

# V-Tap ISDN PRI

## Manual

v1.4



# Contents

<b>1</b>	<b>Introduction.....</b>	<b>4</b>
<b>2</b>	<b>Getting started.....</b>	<b>5</b>
<b>2.1</b>	<b>Hardware installation.....</b>	<b>5</b>
2.1.1	Sniff mode operation.....	6
2.1.2	Pass-Through mode operation.....	6
2.1.3	Parallel connection.....	7
2.1.4	In-Line connection.....	7
<b>2.2</b>	<b>Software installation.....</b>	<b>8</b>
2.2.1	Call Recorder Apresa.....	8
2.2.2	Call Recorder VoIP on the PC.....	9
<b>2.3</b>	<b>Checklist for Tunnel connection.....</b>	<b>10</b>
<b>3</b>	<b>Web interface and Settings.....</b>	<b>11</b>
<b>3.1</b>	<b>IP address.....</b>	<b>11</b>
<b>3.2</b>	<b>Web interface.....</b>	<b>12</b>
<b>3.3</b>	<b>Settings.....</b>	<b>14</b>
3.3.1	General network settings.....	14
3.3.2	Tunnel settings.....	16
3.3.3	Wi-Fi settings.....	18
3.3.4	FTP & Web settings.....	19
3.3.5	Telnet setting.....	20
3.3.6	NTP settings.....	21
3.3.7	Date & Time settings.....	22
3.3.8	ISDN PRI settings.....	23
3.3.9	SD Card settings.....	25
3.3.10	Special network settings.....	27
3.3.11	App Special Flags.....	28
3.3.12	Licenses & Versions.....	30

<b>4</b>	<b>LED's</b> .....	<b>31</b>
4.1	Red Error LED .....	31
4.2	Green Link LED .....	32
4.3	Blue Data LED .....	32
4.4	Amber SD-Power LED .....	33
<b>5</b>	<b>Button functions</b> .....	<b>34</b>
5.1	Remove SD Card safely .....	34
5.2	Enable DHCP temporary .....	35
5.3	Show IP address .....	35
5.4	Factory settings .....	36
5.5	Default IP address .....	36
5.6	Firmware update .....	37
<b>6</b>	<b>Notification &amp; System Messages</b> .....	<b>38</b>
<b>7</b>	<b>Number-list (Black- or White-list)</b> .....	<b>39</b>
<b>8</b>	<b>Remote control with UDP commands</b> .....	<b>40</b>
<b>9</b>	<b>ISDN PRI RJ45 connectors &amp; wiring</b> .....	<b>42</b>
<b>10</b>	<b>Revision History</b> .....	<b>43</b>
<b>11</b>	<b>Acknowledgements</b> .....	<b>44</b>
11.1	Privacy .....	44
11.2	Liability .....	44

# 1 Introduction

The V-Tap ISDN PRI is a hardware and software solution for the recording of telephone calls. The supplied hardware unit can record the audio from an ISDN-30 line with E1 interface. The recorded data is stored digitally onto an SD card and is sent optionally over the network, in which case the data is wrapped into a special Tunnel-format that can be received by the Call Recorder Apresa (running on Linux) or by the Call Recorder VoIP software (running on a Windows PC). The external Apresa recorder or CR-VoIP software can both interpret the Tunnel-format and make playable audio files from it, together with the original date, time and call number information (meta data).

The use of an SD card is mandatory and must be FAT32 formatted. The recorded data is stored in WAV file format on the card (G.711 A-Law). Depending on whether a Tunnel has been defined or not, the files are sent over the network or can be read later by the CR-VoIP software. Note that the V-Tap ISDN PRI does not produce WAV files or store any data on the SD card without Recording Channel Licenses.

The V-Tap ISDN PRI can operate completely stand alone and when the capacity of the SD card is big enough, it can store data for months or even years.

Connection to the V-Tap PRI is made with a network cable or by using Wi-Fi, when available. The web interface can be accessed by using a normal browser. The LAN cable must be connected to the Ethernet port, which is 100 Mbps Full Duplex.

The V-Tap ISDN PRI is a member of a family of compatible products that can be used to create all sorts of Call Recording solutions. There are V-Taps for VoIP, Analog and ISDN telephony, there is an App for mobile recording and all these products communicate with the Apresa Corporate recording solution or Apresa cloud-based recording.

**NOTE 1:** The V-Tap ISDN PRI needs to be powered through USB and a FAT32 formatted SD card must be inserted.

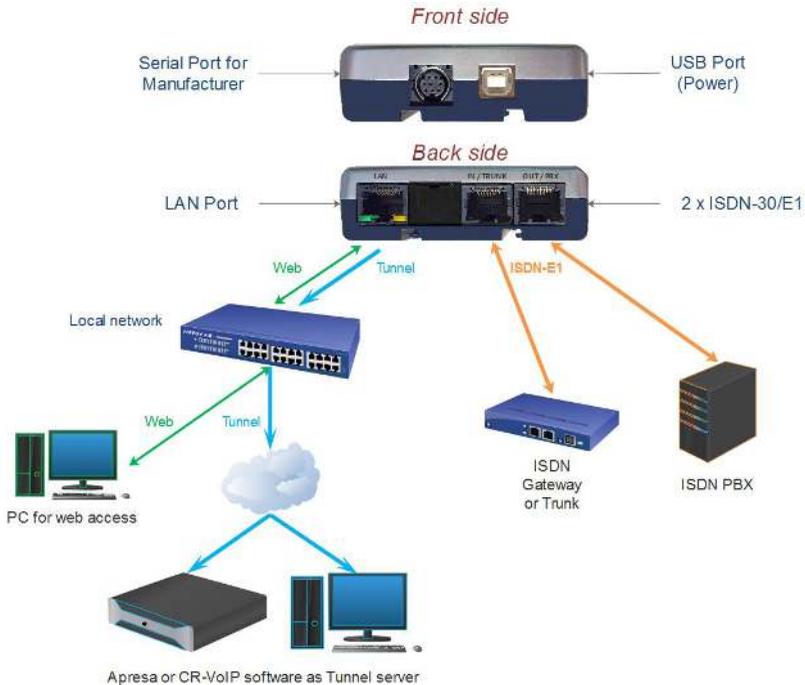
**NOTE 2:** The V-Tap ISDN PRI needs at least one Recording Channel License, else no calls are stored on the SD card.

## 2 Getting started

### 2.1 Hardware installation

The V-Tap ISDN PRI is easy to setup. The following steps are involved:

- The jumpers inside must be set to the right mode; default on Sniff.
- Connect the Trunk and PBX to the ISDN ports of the V-Tap.
- Insert an SD card (up to 32 GB, FAT32 formatted).
- Connect the USB to the V-Tap for power.
- Connect the local network.
- Access the settings in the web interface by using a browser.



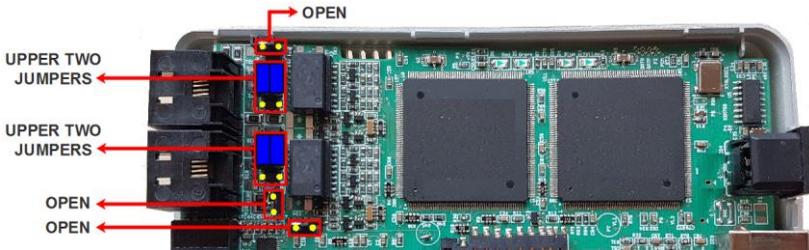
The two possible modes of operation (Sniff or Pass-Through) must be set with the internal jumpers and are described in [2.1.1](#) and [2.1.2](#).

