

V-Tap ISDN PRI

Manual

v1.25



Contents

1	Introduction.....	5
2	Getting started.....	6
2.1	Hardware installation.....	6
2.1.1	Sniff mode operation.....	7
2.1.2	Pass-Through mode operation.....	7
2.1.3	Parallel connection.....	8
2.1.4	In-Line connection.....	8
2.2	Software installation.....	9
2.2.1	Call Recorder Apresa.....	9
2.2.2	V-Archive software on a PC.....	10
2.3	Checklist for Tunnel connection.....	11
3	Web interface and Settings.....	12
3.1	Access & IP address.....	12
3.2	Web interface.....	13
3.3	Settings.....	15
3.3.1	General Network settings.....	15
3.3.2	Tunnel settings.....	17
3.3.3	Special Tunnel & Network settings.....	18
3.3.4	Wi-Fi settings.....	20
3.3.5	Login settings for Web access & FTP.....	21
3.3.6	NTP and Date+Time settings.....	22
3.3.7	ISDN PRI settings.....	23
3.3.8	Black/White-list Numbers.....	25
3.3.9	Special Settings & Commands.....	26
3.3.10	Licenses & Versions.....	29

4	LED's	30
4.1	Red Error LED	30
4.2	Green Link LED	31
4.3	Blue Data LED	32
4.4	Amber SD-Power LED	32
5	Button functions	33
5.1	Remove SD Card safely	33
5.2	Disable DHCP temporary	34
5.3	Show IP address	34
5.4	Copy Settings from SD card	35
5.5	Factory settings	35
5.6	Format SD card	35
5.7	Default IP address	35
5.8	Temporary access with Wi-Fi	36
5.9	Firmware update	37
6	SD card usage	38
6.1	Special SD card settings	39
7	Notification & System Messages	42
8	Number-list (Black- or White-list)	43
9	Telnet connection	44
10	Remote control with UDP commands	45
11	D-channel trace for debug	47
12	ISDN PRI ports & wiring	48
13	Revision History	49

14	Acknowledgements	50
14.1	Privacy	50
14.2	Liability	50

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 calls are stored digitally onto an SD card in WAV files, and therefore the V-Tap ISDN PRI can operate stand-alone. The content of the SD card can be 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 a Windows PC running the [V-Archive software](#). The external Apresa recorder or V-Archive 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 V-Archive software. Note that, without a Channel License for Apresa or PC, the V-Tap ISDN PRI does not produce WAV files or store any data on the SD card.

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 days or even weeks.

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 recording solutions. There are V-Taps for VoIP, Analog, Audio, Audio and ISDN telephony and there is a V-App for mobile recording. All of these products will communicate with the Apresa Corporate or Apresa Cloud-based recording solutions.

NOTE 1: The V-Tap ISDN PRI needs to be powered through USB with 500 mA and a FAT32 formatted SD card must be inserted.

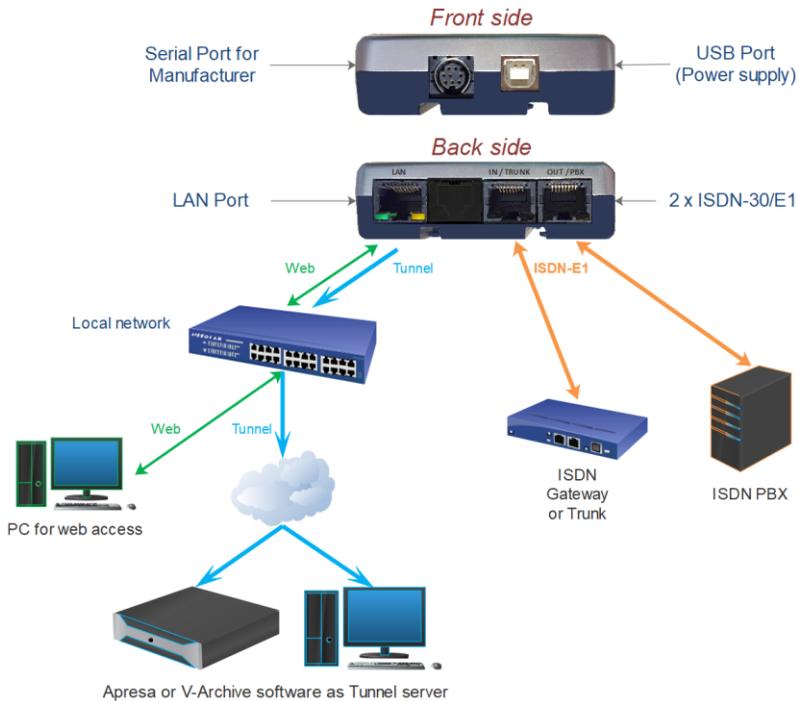
NOTE 2: The V-Tap ISDN PRI needs at least one Recording Channel License, else no calls are stored on the SD card.

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 USB to the V-Tap for power (500 mA).
- Connect the local network.
- Access the settings in the [web interface](#) by using a browser.



