MLink-WNET-C33R





Руководство пользователя



Версия: 1.2 Код документа: ML-WNET-C33R 25.1.7 Дата выпуска: май 2009г.

Микролинк-Связь

111395 г. Москва ул. Аллея Первой Маевки, д. 15, оф. 501. Тел./факс: 941-99-19 E-mail: <u>info@microlink.ru</u> Http:// <u>www.microlink.ru</u>

Оглавление

1 Введение	5
1.1 Комплектация	5
1.2 Техническая характеристика изделия	5
1.3 Свойства устройства	5
1.4 Описание модели (модель А)	6
1.5 Описание панели (модель В)	8
2 Установка	9
2.1 Установка оборудования	9
2.2 Ввод в действие системы программного обеспечения	9
3 Конфигурация	9
3.1 Подготовка вашего компьютера к настройке широкополосного WLAN маршрутизатора	10
3.2 Подключение к широкополосному WLAN маршрутизатору	12
3.3 Управление и настройка широкополосного WLAN маршрутизатора	12
3.3.1 Статус	12
3.3.2 Помощник настройки	13
3.3.3 Режим работы	15
3.3.4 Основные радио-настройки	16
3.3.5 Особые настройки радиосвязи	17
3.3.6 Настройки безопасности	19
3.3.7 Контроль доступа к радиосвязи	20
3.3.8 Настройки WDS	21
3.3.9 Обзор доступных сетей (Site survey)	23
3.3.10 Настройка LAN-интерфейса	24
3.3.11 Настройка WAN-интерфейса	25
3.3.12 Firewall – фильтрация на порту	29
3.3.13 Firewall – IP фильтрация	29
3.3.14 Firewall – MAC фильтрация	30
3.3.15 Firewall - переадресация портов	31
3.3.16 Firewall – URL фильтрация	32
3.3.17 Firewall - DMZ	32
3.3.18 Настройки VPN	33
3.3.19 Управления - статистика	36
3.3.20 Управление - DDNS	36
3.3.21 Управление – настройка часового пояса	37
3.3.22 Управление – отказ от обслуживания	38
3.3.23 Управление – журнал регистрации	
3.3.24 Управление – обновление прошивки	39
3.3.25 Управление – сохранение/перезагрузка настроек	40
3.3.26 Управление – настройка пароля	40
3.3.27 Управление – WatchDog (сторожевое устройство)	41
3.3.28 Управление – Quality of Service (качество сервиса)	41
4 Часто задаваемые вопросы (FAQ)	42
4.1 Где и как найти IP и MAC адрес моего компьютера?	42
4.2 Что такое Wireless LAN?	43
4.3 Что такое ISM полосы?	43
4.4 Как работает беспроводная сеть?	43
4.5 Что такое BSSID?	43
4.6 Что такое ESSID?	44
4.7 Каковы причины возникновения помех?	44
4.8 Что такое Open System и аутентификации Shared Key?	44
4.9 Что такое WEP?	44
4.10 Что такое Fragment Threshold?	45
4.11 Что такое порог RTS (Request To Send)?	45
4.12 Что такое Beacon Interval?	46
4.13 Что такое тип преамбулы?	46
4.14 Что такое широковещательная передача SSID?	46
4.15 Что такое Wi-Fi Protected Access (WPA)?	46
4.16 Что такое WPA2?	47

4.17 Что такое аутентификация 802.1х?	47
4.18 Что такое Temporal Key Integrity Protocol (TKIP)?	47
4.19 Что такое Advanced Encryption Standard (AES)?	47
4.20 Что такое Inter-Access Point Protocol (IAPP)?	47
4.21 Что такое Wireless Distribution System (WDS)?	48
4.22 Что такое Universal Plug and Play (uPNP)?	48
4.23 Что такое размер Maximum Transmission Unit (MTU)?	48
4.24 Что такое клонирование МАС адреса?	48
4.25 Что такое DDNS?	48
4.26 Что такое NTP-клиент?	48
4.27 Что такое VPN?	49
4.28 Что такое IPSEC?	49
4.29 Что такое WLAN реле блокировки между клиентами?	49
4.30 Что такое WMM?	49
4.31 Что такое WLAN ACK TIMOUT?	49
5 Примеры настроек	50
5.1 Пример первый — РРРоЕ на WAN	50
5.2 Пример второй – фиксированный IP адрес на WAN	52

Аббревиатуры

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
ССК	Complementary Code Keying
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/ Collision Detection
DDNS	Dynamic Domain Name Server
DH	Diffie-Hellman Algorithm
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
MAC	Media Access Control
MD5	Message Digest 5
NAT	Network Address Translation
NT	Network Termination
NTP	Network Time Protocol
PPTP	Point to Point Tunneling Protocol
PSD	Power Spectral Density
RF	Radio Frequency
SHA1	Secure Hash Algorithm
SNR	Signal to Noise Ratio
SSID	Service Set Identification
5510	TCP Transmission Control Protocol
ТСР	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UPNP	Universal Plug and Play
VPN	Virtual Private Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 Введение

Беспроводной широкополосный LAN маршрутизатор – это доступное по цене решение для стандарта IEEE 802.11b/g, устанавливающее стандарты высокой производительности для малых офисов и предприятий, безопасную, управляемую и надёжную беспроводную локальную сеть.

В данном документе описаны шаги по настройке WLAN маршрутизатора.

1.1 Комплектация

В комплектацию широкополосного WLAN маршрутизатора входят следующие элементы: широкополосный WLAN маршрутизатор, AC/DC адаптер питания, CD с документацией.

1.2 Техническая характеристика изделия

Название устройства	WLAN широкополосный маршрутизатор
Стандарты	802.11b/g(Wireless), 802.3(10BaseT), 802.3u(100BaseT)
Скорость передачи данных	54Мб/сек (Wireless), 100Мб/сек (Ethernet)
Метод модуляции	CCK(802.11b), OFDM(802.11g)
Полоса частот	2.4ГГц – 2.497ГГц ISM, DSSS
RF выходная мощность	CCK<17 dBm, OFDM<13.5 dBm
Чувствительность приёмника	802.11b -80 dBm, 802.11g -68 dBm
Зона покрытия	от 30 до 280 метров
Антенна	Внешняя съемная антенна
Индикаторы	Power, Active (WLAN/Ethernet)
Безопасность	64-битное/128-битное WEP-шифрование, WPA, WPA2, фильтрация на порту, фильтрация по IP, фильтрация по MAC, переадресация (перенаправление) портов и DMZ.
LAN интерфейс	1 (WAN), 4 (LAN) , 10/100BaseT, RJ45
Потребляемая мощность	7.5B DC адаптер источника питания
Рабочие температуры	0 ~ 50°С: температура окружающей среды
Температуры хранения	-20 ~ 70°С: температура окружающей среды
Влажность	от 5 до 90 % максимум (без конденсации)
Размеры	118х95х25мм (модель A) 120х75х26мм (модель B)

1.3 Свойства устройства

- ✓ Взаимодействие со стандартом IEEE 802.11b/g для 2.4 ГГц WLAN;
- ✓ Поддержка многооперационных режимов (bridge/gateway/WISP) между беспроводными и проводными Ethernet интерфейсами;
- ✓ 64/128-битное WEP-, WPA-, WPA2- шифрование для защиты передачи данных по радиосвязи;
- ✓ Поддержка аутентификации IEEE 802.1х;

- ✓ Поддержка защищённого метода аутентификации Wi-Fi с использованием RADIUS сервера и режима Pre-Shared Key;
- ✓ Поддержка протокола IAPP (Inter-Access Point Protocol);
- ✓ Поддержка WDS (Wireless Distribution System);
- ✓ Поддержка IEEE 802.3x full duplex flow control на интерфейсе 10/100М;
- ✓ Поддержка DHCP-сервера для автоматического назначения IP адреса клиенту;
- Поддержка DHCP-клиента для автоматического назначения IP адреса от провайдера WAN-интерфейсе;
- ✓ Поддержка РРРоЕ на WAN-интерфейсе;
- ✓ Поддержка РРТР- клиента на WAN-интерфейсе;
- Поддержка функции клонирования МАС адресов;
- Поддержка безопасного брандмауэра с использованием: фильтрации на порту, IP фильтрации, MAC фильтрации, перенаправлением портов, trigger port, DMZ и функции фильтрации URL;
- Поддержка веб-интерфейса для настройки и конфигурации;
- ✓ Поддержка UPnP для автоматического доступа к Интернет;
- ✓ Поддержка DDNS;
- ✓ Поддержка сервисов NTP-клиента;
- Поддержка таблицы логов и службы удалённых логов;
- Поддержка установки в режиме помощника;
- Поддержка функции DoS (Denial of Service);
- Поддержка функции WMM;
- ✓ Поддержка Ping watchdog;
- Поддержка функции контроля QoS/Bandwidth;
- ✓ Поддержка соединения VPN;
- ✓ Поддержка шифрования IPSEC (3DES/AES128) и аутентификации (MD5/SHA1);
- 1.4 Описание модели (модель А)



Индикаторы	Статус	Описание
Индикатор питания	Вкл.	WLAN маршрутизатор включен
	Выкл.	WLAN маршрутизатор выключен
Индикатор WLAN	Мигание	Антенна принимает или передаёт данные
	Выкл.	Антенна не принимает и не передаёт данные
Индикатор LAN	Мигание	Данные принимаются или передаются на LAN- интерфейсе
	Вкл.	Порт активен
	Выкл.	Нет активности
Индикатор WAN	Мигание	Данные принимаются или передаются на WAN- интерфейсе
	Вкл.	Порт активен
	Выкл.	Нет активности

Описание состояния индикаторов



Описание интерфейсов

- Antenna WLAN антенна (съемная/ разъем SMA);
- Power Разъем питания DC +7.5;
- LAN Гнёзда RJ-45 обеспечивают LAN-подключение с помощью кабелей UTP 5-й категории. Поддержка авто-определения скорости 10/100M в режиме полного дуплекса и полудуплекса; совместимость с IEEE 802.3/802.3u;
- WAN Гнёзда RJ-45 обеспечивают WAN-подключение с помощью кабелей UTP 5-й категории. Поддержка авто-определения на скорости 10/100М в режиме полного дуплекса и полудуплекса; совместимость с IEEE 802.3/802.3u;

1.5 Описание панели (модель В)



Описание состояния индикаторов

Индикаторы	Статус	Описание
Индикатор питания	Вкл.	WLAN маршрутизатор включен
	Выкл.	WLAN маршрутизатор выключен
Индикатор WLAN	Мигание	Антенна принимает или передаёт данные
	Выкл.	Антенна не принимает и не передаёт данные
Инликатор LAN	Мигание	Данные принимаются или передаются на LAN- интерфейсе
,, 1	Выкл.	Нет активности
10/100 M	Вкл.	Скорость подключения на LAN-интерфейсе составляет 100 Мбит/сек
	Выкл.	Скорость подключения на LAN-интерфейсе составляет 10 Мбит/сек
Инликатор WAN	Мигание	Данные принимаются или передаются на WAN- интерфейсе
	Выкл.	Нет активности
10/100 M	Вкл.	Скорость подключения на WAN-интерфейсе составляет 100 Мбит/сек
	Выкл	Скорость подключения на WAN-интерфейсе составляет 10 Мбит/сек



Описание интерфейсов

- Антенна Антенна WLAN;
- WAN Гнёзда RJ-45 обеспечивают WAN-подключение с помощью кабелей UTP 5-й категории. Поддержка авто-определения на скорости 10/100М в режиме полного дуплекса и полудуплекса; совместимость с IEEE 802.3/802.3u;
- LAN Гнёзда RJ-45 обеспечивают LAN-подключение с помощью кабелей UTP 5-й категории. Поддержка авто-определения на скорости 10/100М в

режиме полного дуплекса и полудуплекса; совместимость с IEEE 802.3/802.3u;

Power - Разъем питания DC +7.5;

2 Установка

2.1 Установка оборудования

Шаг 1: Расположите широкополосный WLAN маршрутизатор для оптимальной передачи данных. Обычно, лучшее положение широкополосного WLAN маршрутизатора для передачи это центр вашей беспроводной сети с прямой видимостью для всех ваших мобильных станций.

Шаг 2: Подключите широкополосный WLAN маршрутизатор к вашей проводной сети. Подключите WAN-интерфейс Ethernet-кабелем 5-й категории к вашему коммутатору/хабу/хDSL-модему или кабельному модему. Требуется прямой Etrhernet-кабель.

Шаг 3: Подайте DC-питание на широкополосный WLAN-маршрутизатор. Используйте только AC/DC источник питания, поддерживаемый этим маршрутизатором; использование альтернативного источника питания может повредить устройство.

Установка оборудования закончена.

2.2 Ввод в действие системы программного обеспечения

Не требуется установка никаких драйверов, пэтчей и утилит, только установка конфигурации. Пожалуйста, обратитесь к главе 3 для получения детальной информации о настройке конфигурации.

