

Описание сети, Ethernet и Wi-Fi (WLAN) для весов Cubis® MCA

В этом документе описано подключение весов к сети через Ethernet и Wi-Fi (WLAN). Приведены примеры, иллюстрирующие настройку и практическое использование весов.



Исполнительное резюме

Лабораторные весы Cubis® MCA Premium предлагают комплексные и гибкие возможности подключения для интеграции весов в лабораторные IT. Большое количество стандартизированных IT-протоколов, таких как веб-сервис REST, SMB или LDAP, доступны через Ethernet и Wi-Fi, что обеспечивает прямую интеграцию без использования дополнительного промежуточного программного обеспечения. Кроме того, Cubis® можно дистанционно управлять по сети с помощью веб-браузера и просматривать журнал аудита и другую информацию о состоянии.

1	Сетевое подключение Ethernet и Wi-Fi	4
1.1	Общие настройки	4
1.2	Ethernet (LAN)	4
1.2.1	Протокол IPv4	5
1.2.2	Протокол IPv6	5
1.2.3	DNS 1 и DNS 2	5
1.3	Wi-Fi (WLAN)	5
1.3.1	SSID и пароль Wi-Fi	6
1.3.2	Протокол IPv4/IPv6 и DNS 1/2	6
2	Сетевые услуги	6
2.1	Последовательная связь	6
2.1.1	Протокол SBI	6
2.1.2	Протокол xBPI	7
2.1.3	Протокол SICS	7
2.1.4	QAPP напрямую	7
2.2	Сетевые разъемы	7
2.2.1	YDP30-NET	7
2.2.2	Сетевой принтер	7
2.2.3	FTP / FTPS	8
2.2.4	Протокол SMB	8
2.3	Сайт	8
2.3.1	Веб-сервисы	8
2.4	NTP-сервер для даты и времени	8
2.5	Сертификаты	8
2.5.1	Обязательства оператора	8
2.5.2	Сброс сертификатов	9
2.5.3	Установка или обновление сертификатов	9
2.5.3.1	Сертификаты клиента	9
2.5.3.2	Сертификаты ЦС	9
2.5.3.3	Типы файлов сертификатов	9
2.5.4	Типы сертификатов	10
2.5.4.1	Сертификаты ЦС	10
2.5.4.2	Неизвестные центры сертификации	10
2.5.4.3	Сертификаты устройств	10
2.5.4.4	Сертификаты Wifi	11
2.5.4.5	Сертификаты LDAPS	11
2.5.5	Защищенные сетевые соединения с помощью SSL/TLS	11
2.5.5.1	Неизвестные центры сертификации	11
3	Примеры применения	11
3.1	Отчет о настройках меню на файловом сервере Windows	12
3.1.1	Настройка	12
3.1.2	Приложение	12
3.1.3	Устранение неполадок	13

3.2 Обновление QAPP Center на FTP-сервере	13
3.2.1 Настройка	13
3.2.2 Приложение	13
3.2.3 Устранение неполадок	14
3.3 Просмотр записей журнала аудита через веб-браузер	14
3.3.1 Настройка	14
3.3.2 Приложение	15
3.3.3 Устранение неполадок	15
3.4 Синхронизация даты и времени с сервером NTP	15
3.4.1 Настройка	15
3.4.2 Устранение неполадок	16
4 Приложение	16
4.1 Поддерживаемые Wi-Fi адаптеры	16
5. Сокращения	17

1 Сетевое подключение Ethernet и Wi-Fi

Весы Cubis® MCA могут быть подключены к сети на базе TCP/IP с помощью кабеля через Ethernet-соединение (гнездо RJ45) и беспроводным способом через USB-адаптер Wi-Fi (WLAN адаптер).

Скорость передачи данных сетевого соединения составляет 10 Мбит/с (10BASE-T, Ethernet) и 100 Мбит/с (100BASE-TX Fast Ethernet).

Соединение Ethernet осуществляется с помощью соединительного кабеля CAT 5 или выше, скрученного попарно, экранированного, 1:1, UTP/STP, разъем RJ45; например, коммутационный кабель CAT 5 в зависимости от использования (прямой/перекрестный).

Для беспроводного подключения Cubis® MCA поддерживает наиболее распространенные USB-адаптеры Wi-Fi (WLAN-флешки), которые предлагаются на рынке.

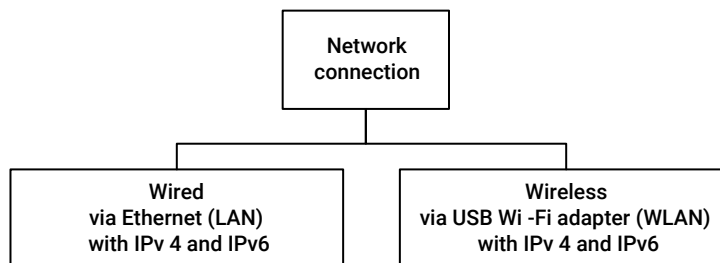


Рисунок 1: Сетевое подключение

весы Cubis® MCA может иметь по одному IPv4 и IPv6 адресу в сетях Ethernet и Wi-Fi соответственно, т.е. до 4 адресов.

Через сетевые соединения Ethernet (LAN) и Wi-Fi (WLAN) весы Cubis® MCA одновременно предлагает несколько сетевых услуг.

1.1 Общие настройки

Имя хоста весов, по умолчанию, состоит из обозначения серии и последних 3 байт MAC-адреса, например, [cubis-1a477e]. Имя хоста может быть выбрано произвольно, но должно быть уникальным в сети.

1.2 Ethernet (LAN)

Для Ethernet-подключения весов могут использоваться протоколы IPv4, а также IPv6. Для каждого протокола можно отдельно установить, будет ли IP-адрес получен автоматически или балансу будет присвоен фиксированный IP-адрес. Соответствующий протокол можно также полностью отключить.

В обзоре настроек для Ethernet статус показывает, установлено ли соединение с сетью. Кроме того, здесь же отображается уникальный MAC-адрес весов, например, [00:30:D6:1F:77:569].