The two possible ways of connecting the V-Tap PRI physically to the E1 line (Parallel or In-Line) are shown in [2.1.3](#) and [2.1.4](#).

## 2.1.1 Sniff mode operation

The Sniff mode of operation is the default mode when the V-Tap PRI is shipped. It means that the V-Tap is a listener to the ISDN line and the transmitters on the jacks are disabled. A notification message or record-on-demand is not possible in this mode.

In Sniff mode, the V-Tap PRI can be connected Parallel or In-Line. There are 7 jumpers involved to set Sniff or Pass-Through mode. These jumpers can be found on the board. After opening the case (press both sides firmly), the jumpers must be placed as follows for Sniff mode:



## 2.1.2 Pass-Through mode operation

The Pass-Through mode of operation must be set first with the 7 jumpers on the board. The system automatically detects the jumper settings after restart and will change the web interface with additional parameters. Pass-Through mode enables the transmitters on the ISDN jacks and extra features become available, such as the notification message and record-on-demand with DTMF \*\*.

In Pass-Through mode, the V-Tap PRI can only be connected as In-Line. The 7 jumpers must be placed as follows for Pass-Through mode:

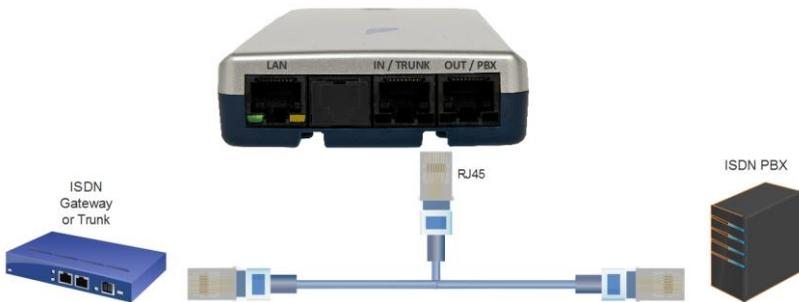


### 2.1.3 Parallel connection

Connecting the V-Tap PRI parallel to the line has the advantage that the ISDN line keeps on functioning when the V-Tap is disconnected. So, no interruption of the line takes place when the V-Tap is removed.

Only one ISDN jack needs to be connected to the line. Using the IN- or OUT-jack in this case, does not matter. This way of connecting is only possible for Sniff mode.

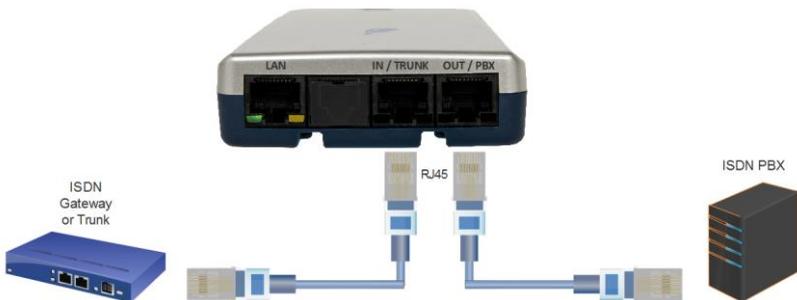
Parallel connection must be made using a normal 3-way splitter (one-to-one T-splitter):



### 2.1.4 In-Line connection

Connecting the V-Tap PRI as In-Line is an option for Sniff mode (listener) but is mandatory when Pass-Through mode is selected with the jumpers.

The advantage of connecting In-Line is, that the V-Tap cannot be removed without notice, because the ISDN line will be interrupted when doing so. In-Line connection is shown below:



## 2.2 Software installation

External software is needed to extract the recorded calls from the Tunnel data that is produced by the V-Tap ISDN. Also, when the calls are first stored on an SD card, external software is needed to interpret this data from the card, especially when the data is encrypted.

The Tunnel data stream, coming from the V-Tap, can be send to the Call Recorder Apresa or the Call Recorder VoIP software.

### NOTE:

The V-Tap needs at least one Apresa or PC upload-channel license key before the Apresa or CR-VoIP software can record your calls.

### 2.2.1 Call Recorder Apresa

The Call Recorder Apresa is recorder software running on the Linux operating system. The Apresa can receive Tunnel data from the V-Tap, convert this data into audio files and store these into its own database. The Apresa can receive multiple data streams from many V-Tap units simultaneously. In that case the recordings of different locations are centrally stored in one database.

To setup the Apresa to act as a Tunnel server for a V-Tap, go to System settings, Network tab and enable "V-Tap" as is shown below:

The screenshot shows a configuration window for V-Tap. It includes several checkboxes and input fields:

- V-Tap:
- V-Tap Tunnel port number: 2016
- V-Tap Data separation:
- Accept only known V-Taps:
- Accept only encrypted V-Tap connections:
- V-Tap Encryption password: [password field]  Define new password

MAC address	Encryption password	Tenant	Delete
000349010041	*****	TN-793471005	<input type="checkbox"/>

Below the table are buttons for 'Add' and 'Delete'. At the bottom of the window are 'Apply' and 'Cancel' buttons.

**NOTE1:** Apresa's IP address is the "Tunnel Server Address" in the V-Tap.

**NOTE2:** Be sure the Encryption password is the same as in the V-Tap unit.

## 2.2.2 Call Recorder VoIP on the PC

The Call Recorder VoIP software for the PC can also receive Tunnel data from the V-Tap ISDN, convert this data into audio files and store the files into its own database. The CR-VoIP software can also receive multiple data streams from different V-Tap units simultaneously.

To setup the CR-VoIP software to accept connections from a V-Tap, go to Options, Setup, Recording tab and enable as is shown below:



**NOTE1:** The PC's IP address is the "Tunnel Server Address" in the V-Tap.

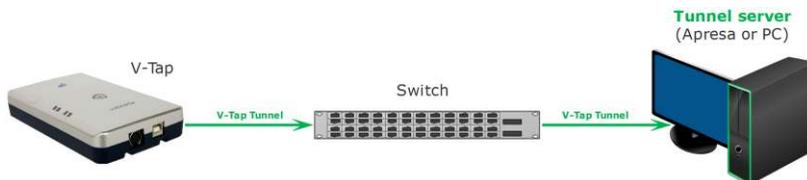
**NOTE2:** Be sure that the PC's firewall is open for TCP port 2016, the default "Tunnel Destination Port" in the V-Tap unit.

**NOTE3:** Be sure the Encryption password is the same as the "Encryption Password" in the V-Tap unit.

**NOTE4:** The CR-VoIP software does not need licenses to receive from the V-Tap unit.

*The Call Recorder VoIP software for the PC has its own manual and is therefore further not described in this manual.*

## 2.3 Checklist for Tunnel connection



A connection between V-Tap and Apresa or PC software is needed to get the recorded data automatically into a user accessible database.

The following checklist can be used to setup this Tunnel connection:

- 1) Install the [Hardware](#).
- 2) Install the Apresa or PC [Software](#) and enable V-Tap connections.
- 3) Assign an [IP address](#) to the V-Tap and open the [Settings page](#).
- 4) The "[Tunnel Server Address](#)" must be filled in with the IP address or name of the Apresa recorder or the PC.
- 5) Any **firewall** must be setup to let pass TCP port **2016**, the default "[Tunnel Destination Port](#)".
- 6) The Tunnel connection to the Apresa or PC software is stable when the **GREEN LED is steady**, not blinking!
- 7) For first tests, better turn off "Tunnel Data Encryption". Otherwise, be sure that the Encryption password is the same for both V-Tap and Tunnel server.
- 8) When data is stored during a call then the **BLUE LED** blinks.
- 9) To see if the Apresa or PC receives something from the V-Tap, it is possible to make a network trace for test purposes. On the PC go to menu Action and select 'Network trace'. The 'tunneltrace.pcap' file can be read afterwards with Wireshark.
- 10) The SD card in the V-Tap should contain ".WAV" files. The SD card can be read by the PC software in menu File and 'Import from V-Tap'.

