Pace Unified Software CLI tree description

S.Grelet

March 2011

Pace plc, Victoria Road, Saltaire BD18 3LF UK
Tel: +44 (0) 1274 532000 Fax: +44 (0) 1274 532010

BRINGING TECHNOLOGY HOME
www.pace.com

Table of contents

1 CONFIG

This object may contain information about a specific configuration (description, version...).

1.1 VERSION

The current version of the configuration system.

Must not be modified is it is tested in shell scripts to test compatibility.

1.2 DESCRIPTION

Human-readable description of the configuration.

2 HARDWARE

Hardware platform capabilities.

This object contains the hardware capabilities of the device. The parameters inside this object can be checked by programs or web pages to drive their behavior.

2.1 WATCHDOG

The hardware includes a watchdog timer.

When set, will enable the use of this timer in the firmware.

2.2 REALTIMECLOCK

The hardware includes a permanent real time clock with a battery.

When set, will enable the use of this clock in the firmware. The firmware will set its date/time at boot time from the hardware clock.

2.3 USBMASTER

The hardware includes an USB host controller.

The firmware checks this parameter to enable loading of modules and services based on the USB host. Among these are hard disks, webcam, 3G modem ...

2.4 BLUETOOTHONUSB

The firmware includes BlueTooth on USB modules and services.

The web pages check this parameter to allow display and setting up of the BlueTooth over USB services.

Dependency: _Hardware_USBMaster must be set too.

Note: (obsolescence) This parameter is only used on Generic Ibox and the feature is not maintained.

2.5 VOIP

The hardware includes Voice Over IP capabilities.

Firmware checks this parameter to enable loading of VoIP modules and services.

2.6 WIFIN

The hardware includes a 802.11n WIFI controller.

When unset, the WIFI controller can only do 802.11bg. The web pages check this parameter to authorize the user of selecting 802.11n data rates.

3 DEVICE

Object containing parameters and status information that are global to the CPE.

3.1 PRODUCT

Object gathering Product information.

3.1.1 CODE

A unique hexadecimal number presented as a string.

This parameter uniquely identifies the firmware type. Different web pages or different factory configuration implies different Product Codes.

3.1.2 NAME

A human readable string that identifies the device (hardware + firmware).

This parameter is generally displayed in the main web configuration page. It is also transmitted by remote management like TR-069 protocol.

3.1.3 SUBNAME

A substring associated to _Device_Product_Name.

Complementary information associated to the Name above.

3.1.4 DESCRIPTION

Optional description of the device.

Generally unused.

3.1.5 PRODUCTCLASS

A String used by the TR-069 protocol.

The remote TR-069 server checks this parameter to uniquely identify the device type. If this parameter is left empty the _Device_Product_Code is used instead.

3.1.6 MANUFACTURER

The manufacturer / editor of the hardware / firmware.

say, BeWAN systems.

3.1.7 MANUFACTUREROUI

The Organization Unique Identifier of the manufacturer.

This is the first 3 bytes of the MAC address (for BeWAN, 000CC3). The TR-069 protocol sends this parameter to the remote server (ACS).

3.1.8 PROVISIONINGCODE

This parameter is directly used by TR-069 protocol.

See a detailed description in the TR-069 specifications. Generally set by the ACS to indicate the options pushed in the box.

3.1.9 CONFIGFILE

This objects are not used in the standard firmware.

- Name

Used by TR-069 protocol.

This parameter is read by the ACS of one of our customer.

- Version

Used by TR-069 protocol.

This is read / written by the ACS of one of our customer.

- Date

This is read / written by the TR-069 ACS of one of our customer.

- Description

This is read / written by the TR-069 ACS of one of our customer.

3.2 HOSTNAME

The network hostname of the device.

The device is recognized in the Local Area Network as hostname. It will answer if we ping hostname.

Note: An entry is created in the file {{{/etc/hosts}}} to associate the device LAN IP address to hostname.

3.3 ALIASES

List of aliases to hostname.

Alternative network names for the device (i.e. the device will also answer if we ping or connect to those names).

Note: Additional entries are created in {{{/etc/hosts}}} for aliases.

3.4 DOMAIN

DNS domain of the device.

The device will answer if we ping {{{hostname.domain}}}. The domain is also recorded in the {{{/etc/hosts}}} file.

3.5 PAGEZERO

This object displays status information stored in the boot loader flash partition.

3.5.1 LANMAC

The MAC address of the device stored in page zero.

The MAC address is unique for each device sample. It is recorded in the boot loader so that the information is not overwritten by firmware upgrades. The unique MAC address is programmed during the manufacturing test process. This MAC address is used by firmware to initialize the LAN interfaces.

3.5.2 WANMAC

This is a secondary MAC address for WAN interfaces.

Must have the same value as _Device_PageZero_LanMac.

We reserved this place in boot loader but we don't use a secondary factory MAC address. We use instead locally derived MAC addresses for the different network interfaces of the device.

Locally derived MAC addresses are generated by adding "n*6" (with n=0,1,2,3...) to the first byte of the MAC address (See description of the _ATMEthernetInterface_?_HwMacId parameter).

3.5.3 WEPKEY

A string used to initialize the default WEP or WPA keys.

13 characters - This string is generated during manufacturing process. It is unique to each device sample so that it cannot be the same between two devices. After a factory reset, the WIFI access point is initialized with this default key.

3.5.4 SerialNumber

The unique serial number of the device.

The Serial Number (SN) allows the remote management to discriminate the different devices/subscribers.

Note: string of numeric characters of a specific format - generated during manufacturing process. The format of the string is described in another document.

3.5.5 ProductCode

The Product Code that identifies the firmware.

This parameter stored in the boot loader is a copy of the _Device_Product_Code parameter. This copy is checked by the firmware upgrade utility to disallow a change of firmware type.

3.5.6 LoaderVersion

This is the subversion revision number of the boot loader code.

3.5.7 ProductFamily

The Product Family that identifies the hardware type of the board.

Same format as _Device_PageZero_ProductCode. This parameter stored in the boot loader. This copy is checked by the firmware upgrade utility to disallow a change of hardware type.

3.5.8 Firmware

Information about the firmware stored in the flash.

- CurrentFirmware

Name of the firmware currently running in the device.

The format of the firmware name is something like {{{PRODUCTCODE-NAME-REVISIONNUMBER.bin}}}.

- PreviousFirmware

Name of the firmware previously programmed in the device.

Same format as _Device_PageZero_Firmware_CurrentFirmware - The flash contains two firmware versions.

Note: The upgrade utility programs the new firmware into the alternate bank of the flash. It then checks the integrity of the new firmware before switching the banks.

3.6 FirmwareVersion

Version of the firmware currently running.

Format is {{{PRODUCTCODE-NAME-REVISIONNUMBER}}}. This information is coming from the file {{{/etc/release}}}.

3.7 StrippedFirmwareVersion

Stripped Firmware Name.

3.8 Uptime

Time elasped since last boot.

Two numbers with dots - Format is x.y seconds where x is seconds and y hundredths of seconds. The first number indicates total time elapsed since boot and the other the number of seconds where the system was idle.

3.9 MemInfo

Object reporting status information about memory used by the system.

All this information is extracted from the results of the command {{{cat /proc/meminfo}}}.

3.9.1 MemTotal

Total physical RAM used by linux.

3.9.2 MemFree

Free physical memory (more memory is available because the system can flush execution code).

3.9.3 Cached

Amount of memory used by the file system cache.

3.9.4 Committed_AS

Amount of physical memory containing modified data.

3.10 LogRead

The contents of the first lines of the syslog.

This information is the truncated result of the command logread.

3.11 FirstInternetConnection

When set to 1, indicates that no successful connection to Internet has been done yet by the device.

This parameter allows some diagnostics. If the connection to the Internet fails and _Device_FirstInternetConnection is unset, we can conclude to a network failure. If _Device_FirstInternetConnection is set, this means that the device is probably not configured correctly (e.g. wrong PPP login/password, ...).

3.12 USBInfo

List all USB devices connected to the box.

Note: For more info, you can check "proc_usb_info.txt" in "linux-2.6.16.x/Documentation/usb/"

3.12.1 BUS

3.12.2 PARENT

3.12.3 LEVEL

3.12.4 CONNECTOR

3.12.5 COUNTOFDEVICES

3.12.6 DEVICENUMBER

3.12.7 SPEED

3.12.8 MAXCHILDREN

3.12.9 VERSION

3.12.10 CLASS

3.12.11 SUBCLASS

3.12.12 PROTOCOL

3.12.13 MAXPACKETSIZE

3.12.14 NUMBEROFCONFIGURATIONS

3.12.15 VENDORID

3.12.16 PRODUCTID

3.12.17 PRODUCTREVISION

3.12.18 VENDORNAME

Manufacturer of this device as read from the device.

3.12.19 PRODUCTNAME

3.12.20 SERIALNUMBER

3.12.21 BANDWIDTH

Applies only to USB host controllers.

- Allocated

Show approximation of how much of one frame (millisecond) is in use.

- InterruptRequest

Stats about number of interrupt requests.

- IsochronousRequest

Stats about number of isochronous requests.

3.12.22 CONFIGURATION

- Active
- NumberOfInterface

- ConfigurationNumber
- Attributes
- MaxPower
- Interface_Count
- Interface
- Active
- InterfaceNumber
- AlternateSettingNumber
- NumberOfEndpoint
- Class
- SubClass
- Protocol
- Driver

The name of linux driver/module that drive this interface.

- Endpoint
- Address
- Mode
- Attributes
- Type
- MaxPacketSize
- Interval

4 HOSTTABLE

MAC addresses to LAN hostnames association.

This object is intended to be used by the Web User Interface.

The goal is to associate PCs connected to the LAN to human-readable names. PCs are identified by their MAC address but they are shown in the Web UI by their name. Each time we need to enter a MAC address in the GUI, we can enter a name instead.

Note: This object is obsolete.

4.1 CLIENTNAME

Unused

4.2 MACADDRESS

Unused

5 UserTable

Describes a registered user of the CPE.

Each user can be enabled/disabled for CPE services.

Note: IAD HTML, the WUI configurator, uses user login and password in _WebConfigurator (see it) CLI forbid to create 'root' and 'www' user. If _UserTable_?_Unix_Password is set to 'invalid', the CLI will refuse to change it.

5.1 UserName

Login that will be used in authentification.

5.2 UserEmail

Email of current user (used for Web for example).

5.3 RootDir

Set the home directory for current user (see Notes).

Note: Not used in {{{/etc/passwd}}} when _UserTable_?_Unix_Enable is set.

5.4 AliasOnDisks

When set, creates a symbolic link from {{{/var/mnt}}} to {{{/var/home/$USER/Disks}}}.

5.5 AliasOnHomes

When set, creates a symbolic link from {{{/var/mnt}}} to {{{/var/home/$USER/Home}}}.

5.6 Unix

If enabled, current user can use Telnet or SSH services.

5.6.1 Enable

If set, current user will be added in {{{/etc/passwd}}}.

5.6.2 Password

the password in crypt format.

5.7 Samba

If enabled, current user can connect on Samba services.

5.7.1 Enable

If enabled, current user can connect on Samba services. Check _SambaConfigurator_Opened for anonymous mode

5.7.2 Password

Password encrypted with smbpasswd executable.

5.8 PureFTPD

A fully parametrable FTP server for the CPE.

5.8.1 Enable

When set, enables the embedded FTP server.

5.8.2 Password

Password for current user for FTP access

5.8.3 DownloadLimit

Download bandwidth limit, please check PureFTP doc

5.8.4 UploadLimit

Upload bandwidth limit, please check PureFTP doc

5.8.5 MaxNumberFiles

Max number of files allower by FTP server for current user, please check PureFTP doc

5.8.6 MaxMBytes

Max bytes (in MB) allowed for the current user. Please check PureFTPD doc (quota)

5.8.7 RatioDownload

Ratio Upload/Download, please check PureFTP documentation.

5.8.8 RatioUpload

Ratio Upload/Download, please check PureFTP documentation.

5.8.9 AllowClientIpMask

Allow clients connections from the given IP/mask.

5.8.10 DenyClientIpMask

Deny clients connections from the given IP/mask.

5.8.11 MaxNumberConcurrentSessions

5.9 Http

When set, current user can use NAS HTML services (if enabled in FirmWare).

5.9.1 Enable

If set, current user will be added in {{{.naspasswd}}} and {{{.nasaudiopasswd}}}.

5.9.2 Password

Password in MD5 (for lighttpd {{{.htpasswd}}}).

5.9.3 HtPassword

Password encrypted with htpasswd executable (for {{{.htpasswd}}}'s thttpd).

5.9.4 PasswordClear

Password in clear.

5.9.5 Rights

Reserved for future usage.

6 SambaConfigurator

Samba/CIFS file server configuration settings.

Samba/CIFS file server.

6.1 Enable

Enable samba/CIFS service.

6.2 Opened

Automatically share all the connected storage devices without user authentication.

6.3 Port

6.4 NmbPort

6.5 ServerString

Optional short description of the Samba server.

6.6 ShareName

The name of the Samba/CIFS share.

6.7 ShareNameLength

6.8 Workgroup

Samba/CIFS workgroup.

6.9 InterfaceList

Make the Samba/CIFS server listen on given network interfaces.

6.10 PrinterEnable

Make the Samba/CIFS share the printers.

6.11 StorageEnable

Make the Samba/CIFS share the storage.

6.12 Status

Samba activity.

7 PureFtpdConfigurator

Configuration for the embedded FTP server.

7.1 Enable

When set, enables the FTP server.

7.2 AnonymousLoginsProhibited

When set, disable access for anonymous clients.

7.3 AnonymousRootDir

7.4 DisallowUploadForAnonymousUsers

When set, deny files uploading to the non-authentified users.

7.5 DisallowDownloadForAnonymousUsers

When set, deny files downloading to the non-authentified users.

7.6 AllowAnonymousUsersToCreateDirectories

7.7 ConnectionsMax

Maximum connections allowed on the server at the same time.

7.8 ConnectionsMaxSameIP

Maximum connections from the same IP address allowed on the server at the same time.

7.9 MaxUserLogins

7.10 MaxAnonymousLogins

7.11 WelcomeMessage

Welcome message that will be sent to incoming connections.

7.12 UploadPercentLimit

7.13 DownloadLimit

Bandwidth limit for downloads, in Kb/s.

7.14 UploadLimit

Bandwidth limit for uploads, in Kb/s.

7.15 RatioDownload

7.16 RatioUpload

7.17 Port

The port on which the FTP server should listen for incoming connections.

8 StorageConfigurator

Register and manage USB storage devices.

8.1 Enable

When set, enables USB storage device management.

8.2 Storage

A registered storage device.

8.2.1 Identifier

An unique identifier for the current storage device.

8.2.2 Description

Vendor and model information for current storage device.

8.2.3 ShareName

Name of the current storage device when shared on local networks.

8.2.4 ShareEnable

When set, share the current storage device on local networks.

8.2.5 ShareWritable

8.2.6 PartitionName

8.2.7 Status

Indicates the state of the device (Disconnected,Connected,ConnectedMounted,ConnectedUnmounted,ConnectedUnusable).

8.2.8 MountPoint

If _StorageConfigurator_Storage_?_Status is ConnectedMounted, then indicates where the device is currently mounted. In other cases, says where it should be mounted.

8.2.9 Device

The device path associated with current storage object.

8.2.10 SysDevice

The sysdevice path associated with current storage object.

8.2.11 Writable

When set, allow write access on the current storage device via network shares.

8.2.12 Stats

- BytesRead
- BytesWritten

8.2.13 Size

- Used

Used space on storage, in bytes

- Total

Total space on storage, in bytes

9 PRINTERCONFIGURATOR

Printer settings definitions.

9.1 ENABLE

When set, connected printer(s) are shared.

Dependency: Use usblp module in Linux kernel.

9.2 MULTIPRINTER

When set, manage multiple printers at the same time.

9.3 PORT

Listen on given port for the mono-printer service.

9.4 PRINTER

A printer that was registered on the CPE.

Each printer that was connected to CPE is saved in this list to remember used Port, Name, and Sharing status.

9.4.1 ENABLE

When set, current printer is shared (if connected).

9.4.2 DESCRIPTION

Name of printer, the default value is "Manufacturer-Product".

9.4.3 SHARENAME

9.4.4 IDENTIFIER

UID that is send by printer.

9.4.5 PORT

Port used by current printer (it can't be used by other printers).

9.4.6 STATUS

Indicates the state of the device (Disconnected,Connected).

9.4.7 DEVICE

9.4.8 SYSDEVICE

9.4.9 MANUFACTURER

9.4.10 PRODUCT

9.4.11 STATS

BytesRead

BytesWritten

10 HttpServer

HTTP server for the Network Attached Storage (NAS).

This object describes which services are enabled or disabed for NAS. NAS contains for example a html page for viewing webcam or listening music from network (LAN or WAN). NAS is not intended for modifying CPE's parameters.

Note: {{{/etc/init.d/web}}} script will try to guess which http server to launch (thttpd or lighttpd). It's possible to have another instance of http server to deliver mp3 (check {{{/etc/init.d/web}}} and {{{/etc/init.d/nas_audio}}}).

10.1 Enable

Set this parameter to 1 to enable the NAS services.

10.2 LogQueries

Set this parameter to 1 to print in syslog all files requested from http

10.3 Language

Current language for web.

It represents the default language.

10.4 NativeLanguage

Set box native language for webpages.

It is used to know between which languages the webpages must switch (en_US and the NativeLanguage).

10.5 RootDir

Define the root directory for the web.&lt;br The default value is {{{/etc/config.default/web}}}.

Note: If you want to change it, make sure to update {{{/etc/init.d/web}}} and {{{Makefile}}} in {{{/trunk/user/nas_html}}}.

10.6 AnonymousRights

Unix permissions for the anonymous user.

Note: '''Obsolete'''. Only kept for compatibility reason. See _UserTable_?_Http_Rights .

10.7 Port

Port to use for web server.

Make sure that _WebConfigurator_LocalPort and _HttpServer_Port are different.

10.8 SkipAuth

Tell to web server to skip .htpasswd

thttpd extract the IP of interface the first use, since IP can be change after start of thttpd (for example with dhcp)

Note: only implemented with thttpd

10.8.1 Enable

if set, skip authentification to ip matching the ethernet interface below (in 255.255.255.0)

10.8.2 Interface

indicates wich interface to skip authentification

Note: LANDevice must be used in 99% (the only special case is iCam)

10.8.3 InterfaceNumber

tell wich number of LANDevice or WANConnectionDevice to use

10.9 NAS

Web access from NAS.

Note: See also _StorageConfigurator.

10.9.1 Disk

Mounted disk access settings.

Note: This variable is also tested by {{{nas.cgi}}} when used with remote access.

- Enable

If set to 1, allow NAS to use mounted disk

10.9.2 USBWebcam

USB webcam access settings.

Note: See also _WebCam_? for more parameters related to HTTP.

- Enable

When set, enable webcam access from NAS.

10.9.3 iCam

iCam access settings.

- Enable

When set, enable iCam access from NAS.

10.9.4 Music

Music access settings.

- Enable

When set, enable webcam access from NAS.

11 ProxyHTTPServer

Proxy HTTP server.

11.1 Enable

Set this parameter to 1 to enable the HTTP Proxy Server.

11.2 Nice

Set the nice value (priority) of the HTTP Proxy Server.

11.3 ListenPort

Port used to listen for incoming requests.

11.4 ConnectionTimeout

The number of seconds of inactivity a connection is allowed to have before it closed

11.5 LogLevel

Log level, possible values : Info Connect Notice Warning Error Critical .

11.6 MaxClients

Only MaxClients number of clients can be connected at the same time.

11.7 MinServers

At least MinServers processes are created at startup

11.8 MaxServers

Only MaxServers processes can be running at the same time.

11.9 Auth

Tell proxy to make authentication

11.9.1 Enable

if set, authentication is performed by tinyproxy

11.9.2 Method

Method used for authentication

11.9.3 ForcedRealm

Dont send the realm name when authorization is requested, send the hostname as realm instead (thx to Sly)

11.9.4 Realm

List of realms used for authentication

- Name

Name of the realm

- PasswdFile

Password file associated to this realm

- Directories

List the directories (sub-directories are included) included in this realm

- Name

Path of the directory for this given realm

- SkipAuth

Tell to proxy server to skip .htpasswd for this realm

  - Enable

if set, skip authentification to ip matching the ethernet interface below (in 255.255.255.0)

  - Interface

indicates wich interface to skip authentification

Note: LANDevice must be used in 99% (the only special case is iCam)

  - InterfaceNumber

tell which number of LANDevice or WANConnectionDevice to use

11.10 REDIRECTION

Allow proxy to redirect trafic

11.10.1 DEFAULT

If requests dont match any pattern, they are redirected on localhost to this port

11.10.2 DYNAMIC

Allow proxy to dynamically redirect trafic to a remote device

- Enable

If set, use dynamic redirection based on the criteria "detectedBy"

- DetectedBy

Tell which type of service is detecting the remote devices (miniupnpd for now)

11.10.3 STATIC

List of local redirection (match on pattern in url).

- Pattern

If URL starts with this pattern the associated port is used for redirection on localhost.

- IP

IP used to redirect traffic when URL starts with associated pattern.

- Port

Port used to redirect traffic when URL starts with associated pattern.

- SkipPattern

Port used to redirect traffic when URL starts with associated pattern.

12 WebConfigurator

Parameters for configurating the embedded web server.

12.1 Enable

Enable or disable web configuration.

12.2 Nice

Set a nice value for http server.

12.3 LogQueries

Set this parameter to 1 to print in syslog all files requested from http

12.4 StartupMode

Tell which mode will be used by default .

12.5 SwitchModeAllowed

Forbid switch to change mode kept for compatibility reason.

12.6 Language

Current language for web.

The old behavior was to write on router.conf the value of language when switching on web pages. It represents now the default language.

12.7 NativeLanguage

Set box native language for webpages.

It is used to know between which languages the webpages must switch (en_US and the NativeLanguage).

12.8 RootDir

Root dir of files, by default {{{/etc/config.default/html}}}.

12.9 SkipAuth

Tell to web server to skip .htpasswd

thttpd extract the IP of interface the first use, since IP can be change after start of thttpd (for example with dhcp)

Note: only implemented with thttpd

12.9.1 Enable

if set, skip authentification to ip matching the ethernet interface below (in 255.255.255.0)

12.9.2 Interface

indicates wich interface to skip authentification

Note: LANDevice must be used in 99% (the only special case is iCam)

12.9.3 InterfaceNumber

tell wich number of LANDevice or WANConnectionDevice to use

12.10 UserLogin

User login for basic mode.

12.11 UserPassword

User password for basic mode.

12.12 ExpertLogin

Login for expert mode.

User login for expert mode.

12.13 ExpertPassword

Password for export mode.

Password for export mode.

12.14 SuLogin

Login for admin mode.

12.15 SuPassword

Password for admin mode.

12.16 Localized

Use the new tree for translation.

By default, true. The page for old BOX was splitted in two modes, basic, expert, then languages, for example - {{{basic/us/wifi.htm}}} and {{{expert/fr/telnet.htm}}}. Since the use gettext for automatic translation, it's now {{{en_US/basic/wifi.htm}}} and {{{fr_FR/expert/telnet.htm}}}. This parameter is important to redirecting on correct page after submit CGI.

12.17 RestrictedAccess

Can be used for webpages to allow access for admin profil (or unlock parameters in webpages).

12.18 Refresh

Delay (in seconds) before refreshing page.

Used for status or diagnostics pages.

12.19 LocalPort

HTTP port used.

Port listening used by http server.

12.20 LocalIP

IP on which is binded the listening HTTP socket.

12.21 PPPLoginAuto

Use factory PPP login/password.

Can be used by webpage to use current value or factory login/password.

12.22 DefaultFWRules

Default firewall level.

12.23 RemoteWeb

Timer used to disable remote access.

12.23.1 Timer

Indicate time before lauching the script rmthttp will be launched.

The {{{/etc/init.d/rmthttp}}} will be reset the WebConfigurator_RemoteWeb to blank and remove in _WANConnectionDevice_?_Service_? the entry for rmtweb.

12.23.2 Login

Login for remote access.

12.23.3 PWD

Password for remote access for thttpd.