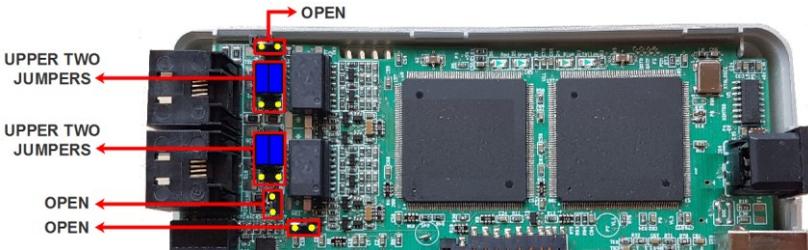
The two possible modes of operation (Sniff or Pass-Through) must be set with the internal jumpers and are described in [2.1.1](#) and [2.1.2](#) .

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 ports 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 ports 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:

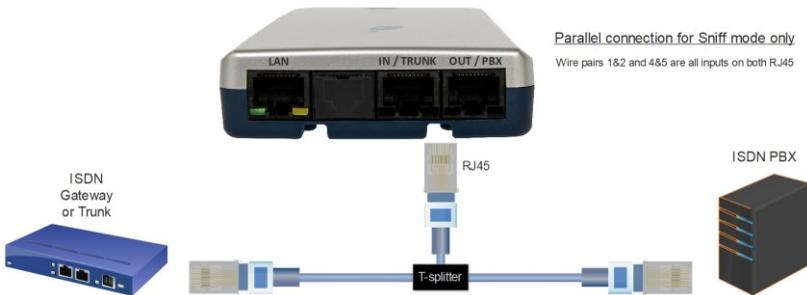


2.1.3 Parallel connection

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.

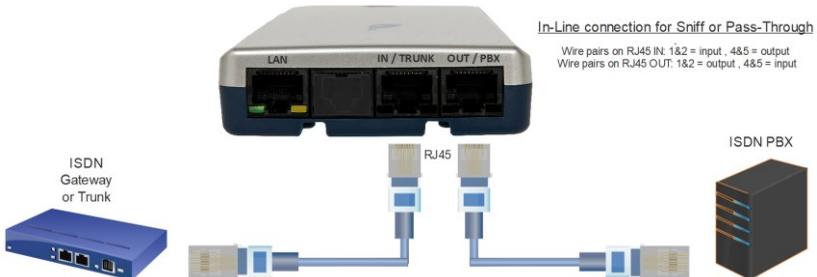
Only one of the ISDN ports needs to be connected to the line. Using the IN- or OUT-port makes no difference in this case, because the wire pairs (1&2 and 4&5) on both ports are all inputs. This way of connecting is only possible for Sniff mode.

Parallel connection can use a simple 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) and 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:



For more details about the wiring, see [ISDN PRI ports and wiring](#).

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 directly from the V-Tap, can be sent to the [Call Recorder Apresa](#) or the [V-Archive software](#).

NOTE:

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

2.2.1 Call Recorder Apresa

The [Call Recorder Apresa](#) is recorder software running on the Linux Debian 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 page for V-Tap. The settings are as follows:

- V-Tap:
- V-Tap Tunnel port number: 2016
- V-Tap over TLS:
- V-TAP over TLS Port: 2017
- V-TAP over TLS Certificate: None
- V-Tap Data separation:
- Accept only known V-Taps:
- Accept only encrypted V-Tap connections:
- Store V-Tap recordings in received format:
- V-Tap Encryption password: Default: [empty field]

MAC address	Encryption password	Tenant	Name	Delete
None				

Buttons: Add, Delete

Always generate an alarm when a V-Tap in the table is not connected:

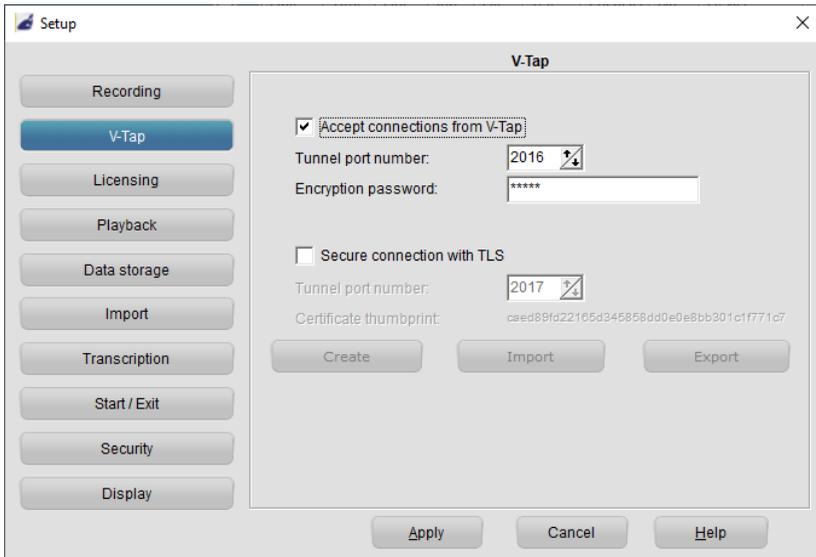
NOTE1: Apresa’s IP address is the “Tunnel Server Address” in the V-Tap.

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

2.2.2 V-Archive software on a PC

The [V-Archive software](#) for the PC can, just as the Apresa, receive Tunnel data from the V-Tap ISDN, convert this data into audio files and store the files into its own database. The V-Archive software can also receive multiple data streams from different V-Tap units simultaneously.

