

Настройка DAP-1155 в режиме Точка доступа (Access Point)



Подключите устройство к компьютеру кабелем, поставляющимся в комплекте. На сетевой карте, к которой подключено устройство, в настройках TCP/IP укажите IP-адрес – **192.168.0.51** и маску подсети – **255.255.255.0**.

Откройте браузер (рекомендуется использовать Internet Explorer или Mozilla Firefox) и наберите в строке адреса: **dlinkap** или **192.168.0.50**.

Подключение по беспроводной связи к устройству или попытка открытия настроек через любой другой Интернет-браузер не всегда могут быть успешными.

Login: admin

Password: (по умолчанию пароль отсутствует)

Зайдите на вкладку **Setup** (строка вкладок сверху) в раздел **Wireless Setup** (список слева).

Wireless Mode – выберите режим работы устройства Access Point (режим точки доступа);

Wireless Network Name (SSID) – введите название Вашей беспроводной сети (до 32 латинских символов);

802.11 Mode – стандарт Вашей беспроводной сети: Mixed 802.11n, 802.11g and 802.11b; Mixed 802.11n and 802.11g; 802.11n only;

Wireless Channel – канал беспроводной сети (1-13), доступно для выбора если отключена опция автоматического выбора канала (**Enable Auto Channel Scan**);

Channel Width – ширина канала беспроводной сети (20MHz или Auto 20/40MHz);

Visibility Status: Visible – имя вашей сети (SSID) определяется при сканировании;

Invisible – скрытая сеть, для подключения необходимо создать профиль вручную и правильно ввести имя сети (SSID);

Security Mode – тип безопасности вашей сети, доступные типы безопасности: Open, WEP, WPA-Personal, WPA-Enterprise. Рекомендуется использовать типы безопасности WPA-Personal или WPA-Enterprise.

Если Вы установили значение параметра 802.11 Mode – 802.11n only, то типы безопасности WEP и WPA-Personal/Enterprise с типом шифра TKIP будут недоступны для использования.

DAP-1155 //

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

WIZARD

WIRELESS SETUP

LAN SETUP

WIRELESS NETWORK

Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made on this section may also need to be duplicated on your wireless client and PC.

Save Settings

Don't Save Settings

WIRELESS NETWORK SETTINGS :

 Enable Wireless : Always

 Wireless Mode : Access Point

Wireless Network Name : dlink1155 (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Wireless Channel : 6

 Enable Auto Channel Scan :

Channel Width : 20MHz

 Visibility Status : Visible Invisible

WIRELESS SECURITY MODE :

 Security Mode : None

- None
- WEP
- WPA-Personal
- WPA-Enterprise

Helpful Hints..

Wireless Mode :
Select a function mode to configure your wireless network. Function wireless modes include Access Point, AP Client, Bridge, Bridge with AP, Repeater, WISP Client Router and WISP Repeater. Function wireless modes are designed to support various wireless network topologies and applications.

Wireless Network Name :
Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.

Hidden Wireless :
Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to

Примеры настройки различных типов безопасности беспроводной сети будут рассмотрены ниже.

После того как Вы настроили беспроводную сеть (в том числе и тип безопасности) нажмите кнопку **Save Settings** для сохранения настроек и дождитесь готовности устройства.

Пример настройки типа безопасности WEP.

WEP Encryption – Количество бит ключа WEP шифрования:

64 bit – ключ 5 символов ASCII (латинские буквы и цифры) или 10 символов HEX (цифры и буквы от A до F);

128 bit – ключ 10 символов ASCII или 23 символа HEX;

WEP Key 1 – поле для ввода ключа шифрования;

WIRELESS SECURITY MODE :	
Security Mode :	WEP
WEP :	
WEP is the wireless encryption standard. To use it you must enter the same key(s) into the AP and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.	
You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. 5 text characters can be entered for 64 bit keys, and 13 characters for 128 bit keys.	
If you choose the WEP security option this device will ONLY operate in Legacy Wireless mode (802.11B/G) . This means you will NOT get 11N performance due to fact that WEP is not supported by the Draft 11N specification.	
WEP Encryption :	64Bit(10hex digits)
WEP Key 1 :	12345
Authentication :	Both

Hidden Wireless :
Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.

Security Keys :
If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

Bridge setting :
If you want to bridge with the other Bridge AP, please write down the MAC address of the Bridge AP. Besides, you also need to write down the MAC address of your Bridge AP to the other one.

Пример настройки типа безопасности WPA-Personal.

WPA Mode – выберите технологию WPA: WPA, WPA2, AUTO (WPA or WPA2);

Cipher Type – алгоритм шифрования: TKIP, AES, TKIP and AES;

Pre-Shared Key – поле для ввода парольной фразы (от 8 до 63 символов – латинские буквы или цифры);

WIRELESS SECURITY MODE :	
Security Mode :	WPA-Personal
WPA	
Use WPA of WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access some gaming and legacy devices work only in this mode.	
To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher)	
WPA Mode :	AUTO(WPA or WPA2)
Cipher Type :	AES
PRE-SHARED KEY	
Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.	
Pre-Shared Key :	••••••••

Hidden Wireless :
Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.

Security Keys :
If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

Bridge setting :
If you want to bridge with the other Bridge AP, please write down the MAC address of the Bridge AP. Besides, you also need to write down the MAC address of your Bridge AP to the other one.

Для обеспечения высокого уровня безопасности Вашей беспроводной сети рекомендуется использовать технологию WPA2 и тип шифрования AES.

Пример настройки типа безопасности WPA-Enterprise.

Тип безопасности WPA-Enterprise предусматривает использование внешнего сервера аутентификации (RADIUS сервера).

WPA Mode – выберите технологию WPA: WPA, WPA2, AUTO (WPA or WPA2);

Cipher Type – алгоритм шифрования: TKIP, AES, TKIP and AES;

RADIUS Server IP Address – ip адрес внешнего RADIUS сервера;

RADIUS Server Port – порт, на который будут отправлены запросы проверки подлинности клиентов;

RADIUS Server Shared Secret – парольная фраза для подключения к RADIUS серверу;

Advanced – расширенные параметры, используются для настройки подключения к альтернативному RADIUS серверу.

The screenshot displays the configuration interface for wireless security. It is divided into several sections:

- WIRELESS SECURITY MODE :** A dropdown menu is set to "WPA-Enterprise".
- WPA:** A text block explains that WPA2 mode provides a balance of security and compatibility. It notes that WPA2 Only mode uses AES(CCMP) and that legacy devices are not supported. Below this, "WPA Mode" is set to "AUTO(WPA or WPA2)" and "Cipher Type" is set to "AES".
- EAP (802.1X):** A note states that when WPA enterprise is enabled, the router uses EAP(802.1x) to authenticate clients via a remote RADIUS server. Below this, three fields are filled: "RADIUS Server IP Address" (192.168.0.254), "RADIUS Server Port" (1812), and "RADIUS Server Shared Secret" (test). An "Advanced" button is located at the bottom left of this section.
- Hidden Wireless :** A sidebar note explaining that enabling hidden mode prevents wireless clients from seeing the network during scans.
- Security Keys :** A sidebar note advising that users should write down WEP keys or passphrases for manual entry on wireless devices.
- Bridge setting :** A sidebar note instructing users to write down MAC addresses of bridge APs.
- Bridge Security :** A sidebar note advising users to write down WEP keys or passphrases for bridge security.

Для обеспечения высокого уровня безопасности Вашей беспроводной сети рекомендуется использовать технологию WPA2 и тип шифрования AES.