12.23.4 PASSWORD

Password for remote access password - writable - for lighttpd.

13 Services

This object is gathering most of the services that can be configured to run in the box.

13.1 UnixAdmin

With this object, we can create a special user that can log to the CPE with telnet or ssh.

This UnixAdmin user is considered as an administrator with no root privileges.

13.1.1 Username

The login name of the user. If left empty, the user is not created.

13.1.2 Password

The password for this login.

13.1.3 UserID

The unix userid of the user (must not be 0, default is 1).

13.1.4 GroupID

The unix gid of the user (must not be 0, default is 0).

13.1.5 Shell

This is the front end application of the user when logged.

Could be set to {{{/bin/cli}}} for the configuration command line interface.

13.2 Telnet

An embedded Telnet server for the CPE.

The telnet server listens for incoming calls on port 23. To allow incoming calls for telnet from a WAN interface, you need to open the firewall for this interface. You can also specify a translation in the listening port. See _WANConnectionDevice_?_Service entries.

Dependency: The telnet server is based on the well known inetd linux daemon and the associated telnetd program that takes it's input/output through stdin/stdout.

You must enable this feature in the firmware via menuconfig:

{{{[*] Customize BusyBox Settings Networking Utilities ---

[*] inetd

[*] telnetd

[*] Support call from inetd only.}}}

13.2.1 Enable

When set, enables the Telnet service.

13.3 SSH

Enables the SSH server on the box.

The SSH server listens for incoming calls on port 22. To allow incoming calls for ssh from a WAN interface, you need to open the firewall for this interface. You can also specify a translation in the listening port. See _WANConnectionDevice_?_Service entries.

Dependency: The SSH server is based on the well known inetd linux daemon and the associated sshd program that takes it's input/output through stdin/stdout.

You must add this feature in the firmware with make menuconfig:

[*] Customize BusyBox Settings Networking Utilities ---

[*] inetd

[*] Customize User Settings Network Applications ---

[*] sshd

13.3.1 Enable

When set, enables the embedded SSH server.

13.4 TftpServer

A TFTP (Trivial FTP) service for the iBox.

The TFTP server listens for incoming calls on port 69.

Dependency: The TFTP server is based on the well known inetd linux daemon and the associated tftpd program that takes it's input/output through stdin/stdout.

You must add this feature in the firmware with make menuconfig:

[*] Customize BusyBox Settings Networking Utilities ---

[*] inetd

[*] Customize User Settings Network Applications ---

[*] tftpd

Note: The TFTP server is rarely used in end-user environments, but most probably for debug purpose.

13.4.1 Enable

When set, enables the embedded TFTP server.

13.4.2 RootDir

The root directory where files are being received / transmitted.

13.5 MDNSResponder

Multicast DNS responder (Apple Rendezvous protocol) settings.

This server advertise some of the box services through the Rendezvous protocol from Apple. Currently the services advertised are the device web configurator and the NAS server.

Dependency: The MDNS responder is a standalone daemon you need to include in the firmware with make menuconfig.

[*] Customize User Settings BeWAN tools ---

[*] Rendezvous

13.5.1 Enable

When set, enable the embedded Multicast DNS responder (Apple Rendezvous protocol).

13.6 SSDPProxy

The role of the SSDP Proxy is make appear distant UPnP MediaServers as local ones for the SSDP service discovery and notification.

Rest of the UPnP protocol message exchanges are carried out directly between UPnP ControlPoint and UPnP MediaServer.

13.6.1 Enable

When set, enables the SSDP proxy service.

13.6.2 UUID

An universal unique identifier (UUID) that should be identical to the one the distant MediaServer sends in its network device description ({{{description.xml}}}).

13.6.3 Host

Enables or disables the service.

Remote MediaServer's internet address.

13.6.4 Port

The port on which SSDPProxy will listen and answer to queries.

13.6.5 Iface

Network interface to listen on (ie: eth0, lan1, etc.).

13.6.6 Interval

Interval (in seconds) between SSDP presence notifications.

13.6.7 AuthEnable

When set, enables user authentication for the remote MediaServer access.

13.6.8 AuthUser

Password for the authentication.

13.6.9 AuthPass

Username for the authentication.

13.6.10 AuthHost

Remote hostname for the authentication server.

13.6.11 AuthPort

Remote port for the authentication server.

13.7 Rsync

A simple local to remote storage synchronization service for the CPE.

13.7.1 Enable

Enables or disables the Rsync service.

13.7.2 Sync

A synchronizable object.

- Enable

Enables or disables the current synchronizable object.

- Host

Remote host for directory sync.

- Port

Remote port for directory sync.

- Username

Username for remote synchronizable directory.

- Password

Password for remote synchronizable directory.

- LocalDir

Local directory to synchronize.

- RemoteDir

Remote directory where local data will be replicated.

- CustomParams

Rsync-specific parameters.

Note: See "rsync --help" for more details.

- Schedule

Synchronization scheduling (in crontab-like format).

13.8 UPnP

A service providing the Universal Plug and Play Internet Gateway Device in the box (UPnP IGD).

The UPnP IGD is used by some PC network applications such as MSN. The main purpose is to allow these applications to work behind a NAT router. Through the UPnP IGD protocol, they are able to know the public IP address of the router, to open incoming ports on the firewall and redirect the stream to their private IP address. The daemon upnpd is conforming to the UPnP specifications version 1.0.

Dependency: upnpd is a standalone daemon you need to include in the firmware with make menuconfig.

{{{[*] Customize User Settings BeWAN tools ---

[*] UPnP support

[*] UPnP Internet Gateway}}}

13.8.1 Enable

When set, enables the UPnP Internet Gateway Device server.

13.9 UPnPAVServer

UPnP Audio/Video MediaServer configuration settings.

UPnP Audio/Video MediaServer configuration settings.

Note: If enable and no Dir defined below, it will share {{{/var/media}}} filled by _Services_MediaFileSystem.

13.9.1 Enable

When set, enables the UPnP Audio/Video MediaServer.

13.9.2 Dir

A directory that could be shared with the UPnP MediaServer.

- Enable

When set, share the current directory in the UPnP MediaServer.

- Name

Visible name of the current directory from the remote side.

13.9.3 ShareName

13.9.4 InterfaceList

Make the UPnPAV server listen on given network interfaces. (lan only)

13.10 MiniUPnPd

A service providing the Universal Plug and Play Internet Gateway Device in the box (UPnP IGD), or a basic Device in the camera (UPnP Basic).

The UPnP IGD is used by some PC network applications such as MSN. The main purpose is to allow these applications to work behind a NAT router. Through the UPnP IGD protocol, they are able to know the public IP address of the router, to open incoming ports on the firewall and redirect the stream to their private IP address. The daemon upnpd is conforming to the UPnP specifications version 1.0. The UPnP Basic is used to broadcast a presence on the network

Dependency: MiniUPnPd is a standalone daemon you need to include in the firmware with make menuconfig.

{{{[*] Customize User Settings BeWAN tools ---

[*] UPnP support

[*] miniUPnP IGD server}}}

13.10.1 Enable

When set, enables the MiniUPnPd server.

13.10.2 Debug

13.10.3 EnableUPnP

When set, enables the UPNP function of the MiniUPnPd server.

13.10.4 EnableNATPMP

When set, enables NATPMP function of the MiniUPnPd server.

13.10.5 FriendlyName

13.10.6 ManufacturerName

13.10.7 ManufacturerURL

13.10.8 ModelName

13.10.9 ModelURL

13.10.10 ListenInterfaces

13.10.11 NotifyInterval

13.10.12 SecureMode

When enabled, UPnP client are allowed to add mappings only to their IP

13.10.13 EnableiCamDetection

13.10.14 UUID

13.10.15 PortMapping

- ExternalPort
- Protocol
- InternalPort
- InternalClient
- Description

13.10.16 DetectediCam

Array of detected iCam on the network

- Ip

IP of the detected iCam

- Hostname

Hostname of the detected iCam

- ExternalPort

External port opened for the detected iCam

13.11 MediaFileSystem

A userspace fuse-based filesystem retrieving metadata from media files (mp3, photos, etc.) in a source directory and providing a view through metadata-hierachized directories.

13.11.1 Enable

When set, enable the MediaFileSystem daemon.

13.11.2 MountPoint

Mountpoint for the metadata-hierachized view of files.

13.11.3 MemoryLimit

Maximum amount of memory (in kilobytes) that will be used to store index and metadata.

13.12 DynDNS

A dynamic DNS client utility on the box.

Dynamic DNS is an internet service that provides a host.domain name to devices connected to the network. The public IP address is recorded to the DNS server of the corresponding service. This is done by a registration refresh to the DNS server each time the box gets a new address from the network upon PPP or DHCP establishment process.

Dependency: The services dyndns, easydns, ezip are managed through the user-space utility ez-ipupdate.

The service no-ip is managed through the utility ddnsu.

You need to include these programs in the firmware with make menuconfig:

{{{[*] Customize User Settings BeWAN tools ---

&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;[*] ez-ipupdate

&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;[*] ddnsu}}}

13.12.1 Enable

When set, enables the dynamic DNS client utility.

13.12.2 Server

Can take the following values: dyndns, easydns, no-ip, ezip.

13.12.3 ServerName

can be left empty, or may need to be specified for private providers.

13.12.4 Username

The user name declared upon subscription to the service.

13.12.5 Password

The password declared upon subscription to the service.

13.12.6 Host

The Fully Qualified Domain Name (FQDN) of the box as declared upon subscription to the service.

13.12.7 Mx

Specify The MX record for your host if you have a mail server and want mail redirection (generally not needed).

13.12.8 Cache

Left blank. This parameter is updated automatically each time you get a new IP address. It 's purpose it to avoid sending unneeded requests to your dynamic DNS provider when your public IP address remains the same.

13.12.9 Status

13.13SyslogRemote

Redirection of the local syslog messages to a remote terminal.

You can use any well known syslog utility running on a Windows or Linux host to read the syslog messages. The network packets are by default UDP datagrams to port 514.

Dependency: The daemon syslogd is part of the BusyBox. The firmware always launches this daemon during boot so it is mandatory to include it in the BusyBox compilation options with make menuconfig. The utility logread is also needed to retrieve the syslog messages locally.

[*] Customize BusyBox? Settings System Logging Utilities ---

[*] syslogd

[*] Rotate message files

[*] Remote Log support

[*] Circular Buffer support (64) Circular buffer size in Kbytes (minimum 4KB)

[*] logread

[*] logread double buffering

[*] klogd

[*] logger

13.13.1 Enable

When set, enables the redirection of syslog messages to a remote terminal.

13.13.2 Host

The IP address of the terminal running the syslog utility.

13.13.3 Port

The UDP port on which the syslog utility is listening.

13.14 Upgd

13.14.1 Enable

13.14.2 Port

13.14.3 Upgrade

13.15 Ioctld

Obsolete

13.15.1 Enable

Unused

13.16 TR069

A TR-069 remote management stack.

The TR-069 remote management module allows a remote server to configure the box, get status information from the box and schedule firmware upgrades.

Dependency: You need to include these programs in the firmware with make menuconfig:

[*] Customize User Settings BeWAN tools ---

[*] TR069-2

[*] Install Curl CA Bundle (the firmware will include the CA root certificates)

[*] Disable MD5 sum in cli scripts (private configuration files uploaded by the ACS are in the format of CLI scripts)

[ ] Disable DSL configuration (set if the box is not a DSL modem)

[ ] Builtin ACS emulation (for debug) (set to compile the tiny ACS emulator, see parameter ACSEmul)).

13.16.1 Enable

When set, enables the TR-069 remote management stack.

13.16.2 Debug

Enables debug messages to the console output (don't use it if you have no serial console).

13.16.3 Interface

Leave empty if the TR-069 protocol operates on the default route (Internet connection). Specify the WAN interface index if the TR-069 protocol operates on a private secondary WAN network interface.

13.16.4 ACSEmul

Enables a built-in tiny ACS emulator for debug purpose. In that case, specify {{{http://localhost:1902/tr069.cgi}}} in the _Services_TR069_ACSUrl parameter.

13.16.5 SrvPort

Specify the TCP port on which the TR-069 module listens for Connection Requests from the ACS (default is 1901).

13.16.6 SrvLogin

Specify the login name for HTTP incoming Connection Requests from ACS (This parameter is provisioned by the ACS).

13.16.7 SrvPassword

Specify the password for HTTP incoming Connection Requests from ACS (This parameter is provisioned by the ACS).

13.16.8 ACSUrl

Specify the full URI of the ACS (remote management server). This parameter needs to be set-up on the factory profile of the box to be able to bootstrap the provisioning process.

13.16.9 ACSLogin

Specify the login name associated with the URL of the ACS. This parameter needs to be set-up on the factory profile of the box to be able to bootstrap the provisioning process.

13.16.10 ACSPassword

Specify the password associated with the URL of the ACS. This parameter needs to be set-up on the factory profile of the box to be able to bootstrap the provisioning process.

13.16.11 VerifyCert

Set to 0 to disable HTTPS verification (for debugging only).

Set to 1 verify the certificate.

Set to 2 verify the certificate and the hostname of the peer.

13.16.12 ACSCertPem

You can specify here the certificate of the ACS (if HTTPS is used). You enter the certificate as a string in a .pem format between quotes. Or you specify the certificate in the factory profile.

13.16.13 DSCPMark

You can specify here the DSCP mark value.

13.16.14 RebootNoTraffic

When set to 1, the box will wait until there is no traffic on the WAN side when a reboot is needed (on firmware upgrade). Use this with caution because the reboot may be postponed indefinitely.

13.16.15 TrafficThreshold

Set the threshold for the RebootNoTraffic. If during 10 seconds, the number of receive packets on all wan is less than this value, we can reboot the box.

13.16.16 SessionTimeout

When a session to the ACS is established but the ACS is dead (no data received), the TR-069 module will close the TCP socket after this timer expires.

13.16.17 ChunkedEncoding

When set, the TR-069 client will try to use the TCP chunked encoding mode when sending the answers to requests.

Sometimes, a huge amount of information is transfered when requests use a wild card. TCP chunked Encoding is necessary to save memory during the response processing.

13.16.18 InformEnable

Enables periodic Informs (see TR-069 specifications).

13.16.19 InformPeriod

Specify Inform period (delay between periodic TR-069 sessions).

13.16.20 InformTime

date/time (0000-00-00T00:00:00) - When specified, the periodic Informs will be scheduled at this date/time plus multiples of the Inform period.

13.16.21 UpgdManaged

This flag indicates if the firmware upgrades are managed by the TR-069 protocol. The local configuration web pages should not allow the user to do an upgrade.

13.16.22 BootStrap

This flag is used internally by the TR-069 protocol. this flag is set in the factory profile by default an automatically reset when a successful session has been established to the ACS. This flag may be tested by the ACS to know if the device has been provisioned.

13.16.23 FirstUsedDate

date/time - This parameter is automatically set to the current date/time when the first successful connection to the ACS has been done.

13.16.24 RebootKey

Used internally by the TR-069 protocol.

13.16.25 PersistentData

Used internally by the TR-069 protocol.

13.16.26 UpgradeComplete

Used internally by the TR-069 protocol. the TR-069 module writes information in this parameter upon successful firmware upgrade so that the next session after reboot will indicate an Upgrade Complete Event to the ACS.

13.16.27 UpgradeInProgress

Used internally by the TR-069 protocol. the TR-069 module writes information in this parameter upon successful firmware upgrade request is receive. If there is a problem during the download (the box is restarted), at the next session after reboot, the download will restart.

13.16.28 SessionStatus

Indicate the status of the TR069 session.

13.17IgmpProxy

A Layer 3 IGMP proxy for the CPE.

The IGMP proxy service is a daemon that listens to IGMP membership reports/leaves coming from the LAN networks (downstream interfaces) and forwards them to a WAN interface (upstream interface).

It programs the multicast routing tables of the linux kernel to route the multicast packets coming from the upstream interface to the corresponding LAN networks.

13.17.1 ENABLE

When set, enables the embedded Layer 3 IGMP proxy.

13.17.2 LOGLEVEL

Set the level of the debugging trace messages recorded in the syslog (upper is more verbose).

13.17.3 QUICKLEAVE

When set, the proxy service will immediately forward IGMP leaves to the upstream interface. This supposes that there is always only one client that is requesting the multicast stream.

13.17.4 HOSTTRACKING

When set, the proxy service will immediately forward IGMP leaves to the upstream interface when no more host is in the multicast stream. If you activate this one, you need to disable QuickLeave.

13.17.5 UPSTREAMINTERFACE

Gives the index of the upstream WAN interface.

If left empty, the daemon will only send IGMP queries to the downstream interfaces without doing any routing. This feature can be used to trigger aging in the IGMP snooping mechanism implemented in the box (see _Layer2Bridging_IGMPSnooping).

13.17.6 DOWNSTREAMINTERFACES

Optional, gives a list of the indexes of downstream LAN networks. If left empty all LAN networks are processed.

13.17.7 ALTERNATENETWORK

Alternate subnet address for incoming multicast packets.

By default the IGMP proxy service discards incoming multicast packets with a source address that is not in the subnet of the upstream network interface. You need to specify here the subnet of the source of the multicast packets (streaming server IP address).

Note: To disable this constraint, specify 0.0.0.0 in the parameters _Services_IgmpProxy_AlternateNetwork and _Services_IgmpProxy_AlternateMask.

13.17.8 ALTERNATEMASK

Associated with the _Services_IgmpProxy_AlternateMask parameter.

13.18 DEVICEREMOTEMANAGEMENT

13.18.1 TR111ENABLE

13.18.2 WT111ENABLE

13.18.3 DEVICE

- MACAddress
- IPAddress
- Type

- ManufacturerOUI
- SerialNumber
- ProductClass
- Active
- RetainDeviceEntry
- ConnectionRequestPassThroughEnable
- DeviceConnectionRequestURL
- ConnectionRequestURL

13.19 AntiSpam

An anti-spam mail filtering service for CPE.

Note: Obsolete

13.19.1 Enable

When set, enables the antispam service.

13.19.2 Port

Obsolete

13.19.3 PortRedirect

Obsolete

13.19.4 MaximumMailSize

Obsolete

13.19.5 MaxSessions

Obsolete

13.19.6 TagSpam

Obsolete

13.19.7 Mail

Obsolete

13.19.8 CheckUpdateMinutes

Obsolete

13.19.9 URLUpdate

An URL where the CPE will regulary check for software updates.

13.20 Cron

Cron is a time-based scheduling service.

Cron is a system service driven by a crontab, a configuration file that specifies shell commands (tasks) to run periodically on a given schedule.

13.20.1 Enable

When set, enable the cron service.

13.20.2 Task

A periodically scheduled task.

- Enable

When set, enable the current task.

- Label

Short machine-readable label associated to the current task.

- Minute

Minute-related part of the task schedule.

- Hour

Hour-related part of the task schedule.

- DayOfMonth

DayOfMonth-related part of the task schedule.

- Month

Month-related part of the task schedule.

- DayOfWeek

DayOfWeek-related part of the task schedule.

- Command

The task command line that will be run periodically.

13.21 At

At is a time-based scheduling service.

At is a system service driven by a configuration file that specifies shell commands (tasks) to run at given time.

13.21.1 Enable

When set, enable the atd daemon.

13.21.2 Task

A scheduled task.

- Enable

When set, enable the current task.

- Minute

Minute-related part of the task schedule.

- Hour

Hour-related part of the task schedule.

- Day

Day part of the task schedule.

- Month

Month part of the task schedule.

- Year

Year part of the task schedule.

- Command

The task command line that will be run at the given time.

13.22 SFR

Private Services

13.22.1 AutoDSLAM

Private parameter.

This parameter activates a mechanism which detects automatically the type of DSLAM on which the box is cross-connected. This function works only on the Neuf Cegetel network infrastructure. The algorithm sends DHCP requests on ATM interfaces 1 and 2. It recognizes an Alcatel DSLAM if there is a response on ATM2 and a Huawei DSLAM if there is a response on ATM1. It then reprograms the WAN interfaces according to these results.

13.23 FtpProvisioning

This enables the FTP remote management system in the box.

The FTP remote management module allows the remote configuration the box and scheduled firmware upgrades.

13.23.1 Enable

When set, enables the remote FTP/HTTP provisioning.

13.23.2 FtpInformationServer

The hostname of the remote information server.

13.23.3 InformationServerProtocol

The used protocol, ftp or http available.

13.23.4 InformationLogin

The username needed to access the remote information server.

13.23.5 InformationPassword

The password needed to access the remote information server.

13.23.6 InformationFilename

The path to the information file on the remote information server.

13.23.7 FtpConfigurationServer

The hostname of the remote configuration server.

13.23.8 ConfigurationServerProtocol

The used protocol, ftp or http available.

13.23.9 ConfigurationLogin

The username needed to access the remote configuration server.

13.23.10 ConfigurationPassword

The password needed to access the remote configuration server.

13.23.11 ConfigurationFilename

The path to the configuration file on the remote configuration server.

13.23.12 FirmwareFilename

The path to the firmware file on the remote firmware server.

13.23.13 FtpFirmwareServer

The hostname of the remote firmware server.

13.23.14 FirmwareServerProtocol

The used protocol, ftp or http available.

13.23.15 FirmwareLogin

The username needed to access the remote firmware server.

13.23.16 FirmwarePassword

The password needed to access the remote firmware server.

13.23.17 RebootOnIdle

When set, the box will wait until there is no traffic on the WAN side when a reboot is needed (on firmware upgrade).

Note: Use this with caution because the reboot may be postponed indefinitely.

13.23.18 Schedule

A crontab-like format scheduling.

13.23.19 UpdateStatus

Display generic update status (Error|Updatable|Downloading|UpToDate).

13.23.20 UpdateMessage

Display detailed status message related to _Services_FtpProvisioning_UpdateStatus .

13.23.21 DelayMax

13.24 SupervisionServer

The supervision script (by default, {{{/etc/eom.d/supervision}}}) is launched when an ip-up occurs to inform ISP.

Dependency: The script {{{/etc/eom.d/supervision}}} must be present in box.

13.24.1 Enable

If set (and if supervision script is present), script will launched at ip-up.

13.24.2 Url

The URL to post info.

13.24.3 Passphrase

Can be use for authentificate CPE to ISP.

13.24.4 Login

The username needed to access the remote supervision server

13.24.5 PASSWORD

The password needed to access the remote supervision server

13.25 DNSFORWARDER

Enables the DNS proxy of the box.

The DNS forwarder/proxy is a daemon that listens to DNS requests on port 53. The Box acts as a DNS server for all the PC connected to the LAN interfaces. It forwards the requests to the external DNS servers retrieved by the WAN interfaces. The WAN interfaces retrieve their DNS servers during PPP or DHCP negotiation. The DNS proxy contains a cache of DNS entries and does not resubmit requests already done. The file {{{/etc/config/resolv.conf}}} contains the IP addresses of the external DNS servers retrieved by the WAN interfaces. The WAN interface of index X updates this file when it comes up if the parameter _WANConnectionDevice_?_DNSEnable is set to 1.

13.25.1 ENABLE

Enables the DNS forwarder of the CPE

13.25.2 PORT

Defines the port on which the DNS forwarder will listen to queries (default is 53)

13.25.3 LOGQUERIES

Records a trace of the DNS queries in the syslog.

13.25.4 DNSREDIRECT

Enables DNS redirection. When activated, the DNS forwarder returns the IP address of the box in the answer of the queries when the file {{{/etc/config/resolv.conf}}} is empty (no WAN interface is up). In that case the box will receive all the HTTP requests from the clients and is able to display an error or diagnostic page.

13.25.5 REMOVEDNSREDIRECTFROM

IP address - Disable DNS redirection on queries whose source IP address is specified by this parameter.

13.25.6 DOMAINALTERNATEDNS

Specify DNS IP address for a specific domain name.

- Domain

Domain name that will be resolv with a specific DNS server.

- DNS

IP of the DNS server use to contact the specific Domain name.

13.26 ADDDNSFORWARDER

Object defining a list of additional DNS forwarders in the CPE

The main DNS forwarder is defined in _Services_DnsForwarder (see the description of this object). An additional DNS forwarder listens on a different port than 53. It works with a different resolv.conf file. It gathers DNS servers from the WAN interface where _WANConnectionDevice_?_AltDNSForwarder points to the index of this object.

