Mitel IP Sets

ENGINEERING GUIDELINES

Version 3.2

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel”) or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Mitel IP Sets Engineering Guidelines
Version 3.2

List of Tables

List of Figures

About This Document

These guidelines will be of assistance to individuals who are planning for the installation of Mitel IP phones. These guidelines discuss topics that need to be considered prior to deploying IP phones.

In addition to these guidelines, there are several other documents available that discuss IP phone features, installation and operation. When planning an installation, the other IP phone related documents should also be referenced. These documents can be found on Mitel's Document Centre and are highlighted under the section called Additional Information.

This document is Call Control agnostic - it does not discuss Call Control servers, Call Directors or PBXs in detail. For IP phone information that is specific to a particular Call Control server, refer to the appropriate Call Control server documents.

Changes to the Mitel IP Phone Engineering Guidelines

New in This Document Version

This document includes the following updates:

- MiVoice Business now supports a Class of Service (CoS) option that can be used to disable the Bluetooth interface on the 6930, 6940 and 6970 IP sets on a per DN basis.
- Support for Ray Baum Legislation: Some Teleworker phones (phones deployed behind an MBG) now have the ability to detect a change in the gateway MAC address and can now report the change of location to the MiVoice Business.

Overview

Mitel offers a comprehensive line of business IP desktop devices (MiNET and SIP based), everything from affordable, entry-level phones to sophisticated IP phones and devices with cordless handsets, conference units, and attendant consoles.

Additional Information

This document covers engineering guidelines for the 50xx, 52xx, 53xx, and 69xx series of IP MiNET phones as well as a number of specialized phones and consoles.

This document discusses cabling, power and also some networking information for the 67xx, 68xx and 69xx series of SIP phones, more extensive information may be found on Mitel's Document Center web site.

> **Note:** The 6900 series of IP phones can operate in MiNET mode or in SIP mode. This document discusses several aspects of the 6900 phones when operating in either mode, however for information regarding the administration of the 6900 sets, there are separate documentation suites for MiNET and for SIP. The Administrator should refer to the relevant Administration guides depending on whether the phones are operating in MiNET mode or SIP mode.
>
> For administration information related to the 6800 /6900 Series of SIP Phones, refer to the *6800/6900 Series SIP Phones Administrator Guide* which may be found on Mitel's Document Center.
>
> For administration information related to the 6900 Series of MiNET Phones, refer to the *MiVoice 6900 Series IP Phones Administrator Guide* which may be found on Mitel's Document Center.

For documentation related to other products such as SIP-DECT phones, IP-DECT phones, Conference and video phones, IP consoles and Digital desktop phones see the Mitel Document Center web site.

All IP phones and consoles are supported with additional documentation such as administration guides, user guides and data sheets. See the Mitel Document Centre web site or the Mitel InfoChannel web site for this additional information.

The following documentation related to comparing and selecting IP phones and peripherals is available at the Mitel Document Centre:

- Mitel IP Desktop Phones and Peripherals Feature Matrix
- Mitel IP Desktop Phones and Peripherals Brochure
- IP Desktop FAQ
- IP Phone Product Briefs
- Product Bulletins

The following tools related to network powering of IP phones are available:

- MiVoice Business System Engineering Tool found at the Mitel Document Centre.
- Mitel Streamline Power Calculator found at the Mitel Document Centre.

The following documentation is related to deploying IP phones and can be found at the Mitel Document Centre:

- Network Engineering for IP Telephony
- Wireless Telephony, Planning and Troubleshooting
- Ethernet Twisted Pair Cabling Plant, Power and Grounding Guidelines

67xx and 68xx Phones Series

The 6700 and 6800 series of phones are SIP only devices. Documentation for the 67xx and the 68xx families of Phones can be found on the Mitel Document Centre web site. Included on the Document Center are User Guides, Set and Administration Guides, Declarations and software downloads. Data sheets may be found at the Mitel Document Center web site or the Mitel InfoChannel web site.

IP Phones and Ethernet Cabling

Note: For security reasons an IP phone or an IP conference phone should never be connected directly to the internet. The IP phone or IP conference should always reside behind an appropriate firewall so that firewall rules can be used to protect the phone from malicious attacks.

Mitel’s desktop IP phones are designed to connect to an IEEE 802.3 compliant Twisted Pair Ethernet LAN.

There are several different IEEE 802.3 Twisted Pair Ethernet LAN standards in existence; the primary difference between these standards is the maximum supported data transmission speed, see Table 1 IEEE 802.3 Standards.

The Telecommunications Industry Association (TIA) created a set of telecommunications standards which are referred to as TIA/EIA-568, these standards address cabling for telecommunications products and services.

The TIA/EIA-568 standards specify the parameters that Twisted Pair cabling plant must meet to comply with to support a given data transmission speed. The TIA/EIA-568 standard places cabling plant technology into different cabling Categories (CAT), these Categories align with the maximum supported data transmission speed as shown in the following Table 1 IEEE 802.3 Standards.

Table 1 IEEE 802.3 Standards

IEEE 802.3 STANDARD	ALTERNATE NAME	MAXIMUM TRANSMISSION SPEED	MINIMUM REQUIRED CABLING PLANT CATEGORY (CAT)
802.3i	10BASE-T	10 Mb/s	CAT-3
802.3u	100BASE-T (Fast Ethernet)	100 Mb/s	CAT-5
802.3ab	1000BASE-T (Giga Bit Ethernet)	1000 Mb/s	Cat-5 or better (CAT-5e) Note 1

Note: CAT-5 installations should be tested and certified for 1000 BASE-T Operation.

The majority of Mitel IP phones support both 10BASE-T and 100BASE-T operation and will auto-negotiate their speed of operation. Mitel also has a number of phones and accessories that support 10BASE-T, 100BASE-T and 1000BASE-T operation and will auto-negotiate their speed of operation.

To determine which IEEE 802.3 standard(s) a phone supports, consult the IP phone data sheet. Data sheets can be found on Mitel’s Document Centre or Mitel’s InfoChannel web site.

Cabling Plant, PoE Considerations

The IEEE 802.3at Power over Ethernet (PoE) standard allows for higher power delivery to the end point than is allowed under the IEEE 802.2af PoE standard. As a result of increased power capabilities, IEEE 802.3at PoE deployments should be made only on CAT-5 (or better) cabling plant. CAT-3 cable has a higher DC resistance per meter than CAT-5 cable; as a result, given the same length of cable, CAT-5 cable can carry higher currents than CAT-3 cable.

> **Note:** CAT-3 cable is acceptable only for IEEE 802.3af PoE deployments.

Ethernet Cabling Plant, Finding Additional information

The Mitel Technical Paper *Ethernet Twisted Pair Cabling Plant, Power and Grounding Guidelines* provides detailed information on cable types, allowable distances, structured wiring practices and connectorization standards. This Technical Paper can be found at the Mitel Document Center.

When the Cabling Plant does not meet the Required Standards

The TIA/EIA-568 standard specifies several cable and transmission line characteristics for the various categories of twisted pair cabling so that signal integrity will be assured.

The IEEE 802.3 standards specify that the twisted pair Ethernet LAN cable cannot exceed 100 meters (328’) in length between stations. This cable length limitation is in place to guarantee the received signal’s integrity and to satisfy protocol timers.

Two IEEE Power over Ethernet standards (IEEE 802.1af and IEEE 802.3at) also specify that cable length cannot exceed 100 meters (328’). This cable length limitation is in place to ensure that adequate power can be delivered over the twisted pair cable to a device such as an IP phone.

There may be situations where the Customer’s existing cabling plant does not comply with the above-mentioned standards, for instance the cabling may exceed the maximum allowable distance of 100 meters (328’), or the cabling plant may be designed to a transmission standard that is less stringent than the minimum required CAT-3 standard, for example - British Telecom’s CW1308 cabling standard.

Sometimes the Customer may be unable to upgrade their wiring plant to comply with the TIA/EIA-568 standard. This could be due to costs that are prohibitive, historical building restrictions or the risk of disturbing hazardous building materials. Also, some portions of the cabling plant may need to cover a distance greater than 100 meters (328’).

In situations such as these, where the cabling plant is not TIA/EIA-568 compliant and an upgrade of the cabling plant to meet the TIA/EIA-568 standard is not feasible, a Mitel Streamline switch could provide a suitable solution.

The Mitel Streamline family of Ethernet LAN switches allows Ethernet devices to operate over some twisted pair cabling plant that does not meet the transmission line standards, or a length of cable that exceeds 100 meters (328’).

If the IP phone is being powered locally, the Streamline switch may be used to just provide data connectivity to the IP phone. However, if remote phone powering is preferred, the Streamline switch can also provide power to most IEEE 802.2af compliant IP phones over distances greater than 100 meters (328’).

For more information refer to the Mitel Streamline documentation, the documents can be found on Mitel’s Document Centre.

> **Note:** The StreamLine switches support PoE to IEEE 802.3af Class 1 and Class 2 end points. Some Class 3 end points are also supported, but the Powered Device (PD) must be rated at 10 Watts or less.

Powering IP Phones

Depending on the model of phone, power may be provided to the IP phone either locally by an AC to DC power adapter, or remotely by a network device or network switch that supports Power over Ethernet (PoE). To determine which powering options are available for a particular model of phone, refer to Table 2 IP Phone Powering Options and PoE Standards - Listed by Phone Model Number.

When planning IP phone installations there are several factors that should be taken into consideration, for example:

- Is it necessary that the IP phone remain operational during a mains power outage? If this is the case, then a centralized PoE solution combined with an Uninterruptible Power Supply (UPS) should be considered.
- Is there an AC power outlet in close proximity to where the phone will be installed? If an AC outlet is not in close enough proximity, PoE should be considered.
- If the phone is to be powered locally by an AC adapter, is the AC power outlet part of a branch circuit that is reliable. Could the AC branch circuit breaker be tripped accidentally by personnel overloading the circuit with other devices or could the phone’s AC adapter be inadvertently unplugged. If the reliability of the AC circuit is questionable, consider using PoE.

Recommended Phone Powering Practices

Even though IP phones may be powered locally with an AC mains adapter or with an in-line Ethernet power adapter, Power over Ethernet (PoE) provided from PoE Ethernet L2 switch located in a central location such as a wiring closet is recommended whenever possible, resulting in the following benefits:

- IP phone power can be made redundant with UPS systems allowing IP phones and related infrastructure to remain operational during a mains power outage, this capability is especially important for emergency 911 capabilities
- Power savings - using PoE is generally more energy efficient than using AC mains adapters
- Lower installation costs (existing cabling can be used)
- Remote reset and power-off capability
- Remote power management and monitoring capability, most PoE switches support SNMP capabilities

> **Note:** To ensure proper operation, avoid connecting an IP phone to both local and remote power sources simultaneously. An IP phone that is locally powered, either through an AC or an Ethernet power adapter, should not receive power from a remote location. Refer to the L2 PoE Switch vendor's documentation for information on disabling PoE for a particular port.

IP Phones - Available Powering Options

This section provides details on which powering options are available for a particular model of IP phone and which PoE standards a phone is compliant with.

Table 2 IP Phone Powering Options and PoE Standards - Listed by Phone Model Number

Phones	In-Line Ethernet AC Power Adapter (48 VDC LAN)	AC Power Adapter (24 VDC)	Power Dongle (Cisco-Compliant)	AC Power Adapter (48 VDC)	IEEE 802.3at Compliant	IEEE 802.3af Compliant
5001	Yes	No	Yes	No	No	Yes
5005	Yes	No	Yes	No	No	Yes
5055 (SIP)	Yes	Yes	Yes	No	No	Yes
5010	Yes	Yes	Yes	No	No	Yes
5020	Yes	Yes	Yes	No	No	Yes
5201	Yes	No	Yes	No	No	Yes
5205	Yes	No	Yes	No	No	Yes
5207	Yes	No	Yes	No	No	Yes
5212	Yes	No	Yes	No	No	Yes
5215	Yes	No	Yes	No	No	Yes
5215 Dual Mode	Yes	No	Yes	No	No	Yes
5220	Yes	Yes	Yes	No	No	Yes
5220 Dual Mode	Yes	Yes	Yes	No	No	Yes
5224	Yes	Yes	Yes	No	No	Yes
5230	Yes	No	Yes	No	No	Yes
5235	Yes	No	Yes	No	No	Yes
5140	Yes	Yes	Yes	No	No	Yes
5240	Yes	Yes	Yes	No	No	Yes
5302	Yes	No	No	No	No	Yes
5304	Yes	No	No	No	No	Yes

Phones	In-Line Ethernet AC Power Adapter (48 VDC LAN)	AC Power Adapter (24 VDC)	Power Dongle (Cisco-Compliant)	AC Power Adapter (48 VDC)	IEEE 802.3at Compliant	IEEE 802.3af Compliant
5312	Yes	No	Yes	No	No	Yes
5324	Yes	No	Yes	No	No	Yes
5320	Yes	No	No	No	No	Yes
5320e	Yes	No	No	No	No	Yes
5330	Yes	No	Yes	No	No	Yes
5330e	Yes	No	Yes	No	No	Yes
5340	Yes	No	Yes	No	No	Yes
5340e	Yes	No	Yes	No	No	Yes
5360	Yes, though note that the only power supply approved for use is: Mitel Part # 51015131)	No	No	No	No	Yes (Power Hub must support Gigabit Ethernet and must be 802.3af compliant)
5505	Yes	No	No	No	No	Yes
5485 IP Pager	No	Yes	No	No	No	No
5540	Yes	No	No	No	No	Yes
5550-TKB (5550 IP Console)	No	Yes	No	No	No	No
5560 IPT (Note 3)	Yes	No	No	No	No	Yes
Navigator	Yes	No	Yes	No	No	Yes
TeleMatrix 3000IP	Yes	No (Note 1)	Yes	No	No	Yes

Phones	In-Line Ethernet AC Power Adapter (48 VDC LAN)	AC Power Adapter (24 VDC)	Power Dongle (Cisco-Compliant)	AC Power Adapter (48 VDC)	IEEE 802.3at Compliant	IEEE 802.3af Compliant
Gigabit Ethernet Phone Stand	No	No (An AC to 48VDC power adapter is provided with this unit)	No	No	No	Yes (Power Hub must support Gigabit Ethernet and must be 802.3af compliant)
Wireless LAN Phone Stand	No	No (An AC to 48VDC power adapter is provided with this unit)	No	No	No	No
MiVoice Video/Conference	(See Note 2)	No	No	No	Yes	No
6731i	Yes	No	No	Yes	No	Yes
6735i	Yes	No	No	Yes	No	Yes
6737i	Yes	No	No	Yes	No	Yes
6739i	Yes	No	No	Yes	No	Yes
6863i	Yes	No	No	Yes	No	Yes
6865i	Yes	No	No	Yes	No	Yes
6867i	Yes	No	No	Yes	No	Yes
6869i	Yes	No	No	Yes	No	Yes
6873i	Yes	No	No	Yes	Yes	Yes
6905	Yes	No	Yes	Yes	Yes	Yes
6910	Yes	No	Yes	Yes	Yes	Yes
6920	Yes	No	Yes	Yes	Yes	Yes
6930	Yes	No	No	Yes	Yes	Yes

Phones	In-Line Ethernet AC Power Adapter (48 VDC LAN)	AC Power Adapter (24 VDC)	Power Dongle (Cisco-Compliant)	AC Power Adapter (48 VDC)	IEEE 802.3at Compliant	IEEE 802.3af Compliant
6940	Yes	No	No	Yes	Yes	Yes
6970	Yes	No	N/A	No	Yes	Yes

> **Note 1:** Refer to TeleMatrix 3000IP Technical documentation for details.
>
> **Note 2:** The MiVoice Video/Conference must be powered from an IEEE 802.3at compliant PoE source, for details refer to the MiVoice Video/Conference Engineering Guidelines.
>
> **Note 3:** For additional information refer Powering the 5560 IPT.
>
> **Note 4:** For additional information pertaining to the 67xx and 68xx series of phones, refer to the 67xx and 68xx product documentation found on Mitel's Document Centre.

Powering Phones with Local Power

Depending on the model, the IP phone can be powered locally with the following methods:

- With an AC mains power adapter that converts mains voltage into the 24 VDC required by the phone.
- With an AC mains power adapter that converts mains voltage into the 48 VDC required by the phone.
- With a special in-line Ethernet power adapter called an in-line Ethernet power injector, this adapter converts mains voltage into 48 VDC, injects the 48 VDC power into the Ethernet cable and the phone obtains its power from the Ethernet cable.

Refer to Table 2 IP Phone Powering Options and PoE Standards - Listed by Phone Model Number, to determine which powering options are available for a particular phone.

AC Power Adapters

These adapters plug into a mains outlet and convert the mains voltage to a DC voltage for the phones.

24 VDC Power Supplies:

Phones that require 24 VDC (see Table 2) are shipped with an AC to DC power adapter (24 VDC), which has a 3 meter (10 ') power cord. If a longer power cord is required, Part Number 57004243 may be used (universal AC input, 24 VDC, 4.5 meter, (15 ') power cord).

For further information on AC power adapters, refer to the appropriate Mitel phone data sheet.

48 VDC Power Supplies:

The 69xx series of IP phones may use the following AC to DC power adapters:

- 50006814 - AC Adapter L6 48V Universal

- 50006822 - AC Adaptor L6 48V NA (North America)
- 50006824 - AC Adaptor L6 48V EU (Europe)

The following AC power adapters are for the 6800 and 6900 series of IP phones. They will provide power for all 6800 and 6900 IP phone configurations e.g. sets configured with PKMs, or DECT accessories.

50006924	6800/6900 AC UK/AU/BR/CN (QTY10)
50008236	6800/6900 AC Adapter NA (QTY10)
50008235	6800/6900 AC Adapter EU (QTY 10)

For further information on AC power adapters, refer to the appropriate Mitel phone data sheet.

In-Line Ethernet AC Power Adapters

In-Line Ethernet power adapters (injectors) can provide a local power feed to a wide range of PoE capable Mitel IP Phones. Refer to Table 2 IP Phone Powering Options for details on which models support this powering option.

The power adapter plugs into a standard AC mains power outlet and has two RJ-45 connections, one for connecting to the network, and the other for providing a LAN connection and power feed to the phone. Available units are listed below:

For the 50xx, 52xx, and 53xx series of IP phones:

- 50002070 - 48 VDC Ethernet Power Adapter NA 120 V 50-60 Hz
- 50002080 - 48 VDC Ethernet Power Adapter UK 240 V 50 Hz
- 50002090 - 48 VDC Ethernet Power Adapter Europe 240 V 50 Hz.

For the 5360 IP phone:

If the installer chooses to power the 5360 phone locally, then the following in-line Ethernet adapter must be used as it is the only adapter approved for use with the 5360 phone.

- 51015131: 802.3af 48 VDC Gb Ethernet Power Adapter Universal, 100-240 V 50-60 Hz

For the 68xx and 69xx series of IP phones:

- 51301151 - Gb 802.3at Power Adapter Universal 90-264 VAC

> **Note:** 802.3af PoE adapters will power devices that require up to 12.95 watts and 802.3at PoE adapters will power devices that require up to 25.5 watts. Within the 68xx/69xx series of sets there are some sets that require 802.3af PoE adapters and other sets that require 802.3at PoE adapters. **The simplest solution is to use 802.3at power adapters for all 68xx/69xx sets, this will ensure that all sets are correctly powered.**

> **Note:** Ensure that In-Line Ethernet power adapters and the associated IP phones are co-located; In-Line Ethernet power adapters are not suitable for use over long lengths of cable.

Powering Specialized Devices

Powering the 5560 IPT

The 5560 IPT is equipped with two Ethernet ports labeled LAN 1 and LAN 2. These ports comply with the IEEE 802.3af Power over Ethernet (PoE) standard. The port labeled LAN 2 is not currently used for data connectivity; however, this port does support PoE.

For data connectivity, the 5560 IPT should only be connected to LAN equipment via the port labeled LAN 1.

The following methods can be used to provide PoE to the 5560 IPT:

- Non-Redundant PoE: The 5560 IPT can be powered from a single PoE compliant L2 switch through either of the two Ethernet ports.
- Redundant PoE: Providing redundant PoE supplies is accomplished by connecting both of the 5560 IPT's Ethernet ports to PoE compliant L2 switches. The 5560 IPT will draw power from both the LAN 1 and the LAN 2 connections. In the event that there is a power failure on one of the LAN ports the 5560 IPT will continue to be powered from the remaining LAN port.

Powering the 5550 IP Console and the 5310 IP Conference Unit

The 5550 IP Console and the 5310 IP Conference Unit can only be powered with AC adapters that provide a 24 VDC output.

> **CAUTION:** To prevent damage do not use PoE or an In-Line Ethernet AC Power Adapter to power either of these devices.

Powering Phones with Remote Power

PoE (Power over Ethernet) is a technology that is used for providing power to IP phones over the Ethernet wiring that the phones use for connecting to the LAN. There are both proprietary and open standard methods of providing PoE to IP connected devices; the methods listed below are discussed in detail in the following sections:

- Some Mitel IP phone installations may require the use of the Mitel 3300 Power Dongle so that they can operate with an older proprietary method.
- Some Mitel IP phone installations will require the use of a Mitel Streamline switch - which is proprietary - so that they can operate over non-compliant wiring plant.
- Mitel IP phones comply with either the IEEE 802.3af PoE standard or the IEEE 802.3at PoE standard. Remote PoE for these phones can be provided from 3rd party IEEE 802.3af or IEEE 803.2at compliant L2 Ethernet switches.

> **Note:** In situations where the phone supports the IEEE 802.3af or IEEE 802.3at Power over Ethernet standard, but the Customer's existing Ethernet switch does not support the IEEE 802.3af or IEEE 802.3at power standard, a midspan IEEE 802.3af or IEEE 802.3at power hub can be used to remotely supply power to the phone over the Ethernet cabling. The mid-span power hub resides between the non-PoE Ethernet switch and the IP phone.

Mitel 3300 Power Dongle (Cisco Compliant)

Certain older Cisco network switches are capable of providing power but are not fully IEEE 802.3af compliant. In this instance, a separate 3300 Power Dongle (Cisco-compliant) can be used to get powered operation. The 3300 Power Dongle (Cisco-compliant) may not be required when powering Mitel phones behind a Cisco Catalyst 4500/6500. For this to be the case, you must ensure you are using an 802.3af-compliant version of the 4500/6500 switch.

Mitel Streamline - When the Cable Plant is Non-Compliant

The IEEE 802.1af and IEEE 802.3at PoE standards are both designed to work over a maximum cable length of 100 meters (328'). When power and connectivity need to be provided to an IP phone over cable lengths greater than 100 meters (328'), a Mitel Streamline switch may be used as a PoE source, providing the IP phone does not require more than 10 watts of power.

The Streamline switch can also be used to provide power and connectivity to IP phones over cabling plant that does not comply with the TIA/EIA-568 standards.

> **Note:** The StreamLine switches support PoE to IEEE 802.3af Class 1 and Class 2 end points. Some Class 3 end points are also supported, but the Powered Device (PD) must be rated at 10 Watts or less.

The Mitel Streamline PoE switches use a proprietary mechanism for delivering PoE to devices over cable lengths that exceed 100 meters (328'). For information on the Mitel Streamline Switch family, refer to the product documentation found on Mitel's Document Centre, and also the section called - *When the Cabling Plant does not meet the Required Standards.*

IEEE 802.3af and IEEE 802.3at PoE Standards

The IEEE 802.3af and IEEE 802.3at PoE standards allow devices such as IP phones to receive power as well as data over a TIA/EIA-568 compliant twisted pair Ethernet LAN infrastructure.

IEEE 802.3af PoE

The original IEEE standard for Power over Ethernet is IEEE 802.3af. This standard allowed for a maximum of 12.95 watts of power to be delivered to an end device such as an IP phone.