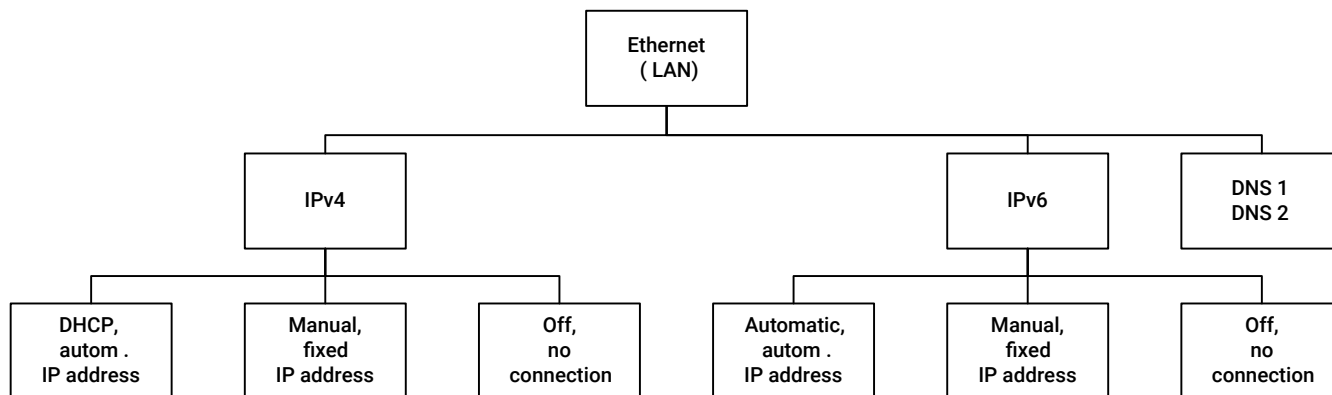


Рисунок 2: Ethernet с IPv4/IPv6

Для работы с фиксированным IP-адресом помимо IP-адреса, в зависимости от протокола, необходимо также вручную ввести маску подсети и шлюз для IPv4, или длину префикса и шлюз для IPv6. Ввод шлюза

необязателен и необходим только при необходимости подключения к Интернету.

Всю необходимую для этого информацию может предоставить сетевой администратор, отвечающий за сеть компании.

1.2.1 Протокол IPv4

IP-адрес для протокола IPv4 (4*8 бит = 32 бита) состоит из 4 десятичных чисел от 0 до 255, которые разделяются точкой, например, [123.4.56.123]. Этот формат применяется для ввода фиксированного IP-адреса, обозначения подсети и шлюза.

1.2.2 Протокол IPv6

IP-адрес для протокола IPv6 (8*16 бит = 128 бит) состоит из 8 буквенно-цифровых шестнадцатеричных чисел от 0 до FFFF, которые разделяются двоеточием, например, [esb1:d583:6341:baf76:0:0:1].

Первые 4 блока (64 бита) составляют префикс, а последние 4 блока - идентификатор интерфейса. Маска сети IPv4 и адрес сети IPv4 в IPv6 заменены длиной префикса и префиксом. Длина префикса определяет количество битов, составляющих префикс. Типичная длина префикса составляет 64. Префикс заменяет маску подсети в случае IPv6.

1.2.3 DNS 1 и DNS 2

В сетевых системах на базе IP DNS (Domain Name System) помогает отвечать на запросы разрешения имен. В сети может быть несколько DNS-серверов, Cubis® MCA поддерживает ввод двух серверов.

Для каждого DNS-сервера можно ввести IP-адрес или имя сервера.

В случае DHCP DNS-сервер предоставляется автоматически сервером DHCP. Кроме того, в этом случае DNS1 и DNS2 добавляются в список DNS-серверов.

1.3 Wi-Fi (WLAN)

К балансу MCA можно подключить USB-адаптер Wi-Fi (WLAN stick); несколько адаптеров этого типа не поддерживаются.

В обзоре настроек для Wi-Fi (WLAN) отображается статус, подключен ли соответствующий USB-адаптер Wi-Fi и подключен ли он к сети.

дисплей состояния

- Нет доступного устройства - Не подключен USB-адаптер Wi-Fi.
- Отключено - Нет подключения к сети Wi-Fi, например, не выполнен вход в систему с помощью идентификатора Wi-Fi SSID и пароля.
- Готов - Установлено соединение с сетью Wi-Fi.
- Онлайн - Установлено соединение с сетью Wi-Fi и Интернетом.

Если соединение установлено, то здесь также отображается уникальный MAC-адрес USB-адаптера Wi-Fi, например, 34:C9:F0:89:6F:D6.

В Приложении, раздел: Совместимые Wi-Fi стики.

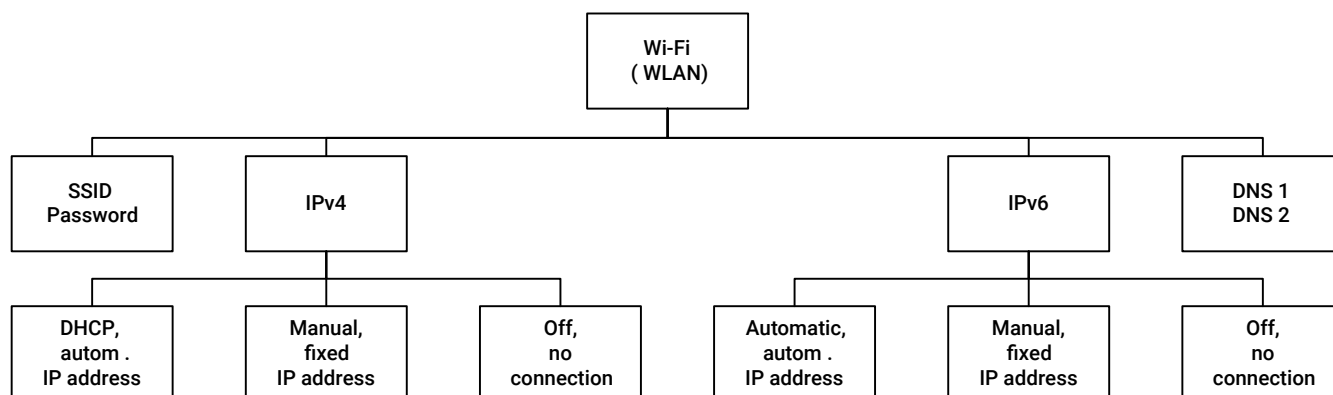


Рисунок 3: Wi-Fi с IPv4/IPv6

Для работы с фиксированным IP-адресом помимо IP-адреса, в зависимости от протокола, необходимо также вручную ввести маску подсети и шлюз для IPv4, или длину префикса и шлюз для IPv6. Ввод шлюза необязателен и необходим только при необходимости подключения к Интернету.

Всю необходимую для этого информацию может предоставить сетевой администратор, отвечающий за сеть компании.

1.3.1 SSID и пароль Wi-Fi

Для подключения к сети Wi-Fi необходимо ввести Wi-Fi SSID (уникальное имя сети Wi-Fi) и Wi-Fi пароль (ключ сети Wi-Fi).

Для аутентификации весы MCA поддерживают стандарты WEP, WPA-PSK и WPA2-PSK, а следовательно, и метод PSK для шифрования.

1.3.2 Протокол IPv4/IPv6 и DNS 1/2

Для протокола IPv4 и IPv6, а также для DNS 1 и DNS 2, для Wi-Fi (WLAN) применяется такое же описание, как и в случае Ethernet (LAN).

