Cynap WolfProt Developer's Guide

Version 1.9
March 2018

Covers Cynap and Cynap Core firmware 1.20h and up.

WolfVision GmbH, Oberes Ried 14, A-6833 Klaus, Austria

Foreword

Cynap and Cynap Core are two of our most innovative and outstanding systems. They offer a level and complexity of collaboration services which has never before been possible.

WolfProt, our command language for controlling Cynap and Cynap Core functions has been extended. It provides you with a sophisticated and versatile interface, enabling a broad range of options for customising your own installation.

These award-winning products are already considered to be a significant step forward in collaborative working and learning space design . With your added integration and customisation skills, i'm sure that you will create an outstanding setup!

Andreas Ganahl
Head of Innovation and Product Management

Table of Content

This document is structured into three parts.

Part 1
WolfProt basics

Part 2
Cynap and Cynap Core for developers

Part 3
Practical examples and tutorials on how to use WolfProt with Cynap and Cynap Core.

Cynap WolfProt Developer Guide

1 Introduction

WolfProt protocol: A simple and fast way to operate Cynap from your Room Management System solution or from a customised webpage using web-sockets.

Our WolfProt command language aims to offer versatility and sophisticated access when it comes to develop your next Room Management System integration.

The commands allow to use functions beyond the scope of its pre-defined user interface (e.g. setting a customised AirPlay PIN instead of having a randomised one generated on Cynap).

Our WolfProt APIs do work on all our products but this guide covers WolfProt integration on Cynap and Cynap Core.

Cynap itself supports PJLink protocol to send out commands to PJLink controllable devices (e.g. monitors, projectors, etc.). WolfProt behaves similar to WolfProt with its set and get command types. Peripheral Commands on Cynap are not part of this documentation.

1.1 Disclaimer

This manual is intended for Room Management System developers. Therefore it is assumed that you already have a good understanding of AMX/Crestron/Cue-system programming and integration (see http://www.howtoprogramcrestron.com/resources.html for Crestron integration or http://www.amx.com/products/NetLinxStudio.asp for AMX integration).

Our provided templates contain the whole range of Cynap functions, most of the time not all are needed for each implementation at your customers' site. We strongly advise to adapt our demonstration template to your customer needs before installing the provided demonstration template.

Knowledge of TCP/IP networking is beneficial. It is also assumed that your processor and touch panel/terminals are installed and do function correctly and reside on the same network (Wi-Fi or Ethernet) as Cynap.

Integration of Cynap and Cynap Core at customers site requires an in-depth knowledge of how Cynap and Cynap Cores are working.

1.2 Useful links

If you're reading this document to find the latest commands in WolfProt, then please have a look here:

Cynap	https://wolfvision.com/wolf/commands_cynap_wolfvision/protocol/commands_cynap.html
Cynap Core	https://wolfvision.com/wolf/commands_cynap_wolfvision/protocol/commands_cynap_core.html
Changes in APIs	https://wolfvision.com/wolf/commands_cynap_wolfvision/protocol/changes_cynap.htm
All Visualizer products	https://wolfvision.com/wolf/protocol_command_wolfvision/protocol_command.htm#t=general_information%2Fabout.htm

1.3 Help and Support

We do provide a number of support documents to help you integrate Cynap into your environment.

Please browse on the various download sections of our website, https://www.wolfvision.com or call us in case you need support.

Please make yourself familiar with the operations and installation procedures of Cynap by reading its *extensive HELP file* accessible through Cynap's *toolbar menu*.

We are, however, unable to support you with skills in programming languages needed to build your Room Management System solution.

WolfProt basics

Programmer, a machine that turns coffee into code.

2 General WolfProt

WolfProt is the official command protocol to control any WolfVision device. It is an easy accessible Protocol that allows you to control various functions on Cynap and Wolfvision Visualizers.

The connection between your Room Management System and Cynap/Visualizer uses TCP/IP (BSD or WebSocket) and is password protected.

At first it needs to be activated and configured (Enable and set Room Management System user).

The commands are divided into **GET** and **SET** commands.

GET commands retrieve information from the devices; SET commands change settings or initiate a direct command.

WolfProt commands are organised in request-reply pairs (SET/GET).
They start with a header, followed by the command, the length and data.

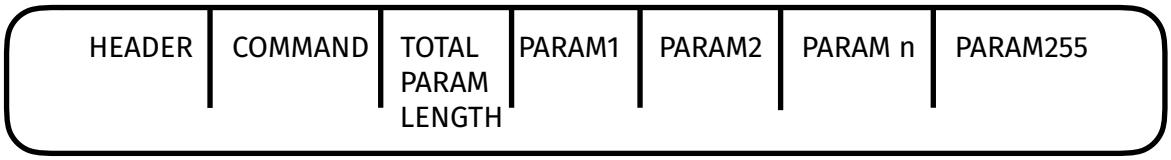
If you send a SET command you need to follow up with the appropriate GET command to check, if the SET command got executed. Return codes simply tells the agent that the command has or hasn't been received on Cynap/Visualizer.

Communication should use **either BSD or WebSockets**.
Connection: **Ethernet or Wi-Fi, Protocol is TCP/IP**.
Cynap: Port **50915 (unencrypted connection) or Port 50917 (encrypted connection)**
Visualizer connected to Cynap: **Port 50916 (unencrypted connection only)**

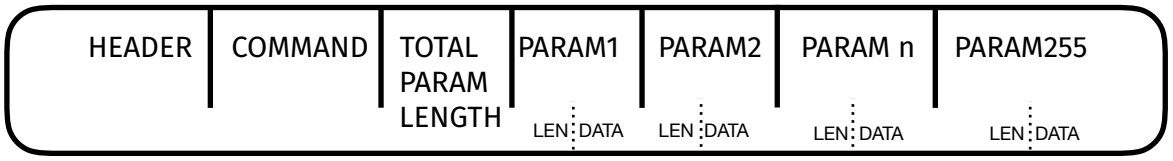
2.1 WolfProt Command Structure

There are no parameter delimiters, therefore some parameters need a prerequisite length of a parameter to function.

Command with no sizeof value in parameter
An example could be a command to mute audio



Command with custom size of parameter
Some parameters require an additional size value and it renders the parameters into required size and data value pair. (e.g. size of URL and the URL itself, etc.).
An example could be a command that opens a window with content type of browser and a URL



Please check each command, what kind of parameter and how the parameters are structured.

2.2 Header Definition

The header defines the size and the command mode. A GET commando queries values from the system and SET commands execute a defined function or change a configuration setting.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Reserved	**Reserved**	**Reserved**	**Reserved**	**0 Cmd 1 Byte**	**0 Len 1 Byte**	**0 Header 1 Byte**	**0 GET Cmd**
Reserved	**Reserved**	**Reserved**	**Reserved**	**1 Cmd 2 Byte**	**1 Len 2 Byte**	**1 Header 2 Byte**	**1 SET Cmd**

Commands requiring larger parameter sizes might need more allocated space which are being defined when using the command itself.

2.3 Return Codes

OK and ERROR reply bits that are not specified remain unchanged as in GET/SET command. The command 0xFF is reserved as an error code for an unknown command.

Return	Description	1	*Time out*
2	*Invalid command*	**3**	*Invalid parameter*
4	*Invalid length*	**5**	*Queue full (FIFO)*
6	*Firmware update error*	**7**	*Access denied*
8	*Authentication required*	**9**	*Busy*

For instance:

Start Video Recording	Command	Replies	
	09 CB 25 01 00	09 CB 25 00	*OK*
	09 CB 25 01 40	89 CB 25 03	*Invalid parameter*
	01 11 01 10	81 11 02	*Invalid command*

There are 10 return codes in total. The return codes are placed in Header Bit 7 in the return message. To know, if a command succeeded you need to send a get command to receive the status of your request.

The reply packet to each command tells you:
- on set commands: the command got executed
- on get commands: the status or parameters that have been set on Cynap

Otherwise you will receive an error code if you did violate the protocol.

Please be aware that if you don't get a reply packet after sending a set command, you're not violating the protocol but the socket is still expecting some additional values and waits forever for its completion.

Example: when sending a larger number on "parameter length" but not providing the necessary parameter (e.g. size of *cynap.net* of 9 chars as being 20 chars).

A common mistake is using the wrong AccessLevel; not being logged in at all or logged in as User when an Administrator log in is required.

Example:
Request the streaming resolution (Administrator log in required) and being connected to Cynap as User and issuing a GET command.

Request streaming resolution >> 08 CB 23 00

When logged in as Administrator you will receive one of:
- 08 CB 23 01 00 (Full HD)
- 08 CB 23 01 01 (HD)
- 08 CB 23 01 00 (qHD)
- 08 CB 23 01 00 (nHD)

When not logged in or logged in as User you will receive
- 88 CB 23 07

Same happens with a SET command when you're not logged in as Administrator

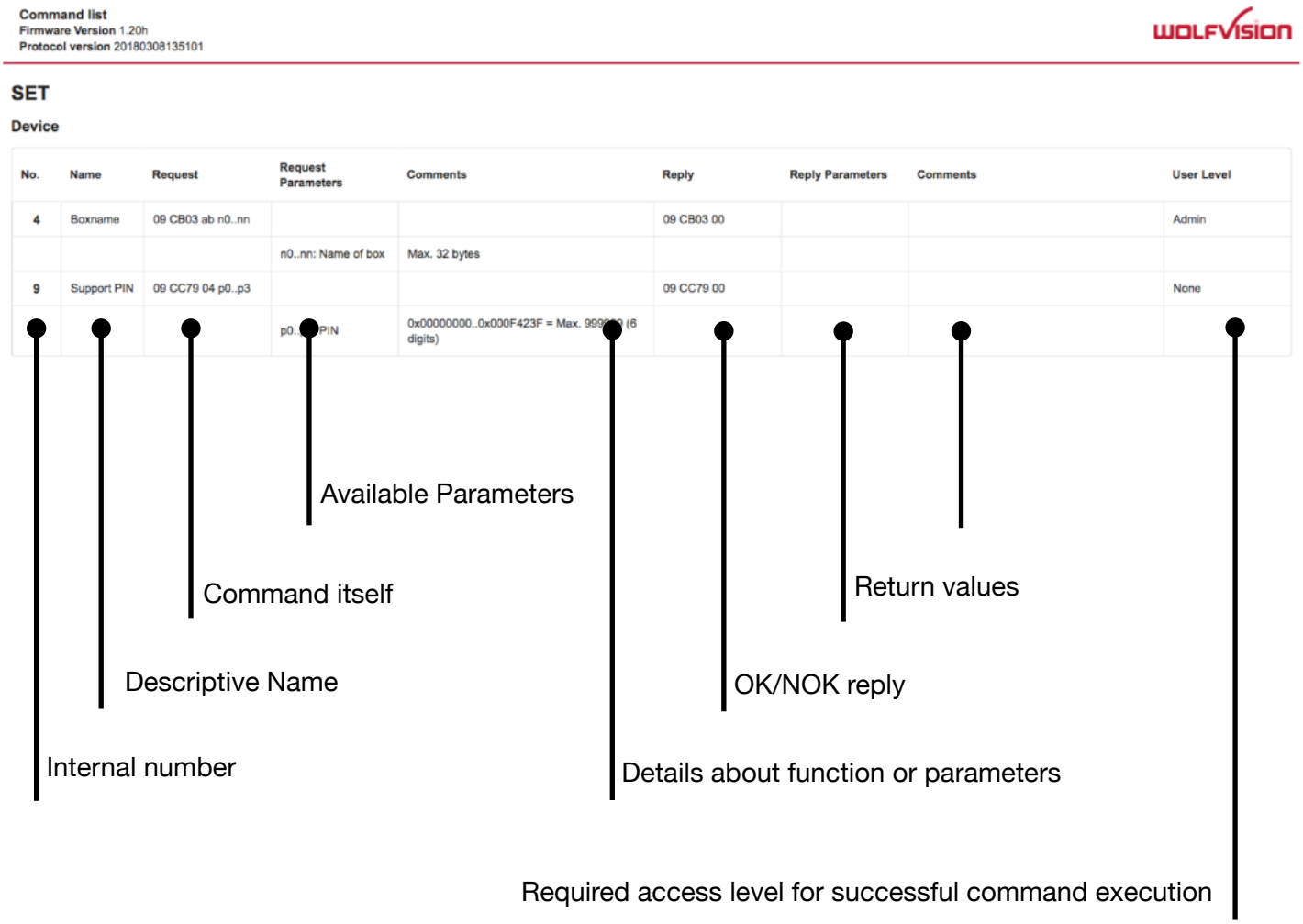
Set streaming resolution >> 09 CB 23 01 00 (for Full HD)

When not properly logged in you will receive following hex values:
- 89 CB 23 07

Pro tip:
To quickly translate ASCII into hex use one of the many online hex converters - also, your on board calculator might support a developer mode to calculate hexadecimal values.

2.4 How to read the WolfProt command list PDF

With each firmware update for Cynap and Cynap Core there will be an updated WolfProt Command List PDF available on the Web (not necessarily on the same release date).



Cynap and Cynap Core

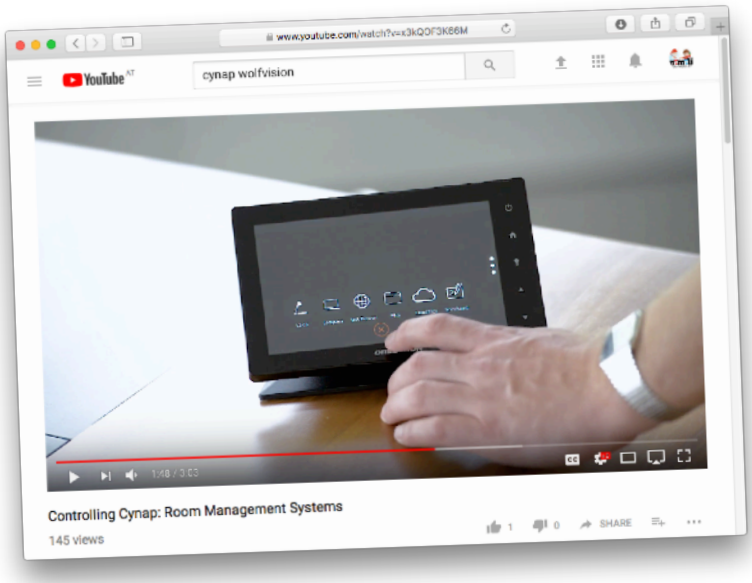
3 Cynap

Cynap is a collaboration device which supports a large number of resources (videos, office formats or images), several input sources (on 2 HDMI in) on up to 4 windows as well as internal functions such as Recording/Streaming and Annotation, Whiteboard or WebRTC.

