```
SET SWITCH QOS DSCP=24,37 PRI=HIGH
```

See Also

SHOW SWITCH

Syntax	SHOW SWITCH
Short Syntax	SH SWITCH
Description	This command displays configuration information for the switch functions.
Examples	To display the configuration of the switch module, use the command: SHOW SWITCH
See Also	

Figure 25. Example output from the SHOW SWITCH command.

```
0123456789012345678901234567890123456789012345678901234567890123456789
Switch configuration
-----
Switch address          00-00-CD-00-45-C7
Learning                ON
Ageing timer           ON
Ageing time            300 Sec. (NORMAL)
UpTime                 00:01:34
-----
```

Table 24. Parameters displayed in the output of the SHOW SWITCH command.

Parameter	Meaning
Switch address	The MAC address of the switch; it is used as the source address in pause control frames.
Learning	Whether or not the switch's dynamic learning and updating of the Forwarding Database is enabled.
Ageing timer	Whether or not the ageing timer is enabled.
Ageing time	The value of the ageing timer, after which a dynamic entry is removed from the Forwarding Database.
UpTime	The time in hours:minutes:seconds since the switch was last powered up, rebooted, or restarted.

SHOW SWITCH FDB

Syntax	SHOW SWITCH FDB [[ADDRESS=macadd] [PORT={port-list ALL}] [VLAN={vlanname 1..4094}]]
Short Syntax	SH SWITCH FDB [[ADDR=macadd]

```
[PORT={port-list|ALL}] | [VLAN={vlanname|1..4094}]]
```

Where:

- *macadd* is an Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by hyphen
- *port-list* is an identifier or a comma separated list of port identifiers. Port identifier could be: VOIP, WAN, LAN1, LAN2 and LAN3.
- *vlanname* is a unique name for the VLAN, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9) the underscore character (“_”), and the hyphen character (-). The *vlanname* cannot be a number or ALL.

Description This command displays the contents of the Forwarding Database.

The ADDRESS parameter specifies the MAC address of the device for which the contents of the Forwarding Database are to be displayed.

The PORT parameter specifies that only those entries in the Forwarding Database which were learned from the specified port are to be displayed.

The VLAN parameter specifies the VLAN identifier of the VLAN for which the contents of the Forwarding Database are to be displayed.

Examples To display the contents of the Forwarding Database, use the command:
SHOW SWITCH FDB

See Also

Figure 26. Example output from SHOW SWITCH FDB command.

```
0123456789012345678901234567890123456789012345678901234567890123456789
Switch Forwarding Database
-----
VLAN    MAC address          Port    Status
-----
1       00-00-cd-00-45-c7   VOIP    dynamic
15      00-00-c0-1d-2c-f8   WAN     dynamic
1       00-00-c0-71-e0-e4   WAN     dynamic
15      00-00-cd-00-a4-d6   LAN2    dynamic
4032    00-00-cd-00-ab-dc   WAN     dynamic
15      00-60-b0-ac-18-51   LAN2    dynamic
4032    00-90-27-32-ad-61   LAN1    dynamic
15      08-00-09-be-06-cd   LAN2    dynamic
15      01-00-5e-be-06-cd   WAN     static
-----
```

Table 25. Parameters displayed in the output of the SHOW SWITCH FDB command.

Parameter	Meaning
VLAN	VLAN identifier (VID).

MAC Address	The MAC address as learned from the source address field of a frame, or entered as part of a static filter entry.
Port	The port from which the MAC address was learned.
Status	Whether the entry was a static filter entry or dynamically learned; one of "dynamic" or "static".

SHOW SWITCH PORT

Syntax	SHOW SWITCH PORT [= { <i>port-list</i> ALL}]
Short Syntax	SH SWITCH PORT [= { <i>port-list</i> ALL}]
	Where:
	<ul style="list-style-type: none"> ▪ <i>port-list</i> is an identifier or a comma separated list of port identifiers. Port identifier could be: VOIP, WAN, LAN1, LAN2 and LAN3.
Description	This command displays general information about the specified switch ports or all switch ports.
Examples	To display the configuration for switch port 1, use the command: SHOW SWITCH PORT=1
See Also	

Figure 27. Example output from SHOW SWITCH PORT command.

```

0123456789012345678901234567890123456789012345678901234567890123456789
Switch Port Information
-----
Port: WAN
  Description                To intranet hub
  Status                     Enabled
  Link state                 Up
  Uptime                    00:35:03
  Port media type           ISO8802-3 CSMACD
  Configured speed/duplex   Autonegotiate
  Actual speed/duplex       100 Mbps, full duplex, MDI
  Acceptable frame type     Admit all frames
  Broadcast rate limit      -
  Multicast rate limit      -
  Receive rate limit        9984 kbps
  Current learned, lock state 15, not locked
  Enabled flow control(s)    Jamming
                             Pause
  Send tagged pkts for VLAN(s) marketing (87)
                             sales (321)
  Port based VLAN           default (1)
  Ingress filtering         OFF
-----

```

Table 26. Parameters displayed in the output of the SHOW SWITCH PORT command.