IEEE 802.3at PoE

The IEEE 802.3at PoE standard was introduced to accommodate end points that require more power than was allowed under the IEEE 802.3af standard. The newer IEEE 802.3at standard allows for a maximum of 25.5 watts to be delivered to an end point such as an IP phone.

The IEEE 802.3at standard is basically an extension of the IEEE 802.3af standard and as such it is backwards compatible with the IEEE 802.3af standard. In other words, an IEEE 802.3at compliant L2 switch will support all Classes of IEEE 802.2af end points, however an IEEE 802.3af compliant L2 switch will only support Classes 0 through 3, Class 4 will not be supported - see warning below.

> **WARNING:** DEVICES THAT REQUIRE MORE THAN 12.95 WATTS ARE DESIGNATED AS IEEE 802.3AT CLASS 4 DEVICES. TO OPERATE CORRECTLY, ALL IEEE 802.3AT CLASS 4 DEVICES MUST BE CONNECTED TO A L2 POE SWITCH THAT IS IEEE 802.3AT COMPLIANT.

> SOME IEEE 802.3AT L2 POE SWITCHES REQUIRE CONNECTED DEVICES TO SEND POWER ALLOCATION REQUESTS IN EXCESS OF 12.95 W (CLASS 4) USING LLDP-MED. THEREFORE, ADMINISTRATORS MUST ENSURE THAT LLDP-MED IS ENABLED ON THE L2 SWITCH.
>
> ALTERNATIVELY, IEEE 802.3AT CLASS 4 DEVICES MAY BE POWERED WITH AN IN-LINE IEEE 802.3AT POWER INJECTOR, OR IF SUPPORTED, AN AC TO DC ADAPTER.

IEEE 802.3at PoE Cabling Plant Requirements

The IEEE 802.3at Power over Ethernet (PoE) standard allows for higher power delivery to the end point than is allowed under the IEEE 802.2af PoE standard. As a result, IEEE 802.3at PoE deployments should be made only on CAT-5 (or better) cabling plant. CAT-3 cable has a higher DC resistance per meter than CAT-5 cable; as a result, given the same length of cable, CAT-5 cable can carry higher currents than CAT-3 cable. CAT-3 cable is acceptable only for IEEE 802.3af deployments.

PoE Connector Pin Designations for power

There are two wiring conventions allowed in the IEEE 802.3af and the IEEE 802.3at standards:

- Power is delivered using RJ-45 pins 1, 2, 3 and 6. Pins 1 & 2 carry positive DC, and pins 3 & 6 carry negative DC.
- Power is delivered using RJ-45 pins 4, 5, 7 and 8. Pins 4 & 5 carry positive DC, and pins 7 & 8 carry negative DC.

IEEE 802.3af and IEEE 802.3at Operation and Naming Conventions

As mentioned in the previous sections, IEEE 802.3af was the original PoE standard and IEEE 802.3at is the newer PoE standard that is backwards compatible with IEEE 802.3af and also allows for higher power delivery to end points.

It should be noted that the IEEE 802.3at standard uses the following naming conventions to refer to the new and the old standards:

- The IEEE 802.3at standard refers to the IEEE 802.3af lower power standard as “802.3at Type 1’.
- The IEEE 802.3at standard refers to the IEEE 802.3at higher power standard as “802.3at Type 2’.

Within the PoE standards, devices that provide power, are called are called “Power Sourcing Equipment” (PSE), and devices that accept the power are called “Powered Devices” (PD).

The IEEE 802.3af standard requires that a “signature” be detected by a PSE port prior to applying any significant power on the cable. Regular PC NICs do not have this signature, whereas Mitel IP Phones do provide the signature.

A Power over Ethernet port generates current limited, low voltage pulses which allow it to probe the far end for a specific impedance signature at the end of the Ethernet cable. If this “signature” is detected (an IP Phone, for example), then the PSE assumes that power is required. If the signature is not detected (e.g. PC NIC), then the PSE does not apply power.

Once the signature or impedance has been detected, the voltage is increased, and current draw is monitored. The amount of current drawn allows the PSE to classify the device into a power class for Power over Ethernet requirements.

PD classification (or advertising) is an optional part of the standard and allows the PD end device to inform the PSE of its power requirements.

- Class 0 is the default class. When encountering devices that do not support the optional PD classification, the PSE will assign this default class to the device.
- Class 0 requests that the PSE provide the PD with power ranging from 0.44 to 12.94 Watts.
- Class 1 requests that the PSE provide the PD with power ranging from 0.44 to of 3.84 Watts.
- Class 2 requests that the PSE provide the PD with power ranging from 3.84 up to 6.49 Watts.
- Class 3 requests that the PSE provide the PD with power ranging from 6.49 up to 12.95 Watts.
- Class 4 requests that the PSE provide the PD with power ranging from 12.95 up to 25.5 Watts.

> **Note:** Class 4 is valid only for IEEE 802.3at Type 2 devices, Class 4 Is not allowed for IEEE 802.3at Type 1 (IEEE 802.3af) devices.

Power required for Mitel IP phones is fairly constant whether the phone is in use or idle. Very loud ringer and hands-free settings can draw more power than normal. Note that when additional devices or peripherals are connected to the IP phone (such as a PKM, a LIM, a Conference Unit or a DECT or wireless accessory), the power required by the phone will increase. Depending on the amount of additional power required, the phone may advertise a different power level to the PoE L2 switch.

Table 2 IP Phone Powering Options and PoE Standards - Listed by Phone Model Number can be used to determine which PoE standard a phone complies with and which powering options are supported.

PoE Advertisement Standards

Mitel IP phones can use one of three different communication standards to advertise their power requirements to a PoE Ethernet switch. In all cases, both the phones and the PoE Ethernet switch must comply with the same standard. The three standards are:

- IEEE 802.3af/at Power Over Ethernet Standard (PoE)
- IEEE 802.3ab Link layer Discovery Protocol (LLDP-MED)
- Cisco Discovery Protocol (CDP)

To determine what the power advertisement value is for a particular phone, refer to the following tables:

- Table 3 CDP Power Advertisement Values - Listed by Phone Model Number
- Table 4 IEEE 802.3at Power Class Advertisement Values - Listed by Phone Model Number
- Table 5 LLDP-MED Power Class Advertisement Values - Listed by Phone Model Number

> **Note:** When using PoE to provide power to the phones, consult the data sheet for the mid-span hub or the powered Ethernet switch to determine the maximum power supply capabilities of the powered Ethernet switch or the mid-span hub so that the hub or switch maximum rating is not exceeded.
>
> **Note:** If a phone supports the IEEE 802.3af power over Ethernet standard and the IEEE 802.3AB LLDP-MED standard and the powered Ethernet switch also supports both of these standards, then the phone can advertise its power requirements to the L2 switch using either standard.
>
> **Note:** Depending on the particular PoE advertising protocol used, the phone may advertise a power requirement value that is different from the actual phone power consumption shown in Table 6 IP Phone Power Consumption - Listed by Phone Model Number. Any difference between the advertised values and the actual values is intentional to ensure correct interworking with the PoE protocol.

CDP PoE Advertisement Values

Table 3 CDP Power Advertisement Values - Listed by Phone Model Number can be used to determine the CDP power advertisement value a phone will transmit to the PSE device.

> **Note:** CDP power advertisement values should not be used for designing a PoE power budget. These values may not reflect the actual power consumption; the values used were chosen to satisfy the CDP protocol so that if necessary, the phones may obtain VLAN information.

For actual phone power consumption refer to Table 6 IP Phone Power Consumption - Listed by Phone Model Number. For advertised power values, refer to the appropriate table in the following sections.

Table 3 CDP Power Advertisement Values - Listed by Phone Model Number

Device	CDP Power Advertisements (see Notes)
5001 IP Phone	4.5 W
5005 IP Phone	4.5 W
5010 IP Phone	6.3 W
5020 IP Phone	6.3 W
5020 IP Phone + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	6.3 W
5020 IP Phone + PKM(s) (PKMs are powered with AC adapter 24 VDC)	6.3 W
5201 IP Phone	4.5 W
5205 IP Phone	4.5 W
5207 IP Phone	4.5 W
5212 IP Phone	6.1 W

Device	CDP Power Advertisements (see Notes)
5215 IP Phone	6.3 W
5215 IP Phone (Dual Mode)	6.1 W
5220 IP Phone	6.3 W
5220/5224 IP Phone + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	6.3 W
5220/5224 IP Phone + PKM(s) (PKMs are powered with AC adapter 24 VDC)	6.3 W
5220/5224 IP Phone (Dual Mode)	6.1 W
5230 IP Appliance	6.1 W
5235 IP Phone	6.1 W
5140 IP Appliance	7.2 W
5240 IP Appliance	7.2 W
5302	not supported
5304	5.0 W
5312	6.1 W
5320	6.1 W
5320e	6.1 W
5324	6.1 W
5324 IP Phone + 5310 Conference Unit	6.1 W
5324 + PKMs	6.1 W
5330	6.1 W
5330 with 1 PKM	6.1 W
5330 with 2 PKMs	6.1 W
5330e	6.1 W
5330e with 1 PKM	6.1 W
5330e with 2 PKMs	6.1 W
5340	6.1 W

Device	CDP Power Advertisements (see Notes)
5340 with 1 PKM	6.1 W
5340 with 2 PKMs	6.1 W
5340e	6.1 W
5340e with 1 PKM	6.1 W
5340e with 2 PKMs	6.1 W
5360	12.0 W
5505	5.0 W
5540	6.1 W
5560 IPT	6.1 W
Navigator	6.1 W
TeleMatrix 3000 IP	5.0 W
MiVoice Video/Conference	5.0 W
67xx Series	See Note 4
68xx Series	See Note 4
6905	2.6 W (See Note 5)
6910	3.2 W (See Note 5)
6920	3.7 W (See Note 5)
6920 With 1 M695 PKM	6.04 W (See Note 5)
6920 With 2 M695 PKMs	8.38 W (See Note 5)
6920 With 3 M695 PKMs	10.72 W (See Note 5)
6930	7.94 W (See Note 5)
6930 With DECT Headset	10.03 W (See Note 5)
6930 With 1 M695 PKM	10.28 W (See Note 5)
6930 With 2 M695 PKMs	12.62 W (See Note 5)
6930 With 3 M695 PKMs	14.96 W (See Note 5)

Device	CDP Power Advertisements (see Notes)
6930 With 3 M695 PKMs + DECT Headset	17.05 W (See Note 5)
6940	9.92 W (See Note 5)
6940 With DECT Headset	12.01 W (See Note 5)
6940 With 1 M695 PKM	12.26 W (See Note 5)
6940 With 2 M695 PKMs	14.6 W (See Note 5)
6940 With 3 M695 PKMs	16.94 W (See Note 5)
6940 With 3 M695 PKMs + DECT Headset	19.03 W (See Note 5)
6970	9.0 W (See Note 5)

> **Note 1:** The Gigabit Ethernet phone stand does not transmit CDP power advertisements; however, the stand allows the phone's CDP power advertisements to be passed through to the network.
>
> **Note 2:** See the section Gigabit Ethernet Phone Stand, Power Restrictions for information about power restrictions related to the Gigabit Ethernet Phone Stand.
>
> **Note 3:** These advertised values assume that a 3300 Power Dongle is used with the phones, and the power requirements shown in the table include the power required by both the phone and the 3300 Power Dongle.
>
> **Note 4:** The 67xx and 68xx series of SIP sets do not support CDP.
>
> **Note 5:** The 69xx series of sets do not support CDP when operating in SIP mode, the 69xx series of sets do support CDP when operating in MiNET mode.
>
> **N/A** = Not Applicable

IEEE 802.3at Power Class Advertisement Values

Table 4 IEEE 802.3at Power Class Advertisement Values - Listed by Phone Model Number can be used to determine the IEEE 802.3at power class advertisement value a phone will transmit to the PSE.

Table 4 IEEE 802.3at Power Class Advertisement Values - Listed by Phone Model Number

Device	Class Advertised
5001 IP Phone	0
5005 IP Phone	0
5010 IP Phone	0
5020 IP Phone	0

Device	Class Advertised
5020 IP Phone + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	0
5020 IP Phone + PKM(s) (PKMs are powered with AC adapter 24 VDC)	0
5201 IP Phone	0
5205 IP Phone	0
5207 IP Phone	0
5212 IP Phone	2
5215 IP Phone	0
5215 IP Phone (Dual Mode)	2
5220/5224 IP Phone	0
5220/5224 IP Phone + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	0
5220/5224 IP Phone + PKM(s) (PKMs are powered with AC adapter 24 VDC)	0
5220/5224 IP Phone (Dual Mode)	2
5220/5224 IP Phone (Dual Mode) + 5412 PKM	3
5220/5224 IP Phone (Dual Mode) + 5448 PKM	3
5220/5224 IP Phone (Dual Mode) + 5412 PKM + 5448 PKM	3
5220/5224 IP Phone (Dual Mode) + 5448 PKM + 5448 PKM	3
5220/5224 IP Phone (Dual Mode) + 5310 Conference Unit + Saucer	3
5220/5224 IP Phone (Dual Mode) + LIM	2
5230 IP Appliance	0
5235 IP Phone	2
5235 IP Phone + 5412 PKM	3
5235 IP Phone + 5448 PKM	3
5235 IP Phone + 5412 PKM + 5448 PKM	3
5235 IP Phone + 5448 PKM + 5448 PKM	3
5235 IP Phone + 5310 Conference Unit + Saucer	3
5235 + LIM	2
5140 IP Appliance	0

Device	Class Advertised
5240 IP Appliance	0
5302 IP Phone	2
5304 IP Phone	2
5312 IP Phone	2
5320	2
5320e	2
5324 IP Phone	2
5324 IP Phone + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	3
5324 IP Phone + PKM(s) (PKMs are powered with AC adapter 24 VDC)	3
5324 IP Phone (Dual Mode) + 5412 PKM	3
5324 IP Phone (Dual Mode) + 5448 PKM	3
5324 IP Phone (Dual Mode) + 5412 PKM + 5448 PKM	3
5324 IP Phone (Dual Mode) + 5448 PKM + 5448 PKM	3
5324 IP Phone (Dual Mode) + 5310 Conference Unit + Saucer	3
5324 IP Phone (Dual Mode) + LIM	3
5330	2
5330 + 5412 PKM	3
5330 + 5448 PKM	3
5330 + Cordless OM Handset plus Headset	3
5330 + Bluetooth module	3
5330 with backlight	2
5330 with backlight + Bluetooth module	3
5330 with backlight + Cordless OM Handset plus Headset	3
5330e	2
5340	2
5340 + 5412 PKM	3
5340 + 5448 PKM	3
5340 + Cordless OM Handset plus Headset	3

Device	Class Advertised
5340 + Bluetooth module	3
5340e	2
5360	0
5360 + Bluetooth module	0
5505	2
Navigator	3
TeleMatrix 3000IP	2
Gigabit Ethernet Phone Stand Version 1	3
Gigabit Ethernet Phone Stand Version 2	0
5540	3
5560 IPT	0
MiVoice Video/Conference	(See Note 2 & 3)
6731i	1 (See Note 4)
6735i	2 (See Note 5)
6735i With 1 PKM	2 (See Note 5)
6737i	2 (See Note 5)
6737i with 1 PKM	2 (See Note 5)
6739i	3 (See Note 5)
6863i	1
6865i	2
6865i With 1 PKM	3
6865i With 2 PKMs	3
6865i With 3 PKMs	3
6867i	2
6867i With 1 PKM	3
6867i With 2 PKMs	3
6867i With 3 PKMs	3
6869i	3

Device	Class Advertised
6869i With 1 PKM	3
6869i With 2 PKMs	3
6869i With 3 PKMs	3
6873i	3
6873i With 1 PKM	4 (See Note 3)
6873i With 2 PKMs	4 (See Note 3)
6873i With 3 PKMs	4 (See Note 3)
6905	1
6910	2
6920	1
6920 With 1 M695 PKM	3 (See Note 6)
6920 With 2 M695 PKMs	3
6920 With 3 M695 PKMs	3
6930	3
6930 With DECT Headset	3
6930 With 1 M695 PKM	4 (See Notes 3 & 6)
6930 With 2 M695 PKMs	4 (See Notes 3 & 6)
6930 With 3 M695 PKMs	4 (See Note 3)
6930 With 3 M695 PKMs + DECT Headset	4 (See Note 3)
6940	3
6940 With DECT Headset	3
6940 With 1 M695 PKM	4 (See Notes 3 & 6)
6940 With 2 M695 PKMs	4 (See Note 3)
6940 With 3 M695 PKMs	4 (See Note 3)
6940 With 3 M695 PKMs + DECT Headset	4 (See Note 3)
6970	3

> **Note 1:** See section Gigabit Ethernet Phone Stand, Power Restrictions for information about power restrictions related to the Gigabit Ethernet Phone Stand.
>
> **Note 2:** The MiVoice Video/Conference is an IEEE 802.3at (Type 2) Class 4 device. IEEE 802.3at (Type 2) Class 4 devices draw from 12.95 Watts to 25.5 Watts.

Device	Class Advertised

Note 3: Attention - Devices that require more than 12.95 watts are designated as IEEE 802.3at Class 4 devices. To operate correctly, all IEEE 802.3at Class 4 devices must be connected to a L2 PoE switch that is IEEE 802.3at compliant.

Some IEEE 802.3at L2 PoE switches require connected devices to send power allocation requests in excess of 12.95 W (Class 4 devices) using LLDP-MED. Therefore, Administrators must ensure that LLDP-MED is enabled on the L2 switch.

Alternatively, IEEE 802.3at Class 4 devices may be powered with an in-line IEEE 802.3at power injector, or if supported, an AC to DC adapter.

Note 4: The 6731i does not support PKMs under any powering scenarios.

Note 5: The following combinations cannot be powered via PoE; however, these sets can support a full complement PKMs when powered via an AC power adapter, for details refer to the 67xx product documentation.

- 6735i with more than one PKM - Must use an AC Power Adapter
- 6737i with more than one PKM - Must use an AC Power Adapter
- 6739i with PKMs - Must use an AC Power Adapter

Note 6: Upon initial power up, these sets (with associated accessories) will advertise their power Class via IEEE 802.3at. Once these sets have completed power up, they will advertise modified power requirements via LLDP-MED that are less than what was reported by the IEEE 802.3at Class advertisements. However, the L2 switch must have LLDP-MED enabled to take advantage of the lower power advertisement.

Note: Some MiVoice IP phones do not support the optional classification feature, and the PSE connection defaults to Class 0 (15.4 Watts for the IP phones, which is more than they require). Some Ethernet switches can run into problems as they cannot supply 15.4 Watts to all ports simultaneously, so the Ethernet switch specifications should be considered prior to deploying phones.

Note: The IEEE 802.3af Classes for advertising power requirements are very granular, for instance Class 1 covers a range of 4 watts. Class ranges are indicated below:

- Class 0 is the default Class. Devices that do not support the optional classification will default to this setting. Class 0 requests the PSE to provide 15.4 Watts of power.
- Class 1 requests the PSE to provide from 0 to 4 Watts.
- Class 2 requests the PSE to provide from 4 to 7 Watts.
- Class 3 requests the PSE to provide from 7 to 15.4 Watts (like Class 0); however, the PD will always draw at least 7 Watts or more.

IEEE 802.3ab LLDP-MED Power Class Advertisement Values

Table 5 LLDP-MED Power Class Advertisement can be used to determine which LLDP-MED power advertisement value a phone will use.

Table 5 LLDP-MED Power Class Advertisement Values - Listed by Phone Model Number

Device	Power Value Advertised	Power Consumption (Watts)
5001 IP Phone	Not Supported	n/a
5005 IP Phone	Not Supported	n/a
5010 IP Phone	Not Supported	n/a
5020 IP Phone	Not Supported	n/a
5020 IP Phone + 5310 Conference Unit (Conference Unit is powered with AC adapter 24 VDC)	Not Supported	n/a
5020 IP Phone + PKM(s) (PKMs are powered with AC adapter 24 VDC)	Not Supported	n/a
5201 IP Phone	Not Supported	n/a
5205 IP Phone	Not Supported	n/a
5207 IP Phone	Not Supported	n/a
5212 IP Phone	47	4.7
5215 IP Phone	Not Supported	n/a
5215 IP Phone (Dual Mode)	47	4.7
5220 IP Phone	Not Supported	n/a
5220 IP Phone + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	Not Supported	n/a
5220 IP Phone + PKM(s) (PKMs are powered with AC adapter 24 VDC)	Not Supported	n/a
5220 IP Phone (Dual Mode)	47	4.7
5220 IP Phone (Dual Mode) + 5412 PKM	64	6.4
5220 IP Phone (Dual Mode) + 5448 PKM	64	6.4
5220 IP Phone (Dual Mode) + 5412 PKM+ 5448 PKM	81	8.1
5220 IP Phone (Dual Mode) + 5448 PKM+ 5448 PKM	81	8.1
5220 IP Phone (Dual Mode) + 5310 Conference Unit + Saucer	47	4.7
5220 IP Phone (Dual Mode) + LIM	51	5.1
5224 IP Phone	47	4.7
5224 + 5412 PKM	64	6.4

Device	Power Value Advertised	Power Consumption (Watts)
5224 + 5448 PKM	64	6.4
5224 + 5412 PKM + 5448 PKM	81	8.1
5224 + 5448 PKM + 5448 PKM	81	8.1
5224 + Gigabit Ethernet Stand	100	10
5230 IP Appliance	Not Supported	n/a
5235 IP Phone	62	6.2
5235 IP Phone + 5412 PKM	79	7.9
5235 IP Phone + 5448 PKM	79	7.9
5235 IP Phone + 5412 PKM + 5448 PKM	96	9.6
5235 IP Phone + 5448 PKM + 5448 PKM	96	9.6
5235 IP Phone + Conference Unit + Saucer	112	11.2
5235 + Gigabit Ethernet stand	115	11.5
5235 IP Phone + LIM	66	6.6
5140 IP Appliance	Not Supported	n/a
5240 IP Appliance	Not Supported	n/a
5302 IP Phone	Not supported	n/a
5304 IP Phone	37	3.7
5312 IP Phone	47	4.7
5320 IP Phone	47	4.7
5320e IP Phone	55	5.5
5324 IP Phone	47	4.7
5324 IP Phone with LIM	51	5.1
5324 IP Phone + 5412 PKM	64	6.4
5324 IP Phone + 5448 PKM	64	6.4
5324 IP Phone + 5412 PKM + 5448 PKM	81	8.1
5324 IP Phone + 5448 PKM + 5448 PKM	81	8.1
5324 IP Phone + Gigabit Ethernet Stand	100	10.0
5324 + Conference Unit module + saucer	97	9.7
5310 Conference Unit side panel and saucer	47	4.7

Device	Power Value Advertised	Power Consumption (Watts)
5330	58	5.8
5330 + 5412 PKM	75	7.5
5330 + 5448 PKM	75	7.5
5330 + 2 PKMs	92	9.2
5330 + LIM	62	6.2
5330 + Gigabit Ethernet stand (See Note 2)	111 or 5.8	11.1 or 5.8
5330 + Cordless OM Handset plus Headset	88	8.8
5330 + Bluetooth module	88	8.8
5330 + Conference Unit + Saucer	108	10.8
5330e	61	6.1
5330e + 5412 PKM	78	7.8
5330e + 5448 PKM	78	7.8
5330e + 2 PKMs	95	9.5
5330e + LIM	65	6.5
5330e + Gigabit Ethernet stand (See Note 2)	111 or 5.8	11.1 or 5.8
5330e + Cordless OM Handset plus Headset	91	9.1
5330e + Bluetooth module	91	9.1
5330e + Conference Unit + Saucer	111	11.1
5340	58	5.8
5340 + 5412 PKM	75	7.5
5340 + 5448 PKM	75	7.5
5340 + 2 PKMs	92	9.2
5340 + LIM	62	6.2
5340 + Conference Unit module + saucer	108	10.8
5340 + Gigabit Ethernet stand (See Note 2)	111 or 58	11.1 or 5.8
5340 + Cordless OM Handset plus Headset	88	8.8
5340 + Bluetooth module	88	8.8
5340e	61	6.1
5340e + 5412 PKM	78	7.8

Device	Power Value Advertised	Power Consumption (Watts)
5340e + 5448 PKM	78	7.8
5340e + 2 PKMs	95	9.5
5340e + LIM	65	6.5
5340e + Conference Unit module + saucer	111	11.1
5340e + Gigabit Ethernet stand (See Note 2)	111 or 58	11.1 or 5.8
5340e + Cordless OM Handset plus Headset	91	9.1
5340e + Bluetooth module	91	9.1
5360	95	9.5
5360 + Conference Unit	128	12.8
5360 + Cordless OM/Handset + Headset	120	12.0
5360 + Bluetooth module	120	12.0
5360 + LIM	99	9.9
5505	39	3.9
Navigator	86	8.6
TeleMatrix 3000IP	37	3.7
Gigabit Ethernet Phone Stand Version 1 (See Note 2)	53 + Phone	5.3 + Phone
Gigabit Ethernet Phone Stand Version 2 (See Note 2)	0 + Phone	0 + Phone
5540	53	5.3
5560 IPT	129	12.9
MiVoice Video/Conference	200	20
67xx Series	Not Supported	n/a
68xx Series	Not Supported	n/a
6905	26	2.6
6910	32	3.2
6920	37	3.7
6920 With 1 M695 PKM	60	6.0
6920 With 2 M695 PKMs	84	8.4
6920 With 3 M695 PKMs	107	10.7

Device	Power Value Advertised	Power Consumption (Watts)
6930	80	8.0
6930 With DECT Headset	101	10.1
6930 With 1 M695 PKM	103	10.3
6930 With 2 M695 PKMs	127	12.7
6930 With 3 M695 PKMs	150	15
6930 With 3 M695 PKMs + DECT Headset	171	17.1
6940	100	10
6940 With DECT Headset	121	12.1
6940 With 1 M695 PKM	123	12.3
6940 With 2 M695 PKMs	146	14.6
6940 With 3 M695 PKMs	170	17
6940 With 3 M695 PKMs + DECT Headset	191	19.1
6970	90	9.0

Note 1: If a phone does not support LLDP-MED advertisements but does support 802.3af advertisements, then 802.3af will be used.

