WolfVision GmbH
Oberes Ried 14
A-6833 Klaus / AUSTRIA

Tel. +43-5523-52250
Fax +43-5523-52249
E-Mail: wolfvision@wolfvision.com
www.wolfvision.com

Driving the Creation
of Knowledge

Network Integration Guide: CYNAP CORE

WolfVision GmbH
Oberes Ried 14
A-6833 Klaus / AUSTRIA
Tel. +43-5523-52250
Fax +43-5523-52249
E-Mail: wolfvision@wolfvision.com
www.wolfvision.com

vSolution Cynap Core
Network Integration

1. Basics

Before starting, check the existing infrastructure and define the required equipment and settings.
Various examples in this document show the different ways in which Cynap Core can be integrated into the network.
When connecting Cynap Core to LAN and WLAN at the same time, please use different IP ranges in order to prevent address conflicts.
The listed IP addresses are only examples.
Cynap Core can be treated as a standard network device and it is as secure as the supporting network. Cynap Core cannot be considered as a router, switch or firewall. Communication to other networks and access must to be controlled using your existing equipment (firewall, router, switch and so on).
By default, Cynap Core´s second LAN port (LAN 2) is dedicated to fully integrate a WolfVision Visualizer. The behaviour of this LAN port (LAN 2) can be changed to connect Cynap Core e.g. to a RMS network (Room Management System) and mirroring purposes. This way, the built-in DHCP server is de-activated and a Visualizer cannot be fully integrated.
When using vSolution Matrix, it is recommended to connect all station of a room to one single network switch to obtain maximum performance.

Attention:
When the second LAN port (LAN 2) is set to Visualizer Mode, never connect this LAN port for the Visualizer to your existing network infrastructure!
If this port is set to Visualizer mode, Cynap Core acts as DHCP-server on this port and this could cause conflicts with the existing infrastructure.
When using vSolution Matrix, LAN 1 has to be used to connect all stations together.

2. Glossary

This glossary will assist you in setting up the network correctly. Please note that in order to connect Cynap Core to an existing company network, some information from the local administrator is required.

2.1. LAN / Ethernet settings

The following settings are available for LAN 1 and also for LAN 2, when the interface mode is changed to LAN.

Priority Interface Access	The higher prioritized interface (value = 1) will be used for network service first. Ensure that the value is different from the WLAN interface priority.
DHCP	Cynap Core will get all network settings automatically from the DHCP server in the existing network. Switch it to OFF to set the static addresses manually.
IP address	Unique address in the network, i.e. 192.168.0.100. The IP address of Cynap Core can for example be set to 192.168.0.1.
Subnet mask	Available IP addresses can be limited. A commonly used subnet mask would be 255.255.255.0
Gateway	Defines the IP address of the server / connection to other networks (such as the internet). When Cynap Core is directly connected only to a PC, then enter the IP address of the PC.
Name server 1 / 2	Input the IP address of the preferred Domain Name System (DNS). This Server translates domain names into corresponding IP addresses.

Identity	Login credentials to connect Cynap Core in a protected network. (802.1x).
Anonymous Identity	The identity to be used on an unencrypted session before Identity is being validated on an encrypted session.
Authentication Method	Supported are PEAP with MSCHAPv2 and TTLS-PAP
Root Certificate	Only root certificates are supported, load the certificate by using the Web Interface through the WLAN interface. Allowed certificates: • root certificate (CA) with common file extension .crt Base-64-coded X.509 encoded DER certificate • Privacy Enhanced Mail with common file extension .perm Base-64-coded X.509 encoded DER certificate certificate stored between 2 tags: “---Begin Certificate---“and” -----End Certificate-----“

2.2. WLAN settings – access point

Mode OFF	Disable access point.
Mode Access Point	Enable access point.
Channel	Defines the channel used for wireless communication. For optimum performance, select a currently unused channel.
SSID Auto	If activated, an automatic SSID is generated using the Cynap Core serial number
SSID Manual	Defines the network name in plain text for easy identification of the WLAN network. Following characters are supported: - AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz - ÄäÖöÜü - 0123456789 - _-:$& ()
IP address	Defines the IP address of the access point. Cynap Core acts as a DHCP server and provides the necessary network settings to the connected devices.
Subnet mask	Available IP addresses can be limited. A commonly used subnet mask would be 255.255.255.0
Encryption	Defines encryption for safe network traffic. All connected devices must use the same algorithm (WPA2).
Transmit Power	Select the desired transmission power to optimize the range. The maximum power depends on selected channel and region.

Hint:
Cynap Core does not act as router or gateway and only serves up a “Cynap Core closed” network that will not connect to the internet even if the LAN port is connected to the internet.

2.3. WLAN settings – infrastructure (Cynap Core acts as client)

Mode Infrastructure	Enable Infrastructure, Cynap Core can be connected ac client to an existing access point.
Band	By default, Cynap Core uses the 2.4GHz and 5 GHz frequency band. The used frequency band can be limited to either 2.4GHz or 5 GHz. This setting is available in SSID mode only.
Priority Interface Access	The higher prioritized interface (value = 1) will be used for network service first. Ensure that the value is different from the LAN interface priority.
BSSID On / Off	Toggles between SSID and BSSID mode. With BSSID (Basic Service Set Identification), the used access point will be fixed and Cynap Core will connect to the defined access point only. Access point hopping, which is available in SSID mode (Service Set Identification), will be prevented.
SSID	Defines the network name in plain text for easy identification of the WLAN network. Check existing WLAN infrastructure to get SSID. Following characters are supported: - AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz - ÄäÖöÜü - 0123456789 - _-:$& ()
BSSID	Defines the network name in plain text for easy identification of the WLAN network. Check existing WLAN infrastructure to get SSID. This setting is available in SSID mode only.
Subnet mask	Available IP addresses can be limited. A commonly used subnet mask would be 255.255.255.0
Gateway IP	Defines the IP address of the server / connection to other networks (such as the internet). When Cynap Core is directly connected only to a PC, then enter the IP address of the PC.
Name server 1 / 2	Input the IP address of the preferred Domain Name System (DNS). This Server translates domain names into corresponding IP addresses.
Encryption	Defines encryption for safe network traffic. All connected units must use the same algorithm (None, WEP, WPA2, WPA2 Enterprise).
Identity	Login credentials to connect Cynap Core in a WPA Enterprise protected network.
Anonymous Identity	The identity to be used on an unencrypted session before Identity is being validated on an encrypted session.
Authentication Method	Supported are PEAP with MSCHAPv2 and TTLS-PAP
Root Certificate	Only root certificates are supported, load the certificate by using the Web Interface through the LAN interface. Allowed certificates: • root certificate (CA) with common file extension .crt Base-64-coded X.509 encoded DER certificate • Privacy Enhanced Mail with common file extension .perm Base-64-coded X.509 encoded DER certificate certificate stored between 2 tags: “---Begin Certificate---“and” ---

	---End Certificate-----“
Signal Level Limit (dBm)	Defines when Cynap Core start to search for another access point with the same SSID in your infrastructure (WLAN roaming). Monitoring the current signal level to prevent too low values. Lookups could interrupt the network connection shortly and every lookup will be counted (Reconnect Counter (Low Signal Level).
Signal Level	Shows the current strength of the WLAN signal in dBm.
Reconnect Counter (Connection Loss)	Counts every connection loss, e.g. when the selected access point would be powered down.
Reconnect Counter (Low Signal Level)	Counts every lookup then the measured signal falls below the user defined signal level limit.