ВНИМАНИЕ: Загрузка широкополосного WLAN маршрутизатора занимает около 55 секунд после включения устройства; индикатор питания будет включен, и затем замигает индикатор WLAN Activity, как признак того, что WLAN-интерфейс включен и работает нормально.

3 Конфигурация

Для упрощения вашей работы существуют веб-интерфейс.

Широкополосный WLAN маршрутизатор оснащён следующими заводскими параметрами на LAN-интерфейсах. IP адрес по умолчанию: **192.168.1.254**. Маска подсети по умолчанию: **255.255.255.0**.

Логин: <**пусто**>. Пароль: <**пусто**>.

3.1 Подготовка вашего компьютера к настройке широкополосного WLAN маршрутизатора

Для OC Microsoft Windows 95/98/Ме:

- Нажмите кнопку Start (Пуск) и выберите Settings (Параметры), затем кликните по Control Panel (Панель управления). После этого появится окно Control Panel. Внимание: Пользователи Windows ME могут не обнаружить Контрольную панель. Если так и случилось, нажмите View all Control Panel options на левой стороне окна.
- 2. Кликните два раза правой кнопкой мыши по иконе **Network**. Появится окно **Network**.
- Проверьте список установленных компонентов Network Components. Если не установлен TCP/IP, кликните по Add (Добавить), для установки; в противном случае перейдите к пункту 6.
- Выберите *Protocol* в диалоговом окне *Network Component Type* и кликните по *Add.*
- 5. Выберите TCP/IP в диалоговом окне Microsoft Select Network Protocol и затем кликните ОК для установки протокола TCP/IP, возможно, вам понадобится установочный диск Microsoft Windows CD для завершения установки. Закройте это окно и перейдите вновь к диалоговому окну Network после установки TCP/IP.
- 6. Выберите *TCP/IP* и кликните по опции *Properties (Свойства)* в диалоговом окне *Network.*
- Выберите Specify an IP address (Установка IP-адреса) и введите данные как показано в следующем примере: IP адрес: 192.168.1.1, Любой IP адрес из диапазона 192.168.1.1 - 192.168.1.253 подойдёт для подключения WLAN точки доступа. Маска подсети: 255.255.255.0.
- Нажмите ОК для перезагрузки вашего компьютера после завершения установки IP параметров.

Для OC Microsoft Windows 2000, XP:

- 1. Нажмите кнопку *Start* и выберите *Settings*, затем кликните по *Control Panel*. После этого появится окно *Control Panel*.
- 2. Кликните два раза правой кнопкой мыши по иконе Network and Dial-up Connections. Появится окно Local Area Connection. Кликните по кнопке Properties в окне Local Area Connection.

- 3. Проверьте список установленных компонентов *Network Components.* Если не установлен TCP/IP, кликните по *Add*, для установки; в противном случае перейдите к пункту 6.
- 4. Выберите *Protocol* в диалоговом окне *Network Component Type* и кликните по *Add.*
- 5. Выберите TCP/IP в диалоговом окне Microsoft Select Network Protocol и затем кликните OK для установки протокола TCP/IP, возможно, вам понадобится установочный диск Microsoft Windows CD для завершения установки. Закройте это окно и перейдите вновь к диалоговому окну Network после установки TCP/IP.
- 6. Выберите *TCP/IP* и кликните по опции *Properties* в диалоговом окне *Network.*
- Выберите Specify an IP address и введите данные как показано в следующем примере: IP адрес: 192.168.1.1, Любой IP адрес из диапазона 192.168.1.1 - 192.168.1.253 подойдёт для подключения WLAN точки доступа. Маска подсети: 255.255.255.0.
- Нажмите ОК для перезагрузки вашего компьютера после завершения установки IP параметров.

<u>Для OC Microsoft Windows NT:</u>

- 1. Нажмите кнопку *Start* и выберите *Settings*, затем кликните по *Control Panel*. После этого появится окно *Control Panel*.
- 2. Кликните два раза правой кнопкой мыши по иконе **Network**. Появится окно **Network**. Кликните по **Protocol** в окне **Network**.
- Проверьте список установленных компонентов Network Components. Если не установлен TCP/IP, кликните по Add, для установки; в противном случае перейдите к пункту 6.
- Выберите *Protocol* в диалоговом окне *Network Component Type* и кликните по *Add.*
- 5. Выберите TCP/IP в диалоговом окне Microsoft Select Network Protocol и затем кликните ОК для установки протокола TCP/IP, возможно, вам понадобится установочный диск Microsoft Windows CD для завершения установки. Закройте это окно и перейдите вновь к диалоговому окну Network после установки TCP/IP.
- 6. Выберите *TCP/IP* и кликните по опции *Properties* в диалоговом окне *Network.*

- Выберите Specify an IP address и введите данные как показано в следующем примере: IP адрес: 192.168.1.1, Любой IP адрес из диапазона 192.168.1.1 - 192.168.1.253 подойдёт для подключения WLAN точки доступа. Маска подсети: 255.255.255.0.
- Нажмите ОК для перезагрузки вашего компьютера после завершения установки IP параметров.

3.2 Подключение к широкополосному WLAN маршрутизатору

Откройте веб-браузер, например Microsoft Internet Explorer, затем введите 192.168.1.254 в поле URL для подключения к широкополосному WLAN маршрутизатору.

3.3 Управление и настройка широкополосного WLAN маршрутизатора

3.3.1 Статус

На этой странице отображен текущий статус и некоторые основные настройки устройства, включая настройки системы, радиосвязи, информацию о настройке интерфейсов Ethernet LAN и WAN.

Окно статуса маршрутизатора:

	CL I
Broadband Rout	er Status
This page shows the current stat	tus and some basic settings of the device.
Suctem	
Untime	Ddaw0h-2m-32s
Firmware Version	v1 4 2
Wireless Configuration	¥1.7.2
Mode	AP
Band	2.4.0Hz/B+0
SSID	MyWLAN
Channel Number	11
Encryption	Disabled
BSSID	00:0e:8e:b9:16:89
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:0e:8e:b9:16:89
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server
IP Address	0.0.0
Subnet Mask	0.0.0
Default Gateway	0.0.0
DNS 1	0.0.0
DNS 2	0.0.0
DNS 3	0.0.0
MAC Address	00:0e:8e:b9:16:8a

Наиманорания	Описание		
Паимспование	Surface States		
Untimo	System		
Einer Venier	Показывает время работы широкополосного WLAN маршрутизатора		
Firmware Version	Показывает версию прошивки широкополосного WLAN маршрутизатора		
	Wireless Configuration		
Mode	Показывает режим работы радиосвязи		
Band	Показывает текущую рабочую частоту радиосвязи		
	Показывает SSID широкополосного WLAN маршрутизатора. SSID – это		
SSID	уникальное имя широкополосного WLAN маршрутизатора, транслируемое на		
5512	зоне уверенного радиоприёма таким образом, что все устройства,		
	присоединяющиеся к той же беспроводной сети, определяют его.		
Channel Number	Показывает настоящий номер канала, по которому работает радиосвязь		
Encryption	Показывает статус функции шифрования		
DECID	Показывает адрес BSSID широкополосного WLAN маршрутизатора. BSSID –		
BSSID	это 6-байтоввый адрес		
Associated Clients	Показывает количество подключенных клиентов (или станций, компьютеров)		
	TCP/IP Configuration		
Attain IP address	Показывает тип подключения		
	Показывает IP адрес LAN-интерфейса широкополосного WLAN		
IP Address	маршрутизатора		
	Показывает маску подсети LAN-интерфейса широкополосного WLAN		
Subnet Mask	маршрутизатора		
	Показывает шлюз по умолчанию для исходящих пакетов данных LAN-		
Default Gateway	интерфейса		
DHCP Server	Показывает, включен ли DHCP сервер		
N(4,C, 4, 1)	Показывает МАС адрес LAN-интерфейса широкополосного WLAN		
MAC Address	маршрутизатора		
WAN Configuration			
	Показывает, как широкополосный WLAN маршрутизатор получает IP алрес.		
Attain IP Protocol	IP алрес может быть установлен вручную, получен автоматически от DHCP		
	сервера или получен по РРРоЕ/РРТР полключению		
	Показывает IP адрес WAN-интерфейса широкополосного WLAN		
IP address	маршрутизатора		
Subnet Mask	Показывает маску полсети широкополосного WLAN маршрутизатора		
DNS1/DNS2/DNS3	Показывает информацию о DNS сервере		
U101/U102/U103	показывает информацию о DNS сервере		

3.3.2 Помощник настройки

Эта страница поможет вам настроить широкополосный маршрутизатор при

первом подключении.

The s	The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by	
step.	step.	
Welco	nme to Setup Wizard.	
The V	vizard will guide you the through following steps. Begin by clicking on Next.	
1.	Setup Operation Mode	
2.	Choose your Time Zone	
3.	Setup LAN Interface	
4.	Setup WAN Interface	
5.	Wireless LAN Setting	
6.	Wireless Security Setting	

Operation Mode

Эта страница следует за страницей Setup Wizard и показывает возможность выбора режима работы:

1 Operatio	n Modo
1. Operatio	n wode
You can setup differer	nt modes to LAN and WLAN interface for NAT and bridging function.
⊙ Gateway:	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
🔘 Bridge:	In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
○ Wireless ISP:	In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
	Cancel < <back next="">></back>

Time Zone Setting

На этой странице включается и настраивается NTP-клиент.

2. Time Zone Setting		
You can maintain the syster	n time by synchronizing with a public time server over the Internet.	
💌 Enable NTP client upda	te	
Time Zone Select :	(GMT+03:00)Moscow, St. Petersburg, Volgograd	
NTP server :	130.149.17.8 - Europe	
	Cancel < <back next="">></back>	

LAN Interface Setup

На этой странице настраивается IP адрес локальный сети и маска подсети:

3. LAN Interface Setup	
This page is used to cor Access Point. Here you	figure the parameters for local area network which connects to the LAN port of your nay change the setting for IP addresss, subnet mask, DHCP, etc
IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
bnet Mask:	255.255.255.0
	Cancel < <back next="">></back>

WAN Interface Setup

На этой странице тип доступа по WAN-интерфейсу:

4. WAN Inter	face Setup		
This page is used to config Access Point. Here you ma value of WAN Access typ	gure the parameters for Internet ne by change the access method to st e.	twork which connects to the WAN port of yo atic IP, DHCP, PPPoE or PPTP by click the ite	m
WAN Access Type:	DHCP Client Static IP DHCP Client PPPoE PPTP		
		Cancel < <back< td=""><td>Next></td></back<>	Next >

Wireless Basic Settings

На этой странице настраиваются основные параметры радиосвязи: полоса частот, режим, тип SSID, номер канала, клонирование MAC адресов (Single Ethernet Client).

5. Wireless H	Basic Settings		
This page is used to con Point.	ifigure the parameters for wireless LAN clients which may connect to your Access		
Band:	2.4 GHz (B+G) 👻		
Mode:			
Network Type:	Infrastructure 💌		
SSID:	MyWLAN		
Channel Number:	11 💌		
Enable Mac Clone (Single Ethernet Client)			
	Cancel < <back next="">></back>		

Wireless Security Setup

На этой странице настраивается безопасность радиосвязи.

6. Wireless Se	curity Setup
This page allows you setu prevent any unauthorized	o the wireless security. Turn on WEP or WPA by using Encryption Keys could access to your wireless network.
Encryption: None	×
	Cancel <-Back Finished

3.3.3 Режим работы

На этой странице настраивается режим работы широкополосного маршрутизатора:

ou can setup differen	t modes to LAN and WLAN interface for NAT and bridging function.
⊙ Gateway:	In this mode, the device is supposed to connect to internet via ADSL/Cable Moder The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHC client, PPTP client or static IP.
🔿 Bridge:	In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
O Wireless ISP:	In this mode, all ethemet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethemet ports share th same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup if WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Наименование	Описание		
Gateway	Стандартная настройка шлюза. Она используется для подключения к Интернет через ADSL/кабельный модем, LAN-интерфейс, WAN-интерфейс, Wireless интерфейс. NAT и Firewall модули применяются в этом режиме		
Bridge	Каждый интерфейс (WAN, LAN и Wireless) считается бриджом. NAT, Firewall и все функции маршрутизации не поддерживаются		
Wireless ISP	Переключает wireless Интерфейс в WAN и все Ethernet порты в режим бриджа. Wireless интерфейс способен выполнять все функции маршрутизации		
Apply Changes	Нажмите на эту кнопку для завершения и сохранения настроек		
Reset	Нажмите на кнопку <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям.		

3.3.4 Основные радио-настройки

Эта страница используется для настройки параметров для клиентов беспроводной сети, которые могут подключаться к вашему широкополосному маршрутизатору. Здесь вы можете изменить настройки безопасности так же легко, как и остальные параметры радиосвязи.

