Wireless LAN Interfaces

Teldat Dm771-I

Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual.

Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents

Teldat Dm717-I Bridge

Teldat Dm730-I DHCP Protocol

Teldat Dm733-I Radius Protocol

Teldat Dm772-I Common Configurations for Interfaces

Teldat Dm783-I 802.1X Authentication

Teldat Dm799-I Subinterfaces Wireless LAN

Teldat Dm800-I AAA feature

Chapter 1 Wireless LAN

1.1 Introduction

The use of the Wireless Local Area Network (WLAN) interface allows you to have multiple devices connected in a network without using cables. For this, the packets are broadcast using standardized frequency bands and modulations.

The main advantages of wireless networks are mobility and the flexibility to add new users without having to make infrastructure changes. However, the fact that the packets are broadcast means that they are susceptible to eavesdropping, making security an important consideration in wireless networks. This chapter introduces the basic concepts of how wireless networks work, with an emphasis on the security aspect.

1.2 Physical layer

Wireless networking was first defined in the IEEE 802.11 standard. Many new extensions to the standard have since been proposed and approved either to define new modulations (e.g., 802.11a, 802.11b and 802.11g), improve security (e.g., 802.11i) or define new functionalities (e.g., 802.11i, which defines the quality of service in Wireless LAN networks).

Wireless devices can operate in two different frequency bands: 2.4 GHz or 5 GHz.

Mode	Frequency	Maximum Speed
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps

As can be seen in the above table, the 802.11b and 802.11g standards share the same frequency band, allowing devices from both standards to coexist in the same network.

The operating frequency bands are divided into channels. Each country controls its own radio frequency spectrum allocation, which means that the channels allowed within a frequency band vary from country to country. When working in the 2.4 GHz band, if there are two networks operating in the same area, leaving at least 4 channels clear between used channels is recommended to avoid interference. Thus, for example, if one network operates in channel 1, the other network should be using channel 6 to minimize interference.

1.3 Types of wireless networks

The most basic building block in creating a wireless network is the so-called BSS (Basic Service Set), which consists of a set of client stations that communicate with each other. There are two options for creating a wireless network: independent or ad-hoc networks (also called IBSS: Independent Basic Service Set) and wireless network in infrastructure mode.

Wireless networks are identified by a 32-octet network identifier (SSID: Service Set Identifier).

1.3.1 Ad-hoc wireless network

In this type of network, wireless client stations communicate directly with one another without the need for a traffic control element. This mode is designed to create small temporary networks. In this type of network, for two client stations to communicate, they must be able to "listen" to each other. That is, each station must be within range of the station it wants to communicate with.

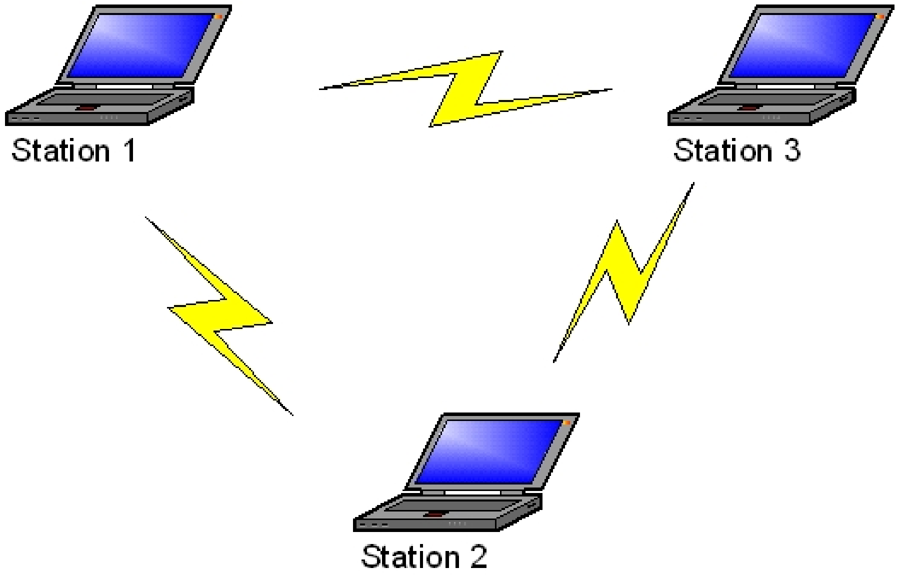


Fig. 1: **IBSS: independent wireless network**

1.3.2 Infrastructure

In ad-hoc networks, client stations cannot communicate directly with external networks. To do so, they need a control element, which not only controls the traffic going to and from the external network, but also controls the traffic between client stations within the wireless network.

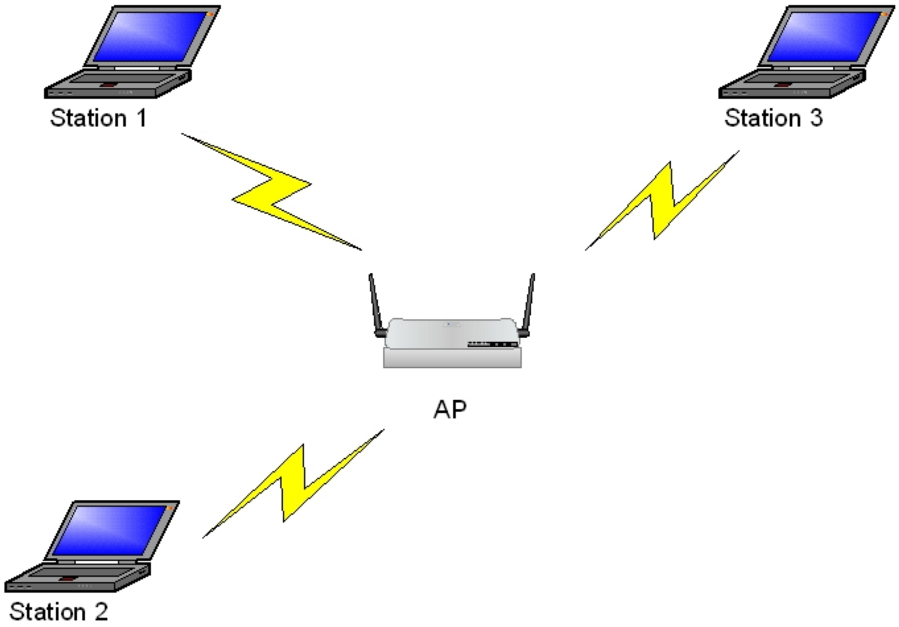


Fig. 2: **Wireless network in infrastructure mode**

This control element is what is called an access point (AP). All the frames that circulate through the wireless network pass through the access point. So if one client station wants to communicate with another, it sends a frame to the AP, indicating the frame's destination station, and the AP is then responsible for forwarding the frame to its destination.

This centralized approach provides the following advantages, among others:

- Client stations do not have to hear each other directly to communicate: if two client stations hear the AP, they can communicate with each other.
- Security becomes centralized. It is the access point that decides whether or not to allow a client station to join the wireless network. This is extremely helpful for defining security strategies.
- Multiple networks can communicate through the access point.

Note

Throughout the rest of this chapter we will focus on wireless networks in infrastructure mode.

1.3.3 Extending wireless networks: the distribution system

The wireless network coverage area within which a client station can communicate is limited in infrastructure networks as it depends on the client station receiving the access point signal. This, in turn, depends mainly on the antenna gain at the client station and access point, the distance from the client station to the access point, and the nature of any physical obstructions between the two elements.

Wireless network coverage can be extended by using multiple access points configured with the same network identifier. An access point's coverage area defines a basic service set or BSS. If a client station moves out of one access point's range and into the range of another, it can send packets through the access point covering the area it has moved to. Similarly, client stations covered by different access points must be able to communicate with each other, since for them the network must be unique. For this, there must be the possibility of sending packets from one access point to another. Communication between BSSs, and between BSSs and external networks, is done through what the IEEE calls a distribution system. The IEEE standards do not expand upon the exact details of the distribution system; they merely indicate some of the system design characteristics that must be met. In practice, the most common distribution system is the Ethernet local area network, as shown in the following figure:

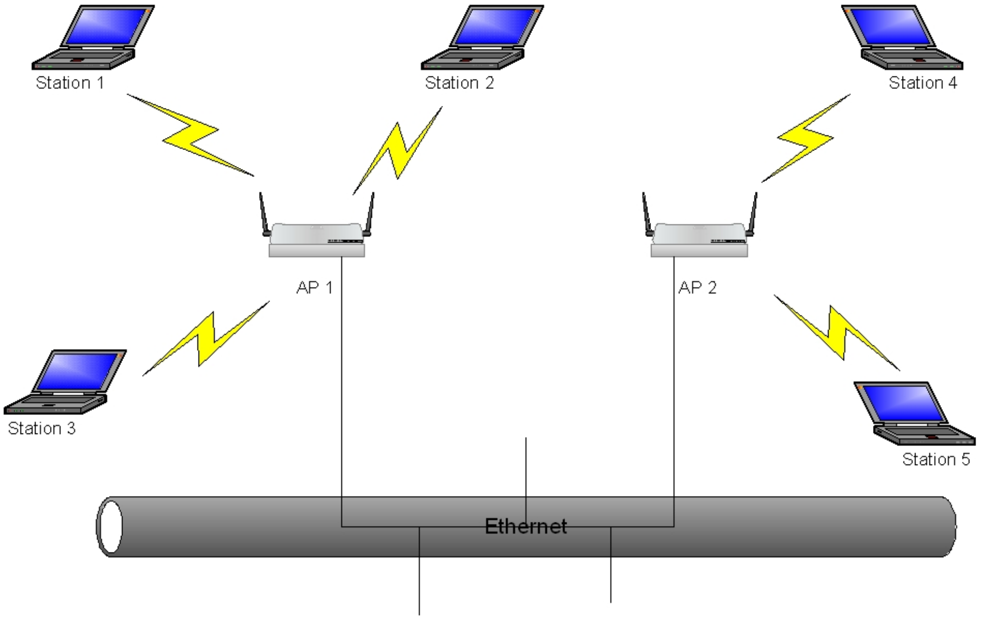


Fig. 3: **ESS: Extended service set**

When several basic service sets (BSS) are joined together, you get an extended service set (ESS). The figure above shows an extended service set consisting of the following elements:

- A basic service set, BSS1, covered by an access point, AP1. Client stations 1, 2 and 3 belong to this service set.
- A basic service set, BSS2, covered by an access point, AP2. Client stations 4 and 5 belong to this service set.
- A distribution system, Ethernet, which allows communication between the elements in the two basic service sets.

If client station 1 wants to send a packet to client station 4, the procedure is as follows:

(1) Station 1 sends the packet to access point AP1 specifying station 4 as the final destination. As you might expect, a WLAN frame needs more than two address fields in order to be correctly routed. In this particular example, three address fields are required: the source address (station 1), the address that receives the packet (AP1), and the destination address (station 4). Most WLAN frames will use as many as four address fields.

(2) AP1 bridges the received packet and relays it on through the distribution system. The Ethernet packet has station 1's MAC address as source, and station 4's MAC address as destination.

(3) AP2 receives the packet sent by AP1. Since the packet is destined for a station that AP2 knows, AP2 sends the packet on to station 4.

(4) Station 4 receives the packet that originated in station 1.

In the previous diagram, station 2 is in close proximity to both AP1 and AP2 and chooses the best access point based on signal strength. If the client station were to move to the right and receive a stronger signal from AP2, it would start using the new access point while remaining within the same network at all times. The key element here is the network identifier or Service Set Identifier (SSID). The SSID is an alphanumeric string that identifies a wireless network; so all access points in an ESS must use the same network identifier.

1.4 WLAN frames

1.4.1 Sending frames in a WLAN: accessing the medium

Before explaining the format of a standard frame in a wireless network and the types of frames that might appear, it is useful to briefly explain the mechanism used for transmitting packets in wireless networks.

In a wireless network, the transmission medium is shared between all client stations making up the network. Here we include the access point as a particular type of client station. When a medium is shared, a client station must listen to the medium before sending data to make sure that no one else is transmitting and that it can transmit without interfering with another frame. The mechanism used is basically the same as for standard Ethernet, namely, Carrier Sense Multiple Access (CSMA), except that a collision avoidance (CA) mechanism, rather than the collision detection (CD) technique, is used. The following sections briefly describe the peculiarities of sending frames over a wireless medium.

1.4.1.1 Active confirmation

When you send a frame over a wired medium, you expect the sent frame to be received correctly at the destination. However, the WLAN transmission medium is subject to all kinds of interferences and obstacles. For this reason, the IEEE opted to use an active confirmation element for frames sent over wireless networks: every time a frame is sent, the receiver must respond with an acknowledgement frame (ACK frame) confirming reception. The only exception is when you have frames addressed to multiple client stations; for obvious reasons, you can't have each and every station in the wireless network confirming they have received the frame.

If the transmitter does not receive a reception acknowledgement, it must consider the frame lost and start the transmission process again. As the sending and confirming operation is considered an atomic operation, mechanisms are provided to reserve the medium for the duration of the entire exchange.

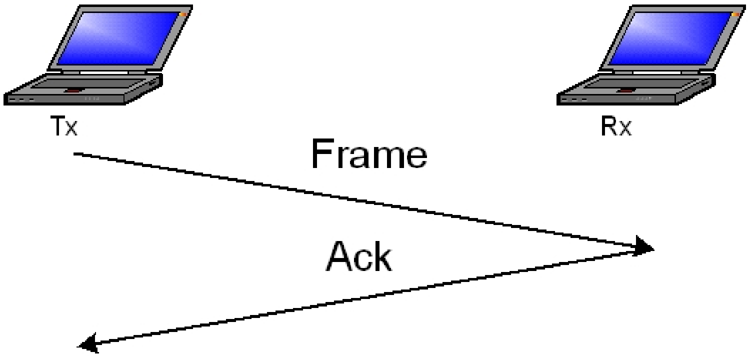


Fig. 4: **WLAN frame transmission: active confirmation**

1.4.1.2 RTS/CTS: the hidden node problem

In an Ethernet network, the cable carries the signal to all the nodes and the nodes can probe the medium to detect possible collisions. In a wireless network, radio transmission makes the network boundaries diffuse. A client station with a high gain antenna can detect a wireless network in a place where another client station with a normal antenna doesn't detect anything. In addition, when stations and obstacles move, they can create shadow areas in which a station does not detect another station's signal despite being close by.

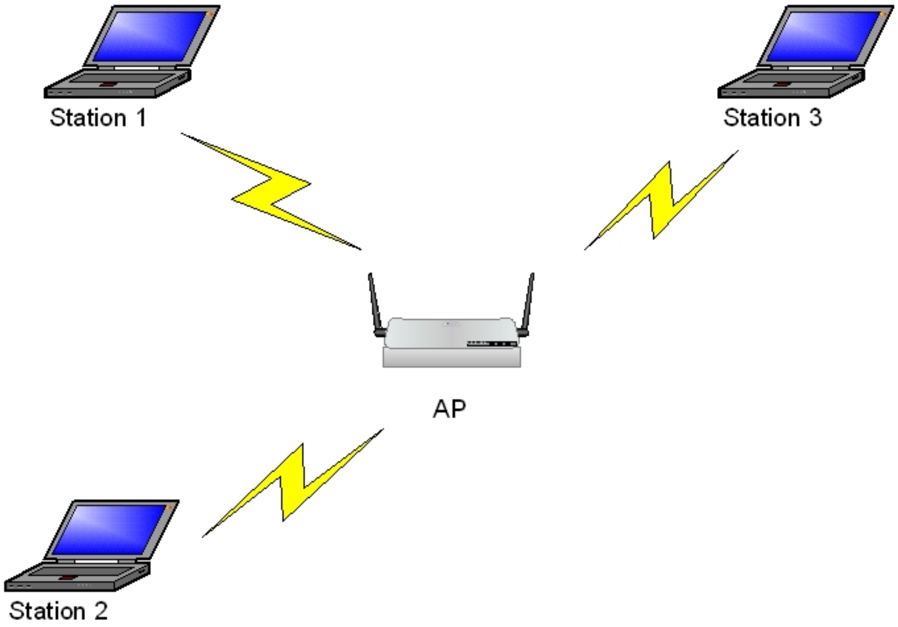


Fig. 5: **The hidden node problem**

Let's imagine that client stations 1 and 3 in the previous figure are able to hear the access point but obstacles or power-related reasons prevent the two stations from hearing each other. In these circumstances, if station 1 is transmitting and station 3 has something to transmit, the latter may erroneously assume that the medium is free because it cannot hear the traffic from station 1. This can lead to multiple collisions, with a consequent degradation in link quality experienced by users.

To solve this so-called hidden node problem, the IEEE introduced an additional transmission mechanism whereby the atomic frame transmission operation is accompanied by a transmission request frame (Request To Send or RTS) and a confirmation frame that transmission is possible (Clear To Send or CTS).

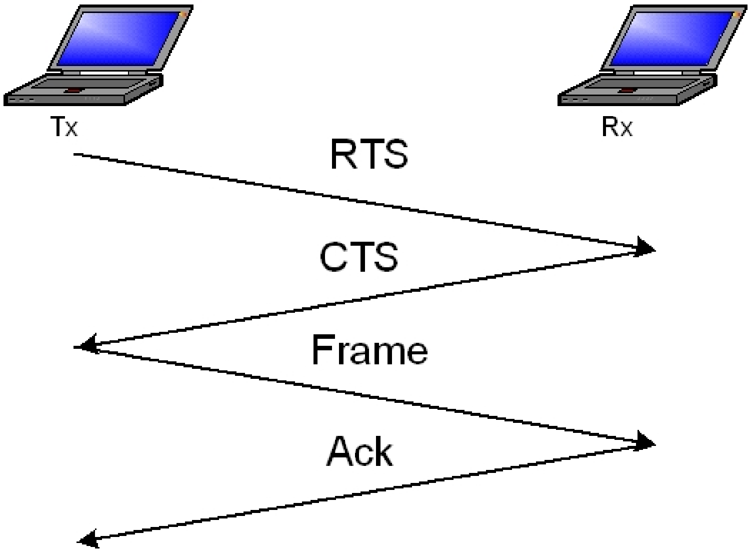


Fig. 6: **Transmitting a frame in a WLAN: active confirmation**

In this case, when station 1 wants to transmit a frame, it first sends an RTS frame to say it is going to use the medium for the duration of the atomic frame exchange operation (RTS duration + CTS duration + frame transmission duration + ACK duration). Since the RTS frame is a small frame, the chances of a collision are reduced. All client stations that hear the RTS must remain quiet for the specified duration. Upon receipt of the RTS frame, the receiving client station will send a CTS frame which indicates that the medium will be occupied for the remainder of the atomic frame exchange operation (CTS duration + frame transmission duration + ACK duration). The client stations that hear the CTS have an obligation to remain quiet for the duration indicated. Once the RTS/CTS exchange is completed, the frame can be sent as shown in the previous section: frame is sent followed by confirmation by the receiving station.

Does this eliminate the hidden node problem? Yes, since it ensures that all client stations in the basic service area will hear either the RTS or the CTS. Please note that the access point intervenes in all frame exchanges and that all client stations listen to the access point. Thus,

- if the client station transmits a frame, the access point will transmit the CTS, which will be heard by all BSS stations.

- if the access point transmits a frame, it will transmit the RTS, which will be heard by all BSS stations.

As the RTS/CTS mechanism introduces an additional transmission overhead, it is not usually used unless frames are long and collisions more likely. Configurable access point parameters routinely include a minimum frame size that activates the RTS/CTS mechanism.

1.4.2 WLAN frame format

Note

The WLAN frame format is constantly changing as modifications to the standard are approved. Here you can see the original format. For a detailed explanation of the various fields, please refer to the latest available version of the standard.

The fields included in a WLAN frame are:

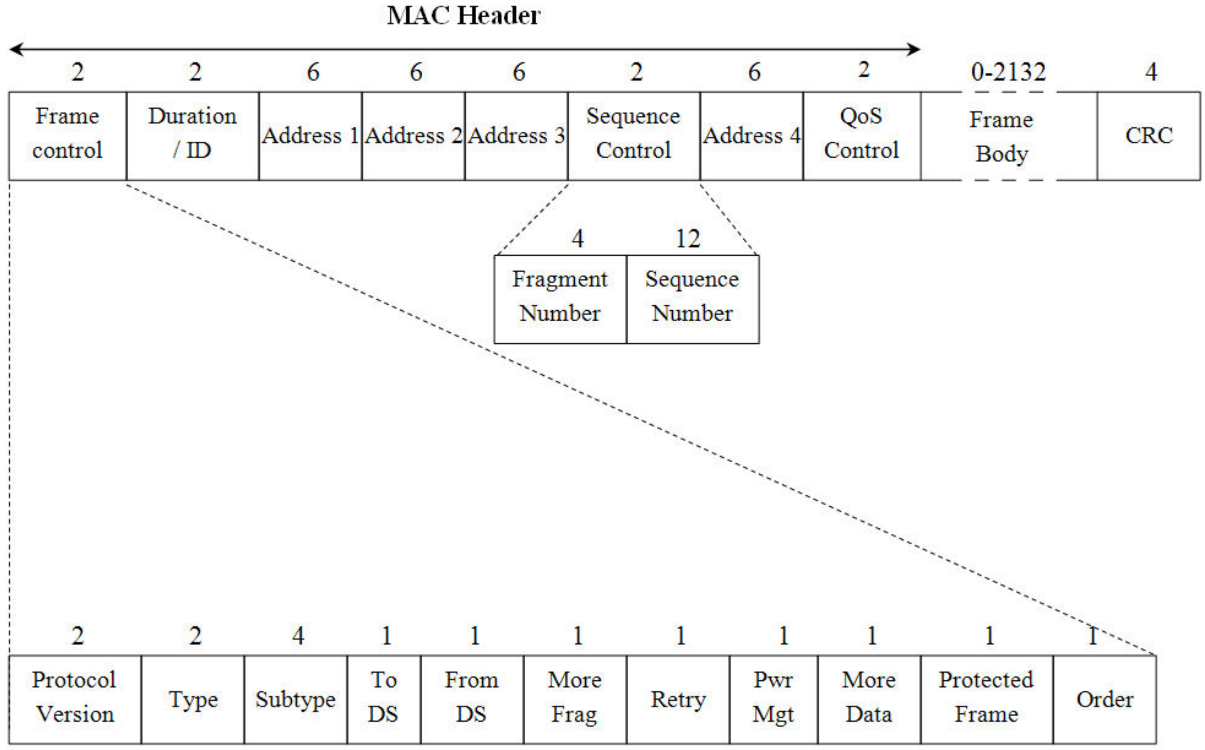


Fig. 7: **WLAN frame format**

Frame Control

Two octets containing information on the characteristics of the frame. The components present in this field are:

- **Protocol Version**: denotes the version of the MAC contained in the frame. At the moment, just one version has been developed and has been assigned the value 0.
- **Type**: Type of frame. There are three frame types in a wireless network:

  - Data frames: carry data from a higher protocol in the frame body.

  - Control frames: transmission medium's control frames. They are RTS, CTS and ACK frames, among others.

  - Management frames: frames to carry out wireless network supervisory functions (association, authentication, etc.).

- **Subtype**: the type and subtype fields identify the type of frame in question.
- **To DS**: This bit denotes whether a frame is intended for the distribution system. This bit is set to 1 in all frames going from an access point to a client station.
- **From DS**: this bit denotes whether a frame comes from the distribution system. This bit is set to 1 in all frames going from an access point to a client station.
- **More Fragments**: This bit is set to 1 in fragmented frames to indicate that the frame is made up of more frag-

ments. In the last fragment, the value of this field is 0.

- **Retry**: Set to 1 when a frame is retransmitted.
- **Power Management**: A client station sets this bit to 1 to inform the access point that it will enter power saving mode once the frame has been sent.
- **More Data**: When a client station has entered power saving mode, the access point buffers frames addressed to that station in order to send them later. The access point uses this bit to tell a retired client station that it has some frames pending transmission. When the access point has finished transmitting the frames to the client station, it sets this bit to 0 to indicate to the client station that it can return to “sleep”.
- **Protected Frame**: Indicates that the frame is protected by some sort of security mechanism. This bit is known as the WEP bit in the original standard.
- **Order**: This is set to 1 to indicate that you want the frame to be delivered in strict order.

DURATION / ID

This two-octet field usually indicates how long you think the medium will take to transmit the frame. In a special frame case, used during power saving mode, it identifies the client station that asks the AP if there are frames outstanding.

ADDRESS 1-4

Address fields are used to address a frame in a wireless network. The first three fields are mandatory and appear in all frames. The fourth address field is optional and is only used in frames transmitted over the wireless network between access points (Wireless Bridge, the distribution system is a WLAN rather than an Ethernet network). WLAN addresses have the same format as MAC addresses used on an Ethernet network. Depending on the frame, MAC addresses can have the following meaning:

- Destination address: end station's address.
- Source address: originating station's address.
- Address of the transmitter: address of the client station that originated the frame. Since the frames all pass through an access point, this address may be different from the source address.
- Receiver address: address of the client station that must receive the frame. This address may be different from the destination address.

If, for example, station 1 sends a frame to station 2 within the same basic service area, using an access point:

(1) The client station generates a frame with three addresses:

source address: that of station 1.

destination address: that of station 2.

receiver address: that of the access point.

(1) The access point receives the frame and sends it on to station 2. The generated frame has three addresses:

source address: that of station 1.

destination address: that of station 2.

receiver address: that of the access point.

SEQUENCE CONTROL

Sequence control. This is made up of a sequence identifier, which is incremented for each new frame sent, and a fragment identifier, used to designate the various fragments that a frame is divided into when fragmentation occurs. When a frame is fragmented into several frames for transmission, the sequence identifier remains the same for all fragments while the fragment identifier changes.

QoS CONTROL

Quality of Service. This contains QoS-related information about the frame. This field is optional and is only present in traffic between client stations that use quality of service.

FRAME BODY

Variable-length field containing the frame data.

FRAME CHECK SEQUENCE

Cyclic redundancy check (CRC) of all WLAN frame fields to check integrity on reception.

1.4.3 Management frame format

While we are not going to provide a detailed description of all the frame types that can appear in a wireless network, a brief description of the management frame format is useful.

As described in section 4.2, the management frames have a header. The data part is divided into a series of fixed fields and a series of information elements.

The fixed fields are fixed-length fields defined in the standard. Among these fields is, for example, the result of an association, a fixed 2-octet-long field.

The information elements are variable-length fields that provide a convenient way to extend the standard. The generic format of an information element is as follows:

1	1	Length
Element ID	Length	Information

Element ID: Information element identifier.

Length: Information length.

Information: The information is interpreted in relation to the element identifier.

Thus, for example, the SSID network identifier is sent using the information element with identifier 0, indicating the SSID in the information field.

The 802.11 standard specifies exactly which fixed fields and information elements must be included in the management frames and the order in which they must be assembled.

1.4.4 Connecting to a wireless network

In an Ethernet network, when a client station wants to join a network, you just physically connect it to the network in question. In a wireless network, given the peculiarities of the transmission medium, the process is inevitably somewhat more complex. Among other things, since it is a free access medium, care must be taken with security, ensuring that only authorized stations are allowed to join the network and that any station that hasn't demonstrated that it is authorized to join the network is denied access. This section briefly describes the process by which a client station joins a wireless network in infrastructure mode.

1.4.4.1 Wireless network identification

The first step when a client station wants to connect to a network is to identify the network in question. A wireless network is identified by its Service Set Identifier (SSID). There are two ways to detect active networks around a client station: through a passive search and through an active search.

1.4.4.1.1 Passive search

During a passive search, the client station sweeps all available channels, listening to the frames that are sent over the medium.

Access points periodically send out management frames called beacon frames. These contain information about the wireless network they belong to, including the network identifier, allowed speeds, security features, etc. The client station conducting the passive search hears the beacons frames and chooses a network to connect to.

Normally, if no network identifier is configured, the client station presents the user with a list of detected networks (with the signal, security and channel characteristics used) so that the user can select one he wants to connect to. If, on the other hand, a network identifier is configured, the client station will attempt to automatically connect to the specified network without involving the user. Where several access points announcing the same network are detected, the client station usually chooses the access point with the strongest signal level.

Passive searching saves on battery power because the client station doesn't send frames.

1.4.4.1.2 Active search

In an active search, the client station searches for a particular network to connect to. In this case, the client station scans all the available channels, but instead of waiting for the beacon frames to find out the available networks (as is the case with a passive search), it asks for the network it is looking for by sending out a management frame called a Probe Request.

When an access point receives a Probe Request that is looking for the network SSID that the access point belongs to, it responds with a Probe Response management frame. The Probe Response frame carries the same information as the beacon frame (that is, it specifies the characteristics of the network in question).

Note

Both beacon and Probe Request frames are broadcast frames, so they are received by all the client stations listening on the channel.

1.4.4.2 Authentication

Once the client station has identified the network it wants to connect to, it needs to authenticate with the access point.

The authentication process, as described in the IEEE standards, is a one-way process: the client station authenticates with the access point, but the access point does not authenticate with the client station.

As you will see, this authentication process is very basic, provides no security and is only maintained for backward compatibility. For a secure authentication method, you should use 802.1X authentication, as described in the 802.11i standard. This authentication method is described briefly in the section on Security.

For now, we will focus on the authentication described in the original standard, for which there are two types of authentication: open authentication and shared key authentication.

1.4.4.2.1 Open Authentication (Open-System Authentication)

This is the easiest authentication method and the only one required under the 802.11 standard. Describing the process as authentication, however, is, of course, very optimistic: the client station issues an Authentication Request frame and the access point responds with an Authentication Response. The response contains the authentication result; under normal conditions, this will be a successful response.

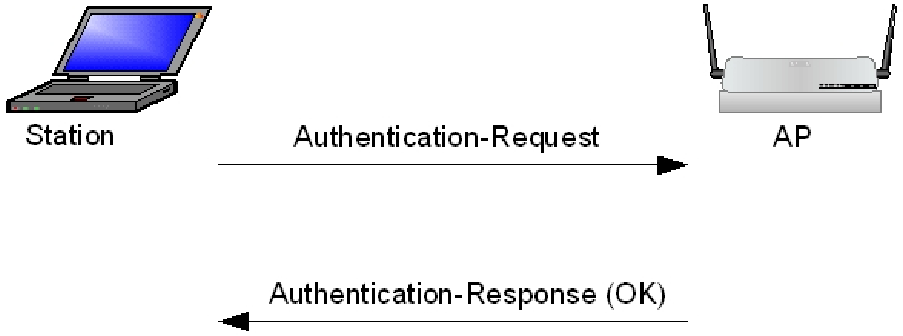


Fig. 8: **Open authentication**

Some access points allow you to associate access rules with MAC addresses. If this is the case, and the authenticating client station's MAC address does not have permission to access the network, the access point will report an authentication error in the response message.

1.4.4.2.2 Shared Key Authentication

Shared key authentication requires that a client station know a key before joining the network. In this case, the authentication process involves four steps:

(1) The client station requests authentication from the access point.

(2) The access point builds a random 128-byte message (challenge) and sends it to the client station.

(3) The client station uses WEP to encrypt the challenge it receives and then sends it to the access point.

(4) The access point decrypts the received message and considers the authentication successful if it matches the message it sent.

