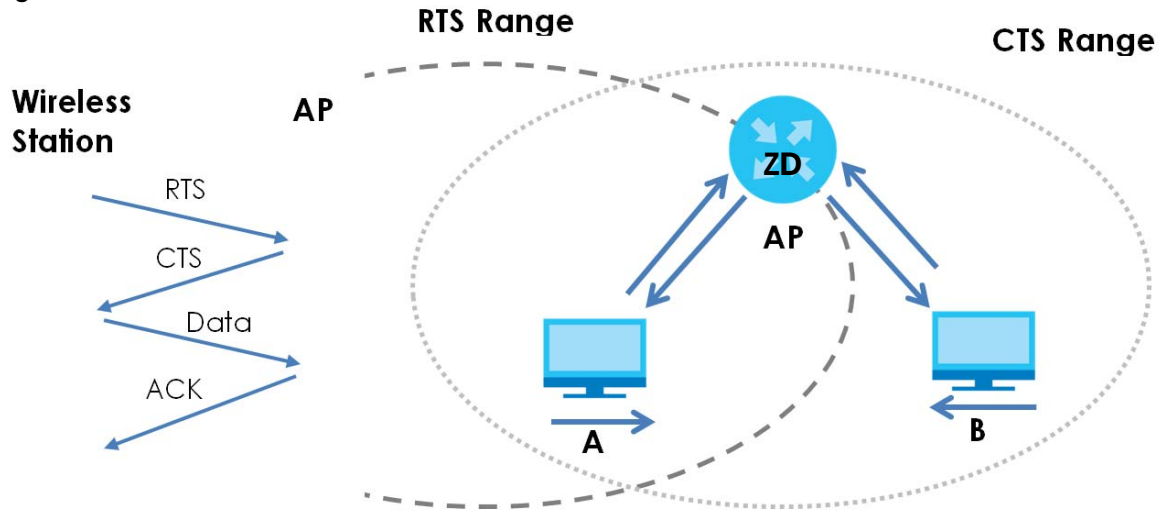


Figure 292 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 191 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between WiFi clients, access points and the wired network.

Wireless security methods available on the Zyxel Device are data encryption, WiFi client authentication, restricting access by device MAC address and hiding the Zyxel Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Zyxel Device.

Table 192 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
Most Secure	WiFi Protected Access (WPA)
	WPA2

Note: You must enable the same wireless security settings on the Zyxel Device and on all WiFi clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the WiFi clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the WiFi client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.
- Access-Challenge
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
Sent by the access point requesting accounting.
- Accounting-Response
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the WiFi client. The WiFi client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the WiFi clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 193 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

WiFi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the WiFi clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and WiFi client. As long as the passwords match, a WiFi client will be granted access to a WLAN.

If the AP or the WiFi clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or WiFi clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a WiFi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevents all wireless devices sharing the same encryption keys. (a weakness of WEP).

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate WiFi clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a WiFi client to store the PMK it derived through a successful authentication with an AP. The WiFi client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the WiFi client (already connected to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

WiFi Client WPA Supplicants

A WiFi client supplicant is the software that runs on an operating system instructing the WiFi client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

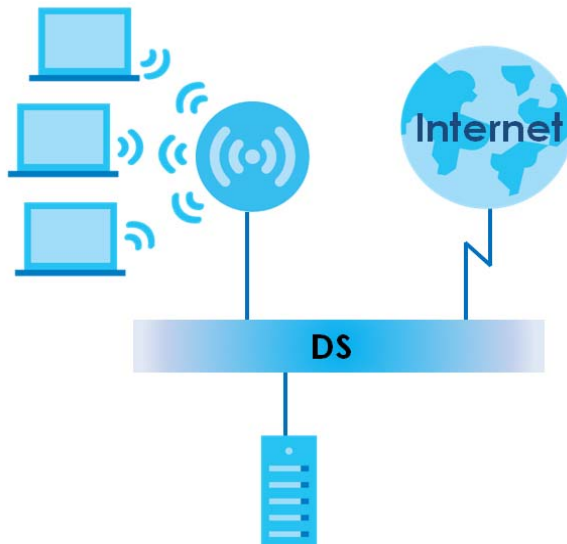
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" WiFi client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the WiFi client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients.