2 Сетевые услуги

Через сеть весы Cubis® MCA предлагают одновременно несколько услуг: последовательная связь с различными протоколами, коннекторы для подключения к сетевым устройствам хранения данных и принтерам, веб-сайт и веб-сервис для удаленного доступа, а также подключение к NTP-серверу для синхронизации даты и времени.

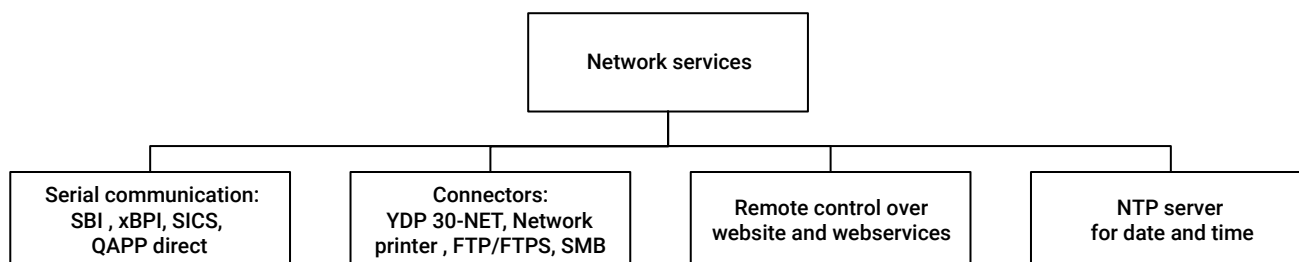


Рисунок 4: Сетевые услуги

2.1 Последовательная связь

Используя сетевое соединение, можно использовать протоколы последовательной связи SBI, xBPI, SICS, miniSICS, которые могут работать независимо от активной задачи и ее использования. Это соединение клиент/сервер требует настроек для общего TCP-порта.

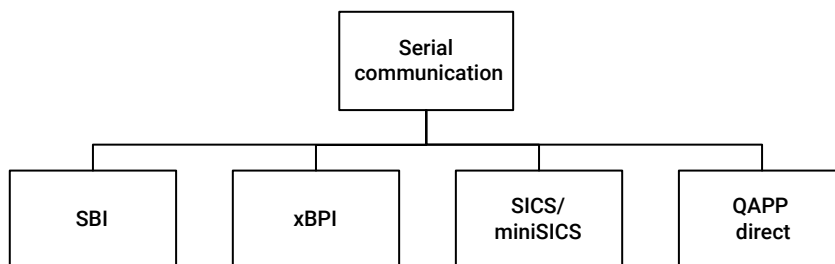


Рисунок 5: Последовательная связь через сеть

2.1.1 Протокол SBI

Этот простой, основанный на ASCII протокол может управлять основными функциями весов с помощью команд ESC. Вывод значений на дисплей может быть запрошен индивидуально через команду ESC, или автоматически с каждым новым результатом взвешивания в цикле последовательности отображения, или автоматически через определенные временные интервалы. Можно выбрать, обеспечивается ли вывод только стабильного отображаемого значения или также без стабильного отображаемого значения. Формат вывода может быть выбран с идентификатором (заголовком) или без него.

Команды SBI и форматы вывода приведены в отдельном описании интерфейса.

2.1.2 Протокол xBPI

Этот двоичный протокол предлагает расширенный набор команд. Он может использоваться для управления многочисленными функциями весов.

Существует отдельное описание интерфейса для возможных команд xBPI.

2.1.3 Протокол SICS

Протокол SICS (Standard Interface Command Set) устанавливает совместимость с протоколом MT-SICS компании Mettler и позволяет отправлять на весы команды для выполнения основных функций. Однако следует отметить, что существуют различия, обусловленные разными аппаратными/программными платформами.

Команды SICS и miniSICS, реализованные в весах, приведены в отдельном описании интерфейса.

2.1.4 QAPP напрямую

Только специальные QAPP, которые запускаются заданием, могут использовать интерфейс для своих целей ввода и вывода. Возможности ввода и вывода через интерфейс описаны в соответствующем специальном QAPP.

2.2 Сетевые разъемы

В Cubis® MCA коннекторы устанавливают соединение с сетевыми серверами, которые должны использоваться в качестве устройств хранения данных или принтеров.

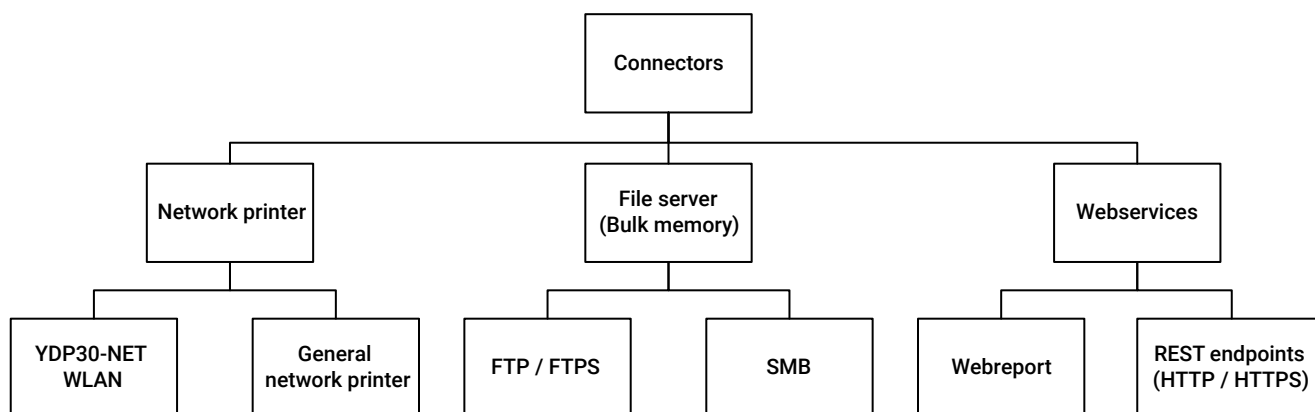


Рисунок 6: Сетевые коннекторы

Сетевой принтер YDP30-NET может быть подключен по WLAN или как общий сетевой принтер к независимой сети Wi-Fi или корпоративной сети с использованием DHCP.

Для подключения к запоминающему устройству, такому как файловый сервер Windows, FTP/FTPS или STARLIMS, необходимо специальное расширение QAPP, которое должно быть активировано через QAPP Center в разделе [Connectivity].

2.2.1 YDP30-NET

Этот коннектор предназначен для подключения принтера YDP30-NET с помощью кабеля (LAN) или беспроводного соединения (WLAN). Коннектор требует ввода на принтере имени разъема, IP-адреса или имени хоста, а также согласованного номера порта между принтером и балансом.