2.4. Date and time

Time source	Cynap Core has a built-in battery-buffered RTC clock (Real Time Clock). Settings will only be lost if the battery is empty. To eliminate the risk of incorrect time stamps, Cynap Core can be synchronized to an external time server. Select external and input a valid IP address or URL of a NTP time server.

2.5. Host name

Host name	The Host name can be changed in the settings under general settings. The host name can be useful for network administrators to see the device name in plain text in the list of clients. Please note, this host name is not automatically listed in the DNS list, and therefore cannot be used in a browser without DNS registration.

2.6. LAN / WLAN port

The LAN port enables integration of Cynap Core into an internal network. Administrators of a large number of Cynap Core systems can use the LAN port to control, support and update all of their units from their local desktop PC.

The list of applications for the Cynap Core LAN port is constantly increasing. It can be used for controlling, capturing still images, viewing live video streams, firmware updates, adjustments, menu settings and for maintenance purposes. Some features are only supported when using vSolution Link software.

The following protocols are supported: TCP/IP, IGMP, RTP, RTSP, UDP and ARP.
Supported (tested) internet browsers are: Microsoft Edge, Firefox, Chrome, and Safari.
By default, DHCP is activated to receive all network settings automatically from the server.

Hint - WLAN:
To ensure optimal performance of supplied remote control (optional), prevent channel 13 in the band of 2.4 GHz. Switch Cynap Core to standby closes all connections.

2.7. FTP Client settings

FTP enable	Enable or disable FTP client functionality to backup and share recorded videos and snapshots. Additional features such as active/passive mode or secure layers (eg. Kerberos etc.) are not supported.
URL	Address of your FTP server in your network, like 192.168.0.100. (up to 256 characters, no space between the characters)
Username	Input the username according your FTP server settings.
Password	Input the password according your FTP server settings.
Test it now	During the test, Cynap Core will upload a text file onto the FTP-server (“Cynap Core.txt” without content)

2.8. Proxy settings

To increase security level, use a proxy server to control HTTP and HTTPS traffic from Cynap Core. Built-in access point and other local services are not controlled. To take effect the new settings, Cynap Core will reboot automatically.

Proxy enable	Enable / disable proxy service When enable, all HTTP and HTTPS traffic will be routed to the your proxy server. Please note, using a Proxy server may block Skype for Business (optional) functionality.
URL	URL of the proxy server in your network, like 104.236.10.17 (or DNS name up to 256 characters, no space between the characters). DNS server not required, when using IP addresses.
Host Port	Port, set the used network port to connect to your proxy server.
Authentication	Disable / enable Authentication When enabled, valid user name and password has to be entered.
Username	Username, given by your server.
Password	Password, given by your server.

2.9. Security

Admin password
Defines the necessary password for administrator access. This login data is needed to change the Ethernet Mode, and an existing administrator password. Using the login data, an administrator can connect to Cynap Core at any time. The default password is “Password”. Remember to make a note of any changed passwords!

Login Security
Accessing Cynap Core can be protected by authentication (admin, moderator or PIN).
To prevent unauthorized access of the settings, the admin password needs to be entered once per session.

Network Security
Accessing Cynap Core can be limited to secure connections only (https). Please note, the accessing application needs to support SSL / TLS (e.g. the most modern browsers are supporting HTML5 and SSL /TLS).
Wolfvision support access can be prohibited by disabling SSH.

LAN Security
When using wired network, use authentication (according 802.1x) to maximize security.
When using certificates, load it busy using the Web Interface.

WLAN (WiFi) Security
When using wireless network, use encryption to maximize security.
Cynap Core complies with following standards:

- WEP
- WPA2
- WPA2 Enterprise (according 802.1x)

Hint
WEP allows password with a length of 13 characters.
WPA2 allows password with a length of 8 ~ 63 characters.
Use special characters carefully, not every third party device can handle it.
When using WPA2 Enterprise, load the certificate by using the Web Interface.

3. Network integration (examples)

The following examples of network integration show the different ways in which Cynap Core can be integrated. Various operating systems can each connect to Cynap Core to transfer different information from different sources onto a large monitor.

3.1. Stand-alone access point mode (without network integration)

Cynap Core is operated in stand-alone access point mode.
The network settings must be set manually on Cynap Core (no DHCP server is available).
Cynap Core generates an independent WLAN, and WLAN enabled devices (BYOD) can connect to Cynap Core.

Advantages:

- No complex network infrastructure necessary
- Cynap Core generates its own stand-alone access point
- No connection to internal IT infrastructure
- Security issues - no other unit from the internal IT infrastructure can access Cynap Core

Disadvantages:

