# Technical Details



# Base Station Specifications

The following table shows the physical and operating environment specifications for the base station.

***Table 1: Physical and Operating Specifications***

| Specification | Value or Range |
|---|---|
| Operating temperature | 32° to 113°F (0° to 45°C) |
| Operating relative humidity | 10% to 90% (noncondensing) |
| Storage temperature | 14° to 140°F (–10° to 60°C) |
| Storage relative hunidity | 10% to 95% (noncondensing) |
| Height | 4.75 in. (120 mm) |
| Width | 4.75 in. (120 mm) |
| Depth | 1.25 in (30 mm) |
| Weight | 6 oz. (167 g) |
| Cables | • Category 3/5/5e/6 for 10-Mbps cables with 4 pairs<br>• Category 5/5e/6 for 100-Mbps cables with 4 pairs |
| Distance Requirements | As supported by the Ethernet Specification, it is assumed that the maximum cable length between each base station and the switch is 100 meters (330 feet). |

| Specification | Value or Range |
|---|---|
| Power | Power adapter for local power<br>Ethernet PoE (Ethernet adaptor for normal power); IEEE 802.3: Power class 2 (3.84 – 6.49W) |
| Radio Frequency (RF) Bands | Bands are set in the factory and cannot be changed by customers.<br>• 1880 - 1895 (Taiwan)<br>•<br>• 1880 – 1900 MHz (Australia and New Zealand – reduced power 22 dBM)<br>• 1880 – 1900 MHz (E.U. and APAC)<br>• 1910 – 1930 MHz (LATAM and Argentina)<br>• 1910 – 1920 MHz (Brazil and Uruguay)<br>• 1910 – 1920 MHz (Uruguay – reduced power 140 mW)<br>• 1910 – 1930 MHz (Chile – reduced power 22 dBM)<br>• 1920 – 1930 MHz (U.S. and Canada) |

For detailed technical information about the base station, see the datasheet at:

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-dect-6800-series-multiplatform-firmware/datasheet-listing.html

## Logging of Configuration Changes of Base Station

You can record configuration changes that users make to the base station using the configuration changes logging function. In a similar manner, you may track configuration changes of a handset. In the changelog, the basic memory stores the information about which parameters is changed. However, this information does not contain the actual details of the changes; rather, it just stores specific changes made to the configuration. The changelog is cleared after the changes have been successfully reported.

## Reporting of Configuration Changes

When base station configuration changes are reported, the base station requests DECT locked handsets for changelogs. The base station sends three requests, one every five seconds, for each locked handset. Once requests for all handsets are complete, the changelogs of the base and the handsets are collected, processed, transformed to the correct XML tags. Then these tags are sent to the configuration server. If a handset doesn't respond, the syslog records this behavior. The handset changelogs from the device are cleared only after successful delivery of it to a base station.

# Handset Specifications

The following table shows the physical and operating environment specifications for the handsets.

*Table 2: Physical and Operating Specifications*

| Specification | Value or Range |
|---|---|
| Operating temperature | 32° to 113°F (0° to 45°C) |
| Operating relative humidity | 10% to 90% (noncondensing) |
| Storage temperature | 14° to 140°F (–10° to 60°C) |
| Storage relative humidity | 10% to 95% (noncondensing) |
| Height | 6825 Handset: 4.6 in. (117 mm)<br>6825 Ruggedized Handset: 4.6 in. (117 mm)<br>6823 Handset: 4.82 in. (122 mm) |
| Width | 6825 Handset: 1.8 in. (46 mm)<br>6825 Ruggedized Handset: 1.8 in. (46 mm)<br>6823 Handset: 1.99 in. (51mm) |
| Depth | 6825 Handset: 0.78 in. (20 mm)<br>6825 Ruggedized Handset: 0.78 in. (20 mm)<br>6823 Handset: 0.91 in. (23 mm) |
| Weight | 6825 Handset: 3 oz. (86 g)<br>6825 Ruggedized Handset: 3 oz. (86 g)<br>6823 Handset: 3.17 oz. (90 g) |
| Power | Rechargeable Lithium ion battery. |

For detailed technical information about the handsets, see the datasheet at:

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-dect-6800-series-multiplatform-firmware/datasheet-listing.html

# Network Protocols

Cisco handsets and base stations support several industry-standard and Cisco network protocols that are required for voice communication. The following table provides an overview of the network protocols that the handsets and base stations support.

