V-Tap VoIP

Manual

V1.0

Contents

1 Introduction

The V-Tap VoIP is a hardware and software solution for the recording of telephone calls that are transported over an IP network. The supplied hardware unit sniffs the digital data coming from external IP telephones and can copy the data back to the network or stores the data directly onto an SD card. In both cases 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 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 build-in switch function allows 4 Ethernet connections (100 Mbps). This makes it possible to connect 3 external IP phones and one connection to the network. For a desktop solution, it is also possible to connect a PC or other network peripherals.
An IP phone can also be a Softphone running on a PC. This is achieved by simply wiring the PC's network through the V-Tap VoIP switch.

In the case that no SD card is inserted, the sniffed data is sent life over the network to the Apresa recorder or CR-VoIP software.
With an SD card inserted, the sniffed data is stored as files on the card. 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.
By using the SD card, the V-Tap VoIP can operate completely stand alone and can store data for months or even years, depending on the capacity of the card.

The internal settings of the V-Tap VoIP can be accessed through a web interface by any browser.

The V-Tap VoIP 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 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.

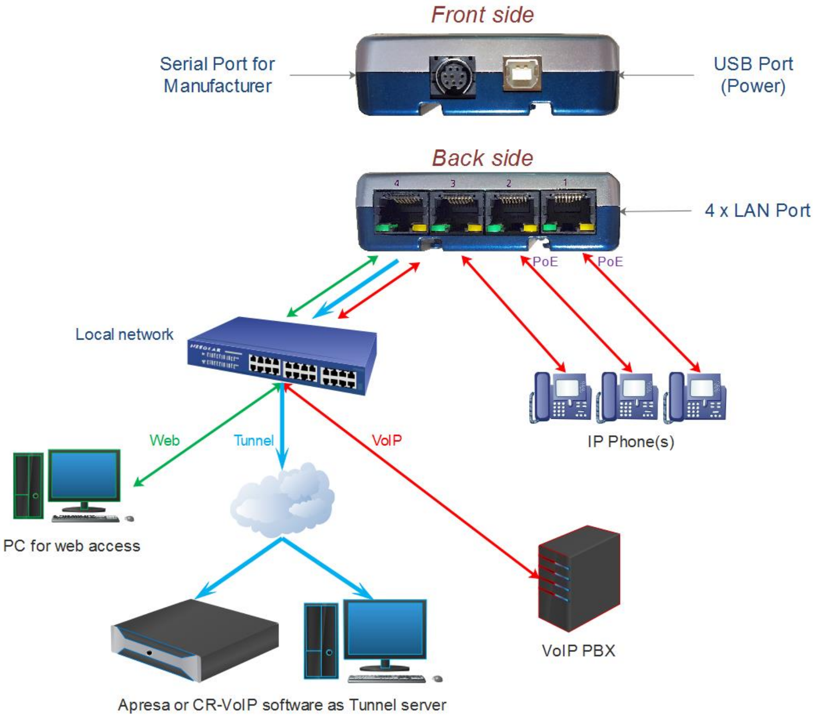
NOTE: The V-Tap VoIP needs to be powered through USB, otherwise the device cannot record from external IP phones.

2 Getting started

2.1 Hardware installation

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

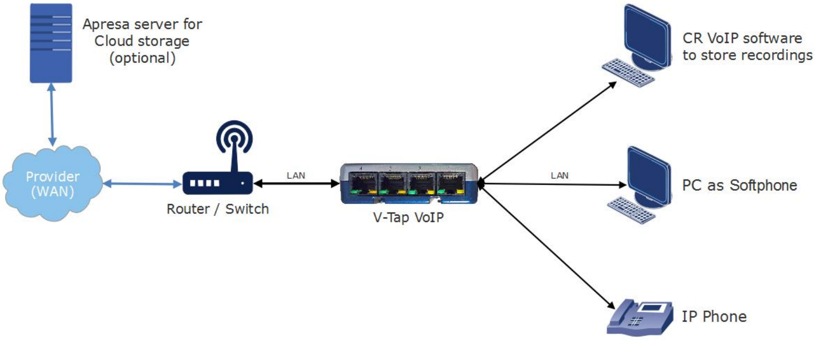
- Connect the local network to the V-Tap VoIP.
- Connect the IP phones or PC's to the V-Tap VoIP.
- Connect the USB to the V-Tap VoIP for power.
- Access the settings of the V-Tap VoIP through the web interface.
- Optionally insert an SD card.