Note: We need to define several DNS forwarders in the CPE when we want that different types of applications or different types of local hosts are routed to different WAN interfaces and query different DNS servers.

13.26.1 Enable

Same description as _Services_DnsForwarder_Enable

13.26.2 Port

Defines the port on which the additional DNS forwarder will listen to queries

Must not be 53. Queries from specific local hosts or local applications can be redirected to this port by defining a rule in _Firewall_Rules containing the target _Firewall_Rules_?_Redirect

13.26.3 LogQueries

Same description as _Services_DnsForwarder_LogQueries

13.26.4 DnsRedirect

Same description as _Services_DnsForwarder_DnsRedirect

13.26.5 RemoveDnsRedirectFrom

Same description as _Services_DnsForwarder_RemoveDnsRedirectFrom

13.27 SNMP

Simple Network Management Protocol is a network monitoring and control protocol.

The SNMP software called an agent runs on each managed system (board) and reports information via SNMP to the managing systems.

Dependency: You need to include these programs in the firmware with make menuconfig:

[*] Customize User Settings BeWAN tools ---

[*] SNMP (agent)

13.27.1 Enable

Activate the SNMP daemon (agent) on the board.

13.27.2 User

- UserName

The name of the user (this is the security name).

- Community

The community name used to connect the SNMP manager to the SNMP server on the box.

- AccessType

The type of access.

You can choose "read" (readonly access) or "write" (readwrite access)

- IPsManager

The IPsManager is a comma separed list of ip address.

This IP is used by the snmp agent to check the request of a manager.

- SNMPVersion

The snmp version allowed for this user.

You can choose between "v1" (snmp version 1), "v2c" (snmpversion V2) or "all" (both snmp version).

13.28 STBMAPPER

This object contains the parameters associated to the service STB mapper.

The STB mapper is a daemon that detects the SetTopBox when connected to a port of the ethernet switch and dynamically remaps the port to a specific VLAN.

The DHCP request packets from the STB must be queued to user space by a firewall rule using the target '''Queue'''. See _Firewall_Rules object for a description of who to achieve this.

Dependency: You need to include the program STB mapper in the firmware with make menuconfig:

Customize User Settings

Core Applications

[*] SetTopBox detector and port mapper

13.28.1 ENABLE

Enables the STB mapper service / daemon.

13.28.2 INTERFACE

Index of the _LANEthernetInterface_? object on which the service operates.

Note: The hardware switch is connected to this network interfcae.

13.28.3 VLANNUMBER

Index of the _LANEthernetInterface_?_VLANInterface_? object specifying the VLAN to which the port will be mapped.

The Ethernet switch port on which the STB is detected will be dynamically mapped to this VLAN interface. This VLAN interface may belong to a bridge including a private WAN interface for IPTV.

13.28.4 TRUNKNUMBER

Index of the _LANEthernetInterface_?_VLANInterface_? object specifying the VLAN to which the port will be trunked.

The Ethernet switch port on which the STB is detected will be dynamically mapped as a tagged port belonging to this VLAN interface.

13.28.5 MAPPING

Status information: comma-separated list of switch ports indexes.

Indexes of _LANEthernetInterface_?_Port_? objects describing the switch ports currently mapped to the VLAN specified by _Services_StbMapper_VlanNumber.

13.29 SAMBACLIENT

This object allows the configuration of the samba client.

13.29.1 ENABLE

Enables or disables the samba client service.

13.29.2 MOUNTPOINT

Path of the mount point of samba client service.

13.29.3 GLOBAL

This item allows a global configuration of the samba client.

- Timeout

Connection timeout in seconds.

- Interval

Interval for updating new shares in minutes.

- Username

Global default username.

- Password

Global default password.

- ShowHiddenShares

If true, list hidden shares.

13.29.4 DetectedNetwork

Detected Networks seen by the Samba client.

13.29.5 Workgroup

A workgroup in the samba networking.

- Name

Name of the workgroup.

- Ignore

Ignore all the servers in the workgroup.

13.29.6 Server_List

List of servers in the samba network.

13.29.7 Server

Declared server in a Samba network.

- Name

Networking name of this server.

- Share

A share repository on this server.

  - Name

Name of the share on this server.

  - Username

Username needed to access this share on this server.

  - Password

Password needed to access this share on this server.

- Ignore

Ignore the server.

- ShowHiddenShares

List hidden shares on this server.

- Username

Username needed to access this server.

- Password

Password needed to access this server.

13.30 MIRROR

This service catches the traffic sent and received on an ATM interface and mirrors it on an Ethernet interface.

You can mirror the ATM traffic on a specific port of the Ethernet switch. Use the port isolation with VLAN mechanism.

13.30.1 ENABLE

Set to 1 to activate the Mirroring service.

13.30.2 ATMINTERFACE

Index of the _ATMEthernetInterface_? object to mirror.

13.30.3 ETHINTERFACE

Index of the _LANEthernetInterface_? object that will catch mirrored traffic.

13.30.4 VLANNUMBER

Leave empty or specify the VLAN index of a _LANEthernetInterface_?_VLANInterface_? object that will catch the traffic.

13.30.5 FRAMEOFFSET

Leave empty or specify an offset in the packets to mirror.

This offset allow to skip the ATM header such as the LLC/SNAP header.

13.31 CLI

used to set CLI in debug mode

13.31.1 TRACE

if set, each CLI line will be send in syslog

13.32 STB

13.32.1 OUI

List of OUI to add in Preassigned table when connected to the box

14 TIME

This object gathers time management configuration parameters.

The date &amp; time of the box must be kept up-to-date. Important services such as SSL and Samba need accurate values for date &amp; time.

14.1 NTPENABLE

Enables the NTP client in the box. The NTP client retrieves the date &amp; time from an external network server.

14.2 NTPSERVERS

List of external NTP servers to query.

14.3 LOCALTIMEZONE

Specification of how to compute local time from UTC time (NTP servers return UTC time). The format of this specification is conforming to the manual page of tzset.

14.4 LOCALTIMEZONEAREA

Human readable name of the local time zone.

15 QoS

15.1 Enable

15.2 Queues

15.3 Queue

15.3.1 PrioMap

15.4 VLAN

15.4.1 PrioMap

15.5 Shaping

15.5.1 Enable

15.5.2 Interfaces_List

15.5.3 Interfaces

- Enable
- IfType
- Index
- MaxBP

16 Firewall

This object gathers tables of global firewall rules.

A good knowledge of Linux kernel iptables is recommended to perfectly understand the behavior of the packets going through the tables.

Note: Rules are specified to filter or modify packets going through the CPE.

16.1 Enable

When set to 1, all the rules specified in the table _Firewall_Rules_? are active, otherwise they are not built.

16.2 UserEnable

When set to 1, the rules specified in the table _Firewall_Rules_? with the parameter _Firewall_Rules_?_User set to 1 are active, otherwise they are not built.

Note: If the global Firewall parameter _Firewall_Enable is not set, the rules with parameter _Firewall_Rules_?_User are not built.

16.3 DefaultPolicy

This is the default policy of the Forward Filter table.

When set to Accept, if no Rule exists in the Forward table, the packets are accepted.

When set to Drop, packets are dropped.

Note: Use a default policy of Drop for a very secure firewall that accepts only a few rules.

16.4 Rules_List

Comma-separated list of indexes of objects _Firewall_Rules_? table.

16.5 Rules

Table of packet filter or mangling rules.

16.5.1 Enable

If set to 1, activates this rule.

16.5.2 User

This parameter indicates if the rule is a user or system rule.

User rules are managed and displayed by the web user interface. System rules are hidden and must not be accessed by the web user interface. The parameter _Firewall_UserEnable allows to enable/disable user firewall rules without affecting system rules.

16.5.3 Description

Human readable description of the rule.

16.5.4 Input

Leave blank or specify a comma-separated list of indexes of WAN or LAN interfaces.

This parameter associated to _Firewall_Rules_?_InputExt and _Firewall_Rules_?_InputNot defines a match in the incoming network interface of the packet. If left blank, any network interface will match the rule.

Note: This parameter has no meaning if a value of Output is specified in the parameter _Firewall_Rules_?_Chain.

16.5.5 InputExt

Specify the type of the input interface (1=WAN interface, 0=LAN interface).

If set to 1, the input network interfaces specified in _Firewall_Rules_?_Input will be _WANConnectionDevice_? interfaces. If left blank or set to 0, the input network interfaces specified in _Firewall_Rules_?_Input will be _LANDevice_? interfaces.

16.5.6 InputNot

If set to 1, the match specified in the parameters _Firewall_Rules_?_Input and _Firewall_Rules_?_InputExt is inverted.

16.5.7 Output

Leave blank or specify a comma-separated list of indexes of WAN or LAN interfaces.

This parameter associated to _Firewall_Rules_?_OutputExt and _Firewall_Rules_?_OutputNot defines a match in the outgoing network interface of the packet. If left blank, any network interface will match the rule.

Note: This parameter has no meaning if a value of Input is specified in the parameter _Firewall_Rules_?_Chain.

16.5.8 OutputExt

Specify the type of the output interface (1=WAN interface, 0=LAN interface).

If set to 1, the output network interfaces specified in _Firewall_Rules_?_Output will be _WANConnectionDevice_? interfaces. If left blank or set to 0, the output network interfaces specified in _Firewall_Rules_?_Output will be _LANDevice_? interfaces.

16.5.9 OutputNot

If set to 1, the match specified in the parameters _Firewall_Rules_?_Output and _Firewall_Rules_?_OutputExt is inverted.

16.5.10 SrcIPStart

Leave blank or specify the first IP address of a source IP address range.

Packets with a source IP address in the range will match the rule if _Firewall_Rules_?_SrcIPNot is set to 0. Packets with a source IP address outside the range will match the rule if _Firewall_Rules_?_SrcIPNot is set to 1. If no range is specified, any source IP address will match the rule.

16.5.11 SrcIPEnd

Leave blank or specify the last IP address of a source IP address range.

Packets with a source IP address in the range will match the rule if _Firewall_Rules_?_SrcIPNot is set to 0. Packets with a source IP address outside the range will match the rule if _Firewall_Rules_?_SrcIPNot is set to 1. If no range is specified, any source IP address will match the rule.

Note: If the first and last IP addresses are the same, this parameter is left blank.

16.5.12 SrcIPNot

If set to 1, the source IP address match will be inverted.

16.5.13 SrcPorts

Leave blank or specify a comma-separated list of source port ranges (for UDP or TCP packets).

Packets with a source port in one of the ranges listed will match the rule if _Firewall_Rules_?_SrcPortsNot is set to 0. Packets with a source port outside all the ranges in the list will match the rule if _Firewall_Rules_?_SrcPortsNot is set to 1. If nothing is specified any source port will match the rule.

Note: The parameter _Firewall_Rules_?_Protos must include the protocol TCP or UDP. The port range format is p1:p2 or p1 if p2=p1.

16.5.14 SrcPortsNot

If set to 1, the source port match will be inverted.

16.5.15 DstIPStart

Leave blank or specify the first IP address of a destination IP address range.

Packets with a destination IP address in the range will match the rule if _Firewall_Rules_?_DstIPNot is set to 0. Packets with a destination IP address outside the range will match the rule if _Firewall_Rules_?_DstIPNot is set to 1. If no range is specified, any destination IP address will match the rule.

16.5.16 DstIPEnd

Leave blank or specify the last IP address of a destination IP address range.

Packets with a destination IP address in the range will match the rule if _Firewall_Rules_?_DstIPNot is set to 0. Packets with a destination IP address outside the range will match the rule if _Firewall_Rules_?_DstIPNot is set to 1. If no range is specified, any destination IP address will match the rule.

Note: If the first and last IP addresses are the same, this parameter is left blank.

16.5.17 DstIPNot

If set to 1, the destination IP address match will be inverted.

16.5.18 DstPorts

Specify a comma-separated list of destination port ranges (for UDP or TCP packets).

Packets with a destination port in one of the ranges listed will match the rule if _Firewall_Rules_?_DstPortsNot is set to 0. Packets with a destination port outside all the ranges in the list will match the rule if _Firewall_Rules_?_DstPortsNot is set to 1. If nothing is specified any destination port will match the rule.

Note: The parameter _Firewall_Rules_?_Protos must include the protocol TCP or UDP. The port range format is p1:p2 or p1 if p2=p1.

16.5.19 DstPortsNot

If set to 1, the destination port match will be inverted.

16.5.20 Protos

Leave blank or specify a comma-separated list of IP protocols.

The packet will match the rule if the IP protocol field is in the list. If nothing is specified any protocol will match the rule.

Note: Format is all,udp,tcp,icmp,esp,ah,gre.

16.5.21 IcmpType

Leave blank or specify the type of ICMP packet.

This parameter can be set to specify a rule that matches ICMP packets of type Echo Request or Echo Reply. The parameter _Firewall_Rules_?_Protos should specify the protocol ICMP.

16.5.22 Mark

Leave blank or specify an integer compared with the mark value of the packet.

This parameter is designed to match packets previously marked by another rule generally from another filter table. The match is inverted if the parameter _Firewall_Rules_?_MarkNot is set to 1. If no Mark is specified, any value will match the rule.

16.5.23 MarkNot

If set to 1, the Mark match will be inverted.

16.5.24 IPPrec

Leave blank or specify an integer compared with the IP precedence field of the packet.

This parameter allow to specify a match in the IP precedence field of the packet (3 most significants bits of the TOS byte).

16.5.25 IPPrecNot

If set to 1, the IP precedence match will be inverted.

16.5.26 AddMatch

Allow to enter any additional known iptables match

Note: See iptables manpage for details

16.5.27 ClampMss

This rule will lower the MSS (Maximum Segment Size) during TCP session establishment to the specified value.

By default the MSS is automatically computed to fit the output network interface MTU.

16.5.28 SetDSCP

Leave blank or specified a new DSCP field for the packet.

The packet DSCP field will be modified with the new value specified in this parameter.

16.5.29 SetClass

Leave blank or modify the Linux priority of the packet.

The Linux priority is used by the queuing processing. All output network interfaces have several queues with a different scheduling priority and the packets are queued according to their Linux priority.

Note: A value of 15 specifies the greatest level of priority.

16.5.30 SetMark

Leave blank or specify an integer. The packet will be tagged with this value.

The tag (mark) can be used later to match the packet in a filter or routing rule.

16.5.31 Redirect

Leave blank or specify a range of ports for redirection.

This rule silently mangles the destination port of an UDP or TCP packet and restores the original port in the response. Works only for packets whose final destination is the CPE. This rule is used to redirect a service like DNS (port 53) to an alternate forwarder.

Note: The parameter _Firewall_Rules_?_Protos must include UDP or TCP.

16.5.32 CHAIN

Specifies the iptables chain where the rule is built.

The Input chain is for packets coming from one network interface and staying in the CPE.

The Output chain is for packets generated by the CPE and leaving the CPE by one network interface.

The Forward chain is for packets crossing the CPE, coming from one network interface and leaving the CPE by another network interface.

The Prerouting chain is for rules modifying a packet before crossing the routing tables (i.e. setting TOS or QoS class or redirecting the port).

The Postrouting chain is for rules modifying a packet after the routing process.

16.5.33 TARGET

Specify what to do with the packet when there is a match.

Drop will silently drops the packet.

Accept will accept the packet and leave the filter table.

Queue will queue the packet to user space for special processing.

RejectNet will drop the packet returning to the sender an ICMP error message 'no route to network'.

RejectHost will drop the packet returning to the sender an ICMP error message 'no route to host'.

RejectProto will drop the packet returning to the sender an ICMP error message 'port unreachable'.

Jump will call an automatically created subchain whose name is given in _Firewall_Rules_?_OtherTarget.

Other will jump to any known iptables target given in _Firewall_Rules_?_OtherTarget.

16.5.34 OTHERTARGET

Allow to enter any other known iptables target

Note: See iptables manpage for details

16.5.35 TABLE

Allow to force the netfilter table where the rule is inserted

Allowed values are Filter, Mangle, Nat or Auto

Note: See iptables manpage for details

16.5.36 SYMETRIC

When set to 1, two symetric rules will be built.

A second rule will automatically be added with source and destination IP address, port, network interface swapped.

16.6 LOGDROPPED

When set to 1, the packets dropped by one of the rules declared in _Firewall_Rules_? will be logged to the syslog buffer.

Note: There is a filter that prevents the syslog buffer to be overloaded by dropped packet events. If more than 8p/s are logged, other events are not recorded.

16.7 URLFILTER

Not used

17 LANEthernetInterface

This array of objects describes the physical Ethernet interfaces of the box.

There is one instance of _LANEthernetInterface_? per hardware MAC (Ethernet Medium Access Controller).

17.1 Enable

When set, enables the physical Ethernet interface.

17.2 IfName

Read-only - specifies the name, i.e. eth0, eth1... of the linux network interface associated to the _LANEthernetInterface_? object.

17.3 Description

Optional description of the physical Ethernet interface.

17.4 MACAddressOverride

When set, overrides the default MAC address with the one specified in _LANEthernetInterface_?_MACAddress.

17.5 MACAddress

Manually defined MAC address of the Ethernet interface if _LANEthernetInterface_?_MACAddressOverride is set to 1.

By default the MAC address of the physical interface is automatically assigned with the value stored in the flash during manufacturing process.

17.6 QosEnable

When set, Linux network output queues will be created according to the parameters configured in the object Qos.

17.7 Port_List

Physical ports associated to the Ethernet interface.

If no Ethernet switch is connected to the Ethernet interface, the value is 1. The value is 1,2,3,4 for a 4 port switch.

17.8 Port

Table of objects describing the physical Ethernet ports associated to the Ethernet interface.

If the board implements an Ethernet switch, more than one port is associated to the Ethernet interface.

17.8.1 PhyId

Read-only - Ethernet PHY Identifier of the port.

The ID must be set in the factory profile and is hardware dependent. This ID is necessary for the mii-tool command to program the mode &amp; speed and get the status of the Ethernet link.

Dependency: menuconfig:

Customize User Settings

Hardware Support

[*] MII programming - mii-tool

17.8.2 PortId

Read-only - This is a bit mask (with only one bit set to 1) indicating the position of the port.

This parameter is necessary if the hardware implements an Ethernet switch and if we want to isolate some of the ports of the switch.

17.8.3 MaxBitRate

You can fix the speed of the link to 10 mbps or 100 mbps or leave it automatically negotiated.

17.8.4 DuplexMode

You can fix the mode of the link to half duplex or full duplex or leave it automatically negotiated.

17.8.5 VLANInterface

Index of the VLAN interface the switch port belongs to.

If you want to isolate a port of the Ethernet switch, you must create VLAN interfaces on the _LANEthernetInterface_? object first and then assign each port of the Ethernet switch to one of these interfaces.

17.8.6 VLANTrunk

Comma-separated list of tagged VLANs the switch port will trunk.

If you want to create tagged VLANs and use a port of the switch to trunk these VLANs, you must create VLANs interfaces on the _LANEthernetInterface_? object first and then indicate the list of VLANs interfaces the switch port will trunk.

17.8.7 Description

Human readable description of the Ethernet port.

17.8.8 Status

This object gathers status information about the Ethernet link.

The object contains link status and a list of MAC addresses detected on the port.

- LinkState

Returns the link status.

- LinkMode

Returns the negotiated link mode (10/100 mbps, Half/Full duplex).

- ARPTable

List of MAC addresses detected on the port by the Ethernet switch.

17.8.9 Counters

Counters of sent or received data (in packets or bytes) on the switch port since the device creation.

- RxPackets

Counters of received packets on the switch port since the device creation.

- RxPacketsErrors

Counters of received in error packets on the switch port since the device creation.

- RxPacketsDiscards

Counters of received packets discard on the switch port since the device creation.

- TxPackets

Counters of sent packets on the switch port since the device creation.

- TxPacketsErrors

Counters of sent packets in error on the switch port since the device creation.

- TxPacketsDiscards

Counters of sent packets discard on the switch port since the device creation.

- RxBytes

Counters of received bytes on the switch port since the device creation.

- TxBytes

Counters of sent bytes on the switch port since the device creation.

17.9 SwitchVLANEnable

Set 1 to Enable the programming of VLANs in the Ethernet Switch.

Note: If no VLAN interfaces are created in the object _LANEthernetInterface_?, there is no need to activate this.

17.10 SwitchVLAN_List

Comma-separated list of _LANEthernetInterface_?_SwitchVLAN_? objects

17.11 SwitchVLAN

Array of parameters defining group of ports belonging to the same physical segment.

These objects allow to program the Ethernet switch for layer 2 VLAN.

Note: Layer 2 VLANs are not tagged VLANs. The groups are justs forwarding rules programmed in the switch to create a physical isolation between different ports of the switch.

17.11.1 Group

Ports indexes for the corresponding group.

Note: 1,2,4 means that the ports 1, 2 and 3 of the Ethernet switch are in the same physical segment but a PC connected to the port 3 will not receive packets from this segment.

17.12 VLANInterface

Array of objects specifying VLAN interfaces associated to the Ethernet interface.

Each VLAN interface is characterized by a VLAN ID and a priority field.

17.12.1 Enable

When set, enables current VLAN interface.

17.12.2 VID

VLAN ID in the tag of current VLAN.

17.12.3 PRI

Priority field in the tag of this VLAN.

17.12.4 SetQosField

If set, the VLAN network interface will assign a value to the priority field of the VLAN tag according to the TOS field in the IP packet.

17.12.5 Counters

Status counters associated to the network VLAN interface.

Counters of sent and received packets, sent and received bytes, and list of MAC addresses.

- RxPackets

Counters received packets on the virtual network interface since the device creation.

- RxPacketsErrors

Counters received packets in error on the virtual network interface since the device creation.

- RxPacketsDiscards

Counters received packets discard on the virtual network interface since the device creation.

- TxPackets

Counters of sent packets on the virtual network interface since the device creation.

- TxPacketsErrors

Counters of sent packets in error on the virtual network interface since the device creation.

- TxPacketsDiscards

Counters of sent packets discard on the virtual network interface since the device creation.

- RxBytes

Counters of received bytes on the virtual network interface since the device creation.

- TxBytes

Counters of sent bytes on the virtual network interface since the device creation.

- ARPTable

Comma-separated list of MAC addresses detected by the ARP protocol on this network interface.

17.13 SwitchIGMPEnable

When set, enables the IGMP snooping function on the ports of the Ethernet switch.

The IGMP snooping function listen to the IGMP packets coming from each of the switch ports. It allows the forwarding of mutlicast packets to a port only if an IGMP report for the same multicast address has been received from that port.

Note: Implemented for switch RTL8306SD

Not yet implemented for switch ADM6996

17.14 Counters

Counters of sent or received data (in packets or bytes) on the physical network interface since the device creation.

17.14.1 RxPackets

Counters of received packets on the physical network interface since the device creation.

17.14.2 RxPacketsErrors

Counters of received in error packets on the physical network interface since the device creation.

17.14.3 RxPacketsDiscards

Counters of received packets discard on the physical network interface since the device creation.

17.14.4 TxPackets

Counters of sent packets on the physical network interface since the device creation.

17.14.5 TXPACKETSERRORS

Counters of sent packets in error on the physical network interface since the device creation.

17.14.6 TXPACKETSDISCARDS

Counters of sent packets discard on the physical network interface since the device creation.

17.14.7 RXBYTES

Counters of received bytes on the physical network interface since the device creation.

17.14.8 TXBYTES

Counters of sent bytes on the physical network interface since the device creation.

17.14.9 ARPTABLE

Comma separated list of MAC addresses detected on the network interface by the ARP protocol.

18 LANUSBInterface

This object describes the USB slave controller network interface.

If the hardware supports an USB slave controller, _LANUSBInterface_Count is greater than 0.

A Linux USB gadget driver implements a network interface over this USB link. Depending on the driver provided by the chip manufacturer, the network interface implements different flavour of ethernet over USB link. The most common is Microsoft Remote NDIS.

18.1 Enable

Activates the network interface.

18.2 IfName

Linux name of the network interface (generally usb0, usb1...).

18.3 Description

Human readable description of the interface to facilitate configuration set-up.

18.4 MACAddressOverride

When set, the network interface will take the MAC address specified in _LANUSBInterface_?_MACAddress.