## 3 Web interface and Settings

There are two ways to access the web interface of the V-Tap:

- 1) When a Wi-Fi module is available and enabled on the V-Tap: Searching for Wi-Fi apparatus on a mobile phone or laptop, will show the name "V-Tap\_.....". The last 6 digits of the name are the last digits of the MAC address. The first 6 digits of the MAC address are always 000349. The complete 12 digits are used as the default Wi-Fi password.
- 2) Connect a network cable to the network port on the unit. The other side of the cable can be connected to a LAN or directly to a PC. There is no need to use a cross-cable.

### 3.1 IP address

By default, the V-Tap unit listens to the IP address 192.168.55.66 and DHCP is disabled for the cable. This IP address can be entered directly in the address bar of your browser.

In the case of using Wi-Fi, the IP address 192.168.55.66 always works as soon as the connection is made over the air. To connect, you need to enter the Wi-Fi password first, which is the 12 digits MAC address of the unit, also found on the bottom of the case.

In the case of using a cable, entering the IP address only works when your PC has an IP address that lies in the same range as the IP address of the V-Tap. The IP address of your PC must therefore lie in the range 192.168.55.0 till 192.168.55.255 and the IP mask should be 255.255.255.0.

Default IP address:	<b>192.168.55.66</b>
Default Web User name:	<b>admin</b>
Default Web Password:	<b>admin</b>
Default Wi-Fi Password:	<b>000349xxxxxx</b> [12 digits MAC address]

**DHCP** on the cable can be enabled temporary by pressing the button for 1 second. The LED's will flash shortly as soon as an IP address is obtained, and the V-Tap is then reachable on that address.  
See also [Enable DHCP temporary](#) and [Show IP address](#).

It is also possible to set a new fixed IP address or enable DHCP for the cable by using an SD card: (*see next page*)

### Defining a fixed IP address with an SD card:



- . Create a text file on your PC, named "IP.TXT".
- . The first line in this file must hold the IP address.
- . The second line is optional and can hold the IP mask.
- . Copy "IP.TXT" to the root directory of an SD card.
- . Insert the SD card into the V-Tap unit.
- . The IP address has now changed and can be accessed.
- . The file "IP.TXT" is deleted from the card by the V-Tap.
- . **Note:** The IP address **0.0.0.0** enables DHCP on the V-Tap.

## 3.2 Web interface

Entering the IP address in your browser will show the following screen:

V-Tap ISDN PRI Login vidicode

Vidicode-Tap ISDN PRI

User name:

Password:

Login

Now enter "admin" for the User name and "admin" for the Password, then press the **Login** button and the Settings menu appears (*see picture on the next page*).

(The settings on the next page are not the default settings, but just an example.)

**V-Tap ISDN PRI Settings** 12-04-2018 16:01:18  vidicode

Name of this V-Tap	V-Tap_PRI_BC8DBF	Record Outgoing Calls	<input checked="" type="checkbox"/>
DHCP Server	<input checked="" type="checkbox"/>	Record Local Side only	<input type="checkbox"/>
IP Address	192.168.0.36	Stereo Recording (else Mono)	<input type="checkbox"/>
Subnet Mask	255.255.255.0	Reversed D-channel Operation	<input type="checkbox"/>
Gateway Address	192.168.0.5	Notification Message Control	0
DNS Server Address	8.8.8.8	DTMF +* Action Control	0
Tunnel Server Address	Alwin PC.vidicode.local	SD File Encryption	<input type="checkbox"/>
Tunnel Destination Port	2018	SD Max Files on Card	10000
Tunnel Source Port	0	SD Max File Size in MB	230
Tunnel Connect Timeout	22	SD Delete File after Sending	<input type="checkbox"/>
Tunnel Idle Timeout	0	SD Interface Speed in MHz	25
Tunnel Data Encryption	<input checked="" type="checkbox"/>	Max Data Length in Packets	1024
Encryption Password	*****	LAN Service Timer	0
FTP & Web User name	admin	MAC Address	0003468C8DBF
FTP & Web Password	*****	App Special Flags	
FTP Port Number	21	Licenses: Apresa / PC / S&U	30 / 0 / 05-05-2055
TelNet Connection	<input checked="" type="checkbox"/>	New License Key	
NTP Server Address	pool.ntp.org	<a href="#">License Activation</a>	
NTP Port Number	123	V-Tap PRI OS Version	1.0.6.12-04-2018
GMT Minutes Correction	60	V-Tap PRI App Version	7.0.4.12.04.2018
New Date (DD-MM-YYYY)		V-Tap PRI Serial Number	500229
New Time (HH:MM:SS)			

Save & Logout Cancel & Logout

By pressing the **Save & Logout** button, the settings are sent to the V-Tap unit. Any ongoing recording is stopped, the file on SD card is closed, and after a few seconds the new settings are activated.

## 3.3 Settings

The settings are divided into groups that are described in the following paragraphs.

### 3.3.1 General network settings

#### Device Name

This field can be filled in with any name you like and is used for remote recognition of the V-Tap unit. The name is shown in the web interface and after connecting with ftp or telnet. The name is also shown when searching for Wi-Fi apparatus on your mobile or laptop. The maximum length is 30 characters.

The single and double quotation marks ( ' and " ) cannot be used !

#### DHCP Server

Default, the DHCP feature is disabled and the V-Tap unit has a fixed IP address. When a DHCP server is available on the network, the IP address, Subnet Mask, Gateway and DNS addresses are automatically assigned. Without DHCP you must enter them manually.

With default settings, DHCP can be enabled temporary by pressing the button for 1 second, see [Enable DHCP temporary](#).

The DHCP setting is not used for Wi-Fi connections.

#### Device IP Address

As part of the network, the V-Tap needs an IP address. In case a DHCP server is used, the DHCP server will assign the V-Tap an IP address. In case a DHCP server is not used, a static IP address must be filled in. The default static address is "192.168.55.66".

#### Subnet Mask

The subnet mask is used for so called 'subnetting', a way to logically divide one network into more networks. The logical AND of the IP address with the mask must be the same for the device and the computer connecting to it. The default mask is "255.255.255.0".

In case DHCP is used, the mask is automatically obtained.

## Gateway Address

The Gateway address is used by the V-Tap unit when access outside the local network (LAN) is required. This sort of access can be needed by the Tunnel protocol for streaming to a remote computer and/or by the NTP feature for obtaining the current date and time. In case DHCP is used, the gateway address is automatically obtained.

## DNS Server Address

The Domain Name Service (DNS) is needed in case a name is entered instead of an IP address for the Tunnel server and/or the NTP server. The default DNS address 8.8.8.8 is the Google Public DNS, but the Gateway must be defined also before this address is reachable. In case DHCP is used, the DNS address is automatically obtained.

## 3.3.2 Tunnel settings

### Tunnel Server Address

Here you fill in the IP address or host name of the Tunnel server that is going to receive the streamed data coming from the V-Tap ISDN. Leaving this field empty will disable the Tunnel function all together, in which case the V-Tap unit must store its data onto an SD card. The receiving server can be an Apresa recorder or a PC running the Call Recorder VoIP software. In both cases, the V-Tap needs a license to allow Tunnel data to be uploaded/streamed to the Tunnel server. **Without a license, the receiving server will discard the Tunnel data.**

### Tunnel Destination Port

The Tunnel protocol is based on the TCP protocol and that involves a Destination Port and a Source Port. Both are numbers from 0 till 65535 that are included in each packet and are very important for the receiving end of the Tunnel data. The receiving Tunnel server must be setup to look for the same port number as is installed in this Tunnel Destination Port.