Parameter	Meaning
Port	Port reference.
Description	A description of the port.
Status	The state of the port; one of "ENABLED" or "DISABLED".
Link state	The link state of the port, one of "Up" or "Down".
Uptime	The count in hours:minutes:seconds of the elapsed time since the port was last reset or initialised.
Port media type	The MAC entity type.
Configured speed/duplex	The port speed and duplex mode configured for this port. One of "Autonegotiate" or a combination of a speed (one of "10 Mbps", "100 Mbps" or "1000 Mbps") and a duplex mode (one of "half duplex" or "full duplex").
Acceptable frame type	The value of the Acceptable Frame Types parameter, one of: "Admit All Frames" or "Admit Only VLAN-tagged Frames".
Broadcast rate limit	The limit of the rate of reception of broadcast frames for this port, in frames per second.
Multicast rate limit	The limit of the rate of reception of multicast frames for this port, in frames per second.
Current learned, lock state	The number of MAC addresses currently learned on this port and the state of locking for this port. The lock state is one of "not locked", "locked by limit" or "locked by command".
Enabled flow control(s)	Flow control parameters set for the port; zero, one or two of "Jamming" and "Pause". If flow control is implemented on the switch, then this kind of flow control is applied to the port.
Send tagged pkts for VLAN(s)	The name and VLAN Identifier (VID) of the tagged VLAN(s), if any, to which the port belongs.
Port based VLAN	The name and VLAN Identifier (VID) of the port-based VLAN to which the port belongs.
Ingress filtering	The state of Ingress Filtering: one of "ON" or "OFF".

SHOW SWITCH PORT COUNTER

- Syntax** `SHOW SWITCH PORT={port-list|ALL} COUNTER`
- Short Syntax** `SH SWITCH PORT={port-list|ALL} CNT`
- Where:
- *port-list is an identifier or a comma separated list of port identifiers. Port identifier could be: VOIP, WAN, LAN1, LAN2 and LAN3.*
- Description** This command displays information about the forwarding counters associated with the switch.
- Examples** To display the switching counters of port WAN, use the command:
`SHOW SWITCH PORT=WAN COUNTER`
- See Also**

Figure 28. Example output from the SHOW SWITCH PORT COUNTER command.

```

0123456789012345678901234567890123456789012345678901234567890123456789
Switch counter
-----
Port: WAN
Combined receive/transmit packets by size (octets) counters:
   64                65                256 - 511                0
   65 - 127          5                 512 - 1023                0
  128 - 255          0                 1024 - 1522                0

General Counters:
Receive:
  Octets                246
  Pkts                  0
  FCSerrors              0
  MulticastPkts         0
  BroadcastPkts         3
  PauseMACctlFrms      0
  OversizePkts          0
  Fragments             0
  Jabbers               0
  MACControlFrms       0
  UnsupportCode         0
  AlignmentErrors       0
  SymErDurCarrier       0
  UndersizePkts         0

Transmit:
  Octets                4320
  Pkts                  57
  MulticastPkts         0
  BroadcastPkts         0
  PauseMACctlFrms      0
  FrameWDeferrdTx      0
  SingleCollsnFrm      0
  MultCollsnFrm        0
  LateCollsns           0
  ExcessivCollsns      0
  CollisionFrames       0

Miscellaneous Counters:
  DropEvents            0
  totalPktTxAbort       0
-----

```


Table 27. Parameters displayed in the output of the SHOW SWITCH PORT COUNTER command.

Parameter	Meaning
Combined receive/transmit packets by size (octets) counter	The number of packets in each size range received and transmitted.
64	Number of 64 octet packets received and transmitted.
65 – 127	Number of 65 - 127 octet packets received and transmitted.
128 – 255	Number of 128 - 255 octet packets received and transmitted.
256 – 511	Number of 256 - 511 octet packets received and transmitted.
512 – 1023	Number of 512 - 1023 octet packets received and transmitted.
1024 – 1522	Number of 1024 - 1522 octet packets received and transmitted.
General Counter	
Receive	Counters for traffic received.
Octets	The number of octets.
Pkts	The number of packets.
FCSErrors	The number of frames containing a Frame Check Sequence error.
MulticastPkts	The number of multicast packets.
BroadcastPkts	The number of broadcast packets.
PauseMACctlFrms	The number of valid PAUSE MAC Control frames.
OversizePkts	The number of oversize packets.
Fragments	The number of fragments.
Jabbers	The number of jabbers frames.
MACControlFrms	The number of MAC Control frames (Pause and Unsupported).
UnsupportCode	The number of MAC Control frames with unsupported opcode (i.e. not Pause).
AlignmentErrors	The number of frames with alignment errors.
SymErDurCarrier	The number of frames with invalid data symbols.
UndersizePkts	The number of undersized packets.
Transmit	Counters for traffic transmitted.
Octets	The number of octets.
Pkts	The number of packets.
MulticastPkts	The number of multicast packets.
BroadcastPkts	The number of broadcast packets.