I won't go into details of all past, present and upcoming Cynap and Cynap Core features.

Please check our YouTube channel where all functions are being explained in detail.

Cynap functions explained:
https://www.youtube.com/user/WolfVisionVisualizer



3.1 Cynap specifications

System

Operating System	Linux
Memory	8GB
Internal storage	64GB
Output resolutions	Up to 4K UHD: 2160p60 (4.2.0), 2160p30 (4.4.4), 1080p60 (4.4.4), 1080p30 (4.4.4)
Compatible mobile device operating systems	iOS, Android, Mac OS, Windows, Windows Mobile, current HTML5 browser
Supported image file formats	GIF, JPEG, BMP, PNG
Supported document file formats	PDF, Word, PowerPoint, Excel, Text, HTML
Supported video file formats	AVI, WMV, MOV, MP4, DivX, MKV, M4V, OGV
Supported audio file formats	MP3, WMA, MKA, OGA, OGG
Supported mirroring protocols	AirPlay, Google Cast, Miracast (no HDCP support), vSolution Cast (up to 30 fps)
HDCP support	Yes, (HDCP 1.4)

Table 1: System specifications

Inputs and Outputs

Video input	HDMI x2 (HDMI 2.0)
HDBaseT 1.0 Input	x 1
Video output	HDMI x2 (HDMI 2.0)
HDBaseT 1.0 Output	x 1
Audio	Line in / Line out (3.5mm mini jacks)
USB ports	Rear USB 3.0 ports x4, front USB 2 port x1, FAT32 limited to 4 GB files

Table 2:Input/Outputs

3.2 Cynap functions

Features

Max. no. of devices simultaneously displaying content on screen	4
Max. simultaneous receiver connections via Capture app	Virtually unlimited (dependent on network infrastructure)
Wireless device mirroring	Yes
Streaming protocols	RTSP, RTP (Unicast/Multicast), RTMP (WebCasting FP)
Local video recording	Yes, 1080p, 30fps
Cloud services	Yes, Box, Google gDrive, Dropbox,
Access to network drives	Yes
Document and media player	Yes
Whiteboard and annotation	Yes
Presentation modes	Protected and open mode
On-screen content arrangement modes	Dynamic
Web conferencing	WebRTC
Dual screen modes	Yes
Integrated web browser	Yes
Customizable background image	Yes

Table 3: Cynap features

4 Cynap Core

Cynap Core offers a limited subset of Cynap's functionality.

For instance you are able to send a video stream to a Cynap Core but you are not able to receive a video stream from a Cynap Core since no stream output functionality has been implemented.

The limit of

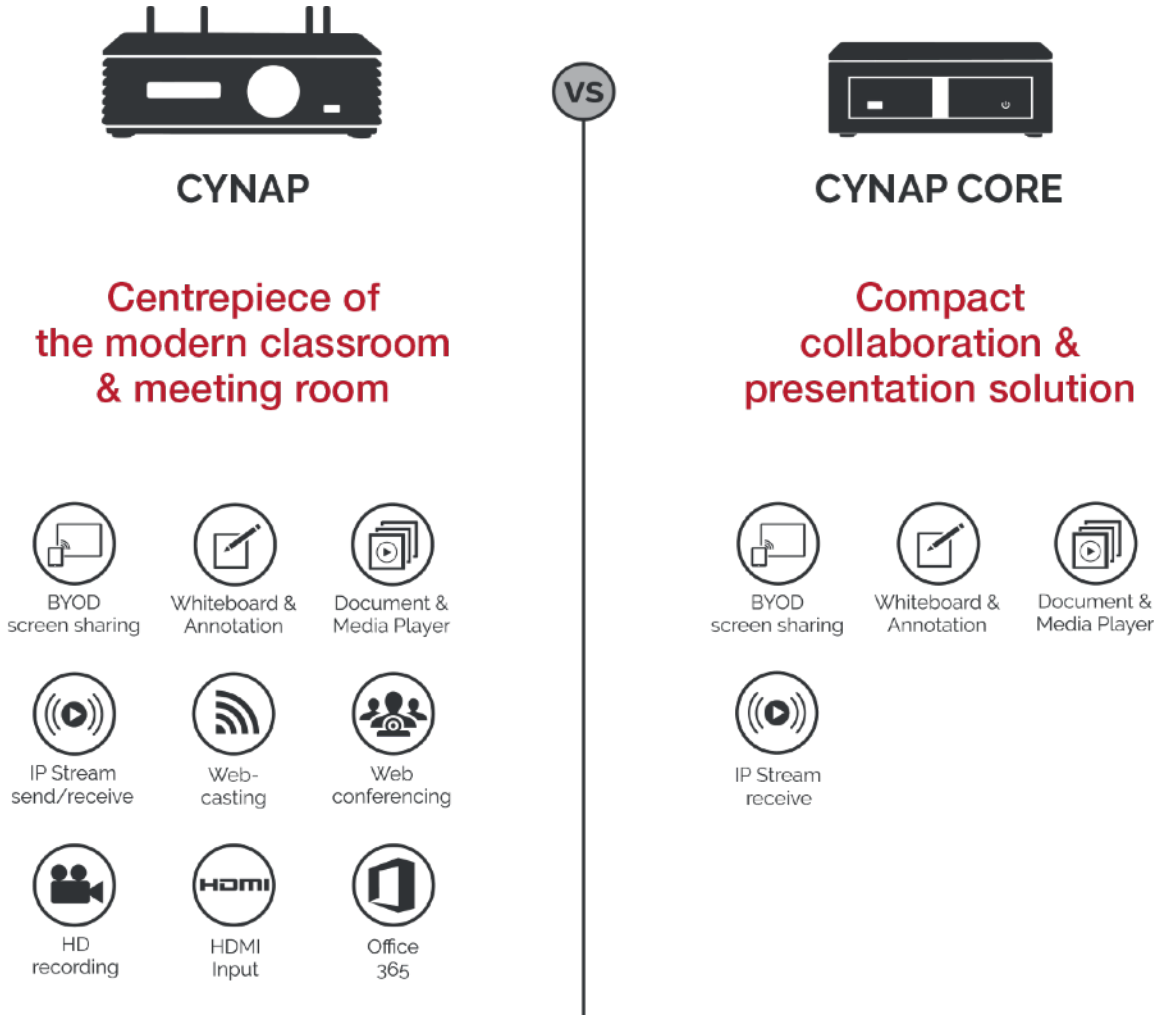
Our ready made Crestron and AMX templates do reflect these changes and so does the WolfProt.

Commands haven't been changed and you are able to use the same commands for Cynap or Cynap Core with the difference that some functions aren't available on Cynap Core based on its limited functions and hardware configuration.

4.1 Cynap Core features

Document and media player	Yes
Compatible device operating systems	All iOS, Android, Mac OS, Windows, Windows Mobile devices, and all current HTML5 supported browsers
Supported mirroring protocols	AirPlay, Chromecast, Mirrorcast, vSolution Cast
Cloud services	Yes, Google Drive, Dropbox, Box, Jianguoyun, OneDrive, WebDAV protocol
Annotation and whiteboard	Yes
Integrated web browser	Yes
Max. no. of open windows	2
Max. resolution	1080p60 (4.4.4), 1080p30 (4.4.4)

4.2 Comparison Cynap vs Cynap Core



5 Connectivity

Wi-Fi standards	802.11 a/b/g/n/ac
Wi-Fi Bands	2.4 and 5 GHz
Data rate	Wireless up to 900Mbps
Network protocols	TCP/IP, FTP, HTTP, HTTPS, SNTP/NTP, RTP, RTSP, RTMP
IP configuration	DHCP, Static, network interface priority
Security encryption	WEP, WPA2, WPA Enterprise or IEEE 802.1x
Max. wireless coverage	Environment dependent
LAN ports	Yes, 2x 1GigE

Table 4: Network connectivity

Cynap supports WolfProt on all networking interfaces. To use it, you simply need to know the IP address of the networking interface you intent to use and also the proper port.

You are able to connect Cynap over a BSD socket or a WebSocket. Using WebSockets instead of BSD sockets offers simplified implementation methods if you want to encrypt access to Cynap using SSL. It also adds JavaScript as new method to control your Cynap or Cynap Core.

Before issuing a command you have to make sure that you're connected to Cynap and logged in as Room Management System user (open socket) or as an admin in case you need to change settings on the fly.

The second LAN port has been provided with a Room Control System in mind. In order to use it, you have to decide if you're binding Cynap into an existing network (LAN2-> set Interface mode to LAN) or if Cynap needs to handle IP addresses (LAN2->Interface mode to WolfVision Visualizer).

Cynap offers TLS encrypted connections – please make sure that you use the corresponding port (see Table 5: Firewall settings).

Cynap offers peripheral control to send specific commands on the attached network to a listening device (such as a projector); issued on startup or while Cynap´s entering standby mode.

Cynap, once in standby mode, needs to be reactivated using Wake-On-LAN (sending a magic packet to Cynap´s MAC address - LAN1 or LAN2).

5.1 Peripheral Control

Sending single commands to a remote unit (Visualizers and Cynaps included) allow for a very simple approach to start or shutdown a device.

You are able to send standardised commands (such as PJLINK) or device dependent commands (such as WolfProt) to be automatically sent while Cynap is booting up or shutting down.

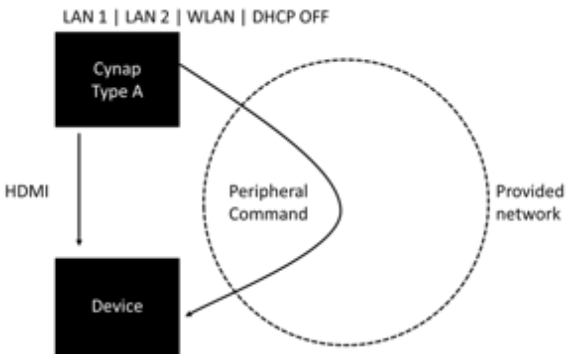
Simply enter the IP address of the device to be controlled along with its port number. Decide if a command is being issued on startup or while entering standby and then the command in hex format as well.

5.2 Integration options

Cynap offers 4 networking ports (3 usable and one solely reserved for Wi-Fi Direct/Miracast). LAN 1 and LAN 2 behave slightly different as LAN2 also supports Visualizer Ethernet Control support and, if activated as WolfVision port starts its own DHCP.

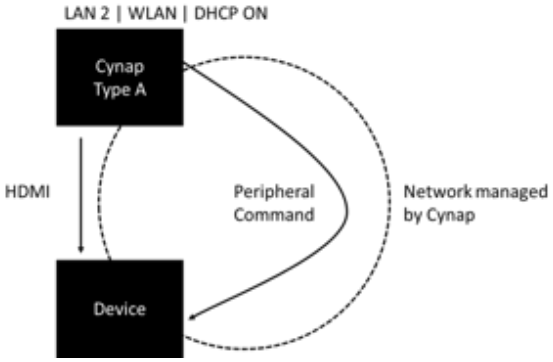
Networking port	Behaviour
Miracast	Wi-Fi only Wi-Fi direct – no support for peripheral control
LAN 1	Considered for being connected to company network DHCP client only
LAN 2	Considered for being connected to Visualizer and Room management system network DHCP client/server
WLAN	Wi-Fi network in client or access point mode DHCP client only
HDBaseT	Certified as Class A, Connected with LAN 2 and an activated DHCP server, a management connection could be established If managed device offers DHCP server functionality, LAN1 and LAN2 can be used (DHCP off)

Configuration 1: Cynap connected to existing customer network



Cynap and controlled device (such as a projector) reside on same network. IP´s on both devices are kept the same to successfully send command to device.

Configuration 2: Cynap providing its own Room Management System network

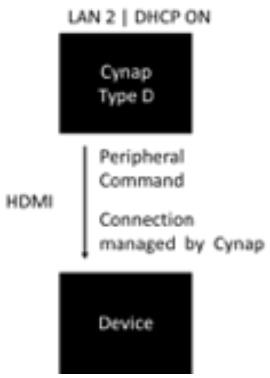


Cynap with DHCP ON creates a network for use with clients and managed devices.
LAN2 with Visualizer on or WLAN in Access point mode starts the DHCP.

Be aware that a Cynap in Access point mode can be detected and used by any device, whereas network access to the network on Ethernet port/ LAN 2 can be protected.

Only a very limited range of IPs is available when activating the DHCP on LAN 2 (from 172.31.255.202 to 172.31.255.210).

Configuration 3



Cynap supports HDBaseT Class A – therefore you are able to send USB, Data and HDMI traffic to your device on a single cable based connection.

On Cynap:
Connect LAN 2 with the HDBaseT Ethernet port.
Activate the DHCP server (Visualizer mode)

On HDBaseT connected device
Based on HDBaseT functionality add a HDBase IP/HDMI splitter.
Read IP Address

On Cynap:
Enter IP address in Peripheral Command settings.

5.3 Serial connectors

Cynap has no serial connector - to use your existing room management system based on serial network, please make sure that you use a RS323-LAN adaptor to send commands to Cynap. Most work perfectly but before buying bulk please test them before purchase.