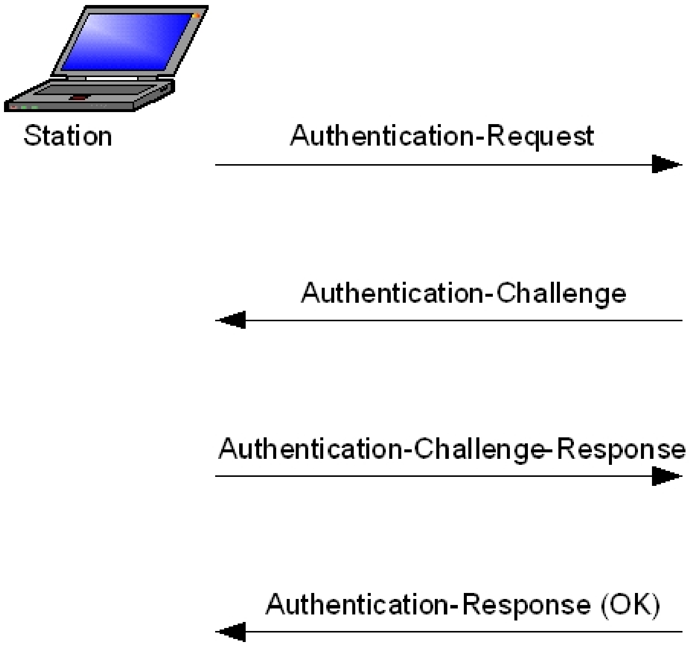

Station
AP
Authentication-Request
Authentication-Challenge
Authentication-Challenge-Response
Authentication-Response (OK)

Fig. 9: **Shared key authentication**

Note

This type of authentication, which can only be used with WEP encryption, can give hackers clues about the keys used to encrypt data. *Teldat* strongly recommends against using this type of authentication method.

1.4.4.3 Association

Once the access point has authenticated the client station, it can associate with the network. The association process consists of a two-frame exchange: the client station issues an association request and the access point replies indicating the result of the request (successful/unsuccessful). The access point can return an error response if, for example, it doesn't have enough resources to associate another client station.

If the association is successful, the access point sends the client station an association identifier (AID), which is used when the client station goes into power saving mode.

Note

In the original standard, a client station can start sending and receiving frames once it has successfully associated with a network. However, if the network is using a security mechanism like WPA or WPA2, a further step is required before the client station can send and receive data frames: the client station and access point must prove to each other that they are who they say they are and that they know the keys that will be used for encrypting the frames. This process is described in the section on wireless network security.

1.4.5 power saving mode

A basic characteristic of wireless network client stations is their mobility. Thus, it is common for client stations to operate from a portable power source (e.g., a battery pack) rather than being connected to a power grid. It is therefore useful for a client station to be able to disconnect the radio component when it is not expecting packets; especially when you consider that the wireless radio component is one of the most power-hungry elements in portable devices. 802.11 client stations can maximize battery life by shutting down the radio component without sacrificing connectivity.

We say that a client station is asleep when it has entered power saving mode; otherwise it is awake.

The access point is the base element for power saving. Independent networks also offer the possibility of entering power saving mode, but it is much less efficient than in networks in infrastructure mode and will not be discussed in this section.

As we have seen, the WLAN frame MAC header contains a bit (power management) that the client station uses to inform the access point of the state it will be in after transmitting/receiving the current frame. In this way, the access point knows the status of all client stations at all times. When a client station is going to enter power saving mode, it notifies the access point by setting the power management bit to 1. From that moment, the access point stops delivering frames to that client station and instead buffers them to be sent at some point in the future.

Buffering frames for a sleeping client station is only part of the process. At some point the client station must wake up to request the buffered frames. In describing the frame delivery process, we need to distinguish between unicast frames (directed exclusively to a sleeping client station) and multicast and broadcast frames (directed to a group of client stations).

1.4.5.1 Unicast frames

As already mentioned, the access point periodically sends out management frames called beacon frames. Beacon frames indicate whether frames are buffered for a client station at the access point.

The access point includes an information element, called a Traffic Indication Map (TIM), in the beacon frame. The TIM contains a 2048-bit map. Each bit corresponds to one of the client stations associated with the access point. If a client station's bit in the TIM is set to 1, there are frames buffered at the access point for the client station.

There are mechanisms that you can use to allow the access point to send only part of the map rather than the entire map.

During the association process, the access point assigns an association identifier to the client station (AID). This identifier is used as an index in the TIM. Thus, the sleeping client station must wake up to listen to the beacon frame and see if the bit corresponding to its association identifier is set to 1.

During the association process, the client station informs the access point of the listening interval it will use: this is the number of beacon frames that it can remain asleep. The listening interval is a contract between a client station and access point whereby the access point undertakes to buffer frames destined for a client station during the time indicated by the listening interval. After this time, if the client station has not requested the buffered frames, the access point can discard them. Obviously, longer listening intervals require more packet buffer space on the access point. If a client station proposes a listening interval that the access point deems unacceptable, then the access point must deny the association.

Based on what we have seen so far:

(1) The client station informs the access point that it is going into power saving mode.

(2) The access point buffers frames destined for the client station.

(3) The access point announces the client station's frames in beacon frames.

(4) The client station wakes up periodically to receive beacon frames and check whether frames are buffered for it at the access point.

Once a client station in power saving mode detects that there are frames for it at the access point, it must request them.To retrieve buffered frames, client stations use a type of management frame called a PS-Poll. When the access point receives a PS-Poll frame, it responds with a buffered frame. The More Data bit will be set to 1 if there are more frames pending for the client station, and to 0 if there are no more frames.

The client station can successively request frames using the PS-Poll frame until it has received all the buffered frames.

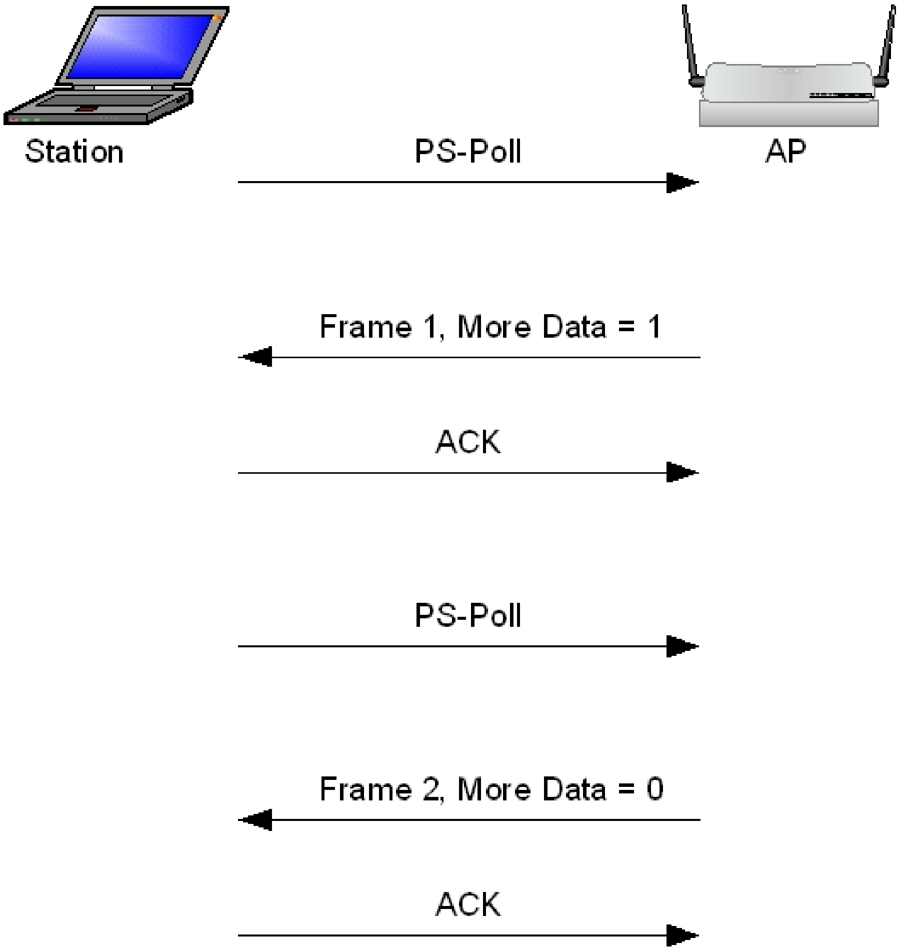


Fig. 10: **Stored frames request**

1.4.5.2 Multicast frames

Frames destined for multiple client stations are treated separately. As soon as one of the client stations enters power saving mode, the access point buffers the group frames. It is not possible to use a polling mechanism to receive the frames because they are destined for a group of client stations.

Every few beacon frames, the TIM information element indicates whether there are any buffered group frames. To do this, the association identifier 0 is used within the TIM bit map. This information element receives a special name: Delivery Traffic Indication Map (DTIM).

Immediately after having received/sent a beacon frame with the DTIM information element, the access point sends any buffered group frames. The More Data bit is used to tell the client stations whether there are more frames pending delivery or whether they have all been sent. If the client stations in power saving mode want to receive the group frames, they must wake up and listen to the beacon frames with the DTIM information element, regardless of their listening interval. Some client stations can enter an extremely low-power mode, whereby they do not wake up to listen to the frames carrying the DTIM element.

All beacon frames include two values in the TIM information element that allow client stations to know when another delivery of buffered group frames will take place:

- The DTIM counter: indicates how many beacon frames to go, including the current one, before the next DTIM. When the counter reaches zero, the TIM is a DTIM.
- DTIM periodicity: indicates the number of beacon frames between DTIMs. A value of 1 indicates that all beacon frames carry the DTIM information element.

1.5 Wireless network security

In wireless networks, the frames travel freely through the air, which means that any client station that is sufficiently close enough can receive them. If the frames are not protected by some type of encryption, any user entering an access point's range can access the data exchanged in the wireless network. Limiting the access point transmit power so that the signal does not leave the building is not the answer here because if sufficiently high power antennas are available, the transmitted data can be accessed despite the power limitation.

There is a further danger that, as well as being able to access the data exchanged on the wireless network, a malicious user could associate with the access point. As access points are usually connected to the local area network, which serves as the distribution system, the associated user would have access to the company network.

With the proliferation of wireless networks, and their increasing popularity, attacks on such networks have become popular. For example, it is common to use a neighbor’s wireless network to navigate from a laptop using the neighbor's Internet access.

Taking all these facts into account, it is not surprising that wireless network security has been one of the biggest headaches for developers and those in charge of implementing company wireless networks. In fact, the lack of security in wireless networks limited their deployment for a while. Today, with the approval of the 802.11i standard, wireless networks can be considered secure enough.

This section briefly describes the different wireless network security alternatives available.

Note

The security alternatives discussed in this section refer to the wireless network as such. Since WLAN frames normally carry higher layer protocol data, it is possible to use the more sophisticated security features of those protocols to protect wireless network data. In particular, the use of IPSec to create a virtual private network is quite widespread.

1.5.1 Mac access control

The first mechanism that you can use to protect access to a wireless network is to configure a MAC address list, indicating for each MAC address whether to allow or deny access to the wireless network.

The MAC address list is configured on the access point. When a client station wants to join the wireless network, the access point queries its address list to see if the client station in question is allowed access or not. If the client station’s MAC address is prohibited from accessing the network, the access point does not allow the client station to connect to the wireless network.

You can usually configure the policy to be followed by the access point if a client station's address is not in the configured address list. If a strict policy is configured, access to the network is only granted to those client stations with explicit permission to join, which they get by being added to the access point's list of approved MAC addresses. With less strict policies, client stations can access the wireless network even though their MAC address is not in the configured address list.

This security mechanism provides little security because it is relatively easy to change a client station’s MAC address. If a user wants to attack a network that only has this type of security, all he needs to do is to capture some traffic and observe the MAC address of one of the client stations correctly connected to the network. When the client station leaves the wireless network (and the attacker has a number of mechanisms at hand to force a client station to leave the network), the user simply has to configure the approved MAC address on his device to gain access to the wireless network.

This security mechanism should only be used to complement other security mechanisms due to the poor security it offers.

1.5.2 WEP encryption

The only defined security mechanism in the original IEEE wireless networking standard (802.11) was one associated with a type of data encryption called Wireless Equivalent Privacy (WEP).

The idea of the standard was to create encryption that would provide similar security levels to those found in a traditional LAN network. Unfortunately, the definition of the encryption algorithm has numerous flaws that make it relatively easy these days to break the WEP encryption and obtain the keys used.

Note

You should only use WEP encryption if you are unable to configure a more robust security mechanism such as WPA or WPA2.

When using WEP, the wireless network frames are encrypted. The client station and access point must be configured with a common key to be able to communicate. The IEEE standard distinguishes two types of WEP keys:

- Shared-keys: Up to four different WEP keys can be configured. Of these four keys, one must be set as the default key (also called the transmission key). This key is the one that is used to encrypt the frames transmitted by the client station when there is no private key associated with the destination MAC address.
- Private keys: WEP keys can be associated with a MAC address. The client station will use this private key to en-

crypt the frames destined for that address and to decode the frames coming from that address.

Note

The 802.11 standard defines WEP keys as 40-bit long keys. However, when WEP encryption security flaws began to emerge, some manufacturers began developing WEP encryption using 104-bit and even 128-bit keys in the (mistaken) belief that they were more secure. To make matters worse, some manufacturers refer to the 40, 104 and 128-bit WEP keys as WEP-64, WEP-128 and WEP-152, respectively.

We do not intend to describe the format of a WEP encrypted frame here; suffice it to say that the frame contains a field for indicating the key index used to encrypt the frame.

To send a packet using WEP:

- The client station looks to see if it has a private key associated with the packet destination address. If one has been configured, it uses that key to encrypt the packet.
- If there is no private key configured, it uses the default shared-key, indicating, in the frame, the key index used.

When receiving a WEP-encrypted packet:

- The client station looks to see if it has a private key associated with the packet source address. If one has been configured, it uses that key to decrypt the packet.
- If there is no private key configured, the shared-key indicated in the received frame is used to decrypt the packet.

The reason that up to four keys can be configured is to facilitate the changing of the WEP key. Imagine that a client station is using key 1 to transmit and wants to change that key. To allow the data encrypted by the client station to be decrypted by all the other client stations, the key must be changed in all client stations. Since there are no defined key transmission mechanisms, normally the person in charge of network management must go client station by client station manually changing the key. When a client station's key is changed, the other client stations will not be able to decrypt its data until the key is updated. To avoid encryption errors during the key change process, two shared-keys are used:

(1) The access point uses key 1 to transmit, and the new key is configured in position 2.

(2) All client stations are updated, configuring the new key in position 2, and configuring said key as the default key.

(3) Now, the updated client stations use key 2 to encrypt the frames they transmit, and the access point, which has that key configured, decodes the frames correctly. The access point and the client stations that haven't been updated continue to use key 1 to encrypt frames. All client stations are able to decrypt said frames since they all have key 1 configured correctly.

(4) When the configuration of the new key in position 2 is completed in all the client stations, key 2 can be configured as the default key in the access point, erasing key 1.

The reason for using up to four shared-keys instead of two is that it allows the access point and the client stations to use different keys to transmit data to each other: the access point can, for example, use key 3 to transmit, while the client station uses key 2.

The above-mentioned mechanism for updating WEP keys is very cumbersome, which is why WEP keys are seldom used in practice.

1.5.3 802.1X authentication

The section dedicated to connecting to a wireless network described the two authentication types defined by the 802.11 standard: open authentication and shared key authentication. As noted above, both of these authentication mechanisms are weak. In fact, WEP shared-key authentication actually provides information that makes it easier to find out the WEP keys used in a wireless network. For this reason, their use is discouraged.

When the first articles about WEP security flaws began to appear, the IEEE started working on a new security standard. This was to eventually crystallize into the 802.11i standard. For the development of this standard, the IEEE looked to existing standards that had already been tested over time in real environments, thereby demonstrating their robustness. Thus, the IEEE focused on the 802.1X standard (initially developed for Ethernet networks) as a method for authenticating client stations in a wireless network.

According to the 802.1X standard, the access point sees each client station association as a controllable logical port. Initially, the port is closed and no data can be exchanged. Only when the client station has been successfully authenticated is the port considered open and data exchange allowed. For the authentication process, another, non-controllable, logical port is used which only allows authentication exchange packets to transit the network.

The Extensible Authentication Protocol (EAP) is the basis of the authentication process. The 802.1X standard defines how to use EAP on LAN networks (wireless or wired). For this, it defines EAP encapsulation for sending over LANs, while also creating new packet types to facilitate EAP use in LAN networks. The encapsulation defined in the

802.1X standard is called EAP Over LAN (EAPOL).

EAP authentication and, by extension, 802.1X authentication, comprises three components:

- Supplicant: the element that wants access to the network. The client station assumes the role of the supplicant in wireless networks.
- Authenticator: the element that controls access to the network. The access point assumes the role of authenticator in wireless networks. The authenticator uses the afore-mentioned controllable logical port to control a client station's access to the network. The client station is only allowed to send and receive data if the controllable port is open (i.e., if the client station has successfully authenticated).
- Authentication server: this is the element that authenticates the supplicant, deciding whether or not it can access the network. The authentication server can assume the role of authenticator, but usually an external element does so.

A simple example will help you to understand the role of each element in the network access process. Imagine that a stranger wants to enter a company's building. This is the supplicant. The company's doorman controls access to the building, granting or denying access. However, he has no power to decide who is allowed to enter and who isn't. The authenticator decides this. When the stranger asks to enter the building, the doorman calls the head of the company and asks whether the stranger has permission to enter. The head probably asks about the stranger. The doorman relays the head's questions to the stranger, and then relays the stranger's responses back to the head. Finally, depending on the answers given, the head will take a decision as to whether to let the stranger enter or not. The head of the company is the authentication server.

The following figure outlines the elements involved in 802.1X authentication.

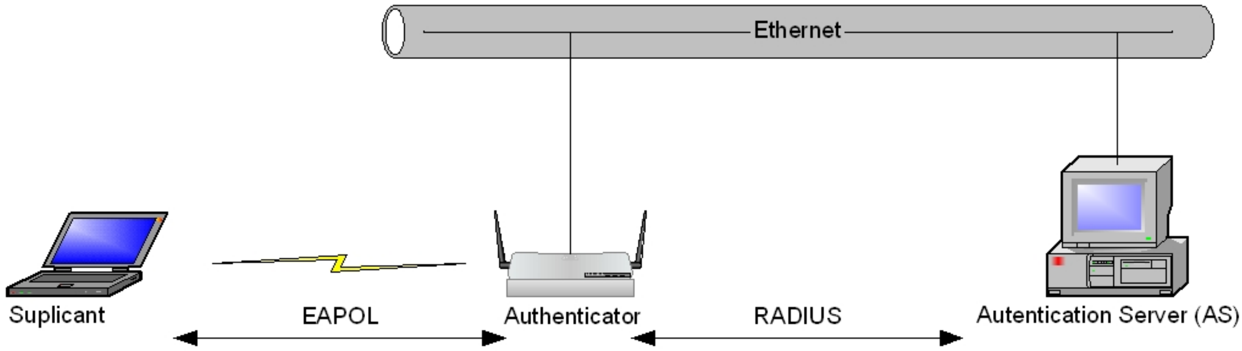


Fig. 11: **802.1X authentication elements**

The authentication process takes place between the supplicant and the authentication server. When the supplicant wishes to access the network, it initiates the authentication process. The authenticator uses the non-controllable port to transmit authentication exchange packets between the supplicant and the authentication server. In other words, the authenticator acts as a relay for the packets between the supplicant and the authentication server. The authenticator should only look at the end result of the authentication: if it is successful, the authenticator authorizes the controlled port and allows the supplicant to access the network.

Communication between the supplicant and the authenticator is performed using EAPOL. In order to have secure authentication, it is imperative that the communication channel between the authenticator and the authentication server be completely secure. There are several alternatives for sending EAP packets between the authenticator and the authentication server; one of the most used makes use of the Radius protocol for sending EAP packets.

EAP is really a superset of authentication protocols. The particular EAP protocol to be used is negotiated during the authentication phase. Numerous authentication methods use EAP databases, including:

- PEAP: Protected EAP
- EAP-TLS: EAP-Transport Layer Secure
- EAP-TTLS: EAP-Tunneled Transport Layer Secure

The 802.11i standard requires that any EAP authentication method used on a WLAN perform mutual authentication: having the authentication server verifying that the supplicant is who it claims to be is not enough; the supplicant must also verify that the authentication server is who it claims to be.

We will not go into detail with regard to EAP and EAPOL frame format or how to send EAP over Radius. The following figure shows the authentication process:

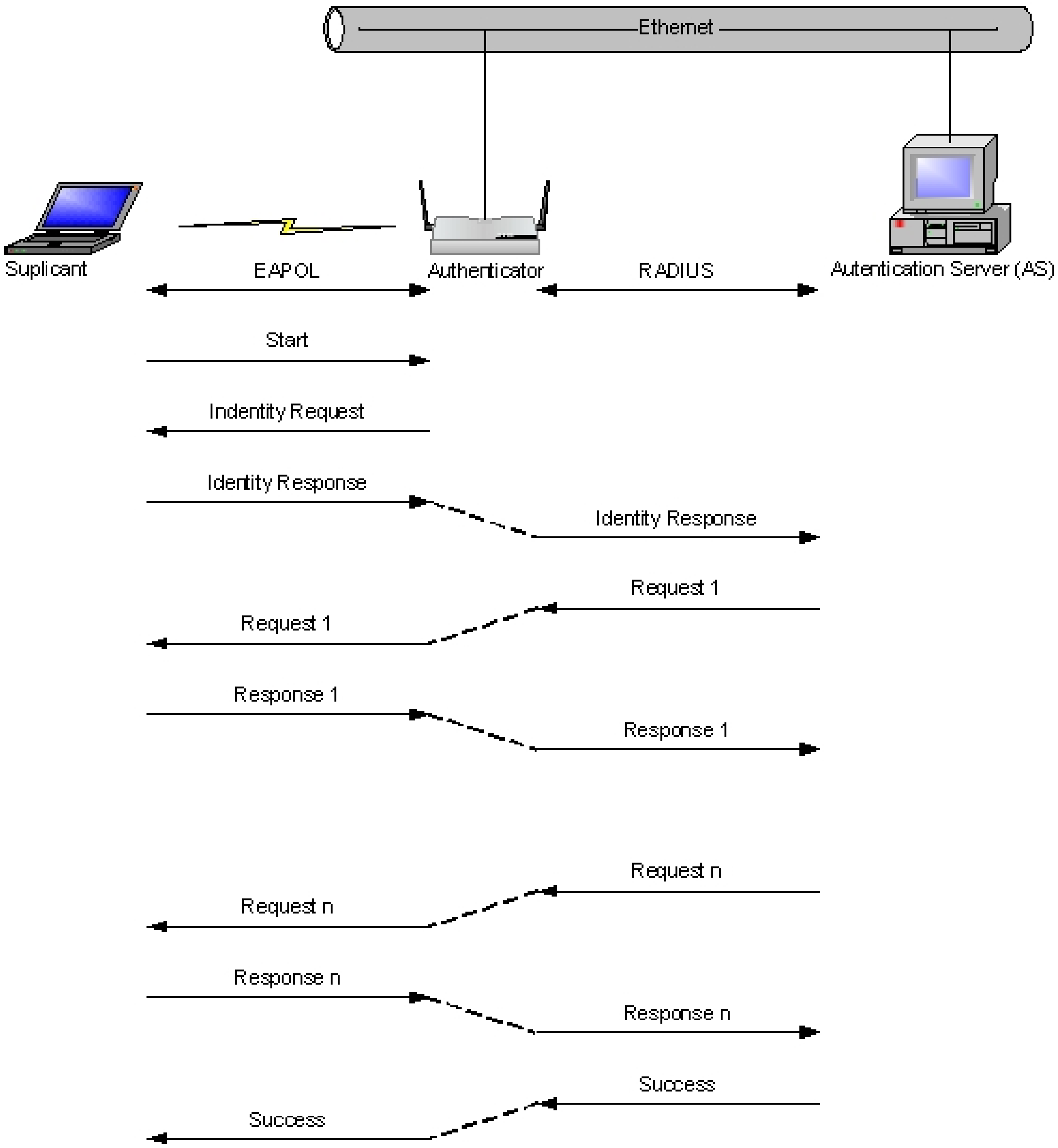


Fig. 12: **802.1X authentication process**

Note

802.1X authentication does not replace the open authentication already described, but is performed once the client station has associated with the access point.

1.5.4 Dynamic WEP encryption

The next step to improving wireless network security is to use the 802.1X authentication described in the previous section along with WEP encryption.

In this scheme, the access point generates a common key for all client stations. This key will be used for multicast packets. In addition, 802.1X authentication is performed each time a client station associates with the access point. As a result of this authentication, the Radius server generates a unique key to use for communication between the access point and the client station. So each client station has a unique key to encrypt its data which, in addition, is modified dynamically from time to time through re-authentications with 802.1X. In this way, attacks on WEP become more complicated.

1.5.5 WPA and WPA2 (RSN)

The last step to improving security is to use robust security, as defined in the IEEE 802.11i standard. The 802.11i standard defines a complete security environment which includes client station authentication, data encryption and key generation and distribution.

There is some confusion around the acronyms used when talking about wireless network security. Here we will try to clarify what the different acronyms mean.

As we've already mentioned, the 802.11i standard was designed to address the shortcomings of 802.11 WEP encryption. Designers had to start from scratch and try to use, as far as possible, standards that were already known and that had been tested over time.

As we've seen above, the 802.1X standard was considered for performing the authentication. When choosing an encryption algorithm, you want something that doesn't require too much memory and processing power. Back when the 802.11i standard was in its infancy, the U.S. National Institute of Standards and Technology (NIST) convened a contest to select an encryption method that would be used by the U.S. government. Advanced Encryption Standard (AES) was the method that was chosen. This really helped the task of the IEEE who, obviously, also adopted AES to encrypt data in the new security standard.

AES is an encryption algorithm that supports various modes of operation. Without entering into details, let us just state that an operating mode called AES Counter Mode-CBC MAC Protocol (AES-CCMP) was chosen for the 802.11i standard.

The problem with the AES encryption algorithm is that it requires more resources than WEP encryption because you need additional hardware for it to work. However, the problems detected with WEP meant that it was necessary to find an encryption algorithm that, while resolving the flaws in WEP, could work using the same hardware as WEP encryption. Thus, older devices without AES encryption hardware could be upgraded to support more secure encryption methods than WEP. Therefore, in addition to AES-CCMP, 802.11i defines another encryption method called Temporal Key Integrity Protocol (TKIP).

On another note, standards can take a long time to be approved. Given the flaws detected in WEP encryption, the industry needed to adopt a new security standard as soon as possible. To do this, the Wi-Fi Alliance, responsible for certification and interoperability of all WLAN devices, took elements from the 802.11i standard that was under development (in particular, TKIP encryption) and added a few small modifications. The result of this effort is what is known as Wi-Fi Protected Access (WPA).

Once the 802.11i standard was approved, the Wi-Fi Alliance adopted it as a new security standard, calling it WPA2.

Both WPA and WPA2 use an information element in beacon frames to advertise the security features of wireless networks. The information element indicates:

- The encryption to be used for group packets (broadcast and multicast frames).
- The set of encryptions that can be used for individual packet encryption between a client station and the access point.
- The set of methods that can be used for authentication and key management.

The information element format for WPA and WPA2 is similar, with the element identifier varying. The way to indicate which encryption, authentication and key management method to use is exactly the same in both cases. For this reason, while the WPA standard does not support AES-CCMP, many devices that support WPA can also be configured with AES-CCMP.

Networks that use WPA or WPA2 are called Robust Security Networks (RSN). If a WEP-enabled client station is allowed to join a network that supports WPA or WPA2, the network is called a Transitional Security Network (TSN).

To recap, WPA and WPA2 networks use an information element in the beacon frames to announce network security features. These include:

- The encryption method to be used.
- The authentication method and type of key management to be used.

ENCRYPTION

The 802.11i standard allows the following encryption types to be announced in the information element:

- WEP-40: 40-bit key WEP encryption.
- WEP-104: 104-bit key WEP encryption.
- TKIP
- AES-CCMP

As already mentioned, the information element can include multiple encryption types. Thus, if multiple encryptions are supported, each client station can select the one it wants based on its characteristics. A client station reports the encryption that it is going to use in the connection request it sends to the access point.

The 802.11i standard imposes some encryption use restrictions:

- WEP-40 and WEP-104 encryption are only valid as group encryption (they can never be advertised as individual encryption) and should only be used in TSN networks to facilitate the transition to an RSN network.

- In case different types of encryption are supported, and since all client stations must be able to receive group frames, the encryption that must be used for group encryption (broadcast and multicast frames) is the least secure, and the order of security, from least secure to most secure, is the one used in the previous listing.

AUTHENTICATION AND KEY MANAGEMENT

The 802.11i standard provides two possibilities for Authentication and Key Management (AKM):

- Authentication using 802.1X
- Pre-shared Key

In the first case, 802.1X authentication is used to obtain a master key (Pairwise Master Key or PMK). In the second case, a master key is configured directly on the wireless device. The master key configured in this second case must be the same for all client stations that belong to the wireless network.

In both cases, the master key is not used directly to encrypt data: both the access point and the client station must use the master key to generate a set of keys (Pairwise Transient Key or PTK) to be used during data encryption.

Once both the client station and the access point have the master key (either through 802.1X authentication or direct configuration on the device), they perform a four-way packet exchange, called the four-way handshake, where:

- Each party confirms that there is a usable master.
- Each party demonstrates to the other end that it knows the master key.
- The PTK to be used during the session is derived.
- The keys to be used are installed.
- The installation of all keys is confirmed.

In this way, each time a client station connects to a wireless network, unique keys are generated for the session. Furthermore, these keys are individual: the access point uses different keys to communicate with each client station. The keys used can also be renewed from time to time by redoing the four-step negotiation process mentioned above.

We still need to consider group packets. Since these packets are addressed to several client stations, they must be encrypted with a common key. To do this, the access point first generates a Group Master Key (GMK) and uses it to derive a Group Transient Key (GTK). It then sends the GTK through a packet exchange called a Group Key Handshake to all client stations that belong to the network.

Each time a client station leaves the wireless network, the access point generates a new GTK and sends it to the client stations, thus avoiding security risks.

The following figure outlines the packet exchange that takes place between a client station and an access point up until the point when the client station can start sending and receiving packets over the wireless network.