PauseMACctlFrms	The number of PAUSE MAC Control frames.
FrameWDeferrdTx	The number of frames deferred once before successful transmission.
SingleCollsnFrm	The number of frames which experienced exactly one collision.
MultCollsnFrm	The number of frames which experienced 2 to 15 collisions (including late collisions).
LateCollsns	The number of frames which experienced late collisions.
ExcessivCollsns	The number of frames aborted before transmission after 16 collisions.
CollisionFrms	Total number of collisions.
Miscellaneous Counters	
DropEvents	The number of packets discarded at ingress port.
totalPktTxAbort	The number of packets aborted during transmission.

SHOW SWITCH QOS

- Syntax** SHOW SWITCH QOS
- Short Syntax** SH SWITCH QOS
- Description** This command displays the current mapping of user priority level to QOS egress queue for the switch.
- Examples** To display the QOS setting, use the command:
SHOW SWITCH QOS
- See Also**

Figure 29. Example output from the SHOW SWITCH QOS command.

```

0123456789012345678901234567890123456789012345678901234567890123456789
Switch Quality Of Service Information
-----
Priority Map:

  Addr | 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
-----|-----
   00 | . . . . . H . . . . .
   20 | . . . . H . . . . . H . . . . H .
   40 | . . . . . . . . . . . H . . . .
   60 | . . . .
-----
    
```

Table 28. Parameters displayed in the output of the SHOW SWITCH QOS command.

Parameter	Meaning
Priority Map	The map shows the High priority DSCP code.

SHOW VLAN

Syntax	SHOW VLAN={ <i>vlanname</i> 1..4094 ALL }
Short Syntax	SH VLAN={ <i>vlanname</i> 1..4094 ALL }
	Where:
	<ul style="list-style-type: none"> ▪ <i>vlanname</i> is a unique name for the VLAN, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9) the underscore character (“_”), and the hyphen character (-). The <i>vlanname</i> cannot be a number or ALL.
Description	This command displays information about the specified VLAN. If no VLAN or ALL is specified, then all VLANs are displayed.
Examples	To display information on the <i>marketing</i> VLAN, use the command: SHOW VLAN=marketing
See Also	

Figure 30. Example output from the SHOW VLAN command.

```

01234567890123456789012345678901234567890123456789012345678901234567890123456789
VLAN Information
-----
Name: default
  Identifier                1
  Status                    static
  Untagged port(s)         VOIP, LAN1, LAN2, LAN3
  Tagged port(s)           WAN

Name: vlan2
  Identifier                2
  Status                    static
  Untagged port(s)         VOIP, LAN1
  Tagged port(s)           WAN

Name: marketing
  Identifier                25
  Status                    static
  Untagged port(s)         LAN2
  Tagged port(s)           WAN
-----

```

Table 29. Parameters displayed in the output of the SHOW VLAN command.

Parameter	Meaning
Name	The name of the VLAN.
Identifier	The numerical VLAN identifier of the VLAN (VID).
Status	The status of the VLAN, either dynamic or static.
Untagged port(s)	A list of untagged ports that belong to the VLAN.
Tagged port(s)	A list of tagged ports that belong to the VLAN.

Glossary

Symbols

802.2 The IEEE standard for the definition of the Logical Link Control protocol for LANs.

802.3 The IEEE standard for the definition of the CSMA/CD (Ethernet) medium access method for LANs.

A

ACK *Acknowledgement*. A packet sent to indicate that a block of data arrived at its destination without error. For example, at the link level, an acknowledgement indicates successful transmission across a single hardware link; at the transport level an acknowledgement indicates successful transmission between end systems (possibly over multiple hardware links). See NAK.

A-Law The ITU-T companding standard used in the conversion between analogue and digital signals in PCM (Pulse Code Modulation) systems. A-law is used primarily in European telephone networks and contrasts with the North American mu (μ)-law standard.

anonymous FTP Anonymous FTP allows a user to retrieve documents, files, programs, and other archived data from anywhere in the Internet without having to establish a user ID and password. By using the special user ID of anonymous the network user will bypass local security checks and will have access to publicly accessible files on the remote system. See archive site, FTP.

ANSI *American National Standards Institute.* An organisation responsible for coordinating and approving U.S. standards. Standards approved by ANSI are often called ANSI standards. ANSI is the U.S. representative to ISO.

archive site A machine that provides access to a collection of files across the Internet. An “anonymous FTP archive site”, for example, provides access to this material via the FTP protocol. See anonymous FTP.