To setup the V-Archive 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.

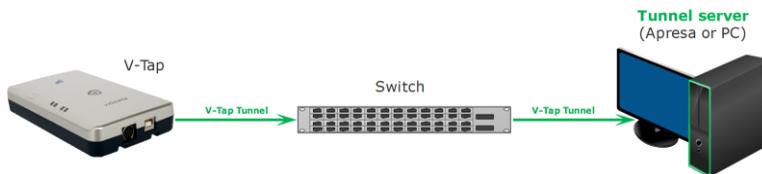
NOTE2: Be sure that the PC's firewall is open for TCP port 2016, the default "Tunnel Destination Port" in the V-Tap. During installation, V-Archive tries to open port 2016 in Windows.

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

NOTE4: The V-Archive software itself does not need licenses to receive from the V-Tap. Licenses are inside the V-Tap.

The V-Archive software for the PC is further not described in this manual; see for more details the [V-Archive 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 Apresa or V-Archive PC [Software](#) and enable V-Tap connections.
- 3) Open the [Settings page](#) of the V-Tap in a browser, <http://vtapXXXX.local> XXXX are the last 4 digits of the MAC address, found on the bottom.
It may take up to a minute after first connect, before this local name is known to the PC.
- 4) On that page, the IP address of the Apresa or the PC with V-Archive must be entered as the "[Tunnel Server Address](#)".
- 5) Any **firewall** must have a rule that makes it possible to receive from TCP port **2016**, the default "[Tunnel Destination Port](#)".
During installation of V-Archive this port is automatically opened, if permitted by the PC.
- 6) The Tunnel connection is stable when the **GREEN LED is steady**, not blinking!
The V-Tap must be shown with its MAC address in the status line of V-Archive.
- 7) For first tests, better turn off "Tunnel Data Encryption". Otherwise, be sure that the Encryption password is the same in both V-Tap and Apresa or PC.
- 8) When data is stored during a call, the **BLUE LED** blinks.
- 9) To see if the PC receives something from the V-Tap, it is possible to make a network trace for test purposes. In V-Archive, go to menu Actions and select 'Network trace', press Start, make a short call, wait 10 seconds, press Stop and then Save. From the zip file 'tunneltrace.pcap' can be analyzed with Wireshark.
The Apresa recorder has a similar option to make a network trace in menu Tools, System.
- 10) The SD card in the V-Tap should contain ".WAV" files. This SD card can be read by the V-Archive software in menu File and 'Import from V-Tap'.

3 Web interface and Settings

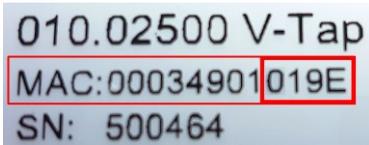
There are two ways to access the web interface of the V-Tap:

- 1) Connect a network cable to the LAN port on the unit. The other side of the cable can be connected to a LAN or directly to a PC.
- 2) The built-in Wi-Fi module may not be enabled by default. To enable [temporary](#), power off and remove the SD card. Hold the button pressed during power on and keep pressed for about 12 seconds until only the Blue LED is on. Release the button, then Wi-Fi is available until the next reboot.

3.1 Access & IP address

In the case of using Wi-Fi, you need to enter the Wi-Fi access password first, which is the 12 digits MAC address of the V-Tap, also found on the bottom of the box. When connected (without internet), the IP address **192.168.55.66** must be entered in a browser. Remember to disabled mobile data on your phone (!), else this IP address is not found.

In the case of using a cable, DHCP is enabled and the V-Tap can be accessed with a browser by entering the address <http://vtapXXXX.local> In which **XXXX** are the last 4 digits of the MAC, as found on the bottom:



For this V-Tap:

Default cable address:	http://vtap019e.local
Default web Username:	admin
Default web Password:	admin
Default Wi-Fi Password:	00034901019E < <i>capitals here!</i>
Default Wi-Fi IP address:	192.168.55.66

<p>If no DHCP server is available on the cable, it can be disabled temporary by pressing the button for 1 second. The LED's will flash shortly and the V-Tap can be accessed on the IP address 192.168.55.66 See also Disable DHCP temporary and Show IP address.</p>
--

If still no access is possible, the easiest way to set a new fixed IP address is to use an SD card:



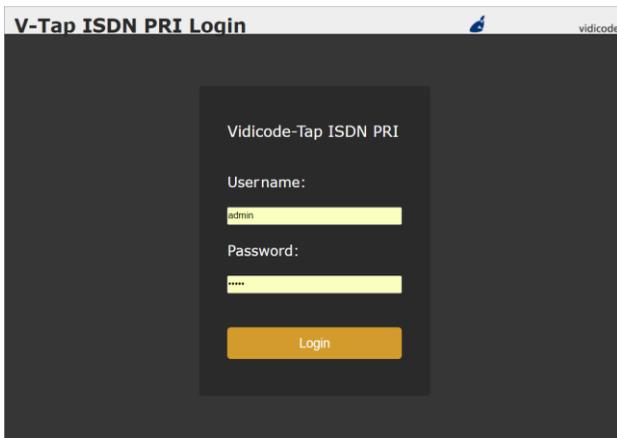
Defining a fixed IP address with an SD card:



- . Create the text file “**IP**” on your PC.
- . 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 address in your browser will show the following screen:



Now enter “admin” for the Username and “admin” for the Password, then press the **Login** button and the Settings page appears:

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

V-Tap ISDN PRI Settings 07-12-20 13:25:22  Vidicode

Name of this V-Tap	V-Tap_PRI_BCBDBD ⓘ	Login Username	admin ⓘ
DHCP Server	<input checked="" type="checkbox"/> ⓘ	Login Password	**** ⓘ
IP Address	192.168.0.27 ⓘ	NTP Server Address	pool.ntp.org ⓘ
Subnet Mask	255.255.255.0 ⓘ	GMT Minutes Correction	60 ⓘ
Gateway Address	192.168.0.5 ⓘ	New Date (DD-MM-YYYY)	ⓘ
DNS Server Address	8.8.8.8 ⓘ	New Time (HH:MM:SS)	ⓘ
Tunnel Server Address	recording.vidicode.com ⓘ	Record Outgoing Calls	<input checked="" type="checkbox"/> ⓘ
Tunnel Destination Port	2018 ⓘ	Record Local Side only	<input type="checkbox"/> ⓘ
Tunnel Data Encryption	<input checked="" type="checkbox"/> ⓘ	Stereo Recording (else Mono)	<input type="checkbox"/> ⓘ
Encryption Password	**** ⓘ	Reversed D-channel Operation	<input type="checkbox"/> ⓘ
Wi-Fi Access Point	<input type="checkbox"/> ⓘ	Notification Message Control	0 ⓘ
Wi-Fi Tunnel AP Name	ⓘ	DTMF "*" Action Control	0 ⓘ
Wi-Fi Tunnel AP Password	ⓘ	Licenses: Apresa / PC / S&U	30 / 0 / 31-12-2021 ⓘ
Black/White-list Numbers	ⓘ	New License Key	ⓘ
Special Settings & Commands	ⓘ	License Activation	
		V-Tap PRI OS Version	1.0.29 07-12-2020 ⓘ
		V-Tap PRI App Version	7.2.29 03-12-2020 ⓘ
		Serial Number / MAC Address	250661 / 0003496CBDBD ⓘ

Putting the mouse cursor on the ‘i’ behind a setting, will show extra information about that setting.

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

Name of this V-Tap

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 not used in the Tunnel protocol. The maximum length is 30 characters. The single and double quotation marks (' and ") cannot be used !

DHCP Server

Default, DHCP is enabled and the V-Tap can be accessed with a browser by entering the address <http://vtapXXXX.local> XXXX are the last 4 digits of the MAC address, found on the bottom. When a DHCP server is available on the network, the IP address, Subnet mask, Gateway address and DNS address are automatically assigned. Without DHCP, they must all be entered manually. With default settings, DHCP can be disabled temporary by pressing the button for 1 second, see [Disable DHCP temporary](#). The DHCP setting is not used for Wi-Fi connections.

IP Address

As part of the local network, the V-Tap needs an IP address. In case DHCP is used, the DHCP server will assign the V-Tap an IP address. In case DHCP is not used, a static IP address must be filled in. The default address is 192.168.55.66 , see also [Access & IP Address](#).

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 V-Tap 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 hostname of the Tunnel server that is going to receive the recordings coming from the V-Tap ISDN. Leaving this field empty will disable the Tunnel function all together, in which case the V-Tap only stores recordings onto the SD card. The receiving server can be an Apresa recorder or a PC running the V-Archive 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 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 V-Archive software, must use the same password. Leaving the password empty is still doing the encryption but is less secure. Comma's and single and double quotation marks cannot be used !

3.3.3 Special Tunnel & Network settings

Next follows a description of some settings for the Tunnel and network, which must be entered in [Special Settings & Commands](#).

.TS<port> = Tunnel Source Port (default 0 = random)

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.

It is therefore not recommended to select a fixed number for the Tunnel Source Port in cases where live streaming is done without using an SD card.

 **.TC<sec> = Tunnel Connect Timeout (default 22 seconds)**

This timeout is used when the V-Tap ISDN 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 the timeout, the V-Tap starts trying again after a few seconds with a new source port number (see above). Storage onto SD card just continues and is not interrupted by any connection or disconnection of the Tunnel.

 **.TI<sec> = Tunnel Idle Timeout (def 0 = always connected)**

This timeout is used to disconnect the active tunnel connection, only when no packets are received (sniffed) anymore from the local connected network. Default, the idle timeout is disabled and the tunnel stays connected forever.

 **.TK<sec> = Tunnel Keep-alive Timer (default 60 seconds)**

This timer is used to keep the connection alive between the V-Tap and the Tunnel server. Default, a dummy TCP packet is sent every 60 seconds by the V-Tap to the server.

 **.LX<size> = Maximum Data Size in packets (default 1024)**

This sets the maximum length of the data portion inside all communicated packets on the network for Tunnel, FTP and Web. 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.

When sending directly on a WAN or very busy LAN, the length might be decreased for better performance (try **.LX512**).