Note 2: The Gigabit Ethernet Stand by itself does not send LLDP-MED power advertisements.

However, when a phone is used with Version 1 the Stand, the phone will detect if the Stand is present and if it is present, the phone will transmit an LLDP-MED power advertisement that includes both the phone power plus the 5.3 watts for the Stand's power.

When a phone is used with Version 2 the Stand, the phone will transmit an LLDP-MED power advertisement that represents the phone's power; the Stand's power of 5.3 watts is not included.

Note 3: See the section called Gigabit Ethernet Phone Stand, Power Restrictions for information about power restrictions related to the Gigabit Ethernet Phone Stand.

Additional Notes:

- The 5215DM / 5212 do not support any adjuncts.
- The 5220DM / 5224 will report that a PKM48 is installed when either a PKM48 or a PKM12 is installed.
- The 5220DM / 5224 do not know if a Conference Unit is connected until the Conference Unit side panel is powered on.
- The 5235 and the 53x0 series of phones offer PoE power only. There is no option for using a 24V power adapter with these phones.

- The 5310 Conference Unit side panel does not work with the 5235 and the 53x0 series of phone. These phones must use the new Conference Unit Module. Unlike the side panel unit used with the 5220DM / 5224, the 5235 and the 53x0 series of phones will know if the Conference Unit Module is plugged in.
- The 5235 will report that a PKM48 is in use when either a PKM12 or a PKM48 is connected.
- The 5330 and the 5340 do not support the PKM12 or the PKM48.

IP Phone Power Consumption

Table 6 IP Phone Power Consumption - Listed by Phone Model Number lists the actual power required by the various IP phones as opposed to what power requirement value the phones may advertise.

> **Note:** In some cases, phone power advertisements may differ slightly from the phone's actual power consumption.
>
> **Note:** Table 6 IP Phone Power Consumption - Listed by Phone Model Number can be used to determine:
>
> 1. If the L2 PoE switch has sufficient power capacity to power the desired combination of phones.
> 2. If power redundancy is required - the UPS capacity that would be required to maintain power to the phones in the event of a mains power outage.

The values shown in Table 6 do not include the 3300 Power Dongle power requirements. For example, a 5220 (Dual Mode) phone requires 4.7 watts of power and a 3300 Power Dongle requires 1.4 watts of power. If the 5220 Dual Mode phone is being used in conjunction with a 3300 Power Dongle the power requirement is 4.7 watts + 1.4 watts for a total power requirement of 6.1 watts.

> **Note:** The power consumption values shown in Table 6 are **Worst Case Maximum** power consumption values, and are generally 10% higher than the **Typical Power** consumption values which are indicated in Mitel's phone data sheets.
>
> **Note:** The **Worst Case Maximum** values shown in Table 6 should always be used when determining engineering L2 PoE switch power supply capacity and UPS backup capacity for a customer site.

Table 6 IP Phone Power Consumption - Listed by Phone Model Number

Device	Power consumption (W) (Worst Case Maximum)
5001 IP Phone	2.0
5005 IP Phone	2.6
5010 IP Phone	5.0
5020 IP Phone	5.0

Device	Power consumption (W) (Worst Case Maximum)
5201 IP Phone	2.0
5205 IP Phone	2.9
5207 IP Phone	3.0
5212 IP Phone	4.7
5215 IP Phone	4.7
5215 IP Phone (Dual Mode)	4.7
5220 IP Phone	4.7
5220 IP Phone (Dual Mode)	4.7
5224 IP Phone	4.7
5230 IP Appliance	5.2
5235	6.2
5140 IP Appliance	6.8
5240 IP Appliance	6.8
5310 IP Conference Unit (for 5235/5330/5330 with backlight/ 5340/5324) (see Note 2)	5.0
5330	4.7
5302	3.84
5304	3.45
5312	3.87
5324	3.87
5320	5.3
5320e	5.5
5330 with back light	5.8
5330e	6.1
5340	5.8
5340e	6.1
5360 (see Note 4)	9.2
5360 + Conference Unit (see Note 4)	12.8
5360 + Cordless OM Handset + Headset (see Note 4)	12.0
5360 + LIM (see Note 4)	9.9

Device	Power consumption (W) (Worst Case Maximum)
5412 PKM (see Note 3)	1.3
5412 PKM + 5448 PKM (see Note 3)	3.0
5448 PKM (see Note 3)	1.7
5448 PKM + 5448 PKM (see Note3)	3.4
5485 Paging Unit	5.0
5540	7.3
5505	3.9
5550-TKB (Used with the 5550 IP Console)	5.0
LIM	0.4
MITEL 3300 power dongle	1.4
Navigator	8.6
TeleMatrix 3000IP	3.7
Gigabit Ethernet Phone Stand Version 1. Note: This power is for the stand only, the phone power is not included.	5.3
Gigabit Ethernet Phone Stand Version 2. Note: This power is for the stand only; the phone power is not included.	3.4
Wireless LAN Phone Stand Note: This power is for the stand only; the phone power is not included.	5.3
Cordless OM / Handset plus headset (for 5330/5330 with backlight/ 5340) (see Note 2)	3.0
5560 IPT	12.9
Bluetooth Module for use with 5330, 5340 and 5360.	3.0
MiVoice Video/Conference	The MiVoice Video/Conference unit can consume up to 25.5 Watts, however typical power consumption is less. For details refer to the MiVoice Video/Conference Engineering Guidelines.
6731i	3.3
6735i	3.74
6737i	3.74
6739i	10.56
6863i	2.2

Device	Power consumption (W) (Worst Case Maximum)
6865i	2.64
6865i With 1 PKM	4.74
6865i With 2 PKMs	7.08
6865i With 3 PKMs	9.42
6867i	3.8
6867i With 1 PKM	6.14
6867i With 2 PKMs	8.48
6867i With 3 PKMs	10.82
6869i	5.2
6869i With 1 PKM	7.54
6869i With 2 PKMs	9.88
6869i With 3 PKMs	12.22
6873i	9.9
6873i With 1 PKM	12.24
6873i With 2 PKMs	14.58
6873i With 3 PKMs	16.92
6905	2.6
6910	3.2
6920	3.7
6920 With 1 M695 PKM	6.04
6920 With 2 M695 PKMs	8.38
6920 With 3 M695 PKMs	10.72
6930	7.9
6930 With DECT Headset	9.99
6930 With 1 M695 PKM	10.24
6930 With 2 M695 PKMs	12.58
6930 With 3 M695 PKMs	14.92
6930 With 3 M695 PKMs + DECT Headset	17.01
6940	9.9
6940 With DECT Headset	11.99

Device	Power consumption (W) (Worst Case Maximum)
6940 With 1 M695 PKM	12.24
6940 With 2 M695 PKMs	14.58
6940 With 3 M695 PKMs	16.92
6940 With 3 M695 PKMs + DECT Headset	19.01
6970	9.0

> **Note 1**: See the section called Gigabit Ethernet Phone Stand, Power Restrictions for information about power restrictions related to the Gigabit Ethernet Phone Stand.
>
> **Note 2**: The power consumed by this device adds to the power consumption of the phone it is attached to.
>
> **Note 3**: The Programmable Key Modules (PKM) are available in two different models, the 5412 and the 5448. In situations where the PKMs are powered via PoE the installer must add the PKM power consumption and the phone power consumption together to determine the total power consumption.
>
> **Note 4:** The 5360 will draw 9.2 Watts when it is in Gigabit Ethernet mode and 7.9 Watts when in 10/100 Mb/s mode.

Power Requirements for 5220 IP Phone - Optional Accessories

The 5220 IP phone and the 5220 IP phone (Dual Mode) support optional accessories which are powered in different ways depending on the option and the phone:

- 5220 IP phone options are powered from a 24 VDC power adapter only.
- 5220 IP phone (Dual Mode) options can be powered from either 24 VDC power adapter or through the Ethernet connection.

> **Note:** To determine whether your phone is a 5220 IP Phone or 5220 IP Phone (Dual Mode), check the label on the back of the set. 5220 IP Phone (Dual Mode) sets are identified as either “5220 Dual Port” or “5220 Dual Mode”.

An alternate way of identifying whether a phone is dual mode or not dual mode is by looking at the “Top Engineering Number” which can be found on a label on the back of the phone, see Table 7 Top Engineering Number by Phone.

Table 7 Top Engineering Number by Phone

Model of Phone	Top Engineering Number (T.E.N. #)
5215	56004354
5220	56004352 & 56005271
5215 Dual Mode	56005585
5220 Dual Mode	56005587

Uninterruptible Power Supplies (UPS)

Use of uninterruptible power supplies (UPS) is recommended when the IP phones, the associated controllers or severs, PC-based consoles, and the LAN infrastructure need to continue to operate during a power failure. UPSs can range from simple local battery units to larger central installations that include backup generators. Consider the following factors to determine the type of unit to use:

- The power to be drawn by attached units
- The power output of the UPS, and its efficiency with battery capability
- The time the UPS must supply power
- The size of the unit.

> **Notes**:
>
> 1. If VoIP service must be operational during a power failure, each of the network components must also be on the UPS.
> 2. The MiVB System Engineering Tool will estimate the amount of power used by each of the MiVB cabinets in the system configuration when running the existing traffic. The estimate does not include the power for other network equipment (L2 switches, and so forth).
> 3. The MiVB System Engineering Tool or the Streamline Power Calculator tool can be used to calculate the amount of power being used by the phones.

Worked Example

Consider a small installation with a LAN switch and some powered phones. The LAN switch draws 100 W and 16 attached phones draw 8 W each. The UPS has a 12 V battery of 55 AH and runs at 70% efficiency. How long can power be maintained for this combination?

- The output power available is 462 VAH (volt-amperes hour) (55 x 12 x 70%).
- The consumption is 228 VA (100 W + 16 x 8 W).
- The time available is 2 hours or 462 VAH / 228 VA.

> **Note:** Volt-Amperes (VA) is equivalent to Watts (W) if the Power Factor Correction (PFC) of the power supply in question has a PFC value of close to 1. Most data switches on the market today will have a PFC value close to 1.

America Power Conversion (APC) is a company that designs and sells UPS systems. Some useful calculations can also be found at the APC web site, see the following URL:

http://www.apc.com/ca/en/tools/ups_selector

IP Ports

> **Note:** For security reasons an IP phone or an IP conference phone should never be connected directly to the internet. The IP phone or IP conference should always reside behind an appropriate firewall so that firewall rules can be used to protect the phone from malicious attacks.

The following diagrams highlight the IP ports for 53xx and 69xx phones.

IP port information for the 67xx and 68xx phones is documented in the 67xx and 68xx product documentation, which can be found on Mitel's Document Centre.

The following key is used to identify the connections in the port diagrams:

- Arrow direction shows initial connection direction.
- A double ended arrow means that the connection is, or may be, established in both directions i.e. an end device might be both a client and a server.
- Description above the line is the destination termination point.
- Description below the line is the source origination point.
- No description on the connection implies that any acceptable port may be used; this is typically in the ephemeral range, which may be defined on a particular device, but typically in the range 1024 to 65535.

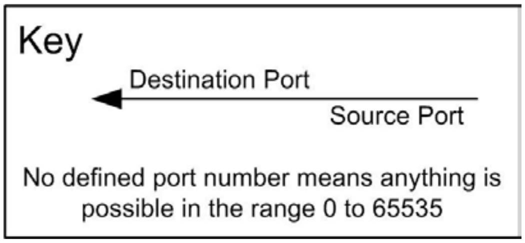
Key
Destination Port
Source Port
No defined port number means anything is possible in the range 0 to 65535

Figure 1 IP Port Key

53xx and 69xx IP Phone Port Differences

The 69xx phones have the following IP port changes with respect to the 53xx phones:

- The 69xx phones no longer use 3999 and 3998 for SAC.
- The 69xx phones are now using IP ports 6800, 6801 and 6802 for supporting SAC and Mitel- like LDAP.

53xx IP Phones

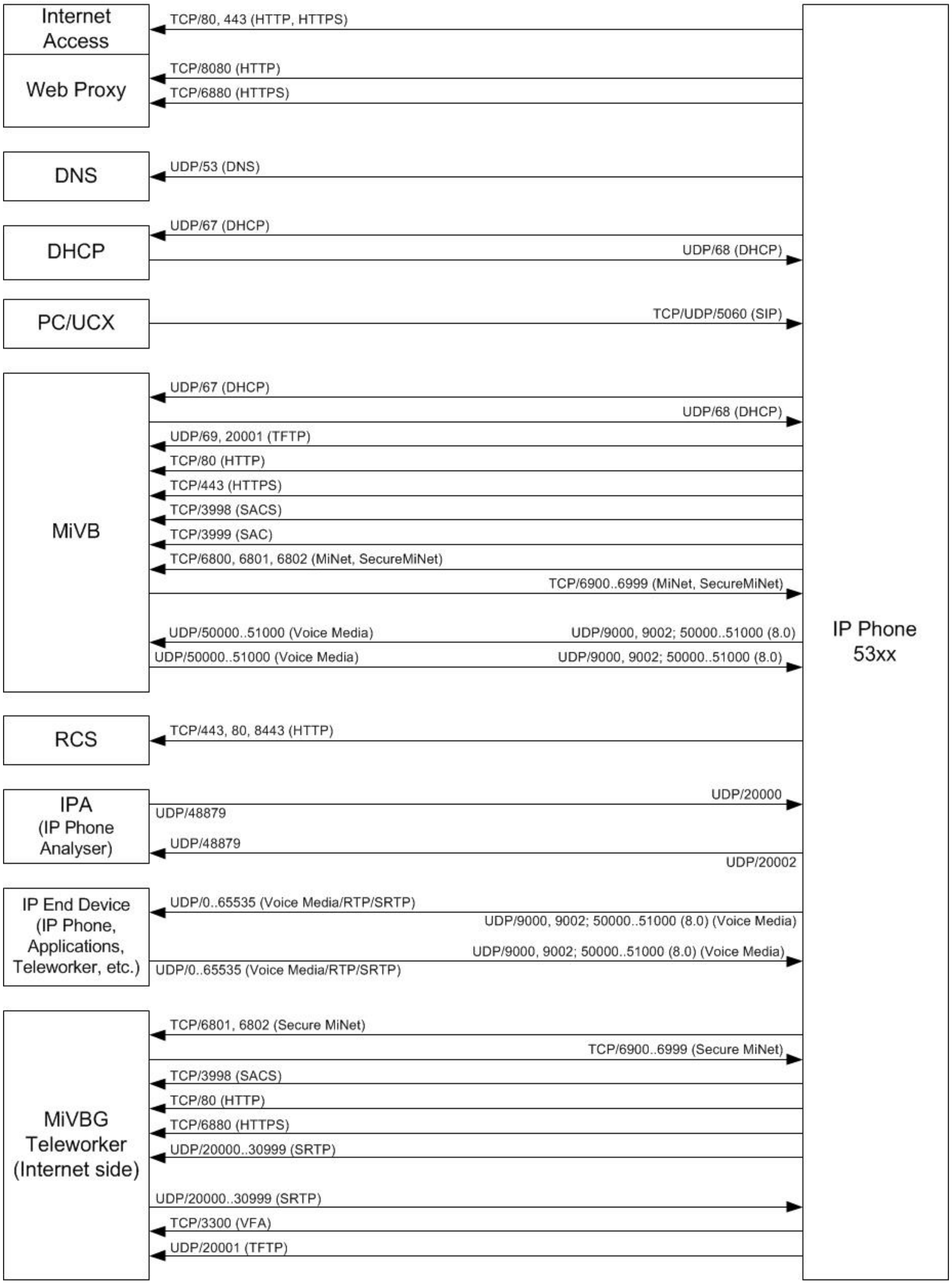
Internet Access
TCP/80, 443 (HTTP, HTTPS)
Web Proxy
TCP/8080 (HTTP)
TCP/6880 (HTTPS)
DNS
UDP/53 (DNS)
DHCP
UDP/67 (DHCP)
UDP/68 (DHCP)
PC/UCX
TCP/UDP/5060 (SIP)
MiVB
UDP/67 (DHCP)
UDP/68 (DHCP)
UDP/69, 20001 (TFTP)
TCP/80 (HTTP)
TCP/443 (HTTPS)
TCP/3998 (SACS)
TCP/3999 (SAC)
TCP/6800, 6801, 6802 (MiNet, SecureMiNet)
TCP/6900..6999 (MiNet, SecureMiNet)
UDP/50000..51000 (Voice Media)
UDP/9000, 9002; 50000..51000 (8.0)
UDP/50000..51000 (Voice Media)
UDP/9000, 9002; 50000..51000 (8.0)
IP Phone 53xx
RCS
TCP/443, 80, 8443 (HTTP)
IPA (IP Phone Analyser)
UDP/20000
UDP/48879
UDP/48879
UDP/20002
IP End Device (IP Phone, Applications, Teleworker, etc.)
UDP/0..65535 (Voice Media/RTP/SRTP)
UDP/9000, 9002; 50000..51000 (8.0) (Voice Media)
UDP/9000, 9002; 50000..51000 (8.0) (Voice Media)
UDP/0..65535 (Voice Media/RTP/SRTP)
MiVBG Teleworker (Internet side)
TCP/6801, 6802 (Secure MiNet)
TCP/6900..6999 (Secure MiNet)
TCP/3998 (SACS)
TCP/80 (HTTP)
TCP/6880 (HTTPS)
UDP/20000..30999 (SRTP)
UDP/20000..30999 (SRTP)
TCP/3300 (VFA)
UDP/20001 (TFTP)

Figure 2 53xx IP Phone IP Ports

69xx IP Phones

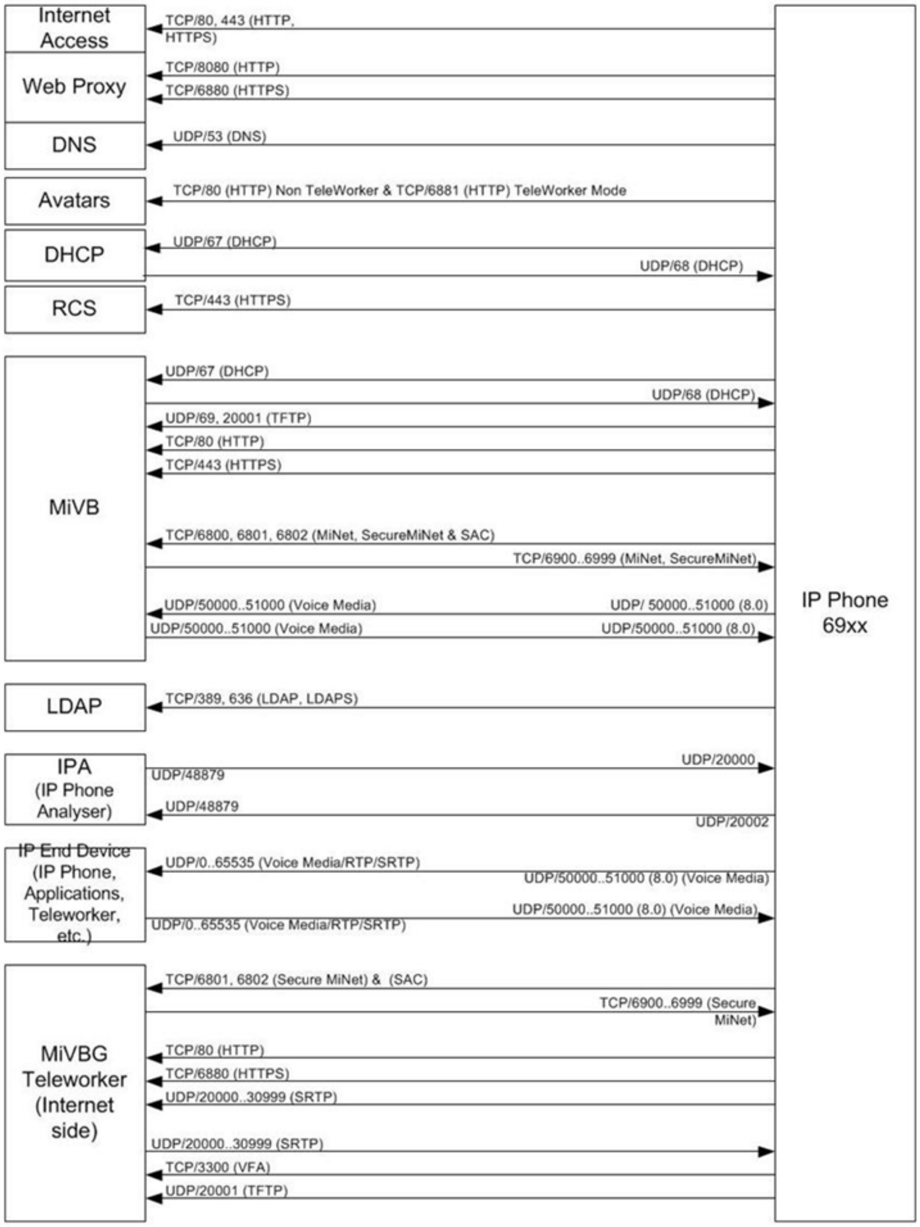
Internet Access
TCP/80, 443 (HTTP, HTTPS)
Web Proxy
TCP/8080 (HTTP)
TCP/6880 (HTTPS)
DNS
UDP/53 (DNS)
Avatars
TCP/80 (HTTP) Non TeleWorker & TCP/6881 (HTTP) TeleWorker Mode
DHCP
UDP/67 (DHCP)
UDP/68 (DHCP)
RCS
TCP/443 (HTTPS)
MiVB
UDP/67 (DHCP)
UDP/68 (DHCP)
UDP/69, 20001 (TFTP)
TCP/80 (HTTP)
TCP/443 (HTTPS)
TCP/6800, 6801, 6802 (MiNet, SecureMiNet & SAC)
TCP/6900..6999 (MiNet, SecureMiNet)
UDP/50000..51000 (Voice Media)
UDP/ 50000..51000 (8.0)
UDP/50000..51000 (Voice Media)
UDP/50000..51000 (8.0)
IP Phone 69xx
LDAP
TCP/389, 636 (LDAP, LDAPS)
IPA (IP Phone Analyser)
UDP/20000
UDP/48879
UDP/48879
UDP/20002
IP End Device (IP Phone, Applications, Teleworker, etc.)
UDP/0..65535 (Voice Media/RTP/SRTP)
UDP/50000..51000 (8.0) (Voice Media)
UDP/50000..51000 (8.0) (Voice Media)
UDP/0..65535 (Voice Media/RTP/SRTP)
MiVBG Teleworker (Internet side)
TCP/6801, 6802 (Secure MiNet) & (SAC)
TCP/6900..6999 (Secure MiNet)
TCP/80 (HTTP)
TCP/6880 (HTTPS)
UDP/20000..30999 (SRTP)
UDP/20000..30999 (SRTP)
TCP/3300 (VFA)
UDP/20001 (TFTP)

Figure 3 69xx IP Phone IP Ports

IP Phones - Obtaining LAN Policy Settings

> **Note:** For security reasons an IP phone or an IP conference phone should never be connected directly to the internet. The IP phone or IP conference should always reside behind an appropriate firewall so that firewall rules can be used to protect the phone from malicious attacks.