Figure 293 WPA(2) with RADIUS Application Example

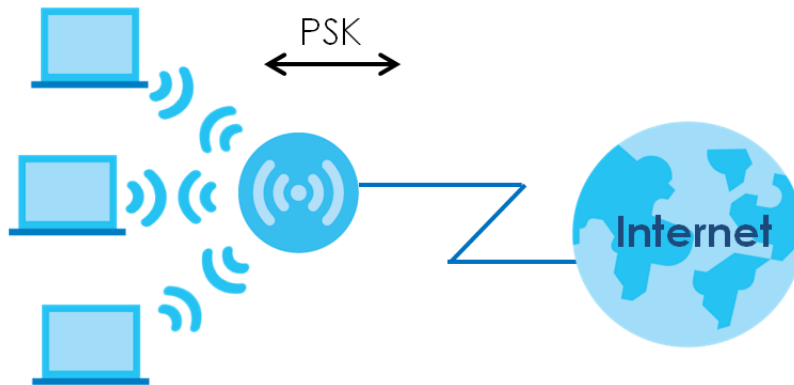


WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all WiFi clients. The Pre-Shared Key (PSK) must consist of between 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.
- 2 The AP checks each WiFi client's password and allows it to join the network only if the password matches.
- 3 The AP and WiFi clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
- 4 The AP and WiFi clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 294 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 194 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4 GHz (IEEE 802.11b and IEEE 802.11g) or 5 GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WiFi

There are two types of antennas used for WiFi applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

APPENDIX C

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as `"/x"` where x is a number. For example,

`2001:db8:1a2b:15::1a2f:0/32`

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of `fe80::/10`. The link-local unicast address format is as follows.

Table 195 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multicast Address

In IPv6, Multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A Multicast address allows a host to send packets to all hosts in a Multicast group.

Multicast scope allows you to determine the size of the Multicast group. A Multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined Multicast addresses.

Table 196 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.

The following table describes the Multicast addresses which are reserved and cannot be assigned to a Multicast group.

Table 197 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 198

MAC	00	:	13	:	49	:	12	:	34	:	56
-----	----	---	----	---	----	---	----	---	----	---	----

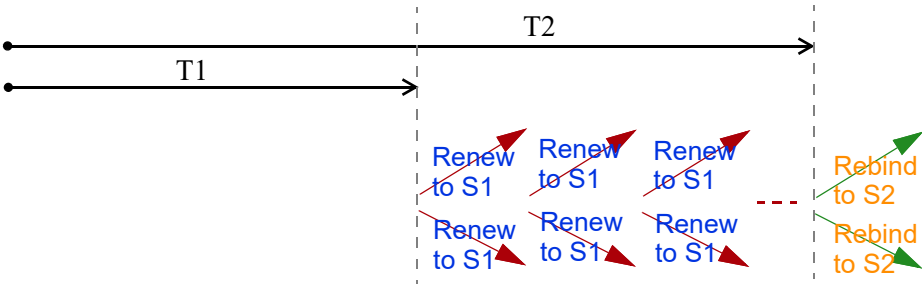
Table 199

EUI-64	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56
--------	----	---	----	---	----	---	----	---	----	---	----	---	----	---	----

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by Multicast, the Zyxel Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical Multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device receives

a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unreach, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive Multicast packets and the IP addresses of Multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which Multicast groups a port can join.

MLD Messages

A Multicast router or switch periodically sends general queries to MLD hosts to update the Multicast forwarding table. When an MLD host wants to join a Multicast group, it sends an MLD Report message for that address.

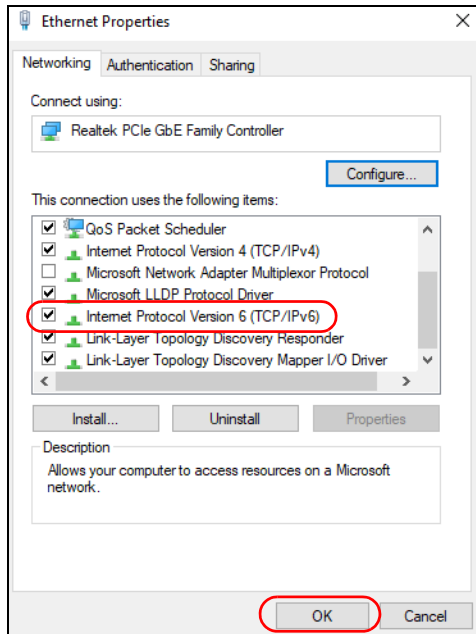
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a Multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 10

Windows 10 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 10 computer.