 **.LS<num> = LAN System Service Timer (default 18 = fastest)**

The default value is for fastest 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 50 and 18 (same as 0) can be used for faster sending.

NOTE: When using the RTR Call Monitoring Software for the PC, the LAN Service Timer must be set to 1 to get a constant audio stream.

3.3.4 Wi-Fi settings

The Wi-Fi module in the V-Tap may not be enabled by default. To enable temporary do the following:

Power off and remove the SD card. Hold the button pressed during power on and keep pressed for about 12 seconds until only the Blue LED is on. Release the button, then Wi-Fi is available until the next reboot.

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:

- Search for Wi-Fi apparatus on your smartphone or laptop, the V-Tap 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 box. The first 6 digits of the MAC are always 000349 and the last 6 digits are also part of the Wi-Fi name.
- Disable mobile data on your phone (!), open a browser and enter the IP address 192.168.55.66. The web login page should appear. Login with username "admin" and password "admin".

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.

Wi-Fi Access Point

This enables or disables the web access using Wi-Fi permanently. The [temporary access](#) with the button is always available. The password to connect with Wi-Fi can be changed in the [Login 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. All further access must then be done through a LAN cable.

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

3.3.5 Login settings for Web access & FTP

The internal web server can be accessed by entering the address of the V-Tap in the address bar of any browser. See also [Access & IP Address](#).

The V-Tap also 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 [Firmware update](#).

FTP is disabled by entering ".FP0" in [Special Settings & Commands](#).

Login Username

Username to log in to the Web settings page and FTP.
The username field can be maximum 30 characters long.
Spaces, commas, the single and double quotation marks (' and "),
and the back- and forward-slashes (\ and /) cannot be used !
The default username is "admin".

Login Password

Password to log in to the Web settings page and FTP and [Telnet](#).
The total password field can be maximum 30 characters long.
Spaces, commas, the single and double quotation marks (' and "),
and the back- and forward-slashes (\ and /) cannot be used as the
password ! The default password is "admin".

The option **W<xxxxxxxx>** can be added to set the Wi-Fi password.
This Wi-Fi password must be minimal 8 characters long.

3.3.6 NTP and Date+Time settings

NTP (Network Time Protocol) can be used to synchronize the internal clock. The V-Tap ISDN 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 packet in the Tunnel protocol and is therefore very important to get the date and time right for all recorded calls. Specially, when Tunnel data is first stored on an SD card and later interpreted by the V-Archive software on the PC.

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

The default port number for NTP is 123 and can be changed by entering ".NP<port>" in [Special Settings & Commands](#).

NTP Server Address

The IP address or the hostname 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.

The option /X can be added behind the address to disable the Summer Time (Daylight Saving Time) correction.

Make this address field empty when no NTP is used.

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).

New Date (DD-MM-YYYY)

New Time (HH:MM:SS)

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

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**.

3.3.7 ISDN PRI settings

Record Outgoing Calls

Outgoing calls are normally recorded, but that 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 sides of all calls. 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 become 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 the inbound or outbound status is 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 archiving 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 recorded.
- +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

This setting is also 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).

3.3.8 Black/White-list Numbers

Black/White-list Numbers

The V-Tap ISDN can record the calls depending on the telephone number. Default, all telephone numbers from the ISDN line are checked against the list; Local, Remote and Connected numbers. Remote and Connected can be disabled with “.IM” and “.IN” in the Special Settings and Commands field.

This field must start with the letter **B** to define a Blacklist, followed by numbers that must NOT be recorded.

This field must start with the letter **W** to define a Whitelist, followed by numbers that MUST be recorded.

Numbers are without leading zeros and must be separated by the plus or semicolon sign.

It is possible to enter the last (right-most) digits only of each number, but then all entries must have the same length. This is handy when recording a lot of local extensions only.

The star sign can be used as a wildcard to define a range of numbers.

Examples:

B793471038+793471056 : Do not record these 2 numbers.

W1094+1077+1023+1010 : Record all extensions that end on one these 4 numbers.

W316*+491* : Define 2 ranges to record.

When this field is left empty, all numbers are recorded.

Maximal 15 numbers can be entered in this field. When there are more (up to 100), it is also possible to make a list of numbers on the PC and put them in a text file, called BLACK.TXT or WHITE.TXT.

See further the chapter [Number-list](#).

3.3.9 Special Settings & Commands

Special Settings & Commands

In this field extra settings can be entered, used to alter functionality or to setup alternative modes of operation.

All special settings start with a dot in front, followed by two letters.

Some of them also require a numeric value behind.

There are a few special commands, without the dot.

Special Commands

- "SD" = Show free space on the card after each reboot; [more info](#).
- "FORMAT CARD" = Format the SD card. All data on the card will be deleted!
- "FACTORY" = Back to factory settings, except all licenses. IP is default!
- "FACTORY WIFI" = Factory settings AND enable Wi-Fi module & settings.
- "FACTORY NOWIFI" = Factory settings AND disable Wi-Fi module & settings.