Before the IP phones can operate correctly on the LAN, they need to obtain IP addressing information and the LAN policy parameters.

The IP addresses or FQDNs that the phone requires are:

- The phone's own IP address
- The default gateway's IP address
- The subnet mask
- The IP address or the FQDN of the call server
- The IP address of the DHCP server
- The IP address or the FQDN of the TFTP server
- The IP address of the DNS server

"LAN Policy" consists of a set of three parameters that are used to control segregation and priority of voice traffic across the network. These parameters are

- VLAN ID (IEEE 802.1Q)
- Layer 2 priority (IEEE 802.1D/p)
- Differentiated Services Code Point (DSCP, Layer 3 priority)

> **Note:** The 5302 start-up sequence differs from the method used by other Mitel phones. Refer to the section called 5302 Startup and DHCP for information about the 5302 phone.

67xx and 68xx Series of Phones

To obtain LAN policy, the 67xx and 68xx series of phones support the use of LLDP and DHCP, the sets also support static programming. For details refer to the 67xx and 68xx product documentation, which can be found on Mitel's Document Centre under IP Phones / 6800 Series.

Options for obtaining VLAN Setting Information

There are four potential methods that MiVoice IP Phones can use to obtain VLAN setting information, they are:

1. Static values that are held in the phone's flash memory. (The installer can program the phone with static values via the phone's keypad).
2. The Voice VLAN may be learned via LLDP-MED.
3. The Voice VLAN may be learned via CDP.
4. The Voice VLAN may be learned via DHCP.

Notes:

1. Not all phones support all of the above options. See section IP Phones and VLAN programmability to determine which phones support which options.
2. The 5550 IP console supports methods 3-4. The 5302 is covered under the section 5302 Startup and DHCP
3. Third-party SIP devices do not necessarily support the options that are supported by Mitel phones. In general, third party SIP phones should be statically programmed.
4. The legacy 5550 TKB does not support configurable DSCP values. All traffic from the 5550-TKB is hard coded with a DSCP value of ‘44’.
5. The legacy 5550 TKB does not support LLDP-MED.

Sources of LAN policy and IP Addressing Information

Table 8 Source of Network Policy Information indicates the LAN Policy parameters and the IP addresses that can be obtained from each of the different sources of information.

Table 8 Source of Network Policy Information

Source of info	Phone IP Address	Default Gateway IP address	Subnet Mask	VLAN (802.1Q) Info	L2 QOS Priority (802.1d/p)	L3 QOS (DSCP)	RTC/ Call Server IP Address or FQDN	TFTP Server IP Address or FQDN	DNS IP Address
Manual entry	Yes	Yes	Yes	Yes	Yes (0-6)	Yes (0-63)	Yes	Yes	Yes
LLDP-MED	N/A	N/A	N/A	Yes	Yes (0-6)	Yes (0-63)	N/A	N/A	N/A
CDP	N/A	N/A	N/A	Yes	See Note 2	N/A	N/A	N/A	N/A
DHCP	Yes	Yes	Yes	Yes, uses double fetch	Yes (0-6)	Yes (0-63)	Yes	Yes	Yes
Default Values	N/A	N/A	N/A	No VLAN, untagged	6 (If VLAN via CDP then default is 5),	46 (Note)	N/A	N/A	N/A

Note:

1. A DSCP value of 46 is recommended for newer installations using DSCP-aware routers. Value 46 will place the voice into the Expedited Forwarding Queue (EF).
2. Depending on certain network conditions the phone will use different DSCP default values. The default values under specific conditions are:
   - If the VLAN information was learnt via CDP, signaling will use a default DSCP value of ‘46’ and voice will use a default DSCP value of ’46’. These values can be changed with additional programming.
   - In situations where VLAN information cannot be learnt from either CDP or DHCP, the phone will use a DSCP value of ‘0’ for both signaling and voice.

Fully Qualified Domain Name Support for 5300 and 6900 Series IP Phones

In addition to the use of IP addresses, the 5300 and 6900 series of IP phones support the use of FQDNs (Fully Qualified Domain Name) to address the RTC/Call Server and the TFTP server.

When FQDNs are used, the phone will use DNS A records to resolve the FQDN, which will return a single IPV4 address. When deployed in a resilient environment, the phone will continue to use the existing MiNET resiliency mechanisms but use FQDNs instead of IP addresses.

The IP address or FQDN of the RTC/Call Server and the TFTP server may be manually entered as a static setting in the IP phone, or the phone may obtain the IP address or FQDN from a DHCP server or the MiVB DHCP server.

For the MiVB DHCP server, there are new tags in option 125/43 to support FQDNs for the RTC/Call Server (call_srvaddr) and TFTP server (sw_tftpaddr). The new tags can include an FQDN, IPV4 address and for future usage an IPV6 address. The phones will check for the new tags first, and in the absence of the new tags, they will use the old tags.

Addressing the MiVoice Border Gateway with an FQDN

In addition to the use of IP addresses, the 5300 and 6900 series of IP phones now support the use of FQDNs (Fully Qualified Domain Name) to address the MiVoice Border Gateway (MBG).

The IP address or the FQDN of the MBG must be manually entered as a static setting in the IP phone.

DNS Requirements for using Fully Qualified Domain Names or the Mitel Re-direction and Configuration Service

At sites where an Administrator would like to make use of FQDNs (Fully Qualified Domain Name) or Mitel’s RCS (Re-direction and Configuration Services) the phone must first obtain the IP address of a DNS server.

The phone can obtain the IP address of the DNS server from the DHCP server (DHCP option 6) or via static configuration (manual entry) on the phone.

Note that the DNS server may be located within the customer’s network or it may be located external to the customer’s network.

The DNS server must be reachable from the phone for FQDNs or RCS to be usable. If there is firewall between the phones and the DNS server, the Administrator will need to ensure that the DNS IP Port (typically 53) is open on the firewall.

Priority of LAN policy sources

To obtain network configuration information such as IP addresses, L2 QoS settings, L3 QoS settings and VLAN information, the phones can be programmed manually or they can obtain information via auto-discovery using LLDP-MED, CDP or DHCP mechanisms.

It is possible to program some network configuration information manually and obtain other information via LLDP-MED, DHCP or CDP and use default values.

The IP phone looks for VLAN setting information and network configuration information in a specific priority order until all of the appropriate fields have been filled in. This priority order for obtaining information is described in the following sections.

> **Note**: If a phone has obtained network configuration information via manual programming, this information will be held by the phone permanently, i.e. other methods cannot overwrite these values and the values will be maintained even if the phone is rebooted. This includes the following values:
>
> - IP address for the phone
> - Default gateway IP address
> - Subnet mask
> - RTC/Call Server IP address or FQDN
> - TFTP server IP address or FQDN
> - DNS server IP address
> - LAN Policy (VLAN, L2 priority, DSCP)

Priority of VLAN setting information sources

The priority levels assigned to each source of VLAN setting information are shown in Table 9 Priority levels for the Various Sources of VLAN Information. The highest priority level is 5 and the lowest is 1. When seeking VLAN information the phone will start with level 5 and proceed through the list in a descending order.

Table 9 Priority levels for the Various Sources of VLAN Information

Source of VLAN Setting Information	Priority Level	Notes
Manual Entry (Static)	5	Programmed by installer
LLDP-MED	4	Information obtained from L2 switch
CDP	3	Phones can discover values if CDP is detected on the LAN
DHCP	2	The first time a phone receives DHCP information it must contain an IP address for the RTC and the TFTP server. This is also true for the double DHCP fetch mechanism. If the phone fetches DHCP information a second time, this information will overwrite the previous values.
Default Values	1	Default Value = No VLAN, untagged

Priority of L2 and L3 QoS information sources

The priority levels assigned to each source used for obtaining L2 and L3 QoS settings are shown in Table 10 Priority levels for the Various Sources of L2/L3 QoS Settings. The highest priority level is 5 and the lowest is 1, such that a higher priority setting always takes precedence over lower attempted re-writes by a lower priority source. When seeking QoS information the phone will collect information from all available sources and use the highest priority information available.

The section called Potential issues with using LLDP-MED in Cisco environments provides an example of a situation where the initial LAN Policy values are overwritten with values obtained from a higher priority source.

Table 10 Priority levels for the Various Sources of L2/L3 QoS Settings

Source of L2 & L3 QoS Settings	Priority Level	Notes
Manual Entry (Static)	5	Programmed by installer
DHCP	4	The first time a phone receives DHCP information it must contain an IP address for the RTC and the TFTP server. This is also true for the double DHCP fetch mechanism. If the phone fetches DHCP information a second time, this information will overwrite the previous values. DHCP can be used to provide separate L2 and L3 QoS values for both signaling and media. If DHCP has only been programmed with one value, the phone will use this value for both signaling and media.
LLDP-MED	3	Information obtained from L2 switch
CDP	2	CDP does not provide values, however if CDP is detected on the LAN the phones will use Cisco 'inferred' values. L2 Value = 5, L3 DSCP Value = 46
Default Values	1	L2 Default Value = 6, L3 DSCP Value = 46. See additional Notes below.

Note:

1. A DSCP value of 46 is recommended for newer installations using DSCP-aware routers. Value 46 will place the voice into the Expedited Forwarding Queue (EF).
2. Depending on certain network conditions the phone will use different DSCP default values. The default values under specific conditions are:

- If the VLAN information was learnt via CDP, signaling will use a DSCP value of '46' and voice will use a DSCP value of '46'.
- In situations where VLAN information cannot be learnt from either CDP or DHCP, the phone will use a DSCP value of '0' for both signaling and voice.

Potential issues with using LLDP-MED in Cisco environments

The Issue:

Erroneous VoIP QoS values have been noted when using LLDP-MED with the following Cisco IOS software releases:

- IOS 12.2(37)
- IOS 12.2(40)

Cisco switches running the above operating systems with LLDP-MED enabled will issue the phones these LAN Policy values:

- Valid VLAN ID
- L2 (802.1p) = 0 (Incorrect value)
- L3 (DSCP) = 0 (Incorrect value)

Since these values are non-user programmable, they cannot be changed by the system administrator. These values do not provide the correct priority levels for voice media at either L2 or L3, therefore the use of these values will potentially cause severe voice quality issues.

The Solutions:

1. If it is a requirement to keep LLDP-MED running on the Cisco switches:
   - Leave LLDP-MED running on the Cisco switches.
   - Use DHCP to provide the phones with the correct L2 and L3 priority settings.

   DHCP learnt values have a higher priority and will override the LLDP-MED learnt values.
2. In situations where there is no requirement to have LLDP-MED and CDP running on the Cisco switches:
   - Disable LLDP-MED on the Cisco switches.
   - Disable CDP on the Cisco switches.
   - Use DHCP with double fetches to provide the phones with the correct L2 and L3 priority settings. Information on DHCP double fetches can be found under 0 DHCP and IP Phone network policy.
3. If there is no requirement to keep LLDP-MED running on the Cisco switches:
   - Disable LLDP-MED on the Cisco switches.
   - Enable CDP to provide the phones with VLAN information.
   - When the phones detect that CDP is present on the LAN they will infer that the ‘default Cisco values’ for L2 and L3 priority should be used.

   The Cisco default values for priority are:

   - L2 (802.1p) = 5
   - L3 (DSCP) = 46

   > **Note:** The inferred Cisco L2 and L3 values used by the phone are not permanent; these values can be overwritten with installer defined DHCP values.

LAN Quality of Service Settings

There are two areas where priority mechanisms can operate in the network to ensure that specific types of traffic will be treated with higher priority by switches and routers than other types of traffic:

- Layer 2 in the LAN through use of VLANs and packet tagging
- Layer 3 in the WAN through use of DiffServ/TOS/Precedence mechanisms

The following Table shows Mitel’s Multi Level QoS model and recommended QoS settings.

General Notes:

- The Voice Service Class is to be used for real-time voice media traffic such as in an IP phone call.
- The Signaling Service Class is to be used for time sensitive protocols such as telephony signaling, e.g. MiNet and SIP.
- The Multimedia Conferencing Service Class is to be used for real-time video media e.g. video conferencing.
- The Standard Service Class is to be used for protocols that have no sensitivity to network latency or packet loss, typically TCP/IP based traffic.

Table 11 Multi Level QoS Model & Recommended QoS Settings

Mitel Service Class	Recommended L2 Values	Recommended L3 Values
Telephony (Voice Media)	6	46 (EF)
Signaling	3	24 (CS3)
Multimedia Conferencing	4	34 (AF41)
Standard	0	0 (DF) (BE)

Additional information on network QoS can be found in the Mitel Technical Paper, Network Engineering for IP Telephony.

DSCP settings for call signaling in Cisco environments

Cisco has supported DSCP 26 (PHB AF31) and more recently DSCP 24 (PHB CS3) for call signaling. As a result, Cisco has “recommended that both AF31 and CS3 be reserved for call signaling”. It is therefore advised to determine whether both or which one of these settings is supported throughout the network before setting the signaling DSCP value for call signaling at installation, e.g. through DHCP settings. Ideally both AF31 (26) and CS3 (24) should be assigned to the same priority queue.

DHCP and IP Phone network policy

When the IP phone uses the DHCP method to obtain VLAN and priority information, it will do sequential fetches on the default (untagged) VLAN and the tagged VLAN. This may double the retrieval of information depending on the way information is entered. It is important that the DHCP servers for the voice and data VLANs each have the same VLAN and priority information.

Also, the ability to provide partial information at each stage allows these three methods to be used together to ease installation. This sequence works with either multiple DHCP servers, one on each VLAN, providing that the router/Layer 3 switch connecting the VLANs has DHCP forwarding capability (also known as DHCP Relay, or IP Helper on certain vendor equipment).

One of the options that the IP phone obtains is the IP address of the call server or in the case of a 3300 ICP the IP address of the RTC (Real Time Complex). Since the IP address in this DHCP option is not dynamic, this IP address must be pre-assigned statically within the call server (or 3300 ICP) before the call server is connected to the network.

The sequence above assumes that the phones get information from a DHCP server. The information can also be manually entered into a phone as it starts to boot up, to make sure the information is fixed and requires little DHCP intervention. This method is particularly useful if a phone is used on a remote WAN link and the router cannot forward DHCP requests, or if a local DHCP server does not exist. It is also useful on VPNs, for the same reasons.

> **Note:** When the call server is a 3300 ICP, it is recommended that the internal 3300 ICP TFTP server be used. An external TFTP server can be used, but then it is important to ensure that the software downloads maintain version control with upgrades that are applied to the ICP, using the most recent software versions available. In a multiple-ICP installation with multiple versions, this can become network management overhead.

Information on how to program the MiVB's integral DHCP server can be found in the MiVB System Administration Tool Help file, this file is available on the MiVB and on Mitel online.

LLDP-MED and IP Phone network policy

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is based on VoIP-specific extensions to the IEEE 802.1AB LLDP standard. LLDP is the IEEE neighbor discovery protocol and allows information to be gathered from network devices such as switches and wireless access points. The information gathered with LLDP, aids in troubleshooting and provides data to management systems so that management systems can create accurate views of the network’s topology.

LLDP-MED allows for information sharing between VoIP endpoints such as IP phones and network devices such as L2 Ethernet switches.

LLDP-MED can be used to simplify the deployment of IP phones with auto-discovery. This means that IP phones can auto-discover network policy from an LLDP-MED compliant L2 switch to obtain the following network policy information:

- VLAN (802.1.Q) information
- QoS L2 Priority (802.1p) information
- DSCP (L3 Priority) information.

Notes Regarding LLDP-MED

Network loading

Traffic from LLDP-MED packets will not cause network loading problems. The packets are sent from the phone to the L2 switch and vice versa and since these packets are not forwarded by L2 switches, the packets remain only on this LAN segment.

Simplifying IP Phone deployment

LLDP-MED can be used in conjunction with DHCP options to provide the phone with network policy information. Using LLDP-MED can remove the requirement to program the DHCP server with VLAN, L2 QoS priority, and DSCP priority information. LLDP-MED can also remove the need to enable DHCP forwarding in the general routing infrastructure.

> **Note:** Some DHCP interaction is still required to provide IP Phones with the IP address of the call server (or ICP) and TFTP server. In cases where DHCP servers are being used, DHCP forwarding (IP Helper) will still need to be enabled on routers, however, with LLDP-MED used to provide LAN policy (VLAN in particular) this will only be needed in the voice VLAN.

LLDP-MED and using scopes

In many situations, especially where part of the network uses different LAN policy from other parts, use of LLDP-MED may simplify network configuration. The appropriate LAN policy values can be applied directly to the L2 switching gear in each section of the LAN separately, rather than creating and managing multiple scopes in the DHCP server. Alternatively, a general policy could be provided in DHCP servers and LLDP-MED used to override it locally in some segments.

Use of LLDP-MED to supply LAN policy also avoids the necessity to “double boot” at IP Phone startup time (once to obtain the voice VLAN ID, then a second time to obtain an IP address and other configuration on the voice VLAN). (Note that that the 69xx series of IP phones do not require a “double boot). With this method, it may also be easier to use the 3300 embedded DHCP server to provide only the remaining configuration values, with LAN policy coming from LLDP-MED, removing the need for any Mitel-specific configuration in 3rd party DHCP servers.

LLDP-MED and network troubleshooting

Through SNMP MIBs defined by LLDP-MED, several highly useful tools are provided for network troubleshooting by querying the L2 switching infrastructure through standard network management tools.

- Inventory Type Linked Values (TLVs) can be used to determine the VoIP endpoint’s manufacturer, model, hardware, firmware, and software versions, etc.
- The device’s physical location can be determined using the Location Identification TLV (if they have been configured into the L2 switch).
- Network policy issues can be identified by comparing the endpoint device’s and the switch’s LAN policy in use, using the Network Policy TLV.
- LAN speed/duplex mismatches can be identified by comparing the MAC/PHY Configuration/Status TLV for the L2 switch and the endpoint.

LLDP-MED can be used to report information about the attached phone. The list of phones below will report the following information:

- The Hardware revision reports “PCB Version: ...”
- The Firmware revision reports “Boot ...”
- The Software revision reports “Main ...”
- The Manufacturer reports “Mitel Corporation”

The following phones support LLDP-MED and report the following Model names.

Table 12 Phones and LLDP-MED Names

Phone Model	Name Reported in LLDP-MED
5212 Dual Mode	“MITEL 5212 DM”
5215 Dual Mode	“MITEL 5215 DM”
5220 Dual Mode	“MITEL 5220 DM”
5224 Dual Mode	“MITEL 5224 DM”
5235 Dual Mode	“MITEL 5235 DM”

Phone Model	Name Reported in LLDP-MED
Navigator	“MITEL NVGT”
3000 IP	“TELEMATRIX 3000IP”
5304 IP Phone	“MITEL 5304 IP”
5312 IP Phone	“MITEL 5312 IP”
5320 Dual Mode	“MITEL 5320 DM”
5320e	“MITEL 5320e IP”
5324 IP Phone	“MITEL 5324 IP”;
5330 Dual Mode	“MITEL 5330 DM”
5330e	“MITEL 5330e IP”
5340 Dual Mode	“MITEL 5340 DM”
5340e	“MITEL 5340e IP”
5360 Dual Mode	“MITEL 5360 DM”
5540 Dual Mode	“MITEL 5540 DM”
MiVoice Video/Conference	“UC360”
6731i	"MITEL 6731i"
6735i	"MITEL 6735i"
6737i	"MITEL 6737i"
6739i	"MITEL 6739i"
6865i	"MITEL 6865i"
6867i	"MITEL 6867i"
6869i	"MITEL 6869i"
6873i	"MITEL 6873i"
6905	“MINET_6905”
6910	“MINET_6910”
6920	“MINET_6920”
6930	“MINET_6930”
6940	“MINET_6940”
6970	“MINET_6970”

IP Phones and VLAN programmability

Table 13 lists which VLAN programming mechanisms are supported on a per phone basis.

Table 13 IP Phones and VLAN programmability

Device	IEEE 802.1AB LLDP-MED Support	VLAN Programmability
5001	No	Yes: CDP and DHCP
5005	No	Yes: CDP, DHCP, and Static
5010	No	Yes: CDP, DHCP, and Static
5020	No	Yes: CDP, DHCP, and Static
5201	No	Yes: CDP and DHCP
5205	No	Yes: CDP, DHCP, and Static
5207	No	Yes: CDP, DHCP, and Static
5212	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5215	No	Yes: CDP, DHCP, and Static
5220dm	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5215dm	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5220	No	Yes: CDP, DHCP, and Static
5224	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5230	No	Yes: CDP, DHCP, and Static
5235	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5302	No	Yes: DHCP
5304	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5312	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5320	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5320e	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5324	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5330	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5330e	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5340	Yes	Yes: LLDP-MED, CDP, DHCP, and Static

Device	IEEE 802.1AB LLDP-MED Support	VLAN Programmability
5340e	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5360	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
Navigator	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
3000IP	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
5140	No	Yes: CDP, DHCP, and Static
5240	No	Yes: CDP, DHCP, and Static
5485IP Pager	No	Yes: CDP and DHCP
5505	Yes	Yes: LLDP-MED, CDP, and DHCP
5550-TKB	No	Yes: CDP and DHCP
5560 IPT	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
MiVoice Video/Conference	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
6731i	Yes	Yes: LLDP, DHCP and Static
6735i	Yes	Yes: LLDP, DHCP and Static
6737i	Yes	Yes: LLDP, DHCP and Static
6739i	Yes	Yes: LLDP, DHCP and Static
6865i	Yes	Yes: LLDP, DHCP, and Static
6867i	Yes	Yes: LLDP, DHCP and Static
6869i	Yes	Yes: LLDP, DHCP and Static
6873i	Yes	Yes: LLDP, DHCP and Static
6905	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
6910	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
6920	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
6930	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
6940	Yes	Yes: LLDP-MED, CDP, DHCP, and Static
6970	Yes	Yes: LLDP-MED, CDP, DHCP, and Static

RFC 3942, reclassifying DHCP options: DeTeWe Phones

DeTeWe has provided a solution for their DECT phones regarding the DHCP options reclassification, however, it is not aligned with the Mitel solution and will require custom configuration of the DHCP servers. For details, refer to DeTeWe documentation.