Беспроводное подключение принтера YDP30-NET описано в отдельных инструкциях.

2.2.2 Сетевой принтер

Коннектор для сетевого принтера позволяет, например, подключаться к принтеру формата A4 в независимой сети Wi-Fi со стандартными компонентами Wi-Fi или в корпоративной сети по DHCP со стандартными методами аутентификации. Сетевой принтер должен поддерживать протокол IPP (Internet Printing Protocol).

Для коннектора требуется ввести имя коннектора, IP-адрес или имя хоста на принтере, а также протокол передачи данных.

В отдельном описании [Концепция печати] описывается настройка и применение сетевого принтера с примером применения.

2.2.3 FTP / FTPS

Протокол передачи файлов (FTP) - это стандартный сетевой протокол для передачи компьютерных файлов между клиентом и сервером в компьютерной сети.

весы являются FTP-клиентом и может хранить файлы на FTP-сервере или получать файлы с FTP-сервера по протоколу. В случае FTPS соединение также шифруется; необходимые для этого сертификаты описаны отдельно.

Для подключения к FTP/FTPS-серверу необходимо создать коннектор с уникальным именем, IP-адресом и номером порта сетевого сервера, при необходимости подкаталогом на сервере, а также именем пользователя и паролем.

Примечание: При наличии нескольких коннекторов на весах к одному серверу, но с разными подкаталогами, хранение данных может быть легко структурировано в соответствии с темой (резервное копирование, отчет, ...).

2.2.4 Протокол SMB

Коннектор файлового сервера Windows использует сетевой протокол SMB. Этот протокол облегчает доступ к разрешенным сетевым дискам компьютеров Windows или Linux для хранения или получения файлов данных в выбранных целевых каталогах.

2.3 Сайт

Веб-сайт весов MCA можно открыть просто через IP-адрес весов с помощью веб-браузера. На странице [My Cubis] (главная страница) отображаются установленные идентификаторы устройств, общая информация об устройстве весов и информация об услуге.

На странице [Удаленное управление], в зависимости от настроек в меню, через браузер можно отобразить либо [Только просмотр], либо [Просмотр и дистанционное управление] весов MCA.

На странице [Снимок экрана] создается PNG-файл текущего экрана, который можно сохранить.

Если расширение QAPP [Audit trail] было активировано в QAPP Center в пакете [Pharma], то также отображается веб-сайт [Audit trail]. Записи в журнале аудита можно фильтровать, сортировать и экспортировать в соответствии с темами.

Доступ к сайту можно полностью деактивировать через меню, а значит, и дистанционное управление через веб-службу REST.

2.3.1 Веб-сервисы

Удаленное управление базовыми функциями весов MCA также может осуществляться через веб-сервис REST.

Существует отдельное описание доступных REST веб-сервисов весов MCA.

2.4 NTP-сервер для даты и времени

Cubis® MCA предлагает возможность синхронизации даты и времени с NTP-сервером. Для этого можно активировать соединение с сервером и ввести IP-адрес сервера в настройках устройства MCA в разделе Дата/Время и NTP Configuration.

2.5 Сертификаты

весы Cubis® MCA поддерживают использование сертификатов для надежной интеграции в локальную IT-инфраструктуру. MCA может обрабатывать сертификаты доверенных центров сертификации (CA), чтобы идентифицировать доверенные серверы. MCA также предоставляет для загрузки собственные сертификаты устройств. Эти сертификаты устройств импортируются в браузеры для безопасного удаленного доступа к веб-сайту устройства.

Существует отдельное описание на тему [Сертификаты].

Сертификаты устройств основаны на стандарте X.509 и используют криптографию с открытым ключом, в которой используется пара ключей, состоящая из открытого и закрытого ключа. Эта пара ключей обеспечивает передачу зашифрованных данных, проверку цифровых подписей и надежную аутентификацию личности. В зависимости от того, как создается и хранится закрытый ключ, перед его использованием может потребоваться расшифровка с помощью ключевой фразы.

2.5.1 Обязательства оператора

Весы Sartorius Cubis MCA поставляются с предустановленными сертификатами устройств, которые имеют ограниченный срок действия. Операторы могут обновлять первоначально установленные сертификаты и импортировать свои собственные.

Оператор несет ответственность за управление и обновление сертификатов, а также за обеспечение их действительности. Во избежание возможных предупреждений или ограничений на безопасные соединения важно регулярно проверять срок действия сертификатов и при необходимости обновлять их.

Обновление сертификата не влияет на функцию взвешивания или на интеграцию в местную ИТ-инфраструктуру. Поэтому при обновлении сертификатов не требуется повторная калибровка или ревалидация устройств.

2.5.2 Сброс сертификатов

Если после сброса сертификата отображается предупреждение об истечении срока действия сертификата, обновите сертификат, как описано в разделе Обновление сертификатов.

1. Предоставить файлы сертификатов таким образом, чтобы к ним можно было получить доступ через разъем на устройстве, например, на USB-накопителе и USB-разъеме
2. Перейдите к настройкам из главного меню
3. Перейдите в меню Подключения в раздел Сертификаты
4. Выберите Сертификаты системы и Сертификаты устройства
5. Выберите значок "Корзина", чтобы обновить сертификаты, и подтвердите сообщение "Сбросить сертификаты" нажатием кнопки "Да".
6. Убедитесь, что доступен новый сертификат "Sartorius Factory Authority". Срок действия этого сертификата истекает в 2043 году.
7. Если в списке отображается "Sartorius Factory Authority", обновление прошло успешно, и создается запись в журнале аудита.

Если после сброса сертификата отображается предупреждение об истечении срока действия сертификата, обновите сертификат, как описано в разделе Обновление сертификатов.

2.5.3 Установка или обновление сертификатов

Чтобы установить или обновить сертификат, следуйте этим инструкциям.

2.5.3.1 Сертификаты клиента

1. Предоставить файлы сертификатов таким образом, чтобы к ним можно было получить доступ через разъем на устройстве, например, на USB-накопителе и USB-разъеме
2. Перейдите к настройкам из главного меню
3. Перейдите в меню Подключения в раздел Сертификаты
4. Перейдите в соответствующее меню, для которого необходимо установить сертификат. Различение и объяснение сертификатов можно найти в главе Типы сертификатов.
5. Нажмите кнопку [IMPORT] и выберите соответствующий разъем, через который можно получить доступ к файлам сертификатов для установки.
6. Выберите [Сертификат] и выберите файл сертификата с открытым ключом из списка файлов, доступных через коннектор. Поддерживаются следующие форматы: .pem и .crt.
7. Выберите [Личный ключ] и выберите файл сертификата с личным ключом из списка файлов, доступных через коннектор. Поддерживаются следующие форматы: .key
8. Выберите [Пароль закрытого ключа] и введите пароль для закрытого ключа.
9. Подтвердите импорт. После успешной проверки файлы будут переданы в систему.