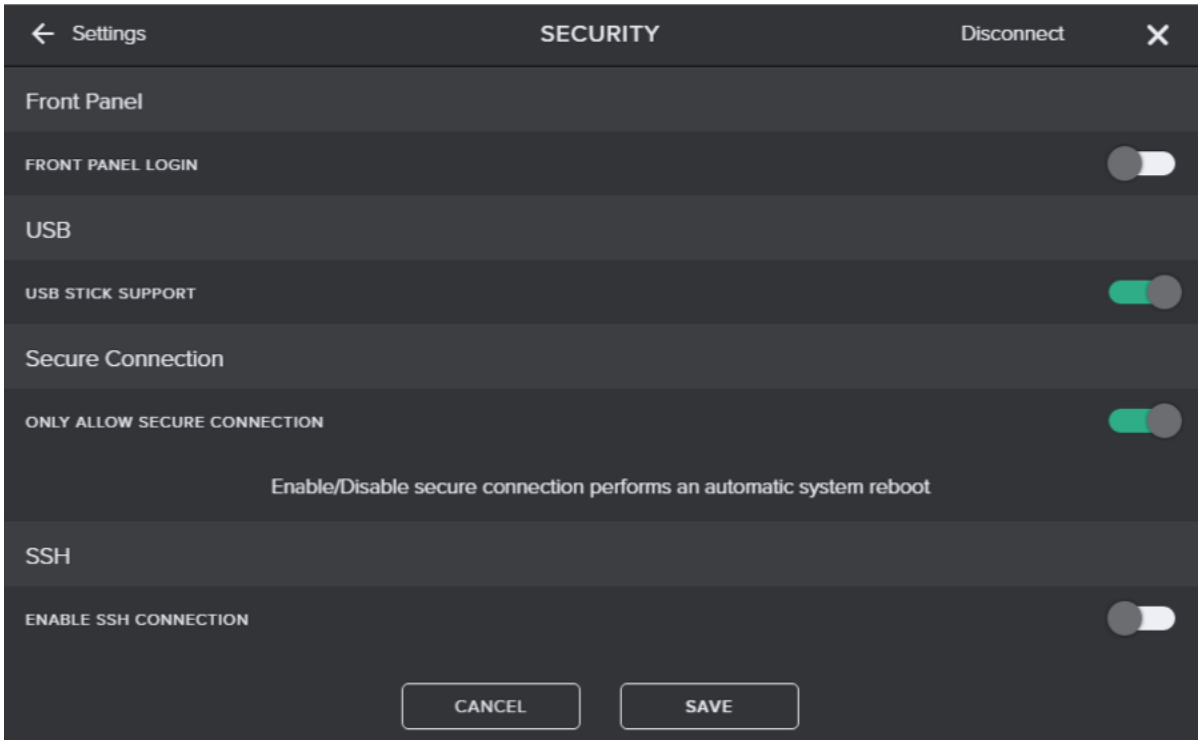
5.4 WolfProt for Cynap and Visualizers

WolfProt has been extended and simplified for use with Cynap. It remains compatible for existing and upcoming Visualizer models.

To address a Visualizer directly, please be aware that communication runs directly over Port 50916 (untouched by Cynap in-between).

Cynap and Cynap Core offer both an unencrypted and encrypted socket connection at the same time.

You're able to switch off unencrypted connections ***by switching on "Only allow secure connection"*** in the *security settings* in which case, the socket uses Port 50917 and blocks the connection on Port 50915.



5.5 Firewall settings

Port #		Feature	Description
50913	UDP/ TCP	WolfVision Device Discovery	Device Discovery (WOL, Wake-On-LAN) Port for WolfVision devices
50915	TCP	Cynap WolfProt	Communication between Room Management System and Cynap
50916	TCP/ UDP	Visualizer WolfProt	Communication between Room Management System and Visualizer
50917	TCP	Cynap WolfProt protected by TLS	SSL encrypted connection to Cynap

Table 5: Firewall settings

Portscan
It requires a port scanner to verify if the necessary ports are available. The laptop (or other scanning device) has to be in the same network and not be obstructed by an activated firewall.

Examples
Portscanner used in examples: nmap (https://nmap.org)
Port **50916** has no Visualizers attached; therefore the service is not running and the port is not responding.

UDP Scan
```
C:\Users\rgraemer>nmap --system-dns --reason -sU -p U:50913,60916 10.0.6.9
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-05 13:23
Nmap scan report for 10.0.6.9
Host is up, received arp-response (0.00013s latency).
PORT      STATE         SERVICE REASON
50913/udp open|filtered unknown no-response
50916/udp closed        unknown port-unreach ttl 64
```

TCP Scan
```
C:\Users\rgraemer>nmap --system-dns --reason -sT -p T:50915-50917 10.0.6.9
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-05 13:21
Nmap scan report for 10.0.6.9
Host is up, received arp-response (0.00034s latency).
PORT      STATE    SERVICE REASON
50915/tcp open     unknown syn-ack
50916/tcp filtered unknown no-response
50917/tcp open     unknown syn-ack
```

For additional port descriptions and networking requirements please read the vSolution Cynap Network Integration Guide manual (available online).

The connection between your Room Management System and Cynap is authenticated by *UserType* and *password*. The session on port *50915* is unencrypted and to use an encrypted session you have to use *50917*.

Visualizer connected to Cynap´s Visualizer Ethernet port: Cynap forwards your Visualizers commands without interfering directly to the Visualizer. The response from the Visualizer will be sent back directly. The connection to your Visualizer is not encrypted.

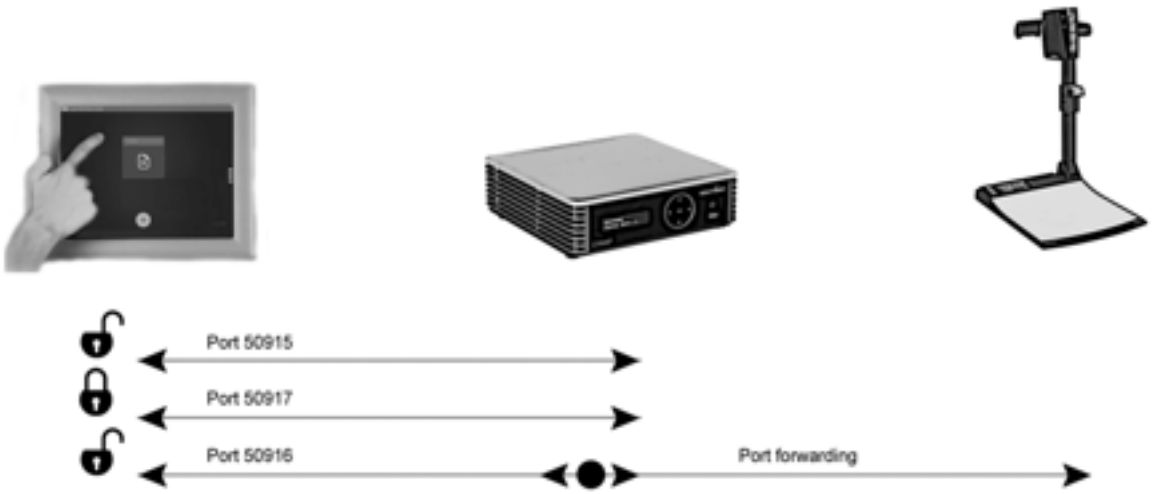


Figure 2: Room Management System Cynap connection to Visualizer (Port forwarding)

WolfVision devices are communicating on Ethernet. To successfully operate and send/ commands, some ports are required to be open.

To send and receive data between Cynap you're able to choose between an SSL encrypted connection or not. To address a Cynap connected Visualizer you still need to use an u**nencrypted session on Port 50916**.

5.6 Get network information from the front panel

Function is limited to the Cynap as the Cynap Core doesn't include a front panel.

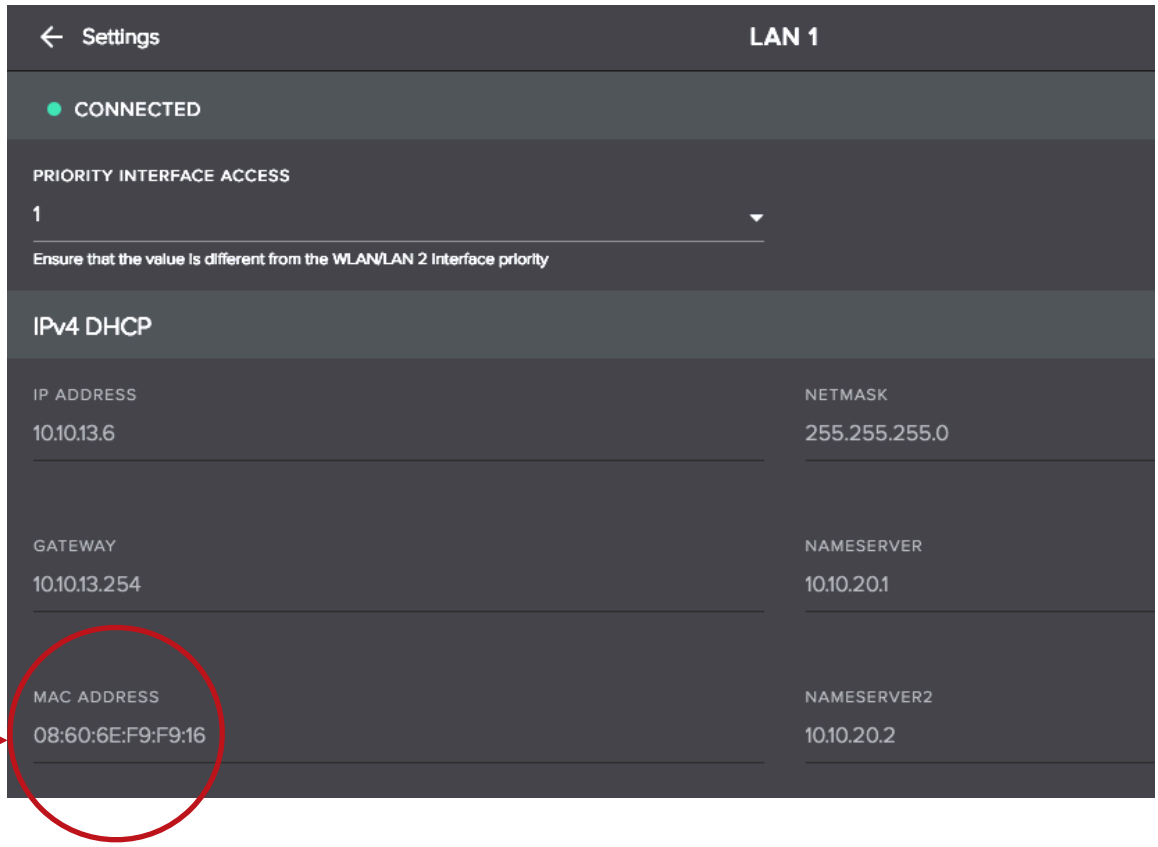
1 Press Down Arrow-Key until you see **LAN Settings**

2 When you see LAN Settings, **press OK**

3 Again, press Down-Arrow-Key until you see the **IP address**

4 Once again, press **Down**-Arrow-Key until you can read the **MAC address**.

The same information can also be fetched from the Browser when you're connected to Cynap's Settings (***Settings -> LAN1 resp. Settings -> LAN2***).



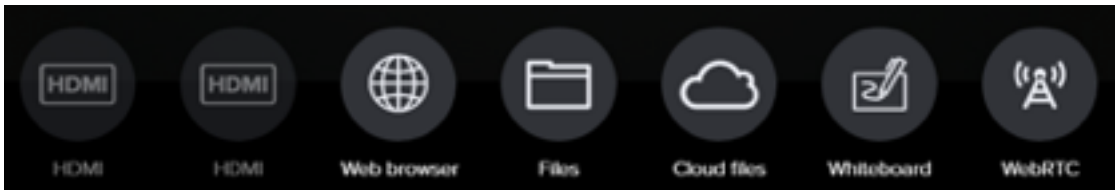
6. User interface

6.1 input sources

Cynap offers various applications, these applications are called sources. Each source, when pressed on the yellow circle (source button) opens up in a new window.

The windows are fixed on a total number of 4. Trying to opening up a fifth one will result in a pop-up message about 4 windows already in use.

WolfProt commands enable you to control the complete user interface.



Icon/label	Description
Web browser	Opens a web browser
Files	Opens the file dialog menus
Cloud files	Opens the Cloud file list or the login screens if not logged in
Whiteboard	Opens an empty whiteboard
WebRTC	Opens a configured WebRTC session - Cynap works best in host mode.
WebCam	UVC attached USB Camera
Input Stream	Video input streams from various sources (IP cameras, Streaming servers, etc.)
Office Documents	Microsoft Office 365 components
HDMI1, HDMI2 input	Attached HDMI input devices
Allow mirroring	Initiate a timed window where a user will be allowed to initiate a screen mirroring connection (times out after 30 sec unless you repeat cycle using the appropriate WolfProt command).

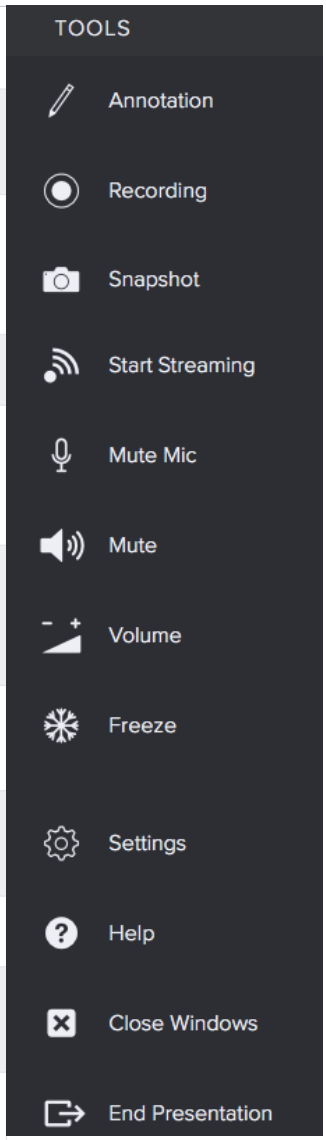
6.2 Toolbar

Controlling the Cynap and Cynap Core in general is hidden behind the menu Toolbar, Indicated by three dots on the right hand side.

It contains action buttons which initiate a direct action such as “Mute”, Create Snapshot etc.

All toolbar functions can be executed using the WolfProt commands.

Label	Description
Annotation	Freezes the screen and displays drawing tools to annotate and save the annotation as a JPG file.
Recording	Starts recording the content on HDMI1 out - if moderator mode in *Settings->Output* is set on HDMI2, then HDMI2 out is being recorded
Snapshot	Creates a JPG image in 1920x1080 resolution (72dpi).
Start/Stop Streaming	Start or stop streaming function - optionally there’s a function to have recording on capturing device disabled
Apps	From Cynap local download of vSolutionCast in cases where guests are not allowed access to internet.
Mute Mic	Mutes the Mic
Volume	Volume up or down
Freeze	Freezes the screen.
Settings	Cynap Configuration settings - admin login required
Help	Onboard help file.
Close Windows	Closes all 4 windows.
End Presentation	End the running presentation - start a new one, enter standby or activate screensaver.



6.3 vSolutionMatrix

vSolution Matrix allows manipulation of video signal traffic between master and clients.

The video signal is being pushed from the master or pulled from the master, the attached client devices do not offer any Matrix functions, all is done on the Matrix master unit (Cynap Core is limited to the client role, and a Cynap can act as master or client).

Therefore integrating the vSolution Matrix by using WolfProt commands is possible on the Matrix master Cynap. All video push and pulls are going through the master, there is no sending signal from client A to client B without going through the master first (pull signal from client A and push signal to client B).