Wireless Bas	sic Settings
This page is used to con your Access Point. Here network parameters.	nfigure the parameters for wireless LAN clients which may connect to e you may change wireless encryption settings as well as wireless
Disable Wireless	LAN Interface
Band:	2.4 GHz (B+G) 💌
Mode:	AP 💌
Network Type:	Infrastructure 🔽
SSID:	MyWLAN
Channel Number:	11 💌
Associated Clients:	Show Active Clients
Enable Mac Clon	e (Single Ethernet Client)
📃 Enable Universal	Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Inter	face:
Apply Changes	Reset

Наименование	Описание		
Disable Wireless LAN Interface	Кликните по полю рядом с этой опцией для отключения передачи данных по LAN		
Band	Кликните для выбора 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(B+G)		
Mode	Кликните для выбора беспроводного режима WLAN AP / Client / WDS / AP+WDS		
SSID	Это имя беспроводной сети. SSID может быть длинной 32 байт		
Channel Number	Выбор номера канала		
Associated Clients	Кликните по кнопке <i>Show Active Clients</i> для того, чтобы открыть таблицу активных беспроводных клиентов, которая показывает МАС адрес, передаваемые пакеты, получаемые пакеты и скорость передачи данных для каждого связанного беспроводного клиента		
Enable Mac Clone	Назначает МАС адрес сетевой карточки ноутбука МАС адресом беспроводного клиента (только в клиентском режиме)		
Enable Universal Repeater Mode	Кликните для включения этой функции Universal Repeater Mode		
SSID of Extended Interface	Назначает SSID, если включена функция Universal Repeater Mode		
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек		
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям		

3.3.5 Особые настройки радиосвязи

Эти настройки – только для пользователей, которые обладают достаточными знаниями о беспроводных сетях. Не следует менять эти настройки до тех пор, пока вы не убедитесь в том, каковы будет последствия их изменения для широкополосного WLAN маршрутизатора.

LAN. These settings should not Point.	be changed unless you know what effect the changes will have on your Acc
Authentication Type:	○ Open System ○ Shared Key ④ Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto 🔽
Preamble Type:	Short Preamble ○ Short Preamble
Broadcast SSID:	💿 Enabled 🛛 Disabled
IAPP:	💿 Enabled 🛛 Disabled
802.11g Protection:	💿 Enabled 🛛 Disabled
RF Output Power:	⊙ 100% ○ 50% ○ 25% ○ 10% ○ 5%
Turbo Mode:	🔿 Auto 🔿 Always 💿 Off
	Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.
Block Relay Between Clients:	🔿 Enabled 💿 Disabled
WMM:	🔿 Enabled 💿 Disabled
ACK Timeout:	0 (0-255) < Current: 11b: 316us / 11g: 72us >

Наименование	Описание	
Authentication Type	Кликните для выбора типа аутентификации: <i>Open System</i> , <i>Shared Key</i> или <i>Auto</i>	
Fragment Threshold	Установка порога для фрагментации пакета данных, значения могут варьироваться от 256 до 2346 байт (см. параграф 4.10 - Что такое Fragment Threshold?)	
RTS Threshold	Установка порога RTS, значение может варьироваться от 0 до 2347 байт	
Beacon Interval	Установка интервала времени для радио маяка, значение может варьироваться от 20 до 1024 мс	
Data Rate	Выберите скорость передачи данных из нисходящего меню. Скорость передачи может быть выбрана автоматически, 11М, 5,5М, 2М или 1 Мбит/сек	
Preamble Type	Кликните для выбора поддержки <i>Long Preamble</i> или <i>Short Preamble</i> для беспроводной передачи пакетов данных. (см.параграф 4.13 - Что такое Preambule Type?)	
Broadcast SSID	Кликните для включения или выключения функции широковещательной передачи SSID. (см. параграф 4.14 - Что такое SSID Broadcast?)	
IAPP	Включите или выключите функцию IAPP. (см. параграф 4.20 - Что такое протокол IAPP?)	
802.11g Protection	Защита пользователя 802.11b	
RF Output Power	Регулировка мощности передатчика	
Turbo Mode	Кликните для включения/выключения турбо режима	
Block Relay Between Clients	Кликните Enable/Disable для решения о ретрансляции пакетов между клиентами	
WMM	Кликните Enable/Disable для инициации свойства WMM.	
ACK Timeout	Установите значения таймаута для АСК. Оно показывает текущее время	
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек	
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям.	

3.3.6 Настройки безопасности

На этой странице вы можете настроить различные режимы безопасности. Включив WEP, WPA, WPA2 и используя ключи шифрования, вы сможете предотвратить несанкционированный доступ к вашей беспроводной сети.

Wireless Security Setup			
This page allo prevent any u	ows you setup the wirel mauthorized access to y	ess security. Turn on WEP or WPA by using Encryption Keys could your wireless network.	
Fuervotion	None	SetWEPKey	
Use 802.	l x Authentication	• WEP 64bits OWEP 128bits	
WPA Auther	ntication Mode:	🔿 Enterprise (RADIUS) 💿 Personal (Pre-Shared Key)	
Pre-Shared I	Key Format:	Passphrase	
Pre-Shared I	Key:		
Enable P	re-Authentication		
Authenticati	on RADIUS Server:	Port 1812 IP address Password	
Note: When e	encryption WEP is sele	cted, you must set WEP key value.	
Apply C	hanges Reset		

Наименование	Описание
	Выберите метод шифрования, используемый для доступа к беспроводной
	сети. Методы шифрования могут быть следующими: None, WEP,
	WPA(TKIP), WPA2 или WPA2 Mixed.
	См. параграфы:
Enormation	4.9 Что такое WEP?
Encryption	4.15 Что такое WPA?
	4.16 Что такое WPA2 (AES)?
	4.17 Что такое 802.1X Authentication?
	4.18 Что такое Temporal Key Integrity Protocol (TKIP)?
	4.19 Что такое Advanced Encryption Standard (AES)?
Line 802 1	Используется вместе с WEP-шифрованием. Кликните по полю, чтобы
Use 802.1x	включить функцию аутентификации IEEE 802.1x.
Authentication	(см. параграф 4.17 - Что такое 802.1X Authentication?)
W/DA Anthentication	Используется вместе с WPA-шифрованием. Кликните для выбора режима
WPA Authentication	аутентификации WPA с Enterprise (RADIUS) или Personal (Pre-Shared Key).
Mode	(см. параграф 4.15 - Что такое WPA?)
	Используется вместе с WPA-шифрованием. Выберите формат pre-shared key
Pre-Shared Key Format	из нисходящего меню. Формат может быть Passphrase или Hex (64 символа).
	[WPA, Personal(Pre-Shared Key) только]
Pre-Shared Key	Введите ключ. [WPA, Personal(Pre-Shared Key) только]
Enchle Dre Authentication	Кликните для включения Pre-Authentication. [WPA2/WPA2
Enable Pre-Authentication	Mixed only, Enterprise только]
Authentication	Задайте IP адрес, информацию о порте и пароле для аутентификации на
RADIUS Server	RADIUS cepsepe
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Pagat	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к
NESEL	предыдущим конфигурациям

Установка WEP-ключа

encryption key, and se	lect ASCII or Hex as the format of input value.	
Key Length:	64-bit 💌	
Key Format:	Hex (10 characters) 💌	
Default Tx Key:	Key 1 💌	
Encryption Key 1:	Xoloblobloblok	
Encryption Key 2:	solooloolook	
Encryption Key 3:	sekelekeleke	
Encryption Key 4:	sciolololololol	

Наименование	Описание
	Выбор длинны секретного ключа.
Koy Longth	Длина может выбираться между 64 и 128 (шифрование, известное, как WEP-
Key Length	2) битами ключа. WEP-ключ составлен из вектора инициализации и
	секретного ключа (40-битного или 104-битного)
Key Format	Выберите формат WEP-ключа из нисходящего меню. Формат может быть
	выбран из ASCII и НЕХ кодами.
Default Tx Key	Установка секретного ключа по умолчанию для функции WEP-шифрования
Encryption Key 1	Секретный ключ 1 функции WEP-шифрования
Encryption Key 2	Секретный ключ 2 функции WEP-шифрования
Encryption Key 3	Секретный ключ 3 функции WEP-шифрования
Encryption Key 4	Секретный ключ 4 функции WEP-шифрования
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Close	Кликните для того, чтобы закрыть окно настройки WEP-ключа
D (Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к
Keset	предыдущим конфигурациям.

3.3.7 Контроль доступа к радиосвязи

Если вы включили контроль доступа к радиосвязи, то доступ к вашей точке доступа будут иметь только те клиенты, чьи МАС адреса находятся в списке контроля доступа.

Когда эта функция включена, ни один из клиентов не будет иметь право доступа, если список контроля доступа пуст.

Wireless Access Control		
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.		
Wireless Access Control Mode: Disable	•	
MAC Address: Comment:		
Apply Changes Reset		
Current Access Control List:		
MAC Address	Comment	Select
Delete Selected Delete All	Reset	

Наименование	Описание
Wireless Access Control Mode	Выберите <i>Disabled</i> , <i>Allow Listed</i> или <i>Deny Listed</i> для определения режима контроля доступа к радиосвязи. Это функция контроля доступа; только зарегистрированные клиенты из списка контроля доступа будут иметь доступ к широкополосному WLAN маршрутизатору
MAC Address	Введите МАС адрес клиента для регистрации возможности доступа к широкополосному WLAN маршрутизатору
Comment	Введите комментарий для зарегистрированного клиента
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям.
Current Access Control List	Показывает зарегистрированных клиентов, которым разрешен доступ к широкополосному WLAN маршрутизатору
Delete Selected	Кликните для удаления выбранных клиентов, которым будет перекрыт доступ к широкополосному WLAN маршрутизатору
Delete All	Кликните для удаления всех зарегистрированных клиентов из разрешенного списка доступа
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям.

3.3.8 Настройки WDS

Wireless Distribution System использует радиосвязь для коммуникации с другими точками доступа, как это делает, например, Ethernet. Для того, чтобы это сделать, вы должны поместить эти точки доступа в один канал и установить MAC адрес другой точки доступа, к которой вы хотите подключиться, в таблице и затем включить WDS.

WDS Settings		
Wireless Distribution System uses wireless media this, you must set these APs in the same channel communicate with in the table and then enable the	to communicate with other APs, like the and set MAC address of other APs whic WDS.	Ethernet does. To do h you want to
Enable WDS		
Add WDS AP: MAC Address	Comment	
Apply Changes Reset Se	t Security Show Statistics	
Current WDS AP List:		
MAC Address	Comment	Select
00:02:72:81:86:0a	AP-1	
00:02:72:81:86:0b	AP-2	
Delete Selected Delete All	Reset	

Наименование	Описание
Enable WDS	Отметьте поле для включения WDS.
	(см. параграф 4.21 - Что такое WDS?)
MAC Address	Введите MAC адрес точки доступа для регистрации возможности доступа WDS
Comment	Введите комментарий для зарегистрированного клиента
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к
	предыдущим конфигурациям.
Set Security	Кликните по этой кнопке для настройки безопасности радиосвязи:
	WEP(64bits), WEP(128bits), WPA(TKIP), WPA2(AES) или None
Delete Selected	Кликните для удаления выбранных клиентов, которым будет перекрыт
	доступ к широкополосному WLAN маршрутизатору
Delete All	Кликните для удаления всех зарегистрированных клиентов из разрешенного
Delete All	списка доступа
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к
Keset	предыдущим конфигурациям

Настройка безопасности WDS

Шаги по настройки: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS.