*Table 3: Supported Network Protocols*

| Network Protocol | Purpose | Usage Notes |
|---|---|---|
| Bootstrap Protocol (BootP) | BootP enables a network device, such as the handset, to discover certain startup information, such as its IP address. | — |

| Network Protocol | Purpose | Usage Notes |
|---|---|---|
| Cisco Discovery Protocol (CDP) | CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment.<br>A device can use CDP to advertise its existence to other devices and receive information about other devices in the network.<br>The Native VLAN type of the CDP can be used to obtain the VLAN network information. | The device uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch. |
| Domain Name Server (DNS) | DNS translates domain names to IP addresses. | The base station has a DNS client to translate domain names into IP addresses. |
| Dynamic Host Configuration Protocol (DHCP) | DHCP dynamically allocates and assigns an IP address to network devices.<br>DHCP enables you to connect a base station into the network and have the base station become operational without the need to manually assign an IP address or to configure additional network parameters. | DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, and gateway on each base station locally.<br>We recommend that you use the DHCP custom option 160, 159. |
| Hypertext Transfer Protocol (HTTP) | HTTP is the standard protocol for transfer of information and movement of documents across the Internet and the web. | The base station uses HTTP for XML services, provisioning, upgrade, and for troubleshooting purposes. |
| Hypertext Transfer Protocol Secure (HTTPS) | HTTPS is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers. | Web applications with both HTTP and HTTPS support have two URLs configured. Base stations that support HTTPS choose the HTTPS URL.<br>A lock icon is displayed to the user if the connection to the service is via HTTPS. |
| Internet Protocol (IP) | IP is a messaging protocol that addresses and sends packets across the network. | To communicate with IP, network devices must have an assigned IP address, subnet, and gateway.<br>IP addresses, subnets, and gateways identifications are automatically assigned if you are using the base station with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each base station locally. |

| Network Protocol | Purpose | Usage Notes |
|---|---|---|
| Link Layer Discovery Protocol (LLDP) | VLAN network information can be collected from the LLDP from numerous subtypes of the type 127. In this implementation, the information will be taken from one of two subtypes, which are prioritised as follows:<br>**1.** IEEE – PORT VLAN ID<br>**2.** Network Policy | |
| Network Time Protocol (NTP) | NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. | The base station uses NTP to communicate with the time server. |
| Real-Time Transport Protocol (RTP) | RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks. | The base station uses the RTP protocol to send and receive real-time voice traffic from other devices and gateways. |
| Real-Time Control Protocol (RTCP) | RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams. | RTCP is disabled by default. |
| Session Description Protocol (SDP) | SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support. | SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by a Third-Party Call Control System or a Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself. |
| Session Initiation Protocol (SIP) | SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints. | Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call. |
| Secure Real-Time Transfer protocol (SRTP) | SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints. | Handsets and base stations use SRTP for media encryption. |
| Transmission Control Protocol (TCP) | TCP is a connection-oriented transport protocol. | — |

| Network Protocol | Purpose | Usage Notes |
|---|---|---|
| Transport Layer Security (TLS) | TLS is a standard protocol for securing and authenticating communications. | When security is implemented, the base station uses the TLS protocol when securely registering with the third-party call control system. |
| Trivial File Transfer Protocol (TFTP) | TFTP allows you to transfer files over the network.<br>On the base station, TFTP enables you to obtain a configuration file specific to the phone type. | TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. |
| User Datagram Protocol (UDP) | UDP is a connectionless messaging protocol for delivery of data packets. | UDP is used only for RTP streams. SIP uses UDP, TCP, and TLS. |

## Reset the Network VLAN

When the advertisement discovery packages arrive, they are monitored and analysed, and the network information contained in them is compared to previous packages. If the VLAN changes, the DECT base must reboot and reconnect to complete a new network initialization.

# SIP Configuration

## SIP and the Cisco IP DECT Phone

The Cisco IP DECT Phone use Session Initiation Protocol (SIP), which allows interoperation with all IT service providers that support SIP. SIP is an IETF-defined signaling protocol that controls voice communication sessions in an IP network.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

In typical commercial IP telephony deployments, all calls go through a SIP Proxy Server. The receiving handset is called the SIP user agent server (UAS), while the requesting handset is called the user agent client (UAC).

SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response routes back to the UAS, and the two user agents connect using a direct peer-to-peer session. Voice traffic transmits between user agents over dynamically assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; RTP does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of UDP.

## SIP over TCP

To guarantee state-oriented communications, the Cisco IP DECT Phone can use TCP as the transport protocol for SIP. This protocol provides *guaranteed delivery* that assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

## SIP Proxy Redundancy

An average SIP Proxy Server can handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. The base station supports the use of backup servers to minimize or eliminate service disruption.