Not all TCP port numbers are available for tunnelling, because some are officially used by other protocols. For example, port 80 is used for HTTP in all browsers to communicate over the World Wide Web. A list of known port numbers can be found on the internet.

The default port number 2016 is not an official port and can be used safely for this Tunnel protocol. The only drawback that comes by using an unknown port is, that a firewall will block this port. For that reason, it is important that any firewall that is passed by the Tunnel stream must be setup right.



**Firewalls must have a rule to let through TCP port 2016.**



### Tunnel Source Port

The Source Port also has an important role in the Tunnel protocol. The default number 0 selects randomly a port number between 49152 and 65535. This range of port numbers is recommended by IANA to be used for dynamic ports.

Once a connection has been established between the V-Tap and the receiving Tunnel server, the chosen port number is kept active for the duration of the communication session. When connection is lost for some reason, a new source port is chosen for the next connection. This ensures fast reconnection, because the TCP protocol does not allow the same source port to be used again within a short time. After an OS specific timeout of normally a few minutes, the port numbers become available again for reuse.

### Tunnel Connect Timeout

This timeout is used when the V-Tap tries to connect to the Tunnel server. The default 22 seconds is enough to send 4 requests. If no reply comes from the remote side within this time, the V-Tap starts trying again after a few seconds with a new source port number. Storage onto SD card just continues and is not interrupted by any connection or disconnection of the Tunnel.

### Tunnel Idle Timeout

This timeout is used to disconnect the active tunnel to the server, only when no data must be sent anymore. Default, the idle-timeout is disabled and the tunnel stays connected forever. The timeout is added for (yet) unknown situations where it is not allowed to have an open TCP connection for a long time.

### Tunnel Data Encryption

The data inside the Tunnel protocol is sent encrypted over the network. The used method is AES with a 256-bit Cryptographic Key. For privacy reasons it is advised to leave the encryption enabled.

### Encryption Password

This parameter is used for the encryption of the Tunnel data and the file on SD card (see below). The receiving side of the Tunnel data, the Apresa or CR-VoIP software, must use the same password. Leaving the password empty is still doing the encryption but is less secure. The single and double quotation marks ( ' and " ) cannot be used !

### 3.3.3 Wi-Fi settings

The Wi-Fi module in the V-Tap may not be enabled by default. To enable, enter "FACTORY WIFI" in the App Special Flags field. After pressing Save and log in again, the 3 Wi-Fi parameters become visible. Once Wi-Fi is enabled, you can use your mobile phone or a laptop to connect to the V-Tap over the air to access the settings. The following steps must be taken:

- Search for Wi-Fi apparatus on your smartphone or laptop, the device name "V-Tap\_PRI\_xxxxxx" is then shown.
- Select it and when asked for a password, use the 12 digits MAC address of the unit, found on the bottom of the case. The first 6 digits of the MAC are always 000349 and the last 6 digits are also part of the Wi-Fi name.
- Open a browser and enter the IP address 192.168.55.66. The web login page should appear. After login with admin/admin, the settings page appears.

The internal Wi-Fi works as an Access Point (AP) for web access and, at the same time, can act as a station to connect to an external AP for the tunnel function. DHCP is always enabled for Wi-Fi.

See [App Special Flags](#) for more specialized Wi-Fi options.

#### Wi-Fi Access Point

This enables or disables the internal AP mode and therefore enables or disables the web access using Wi-Fi. The password to connect with Wi-Fi can be changed in the **FTP & Web & Wi-Fi Password** field.

#### Wi-Fi Tunnel AP Name

#### Wi-Fi Tunnel AP Password

To setup a tunnel connection over Wi-Fi, the V-Tap must connect to an external AP. In most of the cases this will be a router somewhere in the building. The AP's name and password must be filled in here.

The Wi-Fi module can be disabled completely by turning the Wi-Fi Access Point option off in the settings AND the Tunnel AP fields must be left empty. When disabled, all access must be done with a LAN cable.

Sending tunnel data with Wi-Fi is slower than using a LAN cable. So, some delay must be considered.

### 3.3.4 FTP & Web settings

The V-Tap has a built in FTP (File Transfer Protocol) server that allows you to access the internal filing system. At this moment, this is only used for updating the firmware remotely (see chapter Update Firmware). FTP can be disabled by setting the FTP Port to 0 (zero).

#### FTP & Web User name

User name to log in with FTP and the Web service.

The single and double quotation marks ( ' and " ) cannot be used !

The default user name is "admin".

#### FTP & Web & Wi-Fi Password

Password to log in with FTP and the Web service.

Also used as the password to connect to the V-Tap with Wi-Fi, only when this field contains 8 characters or more. Less than 8 characters will use the MAC address for the Wi-Fi password.

The single and double quotation marks ( ' and " ) cannot be used !

The default password is "admin".

#### FTP Port Number

By default, the FTP Port is on 21 for normal FTP access.

The PC tool 'vcUpdater' uses FTP to update the firmware of the V-Tap. This tool can be found on the Vidicode website in the menu Service and Support => Firmware.

By setting the FTP Port to 0 (zero), FTP is disabled completely.

### 3.3.5 Telnet setting

#### TelNet Connection

The V-Tap unit can be accessed with the Telnet network protocol. Telnet is an older protocol to access devices remotely with a simple terminal and then perform maintenance or change settings. Telnet also uses the TCP protocol with the fixed port number 23. Running a Telnet client program on the PC makes it possible to connect to the V-Tap. After connecting, the Device Name is shown, and some debug information is constantly sent to Telnet; Opening and closing of the Tunnel connection and, when an SD card is used, the opening and closing of files.

Further, there are three useful commands:

The command **ATMENU** will first ask you to enter the web access password and then brings you in a remote maintenance menu. Once inside the menu, the tunnel function and SD card storage are stopped.

The menu gives the user the possibility to change the settings, reset the SD file counters, reset to factory settings and change the clock. Normally, there is no need to use any of these functions over Telnet.

The command **ATDEBUG** is a toggle to enable and disable the output of more debug information. This is further not described in this manual.

The command **ATDTEST** jumps to the D-channel trace facility. The ISDN D-channel is outputted and can be captured and interpreted for debug purposes. Recording is not possible during this mode.

### 3.3.6 NTP settings

NTP (Network Time Protocol) can be used to synchronize the internal clock. The V-Tap also has an internal battery to keep the clock running when power fails, but this is not as accurate as the clock on an NTP server. NTP gets the exact date and time from the server and the internal clock is then updated with this.

The clock is added to each recording and is therefore very important to get the date and time right for all recorded calls.

The V-Tap synchronizes the clock 6 times per day (each 4 hours).

#### NTP Server Address

The IP address or the host name of the NTP server. Default, the address is set to "pool.ntp.org", but the Gateway and the DNS server must be defined also for this to work.

Leave this field empty when no NTP is used.

#### NTP Port Number

The used port number for NTP in the TCP protocol. This is always 123.

#### GMT Minutes Correction

The time correction in minutes to the GMT (Greenwich Mean Time) zone. The number can start with the minus sign when needed.

For example, enter "-300" for Eastern Time (that is -5 hours for east-coast US & Canada).

### 3.3.7 Date & Time settings

The current date and time are shown on top of the page. A new date and/or time can be set with the below parameters.

