Cortiva Access Manual

2016 - 09

1709 - Cortiva

Colt CoolStream R

7.8°C 94 % RH

Shows the actual outside temperature and humidity

09:55:06 Tu, 2014/10/28

The actual system time and date

1 — Group Name +

Alarms and events

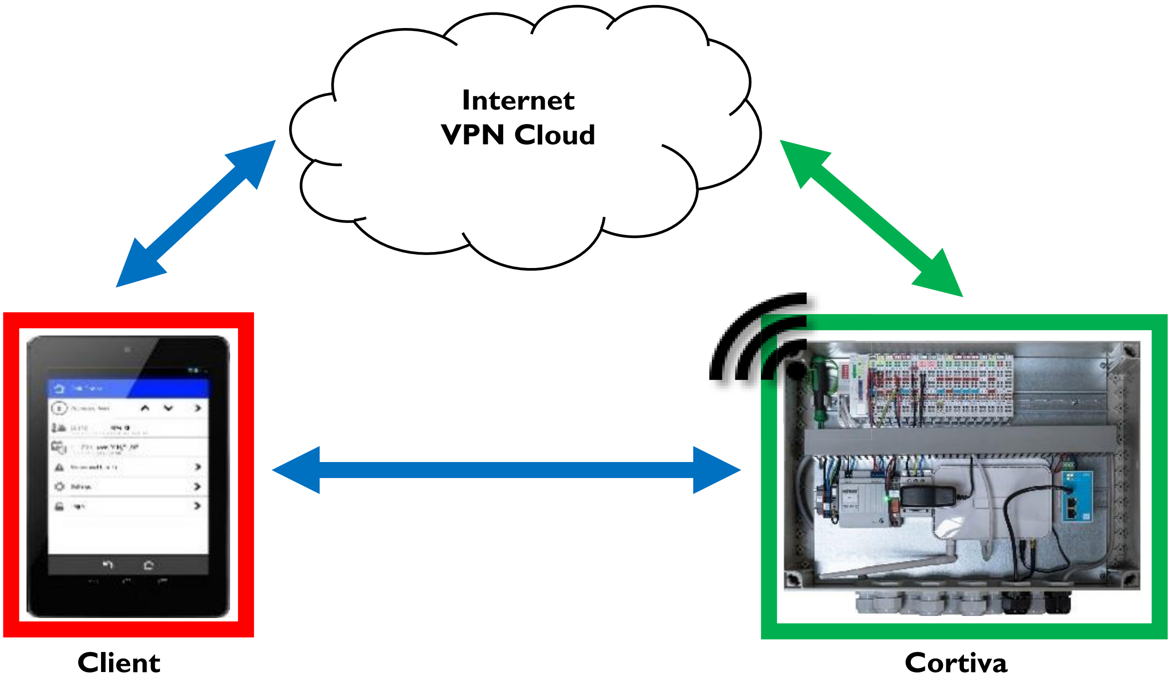
Settings

Login

1 Cortiva: operator access roadmap

This manual serves as a guide for the various access options for operating a Cortiva controls. It provides an initial overview for users (whether they be Colt personnel or customers), but also contains detailed and complete information for service technicians and IT specialists.

1.1 Overview



🟥 See chapter 2

🟦 See chapter 3

🟩 See chapter 4

In principle, any device (so-called “client”) can gain control via any suitable means of access to the Cortiva central controller and thereby to the complete CoolStream system. Thus, for example, it is possible for a tablet to access the system not only via the local network, but also remotely via the Internet. This is **independent** of how the Cortiva control system is connected to the Internet.

2 Client: a free choice

Colt's Cortiva controls can be accessed in a variety of ways. A so-called “client” is required.

2.1 Types of clients

Operating system	Type of client		
Google Android	Tablet 	Smartphone 	Laptop
Apple iOS	iPad 	iPhone 	iPod touch
Microsoft Windows	Laptop Tablet 	Industrial PC touch panel PC 	Desktop PC All-In-One PC
Linux			
Apple Mac OS X	Mac Mini 	iMac 	MacBook
The brand names or trademarks mentioned in this document are for identification purposes only and are the property of their respective owners. Photos: Wikipedia.org licence: Creative Commons by-sa 3.0.			

2.2 Reference client

The Colt reference client is the Google Android Tablet *Samsung Galaxy Tab 3 8.0 (2014)* and its successor *Samsung Galaxy Tab A6 7.0 (2016)*, which are available as standard accessories. Colt also develops and tests many other clients in various versions of the Microsoft Windows, Mac OS X and iOS operating systems. Due to the variety and rapid change of the devices as well as the software used, Colt cannot guarantee the conformity and correctness of the information relating to all possible devices.