To enable IPv6 in Windows 10:

- 1 Click the start icon, **Settings** and then **Network & Internet**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click the Search icon (🔍) and then enter "cmd" in the search box.
- 5 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:f
```

APPENDIX D

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**.
 - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 200 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol – a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for email.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System – NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.

Table 200 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get email from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).

Table 200 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user- defined	A videoconferencing solution. The UDP port number is specified in the application.

APPENDIX E

Legal Information

Copyright

Copyright © 2025 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America



The following information applies if you use the product within USA area.

FCC Statement

- The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful

interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

The following information applies to products with wireless functions.

- For 2.4G WLAN, only channels 1~11 are operational. Selection of other channels is not possible.
- Operation of this device is restricted to indoor use only, unless the relevant user's manual states that this device can be installed outdoors.

FCC Radiation Exposure Statement

- This device complies with FCC Radio Frequency (RF) radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 50 cm (EE6510-10), 21 cm (EE4410-00), and 20 cm (all other models) from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

The following information applies for products operating in the 5.925 - 7.125 GHz band.

Low-power Indoor Access Point

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925 - 6.425 GHz band.
- Operation of transmitters in the 5.925 - 7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Standard Power Access Point

- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.
- Operation of transmitters in the 5.925 - 7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Canada

The following information applies if you use the product within Canada.

CAN ICES(B) / NMB(B)

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:
 - (1) this device may not cause interference, and
 - (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence.
L'exploitation est autorisée aux deux conditions suivantes:
 - (1) l'appareil ne doit pas produire de brouillage;
 - (2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- For 2.4 G WLAN, only channels 1-11 are operational. Selection of other channels is NOT possible.
- Pour le WLAN 2,4 G, seuls les canaux 1 à 11 sont opérationnels. La sélection d'autres canaux n'est PAS possible.
- The device operating in the 5150 - 5250 MHz band is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- Where applicable, antenna type(s), antenna model(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.
- Les dispositifs fonctionnant dans la bande de 5150 à 5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'incidence nécessaires pour rester conforme à la limite de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Industry Canada radiation exposure statement

This equipment complies with ISSED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 23 cm (EE6601-00), 29 cm (EE6510-10), 24 cm (EE4410-00), and 20 cm (all other models) between the radiator and your body.

Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements ISSED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 23 cm (EE6601-00), 29 cm (EE6510-10), 24 cm (EE4410-00), et 20 cm (tous les autres modèles) de distance entre la source de rayonnement et votre corps.

The following information applies for products operating in the 5.925-7.125 GHz band.

RLAN Devices

- Devices shall not be used for control of or communications with unmanned aircraft systems.

dispositifs RLAN

- Les dispositifs ne doivent pas être utilisés pour commander des systèmes d'aéronef sans pilote ni pour communiquer avec de tels systèmes.

Low-power indoor access points and indoor subordinate devices

- Operation shall be limited to indoor use only.
- Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited except for on large aircraft flying above 3,048 m (10,000 ft).

Points d'accès intérieurs de faible puissance et dispositifs subordonnés intérieurs