 New Date (DD-MM-YYYY)

 New Time (HH:MM:SS)

For the date, the entered format must be day, month and year, separated by the minus-sign and always 10 characters long in total. For the time, the entered format must be hour, minutes and seconds, separated by the colon-sign and always 8 characters long in total. The new date and time are set after pressing **Save & Logout**.

### 3.3.8 ISDN PRI settings

#### Record Outgoing Calls

Outgoing calls are normally recorded, but it can be disabled with this setting. Incoming calls are always recorded.

#### Record Local Side only

An ISDN line has the possibility to separate the audio of the local and remote side of a call. The V-Tap PRI can optionally store the local speaker only.

#### Stereo Recording (else Mono)

The V-Tap PRI can store both the local and remote side of a call in a stereo WAV file, each side having its own channel. The only drawback is, that the files will be twice as big, because 16000 bytes per second must be stored then, instead of 8000 bytes per second for the Mono/Mixed mode.

#### Reversed D-channel Operation

It might be that the Rx and Tx wires in the cable are reversed. In that case, the V-Tap PRI will still record all calls correctly, except that inbound and outbound are presented wrong.

This is only possible when the recorder is operating in Sniff mode. In Pass-Through mode the wiring in the cables must be right.

In other words, when the local and remote phone numbers are reversed in the database software, this parameter can be enabled.

## Notification Message Control

This setting is only available when the V-Tap PRI is operating in Pass-Through mode: see Jumper settings in [2.1.2](#).

The notification message can be played by the system in 2 possible ways. Or both parties of the call hear the message at the same time, or the message is heard only by the remote caller when dialling in. With this so-called pre-notification, an inbound call is answered by the V-Tap automatically, then the message is played and then the call is passed to the PBX.

The Notification Message Control field is a numeric value (bit-wise):

- +1** = Enable notification for incoming calls.
- +2** = Enable notification for outgoing calls.
- +4** = Enable Pre-notification mode for incoming calls.
- +8** = Force notification always on incoming calls, so also for calls that are not recording.
- +16** = Force recording always, so also for calls without notification.

For example, the value 5 does a pre-notification on incoming calls.

Note that pre-notification for outgoing calls is not possible.

The message itself is stored in a WAV file on the system and can be changed with an SD card or with FTP.

See [Notification & System Messages](#) for more information.

## DTMF \*\* Action Control

Also this setting is only available when the V-Tap PRI is operating in Pass-Through mode: see Jumper settings in [2.1.2](#).

The user can press DTMF \* twice on the phone to start or stop recording the ongoing call.

The DTMF \*\* Action Control field is a numeric value (bit-wise):

- +1** = Start recording; all calls are default **not** recording.
- +2** = Stop recording; all calls are default recording.
- +4** = Start or Stop can be pressed only once (disable toggling).
- +8** = Single DTMF \* needed for action.
- +16** = use DTMF # instead of DTMF \*
- +32** = Disable action from call that are in the numberlist.
- +64** = DTMF is detected from the remote side, else local side.

After start-recording, the notification is played (NOTIFY.WAV).

After stop-recording, the system beeps are played (BEEPS.WAV).

### 3.3.9 SD Card settings

The SD card is used to store the recorded calls onto. Without an SD card the recording of calls does not work. The V-Tap system stores the recorded data as a WAV file per call in the G.711 A-Law format. This takes 8000 bytes per second of storage space. The SD card must be FAT32 formatted and is used as a big cyclic memory buffer, because the oldest file is deleted automatically when the card is getting full.

The file names on the card are like "00000001.WAV", "00000002.WAV", etc. No call data can be extracted from the name, only the date and time of creation can be read from the directory list. The actual call data with phone numbers is enclosed inside the WAV header of each file and can be extracted by the Apresa or Call Recorder VoIP software on the PC. The WAV files are optionally encrypted, in which case they cannot be played directly by any media player (only noise is heard then).

In case of using a Tunnel server, the files are sent to the server as soon as they are closed. So, data is not sent live to the sever, but only after the call has ended or after a file has reached its maximum size.

In the case that no Tunnel server is used, the files are just stored on the card until the user gets the card out. SD cards with recorded files on them can be read and interpreted by the Call Recorder VoIP software on the PC.

Files are not deleted from the card by the system. Files are written until the card is full (error situation) or until the maximum number of files has been reached, in which case the oldest files are overwritten.

Another function for the SD card is to define a fixed IP address for the V-Tap unit; see [IP address](#). Yet another function is to update the firmware.



#### **Safely removal of the SD Card and Power Off.**

- . Press the button for 2 seconds (Amber & Blue LED OFF).
- . Release the button (Amber LED flashing).
- . Take out the SD card or the USB cable (power off).



### SD File Encryption

By default, the WAV files on the SD card can be played by any media player. By enabling the file encryption, the files only produce noise. The file encryption uses the same Encryption Password as the Tunnel encryption.

### SD Max Files on Card

The maximum number of files on the card has 2 purposes. First, it makes the directory on the card more manageable by the system and any PC. Too many files in one directory make a slow system. The default number of 10000 is reasonable. Secondly, a system can be built to use the card as an endless buffer, without the problem that the card is getting full. However, this must be calculated carefully and depends on the size of the card and the maximum file size (see below). After the maximum number of files has been reached, the file write-counter is reset and older files are overwritten automatically. The maximum tested size of the SD card is 32 GB and it must be formatted with the FAT32 file system.

### SD Max File Size in MB

When a file on SD card reaches the maximum file size, the file is closed for further writing and then send to the Tunnel server, if that function is enabled. The name counter is incremented at the same time and a new file is opened.

An ISDN recording produces 8 Kbytes per second. This means a little less than 30 Mbytes per hour. The default of 230 Mbytes is therefore enough for more than 8 hours per recording. A call that takes longer continues in the next file, without loss of data.

### SD Delete File after Sending

Normally, the files are kept on SD card and are not deleted by the system, except when the maximum number of files is reached in which case the oldest files are overwritten automatically. It is an option to delete files after the content was sent to a Tunnel server. A certain risk is taken then, because data cannot be recovered anymore after deletion.

### SD Interface Speed in MHz

This value must be changed only when there are problems with an SD card. The default is good for most of the cards on the market. Valid speeds to enter: 1 till 22 , 25 , 32 , 40 , 50 and 80.

## 3.3.10 Special network settings

### Max Data Length in Packets

This sets the maximum length of the data portion inside all communicated packets, including those from the Tunnel function, web interface and FTP.

The length excludes the Ethernet, IP and TCP headers, which are 54 bytes together. The maximum length of any packet on the network can be 1514 bytes, so that leaves max **1460** bytes for the data part. The default length is based on optimal performance when sending data from an SD card.

There is probably no need to ever change this parameter when the Tunnel is sending on a normal LAN. When sending directly on a WAN or very busy LAN, the length might be decreased for better performance (try 512).

### LAN Service Timer

The default value is for normal network speed. When a lot of V-Tap units are sending to the same Tunnel server, it might be better to lower the speed to prevent an overload of streams.

The values 65 and 1 can be used for slow and slower sending.

The values 18 and 50 can be used for fast and faster sending.

### MAC Address

The Media Access Control (MAC) address of the device is a unique identifier to communicate over an Ethernet network. The address cannot be changed.

### 3.3.11 App Special Flags

#### App Special Flags

This parameter represents a mixture of internal options and/or commands. When filled in as a numeric value, the used bits are all on/off switches as shown below. The result of the sum of the used bits must be entered as a decimal number. For example, setting both bit3 and bit12 results in the value  $8+4096 = 4104$ .