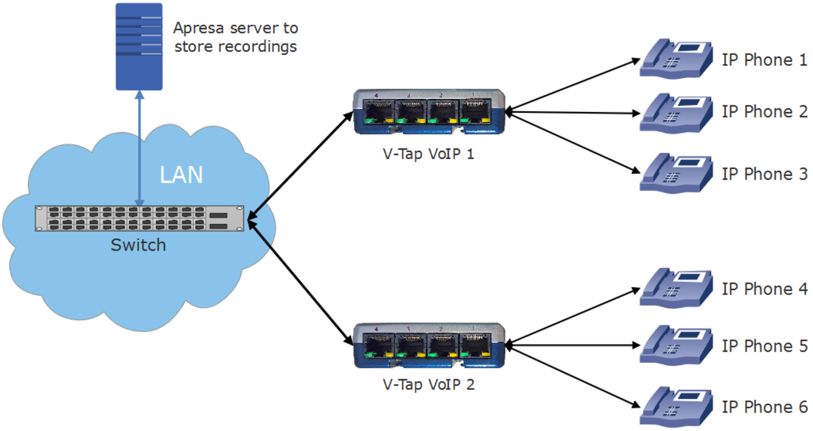
Any LAN port can be used to connect the external network and the IP phones. Different configurations are also possible, see Port settings.
For more schemes see the next page and chapter Connection schemes.

NOTE: Ports 1 and 2 only are suitable to connect Power over Ethernet.

2.1.1 Connection at Home



2.1.2 Connection at the Office



2.2 Software installation

External software is needed to extract the recorded calls from the Tunnel data that is produced by the V-Tap VoIP. Also, when the data is stored on an SD card, then external software is needed to interpret this data later on.
The Tunnel data stream, coming directly from the V-Tap, can be send to the Call Recorder Apresa or the Call Recorder VoIP software.

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 the files 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.
The Apresa software has lots of different other recorder possibilities and is not further described in this manual.

The Call Recorder VoIP software for the PC can also receive Tunnel data from the V-Tap VoIP, convert this data into audio files and store the files into its own database. The VoIP software can also receive multiple data streams from different V-Tap units simultaneously.
The Call Recorder VoIP software for the PC has its own manual and is therefore not described in this manual.

NOTE:
You need to enter at least one recorder-channel license key before the Apresa or CR-VoIP software can record your calls. Recording multiple calls simultaneously need more license keys to be added.

3 Web interface and Settings

The first step to access the web interface of the V-Tap VoIP, is to connect a network cable to any of the 4 ports 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.
Then any web browser can be used to access the web interface of the V-Tap VoIP.

3.1 IP address

By default, the V-Tap unit has DHCP enabled AND listens to the IP address 192.168.55.66.

This IP address can be entered directly in the address bar of your browser, only when the local network does not have a DHCP server and when your PC has an IP address that lies in the same IP range as the IP address of the V-Tap VoIP. The IP address of your PC must therefore lie in the range 192.168.55.0 till 192.168.55.255.
The IP mask should be 255.255.255.0.

Default IP address:	**192.168.55.66** (or from DHCP server)
Default User name:	**admin**
Default Password:	**admin**

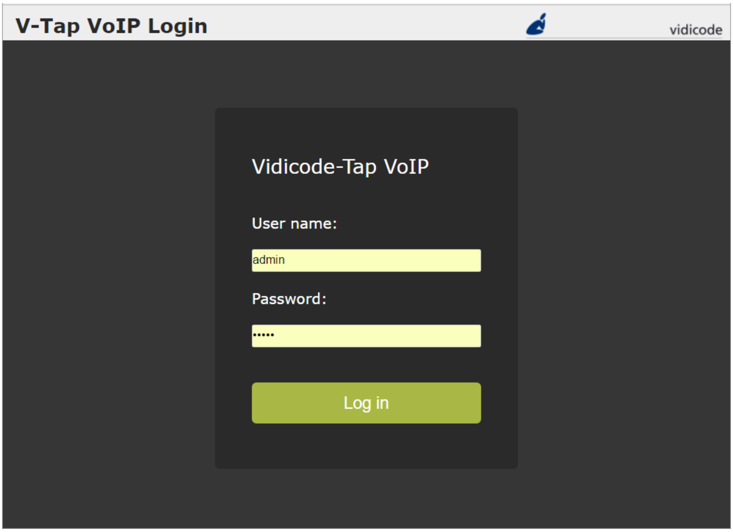
In case the IP address cannot be reached by an external PC, it is also possible to define a fixed IP address with an SD card.