- leur utilisation doit être limitée à l'intérieur seulement;
- leur utilisation à bord de plateformes de forage pétrolier, d'automobiles, de trains, de navires maritimes et d'aéronefs doit être interdite, sauf à bord d'un gros aéronef volant à plus de 3 048 m (10 000 pi) d'altitude.

Standard-power access points and fixed client devices

- Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited.
- Information for antenna type(s), antenna model(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 4.5.4.c shall be clearly indicated.

Points d'accès de puissance normale et dispositifs clients fixes

- leur utilisation à bord de plateformes de forage pétrolier, d'automobiles, de trains, de navires maritimes et d'aéronefs doit être interdite;
- le ou les types d'antennes, le ou les modèles d'antennes et le ou les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la section 4.5.4(c) sur le masque de p.i.r.e par rapport à l'angle de site doivent être clairement indiqués.

Europe and the United Kingdom



The following information applies if you use the product within the European Union and United Kingdom.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK Radio Equipment Regulations 2017

Model List: DE1301-00, DE3301-00, EE1301-00, EE3301-00, EE5301-00, EE6601-00, PE3101-00, PE3301-00, PE5301-01

- Compliance information for wireless products relevant to the EU, United Kingdom, and other Countries following the EU Directive 2014/53/EU (RED) and UK Radio Equipment Regulations 2017. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:

- In the majority of the EU, United Kingdom, and other European countries, the 5 GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5 GHz wireless LANs.
- If this device operates in the 5150 to 5350 MHz band, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF operating power for each band is as follows:
- DE1301-00 / DE3301-00 / EE1301-00
 - 97.05 mW for the 2,400 to 2,483.5 MHz band
 - 198.15 mW for the 5,150 to 5,350 MHz band
 - 957.19 mW for the 5,470 to 5,725 MHz band
 - 199.53 mW for the 5,725 to 5,850 MHz band (UK only)
- EE3301-00 / PE3301-00
 - 97.95 mW for the 2,400 to 2,483.5 MHz band
 - 197.70 mW for the 5,150 to 5,350 MHz band
 - 988.55 mW for the 5,470 to 5,725 MHz band
 - 196.79 mW for the 5,725 to 5,850 MHz band (UK only)
- EE5301-00 / PE5301-01
 - 95.06 mW for the 2,400 to 2,483.5 MHz band
 - 176.20 mW for the 5,150 to 5,350 MHz band
 - 887.16 mW for the 5,470 to 5,725 MHz band
 - 177.42 mW for the 5,725 to 5,850 MHz band (UK only)
- EE6601-00
 - 83.95 mW for the 2,400 to 2,483.5 MHz band
 - 165.58 mW for the 5,150 to 5,350 MHz band
 - 749.89 mW for the 5,470 to 5,725 MHz band
 - 170.22 mW for the 5,725 to 5,850 MHz band (UK only)
 - 165.96 mW for the 5,945 to 6,425 MHz band
- PE3101-00
 - 100 mW for the 2,400 to 2,483.5 MHz band
 - 199.53 mW for the 5,150 to 5,350 MHz band
 - 1000 mW for the 5,470 to 5,725 MHz band
 - 199.53 mW for the 5,725 to 5,850 MHz band (UK only)

Belgium (English)	National Restrictions
België (Flemish)	The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.
Belgique (French)	- Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. - Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. National Restrictions - This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check https://www.mise.gov.it/it/ for more details. - Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare https://www.mise.gov.it/it/ per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan taghmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.

Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.

Notes:

- Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not put the device in a place that is humid, dusty, has extreme temperatures, or that blocks the device ventilation slots. These conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for power rating of the device and operating temperature.
- There is a remote risk of electric shock from lightning: (1) Do not use the device outside, and make sure all the connections are indoors. (2) Do not install or service this device during a thunderstorm.
- The Power Supply is not waterproof, avoid contact with liquid. Handle the Power Supply with care; do not pry open, nor pull or press the pins on it.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device. Opening or removing the device covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connected cables carefully so that no one will step on them or stumble over them.

- Disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect the power adaptor or cord to the right supply voltage (for example, 120 VAC in North America or 230 VAC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove the damaged power adaptor or cord from the device and the power source. Contact your local vendor to order a new one.
- CAUTION: There is a risk of explosion if you replace the device battery with an incorrect one. Dispose of used batteries according to the instructions. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not leave a battery in an extremely high temperature environment or surroundings since it can result in an explosion or the leakage of flammable liquid or gas.
- Do not subject a battery to extremely low air pressure since it may result in an explosion or the leakage of flammable liquid or gas.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For a permanently connected device, a readily accessible method to disconnect the device shall be incorporated externally to the device;
 - For a pluggable device, the socket-outlet shall be installed near the device and shall be easily accessible.
- This product is intended to be supplied by a DC power source marked 'L.P.S' or 'Limited Power Source'. The rating for each model is as follows:
 - DE1301-00 / DE3301-00: 12 VDC / 2 A / Tma 40 °C
 - EE1301-00: 12 VDC / 2 A / Tma 40 °C
 - EE3301-00 / EE5301-00: 12 VDC / 2.5 A / Tma 40 °C
 - EE4410-00: 12 VDC / 3 A / Tma 40 °C
 - EE6510-10: 12 VDC / 3.5 A / Tma 40 °C
 - EE6601-00: 12 VDC / 3.5 A / Tma 40 °C
 - PE3101-00: 12 VDC / 2 A / Tma 40 °C
 - PE3301-00: 12 VDC / 2.5 A / Tma 40 °C
 - PE5301-01: 12 VDC / 3 A / Tma 40 °C

The following information applies for products with PON/Laser:

- CLASS 1 LASER PRODUCT & "IEC 60825-1:2014"
- CLASS 1 CONSUMER LASER PRODUCT & "EN 50689:2021"
- Caution – Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.
- Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019.

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.
- Attention: L'utilisation des commandes ou réglages ou l'exécution des procédures autres que celles spécifiées dans les présents exigences peuvent être la cause d'une exposition à un rayonnement dangereux

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8 W, and/or
- Off mode power consumption < 0.5 W, and/or
- Standby mode power consumption < 0.5 W.

(Wireless setting, please refer to the chapter about wireless settings for more detail.)

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil,

llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 本機限在不干擾合法電台與不被干擾保障條件下於室內使用。本產品使用時建議應距離人體 20 cm 以上。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 – 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓（如：台灣供應電壓 110 伏特）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: <https://service-provider.zyxel.com/global/en/gpl-oss-software-notice>.

Index

Numbers

6rd
IPv6 [168](#)

A

access
troubleshooting [472](#)
Access Control (Rules) screen [349](#)
ACK message [401](#)
activation
firewalls [347](#)
media server [340, 341](#)
SSID [214](#)
Address Resolution Protocol [419](#)
antenna
directional [499](#)
gain [499](#)
omni-directional [499](#)
Any_WAN
Remote Management [443](#)
AP (access point) [490](#)
Application Layer Gateway (ALG) [306](#)
applications
media server [339](#)
activation [340, 341](#)
iTunes server [339](#)
applications, NAT [314](#)
ARP Table [419](#)
Asynchronous Transfer Mode [167](#)
ATM [167](#)
authentication [229](#)

B

backup
configuration [462](#)

backup configuration [462](#)
Backup/Restore screen [461](#)
bandwidth capacity
cable type [27](#)
Basic Service Set, See BSS [488](#)
Basic Service Set, see BSS
blinking LEDs [31](#)
Bridge mode [177, 186](#)
broadband [165](#)
Broadband screen
overview [165](#)
broadcast [201](#)
BSS [231, 488](#)
example [232](#)
button
WLAN [54, 58](#)
BYE request [401](#)

C

CA [373, 494](#)
cable type
Ethernet [27](#)
call hold [406, 407](#)
call service mode [406, 407](#)
call transfer [407, 408](#)
call waiting [406, 408](#)
Canonical Format Indicator See CFI
CCMs [467](#)
certificate
details [374](#)
factory default [366](#)
file format [373](#)
file path [371](#)
import [366, 370](#)
public and private keys [373](#)
verification [374](#)
Certificate Authority
See CA.

- certificate request
 - create [366](#)
 - view [368](#)
 - certificates [365](#)
 - advantages [373](#)
 - authentication [365](#)
 - CA [365](#), [373](#)
 - creating [367](#)
 - public key [365](#)
 - replacing [366](#)
 - storage space [366](#)
 - thumbprint algorithms [374](#)
 - trusted CAs [371](#)
 - verifying fingerprints [374](#)
 - Certification Authority [365](#)
 - Certification Authority, see CA
 - certifications [518](#)
 - viewing [523](#)
 - CFI [200](#)