Special SD card Settings (see also [Special SD card settings](#))

- ".SR" = Remove files from the card after sending.
- ".SA" = Disable Auto Delete when the card is (almost) full.
- ".SP" = Enable SD Power Save Mode (slow clock during idle).
- ".FF<max>" = Maximum number of Files on the card (default 10000).
- ".FS<size>" = Maximum File Size in MB (default 230).
- ".SI<mhz>" = SD card Interface Speed in MHz (default 50).
- ".CS" = Show all current SD file-counters; [more info](#).
- ".CR<cou>" = Set Read file-counter.
- ".CW<cou>" = Set Write file-counter.
- ".CD<cou>" = Set Delete file-counter.

Special Recording Settings

- ".II" = Disable recording of Incoming calls.
- ".IO" = Disable recording of Outgoing calls.
- ".IL" = Record audio of the Local side only.
- ".IR" = Record audio of the Remote side only.
- ".IE" = Record Early; start recording when ringing.
- ".IN" = Disable connected number for the number-list.
- ".IM" = Disable remote number for the number-list.
- ".IB<sec>" = Notification Beep interval in seconds, using "NBEEP.WAV".

Special ISDN Settings

- ".IV" = Reversed line IN<>OUT operation (local & remote switched).
- ".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.

Special Tunnel & Network Settings (see also [Special Tunnel & Network](#))

- ".TS<port>" = Tunnel Source Port 0-32767 (default 0 = random).
- ".TC<secs>" = Tunnel Connect Timeout (default 22 seconds).
- ".TI<secs>" = Tunnel Idle Timeout (default 0 = stay always connected).
- ".TK<secs>" = Tunnel connection Keep-alive Timer value (default 60).
- ".TV<secs>" = Tunnel Encrypt Vector renewal Timer value (default 15).
- ".NP<port>" = NTP Port number 0-32767 (default 123, 0=NTP disabled).
- ".FP<port>" = FTP Port number 0-32767 (default 21, 0=FTP disabled).
- ".FT<secs>" = FTP Failure Timeout (default 30 seconds).
- ".LX<size>" = Maximum Data Size in network packets (default 1024).
- ".LS<byte>" = Internal network service timer (default 18).
- ".DT" = Disable Telnet connections.
- ".TF" = Disable EtherType Filter (default IP & ARP packets only)!
- ".LI" = Disable initializing the IP-stack after closing the tunnel.
- ".LH" = Force Half Duplex on all LAN ports.
- ".LU" = The time is always Summer Time in the NTP function (DST).
- ".LN" = Disable Summer Time correction in the NTP function.
- ".LN" = Disable Summertime Correction in NTP function.
- ".LR" = When DHCP is enabled, a daily reset is done at 03:00.

Special Wi-Fi settings

- ".LAN" = Start with the LAN cable and fallback to Wi-Fi connection.
- ".WF" = Disable Fallback from Wi-Fi to LAN cable.
- ".WW" = Disable WPA2_PSK encryption (= Open Wi-Fi no password).
- ".WC<chan>" = Set Wi-Fi Channel ID; 1 till 13.
- ".WR<pow>" = Set Wi-Fi RF TX Power; 0 till 82 per 0.25 dBm (default 58).
- ".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
- ".WL" = Disable the web login page after Wi-Fi connection.
- ".WT<secs>" = Set Timeout for the TCP web server (default 90).
- ".WK<secs>" = Keep-alive timer for the Wi-Fi Tunnel connection (def 60).
- ".WUP" = Try to update the Wi-Fi module.
- ".WZ1/0" = Disable(WZ1)/Enable(WZ0) Wi-Fi module during recording.

Other Special Settings (debug/test purposes)

- ".UD" = Disable USB function, so no HID recognition (saves power).
- ".UP" = Disable USB Pausing (no interrupts 10 minutes after power on).
- ".UF" = Flash Wait States on 4 (else default on 5).
- ".UC" = Disable CPU Cash Controller (much slower).
- ".UM" = Disable Memory Protect Unit (slower).
- ".LB" = Initialize the IP-stack twice during boot-init.

- ".MAC<hhhh>" = MAC Configuration bits (4 hex digits, default C250).

- ".I2C<num>" = Set I2C interface speed 0-255 (default 98 = 400 KHz).

- ".XO" = Debug mode enabled. Output to the serial port (57600,n81).

- ".XF" = Open Debug Trace file. The file TRACE.TXT is closed again after web login. Then ".DT" must be removed again and the settings saved. TRACE.TXT can be read from the SD card or downloaded with ftp.

- ".XD" = Open D-channel Trace file. The file DTEST.TXT is closed again after web login. Then ".DT" must be removed again and the settings saved. DTEST.TXT can be read from the SD card or downloaded with ftp.
Note: During the time tracing is active, recording is NOT possible!

A step-by-step description of how to make a trace is described in the chapter [D-channel trace for debug](#).

3.3.10 Licenses & Versions

Licenses: Apresa / PC / S&U

New License Key

The Channel Licenses for Apresa and PC and the Support & Update end-date are shown here. A Channel License (also called Recorder License) is the right to upload a recorded call via the Tunnel to the Tunnel server.

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

NOTE:

At least 1 Channel/Recorder License is needed before the system starts recording any calls. Adding new licenses is further described in a separate quick guide about [V-Taps and Licenses](#).