ASCII *American Standard Code for Information Interchange.* A standard character-to-number encoding widely used in the computer industry.

assigned numbers A set of values (usually numeric) used by TCP/IP protocols. They are documented in a number of RFCs, the most recent being RFC 1340. See RFC.

asynchronous Transmission in which each character is sent individually. The time intervals between transmitted characters may be of unequal length. Transmission is controlled by *start* and *stop* elements before and after each character. See synchronous.

authorisation The process of determining what types of activities a user is permitted to undertake. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized for different types of access or activity.

B

bandwidth Technically, the difference, in Hertz (Hz), between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communications circuit. For example, Ethernet has a bandwidth of 10Mbps.

baud Literally, the number of times per second the signal can change on a transmission line. It is normally equal to the number of bits per second that can be transferred. The underlying transmission system may use some of the bandwidth. For asynchronous lines, the number of characters per second that can be transmitted is estimated by dividing the baud rate by ten.

boot A term used in computing to refer to the process of starting a computer, loading the operating system or executive program from disk or ROM.

bps *bits per second.* A measure of the rate of data transmission.

broadcast A packet delivery system that delivers a copy of a given packet to all hosts attached to the network. For example, Ethernet. See directed broadcast, multicast, unicast.

buffer A block of memory used to store data temporarily.

C

challenge/response An authentication technique whereby a server sends an unpredictable challenge to the user, who computes a response using some form of authentication token.

checksum A small, integer value computed from a sequence of octets by treating them as integers and computing the sum. A checksum is used to detect transmission errors. The sender computes a checksum and appends it to a packet when transmitting. The receiver verifies the packet's contents by re-computing the checksum and comparing it to the value sent. Many TCP/IP protocols use a 16-bit checksum computed with one's complement arithmetic.

CIR *Committed Information Rate*. The rate, measured in bits per second and averaged over a set time interval, at which a Frame Relay network provider contracts to transfer information across the network under normal conditions.

codec Compression/decompression. Pertaining to adapters that compress and decompress video files. The letters "CODEC" represent "compression / decompression"; in the past, they represented "coder/decoder."

compression A technique for reducing the apparent amount of traffic on a data link. The router, for instance, supports Van Jacobson's header compression for IP over Point-to-Point Protocol links. This is an option which reduces the normal 40 byte header to 4–5 bytes.

congestion A condition that occurs when the offered load exceeds the capacity of a data communication path.

CPE Customer Promise Equipment.

CPU *Central Processing Unit*. In the router, this is a microprocessor that controls all operations necessary to the functioning of the router.

D

data link layer The network layer that is responsible for data transfer across a single physical connection, or series of bridged connections, between two network entities.

datagram A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network. See frame, packet.

dialup A temporary, as opposed to dedicated, connection between machines established over a standard phone line.

directed broadcast A packet deliver system that delivers a copy of a given packet to "all hosts" on a specific network. A single copy of a directed

broadcast is routed to the specified network where it is broadcast to all machines on that network.

DHCP *Dynamic Host Configuration Protocol*. TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally-administered servers.

DNS *Domain Name System*. The distributed name/address mechanism used in the Internet. It comprises distributed online databases that contain mappings between human-readable names and IP addresses, and servers which provide translation services to client applications.

domain A part of the DNS naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), e.g., "machine.company.com". See DNS.

dotted decimal notation The syntactic representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It is used to represent IP addresses in the Internet, e.g. 172.16.9.197.

DSP *Digital Signal Processor*. Specialized computer chip designed to perform speedy and complex operations on digitized waveforms. Useful in processing sound (like voice phone calls) and video.

DTMF *Dual-Tone Multi-Frequency*. In telephone systems, multi-frequency signaling in which a standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four higher frequencies, are used. Although some military telephones have 16 keys, telephones using DTMF usually have 12 keys. Each key corresponds to a different pair of frequencies. Each pair of frequencies corresponds to one of the ten decimal digits, or to the symbol "#" or "*", the "*" being reserved for special purposes.

E

encapsulation The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data.

EPROM *Erasable Programmable Read-Only Memory*. These devices contain the system software on the router, and may need to be changed in some circumstances to upgrade the software to a new release. They are nonvolatile, i.e. they retain their information during power-down. See FLASH

ethernet A common, 10Mbps local area network technology invented by Xerox Corporation at the Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over thinwire coaxial cable (10BASE2), thickwire coaxial cable (10BASE5), twisted pair cable (10BASET), or fibre optic cable.

F

FCS *Frame check sequence*. Bytes added to a frame so that the integrity of the frame may be checked. Typically the bytes are a CRC of the data in the frame.

FXS *Foreign Exchange Service*. A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., "foreign", exchange, rather than the local exchange area's central office. A FXS line is normally connected to a standard telephone, fax or modem.

file transfer The process of copying of a file from one computer to another over a computer network. See anonymous FTP, FTP.

File Transfer Protocol See FTP.

firewall A system or combination of systems that enforces a boundary between two or more networks.

flag A program-readable indicator that can be used to signal an event or a state, or provide simple data values (e.g. TRUE/FALSE, ON/OFF, use option X). For example, in the HDLC data link protocol, the bit pattern 01111110 is used to flag the beginning and end of a frame.