Страница используется для настройки безопасности радиосвязи между точками доступа. Обратитесь к параграфу 3.3.6 Настройка безопасности.

ure each WDS device has	adopted the same encryption algorithm and Key.
Encryption:	None 🖌
WEP Key Format:	ASCII (5 characters) 👻
WEP Key:	
Pre-Shared Key Format:	Passphrase 👻
Pre-Shared Key:	

Таблица точек доступа WDS

Эта страница используется для обзора статистики WDS:

This table shows the N	AC address, trans	smission, rece	iption packet c	ounters and state
nformation for each co	onfigured WDS AP			
MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)
00:02:72:81:86:0a	22	0	0	1
			0	

Наименование	Описание
MAC Address	Показывает MAC адрес внутри WDS
Tx Packets	Показывает статистику отправленных пакетов на беспроводном LAN-интерфейсе
Tx Errors	Показывает статистику ошибок для отправленных пакетов на беспроводном LAN-интерфейсе
Rx Packets	Показывает статистику полученных пакетов на беспроводном LAN-интерфейсе
Tx Rare (Mbps)	Показывает скорость подключения по радиосвязи для WDS
Refresh	Кликните для обновления статистических показателей на экране
Close	Кликните для того, чтобы закрыть окно

3.3.9 Обзор доступных сетей (Site survey)

Страница используется для обзора других точек доступа, находящихся в зоне действия вашей беспроводной сети:

his page provides tool to scan annally when client mode is e	the wireless network. If any A nabled	ccess Point or	IBSS is fou	ınd, you coul	d choose to (Connect 1t
SSID	BSSID	Channel	Туре	Encrypt	Signal	Select
MyWLAN	00:02:72:00:81:86	11 (B+G)	AP	no	90	0
inux-wlan	00:02:72:f1:02:ad	6 (B)	AP	no	76	0
RTL8186-VPN-GW	00:e0:4c:81:86:23	11 (B+G)	AP	no	66	0
Sales	00:02:72:04:68:92	11 (B)	AP	yes	53	0
Tekom_Office	00:02:72:00:93:fb	9 (B)	AP	yes	35	0
dex	d6:4c:fc:0d:2a:d4	1 (B)	Ad hoc	no	32	0
MyWLAN	00:02:72:85:15:99	11 (B+G)	AP	no	32	0

Наименование	Описание
SSID	Показывает SSID точки доступа
BSSID	Показывает BSSID точки доступа
Channel	Показывает канал, который использует точка доступа
Туре	Показывает, в каком режиме работает точка доступа
Encrypt	Показывает статус шифрования
Signal	Показывает уровень сигнала при приеме
Select	Кликните для выбора точки доступа или клиента, к которому вы хотите
	подключиться
Refresh	Кликните <i>Refresh</i> для повторного обновления информации об узле на экране
Connect	Кликните <i>Connect</i> для установки соединения

3.3.10 Настройка LAN-интерфейса

Эта страница используется для настройки параметров локальной сети. Здесь вы можете изменить настройки IP адреса, маски подсети, DHCP и т.д.

LAN Interfac	e Setup
This page is used to confi LAN port of your Access mask, DHCP, etc	gure the parameters for local area network which connects to th Point. Here you may change the setting for IP addresss, subnet
IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server 💌
DHCP Client Range:	192.168.1.100 - 192.168.1.200 Show Client
Domain Name:	
802.1d Spanning Tree:	Disabled 💌
Clone MAC Address:	00000000000
Apply Changes	Reset

Наименование	Описание
IP address	Введите IP адрес LAN-интерфейсов
Subnet Mask	Введите маску подсети LAN-интерфейсов
Default Gateway	Введите шлюз по умолчанию для исходящих пакетов данных с LAN- интерфейсов
DHCP	Кликните для выбора Disabled, Client или Server
DHCP Client Range	Введите начальный и конечный IP адрес для обозначения диапазона IP адресов; клиенту, у которого включена функция DHCP, будет назначен IP адрес из этого диапазона
Show Client	Кликните, для того, чтобы открыть окно <i>Active DHCP Client Table</i> , которое показывает активных клиентов с назначенными IP адресами, MAC адресами и информацией о времене работы (только для режима сервера)
DNS Server	Ручная настройка адреса DNS сервера
Domain Name	Назначение доменного имени DHCP клиентам. Эта функция - по выбору
802.1d Spanning Tree	Выберите для включения или выключения функции IEEE 802.1d Spanning Tree
Clone MAC Address	Введите МАС адрес, который должен быть клонирован. (см. параграф 4.24 - Что такое клонирование МАС адресов?)
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям

3.3.11 Настройка WAN-интерфейса

На этой странице настраиваются параметры внешней сети, которая подключается к WAN-порту вашего широкополосного WLAN маршрутизатора. Здесь вы можете выбрать метод доступа: *Static IP*, *DHCP*, *PPPoE* или *PPTP* кликнув по полю напротив **WAN Access Type**.

Статический ІР адрес

This page is used to com your Access Point. Here click the item value of W.	ägure the parameters for Internet network which connects to the WAN port- you may change the access method to static IP, DHCP, PPPoE or PPTP by AN Access type.
WAN Access Type:	Static IP 💌
IP Address:	172.1.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	172.1.1.254
MTU Size:	1400 (1400-1500 bytes)
DNS 1:	0.0.0.0
DNS 2:	0.0.0.0
DNS 3:	0.0.0.0
Clone MAC Address:	0000000000
📃 Enable uPNP	
Enable Ping Access	s on WAN
Enable Web Server	Access on WAN
Enable IPsec pass t	hrough on VPN connection
Enable PPTP pass 1	hrough on VPN connection
Enable L2TP pass t	hrough on VPN connection

Наименование	Описание
Static IP	Кликните для выбора поддержки Static IP на WAN-интерфейсе. Вы должны
	выбрать настройки IP адреса, маски подсети и шлюза по умолчанию
IP Address	Если вы выбираете поддержку статического IP адреса на WAN-интерфейсе, введите IP адрес для него
Subnet Mask	Если вы выбираете поддержку статического IP адреса на WAN-интерфейсе, введите маску подсети для него
Default Gateway	Если вы выбираете поддержку статического IP адреса на WAN-интерфейсе,
Denualt Gute way	введите шлюз по умолчанию для отправки исходящих пакетов
MTU Size	Введите размер МТU. Величина по умолчанию равна 1400
DNS 1	Введите IP адрес DNS сервера 1
DNS 2	Введите IP адрес DNS сервера 2
DNS 3	Введите IP адрес DNS сервера 3
Clone MAC Address	Введите МАС адрес, который должен быть клонирован
Enable uPNP	Кликните по полю для включения функции uPNP
Enable Web Server	Кликните по полю для включения веб-конфигурирования через WAN-
Access on WAN	интерфейс
Enable WAN Echo	V пилнита по полно пля рипнонния отрата $WANICMP$
Reply	Кликните по полю для включения ответа w Атутсти
Enable IPsec pass	
through on VPN	Кликните по полю для включения IPSec
connection	
Enable PPTP pass	
through on VPN	Кликните по полю для включения РРТР
connection	

Enable L2TP pass through on VPN connection	Кликните по полю для включения L2TP
Set TTL value	Кликните для включения и введите значение Time to Live
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям.

DHCP клиент

your Access Point. Here click the item value of W.	again and parameters for inferior network wind connects to the ward port you may change the access method to static IP, DHCP, PPPoE or PPTP by AN Access type.
WAN Access Type:	DHCP Client V
Host Name:	
MTU Size:	1400 (1400-1492 bytes)
O Attain DNS Automat	tically
💿 Set DNS Manually	
DNS 1:	0.0.0.0
DNS 2:	0.0.0.0
DNS 3:	0.0.0.0
Clone MAC Address:	0000000000
Enable uPNP	
Enable Ping Access	s on WAN
Enable Web Server	Access on WAN
🗹 Enable IPsec pass t	hrough on VPN connection
🗹 Enable PPTP pass t	hrough on VPN connection
Enable L2TP pass t	hrough on VPN connection
📃 Set TTL Value	64 (1-128)

Наименование	Описание	
DHCР клиент	Кликните для выбора поддержки DHCP на WAN-интерфейсе, для того чтобы	
	IP адреса назначались автоматически DHCP сервером	
Host Name	Введите имя хоста. По умолчанию эта строка пуста	
MTU Size	Введите размер МТU. Величина по умолчанию равна 1400	
Attain DNS	DNG DUCD	
Automatically	Кликните для выоора получения DNS адреса по DHCP	
Set DNS Manually	Кликните для выбора ручной настройки DNS, если включена поддержка DHCP	
DNS 1	Введите IP адрес DNS сервера 1	
DNS 2	Введите IP адрес DNS сервера 2	
DNS 3	Введите IP адрес DNS сервера 3	
Clone MAC Address	Введите МАС адрес, который должен быть клонирован	
Enable uPNP	Кликните по полю для включения функции uPNP	
Enable Web Server	Кликните по полю для включения веб-конфигурирования через WAN-	
Access on WAN	интерфейс	
Enable WAN Echo	Кликните по полю для включения ответа WAN ICMP	
Reply		
Set TTL value	Кликните для включения и введите значение Time to Live	
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек	
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям	

PPPOE	

WAN Interface Setup		
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.		
WAN Access Type:	PPPoE 💌	
User Name:		
Password:		
Service Name:		
Connection Type:	Continuous Connect Disconnect	
Idle Time:	5 (1-1000 minutes)	
MTU Size:	1400 (1360-1492 bytes)	
🔵 Attain DNS Automa	tically	
💿 Set DNS Manually		
DNS 1:	0.0.0.0	
DNS 2:	0.0.0.0	
DNS 3:	0.0.0.0	
Clone MAC Address:	0000000000	
Enable uPNP		
Enable Ping Access on WAN		
Enable Web Server Access on WAN		
Enable IPsec pass through on VPN connection		
Enable Pr IP pass through on VPN connection Frable L2TP pass through an VPN connection		
Set TTI. Value 64 (1.122)		
Apply Changes	Reset	

Наименование	Описание		
РРРоЕ	Кликните для выбора РРРоЕ на WAN-интерфейсе. Здесь вы должны настроить имя пользователя пароль тип полключения и время ожилания		
User Name	Если вы выбираете поддержку РРРоЕ на WAN-интерфейсе, введите имя пользователя для того, чтобы зайти на РРРоЕ сервер		
Password	Если вы выбираете поддержку РРРоЕ на WAN-интерфейсе, введите пароль для того, чтобы зайти на РРРоЕ сервер		
Service Name	Введите Service Name		
Connection Type	Выберите тип подключения из нисходящего меню. Здесь вы можете выбрать <i>Continuous, Connect on Demand</i> и <i>Manual. Continuous</i> означает, что настройка подключения осуществляется с помощью протокола PPPoE, когда бы ни был включен широкополосный WLAN маршрутизатор. <i>Connect on Demand</i> означает, что настройка подключения осуществляется с помощью протокола PPPoE, когда бы ни посылали пакеты данных через WAN-интерфейс; существует сторожевое устройство для закрытия PPPoE подключения в то время, когда пакеты не посылаются дольше, чем составляет настроенное время бездействия системы <i>Manual</i> означает, что настройка подключения осуществляется с помощью протокола PPPoE с помощью двойного клика по <i>Connect</i> и клика по <i>Disconnect</i>		
Idle Time	Если вы выбираете PPPoE и Connect on Demand тип подключения, введите время бездействия для автоматического отключения функции. Эта величина может варьироваться от 1 до 1000 минут		
MTU Size	Введите размер МТU. Величина по умолчанию равна 1400. (см. параграф 4.23 - Что такое размер МТU?)		
Attain DNS	Кликните для выбора получения DNS адреса по РРРоЕ . Выберите Set DNS		
Automatically	Manually если включена поддержка PPPoE		

Set DNS Manually	Кликните для выбора ручной настройки DNS, если включена поддержка статического IP адреса	
DNS 1	Введите IP адрес DNS сервера 1	
DNS 2	Введите IP адрес DNS сервера 2	
DNS 3	Введите IP адрес DNS сервера 3	
Clone MAC Address	Введите МАС адрес, который должен быть клонирован	
Enable uPNP	Кликните по полю для включения функции uPNP	
Enable Web Server	Кликните по полю для включения веб-конфигурирования через WAN-	
Access on WAN	интерфейс	
Enable WAN Echo	Кликните по полю для включения ответа WAN ICMP	
Reply		
Set TTL value	Кликните для включения и введите значение Time to Live	
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек	
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям	

PPTP

Наименование	Описание		
РРТР	Разрешение пользователям создать туннель с удалённым узлом напрямую для обеспечения безопасности при передаче данных между подключенными устройствами. Пользователь может использовать встроенного РРТР клиента, поддерживаемого маршрутизатором для создания VPN туннеля		
IP Address	Если вы выбираете поддержку РРТР на WAN-интерфейсе, введите IP адрес для него		
Subnet Mask	Если вы выбираете поддержку РРТР на WAN-интерфейсе, введите маску подсети для него		
Server IP Address	Введите IP адрес РРТР сервера		
User Name	Если вы выбираете поддержку РРТР на WAN-интерфейсе, введите имя пользователя для того, чтобы зайти на РРТР сервер		
Password	Если вы выбираете поддержку РРТР на WAN-интерфейсе, введите пароль для того, чтобы зайти на РРТР сервер		
MTU Size	Введите размер МТU. Величина по умолчанию равна 1400. (см. параграф 4.23 - Что такое размер МТU?)		
Request MPPE Encryption	Кликните по полю для включения запроса МРРЕ-шифрования		
Attain DNS	Кликните для выбора получения DNS адреса по <i>PPTP</i> . Пожалуйста, выберите		
Automatically	Set DNS Manually если включена поддержка PPTP		
Set DNS Manually	Кликните для выбора ручной настройки DNS, если включена поддержка статического IP адреса		
DNS 1	Введите IP адрес DNS сервера 1		
DNS 2	Введите IP адрес DNS сервера 2		
DNS 3	Введите IP адрес DNS сервера 3		
Clone MAC Address	Введите МАС адрес, который должен быть клонирован		
Enable uPNP	Кликните по полю для включения функции uPNP		
Enable Web Server	Кликните по полю для включения веб-конфигурирования через WAN-		
Access on WAN	интерфейс		
Enable WAN Echo Reply	Кликните по полю для включения ответа WAN ICMP		
Set TTL value	Кликните для включения и введите значение Time to Live		
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек		
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям		

3.3.12 Firewall – фильтрация на порту

Записи в этой таблице используются для ограничения определенных типов пакетов данных в вашей локальной сети, которые могут попасть в Интернет через шлюз. Использование таких фильтров может быть полезным в обеспечении безопасности и ограничении вашей локальной сети.