2.3 System requirements

Operating system	Type of client
Google **Android**	**WAGO-Webvisu-App:** ▶ Webvisu App version 2.0.144 or higher. Download: https://play.google.com/store/apps/details?id=com.wago.Webvisu ▶ Android 3.0 or higher ▶ Minimum resolution: 600x860 pixels
Apple **iOS**	**WAGO-Webvisu-App:** ▶ Webvisu App version 2.0.143 or higher. Download: https://itunes.apple.com/WebObjects/MZStore.woa/wa/viewSoftware?id=726217015&mt=8 ▶ iPhone 5 or higher with iOS 9.3.2 ▶ iPad 4 or higher, iPad Air or higher, iPad mini or higher with iOS 9.3.2
Microsoft Windows	**Browser with Java plug-in: http://www.java.com** ▶ Windows 10 (8u51 and above), Windows 8.x (Desktop), Windows 7 SP1, Windows Vista SP2, Windows Server 2008 R2 SP1 (64-Bit), Windows Server 2012 and 2012 R2 (64-Bit) ▶ Administrator permissions for the installation and, if necessary, the security settings for the Java plug-in* ▶ Browser: Internet Explorer 9 and above, Firefox ▶ Minimum resolution for application: 600x860 pixels
Linux	**Browser with Java plug-in: http://www.java.com** ▶ Oracle, Red Hat Enterprise, Suse or Ubuntu Linux for version information see: http://www.java.com ▶ Administrator permissions for the installation and, if necessary, the security settings for the Java plug-in* ▶ Browser: Firefox ▶ Minimum resolution for application: 600x860 pixels
Apple **Mac OS X**	**Browser with Java plug-in: http://www.java.com** ▶ Intel-based Mac under Mac OS X 10.8.3+, 10.9+ ▶ Administrator permissions for the installation and, if necessary, the security settings for the Java plug-in* ▶ 64-bit browser: Safari, Firefox ▶ Minimum resolution for application: 600x860 pixels

* The Cortiva application contains an electronic certificate from the manufacturer Wago. Depending on the version of the Java plug-in, the certificate is also checked by the certificate issuer before execution. If this is not possible, the application is initially blocked and must be confirmed by the user when requested or is generally released as an exception rule within the system settings of the Java plug-in. This requires a one-off administrator authorisation.

3 Local or via VPN: Your client can access the Cortiva central controller

There are several connection options. The factory-configured, easy-to-configure, local access options are built-in and configured ready for use. Connect your tablet, smartphone or laptop to Cortiva's wireless LAN - then you're ready.

For integration into a customer-oriented network, the local Ethernet connection with port-forwarding is available, as well as access options via the cloud via VPN. The integration must be coordinated with the customer IT department and carried out by this IT department.

Client access		Cortiva central controller	Network diagram
①	**Local access via WLAN**	Standard equipment (included)	chapter 5.2
②	**Local access via Ethernet**	With option /5	
③	**Local access with integration into customer network**	With option /L	chapter 5.3
④	**Internet access via VPN service via web proxy**	With /L or /M options: - 1x Lizence* for each Cortiva	chapter 5.4
⑤	**Internet access via VPN service via OpenVPN Client**	With /L or /M options - 1x licence* for each Cortiva - 1x licence* for each user	chapter 5.5

* License for the INSYS Connectivity Service

3.1 Your client in the cloud: Simple. Secure. VPN!

The client can access the VPN service via a web proxy as well as via a VPN connection from the client to the INSYS Connectivity Service in the cloud. In both cases, the INSYS Connectivity Service ensures a secure VPN connection from the cloud to the Cortiva central controller. Your control system is in no way freely accessible via the Internet.

Web proxy

The web proxy, operated by INSYS, establishes a VPN connection to the Cortiva central controller when a so-called URL (Internet address) is requested. The URL is structured as follows:
https://colt-cortiva.net/K67K5GHPF4

This is your personal URL: only you and certain authorised persons at Colt know this URL. Security is ensured by the encrypted part of the URL. Only with knowledge of the key K67K5GHPF4 can the system be accessed. In addition, only access to the web interface is possible; access to other protocols, e.g. ftp, is not possible. The key - and thus the URL - can be changed at any time through via Colt's IT department if necessary, rendering the previous URL worthless.

VPN connection from the client to the INSYS Connectivity Service

Colt-IT will provide you with an individual, private IP address and a VPN certificate file (access key). The software OpenVPN (available for Windows, Linux, OS X, Android, iOS) is used to establish a VPN connection from the client to the INSYS Connectivity Service. The operation of the Cortiva central controller can be accessed with an IP address in the form https://172.16.5.2, where the 2nd and 3rd digit of the IP address 16.5 are individually different. You will receive this together with the order documentation. With the OpenVPN connection, the entire system can be accessed in the same fashion as with local access.

- OpenVPN for Desktop-OS: https://openvpn.net/index.php/open-source.html
- OpenVPN for Android: https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=en
- OpenVPN for iOS: https://itunes.apple.com/de/app/openvpn-connect/id590379981?mt=8

A system can only be accessed with a suitable VPN certificate - this ensures that only authorized Colt and customer personnel can access the system. Access rights are managed by Colt IT.