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 system.

3.2 Web interface

Entering the IP address in your browser is showing the following screen:

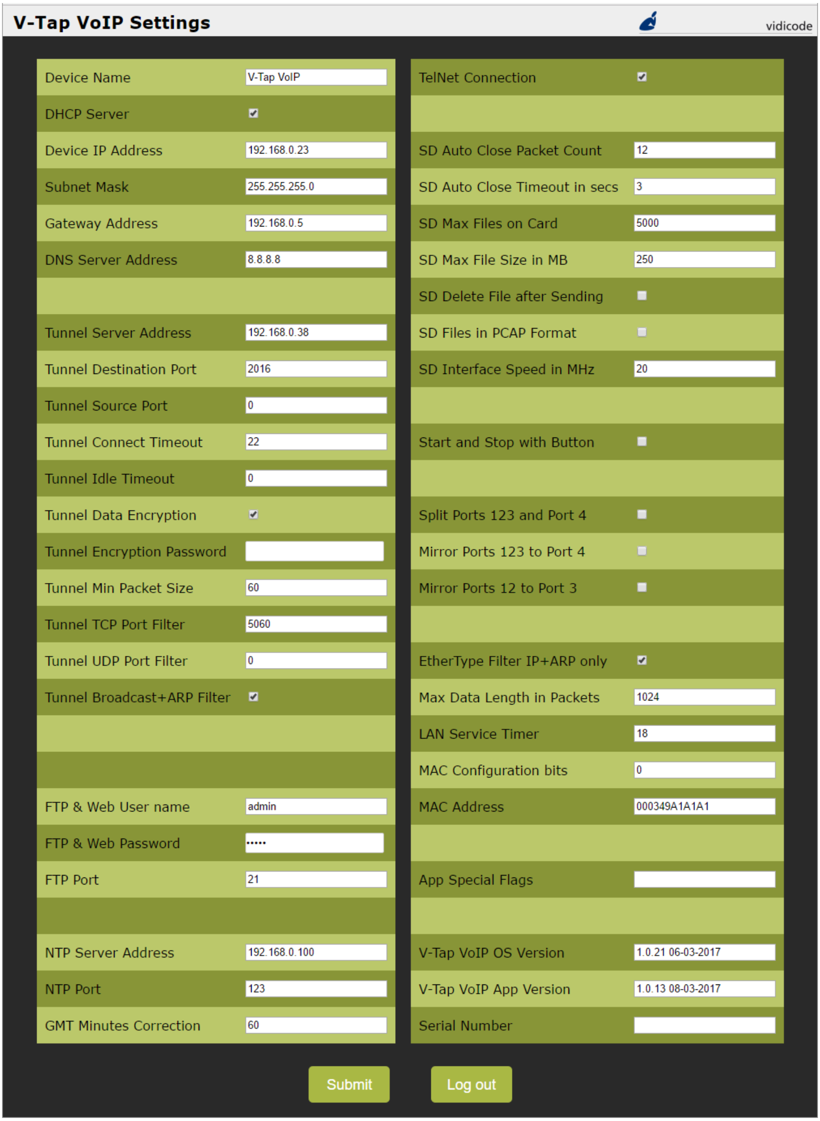


User name: admin

Password: •••••

Now enter “admin” for the User name and “admin” for the Password, then press the **Log in** button and the Settings menu appears:

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



V-Tap VoIP Settings

vidicode

Device Name	V-Tap VoIP	TelNet Connection	☑
DHCP Server	☑		
Device IP Address	192.168.0.23	SD Auto Close Packet Count	12
Subnet Mask	255.255.255.0	SD Auto Close Timeout in secs	3
Gateway Address	192.168.0.5	SD Max Files on Card	5000
DNS Server Address	8.8.8.8	SD Max File Size in MB	250
		SD Delete File after Sending	□
Tunnel Server Address	192.168.0.38	SD Files in PCAP Format	□
Tunnel Destination Port	2016	SD Interface Speed in MHz	20
Tunnel Source Port	0		
Tunnel Connect Timeout	22	Start and Stop with Button	□
Tunnel Idle Timeout	0		
Tunnel Data Encryption	☑	Split Ports 123 and Port 4	□
Tunnel Encryption Password		Mirror Ports 123 to Port 4	□
Tunnel Min Packet Size	60	Mirror Ports 12 to Port 3	□
Tunnel TCP Port Filter	5060		
Tunnel UDP Port Filter	0	EtherType Filter IP+ARP only	☑
Tunnel Broadcast+ARP Filter	☑	Max Data Length in Packets	1024
		LAN Service Timer	18
		MAC Configuration bits	0
FTP & Web User name	admin	MAC Address	000349A1A1A1
FTP & Web Password	•••••		
FTP Port	21	App Special Flags	
NTP Server Address	192.168.0.100	V-Tap VoIP OS Version	1.0.21 06-03-2017
NTP Port	123	V-Tap VoIP App Version	1.0.13 08-03-2017
GMT Minutes Correction	60	Serial Number	

By pressing the **Submit** 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 settings web interface and after connecting with ftp or telnet. The name is not used in the Tunnel protocol. The maximum length is 30 characters. Example are "Richard Phone" or "SalesTrunk".

- DHCP Server

Default, the DHCP feature is not enabled and the V-Tap unit has a fixed IP address. When a DHCP server is available on the network and is used, the IP and Gateway addresses are automatically assigned. Without DHCP you must manually enter an IP address.

- Device IP Address

As part of the network, the V-Tap VoIP needs an IP address. In case a DHCP server is used, the DHCP server will assign the V-Tap VoIP 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 IP 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 IP mask must be the same for the device and the computer connecting to it.
More explanation can be found on the internet and is out of the scope of this manual.

- Gateway Address

The Gateway address is used by the V-Tap VoIP 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 active, 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.

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 VoIP. The receiving server can be an Apresa recorder or a PC running the Call Recorder VoIP software.
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.

- 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 VoIP 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.

Tunnel Connect Timeout

This timeout is used when the V-Tap VoIP 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 VoIP 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.

Tunnel Idle Timeout

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.
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.

Tunnel Encryption Password

This parameter is also used for the encryption of the Tunnel data. The receiving side of the Tunnel data, the Apresa or CR VoIP software, must use the same password.
An empty password still does the encryption, but is less secure.

Tunnel Min Packet Size

Tunnel Packets are network packets sniffed by the V-Tap VoIP. These are the wanted VoIP packets coming from your phone and local network. After they passed the internal filters and match the minimum size, they are sent with the Tunnel protocol to the server or stored onto SD card.
The default minimum size of 60 bytes is also the minimum standard Ethernet packet size. This means that packets of all sizes are taken by default. There may be situations where it is handy to increase the size, to minimize the overhead of stored packets. For example, when the size is set to 61 all ACK-packets from the TCP protocol are discarded.

Tunnel TCP Port Filter

The TCP packets that are recorded (sniffed) from the local network must pass this filter, else they are discarded. The default port 5060 allows only SIP packets to be taken as Tunnel data.
Setting the TCP Port Filter to 0 (zero) allows all TCP packets. In that case, all internet traffic is also stored, including downloads and streaming media. The receiving Tunnel server can still pick out the VoIP calls then. However, on busy local networks this is not advised to do, because the V-Tap VoIP cannot handle very big data streams. When using an SD card, the V-Tap VoIP can store at least 1 Mbytes of data per second. That is enough for 25 uncompressed VoIP calls.

Tunnel UDP Port Filter

UDP packets, coming from the local network, can be filtered in the same way as TCP packets. The SIP protocol uses most of the time UDP with a random port number to transport the voice data, the so called RTP stream.
Because the SIP protocol is not interpreted by the V-Tap unit and therefor the UDP port number is unknown in most cases, all UDP packets must be taken and stored.

With standard SIP on the local network, this filter must be set to 0 (zero) to allow the V-Tap unit to take all UDP packets.

- Tunnel Broadcast + ARP Filter

This filter sees that not too much packets are taken from the local connected network. Many LAN's at the office have a lot of overhead with packets that are not relevant for recording VoIP calls. Therefore, all Broadcast and ARP packets are standard discarded, reducing the Tunnel data.

3.3.3 FTP & Web settings

The V-Tap VoIP has a build 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.