2.5.3.2 Сертификаты ЦС

1. Сделайте файлы сертификатов доступными, чтобы к ним можно было получить доступ через разъем на устройстве, например, на USB-накопителе и через разъем USB.
2. Перейдите к настройкам из главного меню
3. В меню Подключения перейдите к подменю Сертификаты
4. Перейдите в соответствующее меню, для которого необходимо установить сертификат. Различение и объяснение сертификатов можно найти в главе Типы сертификатов.
5. Нажмите кнопку [IMPORT] и выберите соответствующий разъем, через который можно получить доступ к устанавливаемым файлам сертификатов.
6. Выберите файл сертификата из списка файлов, доступных через коннектор. Поддерживаются следующие форматы: .pem и .crt.

2.5.3.3 Типы файлов сертификатов

Краткое руководство по PKI: Ключи состоят из двух половин - открытого и закрытого ключа. Открытый ключ может распространяться публично и широко, и вы можете использовать его для проверки, но не тиражирования информации, полученной с помощью закрытого ключа. Закрытый ключ должен храниться в секрете.

- Файлы .key обычно представляют собой закрытый ключ, используемый сервером для шифрования и упаковки данных для проверки клиентами.
- Файлы .pem обычно представляют собой открытый ключ, используемый клиентом для проверки и расшифровки данных, отправляемых серверами. Файлы PEM также могут быть закодированными закрытыми ключами.
- В файлы .p12 вложены обе половины ключа, так что администраторы могут легко управлять половинами ключей.
- Файлы .cert или .crt представляют собой подписанные сертификаты с открытым ключом, информацией о владельце ключа и цифровой подписью центра сертификации, выдавшего сертификат. Это позволяет третьей стороне классифицировать систему как заслуживающую доверия.
- В файлах .cer сертификаты обычно представлены в двоичном формате или в формате Base64. Поэтому они отличаются от файлов .crt по кодировке.

2.5.4 Типы сертификатов

Для безопасного подключения к сетевым службам весам требуются различные сертификаты, которые можно загрузить в весы. Различают следующие сертификаты:

- CA-сертификаты (доверенные центры сертификации)
- Сертификат устройства.
- Сертификат аутентификации WiFi.
- LDAPS сертификат.

2.5.4.1 Сертификаты ЦС

Сертификат центра сертификации (Certificate Authority Certificate) - это цифровой сертификат, выданный заслуживающим доверия органом - так называемым центром сертификации (Certificate Authority, CA). Его цель - подтвердить подлинность и благонадежность партнера по общению или службы. Когда два устройства или программы общаются друг с другом по сети, сертификат CA позволяет обеим сторонам убедиться, что они действительно подключены к желаемому партнеру, а не к злоумышленнику, который выдает себя за него.

Если сертификат ЦС классифицируется как надежный, устройство автоматически принимает все сертификаты, полученные на его основе. Таким образом создается так называемая цепочка сертификатов, которую можно проследить от корневого сертификата ЦС до соответствующего сертификата устройства.

2.5.4.2 Неизвестные центры сертификации

Устройство также предлагает возможность доверять сертификатам, которые не были выпущены известным центром сертификации. Если эта опция активирована, устройство принимает такие сертификаты без проверки их достоверности по цепочке сертификатов. Это может быть полезно в тестовых средах или средах разработки, но представляет собой риск для безопасности при использовании в промышленных целях, поскольку подлинность и надежность используемых сертификатов не гарантируется.

Эту опцию можно активировать в разделе Сертификаты, Системные сертификаты, [Доверять неизвестным центрам сертификации].

2.5.4.3 Сертификаты устройств

Сертификаты устройств предоставляют устройству уникальную идентификацию, которая позволяет ему аутентифицировать себя в подключенных системах. Это гарантирует, что только авторизованные устройства могут получить доступ к данным и что связь между устройствами защищена. Эти сертификаты основаны на стандартах X.509 и генерируются с помощью сертификатов с открытым ключом (Public Key Infrastructure, PKI). Это позволяет устройствам идентифицировать другие доверенные устройства и серверы.

В соответствии с этим правилом должен быть создан Gerätezertifikat из внутреннего Zertifizierungsstelle (CA) одной организации. Das Zertifikat wird mit dem privaten Schlüssel des Stammzertifikats (CA-Zertifikat) der Organisation signiert, das als Basis für die Signierung weiterer Zertifikate dient.

<Поэтому важно защитить устройство собственным сертификатом, как только оно поступит в вашу организацию. Устройства поставляются в разобранном виде со стандартным сертификатом от Sartorius.

Сертификаты устройств должны создаваться внутри вашей системы и сети, для чего необходим частный ЦС. Существует два подхода:

1. Создайте собственный частный ЦС с помощью таких инструментов, как OpenSSL или Microsoft CA.
2. Наймите поставщика управляемых PKI (mPKI) для решения задач аутентификации и шифрования.

2.5.4.4 Сертификаты Wifi

Сертификат WiFi - это цифровой сертификат, который используется для безопасной аутентификации и шифрования в беспроводной сети (WLAN). Как правило, такие сертификаты используются в составе WPA2-Enterprise или WPA3-Enterprise, в которых применяется метод аутентификации 802.1X (например, EAP-TLS).

При использовании WPA2-Enterprise или WPA3-Enterprise аутентификация обычно осуществляется с помощью так называемого сервера RADIUS, который часто подключен к службе каталогов (LDAP/Active Directory). Для того чтобы клиенты и серверы RADIUS могли безопасно идентифицировать друг друга, используются сертификаты.

2.5.4.5 Сертификаты LDAPS

Серверы LDAP (Lightweight Directory Access Protocol) используют сертификаты для защиты связи с клиентами или другими службами. Серверы LDAP часто отвечают за централизованное управление пользователями и правами. Если соединение не защищено, конфиденциальные данные пользователей (например, пароли, информация о группах или ролях) могут быть перехвачены или подвергнуты манипуляциям.

Поскольку сервер LDAP взаимодействует через LDAPS (LDAP через SSL/TLS), соединение шифруется. Кроме того, клиент использует сертификат сервера для проверки подлинности сервера LDAP. Поэтому сертификат сервера LDAPS должен храниться на устройстве.

2.5.5 Защищенные сетевые соединения с помощью SSL/TLS

Протоколы безопасности, такие как SSL (Secure Sockets Layer) и TLS (Transport Layer Security), используются для безопасной передачи данных. Они определяют, как должны использоваться алгоритмы шифрования и аутентификации, чтобы обеспечить соединение, защищенное от перехвата и манипуляций.