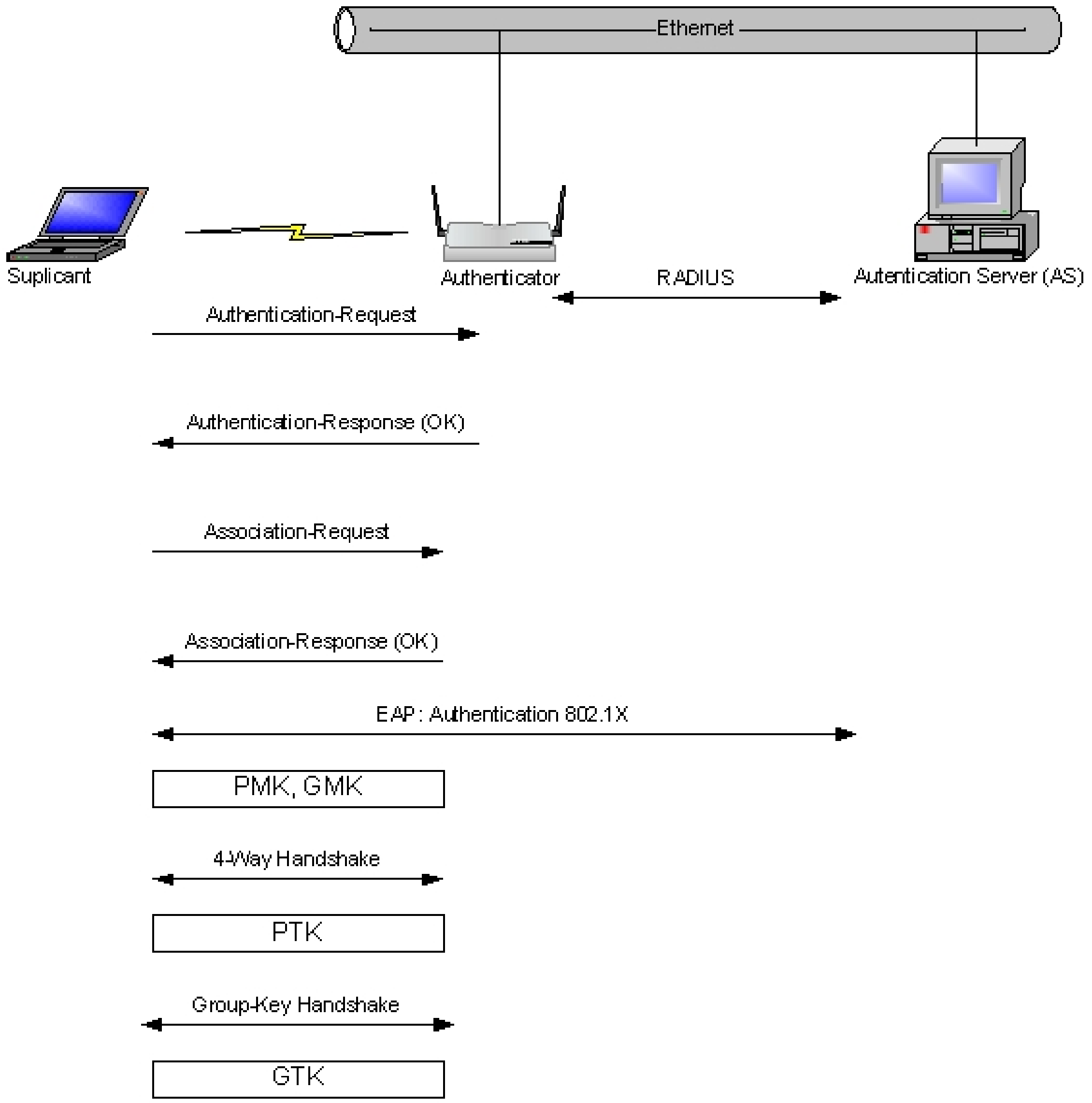


Fig. 13: **Association with an RSN network**

1.5.6 WPS

Wi-Fi Protected Setup (WPS), also known as Wi-Fi Simple Configuration (WSC), is a mechanism developed by the Wi-Fi Alliance that helps you connect a device to a WLAN without having to configure complicated security parameters.

There are two variants:

- PBC
- PIN

In the first, the user initiates a discovery process by pressing a button (physical or virtual) in both the access point and the client station. From there, the client station discovers the access point and is configured with the appropriate security parameters to allow it to connect to the network through a packet exchange.

In the second variant, the user obtains a PIN from the client station and enters it into the access point. Then the process is similar to that described for the first variant, leaving the client station configured with the necessary parameters to allow it to connect to the network.

The WPS protocol can also be used to configure the access point, although it is not usually used.

Note

If using WPS, MAC access control is ignored.

1.6 Quality of service on wireless LAN networks

Different types of traffic can co-exist in a WLAN network. The Quality of Service (QoS) requirements for each of these traffic types may differ markedly from each other. Consider, for example, the different needs of voice, video or file exchange traffic. WLAN QoS issues were not sufficiently addressed in the original version of the 802.11 standard. However, the 802.11e amendment, incorporated in the revised version of IEEE 802.11-2007 standard, defines enhancements for QoS in WLAN networks.

During the 802.11e approval process, the industry started from a draft standard to define the basic QoS concepts to facilitate interoperability between devices from different manufacturers. This resulted in Wireless MultiMedia (WMM), defined by the Wi-Fi-Alliance. Both standards are based on the modification of media access mechanisms.

1.6.1 WMM

According to the DCF (Distributed Coordination Function) protocol, as detailed in the original 802.11 standard, when a client station has a packet to transmit, it is governed by predetermined times for accessing the medium, regardless of the type of traffic. That is, all traffic is treated equally. Among all these times, we will highlight two: DIFS and the contention window (CW) time.

DIFS (DCF IFS) is the minimum time client stations wait before transmitting management or data frames if the medium is clear. If the medium is busy, client stations cannot transmit and must instead defer transmission for a minimum duration of DIFS plus backoff time, defined as:

Backoff time = Random() x Slot time

Where,

- Random() generates a random backoff interval [0, CW], with CW being variable within the limits of the contention window. CWmin # CW # CWmax.

That is, the transmission time for a data frame is imposed, among others, by the DIFS time and by the size of the contention window.

The WMM standard defines Enhanced Distributed Channel Access (EDCA). EDCA behavior is similar to DCF, but allowing QoS in WLAN networks. EDCA introduces the concept of Access Category (AC): classifying packets into different categories according to priority. Four ACs are defined: background, best-effort, video and voice.

As in DCF, where client stations must wait a minimum of DIFS before transmitting data, in EDCA they are required to wait an Arbitration Inter Frame Spacing (AIFS) time period for the same purpose. However, in this case, AIFS is a value that depends on the AC. Consequently, the traffic transmitted by a smaller AIFS AC waits less time to access the medium and therefore has a greater chance of finding it clear and transmitting.

Just as AIFS is a function of the AC, so too are the CWmin, CWmax and TXOP parameters, where:

- CWmin is the minimum contention window size.
- CWmax is the maximum contention window size.
- TXOP (Transmission Opportunity) is the time interval during which client stations can transmit. A 0 value indicates that only one transmission can be made.

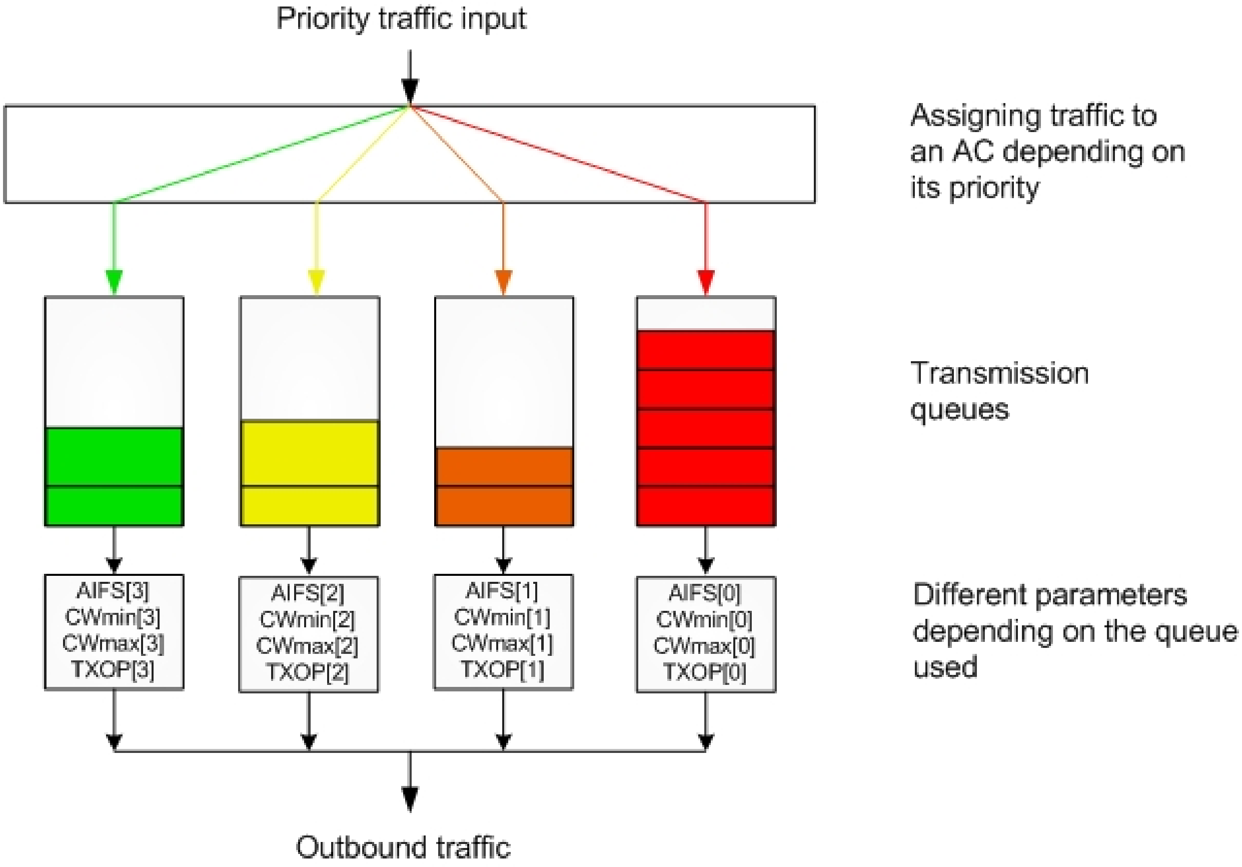


Fig. 14: **Traffic is routed according to its priority**

Chapter 2 Configuring WLAN Interfaces

2.1 Note on WLAN settings

There are several *Teldat* devices with WLAN interfaces. Due to different hardware characteristics in these devices, the configuration commands vary from one device to another. Thus, some commands are only available for one type of hardware and not for another. In addition, there are some configuration options that vary depending on the type of hardware.

2.2 Accessing WLAN settings

Access the Wireless LAN interface as follows:

(1) Enter **list devices** in the *Config>* setup menu to obtain a list of available interfaces.

(2) Enter **network** followed by the identifier of the Wireless LAN interface you want to configure.

Example:

```
*config



Interface             Connector     Type of interface
ethernet0/0           GE0/FE0/LAN1  Fast Ethernet interface
ethernet0/1           GE1/FE1/LAN2  Fast Ethernet interface
serial0/0             SERIAL0/WAN1  Synchronous Serial Line
x25-node              ---           Router->Node
wlan3/0               SLOT3         Wireless LAN Interface
ppp1                  ---           Generic PPP
Config>network wlan3/0

-- Wireless LAN Interface. Configuration --
 wlan3/0 WLAN config>
```

2.3 Configuration menu structure

For some devices with a WLAN interface, you have the option of configuring the use of several wireless networks by creating WLAN subinterfaces. For more information, please see the following manual: *Teldat* Dm799-I Subinterfaces Wireless LAN.

A Wireless LAN interface configuration menu is comprised of two different parts:

- All the parameters common to all BSSs are in the root menu. This menu includes the interface's physical parameters (channel to be used, operating mode, fragmentation threshold, antenna to be used, etc.), as well as other parameters that cannot be differentiated by BSS due to hardware restrictions. This menu is only available in the base WLAN interface.
- When configuring a network identifier (SSID), you access a particular configuration menu for the BSS where you can configure specific parameters of the BSS. In particular, you can configure the specific security parameters that will be used in the BSS (authentication type, encryption, etc.). This menu is available in the base WLAN interface and the WLAN subinterfaces.

While this is the general structure, there are a number of parameters that, despite not being common to all WLAN interfaces, are configured in the root menu instead of the BSS menu. This is the case with WPS-related parameters since these parameters are not associated with a particular SSID.

2.4 Configuration common to all BSSs

This section briefly describes the configurable parameters in a Wireless LAN interface root configuration menu.

2.4.1 Configuring media access parameters

Band

You can configure the operating mode for the wireless network through the **band** command. Use this command to select the operating frequency band and the operating mode. The modes you can configure are 802.11b, 802.11g and 802.11n for the 2.4 GHz band and 802.11a, 802.11n and 802.11ac for the 5 GHz band.

Channel

You can configure the operating channel through the **channel** command. By default, the access point is configured to automatically select the best possible channel. To do this, at start up, it listens to all the channels available in search of wireless networks that might cause interference. Finally, it selects the best quality channel.

User Country

As explained in the introduction, each country regulates their radio-electric spectrum, allocating channels for the different applications available. Because of this, the usable channels depend on the country you are working in.

You can use the **country** command to set the country code to the country of operation and thus set the authorized radio channels. Appendix A shows the available country codes.

⚠ **Caution**

Setting the wrong country code may lead to violation of a country's laws on radio frequency emissions.

5 GHz band

The 5 GHz band is divided into four sub-bands:

- Band 1: UNII-1. 5.15 to 5.25 GHz band (channels 34-48)
- Band 2: UNII-2. 5.25 to 5.35 GHz band (channels 52-64)
- Band 3: UNII-2e .5.47 to 5.725 GHz band (channels 100-140)
- Band 4: UNII-3. 5.725 to 5.825 GHz band (channels 149-165)

Each regulator imposes conditions on the use of the different bands. Certain bands are not available in some countries, while others are only available if certain conditions are met. For example, to operate in the UNII-2 band in the United States, you must use Dynamic Frequency Selection (DFS) so as not to interfere with possible radar signals.

You can use the **regulatory bands allow** command to restrict the bands that are used when working at 5 GHz. If nothing is configured, you can access the bands for which you have obtained certification. You can use the **no regulatory bands allow default** command to remove the automatic selection and manually specify the bands to use. In principal they are all allowed. You can use the **no regulatory bands allow <band>** command to eliminate the channels of a sub-band.

Antenna to use

The **antenna** command allows you to select the antenna that will be used to transmit frames. By default, the access point uses antenna diversity, that is, it selects the most suitable antenna for transmission depending on the detected signal-to-noise ratio. If you want the access point to use only one antenna (if, for example, you have installed a high gain antenna), you should bear in mind that the antennas are referenced looking at the access point from behind. That is, the **antenna left** command selects the left antenna looking at the access point from the rear.

☞ **Note**

We do not recommend specifying the antenna if you are using 802.11n.

Transmission power

You can select the transmission power to use. You use the **power transmit** command for this.

Beacon frame periodicity

You can use the **beacon** command to configure the following:

- Beacon frame periodicity. This is configured using the **beacon period** command and gives the periodicity in time units (TU). One time unit equals 1024 microseconds.
- Delivery Traffic Indication Map (DTIM). This is configured using the **beacon dtim** command and gives the number of beacon frames sent between frames containing the DTIM information element. If, for example, you configure a value of 5, the DTIM information element is sent in 1 out of every 5 beacon frames.

Fragmentation threshold

The **fragment-threshold** command allows you to activate fragmentation by setting a particular WLAN frame size threshold. If the frame that is being transmitted is larger than the threshold, it will trigger the fragmentation function.

Operating Mode

The **opmode** command configures the WLAN interface operating mode: client or access point.

RTS/CTS threshold

The **rts threshold** command allows you to activate the RTS/CTS mechanism by setting a particular WLAN frame size threshold. If the frame that is being transmitted is larger than the threshold, it will trigger the RTS/CTS mechanism, so that an RTS is sent and a CTS frame waited for before sending the frame in question.

2.4.2 Configuring the quality of service parameters (WMM)

You can configure the parameters defining the different transmission queues from the WMM menu.

QoS

By default, quality of service (QoS) is enabled. If you want to disable it, enter the **qos disable** command from the WMM menu.

Example:

The following example disables QoS.

```
wlan3/0 WMM config>qos disable
```

AC Parameters

You can set the four Access Category (AC) queue parameters from the WMM menu. These are: AIFS, CWmin, CWmax and TXOPlimit.

Once a parameter is configured, it is used independently of the mode it is operating in. The default values for these parameters, corresponding to the values proposed by the WMM standard, are shown in the following table:

Parameters the access point announces to the client stations

AC	Cwmin	CWmax	AIFS	TXOP Limit (802.11b)	TXOP Limit (802.11a/g)
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	aCWmax	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	2	6.016ms	3.008ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	2	3.264ms	1.504ms

Parameters used by the access point

AC	Cwmin	CWmax	AIFS	TXOP Limit (802.11b)	TXOP Limit(802.11a/g)
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCWmin+1)-1	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	1	6.016ms	3.008ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	1	3.264ms	1.504ms

Where aCWmin and aCWmax depend on the operating mode, as indicated in the 802.11 standard.

Example:

This example configures the AIFS length used by the access point for background access category (AC) frames.

```
wlanx/x WMM config>background ap AIFS 2
```

Example:

The following example configures the AIFS length used by client stations for background access category (AC) frames.

```
wlanx/x WMM config>background sta AIFS 3
```

2.4.3 Client operation parameters

Scanning for available networks

Use the **scan** command to configure a variety of network search parameters for the client station:

- Bands in which to search for available networks (band option): 2.4 GHz band, 5 GHz band or both.
- Search parameters for new networks once connected (**bgscan** option).
- Enable or disable the access point blacklist (**blacklist** option).

2.5 Configuring the WPS settings

As already indicated, these parameters are configured in the root menu instead of the BSS menu despite being different for each WLAN interface.

WPS

By default, WPS is enabled. If you want to disable it, use the **no wps enable** command. This command is only available when the interface is operating in access point mode.

Updating your settings

By default, the wireless settings received by WPS are not updated in flash memory. If the device restarts, you have to rerun WPS to reconnect to the wireless network. If you want to save the wireless settings in flash memory, use the **wps update-config** command. This command is only available when the interface is operating in client mode. Please note that if the user has changed the configuration without saving the changes, the device will not proceed to save the settings received by WPS. This is to avoid saving temporary configurations,

WPS parameters

The remaining configurable commands refer to device characteristics (code version, router model, etc.). These parameters should not normally be configured. If no value is set, the device will take the default settings consistent with the device and code used.

2.6 Configuring the BSS

To access a BSS configuration, use the **bss** command followed by the network identifier of the network you want to configure. If the BSS does not exist, it is created. If you want to use multiple BSSs on the same WLAN interface, you need to create WLAN subinterfaces. For more information, refer to the following manual: *Teldat* Dm799-I Subinterfaces Wireless LAN.

From the BSS configuration menu, you can configure the BSS security parameters.

2.6.1 Configuring Security

Hiding the Network Identifier

You can use the **ssid-suppress** command to instruct the access point not to send the network identifier (SSID) in the beacon frames. In this way, the access point does not announce the WLAN network that it belongs to, and only those client stations that know the name of the network in question are able to join it. This option provides very little security.

MAC access control list

On some devices the MAC access control lists (ACL) are configured by BSS. You can configure the following parameters in MAC access control lists.

- Type of access control:

  - If you want to configure access control to only allow the client stations whose MAC address appears on the ACL to connect to the wireless network, you use the **access-control allow** command.

  - If, on the other hand, you want to configure access control to block the client stations whose MAC address appears on the ACL from connecting to the wireless network, you use the **access-control deny** command.

  - To disable MAC address access control, use the **access-control disable** command.

  - List of MAC addresses that MAC filtering is applied to, allowing or blocking their association with the access point.

Authentication

You can configure three types of authentication using the **authentication** command:

- Open-system: open authentication. This is the default authentication.
- Shared-key: shared-key authentication.
- Auto: automatic authentication. The access point automatically runs shared-key authentication for WEP-enabled client stations and open authentication for all other client stations.

If you enable WPA or WPA2, you will only be able to configure open authentication.

Note

Because of the security issues associated with shared-key authentication, *Teldat* recommends using open authentication.

WEP Keys

WEP keys can be configured with the following lengths:

- 40 bits.
- 104 bits.
- 128 bits.

WEP keys can be entered as ASCII or hexadecimal characters. They can also be entered in plain or encrypted text.

Note

For security purposes, all configured keys appear in encrypted format when WLAN interface settings are displayed.

The command syntax for configuring a WEP key is as follows:

key <index> size (40|104|128) (ascii|hex) (plain|ciphered) <key>

Example 1:

This example sets the keyke key as a 40-bit private key in index 1, using ASCII characters, and entering it in plain text:

```
key 1 size 40 ascii plain keyke
```

Example 2:

This example configures the ‘12345678901234567890123456’ key as a 104-bit key in index 3, using hexadecimal characters, and entering it in encrypted format:

```
key 3 size 104 hex ciphered 0x018FC2F235ED9867137139F7E20048E31926771CCAFC5C5
FCC4B72452BA4F016
```

For each BSS, you can configure the key index that the access point will use to transmit frames in the BSS. You configure the default key using the **key default <index>** command.

WEP

To enable WEP on an interface, you should use the **privacy-invoked** command. This command starts some kind of security at the access point. If you don't configure WPA or WPA2, WEP security will be invoked.

If you configure WEP, you can configure the type of keys to use with the **wep**-**keysource** command:

- Static: static keys. The keys configured in the WLAN interface configuration menu are used.
- Dynamic: dynamic keys. The keys to be used are obtained from an external authentication server through 802.1X authentication, and are distributed to the client stations via EAPOL.
- Mixed: static and dynamic keys. The key for communicating with a client station is obtained from an external server through 802.1X authentication, and is distributed to the client station via EAPOL. The multicast key is statically configured on the access point.

Note

If using mixed wep-keysource, you should configure the static key in position 2 or 3 because some client stations do not allow the multicast key to be in position 1.

WPA and WPA2 (RSN)

To create a robust security network (RSN), as defined in the 802.11i standard, you need to enable WPA or WPA2. To configure WPA or WPA2 security you must:

(1) Invoke security in the BSS using the **privacy-invoked** command.

(2) Enable WPA or WPA2 using the **rsn** command. You can configure both security methods, in which case the access point includes both the WPA and the WPA2 information element in the beacon frames.

(3) Configure the type of data encryption.To configure encryption in the BSS, you use the **cipher** command. You can configure TKIP or AES-CCMP encryption. The encryption is not exclusive; so when both AES-CCMP and TKIP encryption are configured, the access point announces in the beacon frames that it is capable of using both encryption types. In this case, client stations wishing to connect to the wireless network can choose the type of encryption they want for communication with the access point.

Note

When multiple ciphers are configured, the access point uses the least secure cipher type to send multicast frames. TKIP encryption is less secure than AES-CCMP encryption.

(1) Configure the authentication and key management (AKM) type you want to use using the **akm-suite** command. You can configure:

- dot1x: 802.1X authentication is used to obtain the master key from an external authentication server.
- psk: preshared-key: the master key is configured in both the access point and client station. The specific keys to be used during a session are derived from this key.

(2) If you configure akm-suite psk, you need to configure the master key that will be used to generate the different keys. You can configure the master key in two ways:

- By entering the key directly as a 16 hexadecimal string. To do this, use the **wpa-psk key (plain|ciphered) <key>** command.
- By entering a text string between 8 and 63 characters in length. In this case, the access point uses a procedure defined in the 802.11i standard to generate the master key to use. As it is a standard procedure, you ensure that the key generated in two different devices when entering the same string of text is identical. To configure the master key using a text string, you use the **wpa-psk passphrase (plain|ciphered) <passphrase>** command.

2.6.2 Parameters for client operation

Frames to maintain connection

The **keep-alive** command allows you to specify the periodicity (in seconds) with which a client station sends a frame with no data. In this way, you can ensure that the client station is not disconnected by the access point due to inactivity.

Priority

The **priority** command allows you to decide which network to connect to when several configured networks are detected. The higher the network priority, the sooner an attempt to connect to said network is made.

802.1X Supplicant

The **dot1x** command is used to access the supplicant configuration menu to use 802.1X authentication when the WLAN interface is operating in client mode.

2.6.3 Other parameters

Associated client stations limitation

The **max-associations** command allows you to place a limit on the number of client stations that can simultaneously connect to the access point. If the configured number is reached, no new associations are allowed.

Client isolation

The **client-isolation** command isolates the different client stations connected to the access point, so that they cannot communicate directly with each other (they cannot send MAC frames to each other). This feature is disabled by default; that is, the client stations can communicate with each other.

2.7 Configuration menu commands

This section summarizes the various configuration commands available in the Wireless LAN interface configuration menu.

The following table summarizes the WLAN interface configuration commands. These commands are explained in detail in the following sections.

Some commands are common to all of the device's interfaces. These commands are described in the following manual: *Teldat* Dm772-I Common Configurations for Interfaces.

Command	**Function**
? (HELP)	Displays configuration commands or command options.
ANTENNA	Sets the antenna to be used for transmission
BAND	Configures the WLAN interface operating band and mode.
BEACON	Configures beacon frame transmission parameters.
BSS	Accesses a BSS configuration menu.
CHANNEL	Sets the channel to use.
COUNTRY	Sets the country. The WLAN interface must comply with the standards of said country when selecting the allowed channels.
DEBUG-LEVEL	Configures the driver related traces that are displayed if WLAN traces are enabled in the event subsystem.
FRAGMENT-THRESHOLD	Configures the fragmentation threshold.
INPUT-BUFFERS	Sets the number of reception buffers.
LEGACY-client stationS	Allows connections from legacy (non HT) client stations.
LIST	Displays the configuration.
MODE	Configures the wireless mode that the WLAN interface will use: 802.11a, 802.11b, 802.11g or 802.11n.
N-SPATIAL-STREAMS	Configures the number of spatial streams used in 802.11n.
NO	Sets parameters to their default values.
OPMODE	Sets the interface operation mode in the SSID: AP or client.
OUTPUT-BUFFERS	Sets the number of output buffers for communication with lower layers.
OUTPUT-CONFIRM-BUFFERS	Sets the number of buffers that lower layers can use to confirm packet transmission to an upper layer.
OUTPUT-FAIR	Sets the number of packets that must be in the interface output queue for flow control to act.
POWER	Configures power settings.
PROMISCUOUS-MODE	Enables promiscuous mode.
RADIO-SHUTDOWN	Disables the radio interface.
REGULATORY	Configures parameters related to regulatory entities.
RESET-ON-ERROR	Configures the behavior of the device against software errors.
RETRY-LIMIT	Configures the number of retries for short and long frames.
RTS	Configures parameters related to transmission using the RTS/CTS mechanism.
SCAN	Configures additional network search options for roaming.
SHORT-GUARD-INTERVAL	Enables short guard interval.
SHORT-PREAMBLE	Enables short preamble for 802.11b/g client stations.
SSID-CHANGE	Allows you to change a BSS network identifier (SSID).
SWITCH-CHANNEL-ON-STUCK	Configures behavior when transmission gets stuck.
WMM	Configures the quality of service parameters.
WPS	Configures Wi-Fi Protected Setup (WPS) parameters.
EXIT	Exits the WLAN interface configuration menu.

2.7.1 ? (HELP)

Displays the available commands or command options.

2.7.2 ANTENNA

Configures the antenna that will be used for transmission. You can select the left, right or both antennas (antenna diversity). When selecting the antenna, bear in mind that they are referenced by looking at the device from the rear: the left antenna is the one to the left when looking at the device from behind.

We do not recommend configuring the antenna if you are using 802.11n mode.

Syntax:

```
wlan3/0 WLAN config>antenna ?
  left         selects left antenna
  right        selects right antenna
  diversity    selects antenna diversity
wlan3/0 WLAN config>
```

Antenna diversity is enabled by **default**.

Example:

The following example sets the device to use the right antenna:

```
wlan3/0 WLAN config>antenna right
```

2.7.3 BAND

Configures the WLAN interface mode: 802.11a, 802.11b, 802.11g or 802.11n. Mixed modes can be configured. If, for example, you want to operate in 802.11n mode but allow client stations in 802.11b and 802.11g mode to connect, you need to configure 11b/g and n modes.

This command is only available when the WLAN interface is configured in access point (AP) mode. When configured in client mode, the **Scan Band** command should be used to select the best operating mode supported.

Syntax:

```
wlanx/x WLAN config>mode ?
  2.4GHz    2.4 GHz frequency band
      mode
        11b    Mode 11b
             <cr>
             11g     Mode 11g
                <cr>
                11n    Mode 11n (High Throughput)
        11g    Mode 11g
            11n    Mode 11n (High Throughput)
  5GHz      5 GHz frequency band
      mode
          11a    Mode 11a
             <cr>
             11n     Mode 11n (High Throughput)
                 <cr>
                 11ac    Mode 11ac (Very High Throughput)
```

Default value: The default value depends on the wireless card's characteristics. Thus, the default mode for cards supporting 11n mode in the 2.4 GHz band is 802.11b/g/n Mixed. If the card doesn't support 11n mode in the 2.4GHz band, the default mode is 802.11b/g Mixed.

Example:

The following example configures the WLAN interface to operate using the 802.11a standard.

```
wlan3/0 WLAN config>band 5GHz mode 11a
```

Command history:

Release	Modification
11.01.02	This command was introduced.

2.7.4 BEACON

Configures beacon frame transmission parameters.

Syntax:

```
wlan3/0 WLAN config>beacon ?
  dtim      Configures Data Beacon Rate (DTIM)
  period    Configures beacon transmission period in time units (TUs)
wlan3/0 WLAN config>
```

BEACON DTIM

Sets the number of beacon frames till the next DTIM information element. The DTIM information element is sent periodically in beacon frames and informs the client stations that the multicast/broadcast frames stored in the access point are to be immediately transmitted. The client stations that are in power save mode use this information to listen to multicast/broadcast traffic.

This parameter's configuration affects the client stations in power save mode. The higher the value configured, the longer a client station can remain "asleep" before having to wake up to receive broadcast and multicast traffic. Bear in mind, however, that high values imply that the access point must store more frames for later delivery. If you configure a high value, the access point might not have enough resources to store the frames and will therefore discard them.

The default setting is 1. That is, broadcast/multicast frames are delivered with each beacon frame.

Example:

The following example sets the DTIM period so that every third beacon includes a DTIM information element:

```
wlan3/0 WLAN config>beacon dtim 3
```

BEACON PERIOD

Sets the interval between beacon transmissions. Beacon frames are frames that the access point transmits periodically to advertise specific wireless network information (such as the mode, supported speeds, security requirements, etc).

The beacon frame interval is given in units of time. The IEEE 802.11 standard defines a unit of time, or time unit (TU), as equal to 1,024 microseconds.

This parameter's configuration affects the client stations in power save mode: It has similar implications to those described for the DTIM beacon parameter: the longer the beacon frame interval, the longer client stations can *sleep*; however, the access point must store more frames for later delivery.

The default setting is 100; that is, a beacon frame is sent every 102.4 milliseconds.

Example:

The following example sets the beacon interval so that beacon frames are sent every 300 TU:

```
wlan3/0 WLAN config>beacon period 300
```

2.7.5 BSS

The **bss** command allows you to create a basic service area (BSS) and access its configuration parameters. A BSS is identified by a network identifier (SSID).

Syntax:

```
wlan3/0 WLAN config>bss <ssid>
```

The SSID is an alphanumerical text string of 1-32 characters.

Example:

The following example configures a basic service area with “*Teldat* WLAN” SSID:

```
wlan3/0 WLAN config>bss "Teldat WLAN"


wlan3/0 bss config>
```

Note

Please refer to the section on *BSS configuration menu commands* on page 50 for BSS configuration information.