NOTE **Colt recommends a web proxy for everyday use**

- Due to the increased administrative burden on the certificates, the installation of the OpenVPN client on the client side and the additional license costs per user, Colt recommends the web proxy for the customer and daily service access, and only if necessary the client-side VPN connection.

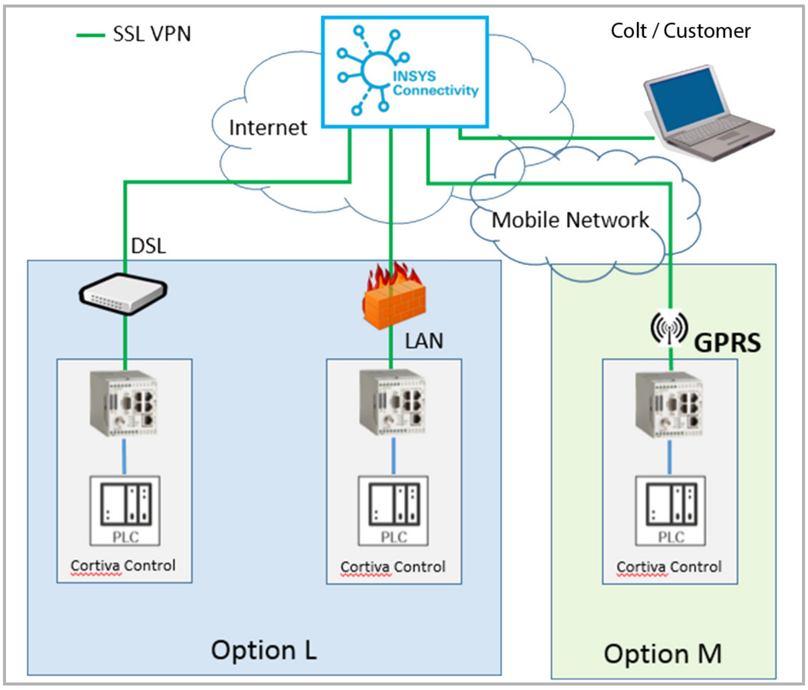
4 Your Cortiva in the cloud: Simple. Secure. VPN!

Colt provides remote support and remote maintenance services to the Cortiva controls through a VPN service from INSYS. The INSYS Connectivity Service combines your Cortiva controls with the Colt service technician with maximum security for your IT infrastructure. The VPN configuration used and the security certificates required for remote access are automatically generated and renewed.

There are basically two options with which the Cortiva finds its way onto the Internet:

/L option	/M option
The VPN router receives Internet access via a LAN or DSL connection	The VPN router receives Internet access via GSM (the mobile network)

- **/L option:** The LAN-based (Local Area Network) option can be used in two ways: either tunnelled through the customer LAN and then connected to the Internet, or with a separate, dedicated DSL / cable connection.
- **/M option:** If the LAN-based option cannot be used at all, the GSM-based option M is an alternative. Speed up to HSPA (3G+) is supported. In addition, a mobile broadband data tariff with a mini-SIM card is required.



/L option features and benefits	/M option features and benefits
No data costs for network connection	Also available where Internet is not possible
Fastest broadband internet connection	Independent of local customer services
Lowest network latency	No coordination with customer IT is necessary
No reception restrictions of a mobile network	

NOTE

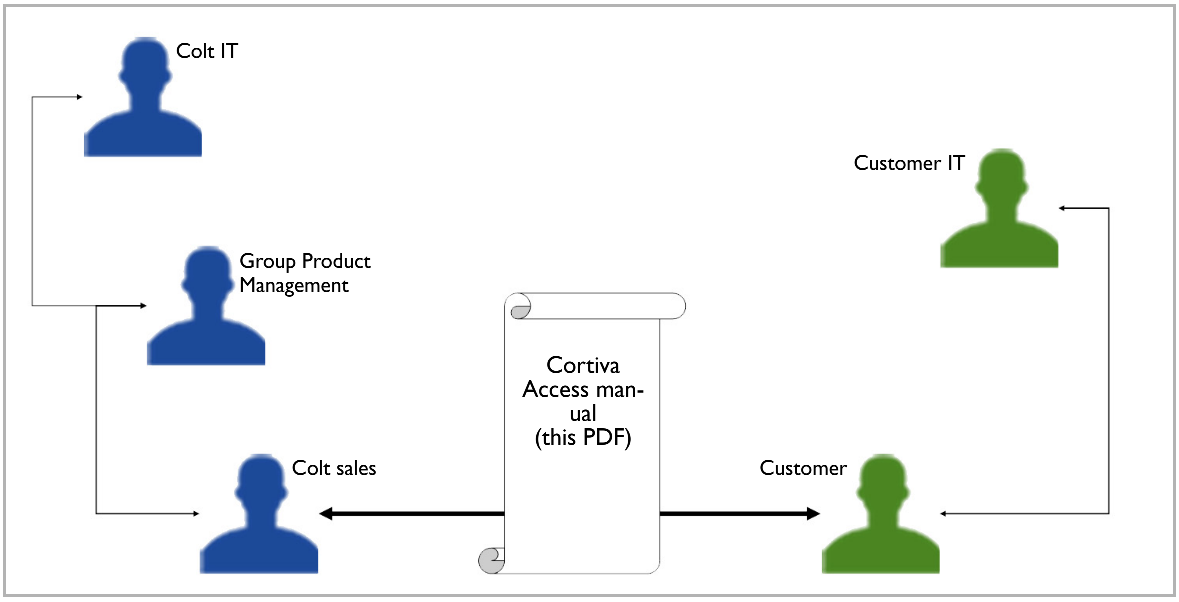
- Colt recommends the /L option
- The /L option requires customer services.