Port Filtering			
Entries in this table are used to re through the Gateway. Use of suc	strict certain types of data pack h filters can be helpful in securi	ets from your local network to ng or restricting your local net) Internet work.
Enable Port Filtering			
Port Range:	Protocol: Both 💙 Comm	neni:	
Apply Changes Re	set		
Current Filter Table:			
Port Range	Protocol	Comment	Select
Delete Selected D	elete All Reset		

Наименование	Описание
Enable Port Filtering	Включение функции фильтрации на порту для обеспечения безопасности
Port Range	Для ограничения передачи данных из локальной сети на определенные
Protocol	порты, введите номер начального и конечного порта, протокола, а также
Comments	введите комментарий
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям
Delete Selected	Кликните для того, чтобы удалить выбранный диапазон портов из списка фильтрации
Delete All	Кликните для удаления всех зарегистрированных записей из списка фильтрации
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям

3.3.13 Firewall – IP фильтрация

Записи в этой таблице используются для ограничения определенных типов пакетов данных в вашей локальной сети, которые могут попасть в Интернет через шлюз. Использование таких фильтров может быть полезным в обеспечении безопасности вашей локальной сети.

IP Filtering			
Entries in this table are used to through the Gateway. Use of s	restrict certain types of data p uch filters can be helpful in sec	oackets from your local netw curing or restricting your loc	ork to Internet al network.
Enable IP Filtering	*		
Loal IP Address:	Protocol: Both 🖌 Con	mment:	
Apply Changes F	Reset		
Current Filter Table:			
Local IP Address	Protocol	Comment	Selec
Delete Selected	Delete All Reset		

Наименование	Описание
Enable IP Filtering	Включение функции IP фильтрации для обеспечения безопасности
Local IP Address Protocol Comments	Для ограничения передачи данных из локальной сети на определенные IP адреса, введите IP адрес и протокол, а также введите комментарий. <i>Protocol</i> может быть TCP, UDP или оба. <i>Сомтенt</i> даст вам знать причины ограничения передачи данных по IP адресу
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям
Delete Selected	Кликните для того, чтобы удалить выбранный IP адрес из списка фильтрации
Delete All	Кликните для удаления всех зарегистрированных записей из списка фильтрации
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям

3.3.14 Firewall – МАС фильтрация

Записи в этой таблице используются для ограничения определенных типов пакетов данных в вашей локальной сети, которые могут попасть в Интернет через шлюз. Использование таких фильтров может быть полезным в обеспечении безопасности вашей локальной сети.

Entries in this table are used to restrict certain types of d through the Gateway. Use of such filters can be helpful i	ata packets from your local net n securing or restricting your lo	work to Internet ocal network.
Enable MAC Filtering MAC Address: Comment: Apply Changes Reset		
Current Filter Table:		
Current Filter Table: MAC Address	Comment	Select
Current Filter Table: MAC Address 00:02:72:00:81:90	Comment ST-1	Select
Current Filter Table: <u>MAC Address</u> 00:02:72:00:81:90 00:02:72:00:81:91	Comment ST-1 ST-2	Select

Наименование	Описание				
Enable MAC Filtering	Включение функции МАС фильтрации для обеспечения безопасности				
MAC Address Comments	Для ограничения передачи данных из локальной сети на определенные МАС адреса, введите МАС адрес, а также введите комментарий. <i>Соттепt</i> даст вам знать причины ограничения передачи данных по IP адресу				
Apply Changes	Кликните по этой кнопке для регистрации МАС адреса в таблице фильтрации МАС адресов				
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям				
Delete Selected	Кликните для того, чтобы удалить выбранный МАС адрес из списка фильтрации				
Delete All	Кликните для удаления всех зарегистрированных записей из списка фильтрации				
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям				

3.3.15 Firewall - переадресация портов

Записи в этой таблице позволяют вам автоматически переадресовывать общие сетевые сервисы на указанное устройство за NAT. Эти настройки необходимы, только если вы желаете разместить какие-то серверы, как например web-сервер или mail-сервер в частной локальной сети за NAT шлюза.

Port Forwardi	ng							
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.								
Enable Port Forwarding	✓ Enable Port Forwarding							
IP Address:	IP Address: Protocol: Both V Port Range: Comment:							
Apply Changes	Apply Changes Reset							
Current Port Forwarding T	able:							
Local IP Address	Protocol	Port Range	Comment	Select				
192.168.1.201	TCP+UDP	20-21	FTP					
Delete Selected	Delete All	Reset						

Наименование	Описание
Enable Port Forwarding	Включение функции безопасности Port Forwarding
IP Address Protocol Port Range Comment	Для переадресации пакетов, приходящих от WAN на указанный IP адрес, который расположен в локальной сети за NAT, введите IP адрес, протокол, диапазон портов и ваши комментарии. <i>Protocol</i> может быть TCP, UDP или оба. <i>Port Range</i> – диапазон портов для передачи данных. <i>Comments</i> дадут вам знать причины разрешения переадресации пакетов на указанный IP адрес и порт
Apply Changes	Кликните по этой кнопке для регистрации IP адреса в списке переадресации IP адресов
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям
Delete Selected	Кликните для того, чтобы удалить выбранный IP адрес и порт из списка фильтрации
Delete All	Кликните для удаления всех зарегистрированных записей из списка

Оборудование семейства MLink											
	переад	цресац	ии п	юртов							
Reset	Кликн преды	ите п дущим	ок кон	кнопке нфигур	Reset ациям	для	прекращения	изменений	И	возврата	К

3.3.16 Firewall – URL фильтрация

URL фильтрация используется для ограничения доступа пользователям к

особым веб сайтам в Интернете.

URL Filtering		
URL filter is used to deny LAN users from accessing the internet listed below.	t. Block those URLs which contain keywo	rd:
Enable URL Filtering		
URL Address:		
Apply Changes Reset		
Current Filter Table:		
URL Address	Select	
Delete Selected Delete All Reset		

Наименование	Описание			
Enable URL Filtering	Включение функции фильтрации URL			
URL Address	Добавьте один URL адрес			
Apply Changes	Кликните по этой кнопке для сохранения настроек			
Basat	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к			
Keset	предыдущим конфигурациям			
Delete Selected	Кликните для того, чтобы удалить выбранный URL адрес из списка			
	фильтрации			
Delete All	Кликните для удаления всех зарегистрированных записей из списка			
Delete All	фильтрации			
Pasat	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к			
Nesei	предыдущим конфигурациям			

3.3.17 Firewall - DMZ

Демилитаризованная зона используется для обеспечения сервисов Интернет без риска доступа к частной локальной сети неавторизованных пользователей. Это часть компьютерной сети, находящаяся между локальной сетью и Интернетом. Обеспечивает выход в Интернет и внешнее присутствие в нём, скрывая при этом внутреннюю сеть организации и предотвращая прямое обращение к ней. Обычно, в DMZ находятся устройства, которые имеют доступ к трафику Интернет, в частности к Web (HTTP) серверам, FTP серверам, SMTP (еmail) серверам и DNS серверам.

DMZ	
A Demilitarized Zone is u private network. Typicall servers, FTP servers, SM	ised to provide Internet services without sacrificing unauthorized access to its local y, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP TP (e-mail) servers and DNS servers.
_	
Enable DMZ	

Наименование	Описание
Enable DMZ	Включение функции DMZ
DMZ Host IP Address	Для поддержки DMZ в вашей схеме брандмауэра, введите IP адрес хоста DMZ, на который можно зайти через WAN-интерфейс
Apply Changes	Кликните по этой кнопке для регистрации IP адреса хоста DMZ
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям

3.3.18 Настройки VPN

Эта страница используется для того, чтобы показать таблицу подключений VPN, настроить IPsec VPN, NAT Traversal, Generate RSA Key, Show RSA Public Key.

En En	able IPSEC N ply Change:	APN S	Enable NAT Traversal Generate RSA Key Show RSA Public Key				
Current VPN Connection Table: WAN IP:0.0.0.0							
	# Name	Active	Local Address	Remote Address	Remote Gateway	Status	
•	ι -	-	-	-	-	-	
•	2 -	-	-	-	-	-	
•	3 -	-	-	-	-	-	
•	4 -	-	-	-	-	-	
•	5 -	-		-	-	-	
•	5 -	-	-	-	-	-	
•	7 -	-	-	-	-	-	
•	3 -	-	-	-	-	-	
•	, -	-	-	-	-	-	
0 1	0 -	-	-		-	_	

Наименование	Описание		
Enable IPSEC VPN	Включение функции IPSEC VPN. (см.параграф 4.27 Что такое VPN? и 4.28 Что такое IPSEC?)		
Enable NAT Traversal	Кликните для включения функции NAT Traversal		
Generate RSA Key	Кликните для генерации RSA ключа		
Show RSA Public Key	Кликните для просмотра публичного RSA ключа, который сгенерировали		
Apply Changes	Кликните по этой кнопке для включения IPSEC VPN, NAT Traversal		
Current VPN	Показывает информацию о конкретном WAN-интерфейсе и таблице		
Connection Table	подключений по VPN		
Edit	Кликните для того, чтобы зайти на страницу конфигурирования VPN туннеля		

Delete	Кликн	ните для удаления настоящего VPN туннеля
Refresh	Кликн	ните для обновления таблицы VPN

Настройки VPN – изменение туннеля

VPN Setup		
Enable Tunnel 1		
Connection Name:	site5	
Auth Type:	PSK 🗸	
Local Site:	Subnet Address 🐱	
Local IP Address/Network	192.168.1.0	
Local Subnet Mask	255.255.255.0	
Remote Site:	Subnet Address 🗸	
Remote Secure Gateway	192.168.3.1	
Remote IP Address/Network	192.168.4.0	
Remote Subnet Mask	255.255.255.0	
Local/Peer ID:		
Local ID Type		
Local ID		
Remote ID Type	IP V	
Remote ID		

Наименование	Описание
Enable Tunnel #	Кликните для включения туннеля IPSEC VPN
Connection Name	Назначьте имя для подключения
Auth Type	Кликните для выбора <i>PSK</i> или <i>RSA</i>
Local Site Local IP Address/Network Local Subnet Mask	Кликните для выбора Single Address или Subnet Address VPN подключения. Введите IP адрес или маску подсети в зависимости от того, какую опцию локального сайта вы выбираете
Remote Site Remote Secure Gateway Remote IP Address/Network Remote Subnet Mask	Кликните для выбора Single Address, Subnet Address, Any Address или NAT-T Any Address удалённого VPN подключения. Введите IP адрес удаленного шлюза. Введите IP адрес или маску подсети в зависимости от того, какую опцию локального сайта вы выбираете. Введите удаленную маску подсети
Local ID Type Local ID	Определите IKE тип обмена информации. Кликните для выбора <i>IP</i> , <i>DNS</i> или <i>E-mail</i> как типа локального коммутатора (обмена). Введите локальные IP за исключением выбранных IP
Remote ID Type	Кликните для выбора <i>P</i> , <i>DNS</i> или <i>E-mail</i> как типа локального коммутатора (обмена)
Remote ID	Введите удалённые ID за исключением выбранных IP

Key Management:	⊙ IKE ○ Manual Advanced
Connection Type	Responder 🗸 Connect Disconnect
ESP	3DES (Encryption Algorithm)
	MD5 💙 (Authentication Algorithm)
PreShared Key	1234567
Remote RSA Key	
Status	Connected
Apply Changes Re	set Refresh Back

Наименование	Описание	
Key Management	Кликните для выбора <i>IKE</i> или режима <i>Manual</i>	
Advanced	Кликните по кнопке <i>Advanced</i> для настройки дополнительных возможностей IKE	
Connection Type	Кликните для выбора режима <i>Initiator</i> или <i>Responder</i>	
Connect	Кликните для ручного подключения (только для режима <i>Responder</i>)	
Disconnect	Кликните для ручного отключения (только для режима <i>Responder</i>)	
ESD	Кликните для настройки шифрования 3DES, AES128 или NULL.	
ESP	Кликните для настройки аутентификации MD5 или SHA1	
PreShared Key	Введите ключ (только для режима IKE)	
Remote RSA Key	Введите RSA ключ удаленного шлюза (только для режима IKE)	
Status	Показывает статус подключения (только для режима ІКЕ)	
SPI	Введите значение параметра Security Parameter Index (Только для режима Manual)	
Encryption Key	Введите ключ шифрования (только для режима Manual)	
Authentication Key	Введите ключ аутентификации (только для режима Manual)	
Apply Change	Кликните по этой кнопке для сохранения настроек	
Pasat	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к	
Keset	предыдущим конфигурациям	
Refresh	Показывает настоящий статус подключения (только для режима Manual)	
Back	Возврат к странице настроек VPN	