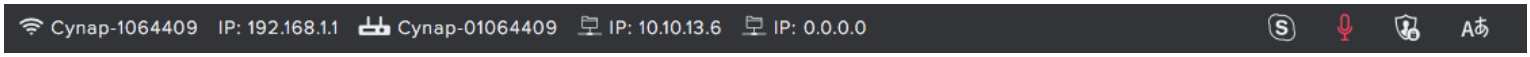
Sharing files from the master unit to the client units is supported on WolfProt. On the vSolution client device you simply mount the Matrix mount to get access to the shared files - it*s as simple as accessing a file on any mounted disk.

Addressing devices is done using the clients serial numbers instead of IP or MAC addresses.

WolfProt commands for this feature is available as a separately sold Feature Pack - The WolfProt commands for this and all other additional Feature Packs (Capture Agent, Office 365 etc.) are always included.

Commands without installed Feature Packs will be ignored by the system.

6.4 Status bar



From left to right: **Wi-Fi SSID, Wi-Fi IP address, hostname, IP LAN 1, IP LAN 2, Skype On/Off, Mic On/Off, admin indicator, Language settings**

The status bar displays the status of various vital functions such as the actual network state and, if allowed, its IP address or if *audio out-mute* has been activated.

It can also be completely switched off if needed. If switched off (for reason of security, etc) you will also gain 20 pixels more screen estate.

The APIs for the querying the status are available for Cynap and Cynap Core, using the same commands.

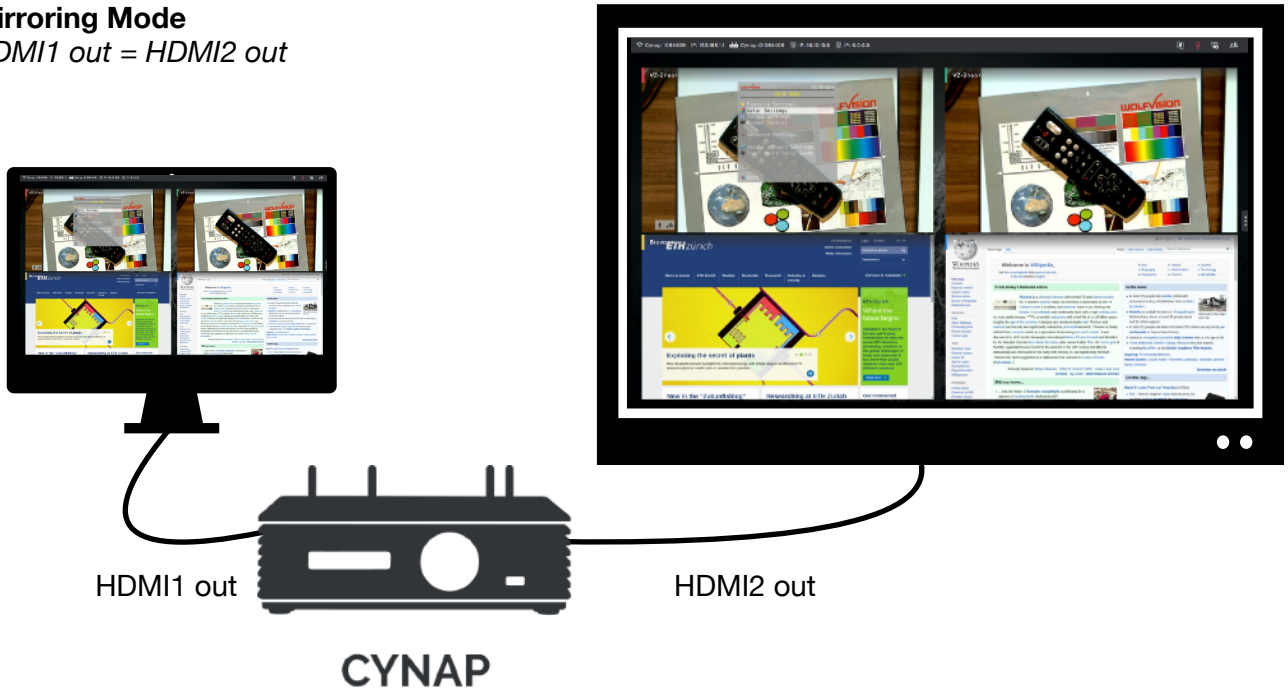
7 Dual Screen management

Cynap offers 2 separate HDMI outs which can be controlled to display different single window content on each of the screen or HDMI1 using an overview to display a specific windows on HDMI2 out.

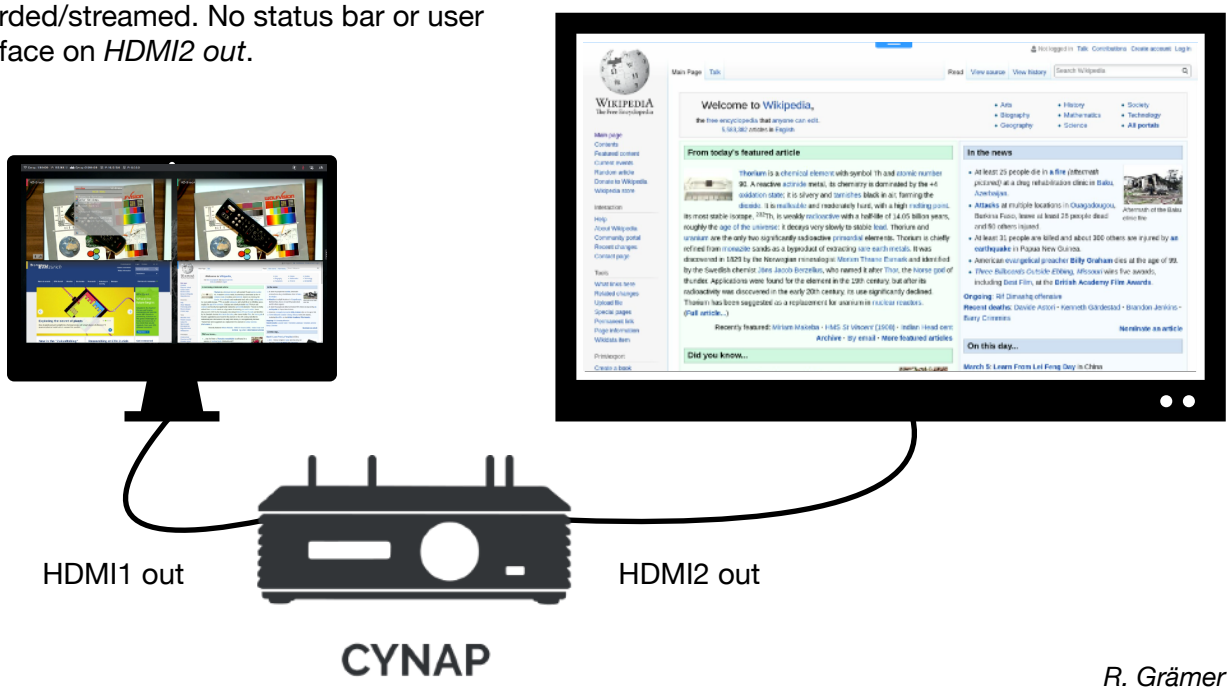
In Content or Moderator Mode, HDMI2 out's output resolution shifts to *1080p60* or *720p60* based on your configured setting.

To manipulate windows settings, shifting contents or restoring previous changed priorities there are a number of commands.

Mirroring Mode
HDMI1 out = HDMI2 out

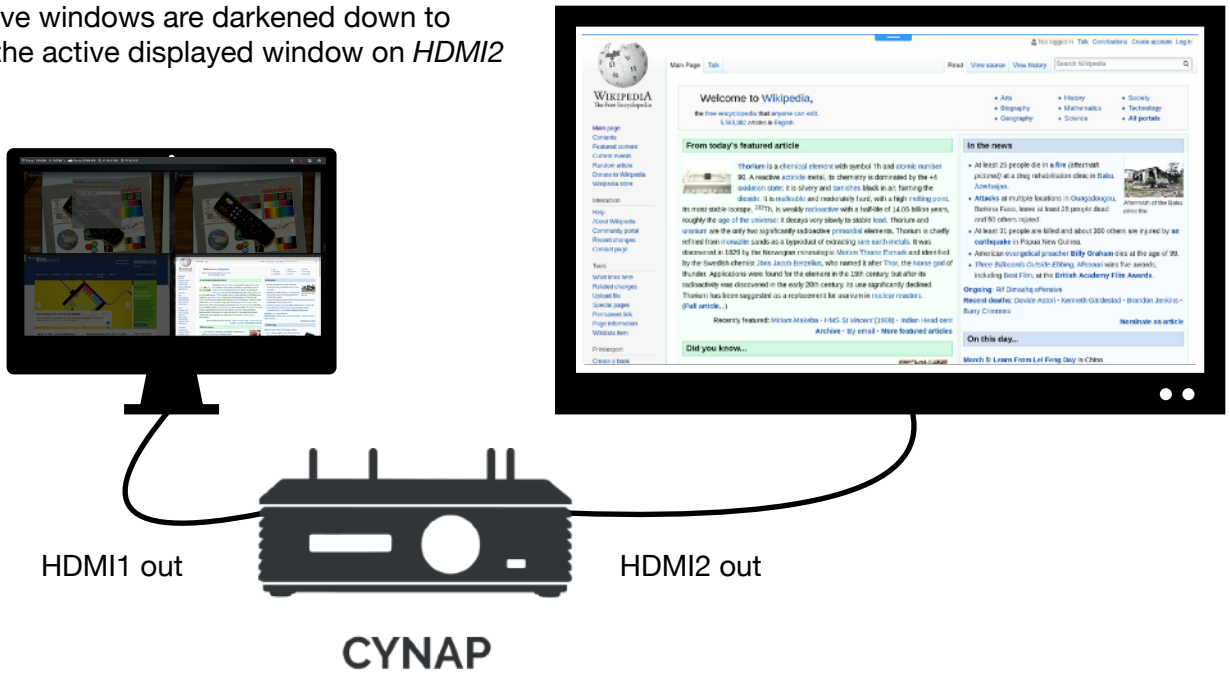


Content Mode
In content mode, *HDMI1 out* will be recorded/streamed. No status bar or user interface on *HDMI2 out*.



Moderator Mode
In Moderator mode, *HDM1 out* becomes an orchestrating window interface - recording and streaming will be done over *HDMI2 out*.

The inactive windows are darkened down to highlight the active displayed window on *HDMI2 out*.



There are specific Window Control commands on WolfProt to manipulate single windows to output specific content on HDMI2 only.

Check Window Control CB28
09 CB 28 02 00 06 to send the first window to *HDMI2 out*.

HDMI1 and HDMI2 are independent HDMI output ports, means, combining 2 HDMI outs to create a single stretched 8K content window or getting 8 independent content windows is not possible.

8 WolfProt for Cynap

WolfProt, the command language for all WolfVision products offers more functionality on Cynap products, as Cynap and Cynap Core in general provide a larger number of functions with higher levels of sophistication.

8.1 Command categories

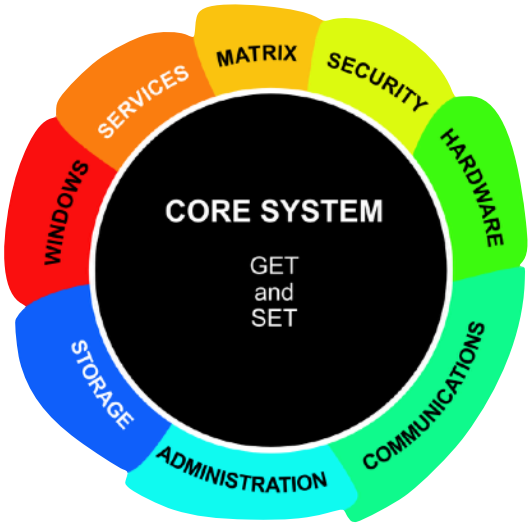


Figure 3: Cynap System Structure

WolfProt API´s are structured into 8 different categories:

Category	Description	Example
Hardware	System commands	Send Standby command
Administration	Basically all the configurable settings (SET commands)	Enable and set GoogleDrive Session
Communications	LAN/WI-FI commands	Stop LAN connection
Services	Cynap services	Start/Stop Recording
Windows	Windows commands	Open new window with content type HDMI 1 in
Storage	File commands	Write to USB
Security	Security related commands	Show Login PIN on HDMI1 out
Matrix	vSolution Matrix commands	Send File to all Matrix clients

Table 6: Command structure

8.2 Cynap specifics

Cynap is slightly different than your usual document cameras - the command syntax not only persists of mainly single commands such as turn on or turn off auto focus.

Most commands also offer an extend data exchange over various kinds of data structures such as JSON.

There are different user levels and additional ways to reach Cynap. And the four content windows need to be addressed to change their outputs.

8.3 Cynap User Authentication

There are 5 Users (or 4 User Types) to control Cynap via WolfProt Commands – if you want to just control Cynap (no changing of configuration settings) then we recommend using the Room Management System User.

The same WolfProt commands are also being used for our range of software (e.g. vSolution Link etc.).

If you need to change certain settings then the user with access level 2, administrator, is the one you need to use to modify Cynap settings.

Passwords have no minimum length; maximum length is 63 bytes (<=63).

API´s which don't require a login will be processed without a required prior login, such a user session will get a user access level of 0 (none).

The difference between Moderator_User and Room Management System_User is, that the Moderator uses a protective layer, forcing web browser visitors/users to log in before they can operate or see content on Cynap.

Note:
you always need to log in (at least on *Access Level 1* – User) to be able to operate with the same commands as a Cynap

Additionally, the password for the Moderator User can be set to a randomised PIN, making it almost impossible to catch up with a proper login to process your own commands and implementation.

If you want to just control Cynap (no changing of configuration settings) then we advise to use the Room Management System User.

The **Room Management System User**, having the same rights as the Moderator, on the other hand, is having its own password and offers no obstructing Cynap created PIN and therefore a simpler access integration for your implementation.

The **Annotation** is the level used for Cynap's annotation functions.

The **Admin user** requires the Password set on Cynap.

The **User None** in general is useful for a quick testing, when you lack the password, and only need to see if you can get a response from Cynap.

Note: It is possible to develop a Cynap controller without a login function. But it requires switching off the login features (user/password combination) and enables everybody with a browser connection to Cynap to possibly interfering with a Cynap presentation.

8.4 Setup Cynap's Room Management System User

There are 5 Users (or 4 User Types) to control Cynap via WolfProt Commands –
If you need to change settings via Terminal then the Admin user is the one you need to get access to Cynap´s settings.

Passwords have no minimum length; maximum length is 63 bytes (<=63).

To avoid confusion between the Cynap moderator and your Room Management System solution and offer the same level of access, we provide an additional user for your Room Management implementation.