SSL - это старая стандартная технология безопасности, которая устанавливает зашифрованное соединение между сервером и клиентом. В случае с балансом (например, Cubis MCA) это может быть зашифрованная связь с веб-браузером, который обращается к веб-сайту устройства. В то же время SSL была заменена технологией TLS (Transport Layer Security) в качестве преемника. Однако, поскольку SSL является более известным термином, TLS/SSL используется в отношении сертификатов или защиты передаваемых данных, даже если в фоновом режиме используется только TLS. В настоящее время баланс поддерживает TLS до версии 1.3.

2.5.5.1 Неизвестные центры сертификации

Устройство также предлагает возможность доверять сертификатам, которые не были выпущены известным центром сертификации. Если эта опция активирована, устройство принимает такие сертификаты без проверки их достоверности по цепочке сертификатов. Это может быть полезно в тестовых средах или средах разработки, но представляет собой риск для безопасности при использовании в промышленных целях, поскольку подлинность и надежность используемых сертификатов не гарантируется.

Эту опцию можно активировать в разделе Сертификаты, Системные сертификаты, [Доверять неизвестным центрам сертификации].

3 Примеры применения

Примеры применения относятся к версии MCA, начиная с пакета 09-03-04.01.xx и далее, вместе с параметрами настройки и функциональными возможностями, которые она содержит. Для настройки

сетевых соединений, коннекторы и интерфейсы требуются соответствующие права пользователя.

Для настройки интерфейса Ethernet и Wi-Fi необходимы базовые знания о сетях на базе TCP/IP и сетевых технологиях в целом.

Необходимым условием для всех примеров является подключение весов к сети через Ethernet (LAN) или Wi-Fi (WLAN).

3.1 Отчет о настройках меню на файловом сервере Windows

Этот пример описывает конфигурацию и использование весов MCA таким образом, чтобы файл отчета со всеми настройками весов можно было экспортировать из меню [Настройки] в формате PDF, через коннектор [Файловый сервер Windows] с использованием сетевого протокола SMB, в целевой каталог разрешенного сетевого диска.

Для передачи файлов по протоколу SMB требуется расширение QAPP [Connection to Windows file server] из пакета [Connectivity]. Расширение можно использовать бесплатно в течение 30 дней, после чего его необходимо лицензировать.

Разрешенный диск с протоколом SMB в вашей сети является обязательным требованием для данного приложения.

Поэтому это приложение можно использовать для централизованного хранения настроек меню всех подключенных к сети балансов MCA.

3.1.1 Настройка

Этапы настройки:

1. Активируйте расширение QAPP [Connection to Windows File Server], если это еще не было сделано.
 - a. Откройте меню [Управление задачами], а затем [QAPP Center].
 - b. Выберите пакет программного обеспечения [Connectivity], а в нем - QAPP [Connection to Windows File Server]. Появится описание и версия QAPP.
 - c. Используйте кнопку [Лицензия] для активации данного QAPP; на экране появится информация о заказе и лицензии.
 - d. Если этот QAPP не был заказан как [заводская лицензия], запустите тестовую версию или введите код лицензии, который вы приобрели для этого QAPP.
2. Настройте подключение к файловому серверу Windows, например, [Мой SMB-сервер для настроек].
 - a. Откройте меню [Настройки].
 - b. Перейдите в [Подключения] -> [Коннекторы] -> [SMB].
 - c. Используйте кнопку [+], чтобы активировать создание нового коннектора.
 - d. Присвойте уникальное имя этому разъему.
 - e. Введите сетевой путь для Host и Share, убедившись, что вы используете правильное написание [//Host name/Share name].
 - f. Также введите имя подкаталога на сервере, в котором будут сохранены файлы.
 - g. Введите имя пользователя и пароль для доступа к авторизованному диску в вашей сети. Обратите внимание на правильность обозначений и здесь, в частности, на заглавные/прописные буквы.

3.1.2 Приложение

Шаги пользователя:

1. В главном меню с помощью кнопки [Setup] откройте меню настроек весов.
2. Нажмите кнопку [Экспорт] на панели навигации и инструментов.
3. Отображается список коннекторов, через которые можно экспортировать файл отчета.
4. Выберите созданный коннектор, например, [Мой SMB-сервер для настроек]. Файл отчета создается и экспортируется на SMB-сервер через коннектор.
5. В качестве подтверждения успешного экспорта вы получаете сообщения [Отчет отправлен] и [Процесс завершен]. Файл отчета в формате PDF с соответствующим файлом проверки теперь находится на сервере и может быть просмотрен.
6. Если файл отчета не удалось экспортировать, то этот файл не потерян, см. раздел Устранение неполадок.

Примечание: Формат файлов PDF - это независимый от платформы формат данных для документов. Распечатки в этом формате можно просматривать на каждом компьютере. Для каждого выходного файла PDF создается соответствующий тестовый файл, содержащий контрольную сумму (хэш-значение MD5) данных PDF. Когда файл передается, эта контрольная сумма сохраняется в журнале аудита. С помощью

соответствующего инструмента этот PDF-файл можно сравнить с контрольным файлом, чтобы убедиться в целостности PDF-данных.

3.1.3 Устранение неполадок

Нет файла отчета, экспортированного в каталог файлового сервера SMB.

1. Убедитесь, что все шаги по настройке, упомянутые выше, были выполнены.
2. Убедитесь, что весы подключены к сети, например, через кабель Ethernet. IP-адрес весов в сети должен отображаться в [Status center] в разделе [Device information].
3. Проверьте сетевой путь в коннекторе и правильность написания Host и Share, а также имя пользователя и пароль для прав доступа к файловому серверу SMB.
4. Проверьте соединение коннекторов с файловым сервером SMB, активировав кнопку [Info] в обзоре установленных значений. Если все настройки верны и файловый сервер SMB доступен, вы получите сообщение о том, что коннектор доступен.
5. Если нет, то проверьте, что файловый сервер SMB присутствует в сети и что файл может быть сохранен там с вашего ПК.
6. Если появляется сообщение об ошибке [Transfer failure], то с экспортом можно поступить следующим образом:
 - a. Повторить: Повторная попытка экспорта файла отчета на сетевой сервер.
 - b. Повторить позже: Экспорт файла отчета повторяется автоматически. Незавершенные передачи отображаются в [Центре состояния] в разделе [Сообщения].
 - c. Перенаправление: Вы можете перенаправить файл отчета на другой коннектор.
 - d. Удалить: Экспорт файла отчета отменяется и удаляется.

3.2 Обновление QAPP Center на FTP-сервере

Этот пример описывает настройку и применение весов Cubis® MCA для загрузки обновления для QAPP Center с FTP-сервера.