Настройка специального протокола ІКЕ

Adavnced VPN Setting for IKE		
This This page is used to provide a	dvanced setting for IKE mode	
Tunnel l		
Phase 1:		
Negotiation Mode	Main mode	
Encryption Algorithm	3DES 💌	
Authenticaiton Algorithm	MD5 💌	
Key Group	DH2(modp1024) 💌	
Key Life Time	3600	
Phase 2:		
Active Protocol	ESP	
Encryption Algorithm	3DES 💌	
Authenticaiton Algorithm	MD5 💌	
Key Life Time	28800	
Ecapsulation	Tunnel mode	
Perfect Forward Secrecy (PFS)	ON 💌	
Ok Cancel		

Наименование	Описание
Phase 1	
Negotiation Mode	Основной режим
Encryption Algorithm	Кликните для выбора шифрования 3DES или AES128
Authentication Algorithm	Кликните для выбора аутентификации <i>MD5</i> или SHA1
Key Group	Кликните для выбора группы ключей <i>DH1(modp768)</i> , <i>DH2(modp1024)</i> или <i>DH5(modp1536)</i>
Key Life Time	Введите значение времени действия ключа в секундах
Phase 2	
Active Protocol	ESP
Encryption Algorithm	Кликните для выбора типа шифрования 3DES, AES128 или NULL
Authentication Algorithm	Кликните для выбора аутентификации <i>MD5</i> или SHA1
Key Life Time	Введите значение времени действия ключа в секундах

Encapsulation	Режим туннеля
Perfect Forward Secrecy (PFS)	Кликните для выбора <i>ON</i> или <i>NONE</i>
Ok	Кликните по кнопке Ok для сохранения текущих настроек туннеля
Cancel	Кликните <i>Cancel</i> для того, чтобы закрыть окно без сохранения изменений настроек

3.3.19 Управления - статистика

На этой странице показаны счётчики пакетов при передаче и приёме для беспроводной сети, сетей Ethernet LAN и Ethernet WAN.

Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	Sent Packets	236
	Received Packets	35715
Ethernet LAN	Sent Packets	1396
	Received Packets	1416
Ethernet WAN	Sent Packets	655
	Received Packets	0

Наименование	Описание	
Wireless LAN	Показывает статистику по отправленным пакетам на беспроводном LAN-	
Sent Packets	интерфейсе	
Wireless LAN	Показывает статистику по полученным пакетам на беспроводном LAN-	
Received Packets	интерфейсе	
Ethernet LAN	Показывает статистику по отправленным пакетам на Ethernet LAN-	
Sent Packets	интерфейсе	
Ethernet LAN	Покази прает статистику по получении и пакетам на Ethernet I AN-интерфейсе	
Received Packets	показывает статистику по полученным пакетам на Еспетнет LAN-интерфейсе	
Ethernet WAN	Показывает статистику по отправленным пакетам на Ethernet WAN-	
Sent Packets	интерфейсе	
Ethernet WAN	Показывает статистику по полученным пакетам на Ethernet WAN-	
Received Packets	интерфейсе	
Refresh	Кликните <i>Refresh</i> для обновления статистических счётчиков на экране	

3.3.20 Управление - DDNS

Эта страница используется для настройки динамического DNS сервиса таким образом, чтобы получить DNS с динамическим IP адресом.

Dynamic DNS	Setting	
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.		
Enable DDNS		
Service Provider :	DynDNS 💌	
Domain Name :	host.dyndns.org	
User Name/Email:		
Password/Key:		
Note: For TZO, you can have a 3 For DynDNS, you can crea	0 days free trial <u>here o</u> r manage your TZO account in <u>control panel</u> ite your DynDNS account <u>here</u>	
Apply Change	Reset	

Наименование	Описание
Enable DDNS	Включение DDNS сервиса. (см. параграф 4.25 - Что такое DDNS?)
Domain Name	Настройка доменного имени
User Name/Email	Настройка имени пользователя, e-mail
Password/Key	Настройка пароля/ключа
Apply Change	Кликните Apply Change для сохранения включения DDNS сервиса
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям

3.3.21 Управление – настройка часового пояса

Эта страница используется для настройки NTP клиента для получения настоящего времени.

Time Zone S	etting					
You can maintain the sy	stem time by sy	nchronizing	with a publi	c time serve	r over the Ir	nternet.
Current Time .	2000	1	_ 1	4	15	~ [9]
Current lime :	Yr 2000	Mon	Day	Hr 4	Mn 15	Sec 50
Time Zone Select :	(GMT+08	3:00)Taipei				•
Enable NTP client	update					
NTP server :	192.5	5.41.41 - No	rth America	1 🗸		
	0		(Manua	1 IP Setting)		
Apply Change	Reset	Refresh				

Наименование	Описание
Current Time	Показывает текущее время
Time Zone Select	Кликните для выбора часового пояса вашей страны
Enable NTP client	Кликните по полю для включения обновления NTP клиента. Обратитесь к
update	параграфу 4.26 Что такое NTP клиент?
NTP Server	Кликните для выбора адреса NTP сервера – по умолчанию или того IP адреса,
Apply Change	Кликните Annly Change лля сохранения включения сервиса NTP клиента
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям
Refresh	Кликните для обновления текущего времени, обновляемого на экране

3.3.22 Управление – отказ от обслуживания

Эта страница используется для включения и настройки защиты от возможных хакерских атак. Обеспечивает большую безопасность для пользователей.

Enable DoS Prevention		
Whole System Flood: SYN	0	Packets/Second
Whole System Flood: FIN	0	Packets/Second
Whole System Flood: UDP	0	Packets/Second
Whole System Flood: ICMP	0	Packets/Second
Per-Source IP Flood: SYN	0	Packets/Second
Per-Source IP Flood: FIN	0	Packets/Second
Per-Source IP Flood: UDP	0	Packets/Second
Per-Source IP Flood: ICMP	0	Packets/Second
TCP/UDP PortScan	Low	Sensitivity
ICMP Smurf		
IP Land		
IP Spoof		
IP TearDrop		
PingOfDeath		
TCP Scan		
TCP SynWithData		
UDP Bomb		
IDP FakeChower		

Наименование	Описание
Enable DoS Prevention	Кликните по полю для включения защиты DoS
Whole System Flood /	
Per-Source IP Flood	Включите и настроите защиту детализировано
Select ALL	Кликните по полю для включения всех функций защиты
Clear ALL	Кликните по полю для выключения всех функций защиты
Apply Changes	Кликните Apply Changes для сохранения настроек
	·

3.3.23 Управление – журнал регистрации

Эта страница используется для настройки удаленного сервера журнала регистрации и просмотра текущих записей в журнале.

This page can be used to set remote lo,	g server and show the system log.	
Enable Log		
🗹 system all	wireless DoS	
Enable Remote Log	Log Server IP Address	
_		
Apply Changes		
Table)		
04am 00-02-18 hr0- port 2	(wland) entering disabled state	
0day 00:02:18 device wland	(wiano) entering uisaorea state O left promiscuous mode	
Oday 00:02:18 br0: port 10	(ethD) entering disabled state	
Oday 00:02:18 device eth0	left promiscuous mode	
107 00100100 or of the second s	outourd a numicourse made	
Oday 00:02:18 device eth0	entered promiscuous mode	
Oday 00:02:18 device eth0 Oday 00:02:18 eth0:phy is	8305	
Oday 00:02:18 device eth0 Oday 00:02:18 eth0:phy is Oday 00:02:18 device wlan	8305 0 entered promiscuous mode	
Oday 00:02:18 device eth0 Oday 00:02:18 eth0:phy is Oday 00:02:18 device wland Oday 00:02:18 br0: port 20	8305 0 entered promiscuous mode (wlan0) entering listening state	
Oday 00:02:18 device eth0 Oday 00:02:18 eth0:phy is Oday 00:02:18 device wland Oday 00:02:18 br0: port 20 Oday 00:02:18 br0: port 10	entered promissions mode 8305 O entered promissions mode (wland) entering listening state (ethD) entering listening state	
Oday 00:02:18 device eth0 Oday 00:02:18 eth0:phy is Oday 00:02:18 device wland Oday 00:02:18 br0: port 2 Oday 00:02:18 br0: port 1 Oday 00:02:18 entering les	entered promiscuous mode 8305 O entered promiscuous mode (wland) entering listening state (ethD) entering listening state aming state	
Oday 00:02:18 device eth0 Oday 00:02:18 th0:phy is Oday 00:02:18 device wlan Oday 00:02:18 br0: port 2(Oday 00:02:18 br0: port 2(Oday 00:02:18 entering le: Oday 00:02:18 br0: port 2(entered promiscuous mode 8305 O entered promiscuous mode (wlanD) entering listening state (ethD) entering listening state arming state (wlanD) entering forwarding state	
Oday 00:02:18 device eth0 Oday 00:02:18 device wlan Oday 00:02:18 br0: port 20 Oday 00:02:18 br0: topolog	entered promiscuous mode 8305 O entered promiscuous mode (wlan0) entering listening state arning state (wlan0) entering forwarding state gy change detected, propagating	
0day 00:02:18 device eth0 0day 00:02:18 eth0:phy is 0day 00:02:18 bt0: port 2 0day 00:02:18 bt0: port 1 0day 00:02:18 bt0: port 1 0day 00:02:18 bt0: port 2 0day 00:02:18 bt0: port 2 0day 00:02:18 bt0: topolog 0day 00:02:18 bt0: port 1	entered promiscuous mode 8305 O entered promiscuous mode (wland) entering listening state arning state (wland) entering forwarding state gy change detected, propagating (eth0) entering learning state	
Oday 00:02:18 device eth0 Oday 00:02:18 device wlan Oday 00:02:18 br0: port 2 Oday 00:02:18 br0: port 1 Oday 00:02:18 br0: port 1 Oday 00:02:18 br0: port 2 Oday 00:02:18 br0: port 2 Oday 00:02:18 br0: topolo Oday 00:02:18 br0: port 1 Oday 00:02:18 br0: port 1	entered promiscuous mode 8305 O entered promiscuous mode (wland) entering listening state (eth0) entering listening state arming state (wland) entering forwarding state gy change detected, propagating (eth0) entering learning state (eth0) entering forwarding state	

Наименование	Описание
Enable Log	Кликните по полю для включения журнала регистрации.
System all	Просмотр всех записей беспроводного широкополосного маршрутизатора.
Wirelessy	Просмотр записей только о радиосвязи.
DoS	Просмотр записей только о Denial-of-Service
Enable Remote Log	Кликните по полю для включения сервиса удалённого журнала регистрации.
Log Server IP Address	Введите IP адрес удалённого журнала регистрации
Apply Changes	Кликните Apply Changes для сохранения настроек
Refresh	Кликните <i>Refresh</i> для обновления журнала регистрации на экране
Clear	Очистка журнала регистрации на экране

3.3.24 Управление – обновление прошивки

Эта страница позволяет вам обновлять прошивку точки доступа до последней версии. Пожалуйста, обратите внимание на то, что не следует отключать питание устройства во время загрузки обновления, поскольку это может повредить систему.

Upgrade	Firmware
This page allows y device during the	rou upgrade the Access Point firmware to new version. Please note, do not power off the upload because it may crash the system.
	<u> </u>
Select File:	Обзор
Upload R	eset

Наименование	Описание
Select File	Кликните по кнопке Browse для выбора файла новой версии прошивки
Upload	Кликните по кнопке Upload для того, чтобы залить выбранный файл на маршрутизатор
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям

3.3.25 Управление – сохранение/перезагрузка настроек

На этой странице вы можете сохранить текущие настройки в виде файла или загрузить файл, который вы сохранили прежде. Кроме того, вы можете вернуть заводские настройки системы.

Save/Reload Setti	ngs	
This page allows you save curren reviously. Besides, you could re	t settings to a file or reload th set the current configuration t	e settings from the file which was saved to factory default.
	or the current county and on t	
Save Settings to File:	Save	
Load Settings from File:		Browse Upload
Reset Settings to Default:	Reset	

Наименование	Описание
Save Settings to File	Кликните по кнопке <i>Save</i> , чтобы сохранить параметры конфигурации на ваш компьютер
Load Settings from File	Кликните по кнопке <i>Browse</i> для того, чтобы выбрать файл конфигурации, а затем кликните по кнопке <i>Upload</i> , чтобы загрузитьить выбранный файл на широкополосный WLAN маршрутизатор
Reset Settings to Default	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к заводским настройкам

3.3.26 Управление – настройка пароля

Эта страница используется для настройки учётной записи для доступа к веб-серверу точки доступа. Пустые поля для имени пользователя и пароля отключают защиту.