4.1 /L option: Internet access via LAN

Interface is the INSYS router in the Cortiva central controller, external LAN interface. Please note the following system requirements, the communication process and also the network diagrams in the appendix.

Communication process

Cortiva central controllers with factory-installed INSYS router option / L are configured, commissioned and tested when delivered. However in order to ensure that the tested system and the remote access function properly at the customer's building, customer services must be provided. The customer and their IT department must coordinate with each other how remote access is to be implemented for the Cortiva control. The following diagram is designed to help you complete this process. The key person is, as for all questions relating to the project, the project manager from sales. The Cortiva access manual (this document) contains all the information that the customer IT needs.



System requirements for the VPN service with the / L option

Name	Port	Protocol	Direction	Destination
DNS service	53	UDP	Outgoing	8.8.8.8 and 8.8.4.4
NTP service	123	UDP	Outgoing	ptbtime1.ptb.de
VPN start service	1194	UDP	Outgoing	init.insys-icom.de
Colt VPN service	1154	UDP	Outgoing	worker1.connectivity-service.insys-icom.de
When delivered, DNS and NTP are set to the above destinations. It is possible to use alternative customer-specific DNS or NTP servers.				
When delivered the external LAN interface of the INSYS router is set to DCHP. This requires a DHCP server from the customer. If this is not possible or desired, the INSYS router can also set to a static IP address.				
If the delivery status changes, the following details must be provided by the customer to start the VPN service:				
▶ DHCP				Yes / no?
▶ Static IP address				Only when DHCP is not being used
▶ Net mask				
▶ Default gateway				
▶ DNS				Only if DNS or NTP as mentioned above are not available
▶ NTP				
Instructions for configuring the static IP address can be found in the appendix see chapter 5.1				

5 Appendix

5.1 Configuration of a static IP address for INSYS router

A

INSYS router connection (/L option)

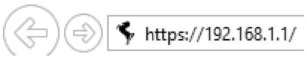
1.) Connect the INSYS router (LAN 2 / ext) to the customer network via Ethernet.

2.) Connect a client locally to the configuration (see *Local Wi-fi and Ethernet Network* diagram).

B

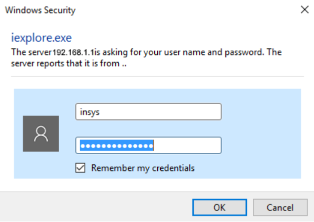
Access to the web interface

1.) Enter the IP address of the router in the browser's address line (https://192.168.1.1).



https://192.168.1.1/

2.) Login with user name and password from the Colt Order Documentation that you receive with the order.



Windows Security

iexplore.exe

The server192.168.1.1is asking for your user name and password. The server reports that it is from ..

insys

••••••••••••••

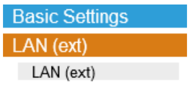
☑ Remember my credentials

OK Cancel

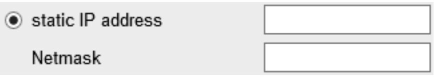
C

Set up a static IP address

1.) Open the **LAN (ext)** menu and select the **static IP address** option.



2.) Enter the static IP address as well as the net mask according to the customer's specification for static IP address and net mask.

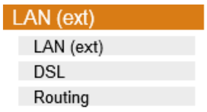


● static IP address

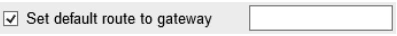
Netmask

3.) Confirm with **OK**.

4.) Open the **Routing** sub-menu.



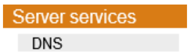
5.) Enter the default gateway associated with the IP network at **Set default route to gateway**.



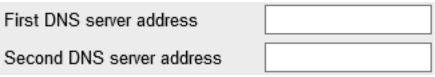
☑ Set default route to gateway

6.) Confirm with **OK**.

7.) Open the **Server services** menu.



8.) Optional: Specify custom DNS servers under **First / Second DNS server address**.