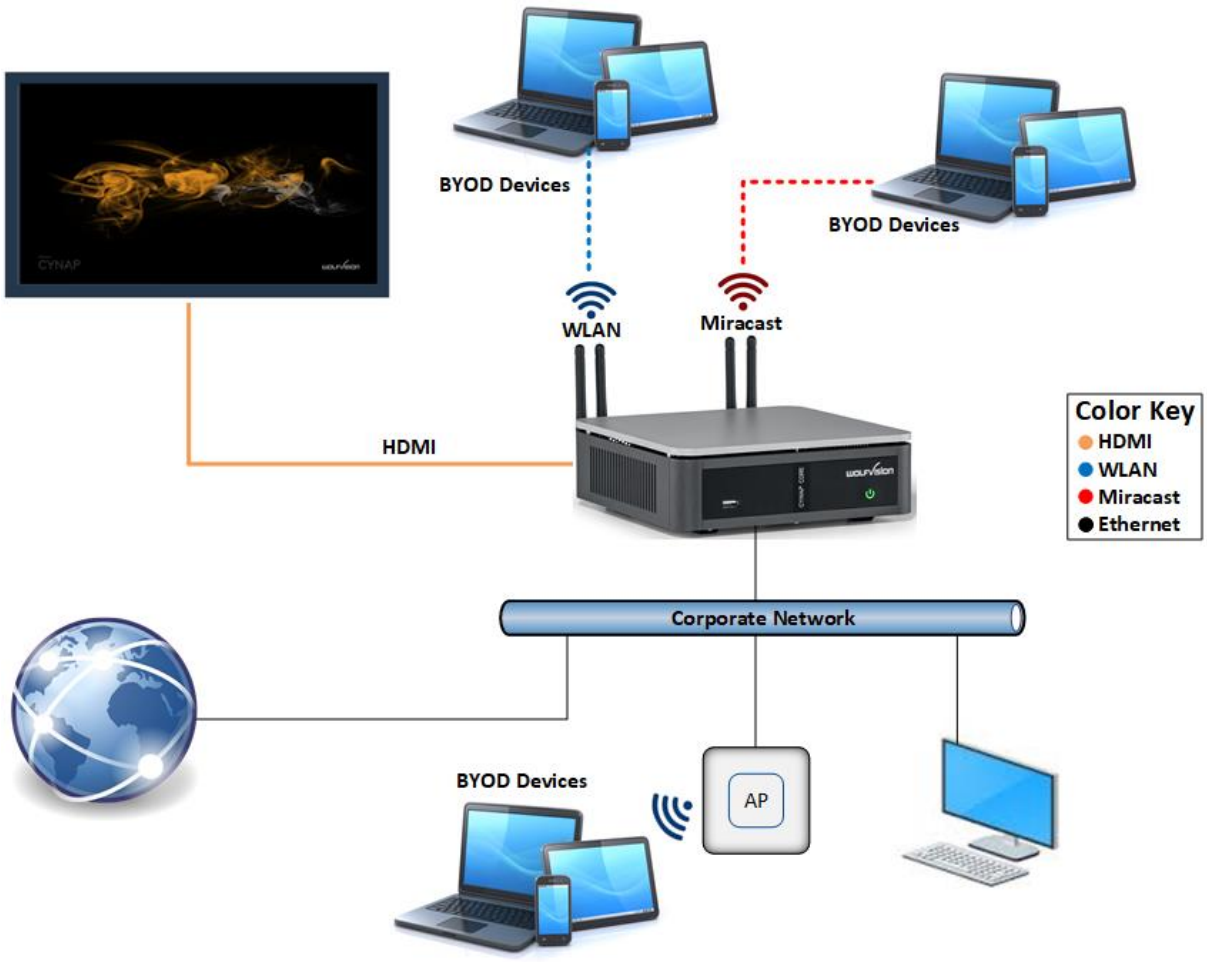
- No devices have internet access
- Cloud services cannot be used

Required settings:

DHCP	Switch to OFF to enable manual setting of addresses
IP Address	Unique address in the network, like 192.168.0.100. The IP address of a connected PC could be set to 192.168.0.1 for maintenance purposes
Subnet Mask	Available IP addresses can be limited. A commonly used subnet mask would be 255.255.255.0
Gateway	Enter the IP address of a directly connected PC for maintenance purposes
Name server	Not needed

3.2. Cynap Core wireless network access point mode

Cynap Core is integrated via a cable connection into an existing network, and is operated in wireless network access point mode. LAN settings for Cynap Core can be provided by the DHCP server. Cynap Core generates an independent WLAN, and WLAN enabled devices (BYOD) can connect to Cynap Core.



Advantages:

- All devices can communicate with each other
- Cynap Core has access to the Internet and cloud services can be activated
- Cynap Core can access the internet to check for firmware updates without using additional devices

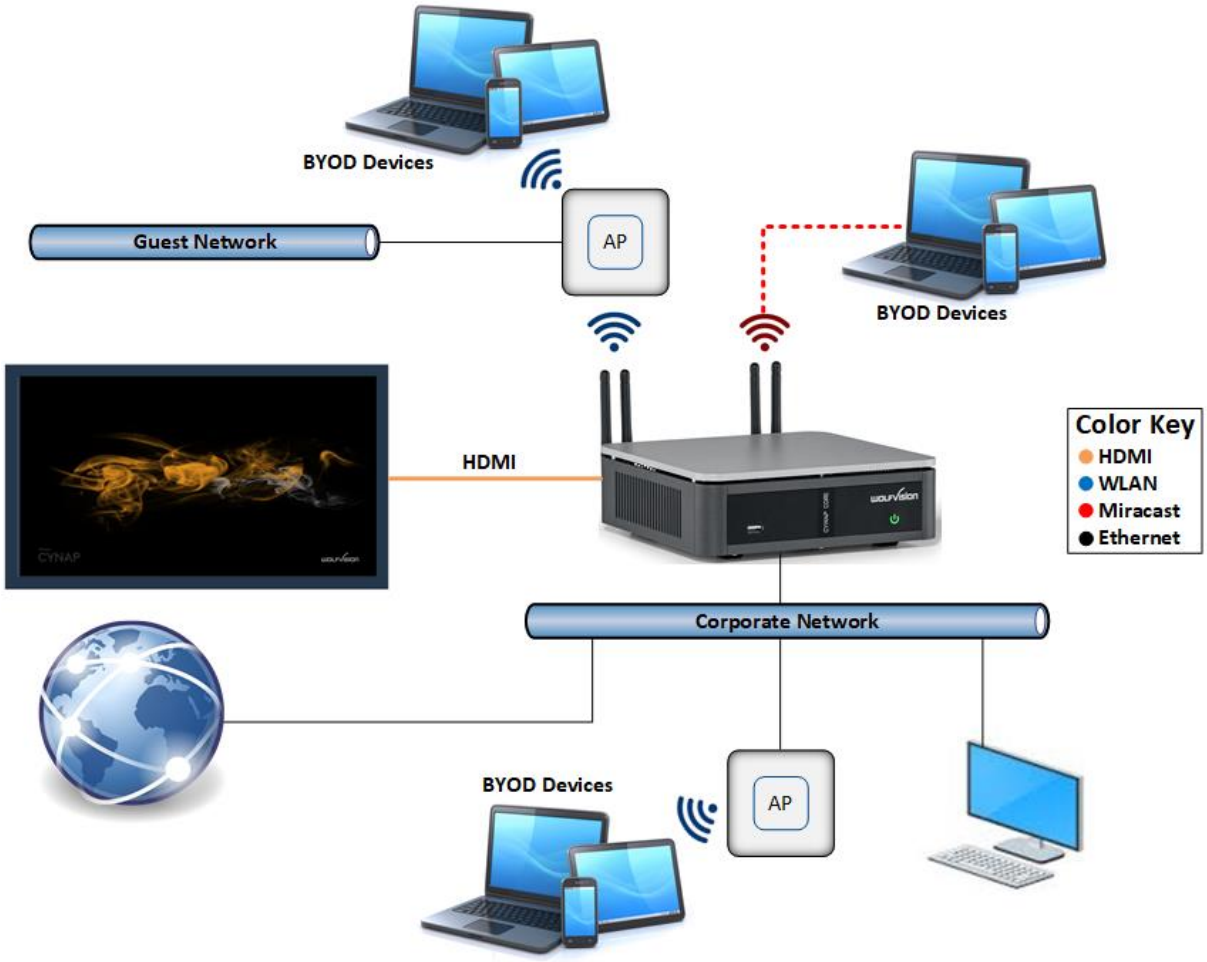
Disadvantages:

- Performance issues (all traffic is on the same network)

Hint:
If the units are in different subnets, Cynap Core might not be able to be discovered automatically by vSolution applications.