18.5 MACAddress

MAC address of the USB network interface when _LANUSBInterface_?_MACAddressOverride is set.

18.6 QosEnable

When set, Linux network output queues will be created according to the parameters configured in the object Qos.

18.7 Status

This object returns status information about the physical link.

18.7.1 LinkState

Returned values are Up, Down - gives the state of the link (Up if a client is connected).

18.7.2 LinkMode

Returned values are Low, High - 12mbps (USBv1.1) or 480mbps (USBv2.0).

18.7.3 ARPTable

comma separated list of MAC addresses - List of MAC addresses of equipments detected through this link (by protocol ARP).

18.8 Counters

Counters of sent or received data (in packets or bytes) on the physical network interface since the initialization of the driver.

18.8.1 RxPackets

Counters of received packets on the physical network interface since the initialization of the driver.

18.8.2 RxPacketsErrors

Counters of received packets in error on the physical network interface since the initialization of the driver.

18.8.3 RxPacketsDiscards

Counters of received packets discard on the physical network interface since the initialization of the driver.

18.8.4 TxPackets

Counters of sent packets on the physical network interface since the initialization of the driver.

18.8.5 TxPacketsErrors

Counters of sent packets in errors on the physical network interface since the initialization of the driver.

18.8.6 TxPacketsDiscards

Counters of sent packets discard on the physical network interface since the initialization of the driver.

18.8.7 RxBytes

Counters of received bytes on the physical network interface since the initialization of the driver.

18.8.8 TxBytes

Counters of sent bytes on the physical network interface since the initialization of the driver.

18.8.9 ARPTable

Comma separated list of MAC addresses detected on the network interface by the ARP protocol.

19 ATMETHERNETINTERFACE

Array of objects describing the ATM interfaces ("Asynchronous Transfer Mode").

The ATM interfaces are the network interfaces connected to the ADSL link. Each ATM interface is characterized by a VPI/VCI, a protocol encapsulation and Quality of Service parameters.

19.1 ENABLE

When set to 1, enables the ATM interface.

19.2 IFNAME

The name of the network interface.

19.3 DESCRIPTION

Human-readable optional description of this interface.

19.4 HWMACID

This parameter is used to modify the MAC address of the ATM network interface.

Add "(n*4)+2" to the first byte of the default MAC address and set the new MAC to this ATM network interface.

Note: Example: if _ATMEthernetInterface_?_HwMacId=1 and the default MAC of the device is 00:0C:C3:01:02:03 then the ATM network interface MAC address will be 06:0C:C3:01:02:03.

19.5 MACADDRESSOVERRIDE

When set to 1, overrides the MAC address of the ATM network interface with the value given in _ATMEthernetInterface_?_MACAddress.

19.6 MACADDRESS

MAC address of the ATM network interface if the parameter _ATMEthernetInterface_?_MACAddressOverride is set to 1.

19.7 QOSENABLE

When set to 1, Linux network output queues will be created according to the parameters configured in the object Qos.

19.8 ATMLINKCONFIG

Object gathering configuration parameters of the ATM link. VPI, VCI, protocol encapuslation and QoS.

19.8.1 ENABLE

Enable ATM Virtual Circuit.

19.8.2 SHARED

When set, allow sharing this ATM interface between multiple _WANConnectionDevice_? objects.

This parameter may be tested by web pages to disallow modifying ATM configuration when this configuration is shared by several WAN devices.

Note: An ATM interface can be shared by several WAN interfaces (_WANConnectionDevice_? objects) only if the Link Type is EoA.

19.8.3 LINKTYPE

Specifies the encapsulation inside the ATM Virtual Circuit.

"'EoA'" : will transmit all kind of Ethernet frames.

'''PPPoE''' : will filter all other frames than PPPoE frames.

'''IPoA''' and '''PPPoA''' : will remove the Ethernet header.

Note: In IPoA mode the ATM network driver answers locally to ARP requests and removes Ethernet headers.

In PPPoA mode the ATM network driver handles locally the PPPoE discovery stage and transmit PPP frames without Ethernet header. Mode Auto is unsupported.

19.8.4 VC

Set VPI/VCI of the ATM virtual Circuit.

19.8.5 ATMEncapsulation

Choose encapsulation between VCMUX and LLC.

Note: VC multiplexed and LLC/SNAP encapsulations are specified in the RFC 2684.

19.8.6 VCSearchList

Unused

19.8.7 ATMClass

ATM class of the Virtual Circuit defining the Quality of Service delivered by the channel.

'''UBR''' : Unspecified Bit Rate,

'''CBR''' : Constant Bit Rate,

'''VBR''' : Variable Bit Rate,

'''-rt''' suffix : real time.

19.8.8 ATMPeakCellRate

Peak Cell Rate must be specified in CBR (Constant Bite Rate) and VBR (Variable Bit Rate) classes.

Left empty if ATM class is UBR.

19.8.9 ATMMaximumBurstSize

Maximum Burst Size (MBS) in VBR class (Variable Bit Rate).

Left empty in classes other than VBR.

19.8.10 ATMSustainableCellRate

Sustainable Cell Rate must be specified in VBR (Variable Bit Rate) class.

Left empty in classes other than VBR.

19.8.11 Stats

ATM Related Statistics

- CRCErrors

The number of received AAL5 CPCS PDU received with CRC-32 errors on this AAL5 VCC

- OversizedSDUs

The number of AAL5 CPCS PDUs discarded because the AAL5 SDUs were too large.

- SARTimeouts

The number of partially re-assembled AAL5 CPCS PDUs which were discarded on timeout.

Partially re-assembled PDUs were not fully re-assembled within the required time period..

19.9 Counters

Counters of sent or received data (in packets or bytes) on the physical network interface since the initialization of the driver.

19.9.1 RxPackets

Counter of received packets on the physical network interface since the initialization of the driver.

19.9.2 RxPacketsErrors

Counter of received packets in errors on the physical network interface since the initialization of the driver.

19.9.3 RxPacketsDiscards

Counter of received packets discard on the physical network interface since the initialization of the driver.

19.9.4 TxPackets

Counter of sent packets on the physical network interface since the initialization of the driver.

19.9.5 TxPacketsErrors

Counter of sent packets in error on the physical network interface since the initialization of the driver.

19.9.6 TxPacketsDiscards

Counter of sent packets discard on the physical network interface since the initialization of the driver.

19.9.7 RxBytes

Counter of received bytes on the physical network interface since the initialization of the driver.

19.9.8 TxBytes

Counter of sent bytes on the physical network interface since the initialization of the driver.

20 MODEM3GINTERFACE

Configure the parameters to use a 3G dongle.

Dependency: For Huawei dongles:

{{{[*] Customize Kernel Settings Device Drivers ---

USB support ---

USB Serial Converter support ---

[M] USB Serial Converter support

[*] USB Generic Serial Driver

[M] USB AirPrime CDMA Wireless}}}

Driver For Option Icon 225 dongle:{{{

[*] Customize User Settings Hardware Support ---

[*] HSO driver

[*] usb_modeswitch}}}

20.1 ENABLE

When set, enables the modem 3G interface.

20.2 IFNAME

This parameters has to be filled but you can put any value.

For example : modem3g0. No network interface with the name modme3g0 will be created. The name of network interface depends on the vendor of the 3G modem.

20.3 DESCRIPTION

Optional description of the device.

20.4 MACADDRESSOVERRIDE

Note: Unused.

20.5 MACADDRESS

Note: Unused.

20.6 QOSENABLE

When set, enable the QoS on this interface.

20.7 PHONENUMBER

Destination phone number. For exemple *99*1# (See 3GPP Technical Specification).**

20.8 APN

Acces Point Network (See 3GPP Technical Specification).

20.9 CGDCONT

Note: Unused.

20.10 DEBUG

20.11 PINCODE

PIN code for the 3G SIM.

20.12 MODEPREF

Choose your connection type between GPRS only, GPRS prefered, 3G prefered or 3G only. If 3G only is set and no 3G network is available, there will be no connection.

20.13 USERNAME

Username of the 3G connection (See 3GPP Technical Specification).

20.14 PASSWORD

Password of the 3G connection (See 3GPP Technical Specification).

21 LANIPoBTDevice

Configure the service providing web browsing on a cell phone via bluetooth.

21.1 Enable

When set, enables the Dial-Up Networking Daemon Bluetooth-related service.

21.2 Ifname

Define the name of the network interface being used.

21.3 LocalIPAddress

Set the local interface IP addresses.

21.4 RemoteIPAddress

Set the remote interface IP addresses.

21.5 Channel

Select the RFCOMM Channel.

22 WLANConfig

This object contains parameters common to all WLAN interfaces.

22.1 WifiEnable

Enable or disable all WiFi interfaces.

This feature is only for Ralink drivers.

22.2 Country

Sets the ISO Country Code.

Used for being coherent with the wireless country laws restrictions. The ISO table can be found at this address : {{{http://www.nw.com/zone/iso-country-codes}}}.

22.3 Channel

Selects which channel will be used.

14 channels are available (1 to 14) but some of them cannot be set due to wireless country laws restrictions. The channel 0 is a specific option to let the WiFi driver use the less interferenced channel (It can be changed anytime even in WiFi usage).

22.4 ChannelRefreshPeriod

Select time (in seconds) between each less interfered channel searches.

This allow to refresh the channel when the traffic is the less important. If parameter set to 0, no refresh will be done.

22.5 Standard

Selects the WiFi 802.11 standard usage.

22.6 BeaconInterval

Sets the interval (in milliseconds) between each WiFi Beacons.

22.7 AssociationTime

For use with pairing either by ACL or WPS.

This defines the time during the Access Point listen for associations requests from stations (default is 120 seconds).

22.8 EasyPairing

Program for WiFi button interaction.

EasyPairing is a functionnality that allows user to interact with the WiFi button. Depending on hardware and options, it can allow ACL opening or/and WPS enabling.

22.9 DiversityEnable

Enable or disable antenna diversity.

Antenna diversity is a mechanism that allows driver to dynamically select the best Rx and the best Tx antennas.

22.10 RxAntenna

Select which antenna for reception.

Auto, the antenna is automatically chosen by driver. Ant1, the antenna 1 is chosen for reception. Ant2, the antenna 2 is chosen for reception.

22.11 TxAntenna

Select which antenna for transmission.

Auto, the antenna is automatically chosen by driver. Ant1, the antenna 1 is chosen for transmission. Ant2, the antenna 2 is chosen for transmission.

22.12 CurrentChannel

Status information giving to current selected channel.

22.13 PBCInterfacesStates

Allow listing the previous WLANInterfaces states for Push Button action.

22.14 WEPSupervisionPeriod

Select time (in minutes) for supervisionning the WEP SSID.

To prevent from WEP key hacking, this feature sets a time during the WEP SSID is supervisionned. If no connection and/or traffic has been logged during this time, the WEP SSID is automatically disabled. To disable the feature, set it to 0.

22.15 DebugLevel

Set debug level

4 levels are possible. 0 : Off, 1 : light debug, 2 : normal debug, 3 intensive debug. This feature is only for Ralink drivers.

22.16 DriverVersion

Get WiFi driver version

This feature is only for Ralink drivers.

22.17 SiteSurveyEnable

Enable/Disable site survey scan

This feature is only for Ralink drivers.

22.18 OtherAP

Display the APs information

22.18.1 SSID

Display the AP SSID

22.18.2 Channel

Display the AP channel

22.18.3 MACAddress

Display the AP MAC address

22.18.4 RSSI

Display the AP RSSI

22.18.5 Security

Display the AP security mode

22.18.6 Mode

Display the AP standard mode

23 WLANINTERFACE

Object defining a WiFi interface.

A WiFi interface can be configured as an Access Point or a station. Several Access Points with different SSIDs and different levels of security (WEP, WPA) can be configured in the box.

Note: The number of WiFi interface is read-only and is limited by the WiFi driver.

23.1 ENABLE

Set to 1 to activate the WiFi interface.

23.2 IFNAME

The name of the WiFi network interface.

This is driver dependent.

Note: Network interfaces of Atheros driver are ath0, ath1... Network interfaces of Ralink driver are ra0, ra1... Network interfaces of Broadcom driver are br0, br1...

23.3 CURRENTMACADDRESS

The current MAC address of current network interface.

23.4 DESCRIPTION

Human readable description of the WiFi interface.

May be use to help understanding a specific configuration.

23.5 QOSENABLE

When set, Linux network output queues will be created according to the parameters configured in the object Qos.

23.6 WMMENABLE

When set, enables WMM (WiFi MultiMedia) for the interface.

23.7 WMMPSENABLE

When set, enables WMM PS (Power Save) for the interface.

23.8 ACLENABLE

Set to 1 to activate on the WiFi interface the Access Control List defined in the object _LANDevice_?_AccessControl.

The ACL is based on MAC addresses and handled at the driver level.

23.9 WPSENABLE

When set, enables the WPS service.

WPS (WiFi Protected Setup) is also known as WSC (WiFi Simple Config).

'''Warning''' : WPS can only be enabled for one WiFi interface. If it is enabled for more than one interface, other WiFi interface may not work correctly. _WLANInterface_?_Config_WPADefaultKey must be set for enabling WPS .

23.10 WPSMETHOD

Select the WPS pairing method.

PBC allows pairing by push button, PIN allows pairing by PIN code, PBC+PIN allows the both methods and External allows to use an External Wired Registrar.

Note: PBC+PIN method is not allowed for Ralink chipsets. WLANConfig_EasyPairing must be enabled for WPS working.

23.11 WCNEnable

When set, enables the WCN-UFD service.

WCN-UFD (Windows Connect Now - USB Flash Drive)

'''Warning''' : WCN can only be enabled for one WiFi interface. If it is enabled for more than one interface, other WiFi interface may not work correctly. _WLANConfig_EasyPairing must be set for enabling WCN .

23.12 APIsolation

When set, enables AP isolation between each Stations of an SSID.

Note: Works only for Broadcom Chipsets

23.13 Config

This object contains parameters to the specific WLAN interface.

23.13.1 SSID

SSID (Service Set Identifier) of the Access Point.

23.13.2 HideSSID

When set, enables SSID hiding.

SSID hiding option allows not to broadcast SSID name.

23.13.3 TargetAP

BSSID (MAC address) of the remote Access Point to be connected to when the WiFi interface is a station.

Sets the AP BSSID (MAC address) to be connected to when ibox is station.

23.13.4 BitRates

Obsolete

Note: Do not use.

23.13.5 MaxBitRate

Sets the max bitrate in bit/seconds.

'''Auto''' option automatically sets the best rate.

23.13.6 MaxUsers

Limit users number at same time.

'''0''' option disable this feature.

23.13.7 RateFallBack

When set, enables rate fallback.

If enabled, it allows WiFi driver to use a lower data rate transmission under noisy environment. Rate will be in the range of 1M and _WLANInterface_?_Config_MaxBitRate.

23.13.8 BeaconType

Sets the security mode for WiFi data encryption.

Basic option allows WEP mode. WPA-Auto automatically adjusts to WPA or WPA2.

23.13.9 WDSMode

Sets the WDS mode (Wireless Distribution System).

23.13.10 WEPEncryption

Sets the WEP Encryption mode.

Set to None if no encryption is required.

In WEP Open mode, the station is considered as connected even if the the WEP key is wrong.

Note: WEP parameters are relevant only when _WLANInterface_?_Config_BeaconType is set to Basic.

23.13.11 WEPKeyIndex

Sets the active WEP Key.

Parameter values : "1,2,3,4". User can enter 4 different keys (HEX or ASCII) in following fields, this parameter sets the key number which is enabled.

23.13.12 WEPKey1

Sets the hexadecimal WEP Key number 1.

Parameter length is 10 or 26 HEXA characters.

23.13.13 WEPKeyAscii1

IHM sets this option to 1 if user chooses to enter an ASCII WEP Key number 1.

ASCII to HEXA conversion was automaticaly made by IHM.

23.13.14 WEPKey2

Sets the hexadecimal WEP Key number 2.

Parameter length is 10 or 26 HEXA characters.

23.13.15 WEPKeyAscii2

IHM sets this option to 1 if user chooses to enter an ASCII WEP Key number 2.

ASCII to HEXA conversion was automaticaly made by IHM.

23.13.16 WEPKey3

Sets the hexadecimal WEP Key number 3.

hexa - Parameter length is 10 or 26 HEXA characters.

23.13.17 WEPKeyAscii3

IHM sets this option to 1 if user chooses to enter an ASCII WEP Key number 3.

ASCII to HEXA conversion was automaticaly made by IHM.

23.13.18 WEPKey4

Sets the hexadecimal WEP Key number 4.

hexa - Parameter length is 10 or 26 HEXA characters.

23.13.19 WEPKeyAscii4

IHM sets this option to 1 if user chooses to enter an ASCII WEP Key number 4.

ASCII to HEXA conversion was automaticaly made by IHM.

23.13.20 WPAEncryption

Sets the WPA Encryption mode.

'''Auto''' option allows TKIP and AES to be available.

Note: WPA encryption parameters are only read when BeaconType is set to '''WPA''', '''WPA2''' or '''WPA-Auto'''.

23.13.21 WPADefaultKey

Sets the default WPA key.

Key can be from 8 to 63 ASCII characters or 64 HEXA characters.

23.13.22 RekeyingPeriod

Sets the rekeying period (milliseconds) in WPA modes.

23.13.23 WPAPSK_List

Comma-separated list of indexes of _WLANInterface_?_Config_WPAPSK_? objects

23.13.24 WPAPSK

Array of (MAC address / WPA key) pairs.

This allows to set different WPA keys for different stations.

- MACAddress

Specify the station by its MAC address.

- Key

Specify the WPA key for a given station.

23.13.25 RTSThreshold

Sets RTS threshold.

Sets the smallest packet size for which the AP sends RTS. Without argument, the option is set to off.

23.13.26 FragThreshold

Sets fragmentation threshold.

Sets maximum fragment size in RTS/CTS mode (256 to 2346 octets). Without argument, the option is set to off.

23.13.27 DTIMPeriod

Sets DTIM period (in milliseconds). Use with caution.

23.13.28 WPSPINCode

Sets WPS PIN code.

Sets the PIN code for WPS (8 ciphers).

23.14 Counters

Counters of sent or received data (in packets or bytes) on the physical network interface since the initialization of the driver.

23.14.1 RxPackets

Counters of received packets on the physical network interface since the initialization of the driver.

23.14.2 RxPacketsErrors

Counters of received packets in error on the physical network interface since the initialization of the driver.

23.14.3 RxPacketsDiscards

Counters of received packets discard on the physical network interface since the initialization of the driver.

23.14.4 TxPackets

Counters of sent packets on the physical network interface since the initialization of the driver.

23.14.5 TxPacketsErrors

Counters of sent packets in error on the physical network interface since the initialization of the driver.

23.14.6 TxPacketsDiscards

Counters of sent packets discard on the physical network interface since the initialization of the driver.

23.14.7 RxBytes

Counters of received bytes on the physical network interface since the initialization of the driver.

23.14.8 TxBytes

Counters of sent bytes on the physical network interface since the initialization of the driver.

23.14.9 ARPTable

Comma separated list of MAC addresses detected on the network interface by the ARP protocol.

23.14.10 UnauthorizedStations

MAC address of the unauthorized stations.

23.15Station

This array of objects gives information about the stations that are connected to the Access Point.

23.15.1 MACAddress

MAC address of the connected /authenticated station.

23.15.2 Rate

Current bit rate of the connection.

23.15.3 RSSI

Receive Signal Strength.

This value is computed by the Radio upon reception of each 802.11 frame.

23.16WPSStatus

Shows WPS status.

23.16.1 Pairing

Status of WPS PBC/PIN pairing.

Shows the status if last WPS PIN pairing has been progressing (Progress), successful (Success), failed (Error, Overlap, Timeout) or not yet proceded (None).

23.17ExtraWLAN

Private - used by web pages.

24 LANDevice

A _LANDevice_? is a subnet (IP mask) including one or more physical network interfaces (Ethernet, wifi, USB).

Note: The _LANDevice_? is implemented in the box as a network bridge.

24.1 Enable

When set, enables current _LANDevice_? object.

Note: A linux network interface named lanx (x=0,1,2...) will be automatically created with parameters set in this object.

24.2 EnableSTP

Enables Spanning Tree Protocol.

A LAN device is an Ethernet bridge that includes several physical interfaces. STP is a protocol that ensures there are no loops between these interfaces. STP can be disabled if the final user cannot create loops between Ethernet, Wifi and USB network segments.

24.3 CurrentMACAddress

The current MAC address of current network interface.

24.4 LANEthernetInterface

Defines which Ethernet interface(s) will be included in the LANDevice object (included in the LAN bridge).

The number of _LANDevice_?_LANEthernetInterface_? objects is specified in the parameter _LANEthernetInterface_Count.

24.4.1 Enable

Set to 1 to include the physical interface in the LAN.

To include the physical network interface _LANEthernetInterface_? in the _LANDevice_? network bridge, set the parameter _LANDevice_?_LANEthernetInterface_?_Enable to 1.

Note: If the Ethernet interface contains VLANs, This parameter MUST be 0, use the _LANDevice_?_LANEthernetInterface_?_VLANInterface_?_Enable instead.

24.4.2 VLANInterface_List

List of VLAN interfaces created in the object LANEthernetInterface_y.

This list is managed automatically through cli by commands mk or statically filled in the factory configuration profile.

Note: _LANDevice_?_LANEthernetInterface_?_VLANInterface objects are created through the CLI by the command mk (see configuration command line documentation).

24.4.3 VLANInterface

Array of objects (one per VLAN interface created in the corresponding Ethernet interface).

This objects contain one parameter (Enable) used to include the VLAN interfaces in the LAN bridge.

- Enable

Set to 1 to include the VLAN interface in the LAN.

To include the VLAN interface _LANEthernetInterface_?_VLANInterface_? in the LANDevice_? network bridge, set the parameter _LANDevice_?_LANEthernetInterface_?_VLANInterface_?_Enable to 1.

24.5 LANUSBInterface

Defines which USB slave network interface(s) will be included in the LANDevice object (included in the LAN bridge).

The number of _LANDevice_?_LANUSBInterface_? objects is specified in the parameter _LANUSBInterface_Count.

24.5.1 Enable

Set to 1 to include the physical interface in the LAN.

To include the physical network interface LANUSBInterface_y in the LANDevice_x network bridge, set the parameter _LANDevice_?_LANUSBInterface_?_Enable to 1.

24.6 WLANInterface

Defines which WLAN (Wifi) interface(s) will be included in the LANDevice object (included in the LAN bridge).

The number of _LANDevice_?_WLANInterface_? objects is specified in the parameter _WLANInterface_Count.

24.6.1 Enable

Set to 1 to include the Wifi interface in the LAN.

24.7 HostARPKeepAlive

Set if box will refresh ARP on Lan side (usefull for LANDevice_x_Host for static entries and detect conflicts on network).

24.8 IPInterface

Array containing the different subnets associated to the LAN (most of the time only one subnet per LAN).

The _LANDevice_?_IPInterface_List parameter contains the different index of the array. Each subnet is configured with it's IPAddress , SubnetMask, and can be Enabled or not.

Note: A secondary IP address / subnet mask is rarely used

24.8.1 Enable

Must be set to 1 to activate the network interface.

24.8.2 IPAddress

Static IP address of the LAN interface, or left blank if AddressingType is DHCP.

24.8.3 SubnetMask

Static subnet mask of the LAN interface or left blank if AddressingType is DHCP.

24.8.4 AddressingType

How the LANDevice address is set. Usually Static.

The IP address of the LAN interface may be defined statically or assigned dynamically by DHCP.

Note: if AddressingType is DHCP, no DHCP server must be programmed in the box for the subnet. An external DHCP must exists instead.

24.9 HostConfig

This object gathers information about the subnet managed by the _LANDevice_? object.

24.9.1 DHCPServerConfigurable

Enables configuration of DHCP

When true, the DHCP configuration is available by TR069. When set to false, all default values are restored and the DHCP configuration is no more available.

24.9.2 DHCPServerEnable

Activates a DHCP server on the LANDevice subnet.

The DHCP server will serve clients connected to the LAN subnet. It will assign a domain name, an IP address, a default gateway and list of DNS servers to the clients.