Для передачи файлов с сетевого сервера FTP требуется расширение QAPP [Connection to FTP/FTPS] из пакета [Connectivity]. Расширение можно использовать бесплатно в течение 30 дней, после чего его также необходимо лицензировать.

Необходимым условием для этого приложения является соответствующим образом настроенный FTP-сервер в вашей сети.

Для сетевых балансов MCA это приложение позволяет обновлять QAPP Center из центрального источника.

3.2.1 Настройка

Этапы настройки:

1. Активируйте расширение QAPP [Подключение к FTP/FTPS], если это еще не было сделано.
 - a. Откройте меню [Управление задачами], а затем [QAPP Center].
 - b. Выберите пакет программного обеспечения [Connectivity], а в нем - QAPP [Connection to FTP/FTPS]. Отобразится описание и версия QAPP.
 - c. Используйте кнопку [Лицензия] для активации данного QAPP; на экране появится информация о заказе и лицензии.
 - d. Если этот QAPP не был заказан как [заводская лицензия], запустите тестовую версию или введите код лицензии, который вы приобрели для этого QAPP.
2. Установите соединение с FTP-сервером, например, [Мой FTP-сервер для обновления QAPP-центра].
 - a. Откройте меню [Настройки].
 - b. Перейдите в меню [Подключения] -> [Коннекторы] -> [FTP].
 - c. Используйте кнопку [+], чтобы активировать создание нового коннектора.
 - d. Присвойте уникальное имя этому коннектору.
 - e. Введите IP-адрес сетевого сервера, убедившись, что вы правильно его написали
 - f. Для подключения требуется номер порта: по умолчанию номер 21. При необходимости можно ввести другой номер порта.
 - g. Для обновления QAPP Center можно также указать подкаталог для файлов, хранящихся на сервере.
 - h. Введите имя пользователя и пароль для доступа к FTP-серверу. Обратите внимание на правильность обозначений, в частности, на верхний/нижний регистр букв.

3.2.2 Приложение

Шаги пользователя:

1. В главном меню с помощью кнопки [Setup] откройте меню настроек весов.
2. Перейдите к пункту меню [Обслуживание устройства] -> [Установить QAPP Center]. Отображается список соединителей, с помощью которых можно загрузить пакет для обновления QAPP Center.
3. Выберите созданный вами соединитель, например, [Мой FTP-сервер для обновления QAPP-центра]. Будет установлено соединение с FTP-сервером и отображен список доступных пакетов для обновления QAPP-центра.
4. Выберите нужную версию QAPP Center и подтвердите сообщение об обновлении.
5. Теперь QAPP-центр скопирован в весы с FTP-сервера и обновлен. В качестве подтверждения отображается обновленная версия QAPP-центра.
6. См. раздел Устранение неполадок, если обновление не удалось выполнить.

3.2.3 Устранение неполадок

Обновление QAPP Center невозможно через коннектор.

1. Убедитесь, что все шаги по настройке, упомянутые выше, были выполнены.
2. Убедитесь, что весы подключены к сети, например, через кабель Ethernet. IP-адрес весов в сети должен отображаться в [Status center] в разделе [Device information].
3. Проверьте IP-адрес и номер порта FTP-сервера, а также имя пользователя и пароль для прав доступа к серверу в коннекторе.
4. Проверьте соединение коннекторов с FTP-сервером, активировав кнопку [Info] в обзоре установленных значений. Если все настройки верны и FTP-сервер доступен, вы получите сообщение о том, что коннектор доступен.
5. Проверьте с помощью компьютера, присутствует ли указанный подкаталог, а также файл для обновления QAPP Center на FTP-сервере в сети.

3.3 Просмотр записей журнала аудита через веб-браузер

Этот пример описывает настройку и использование весов MCA, чтобы записи в журнале аудита весов можно было просматривать с помощью веб-браузера.

Для дистанционного управления весами MCA рекомендуется использовать веб-браузер [Chrome].

Безопасное соединение весов с браузером по протоколу HTTPS требует наличия определенных сертификатов устройства.

Для этого весы MCA предоставляют для загрузки собственные сертификаты устройства. Эти сертификаты устройства должны быть импортированы в браузер для безопасного удаленного доступа к веб-сайту устройства. Существует отдельное описание на тему [Сертификаты].

Полный объем аудиторского следа можно использовать только после активации расширения QAPP [Audit trail] в QAPP Center в разделе [Pharma (QP1)].

Одним из вариантов использования данного приложения является, например, централизованный удаленный контроль настроек на всех балансах MCA, объединенных в сеть.

3.3.1 Настройка

Этапы настройки:

1. Активируйте расширение [Audit trail] QAPP, если это еще не сделано.
 - a. Откройте меню [Управление задачами], а затем [QAPP Center].
 - b. Выберите пакет программного обеспечения [Pharma] и QAPP [Audit trail] в нем. Появится описание и версия QAPP.
 - c. Используйте кнопку [Лицензия] для активации данного QAPP; на экране появится информация о заказе и лицензии.
 - d. Если этот QAPP не был заказан как [заводская лицензия], запустите тестовую версию или введите код лицензии, который вы приобрели для этого QAPP.
2. Активируйте веб-сайт весов MCA, если это еще не сделано.
 - a. Откройте меню [Настройки].
 - b. Перейдите в [Подключения] -> [Веб-сайт / веб-службы].
 - c. Установите для пункта меню [Доступ к веб-сайту] значение [Включено, без аутентификации].
3. При необходимости активируйте удаленный доступ к сайту весов MCA.
 - a. Откройте меню [Настройки].

- b. Перейдите в [Подключения] -> [Веб-сайт / веб-службы].
- c. В пункте меню [Удаленный доступ] выберите настройку [Просмотр и дистанционное управление].

3.3.2 Приложение

Шаги пользователя:

1. Запустите веб-браузер, например, [Chrome] на вашем ПК.
2. Введите IP-адрес ваших весов, который отображается в [Центре состояния] в разделе [Информация об устройстве].
3. Если вы еще не импортировали сертификаты устройств весов в браузер, в браузере появится сообщение [Это не безопасное соединение].
4. С помощью кнопки [Дополнительно] и ссылки [Далее...] можно перейти к IP-адресу весов, который в данном случае рассматривается как небезопасный, иначе необходимо сначала импортировать сертификаты устройства ваших весов в браузер. По теме [Сертификаты] есть отдельное описание.
5. В противном случае в браузере отображается страница [My Cubis] (главная страница).
6. Выберите страницу [Audit trail] для примера.
7. Теперь вы можете сортировать список записей по ID, метке времени и пользователю.
8. Список записей можно отобразить в порядке возрастания или убывания.
9. Вы также можете установить фильтры, чтобы просматривать только определенные группы записей.