3.3. Cynap Core network infrastructure mode

Cynap Core is integrated via a cable connection into an existing network (e.g. Corporate network), and is operated in network infrastructure mode. LAN settings for Cynap Core can be provided by the DHCP server. In infrastructure mode, Cynap Core is connected to an existing wireless access point in the existing network (e.g. Guest network). BYOD devices in the Corporate network and in the Guest network can connect to Cynap Core.



Advantages:

- All devices can communicate with each other
- Cynap Core has access to the internet and cloud services can be activated
- Cynap Core can be moved within the range of the access point
- Cynap Core can access the internet to check for firmware updates without using additional devices

Disadvantage:

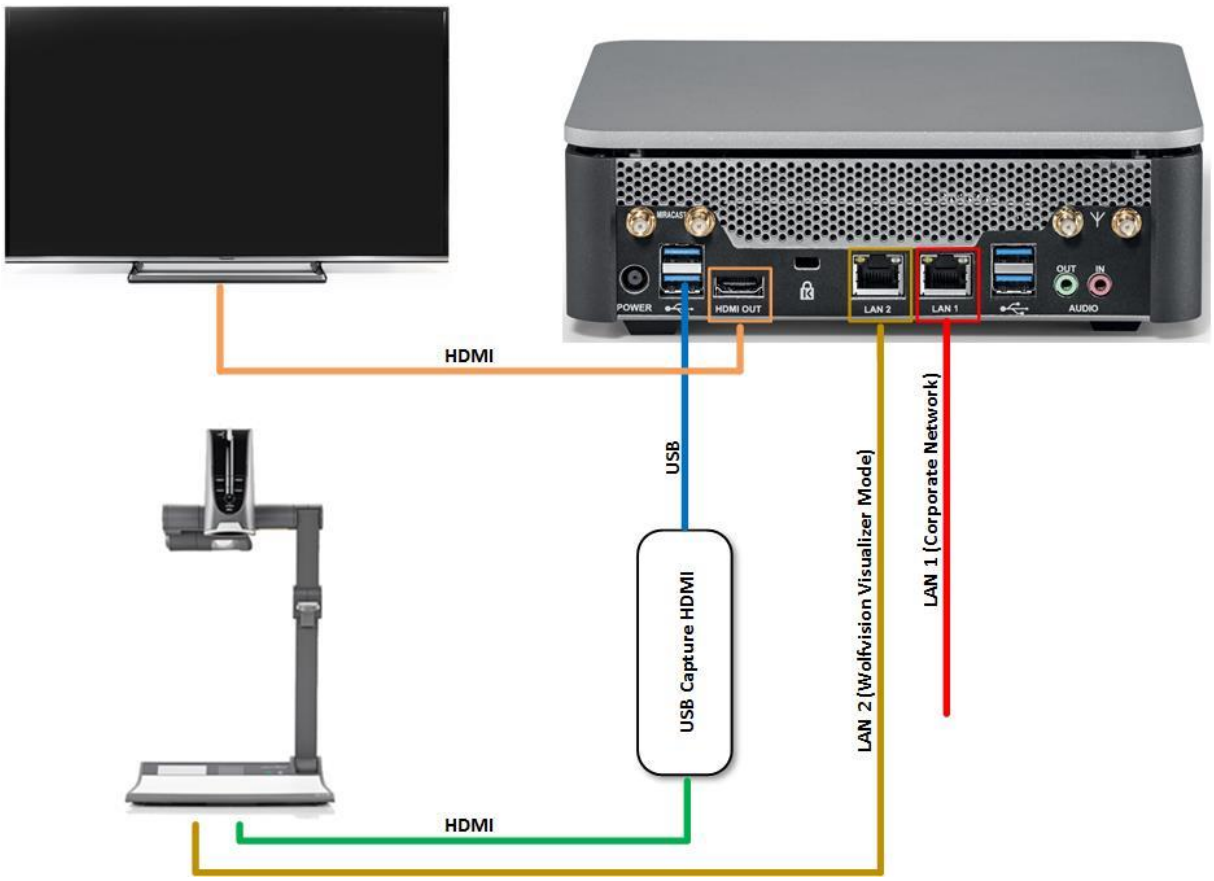
- Performance issues (all traffic is on the same network)

Hint:

If the units are in different subnets, Cynap Core might not be able to be discovered automatically by vSolution applications.
Cynap Core can also be installed in a VLAN.

3.4. Cynap Core connection to a Visualizer

Cynap Core has a dedicated LAN port for connecting to a Visualizer with built-in DHCP server functionality. Activate on the Visualizer to obtain all necessary network settings from Cynap Core automatically. Communication between Visualizer and Cynap Core is over the Wolfprot protocol. The connection between Cynap Core and the Visualizer is a direct connection (point to point) and shouldn't be made through a switch or similar device. More information on this protocol can be found on our website in the support section www.wolfvision.com.



Attention:
When the second LAN port is set to Visualizer Mode, never connect this LAN port for the Visualizer to your existing network infrastructure!
If this port is set to Visualizer mode, Cynap Core acts as DHCP-server on this port and this could cause conflicts with the existing infrastructure.

Hint:

- Connect the Visualizer straight to the dedicated port. Do not add switchers, hubs, routers or similar between Cynap Core and the Visualizer to prevent error sources.
- Cynap Core can be controlled with the keys of the Visualizer. The functions of keys from the camera head are dedicated to control Cynap Core. These keys are note have no effect to the Visualizer anymore. The IR-remote control of the Visualizer is not effective in this setup.
- Visualizer can be controlled with Cynap Core.
- Cynap Core and Wolfvision Visualizer are supporting cable runs up to 100m according Ethernet specification.
- The behaviour of this LAN port can be changed to connect Cynap Core to a dedicated RMS network (Room Management System). This way the built-in DHCP-server is de-activated and a Visualizer cannot be fully integrated.
- Be sure USB input type is not defined as “Visualizer”

4. Firewall rules

Cynap Core has firewall rules that must be adhered to in order to allow successful network communications, and the corresponding services to be used. To use services with user defined addresses and ports, be sure these are not blocked by your firewall.