2.7.6 CHANNEL

Sets the preferred radio channel and channel settings for the device. If you want the access point to automatically select a channel from the detected networks, use the **no channel** command.

Syntax:

```
wlan3/0 WLAN config>channel ?
  number       Channel number
  frequency    Channel frequency in MHz
  bandwidth    Channel bandwidth
       20MHz     20 MHz
       40MHz     40 MHz (automatic selection of secondary channel)
       40+MHz    40 MHz (secondary channel above primary channel)
       40-MHz    40 MHz (secondary channel below primary channel)
       80MHz     80 MHz (automatic selection of secondary channel)
       80+MHz    80 MHz (secondary channel above primary channel)
      80-MHz    80 MHz (secondary channel below primary channel)

  plan <band>    Select channels available
       auto           Automatic channel plan
       user-defined    User defined channel plan
          add <channel>
wlan3/0 WLAN config>
```

number: Configures the channel number to use.

frequency: Configures the channel's center frequency in MHz.

bandwidth: Configures the channel’s bandwidth. Valid when using 11n mode. The default setting is 20 MHz. You can set a 40 MHz bandwidth with the secondary channel above (option **40+MHz**) or below (option **40-MHz**) the main channel.

plan: Configures the allowed radio channels in a frequency band. This parameter is available with the auto channel selection process. The user can select **auto** or **user-defined** in a given band (2.4 or 5 GHz).

The most commonly used channels are available in **auto** mode; that is, channels 1, 6 and 11 are available in the 2.4 GHz band.

In **user-defined** mode, the user specifies the channels that he wants available by explicitly adding them using the **add** option.

Note

If you enter a channel that is not available in the selected mode/country, you will get an error message.

The device is configured by default to automatically select a channel width of 20 MHz.

Note

The access point should be using a 40 MHz bandwidth where possible. If there are lots of neighboring wireless networks, it automatically switches to 20 MHz to avoid interfering with those networks. In practice, it is very hard for an access point to operate at 40 MHz in the 2.4 GHz band.

Example:

This example configures channel 10:

```
wlan3/0 WLAN config>channel number 10
```

Example:

Configuring channel 1 in 802.11b/g mode (2.412 GHz):

```
wlan3/0 WLAN config>channel frequency 2412
```

Example:

This example configures channel 6 with 40 MHz bandwidth, secondary channel below channel 6.

```
wlan3/0 WLAN config>channel number 6
wlan3/0 WLAN config>channel bandwidth 40-MHz
```

Example:

This example shows the error message that you might see if the entered channel is not allowed:

```
wlan3/0 WLAN config>channel number 12
CLI Error: Channel is not part of country code NA or not possible with this hard
ware
CLI Error: Command error
wlan3/0 WLAN config>
```

Example:

The following example configures a user-defined channel plan for the 2.4 GHz band with channels 1 and 11:

```
wlan0/0 WLAN config>channel plan 2.4GHz user-defined add 1
wlan0/0 WLAN config>channel plan 2.4GHz user-defined add 11
```

Command history:

Release	Modification
11.01.00	The **plan** option was introduced.
11.01.02	The *2_4GHz* option is no longer valid and has been changed to *2.4GHz*.
11.01.02	The *80MHz, 80+MHz* and *80-MHz* options have been added to **channel bandwidth.**

2.7.7 COUNTRY

Sets the country whose standards the WLAN interface must comply with when selecting the allowed channels.

Syntax:

```
wlan3/0 WLAN config>country ?
  <2 chars>     Country code
```

The country code is entered as two characters corresponding to the ISO country code. For example, the ISO code for Spain is ES. A list of ISO codes the device recognizes can be found in Appendix A.

Caution

Setting the wrong country may result in violations of the radio frequency regulations that apply in a country.

Caution

The list of available countries is restricted by the regulatory domain license in use.

The default country code depends on the regulatory domain license in use.

Example:

The following example configures the device to comply with Spanish regulations:

```
wlan3/0 WLAN config>country ES
```

2.7.8 DEBUG-LEVEL

Configures the driver-related traces that are displayed if WLAN traces are enabled in the event subsystem.

Syntax:

```
wlanx/x WLAN config>debug-level <ath|hal|ieee80211> <value>
  ath          Atheros Device Object Layer
  hal          Hardware Adaptation Layer
  ieee80211    IEEE 802.11 Protocol Stack Layer
```

Traces can be configured on three different layers. Each layer has an associated hexadecimal value which shows the associated subsystems for which traces are shown. The defined layers are:

- ieee80211: the top lay of the driver. Runs the different WLAN interface protocols. It is a 64-bit mask. To configure the upper 32 bits, use the **debug-level ieee80211 high** command.
- ath: the middle layer of the driver operation. Handles the communication between the *ieee80211* layer and the *hal* layer.
- hal: the bottom layer of the driver (HAL: Hardware Adaptation Layer). Layer responsible for communication with the WLAN chip.

The following tables specify the meaning of each bit for each layer:

2.7.8.1 ath

Mnemonic	**Value**	**Meaning**
FATAL	0x80000000	Fatal errors
BTCOEX	0x40000000	Coexistence in 40 MHz
AGGR_MEM	0x20000000	Memory management
SWR	0x10000000	Software retransmission mechanism
PWR_SAVE	0x08000000	PS Poll and PS save
PPM	0x04000000	PPM management
DCS/CWM	0x02000000	Channel width management
DOTH	0x01000000	802.11h
UAPSD	0x00800000	UAPSD
DCS	0x00400000	Dynamic channel switching
TX99	0x00200000	TX99 tool
LED	0x00100000	LED management
NODE	0x00080000	Node management
STATE	0x00040000	802.11 state transitions
KEYCACHE	0x00020000	Key cache management
CALIBRATE	0x00010000	Periodic calibration
BEACON_PROC	0x00008000	Treatment of beacon interruptions
RX_PROC	0x00004000	Treatment of reception interruptions
TX_PROC	0x00002000	Treatment of transmission interruptions
INTR	0x00001000	Interruptions
HTC_WMI	0x00000800	HTC/WMI
GREEN_AP	0x00000400	*Green AP*
SCAN	0x00000200	Scan
WATCHDOG	0x00000100	Watchdog
BEACON	0x00000080	Beacon frame handling
MAT	0x00000040	MAT for s/w proxysta
RESET	0x00000020	Reset process
RATE	0x00000010	Rate control
RECV_DESC	0x00000008	Receiving descriptors
RECV	0x00000004	Basic receiving operation
XMIT_DESC	0x00000002	Transmitting descriptors
XMIT	0x00000001	Basic transmission operation
ANY	0xffffffff	Any

2.7.8.2 iee80211

Mnemonic	Value	Meaning
DFS	0x8000000000	DFS debug messages
WRAP	0x4000000000	WRAP or Wireless ProxySTA
WIFIPOS	0x2000000000	WiFi Positioning Feature
L2TIF	0x1000000000	Hotspot 2.0 L2 TIF
PROXYARP	0x800000000	11v proxy ARP
P2P_PROT	0x400000000	P2P Protocol driver
WNM	0x200000000	Wireless Network Management
RRM	0x100000000	Radio Resource Management
MLME	0x80000000	MLME
DEBUG	0x40000000	Debugging
DUMPPKTS	0x20000000	Show packets
CRYPTO	0x10000000	Cryption
INPUT	0x08000000	Packet input
XRATE	0x04000000	Handling of frame rate selection
ELEMID	0x02000000	Information elements analysis
NODE	0x01000000	Node handling
ASSOC	0x00800000	Association
AUTH	0x00400000	Authentication
SCAN	0x00200000	Scan
OUTPUT	0x00100000	Packet output
STATE	0x00080000	State machines
POWER	0x00040000	Power Save
WPA	0x00001000	WPA/RSN
ACL	0x00000800	Access lists (ACL)
WME	0x00000400	WME
IQUE	0x00000200	IQUE features
DOTH	0x00000100	802.11h
INACT	0x00000080	Inactivity
ROAM	0x00000040	client station mode roaming
ACTION	0x00000020	*Action* management frames
WDS	0x00000010	WDS (Wireless Distribution System)
SCANENTRY	0x00000008	Scan entries
SCAN_SM	0x00000004	Scan states machine
ACS	0x00000002	Automatic channel selection
TDLS	0x00000001	TDLS
ANY	0xffffffff	Any

2.7.8.3 hal

Mnemonic	Value	Meaning
FCS_RTT	0x20000000	Radio retention
BT_COEX	0x10000000	BT coexistence
DBG_TIMER	0x08000000	Debugging timers
PRINT_REG	0x04000000	Print registers
SPUR_MITIGATE	0x02000000	Spur mitigate
POWER_OVERRIDE	0x01000000	Force transmission power
FORCE_BIAS	0x00800000	Force BIAS
MALLOC	0x00400000	Memory petition
POWER_MGMT	0x00200000	Transmission power management
KEYCACHE	0x00100000	Encryption key management
BEACON	0x00080000	Processing and configuration of beacons
ANI	0x00040000	Automatic Noise Immunity (ANI)
RXDESC	0x00020000	Reception descriptor process
RX	0x00010000	Reception information
TXDEC	0x00008000	Transmission descriptor process
TX	0x00004000	Transmission information
REGULATORY	0x00002000	Regulatory table configuration and selection
DMA	0x00001000	DMA information
DFS	0x00000800	Dynamic frequency selection (DFS)
INTERRUPT	0x00000400	Interruption processing
CHANNEL	0x00000200	Channel selection and configuration
CALIBRATE	0x00000100	Calibration information
NF_CAL	0x00000080	Noise floor calibration
EEPROM	0x00000040	EEPROM read and write
EEPROM_DUMP	0x00000020	EEPROM information
QUEUE	0x00000010	Queue management for WMM
RF_PARAM	0x00000008	Radio frequency parameters
REG_IO	0x00000004	Register read and write. Use with precaution
PHY_IO	0x00000002	PHY read and write
RESET	0x00000001	Reset process
UNMASKABLE	0xffffffff	All

The default setting is 0.

Example:

The following example configures the device to display top layer events (*ieee80211*) that relate to automatic channel selection (0x00000002) and power saving (0x00040000).

```
wlan3/0 WLAN config>debug-level ieee80211 0x0040002
```

Command history:

Release	Modification
11.01.02	New debugging information added.
11.01.03	New **high** option added to **debug-level ieee80211** .

2.7.9 FRAGMENT-THRESHOLD

Configures the fragmentation threshold. If the packet is larger than the configured threshold, it is fragmented for transmission.

Syntax:

```
wlan3/0 WLAN config>fragment-threshold ?
  <256..2346>    Value in the specified range
wlan3/0 WLAN config>
```

Default is 2346.

Example:

The following example configures a fragmentation threshold of 1500 bytes. Packets exceeding this threshold are fragmented.

```
wlan3/0 WLAN config>fragment-threshold 1500
```

2.7.10 INPUT-BUFFERS

Sets the number of buffers to use in reception.

Syntax:

```
wlanx/x WLAN config>input-buffers ?
  <32..256>    Value in the specified range
wlanx/x WLAN config>
```

The default setting is 40.

2.7.11 LEGACY-client stations

Allows legacy (non-HT) client stations to connect. When disabled, only HT-capable client stations (802.11n capable client stations) are allowed to join the BSS.

Syntax:

```
wlanx/x WLAN config>legacy-client stations
```

By default, the device is configured to allow legacy client stations to join the BSS.

Example:

The following example prevents legacy client stations from joining the BSS.

```
wlan3/0 WLAN config>no legacy-client stations
```

Command history:

Release	Modification
11.01.00	This command was introduced.

2.7.12 LIST

Displays the WLAN interface configuration. For security reasons, the configured password will not be displayed when the configuration is listed.

Syntax:

```
wlan3/0 WLAN config>list
```

2.7.13 MODE

Sets the operating mode of the WLAN interface: 802.11a, 802.11b, 802.11g or 802.11n. Mixed modes are supported. If, for example, you want to operate in 802.11n mode and allow client stations in 802.11b and 802.11g mode to connect, you need to configure 11b/g and n mode.

This command is only available when the WLAN interface is set to access point (AP) mode. When it is set to client mode, the **Scan Band** command should be used to select the best operating mode supported.

Syntax:

```
wlan3/0 WLAN config>mode ?
  11a    Mode 11a
```

```
         <cr>
        11n     Mode 11n
  11b    Mode 11b
         <cr>
        11g     Mode 11g
                <cr>
                11n    Mode 11n
  11g    Mode 11g
  11n    Mode 11n
wlan3/0 WLAN config>
```

Default value: The default value depends on the wireless card's characteristics. Thus, the default mode for cards supporting 11n mode in the 2.4 GHz band is 802.11b/g/n Mixed. If the card doesn't support 11n mode in the 2.4GHz band, the default mode is 802.11b/g Mixed.

Example:

The following example configures the WLAN interface to operate using the 802.11a standard.

```
wlan3/0 WLAN config>mode 11a
```

Command history:

Release	Modification
11.01.02	This command is obsolete.

2.7.14 N-SPATIAL-STREAMS

Specifies the maximum number of spatial streams. This parameter only applies to 802.11n access points. If the access point does not support the number of spatial streams configured, its maximum value is used.

Syntax:

```
wlanx/x WLAN config>n-spatial-streams ?
  <1..3>    Value in the specified range
```

By default, the device supports 3 spatial streams.

Example:

The following example configures *2* spatial streams on the device:

```
wlan3/0 WLAN config>n-spatial-streams 2
```

Command history:

Release	Modification
11.01.00	This command was introduced.

2.7.15 NO

Sets parameters to their default values or clears configuration.

Syntax:

```
wlan3/0 WLAN config>no ?
  antenna                     Configures antenna to use
  beacon                      Configures Beacon parameters
  bss                         Configures the Basic Service Set
  channel                     Configures the radio channel
  country                     Configures the country code
  debug-level                 Configures debug level for traps
  fragment-threshold          Configures the fragment threshold
  input-buffers               Configures number of receive buffers
  mode                        Configures the wireless mode
  output-fair                 Configures output fairness
  power                       Configures power parameters
  promiscuous-mode            Enable promiscuous mode
  regulatory                  Configures regulatory constraints
  reset-on-error             Resets the device if an unexpected condition is
                             met
  rts                        Configures RTS parameters
  switch-channel-on-stuck    Channel switching on detection of beacon stuck
  wps                        Configures WPS
wlan3/0 WLAN config>
```

Example:

This example restores the default channel setting.

```
wlan3/0 WLAN config>no channel
```

Example:

This example deletes the key configured in position 3.

```
wlan3/0 WLAN config>no key 3
```

2.7.16 OPMODE

Sets the operating mode of the wireless interface in the BSS: access point (AP) or client.

Syntax:

```
wlan3/0 config>opmode ?
  access-point    operation as an access point
  client          operation as a client
wlan3/0 config>
```

By default, the interface operates in access point mode in the BSS.

Example:

The following example configures the interface to operate in client mode in the BSS.

```
wlan3/0 config>opmode client
```

Command history:

Release	Modification
11.00.04	Command moved from bss menu to root menu.

2.7.17 OUTPUT-BUFFERS

Sets the number of transmission buffers used for communicating with the lower layers.

Syntax:

```
wlanx/x WLAN config>output-buffers ?
  <1..1024>    Value in the specified range
wlanx/x WLAN config>
```

The default setting is 10.

Note

Changing this parameter is not recommended unless you are expressly asked to do so by *Teldat*.

2.7.18 OUTPUT-CONFIRM-BUFFERS

Sets the number of buffers to be used by the lower layers to confirm packet transmission to the upper layer.

Syntax:

```
wlanx/x WLAN config>output-confirm-buffers ?
  <32..1024>    Value in the specified range
wlanx/x WLAN config>
```

The default setting is 128.

Note

Changing this parameter is not recommended unless you are expressly asked to do so by *Teldat*.

2.7.19 OUTPUT-FAIR

Configures the number of packets that must be in the interface output queue for flow control to act. If the number of packets in the WLAN interface's output queue exceeds the configured value, and the interface that received the packet is running out of receiving buffers, the new packet is returned to the input interface without being queued for transmission. In this way, the input interface can still receive packets destined for interfaces that are not so congested in transmission.

Syntax:

```
wlanx/x WLAN config>output-fair ?
  <0..256>    Value in the specified range
wlanx/x WLAN config>
```

The default setting is 40.

Command history:

Release	Modification
11.00.03	This command is now common to all interfaces, and explained in the following manual: *Teldat Dm772-I Common Configuration for Interfaces.*

2.7.20 POWER

Sets power parameters.

Syntax:

```
wlan3/0 WLAN config>power ?
  transmit    Set transmit power
```

POWER TRANSMIT

Sets the transmit power.

Syntax:

```
wlan3/0 WLAN config>power transmit ?
  value      power value in dBm
  full       maximum (normal) power
  half       fractional (1/2) power
  quarter    fractional (1/4) power
  eighth     fractional (1/8) power
  minimum    minimum power
```

value:	Gives the transmit power value in dBm.
full:	Transmits at full power.
half:	Applies a 3 dB attenuation to the transmit power.
quarter:	Applies a 6 dB attenuation to the transmit power
eighth:	Applies a 9 dB attenuation to the transmit power.
minimum:	Transmits at minimum power.

Maximum (full) transmit power is enabled by default.

Example:

This example sets the transmit power on the device to half the normal power (3 dB attenuation).

```
wlan3/0 WLAN config>power transmit half
```

2.7.21 PROMISCUOUS-MODE

Enables **promiscuous-mode.** When in this mode, the WLAN interface accepts all packets/frames transmitted on the media. However, when promiscuous mode is disabled, the interface only accepts packets/frames addressed to it.

> **Note**
>
> *This command is not available on devices with Atheros WLAN drivers because said driver does not support this function.*

Syntax:

```
wlanx/x WLAN config>promiscuous-mode
```

Promiscuous mode is disabled by default.

Example:

```
wlan0/0 WLAN config>promiscuous-mode
```

Command history:

Release	Modification
11.00.07	This command was introduced.
11.01.02	This command was introduced.

2.7.22 RADIO-SHUTDOWN

Disables the radio interface. If the radio interface is shut down, then all WLAN networks using that radio interface are shut down.

Syntax:

```
wlanx/x WLAN config>radio-shutdown
```

The radio interface is enabled by default.

Example:

This example disables the radio interface:

```
wlan3/0 WLAN config>radio-shutdown
```

Command history:

Release	Modification
11.01.00	This command was introduced.

2.7.23 REGULATORY

Configures parameters related to regulatory entities.

Syntax:

```
wlanx/x WLAN config>regulatory bands allow ?
  default    Default based in device certifications for country selected
  unii-1     U-NII-1 (Band 1)
  unii-2     U-NII-2 (Band 2)
  unii-2e    U-NII-2e (Band 3)
  unii-3     U-NII-3 (Band 4)
```

REGULATORY BANDS ALLOW

Configures the allowed sub-bands in the 5 GHz band. If automatic channel selection is configured, only the channels in the allowed bands will be available. By default, the bands in which certification has been obtained are allowed. These bands depend on the country configured on the router. You can use the **no regulatory bands allow default** command to remove the default setting and then configure the bands you want. Changing the default setting is not recommended because it can lead to conditions that are not allowed by the regulators of the country in which you are operating.

Note

You can obtain a list of the allowed bands using the **list** command.

Syntax:

```
wlanx/x WLAN config>regulatory bands allow ?
  default    Default based in device certifications for country selected
  unii-1     U-NII-1 (Band 1)
  unii-2     U-NII-2 (Band 2)
  unii-2e    U-NII-2e (Band 3)
  unii-3     U-NII-3 (Band 4)
```

The four selectable bands are:

- Band 1: UNII-1. 5.15 to 5.25 GHz band (channels 34-48)
- Band 2: UNII-2. 5.25 to 5.35 GHz band (channels 52-64)
- Band 3: UNII-2e .5.47 to 5.725 GHz band (channels 100-140)
- Band 4: UNII-3. 5.725 to 5.825 GHz band (channels 149-165)

By default, the router transmits in the certified bands.

Example:

The following example configures the device to transmit in the United States in the UNII-1 and UNII-2 bands.

```
wlan0/0 WLAN config>country US
wlan0/0 WLAN config>list
…
Wireless LAN Mode: 802.11a/n
Channel bandwith: 20 MHz
                  Allowed bands: UNII-1 UNII-3              …
wlan0/0 WLAN config>no regulatory bands allow default

wlan0/0 WLAN config>list
…
Wireless LAN Mode: 802.11a/n
Channel bandwith: 20 MHz
                  Allowed bands: UNII-1 UNII-2 UNII-2e UNII-3
               …
wlan0/0 WLAN config>no regulatory bands allow unii-2e

wlan0/0 WLAN config>no regulatory bands allow unii-3

wlan0/0 WLAN config>list
…
Wireless LAN Mode: 802.11a/n
Channel bandwith: 20 MHz
                  Allowed bands: UNII-1 UNII-2
…
wlan0/0 WLAN config>
```

2.7.24 RESET-ON-ERROR

Configures the behavior of the device against software problems. If enabled, the router reboots after detecting a serious software error. If disabled, the router saves a bug if it encounters a serious software error, but it does not reboot.

Syntax:

```
wlanx/x WLAN config>reset-on-error
wlanx/x WLAN config>
```

By default, reset-on-error is disabled.

2.7.25 RETRY-LIMIT

Configures the maximum number of times for resending a frame before transmission is considered unsuccessful.

Syntax:

```
wlanx/x WLAN config>retry-limit [long|short] <1..255>
```

short

Maximum number of attempts to send a frame that is less than or equal to the *rts threshold*. The frame is discarded once the retry limit has been reached.

The default is 7.

long

Maximum number of attempts to send a frame that is greater than the *rts threshold*. The frame is discarded once the retry limit has been reached.

The default is 4.

Example:

The following example configures the device to make three attempts to resend a frame that is longer than the RTS threshold.

```
wlan3/0 WLAN config>retry-limit long 3
```

Command history:

Release	Modification
11.01.00	This command was introduced.
11.01.01	This command is obsolete.

2.7.26 RTS

Sets the RTS/CTS parameters used to access the medium.

Syntax:

```
wlan3/0 WLAN config>rts ?
  threshold    Packet size to send an RTS
```

RTS THRESHOLD

Configures the RTS/CTS threshold frame size. If the frame to be transmitted exceeds the configured threshold, the RTS/CTS mechanism is used to reserve the medium before the frame is sent.

Syntax:

```
wlan3/0 WLAN config>rts threshold ?
  <1..2346>    Value in the specified range
wlan3/0 WLAN config>
```

By default, the RTS/CTS threshold is set to 2312 bytes.

Example:

The following example configures the use of RTS/CTS to reserve the medium for packets longer than 1500 bytes.

```
wlan3/0 WLAN config>rts threshold 1500
```

2.7.27 SCAN

Configures different scanning parameters when the WLAN is in client mode.

Syntax:

```
wlanx/0 config>scan ?
  band     bands to use when scanning for APs
  background    Configures background scanning
  blacklist     Enables blacklisting
```

```
wlanx/0 config>
```

Command history:

Release	Modification
11.00.04	Command moved from bss menu to root menu.

2.7.27.1 SCAN BAND

Configures the bands to to be scanned during a network search procedure. You can choose to search networks in the 2.4 GHz band, the 5 GHz band, or both.

Syntax:

```
wlan0/0 config>scan band ?
  2.4GHz    scans the 2.4 GHz band (11b/g/n)
  5GHz      scans the 5 GHz band (11a/n)
  both      scans both the 2.4 GHz and the 5 GHz band
```

By default, both the 2.4 GHz and 5 GHz frequency bands are searched.

Example:

The following example configures the client to only search for networks in the 5 GHz band.

```
wlan3/0 bss config>scan ban 5GHz
```

2.7.27.2 SCAN BACKGROUND

Configures scan parameters used to search for new networks once connected to a network.

Once the client station has connected to an access point, it continues to search periodically for new networks with which to connect. It does this to see if it can find an access point with better signal characteristics. This process is known as *background scanning.*

Syntax:

```
wlanx/0 config>scan background ?
  <cr>     Enables background scanning
  short    short background scan interval
  long     long background scan interval
```

2.7.27.2.1 SCAN BACKGROUND <cr>

This allows the client station to search for new networks once connected to an access point. Use the **no scan background** command to disable searching for new networks.

By default, new networks are searched for once connected.

Example:

The following example disables searching for new networks when the client station is connected to an access point.

```
wlan3/0 config>no scan background
```

2.7.27.2.2 SCAN BACKGROUND SHORT

Configures a *short* time interval between searches for new networks. A client station periodically searches for new networks when it connects to an access point. This parameter is used to define the time interval between searches. The *short* interval changes to a *long* interval after a period of time with no access point changes.

Syntax:

```
wlanx/0 config>scan background short ?
  <1..10000>    Value in the specified range
```

The default setting is 30 seconds.

Example:

The following example configures a 45-second interval between searches.

```
wlan3/0 config>scan background short 45
```

2.7.27.2.3 SCAN BACKGROUND LONG

Configures a *long* time interval between searches for new networks.

Syntax:

```
wlanx/0 config>scan background long ?
  <1..10000>    Value in the specified range
```

The default setting is 300 seconds.

Example:

The following example configures a 600-second interval between searches.

```
wlan3/0 config>scan background short 600
```

2.7.27.3 SCAN BLACKLIST

Enables the access point blacklist: if a client station connects to an access point and then disconnects for some reason, the access point is included on a blacklist. The client station ignores any access points included on the blacklist and will not attempt to connect to them. Only in the absence of other access point candidates to connect to, is the blacklist cleared and all detected access points again considered.

Use the **no scan blacklist** command to disable the blacklist. That is, the client station considers connecting to all access points selected, regardless of whether they have previously been connected and then disconnected.

By default, the blacklist is enabled.

Example:

The following example disables the access point black list.

```
wlan3/0 bss config>no scan blacklist
```

2.7.28 SHORT-GUARD-INTERVAL

Enables the **short-guard-interval.** This is the time between the transmission of two symbols. When this is enabled, said interval is reduced from 800 ns to 400 ns. This allows for better speed but can cause more interference between symbols.

Syntax:

```
wlanx/x WLAN config>short-guard-interval
```

By default, the short guard interval is disabled.

Example:

The following example enables the short guard interval:

```
wlan3/0 WLAN config>short-guard-interval
```

Command history:

Release	Modification
11.01.00	This command was introduced.

2.7.29 SHORT-PREAMBLE

Enables **short-preamble** for 802.11b/g client stations. Preamble is part of the Physical Layer Convergence Protocol (PLCP) layer. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the access point using short preamble.

Syntax:

```
wlanx/x WLAN config>short-preamble
```

By default, short-preamble is disabled.

Example:

This example enables short preamble.

```
wlan3/0 WLAN config>short-preamble
```

Command history:

Release	Modification
11.01.00	This command was introduced.

2.7.30 SSID-CHANGE

Changes a BSS network identifier (SSID) without having to delete the entire BSS configuration.

Syntax:

```
wlanx/x WLAN config>ssid-change ?
  old              old SSID
        <1..32 chars>    old SSID
               <1..32 chars>    new SSID
  <1..32 chars>    new SSID
wlanx/x WLAN config>
```

There are two variants of the command: you can directly indicate the new SSID or you can use the *old* option to enter the old SSID name followed by the new name that you want.

Example:

A *TeldaWLAN* SSID is configured, when you want to configure *TeldatWLAN*. To change it, you can use the **ssid-change** command.

```
wlan2/0 WLAN config>ssid-change old TeldaWLAN TeldatWLAN
```

2.7.31 SWITCH-CHANNEL-ON-STUCK

Configures the device's behavior in case of transmission blockages. In cases of high radio-frequency noise, the WLAN chip may have problems transmitting packets. This command lets you configure a mechanism that forces a channel change if several consecutive transmission errors are detected.

Syntax:

```
wlanx/x WLAN config>switch-channel-on-stuck ?
  enable      Enables channel switching on beacon stuck
  disable     Disables channel switching on beacon stuck
  interval    Time window used for beacon stuck errors
         <1s..86400s>    Time window used for beacon stuck errors
  n_errors    Number of beacon stuck errors needed to trigger channel
              switching
         <2..200>         Number of beacon stuck errors needed to trigger channel
                          switching
```

enable:	Enables the channel switch mechanism when transmission is stuck.
disable:	Disables the channel switch mechanism when transmission is stuck.
interval:	Time interval where transmission errors are considered consecutive.
n_errors:	Number of consecutive errors needed to trigger a change of channel.

By default, the channel switch mechanism is enabled. The device changes channels when the transmission becomes stuck three times within a 120-second time period.

Example:

The following example configures the device to change channels when the transmission becomes stuck five times within a 300-second time period.

```
wlan2/0 WLAN config>switch-channel-on-stuck n_errors 5
wlan2/0 WLAN config>switch-channel-on-stuck interval 300
wlan2/0 WLAN config>
```

2.7.32 WMM

Accesses the wireless Quality of Service (QoS) configuration menu.

Syntax:

```
wlan3/0 WLAN config>wmm
```

Note

Please refer to the section on *WMM configuration menu commands* on page 57 for information on configuring QoS parameters.

2.7.33 WPS

Configures Wi-Fi Protected Setup (WPS) parameters.

Syntax:

```
wlanx/x WLAN config>wps ?
  ap-pin          Configures WPS pin for the AP
  device-name     Device name
  device-type     Device type
  enable          Enables WPS
  manufacturer    Manufacturer
  model-name      Model name
  model-number    Model number
  os-version      Operating System version
  update-config   Update flash configuration
  uuid            UUID
```

WPS AP-PIN

Sets the access point's WPS Personal Identification Number (PIN). This command is only available when the interface is operating in access point mode.

Syntax:

```
wlanx/x WLAN config> wps ap-pin ?
  no-crc      PIN value without CRC digit (7 digits)
        <0..9999999>    PIN value without CRC digit (7 digits)
  complete    PIN value (8 digits, including CRC)
        <0..99999999>    PIN value (8 digits, including CRC)
```

The PIN can be entered in full (8 digits, where the last digit is a CRC of the first 7 digits), or without CRC (7 digits).

By default, no PIN is configured.

Example:

This example configures a PIN with CRC digit.

```
wlan3/0 WLAN config>wps ap-pin complete 12345670
```

WPS DEVICE-NAME

Sets the device name used in WPS messages..

Syntax:

```
wlanx/x WLAN config>wps device-name ?
  <1..32 chars>    Device name
```

By default, the device name is the name assigned by *Teldat* .

Example:

This example sets the device name.

```
wlan3/0 WLAN config>wps device-name MyTeldatK_2
```

WPS DEVICE-TYPE

Sets the device type used in WPS messages.. The format is as follows:

<category>-<OUI>-<subcategory>

Where:

- Category: category to which the device belongs.
- OUI: 4 hexadecimal octets corresponding to the Organizationally Unique Identifier (OUI). For WPS, the value used is 0050F204.
- Subcategory: device subcategory.

The values assigned to the category and subcategory values can be found in the Wi-Fi Alliance's WPS documentation.

Syntax:

```
wlanx/x WLAN config>wps device-type ?
  <1..32 chars>    Device type
```

The default setting is 0006-0050f204-0002, which corresponds to category 6 (Network infrastructure), subcategory 2 (Router).