First DNS server address

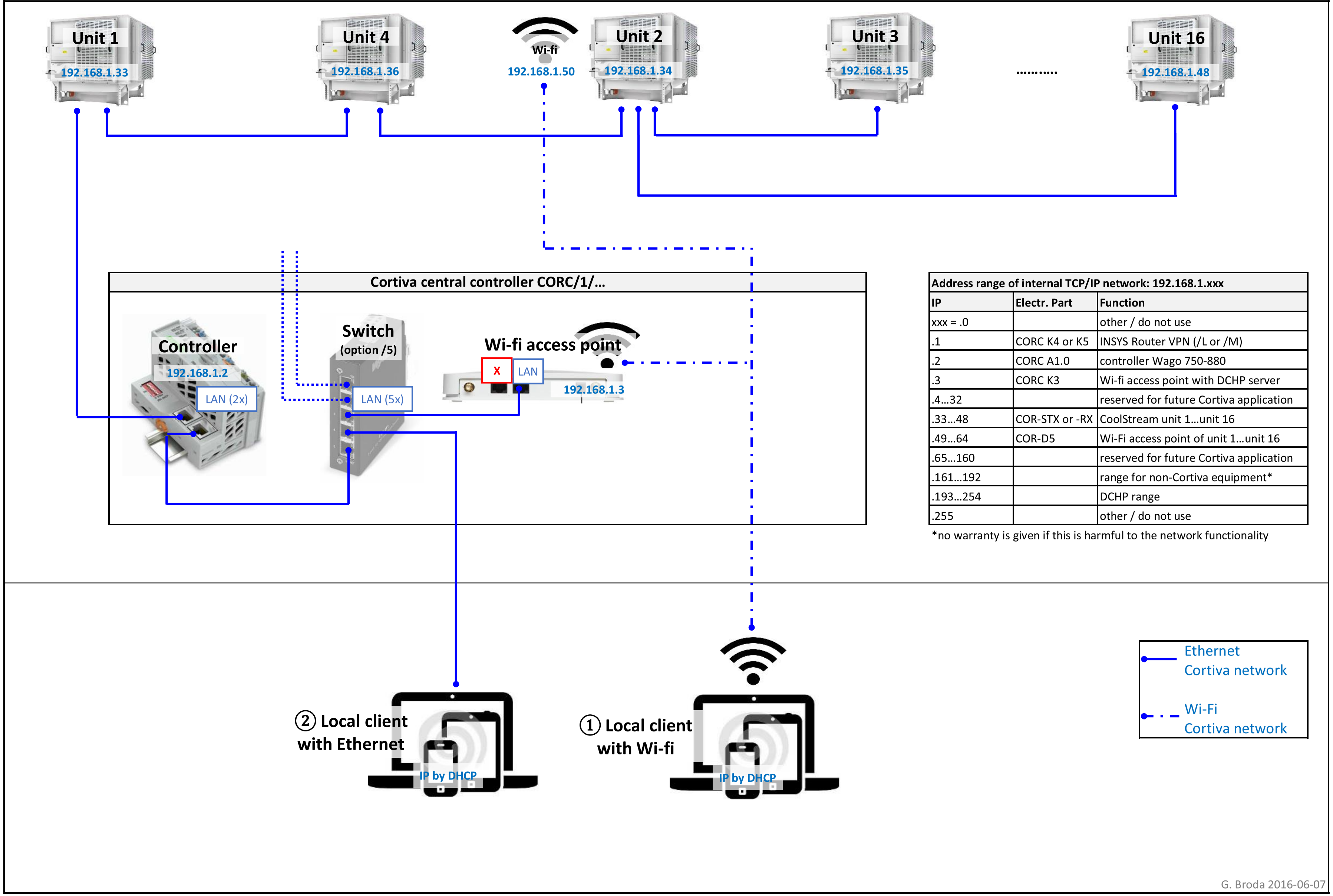
Second DNS server address

9.) Confirm with **OK**.

10.) The configuration is now complete. Make a test connection via the web proxy.