A simple way to support proxy redundancy is to specify a SIP Proxy Server in the base station configuration profile. The base station sends a DNS NAPTR or SRV query to the DNS server. If configured, the DNS server returns SRV records that contain a list of servers for the domain, with their hostnames, priority, listening ports, and so on. The base station tries to contact the servers in the order of the priority. The server with a lower number has a higher priority. Up to six NAPTR records and twelve SRV records are supported in a query.

When the base station fails to communicate with the primary server, the base station can failover to a lower-priority server. If configured, the base station can restore the connection back to the primary. Failover and failback support switches between servers with different SIP transport protocols. The base station doesn't perform failback to the primary server during an active call until the call ends and the failback conditions are met.

### Example of Resource Records from the DNS Server

```
sipurash     3600    IN NAPTR 50   50  "s"  "SIPS+D2T"     ""  _sips._tcp.tlstest
             3600    IN NAPTR 90   50  "s"  "SIP+D2T"      ""  _sip._tcp.tcptest
             3600    IN NAPTR 100  50  "s"  "SIP+D2U"      ""  _sip._udp.udptest

_sips._tcp.tlstest  SRV 1 10 5061 srv1.sipurash.com.
                    SRV 2 10 5060 srv2.sipurash.com.
_sip._tcp.tcptest   SRV 1 10 5061 srv3.sipurash.com.
                    SRV 2 10 5060 srv4.sipurash.com.
_sip._udp.udptest   SRV 1 10 5061 srv5.sipurash.com.
                    SRV 2 10 5060 srv6.sipurash.com.

srv1     3600    IN    A   1.1.1.1
srv2     3600    IN    A   2.2.2.2
srv3     3600    IN    A   3.3.3.3
srv4     3600    IN    A   4.4.4.4
srv5     3600    IN    A   5.5.5.5
srv6     3600    IN    A   6.6.6.6
```

The following example shows the priority of the servers from the perspective of the base station.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS            UP
2nd            2.2.2.2            TLS            UP
3rd            3.3.3.3            TCP            UP
4th            4.4.4.4            TCP            UP
5th            5.5.5.5            UDP            UP
6th            6.6.6.6            UDP            UP
```

The base station always sends SIP messages to the available address with the top priority and with the status UP in the list. In the example, the base station sends all the SIP messages to the address 1.1.1.1. If the address 1.1.1.1 in the list is marked with the status DOWN, the base station communicates with 2.2.2.2 instead. The base station can restore the connection back to 1.1.1.1 when the specified failback conditions are met. For

more details about failover and failback, see SIP Proxy Failover, on page 8 and SIP Proxy Fallback, on page 9.

## SIP Proxy Failover

The base station performs a failover in any of these cases:

- **Fast Response Timer expiry**: In RFC3261 the two transactions timers, TIMER B and TIMER F defines when an INVITE transaction and a Non-INVITE transaction has expired respectively. These are configurable with a default value of 5 sec. When one of these timers expires, and the corresponding SIP transaction fails, failover is triggered. In-dialog requests does not trigger failover.
- **SIP 5xx Response Codes:** If the server responds with a 5xx response to a SIP request, failover is triggered.
- **TCP disconnect:** If the remote server disconnects the TCP connection (ex. TCP RST or TCP FIN), failover is triggered.

We strongly recommend that you set the **Failback before Failover** to **Enabled** when **SIP Transport** is set to **Auto**.

You can also configure this extension-specific parameters in the configuration file (`.xml`):

```
<SIP_Transport_n_>Auto</SIP_Transport_n_>
<Srv_Failback_Before_Failover_n_>Yes</Srv_Failback_Before_Failover_n_>
```

Where, `n` is the extension.

### Base Station Failover Behavior

When the base station fails to communicate with the currently connected server, it refreshes the server list status. The unavailable server is marked with the status DOWN in the server list. The base station tries to connect to the top-priority server with the status UP in the list.

In the following example, the addresses 1.1.1.1 and 2.2.2.2 aren't available. The base station sends SIP messages to 3.3.3.3, which has the top priority among the servers with the status UP.

```
Priority        IP Address      SIP Protocol    Status
1st             1.1.1.1             TLS          DOWN
2nd             2.2.2.2             TLS          DOWN
3rd             3.3.3.3             TCP          UP
4th             4.4.4.4             TCP          UP
5th             5.5.5.5             UDP          UP
6th             6.6.6.6             UDP          UP
```

In the following example, there are two SRV records from the DNS NAPTR response. For each SRV record, there are three A records (IP addresses).