- FTP & Web Password

Password to log in with FTP and the Web service.

- FTP Port

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 unit. 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.

3.3.4 NTP settings

NTP (Network Time Protocol) can be used to synchronize the internal clock. The V-Tap VoIP 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 then sets the internal clock.
The clock is added to each packet in the Tunnel protocol and is 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 (maybe weeks or moths) interpreted by the Call Recorder VoIP software on the PC.
The V-Tap VoIP synchronizes the clock 6 times per day (each 4 hours).

- <u>NTP Server Address</u>

  The IP address or the host name of the NTP server. Leave this field empty when no NTP is used.

- <u>NTP Port</u>

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

- <u>GMT Minutes Correction</u>

  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).

3.3.5 Telnet setting

TelNet Connection

The V-Tap VoIP 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 VoIP. 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 only two commands that can be entered with Telnet:

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.

3.3.6 SD Card settings

The SD card is used to store the recorded VoIP data from the local network. The system writes the data to files in the Tunnel format. This format is the same as sent to a Tunnel server, so default encrypted. The files on SD card are opened and closed automatically, depending on some parameters below. The SD card can be seen as a big cyclic memory buffer for the system.

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 then, but after a no-data timeout 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 Tunnel 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.

Without an SD card, the system has only little buffering capabilities. Any disturbance in the Tunnel connection would then lead to the loss of data.

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 Auto Close Packet Count
- SD Auto Close Timeout in secs

These two parameters are used by the system to close files on SD card automatically. As soon as you insert an SD card, a file is opened for writing and recorded data is put into it. Packets are counted each second again and when the installed threshold is reached, the timeout becomes active. When the Packet Count is under the threshold for time of the installed timeout, the current open file is closed. A new file is opened immediately after that.

A normal VoIP call produces about 100 packets per second for the duration of the call. When the call ends, only a few or no packets are received.
In this way, the Auto Close function can be seen as an off/on-hook detector. The files on SD card will then contain complete calls. Of course, this is only true when one VoIP phone is connected. With more phones connected and more calls active at the same time, the files can also contain multiple calls.

SD Max Files on Card

The maximum number of files on the card has 2 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 make a slow system. The default number of 5000 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.

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 uncompressed VoIP call produces roughly 24 Kbytes per second. This means a little less than 90 Mbytes per hour. The default of 250 Mbytes is therefore enough for about 3 hours of recording. A call that takes longer will continue 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 Files in PCAP Format

  Enabling this option sets the V-Tap unit in a completely different mode. The format of the stored packets in the files on the SD card changes to the PCAP format. The files on the card are given the extension .CAP and are directly readable by PC tools like Wireshark. The Tunnel function itself is disabled, but packets still must pass the Tunnel filters before they are stored.
  This mode can be used for network debugging or network tracing.

- 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 12 , 15 , 17 , 20 , 24 , 30 , 40 and 60.

3.3.7 Button setting

The button can be used to manually start and stop the recording of sniffed data.
Other special functions of the button are described in chapter Button functions .

- Start and Stop with Button

  This parameter changes the recorder function of the V-Tap VoIP. When the button is enabled, the system does not automatically store or forward the sniffed data anymore.
  Start and stop is a toggle function of the button. The LEDs will show if any data is recorded or not. The Red LED ON means “stopped” (no recording) and the Red LED OFF means “started” (active).
  The moment on which the button is pressed to start recording is very important. For VoIP calls, this cannot be in the middle of a conversation, else the recorded data misses the start of the call in the SIP protocol.
  Therefore, the start/stop function is only usable for outgoing calls that are known to be recorded in front.

⊙ The button must be pressed **before** any call becomes active! ⊙

3.3.8 Port settings

Visualization of the below settings can be seen in Connection schemes.

- Split Ports 123 and Port 4

In the case where there are two physical networks, this parameter can be set to separate ports 1,2,3 from port 4. Port 4 is then meant to be used for the Tunnel function and the web interface (the data LAN) and ports 1,2,3 are connected to the VoIP phones and VoIP LAN. Then, only two VoIP phones can be connected instead of three.
The split ports operation can also be used in combination with the mirror functions below.
For a schematic drawing of the split ports see Tunnel with Split Ports.