5302 Startup and DHCP

DHCP options will be used to inform the 5302 of servers that can be contacted to register and retrieve the profiles.

RFC 3925, Vendor-Identifying Option exchange (options 124/125) will be used as the primary mechanism for conveying the addresses of these servers.

The 5302 will transmit a DHCP discover message containing the option 55 (Parameter Request List). Within the request list, each endpoint will include option 124 (Vendor Class Identifier).

Option 124 will be used in the parameter request list as the primary method of specifying the vendor-specific information. This option solicits retrieval of option 125, vendor-specific information, which is returned by the server.

Option 125 will include the address of the 3300 ICP that is to be used as the primary SIP contact point (REGISTRAR). Additional information may be included, such as Layer 2 priority, voice LAN identification (VLAN) and QoS (DSCP), which is used to define packet priority for the IP layer. When these tags are presented in the option 125 response, they will override any associated values found within the local-network or device profile.

DHCP Option Reclassification

With the exception of 69xx series sets, Mitel’s legacy IP device configuration approach, using DHCP options 128 – 135 is still supported, but the preferred methods based on either DHCP options 124/125 or 60/43 are recommended. The standards-based options (124/125 and 60/43) will remove potential DHCP conflict with other devices and manufactures that may be using the same DHCP server for optional information.

The following three points contain general information about the supported Client DHCP Discovery method:

1. RFC 3925 Vendor-Identifying Option exchange (options 124 / 125).
   Option 125 is used to return the vendor-specific configuration in response to option 124 containing the Mitel enterprise number (1027 decimal).
   For MiVoice IP Phones, this option will contain the following sub-fields:
   - *enterprise-number* = 1027 (decimal), the IANA-registered Mitel Enterprise Number
   - *data-len* = length of the following configuration string
   - *vendor-class-data* = Mitel-specific configuration string, as defined in 0 DHCP Vendor information data format (options 125 and 43).
2. RFC 2132 Vendor Class based exchange (options 60 / 43)
   Option 43 is used to return the vendor-specific configuration in response to option 60 containing the Mitel identification string (“ipphone.mitel.com”).
   For Mitel IP Phones, this option will contain only the following sub-fields:
   - vendor-specific-information = Mitel-specific configuration string, as defined in 0 DHCP Vendor information data format (options 125 and 43).

3. Legacy Options 128-135 (for backwards compatibility only) This
In this response, the DHCP server returns options 128 – 135 shown in Table 14 Mitel DHCP Option Usage, and any Mitel partner-specific options. If the 3300 ICP embedded DHCP server does not receive option 124 or option 60, it will also respond this way, if configured to do so for these options. If these options were previously configured in the 3300 ICP DHCP server, they will already be in place (they are not deleted as a result of an upgrade), however they may need to be configured in a new installation if the IP Phones on the site were previously on a system with Active Software Release of 7.0 or earlier. The options will be needed to allow these IP Phones to be upgraded when they first boot up.

> **Note:** Legacy Options 128-135 are not supported on 69xx series IP sets.

Table 14 Mitel DHCP Option Usage

DHCP option	Field Type	Description
3	IP address	Default Gateway (Router) IP address
6	IP address	Preferred DNS IP address (used by Webset, PDA phone only)
44	IP address	Preferred WINS address (used by PDA phone only)
120	IP address	SIP outbound proxy address
128 (Note 1)	IP address list	TFTP Server IP address (for software loads)
129 (Note 1)	IP address list	ICP IP address list
130 (Note 1)	string	Mitel server discrimination string: “MITEL IP PHONE”
131 (Note 1)	IP address	Remote IP Phone Analyzer IP address
132 (Note 1)	long word	802.1Q Layer 2 VLAN ID
133 (Note 1)	long word	802.1Q/D Layer 2 Priority
134 (Note 1)	long word	Diffserv Code Point (DSCP)
135 (Note 1)	string	HTTP Proxy for phone-specific applications

> **Note:** Legacy Options 128-135 are not supported on 69xx series IP sets

Unused options MUST be left blank. Conflict may arise where a number of different devices exist within the same subnet or DHCP scope (e.g. it is known that Microsoft Server 2003 also uses options 132 and 133). It may be necessary to redefine options, or place some equipment in different scopes, or select options based on device MAC address. Otherwise phones will read this information and may give unpredictable results.

IP Phone behavior

The IP Phone is very forgiving of information received through DHCP. It will allow for any of the three possible methods mentioned for delivery of the configuration, and within the vendor-specific methods will account for variability found in how 3rd Party DHCP servers deliver option 43 or option 125 formats.

The following behavior rules apply to the IP Phone for received DHCP parameters:

- IP Phone will accept any one of the three methods; option 125, option 43, or for 5200 and 53xx series sets - options 128-135, in order of priority,
  - If more than one method is received in the same DHCP offer, the one with highest priority will be applied.
- Within option 43 or option 125 responses, the IP Phone will accept the following formats from the DHCP server side:
  - Option 43 or 125, with no sub-options.
  - Option 43 or 125, containing a single sub-option, ID = 1.
  - Within the sub-option method, the final sub-option may be ID 0xFF, the "end of options" option (as per RFC 2132).
  - Within any of above, you may have to null-terminate with a 0x00 character.

3. The "Encapsulated vendor-specific options" formatting as defined in RFC 2132 and RFC 3925 is not normally used in the Mitel-specific exchange, however it is accommodated by the IP Phone in order to support 3rd party DHCP severs that require it.

DHCP Vendor information data format (options 125 and 43)

For vendor information returned in either options 125 or 43, the following common string encoded vendor identifier is used followed by one or more string encoded tag/value pairs:

"id:<mitel_id><separator><tag/value>
<separator><tag/value>... "

where:

<mitel_id> is the Mitel discrimination string "ipphone.mitel.com",
<separator> is a separator special character ';'

For each <tag/value> pair, encoding is in the form: "<tag>=<value>"

The following rules apply to parsing of all tag/value pairs. The internal DHCP Server applies these tag/value parsing rules. For an external server, you will need to apply the rules to the tag/value pairs defined in Table 15 Tag / Value pair Definitions:

- Configuration string is case sensitive and parsed left to right.
- The overall configuration string is led by the "id:<mitel_id><separator>" sequence, which MUST appear before any tag/value pairs;
- End of the configuration string is determined by data length of the enclosing format (option 43 or option 125), i.e. there is no internal length field or end-of-string tag, and no trailing separator is required (however trailing separator(s) are permitted).
- Tag/value pairs may appear in any order and may repeat. If there is a repeat, later items delete and then overwrite previous ones.
- All integer values are decimal encoded (no hex or binary).
- Null <value> in the configuration line (i.e. "<tag>=") indicates the value is not configured.
- All IP address values are assumed to be IPv4, encoded in dot-decimal notation (xxx.xxx.xxx.xxx). Leading 0s are permitted but not required. Specific port can be indicated by "<IP address>:<port>".

- Host fully qualified domain names (FQDNs) are encoded as “<host>.<domain>” or by IP address as above. File paths at a particular host may be encoded as “<FQDN>/<path>. Specific port can be indicated by “<FQDN>:<port>”.
- Space characters are allowed in the string only between tag/value pairs (i.e. at separators) or at beginning or end of line and are ignored.
- Final separator is allowed, but not required.
- Multiple back-to-back separators are permitted, and are ignored (e.g. “;;<tag/value>” is OK).
- tag/value separators: ; (semicolon)
- list item separator: , (comma)

Table 15 Tag / Value pair Definitions - 52xx & 53xx Sets

Type (old option)	Tag	Data Type	Description
SW load TFTP server IP address (128)	sw_tftp	IP Address list	TFTP server IP address, to retrieve software loads
Call Server (ICP) IP address (129)	call_srv	IP Address list	1 to 4 ICP IP addresses
Remote Analysis Server IP (131)	ipa_srv	IP Address	1 IP address (port optional)
Voice VLAN ID (132)	Vlan	Integer	IEEE 802.1Q VLAN ID (0 - 4095)
Voice L2 Priority (133)	l2p	Integer	IEEE 802.1Q/D L2 priority value (0 - 7)
Voice Diffserve Code Point (134)	dscp	Integer	RFC 2474 DSCP (0 - 63) for voice and MiNET signaling.
Voice appliance HTTP Proxy (135)	app_proxy	FQDN:port	1 FQDN (port optional), FQDN string length max 40 characters

Example: id:ipphone.mitel.com;sw_tftp=10.37.20.11;call_srv=10.37.18.11,10.37.10.11; vlan=1056;l2p=6;dscp=46

> **Note:** Legacy Options 128-135 are not supported on 69xx series IP sets.

DHCP Lease Time

To allow users to move off the local subnet, or to let new users join a subnet, a method is needed to give up an IP address and to obtain a new address. If a phone is disconnected, it obviously cannot talk to the DHCP server, so another method is needed to free up unused addresses. DHCP lease time clears out unused IP addresses and makes them available for new requests.

The timer can be set from a few minutes to months. The default is set to **8 hours**, which keeps the amount of checking to see if an IP address is still in use to a reasonable level while providing adequate recovery time to free up any unused addresses.

The exact lease time to use depends upon the system requirements. If there are plenty of spare addresses, then the lease can be extended. Some users will specify up to a week to allow a system to maintain the same IP addresses over a long weekend when power is removed. If addresses are less available, and phones are more mobile, shorter times are preferred.

> **Note:** It is possible to run out of IP addresses with permanent leases, so Mitel recommends minimizing use of these addresses. For example, a laptop user who roams from office to office plugs in the laptop, receives a permanent address, and then disconnects the device. The IP address is never released by the user, and the address is never handed out to another user because the lease never expires. Eventually the server can run out of addresses.

IP Phone Stands

The Gigabit Ethernet phone stand can be installed in place of the regular phone stand on 5200/53xx series IP phones.

The IP DECT phone stand can be installed in place of the regular phone stand on some 53xx series IP phones.

Table 16 indicates which phones support the Gigabit Ethernet and IP DECT stands. The following sections discuss the IP phone stands in detail.

Table 16 Phone Stand Support - Listed by IP Phone Model Number

Phone	Gigabit Ethernet Stand Support	IP DECT Stand (for 5610 DECT Handset) Support
5001	No	No
5005	No	No
5010	No	No
5020	No	No
5201	No	No
5205	No	No
5207	No	No
5212	Yes	No
5215	No	No
5220 Dual Mode	Yes	No
5215 Dual Mode	Yes	No
5220	No	No
5224	Yes	No
5230	No	No
5235	Yes	No
5302	No	No
5304	No	No
5312	Yes	Yes
5324	Yes	Yes
5320	Yes	Yes

Phone	Gigabit Ethernet Stand Support	IP DECT Stand (for 5610 DECT Handset) Support
5320e	Not Applicable	Yes
5330	Yes	Yes
5330e	Not Applicable	Yes
5340	Yes	Yes
5340e	Not Applicable	Yes
5360	Not Applicable (Phone has a Gigabit Ethernet interface)	Yes
5505	No	No
3000IP	No	No
5140	No	No
5240	No	No
5485IP Pager	No	No
5540	No	No
5550-TKB	No	No
5560 IPT	No	No
MiVoice Business Console	Not Applicable	Not Applicable
Navigator	No	No
MiVoice Video/Conference	Not Applicable	Not Applicable
6905	Not Applicable	Not Applicable
6910	Not Applicable	Not Applicable
6920	Not Applicable	Not Applicable
6930	Not Applicable	Not Applicable
6940	Not Applicable	Not Applicable
6970	Not Applicable	Not Applicable

> **Note:** The 67xx and 68xx series of sets do not support the Gigabit Ethernet Stand or the IP DECT Stand.

Gigabit Ethernet Phone Stand

The Gigabit Ethernet Phone Stand allows a 5200/53xx series IP phone to be interfaced to a Gigabit Ethernet LAN. Details on the Gigabit Ethernet Phone Stand can be found in the Gigabit Ethernet Stand Installation Guide found on Mitel's Document Centre.

Gigabit Ethernet Cabling Restriction

- 1000Base-T (Gigabit Ethernet) must be run on Category-5 or better cabling plant. It is recommended that the cabling plant be tested and certified for Gigabit Ethernet operation. This is particularly important in cases where Gigabit Ethernet equipment is being deployed into existing 100Base-T Category-5 networks.

> **Note:** Category 3 cabling plant will not support Gigabit Ethernet operation.

Gigabit Ethernet Phone Stand, Power Restrictions

When IP Phones have the following Mitel accessories installed, the additional power required by the Gigabit Ethernet Stand itself can result in the total required power exceeding the limits of IEEE 802.3af PoE standard.

- 5330, 5340, and 5324 IP Phones with a Conference Unit Module and the Mitel Conference Unit it connects to must use a power adapter that is sold separately and connects directly to this stand.
- 5220, 5224, and 5324 IP Phones with a PKM module and the PKMs it connects to must use a power adapter that is sold separately and connects directly to the Stand.
- The Side Control Unit used to connect a Mitel Conference Unit to a 5220/ 5224 will still need its own 24Vdc power supply and should be connected to the IP Phone as usual. It also requires that the phone and stand be powered using a power adapter that is sold separately and connects directly to this Stand.
- 5330 and 5340 IP Phones that have a cordless handset and/or headset installed must use a power adapter that is sold separately and connects to this stand.

IP DECT Phone Stand for 5610 DECT Handset

The Mitel 5610 DECT Handset and Mitel IP DECT Stand are IP Phone accessories that offer a low-cost wireless solution for personal area mobility on IP Phones.

The stand gives the IP Phone the ability to interface with up to eight 5610 DECT handsets, and it supports three simultaneous calls.

To determine which Phones can be used with the IP DECT Phone Stand, refer to Table 16 Phone Stand Support - Listed by IP Phone Model Number. Additional information related to the IP DECT Phone Stand can be found on Mitel's Document Centre.

DECT Solutions

Mitel offers two different DECT telephony solutions:

- The SIP-DECT solution provides users with SIP-DECT mobile phones and utilizes SIP-DECT access points to provide connectivity between the DECT environment and the customer's LAN.

- Mitel also offers DECT accessories (phone DECT modules, headsets, and handsets) for the 53xx and 69xx series of IP phones. This solution uses the phone as a DECT access point for the handset or headset that is associated with the particular phone.

Cordless (DECT) phones, handsets and headsets offer the option of mobile telephony for enterprise phone users.

The customer's requirements will determine whether it would be better to use DECT accessories with 53xx and/or 69xx phones or to deploy a Mitel SIP-DECT System with DECT phones, which requires the installation of DECT access points - called Radio Fixed Parts (RFP) in the enterprise.

From the user's perspective, the basic difference between these two solutions is that the 53xx/69xx DECT accessories solution allows users to move limited distances away from their desks within their office or adjacent offices while holding a telephone conversation. The SIP-DECT solution provides users with the ability to roam throughout the enterprise while holding a phone conversation.

These two solutions should not be operated in parallel since both solutions will be competing for DECT channels. Operating both solutions in parallel may cause users to experience degraded audio quality and should no DECT channels be available, users may not be able to place a phone call.

Some customers may have users that do not need to move away from their desk/offices and other users who do need to roam throughout the enterprise - in cases such as this it is recommended that the SIP-DECT System be deployed.

If a customer has a future requirement to support enterprise wide roaming for users, or the customer has future requirements to support a higher DECT deployment density than is allowed with 53xx/69xx DECT handsets and headsets, then it is recommended that the SIP-DECT System be deployed.

SIP-DECT Solution

The SIP-DECT solution is not covered in detail in this document. There is a complete suite of supporting documentation available for the SIP-DECT solution on Mitel's web site.

DECT Accessories for Phones

The following sections discuss the DECT accessories that are available for the 53xx and 69xx series of IP phones. Deployment considerations and detailed deployment guidelines are also covered.

53xx Series of Phones

A cordless (DECT) Handset and Headset are supported on the 5330, 5330e, 5340, 5340e and 5360 IP phones.

The 53xx DECT accessories support Narrowband audio and the DECT radios transmit at a High-Power setting. Narrowband audio provides the user with an audio frequency response similar to that of traditional land line telephone. The 53xx DECT accessories do not support Wideband or Low Power settings.

A Cordless Module must be installed into the back of the IP Phone to allow operation with the Cordless Accessories. For details see the Cordless Module and Accessories Installation Guide for Mitel 5330, 5340 or 5360 IP Phones available at Mitel's Document Centre.

69xx Series of Phones

A cordless (DECT) Headset is supported on the 6930 and the 6940 IP phones.

The 69xx cordless DECT Headset offers both Narrowband audio and Wideband audio operation. Narrowband audio provides the user with an audio frequency response similar to that of a traditional land line telephone. Wideband audio provides the user with an enhanced audio frequency response for Hi-Fi sound.

> **Note:** Wideband audio mode requires two DECT radio channels per DECT device and Narrowband audio mode requires one DECT radio channel per DECT device. In environments where there are many DECT devices, the headsets may need to be configured for Narrowband operation to minimize DECT radio channel consumption and also to avoid a long delay-to-audio time.

The DECT Cordless Module must be installed into the side of the IP Phone to allow operation with the DECT Cordless Headset. For details refer to the 69xx Installation Guide, available at Mitel's Document Centre. The 69xx cordless DECT Headset solution can be configured for High Power or Low Power radio transmission.

When the 69xx DECT headset is configured for High Power operation, the user will have the greatest roaming range. When the 69xx DECT headset is configured for Low Power operation, under some circumstances higher density deployments may be possible, but the roaming range will be reduced.

Important: To ensure correct operation, all Mitel DECT devices in the same area must be set to the same RF (Radio Frequency) transmit power level. In situations where both 53xx and 69xx DECT accessories are deployed, the 69xx DECT accessories should be configured for High Power operation, so that they match the 53xx DECT accessory RF power level.

69xx Phones - Default DECT Settings

The 69xx DECT headset default (factory) settings are Wideband audio operation enabled, and High Power operation enabled. Changing these settings is accomplished with a Class of Service (CoS) option within the call control server management interface. For details on how to reconfigure the 69xx DECT headset for Narrowband operation or Low Power operation refer to the appropriate call control server documentation.

DECT Modules and Accessories

The Mitel DECT Modules and Accessories (Handset and Headset) come in two variants. The first works in the Standard DECT RF band of 1880 - 1900 MHz, the second is a DECT 6.0 variant that works in the RF band of 1920 - 1930 MHz.

Table 17 DECT Module and Accessory Part Numbers

Description	Mitel Part Number	Part Marking
Standard DECT Cordless Module for 53xx sets	56008567B	56008567B
DECT 6.0 Cordless Module for 53xx sets	56008567A	56008567A
Standard DECT Handset for 53xx sets	56008564B	56008564B
DECT 6.0 Handset for 53xx sets	56008564A	56008564A
Standard DECT Headset for 53xx sets	57008904	100-79330049-00
DECT 6.0 Headset for 53xx sets	57008905	100-79330059-00
Standard DECT Headset (Integrated) for 69xx sets	51305334	51305334
DECT 6.0 Headset (Integrated) for 69xx sets	51305332	51305332
Replacement DECT Headset (FRU) for 69xx sets (Used for both North America and Europe)	51305335	51305335

Which Device Variant should be used in a Particular Location?

DECT 6.0 products must not be used in Europe or Africa, due to interference with the European and South African cellular networks. Use of DECT 6.0 is prohibited by European Telecommunications Authorities and the Independent Communication Authority of South Africa.

Standard DECT products must not be used in the United States or Canada due to interference with American and Canadian cellular networks, Standard DECT usage is prohibited by the Federal Communication Commission and Industry Canada.

- For operation in the United States and Canada, use DECT 6.0.
- For operation in the United Kingdom and Europe, use Standard DECT.
- For operation in other Countries or regions, refer to http://www.dect.org to determine which variant is appropriate.

Upgrading DECT Accessory Firmware

Mitel supports the use of DECT accessories manufactured by Jabra, Plantronics, and Sennheiser. The Mitel integrated DECT cordless modules are manufactured by Jabra.

Should it be necessary to upgrade a DECT accessory, firmware upgrades may be obtained from the following sites:

https://www.jabra.ca/software-and-services/jabra-direct

https://www.plantronics.com/ca/en/support/downloads-apps/hub-desktop

https://sennheiser.zendesk.com/hc/en-us/articles/217979228-Installing-Updater

DECT Naming Conventions and Definitions

The reader should make themselves familiar with the following naming conventions and definitions before proceeding.

When planning a SIP-DECT or a DECT phone accessory installation, the key considerations for the end users are coverage and capacity, however the Administrator will need to take operating range and density into consideration as they are directly related to coverage and capacity.

- **DECT Operating Range** is the maximum distance - in a straight line - that can be placed between the headset/handset and the IP phone or the headset/handset and the RFP while still maintaining a connection.

  The DECT Operating Range can be graphically represented as the radius of a circle, with the center being the location of the IP phone and the radius being the length from the center to the maximum operating range.

- **DECT Coverage Area** refers to how far away from their desk a user can roam in any direction and still maintain a connection between the headset/handset and the IP phone. In a SIP-DECT system the DECT Coverage Area and the DECT Operating Range is the same.

  In a room with no RF obstructions, the outside edge of the DECT Coverage Area could be graphically represented as the perimeter of a circle, with the center being the location of the IP phone. Coverage is directly related to the DECT operating range.

- **Call Capacity** refers to how many simultaneous telephone calls can be supported when using DECT headsets or handsets. Capacity is a function of how many DECT channels are available in a DECT Coverage Area and how many DECT channels are required to support the phone calls.

- **Density** is the term used to describe how many DECT users can be successfully placed in a DECT Coverage Area.

DECT Deployment - Key Considerations

Following are the key considerations that need to be kept in mind when planning a DECT accessory deployment.

How physically close will the DECT users be to each other?

- The Administrator should have a floor plan that indicates the proposed locations of the DECT users. The minimum recommended user to user spacing is 2 metres (6.5') and is addressed in the section called DECT Capacity.

- There is no limit on how far apart DECT users may be located from each other, in some instances where the number of available DECT channels is insufficient in an area - increasing the user to user spacing will alleviate channel availability issues.

Why is it important to adhere to the minimum user to user spacing?

- If the minimum user to user spacing is not adhered to, the total number of available DECT channels will be reduced. The reason for this is that the DECT devices will stop using channels adjacent to each other in an attempt to prevent adjacent channel interference.

What is the DECT Operating Range?

- The DECT Operating Range is the straight-line distance that a user can roam away from their desk while still maintaining a connection between the headset and IP phone. The DECT Operating Range can vary a great amount based on factors in the operating environment such as obstructions and interference.

- In situations where there is only one, or a small number of DECT users and no RF obstructions, the DECT Operating Range may be used to give an indication of the dimensions of the DECT Coverage Area, which is the area that users can successfully roam from their IP phone sets.

- In situations where there are multiple groupings of DECT users in the building, the DECT Operating Range will help to determine if the multiple groups should be treated as one large group of DECT users, or if it is determined that there is 'dead RF space' between the groups, the groups may be treated as separate groupings of DECT users.

This topic is discussed in the section called DECT Operating Range, actual DECT Operating Ranges will be determined with an RF site survey.

Are there enough DECT channels available to simultaneously support the number of users in the DECT Coverage Area?

- DECT channels in a DECT Coverage Area are a finite resource, the theoretical number of DECT channels available in a DECT Coverage Area varies from 30 to 120 channels, depending on the Country/Region of the installation, and if the devices are configured for narrowband or wideband operation.

- DECT channel availability is discussed in the section called DECT Density. If there is a preexisting DECT system or systems at the site, an RF site survey will be required to determine the existing DECT channel availability in the proposed deployment area.