5.2 Local Wi-fi and Ethernet

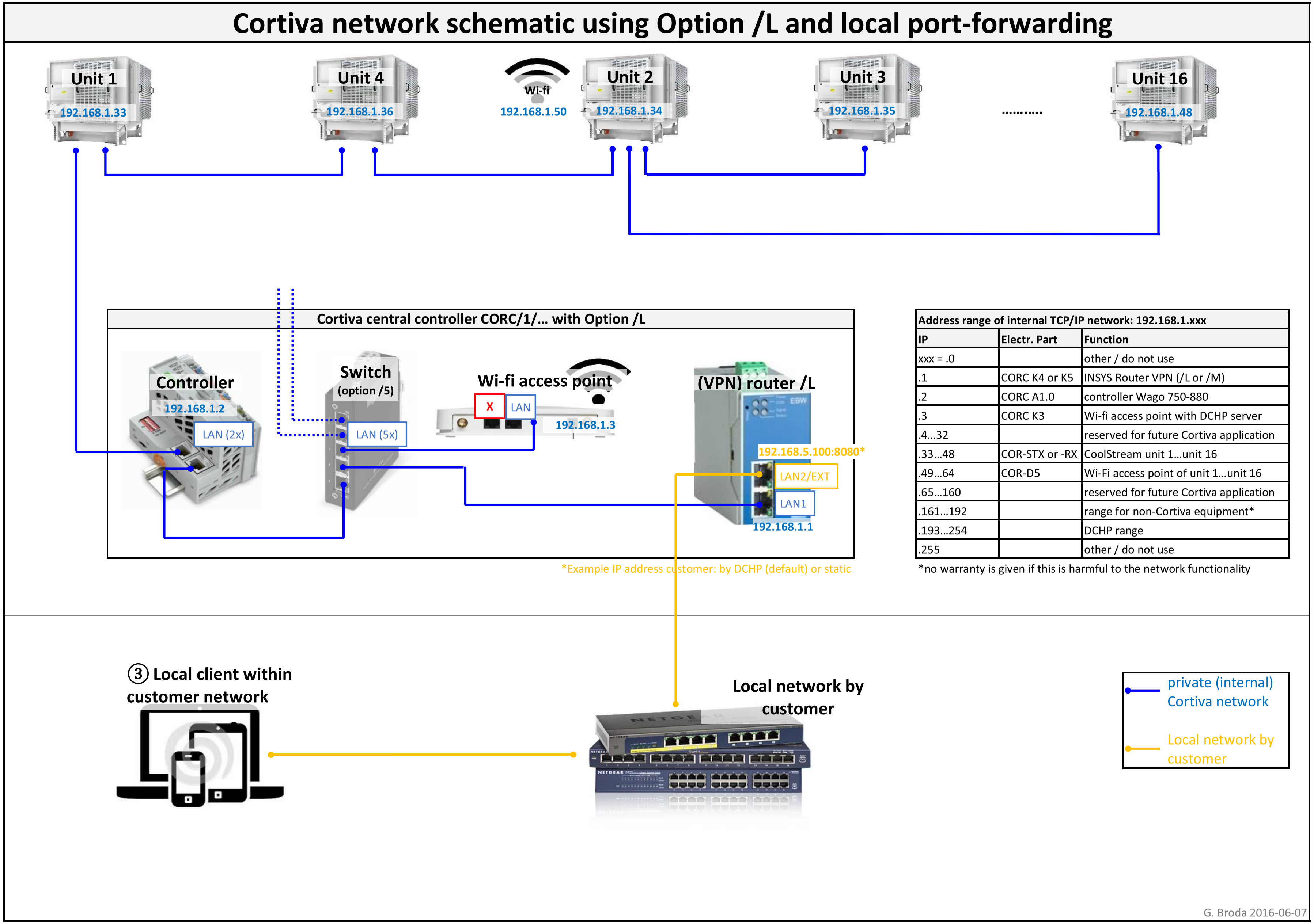
Cortiva network schematic using local Wi-fi and Ethernet



Address range of internal TCP/IP network: 192.168.1.xxx		
IP	**Electr. Part**	**Function**
xxx = .0		other / do not use
.1	CORC K4 or K5	INSYS Router VPN (/L or /M)
.2	CORC A1.0	controller Wago 750-880
.3	CORC K3	Wi-fi access point with DCHP server
.4...32		reserved for future Cortiva application
.33...48	COR-STX or -RX	CoolStream unit 1...unit 16
.49...64	COR-D5	Wi-Fi access point of unit 1...unit 16
.65...160		reserved for future Cortiva application
.161...192		range for non-Cortiva equipment*
.193...254		DCHP range
.255		other / do not use