 - CFM [467](#)
 - CCMs [467](#)
 - link trace test [467](#)
 - loopback test [467](#)
 - MA [467](#)
 - MD [467](#)
 - MEP [467](#)
 - MIP [467](#)
 - channel [490](#)
 - interference [490](#)
 - Class of Service [404](#)
 - Class of Service, see CoS
 - client list [244](#)
 - client-server protocol [398](#)
 - comfort noise generation [403](#)
 - configuration
 - backup [462](#)
 - firewalls [347](#)
 - restoring [463](#)
 - static route [317](#)
 - Connectivity Check Messages, see CCMs
 - contact information [483](#)
 - copyright [511](#)
 - CoS [292](#), [404](#)
 - CoS technologies [276](#)
 - Create Certificate Request screen [367](#)
 - creating certificates [367](#)
 - CTS (Clear to Send) [491](#)
 - CTS threshold [223](#), [229](#)
 - customer support [483](#)
 - customized service [348](#)
 - add [349](#)
 - customized services [349](#)
- ## D
- data fragment threshold [223](#), [229](#)
 - DDoS [346](#)
 - Denials of Service, see DoS
 - DHCP [238](#), [254](#)
 - DHCP Server Lease Time [242](#)
 - DHCP Server State [242](#)
 - diagnostic [467](#)
 - diagnostic screens [467](#)
 - differentiated services [405](#)
 - Differentiated Services, see DiffServ [292](#)
 - DiffServ [292](#)
 - marking rule [293](#)
 - DiffServ (Differentiated Services) [404](#)
 - code points [404](#)
 - marking rule [405](#)
 - digital IDs [365](#)
 - disclaimer [511](#)
 - distance maximum
 - cable type [27](#)
 - DLNA [339](#)
 - DMZ screen [305](#)
 - DNS [238](#), [254](#)
 - DNS server address assignment [201](#)
 - DNS Values [242](#)
 - Domain Name [315](#)
 - domain name system, see DNS
 - DoS [345](#)
 - thresholds [346](#)
 - DoS protection blocking
 - enable [352](#)
 - DS field [293](#), [405](#)
 - DS, see differentiated services
 - DSCP [292](#), [404](#)
 - DSL

- counters [427](#)
- port details [427](#)
- statistics [426](#)
- Dual Stack Lite [168](#)
- dual/tri-radios [24](#)
- dual-band application [24](#)
- dual-band gateway [23](#)
- dynamic DNS [316](#)
 - wildcard [316](#)
- Dynamic Host Configuration Protocol, see DHCP
- dynamic WEP key exchange [495](#)
- DYNDNS wildcard [316](#)

E

- EAP Authentication [494](#)
- ECHO [315](#)
- echo cancellation [403](#)
- email
 - log example [455](#)
 - log setting [455](#)
- Encapsulation [197](#)
 - MER [197](#)
 - PPP over Ethernet [198](#)
- encapsulation
 - RFC 1483 [198](#)
- encapsulation method
 - technical reference [197](#)
- encryption [496](#)
- ESS [489](#)
- Ether Type [284](#)
- Europe type call service mode [406](#)
- Extended Service Set IDentification [210, 216](#)
- Extended Service Set, See ESS [489](#)

F

- factory-default configuration
 - reload [67](#)
- Fast Leave [323](#)
- file sharing [29](#)
- filters

- MAC address [217, 230](#)
- Finger services [315](#)
- firewall
 - enhancing security [354](#)
 - LAND attack [346](#)
 - security considerations [354](#)
 - traffic rule direction [352](#)
- Firewall DoS screen [352](#)
- Firewall General screen [347](#)
- firewall rules
 - direction of travel [353](#)
- firewalls [345, 347](#)
 - actions [352](#)
 - configuration [347](#)
 - customized service [348](#)
 - customized services [349](#)
 - DDoS [346](#)
 - DoS [345](#)
 - thresholds [346](#)
 - ICMP [346](#)
 - Ping of Death [346](#)
 - rules [353](#)
 - security [354](#)
 - SYN attack [345](#)
- firmware [457](#)
- Firmware Upgrade screen [457, 459](#)
- firmware upload [457, 459](#)
- flash key [405](#)
- flashing [405](#)
- fragmentation threshold [223, 229, 491](#)

G

- G.168 [403](#)
- General wireless LAN screen [205](#)
- Guide
 - Quick Start [2](#)

H

- hidden node [490](#)
- Home Security URL filtering [357](#)
- HTTP [315](#)

I

- IBSS [488](#)
- ICMP [346](#)
- ICMPv6 [321](#)
- IEEE 802.11ax [203](#)
- IEEE 802.11g [492](#)
- IEEE 802.1Q [200](#)
- IGA [313](#)
- IGMP [201](#)
 - multicast group list [322, 424, 425](#)
 - version [201](#)
- IGMP Fast Leave [321](#)
- IGMPv2 [321](#)
- IGMPv3 [321](#)
- ILA [313](#)
- Import Certificate screen [371](#)
- importing trusted CAs [371](#)
- Independent Basic Service Set
 - See IBSS [488](#)
- initialization vector (IV) [496](#)
- Inside Global Address, see IGA
- Inside Local Address, see ILA
- interface group [327](#)
- Internet
 - no access [476](#)
 - wizard setup [81](#)
- Internet access
 - wizard setup [81](#)
- Internet Blocking [147](#)
- Internet connection
 - add or edit [170, 180](#)
 - slow or erratic [478](#)
- Internet Control Message Protocol, see ICMP
- Internet Protocol version 6 [167](#)
- Internet Protocol version 6, see IPv6
- Intra LAN Multicast [323](#)
- IP address [255](#)
 - private [255](#)
 - WAN [166](#)