Example:

This example configures the device type as access point.

```
wlan3/0 WLAN config>wps device-type 0006-0050f204-0001
```

WPS ENABLE

Enables WPS. This command is only available if the interface is configured as an access point.

Syntax:

```
wlanx/x WLAN config>wps enable
```

By default, **WPS** is enabled.

WPS MANUFACTURER

Sets the manufacturer used in WPS messages.

Syntax:

```
wlanx/x WLAN config>wps manufacturer ?
  <1..64 chars>    Manufacturer
```

The default setting is*Teldat*

Example:

This example configures the manufacturer.

```
wlan3/0 WLAN config>wps manufacturer MyFakeManufacturer
```

WPS MODEL-NAME

Sets the model name used in WPS messages.

Syntax:

```
wlanx/x WLAN config>wps model-name ?
  <1..32 chars>    Model name
```

By default, the model name takes the same value as the device-name.

Example:

This example sets the model name.

```
wlan3/0 WLAN config>wps model-name Mymodel
```

WPS MODEL-NUMBER

Sets the model number used in WPS messages.

Syntax:

```
wlanx/x WLAN config>wps model-number ?
  <1..32 chars>    Model number
```

The default setting is v1.00.00.

Example:

This example sets the model number.

```
wlan3/0 WLAN config>wps model-number v2.1
```

WPS OS-VERSION

Sets the WPS operating system (OS) version. This is a string of four hexadecimal octets.

Syntax:

```
wlanx/x WLAN config>wps os-version ?
  <hex 0..7fffffff>    Operating System version
```

By default, the CIT version identifier is used.

Example:

This example sets the OS version.

```
wlan3/0 WLAN config>wps os-version 10090807
```

WPS UPDATE-CONFIG

Enables writing the WPS configuration to flash memory. This command is only available if the interface is configured as a client.

Syntax:

```
wlanx/x WLAN config>wps update-config
```

By default, the WPS configuration is not stored to flash.

Example:

This example writes the WPS configuration to flash.

```
wlan3/0 WLAN config>wps update-config
```

WPS UUID

Sets the device identifier (Universally Unique Identifier or UUID).

Syntax:

```
wlanx/x WLAN config>wps uuid ?
  <36 chars>    UUID
```

The UUID consists of: 8 hexadecimal digits, hyphen, 4 hexadecimal digits, hyphen, 4 hexadecimal digits, hyphen, 12 hexadecimal digits.

By default, the device identifier value is obtained from the WLAN interface MAC.

Example:

Sets the UUID.

```
wlan3/0 WLAN config>wps uuid 12345678-9abc-def0-1234-56789abcdef0
```

2.7.34 EXIT

Exits the WLAN interface configuration menu.

Syntax:

```
wlan3/0 WLAN config>exit
```

2.8 BSS configuration menu commands

This section summarizes the various configuration commands available in the WLAN interface's Basic Service Set (BSS) configuration menu.

To access the BSS configuration menu, type **bss** followed by the network identifier in the WLAN interface configuration menu.

```
wlan3/0 WLAN config>bss "Teldat WLAN"



wlan3/0 bss config>
```

The following table summarizes the BSS configuration commands. These commands are explained in detail in the following sections.

Command	**Function**
? (HELP)	Displays configuration commands or command options.
ACCESS-CONTROL	Allows you to configure MAC access control lists.
AKM-SUITE	Sets the authentication and key management policy used in the BSS.
AUTHENTICATION	Sets the authentication method used in the BSS.
CIPHER	Sets the encryption used in the BSS.
CLIENT-ISOLATION	Sets access point (AP) client station isolation.
DOT1X	Accesses 802.1X configuration.
GROUPKEY-UPDATE	Sets parameters for updating the group key in RSN networks.
KEEP-ALIVE	Sets the keep-alive interval.
KEY	Sets the WEP keys.
KEY DEFAULT	Sets the default WEP key used in the BSS.
LIST	Displays the configuration.
MAX-ASSOCIATIONS	Sets the maximum number of client stations that may simultaneously connect to the BSS.
NO	Restores default parameters.
PRIORITY	Configures network priority.
PRIVACY-INVOKED	Enables security in the BSS.
RSN	Sets the Robust Security Network (RSN) used in the BSS.
SSID-SUPPRESS	Suppresses broadcasting the SSID in beacon frames.
WEP-KEYSOURCE	Sets the WEP type used in the BSS.
WPA-PSK	Sets the WPA key used.
EXIT	Exits the WLAN interface configuration menu.

2.8.1 ? (HELP)

Displays the available commands or command options.

2.8.2 ACCESS-CONTROL

Configures MAC access control lists.

Syntax:

```
wlan3/0 WLAN config>access-control
        allow          Allows association to client stations on the MAC list
        deny           Denies association to client stations on the MAC list
        disable        Disables MAC restricted access
        mac-address <mac>    MAC restricted access
```

disable:	Disables MAC access control.
allow:	Enables MAC access control. Access to the configured MAC addresses is allowed.
deny:	Disables MAC access control. Access to the configured MAC addresses is denied.
mac-address:	Includes a MAC address on the access control list.

Example:

This example configures an access list that allows the following addresses: 00-0F-CB-AF-EE-6A and 00-11-95-BB-20-A4.

```
wlan3/0 WLAN config>access-control allow
wlan3/0 WLAN config>access-control mac-address 00-0f-cb-af-ee-6a
wlan3/0 WLAN config>access-control mac-address 00-0b-6b-34-af-03
```

Note

MAC access control is ignored if the WPS functionality is used.

2.8.3 AKM-SUITE

Configures the authentication and key management policy (AKM) used in the BSS.

Syntax:

```
wlan3/0 bss config>akm-suite ?
  dot1x    802.1X authentication with 4-Way Handshake
  psk      Preshared Key with 4-Way Handshake
wlan3/0 bss config>
```

dot1x: 802.1X authentication is used, with a 4-message negotiation (4-way handshake), defined in the 802.11i standard, to derive the keys.

psk: A preset key (pre-shared key) is used as the master key, using the 802.11i 4-message negotiation (4-way handshake) to derive the keys.

By default, no authentication key management policy is configured. You need to explicitly configure a policy to create a robust security network (RSN).

Example:

This example configures 802.1X authentication.

```
wlan3/0 bss config>akm-suite dot1x
```

2.8.4 AUTHENTICATION

Configures the authentication method used in the BSS.

Syntax:

```
wlan3/0 bss config>authentication ?
  auto           auto
  open-system    open system
  shared-key     shared key
wlan3/0 bss config>
```

auto: Automatically selects the authentication to use: shared-key authentication for WEP-enabled client stations and open authentication for non-WEP-enabled client stations.

open-system: Open-system.

share-key: Shared-key authentication. The access point sends a challenge to the client station which the client station must encrypt with the WEP key to prove it knows said key.

Note

If you enable a robust security policy with the **rsn** command, you will only be able to configure open authentication.

Note

Because of the lack of security in shared-key authentication, *Teldat* recommends using only open system security.

By default, the device is configured to accept **open system** authentication as the authentication method.

Example:

This example configures shared-key authentication.

```
wlan3/0 bss config>authentication shared-key
```

2.8.5 CIPHER

Configures the encryption used in the BSS.

Syntax:

```
wlan3/0 bss config>cipher ?
  aes-ccmp     AES-CCMP
  tkip         TKIP
wlan3/0 bss config>
```

aes-ccmp: AES-CCMP is used to encrypt the data.

tkip: TKIP is used to encrypt the data.

Encryption mechanisms are not mutually exclusive. You can configure more than one encryption mechanism within the same BSS, thus allowing client stations that join the BSS to select the encryption that best adapts to their characteristics.

If several encryption methods are configured, the least secure method is used to encrypt group frames (broadcast and multicast frames). The order of the ciphers, from least to most secure, is as follows:

- TKIP
- AES-CCMP

By default, no encryption is set. You must explicitly configure encryption to create a robust security network (RSN).

Example:

The following example configures AES-CCMP encryption in a BSS.

```
wlan3/0 bss config>cipher aes-ccmp
```

Example:

This example configures AES-CCMP and TKIP encryption in a BSS. TKIP encryption will be used for group frames.

```
wlan3/0 bss config>cipher aes-ccmp
wlan3/0 bss config>cipher tkip
```

2.8.6 CLIENT-ISOLATION

Configures access point client station (AP) isolation. If this parameter is enabled, the client stations cannot communicate directly with each other at the MAC layer.

Syntax:

```
wlanx/x bss config>client-isolation
```

By default, this feature is disabled; the client stations can communicate with one another.

Example:

This example enables access point client station isolation.

```
wlan3/0 bss config>client-isolation
```

2.8.7 DOT1X

Accesses the 802.1X authentication configuration menu. This menu is only accessible if the interface is behaving as a client station in the configured BSS.

802.1X supplicant parameters are configured in the 802.1X menu. For further information on configuring the 802.1X supplicant, please see the following manual: *Teldat* Dm783-I 802.1X Authentication.

Syntax:

```
wlan3/0 WLAN config>dot1x
```

Example:

```
wlan3/0 WLAN config>dot1x

- 802.1X User Config --
wlan3/0 bss dot1X config>
```

2.8.8 GROUPKEY-UPDATE

Sets parameters for updating the group key in RSN networks.

Syntax:

```
wlan3/0 bss config>groupkey-update ?
  time    Configures groupkey update interval in seconds
wlan3/0 bss config>
```

GROUPKEY-UPDATE TIME

Sets a group key refresh interval in RSN networks. The refresh interval is specified in seconds.

Syntax:

```
wlan3/0 bss config>groupkey-update time ?
  <30..4294967295>    Value in the specified range
wlan3/0 bss config>
```

The default setting is 1800 seconds; that is, the group key is updated every 30 minutes.

Example:

This example updates the group key every 10 minutes (600 seconds).

```
wlan3/0 bss config>groupkey-update time 600

```

2.8.9 KEEP-ALIVE

Sets the keep-alive interval. This command is only available when the interface is in client station mode in the configured BSS.

Almost all access points will end a connection with a client station if there is no activity for a certain time. Using this command, you can configure a client station to send null data frames (empty frames) to the access point at regular intervals to prevent it from terminating the connection due to lack of activity.

Syntax:

```
wlan3/0 bss config>keep-alive ?
  <0..3600>    Value in the specified range
wlan3/0 bss config>keep-alive
```

The default setting is 180 seconds; that is, a keep-alive frame is sent every 3 minutes. If you want to turn off the keep-alive function, you need to set a value of 0.

Example:

The following example turns off the keep-alive function.

```
wlan3/0 bss config>keep-alive 0
```

2.8.10 KEY

Sets the shared WEP keys.

Syntax:

```
wlan3/0 WLAN config>key <index> size (40|104) (ascii|hex) (plain|ciphered) <key>
```

index:	Index of the key to configure. The valid values are 1 to 4.
size:	WEP key size. The WEP key can be 40, 104 or 128 bits.

ascii: Select this option to enter an ASCII key. Please note that one ASCII character is 8 bits.

hex: Select this option to enter a hexadecimal key. Please note that one hexadecimal character is 4 bits.

plain: Select this option to enter an unencrypted WEP key.

ciphered Select this option to enter an encrypted WEP key.

key WEP key that you want to configure.

Example 1:

This example configures the 104-bit-long **customwepkey2** key in position 2.

```
wlan3/0 WLAN config>key 2 size 104 ascii plain customwepkey2
```

Example 2:

This examples configures the 40-bit-long 0x1234567890 key in position 4.

```
wlan3/0 WLAN config>key 4 size 40 hex plain 1234567890
```

2.8.11 KEY DEFAULT

Sets the default WEP key used in the BSS. This parameter is only useful for BSSs with WEP security.

Syntax:

```
wlan3/0 bss config>key default <index>
```

where index is a value from 1 to 4.

By default, the key that is used to transmit frames in a WEP network is the key in position 1.

Example:

This example configures the key in position 3 as the default key.

```
wlan3/0 bss config>key default 3
```

2.8.12 LIST

Displays the BSS basic service area configuration. For security reasons, the configured key values are not shown when listing the configuration.

Syntax:

```
wlan3/0 bss config>list
```

2.8.13 MAX_ASSOCIATIONS

Sets the maximum number of client stations that may simultaneously connect to the BSS. If the configured number is reached, no new connections are allowed.

Syntax:

```
wlan3/0 bss config>max-associations ?
  <1..128>     Value in the specified range
wlan3/0 bss config>
```

The default setting is 64 client stations.

Example:

This example sets the maximum number of client stations that may connect to the BSS to five.

```
wlan3/0 bss config>max-associations 5
```

2.8.14 NO

Restores default parameters or clears configuration.

Syntax:

```
wlan3/0 bss config>no ?
  akm-suite            Configures Authentication Key Management suite
  authentication       Configures authentication type
  cipher               Configures cipher type
  client-isolation     Configures client station clients isolation
  groupkey-update      Configures groupkey update interval
  keep-alive           Configures time between keep alive frames
  key                  Configures encryption key
  max-associations     Configures maximum associations for ssid
  opmode               Configures operational mode
  privacy-invoked      Enables security
  rsn                  Configures RSN Information Element To Send
  ssid-suppress        Suppress SSID in Beacon Frames
  wep-keysource        Configures WEP encryption keys source
  wpa-psk              Configures WPA-PSK
```

Example:

The following example disables security in the BSS.

```
wlan3/0 bss config>no privacy-invoked
```

2.8.15 PRIORITY

Configures network priority settings. This parameter is used in client mode when there are multiple networks. By default, all networks are given the same priority group (0). If some of the networks are more desirable, this field can be used to change the order in which a client goes through the networks when selecting a BSS. The priority groups are iterated in decreasing priority (i.e., the larger the priority value, the sooner the network is matched against the scan results).Within each priority group, networks are selected based on security policy, signal strength, etc.

Syntax:

```
wlan3/0 bss config>priority ?
  <0..255>    Value in the specified range
wlan3/0 bss config>
```

By default, networks are given priority 0 (lowest).

Example:

This example configures a network with a priority of 10 so that it is selected before other networks.

```
wlan3/0 bss config>priority 10
```

Command history:

Release	Modification
11.00.04	Command moved from bss menu to root menu.

2.8.16 PRIVACY-INVOKED

Enables security in the BSS.

Syntax:

```
wlan3/0 bss config>privacy-invoked
```

If you do not enable a robust security policy with the **rsn** command, WEP will be used.

By default, security in the BSS is disabled.

Example:

The following example enables security in a BSS.

```
wlan3/0 bss config>privacy-invoked
```

2.8.17 RSN

Configures the robust security network (RSN) used in the BSS.

Syntax:

```
wlan3/0 bss config>rsn ?
  wpa     WPA Information Element
  wpa2    WPA2 (802.11i) Information Element
wlan3/0 bss config>
```

wpa: Enables WPA in the BSS.

wpa2: Enables WPA2 in the BSS.

These two options are not mutually exclusive. If WPA and WPA2 are enabled, the access point will include both security policy information elements in the beacon frames. In this way, client stations that join the BSS can select the security policy that best adapts to their characteristics.

If the interface is in WLAN client mode, it can associate with access points that advertise WPA, WPA2, or both.

By default, no robust security policy is configured.

Example:

The following example configures the BSS to support WPA and WPA2.

```
wlan3/0 bss config>rsn wpa
wlan3/0 bss config>rsn wpa2
```

Note

If you configure an authentication other than open authentication, you will not be able to configure an RSN network.

2.8.18 SSID-SUPPRESS

Turns off SSID broadcasting. Normally, the access point broadcasts its network identifier (SSID) in beacon frames. This command allows you to hide this information.

Syntax:

```
wlan3/0 bss config>ssid-suppress
```

By default, the network ID is sent in beacon frames.

Example:

The following example configures the access point to stop broadcasting its network identifier in beacon frames.

```
wlan3/0 bss config>ssid-suppress
```

2.8.19 WEP-KEYSOURCE

Sets the type of WEP encryption used in the BSS.

Syntax:

```
wlan3/0 bss config>wep-keysource ?
  static     Configures WEP encryption with static keys
  dynamic    Configures WEP encryption with dynamic keys
  mixed      Configures WEP encryption with static and dynamic keys
wlan3/0 bss config>
```

static: Static WEP. The keys used are the ones configured on the WLAN interface with the **key**command.

dynamic: Dynamic WEP. The WEP keys used are obtained from an authentication server using 802.1X authentication.

mixed: Mixed WEP. The WEP keys used are obtained through 802.1X authentication. The multicast key is statically configured using the **key** command.

The default setting is static WEP.

Example:

The following example configures dynamic WEP in the BSS.

```
wlan3/0 bss config>wep-keysource dynamic
```

2.8.20 WPA-PSK

Configures the key used for WPA security. This command is only effective if you use a shared-key-based authentication and key management policy, using the **akm-suite psk** command.

Syntax:

```
wpa-psk (passphrase|key) (plain|ciphered) <key-value>
```

passphrase:	Sets the shared-key using an ASCII character passphrase of between 8 and 63 characters. Using a standard procedure, the shared-key is obtained from the configured phrase.
key:	Sets the shared-key to use. The key value must be a 64 hexadecimal character string.
ciphered:	Choose this option to enter the encrypted WPA-PSK key.
key-value:	Shared-key to configure.

By default, no shared-key is configured.

Example:

The following example sets a shared-key passphrase of "*Teldat* Wireless LAN".

```
wlan3/0 bss config>wpa-psk passphrase plain "Teldat Wireless LAN"
```

Example:

The following example sets a shared key directly. The key to use is 0x1234567890, repeated in sequence to complete the 64 hexadecimal characters.

```
wlan3/0 bss config>wpa-psk key plain 1234567890123456789012345678901
234567890123456789012345678901234
```

2.8.21 EXIT

Exits the BSS configuration menu.

Syntax:

```
wlan3/0 bss config>exit
```

2.9 WMM configuration menu commands

This section summarizes the various configuration commands available in the WLAN interface WMM configuration menu.

You access the WMM configuration menu by running the **wmm** command in the WLAN interface configuration menu.

```
wlan3/0 WLAN config>wmm

wlan3/0 WMM config>
```

The following table summarizes the WMM configuration commands. These commands are explained in detail in the following sections.

Command	Function
? (HELP)	Displays configuration commands or command options.
BACKGROUND	Configures background class parameters.
BEST-EFFORT	Configures best-effort class parameters.
NO	Restores parameters to their default values.
QOS	Enables/disables quality of service.
VIDEO	Configures video class parameters.
VOICE	Configures voice class parameters.
EXIT	Exits the WMM setup menu.

2.9.1 ? HELP

Displays the available commands or command options.

2.9.2 BACKGROUND

Configures background access category (AC) parameters.

Syntax:

```
wlan3/0 WMM config>background
       ap     Configure access point
           aifs         Set value for AIFS in slot times units
           ecwmax       Set value for CWmax exponent
           ecwmin       Set value for CWmin exponent
           txoplimit    Set value for TXOPlimit in 32 microsec time slices
       sta    Configure client stations
           aifs         Set value for AIFS in slot times units
           ecwmax       Set value for CWmax exponent
           ecwmin       Set value for CWmin exponent
           txoplimit    Set value for TXOPlimit in 32 microsec time slices
```

ap: Configures the parameters the access point uses to transmit background traffic.

sta: Configures the parameters that client stations use to transmit background traffic. These parameters are sent to the client stations in beacon frames.

aifs: Configures the AIFS in slot-time units.

ecwmin: Sets the value for the CWmin exponent. The final value used is: **2^{ECWmin} -1.**

ecwmax: Sets the value for the CWmax exponent. The final value used is: **2^{ECWmin} -1.**

txoplimit: Configures TXOPlimit in units of 32µs, i.e., the time available for transmission is **txoplimit*32µs**. If this value is set to 0, then only a single transmission is allowed.

2.9.3 BEST-EFFORT

Configures best-effort access category (AC) parameters.

Syntax:

```
wlan3/0 WMM config>best-effort
       ap     Configure access point
           aifs         Set value for AIFS in slot times units
           ecwmax       Set value for CWmax exponent
           ecwmin       Set value for CWmin exponent
           txoplimit    Set value for TXOPlimit in 32 microsec time slices
       sta    Configure client stations
           aifs         Set value for AIFS in slot times units
           ecwmax       Set value for CWmax exponent
           ecwmin       Set value for CWmin exponent
           txoplimit    Set value for TXOPlimit in 32 microsec time slices
```

ap: Configures the parameters the access point uses to transmit best-effort traffic.

sta: Configures the parameters that client stations use to transmit best-effort traffic. These parameters are sent to the client stations in beacon frames.

aifs: Configures the AIFS in slot-time units.

ecwmin: Sets the value for the CWmin exponent. The final value used is: **2^{ECWmin} -1.**

ecwmax: Sets the value for the CWmax exponent. The final value used is: **2^{ECWmax} -1**.

txoplimit: Configures the TXOPlimit in units of 32µs, i.e., the time available for transmission is **txoplimit*32µs**. If this value is set to 0, then only a single transmission is allowed.

2.9.4 NO

Restores parameters to their default values or clears configuration.

Syntax:

```
wlan3/0 WMM config>no ?
  background     Configure background access category
  best-effort    Configure best-effort access category
  qos            Enable, Disable QoS
  video          Configure video access category
  voice          Configure voice access category
```

Example:

The following example restores the AIFS value used by the access point for background traffic to its default value.

```
wlan3/0 WMM config>no background ap aifs
```

2.9.5 QoS

Enables or disables quality of service (QoS). By default, QoS is enabled.

Syntax:

```
wlan3/0 WMM config>qos ?
  enable     Enable QoS
  disable    Disable QoS
```

Example:

Disabling QoS.

```
wlan3/0 WMM config>qos disable
```

> **Note**
>
> By default, quality of service is enabled. To disable it, run the **qos disable** command.

2.9.6 VIDEO

Configures video access category (AC) parameters.

Syntax:

```
wlan3/0 WMM config>video
       ap     Configure access point
           aifs         Set value for AIFS in slot times units
           ecwmax       Set value for CWmax exponent
           ecwmin       Set value for CWmin exponent
           txoplimit    Set value for TXOPlimit in 32 microsec time slices
       sta    Configure client stations
           aifs         Set value for AIFS in slot times units
           ecwmax       Set value for CWmax exponent
           ecwmin       Set value for CWmin exponent
           txoplimit    Set value for TXOPlimit in 32 microsec time slices
```

ap: Configures the parameters the access point uses to transmit video traffic.

sta: Configures the parameters that client stations must use to transmit video traffic. These parameters are sent to the client stations in beacon frames.

aifs: Configures the AIFS in slot-time units.

ecwmin: Sets the value for the CWmin exponent. The final value used is: **2^{ECWmin} -1.**

ecwmax: Sets the value for the CWmax exponent. The final value used is: **2^{ECWmax} -1**.

txoplimit: Configures TXOPlimit in units of 32µs, i.e., the time available for transmission is **txoplimit*32µs**. If this value is set to 0, then only a single transmission is allowed.

2.9.7 VOICE

Configures voice traffic parameters.

Syntax:

```
wlan3/0 WMM config>voice
       ap     Configure access point
```

```
           aifs         Set value for AIFS in slot times units
           ecwmax       Set value for CWmax exponent
           ecwmin       Set value for CWmin exponent
           txoplimit    Set value for TXOPlimit in 32 microsec time slices
       sta    Configure client stations
           aifs         Set value for AIFS in slot times units
           ecwmax       Set value for CWmax exponent
           ecwmin       Set value for CWmin exponent
           txoplimit    Set value for TXOPlimit in 32 microsec time slices
```

ap: Configures the parameters the access point uses to transmit voice traffic.

sta: Configures the parameters that client stations must use to transmit voice traffic. These parameters are sent to the client stations in beacon frames.

aifs: Configures the AIFS in slot-time units.

ecwmin: Configures the value for the CWmin exponent. The final value used is: **2^{ECWmin} -1.**

ecwmax: Configures the value for the CWmax exponent. The final value used is: **2^{ECWmax} -1**.

txoplimit: Configures TXOPlimit in units of 32µs, i.e., the time available for transmission is **txoplimit*32µs**. If this value is set to 0, then only a single transmission is allowed.

2.9.8 EXIT

Exits the WMM configuration menu.

Syntax:

```
wlan3/0 WMM config>exit
wlan3/0 WLAN config>
```

Chapter 3 Monitoring Wireless Interfaces

3.1 Accessing WLAN monitoring

To access WLAN interface monitoring, follow the steps below:

(1) Type **configuration** in the monitoring menu to obtain a list of available interfaces.

(2) Type the **network** command followed by the identifier of the WLAN interface you want to configure.

Example:

```
*monitor
Console Operator

+configuration
P.C.B.=89  Mask=0c10  Microcode=134f0  CLK=262144 KHz  BUSCLK=65536 KHz PCICLK=6
5536 KHz
ID: AT150-16F128R L7.38
5 interfaces:
Connector     Interface          MAC/Data-Link        Status
GE0/FE0/LAN1  ethernet0/0        Ethernet/IEEE 802.3  Up
GE1/FE1/LAN2  ethernet0/1        Ethernet/IEEE 802.3  Testing
SERIAL0/WAN1  serial0/0          HDLC                 Down
---           x25-node           internal             Up
SLOT3         wlan3/0            WLAN                 Up

Encryption Engines:
    Hardware: SEC-8272 Revision: 0xA
+network wlan3/0

--  WLAN Console  --
wlan3/0 WLAN+
```

3.2 Monitoring menu commands

This section summarizes the different monitoring commands available in the WLAN interface monitoring menu.

The following table summarizes the WLAN interface monitoring commands. These commands are explained in detail in the following sections.

Command	**Function**
? (HELP)	Displays monitoring commands or command options.
ACL SHOW	Displays information about access control lists.
BDESCS	Displays information about the buffer descriptors used.
BITRATE	Measures the actual WLAN transmission/reception rate.
BEACON	Displays information about beacon frames.
BSS SHOW	Displays information about the BSS.
CHANNEL SHOW	Displays the available channels for the configured country and mode.
CLEAR INTERNAL-STATS	Clears statistics.
COUNTRY SHOW	Displays the configurable country codes.
DEAUTHENTICATE	De-authenticates a client station.
DOT1X SHOW	Displays information about 802.1X authentication.
DUMP	Displays various information about the WLAN interface.
IWCONFIG	Configures WLAN interface parameters.
IWLIST	Displays WLAN interface parameters.
IWPRIV	Sends a private command to the WLAN interface.
QUEUE SHOW	Displays information about the transmission queues.
RADAR SHOW	Displays radio signal detection information.
RADIO	Provides access to radio interface statistics.
SCAN SHOW	Displays information about the detected networks.

client station SHOW	Displays information about client stations connected to a wireless network.
WPS	Provides access to Wi-Fi Protected Setup (WPS) parameters and commands.
EXIT	Exits the WLAN interface monitoring menu.

3.2.1 ? (HELP)

Displays the available commands or command options.

3.2.2 ACL SHOW

Displays information about access control lists.

Example:

```
wlan2/0 WLAN+acl show
MAC Access Control Mode: client stations on list allowed
MAC Address List (2 entries):
[  0] 00-0f-cb-af-ee-6a
[  1] 00-11-95-bb-20-a4
```

Example:

```
wlan0/0 WLAN+acl show
MAC Access Control Mode: client stations on list allowed
MAC Address List:
00-19-d2-5d-3b-34
00-19-d2-5d-4b-c8
```

The output of this command displays the MAC access control status and the allowed MAC address list.

3.2.3 BEACON

Displays information about beacon frames.

Syntax:

```
wlanx/x WLAN+beacon ?
  cancel-storing    Stops storing beacon frame information
  show              Displays beacon frame information
  start-storing     Starts storing beacon frame information
```

To be able to display information about transmitted beacon frames, you first need to tell the driver to store beacon frames in an auxiliary buffer. You do this using the **beacon start-storing** command. You can use the **beacon show** command to view the last transmitted frame. To stop storing beacon frames, use the **beacon cancel-storing** command.

Note

We recommend running the **beacon cancel-storing** command once you've consulted the beacon frame to avoid unnecessary additional processing.

Example:

```
wlan2/0 WLAN+beacon start-storing
wlan2/0 WLAN+beacon show
Data_length: 183
Raw data:
80 00 00 00 ff ff ff ff ff ff 00 80 48 77 eb c7 00 80 48 77 eb c7 70 77 00 00 00 00
00 00 00 00 64 00 21 04 00 09 70 61 62 6c 6f
 57 4c 41 4e 01 08 82 84 8b 96 0c 12 18 24 03 01 06 05 04 00 01 00 00 2a 01 00 32 04
30 48 60 6c 2d 1a 8c 01 1b ff ff 00 00 00 0
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3d 16 06 00 01 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4a
0e 14 00 0a 00 2c 01 c8 00 14 00 05 00 19 00 7f 01 01 dd 18 00 50 f2 02 01 01 81 00
03 a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f
 00 dd 09 00 03 7f 01 01 00 00 ff 7f
```

```
Decoded frame:
Protocol ver  0  Type        MGT  Subtype       BEACON
To DS         0  From DS       0  More Frag     0
Retry         0  Pwr Mgt       0  More Data     0
Protected     0  Order         0
Duration/ID   0000
Dest Address  ff-ff-ff-ff-ff-ff   Src Address   00-80-48-77-eb-c7
BSS Id        00-80-48-77-eb-c7
Sequence Num  0777  Fragment Num  0
Timestamp     0000000000000000  Beacon Intrv  0064
Capability Information
CF Pollable   0  CF Poll Req   0  ESS           1  IBSS          0
Privacy       0  Allow ShortP  1  Allow ShortS  1
INFO ELEMENT  SSID                               Length  0x09 bytes
Value   70 61 62 6c 6f 57 4c 41 4e
INFO ELEMENT  Supported Rates                    Length  0x08 bytes
Value   82 84 8b 96 0c 12 18 24
INFO ELEMENT  DS Parameter Set                   Length  0x01 bytes
Value   06
INFO ELEMENT  TIM                                Length  0x04 bytes
Value   00 01 00 00
INFO ELEMENT  NONERP element                     Length  0x01 bytes
Value   00
INFO ELEMENT  Ext Supported Rates                Length  0x04 bytes
Value   30 48 60 6c
INFO ELEMENT  HT Capabilities                    Length  0x1a bytes
Value   8c 01 1b ff ff 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00
INFO ELEMENT  HT Operation                       Length  0x16 bytes
Value   06 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00
INFO ELEMENT  Overlapping BSS Scan Parameters    Length  0x0e bytes
Value   14 00 0a 00 2c 01 c8 00 14 00 05 00 19 00
INFO ELEMENT  Extended Capabilities              Length  0x01 bytes
Value   01
INFO ELEMENT  Vendor Private (WME)               Length  0x18 bytes
Value   00 50 f2 02 01 01 81 00 03 a4 00 00 27 a4 00 00
        42 43 5e 00 62 32 2f 00
INFO ELEMENT  Vendor Private (ATH)               Length  0x09 bytes
Value   00 03 7f 01 00 01 00 7f ff
wlan2/0 WLAN+beacon cancel-storing
wlan2/0 WLAN+
```

The output of this command displays the length and content of the last stored beacon frame, interpreting some of the information elements.

3.2.4 BDESCS

Displays information about the buffer descriptors used. This information is for internal use at *Teldat* .

3.2.5 BITRATE

This measures the actual WLAN transmission and reception rate. The rate is measured in 1-second intervals in both the specified units (by default, bits per second) and in packets per second (pps). A new line is created each time a historical maximum is exceeded from the moment the command was run. To stop monitoring the speed, press any key.