24.9.3 Debug

Enable syslog trace of DHCP messages

24.9.4 DHCPRelay

Describe various parameters of DHCP relay mode.

Dependency: Require dhcp-forwarder

- Enable

Enables the DHCP relay mode.

- Servers

List the dhcp server.

  - Name

Name of dhcp server.

  - Address

IP or FQDN of dhcp server.

- Interface

indicate from which network interface dhcp packets are send.

- External

If set to 1, previous field Interface will be set wan otherwise Interface will look for LAN.

- AgentInfo

Set the relay agent info status.

- AgentMismatch

Forward (0) or drop (1) DHCP reply when relay agent info mismatch is detected.

Note: check RFC 3046

- MaxHops

set the TTL of packet send to dhcp server.

Note: not used as this time

- RemoteId

set the remote ID as specified in RFC 3046. (opt 82)

- Trusted

Forward (0) or drop (1) DHCP request packet when a relay info option is already set and giaddr field is 0.

Note: check RFC3046

24.9.5 MinAddress

Mandatory - First address in the range of IP addresses delivered to clients by the DHCP server.

24.9.6 MaxAddress

Mandatory - Last address in the range of IP addresses delivered to clients by the DHCP server.

24.9.7 SubnetMask

Leave blank if the DHCP server subnet is the same as the _LANDevice_?_IPInterface_?_SubnetMask. Otherwise, specify a mask.

Note: Usually left blank.

24.9.8 DNSServers

Usually left blank.

Leave blank if the DHCP server returns the IP address of the box (_LANDevice_?_IPInterface_?_IPAddress) as the DNS server for its subnet. Otherwise specify a comma-separated list of DNS servers.

24.9.9 DomainName

Usually left blank.

Leave blank if the DHCP server returns _Device_Domain as the domain name of the subnet. Otherwise specify a domain name (string).

24.9.10 IPRouters

Usually left blank.

Leave blank if the DHCP server returns the IP address of the box (_LANDevice_?_IPInterface_?_IPAddress) as the default router for its subnet. Otherwise specify a comma-separated list of gateways.

24.9.11 DHCPLeaseTime

Duration in seconds of the lease assigned to a client by the DHCP server.

24.9.12 DHCPMatch

List of LAN hosts classes discriminated by VendorClass or UserClass option

- SetMatchName

Name of match

- VendorClass

Matches a substring of the DHCP VendorClass option

- UserClass

Matches a substring of the DHCP UserClass option

24.9.13 DHCPRange

Define additional pools of IP addresses

- MinAddress

Mandatory - First address in the range of IP addresses.

- MaxAddress

Mandatory - Last address in the range of IP addresses.

- DHCPLeaseTime

Duration in seconds of the lease assigned by the DHCP server.

- MatchName

This pool applies only for hosts matching this class

24.9.14 DHCPOPTIONS

List of specific DHCP options to be sent to LAN hosts

- Enable

Enable this specific option for dhcp server

- Name

Name of option

- Value

Value of option

- Forced

Option is sent even if not required by client

- MatchName

Send option only for hosts that belongs to this class

24.9.15 USEALLOCATEDWAN

Must be set to Normal.

Note: Other values are not implemented.

24.9.16 ASSOCIATEDCONNECTION

This parameter is used for bridging current _LANDevice_? to a WAN interface.

It contains the index of the _WANConnectionDevice_? object bridged to current _LANDevice_? (Otherwise specify 0).

Note: To bridge the WAN x to a LAN, the parameters:

WANConnectionDevice?_WANIPConnection_Enable and

WANConnectionDevice?_WANPPPConnection_Enable must be set to 0.

24.9.17 CLIENTTABLE_LIST

Comma-separated list of indexes of _LANDevice_?_HostConfig_ClientTable_?

24.9.18 CLIENTTABLE

Table of clients that will receive specific IP addresses from the DHCP server.

A table entry is composed of three elements: _LANDevice_?_HostConfig_ClientTable_?_IPAddress, _LANDevice_?_HostConfig_ClientTable_?_MACAddress and _LANDevice_?_HostConfig_ClientTable_?_Hostname.

- Hostname

Hostname of the DHCP client

If a MAC address is also specified, DNS queries to this name will return the IP address of the client.

Note: If left empty, use _LANDevice_?_HostConfig_ClientTable_?_MACAddress to specify a client

- MACAddress

MACAddress of the client whose IP address must be assigned by the DHCP Server

Note: If left empty, use Hostname to specify a client

- IPAddress

IP address assigned, by the DHCP server, to a known client.

A client is known by, either its hostname (_LANDevice_?_HostConfig_ClientTable_?_Hostname) or its MAC address (_LANDevice_?_HostConfig_ClientTable_?_MACAddress).

- User

Is set to 0, this entry should not be displayed and managed by web graphical user interface.

24.9.19 DHCPLEASES

Status giving the list of DHCP clients which have received an IP Address by the DHCP Server.

Each item, whose index is in the List Parameter, contains the _LANDevice_?_HostConfig_DHCPLeases_?_MACAddress, _LANDevice_?_HostConfig_DHCPLeases_?_VendorClass (identifier based on the kind of material) and Hostname of the computer, the assigned _LANDevice_?_HostConfig_DHCPLeases_?_IPAddress, and the _LANDevice_?_HostConfig_DHCPLeases_?_Expiration date in Unix timestamp format.

- IPAddress

Assigned IP address of the current lease.

- MACAddress

MAC address of the current lease.

- Hostname

Hostname of the computer for the current lease.

- VendorClass

VendorClass of the current lease.

- UserClass

UserClass of the current lease.

- Expiration

Expiration date of the current lease, in Unix timestamp format.

24.10 ACCESSCONTROL

Table of clients allowed to access the LAN via a wireless connection.

A table entry is composed of three elements: the client name, a MAC address and the enabled status.

Note: The Access Control List is globally defined for the LAN but only used by wireless connections. If _WLANInterface_? is included in the LAN, _WLANInterface_?_ACLEnable must be set to 1 to activate the Access Control List for this WLAN interface.

24.10.1 ENABLE

Defines whether the computer (specified by _LANDevice_?_AccessControl_?_MACAddress or _LANDevice_?_AccessControl_?_ClientName) can access the LAN.

24.10.2 MACADDRESS

MAC Address of the device allowed to connect to the WLAN

24.10.3 CLIENTNAME

Unused

24.11 COUNTERS

Statistic counters of the LAN network interface.

Counters of sent or received data (in packets or bytes) on the logical network interface since the device creation.

24.11.1 RXPACKETS

Counters of received packets since the device creation.

24.11.2 RXPACKETSERRORS

Counters of received in error packets since the device creation.

24.11.3 RXPACKETSDISCARDS

Counters of received discard packets since the device creation.

24.11.4 TXPACKETS

Counters of sent packets since the device creation.

24.11.5 TXPACKETSERRORS

Counters of sent packets in error since the device creation.

24.11.6 TXPACKETSDISCARDS

Counters of sent packets discard since the device creation.

24.11.7 RXBYTES

Counters of received bytes since the device creation.

24.11.8 TXBYTES

Counters of sent bytes since the device creation.

24.12 ARPTABLE

Status information. Table of clients detected by the ARP protocol through the LAN interface. Each entry contains an IP address and a MAC address.

Dependency: {{{[*] Customize User Settings

Network Applications ---

[*] bridge utils

[*] dhclient(ISC)

[*] enable LINKDETECT feature

[*] dnsmasq V2 (with DHCP server)}}}

24.12.1 IPADDRESS

IPAddress of the entry

24.12.2 MACADDRESS

MACAddress of the entry

24.13 HOSTS

24.13.1 IPADDRESS

24.13.2 MACADDRESS

24.13.3 HOSTNAME

24.13.4 LEASEREMAINING

24.13.5 ADDRESSINGTYPE

24.13.6 INTERFACETYPE

24.13.7 ACTIVE

25 WANDSLINTERFACECONFIG

Describe the Wan DSL interface behavior.

25.1 ENABLE

When set, enable DSL link.

25.2 MODULATIONTYPE

Set the DSL modulation type.

ADSL_multi: all Annex A modes ADSL_G.dmt: 992.1 ADSL_G.lite: 992.2 ADSL_ANSI_T1.413 ADSL_G.dmt.bis: 992.3 ADSL_2plus: 992.5 ADSL_multi_AM: all Annex A and Annex M modes.

Note: The default value is ADSL_multi

26 WANDSLLinkStatus

Give information on the DSL link.

26.1 State

state of the DSL link.

reset, ready, fail, idle, activating, ghs handshaking, initializing, full on.

26.2 Info

Give information on the DSL link.

26.2.1 FirmwareVersion

DSP firmware version.

26.2.2 TimeConnected

Elapsed time from beginning of synchronization.

26.2.3 ATURProvider

Local DSP firmware provider.

26.2.4 ATUCProvider

Remote DSP firmware provider.

26.2.5 Modulation

Current Modulation

26.3 UpBitrates

Give information on the upstream bit rates.

26.3.1 Max

26.3.2 FastChannel

26.3.3 InterleavedChannel

26.4 DownBitrates

Give information on the Downstream bit rates.

26.4.1 Max

26.4.2 FastChannel

26.4.3 InterleavedChannel

26.5 UpLinePerfs

Give information on the Upstream line Performance.

26.5.1 NoiseMargin

26.5.2 Attenuation

26.5.3 OutputPower

26.5.4 InterleavedDelay

26.6 DownLinePerfs

Give information on the Downstream line Performance.

26.6.1 NoiseMargin

26.6.2 Attenuation

26.6.3 OutputPower

26.6.4 InterleavedDelay

26.7 CurrentShowtime

Give statistics information on the current showtime (current DSL synchronization).

26.7.1 Age

Duration of this synchrinization.

26.7.2 LocalRxWords

Local counter: number of received blocks.

26.7.3 RemoteRxWords

Remote counter: number of received blocks.

26.7.4 LocalTxWords

Local counter: number of transmitted blocks.

26.7.5 RemoteTxWords

Remote counter: number of transmitted blocks.

26.7.6 LocalHEC

Local counter: number of Header Error Control.

26.7.7 RemoteHEC

Remote counter: number of Header Error Control.

26.7.8 LocalFEC

Local counter: number of Forward Error Correction.

26.7.9 RemoteFEC

Remote counter: number of Forward Error Correction.

26.7.10 LocalCRC

Local counter: number of Cyclic redundancy Check error.

26.7.11 RemoteCRC

Remote counter: number of Cyclic redundancy Check error.

26.7.12 LocalLof

Local counter: Loss Of Frame.

26.7.13 RemoteLof

Remote counter: Loss Of Frame.

26.7.14 LocalEs

Local counter: number of Second with Error.

26.7.15 RemoteEs

Remote counter: number of Second with Error.

26.7.16 LocalSes

Local counter: number of Severe Second with Error.

26.7.17 RemoteSes

Remote counter: number of Severe Second with Error.

26.7.18 LocalUas

Local counter: number of UnAvailable Seconds.

26.7.19 RemoteUas

Remote counter: number of UnAvailable Seconds.

26.8 PreviousShowtime

Give statistics information on the previous showtime (previous DSL synchronization).

26.8.1 Age

Duration of this synchronization.

26.8.2 LocalRxWords

Local counter: number of received blocks.

26.8.3 RemoteRxWords

Remote counter: number of received blocks.

26.8.4 LocalTxWords

Local counter: number of transmitted blocks.

26.8.5 RemoteTxWords

Remote counter: number of transmitted blocks.

26.8.6 LocalHEC

Local counter: number of Header Error Control.

26.8.7 RemoteHEC

Remote counter: number of Header Error Control.

26.8.8 LocalFEC

Local counter: number of Forward Error Correction.

26.8.9 RemoteFEC

Remote counter: number of Forward Error Correction.

26.8.10 LocalCRC

Local counter: number of Cyclic redundancy Check error.

26.8.11 RemoteCRC

Remote counter: number of Cyclic redundancy Check error.

26.8.12 LocalLof

Local counter: Loss Of Frame.

26.8.13 RemoteLof

Remote counter: Loss Of Frame.

26.8.14 LocalEs

Local counter: number of Second with Error.

26.8.15 RemoteEs

Remote counter: number of Second with Error.

26.8.16 LocalSes

Local counter: number of Severe Second with Error.

26.8.17 RemoteSes

Remote counter: number of Severe Second with Error.

26.9 Current15Min

Give statistics information on the current 15 minutes showtime (statistics counters are reset every 15min).

26.9.1 Age

Duration of this synchronization.

26.9.2 LocalRxWords

Local counter: number of received blocks.

26.9.3 RemoteRxWords

Remote counter: number of received blocks.

26.9.4 LocalTxWords

Local counter: number of transmitted blocks.

26.9.5 RemoteTxWords

Remote counter: number of transmitted blocks.

26.9.6 LocalHEC

Local counter: number of Header Error Control.

26.9.7 RemoteHEC

Remote counter: number of Header Error Control.

26.9.8 LocalFEC

Local counter: number of Forward Error Correction.

26.9.9 RemoteFEC

Remote counter: number of Forward Error Correction.

26.9.10 LocalCRC

Local counter: number of Cyclic redundancy Check error.

26.9.11 RemoteCRC

Remote counter: number of Cyclic redundancy Check error.

26.9.12 LocalLof

Local counter: Loss Of Frame.

26.9.13 RemoteLof

Remote counter: Loss Of Frame.

26.9.14 LocalEs

Local counter: number of Second with Error.

26.9.15 RemoteEs

Remote counter: number of Second with Error.

26.9.16 LocalSes

Local counter: number of Severe Second with Error.

26.9.17 RemoteSes

Remote counter: number of Severe Second with Error.

26.9.18 LocalUas

Local counter: number of UnAvailable Seconds.

26.9.19 RemoteUas

Remote counter: number of UnAvailable Seconds.

26.10 CurrentDay

Give statistics information on the current 24 hours showtime (statistics counters are reset every 24h).

26.10.1 Age

26.10.2 LocalRxWords

Local counter: number of received blocks.

26.10.3 RemoteRxWords

Remote counter: number of received blocks.

26.10.4 LocalTxWords

Local counter: number of transmitted blocks.

26.10.5 RemoteTxWords

Remote counter: number of transmitted blocks.

26.10.6 LocalHEC

Local counter: number of Header Error Control.

26.10.7 RemoteHEC

Remote counter: number of Header Error Control.

26.10.8 LocalFEC

Local counter: number of Forward Error Correction.

26.10.9 RemoteFEC

Remote counter: number of Forward Error Correction.

26.10.10 LocalCRC

Local counter: number of Cyclic redundancy Check error.

26.10.11 RemoteCRC

Remote counter: number of Cyclic redundancy Check error.

26.10.12 LocalLof

Local counter: Loss Of Frame.

26.10.13 RemoteLof

Remote counter: Loss Of Frame.

26.10.14 LocalEs

Local counter: number of Second with Error.

26.10.15 RemoteEs

Remote counter: number of Second with Error.

26.10.16 LocalSes

Local counter: number of Severe Second with Error.

26.10.17 RemoteSes

Remote counter: number of Severe Second with Error.

26.10.18 LocalUas

Local counter: number of UnAvailable Seconds.

26.10.19 REMOTEUAS

Remote counter: number of UnAvailable Seconds.

26.11 TOTAL

26.11.1 AGE

Duration of this synchronization.

26.11.2 LOCALRXWORDS

Local counter: number of received blocks.

26.11.3 REMOTERXWORDS

Remote counter: number of received blocks.

26.11.4 LOCALTXWORDS

Local counter: number of transmitted blocks.

26.11.5 REMOTETXWORDS

Remote counter: number of transmitted blocks.

26.11.6 LOCALHEC

Local counter: number of Header Error Control.

26.11.7 REMOTEHEC

Remote counter: number of Header Error Control.

26.11.8 LOCALFEC

Local counter: number of Forward Error Correction.

26.11.9 REMOTEFEC

Remote counter: number of Forward Error Correction.

26.11.10 LOCALCRC

Local counter: number of Cyclic redundancy Check error.

26.11.11 REMOTECRC

Remote counter: number of Cyclic redundancy Check error.

26.11.12 LOCALLOF

Local counter: Loss Of Frame.

26.11.13 REMOTELOF

Remote counter: Loss Of Frame.

26.11.14 LOCALES

Local counter: number of Second with Error.

26.11.15 REMOTEES

Remote counter: number of Second with Error.

26.11.16 LocalSes

Local counter: number of Severe Second with Error.

26.11.17 RemoteSes

Remote counter: number of Severe Second with Error.

26.11.18 LocalUas

Local counter: number of UnAvailable Seconds.

26.11.19 RemoteUas

Remote counter: number of UnAvailable Seconds.

27 WANConnectionDevice

Array of objects describing the WAN (Wide Area Network) interfaces.

The WAN device objects implement network interfaces configured with features dedicated to a WAN access (firewall, NAT...).

Note: A WAN interface can be configured for IP (DHCP client or static address) or for PPP client or directly bridged to a LAN.

27.1 Enable

Enables the WAN interface.

27.2 IfName

Name of the network interface that will be created.

For example wan1.

Note: Should be set on the factory configuration

27.3 CurrentMACAddress

The current MAC address of current network interface.

27.4 Description

Optional human readable description of the WAN conguration.

27.5 HwMacId

Add (n*4)+2 to the first byte of the default MAC address and set the new MAC to this WAN. Example: if HwMacId=1 and the default MAC is 00:0C:C3:60:FF:FF then the WAN MAC will be set to 06:0C:C3:60:FF:FF.

Note: This feature is necessary when several WAN interfaces are working on the same physical link (ATM, Ethernet...). MAC addresses of each WAN interface MUST be different.

27.6 MACAddressOverride

if 1, override the MAC address to the one specified in _WANConnectionDevice_?_MACAddress.

27.7 MACAddress

Mac address of the network interface if _WANConnectionDevice_?_MACAddressOverride is set to 1.

27.8 MaxMTUSize

Specify the MTU (Maximum Transfer Unit) of the network interface.

If left empty the MTU is automatically set to 1500 unless the WAN interface is PPPoE in which case it is set to 1492. The MTU can be manually decreased using the parameter MaxMTUSize.

Note: There are two PPP encapsulations over ATM. PPPoA with a default MTU of 1500 and PPPoE with a default MTU of 1492.

The type of PPP encapsulation is determined by the parameter _ATMEthernetInterface_?_ATMLinkConfig_LinkType.

27.9 Multicast

Set to 1 if you want to do multicast traffic on the WAN interface.

If set to 0, the WAN interface will filter all incoming and outgoing multicast packets.

27.10 EnableSTP

Enables Spanning Tree Protocol.

WAN device can be an Ethernet bridge that includes several physical interfaces. STP is a protocol that ensures there are no loops between these interfaces. STP can be disabled if the final user could not create loops between all presents segments.

27.11 PhysicalInterface

This object specifies to which physical link the WAN interface is connected.

Possible physical interfaces are ATM/ADSL, Ethernet, ethernet VLANs or WLAN as a station (WiFi).

Note: To use Modem3GInterface put _WANConnectionDevice_?_WANPPPConnection_Enable and _WANConnectionDevice_?_WANIPConnection_Enable to 0 and _WANConnectionDevice_?_WANIPConnection_AddressingType to Static. The Modem3GInterface dynamicaly uses a PPP or IP connection depending of the modem's vendor

27.11.1 Type

Type of interface object the WAN interface will be connected to.

27.11.2 List

List of indexes of physical interface objects which type is specified in _WANConnectionDevice_?_PhysicalInterface_Type.

If more than one index is specified, the physical interfaces will be bridged.

Note: For exemple:

PhysicalInterface_Type=ATMEthernetInterface

PhysicalInterface_List=1,2,3

The WAN interface will bridge atm1, atm2, atm3

27.11.3 VLANNumber

If the physical interface is a LANEthernetInterface, you can specify which VLAN to use.

27.12 PhysicalInterfaceV2

This table is a second version of PhysicalInterface object.

This new version allow to build a WAN interface that will bridge physical interfaces of different types such as Ethernet and WLAN (WiFi).

27.12.1 Enable

Allow to separately activate disable physical interfaces in a WAN bridge.

27.12.2 Type

Type of the physical interface the WAN interface is connected to.

27.12.3 Index

Index of the object which type is specified in Type.

27.12.4 VLANNumber

If Physical interface is of type LANEthernetInterface you may specified a VLAN index.

You must create a VLAN on the corresponding interface.

Note: See _LANEthernetInterface_?_VLANInterface array for more information.

27.13 WANIPConnection

This object contains parameters related to IP configuration and is not used for a PPP connection.

Setting WANIPConnection_Enable to 1 will activate the WAN interface as an IP inrterface using either a DHCP or static IP address.

Note: _WANConnectionDevice_?_WANPPPConnection_Enable and _WANConnectionDevice_?_WANIPConnection_Enable MUST not be set simultaneously

27.13.1 ENABLE

Set to 1 to program the WAN interface as an IP interface.

Note: WANPPPConnection_Enable and WANIPConnection_Enable MUST not be set simultaneously

27.13.2 CREATED

Used by TR-069 protocol.

27.13.3 IPADDRESS

Set the IP address of the WAN interface if AddressingType is Static.

27.13.4 SUBNETMASK

Set the subnet mask of the network interface if AddressingType is Static.

27.13.5 DEFAULTGATEWAY

Set the default gateway of the WAN interface if the AddressingType is Static.

27.13.6 ADDRESSINGTYPE

Select the type of IP connection, DHCP or Static.

Note: Do not use Other (private configuration option)

27.13.7 DHCPHOSTNAME

If specified, send this parameter in the DHCP option 12 (hostname).

Note: Unused if AddressingType is Static

27.13.8 DHCPCLASSIDENTIFIER

If specified, send this parameter in the DHCP option 60 (vendor class).

27.13.9 DHCPECHOINTERVALTIMER

Interval in seconds between ping requests

27.13.10 DHCPECHOFAILURECOUNT

Enables a mechanism of keep alive using pings on the WAN interface.

If not 0, a ping will be automatically sent to the default gateway of the network interface at intervals specified in the parameter _WANConnectionDevice_?_WANIPConnection_DHCPEchoIntervalTimer. If no answer is received after _WANConnectionDevice_?_WANIPConnection_DHCPEchoFailureCount tries the link is considered as down.

Note: This feature allows to trigger a redirection of the network traffic to a backup WAN interface.

27.13.11 DHCPARPINGINTERVALTIMER

Interval in seconds between arping requests

27.13.12 DHCPARPINGFAILURECOUNT

Enables a mechanism of keep alive using arpings on the WAN interface.

If not 0, a arping will be automatically sent to the default gateway of the network interface at intervals specified in the parameter _WANConnectionDevice_?_WANIPConnection_DHCPArpingIntervalTimer. If no answer is received after _WANConnectionDevice_?_WANIPConnection_DHCPArpingFailureCount tries the link is considered as down.

Note: This feature allows to trigger a redirection of the network traffic to a backup WAN interface.

27.13.13 DHCPREQUESTEDOPTIONS

List of strings, Tells DHCP client to request specific options to the server.

Note: The option names and syntax are described in DHCP-ISC documentation.

27.13.14 KEEPALIVE

0 or delay between keep alive ARP requests to the default gateway.

This feature allows to maintain a periodic ARPING to the default gateway of the interface. This may be needed by the remote network infrastructure to refresh ARP tables in the Ethernet switches.

27.13.15 ZEROCONF

Set to 1 to switch automatically to zeroconf IP address in case of DHCP no offer.

This feature allows to setup ad-hoc networking between devices without involvement of either a DHCP server or a network administrator.

27.14 WANPPPCONNECTION

This object contains parameters related to PPP configuration and is not used for an IP connection.

Setting WANPPPConnection_Enable to 1 will activate the WAN interface as a PPP interface.

Note: WANPPPConnection_Enable and WANIPConnection_Enable MUST not be set simultaneously

27.14.1 ENABLE

Set to 1 to program the WAN interface as a PPP interface.

Note: WANPPPConnection_Enable and WANIPConnection_Enable MUST not be set simultaneously

27.14.2 CREATED

Used by TR-069 protocol.

Note: Unused.

27.14.3 DEBUG

When set, activates the debug trace for the pppd deamon.

The debug trace is recorded in the syslog and can be retrived by the command logread.