- IP address assignment [200](#)
- IP alias
 - NAT applications [314](#)
- IP over Ethernet [197](#)
- IP packet

- transmission method [201](#)
- IPoE technical reference [197](#)
- IPv4 firewall [347](#)
- IPv6 [167, 501](#)
 - addressing [167, 201, 501](#)
 - EUI-64 [503](#)
 - global address [501](#)
 - interface ID [503](#)
 - link-local address [501](#)
 - Neighbor Discovery Protocol [501](#)
 - ping [501](#)
 - prefix [167, 202, 501](#)
 - prefix and length [167](#)
 - prefix delegation [169](#)
 - prefix length [167, 202, 501](#)
 - subnet mask [167](#)
 - unspecified address [502](#)
- IPv6 address
 - abbreviation method [201](#)
- IPv6 firewall [347](#)
- IPv6 rapid deployment [168](#)
- iTunes server [339](#)
- ITU-T [403](#)

K

- key combinations [409](#)
- keypad [409](#)

L

- LAN [237](#)
 - client list [244](#)
 - DHCP [254](#)
 - DNS [254](#)
 - IP address [255](#)
 - MAC address [245](#)
 - status [153, 160](#)
 - subnet mask [239, 255](#)
- LAN IPv6 Mode Setup [243](#)
- LAN Setup screen [239](#)
- LAN subnet mask [242](#)
- LAN to LAN multicast [323](#)
- LAND attack [346](#)

LBR [467](#)
LED description [32, 34, 35, 36, 37, 40, 43, 44](#)
limitations
 wireless LAN [231](#)
 WPS [236](#)
link trace [467](#)
Link Trace Message, see LTM
Link Trace Response, see LTR
listening port [388](#)
Local Area Network, see LAN
Local Certificates screen [365](#)
log setting [453](#)
Log Setting screen [453](#)
login [68](#)
 password [68](#)
Login screen
 no access [473](#)
logs [410](#)
Loop Back Response, see LBR
loopback [467](#)
LTM [467](#)
LTR [467](#)

M

MA [467](#)
MAC address [219, 245](#)
 filter [217, 230](#)
 LAN [245](#)
MAC Authentication screen [217](#)
MAC Filter [355](#)
Maintenance Association, see MA
Maintenance Domain, see MD
Maintenance End Point, see MEP
managing the device
 good habits [30](#)
Maximum Burst Size (MBS) [199](#)
MBSSID [232](#)
MD [467](#)
media server [339](#)
 activation [340, 341](#)
 iTunes server [339](#)
MEP [467](#)

MESH
 enable [227](#)
MGMT Services screen [441](#)
MLD [321](#)
MLDv1 [321](#)
MLDv2 [321](#)
MTU (Multi-Tenant Unit) [200](#)
Multi_WAN
 Remote Management [443](#)
multicast [201](#)
Multicast Listener Discovery, see MLD
multi-gigabit [27](#)
multimedia [397](#)
Multiple BSS, see MBSSID
multiplexing [198](#)
 LLC-based [198](#)
 VC-based [198](#)
multiprotocol encapsulation [198](#)

N

NAT [312, 313](#)
 applications [314](#)
 IP alias [314](#)
 default server [305](#)
 DMZ host [305](#)
 example [314](#)
 global [313](#)
 IGA [313](#)
 ILA [313](#)
 inside [313](#)
 local [313](#)
 multiple server example [298](#)
 outside [313](#)
 port number [315](#)
 services [315](#)
NAT ALG screen [306, 307, 309](#)
NAT example [315](#)
Network Address Translation, see NAT
network disconnect
 temporary [458](#)
network map [147](#)
NNTP [315](#)
Nslookup test [468](#)

O

OK response [401, 402](#)
online firmware [459](#)
Optical Signal Status screen [434](#)
Others screen [223](#)

P

Packet Transfer Mode [167](#)
Pairwise Master Key (PMK) [496, 498](#)
parental control
 schedule setup [360, 362](#)
password [68](#)
 admin [473](#)
 lost [473](#)
 user [473](#)
PBC [233](#)
Peak Cell Rate (PCR) [198](#)
Per-Hop Behavior, see PHB [293](#)
PHB [293, 405](#)
phone functions [409](#)
PIN, WPS [233](#)
Ping of Death [346](#)
Ping test [468](#)
Ping/TraceRoute/Nslookup screen [468](#)
Point-to-Point Tunneling Protocol, see PPTP
POP3 [315](#)
port forwarding rule
 add/edit [299](#)
Port Forwarding screen [298, 299](#)
Port Triggering
 add new rule [303](#)
Port Triggering screen [301](#)
ports [31](#)
POWER button [47, 48, 50, 52, 54, 56, 58, 60, 63, 65](#)
POWER LED [32, 34, 35, 36, 37, 39, 40, 41, 43, 44](#)
PPPoE [198](#)
 Benefits [198](#)
 technical reference [198](#)
PPTP [315](#)
preamble [225, 229](#)
preamble mode [232](#)

prefix delegation [169](#)
private IP address [255](#)
problems [471](#)
Protocol (Customized Services) screen [348](#)
Protocol Entry
 add [349](#)
PSK [496](#)
PTM [167](#)
Push Button Configuration, see PBC
push button, WPS [233](#)

Q

QoS [275, 292, 404](#)
 marking [276](#)
 setup [275](#)
 tagging [276](#)
 versus CoS [275](#)
Quality of Service, see QoS
Quick Start Guide [2](#)

R

RADIUS [493](#)
 message types [493](#)
 messages [493](#)
 shared secret key [494](#)
Real time Transport Protocol, see RTP
Reboot screen [465](#)
reset [67](#)
RESET button [47, 48, 51, 52, 54, 56, 58, 60, 63, 65](#)
 using [67](#)
restart system [465, 466](#)
restoring configuration [463](#)
RFC 1058, see RIP
RFC 1389, see RIP
RFC 1483 [198](#)
RFC 1631 [297](#)
RFC 1889 [400](#)
RIP [273](#)