Syntax:

```
wlanX/X ETH+bitrate ?
  kbps    output in Kbps
  mbps    output in Mbps
  <cr>
```

Example:

```
wlan0/0 ETH+bitrate
             Interface wlan0/0
```

```
Trx rate (bps/pps)  Rcv rate (bps/pps)
 --------------------------------------
          0/    0        2000/    3
          0/    0        8000/    5
          0/    0        8000/   13
          0/    0        4000/    5
ethernet0/0 ETH+
```

3.2.6 BSS SHOW

Displays information about the BSS.

Syntax:

```
wlan3/0 WLAN+bss show
```

Example:

```
wlan3/0 WLAN+bss show
wlan2/0   IEEE 802.11ng  ESSID:"TeldatWLAN"
          Mode:Master  Frequency:2462 MHz (Channel 11)  Access Point: 00-80-48-77-EB-C7
          Bit Rate:130.0 Mb/s   Tx-Power:21 dBm
          RTS thr=2312 B   Fragment thr:off
          Power Management:off
          Link Quality=94/94  Signal level=-96 dBm  Noise level=-95 dBm
          Rx invalid nwid:277  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

          Operational Mode: Client station
```

It shows:

- Operating mode.
- ESSID: configured wireless network ID.
- Mode: network type.
- Frequency: wireless network operating channel.
- Access Point: access point MAC address.
- Bit Rate: maximum speed achievable.
- Tx-Power: transmission power.
- RTS thr: RTS/CTS mechanism operating threshold.
- Fragment thr: frame fragmentation threshold.
- Power Management: power management.
- Link Quality: signal quality.
- Signal Level: signal level received.
- Noise level: noise level.
- Different transmission and reception statistics.
- Operational mode: access point or client (client station) operation.

Example:

```
wlan0/0 WLAN+bss show
wlan0/0   ESSID: "TeldatWLAN"
          Mode:Master  Frequency:2412 MHz (Channel 1)  Access Point: 00-26-82-f0-42-59
          RSSI: 0 dBm   noise: 0 dBm    Capability: ESS ShortSlot
          Supported Rates: [ 1(b) 2(b) 5.5(b) 6 9 11(b) 12 18 24 36 48 54 ]
          802.11n Capable:
                Chanspec: 2.4GHz channel 1 20MHz (0x2b01)
                Control channel: 1
                802.11n Capabilities:
                Supported MCS : [ 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ]
          Tx-Power: 15.50 dBm
```

This shows:

- ESSID: configured wireless network ID.

- Mode: network type.
- Frequency: wireless network operating channel.
- Access Point: MAC address of the access point.
- RSSI: Radio Strength Signal Indication: signal level.
- Noise: noise level.
- Capability: wireless network capabilities.
- Supported Rates: supported network speeds.
- Chanspec: wireless network channel characteristics.
- Control channel: control channel used in case of 40MHz channels.
- 802.11n Capabilities: available 802.11n capabilities.
- Supported MCS: 802.11n supported modulation and coding schemes (MCS).
- Tx-Power: last estimated transmit power.

3.2.7 CHANNEL SHOW

Displays a list of available channels for the configured country and mode. This command is useful if you are unsure about which channels to use.

Syntax:

```
wlanx/x WLAN+channel show ?
  active    Active channels
  all       All channels
  country    Channels for a given country code
```

Example 1:

```
wlan3/0 WLAN+channel show active
Available Channels: Channel number (frequency)
         1 (2412 MHz)  2 (2417 MHz)  3 (2422 MHz)  4 (2427 MHz)
         5 (2432 MHz)  6 (2437 MHz)  7 (2442 MHz)  8 (2447 MHz)
         9 (2452 MHz) 10 (2457 MHz) 11 (2462 MHz)
wlan3/0 WLAN+
```

The output of this command displays a list of allowed channels with their corresponding frequency in parentheses. In the above example, there are 11 configurable channels. The center frequency of channel 6, for example, is 2437 MHz.

Example 2:

```
wlan2/0 WLAN+channel show active
Channel   1 : 2412   Mhz 11ng C CU    Channel  64 : 5320*~ Mhz 11na C CL
Channel   2 : 2417   Mhz 11ng C CU    Channel 100 : 5500*~ Mhz 11na C CU
Channel   3 : 2422   Mhz 11ng C CU    Channel 104 : 5520*~ Mhz 11na C CL
Channel   4 : 2427   Mhz 11ng C CU    Channel 108 : 5540*~ Mhz 11na C CU
Channel   5 : 2432   Mhz 11ng C CU CL Channel 112 : 5560*~ Mhz 11na C CL
Channel   6 : 2437   Mhz 11ng C CU CL Channel 116 : 5580*~ Mhz 11na C CU
Channel   7 : 2442   Mhz 11ng C CU CL Channel 120 : 5600*~ Mhz 11na C CL
Channel   8 : 2447   Mhz 11ng C CL    Channel 124 : 5620*~ Mhz 11na C CU
Channel   9 : 2452   Mhz 11ng C CL    Channel 128 : 5640*~ Mhz 11na C CL
Channel  10 : 2457   Mhz 11ng C CL    Channel 132 : 5660*~ Mhz 11na C CU
Channel  11 : 2462   Mhz 11ng C CL    Channel 136 : 5680*~ Mhz 11na C CL
Channel  36 : 5180   Mhz 11na C CU    Channel 140 : 5700*~ Mhz 11na C
Channel  40 : 5200   Mhz 11na C CL    Channel 149 : 5745   Mhz 11na C CU
Channel  44 : 5220   Mhz 11na C CU    Channel 153 : 5765   Mhz 11na C CL
Channel  48 : 5240   Mhz 11na C CL    Channel 157 : 5785   Mhz 11na C CU
Channel  52 : 5260*~ Mhz 11na C CU    Channel 161 : 5805   Mhz 11na C CL
Channel  56 : 5280*~ Mhz 11na C CL    Channel 165 : 5825   Mhz 11na C
Channel  60 : 5300*~ Mhz 11na C CU
```

For each channel, the center frequency and a series of characteristics according to the following table are displayed:

String	Meaning
FHSS	FHSS channel
11na	5 GHz band, capable of 802.11n
11a	5 GHz band (legacy)

11ng	2.4 GHz band, capable of 802.11n
11g	2.4 GHz band (legacy)
11b	2.4 GHz band, DSSS only (802.11b)
Turbo	Turbo mode enabled
C	802.11n control channel capable
CU	802.11n upper extension channel enable
CL	802.11n lower extension chanel enable
V	802.11ac (VHT-20MHz band) control channel capable
VU	802.11ac (VHT-20MHz band) upper extension channel enabled
VL	802.11ac (VHT-20MHz band) lower extension channel enabled
V80-<CH>	802.11ac (VHT-80MHz band) channel with center frequency CH
V160-<CH>	802.11ac (VHT-160MHz band) channel with center frequency CH
*	Passive channel
~	Channel needs DFS

Command history:

Release	Modification
11.01.02	Added VHT flags.

3.2.7.1 CHANNEL SHOW COUNTRY

The **country** option allows you to display the configurable channels for a given country code.

Syntax:

```
wlan0/0 WLAN+channel show country <2 chars> ?
  default-regulatory-bands    Displays the channels for the default regulatory
                              bands
  <cr>
```

Example:

The following example displays the channels that are available in the United States (US country code).

```
wlan0/0 WLAN+channel show country US
Channel   1 : 2412    Mhz 11ng C CU    Channel  56 : 5280 *~ Mhz 11na C CL
Channel   2 : 2417    Mhz 11ng C CU    Channel  60 : 5300 *~ Mhz 11na C CU
Channel   3 : 2422    Mhz 11ng C CU    Channel  64 : 5320 *~ Mhz 11na C CL
Channel   4 : 2427    Mhz 11ng C CU    Channel 100 : 5500 *~ Mhz 11na C CU
Channel   5 : 2432    Mhz 11ng C CU CL Channel 104 : 5520 *~ Mhz 11na C CL
Channel   6 : 2437    Mhz 11ng C CU CL Channel 108 : 5540 *~ Mhz 11na C CU
Channel   7 : 2442    Mhz 11ng C CU CL Channel 112 : 5560 *~ Mhz 11na C CL
Channel   8 : 2447    Mhz 11ng C CL    Channel 116 : 5580 *~ Mhz 11na C
Channel   9 : 2452    Mhz 11ng C CL    Channel 132 : 5660 *~ Mhz 11na C CU
Channel  10 : 2457    Mhz 11ng C CL    Channel 136 : 5680 *~ Mhz 11na C CL
Channel  11 : 2462    Mhz 11ng C CL    Channel 140 : 5700 *~ Mhz 11na C
Channel  36 : 5180    Mhz 11na C CU    Channel 149 : 5745    Mhz 11na C CU
Channel  40 : 5200    Mhz 11na C CL    Channel 153 : 5765    Mhz 11na C CL
Channel  44 : 5220    Mhz 11na C CU    Channel 157 : 5785    Mhz 11na C CU
Channel  48 : 5240    Mhz 11na C CL    Channel 161 : 5805    Mhz 11na C CL
Channel  52 : 5260 *~ Mhz 11na C CU    Channel 165 : 5825    Mhz 11na C
wlan0/0 WLAN+
```

3.2.7.1.1 default-regulatory-bands

Performs filtering in the 5 GHz band, only showing the bands in which certification has been obtained for the indicated country.

Example:

```
wlan0/0 WLAN+channel show country US default-regulatory-bands
Channel   1 : 2412    Mhz 11ng C CU    Channel  11 : 2462    Mhz 11ng C CL
Channel   2 : 2417    Mhz 11ng C CU    Channel  36 : 5180    Mhz 11na C CU
Channel   3 : 2422    Mhz 11ng C CU    Channel  40 : 5200    Mhz 11na C CL
Channel   4 : 2427    Mhz 11ng C CU    Channel  44 : 5220    Mhz 11na C CU
Channel   5 : 2432    Mhz 11ng C CU CL Channel  48 : 5240    Mhz 11na C CL
Channel   6 : 2437    Mhz 11ng C CU CL Channel 149 : 5745    Mhz 11na C CU
Channel   7 : 2442    Mhz 11ng C CU CL Channel 153 : 5765    Mhz 11na C CL
Channel   8 : 2447    Mhz 11ng C CL    Channel 157 : 5785    Mhz 11na C CU
Channel   9 : 2452    Mhz 11ng C CL    Channel 161 : 5805    Mhz 11na C CL
Channel  10 : 2457    Mhz 11ng C CL    Channel 165 : 5825    Mhz 11na C
wlan0/0 WLAN+
```

3.2.8 CLEAR INTERNAL-STATS

Clears internal statistics related to the WLAN interface.

3.2.9 COUNTRY SHOW

Displays the configurable country codes.

Example:

```
wlan3/0 WLAN+country show
ALL - NO COUNTRY SET (ALL CHANNELS)
AF - AFGHANISTAN
XB - AFRICA
AL - ALBANIA
DZ - ALGERIA
AS - AMERICAN SAMOA
AD - ANDORRA
AO - ANGOLA
AI - ANGUILLA
AQ - ANTARCTICA
AG - ANTIGUA AND BARBUDA
AR - ARGENTINA
AM - ARMENIA
AW - ARUBA
AC - ASCENSION ISLAND
AU - AUSTRALIA
AT - AUSTRIA
AZ - AZERBAIJAN
BS - BAHAMAS
BH - BAHRAIN
BD - BANGLADESH
more? y
BB - BARBADOS
BY - BELARUS
BE - BELGIUM
BZ - BELIZE
BJ - BENIN
BM - BERMUDA
BT - BHUTAN
BO - BOLIVIA
BA - BOSNIA AND HERZEGOVINA
BW - BOTSWANA
BV - BOUVET ISLAND
BR - BRAZIL
IO - BRITISH INDIAN OCEAN TERRITORY
BN - BRUNEI DARUSSALAM
BG - BULGARIA
BF - BURKINA FASO
BI - BURUNDI
KH - CAMBODIA
CM - CAMEROON
CA - CANADA
CV - CAPE VERDE
more? n
wlan3/0 WLAN+
```

3.2.9.1 COUNTRY SHOW REG-DOMAIN

Displays the countries available for a given regulatory domain.

Example:

```
wlan3/0 WLAN+country show reg-domain fcc
Regulatory Domain: FCC
US - UNITED STATES
wlan3/0 WLAN+
```

Command history:

Release	Modification
11.01.09	The "*reg-domain*" option was introduced.

3.2.10 DEAUTHENTICATE

Deauthenticates a client station. A cause 1 (unspecified reason) deauthentication frame is sent to the specified client station. You specify a client station by specifying its MAC address or association identifier (AID).

Syntax:

```
wlan3/0 WLAN+deauthenticate client station ?
  aid             AID of the client station to deauthenticate
        <aid>
  mac-address     MAC address of the client station to deauthenticate
        <mac>
```

Example:

The following example deauthenticates the client station whose MAC address is 00-0b-37-35-f5.

```
wlan0/0 WLAN+client station show summary
BSS: TeldatWLAN

 AID     Ifc            MAC Address             State           Cipher  Auth
  AP     wlan0/0        02-2a-11-37-f2-26       up
   1     wlan0/0        00-0b-6b-37-35-f5       associated      AES     WPA2

wlan0/0 WLAN+deauthenticate client station mac-address 00-0b-6b-37-35-f5
```

3.2.11 DOT1X SHOW

Displays 802.1X authentication information.

When the device is operating in access point (AP) mode, it displays information about the authenticating party. Further information on the 802.1X monitoring menu **show authenticator** command can be found in the following manual: *Teldat* Dm783-I 802.1X Authentication.

When the device is operating in client mode, it displays information about the supplicant. Further information on the 802.1X monitoring menu **show supplicant** command can be found in the following manual: *Teldat* Dm783-I 802.1X Authentication.

Example:

Operating in access point mode.

```
wlan3/0 WLAN+dot1x show
STA-mac:  00-13-f7-ee-7e-40
Interface: wlan0/0 (port 1)
Authenticator PAE state : INITIALIZE
Backend Authentication state : AUTH_REQUEST
AdminControlledDirections: Both
OperControlledDirection: Both
AuthControlledPortControl: Auto
AuthControlledPortStatus: Unauthorized
quietPeriod: 60
serverTimeout: 30
```

```
reAuthPeriod: 3600
reAuthEnabled: Disabled
KeyTransmissionEnabled: Yes

Interface: wlan0/0 (port 1)
EAPOL frames received: 2
EAPOL frames transmitted: 2
EAPOL Start frames received: 0
EAPOL Logoff frames received: 0
EAP Resp/Id frames received: 0
EAP Response frames received: 0
EAP Initial Request frames transmitted: 0
EAP Request frames transmitted: 0
Invalid EAPOL frames received: 0
EAP length error frames received: 0
Last EAPOL frame version: 1
Last EAPOL frame source: 00-13-f7-ee-7e-40

Interface: wlan0/0 (port 1)
authEntersConnecting: 0
authEapLogoffsWhileConnecting: 0
authEntersAuthenticating: 0
authAuthSuccessWhileAuthenticating: 0
authAuthTimeoutsWhileAuthenticating: 0
authAuthFailWhileAuthenticating: 0
authAuthEapStartsWhileAuthenticating: 0
authAuthEapLogoffWhileAuthenticating: 0
authAuthReauthWhileAuthenticating: 0
authAuthEapStartsWhileAuthenticated: 0
authAuthEapLogoffWhileAuthenticated: 0
backendResponses: 0
backendAccessChallenges: 0
backendOtherRequestsToSupplicant: 0
backendAuthSuccesses: 0
backendAuthFails: 0

Interface: wlan0/0 (port 1)
Session Octets Received: 0
Session Octets Transmitted: 0
Session Frames Received: 0
Session Frames Transmitted: 0
Session Identifier: wlan0/0-port1-session0
Session Authentication Method: Remote Authentication Server
Session Time:
Session Terminate Cause: Supplicant Logoff
Session User Name:

wlan0/0 WLAN+
```

3.2.12 DUMP

Displays information about the WLAN interface.

Syntax:

```
wlan3/0 WLAN+dump ?
  ani                 Displays ANI (Adaptive Noise Immunity) information
  delta-stats         Displays delta statistics
  eeprom              Displays EEPROM contents
  info                Displays miscellaneous information
  internal-stats      Dump internal stats
  nodes               Displays nodes information
  pmksa-cache         Displays PMKSA cache
  registers           Displays WLAN chip registers
  tx-power            Displays transmit power information
  verbose             Displays verbose information
  wmm                 Displays WMM configuration
```

```
wlan3/0 WLAN+
```

3.2.12.1 DUMP ANI

Displays Adaptive Noise Immunity (ANI) algorithm debugging information. This information is for *Teldat* internal use only.

3.2.12.2 DUMP DELTA-STATS

Displays access point statistics. Displays information about the frames sent or received by the access point during the specified time interval.

Syntax:

```
wlan0/0 WLAN+dump delta-stats ?
  <1..10000>    time between statistics updates
```

Example:

The following example displays statistics every second.

```
wlan0/0 WLAN+dump delta-stats 1
```

3.2.12.3 DUMP EEPROM

Displays EEPROM contents. This information is for *Teldat* internal use only.

3.2.12.4 DUMP INFO

Displays information about the WLAN card used and the driver in use.

Example 1:

```
wlan2/0 WLAN+dump info
ath_pci: 9.2.0_U10.5.13 (Atheros/multi-bss)
Chipset: Atheros 9280 (0x0029)
HAL info:
ath_hal: 0.9.17.1 (AR5212, AR5416, AR9380, RF5111, RF5112, RF2413, RF5413, RF2316, RF2317, DEBUG, REGOPS_FUNC, PRIVATE_DIAG, WR
TE_EEPROM, 11D)
wlan2/0 WLAN+
```

Example 2:

```
wlan0/0 WLAN+dump info
vendorid 0x14e4
deviceid 0x4351
radiorev 0x62056000
chipnum 0xa8d6
chiprev 0x0
corerev 0x10
boardid 0x4d4
boardvendor 0x14e4
boardrev P205
driverrev 0x50a5500
ucoderev 0x1fc007a
bus 0x1
phytype 0x4
phyrev 0x6
anarev 0x8
wlan0/0 WLAN+
```

3.2.12.5 DUMP INTERNAL-STATS

Displays statistics related to the WLAN interface. These statistics are for *Teldat* internal use only.

Example:

```
wlan0/0 WLAN+dump internal-stats

Tx ioctl reqs          = 0
Tx starts              = 0
Tx start failures      = 0
Tx skb allocs failures = 0
Tx completions         = 0
Tx completions with err= 0
Tx completions out-seq = 0
Poll ioctl reqs        = 1902989
Poll enabled           = no
Rx completions         = 0
Rx completions wrong b = 0
Rx missed              = 0 / 0
Rx errs in driver      = 0
Rx int                 = 0
Tx int                 = 0

wlan0/0 WLAN+
```

3.2.12.6 DUMP NODES

Displays information about the transmission queues relating to each client station on the wireless network.

Syntax:

```
wlanx/x WLAN+dump nodes ?
  <cr>
  verbose    Displays verbose information
wlanx/x WLAN+
```

The *verbose* option displays more statistics than the default option.

Example:

```
wifi_id wlan1/0 WLAN+dump nodes
dumping all allocated nodes ...

node 0x1f34000 mac 5c:33:8e:88:81:b3  tmpnode: 0 nodetable : 1 flags 0x0 refcount: 14
        bssid 5c:33:8e:88:81:b3 cap 0x10 dqlen  0 mgtqlen 0  ssid  TeldatWLAN
        tidno 0 tid 0x1f35078 bf 0x0
        tidno 1 tid 0x1f3510c bf 0x0
        tidno 2 tid 0x1f351a0 bf 0x0
        tidno 3 tid 0x1f35234 bf 0x0
        tidno 4 tid 0x1f352c8 bf 0x0
        tidno 5 tid 0x1f3535c bf 0x0
        tidno 6 tid 0x1f353f0 bf 0x0
        tidno 7 tid 0x1f35484 bf 0x0
        tidno 8 tid 0x1f35518 bf 0x0
        tidno 9 tid 0x1f355ac bf 0x0
        tidno 10 tid 0x1f35640 bf 0x0
        tidno 11 tid 0x1f356d4 bf 0x0
        tidno 12 tid 0x1f35768 bf 0x0
        tidno 13 tid 0x1f357fc bf 0x0
        tidno 14 tid 0x1f35890 bf 0x0
        tidno 15 tid 0x1f35924 bf 0x0
        tidno 16 tid 0x1f359b8 bf 0x0


node 0x1f30000 mac 14:d6:4d:48:06:bf  tmpnode: 0 nodetable : 1 flags 0xf refcount: 1
        bssid 5c:33:8e:88:81:b3 cap 0x531 dqlen  0 mgtqlen 0
        tidno 0 tid 0x1f31078 bf 0x0
        tidno 1 tid 0x1f3110c bf 0x0
        tidno 2 tid 0x1f311a0 bf 0x0
        tidno 3 tid 0x1f31234 bf 0x0
        tidno 4 tid 0x1f312c8 bf 0x0
        tidno 5 tid 0x1f3135c bf 0x0
        tidno 6 tid 0x1f313f0 bf 0x0
        tidno 7 tid 0x1f31484 bf 0x0
        tidno 8 tid 0x1f31518 bf 0x0
        tidno 9 tid 0x1f315ac bf 0x0
        tidno 10 tid 0x1f31640 bf 0x0
        tidno 11 tid 0x1f316d4 bf 0x0
        tidno 12 tid 0x1f31768 bf 0x0
        tidno 13 tid 0x1f317fc bf 0x0
        tidno 14 tid 0x1f31890 bf 0x0
        tidno 15 tid 0x1f31924 bf 0x0
        tidno 16 tid 0x1f319b8 bf 0x0
```

The above example shows two nodes: the access point and an associated client station. The queue status of the queues relating to each Traffic Indicator (TID) is displayed for each client station. In this example, none of the TIDs have packets pending transmission.

3.2.12.7 DUMP PMKSA-CACHE

Displays the security association cache contents. This cache is only used when using WPA or WPA2.

Example:

```
wlan3/0 WLAN+dump pmksa-cache
Index     Address                          PMKID                           age
----- -----------------  -----------------------------------------------  ------
  1   00-0b-6b-37-35-f5  ea e8 36 15 b2 6f 78 0b e7 03 26 2c e0 4a e0 08   42464
wlan3/0 WLAN+
```

Each cache entry corresponds to one client station and reports the client station MAC address, the stored PMK identifier (PMKID) and the remaining time, in seconds, before the cache entry expires. Some devices are able to display an additional opportunistic (*opc*) parameter that indicates whether the entry is opportunistic or not.

3.2.12.8 DUMP REGISTERS

Displays the chip register contents for the WLAN interface. This information is for *Teldat*'s internal use only.

Syntax:

```
wlanx/x WLAN+dump registers ?
  all          All registers
  baseband     Baseband registers
  dcu          DCU registers
  keycache     Key Cache registers
  interrupt    Interrupt registers
  public       Public (BASIC+QCU+DCU) registers
  qcu          QCU registers
  xr           eXtended Range registers
  la           MAC/PCU logic analyzer registers
  dmadbg       DMA Debug registers
  <cr>
wlanx/x WLAN+
```

Example:

```
wlan2/0 WLAN+dump registers
CR       00000004  RXDP     035fc7a4  CFG      00000105  IER      00000001
TXCFG    00020085  RXCFG    00000005  MIBC     00000000  TOPS     00000008
RXNPTO   00000008  TXNPTO   00000010  RPGTO    00000000  RPCNT    0000001f
MACMISC  00000000  D_SIFS   00000160  D_SEQNUM 00000002  D_SLOT   00000370
D_EIFS   00003e38  D_MISC   00000000  D_FPCTL  00000000  D_TXPSE  00010000
RC       00000000  SREV     00000000  STA_ID0  77488000  STA_ID1  b880c7eb
BSS_ID0  ffffffff  BSS_ID1  0000ffff  TIME_OUT 08400b00  RSSI_THR 00000700
USEC     12e0002b  RX_FILTR 00001497  MCAST_0  ffffffff  MCAST_1  ffffffff
DIAG_SW  40000000  TSF_L32  0000b0d0  TSF_U32  00000000  TST_ADAC 00000000
DEF_ANT  00000001  LAST_TST c4557f21  NAV      00000000  RTS_OK   00000000
RTS_FAIL 00000000  ACK_FAIL 00000000  FCS_FAIL 00000000  BEAC_CNT 00000000
SLEEP1   00000000  SLEEP2   00400000  BSSMSKL  ffffff8d  BSSMSKU  0000ffff
TPC      003f3f3f  TFCNT    0001a293  RFCNT    00089645  RCCNT    000f3cc9
CCCNT    001741e0  TSF_PARM 00020207  PHY_ERR  00000000
wlan2/0 WLAN+
```

3.2.12.9 DUMP TX-POWER

Displays transmit power information.

Example:

```
wlan0/0 WLAN+dump tx-power
Power Control:           On, HW
Current channel:         1
BSS channel:             1
BSS Local Max:          63.0  dBm
BSS Local Constraint:    0.0  dB
User Target:            31.75 dBm
SROM antgain:            2G: 2.0 dB, 5G: 0.0 dB

Regulatory Limits:
CCK                   : 17.0
Legacy OFDM 20MHz SISO: 17.0
Legacy OFDM 20MHz CDD : 17.0
MCS 0-7 20MHz SISO    : 17.0
MCS 0-7 20MHz CDD     : 13.0
MCS 0-7 20MHz STBC    : 13.0
MCS 8-15 20MHz SDM    : 13.0
Legacy OFDM 40MHz SISO:  0.0
Legacy OFDM 40MHz CDD :  0.0
MCS 0-7 40MHz SISO    :  0.0
MCS 0-7 40MHz CDD     :  0.0
MCS 0-7 40MHz STBC    :  0.0
MCS 8-15 40MHz SDM    :  0.0
MCS 32                :  0.0

Board Limits:
CCK                   : 19.0
Legacy OFDM 20MHz SISO: 17.50
Legacy OFDM 20MHz CDD : 17.50
MCS 0-7 20MHz SISO    : 17.50
MCS 0-7 20MHz CDD     : 17.50
MCS 0-7 20MHz STBC    : 17.50
MCS 8-15 20MHz SDM    : 17.50
Legacy OFDM 40MHz SISO: 15.50
Legacy OFDM 40MHz CDD : 15.50
MCS 0-7 40MHz SISO    : 15.50
MCS 0-7 40MHz CDD     : 15.50
MCS 0-7 40MHz STBC    : 15.50
MCS 8-15 40MHz SDM    : 15.50
MCS 32                : 15.50

Power Target:
CCK                   : 15.50
Legacy OFDM 20MHz SISO: 15.50
Legacy OFDM 20MHz CDD : 11.50
MCS 0-7 20MHz SISO    : 15.50
MCS 0-7 20MHz CDD     : 11.50
MCS 0-7 20MHz STBC    : 11.50
MCS 8-15 20MHz SDM    : 11.50
Legacy OFDM 40MHz SISO:  8.0
Legacy OFDM 40MHz CDD :  8.0
MCS 0-7 40MHz SISO    :  8.0
MCS 0-7 40MHz CDD     :  8.0
MCS 0-7 40MHz STBC    :  8.0
MCS 8-15 40MHz SDM    :  8.0
MCS 32                :  8.0

Maximum Power Target among all rates:   15.50  15.50
Rate index with Maximum Power Target:   0     0
Last adjusted est. power            :   0.0  15.50
wlan0/0 WLAN+
```

3.2.12.10 DUMP VERBOSE

Displays detailed information about the WLAN operation.

Syntax:

```
wlan0/0 WLAN+dump verbose ?
  dot11i    802.11i information
```

3.2.12.10.1 DUMP VERBOSE DOT11i

Displays detailed operating information about the 802.11i protocol (this is the protocol relating to WLAN security). It also displays the status of all internal variables used during 802.11i operation.

Syntax:

```
wlan0/0 WLAN+dump verbose dot1ii ?
mac-address    Displays detailed information about an associated client station
        <mac>
all            Displays detailed information about every associated client station
global         Displays global 802.11i information
summary        Displays a summary of associated client stations
```

mac-address	Displays information related to the specified client station.
all	Displays all 802.11i protocol information.
global	Displays global 802.11i protocol information.
summary	Displays a summary on the 802.11i protocol.

Example 1:

```
wlan0/0 WLAN+dump verbose dot11i all
                ----------------
                Global Variables
                ----------------
        local address ................. 02-2a-11-37-f2-26
        use PSK ....................... No
        use WPA ....................... WPAv1 and WPAv2
        unicast key index ............. 1
        Counter .......................
        0000: f3 22 06 f0 35 49 2e 11 e5 a8 eb e8 06 c6 9b 36
        0016: fd 6b 66 4f 64 09 02 a1 cc 98 a4 8c be 53 df 00
                -----------------------
                Group Key Control Block
                -----------------------
        state ......................... Global GTK - SETKEYSDONE
        GInit ......................... False
        GTKAuthenticator .............. True
        GTKRekey ...................... False
        GKeyDoneclient stations .............. 0
        GNoclient stations ................... 1
        GN ............................ 1
        GM ............................ 2
        GTKLength ..................... 32
        GMKLength ..................... 32
        GTKCipher ..................... TKIP
        GNonce ........................
        0000: c9 e4 a7 63 f2 4a f8 fe 47 5a 98 87 e4 1c 29 58
        0016: 9c fe 48 43 f2 da 04 39 14 4e 56 ab fe ec 4b f2
        gRekeyEnabled ................. False
        gRekeyPeriod .................. 0
        sm_sched ...................... False
        is_in_loop .................... False
                -----------------
                client station Variables
                -----------------
        address ....................... 00-0b-6b-37-35-f5
        wpa ........................... WPAv2
        aid ........................... 1
        role .......................... Authenticator
        linked ........................ True
        sm_sched ...................... False
        is_in_loop .................... False
                -----------------------
                Authenticator Variables
                -----------------------
        state ......................... client station PTK - PTKINITDONE
                                        client station GTK - IDLE
        Init ........................ False
        AuthenticationFailed ......... False
        AuthenticationRequest ........ False
        ReAuthenticationRequest ...... False
        DeAuthenticationRequest ...... False
        Disconnect .................. False
        EAPOLKeyReceived ............ False
        EAPOLKeyRequest ............. False
        EAPOLKeyPairwise ............ True
        GTimeoutCtr ................. 0
        IntegrityFailed ............. False
        TimeoutEvt .................. False
        TimeoutCtr .................. 1
        MICVerified ................. True
        GUpdateclient stationKeys .......... False
        ANonce ......................
        0000: f3 22 06 ee 35 49 2e 11 e5 a8 eb e8 06 c6 9b 36
        0016: fd 6b 66 4f 64 09 02 a1 cc 98 a4 8c be 53 df 00
        SNonce ......................
        0000: 13 6b df 34 24 e8 e8 c9 cd b0 47 33 15 3a d3 70
        0016: 9e 8a 39 09 cf 94 44 8d 73 dc dd 6d b4 20 9e 00
        keycount .................... 0
        PTK_valid ................... True
        TPTK_valid .................. False
        PTKRequest .................. False
        client station_counted ............. True
        PInitAKeys .................. False
        requestReplayCtr ............ 0x0000000000000000
        replayCtr ................... 0x0000000000000010
        rx_replayCtr_set ............ False
        descType .................... AES
        keyLength ................... 16
        isSecure .................... True
        isPreAuthSession ............ False
        pmkNegotiated ............... False
        Pair ........................ True
        IBSS ........................ False
        has_GTK ..................... False
        flags ....................... 0x00000001
                                       In use
        msg_rcv ..................... Pairwise M4
        last_eapol_key .............. 0x013896d0
```

Example 2:

```
wlan0/0 WLAN+dump verbose dot11i summary
        local address ................ 02-2a-11-37-f2-26
        use PSK ...................... No
        use WPA ...................... WPAv1 and WPAv2
        GTKAuthenticator ............. True
        GTKCipher .................... TKIP

   MAC Address     WPA   AID  Role Cipher Secure Preauth          flags
----------------- ----- ----- ---- ------ ------ ------- ----------------------
00-0b-6b-37-35-f5 WPAv2   1   Auth   AES    True   False 0x00000001 (used )
```

3.2.12.11 DUMP WMM

Displays QoS-related parameters.