- bit0 (+1) : Disable Auto Delete function when SD card is almost full.
- bit1 (+2) : Enable SD Power Save Mode (slow clock during idle time).
- bit2 (+4) : Disable initializing the IP-stack instead of Tunnel Close.
- bit3 (+8) : unused
- bit4 (+16) : Force Half Duplex on the LAN port.
- bit5 (+32) : Force 10 Mbps on the LAN port.
- bit6 (+64) : Set time as Daylight Saving Time.
- bit7 (+128) : Disable Daylight Saving Time Correction in the NTP function.
- bit8 (+256) : Flash Overclocking (not safe to do).
- bit9 (+512) : Disable CPU Cash Controller (system much slower).
- bit10 (+1024) : Disable Memory Protect Unit (not safe to do).
- bit11 (+2048) : Disable USB function, so no HID recognition (saves power).
- bit12 (+4096) : Disable USB sleep function 10 minutes after start-up.

The App Special Flags field can also be used to enter commands for extra settings and features (most of them are preceded by a dot):

- "FACTORY" = Factory settings! The IP address is back on 192.168.55.66.
- "FACTORY WIFI" = Factory settings AND enable Wi-Fi module & settings.
- "FACTORY NOWIFI" = Factory settings AND disable Wi-Fi module & settings.

#### Extra ISDN & Recording settings:

- ".II" = Disable recording of Incoming calls.
- ".IR" = Record audio of Remote side only.
- ".IN" = Disable connected number for the number-list.
- ".IM" = Disable remote number for the number-list.
- ".IV" = Reversed IN<>OUT line operation.
- ".IF" = Enable Frame transmission with In-Line mode.
- ".IX" = Alternative Pass-Through method.
- ".IC" = Disable CRC-4 Multi-frame on the ISDN-E1 line.
- ".IA<num>" = Transmitter Amplification 1-255 (default 100).
- ".IS<num>" = Receiver Sensitivity 1-255 (default 96). 1024 enables AGC.
- ".IB<sec>" = Notification Beep interval in seconds, using "NBEEP.WAV".

## Extra Wi-Fi settings

- ".LAN" = Start with LAN cable and fallback to Wi-Fi connection.
- ".WF" = Disable Fallback from Wi-Fi to LAN cable.
- ".WC<num>" = Set Wi-Fi Channel ID; 1 till 13.
- ".WR<num>" = Set Wi-Fi RF TX Power; 0 till 82 per 0.25 dBm.
- ".WD" = Set the DNS server for Wi-Fi the same as the LAN cable.
- ".WN" = Disable NTP from Wi-Fi.
- ".WI<ip>" = Set IP address for web server access, default 192.168.55.66
- ".WH" = Set DHCP range <ip>1 till <ip>9 when using .WI.
- ".WK<num>" = Keep-alive timer in seconds for Wi-Fi Tunnel connection.
- ".WL" = Disable web Login page after Wi-Fi connection.
- ".WT<num>" = Set Timeout in seconds for the TCP web server; default 90.
- ".WUP" = Update Wi-Fi module (version returned in App Special Flags).
- ".WZ0/1" = Disable/Enable Wi-Fi module during recording.

## Extra SD card settings

- ".CS" = Show all current SD file-counters in the App Special Flags.  
**Note:** The Read file-counter on 0 will resend all files again!
- ".CR<num>" = Set SD card Read file-counter from 0 till 32767.
- ".CW<num>" = Set SD card Write file-counter from 0 till 32767.
- ".CD<num>" = Set SD card Delete file-counter from 0 till 32767.

## Debug settings

- ".D" = Debug mode enabled. Output to serial port only.
- ".D<time>" = Debug enabled and update set per 10ms (default 1 sec).
  
- ".D.T" = Open Debug Trace file. The file TRACE.TXT is closed again after web login. Then ".D.T" must be removed from the App Special Flags and the settings must be saved. Then TRACE.TXT can be downloaded with ftp.
  
- ".DT" = Open D-channel Trace file. The file DTEST.TXT is closed again after web login. Then ".DT" must be removed from the App Special Flags and the settings must be saved again. Then DTEST.TXT can be downloaded with ftp. Recording is not possible when a D-channel trace is active!

### 3.3.12 Licenses & Versions

#### Licenses: Apresa / PC / S&U

The Channel Licenses for Apresa and PC and the Support & Update end-date are shown here.

The Channel Licenses are also used as Recording Licenses, so they show the maximum number of simultaneously recorded calls from the ISDN PRI line.

At least one Channel License is needed before the system starts recording any calls and before uploading to the Tunnel server is possible.

Adding new licenses is further described in the separate quick guide about V-Taps and Licenses.

#### New License Key

This field is used when new licenses must be added. This is further described in the separate quick guide about V-Taps and Licenses.

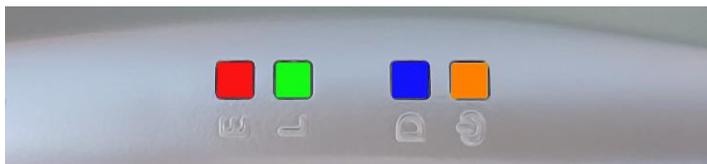
#### V-Tap ISDN PRI OS Version

#### V-Tap ISDN PRI App Version

#### V-Tap ISDN PRI Serial Number

Firmware versions and the serial number are shown for information purposes only and cannot be changed.

## 4 LED's



E = Error (Red)  
L = Link (Green)  
D = Data (Blue)  
@ = SD-Power (Amber)

The 4 LED's are important for feedback to the user. Specially during first installation, the LED's can tell you if things are going wrong or right.

Situations with the LED's that are related to pressing the button are described in the next chapter [Button functions](#) .

The situations during normal operation are described below, per LED.

### 4.1 Red Error LED

The Red LED is used to indicate an error situation.

- *Red LED steady ON plus Amber LED blinking.*  
This is the factory default and means that no SD card is inserted, so no data is stored. Inserting an SD card solves the situation.
- *Red LED steady ON plus Amber LED blinking fast.*  
A read- or write-error happened on the SD card or the SD card is not usable by the system. This can only be solved by removing the card again. Check if the card lock-switch is on, else it is recommended to verify the card on an external PC.
- *Red LED steady ON plus Amber steady ON.*  
This can happen as soon as a call starts, and the system has no Recording Channel Licenses.

- *Red LED blinking plus Green LED blinking.*  
The system cannot connect to the Tunnel server.  
See also *Green LED blinking* below.
- *Red LED blinking once per second.*  
This happens when you take out the SD card while the system was still busy writing to it. So, an unclosed (0 bytes) file is now on the card. For more information, see [Remove SD Card safely](#).
- *Red LED blinking fast.*  
This indicates that the ISDN line is disconnected.
- *Red LED blinking fast, together with all other LED's.*  
This happens after a fatal error in the application. The firmware must be updated.

## 4.2 Green Link LED

The Green LED shows the status of the link to the Tunnel server.

- *Green LED blinking.*  
The system tries to connect to the Tunnel server. This can last forever, but normally it should take a few seconds after reset. When longer, the Tunnel server could not be found, or the network connection is bad. The Red LED also starts blinking in that case. Check the **firewall** on the PC or switch!  
The Green LED goes to steady ON when a connection is made.
- *Green LED steady ON.*  
The link to the Tunnel server is OK.
- *Green LED OFF.*  
The only normal situation with the Green LED OFF is, when no Tunnel server is defined in the settings.

## 4.3 Blue Data LED

The Blue LED blinks when data is stored during recording.

- *Blue LED blinking.*  
The Blue LED is on to indicate that audio data is stored. In other words, recording is active, so a file is opened on the SD card and data is written to it.  
Also during Wi-Fi initialization, the Blue LED can blink shortly.

## 4.4 Amber SD-Power LED

The Amber LED shows the status of the SD card.