3.3.3 Устранение неполадок

Главная страница весов не отображается в браузере.

1. Убедитесь, что весы подключены к сети, например, через кабель Ethernet. IP-адрес весов в сети должен отображаться в [Status center] в разделе [Device information].
2. Убедитесь, что для пункта меню [Доступ к веб-сайту] установлено значение [Включено].

В браузере соединение с весами отображается как [Unsecure].

1. Импортируйте сертификаты устройства весов в браузер. Существует отдельное описание на тему [Сертификаты].

Страница [Audit trail] не может быть выбрана на главной странице весов.

1. Убедитесь, что все шаги по настройке, упомянутые выше, были выполнены. В частности, расширение QAPP [Audit trail] было активировано, и лицензия на него все еще действительна.

3.4 Синхронизация даты и времени с сервером NTP

Этот пример описывает настройку и применение Cubis® MCA, чтобы включить синхронизацию даты и времени весов с NTP-сервером.

Необходимым условием для такого использования является доступ к серверу NTP в сети вашей компании или в публичной сети.

Отклонение времени между весами и NTP-сервером проверяется каждые 10 минут. Если отклонение составляет более 3 секунд, время в весах корректируется, и изменение вносится в журнал аудита.

Это приложение позволяет легко автоматически обновлять и синхронизировать дату и время на всех сетевых балансах MCA.

3.4.1 Настройка

Этапы настройки:

1. Установите активную конфигурацию NTP.
 - a. Откройте меню [Настройки].
 - b. Перейдите в [Настройки устройства] -> [Дата и время] -> [Настройка NTP].
 - c. Активируйте настройку параметров сервера NTP с помощью кнопки [Edit].
 - d. Установите для пункта меню [Состояние работы NTP] значение [Включено].
 - e. Через [Server IP] введите адрес NTP-сервера в формате IPv4, например, 192.53.103.108. (Это NTP-сервер Физико-технического федерального института в Брауншвейге, Германия).
 - f. Подтвердите конфигурацию NTP кнопкой [OK].
 - g. Проверьте подключение к серверу NTP, активировав кнопку [Info] в обзоре конфигурации NTP.
2. Установите правильный часовой пояс для вашего местоположения.
 - a. Откройте меню [Настройки].

- b. Перейдите к [Настройки устройства] -> [Дата и время] -> [Установить дату и время].
 - c. Активируйте настройки даты и времени с помощью кнопки [Edit].
 - d. Установите свое местоположение с помощью пункта меню [Часовой пояс], [UTC +/- время, место].
- После этого время и дата будут отображаться в соответствии с местным временем.

Примечание: После установки даты, времени и часового пояса весы MCA попросят вас перезагрузить систему.

3.4.2 Устранение неполадок

Нет возможности подключения к серверу NTP.

1. Убедитесь, что все шаги по настройке, упомянутые выше, были выполнены.
2. Убедитесь, что весы подключены к сети, например, через кабель Ethernet. IP-адрес весов в сети должен отображаться в [Status center] в разделе [Device information].
3. Проверьте с помощью компьютера, можете ли вы получить доступ к IP-адресу NTP-сервера.

4 Приложение

4.1 Поддерживаемые Wi-Fi адаптеры

Cubis® MCA поддерживает наиболее распространенные Wi-Fi адаптеры (USB WLAN-адаптеры), которые доступны на рынке.

При выборе адаптера Wi-Fi учитывайте следующие моменты:

1. Избегайте адаптеров Wi-Fi без названия. Всегда покупайте известный бренд.
2. Если возможно, проверьте спецификацию адаптера Wi-Fi, чтобы убедиться, что он содержит один из следующих поддерживаемых наборов микросхем.

Поддерживаются следующие наборы микросхем Wi-Fi:

- Atheros - AR5523, AR9271, AR6004
- Atmel - at76c503, at76c505 or at76c505a
- Broadcom - BCM43235 (Revision 3), BCM43236 (Revision 3), BCM43238 (Revision 3), BCM43143, BCM43242, BCM43566, BCM43569
- Intersil's Prism54 chips - ISL38xx
- Marvell - Libertas 8388, Libertas 8682, 8766/8797/8897
- Ralink - RT2571, RT2571W, RT2572, RT2573 & RT2671 (no firmware), RT2770, RT2870 & RT3070, RT3071 & RT3072 & RT3370 (rt2870.bin)
- Realtek - RTL8192CU/RTL8188CU, RTL8712U/RTL8192SU, RTL8188EU, RTL8187 and RTL8187B
- Redpine Signals Inc - 91x
- ZyDAS - ZD1201, ZD1211/ZD1211B

5. Сокращения

DHCP	Dynamic Host Configuration Protocol	Протокол связи в компьютерных технологиях. Он позволяет серверу распределять конфигурацию сети между клиентами.
DNS	Domain Name System	Система для преобразования имен компьютеров в IP-адреса и наоборот.
FTP	File Transfer Protocol	Стандартный сетевой протокол для передачи файлов между клиентом и сервером в сети.
FTPS	FTP over TLS	Метод шифрования протокола передачи файлов (FTP).
HTTPS	Hypertext Transfer Protocol Secure	Протокол связи, с помощью которого данные могут передаваться в зашифрованном виде.
IPv4	Internet Protocol version 4	Интернет-протокол версии 4.
IPv6	Internet Protocol version 6	Интернет-протокол версии 6.
MAC address	Media Access Control address	Физический аппаратный адрес, уникальный идентификатор устройства в сети.
NTP	Network Time Protocol	Стандарт для синхронизации часов в компьютерных системах.
PNG	Portable Network Graphics	Портативная сетевая графика, формат растровой графики со сжатием данных без потерь.
PSK	Pre-shared key	Метод шифрования, при котором ключ должен быть известен обоим участникам до начала общения.
REST	Representational State Transfer	Парадигма программирования для распределенных систем, в частности для веб-сервисов.
SMB	Server Message Block	Сетевой протокол для файловых, печатных и других серверных служб в компьютерных сетях.
SSID	Service Set Identifier	Свободно выбираемое имя сети, например, для Wi-Fi.
URL	Uniform Resource Locator	Идентификация для Интернета или веб-адресов.
UTC	Universal Time, Coordinated	Мировое время, также земное или универсальное время.
WEP	Wired Equivalent Privacy	Стандартные протоколы шифрования для WLAN.
Wi-Fi	Wireless Fidelity	Беспроводная сеть, синоним WLAN.
WLAN	Wireless Local Area Network	Беспроводная, локальная сеть.
WPA	Wi-Fi Protected Access	Методы шифрования для беспроводной сети. Преемник WEP.
WPA2	Wi-Fi Protected Access 2	Реализация стандарта безопасности для радиосетей. Преемник WPA.