27.14.4 PPPOEACNAME

Leave empty or desired PPPoE Access Concentrator name.

Note: Used in PPPoE Discovery Stage

27.14.5 PPPOESERVICENAME

Leave empty or desired PPPoE Service Name.

Note: Used in PPPoE Discovery Stage

27.14.6 USERNAME

User/login name for the PPP authentication.

27.14.7 Password

Password for the PPP authentication.

27.14.8 LcpRetranIntervalTimer

Delay in seconds between retransmissions of LCP Configure Requests.

27.14.9 LcpMaxRetranCount

Maximum number of LCP Configure Request transmissions.

27.14.10 LcpEchoIntervalTimer

Delay in second between LCP Echo Requests.

27.14.11 LcpEchoFailureCount

Number of unreplied LCP Echo Requests that will trigger a link down.

27.14.12 HoldOffTimeouts

Comma-separated list of delays that will be introduced between attempts of connections upon failure.

This feature allows to randomize reconnection delay when the link is temporary down. This will prevent an overload of the PPP server when numerous CPEs try to reconnect after a server failure.

27.14.13 SessionInfo

Internally used by Force TermReq feature

On IP Up event, PPPoE session ID and MAC address of the Access Concentrator are saved permanently in configuration. A TermReq and PADT packets on the previous session are sent before each connection establishment.

Dependency: Make menuconfig - User - PPP - Force TermReq before connecting

Note: The purpose of this feature is to cleanup orphan session on the server if something got wrong when terminating the last session.

27.15WANTTYLinkConfig

Obscolete, used Modem3GInterface to configure.

27.15.1 Enable

Obscolete, used Modem3GInterface to configure.

27.15.2 PhoneNumber

Obscolete, used Modem3GInterface to configure.

27.15.3 InitString

Obscolete, used Modem3GInterface to configure.

27.15.4 DialString

Obscolete, used Modem3GInterface to configure.

27.15.5 APN

Obscolete, used Modem3GInterface to configure.

27.15.6 CGDCONT

Obscolete, used Modem3GInterface to configure.

27.15.7 PINCODE

Obscolete, used Modem3GInterface to configure.

27.15.8 MODEPREF

Obscolete, used Modem3GInterface to configure.

27.16 L2FILTER

Allow to filter datagrams on the WAN interface.

'''None''' : No filter is applied.

'''PPPoE''' : Only PPPoE frames are forwarded on the interface.

'''IPARP''' : Only IP and ARP frames are forwarded on the interface.

27.17 CONNECTIONTRIGGER

Indicates when the interface will go up.

'''AlwaysOn''' : the connection will always be present;

'''OnDemand''' : the connection will be established automaticaly at the first frame that wants to go out;

Manual : the user will be asked before connect.

27.18 AUTODISCONNECTTIME

The network interface comes down after n seconds being connected.

Note: Not implemented, use _WANConnectionDevice_?_IdleDisconnectTime instead.

27.19 IDLEDISCONNECTTIME

Disconnect after n seconds of inactivity on the network interface.

27.20 AUTORECONNECTTIME

Reconnect automatically after a specified delay in seconds.

Works only when the parameter _WANConnectionDevice_?_ConnectionTrigger is 'OnDemand'. The link will reconnect automatically after _WANConnectionDevice_?_AutoReconnectTime seconds disconnected.

27.21 DNSENABLE

Set to use the DNS servers retrieved by the WAN interface.

The DNS servers retrieved through the DHCP client or PPP negotiation on this interface will be added to the global list of the CPE.

Note: The IAD maintains a global list of DNS servers that is used by the DNS forwarder for all Domain Name resolutions.

The first DNS server in the list is tried first. See also _Services_DnsForwarder.

27.22 DNSOVERRIDETR98

DNSOverrideAllowed parameter according to behavior of TR-098 specifications.

If set, the list of statically configured DNS servers specified in the parameter _WANConnectionDevice_?_DNSServers will be overridden by those retrieved during the DHCP or PPP negotiation.

Note: This parameter was created because the implementation of the parameter DNSOverrideAllowed was not conforming to the TR-098 specifications.

27.23 DNSOverrideAllowed

Use a static list of DNS servers.

If set, the list of DNS servers statically configured in the parameter _WANConnectionDevice_?_DNSServers will be used instead of those dynamically retrieved by the DHCP client or PPP negotiation.

Note: See also _WANConnectionDevice_?_DNSEnable and _Services_DnsForwarder.

27.24 DNSServers

Comma-separated list of DNS server IP addresses.

WANConnectionDevice?_DNSEnable and _WANConnectionDevice_?_DNSOverrideAllowed must also be set to 1. The DNS servers will be added to the global list of the DNS servers of the IAD.

Note: See also _WANConnectionDevice_?_DNSEnable, _WANConnectionDevice_?_DNSOverrideAllowed, and _Services_DnsForwarder.

27.25 PrivateDNSServers

Comma-separated list of domain name and associated DNS server IP addresses.

WANConnectionDevice?_DNSEnable and _WANConnectionDevice_?_DNSOverrideAllowed must also be set to 1. The DNS servers will be added to the global list of the DNS servers of the IAD and will only be used for a specific domain name.

Note: See also _WANConnectionDevice_?_DNSEnable, _WANConnectionDevice_?_DNSOverrideAllowed, and _Services_DnsForwarder.

27.26 AltDNSForwarder

Specifies the index of an alternate DNS forwarder for this WAN interface. The remote DNS servers retrieved on this interface will be used by the alternate DNS server. See description of _Services_AddDnsForwarder_?.

27.27 RouteProtocolRx

Unused

27.28 NATEnable

Enable Network Address/Port Translation (NATPT) on the WAN interface.

When using NATPT, all outgoing packets on the WAN interface will have their source IP address mangled to the IP address of the WAN interface.

Note: All devices connected to the LAN side can be reached from the WAN side with port mapping rules set in the table PortMapping

27.29 NATTimeout

Specify the persistence of UDP connection tracking entries in the NAT table.

The specific persistence timer will be used for streaming UDP and non streaming UDP with source port less than 8000.

Note: Default values is 180 seconds for streaming UDP and 30 seconds for non streaming UDP.

27.30 DMZEnable

Enable the DMZ feature (see also the parameter DMZ).

27.31 DMZ

IP address of the Demilitarized Zone (DMZ). See also _WANConnectionDevice_?_DMZEnable.

The DMZ works only when the WAN interface is configured for doing NAT (_WANConnectionDevice_?_NATEnable=1). The DMZ is the IP address of a device connected to the LAN interface.

Note: _WANConnectionDevice_?_DMZEnable should be set to activate the DMZ. All incoming packets that are not for a programmed port in the PortMapping table are redirected to this IP address.

27.32 PORTMAPPING

Array of objects describing port mapping rules when NAT is enabled on the interface.

A port mapping rule specifies to forward incoming packets in a range of UDP or TCP ports to an IP address on the LAN side.

27.32.1 ENABLE

When set, enables current port mapping.

27.32.2 REMOTEHOST

When specified, the port mapping rule will forward packets only if the source IP address is equal to this parameter.

27.32.3 EXTERNALPORT

Specifies a port or a range of ports or a list of ports/ports ranges to redirect.

Note: The format used for port range is a:b where ba.

27.32.4 INTERNALPORT

Specifies the target port of the redirection.

If a list or a range of port is specified in ExternalPort the whole range is translated to a range of ports starting at InternetlPort.

Note: If InternalPort is left empty there is no translation. The target ports are the same as the redirected ports.

27.32.5 PORTSURJECTION

Leave empty unless you want to redirect a whole range of ports to a unique target port.

All the ports specified in the range of ports defined in ExternalPort will be redirected to the unique port specified in PortSurjection.

27.32.6 PROTOCOL

Specify the type of packet (all is udp+tcp).

27.32.7 INTERNALCLIENT

Specifies the redirection target IP address (should be on a LAN subnet).

27.32.8 DESCRIPTION

Optional human-readable description of this port mapping.

27.33 FIREWALL

This object contains parameters for setting a simple firewall on this WAN interface.

The simple firewall protects the IAD from malicious incoming packets.

Note: More complex firewall rules can be set in the _Firewall_Rules_? table.

27.33.1 ENABLE

When set, activates the simple firewall on the WAN interface.

27.33.2 ATTACKDETECTION

Enables the detection and filtering of attacks such as ICMP flood, TCP SYN flood.

27.33.3 REMOTEPING

Allow/Disallow remote ping.

When set, the IAD will respond to incoming ICMP requests from this interface.

27.34 SERVICE_LIST

Comma-separated list of indexes of objects Services.

27.35 SERVICE

Array of objects describing rules to open a port or range of ports in the WAN interface firewall.

This table is effective only if _WANConnectionDevice_?_Firewall_Enable is set. We need to open a port or range of ports in the WAN interface firewall when there is a service in the IAD that listens to that port.

Note: You can also specify a port translation for the incoming packets (see RemotePort parameter).

27.35.1 ENABLE

Enable / Disable this table entry.

27.35.2 REMOTEPORT

You can redirect a remote port to a local port in the IAD.

Note: Exemple: _WANConnectionDevice_?_Service_?_RemotePort=2323, _WANConnectionDevice_?_Service_?_Port=23, _Services_Telnet_Enable=1. The telnet server is running in the box and can be accessed through the WAN interface on the port 2323.

27.35.3 PORT

Specify the port or range of ports to open in the WAN interface firewall.

Note: This port should corresponds to a service running in the IAD.

27.35.4 PROTOCOL

Specified the protocol associated to the port.

Note: For esp, ah the port is not needed

27.35.5 UNIQUEKEY

This string is used by the web interface to uniquely identify which service is programmed in the Service table.

For each table entry you specify a UniqueKey recognized by the web interface so it is able to enable / disable the remote access or change the port or port redirection.

27.36 STATUS

This object gathers information related to the current state of the WAN interface.

27.36.1 STATE

State of the WAN interface including PPP negotation stages.

27.36.2 UpTime

Seconds elapsed since network interface is up.

27.36.3 IPAddress

IP address of the WAN interface dynamically assigned or statically programmed.

27.36.4 SubnetMask

Subnet mask of the network interface dynamically retrieved or statically programmed.

Note: Subnet mask is 255.255.255.255 for a PPP connection

27.36.5 MACAddress

MAC address of the WAN interface dynamically assigned or statically programmed.

27.36.6 MTU

MTU of the WAN interface.

27.36.7 Remote

Left empty otherwise specifies the PPP server address for a PPP connection.

27.36.8 Gateways

List of gateways dynamically retrieved or statically programmed on the WAN interfaces.

27.36.9 DNSServers

List of DNS servers dynamically retrieved or statically programmed on the WAN interface.

27.36.10 RemoteDomainName

Domain name received from the DHCP exchange.

27.37 Counters

Counters of sent/received packets/bytes on the network interface.

27.37.1 RxPackets

Counter of received packets since initialization.

27.37.2 RxPacketsErrors

Counter of received packets in error since initialization.

27.37.3 RxPacketsDiscards

Counter of received packets discard since initialization.

27.37.4 TxPackets

Counter of transmitted packets since initialization.

27.37.5 TxPacketsErrors

Counter of transmitted packets in error since initialization.

27.37.6 TxPacketsDiscards

Counter of transmitted packets discard since initialization.

27.37.7 RxBytes

Counter of received bytes since initialization.

27.37.8 TxBytes

Counter of transmitted bytes since initialization.

28 LAYER3FORWARDING

Routing tables configuration.

For each IP packet crossing the box, Linux routing tables are inspected in the following order: '''local''' table which routes to local interface IP addresses and broadcasts, '''main''' table that routes to subnets associated to local interfaces, then tables associated to static source routing rules declared in _Layer3Forwarding_Forwarding_? then table named '''default''' is inspected. Default routes are stored in this last table.

Note: Routing tables of the Linux kernel can be inspected with the following shell commands:

```
# ip rule show
```

```
# ip route list table all
```

28.1 DEFAULTCONNECTIONSERVICE

Index of the object _WANConnectionDevice_? considered as the default route in the CPE.

A route to the associated network interface is automatically created in the table named '''default'''.

28.2 INTERNETCONNECTIONSERVICE

28.3 FORWARDING

This array of objects contains static source routing rules.

Source routing rules can be created to force some IP packets to be forwarded to specific network interfaces in the CPE. Routing can be done according to source and destination IP address of the packet or TOS value or a tag (mark) previously set by rules in _Firewall_Rules_? objects.

28.3.1 ENABLE

Set to 1 to activate this routing rule.

28.3.2 DESCRIPTION

A human readable description of the purpose of this rule.

28.3.3 USER

If set to 1, this routing rule can be displayed and modified by web User Interface.

If set to 0, this routing rule must be considered as a system route and should be hidden.

28.3.4 EXTERNAL

Set to 1 to specify a WAN interface, set to 0 to specify a LAN interface.

If set to 1, the parameter _Layer3Forwarding_Forwarding_?_Interface will be the index of an object _WANConnectionDevice_?. If set to 0, the parameter _Layer3Forwarding_Forwarding_?_Interface will be the index of an object _LANDevice_?.

28.3.5 INTERFACE

Specify the index of the object _WANConnectionDevice_? or _LANDevice_? according to parameter _Layer3Forwarding_Forwarding_?_External. The packet will be forwarded to the network interface associated with this object.

28.3.6 SOURCEIPADDRESS

Leave empty or specify a match in the source IP address of the packet.

This parameter is associated with _Layer3Forwarding_Forwarding_?_SourceSubnetMask.

28.3.7 SourceSubnetMask

Leave empty or specify a match in the subnet mask of the source IP address of the packet.

This parameter is associated with _Layer3Forwarding_Forwarding_?_SourceIPAddress.

28.3.8 DestIPAddress

Leave empty or specify a match in the destination IP address of the packet.

If empty or set to 0.0.0.0, the rule becomes a default route for the matched packet.

Note: This parameter is associated with _Layer3Forwarding_Forwarding_?_DestSubnetMask

28.3.9 DestSubnetMask

Leave empty or specify a match in the subnet mask of the destination IP address of the packet.

This parameter is associated with _Layer3Forwarding_Forwarding_?_DestIPAddress.

28.3.10 TOS

Leave empty or specify a match in the TOS value of the packet.

If left empty, no test is done.

28.3.11 Mark

Specify a match in the tag (mark) of the packet.

IP packets can be marked by a rule specified in _Firewall_Rules_?. The marking is a powerful feature of Linux kernel.

28.3.12 GatewayIPAddress

Leave empty or specify a gateway for this route.

The gateway must be in the subnet of the network interface defined by parameters _Layer3Forwarding_Forwarding_?_Interface and _Layer3Forwarding_Forwarding_?_External. If left empty the default gateway of the network interface is automatically used.

28.3.13 ForwardingMetric

We can specify a routing metric for this route (default is 1).

28.3.14 MTU

Specify an MTU (Maximum Transfer Unit) to apply to this route.

Default value is the MTU of the forwarding interface.

28.3.15 Table

Index of the new table to be created

Default value is the table default

28.3.16 TablePref

Priority of the table with the index Table

Default value is the default table pref

29 LAYER3ROUTING

Layer 3 (network services) routing management.

29.1 ENABLE

When set, enables the Layer 3 (network services) routing daemons.

29.2 BGP

BGP routing daemon management.

29.2.1 ENABLE

When set, enable the BGP routing daemon.

29.3 RIP

RIP routing daemon management.

29.3.1 ENABLE

When set, enable the RIP routing daemon.

29.4 RIPNG

RIP-ng routing daemon management.

29.4.1 ENABLE

When set, enable the RIP-ng routing daemon.

29.5 OSPF

OSPF routing daemon management.

29.5.1 ENABLE

When set, enable the OSPF routing daemon.

29.6 OSPF6

OSPF6 routing daemon management.

29.6.1 ENABLE

When set, enable the OSPF6 routing daemon.

30 LAYER2BRIDGING

This object contains parameters and information related to bridging capabilities of the CPE.

You can set-up and configure IGMP snooping on the bridge ports. You can set-up filter rules for network packets crossing the bridges.

Note: Each _LANDevice_? object is a bridge and includes physical ports.

A _WANConnectionDevice_? object can be a bridge if :

WANConnectionDevice?_PhysicalInterface_List or _WANConnectionDevice_?_PhysicalInterfaceV2_List contains several indexes.

Physical WAN bridge ports are directly included in the LAN bridge if

LANDevice?_HostConfig_AssociatedConnection points to the index of the WAN object.

30.1 ENABLE

Must be set to 1 to enable Layer2Briging features of the CPE.

Layer 2 bridging is based on linux ebtables (kernel bridge netfilter).

Dependency: Make menuconfig - User - Ebtables

Make menuconfig - Kernel - Networking - Netfilter - Bridge Netfilter

30.2 INPUTPOLICY

Specify the default terminating action of the '''Input''' chain.

The policy '''Accept''' will definitely accept the packet if no filter rule matches the packet. The policy '''Drop''' will discard the packet if no filter rule matches it.

30.3 OUTPUTPOLICY

Specify the default terminating action of the '''Output''' chain.

The policy '''Accept''' will definitely accept the packet if no filter rule matches the packet. The policy '''Drop''' will discard the packet if no filter rule matches it.

30.4 FORWARDPOLICY

Specify the default terminating action of the '''Forward''' chain.

The policy '''Accept''' will definitely accept the packet if no filter rule matches the packet. The policy '''Drop''' will discard the packet if no filter rule matches it.

30.5 HACKDHCPSTB

If not 0, activates a hack which detects miss-behaved Set-Top-Box during reboot. This parameter is the index of a _LANDevice_? object on which bridge the Set-Top-Box is detected.

Some Set-Top-Box do not detect the Ethernet link drop and do not send a DHCP request after a reboot of the CPE. So layer 2 filter rules that use the DHCP option as a matching parameter cannot work. To overcome this issue the layer 2 DHCP option detection module also recognizes IGMP report from an IP address not in the LAN subnet as a packet coming from the Set-Top-Box. It adds the MAC address of the source in the list of matching MAC addresses for the first declared filter rule with a DHCP option matching parameter.

30.6 FILTER_LIST

Comma-separated list of indexes of objects _Layer2Bridging_Filter_?.

30.7 FILTER

Array of bridge filter rules.

Bridge filter rules include matching on input or output network interface, matching on source and destination MAC and IP addresses or MAC addresses of selected hosts with DHCP options, matching on IP protocol. A rule can '''accept''' or '''drop''' or '''mark''' the matched packet.

Dependency: Bridge netfilter modules must be included in the kernel (ebtables with filter table, IP and DHCP Vendor CLass filters, mark and classify targets, log support). Ebtables user space utility is needed.

30.7.1 Enable

Set to 1 to activate / build the rule.

30.7.2 Description

Human readable description of the rule.

30.7.3 Input

Leave blank or specify the index of a network interface object.

This parameter allow to specify a match in the physical network interface from which the packet is entering the box. This parameter associated with _Layer2Bridging_Filter_?_InputType, _Layer2Bridging_Filter_?_InputNot and _Layer2Bridging_Filter_?_InputVlanNumber specifies the input physical interface.

30.7.4 InputType

Type of the incoming physical network interface.

See _Layer2Bridging_Filter_?_Input for a full description of the incoming interface match.

30.7.5 InputVlanNumber

This parameter is part of the specification of the incoming interface match.

Leave blank or specify the index of an object _LANEthernetInterface_?_VLANInterface_?

30.7.6 InputNot

If set to 1, the match of incoming network interface is inverted.

30.7.7 Output

Leave blank or specify the index of a network interface object.

This parameter allow to specify a match in the physical network interface from which the packet is leaving the box. This parameter associated with _Layer2Bridging_Filter_?_OutputType, _Layer2Bridging_Filter_?_OutputNot and _Layer2Bridging_Filter_?_OutputVlanNumber specifies the outgoing physical interface.

30.7.8 OutputType

Type of the outgoing physical network interface.

See _Layer2Bridging_Filter_?_Output for a full description of the outgoing interface match.

30.7.9 OutputVlanNumber

This parameter is part of the specification of the outgoing interface match.

Leave blank or specify the index of an object _LANEthernetInterface_?_VLANInterface_?

30.7.10 OutputNot

If set to 1, the match in outgoing network interface is inverted.

30.7.11 SrcMac

Specify a match in the source MAC address of the packet.

A match is detected if the source MAC address of the packet anded with _Layer2Bridging_Filter_?_SrcMask is equal to _Layer2Bridging_Filter_?_SrcMac. If _Layer2Bridging_Filter_?_SrcNot is set to 1 the match is inverted.

30.7.12 SrcMask

Specify a match in the source MAC address of the packet.

A match is detected if the source MAC address of the packet anded with _Layer2Bridging_Filter_?_SrcMask is equal to _Layer2Bridging_Filter_?_SrcMac. If _Layer2Bridging_Filter_?_SrcNot is set to 1 the match is inverted.

30.7.13 SrcNot

Specify a match in the source MAC address of the packet.

A match is detected if the source MAC address of the packet anded with _Layer2Bridging_Filter_?_SrcMask is equal to _Layer2Bridging_Filter_?_SrcMac. If _Layer2Bridging_Filter_?_SrcNot is set to 1 the match is inverted.

30.7.14 DstMac

Specify a match in the destination MAC address of the packet.

A match is detected if the destination MAC address of the packet anded with _Layer2Bridging_Filter_?_DstMask is equal to _Layer2Bridging_Filter_?_DstMac. If _Layer2Bridging_Filter_?_DstNot is set to 1 the match is inverted.

30.7.15 DstMask

Specify a match in the destination MAC address of the packet.

A match is detected if the destination MAC address of the packet anded with _Layer2Bridging_Filter_?_DstMask is equal to _Layer2Bridging_Filter_?_DstMac. If _Layer2Bridging_Filter_?_DstNot is set to 1 the match is inverted.

30.7.16 DstNot

Specify a match in the destination MAC address of the packet.

A match is detected if the destination MAC address of the packet anded with _Layer2Bridging_Filter_?_DstMask is equal to _Layer2Bridging_Filter_?_DstMac. If _Layer2Bridging_Filter_?_DstNot is set to 1 the match is inverted.

30.7.17 SrcIP

Specify a match in the source IP address of the packet.

A match is detected if the source IP address of the packet is in the subnet specified by _Layer2Bridging_Filter_?_SrcIP and _Layer2Bridging_Filter_?_SrcIPMask . If _Layer2Bridging_Filter_?_SrcIPNot is set to 1 the match is inverted.

30.7.18 SrcIPMask

Specify a match in the source IP address of the packet.

A match is detected if the source IP address of the packet is in the subnet specified by _Layer2Bridging_Filter_?_SrcIP and _Layer2Bridging_Filter_?_SrcIPMask . If _Layer2Bridging_Filter_?_SrcIPNot is set to 1 the match is inverted.

30.7.19 SrcIPNot

Specify a match in the source IP address of the packet.

A match is detected if the source IP address of the packet is in the subnet specified by _Layer2Bridging_Filter_?_SrcIP and _Layer2Bridging_Filter_?_SrcIPMask . If _Layer2Bridging_Filter_?_SrcIPNot is set to 1 the match is inverted.

30.7.20 DstIP

Specify a match in the destination IP address of the packet.

A match is detected if the destination IP address of the packet is in the subnet specified by _Layer2Bridging_Filter_?_DstIP and _Layer2Bridging_Filter_?_DstIPMask . If _Layer2Bridging_Filter_?_DstIPNot is set to 1 the match is inverted.

30.7.21 DstIPMask

Specify a match in the destination IP address of the packet.

A match is detected if the destination IP address of the packet is in the subnet specified by _Layer2Bridging_Filter_?_DstIP and _Layer2Bridging_Filter_?_DstIPMask . If _Layer2Bridging_Filter_?_DstIPNot is set to 1 the match is inverted.

30.7.22 DstIPNot

Specify a match in the destination IP address of the packet.

A match is detected if the destination IP address of the packet is in the subnet specified by _Layer2Bridging_Filter_?_DstIP and _Layer2Bridging_Filter_?_DstIPMask. If _Layer2Bridging_Filter_?_DstIPNot is set to 1 the match is inverted.

30.7.23 SrcOpt

Specify a match in the source MAC address of the packet.