Administrator - (access level hex 02):
full access to all functions and settings

User and **RMS User - (access level hex 01):**
access to all operations and querying some settings

Annotation User - (access level hex 03):
for annotate functions only

None - (access level hex 00):
connected but not logged in user has access to limited functions

The user Room Management System offers the same moderator-user rights; but without a randomised PIN.

However, if you don't configure the Room Management System user to protect your access to Cynap, your opened web socket connection will automatically be granted the level USER instead of just UserLevel NONE.

This convenient login feature only works as long as the Moderator USER has no password set.

As soon as the Moderator password has been activated, your setup won't work anymore and a login procedure or the setup of the Room Management System user will be required.

Your anonymous access will be automatically downgraded to user None and most functions will cease to work.

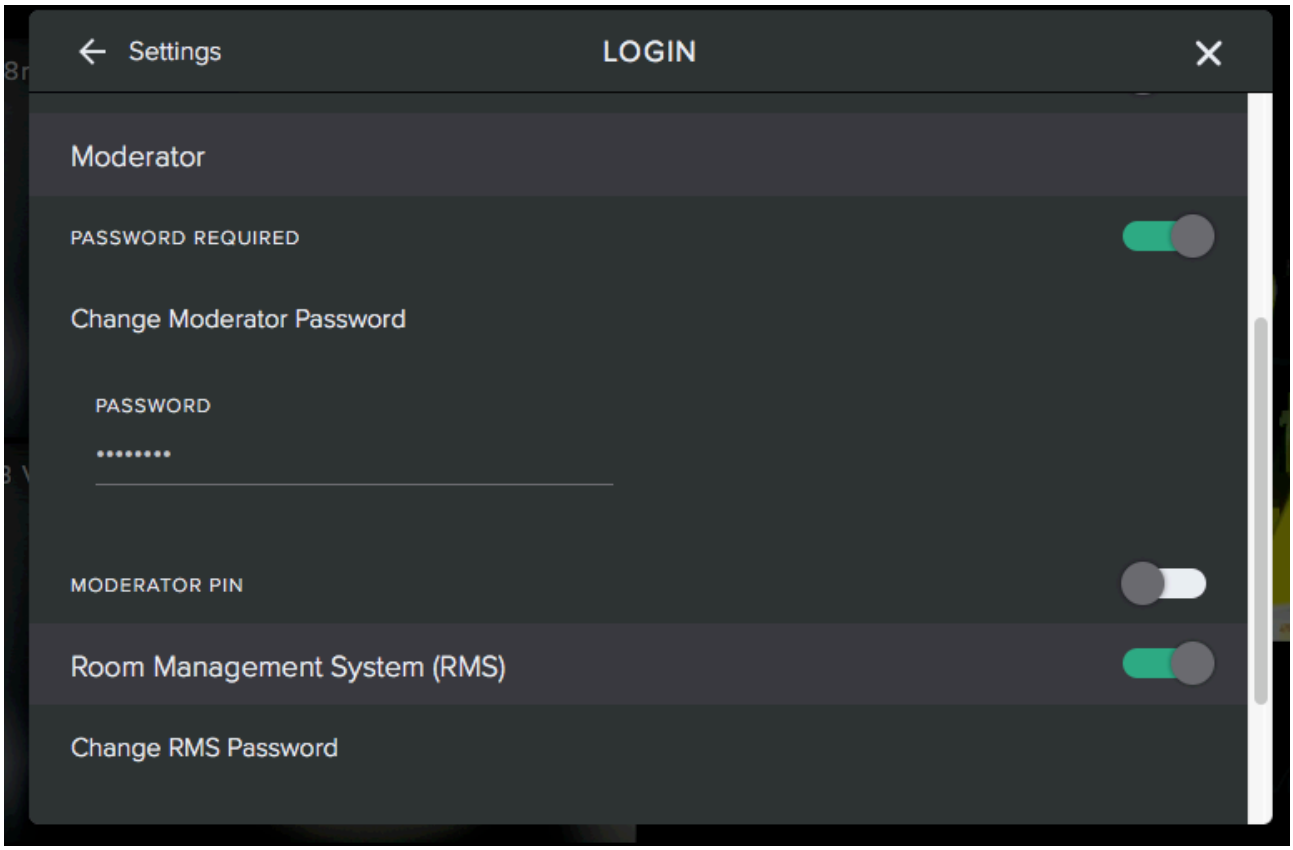
To see which login level for a certain function is needed please check the WolfProt command list PDF on our website

Passwords: we strongly advise to change the initial default user password, also make sure that the user password differs from the RMS user password.

The API´s which require User Level None will be processed without a required prior login.

8.5 Steps to activate your RMS user

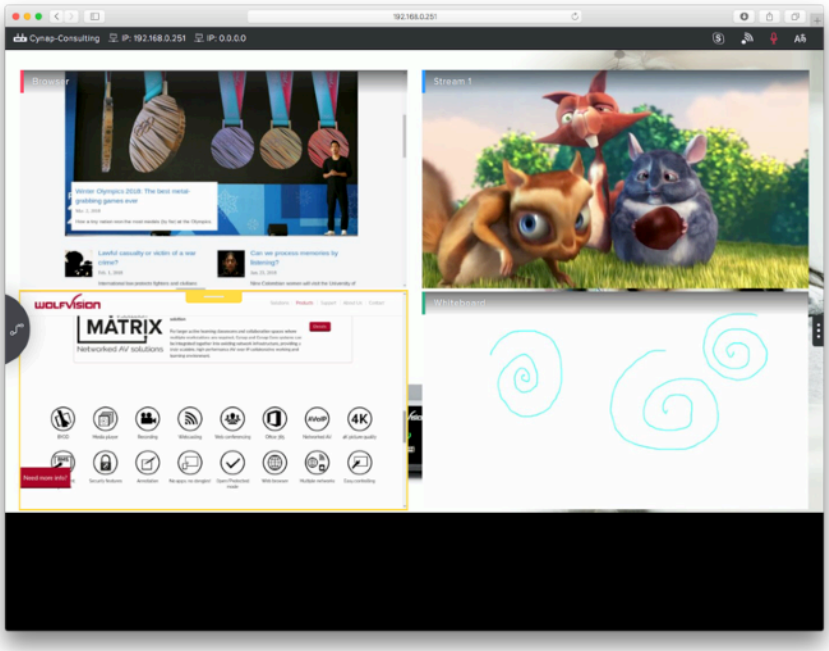
1. Enter the LOGIN settings on Cynaps Settings page.
2. Scroll to the bottom.
3. Activate the RMS user (switch enable button) and then add a password for your RMS user.



9 Windows

There are four controllable windows on Cynap. They are differentiated on IDs which represents always the same color. Opening, closing and manipulating windows can be enriched with parameters to achieve a different outcome (open browser vs open browser using URL xyz).

After a total of 4 windows got opened the used won't be able to use a fifth one without closing one of the existing 4. File functions, such as save a recording on a specific cloud service, are still available.



9.1 Windows Control

In general windows can be opened/closed, muted, put in full screen or set, if configured, on a second screen (HDMI2 out) called **Dual screen** feature.

WindowControl gives you control to manipulate the 4 Cynap windows. In the API, the set command to open a window uses following structure:

Color and corresponding WindowID:

Priority (same on remote)	Color	WindowID (d0)
1st	red	0
2nd	green	1
3rd	yellow	2
4th	blue	3
SourceButton	autoarrange	-1 (ff)

Table 9: Remote Window Color ID

Figure 4: color coded windows on remote

9.2 Window Control (CB 28)

Common control Commands (Window Control) when selecting a specific window.

Set	Command	Window ID (d0)	Action	Function
09	CB 28 02	D0	0	Close window
09	CB 28 02	D0	1	Size: Full screen
09	CB 28 02	D0	2	Size: Window
09	CB 28 02	D0	5	Toggle Full screen/Window
09	CB 28 02	D0	6	HDMI2 Copy: On
09	CB 28 02	D0	7	HDMI2 Copy: Off
09	CB 28 02	D0	8	HDMI2 Copy: Toggle

Table 10: Window Commands

Command for specific audio control commands.

Set	Command	Window ID (d0)	Action	Function
09	CB 28 02	D0	3	0x00 mute off 0x01 mute on
09	CB 28 03	D0	0x04	0x00 to 0x64 (volume in %)

Content-Aware commands such as to pause a video or adding a different URL on a browser content are being executed by processing WindowTypes (see below) and its specific commands.

9.3 Window Start (Window Types) CB 2C

Based on the content the window changes its type. For example, a video content behaves differently than a PDF in that manner that the video player can be paused and a PDF file can be zoomed in. The parameter of a web browser consists of the URL and the parameter of an image of the file source location.

Window Types are used for the Window Start (0D CB2C) command. Based on the WindowType its parameters also change.

WindowTypes are:

ID	Name	Functionality	Parameter
0	None	Available window All 4 windows are always on and hidden. If you run out of Window type 0x00 then this means that all 4 windows are being in use.	none
1	Visualizer	Wolfvision Visualizer support	None
2	HDMI Input	Select HDMI1 or HDMI2 input	**0x00** for HDMI1 or **0x01** for HDMI2
3	Web Browser	Start web browser If no URL is specified it will take the default page (either 4 icons or the start page from (Settings -> General).	URL
4	Miracast	Microsoft´s Wi-Fi direct connection	none
5	AirPlay/ GoogleCast	AirPlay and GoogleCast	none
6	Video	.mp4, .mkv, .avi	Location and name
7	vSolutionCast	BYOD for Windows 7	none
8	Image	gif, jpg, png, bmp	Location and name
9	PDF	PDF files	Location and name
0a	Office presentation	PowerPoint files	Location and name
0b	Office text	Word files	Location and name
0c	Office calculation	Excel files	Location and name
0d	Whiteboard	Drawing board	None
0e	Audio	.mp3, .oga	Location and name
0f	Webconference	WebRTC client	None
10	Webcam	USB Camera support	None
11	Stream Input	RTSP Input stream	0x00 to 0x03 Index # of predefined URL

12	Skype for Business	Skype for Business window	None
13	Office 365: Outlook	Outlook window	None
14	Office 365: Word	Word window	None
15	Office 365: Excel	Excel window	None
16	Office 365: PowerPoint	PowerPoint window	None
17	Office 365: OneNote	OneNote window	None

Table 11: Cynap Window Types

10 File Operations

Cynap supports various file types and file services. If a Cynap user did log into a cloud service will grant you access to upload a snapshot or a recording without the need of mounting the cloud service yourself (no cloud login procedure necessary - just fetch the list of mounted drives and check if a preferred cloud has already been mounted).

Supported are FAT16 and NTFS on a USB memory stick - when storing files on a FAT16 stick, make sure that you remind the user of the 4 GB file limit before copying fails.

API	Command	Description
Get Mounts List	08 CB 3D 00	Information on available mounted file system and their status (JSON array)
Get File List	0C CB 3E	Provide the root path and you will get a list of files (JSON array)
Get File Download List	08 CB 7B 01	If you send a length of 0 you will get a merged list of all downloads otherwise (length == 1) you´re able to filter 0: DropBox 1: Google Drive 2: Box
Get File Upload List	08 CB C1 01	JSON array of all file uploads in progress
Get Cloud Mode	08 CB 8F 00	Disabled/enabled returns per cloud service
Get Cloud Status	08 CB 4C 00	Status on all cloud services returned
Get FTP Mode	08 CB 62 01	FTP server configured – no status on availability

Table 12: File commands

The array of the mounted drive not only tells you the name but also if the drive is writeable or available in the cloud.

name l name of mount	Id l unique ID	type l local, net	status l mounted or not	perms l read/write
Internal	Internal	Local	mounted/notMounted	ro: read only
System	System	system	notMounted	
USB	USB	usb	mounted/notMounted	rw: read, write
Dropbox	dropbox	cloud	mounted/notMounted	rw: read, write
Google Drive	gdrive	cloud	mounted/notMounted	rw: read, write
Box	box	cloud	mounted/notMounted	rw: read, write
Jianguoyun	jianguoyun	cloud	mounted/notMounted	rw: read, write
OneDrive	Onedrive	cloud	mounted/notMounted	rw: read, write
WebDAV	webdav	cloud	mounted/notMounted	rw: read, write

Network Drive 0	netdrive0	netdrive	mounted/disabled	ro/rw
Network Drive 1	Netdrive1	netdrive	mounted/disabled	ro/rw
Network Drive 2	Netdrive2	netdrive	mounted/disabled	ro/rw
Network Drive 3	Netdrive3	netdrive	mounted/disabled	ro/rw
Network Drive 4	Netdrive4	netdrive	mounted/disabled	ro/rw
Network Drive 5	Netdrive5	netdrive	mounted/disabled	ro/rw
Network Drive 6	Netdrive6	netdrive	mounted/disabled	ro/rw
Network Drive 7	Netdrive7	netdrive	mounted/disabled	ro/rw
Network Drive 8	Netdrive8	netdrive	mounted/disabled	ro/rw
Network Drive 9	Netdrive9	netdrive	mounted/disabled	ro/rw
FTP	FTP	ftp	mounted/disabled	wo
cdrive	*cdrive*	*cdrive*	*mounted/notMounted*	*For future use*
Matrix Master	matrixMaster	matrix_master	mounted/notMounted	ro
Matrix Station	matrixStation	matrix_station	mounted/notMounted	ro

The ftp session won't be checked every 10 secs unlike the network drives – the status mounted therefore doesn't tell you if the ftp-connection is working; the status mounted informs you that an ftp connection has been configured.

Cynap's operating system does not allow file manipulations - for security reasons: the file systems are being purged as soon as a new presentation starts or Cynap got rebooted. Temporarily sharing media files content from local and remote resources are allowed (e.g. download from cloud and present on Cynap in image viewer).

- Downloading video images office documents from the cloud services
- Displaying video images office documents from internal/external/remote locations
- Uploading recordings and snapshots only from internal location

The file list array consists of two fields. Field one requires the file name and field two contains the file type.

The file types supported by Cynap have a specific identifier and file types not supported by Cynap are specified as unknown.

To open a file, you have to prepare its fully qualified name. The fully qualified name is generated from the mounted storage device, 3 leading slashes, the path and the filename itself.

e.g. USB:///Folder1/video1.mp4

File Type	Description
Audio	Audiofile (e.g. .mp3, oga, …)
calc	Spreadsheet files (.xls, xlsx)
dir	Directory
html	Locally saved webpage
image	Pictures in gif, png or other supported formats
pdf	PDF file
presentation	Powerpoint
text	Word or text files
unknown	Unknown file format - please hide or mark as unknown
video	Supported video format

10.1 File Transfer (FTP)

When uploading a file from Cynap to an FTP server please make sure, that your FTP server is already set up with a user and password combination and owns the proper rights to create/ replace files – FTP file transfer offers a user/password combination but no further settings such as ACTIVE/PASSIVE or specific parameters such as Kerberos login or other sFTP options.