Function / Application	Port	Type	Inbound / Outbound	Description
Airplay				
Multicast DNS (mDNS)	5353	UDP	Inbound / Outbound	Multicast DNS (mDNS 224.0.0.251) Bonjour
Audio	4100	TCP / UDP	Inbound	Audio for Airplay
Airplay	7000	TCP	Inbound	Primary Airplay communication
Video	7100	TCP	Inbound	Airplay video communication
Audio	47000	TCP	Inbound	Airplay audio communication
Airplay Bluetooth for Device Discovery				
Audio	4100	TCP / UDP	Inbound	Audio for Airplay
Airplay	7000	TCP	Inbound	Primary Airplay communication
Video	7100	TCP	Inbound	Airplay video communication
Audio	47000	TCP	Inbound	Airplay audio communication
Chromecast				
Multicast DNS (mDNS)	5353	UDP	Inbound / Outbound	Multicast DNS (mDNS 224.0.0.251)
Discovery	1900	UDP	Inbound	Chromecast discovery
Audio	4100 – 4164	TCP / UDP	Inbound	Audio for Chromecast
Chromecast	8008	TCP	Inbound	Primary Chromecast communication
Chromecast	8009	TCP	Inbound	Communication Chromecast
Video data stream	32768 – 61000	UDP	Inbound /Outbound	Chromecast (video data stream)
Miracast MS-MICE				
Multicast DNS (mDNS)	5353	UDP	Inbound	Multicast DNS (mDNS 224.0.0.251)
DHCP	67 / 68	UDP	Inbound	DHCP communication between device and receiver
RTP Stream	19000 – 19007 19010 – 19017	UDP	Inbound	RTP media traffic port for delivering audio and video
RTSP Control	7236	TCP	Outbound	RTSP control port is used to establish and manage session
MS-MICE Control	7250	TCP	Inbound	Control port on which Cynap family system listen for Miracast packets when over existing network mode is enabled
Touchback	50000	TCP	Outbound	This port is for touchback to send mouse events back between Cynap to the Windows computer. If this port is blocked, bi-directional inputs is not possible.
Hardware cursor extension	19020 – 19027 19030 – 19037	UDP	Inbound	Hardware cursor to reduce latency when using touchback.
Wake On LAN	7 / 9	UDP	Inbound / Outbound	Usually port 7 is used for sending the magic packet

FTP	21	TCP	Outbound	Connection to FTP server
SSH	22	TCP	Inbound	Access for Wolfvision support
http, Cynap control	80	TCP	Inbound	This port used to connect to Cynap web interface (httpd). If this port is blocked, no connection can be made.
https, SSL, e.g. Cloud Service, Cynap control	443	TCP / UDP	Inbound	This port is used to cloud service and for secure connect to Cynap web for secure connect to Cynap web interface. If this port is blocked, no connection can be made.
Proxy	8080	TCP / UDP	Outbound	Default port proxy function (This port can be changed in the Proxy settings).
NFS	111 / 2049	TCP / UDP	Outbound	Connection to network drives
CIFS	137 / 139	TCP / UDP	Outbound	Connection to network drives
NTP	123	UDP	Outbound	For optional clock synchronization by a time server (Network Time Protocol, NTP)
LDAP	389	TCP / UDP	Outbound	Connection to LDAP server
LDAPS	636	TCP / UDP	Outbound	Connection to LDAPS server (TLS)
Streaming Multicast / Unicast	8800 – 9000	UDP	Inbound	Used for Multicast / Unicast / Audio / Video Streaming
Streaming RTSP	554	TCP	Inbound	This is the communication port for the RTSP stream. This used UDP port will be handled automatically
PJLink	4352	TCP	Outbound	This is the default port for PJLink and cab be changed in the settings (Peripheral Control)
vSolution Cast				
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, vSolution applications may not be able to find devices automatically.
Device Discovery	50913	UDP	Inbound	This port is used for device discovery
For control purposes	50915	TCP	Inbound	This port is used for control purposes e.g. room control system, and others). If this port is blocked, no control is possible
TLS Control	50917	TCP	Inbound	This port is for secure communication between WolfVision applications (e.g. vSolution App) to Cynap and / or Visualizer. If this port is blocked, secure communication to Cynap and / or Visualizer, inclusive firmware updates are blocked.
Video streams	50921	TCP	Inbound	Video streams between Wolfvision App to Cynap and Visualizer. If this port is blocked, no stream are possible.

Touchback	50922	TCP	Outbound	This port is for touchback between Cynap and Wolfvision App vSolution Cast to send mouse events back to the Windows computer. If this port is blocked, bi-directional inputs is not possible
vSolution App iOS / Android / Windows				
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, vSolution applications may not be able to find devices automatically.
http, Cynap control	80	TCP	Inbound	This port is used to connect to the Cynap web interface (httpd). If this port is blocked, no connection can be made.
https, SSL, e.g. Cloud Service, Cynap control	443	TCP	Inbound	This port is used to cloud services and for secure connect to the Cynap web for secure connect to the Cynap web interface. If this port is blocked, no connection can be made.
Device Discovery	50913	UDP	Inbound	This port is used for device discovery.
For control purposes	50915	UDP	Inbound	This port is used for device discovery.
TLS Control	50917	TCP	Inbound	This port is for secure communication between WolfVision applications (e.g. vSolution App) to Cynap and / or Visualizer. If this port is blocked, secure communication to Cynap and / or Visualizer, inclusive firmware updates are blocked
WebRTC	10000 – 16000 50000 - 65000	TCP / UDP	Outbound	Communication Port
WebRTC (Pexip)	1720	TCP	Outbound	This port used WebRTC services like Pexip
TLS Control	50917	TCP	Inbound	This port is for secure communication between Wolfvision application (e.g. vSoltuion Link) t Cynap and / or Visualizer. If this port is blocked, secure communication to Cynap and / or Visualizer, inclusive firmware updates are blocked.
WebSocket	7681	TCP	Inbound	User interface communication with Cynap (via browser)
WebSocket	7682	TCP	Inbound	User interface communication with Cynap (via fully integrated Visualizer)

vSolution Link Pro				
Wake On LAN	7 / 9	UDP	Inbound / Outbound	Wake On LAN – Usually port 7 is used for sending the magic packet
DNS	53	TCP / UDP	Inbound / Outbound	DNS – This port will be used for Domain Name System. If this port is blocked, DNS service are not available
http, Cynap control	80	TCP	Inbound	This is the default port to connect to the web interface (httpd) of vSolution Link Pro. Of this port is blocked, connection cannot be established
https, SSL, e.g. Cloud Service, Cynap control	443	TCP	Inbound	This is the default port to connect to web interface (https) of vSolution Link Pro. If this port is blocked, connection cannot be established.
SMTP	587	SMTP	Outbound	Mail Server – Port for communication with SMTP server.
Discovery Multicast	50000	UDP	Inbound	This port is used for device discovery all available Cynap and Visualizer in the network by vSolution applications (uses Multicast IP address 239.255.255.250). If this port is blocked, device discovery is not possible
Device Discovery	50913	UDP	Inbound	This port is used for device discovery. If this port is blocked, device discovery is not possible.
For control purposes	50915	TCP	Inbound	This port is used for control purposes. If this port is blocked, no control is possible
Zoom				
http	80	TCP	Outbound	For Zoom clients and meeting connector
http over TLS / SSL	443	TCP	Outbound	For Zoom clients
	8801	TCP	Outbound	For Zoom clients
	8802	TCP	Outbound	For Zoom clients
	3478	UDP	Outbound	For Zoom clients
	3479	UDP	Outbound	For Zoom clients
	8801 – 8810	UDP	Outbound	For Zoom clients

5. Differences in Open Mode / Protected Mode

When using Cynap Core, it is possible to choose between either open mode or protected mode.
This different mode can be selected using Cynap Core settings.