FLASH A new memory technology which combines the nonvolatile features of EPROMs with the easy in-system reprogramming of conventional volatile RAM. See EPROM.

flow control Control of the rate at which devices inject packets into a network, usually to avoid congestion. Flow control mechanisms can be implemented in hardware and/or software, at various protocol layers, and with varying complexity.

frame A frame is a data link layer "packet" which contains the header and trailer information required by the physical medium. That is, network layer packets are encapsulated to become frames. See datagram, encapsulation, packet.

FTP *File Transfer Protocol*. The TCP/IP standard, high-level protocol for transferring files from one computer to another over a network. FTP is also

usually the name of the program that the user invokes to execute the protocol.

See anonymous FTP.

G

G.711 ITU-T recommendation for an algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48, 56, and 64 kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

G.723.1 A Codec that provides the greatest compression, 5.3 kbps or 6.3 kbps; typically specified for multimedia applications such as H.323 videoconferencing.

G.729/G.729A A Codec that provides near toll quality at a low delay which uses compression to 8 Kbps (8:1 compression rate).

gateway A device linking two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).

gatekeeper A gatekeeper identifies, controls, counts, and supervises the traffic or flow through the network. It also provides functions such as terminal and gateway registration, address resolution, band-width control, and admission control.

H

H323 An umbrella standard for audio/video conferencing over unreliable networks; architecture and procedures are covered by this standard; H.323 relies on H.225 and H.245.

header The portion of a packet, preceding the actual data, containing source and destination addresses, and error checking and other fields. A header is also the part of an electronic mail message that precedes the body of a message and contains, among other things, the message originator, date and time. See packet.

hello packet Hello packets are used in a number of network protocols, to perform similar functions. Typically, a Hello packet is used to advertise a node's presence to the network or to establish and maintain information about the presence of other nodes (including hosts and routers) in the network.

heterogeneous network A network running multiple network layer protocols, e.g. DECnet, IP, IPX.

host An (end-user) computer system that connects to a network, such as a PC, minicomputer or mainframe.

I

ICMP *Internet Control Message Protocol*. The TCP/IP protocol used to handle errors and control messages at the IP layer. ICMP is part of the IP protocol. Gateways, routers and hosts use ICMP to send reports of problems about datagrams back to the original source that sent the datagram.

IEEE *Institute of Electrical and Electronics Engineers*. A standard-making body in the U.S. responsible for the 802 standards for local area networks.

IEEE 802.3 See 802.3.

IETF *Internet Engineering Task Force*. One of the task forces of the IAB (*Internet Activities Board*). It is a large, open community of network designers, operators, vendors, and researchers whose purpose is to coordinate the operation, management and evolution of the Internet, and to resolve short-range and mid-range protocol and architectural issues. It is a major source of proposals for protocol standards which are submitted to the IAB for final approval.

IGMP *Internet Group Management Protocol* A protocol for managing the addition and deletion of hosts from multicast groups.

interface One of the physical ports on the router, including the Ethernet, asynchronous and synchronous ports.

interface type The type (Ethernet, Frame relay or Point-to-Point) of one of the interfaces on the router.

International Organisation for Standardisation See ISO.

internet A collection of networks interconnected by a set of routers which allow them to function as a single, large virtual network.

Internet (note the capital "I") The largest internet in the world consisting of large national backbone networks (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. The Internet is a multiprotocol network, but generally carries TCP/IP.

Internet address See IP address.

Internet Protocol See IP.

interoperability The ability of software and hardware on multiple machines from multiple vendors to communicate meaningfully.

IP *Internet Protocol*. The network layer protocol for the TCP/IP protocol suite. It is a connectionless, best-effort packet switching protocol.

IP address A 32-bit address assigned to hosts using TCP/IP. The address specifies a specific connection to a network, not the host itself. See dotted decimal notation.

IP datagram The fundamental unit of information passed across the Internet. It contains a source and destination address along with data and a number of fields which define such things as the length of the datagram, the header checksum, and flags to say whether the datagram can be (or has been) fragmented.

IP interface An entity representing an IP layer attached to a layer 2 interface and all information the IP routing algorithm needs to know to use the layer 2 interface to transmit datagrams over that physical connection. An IP interface consists of one or more IP logical interfaces.

IP logical interface An entity which represents an IP layer interface and holds all network layer specific information such as network address, mask, metric, etc. Multiple logical interfaces can be bundled together in a single IP interface.

ISDN *Integrated Services Digital Network*. A technology which combines voice and digital network services in a single medium, making it possible for telecommunications providers to offer customers digital data services as well as voice connections through a single "wire". The standards that define ISDN are specified by CCITT.

IS-IS *Intermediate System-Intermediate System*. The OSI interior gateway protocol for exchanging routing information between routers within an autonomous system.