A match is detected if the source MAC address of the packet has been detected previously as the source MAC address of a DHCP request including a specified DHCP option. The match is inverted if _Layer2Bridging_Filter_?_SrcOptNot is set to 1. The DHCP option type and value are given in _Layer2Bridging_Filter_?_SrcOptType and _Layer2Bridging_Filter_?_SrcOpt.

Note: The type of the DHCP option is specified in _Layer2Bridging_Filter_?_SrcOptType. DHCP options supported are Vendor Class (60), User Class (77), Vendor-Identifying Vendor (124), Vendor-Identifying Vendor-Specific (125). The value of the DHCP option is compared with one of the strings given in _Layer2Bridging_Filter_?_SrcOpt. _Layer2Bridging_Filter_?_SrcOpt may contain several strings separated by ; characters. A wildcard can be used (character *) in the comparison of the strings. The wildcard allow a partial match at the beginning or at the end of the string.

30.7.24 SrcOptType

Specify a match in the source MAC address of the packet.

See _Layer2Bridging_Filter_?_SrcOpt for a full description of the DHCP option and MAC address match.

30.7.25 SrcOptNot

Specify a match in the source MAC address of the packet.

See _Layer2Bridging_Filter_?_SrcOpt for a full description of the DHCP option and MAC address match.

30.7.26 DstOpt

Specify a match in the destination MAC address of the packet.

A match is detected if the destination MAC address of the packet has been detected previously as the source MAC address of a DHCP request including a specified DHCP option. The match is inverted if _Layer2Bridging_Filter_?_DstOptNot is set to 1. The DHCP option type and value are given in _Layer2Bridging_Filter_?_DstOptType and _Layer2Bridging_Filter_?_DstOpt.

Note: The type of the DHCP option is specified in _Layer2Bridging_Filter_?_DstOptType. DHCP options supported are Vendor Class (60), User Class (77), Vendor-Identifying Vendor (124), Vendor-Identifying Vendor-Specific (125). The value of the DHCP option is compared with one of the strings given in _Layer2Bridging_Filter_?_DstOpt. _Layer2Bridging_Filter_?_DstOpt may contain several strings separated by ; characters. A wildcard can be used (character *) in the comparison of the strings. The wildcard allow a partial match at the beginning or at the end of the string.

30.7.27 DstOptType

Specify a match in the destination MAC address of the packet.

See _Layer2Bridging_Filter_?_DstOpt for a full description of the DHCP option and MAC address match.

30.7.28 DstOptNot

Specify a match in the destination MAC address of the packet.

See _Layer2Bridging_Filter_?_DstOpt for a full description of the DHCP option and MAC address match.

30.7.29 Log

Will produce a trace of matched packets in the syslog.

30.7.30 Proto

Leave blank or specify a match in the Ethertype field of the frame.

30.7.31 ProtoNot

If set to 1, the match in Ethertype field is inverted.

30.7.32 IPProto

Leave blank or specify a match in the IP protocol field of the packet.

30.7.33 IPProtoNot

If set to 1, the match in IP protocol field is inverted.

30.7.34 AddMatch

Allow to enter any additional ebtables match

Note: See ebtables manpage for details

30.7.35 SetMark

The matching packet will be marked (tagged) with the value specified in this parameter.

The mark can be tested by rules specified in _Firewall_Rules_?. The packet will continue to cross the chain. Next rule in the chain will be applied to the matched packet.

30.7.36 SetClass

Leave blank or modify the Linux priority of the matching packet.

The Linux priority is used by the queuing processing. All output network interfaces have several queues with a different scheduling priority and the packets are queued according to their Linux priority.

Note: A value of 15 specifies the greatest level of priority.

30.7.37 Chain

Specify the chain in which the rule is built.

'''Input''' chain is crossed by packets whose final destination is the CPE. '''Output''' chain is crossed by packets generated by the CPE and leaving the CPE through one output network interface. '''Forward''' chain is crossed by packets entering the CPE by one network interface and leaving the CPE through another network interface.

30.7.38 Target

Specify the action to take on the matched packet.

'''Drop''' will discard the packet. '''Accept''' will leave the chain definitely retaining the packet. '''Continue''' will let the next rules in the chain inspecting the packet.

30.7.39 OtherTarget

Allow to enter any other ebtables target

Note: See ebtables manpage for details

30.8 IGMPSnooping

This object gathers information related to the software IGMP snooping module of the box.

30.8.1 Enable

Enable the IGMP snooping mechanism to operate on the network interfaces included in the software bridges of the box.

The IGMP snooping mechanism allows to forward multicast packets only to network interfaces where IGMP Reports have been detected for the corresponding multicast group.

30.8.2 Output_List

Comma-separated list of _Layer2Bridging_IGMPSnooping_Output_? objects.

30.8.3 Output

Array of network interface objects.

This parameter allows to specify network interfaces where IGMP Reports must be forwarded. If left blank the IGMP Reports are fowarded to the network interfaces where an IGMP router is detected. The IGMP router is detected by the presence of IGMP Queries.

- Index

Index of the network interface object.

- Type

Type of the network interface object.

30.8.4 Exclude_List

Comma-separated list of _Layer2Bridging_IGMPSnooping_Exclude_? objects.

30.8.5 Exclude

Array of network interface objects.

This parameter allow to specify the network interface excluded from the software IGMP snooping mechanism. You must exclude from the IGMP snooping mechanism the network interface where an hardware Ethernet Switch is connected.

Note: The IGMP snooping mechanism of the hardware Ethernet Switch cannot operate properly if the software IGMP snooping mechanism operates on the network interface where it is connected.

- Index

Index of the network interface object.

- Type

Type of the network interface object.

31 VOICE

The top-level object for VoIP CPE.

Dependency: {{{VoIP applications ---

&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;[*] Asterisk PBX v 1.2.x

&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;[*] VOIP firmware}}}

31.1 ENABLE

Enables or disables VoIP.

31.2 DEBUG

Set the level of the debugging trace messages (higher is more verbose).

31.3 REGION

The geographic region associated with this profile. This is used by the CPE to customize localization settings.

31.4 WANINTERFACE

The number of the WAN interface used by VoIP, or 0 to bind to any interface.

Note: The script {{{/etc/init.d/host}}} uses this information to put the IP address of the wan interface in {{{/etc/config/hosts}}} as the name "iad_voip_host". If "iad_voip_host" exists, VoIP will bind to this address.

31.5 SIP

Global Voice profile parameters that are specific to SIP user agents.

Dependency: {{{VoIP applications ---

&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;[*] SIP support}}}

31.5.1 USERAGENTPORT

Port used for incoming call control signaling.

31.5.2 REGISTRATIONPERIOD

Period over which the user agent must periodically register, in seconds.

31.5.3 DSCPMARK

Diffserv code point to be used for outgoing SIP signaling packets.

31.5.4 USERAGENT

User-Agent SIP header in SIP signalling packets.

31.6 MGCP

Global Voice profile parameters that are specific to MGCP call signaling.

Dependency: {{{VoIP applications ---

&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;[*] MGCP UA support}}}

31.6.1 LOCALPORT

Port listening for incoming call control signaling.

31.6.2 DSCPMARK

Diffserv code point to be used for outgoing MGCP signaling packets.

31.7 H323

Global Voice profile parameters that are specific to H.323 call signaling.

Dependency: {{{VoIP applications ---

[*] H.323 support}}}

31.7.1 DebugLevel

Debug Level for H.323 (0 - no debug, 6 - max debug).

Note: Can also be set with '{{{asterisk -r -x "ooh323 debug DEBUGLEVEL"}}}'.

31.7.2 Gatekeeper

Host name or IP address of H.323 Gatekeeper.

Note: Only IP address allowed for the moment.

31.7.3 GatekeeperPort

Destination port to be used in connecting to the H.323 Gatekeeper.

31.7.4 GatekeeperID

Gatekeeper ID.

Note: The Gatekeeper ID may consist of id and password where the passwords starts with '$'.

31.7.5 AltGatekeeper

Host name or IP address of H.323 Alternate Gatekeeper.

Note: Only IP address allowed for the moment.

31.7.6 AltGatekeeperPort

Destination port to be used in connecting to the H.323 Alternate Gatekeeper.

31.7.7 AltGatekeeperID

Alternate Gatekeeper ID.

31.7.8 LocalPort

Port listening for incoming call control signaling.

31.7.9 LocalRASPort

Port listening for incoming RAS signaling.

31.7.10 DSCPMark

Diffserv code point to be used for outgoing H.323 signaling packets.

31.7.11 FastStart

When set, supports H323 fast start.

31.7.12 H245Tunnelling

When set, supports H245 tunnelling.

31.7.13 TimeToLive

In seconds, defines the TimeToLive specification in the registration with the Gatekeeper.

31.8 RTP

Global Voice profile parameters related to the voice stream sent via RTP.

31.8.1 LocalPortMin

Base of port range to be used for incoming RTP streams for this profile.

31.8.2 LocalPortMax

Top of port range to be used for incoming RTP streams for this profile.

31.8.3 DSCPMark

Diffserv code point to be used for outgoing RTP packets for this profile.

31.8.4 TelephoneEventPayloadType

31.8.5 RTCP

Voice profile parameters related to RTCP. .

- Enable

Enable or disable RTCP.

- TxRepeatInterval

Transmission repeat interval, in milliseconds.

- LocalCName

Local Cname (canonical name).

31.9 FaxT38

T.38 Fax information for devices that support T.38 relay.

31.9.1 Enable

Enable or disable the use of T.38.

31.9.2 BitRate

Maximum data rate for fax.

31.9.3 HighSpeedPacketRate

The rate at which high speed data wiacross the network, in milliseconds.

Note: Not used.

31.9.4 HighSpeedRedundancy

Specifies the packet-level redundancy for highspeed data transmissions (i.e., T.4 image data). The value MUST be in the range 0 through 3.

31.9.5 LowSpeedRedundancy

Specifies the packet-level redundancy for lowspeed data transmissions (i.e., T.30 handshaking information). The value MUST be in the range 0 through 5.

31.9.6 TCFMethod

The method with which data is handled over the network. Enumeration of: Local Network.

31.10 NumberingPlan

This object contains information related to the global numbering plan.

31.10.1 PSTNFailOver

Specifies whether or not the CPE SHOULD fail over to PSTN service, if available, on loss of connectivity to the VoIP service.

This parameter is appropriate only in implementations in which PSTN fail-over is possible.

31.10.2 InterDigitTimerStd

This timer is the maximum allowable time (expressed in milliseconds) between the dialing of digits.

This timer is restarted every time a digit is dialed. Expiration of this timer indicates "End of Dialing".

31.10.3 InterDigitTimerOpen

This timer is the maximum allowable time (expressed in milliseconds) between the dialing of digits once the minimum number of digits defined on a prefix based has been reached.

This timer is only applicable to "open numbering", where the exact number of digits for a prefix is not known.

31.10.4 EmergencyNumbers

This is a list of numbers that should use the PSTN service, regardless of other numbering plans.

31.10.5 EchoNumber

This number is used to echo back the voice for test purposes.

31.10.6 TestNumber

This number is used to echo back the voice for test purposes.

31.10.7 DomoNumber

This number is used for Domotic services.

Dependency: VoIP applications --- [*] Domotic sounds

31.10.8 PSTNSwitchOver

This number is used to force the use of the PSTN service on this outgoing call.

31.11 Capabilities

The overall capabilities of the VoIP CPE.

31.11.1 EnableSupplementaryServices

This is used to enable the use of supplementary services. If set, the CPU will handle the supplementary services.

31.11.2 RingDuration

Maximum duration of the ring on the FXS ports.

31.11.3 EnableCallWaiting

This is used to enable call waiting feature (signal an incoming call if busy).

31.11.4 DoNotSendCallerID

When set to True, the Caller ID is not sent.

31.11.5 RejectAnonymousCall

Set to True to reject incoming calls without Caller ID.

31.11.6 DenyCallForward

set this to reject an already forwarded call.

31.11.7 VoiceMailFunction

Set to None do disable VoiceMail.

Set to Direct to forward incoming calls to VoiceMail.

Set to Busy, Noanswer, BusyNoanswer to forward incoming calls to VoiceMail on busy and/or no answer.

Dependency: VoIP applications --- [*] VoiceMail support [*] English sounds [*] French sounds

31.11.8 VoiceMailDir

The directory used to store VoiceMail messages.

31.11.9 VoiceMailFormat

Format to store VoiceMail messages.

31.11.10 CallForwardDirect

Forward the incoming call directly to this number.

31.11.11 CallForwardBusy

Forward the incoming call if busy to this number.

31.11.12 CallForwardNoAnswer

Forward the incoming call if no answer to this number.

31.12 FeatureCodes

Supplementary services feature codes.

Ignored if _Voice_Capabilities_EnableSupplementaryServices not set.

To turn a feature on, dial '*code*'.

To turn a feature off, dial '#code#'.

To test if a feature is enabled, dial '*#code#'.

31.12.1 BlindTransfer

The call is forwarded without checking if forwarded call has answered.

31.12.2 AttendedTransfer

The call is forwarded when the forwarded call has answered.

31.12.3 RecallLastCaller

Code to recall last caller.

31.12.4 EnableCallerID

Prefix to enable the sending of the Caller ID for a given call.

31.12.5 DisableCallerID

Prefix to disable the sending of the Caller ID for a given call.

31.12.6 RejectAnonymousCall

Code to reject anonymous call (without Caller ID).

31.12.7 DoNotDisturb

Code to disable ringing.

31.12.8 DenyCallForward

Code to deny forwarding of the call.

31.12.9 AbsentSubscriber

NA

Note: Not implemented.

31.12.10 DoNotSendCallerID

Code to disable the sending of the Caller ID for all calls.

31.12.11 CallWaiting

Code to set the call waiting feature (indicate incoming call by call waiting tone).

31.12.12 CallForwardDirect

Code to forward the call directly to CallForwardDirect.

31.12.13 CallForwardBusy

Code to forward the call if busy to CallForwardBusy.

31.12.14 CallForwardNoAnswer

Code to forward the call if no answer to CallForwardNoAnswer.

31.12.15 VoiceMailSet

Code to set VoiceMail on or off.

31.12.16 VoiceMailRead

Code to read the VoiceMail.

31.12.17 VoiceMailPassword

Password for reading the VoiceMail.

31.12.18 RemoteDialPassword

Password for remote dialing.

31.13 Announcements

The announcement is played if the dial status matches.

31.13.1 DialStatus

Dial status string. The dial status can be 'CHANUNAVAIL','CONGESTION','NOANSWER','BUSY','ANSWER','CANCEL'.

31.13.2 SoundFile

Sound file to play if the status returned when dialing matched the DialStatus string. The sound file should be in 'gsm' or 'wav' format.

31.14 AllowFXSReinjection

Specifies if the FXS should be reinjected to the FXO port, so the telephones on the POTS side still works.

32 SIPPHONE

Object associated with a SIP phone.

32.1 ENABLE

When set, enables current SIP phone.

32.2 DESCRIPTION

A description of the SIP Phone

32.3 SIGNALINGPROTOCOL

The protocol to be used for this profile.

Note: Always SIPLocal

32.4 EXTENSION

The phone extension associated with this SIP phone.

32.5 AUTHUSERNAME

Username used to authenticate the connection to the server.

32.6 AUTHPASSWORD

Password used to authenticate the connection to the server.

32.7 DTMFMETHOD

Method by which DTMF digits MUST be passed.

32.8 STATUS

Is the SIPPhone registered ?

32.9 LINE

Object associated with a distinct SIP phone.

32.9.1 CODEC

Table to describe the set of codecs enabled for use with this line. Each entry in this table refers to a distinct combination of codec and bit rate.

- Codec

Bit rate, in bits per second.

- BitRate

Bit rate, in bits per second.

Note: Ignored, always 64000.

- PacketizationPeriod

Packetization period, in milliseconds.

- SilenceSuppression

Indicates support for silence suppression for this codec.

If silence suppression is supported, it can be disabled for this codec/bit-rate by setting this parameter to false.

- Enable

When set, use of this combination of codec parameters.

- Priority

Indicates the priority for this combination of parameters, where 1 is the highest priority.

Where the priority differs between entries in this table, the CPE SHOULD use the highest priority (lowest numbered) entry among those supported by the remote endpoint and consistent with the available bandwidth. Where the priorities are equal among multiple entries, the CPE MAY apply a local criterion for choosing among them.

32.10 RING

Ring a registered SIPPhone.Set the ring duration in seconds.

33 VOICEPROFILE

Voice line specific settings.

Dependency: {{{VoIP applications ---

&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;[*] Asterisk PBX v 1.2.x

&amp;nbsp;&amp;nbsp;&amp;nbsp;&amp;nbsp;[*] VOIP firmware}}}

33.1 ENABLE

Enables or disables all lines in this profile.

33.2 NAME

Human-readable string to identify the profile instance.

33.3 SIGNALINGPROTOCOL

The protocol to be used for this profile.

Dependency: VoIP applications --- [*] SIP support [*] MGCP UA support [*] H.323 support

33.4 DTMFMETHOD

Method by which DTMF digits MUST be passed.

33.5 FAXPASSTHROUGH

Specifies the behavior of the CPE for passthrough of fax data.

Note: Ignored.

33.6 MODEMPASSTHROUGH

Specifies the behavior of the CPE for passthrough of modem data.

33.7 DIGITMAP

Digit map controlling the transmission of dialed digit information.

The string defines the criteria to be met as digits are collected before an outgoing request (e.g., a SIP INVITE) can be initiated.The syntax of this parameter is exactly the syntax used by MGCP as defined in [5], section 2.1.5.This parameter is applicable only if the device supports a dialing mechanism for which a dialing plan is needed (for example, a device with an explicit Dial button may not need to be aware of the dialing plan) and if the device does not already support a dialing plan mechanism for this profile (e.g., in-band via MGCP).

33.8 DIGITMAPENABLE

Enables the use of the DigitMap parameter in this object.

Note: This parameter is required if and only if both the DigitMap parameter in this object and the VoiceService.{i}.VoiceProfile.{i}.NumberingPlan object are present.

33.9 SIP

Voice profile parameters that are specific to SIP user agents.

33.9.1 PROXYSERVER

Host name or IP address of the SIP proxy server.

All SIP signaling traffic are sent to the host indicated by this parameter and the port indicated by the _VoiceProfile_?_SIP_ProxyServerPort parameter unless _VoiceProfile_?_SIP_OutboundProxy parameter is non-empty or a different route was discovered during normal operations SIP routing operation. Regardless of which host the traffic gets sent to (the _VoiceProfile_?_SIP_ProxyServer or the _VoiceProfile_?_SIP_OutboundProxy), the value of this parameter is used to derive the URI placed into the

SIP Route header field of all requests originated by this end-point unless a different proxy host was discovered dynamically during normal SIP routing operations.

33.9.2 ProxyServerPort

Destination port to be used in connecting to the SIP server.

33.9.3 RegistrarServer

Host name or IP address of the SIP registrar server.

If this parameter is empty, the CPE obtains all of the registrar server configuration information, including host name or IP address, port, and transport protocol, from the corresponding _VoiceProfile_?_SIP_ProxyServer parameters (_VoiceProfile_?_SIP_ProxyServer, _VoiceProfile_?_SIP_ProxyServerPort, and _VoiceProfile_?_SIP_ProxyServerTransport), ignoring all of the registrar server parameters (_VoiceProfile_?_SIP_RegistrarServer, _VoiceProfile_?_SIP_RegistrarServerPort and _VoiceProfile_?_SIP_RegistrarServerTransport).

33.9.4 RegistrarServerPort

Destination port to be used in connecting to the SIP registrar server.

33.9.5 UserAgentDomain

CPE domain string. If empty, the CPE uses its IP address as the domain.

33.9.6 OutboundProxy

Host name or IP address of the outbound proxy. If a non-empty value is specified, the SIP endpoint send all SIP traffic (requests and responses) to the host indicated by this parameter and the port indicated by the OutboundProxyPort parameter. This is done regardless of the routes discovered using normal SIP operations, including use of Route headers initialized from Service-Route and Record-Route headers previously received. The OutboundProxy value is NOT used to generate the URI placed into the Route header of any requests.

33.9.7 OutboundProxyPort

Destination port to be used in connecting to the outbound proxy. This parameter is ignored unless the value of the OutboundProxy parameter in this object is non-empty.

33.9.8 AuthUserName

Username used to authenticate the connection to the server.

33.9.9 AuthPassword

Password used to authenticate the connection to the server.

33.9.10 URI

URI by which the user agent will identify itself for this line.

If empty, the actual URI used in the SIP signaling is automatically formed by the CPE as: 'sip:UserName@Domain' Where UserName is username given for this line (_VoiceProfile_?_SIP_AuthUserName), and Domain is the domain given for this profile (_VoiceProfile_?_SIP_UserAgentDomain). If this domain parameter is empty, then the IP address of the CPE is used for the domain. If URI is non-empty, but is a SIP or SIPS URI that contains no '@' character, then the actual URI used in the SIP signaling is automatically formed by the CPE by appending this parameter with an '@' character followed by the domain given for this profile (_VoiceProfile_?_SIP_UserAgentDomain). If this domain parameter is empty, then the IP address of the CPE is used for the domain.

33.9.11 UseCodecPriorityInSDPResponse

33.9.12 EventSubscribe_List

List of Event Subscriptions.

33.9.13 EventSubscribe

Table to specify the SIP events to which the CPE subscribes.

Dependency: VoIP applications --- [*] SUBSCRIBE/NOTIFY MWI support

- Event

SIP event name to appear in the EVENT header of the SIP SUBSCRIBE request.

Note: Only 'message-summary' supported for now.

- Notifier

Host name or IP address of the event notify server.

- NotifierPort

Destination port to be used in connecting to the event notifier.

- ExpireTime

Subscription refresh timer, in seconds.

33.9.14 Status

Shows SIP status (registered,failed,...).

33.9.15 TimerT1

Value of SIP timer T1, in milliseconds, as defined in RFC 3261.

33.10MGCP

Voice profile parameters that are specific to MGCP call signaling.

Dependency: VoIP applications --- [*] MGCP UA support

33.10.1 CallAgent1

Host name or IP address of the main MGCP call agent.

33.10.2 CallAgentPort1

Destination port to be used in connecting with the main MGCP call agent.

33.10.3 CallAgent2

Host name or IP address of the backup MGCP call agent.

33.10.4 CallAgentPort2

Destination port to be used in connecting with the backup MGCP call agent.

33.10.5 RetranIntervalTimer

Message retransmit interval, in seconds.

33.10.6 MaxRetranCount

Max number of message retransmissions.

33.10.7 MaxRestartDelay

Maximum delay before sending a new RSIP if register failed.

33.10.8 RegisterMode

Register mode.

Note: Not used.

33.10.9 Domain

CPE domain string. If empty, the CPE uses its IP address.

Note: Not used.

33.10.10 User

User string used in accessing the call agent.

Note: If empty, the CPE will use its IP address between square brackets ([x.x.x.x]) as the user string.

33.10.11 AllowPiggybackEvents

Indicates whether or not piggyback events are allowed to the MGCP call agent.

33.10.12 SendRSIPImmediately

Indicates whether or not to send RSIP immediately on restart.

Note: if not set, the RSIP will be sent at a random delay between 0 and MaxWaitingDelay seconds after restart.

33.10.13 MaxWaitingDelay

When a gateway is powered on, it MUST initiate a restart timer to a random value, uniformly distributed between 0 and a maximum waiting delay (MWD).

Note: Ignored if SendRSIPImmediately is true.

33.10.14 LineName

Used to identify the line when using MGCP signaling. If empty, the CPE uses the default names 'aaln/1', etc.

33.10.15 NCSEnabled

If enabled, the CPE will inidcate support for NCS 1.0 as well as MGCP 1.0 in the version string.

33.10.16 MaxKeepAliveDelay

If different from zero, the CPE will send RSIP to the Call Agent if no AUEP or 200 response received within MaxKeepAliveDelay seconds.

Note: As a configurable option, the RSIP can be sent with X-keepalive as the restart method.

33.10.17 RSIPTimeouts

A comma separated list of timeouts in seconds that will be used to provide a delay between RSIP's if register failed. The timeout is clamped to the latest timeout in the list. Normally used to provide exponential backoff in order to avoid overloading the Call Agent.

Note: Replaces MaxRestartDelay if not empty.