Modes:

Open Mode
The open is intended for quick and easy connections and BYOD without the need of high security and big effort for administration.
When Open Mode is active, all available devices can connect to Cynap Core.
In the Open Mode, Airplay PIN can be used to prevent disturbance of extern Apple devices.
The PIN will be shown on the connected display only HDMI.

Protected Mode
Is a password protected mode to prevent misuse and disturbances

- Users with knowledge of the password can connect to Cynap Core
- Users who knowing the security PIN, the PIN will be displayed on the selected interface(s)
- Users can connect when Cynap Core is awaiting a mirror connection

For more information, please refer to the manual.

6. BYOD

Cynap Core is designed to make it as easy as possible for users to connect to it. Cynap Core supports integrated mirroring protocols in its operating system. Users can connect to Cynap Core without needing any additional software. The mobile platforms are AirPlay for iOS devices and Miracast for Android and Windows devices. Regarding laptop and computer operating systems, AirPlay is also supported for Mac OS X. Windows Intel Wireless Display is also supported, and this integrates natively with Windows 8.1.

AirPlay	Support for iOS 5.0 (released 2011) and above, or OS X 10.8 Mountain Lion (released 2012) and above. AirPlay is transmitted via Ethernet / WLAN. It can be used for displaying up to four sources.
vSolution Cast for iOS (App)	For use in network environments where the Bonjour service (device discovery protocol) has been disabled.
Miracast	Miracast is based on a Wi-Fi direct connection. This means that Miracast can only be used in close proximity to Cynap Core. Due to the direct communication with a device, only one connection to Cynap Core is possible at the same time (HDCP will be not supported). When using Microsoft Windows PCs or tablets, the use of vSolution Cast is recommended.
vSolution Cast (Windows)	In applications where a Wi-Fi direct connection is not possible due to the installation, multiple Windows devices can be connected at the same time using the alternative vSolution Cast.
vSolution Connect	vSolution Connect is a professional presentation tool which offers an alternative to mirroring for Android and iOS. Mirroring has some disadvantages, and can, for example, allow incoming messages or calendar pop-ups to be visible on-screen to all participants during a presentation.
Chromecast Screen Mirroring	Support for Chromecast capable devices. Chromecast is transmitted via Ethernet / WLAN. It can be used for displaying up to four sources.

AirPlay, Chromecast, Miracast and vSolution Cast are based on device discovery technologies for maximum ease of use. Therefore it is necessary that the appropriate services (See Firewall rules) are available. Alternatively, when using vSolution Cast, a Cynap Core IP address can be entered manually. On Windows systems, vSolution Cast can either be run temporarily by users, or permanently installed (copied). The application can also be used from a USB stick without needing administrator rights, however with the restriction that no sound is transmitted.
Switching Cynap Core to standby closes all connections.

7. Document and media player

Cynap Core can present almost all commonly used document and video file formats. This functionality is built in to Cynap Core and no additional applications need to be installed.

Cynap Core also supports different storage media for presentation of documents and video.

The following storage media are available for Cynap Core.

- Internal storage
- USB flash drive
- Network Drive
- Cloud services

The following media formats are supported:

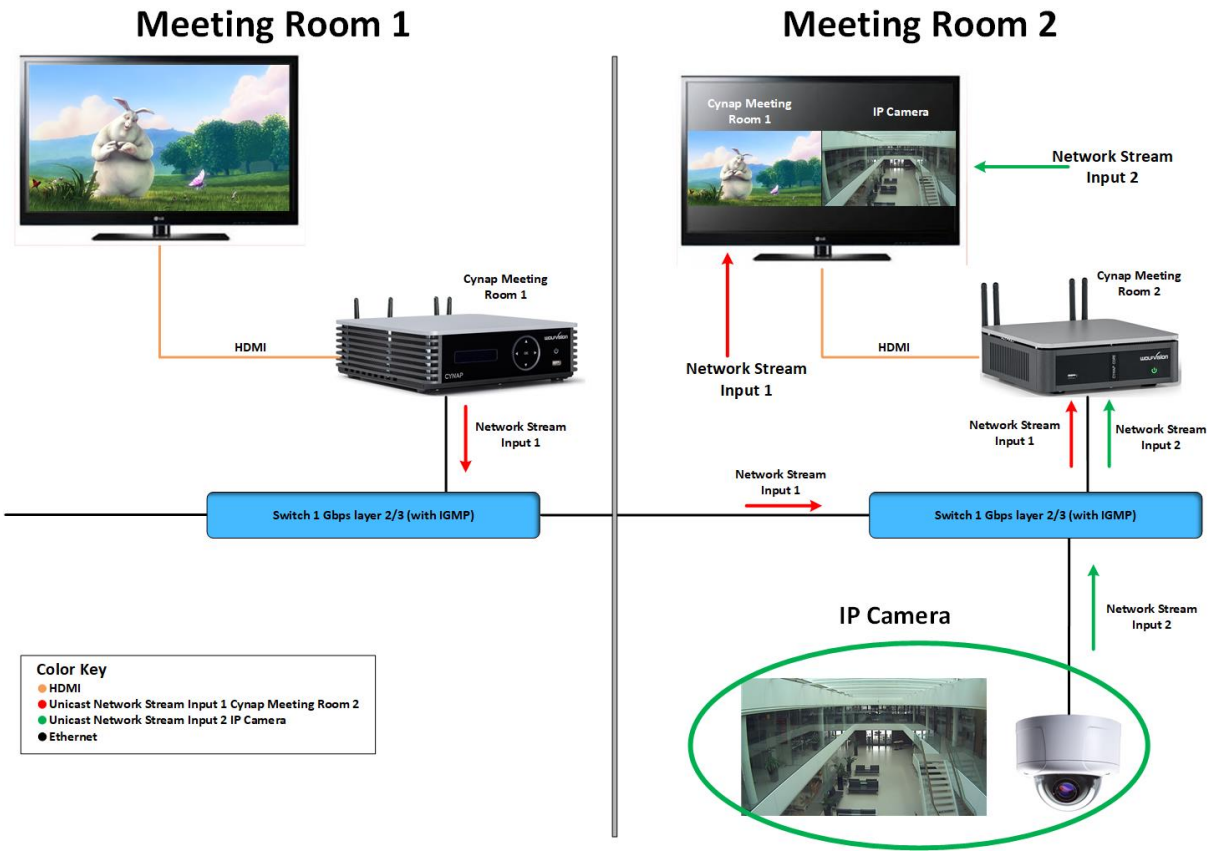
- Supported pictures file formats: GIF, JPEG, BMP,PNG
- Supported video file formats: AVI, WMV, MOV, MP4, DivX, MKV, M4V, OGV
- Supported document file formats: PDF, Word, PowerPoint, Excel
- Supported audio file formats: MP3, MKA, OGA, OGG, WMA