ISO *International Organisation for Standardisation*. An international body that develops standards in many areas, including network protocols. It is best known for the seven-layer OSI (Open Systems Interconnection) suite of network protocols.

ITS *Internet telephony service provider*

ITU-T *International Telecommunication Union - Telecommunications Sector*

L

LAN *Local Area Network*. Any physical network technology (such as Ethernet) that operates at high speed (typically 10 Mbits per second or more) over short distances (up to a few kilometres). See WAN.

layer Communication networks for computers may be organized as a set of more or less independent protocols, each in a different layer (also called level).

The lowest layer governs direct host-to-host communication between the hardware on different hosts; the highest layer consists of user applications. Each layer builds on the layer beneath it. For each layer, programs at different hosts use protocols appropriate to the layer to communicate with each other. TCP/IP has five layers of protocols; OSI has seven. The advantages of different layers of protocols is that the methods of passing information from one layer to another are specified clearly as part of the protocol suite, and changes within a protocol layer are prevented from

affecting the other layers. This greatly simplifies the task of designing and maintaining communication programs.

layer 2 interface An entity representing the layer 2 interface in the OSI/ISO network layering model, also referred to as a link layer interface. Examples are Ethernet, PPP, X.25 and Frame Relay.

LED *Light Emitting Diode*. A luminous indicator.

local interface A default logical interface for all locally generated IP packets.

loopback A state in which data transmitted is also received. Normally it is used to test data links by applying a loopback at various points and verifying successful reception of the data transmitted.

M

MAC *Media Access Control*. The lower portion of the data link layer. The MAC differs for various physical media.

MAC address The hardware address of a device connected to a shared media. For example, the MAC address of a PC on an Ethernet is its Ethernet address.

Management information base See MIB.

mask A bit pattern used to “mask out” portions of data.

Mb/s Megabits per Second. Unit of data transmission speed.

MCU *Multipoint control unit*. Unit that manages conference resources, negotiates between terminals for the purpose of determining the audio or video coder/decoder (CODEC) to use, and may handle the media stream.

MIB *Management Information Base*. The set of parameters an SNMP management station can query or set in the SNMP agent of a network device (e.g., router). Standard MIBs have been defined, and vendors can develop private MIBs. In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB. See SNMP.

modem *Modulator/demodulator*. A device that takes digital data from a computer and encodes it in analog form for transmission over a phone line. See NTU.

MTU *Maximum Transmission Unit*. The largest possible unit of data that can be sent on a given physical medium. For local area networks (e.g. Ethernet), the MTU is determined by the network hardware. For wide area networks using serial lines, the MTU is determined by software. The MTU of Ethernet is 1500 bytes.

multi-homed gateway A dual homed gateway is a system that has two or more network interfaces, each of which is connected to a different network.

In firewall configurations, a multi homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks.

multicast A special form of broadcast where copies of the packet are delivered to only a subset of all possible destinations. See broadcast, directed broadcast, unicast.

N

NAK *Negative acknowledgement*. A response sent to indicate unsuccessful reception of information. Usually, a NAK triggers retransmission of the lost data. See ACK.

name resolution The process of mapping a name into the corresponding address. See DNS.

NCP *Network Control Protocol*. A protocol forming part of the Point-to-Point Protocol, used to establish and configure different network layer protocols running over point-to-point links. Each network layer protocol (e.g. IP, IPX, DECnet) has it's own associated NCP.

network A computer network is a data communications system which interconnects computer systems at various different sites. A network may be composed of any combination of LANs, MANs or WANs.

network address The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique. See IP address.

network number See network address.

network-level firewall A firewall in which traffic is examined at the network protocol packet level.

NIC *Network Information Center*. A group at SRI International, Menlo Park, CA, responsible for providing users with information about TCP/IP and the connected Internet. The machine named NIC.DDN.MIL is an online archive of RFCs and other documents related to TCP/IP.

NSAP Network Service Access Point. The point at which network services are provided by a network entity to a transport entity according to the OSI reference model. NSAP addresses are assigned by a hierarchy of registration authorities so that each valid NSAP address provides a globally unambiguous identification of one system. One system may have multiple NSAP addresses

NTU *Network Terminating Unit*. A device that takes digital data from a computer and encodes it for transmission over digital telecommunication lines. It is the equivalent of a modem for modern digital links. See modem.

NVS *Nonvolatile Storage*. Static RAM that has its contents preserved through gateway power cycles through the use of a battery that maintains power to the RAM.

O

octet An octet is 8 bits. This term is used in networking, rather than byte, because some systems have bytes that are not 8 bits long.

OSI *Open Systems Interconnection*. A suite of protocols, specifically ISO standards, to be the international standard computer network architecture. See ISO.