Cynap's FTP client connection is not polled and uploading a file to the FTP server requires your implementation to handle connection continuity.

10.2 Cloud support

The cloud as read-write device, once logged in by the user, behaves like a common network file share (CIFS).

Mount names of type Cloud

Mount	Id	URL
Box:///	Box	https://www.box.com
Dropbox:///	Dropbox	https://www.dropbox.com/
Google Drive:///	Gdrive	https://www.google.com/drive/
Jianguoyun:///	Jinanguoyun	https://www.jianguoyun.com
OneDrive:///	OneDrive	https://www.onedrive.com
WebDAV:///	WebDAV	Custom WebDAV link

Cloud status: WPC_Cloud_Status (0xCB4C)

0x00	Disconnected	Connect if required
0x01	Oauth Open Authorization 2.0	wait
0x02	Connected	file list access pending: wait before fetching the cloud file list
0x03	Connection failed	Network/authorization problem
0x04	Synced	Cloud directory read: Ready to
0x05	Disabled (not configured)	

Cloud API´s

	WPC_CLOUD_CONNECT	0xCB 0x45
	WPC_CLOUD_PRELOAD	0xCB 0x46
	WPC_CLOUD_STATUS	0xCB 0x4C
Enable/Disable cloud services	WPC_CLOUD_MODE	0xCB 0x8F
	WPC_CLOUD_UPLOAD	0xCB 0xA1
	WPC_BOX_CLOUD_DATA	0xCB 0xCC

10.3 Network file share (CIFS)

Cynap´s network file share is based on CIFS (Common Internet File Share). Once configured (up to 10 drives) it allows you to up/download files from Microsoft servers. A CIFS share can also be configured as a default destination for snapshots and recordings.

Please bear in mind that a CIFS name (e.g. MYSERVER1) needs to be configured on your local DNS server otherwise you have to use the IP address to access the CIFS share.

10.4 USB external HDD or memory stick

A single FAT32 or NTFS formatted drive can be attached and accessed via Cynap. Feature Pack **Capture Agent** allows for an ***ext4*** attached drive connection in combination with an Opencast LMS.

10.5 Internal storage

There are two types of files:
1. Cynap created content such as *snapshots* and *recordings* and
2. Temporary files such as downloaded content from attached remote locations

Only Cynap created files can be deleted, uploaded or copied to a USB storage device.

Example: JSON Array of list of mounted storage


```
[
{"id":"Internal","name":"Internal","type":"local","status":"mounted","perms":"ro"},
{"id":"System","name":"System","type":"system","status":"notMounted"},
{"id":"USB","name":"USB","type":"usb","status":"notMounted"},
{"id":"dropbox","name":"Dropbox","type":"cloud","status":"disabled"},
{"id":"gdrive","name":"Google Drive","type":"cloud","status":"disabled"},
{"id":"box","name":"Box","type":"cloud","status":"disabled"},
{"id":"jianguoyun","name":"Jianguoyun","type":"cloud","status":"disabled"},
{"id":"onedrive","name":"OneDrive","type":"cloud","status":"disabled"},
{"id":"webdav","name":"WebDAV","type":"cloud","status":"disabled"},
{"id":"netdrive0","name":"Network Drive 1","type":"netdrive","status":"disabled"},
{"id":"netdrive1","name":"Network Drive 2","type":"netdrive","status":"disabled"},
{"id":"netdrive2","name":"Network Drive 3","type":"netdrive","status":"disabled"},
{"id":"netdrive3","name":"Network Drive 4","type":"netdrive","status":"disabled"},
{"id":"netdrive4","name":"Network Drive 5","type":"netdrive","status":"disabled"},
{"id":"netdrive5","name":"Network Drive 6","type":"netdrive","status":"disabled"},
{"id":"netdrive6","name":"Network Drive 7","type":"netdrive","status":"disabled"},
{"id":"netdrive7","name":"Network Drive 8","type":"netdrive","status":"disabled"},
{"id":"netdrive8","name":"Network Drive 9","type":"netdrive","status":"disabled"},
{"id":"netdrive9","name":"Network Drive 10","type":"netdrive","status":"disabled"},
{"id":"cdrive","name":"cdrive","type":"cdrive","status":"disabled"},
{"id":"FTP","name":"FTP","type":"ftp","status":"disabled"},
{"id":"matrixMaster","name":"Matrix
Master","type":"matrix_master","status":"mounted","perms":"ro"},
{"id":"matrixStation","name":"Matrix
Station","type":"matrix_station","status":"notMounted"}
]
```

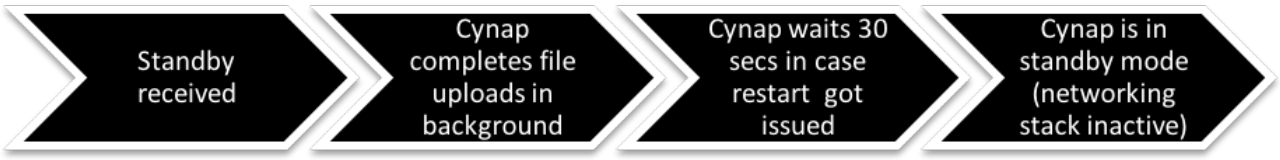

Example: JSON Array of file listing (root USB:///)


```
[
{ "name": "wolfvision", "type": "dir" },
{ "name": "bigbunny.avi", "type": "video" },
{ "name": "compressed.rar", "type": "unknown" },
{ "name": "cynap.log", "type": "unknown" },
{ "name": "music.mp3", "type": "audio" },
{ "name": "test.txt", "type": "text" },
{ "name": "user.data, "type": "unknown" },
{ "name": "video1.mp4", "type": "video" }
{ "name": "video2-h265.mkv", "type": "video" },
]
```


Remember:
Cynap will not support files of type listed as *unknown*.

11 Cynap in standby

Figure 5: Standby process



Once the user presses the standby button, Cynap will enter the standby mode by checking if vital background processes are needed to be completed (such as an initiated upload on a recording) and adds a grace period of 30 seconds before entering standby (in case a restart command got received).

The networking stack and all other monitoring activities are shut down. The only way to start a Cynap from standby is to use the remote, the power button on the front panel or cable based network* to send a Wake-On-LAN command.

Since your Room Management System is connected to Cynap via Ethernet, you will need to issue a Wake-On-LAN command.

Polling to keep a connection on Cynap via ping or echo command does not work - you will have to issue a GET command to get the proper status (esp. if Cynap is entering standby)

To wake Cynap from standby a user needs to press the power button on the remote or on Cynap.

Your Room Management System implementation needs to send a broadcast to the MAC address of Cynap issued in a magic packet to initiate the start-up process.

Figure 6: Wake-on-LAN process

***Wake on WI-FI is not supported as antennas are not powered**

For an example please head to the WakeOnLAN source code section in Hands On part

Part Hands On

Only Chuck Norris writes perfect code that optimises itself.

12 Tutorials

12.1 Hello World: Audio Toggle

As a basic fist and simple setup we won't start with a complicated setup; instead we are using the existing Cynap in front of you, which allows us to send a command that will be processed by the device itself.

A simple Audio-Toggle command allows us to see and hear a difference in Cynap behaviour.

To process the command we are using the Peripheral Command feature of Cynap.

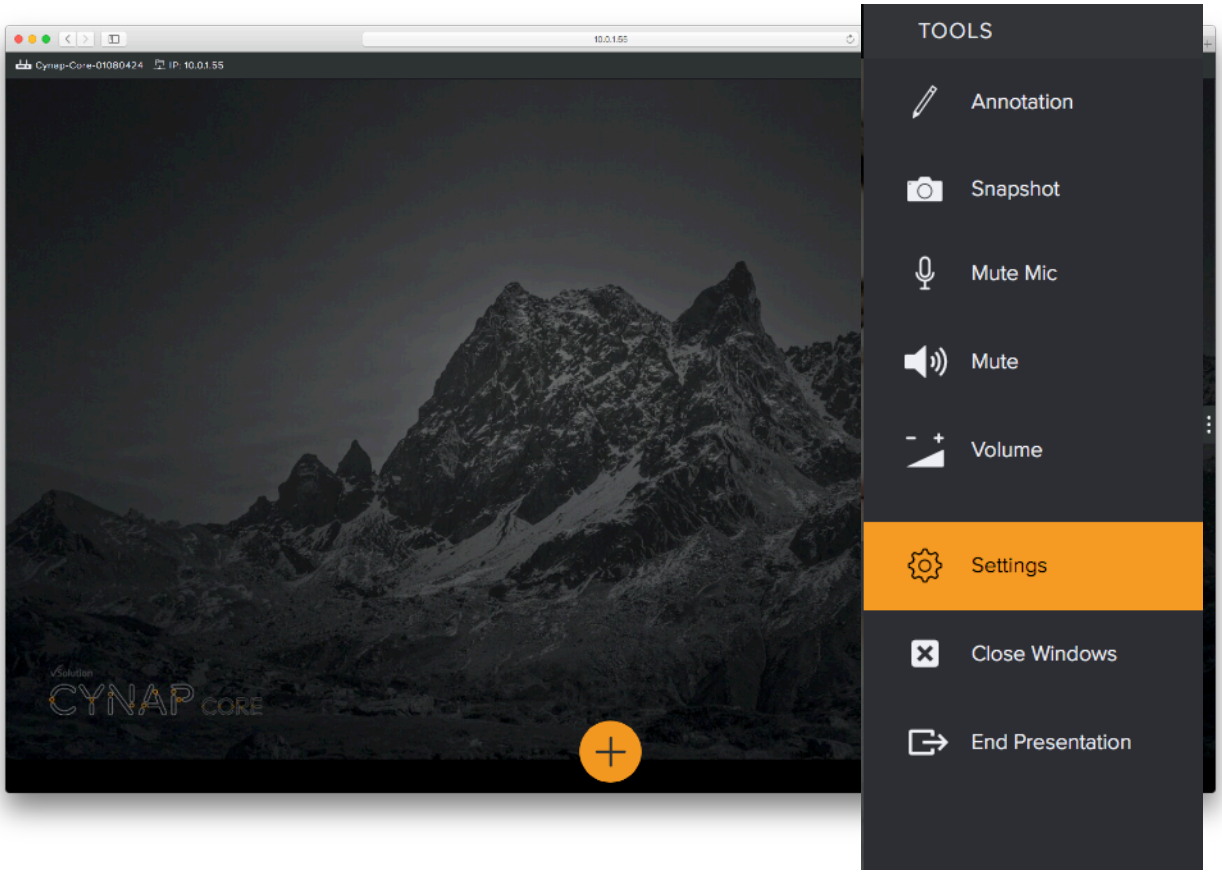
Things to consider:
IP of controlled Cynap (in that case, localhost), Command and the typical WolfProt command port.

IP	Port	Command
127.0.0.1	50915	09CB580102

CB58: Master mute - with parameter "Toggle"

First step

Open Cynap's Toolbar menu and click on Settings to log into the settings menu.