Deploying Phones with DECT Accessories - Simple Guidelines

When deploying DECT accessories it is necessary to do some degree of advance planning to ensure good voice quality and a high signal to noise ratio. These simple guidelines apply to both Standard DECT and DECT 6.0.

A successful DECT accessory deployment will be based on complying with a minimum phone to phone spacing and maintaining an average area per DECT accessory. There can be situations where too many DECT devices in a confined area will perform poorly due to radio interference, and this will result in poor voice quality.

The quantity of DECT devices that can be successfully deployed in a particular area depends on many factors, such as, the size of the area, furnishings, carpeting, walls, the presence of metallic objects or large glass areas and the DECT radio settings.

Because of the nature of radio technology, the following simple guidelines are intentionally conservative, in some instances, the Administrator may achieve better device density, and in some cases results may be worse.

Number of DECT Accessories

The DECT device deployment should be successful if the number of DECT devices in an area is kept below the following limits:

- Standard DECT (Europe) Narrowband - Less than 60 DECT devices
- Standard DECT (Europe) Wideband - Less than 30 DECT devices
- DECT 6.0 (North America) Narrowband - Less than 30 DECT devices
- DECT 6.0 (North America) Wideband - Less than 15 DECT devices

If the number of DECT devices in an area is equal to or exceeds the above recommendations, refer to the section called Deploying Phones with DECT Accessories - Detailed Guidelines.

When counting devices, a DECT headset is counted as a device and a DECT handset is counted as a device, for a simple deployment it is recommended to have only one DECT device per IP phone. For details on supporting two DECT devices per IP phone, refer to the Detailed Guidelines.

Device to Device Spacing

A device to device spacing of at least 2 to 4 metres (7 to 13 ft) should be adhered to, even if the number of devices is well below the number of DECT accessories listed above.

Deployment Area

Identify the area where the DECT devices are to be deployed; an area is a separate isolated section of office space, and each are needs to be considered one at a time. Measure the area and ensure that the desired number of DECT devices can be deployed in this area while complying with allowed number of DECT devices and the device to device spacing rule.

DECT Settings

As indicated above, the use of Wideband audio reduces the allowable number of devices in an area by half.

Configuring the DECT devices for Low Power operation will improve device performance in a dense installation, but it will also reduce the Operating Range and area.

> **Note:** All DECT devices in a given area must be configured to operate at the same transmit power setting.

DECT Accessory Utilization Rates

When planning for DECT capacity, the Administrator should always assume a 100% headset/handset utilization rate.

If average utilization rates are used, the lack of an available channel - which could happen if there are more calls than then the average utilization rate - will result in of loss of communication between a headset/handset and a base, and the IP phone will need to be rebooted to reestablish pairing.

Other DECT Systems

If there are any other DECT systems, telephony accessories or DECT WLAN systems operating in the area - the number of channels utilized by these systems must be accounted for when determining how many DECT devices will be operating in the area.

Deploying Phones with DECT Accessories - Detailed Guidelines

The first step *prior* to planning a DECT deployment is to determine if a Radio Frequency (RF) site survey is or is not required.

If it is decided that an RF site survey is required, the survey should be completed, and the survey results evaluated to determine if there is anything that will impact the deployment of DECT solutions.

For recommendations on whether or not an RF site survey is required, refer the sections on RF Site Survey and DECT Coverage and Capacity Planning.

The following sections provide the Administrator with a detailed procedure for planning a DECT accessory deployment.

DECT Device-to-Device Minimum Spacing Guidelines

For both Standard DECT (Europe) and DECT 6.0 (North America) the spacing between the IP phones (DECT base stations) should comply with the following rule:

There should be 2 meters (6.5 feet) between IP phones - on all three axes.

Warning: To comply with the spacing rules on the vertical axis, the Administrator should avoid installing DECT devices on adjacent floors directly above or below the proposed deployment area.

Should installation on adjacent floors be desired, an RF site survey should be conducted to determine if the RF attenuation factor of the building's floors/ceilings are adequate to isolate DECT devices on adjacent floors from each other.

The following diagram shows 25 phones (as black dots) each phone has one DECT device installed and the phones are deployed with the recommended minimum phone-to-phone spacing of 2 metres (6.5') in an area of 100 sq metres (1075 sq ft).

Assuming that this environment is devoid of any RF interference and that there are no other DECT devices or DECT systems operating in this area consuming DECT channels, the following guidelines may be used:

- When all the DECT devices are configured for **High Power and Narrowband operation** - all **25 DECT** devices should be able to operate simultaneously.
- When all the DECT devices are configured for **High Power and Wideband operation** - **15 DECT** devices should be able to operate simultaneously.

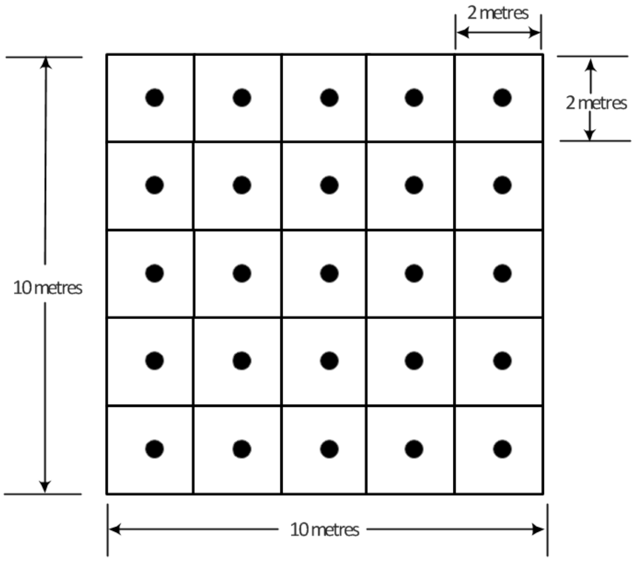

Figure 4 DECT Device-to-Device Minimum Spacing Guidelines

Device-to-Device Spacing of Less Than 2 Metres

Under some circumstances, the Administrator may be able to achieve slightly higher DECT device densities by operating **all** of the DECT devices at the **Low Power** setting, and by ensuring that cubicle walls - that offer some degree of RF attenuation - are in place between the DECT devices.

However, the Administrator should be aware that when the minimum DECT device-to-device spacing of 2 metres (6.5') is violated, the number of usable DECT channels will be reduced as the DECT radios attempt to prevent adjacent channel interference. Calculations indicate that the number of available channels may be reduced by up to 66%. *Spacing of less than 2 metres between DECT devices is not recommended by Mitel.*

Note: In scenarios where multiple DECT devices are deployed in very close proximity to each other (< 2 meters between sets) and IP sets are programmed to be in collective ring (all-ring) groups, Mitel recommends not exceeding a total of 14 DECT devices (14 IP Phones with 1 DECT handset or headset each, or 7 IP Phones with both DECT handset & headset).

Exceeding these limits could lead to choppy audio, one way audio, dropped calls or a loss of DECT pairing, which then requires the IP phone to be reset to recover.

DECT Operating Range

The DECT standard sets the RF output level of a DECT Cordless Module at +20 dBm, and the minimum receive field strength is set at -83 dBm. This means that there is a theoretical operational RF signal strength budget of approximately 100 db.

This budget is dependent on a number of environmental factors and in practice is reduced to a range of 85 db. This budget may be further reduced depending on the characteristics of the actual product implementation.

The theoretical Operating Range when the DECT device is configured for High Power transmission in an unobstructed open space (free air) can range from 90 meters to 300 meters (295’ to 984’). However, because the open space RF signal strength is greatly reduced at ranges in excess of 90 metres, the practical open space Operating Range is 90 metres.

The Operating Range in a typical office environment will be significantly less than the open space ranges due to RF obstructions, reflections and RF interference.

For planning purposes, the Administrator should use the following practical DECT Operating Range values.

Table 18 RF Practical DECT Operating Range Values

53xx DECT Devices	69xx DECT Devices	Open Space	Typical Office
Handset High Power	Handsets are not available for 69xx phones	90 metres (295 feet)	50 metres (164 feet)
Headset High Power	Headset High Power	90 metres (295 feet)	30 metres (98 feet)
53xx devices do not support Low Power operation.	Headset Low Power	50 metres (164 feet)	16 metres (52 feet)

Important: To ensure correct operation, all Mitel DECT devices in the same area must be set to the same RF (Radio Frequency) transmit power level. In situations where there are both 53xx and 69xx DECT accessories are deployed, the 69xx DECT accessories should be configured for High Power operation (default setting), so that they match the 53xx DECT accessory RF power level.

Based on the building materials and the number and type of obstructions within the operating space, you can roughly calculate the coverage area for an individual DECT accessory. However, it is still necessary to carry out measurements and if necessary, a thorough planning and RF survey to guarantee coverage.

Refer to Table 19 RF Attenuation of Common Building Materials for the attenuation characteristics of common building materials.

There are many documents that discuss the RF attenuation characteristics of building materials; one exhaustive study is captured in the National Institute of Standards and Technology (NIST) publication NISTIR 6055 - *Electromagnetic Signal Attenuation in Construction Materials.*

> **Note:** Both the Handset and Headset will emit a repetitive 3-pitch tone when they are out of communication range with the IP phone, the warning tone will cease either after one minute has elapsed or when the user moves back into communication range.

Table 19 RF Attenuation of Common Building Materials

Typical RF signal attenuation of building materials at 1.9 GHz (values are approximate) are listed below:

Inner partition walls	2-5 dB
Wood-/thin material walls	5 dB
Steel shelves/cupboards	15 dB
Various brick types	6-12 dB
Concrete walls	10-20 dB
Concrete ceilings/floors	20 dB
Elevator cars	20-30 dB

DECT Capacity

> **Note:** When planning for DECT capacity, the Administrator should always assume a 100% headset/handset utilization rate.

If average utilization rates are used, the lack of an available channel - which could happen if there are more calls than then the average utilization rate - will result in of loss of communication between a headset/handset and a base, and the IP phone will need to be rebooted to reestablish pairing.

Many factors will affect the channel capacity of the DECT handset/headset solution.

- First is the RF spectrum allocated for the DECT standard, which differs based on the Country or region where the DECT devices will be deployed.

  The Standard DECT variant (European) uses 10 RF carrier frequencies, while the DECT 6.0 variant (North American) has only 5. Each RF carrier is subdivided into 12 full duplex TDM channels.

Therefore:

  - Standard DECT (Europe) has a maximum of 10 x 12 = 120 DECT channels.
  - DECT 6.0 (North America) has a maximum of 5 x 12 = 60 DECT channels.

- Next is the number of DECT channels required by a DECT device.
  - Narrowband audio operation uses one DECT channel for each DECT accessory.
  - Wideband audio operation uses two DECT channels for each DECT accessory.

The following table shows the theoretical maximum number of DECT channels.

Table 20 Theoretical Maximum Number of DECT Channels

DECT Standard	Maximum Number of DECT Channels for Narrowband Audio	Maximum Number of DECT Channels for Wideband Audio
Standard DECT	120	60
DECT 6.0	60	30

To complete the capacity planning, the Administrator also needs to consider for the following factors:

- The number of users that have two DECT devices must be accounted for.
  - A handset is considered a DECT device and a headset is considered a DECT device. If a phone is configured with both a handset and a headset, the Administrator will need to count this as two DECT devices.
  - When a DECT handset or headset is powered on, and on hook (or in its cradle) the DECT device will consume 1/5 of a DECT channel, this partial channel is required by the DECT protocol for pairing and status purposes. This channel will be removed from the pool of available channels and will not be available for another device to use.
  - When a DECT handset or headset goes off hook, the DECT device will consume one DECT channel for Narrowband operation (not 1 1/5 channels), or two channels for Wideband operation (not 2 1/5 channels).

DECT Capacity - Conclusion:

- If a user has only one DECT device, then the Administrator should budget one DECT channel for a Narrowband user and two DECT channels for a Wideband user. However, in the case where a user has both a handset and a headset, the Administrator should budget two DECT channels for a Narrowband user, and three DECT channels for a Wideband user.

  > **Note:** Even though the user will only ever have one DECT device off hook at a time, the second DECT device will consume 1/5 of a DECT channel while it is on hook, and this channel will not be free for use by another DECT device.

- <u>DECT deployment should be based on a 100% headset/handset utilization rate.</u>

RF Site Survey

For installations that call for only a small quantity of DECT accessories, a simple trial and error test with the actual cordless DECT accessories might be sufficient to ensure satisfactory operation.

For installations where a large number of users will be using cordless DECT accessories, using a trial and error approach could be challenging due to physical factors such as building construction and layout, a site survey can help to ensure that optimum performance is obtained from the DECT accessories.

Planning and Process

To ensure a successful DECT deployment it is recommended that the following steps be followed:

- The Administrator needs to obtain a building floor plan or blueprint. The floor plan should show interior construction details such as partition walls, structural walls, telecom and electrical rooms, elevator shafts, washrooms, stairwells, etc. It is important to understand:
    - Where RF attenuation or RF blockages may occur from features such as gypsum walls, masonry walls, structural steel and metallic structures such as ventilation ducting.
    - Where the potential sources of RF interference are located, such as electrical motors, HVAC equipment, power distribution systems, microwave ovens, medical and industrial equipment.
- The Administrator should update the floor plan so that it shows the location of non-construction details, such as desks, bookcases, cubicle walls, white boards, etc. The floor plan should also show the location of WLAN Access Points (Wi-Fi and DECT) and any other sources of RF transmission in the proposed deployment area.
- The Administrator needs to define on the building floor plan where they are proposing to deploy the DECT accessories; a minimum phone to phone (DECT base station to DECT base station) spacing of 2 meters (6.5 feet) should be maintained.
    - While a phone to phone spacing of less than 2 metres is not recommended, there could be some circumstances where the Administrator may decide it is necessary to space phones at less than 2 metres apart. In these situations, it is recommended that the Administrator configure the phones for Low Power RF transmission, for additional details see the section called 69xx Series of IP Phones.

Important: To ensure correct operation, all Mitel DECT devices in the same area must be set to the same RF (Radio Frequency) transmit power level. In situations where both 53xx and 69xx DECT accessories are deployed, the 69xx DECT accessories should be configured for High Power operation, so that they match the 53xx DECT accessory RF power level.

- An RF site survey should be completed in the areas proposed for DECT deployments.

  The RF site survey (and the updated floor plan) should identify any known and/or newly discovered DECT equipment (WLAN Access Points and cordless accessories) that can reach the area proposed for DECT accessory deployment; this includes equipment in use by other tenants on the same floor, on adjacent floors (above and below) and occupants of any nearby buildings.

  It may be necessary to perform this part of the site survey more than once, since other tenants and/or neighbors may not always have their DECT systems operating at full traffic capacity.

Warning: Installing DECT devices on adjacent floors directly above or below the proposed deployment area is not recommended.

Should installation on adjacent floors be desired, an RF site survey needs to be conducted to determine if the RF attenuation factor of the building's floors/ceilings are adequate to isolate DECT devices on adjacent floors from each other.

- The floor plan should indicate if the DECT accessory users are located in one physically contiguous grouping or if the DECT accessory users are located in two or more physically separated groups.

- The DECT Operating Range of the DECT accessories - for the selected RF transmit power setting - needs to be determined by conducting measurements for each group of DECT accessory users, and this information needs to be mapped to the floor plan. This information this will help to determine if the DECT user groups should be considered as belonging to one DECT Coverage Area or multiple DECT Coverage Areas.

Note: The reason for this process is to determine if there are enough DECT channels available in a given DECT Coverage area to support all of the proposed DECT users.

In the following figure, the black dots represent IP phones with a single DECT accessory. There are three groups of DECT users, Group 1, 2, and 3 and they are separated from each other by some amount of distance. The circles around each group of DECT users represent the DECT Operating range for each group of DECT users.

From the following figure it can be seen:

- That Group 3 can be treated as one DECT Coverage Area and will have its own pool of DECT channels.

- That the DECT Coverage Areas for Group 1 and Group 2 overlap. This means that these two DECT user groups will have to be treated as one DECT coverage area, and the two DECT user groups will share the same pool of DECT channels.

- Based on the RF site survey and the information recorded on the floor plan, the Administrator will now need to determine how many DECT channels are available for each DECT Coverage Area and then map this channel availability information to the floor plan.

If there are an adequate number of DECT channels available in each DECT Coverage Area, then the proposed deployment plan will be acceptable.

Should there not be enough DECT channels available in a particular DECT Coverage Area, then changes to the deployment plan will need to be made. The Administrator can consider the following options:

1. Configure all of the DECT devices in the problem Coverage Area to operate at the Low Power transmit setting.

2. In the problem Coverage Area, increase the device to device spacing and area as follows:

   Standard DECT Europe: 5-7 m (16–23 ft) spacing, (25 to 49 sq metres area)

   DECT 6.0 North America: 7 - 10 m (23 - 33 ft) spacing, (49 - 100 sq metres area)

3. Create an RF dead zone to partition the DECT users into two groups, either by physically relocating the overlapping users, or providing users that are overlapping with wired handsets or Bluetooth devices.

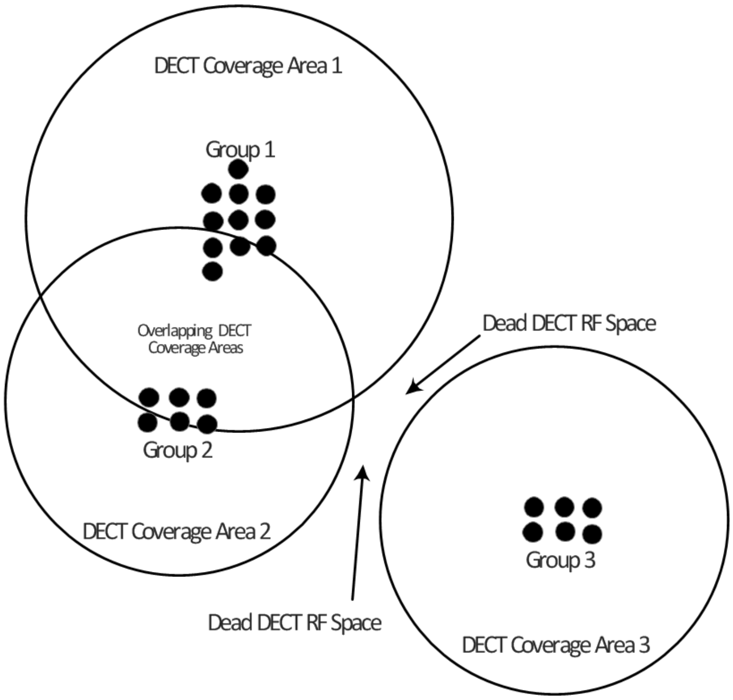

Figure 5 DECT Coverage Areas that Overlap

- At this point the floor plan should show:
    - Where the groups of proposed DECT accessory users are located.
    - The dimensions of the DECT Coverage Area are for each DECT user group.
    - If the DECT user groups should be treated as belonging to one DECT Coverage Area or if the DECT user groups should be treated as belonging to their own DECT Coverage Area.
    - The number of DECT users that are located in each DECT Coverage Area.
    - If there are WLAN DECT Access Points to take into consideration and/or if there are other DECT sources to consider, originating from adjacent floors, the same floor, other tenants or other neighbors.
    - The number of DECT channels that are available for telephony usage in each DECT Coverage Area.

What to Expect from an RF Site Survey

There are many companies that can be contracted to conduct an RF site survey; however, these companies may or may not be familiar with providing surveys and deployment recommendations for a DECT headset/handset telephony solution.

The more commonly found DECT solution (the one that contractors are familiar with) involves the installation of several DECT fixed Access Points throughout the building, and users that have DECT mobile phones. The Operating Range of the DECT Access Points will typically overlap which gives users the ability to roam throughout the building. The DECT Access Points will handle the hand off process and DECT channel management that is required to support enterprise wide roaming.

A site survey for a DECT solution that uses Access Points and DECT mobile phones is designed for a very different set of end goals than a site survey that is using DECT telephone accessories.

When engaging companies to conduct a site survey, the Administrator is advised to make these different requirements very clear to the survey company. The Administrator should consider sharing this document with the survey company prior to signing a contract for work, so that there are no misunderstandings on what the site survey is expected to provide.

The survey should determine the acceptable locations for the IP phones with cordless DECT accessories; the survey will also identify any areas of the building that might present operational problems.

A diagram of the building is essential for noting structural details and marking the locations of the phones with cordless accessories, this diagram forms the basis of the completed site survey.

The site survey should also indicate how far the user can move away from the IP phone and still maintain a connection.

Additional details regarding what the survey needs to determine can be found in the section called DECT Deployment Planning Process.

The Mitel document SIP-DECT Site Survey Kit User Guide covers how to conduct a site survey for a complete SIP-DECT wireless system - a system with Radio Fixed Access Points and mobile DECT users. This document can be found on Mitel's web site. While this document is not intended to cover site surveys for cordless DECT telephone accessories, it does contain information that can be useful for planning a site survey for cordless accessories, or for conducting a preliminary investigation.

RF Site Survey - General Considerations

It is recommended that the installer and/or Administrator review the following recommendations, notes and warnings.

Communication between the IP phone (DECT base station) and the DECT Handset/Headset can be negatively affected by certain types of office equipment and certain building structures, the installer/Administrator should consider the following points when planning a deployment and installation:

- Steel structures such as shelves, metal backed white boards, filing cabinets and dividers will block or impede the transmission of RF signals.
- Some other radio systems may have a negative effect on DECT operation.
- If other DECT systems are in use at the site, there will be a reduction in the number of available DECT channels.
- In general, DECT will not be affected by Wi-Fi or Bluetooth systems.
- Building equipment involving electrical motors (i.e. HVAC systems, elevators, pumps) may have a negative effect on DECT operation.
- Malfunctioning electrical equipment (i.e. defective florescent light ballasts) may have a negative effect on DECT operation.
- Large windows that have a metallic based tint may cause RF energy to be reflected back into the building and have a negative effect on DECT operation.
- Metallic window blinds may cause RF energy to be reflected back into the building and have a negative effect on DECT operation.
- Building materials such as steel doors, steel reinforced concrete, concrete, drywall and wood will either block or attenuate RF transmission to varying amounts.
- Office furnishings (i.e. cubicle walls, chairs, bookcases, etc.) will attenuate radio signals; this has two different effects on DECT deployments:
    - When a site has lots of furnishings and clutter, the user's roaming distance will be reduced - due to radio signal attenuation, but the attenuation introduced by the furnishings will allow for a higher deployment density than an environment that has no furnishings at all.
    - When a site has no furnishings that introduce radio signal attenuation, users will be able to roam to the maximum distances, but deployment density will be reduced due to interference from adjacent channels.
- RF energy may pass through floors and ceilings. This can affect deployment density and performance. When planning an installation interference from adjacent floors must be taken into account.

DECT Security and Safety Considerations

Depending on the particular installation, the following issues may need to be considered:

- The Cordless Handset and Headset use the DECT protocol to support RF transmission and as a result encryption as per the DECT standard is supported. However, transmission of voice over an RF link always presents potential security issues that system Administrators and users should be aware of.
- Electro-Magnetic Interference generated by the Cordless (DECT) Handset and Headset might need to be considered in sensitive environments such as health care facilities, research laboratories and some industrial sites since this interference could affect the operation of critical equipment in the facility.
- Electro-Magnetic Susceptibility needs to be considered since reception on the Cordless (DECT) handset and headset may be affected by other RF devices. A site survey should identify any potential sources of RF interference; however, customer sites are seldom static - new equipment will likely be introduced over time that was not accounted for in the original site survey.

Bluetooth Handsets, Headsets and Devices

Cordless Bluetooth Handsets or Headsets allow the user to move limited distances away from their desk within their office or adjacent offices while holding a telephone conversation. These accessories are targeted at the typical knowledge worker and are not intended to be a solution for mobile workers who may want to roam throughout the enterprise. If support for enterprise roaming is required, then a different Mitel solution should be utilized. Refer to Mitel's Document Centre for information on solutions that are suitable for enterprise roaming.