- *Amber LED steady ON.*  
This indicates that an SD card is inserted and is ready to be used by the system.
- *Amber LED blinking short (Red LED OFF).*  
This indicates that an SD card is inserted, and the system is reading data from a file during sending with the Tunnel function.
- *Amber LED blinking fast (Red LED ON): SD card ERROR.*  
A read- or write-error happened on the SD card or the SD card is not usable by the system. The card must be removed and checked.

## 5 Button functions



The various button functions are described in the following paragraphs.

### 5.1 Remove SD Card safely

In the case the SD card is taken out without precaution, the current open file is not closed properly and will have a content of zero bytes. The appearance in the directory remains. Also, there is a very small chance that the directory or some file gets corrupted by doing so. Therefore, to take out the card safely it is recommended to close all files first with the following procedure:

- **Press the button: All LED's are ON.**
- **Hold pressed for 2 seconds: Amber and Blue LED go OFF.**
- **Release the button: Amber LED starts flashing.**
- **Take out the SD card safely now.**

**NOTE:** When the Blue LED is not blinking, then no recording is busy, so no data is written, in which case the SD card can just be taken out.

## 5.2 Enable DHCP temporary

When running with default settings, there is a way to enable DHCP temporary. Then the settings page can be reached through the web interface and DHCP can be set permanently or a fixed IP address can be defined. If no settings are done, then DHCP is disabled again after reset.

- Press the button: All LED's are ON.
- Hold pressed for 1 second.
- Release the button: Red, Green and Blue LED's flash 3 times
- After about 2 seconds Red, Green and Blue flash again if an IP address is assigned by the DHCP server.
- The V-Tap can show the IP address with the LED's, see below.
- Or the IP address must be obtained with some network tool.
- The web page is now reachable on this IP address.

## 5.3 Show IP address

The IP address of the V-Tap unit can get lost for some reason or is unknown because a DHCP server is used. In other words, the user cannot reach the web interface anymore. There is a way to reset all settings to factory values (see further), after which the IP address is on default again. If that is not desirable, then there is a way to show the IP address with the LED's:

- Press the button: All LED's are ON.
- Hold pressed for 5 seconds: All LED's go OFF.
- Release the button: Only the Green LED goes ON.
- Press the button now and the first digit is shown:
  - Green LED goes OFF,
  - Red LED blinks the first decimal digit (count!),
  - Green LED goes ON when finished.
- Repeat pressing the button for the next digits. For example: "192.168.0.10" needs the button to be pressed 12 times.
- The Blue LED blinks once to show there is a dot in the address.
- When no Green or Blue is blinking at all in between Green going OFF-ON, it means the zero digit.
- After the last digit, the system waits 5 seconds and then continues normal operation.

## 5.4 Factory settings

To reset all settings to factory default, the following must be done:

- Remove the SD card.
- Power off the unit.
- Press the button.
- Power on and hold the button pressed; all LED's are ON.
- Release the button within 5 seconds; RGB LED's go OFF.
- Press the button 5 times again; RGB LED's blink fast.
- After 5 seconds, the system reboots automatically.

The procedure above is only possible when the system is running normal. With corrupted firmware, a special update must be done with an SD card (see [Firmware update](#)).

## 5.5 Default IP address

When the application does not seem to run at all anymore, then a reset to factory settings is not possible. Besides a special update with the SD card (see below), there is still a way to look with FTP in the filing system remotely. The following can be done:

- Remove the SD card.
- Power Off the unit.
- Press the button.
- Power On and hold the button pressed for 1 second.
- Release the button.
- The IP address is now on default 192.168.55.66
- Only access with FTP is now possible (no web interface).

## 5.6 Firmware update

When a firmware update must be applied, there are two possible states:

### I. The system is running normal.

When the system is accessible through FTP, the firmware can be updated with the PC tool 'vcUpdater'. This tool can be found on the Vidicode website in the menu Service and Support > Firmware.

Another way to update is by using an SD card as follows:

- The manufacturer must provide the necessary files first.
- Prepare an SD card with all unzipped files in the root directory.
- The V-Tap unit must run normal.
- Hold the button pressed while inserting the SD card.
- All LED's start flashing.
- Release the button, then update starts immediately.
- Normal operation resumes after maximal 30 seconds.

At least the files UPDATE.SD and PTAP.ROM and/or PTAP.CPY must be on the card. The files SAVECONF, DELCONF and CLEARROM are optional.

### II. The system is not running at all.

The following method is always valid to update or re-install the firmware (if the SD interface is still working):

- The manufacturer must provide the necessary files first.
- Prepare an SD card with all unzipped files in the root directory.
- Power Off the V-Tap unit.
- Insert the SD card.
- Hold the button pressed while applying power (insert USB cable).
- All LED's start flashing.
- Release the button, then update starts immediately.
- Normal operation resumes after maximal 30 seconds.

The files BOOT, UPDATE.SD , VTAP.ROM and VTAP.CPY must be on the card. The files SAVECONF, DELCONF and CLEARROM are optional.

## 6 Notification & System Messages

The following audio files are used by the system:

- NOTIFY.WAV** : The Notification message. This file is played by the system when the notification is enabled and a recording starts. The message usually says something like: "Welcome.... this call will be recorded...". Also, each time DTMF \*\* starts a recording, this message is heard.
- NOUTG.WAV** : Notification message for outgoing calls. This is used when notification is enabled and when this file exists. Default, this file does not exist on the system.
- NBEEP.WAV** : Notification beep. Used when ".IB<sec>" is entered in the App Special Flags. A short beep is heard by both parties during the whole conversation.
- BEEPS.WAV** : System beeps. This file is played by the system and heard by both parties of the call when a recording is stopped with DTMF \*\* or when a recording starts and NOTIFY.WAV does not exist.
- ALERT.WAV** : Alerting (ringing) tone. This message is heard by the caller, after the system played the notification and transferred the call to the PBX, before the local phone is picked up. Only used in pre-notification mode.

### Format of the messages:

G.711 A-Law, 8000 Hz (64 Kbps), Mono.

### Putting the messages onto the system:

1. With an SD card:  
Put your .WAV file(s) in the root of an SD card.  
Insert the SD card into the V-Tap. The system will automatically copy the file(s) to its internal memory and delete the file(s) from the card.  
Then the system reboots and the new messages are used.
2. With FTP:  
Connect to the V-Tap with FTP and upload your .WAV file(s).

## 7 Number-list (Black- or White-list)

The V-Tap ISDN can record the calls depending on the local telephone number. A text file containing a list of numbers must exist in the V-Tap:

**BLACK.TXT** : A black-list is used.  
**WHITE.TXT** : A white-list is used.

Only one of these two files can be active at the same time. When both exist, then BLACK.TXT is taken.

### When using a black-list:

If the number is found in the black-list, the call is not recorded. All other numbers/calls are recorded.

### When using a white-list:

If the number is found in the white-list, the call is recorded. All other numbers/calls are not recorded.

### Putting the number-list onto the system:

1. With an SD card:  
Put the file BLACK.TXT or WHITE.TXT in the root of an SD card. Insert the SD card into the V-Tap. The system will automatically copy the file to its internal memory and delete the file from the card. Then the system reboots and the new list is active.
2. With FTP:  
Connect to the V-Tap with FTP and upload BLACK.TXT or WHITE.TXT.

### Rules for the number-list:

- The black- or white-list can hold maximal 100 numbers.
- All numbers must be put on a separate line.
- Empty lines are not allowed in the list. They mark the end of the list.
- The numbers in the list must have the same format as on the ISDN line, but without preceding zero's (0793471001 becomes 793471001).
- It is also possible to enter the last (right-most) digits only of each number. But then, all entries must have the same length!
- The wildcard character "\*" can be used to denote a range (79347\*).