```
Priority        IP Address      SIP Protocol    Server          Status
1st             1.1.1.1             UDP         SRV1            DOWN
2nd             1.1.1.2             UDP         SRV1            UP
3rd             1.1.1.3             UDP         SRV1            UP
4th             2.2.2.1             TLS         SRV2            UP
5th             2.2.2.2             TLS         SRV2            UP
6th             2.2.2.3             TLS         SRV2            UP
```

Let's assume that the base station failed to connect to 1.1.1.1 and then registered to 1.1.1.2. When 1.1.1.2 goes down, base station behavior depends on the setting of **Proxy Fallback Intvl**.

- When **Failover SIP Timer B** is set to **0**, the base station tries with the addresses in this order: 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.
- When **Failover SIP Timer B** is set to a value other than zero, the base station tries with the addresses in this order: 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.

## SIP Proxy Fallback

The proxy fallback requires that the field **Failback before Failover** in the **Server** web page is set to **Enabled**. If you set this field to **Disabled**, the SIP proxy failback feature is disabled. You can also configure this extension-specific parameter in the configuration file (`.xml`) in this format:

```
<Srv_Failback_Before_Failover_n_>yes</Srv_Failback_Before_Failover_n_
```

Where, `n` is the extension number.

The time when the base station triggers a failback depends on the configuration and the SIP transport protocols in use.

To enable the base station to perform failback between different SIP transport protocols, set **SIP Transport** to **Auto** on the **Servers** web page. You can also configure this extension-specific parameter in the configuration file (`.xml`) with the following XML string:

```
<SIP_Transport_@SRVIDX_>AUTO</SIP_Transport_@SRVIDX_>
```

Where, `n` is the server index.

### Failback from a UDP Connection

The failback from a UDP connection is triggered by SIP messages. In the following example, the base station first failed to register to 1.1.1.1 (TLS) at the time T1 since there's no response from the server. When SIP Timer F expires, the base station registers to 2.2.2.2 (UDP) at the time T2 (T2=T1+SIP Timer F). The current connection is on 2.2.2.2 via UDP.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS          DOWN        T1 (Down time)
2nd            2.2.2.2            UDP          UP
3rd            3.3.3.3            TCP          UP
```

The base station has the following configuration:

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

where *n* is the extension number.

The base station refreshes the registration at time T2 (T2=(3600-16)*78%). The base station checks the address list for the availability of the IP addresses and the down time. If T2-T1 > = 60, the failed server 1.1.1.1 resumes back to UP and the list is updated to the following. The base station sends SIP messages to 1.1.1.1.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS           UP
2nd            2.2.2.2            UDP           UP
3rd            3.3.3.3            TCP           UP
```

## Failover and Recovery Registration

- Failover—The base station performs a failover when transport timeout/failure or TCP connection failures; if **Failover SIP Timer B** and **Failover SIP Timer F** values are datafilled.
- Recovery—The base station attempts to reregister with the primary proxy while registered or actively connected to the secondary proxy.

  Auto register when failover parameter controls the failover behavior when there is an error. When this parameter is set to yes, the base station re-registers upon failover or recovery.

### Fallback Behavior

The fallback occurs when the current registration expires or Proxy Fallback Intvl fires.

If the Proxy Fallback Intvl is exceeded, all the new SIP messages go to primary proxy.

For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback triggers 600 seconds later.

When the value for Register Expires is 800 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback triggers at 800 seconds.

After successful registration back to the primary server, all SIP messages go to the primary server.

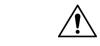
# External Devices

We recommend that you use good-quality external devices that are shielded against unwanted radio frequency (RF) and audio frequency (AF) signals. External devices include headsets, cables, and connectors.

Depending on the quality of these devices and their proximity to other devices, such as mobile phones or two-way radios, some audio noise may still occur. In these cases, we recommend that you take one or more of these actions:

- Move the external device away from the source of the RF or AF signals.
- Route the external device cables away from the source of the RF or AF signals.
- Use shielded cables for the external device, or use cables with a better shield and connector.
- Shorten the length of the external device cable.
- Apply ferrites or other such devices on the cables for the external device.

Cisco cannot guarantee the performance of external devices, cables, and connectors.



**Caution** In European Union countries, use only external speakers, microphones, and headsets that are fully compliant with the EMC Directive [89/336/EC].