33.10.18 STATUS

Shows MGCP status (registered,failed,...).

33.11 H323

Voice line parameters that are specific to H.323 call signaling.

33.11.1 H323ID

The H323ID assigned to the line.

Note: The H323ID may be appended by a password separated with a '$'.

33.11.2 EMAILID

The email id assigned to the line.

33.11.3 URLID

The URL id assigned to the line.

33.11.4 E164ADDRESS

The E.164 number assigned to the line.

33.11.5 STATUS

shows H.323 Gatekeeper status (registered,failed,...).

33.12 NUMBERINGPLAN

This object contains information related the numbering plan.

33.12.1 FXSLISTIN

A comma separated list of FXS indexes that will ring on incoming calls for this voice profile.

Note: See objects FXSInterface in config FXSInterface.

33.12.2 FXSLISTOUT

A comma separated list of FXS indexes that are allowed to make outgoing calls for this voice profile.

33.12.3 LOCALLISTIN

A comma separated list of SIPPhone indexes that will ring on incoming calls for this voice profile.

Note: See SIPPhone list in config.

33.12.4 LOCALLISTOUT

A comma separated list of SIPPhone indexes that are allowed to make outgoing calls for this voice profile.

33.12.5 MINIMUMNUMBEROFDIGITS

This is the minimum number of digits that must be collected before an outgoing request (e.g., a SIP INVITE) can be initiated. If "End of Dialing" (refer to the definition of the InterDigitTimer) occurs before the minimum number of digits has been reached then the number will be considered incomplete and no request will be initiated. In practice, searching the "PrefixInfo" list should only commence once the minimum number of digits (as specified by this parameter) has been received.

33.12.6 MaximumNumberOfDigits

This is the maximum number of digits that may be collected before an outgoing request (e.g., a SIP INVITE) is initiated. Any additional dialed digits will be ignored. This parameter is only used in the case that no match in the \"PrefixInfo\" list has been found.

33.12.7 RemoteDialAllowed

If enabled, remote dialing is allowed.

33.12.8 PrefixInfo

Each entry in this table contains information related to an individual prefix in the numbering plan. It is anticipated that once the minimum number of digits has been received, the VoIP device will search this prefix list every time a new digit is received. If no new entry is found, then the object that was previously found will be used instead.

- PrefixRange

This is a string representation of a range of prefixes. Each prefix consists of a "From" part consisting of 1 to n digits (string representation) followed by an optional "To" part consisting of exactly one digit prefixed by a "-" symbol. It should be noted that only the characters "0-9", "*": and "#" can be used to represent the "From" and "To" parts of the prefix range. A further constraint is that the "To" digit MUST always be numerically greater than the last digit of the "From" part. Examples: 02 031-5 032 0325 *#34 #22.

- PrefixMinNumberOfDigits

This is the minimum number of allowable digits for the prefix range. Once the minimum number of digits has been reached, the \"InterDigitTimerOpen\" will be used instead of the \"InterDigitTimerStd\". If the minimum number of digits has been reached and the inter-digit timer expires, an outgoing request is initiated.

- PrefixMaxNumberOfDigits

This is the maximum number of allowable digits for the prefix range. Once the number of digits received reaches this value an outgoing request is initiated.

- NumberOfDigitsToRemove

If this parameter has a non-zero value, the specified number of digits will be removed from the beginning of the dialed digits before the outgoing call request.

Note: Not the same as in TR-104.

- PrefixInsert

If not empty, these digits will be inserted before the dialed digits before the outgoing call request is initiated.

- PrefixAppend

If not empty, these digits will be inserted after the dialed digits before the outgoing call request is initiated.

33.13 Line

Object associated with a distinct voice line.

33.13.1 DirectoryNumber

Directory number associated with this line.

May be used to identify the line to the user. In case of H.323 signaling, this MUST be an E.164 number.

33.13.2 CallingFeatures

Voice line parameters related to optional endpoint based calling features.

- CallerIDName

String used to identify the caller.

33.13.3 VOICEPROCESSING

Voice line parameters related to voice processing capabilities.

- TransmitGain

Gain in units of 0.1 dB to apply to the transmitted voice signal prior to encoding. This gain is a modifier of the default transmit-gain, which is unspecified.

- ReceiveGain

Gain in units of 0.1 dB to apply to the received voice signal after decoding. This gain is a modifier of the default receive-gain, which is unspecified.

- EchoCancellationEnable

Enable or disable echo cancellation for this line.

33.13.4 CODEC

Table to describe the set of codecs enabled for use with this line.

Each entry in this table refers to a distinct combination of codec and bit rate.

- Codec

Identifier of the codec type.

- BitRate

Bit rate, in bits per second.

Note: Ignored, always 64000.

- PacketizationPeriod

Packetization period, in milliseconds.

- SilenceSuppression

Indicates support for silence suppression for this codec.

If silence suppression is supported, it can be disabled for this codec/bit-rate by setting this parameter to false.

- Enable

Enable or disable the use of this combination of codec parameters.

- Priority

Indicates the priority for this combination of parameters, where 1 is the highest priority.

Where the priority differs between entries in this table, the CPE SHOULD use the highest priority (lowest numbered) entry among those supported by the remote endpoint and consistent with the available bandwidth.

Where the priorities are equal among multiple entries, the CPE MAY apply a local criterion for choosing among them.

33.14 LINEV2

Object associated with a distinct voice line.

33.14.1 ENABLE

Enables or disables this line.

33.14.2 DIRECTORYNUMBER

Directory number associated with this line.

May be used to identify the line to the user. In case of H.323 signaling, this MUST be an E.164 number.

33.14.3 CALLINGFEATURES

Voice line parameters related to optional endpoint based calling features.

- CallerIDName

String used to identify the caller.

33.14.4 STATUS

Indicates the status of this line.

33.14.5 CALLSTATE

Indicates the call state for this line.

33.14.6 PHYREFERENCELIST

A comma separated list of Physical Interface Identifiers that this Line is associated with.

33.14.7 SIP

Voice line parameters that are specific to SIP call signaling.

- AuthUserName

Username used to authenticate the connection to the server.

- AuthPassword

Password used to authenticate the connection to the server.

- URI

URI by which the user agent will identify itself for this line.

If empty, the actual URI used in the SIP signaling is automatically formed by the CPE as: 'sip:UserName@Domain' Where UserName is username given for this line (_VoiceProfile_?_SIP_AuthUserName), and Domain is the domain given for this profile (_VoiceProfile_?_SIP_UserAgentDomain). If this domain parameter is empty, then the IP address of the CPE is used for the domain. If URI is non-empty, but is a SIP or SIPS URI that contains no '@' character, then the actual URI used in the SIP signaling is automatically formed by the CPE by appending this parameter with an '@' character followed by the domain given for this profile (_VoiceProfile_?_SIP_UserAgentDomain). If this domain parameter is empty, then the IP address of the CPE is used for the domain.

- EventSubscribe_List

Table of SIP Events automatically populated by the CPE with each of the SIP event subscriptions in the table VoiceProfile.{i}.SIP. EventSubscribe.{i}. This table allows specification of the authentication credentials needed for each event subscription.

- EventSubscribe

Authentication credentials for event subscriptions.

  - Event

SIP event name corresponding to the value given in the table VoiceProfile.{i}.SIP.EventSubscribe.{i}.

- AuthUserName

Username used to authenticate the connection to the event notify server.

- AuthPassword

Password used to authenticate the connection to the event notify server.

33.14.8 MGCP

Voice line parameters that are specific to MGCP call signaling.

- LineName

Used to identify the line when using MGCP signaling. If empty, the CPE uses the default names 'aaln/1', etc.

33.14.9 H323

Voice line parameters that are specific to H.323 call signaling.

- H323ID

The H323ID assigned to the line.

Note: The H323ID may be appended by a password separated with a '$'.

33.14.10 VoiceProcessing

Voice line parameters related to voice processing capabilities.

- TransmitGain

Gain in units of 0.1 dB to apply to the transmitted voice signal prior to encoding. This gain is a modifier of the default transmit-gain, which is unspecified.

- ReceiveGain

Gain in units of 0.1 dB to apply to the received voice signal after decoding. This gain is a modifier of the default receive-gain, which is unspecified.

- EchoCancellationEnable

Enable or disable echo cancellation for this line.

33.14.11 Codec

Table to describe the set of codecs enabled for use with this line.

Each entry in this table refers to a distinct combination of codec and bit rate.

- Codec

Identifier of the codec type.

- BitRate

Bit rate, in bits per second.

Note: Ignored, always 64000.

- PacketizationPeriod

Packetization period, in milliseconds.

- SilenceSuppression

Indicates support for silence suppression for this codec.

If silence suppression is supported, it can be disabled for this codec/bit-rate by setting this parameter to false.

- Enable

Enable or disable the use of this combination of codec parameters.

- Priority

Indicates the priority for this combination of parameters, where 1 is the highest priority.

Where the priority differs between entries in this table, the CPE SHOULD use the highest priority (lowest numbered) entry among those supported by the remote endpoint and consistent with the available bandwidth.

Where the priorities are equal among multiple entries, the CPE MAY apply a local criterion for choosing among them.

33.14.12 STATS

Statistics for this voice line instance.

- ResetStatistics

When set to one, resets the statistics for this voice line. Always False when read.

- PacketsSent

Total number of RTP packets sent for this line.

- PacketsReceived

Total number of RTP packets received for this line.

- BytesSent

Total number of RTP payload bytes sent for this line.

- BytesReceived

Total number of RTP payload bytes received for this line.

- PacketsLost

Total number of RTP packets that have been lost for this line.

- Overruns

Total number of times the receive jitter buffer has overrun for this line.

- Underruns

Total number of times the receive jitter buffer has underrun for this line.

- IncomingCallsReceived

Total incoming calls received.

- IncomingCallsAnswered

Total incoming calls answered by the local user.

- IncomingCallsConnected

Total incoming calls that successfully completed call setup signaling.

- IncomingCallsFailed

Total incoming calls that failed to successfully complete call setup signaling.

- OutgoingCallsAttempted

Total outgoing calls attempted.

- OutgoingCallsAnswered

Total outgoing calls answered by the called party.

- OutgoingCallsConnected

Total outgoing calls that successfully completed call setup signaling.

- OutgoingCallsFailed

Total outgoing calls that failed to successfully complete call setup signaling.

- CallsDropped

Total calls that were successfully connected (incoming or outgoing), but dropped unexpectedly while in progress without explicit user termination.

- TotalCallTime

Cumulative call duration in seconds.

- ServerDownTime

The number of seconds the CPE is unable to maintain a connection to the server. SHOULD not include time in which overall network connectivity is unavailable. Applies only to SIP.

- ReceivePacketLossRate

Current receive packet loss rate in percent.

- FarEndPacketLossRate

Current far end receive packet lost rate in percent.

- ReceiveInterarrivalJitter

Current receive interarrival jitter in microseconds.

- FarEndInterarrivalJitter

Current Interarrival jitter in microseconds as reported from the far-end device via RTCP.

- RoundTripDelay

Current round trip delay in microseconds.

- AverageReceiveInterarrivalJitter

Average receive interarrival jitter in microseconds since the beginning of the current call.

- AverageFarEndInterarrivalJitter

Average far-end interarrival jitter in microseconds since the beginning of the current call.

- AverageRoundTripDelay

Average round trip delay in microseconds since the beginning of the current call.

34 PSTNPROFILE

Object associated with a PSTN line (FXO).

Note: The number of PSTNProfile's should be less or identical to the number of FXOInterface's.

34.1 ENABLE

Enables or disables the line in this profile.

34.2 SIGNALINGPROTOCOL

The protocol to be used for this profile.

Note: Always 'PSTN'.

34.3 NUMBERINGPLAN

This object contains information related the numbering plan.

34.3.1 FXSLISTIN

A comma separated list of FXS indexes that will ring on incoming calls for this PSTN profile.

Note: See FXS objects in config FXSInterface.

34.3.2 FXSLISTOUT

A comma separated list of FXS indexes that are allowed to make outgoing calls for this voice profile.

34.3.3 LOCALLISTIN

A comma separated list of SIPPhone indexes that will ring on incoming calls for this voice profile.

Note: See SIPPhone list in config.

34.3.4 LOCALLISTOUT

A comma separated list of SIPPhone indexes that are allowed to make outgoing calls for this voice profile.

34.3.5 MINIMUMNUMBEROFDIGITS

This is the minimum number of digits that must be collected before an outgoing request (e.g., a FXO off hook dialing) can be initiated. If \"End of Dialing\" (refer to the definition of the InterDigitTimer) occurs before the minimum number of digits has been reached then the number will be considered incomplete and no request will be initiated. In practice, searching the \"PrefixInfo\" list should only commence once the minimum number of digits (as specified by this parameter) has been received.

34.3.6 MAXIMUMNUMBEROFDIGITS

This is the maximum number of digits that may be collected before an outgoing request (e.g., a FXO off hook + dialing) must be initiated. Any additional dialed digits will be ignored. This parameter is only used in the case that no match in the "PrefixInfo" list has been found.

34.3.7 REMOTEDIALALLOWED

34.3.8 PREFIXINFO

Each entry in this table contains information related to an individual prefix in the numbering plan. It is anticipated that once the minimum number of digits has been received, the VoIP device will search this prefix list every time a new digit is received. If no new entry is found, then the object that was previously found will be used instead.

- PrefixRange

This is a string representation of a range of prefixes. Each prefix consists of a "From" part consisting of 1 to n digits (string representation) followed by an optional "To" part consisting of exactly one digit prefixed by a "-" symbol. It should be noted that only the characters "0-9", "*": and "#" can be used to represent the "From" and "To" parts of the prefix range. A further constraint is that the "To" digit MUST always be numerically greater than the last digit of the "From" part. Examples: 02 031-5 032 0325 *#34 #22.

- PrefixMinNumberOfDigits

This is the minimum number of allowable digits for the prefix range. Once the minimum number of digits has been reached, the "InterDigitTimerOpen" will be used instead of the "InterDigitTimerStd". If the minimum number of digits has been reached and the inter-digit timer expires, an outgoing request should be initiated.

- PrefixMaxNumberOfDigits

This is the maximum number of allowable digits for the prefix range. Once the number of digits received reaches this value an outgoing request should be initiated.

- NumberOfDigitsToRemove

If this parameter has a non-zero value, the specified number of digits will be removed from the beginning of the dialed digits before the outgoing call request.

35 FXSInterface

Table of objects describing the FXS interfaces.

Each instance is associated with a distinct physical FXS ("Foreign eXchange Station") port. Instances of this object are statically created in the factory profile, according to the hardware implementations.

35.1 Description

A description of the physical port.

35.2 InterfaceID

The unique identifier of the physical port. The first SLIC on the board has InterfaceID 1.

Note: On some boards with the place for two FXS's, the first SLIC is not mounted. In this case use InterfaceID 2 for the FXS.

35.3 PhoneName

The name of the physical port used in the dialplan. Should have the name 'Ctlm/fxs1', Ctlm/fxs2', etc.

35.4 Extension

The phone extension associated with this physical port (used to build the dialplan).

35.5 ReinjectionSupported

Specifies whether the hardware can do FXS reinjection to the FXO port, so the phones on the POTS side still works.

35.6 StartTest

35.7 Tests

Voice port tests.

35.7.1 TestState

Indicates the current test state.

35.7.2 TestSelector

Indicates which test to perform.

35.7.3 PhoneConnectivity

Indicates whether or not at least one phone associated with this physical port is properly connected.

35.8 Ring

set start to make ring, set stop to stop ringing.

36 FXOInterface

Table of objects describing the FXO interfaces.

Each instance is associated with a distinct physical FXO ("Foreign eXchange Office") port. Instances of this object are statically created in the factory profile, according to hardware.

36.1 Description

A description of the physical port.

36.2 InterfaceID

The unique identifier of the physical port. The first DAA on the board has the InterfaceID next to the last SLIC.

36.3 PhoneName

The name of the physical port used in the dialplan. Should have the name 'Ctlm/fxo'.

36.4 ReducedFXO

Set this if the board has a Reduced FXO (only ring and on hook detect) instead of a DAA.

37 NetGem

Note: Private - do not use.

37.1 Enable

37.2 IntfIndex

37.3 DestPort

37.4 DestAddr

37.5 DestUrlCid

37.6 DestUrlCmd

38 BluetoothConfig

Configure the bluetooth network.

38.1 Enable

When set, enables the bluetooth network.

38.2 Pin

Pin code used to connect to the bluetooth network.

38.3 Visible

When set, make the box name visible on the bluetooth network.

39 OBEXPUSHCONFIG

The Obex Push service is used to download files from a bluetooth device to the box.

39.1 ENABLE

When set, enables the Obex Push Services.

39.2 ROOTDIR

Define the directory where files are downloaded.

39.3 IMAGEDIR

Directory where the image downloaded are placed (files extensions that match jpg, gif, etc...). This directory is relative to _ObexPushConfig_RootDir.

39.4 VIDEODIR

Directory where the video downloaded are placed (files extensions that match avi, etc...) This directory is located in _ObexPushConfig_RootDir.

39.5 MUSICDIR

Directory where the music downloaded are placed (files extensions that match mp3, etc...) This directory is relative to _ObexPushConfig_RootDir.

40 X10CONFIG

Enable X10 protocol daemon for managing domotic devices.

Dependency: Depend on module kernel USB_X10 (Device Drivers / USB X10 (experimental))

40.1 ENABLE

When set, enables the X10 protocol daemon.

41 WebCam

Webcam settings definitions.

Configuration settings for current webcam.

Dependency: Works with both "vidgrab" or "motion" for image capture. By default "motion" will be used. If "motion" was not included in firmware, then "vidgrab" will be automatically used.

41.1 Enable

Enable current webcam.

41.2 Name

indicates webcam name.

41.3 Device

Absolute path of the USB webcam device.

41.4 Rate

WebCam Rate (snapshots per second).

41.5 Interval

Amount of time between two snapshots (in seconds).

Note: Work only with motion.

41.6 Image

Filename of the saved snapshot.

41.7 HttpPort

Listen on this port for video stream clients.

41.8 Format

Video frame format (WIDTHxHEIGHT).

41.9 UploadImage

An object managing snapshots uploads on a remote server.

Dependency: Work only with motion and sftp

41.9.1 Enable

When set, enable snapshot uploading.

41.9.2 Server

Remote server's name.

41.9.3 Port

Remote server's port.

41.9.4 Login

Login name for accessing the remote server.

41.9.5 Password

Password for accessing the remote server.

41.10 Status

Show status for the current webcam.

41.10.1 State

Show state if a webcam is connected or not (ok or nok).

41.10.2 Model

Model name of connected webcam (extracted by vidgrab using ioctl on v4l device

42 VPN

42.1 PPTP

42.2 L2TP

42.3 IPSec

42.4 IPSecDebug

42.5 IPSecSecurity

42.5.1 Enable

42.5.2 DHGroup

42.5.3 Behaviour

- Enable
- Encryption
- Hash

42.5.4 Timeout1

42.5.5 Encryption

42.5.6 Signature

42.5.7 Timeout2

42.5.8 NATT

42.5.9 DPD

42.5.10 PFS

42.6 Network

42.6.1 WanIP

43 VPNConnection

43.1 Enable

When set to 1, enables current object.

43.2 Name

43.3 Interface

43.4 DestIP

43.5 DestDN

43.6 DnRefresh

43.7 IdleTimeout

43.8 PingIP

43.9 DefaultDirection

43.10 Output

43.11 Input

43.12 IPSecSecurity

43.12.1 Enable

43.12.2 IKEKey

43.12.3 LocalIP

43.12.4 LocalID

43.12.5 HostIP

43.12.6 HostID

43.12.7 Mode

43.12.8 DHGroup

43.12.9 Behaviour

- Enable
- Encryption
- Hash

43.12.10 Timeout1

43.12.11 Encryption

43.12.12 Signature

43.12.13 Timeout2

43.12.14 NATT

43.12.15 DPD

43.12.16 PFS

43.13 L2TP

43.13.1 Enable

43.13.2 Interface

43.13.3 PPPUnit

43.13.4 IPSecRules

43.14 PPTP

43.14.1 Enable

43.14.2 PPPUnit

43.15 Authentication

43.15.1 Enable

43.15.2 Username

43.15.3 Password

43.15.4 ServerCert

43.15.5 AuthMethod

43.16 Network

43.17 Enable

43.18 WanIP

43.19 WanMask

43.20 WanGateway

43.21 DefaultRoute

43.22 RmtIP

43.23 RmtMask

43.24 LocalNetworks

43.25 SubNetwork_List

43.26 SubNetwork

43.26.1 Enable

43.26.2 IPAddress

43.26.3 Mask

43.27NAT

43.28RIP

43.28.1 Enable

43.28.2 Direction

43.28.3 Version

44 AutomaticLedExtinction

This feature allows switching off the CPE's LEDs during a given period each day.

Dependency: {{{[*] Customize User Settings FHLP tools ---

[*] LEDs extinction shedule/manual

[CONFIG_USER_MISC_LEDEXTINCTION=y] Define which leds are involved in the management of extinction.

[*] Customize Kernel Settings Device Drivers ---

FHLP Products and Drivers Configuration ---

[*] enable schedule/manual management for power LED [CONFIG_FHLP_LEDBUTTON_LEDPOWER_SLEEP=y]

[*] enable schedule/manual management for DSL/PPP sync LED

[CONFIG_FHLP_LEDBUTTON_LEDSYNC_PPP_SFR_SLEEP=y] [*] enable schedule/manual management for VOIP LED [CONFIG_FHLP_LEDBUTTON_LEDVOIP_SFR_SLEEP=y]

[*] enable schedule/manual management for WIFI LED [CONFIG_FHLP_LEDBUTTON_LEDWIFI_SFR_SLEEP=y]

[ ] enable schedule/manual management for voice mail LED}}}

Note: The _AutomaticLedExtinction parameters are visible in the user interface.

44.1 Enable

Determine whether the schedule LEDs management feature is enabled or not.

44.2 LedOffHour

IAD's leds are automatically "switched OFF" at specific time h:m where h=_AutomaticLedExtinction_LedOffHour and m=_AutomaticLedExtinction_LedOffMin.

44.3 LedOffMin

IAD's leds are automatically "switched OFF" at specific time h:m where h=_AutomaticLedExtinction_LedOffHour and m=_AutomaticLedExtinction_LedOffMin.

44.4 LedOnHour

IAD's leds are automatically "switched ON" at specific time h:m where h=_AutomaticLedExtinction_LedOnHour and m=_AutomaticLedExtinction_LedOnMin.

44.5 LedOnMin

IAD's leds are automatically "switched ON" at specific time h:m where h=_AutomaticLedExtinction_LedOnHour and m=_AutomaticLedExtinction_LedOnMin.

45 ManualLedExtinction

Enable or disable IAD's led switch OFF on long wifi button press.

IAD's leds are switched OFF by a long press on wifi button. IAD's leds are switched to their current normal working state when wifi button is pushed again.

Dependency: Same as _AutomaticLedExtinction.

45.1 Enable

Determine whether the manual LEDs management feature is enabled or not.

45.2 SleepModeRunning

Internal status indicating whether the sleep mode is currently active or not.

46 IRLEDEXTINCTION

Disable IAD's led extinction management by ledextinction daemon

Manage by IR Led daemon instead

46.1 ENABLE

Determine whether the IR LEDs management feature is enabled or not.

47 CONNTRACK

Info about current state of conntrack

47.1 ENABLESTATUS

Enable/Disable status

47.2 ITEM

current NAT info

47.2.1 IFNAME

Interface network used

47.2.2 PROTO

Protocol

47.2.3 SOURCEIP

Source IP

47.2.4 SOURCEPORT

Source Port

47.2.5 DESTINATIONIP

Destination IP

47.2.6 DESTINATIONPORT

Destination Port

47.2.7 EXPIREIN

Expire in (in secondes)

48 ZIGBEECONFIG

48.1 ENABLE

48.2 LASTCHANGE

48.3 DEBUG

48.4 DEVICE

48.4.1 NWKADDRESS

48.4.2 ENDPOINTS_LIST

48.4.3 ENDPOINTS

- Type
- ClustersI
    - Type
    - Params
        - param
- ClustersO_List
- ClustersO
    - Type
    - Params
        - param