- There are a number of third-party Bluetooth headsets which can be used with Mitel IP phones. For details refer to the appropriate IP Phone User Guide, which can be found on Mitel's Document Centre.

- The 5330, 5340 and 5360 IP Phones support an optional Mitel Bluetooth Handset; the Mitel Bluetooth Module must be installed in the phone. For details refer to the appropriate IP Phone Installation Guide.

- The 69xx series of IP phones offer users Bluetooth headsets, handsets, and the MiVoice S720 Bluetooth Speakerphone.

- The 6970 IP Conference Phone and other IP phones allow the user to pair the Mitel phone with another device via a Bluetooth connection.

- The 6930 and 6940 IP phones have a feature called PCLink that enables the phones to be used as the audio device for PC and MAC video conferencing applications.

  The Administrator should follow the Bluetooth deployment recommendations in the following sections of this document since they are applicable to 6930 and 6940 phones when they are used with PCLink to act as audio devices for video conferencing applications.

  For additional information about PCLink and supported video conferencing applications, refer to the Mitel 6930 and 6940 IP Phone User Guides.

For configuration and usage information, refer to the appropriate IP phone documentation and accessory documentation on Mitel's Document Centre.

Bluetooth Accessory Deployment - Recommendations

To ensure a successful Bluetooth installation requires careful planning. It is recommended that the installer and/or Administrator review the recommendations in the following sections.

The key considerations for Bluetooth telephone accessory functionality are user range and user density, where range refers to how far away from their desk a user can roam while maintaining a connection with the IP phone and density refers to how may simultaneous users can be supported in a given area.

Evaluating the Site for RF Blockages and Interference

Performing an RF (Radio Frequency) site survey prior to deploying the Bluetooth devices may be beneficial, allowing the Administrator to understand where there are building structures and office furniture that may attenuate or completely block Bluetooth signals. For a further discussion regarding RF site surveys, see the subsection called RF Site Surveys which is contained in the previous section on DECT Handsets and Headsets.

While not all Bluetooth deployments require an RF site survey, the Administrator does need to assess the site's RF obstructions and identify all sources of RF interference. See the section called Bluetooth and RF Interference from 2.4 GHz Sources, for a partial list of sources of potential interference. A site assessment will go a long way towards ensuring a successful deployment.

Bluetooth Operating Range

Mitel's Bluetooth devices are designated as Class 2 Devices have a typical operating range of up to 10 metres.

In environments where there are no RF blockages or RF interference, the operating range may be in excess of 10 metres, but to determine just how far the user may successfully roam would have to be determined on a case by case basis.

There may be cases where the Bluetooth operating range is hampered, and the operating range is less than 10 metres.

In situations such as this where the range appears to be less than 10 metres, the user or the Administrator should look for obvious (or not so obvious) RF blockages. Possibly a steel filing cabinet or, a steel backed white board is blocking the RF connection between the Bluetooth device and the IP phone. Other RF impediments to consider are large HDMI displays, desk top computer enclosures and steel shelving units.

Number of Bluetooth Users

Bluetooth will work well for installations that have less than 200 users, providing the recommendations and guidelines are followed.

If a particular installation requires more than 200 Bluetooth devices, the Administrator should contact Mitel Professional Services.

Bluetooth Density Guidelines

Once the Administrator has evaluated the area where the Bluetooth accessories are to be deployed for RF blockages and all of the Wi-Fi Access Points and other sources of RF interference have been identified, then density planning may proceed.

Adhering to the Bluetooth device density guidelines is important, in cases where an installation does not follow the guidelines; the users will likely experience poor audio quality, in cases where the guidelines are completely ignored, users may not be able to place calls.

The Administrator needs to know in advance if the proposed deployment area will support the number of users and provide optimum audio quality.

Call Traffic

The following density guidelines are based on 100% of the users being off hook (in a call state) simultaneously. Higher densities will be achievable when the number of simultaneous users is less than 100%. However, to avoid a situation where call traffic bursts might introduce voice quality issues to some users, it is recommended to plan for 100% utilization.

If the Administrator knows that only 50% of the users will be off hook simultaneously, twice the number of Bluetooth devices may be successfully deployed in the same area that would be required to support users who are off hook simultaneously 100% of the time.

Device to Device Spacing

This section provides phone-to-phone minimum spacing guidelines. *The Administrator should comply with these minimum spacing guidelines on all 3 axes.*

If the total number of Bluetooth accessories to be deployed in a given area is less than 25 there should be no deployment issues, but the Administrator should ensure that phone to phone spacing is 1 to 1.5 metres (3.3' to 4.9').

To give an idea of how much area is required to support 25 users - If 25 phones are distributed on a grid with a phone to phone spacing of 1 metre (3.3'), the area required for this deployment will be 25 sq. metres (268 sq. ft).

If there are 25 or more Bluetooth devices, the required phone to phone spacing and the area required for each phone will increase proportionality.

In addition to the above spacing requirements, Bluetooth device to device spacing requirements will increase when there are one or two Wi-Fi Access Points within operating range.

Warning: If there are three Wi-Fi Access Points within operating range, a successful Bluetooth deployment will likely not be possible - contact Mitel Professional Services.

The following tables offer device to device spacing requirements and the area required for each Bluetooth device, based on the number of users and if there are Wi-Fi Access Points (AP) present.

Table 21 Device Minimum Spacing - No Wi-Fi APs Present

Number of Devices	**Device to Device Spacing**	**Area Required per User**
0 to 50	1.5 m (4.9')	2.25 sq metres (24 sq ft)
50 to100	1.5 to 2 m (4.9' to 6.5')	2.25 to 4 sq metres (24 to 42 sq ft)
100 to 200	2 to 3 m (6.5' to 9.8')	4 to 9 sq metres (24 to 96 sq ft)

Table 22 Device Minimum Spacing - One Wi-Fi AP Present

Number of Devices	Device to Device Spacing	Area Required per User
0 to 50	3.73 m (12.2')	13.9 sq metres (148 sq ft)
50 to100	4.23 m (13.8')	17.8 sq metres (190 sq ft)
100 to 200	5.23 m (17')	27.3 sq metres (289 sq ft)

Table 23 Device Minimum Spacing - Two Wi-Fi APs Present

Number of Devices	Device to Device Spacing	Area Required per User
0 to 50	6.1 m (20')	37.2 sq. metres (400 sq. ft)
50 to100	7.2 m (23.6')	51.8 sq. metres (557 sq. ft)
100 to 200	8.5 m (27.8')	72.3 sq. metres (773 sq. ft)

Bluetooth Channel Availability

For installations that will have less than 200 Bluetooth devices the technology does not present any issues related to channel availability.

Note: If the installation requires more than 200 Bluetooth devices, the Administrator should contact Mitel Professional Services.

Bluetooth frequencies are all located within the 2.4 GHz Industrial, Scientific, and Medical radio band (ISM). The ISM band typically extends from 2.4000 to 2.4835 GHz. The Bluetooth channels are spaced 1 MHz apart. Starting at 2.402 GHz and finishing at 2.480 GHz. This can be calculated as 2401 + n, where n varies from 1 to 79.

This arrangement of Bluetooth channels gives a guard band of 2 MHz at the bottom end of the band and 3.5 MHz at the top, and up to 79 channels.

A Bluetooth transmission only occurs on a given frequency for a short time, and if any interference is present the data will be re-sent later when the signal has changed to a different channel which is likely to be clear of other interfering signals. The Bluetooth standard uses a hopping rate of 1600 hops per second, and the system hops over all the available frequencies using a pre-determined pseudo-random hop sequence based upon the Bluetooth address of the master node in the network.

In order to enable effective communications to take place in an environment where a number of devices may receive the signal, each device has its own identifier. This is provided by having a 48-bit hard wired address identity giving a total of 2.815 x 10^14 unique identifiers.

Bluetooth Wideband Audio

The 69xx Bluetooth accessories support Wideband audio operation; the Bluetooth devices require only one Bluetooth channel, for both Narrowband and Wideband operation. For more information on Bluetooth Wideband usage, see the 69xx documentation.

The 6930 and the 6940 IP phones support Wideband audio operation when paired when paired with a PC or MAC via PCLink. The phone to PC/MAC audio path requires one Bluetooth channel.

Bluetooth and Wi-Fi Coexistence

Bluetooth solutions must be used with care if Wi-Fi networks are being used in the same area.

A number of the Wi-Fi standards operate in the 2.4 GHz RF band, this is the same RF band used by Bluetooth. The transmissions from Wi-Fi Access Points will reduce the number of available Bluetooth channels when these systems are co-located.

The Wi-Fi IEE 802.11a standard operates in the 5.8 GHz RF band. The Administrator may choose to configure their Wi-Fi Access Points for 802.11a operation to eliminate interference. However, Wi-Fi systems operating at 5.8 GHz will have a shorter operating range than Wi-Fi systems operating at 2.4 GHz so for some Administrators this may not be a feasible option.

Mitel's Bluetooth solutions use Adaptive Frequency Hopping (AFH). This allows the Bluetooth devices to avoid using channels within the 2.4GHz band that are in active use by Wi-Fi Access Points. Wi-Fi Access Points generally operate within only one third of the 2.4G Hz band, and adjacent Access Points use different thirds*. As a result, a Bluetooth device can usually find at least a third of the RF band to use, providing there are only one or two Wi-Fi Access Points in the operating area.*

However, as the presence of Wi-Fi transmissions increase in an area, AFH will have fewer Bluetooth channels to hop between, and Bluetooth density will be reduced.

Channel availability will be severely impacted when Bluetooth devices are within Operating Range of three Wi-Fi access points, or when several Bluetooth accessories are deployed in the Operating Range of a Wi-Fi Access Point. When this happens, it is usually Bluetooth voice traffic, rather than Wi-Fi traffic, which suffers. Each Bluetooth packet carries a tiny 1/1600-second sample of real time voice traffic. Wi-Fi interference will cause Bluetooth packet loss. Each lost packet is heard by the user as a small click, while the occasional click may not be problematic to the user, if there are too many clicks, the user will find the audio quality unacceptable.

Bluetooth and RF Interference from 2.4 GHz Sources

The 2.4 GHz RF spectrum used by Bluetooth is also shared by many other non-Bluetooth devices. Even though these other devices are not Bluetooth devices, their RF transmissions can have a negative impact on Bluetooth channel availability. For example, the lack of available Bluetooth channels in a particular area may cause excessive clicking in the audio path, or the users may experience dropped calls, or users may be unable to initiate a call. In some cases, the user may be able to successfully place phone calls, but the audio quality is reduced, while on a call the user may hear crackles, pops, and whistles.

The following is a list (which is not exhaustive) of common devices that use the 2.4 GHz spectrum and could be sources of Bluetooth interference.

- 2.4 GHz cordless phones
- ZigBee networks
- Wireless USB
- Wi-Fi
- Microwave ovens
- Car alarms
- Nursery monitors
- Plastic welding equipment
- Alarm systems
- Wireless microphones
- Video senders
- Amateur radio - voice and video
- Wireless speakers
- Wireless cameras
- Some LCD displays
- DSS Direct Satellite Services - leaky cables and connectors
- Medical equipment

Bluetooth Deployment Considerations

Communication between the IP phone (base station) and the Bluetooth handset/headset can be negatively affected by several types of equipment and building structures, the installer should consider the following when planning a Bluetooth deployment:

- Steel structures such as shelves, metal backed white boards, filing cabinets and dividers will block or impede the transmission of RF signals.
- RF energy emitted by equipment such as photocopiers, printers and microwave ovens can have a negative effect on Bluetooth operation.
- Other radio systems such as Wi-Fi, ZigBee and some proprietary systems may have a negative effect on Bluetooth operation.
    - If Bluetooth devices are to be deployed in the same area where a Wi-Fi network is operating, it is recommended that the Wi-Fi network should be an IEEE 802.11a network, which operates at 5.8 GHz.
- Direct satellite Services, faulty coax cabling and/or connectors may allow RF energy to leak into the environment and effect Bluetooth operation.
- Mains power sources, avoid locating Bluetooth accessories near circuit breaker panels, power lines, or any source of electrical arcing, i.e. electric motors, street cars or industrial equipment.
- Cordless phones operating at 2.4 GHz may cause interference.
- Some flat panel LCD displays may emit RF around 2.4 GHz, be aware of poorly shielded cabling connecting laptops to larger displays.
- Some wireless speakers that operate in the 2.4 GHz spectrum may cause interference.
- Wireless microphones often operate in the 2.4 GHz spectrum.

- USB 3.0 interfaces have been identified as a source EMI that can interfere with Bluetooth operation.
- Wireless video senders and wireless HDMI senders operate in the 2.4 GHz spectrum.
- Building equipment involving electrical motors (i.e. HVAC systems, elevators, pumps) may have a negative effect on Bluetooth operation.
- Malfunctioning electrical equipment (i.e. defective florescent light ballasts) may have a negative effect on Bluetooth operation.
- Large windows that have a metallic based tint may cause RF energy to be reflected back into the building and have a negative effect on Bluetooth operation.
- Metallic window blinds may cause RF energy to be reflected back into the building and have a negative effect on Bluetooth operation.
- Building materials such as steel doors, steel reinforced concrete, concrete, drywall, and wood will block or attenuate RF transmission to varying amounts.
- Office furnishings (i.e. cubicle walls, chairs, bookcases, etc.) will attenuate radio signals; this has two different effects on Bluetooth installations:
- When a site has lots of furnishings and clutter, the user's roaming distance will be reduced - due to radio signal attenuation, but the attenuation introduced by the furnishings will allow for higher density than an environment that has no furnishings.
- When a site has no furnishings that introduce radio signal attenuation, users will be able to roam to the maximum distances, but deployment density will be reduced due to interference from adjacent channels.
- RF energy will pass through floors and ceilings. This can affect deployment density and performance. When planning an installation across multiple floors, interference from adjacent floors must be considered.
- The Administrator and/or installer may want to consider if a RF site survey should be conducted prior to purchasing Bluetooth accessories.
- If a large number of Bluetooth accessories are to be deployed, a site survey may be warranted.
- If a relatively small number of Bluetooth accessories are to be deployed, trialing a few devices prior to completing the sale may be sufficient.

Bluetooth Security and Safety Considerations

Depending on the particular installation, the following issues may need to be considered:

- The Cordless handset and headset use the Bluetooth protocol to support RF transmission and as a result encryption as per the Bluetooth standard is supported. However, transmission of voice over an RF link always presents potential security issues that system Administrators and users should be aware of.
- Electro-Magnetic Interference generated by the Cordless (Bluetooth) handset and headset might need to be considered in sensitive environments such as health care facilities, research laboratories and some industrial sites since this interference could affect the operation of critical equipment in the facility.
- Electro-Magnetic Susceptibility needs to be considered since reception on the Cordless (Bluetooth) handset and headset may be affected by other RF devices. A site survey should identify any potential sources of RF interference; however, installation sites are seldom static - new equipment will likely be introduced over time that was not accounted for in the original site survey.

Disabling the Bluetooth Interface

If required, for security reasons the Bluetooth interface on the 6930, 6940 and 6970 IP sets can be disabled. MiVoice Business supports a Class of Service (CoS) option that the Administrator can use to disable the Bluetooth interface on the 6930, 6940 and 6970 IP sets on a per DN basis. When the Bluetooth interface is disabled, it is not possible for the user to reenable the interface from the phone.

For further information see the MiVoice Business *Class of Service Options Form* and the *Blue Tooth Control Form.*

Bluetooth Accessory - Poor Performance

Should poor audio performance or telephone operation be encountered by Bluetooth accessory users, the Administrator should review the recommendations and deployment considerations discussed in this document. The following information may help with troubleshooting.

When Bluetooth Performance Suddenly Changes

If all of the recommendations and deployment considerations have been followed and Bluetooth accessory performance was originally satisfactory. The Administrator should review the following questions and determine if these changes may have impacted Bluetooth operation:

- Have any new Bluetooth telephone accessories have been introduced into the environment.
- Have any other Bluetooth based devices been introduced into the environment such as wireless speakers, keyboards or mice.
- Has any RF based equipment using 2.4 GHz frequencies been introduced into the environment such as wireless microphones, alarms systems, smart building controls, etc.

Bluetooth Performance Issues

The following section provides some suggestions that may alleviate certain performance issues:

- **Poor Operating Range:** The user should be able to roam 10 metres from their phone's location, if this is not possible the Administrator should look for any possible RF blockages in the immediate area.
- **Dropped Calls:** Dropped calls or calls that cannot be initiated may be an indication that free channel availability in the user's area is inadequate. This could be the result of poor deployment planning, higher than usual call rates or RF interference from Wi-Fi Access Points, other Bluetooth devices or other RF equipment that uses the 2.4 GHz RF spectrum.
- **Clicking Sound:** When a user hears a clicking sound in their headset or handset, it is an indication that there has been packet loss. Packet loss could be due to RF blockages or RF reflections.

If the problem occurs consistently while the user is stationary, look for RF blockages and/or reflections in their immediate office area.

If this problem occurs when the user roams away from their desk, look for RF blockages or reflections that the user encounters as they roam.

Clicking sounds may also be an indication of interference from other RF sources that use the 2.4 GHz spectrum, or from competition with Wi-Fi Access Points.

Should a user experience choppy audio (packet loss) and/or dropped calls and the source of interference cannot be determined or remedied - it is recommended that a corded handset be used. In an office installation with a high density of users and the users are located in close proximity to each other, it may be necessary for every second phone to use a corded (non-Bluetooth) handset.

Emergency Calls, 911 & 999

When planning an IP phone installation, the Administrator may need to ensure that emergency services are supported. To support emergency call services, the IP Phones report L2 switch network connectivity information. This information can be used to provide location information to the emergency Services database.

IP phone move detection is accomplished by analyzing data reported from the Spanning Tree Protocol/Rapid Spanning Tree Protocol or the Cisco Discovery Protocol. When an IP phone is moved to a new physical location, the phone reports the new location information to the call control server and the CESID directory is automatically updated.

The Administrator may require that specific IP phones remain operational for emergency calls even during a mains power outage. To keep IP phones operational during a power outage, the Administer will need to ensure that the IP phone and the associated networking switches, routers and gateways remain powered for the required time period by a backup power system.

More information on this topic can be found in the MiVoice Business Engineering Guidelines and the Technical Paper, Networking for IP Telephony - under VMPS, CDP, and Location Change Indication (E911).

In some cases, the Administrator may choose to use a Line Interface Module (LIM) to provide an IP phone with PSTN connectivity in the event of a mains power outage.

The Line Interface Module allows the connection of an analog line to an IP Phone. The LIM enables access to a local PSTN line for emergency calls or failover capability for IP phones. It is ideal for remote Teleworkers or users requiring phone access in the event of LAN failures.

For more information on the LIM, refer to the product documentation.

Teleworker Phones - Support for Ray Baum Legislation

Teleworker phones (those deployed behind a MiVoice Border Gateway) now have the ability to detect a change in the gateway MAC address and can now report the change of location to the user via a pop up message and also report the change of location to the MiVoice Business. When the MiVoice Business receives a change of location report, the CESID directory is automatically updated.

The phones that support the ability to detect a change in the gateway MAC address while in Teleworker mode are:

- 6900 series IP phones
- 5304, 5312, 5320, 5320e, 5330e, 5340e, 5540 and 5360

For additional information pertaining to Ray Baum support, refer to the MiVoice Business Engineering Guidelines.

Security

Most Mitel IP phones support voice media and signaling encryption; however, whether or not encryption will be enabled is dependent on the phone and the call control server that the phone is registered with. Information related to call control server encryption can be found in the call control server documentation.

For phones associated with a MiVB, refer to the MiVoice Business Engineering Guidelines, under the heading Security Support with Mitel VoIP.

Table 24 Security Support by Device, below lists the IP phones and which encryption measures are supported on each phone.

> **Note:** For security reasons an IP phone or an IP conference phone should never be connected directly to the internet. The IP phone or IP conference should always reside behind an appropriate firewall so that firewall rules can be used to protect the phone from malicious attacks.

Voice Encryption

To encrypt the voice media, Mitel IP phones may use Mitel SRTP or SRTP. SRTP allows voice encryption between Mitel IP phones and supported third party devices. SRTP requires more call server computing resources than Mitel SRTP and therefore is only supported on certain call control platforms. For further information, refer to the call control platform documentation.

Signaling Encryption

There are two main methods used to secure a signaling channel:

- SSL (Secure Socket Layer) or TLS (Transport Layer Security), both are open standards however SSL is only used with the older families of IP sets.
- Secure MiNET (a Mitel proprietary standard) is used for the proprietary MiNET IP phones.

Mitel's secure MiNET protocol uses the Advanced Encryption Standard (AES) to encrypt call control packets. Using secure MiNET ensures that call control signaling packets between the IP phones and the call control server are protected from eavesdropping.

SSL and TLS Certificates for call signaling security are managed from the call server, in the case of MiVB refer to the MiVB System Administration Tool On-line Help files.

Table 24 Security Support by Device

Device	Signaling Security	Voice (Media) Security
5001	Secure MiNET	Mitel SRTP
5005	Secure MiNET	Mitel SRTP
5010	Secure MiNET	Mitel SRTP
5020	Secure MiNET	Mitel SRTP
5201	Secure MiNET	Mitel SRTP
5205	Secure MiNET	Mitel SRTP
5207	Secure MiNET	Mitel SRTP
5212	Secure MiNET and SSL	Mitel SRTP
5215	Secure MiNET	Mitel SRTP
5215 (Dual Mode)	Secure MiNET and SSL	Mitel SRTP
5220	Secure MiNET	Mitel SRTP
5220 (Dual Mode)	Secure MiNET and SSL	Mitel SRTP
5224	Secure MiNET and SSL	Mitel SRTP
5230	Secure MiNET	Mitel SRTP
5235 (Dual Mode)	Secure MiNET and SSL	Mitel SRTP
5140	Secure MiNET	Mitel SRTP
5240	Secure MiNET	Mitel SRTP
5302 (SIP Device)	No	No
5304	Secure MiNET and TLS 1.2	Mitel SRTP and SRTP
5312	Secure MiNET and TLS 1.2	Mitel SRTP and SRTP
5320	Secure MiNET and TLS 1.2	Mitel SRTP and SRTP

Device	Signaling Security	Voice (Media) Security
5320e	Secure MiNET and TLS 1.2	Mitel SRTP and SRTP
5324	Secure MiNET and TLS 1.2	Mitel SRTP and SRTP
5330	Secure MiNET	Mitel SRTP and SRTP
5330e	Secure MiNET and TLS 1.2	Mitel SRTP and SRTP
5340	Secure MiNET	Mitel SRTP and SRTP
5340e	Secure MiNET and TLS 1.2	Mitel SRTP and SRTP
5360	Secure MiNET and TLS 1.2	Mitel SRTP and SRTP
5485 IP Pager	Secure MiNET	Mitel SRTP
5540	Secure MiNET and TLS 1.2	Mitel SRTP and SRTP
5505 (SIP Device)	No	No
5550 IP Console	Secure MiNET	No
5550-TKB	Secure MiNET	Mitel SRTP
5560 IPT	Secure MiNET	Mitel SRTP
MiVoice Video/Conference	TLS 1.2	SRTP
MiVoice Business Console	Secure MiNET	Mitel SRTP and SRTP
6905	TLS 1.2	SRTP
6910	TLS 1.2	SRTP
6920	TLS 1.2	SRTP
6930	TLS 1.2	SRTP
6940	TLS 1.2	SRTP
6970	TLS 1.2 and Secure MiNET	SRTP

Ciphers and Cipher Suites

Ciphers and Cipher Suites supported by the 68xx and 69xx series of phones are listed below.

Table 25 68xx/69xx SIP Mode - Ciphers and Cipher Suites

The following table shows the cipher suite and ciphers used by the 68xx and 68xx sets when in SIP mode.