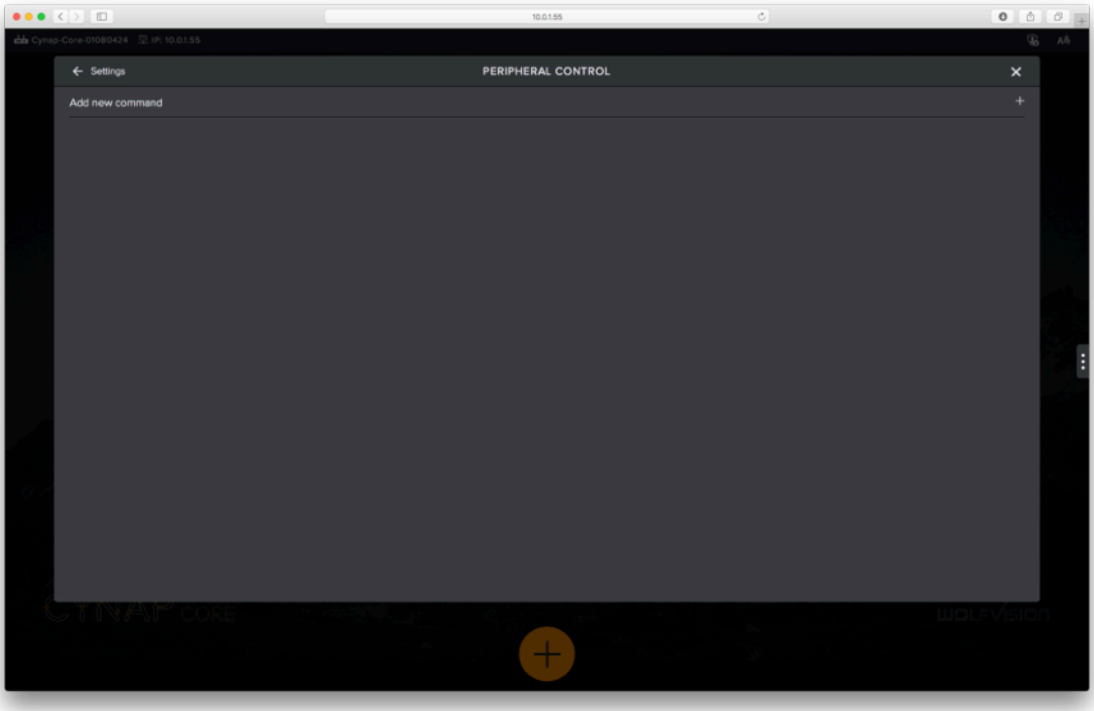


Step 2

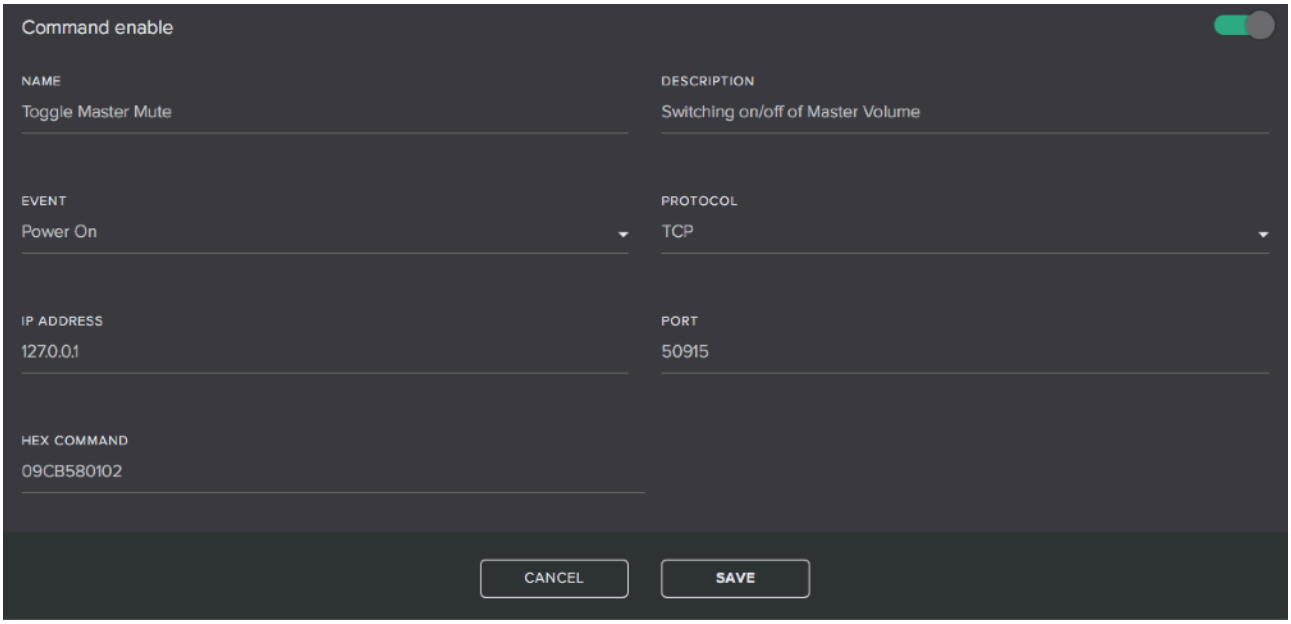
Click on Peripheral Commands

Step 3

Add a new command



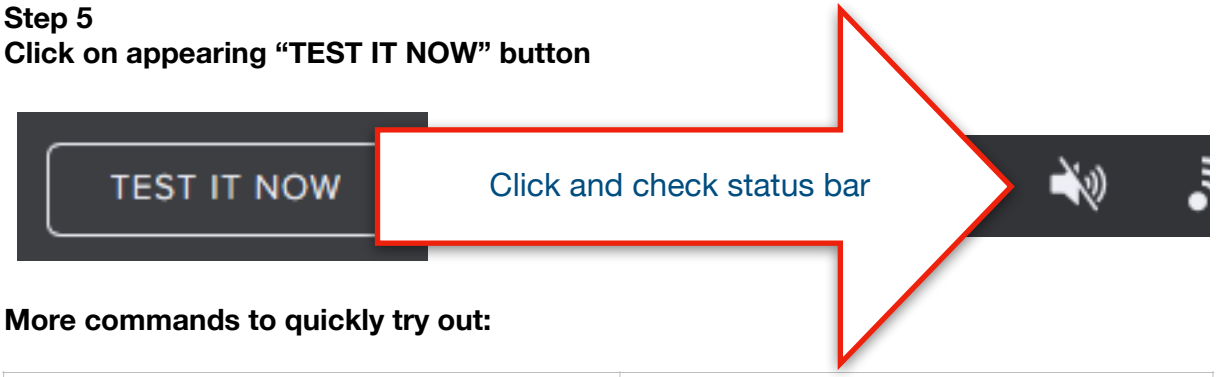
Step 4
Enter necessary details from table below and press SAVE, right after save a new test button will show up.



Necessary details:

Name: customised Name, eg. **Toggle Mute**	Desc.: maybe a bit more, **esp. if you are executing more than one command at once**
Event: **Power On**	Protocol: **TCP**
IP Add: Localhost, **127.0.0.1**	Port: **50915** or **50917 (SSL encr.)**
Hex Command: **09CB580102**	

Step 5
Click on appearing "TEST IT NOW" button



More commands to quickly try out:

Start streaming: **09CB200101**	Open window using HDMI1 input: **0DCB2C0005FF02000100**
Log in as admin, using Password as password and switching Mirroring mode from *open mode* to *protected mode*: **09CB420A02085061737377 6f726409CBD30130**	Enable mirroring in protected mode: **09CB3B0101**

Please remove entries afterwards unless you want to keep them to be issues on startup/ standby.

12.2 Open WebSocket in JavaScript

Unlike the BSD socket which uses port 50915, the WebSocket port can be accessed using the standard ports (unencrypted: 80, SSL encrypted. 443).

It's a HTML5 feature and allows you to operate Cynap from standard WebTechnologies such as JavaScript or PHP to send commands and receive messages.

It is supported by most major browsers such as Chrome, Edge, IE, Firefox, Safari and Opera.

URL (wsURL): **ws://<IP-of-Cynap>/xxx** e.g. ws:///192.168.0.1/xxx

```
function init_websocket(wsURL) {

        myWebSocket = new WebSocket(wsURL /*,'dumb-increment-protocol'*/ /*'binary'*/ );
        myWebSocket.binaryType = "arraybuffer";

        myWebSocket.onopen = function (evt) {
                console.log("Websocket connection '" + wsURL + "' is now open.");

                // cyclical check of websocket connection and send keepalive command
                setInterval(function () {
                        switch (myWebSocket.readyState) {
                        case WebSocket.CONNECTING:
                                return -1;
                        case WebSocket.OPEN:
                                // no action needed
                                break;
                        case WebSocket.CLOSING:
                                return -1;
                        case WebSocket.CLOSED:
                                // try to reopen the connection
                                myWebSocket.open();
                                return -1;
                        default:
                                // this never happens
                                break;
                        }

                }, 60000);
        };
}
```

12.3 Login command CB42

The login command is a set command which requires the access level you want to get combined with the necessary password.

// open connection, using *BSD* or *web socket* and then send following command:
// 09 CB 42 {*password_length* + *2*} {*access_level*} {*password_length* <=63} {*password*}

Send hex command: 09 CB 42 0A 01 08 t e s t I n g 8

0x09	The command starts with a 09 as a set command, the size of the parameters won't exceed 256 therefore the initial hex set command starts with a 09 instead of a 0D.
0xCB 0x42	the call for the Cynap Login command
0A	the size of all parameters in total is 10
0x01	0x01: User level 0x02: Admin level 0x03: Annotation level
0x08	Length of CHARS of password
testing8	Password value Does not need to be converted into hex (ASCII c equals to 0x63)

Troubles?:
You are able to use the Peripheral Command feature of Cynap to experiment with any command even with the login command.

My advise:
Use the admin login command concatenated with a command requiring admin level rights to see if it works.

12.4 Window Start (open browser with URL) Example

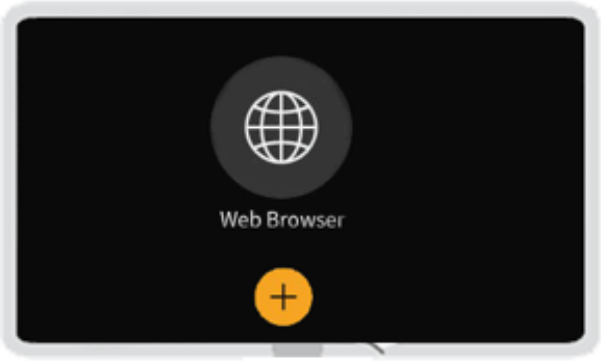
Scenario:
Provide a simple Web Browser function on your Room Management System where the user is able to use the keyboard to enter a URL and then visit the URL on Cynap's web browser.

Should you not provide a URL as a parameter, then Window Start (CB2C) will open the browser with its starting page (either the one you configured in the settings or the default one with the four icons for WolfVision, Wikipedia, YouTube and Google).

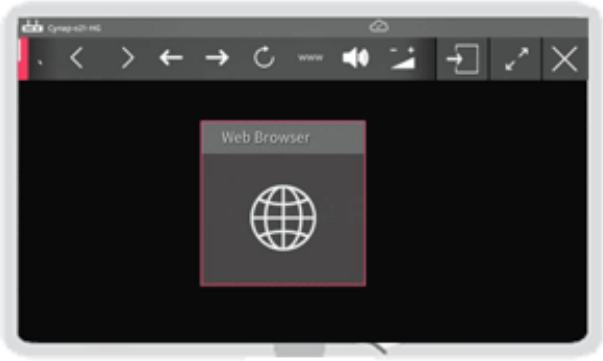
On Cynap we are able to see the newly opened web browser window with a destination URL already loaded.

For simplicity we use the parameter autoarrange (-1 or 0xff) where Cynap opens up the next possible window; if you want to try out the windows ID you're welcome to use one of the four ID´s - *0x00, red, to 0x03, blue,* - to open one of the four specific content windows.

Start with defining your layout



1. Implement your Menu
Simple layout with your own colours and symbols



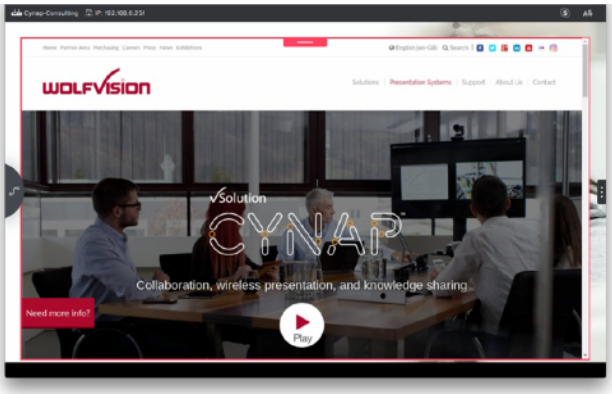
2. Create context
Add context sensitive toolbar (e.g. button for URL)

3. Enable keyboard
Show up keyboard to have URL entered

4. After you store the URL you are able to issue the WolfProt Command :
set the *WindowType* to *Browser* with a specific web address (cynap.net).

The URL will not be parsed by the WolfProt Command Agent – a malformed URL will be displayed as not found – the developer of the controller implementation needs to take care of validating the entered URL which a user typed in.

As soon as you execute the command, a browser window of cynap.net should show up.



WolfProt Command:

```
// Your RMS layout/implementation done
// Loop: Open socket and poll public GET command
//                          (e.g. polling a get command to receive a PIN,
//                          see PIN Status Room, 08 CB 54 00)
// Loop: Check if AuthorizationLevel is set to RMS_User
//                          (Set Login, 09 CB 42 01, see Login)
// All OK? Then send "Window Start, WindowID=auto arranged,
WindowType=browser"

While (socketOpen)
  While (RMS_User_logged_in)
    Send 0D CB 2C 00 0D FF 03 00 09 c y n a p . n e t
```

Command explained

0x0D	This command doesn´t start with the usual 09 visible in the set command, as the length of the parameter could exceed 256 (e.g. URL > 256 chars).
0xCB 0x2C	the call for Window Start
0x00 0x0D	the size of the parameter is 13 or in hex 0D. Since we have to follow protocol, the first 00 must be set to 0 since we are not exceeding 0xFF on the first length parameter.
0xFF	-1 for auto arranging the window (the next free one will be taken until all are used up. Before issuing a window start please make sure that not all Windows already show user content.
0x03	type of window in this example opens browser content
0x00 0x09	size of parameter, in this case, size of the following web address
c y n a p . n e t	Does not need to be converted into hex (ASCII c equals to 0x63)

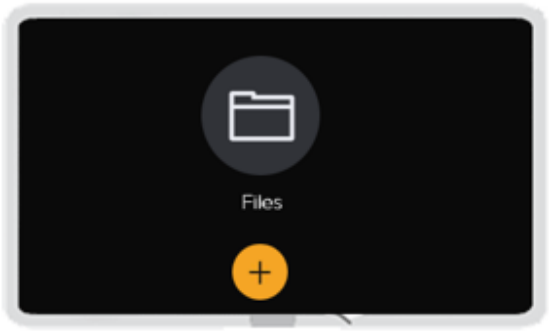
12.5 Tutorial: File Operations

Scenario:
To fetch the file list of an inserted USB Memory stick and open/use a specific file on it. Before a file list can be requested, it is necessary to get information on the mounted drives.

Some files aren't supported by Cynap and we recommend hiding them or at least mark them as unsupported.

User behaviour:
The Cynap user presses the orange Plus-Icon (Source-Button) and selects the files icon. All available sources, including the file source (indicated by “Files” and an icon of a folder), are displayed.

Layout
- Create File list button
- When pressed, show the mounted drives
- Open drive and request the list of files
- Open selected file with the appropriate window type

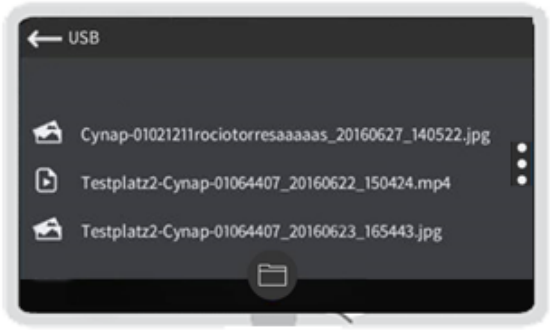


1. Implement File dialogue

Execute command **GET Windows, 08 CB BA 00**

2. Get the list of mounted drives

Execute command
GET Mounts List, 08 CB 3D 00

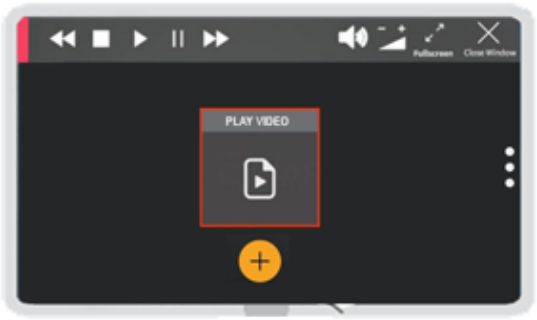


3. Show file list – filter out files of type unknown which can not be displayed on Cynap

Execute command ***GET File List, 0C CB 3E xx***

4. Play the selected file

Execute command
SET Open File,
0D CB 3C xx
Use fully qualified name:
e.g. USB:///video.mp4



5. Set controls based on context of content
Execute command
Get Windows, 08 CB BA 00

WolfProt Commands:

```
// Your layout/implementation done
// Loop: Open socket and poll public GET command
//                            (e.g. polling a get command to receive a PIN,
//                            see PIN Status Room, 08 CB 54 00)
// Loop: Check if AuthorizationLevel is set to RMS_User
//                            (Set Login, 09 CB 42 01)
// All OK? Then send "Window Start, WindowID=auto arranged, WindowType=browser"

While (socketOpen)
  While (RMS_User_logged_in)

    //get and use list of mounted drives
    Send 08 CB 3D 00   //get mounted storage devices
    // process returned JSON array   (e.g. USB:///)

    //fetch event and get list of selected storage device
    // user clicks on USB storage device

    //send mounted device and parent path to show files and directories
    Send 08 CB 3E 00 07 u s b : / / /
    // process returned JSON array  (e.g. video1.mp4)
    // hide files of type unknown or clearly mark them as inaccessible

    //fetch event and open requested file
    // next available window on Cynap will open itself
    Send 0D CB 3C 00 10 u s b : / / / v i d e o . m p 4
```

12.6 Visualizer control through Cynap

Scenario:
Changing the Autofocus from *off* to *on.*

The existence of a Visualizer must be checked and also if the Autofocus setting hasn't been set already.