Example:

```
wlan0/0 WLAN+dum wm
        AC_BE cwmin  4 cwmax  6 aifs  3 txopLimit    0 us (0)
```

```
              cwmin  4 cwmax 10 aifs  3 txopLimit    0 us (0)
        AC_BK cwmin  4 cwmax 10 aifs  7 txopLimit    0 us (0)
              cwmin  4 cwmax 10 aifs  7 txopLimit    0 us (0)
        AC_VI cwmin  3 cwmax  4 aifs  1 txopLimit 3008 us (94)
              cwmin  3 cwmax  4 aifs  2 txopLimit 3008 us (94)
        AC_VO cwmin  2 cwmax  3 aifs  1 txopLimit 1504 us (47)
              cwmin  2 cwmax  3 aifs  2 txopLimit 2048 us (64)
```

The QoS-related parameters for each access point and client station are displayed for each queue and operating mode.

- AIFS, CwMin, CwMax, TXOP. For further information on these parameters, please see *Configuring the quality of service parameters (WMM)* on page 25.
- ACM: Admission Control Mandatory. If *acm* is displayed, it indicates that the client station must request permission before sending a certain type of data.
- ACK Policy: Reports the ACK policy. If *ack* is displayed, it indicates that the frames are not explicitly acknowledged by ACK. If nothing is displayed, this indicates normal ACK.

3.2.13 IWCONFIG

Configures WLAN interface parameters. When used without any additional parameters, it displays the same information as the **bss show** command.

Syntax:

```
wlanx/x WLAN+iwconfig -h
Usage: iwconfig
                essid {NNN|any|on|off}
                mode {managed|ad-hoc|master|...}
                freq N.NNN[k|M|G]
                channel N
                bit {N[k|M|G]|auto|fixed}
                rate {N[k|M|G]|auto|fixed}
                enc {NNNN-NNNN|off}
                key {NNNN-NNNN|off}
                power {period N|timeout N|saving N|off}
                nickname NNN
                nwid {NN|on|off}
                ap {N|off|auto}
                txpower {NmW|NdBm|off|auto}
                sens N
                retry {limit N|lifetime N}
                rts {N|auto|fixed|off}
                frag {N|auto|fixed|off}
                modulation {11g|11a|CCK|OFDMg|...}
                commit
```

3.2.14 IWLIST

Displays WLAN interface parameters.

Syntax:

```
wlanx/x WLAN+iwlist ?
  scanning        Gets scanning results
  channel         Channel
  ap              Access points
  auth            Authentication
wlanx/x WLAN+
```

3.2.14.1 SCANING

Shows results of scanning the different channels.

Syntax:

```
wlan2/0 WLAN+iwlist scanning ?
  essid    SSID
  last     last scanning results stored
  <cr>
wlan2/0 WLAN+
```

3.2.14.1.1 <cr>

Carries out a new scan and displays the results.

3.2.14.1.2 essid <ssid>

Performs a scan that sends probe request frames asking for the specified network ID. This allows you to detect networks that don't advertise their SSIDs in beacon frames.

3.2.14.1.3 last

Displays the results of the last scan that the device performed.

Example:

```
wlan2/0 WLAN+iwlist scanning
Retrieving scan information, please wait ... (Press ctrl+c to abort)
wlan2/0   Scan completed :
          Cell 01 - Address: 94-0C-6D-CA-EE-6C
                    ESSID:"E-Learning"
                    Mode:Master
                    Frequency:2412 MHz (Channel 1)

                    Quality=31/94  Signal level=-82 dBm  Noise level=-95 dBm
                    Encryption key:on
                    Bit Rates:1.0 Mb/s; 2.0 Mb/s; 5.5 Mb/s; 11.0 Mb/s; 6.0 Mb/s
                              9.0 Mb/s; 12.0 Mb/s; 18.0 Mb/s; 24.0 Mb/s; 36.0 Mb/s
                              48.0 Mb/s; 54.0 Mb/s
                    Extra:bcn_int=100
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    IE: WPA Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    Extra:wme_ie=dd180050f2020101840003a4000027a4000042435e0062322f00
                    Extra:ath_ie=dd0900037f01010000ff7f
          Cell 02 - Address: 00-05-7B-70-AB-78
                    ESSID:"WifiTeldat"
                    Mode:Master
                    Frequency:2412 MHz (Channel 1)

                    Quality=56/94  Signal level=-74 dBm  Noise level=-95 dBm
                    Encryption key:on
                    Bit Rates:1.0 Mb/s; 2.0 Mb/s; 5.5 Mb/s; 11.0 Mb/s; 6.0 Mb/s
                              9.0 Mb/s; 12.0 Mb/s; 18.0 Mb/s; 24.0 Mb/s; 36.0 Mb/s
                              48.0 Mb/s; 54.0 Mb/s
                    Extra:bcn_int=100
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    Extra:wme_ie=dd180050f2020101810003a4000027a4000042435e0062322f00
                    Extra:ath_ie=dd0900037f01010000ff7f
          Cell 03 - Address: 5C-33-8E-88-81-B3
                    ESSID:"wifi_id_teldat"
                    Mode:Master
                    Frequency:2437 MHz (Channel 6)
                    Quality=94/94  Signal level=-44 dBm  Noise level=-95 dBm
                    Encryption key:on
                    Bit Rates:1.0 Mb/s; 2.0 Mb/s; 5.5 Mb/s; 11.0 Mb/s; 6.0 Mb/s
                              9.0 Mb/s; 12.0 Mb/s; 18.0 Mb/s; 24.0 Mb/s; 36.0 Mb/s
                              48.0 Mb/s; 54.0 Mb/s
                    Extra:bcn_int=100
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    Extra:wme_ie=dd180050f2020101850003a4000027a4000042435e0062322f00
                    Extra:ath_ie=dd0900037f01010000ff7f
```

Displays the basic network characteristics for each network detected.

3.2.14.2 CHANNEL

Displays the available channels.

Example:

```
wlan2/0 WLAN+iwlist channel
wlan2/0   113 channels in total; available frequencies :
          Channel 01 : 2412 MHz
          Channel 02 : 2417 MHz
          Channel 03 : 2422 MHz
          Channel 04 : 2427 MHz
          Channel 05 : 2432 MHz
          Channel 06 : 2437 MHz
          Channel 07 : 2442 MHz
          Channel 08 : 2447 MHz
          Channel 09 : 2452 MHz
          Channel 10 : 2457 MHz
          Channel 11 : 2462 MHz
          Channel 12 : 2467 MHz
          Channel 13 : 2472 MHz
          Channel 36 : 5180 MHz
          Channel 40 : 5200 MHz
          Channel 44 : 5220 MHz
          Channel 48 : 5240 MHz
          Channel 52 : 5260 MHz
          Channel 56 : 5280 MHz
          Channel 60 : 5300 MHz
          Channel 64 : 5320 MHz
          Channel 100 : 5500 MHz
          Channel 104 : 5520 MHz
          Channel 108 : 5540 MHz
          Channel 112 : 5560 MHz
          Channel 116 : 5580 MHz
          Channel 120 : 5600 MHz
          Channel 124 : 5620 MHz
          Channel 128 : 5640 MHz
          Channel 132 : 5660 MHz
          Channel 136 : 5680 MHz
          Channel 140 : 5700 MHz
          Current Frecuency:2412 MHz (Channel 1)

wlan2/0 WLAN+
```

3.2.14.3 AP

Displays information about detected access points.

Example:

```
wlan2/0 WLAN+iwlist ap
wlan2/0   Peers/Access-Points in range:
    00-A0-26-6E-00-BD : Quality=94/94  Signal level=-13 dBm  Noise level=-95 dBm
    00-05-7B-70-AB-78 : Quality=66/94  Signal level=-71 dBm  Noise level=-95 dBm
    94-0C-6D-CA-EE-6C : Quality=27/94  Signal level=-83 dBm  Noise level=-95 dBm
    5C-33-8E-88-81-B3 : Quality=94/94  Signal level=-44 dBm  Noise level=-95 dBm
    90-A4-DE-7D-14-C9 : Quality=37/94  Signal level=-80 dBm  Noise level=-95 dBm
    00-A0-26-7C-07-04 : Quality=79/94  Signal level=-67 dBm  Noise level=-95 dBm
    00-A0-26-7C-07-05 : Quality=82/94  Signal level=-66 dBm  Noise level=-95 dBm
    BA-A3-86-05-9A-92 : Quality=86/94  Signal level=-64 dBm  Noise level=-95 dBm
    00-05-7B-70-AB-A0 : Quality=8/94  Signal level=-89 dBm  Noise level=-95 dBm
    90-A4-DE-8A-0F-B4 : Quality=18/94  Signal level=-86 dBm  Noise level=-95 dBm

wlan2/0 WLAN+
```

3.2.14.4 AUTH

Displays information about the authentication type supported by the interface.

Example:

```
wlan2/0 WLAN+iwlist auth
wlan2/0   Authentication capabilities :
                WPA
                WPA2
                CIPHER-TKIP
                CIPHER-CCMP


wlan2/0 WLAN+
```

3.2.15 IWPRIV

Sends a private command to the WLAN interface.

Syntax:

```
wlanx/x WLAN+iwpriv ?
  radio    iwpriv for the radio interface
        <1..70 chars>    Text
        <cr>
  vap      iwpriv for the VAP interface
        <1..70 chars>    Text
        <cr>
```

3.2.15.1 radio

Sends a private command to the radio interface that is common to all WLAN interfaces.

3.2.15.2 vap

Sends a private command to the WLAN interface.

3.2.16 QUEUE SHOW

Displays information about transmission and reception queues. This information is for *Teldat*'s internal use only.

Syntax:

```
wlanx/x WLAN+queue show ?
  <cr>
```

Example:

```
wlan2/0 WLAN+queue show
TXQ[0] TXDP 0x00000000 txq->axq_depth 0 pending 0 schednone 13
no descriptors for queue 0
TXQ[1] TXDP 0x00000000 txq->axq_depth 0 pending 0 schednone 13
no descriptors for queue 1
TXQ[2] TXDP 0x00000000 txq->axq_depth 0 pending 0 schednone 13
no descriptors for queue 2
TXQ[3] TXDP 0x0362e534 txq->axq_depth 0 pending 0 schednone 408
Stuck descriptor dump for queue 3
bf 0x1bd2690 bf->mpdu 0x0 bf_daddr 0x0362e534 len 230 bf_status 0x00000002 bf_flags 0x00000011
TXDP 0362e534 status 0x00000000
desc :  00000000 03962138 212a00ea 004000e6
```

```
Control words

00048000 0000001b 00000810 00000000
00000000 01b0000c 5008f0d0 0a000000
0a000000 0a000000 00808080 00000402
2febaf6b 00000000 00000000 80808080
80808080 80808080 80808080 00000165

no inprogress descriptors for  queue 3
TXQ[8] TXDP 0x00000000 txq->axq_depth 0 pending 0 schednone 13
no descriptors for queue 8
sc->sc_rxlink 0x35fd000 sc->sc_rxpending 0x0
[0] RX bf 0x0x1bdca90 bf->bf_mpdu 0x195a0fc
[1] RX bf 0x0x1bdcb38 bf->bf_mpdu 0x195a900
[2] RX bf 0x0x1bdcbe0 bf->bf_mpdu 0x19540cc
[3] RX bf 0x0x1bdcc88 bf->bf_mpdu 0x195a654
[4] RX bf 0x0x1bdcd30 bf->bf_mpdu 0x1954378
[5] RX bf 0x0x1bdcdd8 bf->bf_mpdu 0x1954624
[6] RX bf 0x0x1bdce80 bf->bf_mpdu 0x195bbb4
[7] RX bf 0x0x1bdcf28 bf->bf_mpdu 0x1963144
[8] RX bf 0x0x1bdcfd0 bf->bf_mpdu 0x194ddf0
[9] RX bf 0x0x1bdd078 bf->bf_mpdu 0x1954e28
[10] RX bf 0x0x1bdd120 bf->bf_mpdu 0x1955380
[11] RX bf 0x0x1bdd1c8 bf->bf_mpdu 0x195c10c
[12] RX bf 0x0x1bdd270 bf->bf_mpdu 0x1955b84
[13] RX bf 0x0x1bdd318 bf->bf_mpdu 0x195c664
[14] RX bf 0x0x1bdd3c0 bf->bf_mpdu 0x1956388
[15] RX bf 0x0x1bdd468 bf->bf_mpdu 0x1956634
[16] RX bf 0x0x1bdd510 bf->bf_mpdu 0x195c910
[17] RX bf 0x0x1bdd5b8 bf->bf_mpdu 0x196414c
[18] RX bf 0x0x1bdd660 bf->bf_mpdu 0x19568e0
[19] RX bf 0x0x1bdd708 bf->bf_mpdu 0x194806c
[20] RX bf 0x0x1bdd7b0 bf->bf_mpdu 0x195d66c
[21] RX bf 0x0x1bdd858 bf->bf_mpdu 0x195d114
[22] RX bf 0x0x1bdd900 bf->bf_mpdu 0x195d918
[23] RX bf 0x0x1bdd9a8 bf->bf_mpdu 0x1956b8c
[24] RX bf 0x0x1bdc010 bf->bf_mpdu 0x19578e8
[25] RX bf 0x0x1bdc0b8 bf->bf_mpdu 0x1957e40
[26] RX bf 0x0x1bdc160 bf->bf_mpdu 0x195f67c
[27] RX bf 0x0x1bdc208 bf->bf_mpdu 0x1966eb8
[28] RX bf 0x0x1bdc2b0 bf->bf_mpdu 0x1958644
[29] RX bf 0x0x1bdc358 bf->bf_mpdu 0x195fe80
[30] RX bf 0x0x1bdc400 bf->bf_mpdu 0x1952b6c
[31] RX bf 0x0x1bdc4a8 bf->bf_mpdu 0x195f928
[32] RX bf 0x0x1bdc550 bf->bf_mpdu 0x1966960
[33] RX bf 0x0x1bdc5f8 bf->bf_mpdu 0x19590f4
[34] RX bf 0x0x1bdc6a0 bf->bf_mpdu 0x195fbd4
[35] RX bf 0x0x1bdc748 bf->bf_mpdu 0x196012c
[36] RX bf 0x0x1bdc7f0 bf->bf_mpdu 0x1952614
[37] RX bf 0x0x1bdc898 bf->bf_mpdu 0x196168c
[38] RX bf 0x0x1bdc940 bf->bf_mpdu 0x1960930
[39] RX bf 0x0x1bdc9e8 bf->bf_mpdu 0x19538c8
[40] RX bf 0x0x1bdca90 bf->bf_mpdu 0x194d094
[41] RX bf 0x0x1bdcb38 bf->bf_mpdu 0x1969174
[42] RX bf 0x0x1bdcbe0 bf->bf_mpdu 0x19540cc
[43] RX bf 0x0x1bdcc88 bf->bf_mpdu 0x19593a0
[44] RX bf 0x0x1bdcd30 bf->bf_mpdu 0x195964c
[45] RX bf 0x0x1bdcdd8 bf->bf_mpdu 0x19598f8
[46] RX bf 0x0x1bdce80 bf->bf_mpdu 0x1960684
[47] RX bf 0x0x1bdcf28 bf->bf_mpdu 0x195a3a8
[48] RX bf 0x0x1bdcfd0 bf->bf_mpdu 0x19548d0
wlan2/0 WLAN+
```

3.2.17 RADAR SHOW

Displays information related to radar detection. This command is only effective when the router is operating in 802.11a mode. Since the frequencies used in this mode can coincide with radar frequencies, the 802.11h standard requires the router to abandon a channel when it detects a radar signal. This regulation only applies in Europe, although other RF regulatory bodies are in the process of developing similar standards.

Example:

```
wlan3/0 WLAN+radar show
No radar detection for the selected wireless interface
wlan3/0 WLAN+
```

3.2.18 RADIO

Accesses radio interface statistics.

Syntax:

```
wlan2/0 WLAN+radio ?
  clear-stats    Clear radio stats
  stats          Displays radio stats
wlan2/0 WLAN+
```

3.2.18.1 clear-stats

Deletes radio interface related statistics.

3.2.18.2 stats

Displays radio interface statistics.

3.2.19 SCAN SHOW

Displays information on detected networks.

Syntax:

```
wlan2/0 WLAN+scan show ?
  summary    Displays a summary scan results
  essid      SSID
  last       last scanning results stored
  <cr>
```

3.2.19.1 <cr>

Performs a new scan and displays the results. This command is the same as the **iwlist scan <cr>** command.

3.2.19.2 essid <ssid>

Performs a scan that sends probe request frames asking for the specified network ID. Allows you to detect networks that do not advertise their SSID in beacon frames. This command is the same as the **iwlist scan essid <ssid >** command.

3.2.19.3 last

Shows the results of the last scan performed by the router. This command is the same as the **iwlist last** command.

3.2.19.4 summary

Displays a summary of the networks detected in the last scan the router performed.

Example:

```
wlan3/0 WLAN+scan show summary
number of BSS found: 4
```

```
      SSID              BSSID        Chann    Mode   Beacon     Capabilities
---------------  -----------------  -----  -------  ------  ------------------
WTeldat          00-07-40-a2-5e-9d   2442  802.11g     100  0x0411
                                                                ESS
                                                                Privacy
Private WLAN     00-0b-6b-4e-f7-3d   2462  802.11g     100  0x0431
                                                                ESS
                                                                Privacy
INTEGRAT         00-13-46-76-82-7d   2442  802.11g     100  0x0431
                                                                ESS
                                                                Privacy
                                                                WPA
WPA Information Element:
  ID: 0xDD Len: 28
  Data:
        0000: 00 50 f2 01 00 01 02 f2 50 00 00 02 04 f2 50 00
        0016: 02 f2 50 00 00 01 01 f2 50 00 00 0c
  WPA:
        multicast cipher: TKIP
        unicast ciphers(2): AES-CCMP TKIP
        AKM Suites(1): 802.1X
        Capabilities(0x000c): Pairwise, 16 PTK Replay Ctrs

visitasteldat    04-11-46-76-82-7d   2442  802.11g     100  0x0011
                                                                ESS
                                                                Privacy
wlan3/0 WLAN+
```

Displays the following information for each detected network:

- SSID: network ID.
- BSSID: the access point's MAC address.
- Chann: the detected network frequency, in MHz.
- Beacon: beacon frame periodicity.
- Capabilities: the capabilities announced by the access point for the network are displayed in hexadecimal format. This also says whether the capabilities correspond to an independent network (IBSS) or an infrastructure (ESS), and whether some sort of privacy is used. Additionally, if the network announces WPA or RSN (WPA2) information elements, the broadcast encryption (unicast and multicast) and authentication characteristics are given.

The above example shows three WEP networks (that announce privacy but do not include WPA or RSN information elements) and a WPA network. The latter uses 802.1X and allows AES and TKIP encryption for unicast frames. Multicast frames use TKIP encryption.

Example:

```
wlan2/0 WLAN+scan show summary
SSID            BSSID              CHAN RATE  S:N   INT CAPS
pabloWLAN       00-a0-26-6e-00-bd    1   54M 82:0   100 Es
WifiTeldat      90-a4-de-7d-14-c9   11   54M 15:0   100 EPSs
Visitas Teldat  ba-a3-86-05-9a-92   10   54M 29:0   100 EPSs
WifiTeldat      00-05-7b-70-ab-a0   11   54M  6:0   100 EPSs
pruebasWeb      90-a4-de-8a-0f-b4   11   54M  8:0   100 EPSs
wlan2/0 WLAN+
```

- SSID: network identifier.
- BSSID: access point's MAC address.
- CHAN: the channel where the network was detected.
- RATE: maximum network speed. By failing to take into account 802.11n capabilities, the information in this field may be erroneous.
- S:N: signal/noise ratio. The first number is the last RSSI received from the access point; the second is the noise value.
- INT: interval between beacon frames.
- CAPS: network capabilities, according to the following table:

Capabilities	Meaning
E	ESS
I	IBSS

c	Pollable
C	Poll Request
P	Privacy enabled
S	Short preamble
B	PBCC
A	Channel Agility
s	Short slot time
D	DSSS/OFDM

3.2.19.5 blacklist

Displays access points that are on the client station's blacklist.

3.2.20 client station SHOW

Displays information about the client stations that are connected to a particular wireless network.

The **client station show** command supports a number of different options:

- Followed by the **summary** option, it allows you to view a status summary for the client stations belonging to the wireless network.
- Followed by the **ap** option, it displays detailed information about the access point.
- Followed by a client station's ID number or **mac-address** option and the client station's MAC address, it shows detailed information about the specified client station.
- Followed by the **all** option, it displays detailed information on all client stations belonging to the wireless network, including the access point.

Syntax:

```
wlan3/0 WLAN+client station show ?
  mac-address    Displays detailed information about an associated client station
  <1..2007>      Displays detailed information about an associated client station
  all            Displays detailed information about the access point and every
                 associated client station
  ap             Displays detailed information about the access point
  summary        Displays a summary of associated client stations
      verbose    Displays verbose information
      <cr>
wlan3/0 WLAN+
```

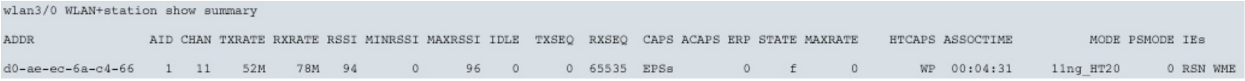
Example:

```
wlan3/0 WLAN+client station show summary
BSS: mssid_1
client stations connected: 1

 AID            MAC Address             State           Cipher  Auth
  AP            00-0b-6b-37-35-f5       up
   1            00-0b-6b-34-af-03       associated      TKIP    WPA-PSK


Wlan3/0 WLAN+
```

The following information is displayed:

- BSS: shows the network SSID.
- Connected client stations: reports the number of connected client stations.
- AID: client station ID. Identifier used to display client station-specific information.
- MAC Address: client station's MAC address.
- State: WLAN client station status.
- Cipher: type of encryption used by the client station.
- Auth: type of authentication used by the client station. This includes WPA and WPA2.

Example:



```
wlan3/0 WLAN+station show summary
ADDR              AID CHAN TXRATE RXRATE RSSI MINRSSI MAXRSSI IDLE  TXSEQ  RXSEQ  CAPS ACAPS ERP STATE MAXRATE    HTCAPS ASSOCTIME         MODE PSMODE IEs
d0-ae-ec-6a-c4-66   1   11    52M    78M   94       0      96    0      0  65535  EPSs        0     f       0        WP  00:04:31    11ng_HT20      0 RSN WME
```

The following information is displayed:

- ADDR: client station MAC address.
- AID: client station ID.
- CHAN: channel used.
- TXRATE: current transmit data rate.
- RXRATE: current receive data rate.
- RSSI: signal strength of the last packet received. For MIMO devices, this is the mean value of all active receive channels.
- MINRSSI: minimum signal strength of received packets.
- MAXRSSI: maximum signal strength of received packets.
- TXSEQ: sequence number of the last transmitted packet.
- RXSEQ: sequence number of the last received packet.
- CAPS: client station capabilities.

E: ESS

I: IBSS

c: Pollable.

C: Poll Request.

P: Privacy.

S: Short preamble.

B: PBCC

A: Channel Agility.

s: Short slot time.

D: DSSS/OFDM

- ACAPS: Advanced capabilities (Atheros).

D: Turbo G.

C: Compression.

F: Fast frame.

X: XR radio.

A: Advanced radio.

T: Boost.

- ERP: transmission power radiated in dBm.
- STATE: client station status. Bitmap formed by the following values:

0x0001: Authorized for data transfer.

0x0002: QoS enabled.

0x0004: ERP enabled.

0x0008: HT (802.11n) speeds enabled.

0x0010: Power saving mode enabled.

0x0020: Authentication reference maintained.

0x0040: uAPSD enabled.

0x0080: triggerable uAPSD.

0x0100: uAPSD SP in progress.

0x0200: Atheros node.

0x0400: WDS fix required.

0x0800: WDS link.

- MAXRATE: maximum rate configured for a client (0 for unlimited).
- HTCAPS: 802.11n capabilities (HT: High Throughput):

A: Advanced encoding.

W: 40 MHz bandwidth.

P: MIMO power saving enabled.

Q: Static MIMO power saving.

R: Dynamic MIMO power saving.

G: Greenfield preamble.

S: Short GI (40MHz).

D: Block ACK delayed.

M: Max. AMSDU size.

- ASSOCTIME: client station association time.
- IEs: client station information elements:

WPA

WME

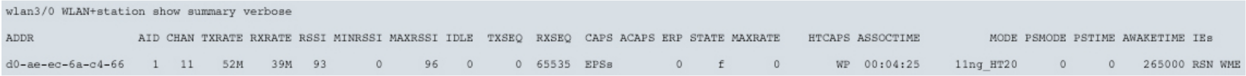
ATH: Atheros information elements.

VEN: Manufacturer-specific.

RSN

- MODE: Current 802.11 mode.
- PSMODE: connected client station power saving mode.

Example:



```
wlan3/0 WLAN+station show summary verbose
ADDR              AID CHAN TXRATE RXRATE RSSI MINRSSI MAXRSSI IDLE  TXSEQ  RXSEQ  CAPS ACAPS ERP STATE MAXRATE    HTCAPS ASSOCTIME          MODE PSMODE PSTIME AWAKETIME IEs
d0-ae-ec-6a-c4-66   1   11    52M    39M   93       0      96    0      0  65535  EPSs        0     f       0        WP  00:04:25    11ng_HT20      0      0    265000 RSN WME
```

Displays power save information for the connected client stations.

Example 1:

Detailed information about the access point.

```
wlan0/0 WLAN+client station show ap
Associated client stations: 1

Num     Mac Address        Time
1    00-0b-6b-37-35-f5    00:00:04:38

n_client stations: 1
Security: WPA/WPA2
Encryption: TKIP/AES
MicErrorKeyMsgs         0       MicErrorRcv     0
TKIPCountermeasures     0
RSN Information Element:
  ID: 0x30 Len: 24
  Data:
        0000: 00 01 02 ac 0f 00 00 02 04 ac 0f 00 02 ac 0f 00
        0016: 00 01 01 ac 0f 00 00 0c
  RSN:
        multicast cipher: TKIP
        unicast ciphers(2): AES-CCMP TKIP
        AKM Suites(1): 802.1X
        Capabilities(0x000c): No Pre-Auth, Pairwise, 16 PTK Replay Ctrs, 1 GTK R
eplay Ctr
WPA Information Element:
  ID: 0xDD Len: 28
  Data:
        0000: 00 50 f2 01 00 01 02 f2 50 00 00 02 04 f2 50 00
        0016: 02 f2 50 00 00 01 01 f2 50 00 00 0c
  WPA:
        multicast cipher: TKIP
        unicast ciphers(2): AES-CCMP TKIP
        AKM Suites(1): 802.1X
        Capabilities(0x000c): Pairwise, 16 PTK Replay Ctrs
```

Example 2:

Detailed information about client station 1.

```
wlan0/0 WLAN+client station show 1
00-0b-6b-37-35-f5 STA, AID: 1
         rateset [ 1 2 5.5 6 9 11 12 18 24 36 48 54 ]
         idle 53 seconds
         in network 650 seconds
         state: AUTHENTICATED ASSOCIATED AUTHORIZED
         flags 0x403a: WME
         tx pkts: 10
         tx failures: 0
         rx ucast pkts: 9
         rx mcast/bcast pkts: 0
         rate of last tx pkt: 1000 kbps
         rate of last rx pkt: 1000 kbps
RSN Information Element:
  ID: 0x30 Len: 20
  Data:
        0000: 00 01 02 ac 0f 00 00 01 04 ac 0f 00 00 01 01 ac
        0016: 0f 00 00 00
  WPA:
        multicast cipher: TKIP
        unicast ciphers(1): AES-CCMP
        AKM Suites(1): 802.1X
        Capabilities(0x0000): No Pre-Auth, Pairwise, 1 PTK Replay Ctr, 1 GTK Rep
lay Ctr
STA-mac:  00-0b-6b-37-35-f5
Identity: teldat-user
Current Auth state: AUTHENTICATED   Current AS state: AUTH_IDLE

Authenticator Stats:
====================
authEntersConnecting:                           1
authEapLogoffsWhileConnecting:                  0
authEntersAuthenticating:                       1
authAuthSuccessesWhileAuthenticating:           1
authAuthTimeoutsWhileAuthenticating:            0
authAuthFailWhileAuthenticating:                0
authAuthEapStartsWhileAuthenticating:           0
authAuthEapLogoffWhileAuthenticating:           0
authAuthReauthsWhileAuthenticated:              0
authAuthEapStartsWhileAuthenticated:            0
authAuthEapLogoffWhileAuthenticated:            0

RADIUS state:
==============
backendResponses:                               7
backendAccessChallenges:                        6
backendOtherRequestsToSupplicant:               7
```

```
backendAuthSuccesses:                                  1
backendAuthFails:                                      0
```

Command history:

Release	Modification
10.09.20	The **verbose** option was introduced.
11.00.03	The **verbose** option was introduced.
11.01.02	New monitoring info added to **client station show summary**.

3.2.21 WPS

Provides access to commands to start the negotiation via WPS.

3.2.21.1 Client operation

3.2.21.1.1 WPS PBC

Simulates the push of a button to start the WPS negotiation using the Push Button configuration (PBC) method. You have two minutes in which to push a button on the access point to start this method.

Example:

```
wlan2/0 WLAN+wps pbc
wlan2/0 WLAN+
```

3.2.21.1.2 WPS PIN

Parameters to start the WPS negotiation using the PIN method.

Syntax:

```
wlanx/x WLAN+wps pin
  get       Get random PIN
  any       Wildcard BSSID
       <word>     PIN
  <mac>     BSSID
       <word>     PIN
```

The **get** option allows you to obtain a random PIN to use during the WPS session. This PIN must be entered in the access point.

To start the WPS negotiation on the client station, the obtained PIN must be entered into the device using the **any** option if you do not want to specify the access point's MAC address, or the **<mac>** option if you do want to associate the PIN with the access point's MAC address.

The procedure for using WPS with the PIN method is as follows:

(1) Get a random PIN for the client station.

```
wlan2/0 WLAN+wps pin get
PIN: 54576278
wlan2/0 WLAN+
```

(2) Enter the obtained PIN in the access point. In the above example, you would enter PIN **54576278**.