P

packet The unit of data sent across a network. "Packet" is a generic term used to describe units of data at all levels of the protocol stack, but it is most correctly used to describe application data units. See datagram, frame.

packet switching A communications paradigm in which packets (messages) are individually routed between hosts, with no previously established communication path.

parity A method of checking the integrity of characters transmitted serially. It does this by defining an extra bit whose value is set to ensure either an even (even parity) or odd (odd parity) number of '1' bits in the character.

patch A piece of computer code used to correct or enhance an existing piece of code. In the router, patches are applied by "overlying" them on existing code in RAM. The patches are loaded into the router using a process called *downline loading*.

PBX *Private Branch Exchange* (1) An automatic or manual private telephone exchange for transmission of calls to and from the public telephone network. (2) A switching system located on a customer's premises that consolidates the number of inside lines (extensions) into a smaller number of outside lines (trunks). Many PBXs also provide advanced voice and data communication features.

ping *Packet InterNet Groper*. A program used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply. The term is used as a verb: "Ping host X to see if it is up!".

POTS *Plain Old Telephone System*. Standard telephone service used by most residential locations; basic service supplying standard single line telephones, telephone lines, and access to the public switched network.

privilege A term used in computing to refer the access rights or level of trusted afforded to a user of the computer system. A privileged user has access to "more powerful" commands which may (adversely) affect the

operation of the system or the activities of other users. The router has two levels of privilege, **MANAGER** and **USER**. Users with **USER** privilege (most users) have access to a limited subset of the commands available to **MANAGER** level users.

prompt A text string displayed on a terminal by a computer to indicate that it is ready to receive the next command from the user.

protocol A formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces (e.g., the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (e.g., the way in which two programs transfer a file across the Internet).

proxy A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user is permitted to use the proxy, performs any additional authentication, and then completes a connection on behalf of the user to a remote destination.

PSN *Packet Switch Node*. A dedicated computer whose purpose is to accept, route and forward packets in a packet switched network. See packet switching.

PSTN *Public-Switched Telephone Network*. A communication common carrier network that provides voice and data communication services over switched lines.

Q

QCIF *Quarter common intermediate format*

R

RAS *Reliability, availability, and serviceability*. Rated throughput for data links, the rate at which all of the offered frames are forwarded by the device.

RFC *Request for comments*. The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs.

router A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as "routing metrics." See gateway.

RS-232 An EIA (Electronics Industry Association) standard that specifies the electrical characteristics of low speed interconnections between terminals and computers or between two computers.

RTCP *Real-time transport control protocol*. Is the counterpart of RTP that provides control services.

RTP *Real-time transport protocol*. Provides end-to-end delivery services of real-time audio and video.

S

SCN *Switched circuit network*

serial A method of transmission in which each bit of information is sent sequentially on a single channel rather than simultaneously as in parallel transmission.

server A network device that provides services to client stations. Examples include file servers and print servers.

SIP *Session initiation protocol*. Is an application layer, control/signalling protocol for creating, modifying and terminating sessions with one or more participants. These sessions may include Internet multimedia conferences, distance learning, Internet telephone calls and multimedia distribution.

SNMP *Simple Network Management Protocol*. The Internet standard protocol developed to manage nodes on an IP network. See MIB.

stop bits A technique used in asynchronous serial communications in which 1, 1.5 or 2 bits are transmitted after the start bit, a variable number of data bits and optional parity bit are transmitted. It is designed to frame the character.

subnet A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an internet.

subnet address The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using an address or subnet mask. See subnet mask, IP address, network address.

subnet mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called address mask.

synchronous Transmission in which the data characters and bits are transmitted at a fixed rate with the transmitter and receiver synchronised. This eliminates the need for start-stop elements, as in asynchronous transmission, but requires a flag character to be transmitted when there is no data to transmit. See asynchronous.

T

TCP *Transmission Control Protocol*. The TCP/IP standard transport layer protocol in the Internet suite of protocols, providing reliable, connection-oriented, full-duplex streams. It uses IP for delivery.

TCP/IP Protocol Suite *Transmission Control Protocol over Internet Protocol*. This is a common shorthand which refers to the suite of transport and application protocols which runs over IP. See IP, ICMP, TCP, UDP, FTP, Telnet, SNMP.

telephony The science of translating sound into electrical signals, transmitting them, and then converting them back into sound.

telnet The virtual terminal protocol in the TCP/IP suite of protocols, which allows users of one host to log into a remote host and interact as normal terminal users of that host.

TFTP *Trivial File Transfer Protocol*. The TCP/IP standard protocol for file transfer with minimal capability and minimum overhead, based on UDP. It is often used by diskless workstations that keep software in ROM and use it to bootstrap themselves. It is used in the router for downloading patches.

U

UDP *User Datagram Protocol*. A transport layer protocol in the TCP/IP suite of protocols. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgements or guaranteed delivery.

unicast A packet broadcast to a single host attached to the network. See broadcast, directed broadcast, multicast.

V

VLAN *Virtual Local Area Network*. Secure connection of TCP/IP based networks, intranets and extranets across the Internet

VPN *Virtual Private Network*. A private network built over an insecure public network, such as the Internet, in which communication between peer sites is encrypted to prevent unauthorised monitoring of session data and unauthorised access into the VPN from the public network.