User behaviour:
User presses autofocus ON

WolfProt Commands:

```
//
// VISUALIZER ZOOM VIA PORT 50916 (INSTEAD OF CB_EVENT WHERE THE REMOTE BUTTONS ARE USED
//
//
// the Visualizer can be controlled without an open Visualizer window on cynap. However it
// is useful if the user needs visual confirmation on Cynap (e.g. zooming in and see reaction
on
// Cynap window.

while (connected and logged in) {
    // Visualizer connected/disconnected?
    send 08 CB 68 00
    if return == 08 CB 68 01 00 // 00 disconnected 01 connected
    {
    feedback: no visualizer connected
    }
    else {
       open socket to Visualizer (Port 50916) // no login necessary, the Visualizer commands
are directly routed over
        while (connected to Visualizer) {
        // First open a Visualizer window on Cynap
        open new window
        // then check if Autofocus is on or off
        send
        if autofocus is off
          (
          send 09 CB 29 02 d0 0
          )
        else
          (
          feedback: autofocus already on
          )
        }
     }
 }
```

12.7 Sample C Code for a Wake on LAN (WoL) Broadcast command

Depending on your network configuration a UDP broadcast might be filtered out, making it impossible to wake up/start Cynap.

Please check our *Network Integration Guide* available on our website for more information about required network configurations.

```
// Prepare Broadcasting
// IP = 255.255.255.255  Broadcast IP
// Port = 0xC6E1 Port 50913 decimal to hex
Cynap.connect (
       (0xffffffff), // 255.255.255.255 in hex
       (0xc6e1)      // Port 50913 in hex

// prepare SendBuffer
Init SendBuffer[1024] //address buffer of size of 1024 bytes
int counter=0  // pointer to be used to add required information at correct
buffer pointer location

// first 6 bytes should be 0xff
for (int c=0;c<6;c++)
       SendBuffer[counter++] = "0xff"

// next add 16 times the CYNAP_MAC_ADRESS
CYNAP_MAC_ADDRESS ="086066ff66ff" // (should look like 08:60:66:FF:66:FF or
086066FF66FF)
for  (int c=0; c<16;c++){
       int d=0
       // convert CYNAP_MAC_ADDRESS into hex-format
       for (int e=0;e<6;e++) //6 bytes of CYNAP_MAC_ADDRESS{
              SendBuffer[counter++] = ConvertToHex
(CYNAP_MAC_ADDRESS.substring(d,2),HexValue)
              d+=2}}

// Send Broadcast to activate MAC addressed device
send status=Cynap.send (SendBuffer,1024)
```

13 Limitations

Cynap's streaming services can cause increased network traffic which might interfere with a Crestron or AMX processor.

It is highly recommended to follow your Room Management System brand's network guide lines in any setup.

Protocol changes do happen, and new commands will be added regularly with every updated release of an updated firmware. We therefore advise to check for obsolete and changed commands in your implementation before you apply a new firmware release.

The data sent to Cynap via WolfProt won't be neither parsed nor validated. Please mind this fact before changing vital settings (e.g. network configuration) when using Administrator Access Level commands.

14 Troubleshooting

14.1 Command issues

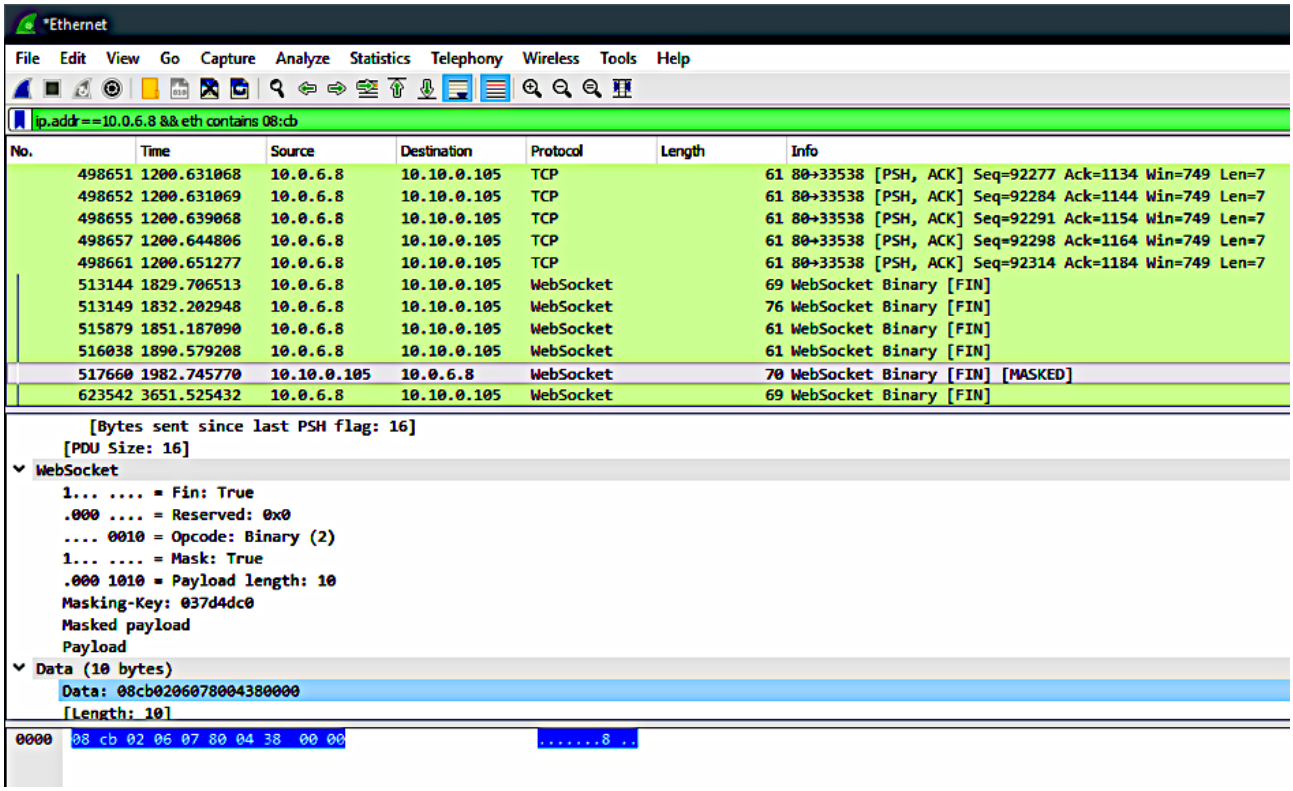
Check that the MAC and IP address as well as all TCP/UDP ports are configured correctly.

Start Wireshark

Using Wireshark to verify your get and set commands

Start collecting the traffic on the interface used for Cynap communication (e.g. Ethernet) – Important: connect to Cynap after the start of traffic collection, otherwise Wireshark won't be able to initiate properly and won't catch traffic on the WebSocket protocol.

Filter the IP address of your Cynap and your command in hex.
For instance: ***ip.addr == 192.168.10.10 && eth contains 08:cb***



Example of *Get Access Token* command, **08 CB 02** (Screenshot: lines marked in blue).

14.2 Authorisation issues

Check that the Room Management System user has been set up with the same corresponding password (on both ends).

Make sure that the command you're sending is being covered by the necessary Access Level of your former login command and is using the same connection.

Try using the *Peripheral Control* in the *settings* of Cynap to issue a simple command.

14.3 Networking issues

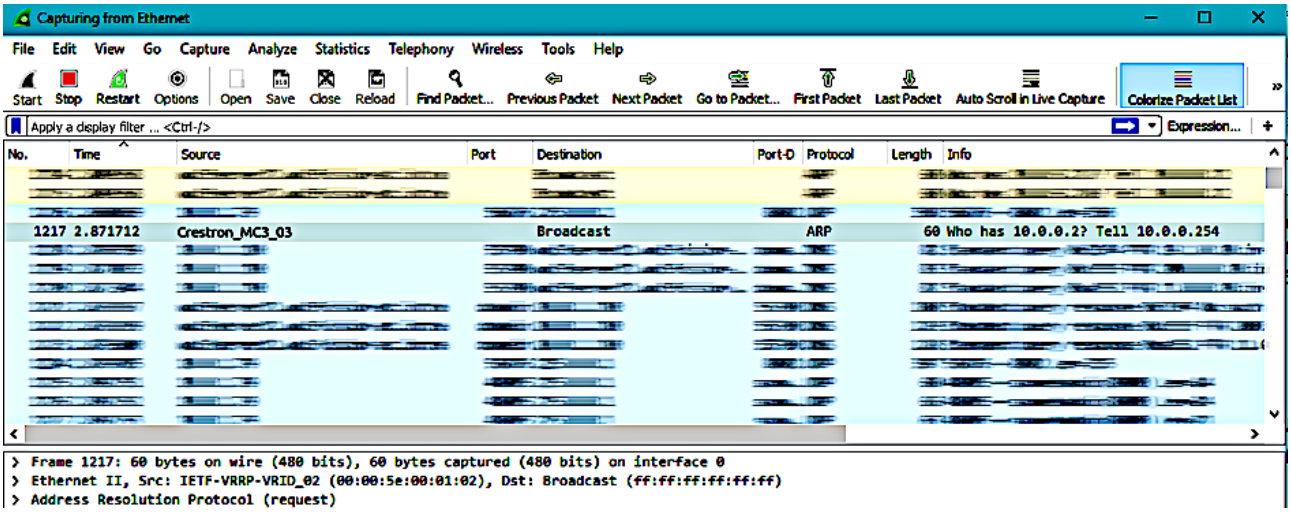
Command line, terminal or shell: ***ping*** the gateway of your network and issue an ***arp –a to*** get a list of IP and MAC address combinations to check if your Cynap's MAC address is found.

14.4 Device issues

Check that the Cynap module is being executed on your RMS processor.
Check that the layout file has been transferred to your touch terminal.

14.5 IP Address of Crestron master lost

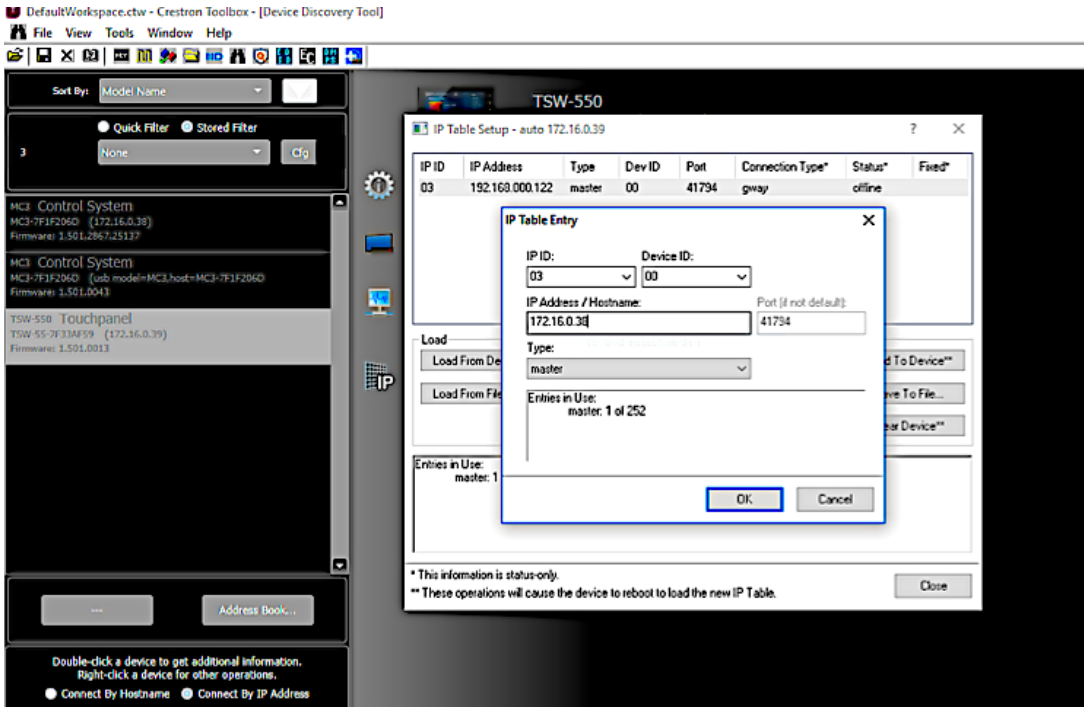
When you lost your static IP address of your connecting devices then connect your laptop to the same network or hook it up directly attached to your PC/laptop and then start Wireshark. Observe the traffic and check the UDP broadcasts to see, which IP addresses are broadcasting (WHO HAS-ARP messages).



14.6 Every Crestron device got its IP and still nothing is happening on Cynap?

Verify if the IP table on your touch panel lists the master console.

Open op the *Crestron toolbox*, enter the *device discovery* and double-click on your touch panel device. There click on the *button IP tables* and enter the corresponding control unit.



15 Changes

Ver 1.0	Initial release	30.8.2016	rg
Ver 1.1	Separating into 2 parts (RMS template integration and coding with WolfProt) Adding latest WolfProt development	16.9.2016	rg
Ver 1.2	Separate two parts into two separate documents – changing structure for template integrators or WolfProt developers	12.11.2016	rg
Ver 1.3	Added APIs by AuthorizationLevel	16.11.2016	rg
Ver 1.4	Added fully fleshed out tutorials	01.12.2016	rg
Ver 1.5	WolfProt commands based on input from AMX dev	12.12.2016	rg
Ver 1.6	Userlevels added, every cmd verified	30.01.2017	rg
Ver 1.7	Updates of 1.11/1.12 added	07.02.2017	rg
Ver 1.7	Dev feedback added	19.02.2017	rg
Ver 1.8	New automated WolfProt command list linked on web replaces former API description New examples on how to use WolfProt commands Notes on Peripheral Control functionality	07.06.2017	rg
Ver 1.9	WebSocket, updates document structure, Extensive examples, New document template	20.03.2018	rg