(3) Enter the PIN on the client station to start WPS negotiation.

```
wlan2/0 WLAN+wps pin any 54576278
```

3.2.21.2 Access point operation

3.2.21.2.1 WPS PBC

Simulates the push of a button to start the WPS negotiation using Push Button Configuration (PBC). To start this method, you have two minutes in which to press a button on the client station.

Example:

```
wlan2/0 WLAN+wps pbc
wlan2/0 WLAN+
```

3.2.21.2.2 WPS PIN

Parameters to start the WPS negotiation using the PIN method.

Syntax:

```
wlanx/x WLAN+wps pin {any | <uuid>} <pin> {timeout <value>} {mac-address <mac>}
```

Allows you to enter a client station's PIN in the access point in order to start the WPS negotiation process. The available parameters are:

- *uuid*: Universally Unique Identifier. Universal station ID. If you do not want to enter this, you can use the **any** option to indicate any UUID.
- *pin*: Client station PIN value.
- *timeout*: This is an optional value to specify how long the entered PIN is valid for. If no value is specified, it is always valid.
- *mac-address*: Client station MAC address.

The procedure for using WPS with the PIN method is as follows:

(1) Get a PIN from the client station.

(2) Enter the obtained PIN in the access point.

```
wlan2/0 WLAN+wps pin any 37968076
```

3.2.22 EXIT

Exits the WLAN interface monitoring menu.

```
wlan3/0 WLAN+exit
+
```

Chapter 4 Configuration Examples

4.1 Basic configuration: bridge and DHCP

This example configures a *Teldat* device with the most common configuration: a bridge between the Ethernet and the WLAN. In addition, the access point uses DHCP to assign addresses to the client stations that belong to the wireless network.

4.1.1 Scenario

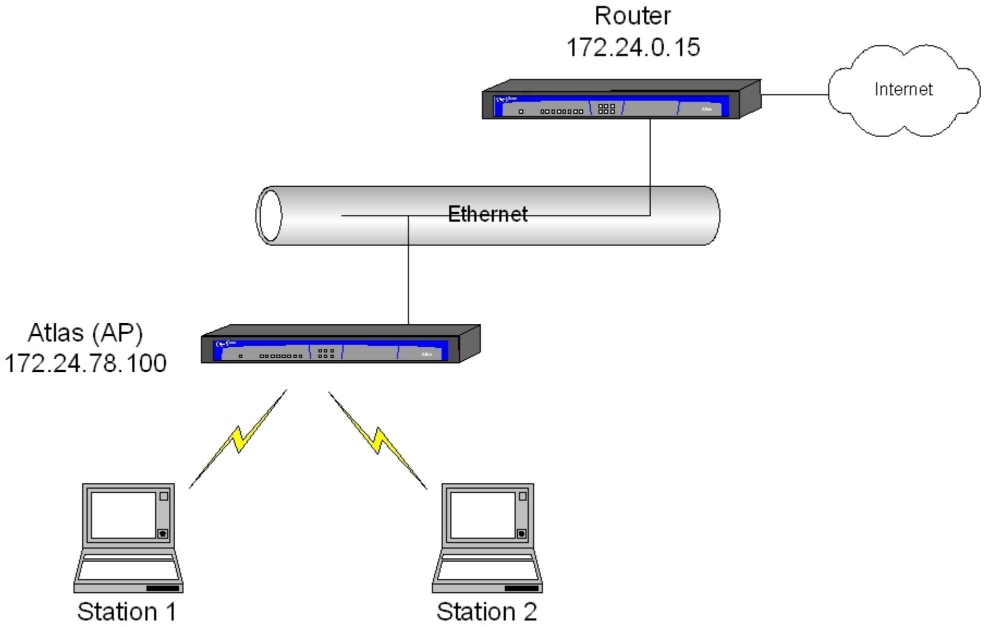


Fig. 17: **Basic configuration: bridge and DHCP**

In this scenario, client stations 1 and 2 connect to the access point (AP) and the AP uses DHCP to assign them addresses in the 172.24.78.1 to 172.24.78.100 range. In addition, DHCP is used to indicate the default router address to access Internet (172.24.0.15) and the DNS server address (172.24.0.23).

4.1.2 Configuring wireless LAN

The WLAN interface configuration in this section is very simple: you set up a *Teldat* WLAN network identifier, leaving the other parameters set to their default values.

```
network wlan3/0
; -- Wireless LAN Interface. Configuration --
   bss "Teldat WLAN"
   exit
;
exit
;
```

4.1.3 Configuring bridge

In our example, a bridge is configured between the WLAN interface and the Ethernet interface (ethernet0/0). For information on creating a bridge configuration, see the following manual: *Teldat* Dm717-I Bridge.

```
protocol asrt
; -- ASRT Bridge user configuration --
   bridge
   irb
   port ethernet0/0 1
   port wlan3/0 2
   route-protocol ip
exit
```

```
;
```

4.1.4 Configuring DHCP

In our example, the *Teldat* device is configured to assign addresses in the 172.24.78.1 to 172.24.78.100 range. For further information on DHCP configuration, please see the following manual: *Teldat* Dm730-I DHCP Protocol.

```
protocol dhcp
; -- DHCP Configuration --
   enable server
;
   server
; -- DHCP Server Configuration --
      shared 1
      shared 2
;
      subnet wi-fi 2 network 172.24.78.0 255.255.0.0
      subnet wi-fi 2 range 172.24.78.1 172.24.78.100
      subnet wi-fi 2 dns-server 172.24.0.23
      subnet wi-fi 2 router 172.24.0.15
;
   exit
;
exit
;
```

4.1.5 Complete configuration

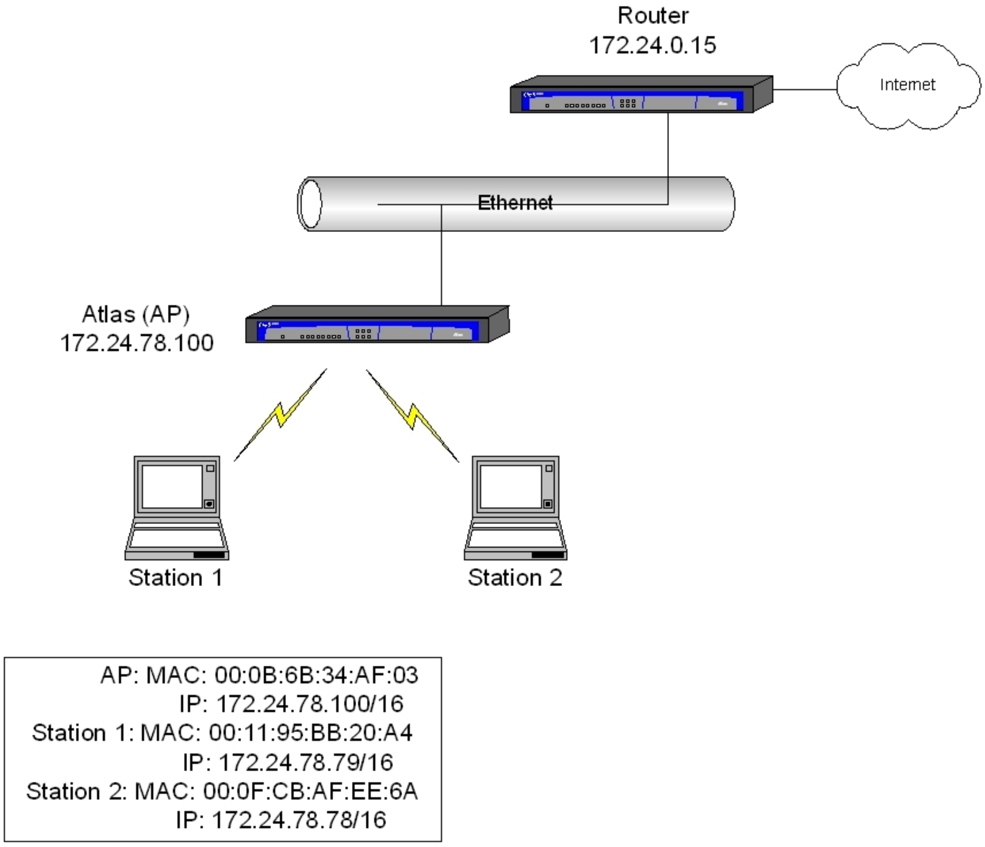
The complete configuration, including an address in the bridge interface, is as follows:

```
; Showing System Configuration for access-level 15 ...

log-command-errors
no configuration
add device bvi 0
set data-link x25 serial0/0
;
;
network ethernet0/0
; -- Ethernet Interface User Configuration --
   no ip address
;
exit
;
;
;
network ethernet0/1
; -- Ethernet Interface User Configuration --
   no ip address
;
exit
;
;
;
network x25-node
; -- X25-node interface configuration --
   no ip address
;
exit
;
;
;
network wlan3/0
; -- Wireless LAN Interface. Configuration --
   no ip address
;
   bss "Teldat WLAN"
   exit
;
exit
;
;
network bvi0
; -- Bridge Virtual Interface configuration --
   ip address 172.24.78.100 255.255.0.0
;
;
;
;
exit
;
protocol asrt
; -- ASRT Bridge user configuration --
   bridge
   irb
   port ethernet0/0 1
   port wlan3/0 2
   route-protocol ip
exit
;
;
protocol dhcp
; -- DHCP Configuration --
   enable server
;
   server
; -- DHCP Server Configuration --
      shared 1
      shared 2
;
      subnet wi-fi 2 network 172.24.78.0 255.255.0.0
      subnet wi-fi 2 range 172.24.78.1 172.24.78.100
      subnet wi-fi 2 dns-server 172.24.0.23
      subnet wi-fi 2 router 172.24.0.15
;
   exit
;
exit
;
dump-command-errors
end
; --- end ---
```

4.2 Static WEP with MAC access control

This example shows you how to configure a wireless network with static WEP security.

4.2.1 Scenario



AP: MAC: 00:0B:6B:34:AF:03
IP: 172.24.78.100/16
Station 1: MAC: 00:11:95:BB:20:A4
IP: 172.24.78.79/16
Station 2: MAC: 00:0F:CB:AF:EE:6A
IP: 172.24.78.78/16

Fig. 18: **Static WEP with MAC access control**

A wireless network will be created with two client stations that are connected to the access point. The wireless network that is formed uses static WEP for data encryption. A 104-bit key will be used in position 3. The configured key is **customwepkey3**.

For added security, only those client stations shown in the above image will be allowed to connect.

4.2.2 Configuration

Only the WLAN interface configuration is displayed.

(1) Access the WLAN interface configuration.

```
*config


Config>net wlan3/0

-- Wireless LAN Interface. Configuration --
wlan3/0 WLAN config>
```

(2) Configure the network identifier, *Teldat* WLAN, and access the BSS configuration.

```
wlan3/0 WLAN config>bss "Teldat WLAN"


wlan3/0 bss config>
```

(3) Invoke security in the BSS.

```
wlan3/0 bss config>privacy-invoked
wlan3/0 bss config>
```

(4) Set the key in position 2 as the default key.

```
wlan3/0 bss config>key default 3
wlan3/0 bss config>
```

(5) Exit the BSS configuration.

```
wlan3/0 bss config>exit
```

```
wlan3/0 WLAN config>
```

(6) Configure the WEP key in position 3.

```
wlan3/0 WLAN config>key 3 size 104 ascii plain customwepkey3
wlan3/0 WLAN config>
```

(7) Enable MAC address access control.

```
wlan3/0 WLAN config>access-control allow
wlan3/0 WLAN config>
```

(8) Allow client stations with MAC addresses 00-11-95-bb-20-a4 and 00-0f-cb-af-ee-6a to connect.

```
wlan3/0 WLAN config>access-control mac-address 00-11-95-bb-20-a4
wlan3/0 WLAN config>access-control mac-address 00-0f-cb-af-ee-6a
wlan3/0 WLAN config>
```

(9) Exit the WLAN interface configuration.

```
wlan3/0 WLAN config>exit
Config>
```

The complete configuration of the WLAN interface is as follows:

```
network wlan3/0
; -- Wireless LAN Interface. Configuration --
   no ip address
;
   bss "Teldat WLAN"
      privacy-invoked
      access-control allow
      access-control mac-address 00-11-95-bb-20-a4
      access-control mac-address 00-0f-cb-af-ee-6a
;
      key default 3
   exit
;
;key 3 size 104 ascii plain customwepkey3
   key 3 size 104 ascii ciphered 0x907EE074234C46DD1E3B4097FD40460E
;
exit
;
```

4.3 Dynamic WEP

This example shows you how to configure a wireless network with dynamic WEP security. A Radius server is available for this purpose.

4.3.1 Scenario

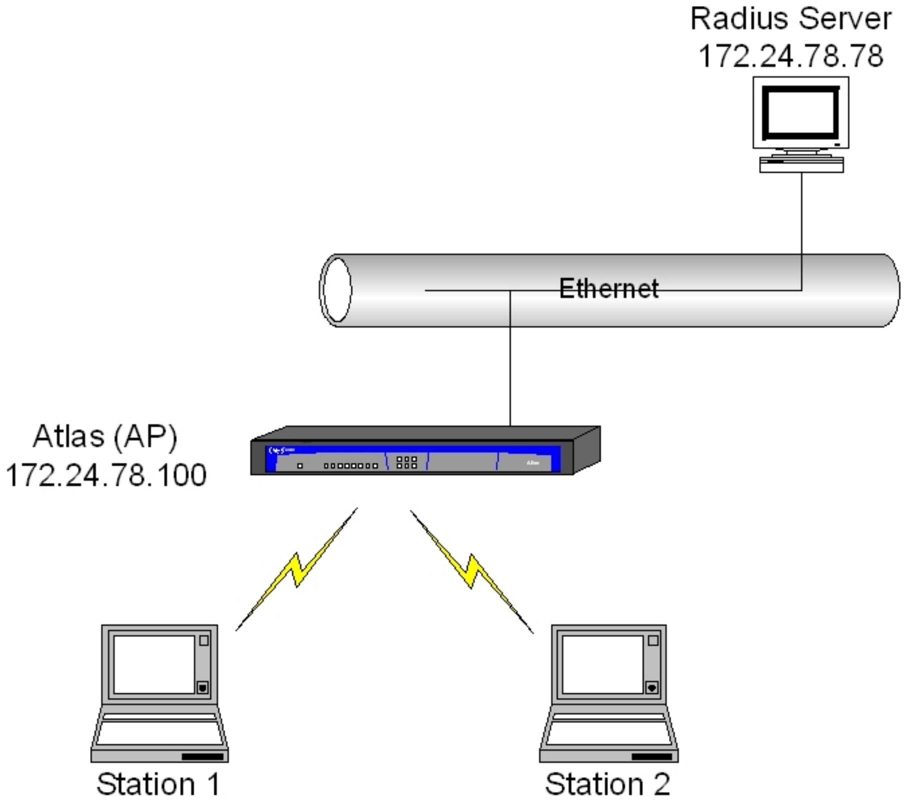


Fig. 19: **Dynamic WEP**

4.3.2 Configuration

Configuring the WLAN interface:

(1) Access the WLAN interface configuration.

```
*config


Config>net wlan3/0

-- Wireless LAN Interface. Configuration --
wlan3/0 WLAN config>
```

(2) Configure the network identifier, *Teldat* WLAN, and access the BSS configuration.

```
wlan3/0 WLAN config>bss "Teldat WLAN"


wlan3/0 bss config>
```

(3) Invoke security in the BSS.

```
wlan3/0 bss config>privacy-invoked
wlan3/0 bss config>
```

(4) Specify the use of dynamic WEP.

```
wlan3/0 bss config>wep-keysource dynamic
wlan3/0 bss config>
```

(5) Exit the BSS configuration.

```
wlan3/0 bss config>exit
wlan3/0 WLAN config>
```

(6) Exit the WLAN interface configuration.

```
wlan3/0 WLAN config>exit
Config>
```

You also need to configure the Radius server. For more information on how to configure the Radius server, please see the following manuals: *Teldat* Dm733-I Radius Protocol or Dm800-I AAA feature.

The complete configuration for the WLAN interface looks like this:

```
network wlan3/0
; -- Wireless LAN Interface. Configuration –
;
;
   no ip address
;
   bss "Teldat WLAN"
      privacy-invoked
      wep-keysource dynamic
   exit
;
exit
;
```

4.4 WPA-PSK

This example configures a wireless network with WPA security with shared-key (WPA-PSK) and AES-CCMP encryption.

4.4.1 Scenario

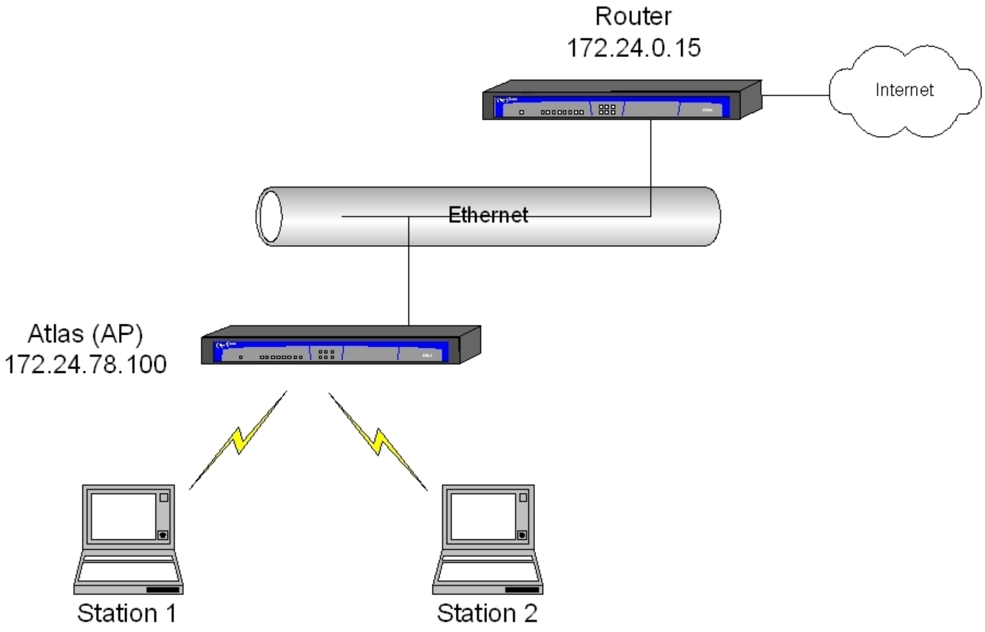


Fig. 20: **Wireless network with WPA-PSK**

4.4.2 Configuration

Configuring the WLAN interface:

(1) Access the WLAN interface configuration.

```
*config


Config>net wlan3/0

-- Wireless LAN Interface. Configuration --
wlan3/0 WLAN config>
```

(2) Configure the network identifier, *Teldat* WLAN, and access the BSS configuration.

```
wlan3/0 WLAN config>bss "Teldat WLAN"
```

```
wlan3/0 bss config>
```

(3) Invoke security in the BSS.

```
wlan3/0 bss config>privacy-invoked
wlan3/0 bss config>
```

(4) Specify the use of WPA security.

```
wlan3/0 bss config>rsn wpa
wlan3/0 bss config>
```

(5) Configure the preshared-key.

```
wlan3/0 bss config>akm-suite psk
wlan3/0 bss config>
```

(6) Configure the key.

```
wlan3/0 bss config>wpa-psk passphrase plain "Teldat WPA PSK"
wlan3/0 bss config>
```

(7) Configure the encryption: AES-CCMP.

```
wlan3/0 bss config>cipher aes-ccmp
wlan3/0 bss config>
```

(8) Exit the BSS configuration.

```
wlan3/0 bss config>exit
wlan3/0 WLAN config>
```

(9) Exit the WLAN interface configuration.

```
wlan3/0 WLAN config>exit
Config>
```

The complete WLAN interface configuration looks like this:

```
network wlan3/0
; -- Wireless LAN Interface. Configuration --
   no ip address
;
   bss "Teldat WLAN"
      privacy-invoked
      rsn wpa
      cipher aes-ccmp
      akm-suite psk
      wpa-psk passphrase plain "Teldat WPA PSK"
      wpa-psk passphrase ciphered 0xFCCD3929AA296054C9784E10C9691488
   exit
;
exit
;
```

4.5 WPA, WPA2 with Radius server

This example configures a wireless network with WPA and WPA2 security. In addition, both AES-CCMP and TKIP encryption will be allowed. In this way, client stations have the flexibility to select the security policy that best fits their characteristics.

An external Radius server is available for authentication.

4.5.1 Scenario

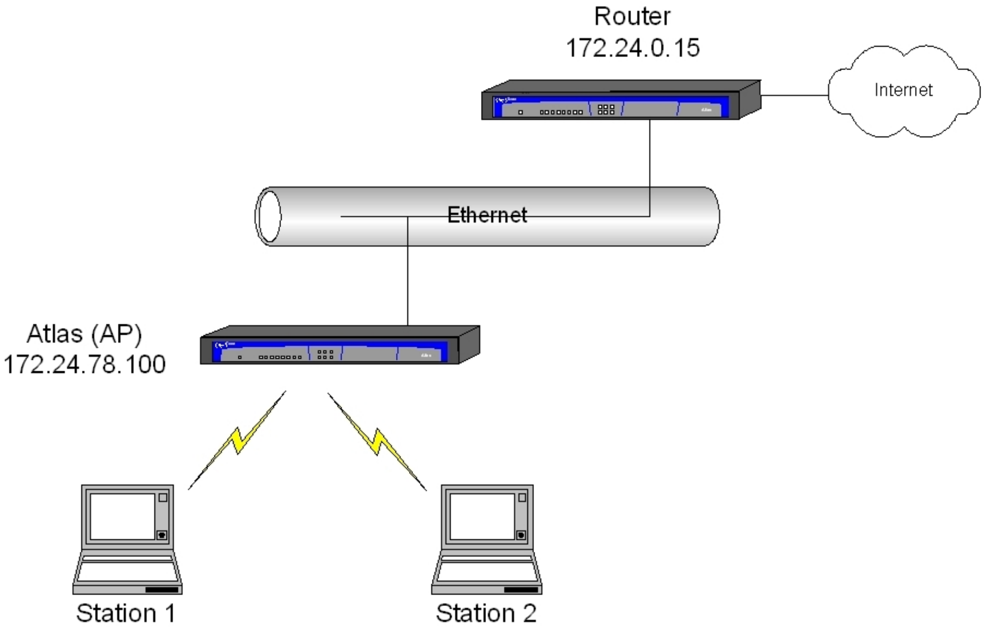


Fig. 21: **Wireless network with WPA and WPA2 security**

4.5.2 Configuration

WLAN interface configuration:

(1) Access the WLAN interface configuration.

```
*config


Config>net wlan3/0

-- Wireless LAN Interface. Configuration --
wlan3/0 WLAN config>
```

(2) Configure the network identifier, *Teldat* WLAN, and access the BSS configuration.

```
wlan3/0 WLAN config>bss "Teldat WLAN"


wlan3/0 bss config>
```

(3) Invoke security in the BSS.

```
wlan3/0 bss config>privacy-invoked
wlan3/0 bss config>
```

(4) Specify the use of WPA and WPA2.

```
wlan3/0 bss config>rsn wpa
wlan3/0 bss config>rsn wpa2
wlan3/0 bss config>
```

(5) Configure 802.1X authentication and distribution.

```
wlan3/0 bss config>akm-suite dot1x
wlan3/0 bss config>
```

(6) Configure the encryption: AES-CCMP and TKIP.

```
wlan3/0 bss config>cipher aes-ccmp
wlan3/0 bss config>cipher tkip
wlan3/0 bss config>
```

(7) Exit the BSS configuration.

```
wlan3/0 bss config>exit
wlan3/0 WLAN config>
```

(8) Exit the WLAN interface configuration.

```
wlan3/0 WLAN config>exit
Config>
```

You also need to configure the Radius server. For information on configuring the Radius server, please see the following manual: *Teldat* Dm733-I Radius Protocol.

(1) Access the Radius configuration menu.

```

Config>feature radius

-- RADIUS User Configuration --
RADIUS config>
```

(2) Configure the Radius server address.

```
RADIUS config>primary-address 172.24.78.78
RADIUS config>
```

(3) Configure the key for the Radius server.

```
RADIUS config>primary-secret whatever
RADIUS config>
```

(4) Enable Radius.

```
RADIUS config>enable radius
RADIUS enabled
RADIUS config>
```

(5) Exit the Radius configuration menu.

```
RADIUS config>exit
Config>
```

The complete WLAN interface configuration looks like this:

```
network wlan3/0
; -- Wireless LAN Interface. Configuration --
   no ip address
;
   bss "Teldat WLAN"
      privacy-invoked
      rsn wpa
      rsn wpa2
      cipher aes-ccmp
      cipher tkip
      akm-suite dot1x
   exit
;
exit
;
```

And for the Radius server:

```
feature radius
; -- RADIUS User Configuration --
   primary-address 172.24.78.78
   primary-secret whatever
   enable radius
exit
;
```

Appendix A Codes

A.1 Country codes allowed

The two-letter country codes that you can use with the **country** configuration command are shown below. The codes are taken from ISO 3166.

Country	Country Code
No country	ALL
Afghanistan	AF
Africa	XB
Albania	AL
Algeria	DZ
American Samoa	AS
Angola	AO
Anguilla	AI
Antigua And Barbuda	AG
Argentina	AR
Armenia	AM
Aruba	AW
Ascension Island	AC
Australia	AU
Austria	AT
Azerbaijan	AZ
Bahamas	BS
Bahrain	BH
Bangladesh	BD
Barbados	BB
Belarus	BY
Belgium	BE
Belize	BZ
Benin	BJ
Bermuda	BM
Bhutan	BT
Bolivia	BO
Bosnia And Herzegovina	BA
Botswana	BW
Bouvet Island	BV
Brazil	BR
British Indian Ocean Territory	IO
Brunei Darussalam	BN
Bulgaria	BG
Burkina Faso	BF
Burundi	BI
Cambodia	KH
Cameroon	CM
Canada	CA
Cape Verde	CV
Cayman Islands	KY
Central African Republic	CF
Chad	TD

Chile	CL
China	CN
Christmas Island	CX
Clipperton Island	CP
Cocos (Keeling Island)	CC
Colombia	CO
Comoros	KM
Congo	CG
Congo, The Democratic Republic of the	CD
Cook Islands	CK
Costa Rica	CR
Ivory Coast	CI
Croatia	HR
Cuba	CU
Cyprus	CY
Czech Republic	CZ
Denmark	DK
Djibouti	DJ
Dominica	DM
Dominican Republic	DO
Eastern Europe	XW
Ecuador	EC
Egypt	EG
El Salvador	SV
Equatorial Guinea	GQ
Eritrea	ER
Estonia	EE
Ethiopia	ET
European Union	EU
Falkland Islands (Malvinas)	FK
Faroe Islands	FO
Fiji	FJ
Finland	FI
France	FR
French Guiana	GF
French Polynesia	PF
French Southern Territories	TF
Gabon	GA
Gambia	GM
Georgia	GE
Germany	DE
Ghana	GH
Gibraltar	GI
Greece	GR
Grenada	GD
Guadeloupe	GP
Guam	GU
Guatemala	GT
Guernsey	GG
Guinea	GN
Guinea-Bissau	GW

Guyana	GY
Haiti	HT
Heard Island and Mc Donald Islands	HM
Holy See (Vatican City State)	VA
Honduras	HN
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Indonesia	ID
Iran, Islamic Republic of	IR
Iraq	IQ
Ireland	IE
Israel	IL
Italy	IT
Jamaica	JM
Japan	JP
Japan1	J1
Japan2	J2
Japan3	J3
Japan4	J4
Japan5	J5
Japan6	J6
Jersey	JE
Jordan	JO
Kazakhstan	KZ
Kenya	KE
Kiribati	KI
Korea, Democratic People's Republic Of	KP
Korea Republic	KR
Korea Republic2	K2
Kuwait	KW
Kyrgyzstan	KG
Lao People's Democratic Republic	LA
Latvia	LV
Lebanon	LB
Lesotho	LS
Liberia	LR
Libyan Arab Jamahiriya	LY
Liechtenstein	LI
Lithuania	LT
Luxembourg	LU
Macao	MO
Macedonia, The Former Yugoslav Republic of	MK
Madagascar	MG
Malawi	MW
Malaysia	MY
Maldives	MV
Mali	ML

Malta	MT
Man, Isle of	IM
Marshall Islands	MH
Martinique	MQ
Mauritania	MR
Mauritius	MU
Mayotte	YT
Mexico	MX
Micronesia, Federated States Of	FM
Moldova, Republic Of	MD
Monaco	MC
Mongolia	MN
Montenegro	ME
Montserrat	MS
Morocco	MA
Mozambique	MZ
Myanmar	MM
Namibia	NA
Nauru	NR
Nepal	NP
Netherlands	NL
Netherlands Antilles	AN
New Caledonia	NC
New Zealand	NZ
Nicaragua	NI
Niger	NE
Nigeria	NG
Niue	NU
Norfolk Island	NF
Northern Mariana Islands	MP
Norway	NO
Oman	OM
Palau	PW
Palestinian Territory, Occupied	PS
Pakistan	PK
Panama	PA
Papua New Guinea	PG
Paraguay	PY
Peru	PE
Philippines	PH
Pitcairn	PN
Poland	PL
Portugal	PT
Puerto Rico	PR
Qatar	QA
Reunion	RE
Romania	RO
Russian Federation	RU
Rwanda	RW
Saint Helena	SH
Saint Kitts and Nevis	KN

Saint Lucia	LC
Saint Martin	MF
Saint Pierre and Miquelon	PM
Saint Vincent and the Grenadines	VC
Samoa	WS
San Marino	SM
Sao Tome and Principe	ST
Saudi Arabia	SA
Senegal	SN
Serbia	RS
Seychelles	SC
Sierra Leone	SL
Singapore	SG
Slovakia	SK
Slovenia	SI
Solomon Islands	SB
Somalia	SO
South Africa	ZA
South Georgia and the South Sandwich Islands	GS
Spain	ES
Sri Lanka	LK
Sudan	SD
Suriname	SR
Svalbard and Jan Mayen	SJ
Swaziland	SZ
Sweden	SE
Switzerland	CH
Syrian Arab Republic	SY
Taiwan, Province of China	TW
Tajikistan	TJ
Tanzania, United Republic of	TZ
Thailand	TH
Timor-Leste (East Timor)	TL
Togo	TG
Tokelau	TK
Tonga	TO
Trinidad & Tobago	TT
Tristan Da Cunha	TA
Tunisia	TN
Turkey	TR
Turkmenistan	TM
Turks And Caicos Islands	TC
Tuvalu	TV
Uganda	UG
Ukraine	UA
United Arab Emirates	AE
United Kingdom	GB
United States	US
United States Minor Outlying Islands	UM

Uruguay	UY
Uzbekistan	UZ
Vanuatu	VU
Venezuela	VE
Viet Nam	VN
Virgin Islands, British	VG
Virgin Islands, U.S.	VI
Wallis And Futuna	WF
Western Sahara	EH
World	XA
Yemen	YE
Yugoslavia	YU
Zambia	ZM
Zimbabwe	ZW