## 8 Remote control with UDP commands

The V-Tap ISDN PRI can send information and receive commands over the network, using UDP packets.

The UDP packets are only activated when this is enabled in the V-Tap. To enable UDP packets do the following:

- On the PC edit a text file, called VMON.TXT
- On the first line of VMON.TXT enter the IP address of the system that receives UDP packets.
- Optionally, the second and third lines can hold the UDP port numbers (destination and source).
- The file VMON.TXT must be placed in the root of an SD card.
- The SD card must be inserted into the V-Tap; VMON.TXT is deleted and the V-Tap reboots.
- UDP is now automatically enabled and call information is sent to the defined IP address.

The file VMON.TXT can also be put onto the V-Tap using an FTP connection.

### UDP Port numbers

When no other ports are defined in the file VMON.TXT, the port number 1001 is used as the destination and the source port. This means that the server software must listen and send commands on UDP port 1001.

### UDP information packets, send by the V-Tap

The V-Tap sends an information packet at the start and at the end of each call. An information packet contains one text string. The format is already used in the Vidicode RTR Call Monitor software for the PC and looks as follows:

Start of a call string = **"Z-file..."**  
End of a call string = **"HANGUP:Z-file..."**

The **"Z-file..."** represents a file name of 68 characters long (fixed length), containing all call information.

The Vidicode Call Recorder VoIP software for the PC also uses this name format.

The extension .WAV is added by the software before the file is stored.

The same file name can also be found inside the file, in the note-field of the WAV header and contains the following information per character:

Char.1 = "Z" = Archived recording.  
Char.2 = "C" = The recording is a recorded Call.  
Char.3 = year = "0"- "9" = 2000-2009 or "A" - "Z" = 2010-2035  
Char.4 = month = "1"- "9" = 1-9 (jan-sep) or "A"- "C" = 10-12 (oct-dec)  
Char.5 = day = "1"- "9" = 1-9 or "A"- "V" = 10-31  
Char.6 = hour = "0"- "9" = 0-9 or "A"- "N" = 10-23  
Char.7 = min.H = "0"- "5" = 0-5  
Char.8 = min.L = "0"- "9" = 0-9  
Char.9 = secs = "0"- "9" = 0-18 (x2) or "A"- "T" = 20-58 (x2)

Char.10 – 15 = "\_\_\_\_\_" = No additional information  
or = "00MMSS" = Waiting Time before Answering

Char.16 = WAV codec format:  
"0" = Empty file used for statistics & lost calls  
"6" = G.711 A-Law Mono 8000 Hz, Non-encrypted  
"8" = G.711 A-Law Stereo 8000 Hz, Non-encrypted  
"F" & "V" = G.711 A-Law Mono 8000 Hz, Encrypted on SD card only  
"H" & "X" = G.711 A-Law Stereo 8000 Hz, Encrypted on SD card only

Char.17 + 18 = **V-Tap ID** = "00" till "ZZ"

Char.19 = Line number = "1"-"9" or "A"-"V" = ISDN B-channel 1-9 or 10-31

Char.20 = Call direction = "1" = Incoming , "0" = Outgoing

Char.21 – 36 = Local telephone number  
Char.37 – 52 = Remote telephone number  
Char.53 – 68 = Connected number

*Char.69 – 80 = V-Tap MAC address (only in WAV header)*  
*Char.81 – 83 = Apresa Channel Licenses (only in WAV header)*  
*Char.84 – 86 = PC Channel Licenses (only in WAV header)*

## UDP command packets, received by the V-Tap

A command is a simple text string. After receiving a command, the V-Tap always sends back a reply string. The following commands are recognized by the V-Tap:

<b>Command</b>	<b>Description</b>	<b>Reply</b>
PING	[check connection]	OK-<id>:PING
INFO	[V-Tap model]	INFO-<id>:ISDN30
NAME	[V-Tap name]	NAME-<id>:<V-Tap device name>
CLOCK	[read clock]	CLOCK-<id>=<date>,<time>
CLOCK,<date>,<time>	[set clock]	CLOCK-<id>=<date>,<time>
BUSY,<line1-31>	[check busy]	OK- or NOP-<id>:BUSY,<line>
START,<line1-31>	[start recording]	OK- or NOP-<id>:START,<line>
STOP,<line1-31>	[stop recording]	OK- or NOP-<id>:STOP,<line>
PAUSE,<line1-31>	[pause recording]	OK- or NOP-<id>:PAUSE,<line>
RESUME,<line1-31>	[resume recording]	OK- or NOP-<id>:RESUME,<line>
PLAY,<line1-31>,<file>	[playback WAV file]	OK- or NOP-<id>:PLAY,<line>

<id> is the V-Tap ID, the same as characters 17+18 in the file name above.  
<date>,<time> has the format "dd-mm-yy","hh:mm:ss" (14-12-18,16:35:07).  
A recording command for a non-busy channel sends a "**NOP**..." message back.  
An unknown or bad command sends an "**ERR**.." message back.

## 9 ISDN PRI RJ45 connectors & wiring

The connectors used on the PRI to connect the telephone trunk (E1 only) and the PBX, are RJ45 modular types. The pin-assignment is based on the G.703 standard.

Please note that the pinning of the 2 IN/OUT connectors is different.

Label on PRI →	"ISDN IN"		"ISDN OUT"	
Connect to →	PSTN / E1 trunk		PBX	
PRI - PIN nr	PRI signal	Connect to	PRI signal	Connect to
1	Input = R+	T+	Output = T+	R+
2	Input = R-	T-	Output = T-	R-
3	x	x	x	x
4	Output = T+	R+	Input = R+	T+
5	Output = T-	R-	Input = R-	T-
6	x	x	x	x
7	x	x	x	x
8	x	x	x	x

Looking inside the PRI connectors, pin 1 is on the *right-hand* side of the RJ45 connector.

The Rx twisted pair and Tx twisted pair have approx. 120 Ohm impedance.

The PRI interface circuits support the 'Short Haul' interface implementation. Generally, this means that the hazard protection scheme of the PRI E1 interface allows wiring inside buildings only.

### Cable Specification suggestion

24AWG / 2 pairs / 100-120 Ohm impedance, no shielding required. Generally, CAT 2 cable or better will work fine.

### For use in The Netherlands only

The pin assignment on the PRI allows the use of standard 1:1 CAT 5 network cable for the connection to the incoming line from the provider unit and the outgoing connection to the PBX. It has shown that this is also the situation for many other countries.

## 10 Revision History

### V1.4 December 2018

- New chapter: Remote control with UDP commands.

### V1.3 November 2018

- New chapter: Checklist for Tunnel connection.
- Picture in Apresa install replaced.

### v1.2 September 2018

- Page numbers on the right side & changes in the text.
- Recording Licenses removed.

### v1.1 July 2018

- Small changes in the text.

### v1.0 April 2018

- First release.

# **11 Acknowledgements**

## **11.1 Privacy**

When recording telephone conversations, the privacy of your conversation partner must be considered.

In some countries, there is an obligation to notify your conversation partner of the recording. Check your national legal obligations on this and other issues concerning the use of any Call Recorder.

Vidicode is not a source of official interpretation of laws of any country or state and shall not be construed as a source for making decisions whether to provide notification or not. Vidicode assumes no liability regarding incorrect notification of call recording.

## **11.2 Liability**

Correct functioning of the V-Tap ISDN PRI cannot be guaranteed under all conditions and thus we do not accept any liability for loss of information or other damages due to the use of the V-Tap ISDN PRI.