Password Set	սթ
This page is used to set th will disable the protection.	e account to access the web server of Access Point. Empty user name and password
User Name:	
New Password:	
Confirmed Password:	
Confirmed Password: Apply Changes	Reset

Моментальный снимок экрана – управление – настройка пароля.

Наименование	Описание
User Name	Введите имя пользователя для контроля логина с помощью веб управления
New Password	Введите пароль для контроля логина с помощью веб управления
Confirmed Password	Т.к. пароль, который вы вводите, невидим, введите его повторно для полтверждения
Apply Changes	Если поля для имени пользователя и пароля останутся пустыми, это будет означать, что контроль логина с помощью веб-управления отключен
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к предыдущим конфигурациям

3.3.27 Управление – WatchDog (сторожевое устройство)

Эта страница используется для выполнения функции watchdog с помощью команды ping. Пользователь устанавливает IP адрес, интервал и другие условия для команды Ping, чтобы понять перезагружается маршрутизатор или нет.

WatchDog Setting
Use ping command to identify whether the router is functional or not. User has to set IP address, interval an fail count to decide reboot router.
Enable WatchDog
WatchDog IP Address: 0.0.0.0
Ping Interval: 30 (30-600 seconds)
Ping Fail to reboot Counter: 3 (3-30)
Apply Changes Reset

Наименование	Описание
Enable WatchDog	Кликните для включения функции watchdog
WatchDog IP Address	IP адрес, к которому обращается устройство
Ping Interval	Введите значение в секундах
Ping Fail to reboot	Введите пороговое значение для перезагрузки маршрутизатора, когда
Count	пропадают пинги
Apply Changes	Кликните по кнопке Apply Changes для завершения новых настроек
Pagat	Кликните по кнопке Reset для прекращения изменений и возврата к
Keset	предыдущим конфигурациям

3.3.28 Управление – Quality of Service (качество сервиса)

Эта страница используется для управления шириной полосы по IP адресу. Пользователь устанавливает общую и неопределенную полосу в первую очередь. Затем регулирует полосу заданием диапазона IP адресов.

Quality of Service
guarantee downstream, upstream and priority and display current settings in the table.
Enable QoS
ISP Bandwidth: Download 0 KB/s Upload 0 KB/s
Undef IP Bandwidth: Download 0 KB/s Upload 0 KB/s
Apply Changes Reset
Bandwith Control
IP Address Range: -
Guarantee Bandwidth: Download KB/s Upload KB/s
Priority: High Y
Apply Changes Reset
Current Bandwidth Control Table:
From IP Addr To IP Addr Downstream (KB/s) (KB/s) Priority Select

Наименование	Описание
Enable QoS	Кликните для включения QoS
ISP Bandwidth	
Download	Введите значения для скорости скачивания в КБ/сек
Upload	Введите значения для скорости закачивания в КБ/сек
Undef IP Bandwidth	

Оборудование семейства MLink

Download	Определите полосу для скачивания, которая ещё не определена	
Upload	Определите полосу для закачивания, которая ещё не определена	
Apply Changes	Кликните по кнопке Apply Changes для завершения новых настроек	
Deset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к	
Reset	предыдущим конфигурациям	

Наименование	Описание
Bandwidth Control	
IP Address Range	Введите начальный и конечный IP адрес
Guarantee Bandwidth	
Download	Введите значения для скорости скачивания в КБ/сек
Upload	Введите значения для скорости закачивания в КБ/сек
Piority	Выберите приоритет: High (высокий), Medium(средний) или Low (низкий)
Apply Changes	Кликните по кнопке Apply Changes для завершения новых настроек. Они
	добавлены в Current Bandwidth Control Table
Reset	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к
Reset	предыдущим конфигурациям
Delete Selected	Кликните для удаления выбранных IP адресов из Current Bandwidth Control
Delete Selected	Table
Delete All	Кликните для удаления всех зарегистрированных записей из Current
Delete All	Bandwidth Control Table
Pagat	Кликните по кнопке <i>Reset</i> для прекращения изменений и возврата к
Keset	предыдущим конфигурациям

4 Часто задаваемые вопросы (FAQ)

4.1 Где и как найти IP и MAC адрес моего компьютера?

IP адрес - это идентификатор компьютера или устройства в сети TCP/IP. Сети, использующие протокол TCP/IP, маршрутизируют сообщения, руководствуясь IP адресом назначения. Формат IP адреса представляет собой 32битный числовой адрес, записанный в виде 4 чисел, разделенных точками. Каждое число может быть от 0 до 255. Например, 191.168.1.254 может быть IP адресом.

МАС адрес (Media Access Control) это уникальный аппаратный номер вашего компьютера. (В сети Ethernet LAN это тот же самый адрес, что и ваш Ethernet adpec). Когда ваш компьютер (или хост, как его определяет Интернетпротокол) подключен к Интернету, ваш физический МАС и IP адреса LANинтерфейса сравниваются в таблице соответствий.

Для того чтобы найти ваш IP и MAC адрес:

- ✓ Откройте программу Command в Microsoft Windows.
- ✓ Впечатайте *ipconfig/all* и нажмите Enter
- ✓ IP адрес вашего компьютера так и будет назван, а МАС адрес определяется как физический адрес

4.2 Что такое Wireless LAN?

Wireless LAN (WLAN) – это сеть, которая обеспечивает доступ в Интернет без проводных соединений к пользовательским машинам.

4.3 Что такое ISM полосы?

(Industrial, Scientific and Medical band) - диапазон ISM

Различные диапазоны радиочастотного спектра, выделяемые на основе международных соглашений для некоммерческого использования в перечисленных выше областях, например 902 - 928 МГц. В 2001 г. частоты с 2,4 по 2,4835 ГГц (UHF) были выделены для беспроводных сетей (WLAN) и других беспроводных технологий.

4.4 Как работает беспроводная сеть?

Стандарт 802.11 определяет два режима: режим инфраструктуры и специальный режим. В первом режиме беспроводная сеть состоит, по крайней мере, из одной точки доступа, подключенной к инфраструктуре проводной сети и комплекта беспроводных станций.

Эта конфигурация называется Basic Service Set (BSS).

Extended Service Set (ESS) – это комплект из двух или больше BSS, формирующих одну подсеть. С тех пор как корпоративные сети WLAN предоставляют доступ к проводным сервисам LAN (файловые сервисы, принтеры, Интернет ссылки), они работают в режиме инфраструктуры.



Пример 1. Режим беспроводной инфраструктуры

4.5 Что такое BSSID?

6-байтовый адрес, который разделяет определенную точку доступа от других. Также известен как просто SSID. Выступает в роли идентификаторы сети или имени.

4.6 Что maкoe ESSID?

Extended Service Set ID (ESSID) – это имя сети, к которой вы хотите получить доступ. Оно используется для идентификации разных беспроводных сетей.

4.7 Каковы причины возникновения помех?

Факторы, вызывающие помехи:

- Преграды: стены, потолки, мебель и т.д.
- Строительные материалы: металлические двери, алюминиевые брусья.
- Электрические устройства: микроволновые печи, мониторы и электрические моторы.

Решения, позволяющие преодолеть помехи:

- Минимизация количества стен и потолков.
- Расположение WLAN антенны для лучшего приёма.
- Держите устройства WLAN вдали от других электрических приборов. В том числе от: микроволновых печей, мониторов, электрических моторов и т.д.
- Добавьте дополнительные WLAN точки доступа, если требуется.

4.8 Что такое Open System и аутентификации Shared Key?

Стандарт IEEE 802.11 поддерживает два подтипа сервисов аутентификации в сетях: open system и shared key. При работе аутентификации open system любая беспроводная станция запрашивает аутентификацию. Станция, которая запрашивает аутентификацию от другой беспроводной станции, посылает аутентификационный управляемый фрейм, который содержит идентификатор станции. Принимающая станция затем возвращает фрейм, который сигнализирует о том, распознаёт ли он посылающую станцию. При использовании shared key аутентификации предполагается, что каждая беспроводная станция получила секретный ключ shared key по безопасному каналу, который независим от канала связи беспроводной сети стандарта 802.11.

4.9 Что такое WEP?

Опциональная функция IEEE 802.11 предлагает приватность при передаче фреймов аналогичную той, которая существует в проводных сетях. Wired Equivalent Privacy (WEP) формирует секретные ключи (shared keys) шифрования таким образом, что обе станции – источника и назначения – могут использовать для сигнализации фреймы с битами для того, чтобы избежать распознавания устройствами слежения.

WEP полагается на секретный ключ, который рассекречен для мобильной станции (например, лэптопа с беспроводной Ethernet картой) и точки доступа

(например, базовой станции). Секретный ключ используется для шифрования пакетов перед их передачей, и проверка однозначности (интерпретации данных) используется для того, чтобы убедиться в неизменности пакетов при передаче. *4.10 Что такое Fragment Threshold?*

Предложенный протокол использует механизм фрагментации фреймов, определенный стандартом IEEE 802.11 для достижения параллельных передач. Большой фрейм данных фрагментируется на несколько блоков, каждый из которых по размеру равен порогу фрагмента (Fragment Threshold). Настраивая значение порога фрагмента, мы можем использовать переменные размеры фрагментов. Определение эффективного порога фрагмента важная задача в этой процедуре. Если порог фрагмента мал, перекрывающая часть основной и параллельной передачи велика. Это означает, что доля пространственного использования параллельной передачи велика. И, наоборот, при большом пороге фрагмента, перекрывающая часть мала и доля пространственного использования мала. Большой порог фрагмента приводит к малым потерям фрагмента.

Порог фрагмента – это максимальный размер пакета, используемый для фрагментации. Пакеты больше запрограммированного размера в соответствующем поле будут фрагментированы.

Если вы обнаружили поврежденные пакеты или ассиметричный приём пакетов, вы можете уменьшить порог фрагмента. Это разобьёт пакеты на более мелкие фрагменты. Эти маленькие фрагменты, если они повреждены, могут быть посланы повторно быстрее, чем большие. Фрагментация увеличивает накладные расходы на передачу, поэтому, выгодно задавать соответствующее значение как можно более близким к максимально возможному.

4.11 Что такое порог RTS (Request To Send)?

Порог RTS – это размер пакета, который допустим для передачи при операции связи RTS/CTS. Стандарт IEEE 802.11-1997 позволяет коротким пакетам передаваться без операции связи RTS/CTS. Каждая станция может иметь разный порог RTS. RTS/CTS используется, когда размер пакетов данных превышает определенный порог RTS. Используя механизм передачи CSMA/CA, передающая станция посылает RTS пакет принимающей станции и ждёт, когда принимающая станция пришлёт обратно пакет CTS (Clear to Send) перед посылкой актуальных пакетов данных.

Эти настройки полезны для сетей с большим количеством клиентов.

С большим количеством клиентов и высокой загрузкой сети будет гораздо больше коллизий. Уменьшая порог RTS, можно уменьшить количество коллизий, и производительность должна возрасти. Пакеты RTS используют полноценную полосу, таким образом, уменьшение полосы может привести к ухудшению производительности.

4.12 Что такое Beacon Interval?

Пакет, переданный точкой доступа для синхронизации в сети. 4.13 Что такое тип преамбулы?

Существует два типа преамбул, определенных в спецификации стандарта IEEE 802.11. Длинная преамбула обычно даёт декодеру больше времени на её обработку. Все устройства 802.11 поддерживают длинную преамбулу. Короткая преамбула разработана для повышения эффективности (например, систем VoIP). Различие между этими двумя типами преамбул находится в поле синхронизации. Длинная преамбула состоит из 128 битов, а короткая - из 56 битов.

4.14 Что такое широковещательная передача SSID?

Широковещательная передача SSID организована в точках доступа с применением радиомаяков. Это позволяет анонсировать вашу точку доступа (включая различные биты информации о ней) для беспроводных устройств в сети. При отключении этой опции, SSID, настроенный у клиента должен согласовываться с SSID точки доступа.

Некоторые беспроводные устройства не могут нормально работать, если SSID не передаётся по широковещательной передаче (например, адаптер D-link DWL-120 USB 802.11b). Как правило, если аппаратура вашего клиента поддерживает работу с отключенным SSID, то это может быть полезно с точки зрения повышения безопасности сети. Однако это не заменит WEP, MAC фильтрацию и другие средства защиты.

4.15 Что такое Wi-Fi Protected Access (WPA)?

Оригинальный механизм безопасности Wi-Fi, Wired Equivalent Privacy (WEP), считается недостаточным для осуществления безопасных бизнес коммуникаций. **Wi-Fi Protected Access** (**WPA** и **WPA2**) — протокол безопасности, применяемый для обеспечения безопасности в беспроводных Wi-Fi сетях.