- Mirror Ports 123 to Port 4
- Mirror Ports 12 to Port 3

By enabling one of the two Mirror functions, the Tunnel function is lost. Data storage is not done anymore and the V-Tap unit is only used as a flow controller, where the data is sent real-time back to the network.
Port mirroring is used to send a copy of the network packets to the selected port. On the receiving side, there can be an Apresa recorder processing those packets and making calls out of them.
Mirroring to port 3 can be used when port 4 is not needed for copy. In that case the PC network can be connected to port 4 for continuous web access.
The separation of the mirrored ports and port 4 is even bigger when the split-ports operation is enabled (see above).
Both Mirror functions should not be enabled at the same time, in which case port 4 is selected. The Blue LED is steady ON with mirroring enabled.
Schemes of the mirror function: Mirror to Port 4 and Mirror to Port 3.

NOTE: The Tunnel function is disabled when using the Mirror function!

3.3.9 Special network settings

- EtherType Filter IP + ARP only

This hardware filter is very fast and looks at two bytes in all Ethernet packets, called the EtherType. When active, only two protocols are let through, namely Internet Protocol version 4 (IPv4) and the Address Resolution Protocol (ARP). Both are always needed for normal operation. All other protocols from the Internet Layer are not needed when recording VoIP calls only.
More filtering can be done with the Tunnel filters, described above.

- 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, FTP, etc.
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 (like 1024 or 512).

- Service Timer

The default value is for optimal network speed. When a lot of V-Tap units are sending to the same PC, it might be better to lower the speed to prevent an overload of streams. The values 129, 65 and 1 can be used for slow, slower and slowest sending.

- MAC Configuration bits

This parameter holds important configuration bits for the network interface and is further not explained in this manual. Do not alter any of these bits without consulting the manufacturer.
The default value 0 is the same as C354, in which case the Ethernet multicast packets are being filtered for the Tunnel function. To enable the reception of multicast packets, set the value to C344.

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.

3.3.10 Special Flags & Versions

App Special Flags

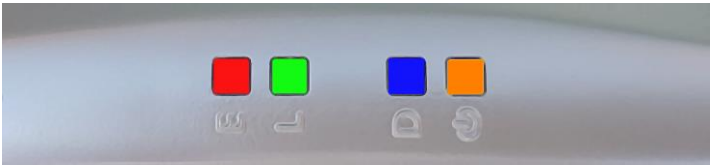
This parameter represents a mixture of internal options. The used bits are all on/off switches and shown below, but are further not explained in this manual.
The result of the sum of the used bits must be entered as a decimal number.

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)	:	Enable Button-flag in Tunnel for remote manual start/stop.
bit4	(+16)	:	Force Half Duplex on all LAN ports, except a mirror port.
bit5	(+32)	:	Force 10 Mbps on all LAN ports, except a mirror port.
bit6	(+64)	:	Set time as Daylight Saving Time for PCAP files.
bit7	(+128)	:	Disable Daylight Saving Time Correction in the NTP function.
bit8	(+256)	:	Enable CPU Overclocking (10 % faster).
bit9	(+512)	:	Disable CPU Cash Controller (20 % slower).
bit10	(+1024)	:	CPU running on overclocking (5% faster).
bit11	(+2048)	:	Disable USB function, so no HID recognition (saves power).
bit12	(+4096)	:	Disable USB sleep function 10 minutes after startup.
bit13	(+8192)	:	VLAN tags are not removed from the mirror port.

V-Tap VoIP OS Version
V-Tap VoIP App Version
Serial Number

Firmware versions and the serial number cannot be changed.

4 LED's



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

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

The Blue LED may always blink a little when a VoIP network is connected. This means that data is received by the V-Tap VoIP. The device's status must be read from the Red, Green and Yellow LED's.

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 Green LED and Amber LED blinking opposite.*
  This is the factory default and means that no Tunnel server is defined and no SD card is inserted, so no data is stored or sent. Entering an address for the Tunnel server and/or inserting an SD card solves the situation.

- *Red LED steady ON plus Green LED blinking slow.*
  The V-Tap unit tries to connect to the Tunnel server.

- *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. Then it is also recommended to check the card on an external PC.

- *Red LED steady ON with "Start and Stop with Button" function.*
  If manual recording with the button is enabled, then the Red LED ON means that recording has stopped (no data storage).

- *Red LED blinking once per second ON and OFF.*
  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 paragraph Remove SD Card safely.