V-Tap ISDN PRI OS Version

V-Tap ISDN PRI App Version

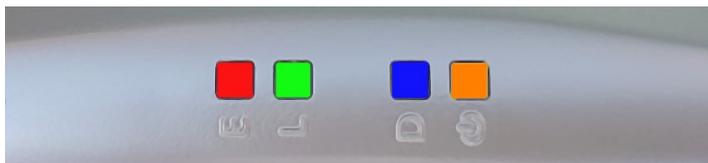
Firmware versions are shown here for information purposes only and cannot be changed.

Serial Number / MAC Address

The Media Access Control (MAC) address of each device operating on an Ethernet network is a unique identifier that is needed to route the packets over the LAN.

The serial number and MAC address are both shown for information purposes 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 steady ON and all other LED's OFF.*
This situation can happen in two cases:
Or the USB power supply does not generate enough current; try using a stronger USB port or power supply.
Or the software in the system does not run at all, due to a hardware failure; contact your dealer.
- *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 and power.

- *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 Disable DHCP temporary

When running with default settings, there is a way to disable DHCP temporary. Then the settings can be reached through the web interface with the fixed IP address 192.168.55.66. If no settings are done, then DHCP is enabled 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
- The web page is now reachable on IP address 192.168.55.66

NOTE: The IP address of your PC must lie in the range 192.168.55.0 till 192.168.55.255 and the IP mask should be 255.255.255.0.

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 and the name protocol does not work (MDNS). In other words, the user cannot reach the web interface anymore. There is a way to reset all settings to factory values (see next chapter), after which DHCP is enabled again.

If that is not desirable, then there is a way to show the IP address with the LED's (this does **not** work when the Button Mode is set):

- 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 Red or Blue is not 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 Copy Settings from SD card

The V-Tap automatically copies the settings files to the root of the SD card, directly after insertion (only if they do not exist already).

The file CFG.VTP from the SD card can be edited with a text editor on the PC and then be copied back to internal memory. To do so, the SD card must be inserted while holding the button pressed on the V-Tap.

5.5 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 more times; 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](#)).

5.6 Format SD card

To format an SD card, insert the card somewhere during the factory settings procedure above, after the first release of the button.

A second method is to enter "FORMAT CARD" in [Special Settings](#).

5.7 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.
- The IP address is now on the default value 192.168.55.66
- Only access with FTP is now possible (no web interface).

5.8 Temporary access with Wi-Fi

The V-Tap may have a built-in Wi-Fi module that is not enabled by default. To enable Wi-Fi temporary do the following:

- Power off and remove the SD card.
- Hold the button pressed during power on and keep pressed for about 12 seconds until only the BLUE LED is ON.
- Release the button; the BLUE LED goes off.
- Wi-Fi AP is now temporary active, until the next reboot.
- Connect with Wi-Fi your phone or laptop to "V-Tap.....".
- Enter the MAC address of the V-Tap as the Wi-Fi password.
- The MAC can be found on the bottom of the box.
- Disable mobile data on your phone, else the IP is not found!
- Open a browser and enter the IP address 192.168.55.66
- In the login page, enter "admin" and "admin".
- The settings page now appears.
- After Save & Logout, Wi-Fi is disabled again.
- To enable access permanently, enable [Wi-Fi Access Point](#).

5.9 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 present on the card. The files SAVECONF, DELCONF and CLEARROM perform an action during update and 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 , PTAP.ROM and PTAP.CPY must be on the card. The files SAVECONF, DELCONF and CLEARROM are optional.

6 SD card usage

The SD card is used to store the recorded calls. 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 can be seen 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 number is enclosed inside the WAV header of each file and can be extracted by the Apresa or V-Archive 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 server, 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 V-Archive 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.

Formatting an SD card is possible in two ways; see [Format SD card](#).



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).



6.1 Special SD card settings

Next follows a description of some settings for the SD card, which must be entered in [Special Settings & Commands](#).

.SD = Show free space on the card after each reboot

Enter “SD” as the first command in “Special Settings & Commands”. After each reboot and login, free space on the card is shown then. (A reboot is also done after pressing the ‘Save & Logout’ button.)

.SR = Remove files from the card 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 the files after the content was sent to a Tunnel server. A certain risk is taken then, because data cannot be recovered anymore after deletion.

.SA = Disable Auto Delete when the card is almost full

When the card is almost full, the oldest files are deleted automatically by the system to create space. This process can be disabled, but new recordings will get lost in that case. When disabled, the user must replace the card on time.

.FY = Enable encryption of WAV files on the card

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.

 **.FS<max> = Maximum Files on the card (default 10000)**

The maximum number of files on the card has two purposes. First of all, it makes the directory on the card more manageable by the system and any PC. Too many files in one directory makes 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, the maximum file size (see below), the auto close function (see above) and the amount of recorded data (number of connected phones). 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 the card must be formatted with the FAT32 file system.

 **.FS<max> = Maximum File Size in MB (default 230)**

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. 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 about 8 hours of recording. A call that takes longer will continue in the next file, without loss of data.

 **.SI<mh> = Card Interface Speed in MHz (default 50)**

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 12, 15, 17, 20, 24, 25, 30, 40, 50 and 60.