Signaling	Media
TLS_RSA_WITH_AES_256_GCM_SHA384	AES_CM_128
TLS_RSA_WITH_AES_256_CBC_SHA256	AES_CM_128_HMAC_SHA1_80
TLS_RSA_WITH_AES_256_CBC_SHA	AES_CM_128_HMAC_SHA1_32
TLS_RSA_WITH_AES_128_CBC_SHA	
TLS_RSA_WITH_RC4_128_SHA	

Table 26 53xx/69xx MiNET Mode - Ciphers and Cipher Suites

The following table shows the cipher suite and ciphers used by the 53xx and 69xx sets when in MiNET mode.

Signaling (MiNET)	Media
TLS_RSA_WITH_AES_128_GCM_SHA256	AES_CM_128_HMAC_SHA1_80
TLS_RSA_WITH_AES_128_CBC_SHA256	AES_CM_256_HMAC_SHA1_80
TLS_RSA_WITH_AES_128_CBC_SHA	
TLS_RSA_WITH_3DES_EDE_CBC_SHA	
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	

IP Phone - Integral Micro Firewall

Several Mitel IP Phones support an integral Micro Firewall; the following IP phones support the Micro Firewall:

Table 27 Sets with Integral Micro Firewall

5212	5304	5324	5340e	MiVoice Video/Conference
5215 Dual Mode	5312	5330	5360	
5220 Dual Mode	5320	5330e	5505	
5224	5320e	5340	5540	

The Micro Firewall blocks all undesirable packets (e.g. ARP packet not for the phone).

Table 28 Micro Firewall - Packet Rates

Packet Type	Rate (Packet/Second)	Burst Handling (Packets)
CDP, STP, LLDP	5	25
DNS	30	20
ARP, ICMP	5	50
RTP (per stream)	110	0

The Micro Firewall will filter the packets and allow bursts up to the "credit" limit shown above. After a protocol type has exhausted its credits with a burst that reached the prescribed limit, the credits are added back at prescribed rates. For instance, the Micro Firewall may allow up to 50 ICMP packets in a burst, and then discard any additional ones that arrive before the Micro Firewall will begin adding credits at the rate of 5 a second.

All packets blocked by the Micro Firewall will be discarded transparently at the Ethernet layer without the phone's upper layers being affected in any way.

Authentication Protocol Support

Several L2 switches support a level of access restriction to the network ports. A device that connects to one of these ports needs to be authenticated as valid before connections can be established. The following protocols that can do this:

- Cisco VMPS
- 802.1X

VMPS

Cisco VLAN Management Policy Server (VMPS) is a Cisco proprietary authentication protocol and has been deprecated by the IEEE 802.1X authentication protocol. Cisco VMPS is described in Network Engineering for IP Telephony.

IEEE 802.1X

The IEEE 802.1X standard is similar in operation to VMPS but uses a RADIUS Server for authentication. Devices that authenticate through 802.1X require an identification name and password before being allowed access.

Current models of Mitel IP phones support the IEEE 802.1X authentication protocol. Most phones support EAP-MD5, EAP-PEAP, and proxy logoff. Users authenticate through the phone interface by entering a username and password. The 6905, 6910, 6920, 6930 and 6940 also support EAP-TLS, for additional information, refer to the 69xx IP Sets product documentation.

For a list of the phones that support the IEEE 802.1X authentication protocol, refer to Table 27.

IEEE 802.1X Operation

If the administrator configures the L2 Switch for port access control, the connected IP Phone will prompt the user for an account name and password if one has not already been entered or if the information saved in the phone is invalid. Based on the response,

- the port may be opened for access
- the VLAN settings may change
- the port could be opened to a guest VLAN
- the port could be shut down.

When a PC is connected to a port, it will be interrogated in the same manner as an IP phone, and user input will be required.

Typically, 802.1X will only allow a single device to be authenticated and connected to a port. This restricts how devices can be connected into the network infrastructure. Where a network port only supports a single connected device, then, for full authentication, only a phone or a PC should be connected to this port. If it is required that both a phone and a PC must be connected to the same L2 switch port, then only the phone should provide authentication. If authentication is provided only by the PC and the PC is not present, the phone may not work.

Not all network access devices place single device restrictions on connected devices. HP switches allow multiple devices to be connected and authenticated on a single port. With Cisco switches, where the IP Phone uses the Auxiliary VLAN setting, both an IP Phone and a connected PC can operate on the same port.

A PC connected behind a phone may need to authenticate access. Failure to do this correctly may result in the network port being shut down. This may result in the IP Phone also being disconnected. Ideally, the PC should be programmed with the necessary information for 802.1X authentication through the “PC Network Properties.” If not, then it is possible that the PC could fail the authentication time-out at the port or at subsequent authorization requests. It may also be necessary to connect the PC to the phone after the phone has authenticated the connection.

An 802.1X port may be configured to request authentication only at startup of the network port and this may include regular authentication retries.

Because authentication is based on a network port becoming active, it is possible, with some network switches, that an unauthorized device could be connected behind an IP Phone once the IP Phone has itself gained access to the port. Therefore, it is recommended that you enable the re-authentication response to regularly check access to the port and identify such connections. The default time is often of the order of 3600 seconds.

IEEE 802.1X Proxy Logoff - 53xx and 69xx Sets

The 5.2.2.x Release of phone set firmware introduced support for 802.1X proxy logoff to the 53xx and 69xx series of phones.

This logoff feature will become enabled when 802.1X is enabled on the phone. With proxy logoff, when a PC is physically disconnected from the phone's PC Ethernet port, the phone's PC Ethernet port will be reset. Once the PC Ethernet port has been reset, if a PC is reconnected to the phone's PC port, the PC will have to re-authenticate before being allowed access to the network.

A phone that supports 802.1X will indicate, during power up, that it is attempting 802.1X authentication. It is possible to disable 802.1X via a CONFIG application menu under Tools and Features. This menu also allows you to delete any stored usernames and passwords.

For details on 802.1X, refer to the “802.1X EAP - MD5 Authentication Protocol Support” Knowledge Base article on Mitel’s Document Centre.

> **Note:**
>
> 1. Some vendors, Hewlett Packard, for example, manufacture switches that support multiple instances of 802.1X for devices that are connected to the same port. In this case, you can enable support on both devices without risking access conflicts.
> 2. In some cases, network administrators may be running 802.1X to prevent unauthorized users from accessing the network. As an example, Ethernet drops in semi-public spaces such as reception areas would likely be protected with 802.1X.
>
>   Use caution if deploying phones that do not support 802.1X in these situations, because the network administrator will not be able to enable 802.1X on this network port. If the phone provides a secondary ethernet port, this port will also be unable to provide authentication support.

6800 and 6900 SIP Sets – 802.1X Support

From SIP Release 5.1 the following versions of IEEE 802.1X are supported.

- IEEE 802.1X-2001
- IEEE 802.1X-2004
- IEEE 802.1X-2010

6900 IEEE 802.1X EAP TLS-Certificates

The process for configuring and downloading IEEE 802.1X EAP-TLS certificates, and staging of the phones is discussed in detail in the 6900 Series IP Phone Administrator Guide.

Simple Certificate Enrollment Protocol

With Release 1.5.1, support is provided in the 69xx MiNet phones for the Simple Certificate Enrollment Protocol (SCEP), which is a protocol used for enrollment and other Public Key Infrastructure (PKI) operations.

The 69xx SCEP client is capable of the following operations:

- CA Authentication
- Client Enrollment
- Client Re-enrollment using Renewal

Please refer to https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/116167-technote-scep-00.html for more details regarding these operations.

The 69xx SCEP client does not support Rollover which is a special case while renewing the certificate and is only applicable if the CA certificate expires.

For information on how to configure SCEP in the 69xx phones, refer to the Mitel MiVoice 6900 Series IP Phones Administrator Guide.

MiNET DEVICES THAT SUPPORT IEEE 802.1X

Table 29, lists the IP MiNet Phones that support IEEE 802.1X.

Table 29 Devices That Support IEEE 802.1X

Device	802.1X Support
5001	No
5005	No
5010	No
5020	No
5140	No
5201	No
5205	No
5207	No
5212	Yes
5215	No
5220	No
5224	Yes
5230	No
5240	No
5302	No
5304	Yes - EAP PEAP
5312	Yes - EAP PEAP
5320	Yes - EAP PEAP
5324	Yes - EAP PEAP
5330	Yes - EAP PEAP
5340	Yes - EAP PEAP
5360	Yes - EAP PEAP
5505	Yes - EAP MD5

Device	802.1X Support
5540	Yes - EAP MD5
5215 (Dual Mode)	Yes - EAP MD5
5220 (Dual Mode)	Yes - EAP MD5
5235 (Dual Mode)	Yes - EAP MD5
5320e	Yes - EAP PEAP
5330e	Yes - EAP PEAP
5340e	Yes - EAP PEAP
5485 IP Pager	No
5550 TKB	No
5560 IPT	Yes
DECT wireless	No
Navigator	Yes - EAP MD5
MiVoice Video/Conference	Yes - EAP MD5
6905	Yes - EAP PEAP
6910	Yes - EAP PEAP
6920	Yes - EAP PEAP
6930	Yes - EAP PEAP
6940	Yes - EAP PEAP
6970	Yes - EAP PEAP

Appendix A - Set Status at MiVB Release 9.0

Note: 5200 series IP Sets support level at MiVB Release 9.0

While Mitel expects the 5200 series of phones will operate as normal, the 5200 sets will not have the normal support level. Specifically, this means that, should issues arise after the upgrade to release 9.0, Mitel reserves the right to **not** fix specific issues isolated to the 5200 series sets operation.

For more information, refer to Product Bulletin – PB20170185.

The following table lists:

- The devices that available for purchase as of February 2018.
- The sets that are blocked from connecting to MiVB at Release 9.0.
- Set firmware status at MiVB Release 9.0.
- Sets that have reached end of life as of September 2020.

Legend

- “Firmware Included” means the set firmware is included in the MiVB Release 9.0 software, and the set will connect to the MiVB.
- "Firmware Not Included" means the set firmware is not included in the MiVB Release 9.0 software. In this case the set will connect to the MiVB only if the set already has its firmware or if the set can obtain the set firmware from a server.
- “Blocked” means the set will be intentionally blocked during a database migration from an earlier MiVB Release to MiVB Release 9.0. In other words, a "Blocked" set will no longer be programmable in ESM and will not connect to the MiVB.
- "Set uses alternate source" means that the set gets its firmware from an alternate source rather than from the MiVB. This is pre-existing behaviour and is unrelated to MiVB Release 9.0.

Table 30 Set Status at MiVB release 9.0

Set Model	Set Status at MiVB Release 9.0	Set is available for purchase as of February 2018	Notes
5001 IP	Firmware Not Included	No	
5005 IP	Firmware Not Included	No	
5010 IP	Firmware Included	No	
5020 IP	Firmware Included	No	
5055 (SIP)	Set Uses Alternate Source	No	
5140 IP	Firmware Not Included	No	
5201 IP	Firmware Not Included	No	
5205 IP	Firmware Not Included	No	

Set Model	Set Status at MiVB Release 9.0	Set is available for purchase as of February 2018	Notes
5207 IP	Firmware Not Included	No	
5212 IP	Firmware Included	No	
5215 IP	Firmware Included	No	
5215 IP DM	Firmware Included	No	
5220 IP	Firmware Included	No	
5220 IP DM	Firmware Included	No	
5224 IP	Firmware Included	No	
5230 IP	Firmware Not Included	No	
5235 IP	Firmware Included	No	At MiVB Release 9.0, will only operate as a single line IP set, no special features are supported. SAC support was removed in MiVB 8.0
5240 IP	Firmware Not Included	No	
5302 IP	Firmware Not Included	No	
5304 IP	Firmware Included	Yes	
5312 IP	Firmware Included	Yes	
5320 IP	Firmware Included	Yes	
5320e IP	Firmware Included	Yes	
5324 IP	Firmware Included	No	Product status is end of life in May 2021
5330 IP	Firmware Included	No	
5330e IP	Firmware Included	Yes	
5340 IP	Firmware Included	No	
5340e IP	Firmware Included	Yes	
5360 IP	Firmware Included	No	Product status is end of life in May 2021
5401 IP	Blocked	No	
5485 IP pager	Firmware Included	Yes	Registers as a 5010
5505 SIP	Firmware Included	Yes	
5540 IP Console	Firmware Included	Yes	

Set Model	Set Status at MiVB Release 9.0	Set is available for purchase as of February 2018	Notes
MiVoice Business Console	Set Uses Alternate Source	Yes	
5550-TKB (5550 IP Console)	Blocked	No	Not supported since MiVB 7.0 SP2
5560 IPT	Firmware Included	No	
5603 SIP	Set Uses Alternate Source	No	
5604 SIP	Set Uses Alternate Source	No	
5607 SIP	Set Uses Alternate Source	No	
5610 SIP	Set Uses Alternate Source	No	
5624 Wi-Fi Phone	Set Uses Alternate Source	No	Product status is end of life in May 2020
612 SIP-DECT	Set Uses Alternate Source	No	
622 SIP-DECT	Set Uses Alternate Source	No	
632 SIP-DECT	Set Uses Alternate Source	No	
650 SIP-DECT	Set Uses Alternate Source	No	
6600 YA Pro	Blocked	No	Relies on legacy MiTAI interface that was removed in MiVB 8.0
6731i	Set Uses Alternate Source	No	
6735i	Set Uses Alternate Source	No	
6737i	Set Uses Alternate Source	No	
6739i	Set Uses Alternate Source	No	
6863i	Set Uses Alternate Source	Yes	
6865i	Set Uses Alternate Source	Yes	
6867i	Set Uses Alternate Source	Yes	
6869i	Set Uses Alternate Source	Yes	
6873i	Set Uses Alternate Source	Yes	
6920 IP	Firmware Included	Yes	
6930 IP	Firmware Included	Yes	
6940 IP	Firmware Included	Yes	

Set Model	**Set Status at MiVB Release 9.0**	**Set is available for purchase as of February 2018**	**Notes**
App Server	Blocked	No	Relies on legacy MiTAI interface that was removed in MiVB 8.0
Citel Link 1	Firmware Included	No	
Citel Link 2	Firmware Included	No	
DMP	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
Generic SIP Phone	Firmware Included	No	
Navigator	Firmware Included	No	
Netvision IP	Firmware Included	No	
OpenPhone 26/27	Firmware Included	No	
SC1000 Console	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
Spectralink (wireless)	Firmware Included	No	
SS4001	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
SS401	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
SS4015	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
SS4025	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
SS410	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
SS4125	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
SS4150	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB

Set Model	Set Status at MiVB Release 9.0	Set is available for purchase as of February 2018	Notes
			9.0
SS420	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
SS4230	Blocked	No	Relies on PER/DSU for connectivity - PER/DSU support discontinued in MiVB 9.0
TeleMatrix 3000IP	Set Uses Alternate Source	No	
UC Endpoint	Set Uses Alternate Source	Not Applicable	
Gigabit Ethernet Stand	*See note column*	Yes	Support depends on the actual IP Set being used with the Stand
Wireless LAN Stand	*See note column*	No	Support depends on the actual IP Set being used with the Stand
MiVoice Video/Conference	Set Uses Alternate Source	Yes	MiVoice Video/Conference registers as a UC Endpoint

Appendix B - Mitel 6900 Series Phones - Interfaces Security Bulletin

Version 1 - February 2019

Background

Mitel's 6900 series phones have a number of connectors that are used to interface the phone set to the LAN, Desk Top PC and also to phone accessories.

The intent of this bulletin is to inform Mitel customers regarding the interface connectors on the 6900 series of phones and their functionality.

The interface connectors may be grouped into two different categories; interface connectors that are secured via a cyber security mechanism, and interface connectors that are hardened to limit their functionality.

6920 Phone - Interfaces and Security Mechanisms

The following table describes the interface connectors supported on the 6920 phone set, the interface connector's purpose and if applicable, the interface connector's security mechanism.

Connector	Description	Purpose	Security Mechanism
Direct Network Connection	RJ45 Jack located on the back of the phone.	The direct network connection is used to connect the phone to the ethernet LAN and may also be used to power the phone from the LAN via Power over Ethernet.	This network connection supports the IEEE 802.1X network access control protocol, when this protocol is enabled and the phone is connected to a L2 access switch that is running the 802.1X protocol, the L2 access switch will need to authenticate the phone before the phone is granted access to the network.
Shared Network Connection	RJ45 Jack located on the back of the phone.	The shared network connection allows another network device to share the phone's connection to the network. Typically, the network device connected here would be a user's desk top PC. This feature is useful where there is only a single network connection available.	This network connection supports the IEEE 802.1X network access control protocol, when a device is connected to this port, the device will need to be authenticated by the L2 access switch before it is allowed to access the network. If the device is disconnected from this port and then reconnected, the device will have to be authenticated again before the device is granted access to the network.
Handset Connection	RJ9 Jack located on the back of the phone.	The handset connector is used to connect the Mitel supplied analog handset to the phone.	The handset connection supports the analog audio paths between the phone and the handset**. This interface cannot be used to compromise the phone's software. Cyber security controls are not applicable.**
Headset Port	RJ45 Jack located on the back of the	This headset port is used to connect a Wired Analog headset or a	The headset port supports the analog audio paths between the phone and the headset and also an

Connector	Description	Purpose	Security Mechanism
	phone.	DHSG/EHS Headset to the phone.	electronic hook switch circuit. **This interface cannot be used to compromise the phone's software. Cyber security controls are not applicable.**
USB Port	USB Type 'A' 4-pin Jack located on the back of the phone.	This connector supports USB 2.0 and 100mA of power, the connector is used to connect a USB based headset to the phone.	This USB port only supports a few Human Interface Device (HID) profiles. **This interface cannot be used to compromise the phone's software. The interface is hardened to only recognize HID messages.**
PKM Connector	A Mitel proprietary connector located on the back of the phone.	This Mitel proprietary interface is used to connect a M695 Colour Programmable Key Module (PKM) to the set.	This interface can only be used to provide connectivity between the phone and the PKM modules. **This interface cannot be used to compromise the phone's software. The interface is hardened to only communicate with PKM modules.**
Keyboard Connector	A 4-pin serial connector located on the bottom edge of the phone, below the dial pad.	This connector is used to connect an optional K680i keyboard to a phone. This functionality is only supported on the set when the set is running SIP software.	This interface can only be used to provide connectivity between a SIP based phone and the K680i keyboard. **This interface cannot be used to compromise the phone's software. The interface is hardened to only communicate with a K680i keyboard.**

Note: For diagrams showing connector locations, refer to the appropriate phone installation guide.

6930 Phone - Interfaces and Security Mechanisms

The following table describes the interface connectors supported on the 6930 phone set, the interface connector's purpose and if applicable, the interface connector's security mechanism.

Connector	Description	Purpose	Security Mechanism
Direct Network Connection	RJ45 Jack located on the back of the phone.	The direct network connection is used to connect the phone to the ethernet LAN and may also be used to power the phone from the LAN via Power over Ethernet.	This network connection supports the IEEE 802.1X network access control protocol, when this protocol is enabled and the phone is connected to a L2 access switch that is running the 802.1X protocol, the L2 access switch will need to authenticate the phone before the phone is granted access to the network.
Shared Network Connection	RJ45 Jack located on the back of the phone.	The shared network connection allows another network device to share the phone's connection to the network. Typically, the network device connected here would be a user's desk top PC. This feature is useful where there is only a single	This network connection supports the IEEE 802.1X network access control protocol, when a device is connected to this port, the device will need to be authenticated by the L2 access switch before it is allowed to access the network.

Connector	Description	Purpose	Security Mechanism
		network connection available.	If the device is disconnected from this port and then reconnected, the device will have to be authenticated again before the device is granted access to the network.
Handset Connection	RJ9 Jack located on the back of the phone.	The handset connector is used to connect the Mitel supplied analog handset to the phone.	The handset connection supports the analog audio paths between the phone and the handset**.** **This interface cannot be used to compromise the phone's software. Cyber security controls are not applicable.**
Headset Port	RJ45 Jack located on the back of the phone.	This headset port is used to connect a Wired Analog headset or a DHSG/EHS Headset to the phone.	The headset port supports the analog audio paths between the phone and the headset and also an electronic hook switch circuit. **This interface cannot be used to compromise the phone's software. Cyber security controls are not applicable.**
USB Port	USB Type 'A' 4-pin Jack located on the back of the phone.	This connector supports USB 2.0 and 500mA of power, the connector is used to connect a USB based headset to the phone.	This USB port only supports a few Human Interface Device (HID) profiles. **This interface cannot be used to compromise the phone's software. The interface is hardened to only recognize HID messages.**
PKM Connector	A Mitel proprietary connector located on the back of the phone.	This Mitel proprietary interface is used to connect a M695 Colour Programmable Key Module (PKM) to the set. This connector may also be used to connect to the Mitel Integrated DECT Headset.	This interface can only be used to provide connectivity from the phone to PKM modules and/or the Mitel Integrated DECT Headset. **This interface cannot be used to compromise the phone's software. The interface is hardened to only communicate with PKM modules and DECT Headsets.**
Keyboard Connector	A 4-pin serial connector located on the bottom edge of the phone, below the dial pad.	While physically present, this connector is not supported on the 6930 phone. The connector is not connected to any circuitry inside the phone.	This interface has no connectivity into the phone. **This interface cannot be used to compromise the phone's software since it does not actually connect to anything within the phone.**

Note: For diagrams showing connector locations, refer to the appropriate phone installation guide.

6940 Phone - Interfaces and Security Mechanisms

The following table describes the interface connectors supported on the 6940 phone set, the interface connector's purpose and if applicable, the interface connector's security mechanism.

Connector	Description	Purpose	Security Mechanism
Direct Network Connection	RJ45 Jack located on the back of the phone.	The direct network connection is used to connect the phone to the ethernet LAN and may also be used to power the phone from the LAN via Power over Ethernet.	This network connection supports the IEEE 802.1X network access control protocol, when this protocol is enabled and the phone is connected to a L2 access switch that is running the 802.1X protocol, the L2 access switch will need to authenticate the phone before the phone is granted access to the network.
Shared Network Connection	RJ45 Jack located on the back of the phone.	The shared network connection allows another network device to share the phone's connection to the network. Typically, the network device connected here would be a user's desk top PC. This feature is useful where there is only a single network connection available.	This network connection supports the IEEE 802.1X network access control protocol, when a device is connected to this port, the device will need to be authenticated by the L2 access switch before it is allowed to access the network. If the device is disconnected from this port and then reconnected, the device will have to be authenticated again before the device is granted access to the network.
Handset Connection	RJ9 Jack located on the back of the phone.	The handset connector is used to connect the Mitel supplied analog handset to the phone.	The handset connection supports the analog audio paths between the phone and the handset**.** **This interface cannot be used to compromise the phone's software. Cyber security controls are not applicable.**
USB Port	USB Type 'A' 4-pin Jack located on the back of the phone.	This connector supports USB 2.0 and 500mA of power, the connector is used to connect a USB based headset to the phone.	This USB port only supports a few Human Interface Device (HID) profiles. **This interface cannot be used to compromise the phone's software. The interface is hardened to only recognize HID messages.**
PKM Connector	A Mitel proprietary connector located on the back of the phone.	This Mitel proprietary connector is used to connect a M695 Colour Programmable Key Module (PKM) to the set. This connector may also be used to connect to the Mitel Integrated DECT Headset.	This interface can only be used to provide connectivity from the phone to PKM modules or the Mitel Integrated DECT Headset. **This interface cannot be used to compromise the phone's software. The interface is hardened to only communicate with PKM modules and DECT Headsets.**

Note: For diagrams showing connector locations, refer to the appropriate phone installation guide.

Mitel

Powering connections

mitel.com