- *Red LED blinking fast.*
  This indicates that data was lost. The internal buffer was overflown, because the connection to the Tunnel server was lost or writing to the SD card failed. This situation can solve itself after connection to the Tunnel server has been restored.

- *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 is used to show 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, then the Tunnel server could not be found or the network connection is bad.
  The Green LED goes to steady ON when 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 and an SD card is inserted.

4.3 Blue Data LED

- *Blue LED blinking.*
  The Blue LED blinks when data is received from the local network. Only the stored packets, that have passed the filters, will activate a blink.

- *Blue LED steady ON.*
  The Mirror function in the V-Tap VoIP is enabled. See Port settings.

4.4 Amber SD-Power LED

The Amber LED is used to show 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 writing data to a file or reading data from a file during sending with the Tunnel function.

- *Amber LED steady ON with "Start and Stop with Button" function.*
  If manual recording with the button is enabled, then the Amber and Red LED's ON mean, that recording has stopped and an SD card is inserted. No writing to the card is done and the card can be removed safely.

5 Button functions

The various button functions are described in the following paragraphs.

5.1 Start & Stop recording

When the "Start and Stop with Button" function is enabled, the Red LED indicates if recording is active or not. The Red LED ON means that recording has stopped. The Red LED OFF means that recording is busy and data is stored on SD card or sent to the Tunnel server.
Manual recording with the button is further explained in Button setting.

5.2 Remove SD Card safely

Directly after inserting an SD card, a file on the card is opened for writing. This is done to gain speed when data must be written. The file remains open for writing until it is closed automatically, after which a new file is opened immediately.
See for further explanation paragraph SD Card settings.

In the case the SD card is taken out without precaution, the current open file is not closed properly and will have a contents of zero bytes. The appearance in the directory still 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.**

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 later), 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 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.
- 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 go ON.
- Release the button within 5 seconds; all LED's go OFF.
- Now press the button 5 times on a row; all 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 below).

5.5 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 VTAP.ROM and/or VTAP.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.

5.6 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 above), there is still a way to look with FTP in the filing system remotely. The following can be done:

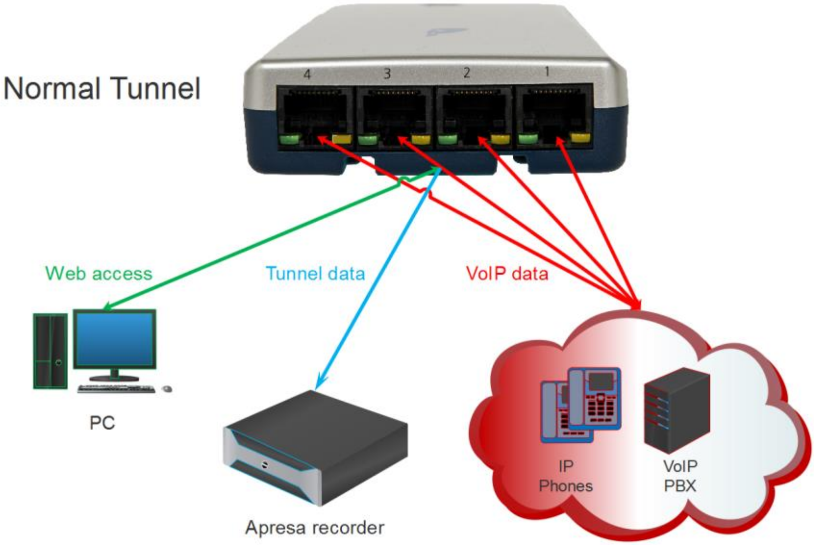
- Remove the SD card.
- Power Off the unit.
- Press the button.
- Power On and hold the button pressed for 1 second.
- Release the button.
- The IP address is now on default 192.168.55.66
- Only access with FTP is probably possible (no web interface).

6 Connection schemes

In the following paragraphs the connection schemes for some situations of connecting things are drawn. The settings to change these different ways of operating are described in Port settings.