Он был создан в качестве замены для **Wired Equivalent Privacy** (WEP), который более уязвим. WPA реализует большую часть стандарта IEEE 802.11i и предназначен для замены WEP пока 802.11i не будет готов.

Для обновления WLAN сети таким образом, чтобы она поддерживала WPA, точка доступа затребует программное обеспечение WPA. Клиенты затребуют

обновления программного обеспечения для сетевых карт, и, возможно, обновления операционной системы. Для сетей больших компаний сервер аутентификации (обычно тот, который поддерживает RADIUS и выбранный протокол аутентификации EAP) будет добавлен в сеть.

4.16 Что такое WPA2?

Это второе поколение WPA. WPA2 базируется на поправке IEEE 802.11i к стандарту 802.11. WPA2 реализует полный стандарт, но он не будет работать на некоторых старых сетевых картах.

4.17 Что такое аутентификация 802.1x?

802.1х – это основа для контроля доступа, аутентификации, по МАС адресу, которая определяет Extensible Authentication Protocol (EAP) по сетям LAN (WAPOL). Стандарт инкапсулирует и использует многое из протокола EAP, который был определен для dial-up аутентификации с протоколом точка-точка (Point-to-Point) в RFC 2284. Кроме инкапсуляции пакетов EAP стандарт 802.1х также определяет сообщения EAPOL, которые передают информацию о ключах шифрования (shared key), необходимую для безопасности беспроводной сети.

4.18 Что такое Temporal Key Integrity Protocol (TKIP)?

Тетрогаl Key Integrity Protocol (TKIP) - это часть стандарта шифрования IEEE 802.11i для беспроводных LAN. TKIP – это протокол следующего поколения WEP-шифрования (Wired Equivalency Protocol), который используется для безопасности беспроводных LAN стандарта 802.11. TKIP предоставляет ключи, строящиеся на смешении пакетов, целостности сообщений и механизме смены одного или более шифровальных ключей (re-keying), устраняя, таким образом, недостатки WEP.

4.19 Что такое Advanced Encryption Standard (AES)?

Средства безопасности являются приоритетными для беспроводных LAN. В правительстве США криптографический алгоритм следующего поколения AES заменяет DES и 3DES.

4.20 Что такое Inter-Access Point Protocol (IAPP)?

Протокол стандарта IEEE 802.11f Inter-Access Point Protocol (IAPP) обеспечивает совместимость с производителем точек доступа (Access Point Vendor), включая роуминг станций 802.11 внутри IP-подсети.

IAPP определяет сообщения и данные, которыми обмениваются точки доступа, объекты IAPP и объекты более высоких уровней, для поддержки роуминга. Протокол IAPP использует TCP для связи с Inter-access точками

доступа и UDP для обмена запросами/ответами RADIUS. Он также использует фреймы второго уровня для обновления таблицы адресации устройств второго уровня.

4.21 Что такое Wireless Distribution System (WDS)?

Wireless Distribution System (WDS) - это опция, позволяющая WLAN точкам доступа связываться напрямую с другими точками доступа по беспроводному каналу (например, беспроводные мосты, сервисы повторителей).

4.22 Что такое Universal Plug and Play (uPNP)?

UPnP – это открытая сетевая архитектура, которая состоит из сервисов, устройств и точек контроля. Её конечная цель заключается в разрешении передачи данных между всеми uPnP устройствами в независимости от того, осуществляется ли эта передача в аудиовизуальной среде, среде операционных систем, языков программирования, проводной/беспроводной среде.

4.23 Что такое размер Maximum Transmission Unit (MTU)?

Махітит Transmission Unit (MTU) - максимальный размер передаваемого блока данных сигнализирует о том, что сетевой стек каких-либо пакетов больше величины, которая будет фрагментирована перед передачей. Во время PPP соединения узел PPP подключения отобразит MRU (список последних по времени использования файлов) и будет принят. Настоящий MTU PPP подключения будет назначен самому малому MTU и MRU узла. Значение по умолчанию – 1400.

4.24 Что такое клонирование МАС адреса?

Клонирование МАС адреса предназначено для ваших специальных приложений, которые требуют регистрации клиентов на сервере с одним идентифицированным МАС адресом.

С тех пор как все клиенты выходят во внешние сети через широкополосный WLAN маршрутизатор, функция клонирования МАС адресов, установленная на маршрутизаторе, обеспечивает правильную работу устройств.

4.25 Что такое DDNS?

Аббревиатура DDNS расшифровывается как Dynamic Domain Name Server (сервер динамических доменных имен). DDNS разработан для того, чтобы пользователи получали DNS сервер с динамическим WAN IP адресом.

4.26 Что такое NTP-клиент?

NTP-клиент разработан для получения временной метки из Интернета с помощью протокола Network Time Protocol. Пользователь может указать часовой пояс, IP адрес NTP-сервера.

4.27 Что такое VPN?

Аббревиатура VPN расшифровывается как Virtual Private Network (частная виртуальная сеть). Она разработана для создания частного канала точка-точка в сети общего пользования или публичной сети.

4.28 Что такое IPSEC?

Аббревиатура IPSEC расшифровывается как IP Security (безопасность IP). Используется для безопасной передачи данных по VPN.

4.29 Что такое WLAN реле блокировки между клиентами?

Infrastructure Basic Service Set – это BSS (оборудование базовой станции) с компонентом, называемым Access Point (точка доступа). Точка доступа выполняет функцию локального реле для BSS. Все станции в BSS связываются с точками доступа и более не связываются напрямую. Станции обмениваются фреймами с помощью точек доступа. Эта функция локального реле эффективно дублирует диапазон IBSS.

4.30 Что такое WMM?

WMM основан на подсети стандарта IEEE 802.11e WLAN QoS. WMM возможности Wi-Fi сетям добавляет приоритетные и оптимизирует их производительность, когда одновременно запущенные различные приложения, с разными требованиями по пропускной способности и задержке, конкурируют за доступ сетевым ресурсам. Используя WMM, требования К конечных пользователей удовлетворяются и поддерживаются на более высоком уровне при работе в различных условиях трафика и окружения. WMM делает возможным для домашних пользователей и менеджеров сетей крупных компаний решить, какие информационные потоки наиболее важны, и назначить им соответствующий приоритет по трафику.

4.31 Что такое WLAN ACK TIMOUT?

Фрейм АСК должен получить истечение времени ожидания события (timeout ACK frame). Если удалённо не получилось его получить в указанный период времени, то timeout фрейм будет послан ещё раз.

5 Примеры настроек

5.1 Пример первый – РРРоЕ на WAN

Настройки WAN:

PPPoE

User Name (имя пользователя)	H890123456
Password (пароль)	PW192867543210

Настройки LAN:

IP Address (IP adpec)	192.168.1.254
Subnet Mask (маска подсети)	255.255.255.0
Default Gateway (шлюз по умолчанию)	0.0.0.0
DHCP Client Range (диапазон адресов)	192.168.1.100 - 192.168.1.200

Настройки WLAN:

SSID	MyWLAN
Channel Number (номер канала)	11



Рисунок 5.1 Первый пример конфигурации – РРРоЕ на WAN

Настройка на WAN-интерфейсе

Откройте страницу настроек WAN-интерфейса, затем выберите PPPoE и введите имя пользователяt PPPoE:

"H890123456" и пароль;

" PW192867543210 ",	пароль	на экране	зашифрован.
----------------------------	--------	-----------	-------------

WAN Access Type:	PPPoE [~			
Jser Name:	H890123456		1		
assword :					
Service Name:]		
Connection Type:	Continuous	~	Connect	Disconnect	
Idle Time:	5	(1-1000 m	(setouin		
MTU Size:	1400	(1.360-145	2 bytes)		
O Attain DNS Automa	tically				
• Set DNS Manually					
DNS 1:			1		
DNS 2:			1		
DNS 3:			1		
Clone MAC Address:	000000000000		1		
Enable uPMP					
Enable Ping Acces	S On WAN				
Enable Web Serve	r Access on WA	H			
			and the second se		
Enable IPsec pass	through on YPN	comments			

Нажмите кнопку **Apply Changes** для подтверждения настроек.

Настройка на LAN-интерфейсе:

Откройте страницу настроек LAN-интерфейса, введите IP адрес "192.168.1.254", маску подсети "255.255.255.0", шлюз по умолчанию "0.0.0.0", включите DHCP сервер, DHCP клиентский диапазон адресов от "192.168.1.100" до "192.168.1.200".

AN port of your Access	gure the parameters for local area network which connects to the Point. Here you may change the setting for IP addresss, subnet
nask, DHCP, etc	
IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server 💌
DHCP Client Range:	192.168.1.100 - 192.168.1.200 Show Client
DNS Server:	
Domain Name:	
802.1d Spanning Tree:	Disabled 💌
Clone MAC Address:	00000000000

Нажмите кнопку **Apply Changes** для подтверждения настроек.

Настройка на WLAN-интерфейсе

Откройте страницу настроек WLAN-интерфейса, введите SSID "**MyWLAN**", номер канала"**11**".

Wireless Ba	sic Settings
This page is used to co your Access Point. Her network parameters.	nfigure the parameters for wireless LAN clients which may connect to e you may change wireless encryption settings as well as wireless
Disable Wireless	LAN Interface
Band:	2.4 GHz (8+G) 💌
Mode:	AP 💌
Network Type:	Infrastructure V
SSID:	MyWLAN
Channel Number:	11 💌
Associated Clients:	Show Active Clients
Enable Mac Clon	e (Single Ethernet Client)
📃 Enable Universal	Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Inter	rface:
Apply Changes	Reset

Нажмите кнопку Apply Changes для подтверждения настроек.

5.2 Пример второй – фиксированный IP адрес на WAN

Настройки WAN:

IP Address (IP adpec)	192.168.2.254
Subnet Mask (маска подсети)	255.255.255.0
Default Gateway(шлюз по умолчанию)	192.168.2.10
DNS Address(adpec DNS)	168.95.1.1

Настройки LAN:

IP Address (IP adpec)	192.168.1.254
Subnet Mask (маска подсети)	255.255.255.0
Default Gateway (шлюз по умолчанию)	0.0.0.0
DHCP Client Range (диапазон адресов)	192.168.1.100 - 192.168.1.200

Настройки WLAN:

SSID	MyWLAN
Channel Number (номер канала)	11



Рисунок 5.2 Второй пример конфигурации – фиксированный IP адрес на WAN

Настройка на WAN-интерфейсе:

Откройте страницу настроек WAN-интерфейса, затем выберите Fixed IP и введите IP адрес "**192.168.2.254**", маску подсети "**255.255.255.0**", шлюз по умолчанию "**192.168.2.10**".

Point, Here you may change WAN Access type.	e me parameters for internet setwork which connects to the w Aiv port of your Acces the access method to static IP, DHCP, PPPoE or PPTP by click the item value of
WAN Access Type:	Static IP 🛛 💌
IP Address:	192.168.2.254
Subact Mask:	255.255.255.0
Default Gateway:	192.168.2.10
MTU Size:	1400 (1400-1500 bytes)
DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	00000000000
Enable uPNP	
Enable Ping Acces	3 on WAN
Enable Web Serve	Access on WAN
Enable IPsec pass	through on VPN connection
Enable PPTP pass	through on VPN connection
Enable L2TP pass	through on VPN connection

Нажмите кнопку **Apply Changes** для подтверждения настроек.

Настройка на LAN-интерфейсе:

Откройте страницу настроек LAN-интерфейса, введите IP адрес "**192.168.2.254",** маску подсети "**255.255.255.0**", включите DHCP сервер, введите клиентский диапазон IP адресов "**192.168.1.100**" - "**192.168.1.200**".

Нажмите кнопку **Apply Changes** для подтверждения настроек.

LAN port of your Access	Point. Here you may change the setting for IP addresss, subr
mask, DHCP, etc	
IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server ¥
DHCP Client Range:	192.168.1.100 - 192.168.1.200 Show Client
DNS Server:	
Domain Name:	
802.1d Spanning Tree:	Disabled 💌
Clone MAC Address:	00000000000

Настройка на WLAN-интерфейсе:

Откройте страницу настроек WLAN-интерфейса, введите SSID "**MyWLAN**", номер канала"**11**".

Wireless Basic Settings		
This page is used to co your Access Point. Her network parameters.	nfigure the parameters for wireless LAN clients which may connect to e you may change wireless encryption settings as well as wireless	
🔲 Disable Wireless	LAN Interface	
Band:	2.4 GHz (8+G) 💌	
Mede:	AP 🖌	
Network Type:	Infrastructure 👻	
SSID:	MyWLAN	
Channel Number:	11 💌	
Associated Clients:	Show Active Clients	
Enable Mac Clon	e (Single Ethernet Client)	
📃 Enable Universal	Repeater Mode (Acting as AP and client simultaneouly)	
SSID of Extended Inter	fice:	
Apply Changes	Reset	