*no warranty is given if this is harmful to the network functionality

5.3 Local Ethernet and Portforwarding

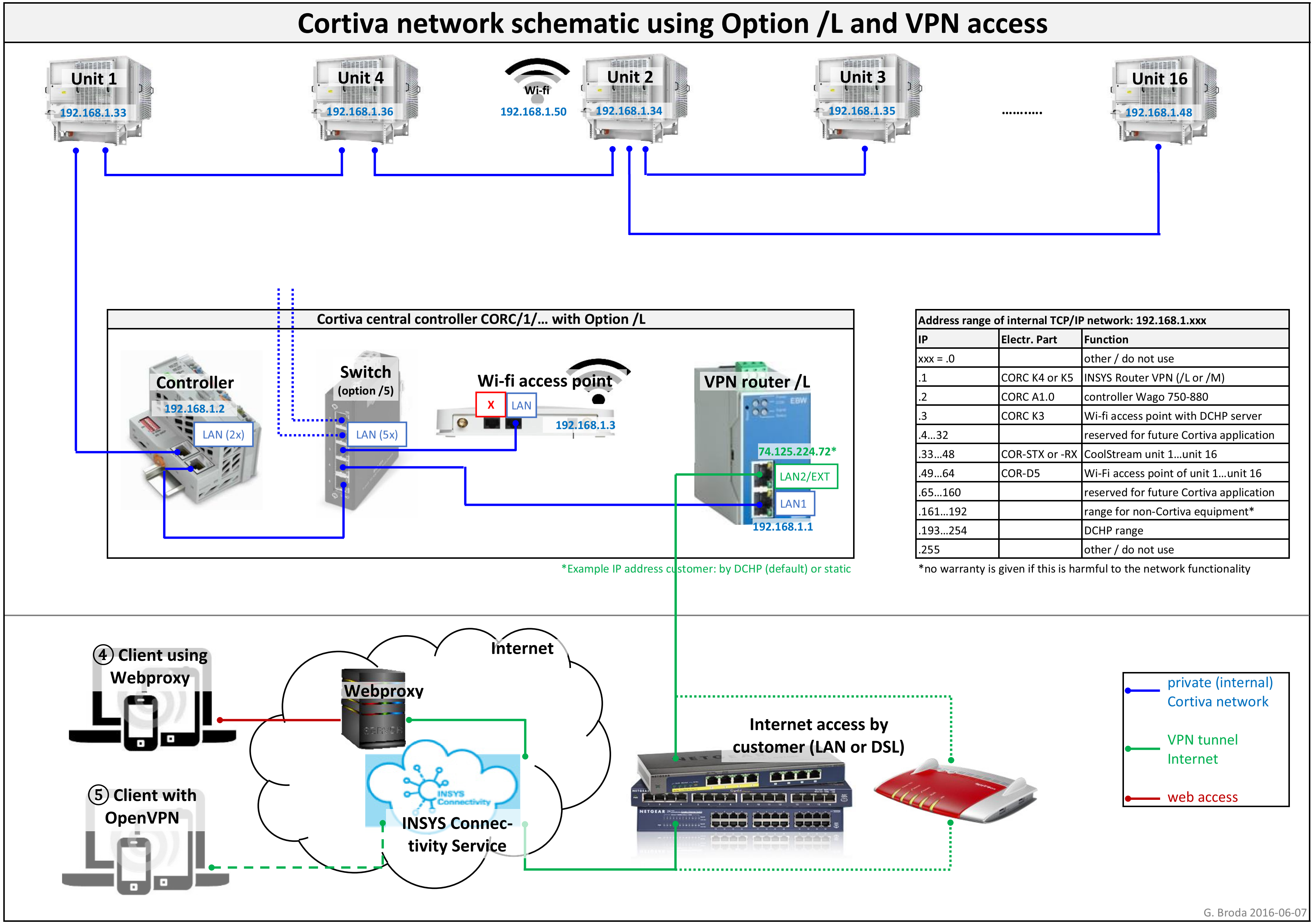

Cortiva network schematic using Option /L and local port-forwarding
Unit 1
192.168.1.33
Unit 4
192.168.1.36
Wi-fi
192.168.1.50
Unit 2
192.168.1.34
Unit 3
192.168.1.35
....
Unit 16
192.168.1.48
Cortiva central controller CORC/1/... with Option /L
Controller
192.168.1.2
LAN (2x)
Switch
(option /5)
LAN (5x)
Wi-fi access point
X
LAN
192.168.1.3
(VPN) router /L
192.168.5.100:8080*
LAN2/EXT
LAN1
192.168.1.1
*Example IP address customer: by DCHP (default) or static
③ Local client within customer network
Local network by customer
private (internal) Cortiva network
Local network by customer
G. Broda 2016-06-07

Address range of internal TCP/IP network: 192.168.1.xxx

IP	Electr. Part	Function
xxx = .0		other / do not use
.1	CORC K4 or K5	INSYS Router VPN (/L or /M)
.2	CORC A1.0	controller Wago 750-880
.3	CORC K3	Wi-fi access point with DCHP server
.4...32		reserved for future Cortiva application
.33...48	COR-STX or -RX	CoolStream unit 1...unit 16
.49...64	COR-D5	Wi-Fi access point of unit 1...unit 16
.65...160		reserved for future Cortiva application
.161...192		range for non-Cortiva equipment*
.193...254		DCHP range
.255		other / do not use