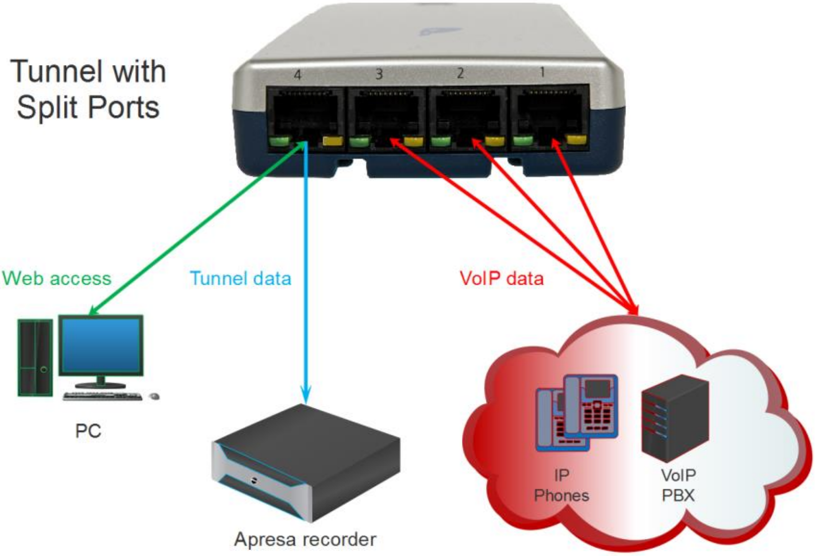
6.1 Tunnel function

This is the default startup situation of the V-Tap VoIP. All ports can be used for web access, VoIP data and Tunnel connection.



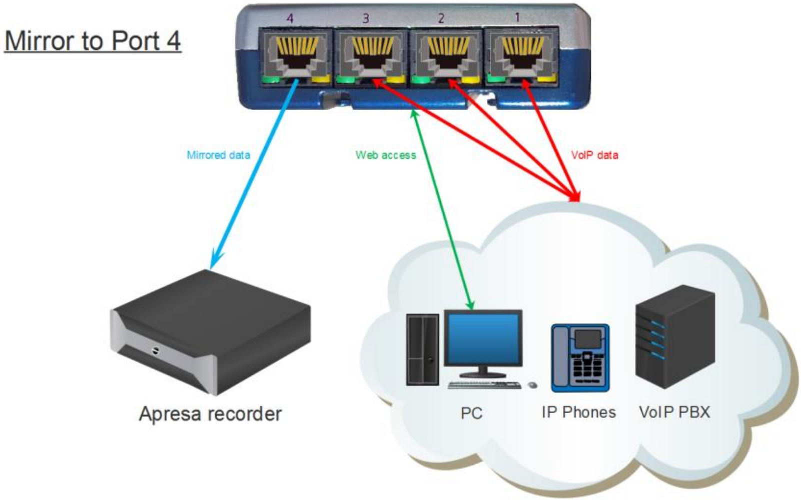
6.2 Tunnel with Split Ports

This can be set with the parameter “Split Ports 123 and Port 4“.



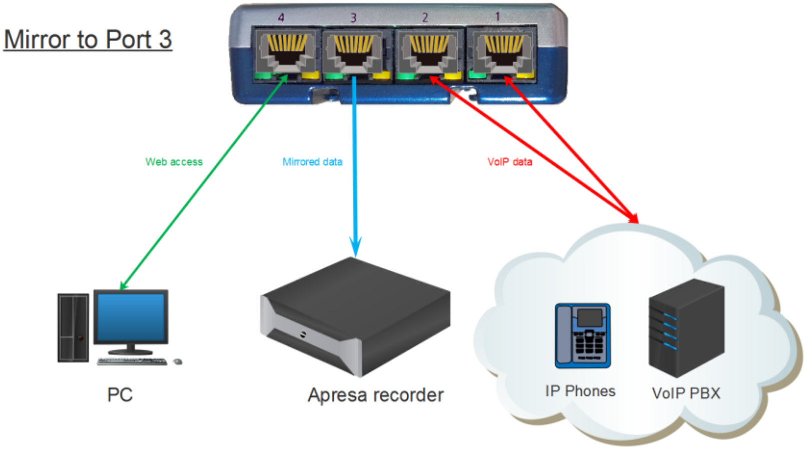
6.3 Mirror to Port 4

This can be set with the parameter “Mirror Ports 123 to Port 4“.



6.4 Mirror to Port 3

This can be set with the parameter “Mirror Ports 12 to Port 3“.



7 Acknowledgements

7.1 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.

7.2 Liability

Correct functioning of the V-Tap VoIP 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 VoIP.