Routing Information Protocol, see RIP
routing table [421](#)

RTP [400](#)

RTS (Request To Send) [491](#)
threshold [490, 491](#)

RTS threshold [223, 229](#)

S

security

network [354](#)

wireless LAN [229](#)

Security Log [411](#)

Security Parameter Index, see SPI

service access control [444](#)

Service Set [210, 216](#)

services

port forwarding [315](#)

Session Initiation Protocol, see SIP

setup

firewalls [347](#)

static route [317](#)

silence suppression [403](#)

Single Rate Three Color Marker, see srTCM

SIP [397](#)

account [397](#)

call progression [400](#)

client [398](#)

identities [397](#)

INVITE request [401, 402](#)

number [397](#)

OK response [402](#)

proxy server [398](#)

redirect server [399](#)

register server [400](#)

servers [398](#)

service domain [397](#)

URI [397](#)

user agent [398](#)

SMTP [315](#)

SPI [346](#)

srTCM [295](#)

SSH

unusable [475](#)

SSID [230](#)

activation [214](#)

MBSSID [232](#)

static DHCP [244](#)

configuration [246](#)

Static DHCP screen [244](#)

static route [264, 273](#)

configuration [317](#)

status [147](#)

LAN [153, 160](#)

WAN [152](#)

wireless LAN [153](#)

status indicators [31](#)

subnet mask [255](#)

supplementary services [405](#)

Sustained Cell Rate (SCR) [199](#)

SYN attack [345](#)

syslog logging

enable [455](#)

syslog server

name or IP address [455](#)

system

firmware [457](#)

online firmware [459](#)

password [68](#)

reset [67](#)

status [147](#)

LAN [153, 160](#)

WAN [152](#)

wireless LAN [153](#)

time [447](#)

T

Telnet

unusable [475](#)

three-way conference [407, 408](#)

thresholds

data fragment [223, 229](#)

DoS [346](#)

RTS/CTS [223, 229](#)

time [447](#)

ToS [404](#)

TPID [200](#)

Trace Route test [468](#)

traffic shaping [198](#)

transmission speed

cable type [27](#)

troubleshooting [471](#)
trTCM [295](#)
Trust Domain
 add [444](#)
Trust Domain screen [443](#)
Trusted CA certificate
 view [372](#)
Trusted CA screen [370](#)
Two Rate Three Color Marker, see trTCM
TWT (Target Wakeup Time) [203](#)
Type of Service, see ToS

U

unicast [201](#)
Uniform Resource Identifier [397](#)
Universal Plug and Play, see UPnP
upgrading firmware [457](#)
upgrading online firmware [459](#)
UPnP [246](#)
 forum [239](#)
 NAT traversal [238](#)
 security issues [239](#)
 state [247](#)
 usage confirmation [238](#)
UPnP screen [246](#)
UPnP-enabled Network Device
 auto-discover [258](#)
USA type call service mode [407](#)
USB feature
 Media Server [29](#)
USB features [29](#)

V

VAD [403](#)
Vendor ID [249](#)
Virtual Circuit (VC) [198](#)
Virtual Local Area Network See VLAN
VLAN [200](#)
 Introduction [200](#)
VLAN ID [200](#)

VLAN tag [200](#)
voice activity detection [403](#)
voice coding [402](#)
VoIP [397](#)

W

Wake on LAN [249](#)
WAN
 status [152](#)
 Wide Area Network, see WAN [165](#)
WAN IP address [166](#)
warranty
 note [523](#)
Web Configurator
 login [68](#)
 password [68](#)
WEP [211](#)
WEP Encryption [212](#)
WiFi
 MBSSID [232](#)
WiFi 6 introduction [203](#)
WiFi Protected Access [495](#)
wireless client WPA supplicants [497](#)
Wireless General screen [206](#)
wireless LAN [203](#)
 authentication [229](#)
 BSS [231](#)
 example [232](#)
 example [228](#)
 fragmentation threshold [223](#), [229](#)
 limitations [231](#)
 MAC address filter [217](#), [230](#)
 preamble [225](#), [229](#)
 RTS/CTS threshold [223](#), [229](#)
 security [229](#)
 SSID [230](#)
 activation [214](#)
 status [153](#)
 WPS [233](#)
 example [234](#)
 limitations [236](#)
 PIN [233](#)
 push button [233](#)
wireless security [492](#)

- wizard setup
 - Internet [81](#)
- WLAN
 - interference [490](#)
 - security parameters [498](#)
- WMM screen [221](#)
- WPA [211, 495](#)
 - key caching [496](#)
 - pre-authentication [497](#)
 - user authentication [496](#)
 - vs WPA-PSK [496](#)
 - wireless client supplicant [497](#)
 - with RADIUS application example [497](#)
- WPA2 [211, 495](#)
 - user authentication [496](#)
 - vs WPA2-PSK [496](#)
 - wireless client supplicant [497](#)
 - with RADIUS application example [497](#)
- WPA2-Pre-Shared Key [495](#)
- WPA2-PSK [211, 495, 496](#)
 - application example [497](#)
- WPA3-SAE (Simultaneous Authentication of Equals handshake) [211](#)
- WPA-PSK [496](#)
 - application example [497](#)
- WPA-PSK (WiFi Protected Access-Pre-Shared Key) [211](#)
- WPS [233](#)
 - activate [67](#)
 - example [234](#)
 - limitations [236](#)
 - PIN [233](#)
 - push button [233](#)
- WPS button [47, 48, 51, 52, 55, 56, 59, 60, 63, 65](#)
 - using [67](#)
- WPS screen [219](#)

Z

- Zyxel Device
 - managing [29](#)