- 🔗 **.CS = Show the card file counters after next login**
- 🔗 **.CR<cou> = Set new Read file counter**
- 🔗 **.CW<cou> = Set new Write file counter**
- 🔗 **.CD<cou> = Set new Delete file counter**

Enter “.CS” in “Special Settings & Commands” (place at the end, if there are other settings). The next web login will then show the current file counters, used by the card filing system.

For example: **W=500 R=501 D=1**

This shows that the write-counter is on 500, the read-counter on 501 and the delete-counter on 1.

Meaning, that there are 500 files on the card (next file to open is 501), that file 500 was sent successfully to the Tunnel server (next file to send is 501), and that no file was automatically deleted yet.

When the connection to the Tunnel server is right, then the read-counter is always one above the write-counter.

The delete-counter only moves, when the SD card is full and old files are being deleted by the system.

The counters can have a maximum value, the same as the maximum number of files on the card, and can be changed by the “.FF” setting.

The read-counter can be set back to resend files. For example, “.CRO” will resend all recorder files from the card to the Tunnel server.

7 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 [Special Settings & Commands](#). 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).

8 Number-list (Black- or White-list)

The V-Tap ISDN can record the calls depending on the telephone number. Besides the web setting [Black/White-list Numbers](#), also a text file containing a list of numbers may exist inside 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. Numbers from the web setting are added to this list (for both in total maximal 100 numbers).

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*).

9 Telnet connection

The V-Tap can be accessed with the Telnet (Teletype 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 V-Tap Name is shown, and some debug information is constantly sent; Opening and closing of the Tunnel connection and, when an SD card is used, the opening and closing of files on the card.

Further there are two commands that can be entered with Telnet:

The command **ATMENU** will first ask you to enter the Login Password, which is the same as the one used for web access (default "admin"), 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 file counters on the SD card, reset to factory settings and change the clock. Normally, there is no need to use 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 still possible in sniff mode. In pass-through mode recording is stopped, and only a trace is made.

A better way to get a D-channel trace is described further on in the manual in the chapter [D-channel trace for debug](#).

Telnet is disabled by entering ".DT" in [Special Settings & Commands](#).

10 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, A reboot is needed after upload.

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 ISDN PRI

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 Monitoring 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 V-Archive 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 ISDN PRI

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:

Command	Description	Reply
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.

11 D-channel trace for debug

In case there are no recordings made by the V-Tap PRI, or recordings are wrongly made, it is possible to make a trace of the ISDN D-channel. The trace text is then written to the file DTEST.TXT.

To make the D-channel trace:

- Go to the Web Settings page of the V-Tap PRI.
- In **Special Settings & Commands** fill in **.XD** (with dot).
- Press **Save & Logout**.
- Leave the trace running for some period. This can be even days when needed.
Recording is still possible when the system is in sniff mode. In pass-through mode, only a trace is made.
- The trace is stopped when you login again on the Web Settings page.
- Then **.XD** must be removed from **Special Settings & Commands** and the settings saved again, if this was not done by the system already.
- The trace file **DTEST.TXT** is written to the SD card or can be download with FTP.
For analysis, it can be sent to support@vidicode.com

12 ISDN PRI ports & wiring

The ports 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.

Standard, the V-Tap PRI is in sniff mode, meaning that all pins on both RJ45 ports are inputs, and the V-Tap can only listen to the line. It does not matter then how the PRI line is connected ([parallel](#) or [in-line](#)), as long as the Rx/Tx signals are available on the wiring pairs 1&2 and 4&5.

When pass-through mode is selected with the jumpers, the wiring becomes different, because the V-Tap PRI also must transmit on the line. All that is received on the Rx pairs on one site, is transmitted on the Tx pairs on the other site. The pins in pass-through mode:

Label on PRI → Connect to →	"ISDN IN"		"ISDN OUT"	
	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 RJ45 port (both), pin 1 is on the *right-hand* side.

The Rx and Tx twisted pairs have approximately 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.

13 Revision History

v1.25 February 2024

- Text for D-channel trace changed.

V1.24 Februari-April 2022

- Connection schemes and wiring explained better in chapters 2 and 12.

V1.23 November 2021

- New procedure to enable Wi-Fi from default.

V1.22 April till November 2021

- VLAN usage removed (is not available in a V-Tap PRI).
- V-Archive installation does not need the V-Tap to be connected.

V1.21 December 2020

- New web setting 'Black/White-list Numbers'.

V1.20 November 2020

- Settings page is much smaller! Removed settings are now in 'Special Settings'.

V1.13 May/Juli/August 2020

- Introduction changed some.
- Added "Format SD card" and improved some text.

V1.12 February 2020

- Changed scheme in 2.1 and added text about USB for V-Archive installation.

V1.11 February 2020

- New chapter added: "D-channel trace for debug".

V1.10 December 2019

- New chapter in Button function: "Copy Settings from SD card".

V1.9 October 2019

- Improved some text in General network settings.

V1.8 October 2019

- Access description has changed because DHCP is default enabled now.

V1.7 September 2019

- Help function in web settings added and text improvements.

V1.6 August 2019

- USB information added and text improvements.

V1.5 April 2019

- Changes in text of FTP, Telnet and MAC Address and "Device Name/IP".
- Replaced software name "Call Recorder VoIP" by "V-Archive".

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 & Recording Licenses removed.

14 Acknowledgements

14.1 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.

14.2 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.