*no warranty is given if this is harmful to the network functionality

5.4 VPN Option /L



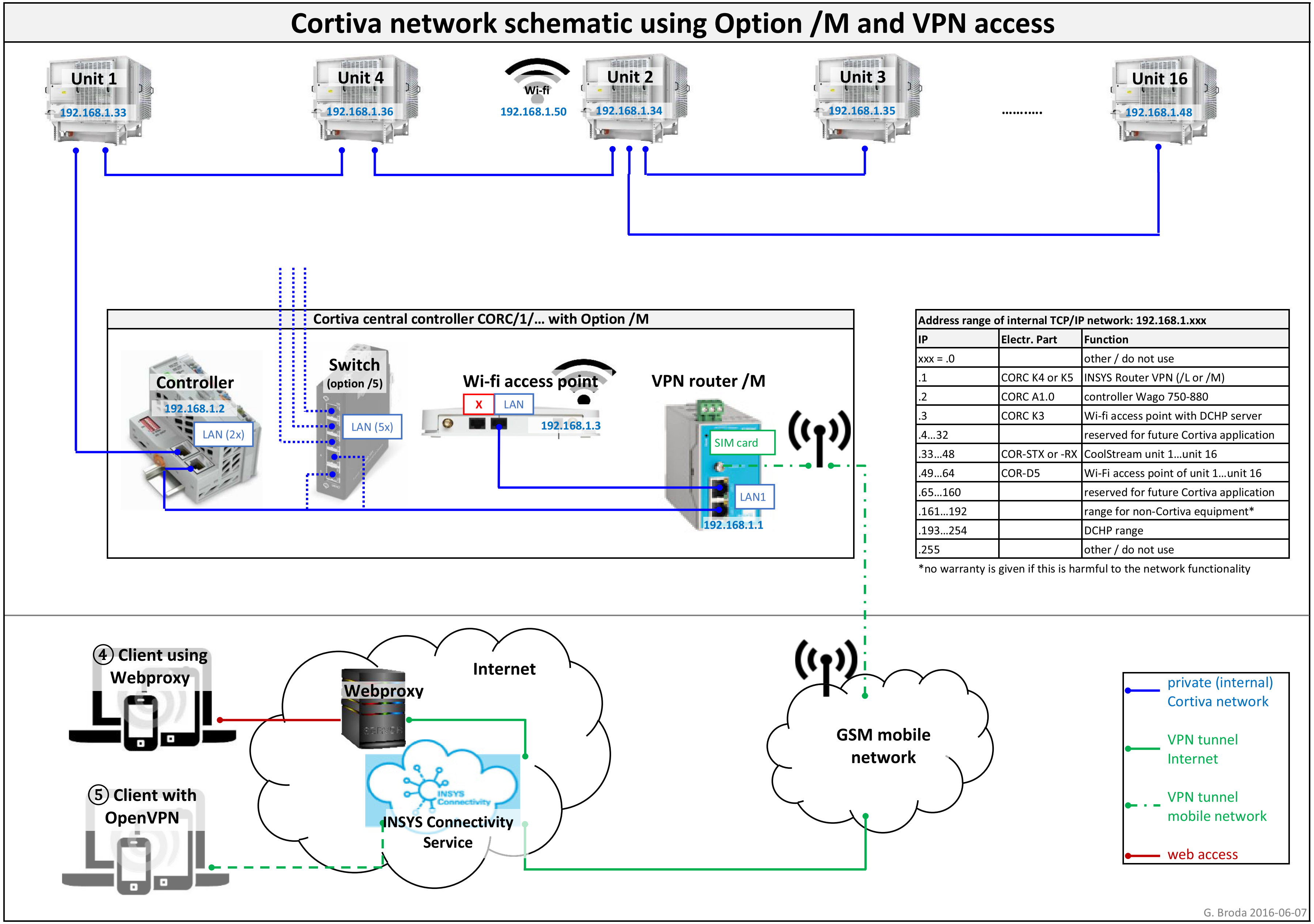
Cortiva network schematic using Option /L and VPN access

*Example IP address customer: by DCHP (default) or static

Address range of internal TCP/IP network: 192.168.1.xxx		
IP	Electr. Part	Function
xxx = .0		other / do not use
.1	CORC K4 or K5	INSYS Router VPN (/L or /M)
.2	CORC A1.0	controller Wago 750-880
.3	CORC K3	Wi-fi access point with DCHP server
.4…32		reserved for future Cortiva application
.33…48	COR-STX or -RX	CoolStream unit 1…unit 16
.49…64	COR-D5	Wi-Fi access point of unit 1…unit 16
.65…160		reserved for future Cortiva application
.161…192		range for non-Cortiva equipment*
.193…254		DCHP range
.255		other / do not use

*no warranty is given if this is harmful to the network functionality

5.5 VPN option /M



Cortiva network schematic using Option /M and VPN access

Address range of internal TCP/IP network: 192.168.1.xxx		
IP	Electr. Part	Function
xxx = .0		other / do not use
.1	CORC K4 or K5	INSYS Router VPN (/L or /M)
.2	CORC A1.0	controller Wago 750-880
.3	CORC K3	Wi-fi access point with DCHP server
.4...32		reserved for future Cortiva application
.33...48	COR-STX or -RX	CoolStream unit 1...unit 16
.49...64	COR-D5	Wi-Fi access point of unit 1...unit 16
.65...160		reserved for future Cortiva application
.161...192		range for non-Cortiva equipment*
.193...254		DCHP range
.255		other / do not use

*no warranty is given if this is harmful to the network functionality

www.coltgroup.com

Find out more about Colt by going to: **www.coltgroup.com**

Cortiva Access Manual 2016-09