VT-100 A popular model of DEC terminal. Many third party vendors make VT-100 compatible terminals. The term VT-100 is also used to describe the characteristics of terminals that may be connected to a device.

VoIP *Voice Over Internet Protocol*. The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

W

WAN *Wide Area Network*. Any physical network technology that spans large geographic distances. WANs usually operate a slower speeds than LANs or MANs. See WAN.

WWW *World Wide Web*. A hypertext-based, distributed information system based on a client-server architecture. Web browsers (client applications) request documents from Web servers. Documents may contain text, graphics and audiovisual data, as well as links to other documents and services. Web servers and documents are identified by URLs (Uniform Resource Locators).

Index

- ADD NTP SERVER, 29
- ADD VLAN PORT, 85
- Addressing, **21**
- CLI, 2, 5, 6, 31, 48
- Command Line Interface, **2**. *See also CLI*
- Configuration Script, 5, 28
- CREATE CONFIG, 7
- CREATE L2TP, 65
- CREATE SIP PORT, 52
- CREATE VLAN, 86
- DELETE CONFIG, 8
- DELETE L2TP, 66
- DELETE NTP SERVER, 29
- DELETE SIP PORT, 54
- DELETE VLAN, 87
- DESTROY VLAN, 87
- DHCP, x, **27**
- DHCP Server, 2, **28**
- DISABLE IP IGMP, 30
- DISABLE L2TP, 65
- DISABLE SIP, 54
- DISABLE SNMP, 60
- DISABLE SWITCH AGEINGTIMER, 88
- DISABLE SWITCH LEARNING, 88
- DISABLE SWITCH PORT, 89
- DNS, **39**
- ENABLE IP IGMP, 30
- ENABLE L2TP, 64
- ENABLE NTP, 31
- ENABLE SIP, 54
- ENABLE SNMP, 60
- ENABLE SWITCH AGEINGTIMER, 89
- ENABLE SWITCH LEARNING, 90
- ENABLE SWITCH PORT, 90
- ENABLE TELNET, 31
- EXEC CONFIG, 9, 2, 5, 71, 72, 73, 76, 78, 108
- H.323, x
- Help, **5**
- HELP, 9
- ICMP, x
- IEEE 802.2, x
- IEEE 802.3, x
- IGMP, **24, 25**
- IGMP snooping, **26**
- Internet, **18**
- Internet Protocols, x, xi
- IP, x, 9, **18**
- L2TP, **63**, 1, 28, 48, 49
- LOAD CONFIG, 9
- LOAD IMAGE, 10
- LOGOUT, 11
- MGCP, 1
- MIB, 58, 59
- NSLOOKUP HOST, 43
- NTP, x
- NTP Protocol, **28**
- Operation, **1**
- Phone, **68**
- PING, 31
- PSTN, viii, 1, 2, 48, 74, 75, 80
- RESET SWITCH, 91
- RESET SWITCH PORT, 91
- RESTART REBOOT, 11
- Ring, 71, 48
- RTP, x, 48, 53, 57, 73
- SAVE CONFIG, 11
- SDP, x
- SET CONFIG, 12
- SET DNS IP, 40
- SET DOMAIN, 40, 55

- SET IP IGMP, 31
- SET IP INTERFACE, 33
- SET IP NAMESERVER, 41
- SET IP SECONDARYNAMESERVER, 41
- SET LOADER, 12
- SET NTP, 34
- SET PASSWORD, 13
- SET PHONE, 75
- SET SIP PORT, 55
- SET SNMP COMMUNITY, 60
- SET SNMP MANAGER, 61
- SET SWITCH AGEINGTIMER, 92
- SET SWITCH PORT, 92
- SET SWITCH QOS, 94
- SET SYSTEM, 13
- SHOW CONFIG, 14
- SHOW DNS, 41, 56
- SHOW IP HOST, 42
- SHOW IP IGMP, 35
- SHOW IP INTERFACE, 36
- SHOW L2TP, 66
- SHOW LOADER, 15
- SHOW NTP, 37
- SHOW PHONE, 77
- SHOW SIP PORT, 56
- SHOW SNMP, 61
- SHOW SWITCH, 95
- SHOW SWITCH FDB, 95
- SHOW SWITCH PORT, 97
- SHOW SWITCH PORT COUNTER, 99
- SHOW SWITCH QOS, 101
- SHOW SYSTEM, 16
- SHOW VLAN, 102
- SIP, x, xii, 1, 9, 51
- SIP Protocol, 44
- SNMP, x, **58**, 59
- Subnets, **23**
- Switch, **81**, 83
- TCP, x, 19
- Telnet, x, 19
- TFTP, x, 2, 5, 7, 28
- Tone, 71
- UDP, x
- VIEW CONFIG, 17
- VLAN, 81, 82, 84
- VOIP, viii, xii, 2, 74, 75, 80
- X.25, 19