8. Network Stream (input)

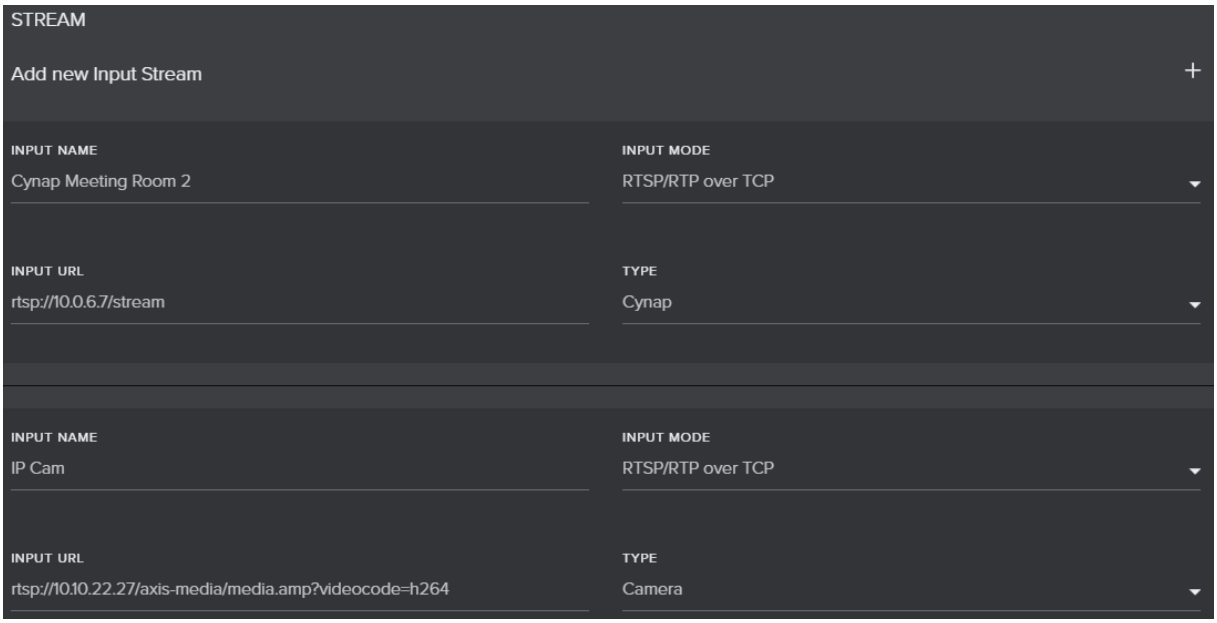
Cynap Core has a built-in streaming client which is capable of receiving broadcast video content over the network.
Up to four Stream sources can be defined and individually named in the GUI settings (Input).

Add new Input Stream	Allows adding up to four network streams selectable as source (click the + symbol).
Input name	Gives the source an individual name for easy identification
Input mode	Defines the kind of stream. • None, disables receiving this stream • Generic allows streams using UDP and TCP protocol • RTSP / RTP over TCP allows TCP protocol only
Input URL	Record Stream Input URL defines the source of the stream

Example:
Network stream input with two devices, one from Meeting Room 1 Cynap to Meeting Room 2 Cynap Core and one IP Camera.



At the Cynap Core Meeting Room 2 are two network stream input configured with the following settings.



After saving configuration the new two sources (IP Camera, Cynap Core Meeting Room 1) are available.
At the Cynap Meeting Room 1 the RTSP Stream is enabled and Streaming must be started. Then choose the sources IP Camera and Cynap Core Meeting Room 2 and then contents will be displayed Cynap Core Meeting Room 2.

9. Control of Peripheral Devices

Cynap Core is able to send up to 10 commands to connected network devices, e.g. to fully power up the connected projector. This feature will be triggered by power events of Cynap Core.
The peripheral devices, like projectors, monitor, lightings, windows shades, etc. need to be in the same network as Cynap Core.

Command enable	Enable / disable certain commands (entered command settings will be not deleted
Name	To give the command an individual name (like “projector”)
Description	To give the command a detailed description (like “power up”)
Event	To define at which power state of Cynap Core the command will be sent (Power ON or Power OFF). Select event None to delete this entry.
Protocol	Defines the used network protocol (TCP,UDP or PJLink)
IP address	Defines the destination, enter the address of the third party device
Port	Defines at which network port the command will be sent (note documentation of the third party device and firewall settings)
Hex Command	Enter the command according documentation of the third party device.
Password	Available when protocol PJLink is selected

10. Cloud services

Cynap Core supports Google Drive ,Dropbox, Box, Jianguoyun, OneDrive and WebDAV cloud services. These services can be enabled or disabled in the settings. For specific firewall settings, check the individual service provider.

11. Network Drive

Cynap Core allows direct access to network drives (writeable or read-only). A default drive can be specified to simplify the upload functionality of a recording or snapshot.

Up to 10 network drives can be configured in the network drive settings.

CIFS and NFSv3 file systems are supported.

12. User interface

Cynap Core can be controlled using any current standard browser. The user interface has been developed using the latest web programming standards, and this means that there is no need for additional add-ons or plugins such the Java Platform, in order to have full control of Cynap Core. HTML5 technology only requires a browser that can handle JavaScript and Websockets, and this has been state-of-the-art for the last few years.
You can also adjust the settings using the remote control (optional). The remote control uses the 2.4 GHz band. The remote control has a built-in gyro sensor and can be used as a digital laser pointer.
Cynap Core can also be used in combination with room management systems. Communication is possible via the Wolfprot protocol. More information about this protocol can be found in the support section of our website www.wolfvision.com .
The vSolution Control app allows smartphones / tablets (iOS, Windows, Android) to control Cynap Core directly via WLAN. More information about the vSolution Control App can be found on in the support section of our website www.wolfvision.com .

13. Hardware and OS

Cynap Core uses a Linux operating system. The distribution is a WolfVision specific variant, which in addition to the Linux kernel contains only the individual libraries and packages required for the functionality of Cynap Core. This operating system is efficient, secure and lean. The operating system is installed after the installation process, and every update is installed to a read-only partition that cannot be changed after the installation process. This feature and the strict separation of system and user data, such as pictures, videos etc. ensures a very high level of system security. The system structure is protected against any external access, and it does not require additional security programs (antivirus, firewall, etc.). The Cynap Core system includes all viewer and software packages, and no additional licenses are required.

The current hardware specifications, connectors, delivery, and technical specifications can be found on our website www.wolfvision.com.

A 19” rack mount is available as an optional accessory if required for installing Cynap Core (2HE).

14. Administration

Cynap Core can be managed using the vSolution Link software.
With vSolution Link software, administration tasks can be performed for multiple Cynap Core systems. With this admin tool, you can perform central firmware upgrades as well as determining the state of Cynap Core and Wake-on-LAN (WoL). You can also create, manage, and distribute a settings profile to all Cynap Core systems using vSolution Link software.

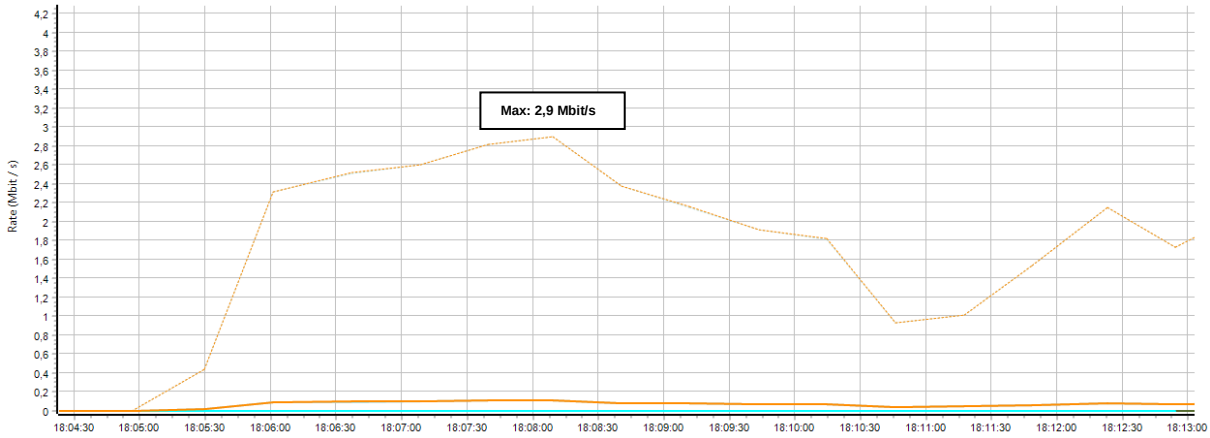
More information about vSolution Link software can be found in the support section of our website www.wolfvision.com.

15. Bandwidth Measurement Data

This bandwidth measurement data has been taken using a notebook PC with a Windows operating system. The computer was connected to Cynap Core via WLAN, and was operating in network infrastructure mode.

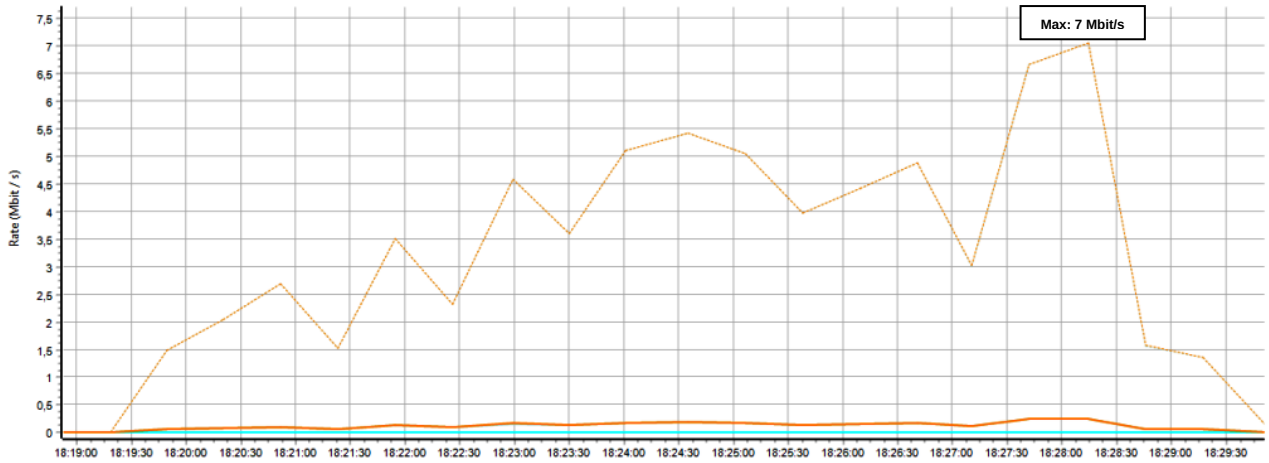
15.1. PowerPoint Presentation

Presentation with text and a few graphics are displayed from the notebook and are mirrored to Cynap Core using vSolution Cast Software to a single connected client. (Traffic Out)



15.2. Multimedia from Notebook to Cynap Core using vCast Software

1080p video (Big Buck Bunny) is displayed on the notebook and is mirrored using the vSolution Cast Software to a single connected client. (Traffic Out)



16. Client System Requirements

Requirement Airplay Mirroring OS X Mountain Lion v10.8 (Release 2012) or later:

Product	Version
iMac	Mid 2011 or later
Mac mini	Mid 2011 or later
MacBook Air	Mid 2011 or later
MacBook Pro	Early 2011 or later
Mac Pro	Late 2013 or later

Requirement Airplay Mirroring iOS 5.0 (Release 2011) or later:

Product	Version
iPhone	4 or later
iPad	2 or later
iPad	mini or later
iPod touch	5th generation or later

Requirement Miracast:

Product	Version
Android	4.4.2 or later
Microsoft Windows	8.1, 10 Hardware with Miracast support required
Windows Phone	8.1, 10
Blackberry	10.2.1 or later

Requirement Chromecast:

Product	Version
Android	4.0.3 or later (Chromecast required)
Microsoft Windows	7, 8.1, 10 (Chromecast Browser Plugin required)

17. Index

Version	Date	Changes
1.0	31.01.2018	Created
1.1	26.07.2018	- Minor text edits - Addition Firewall rules - Added vSolution Matrix
1.2	02.11.2018	- Minor text edits - Addition Firewall rules
1.3	21.02.2020	- Minor text edits - Addition Firewall rules - Illustrations updated
1.4	30.11.2020	- Minor text edits - Addition Firewall rules (Miracast / MS-Mice – Hardware cursor extension)