

MITEL

# Technical | Engineering Guidelines

## Teleworker Solution

Release 4.5

 **MITEL** | it's about **YOU**

## **NOTICE**

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks Corporation. The information is subjected 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 changes.

No part of this document may be reproduced or transmitted in any form by any means – electronic or mechanical – for any purpose without written permission from Mitel Networks Corporation.

**TELEWORKER Release 4.5 Engineering Guidelines**  
**September 2007**

**®,<sup>TM</sup> Trademark of MITEL Networks Corporation**  
**© Copyright 2007 MITEL Networks Corporation**  
**All rights reserved**

## TABLE OF CONTENTS

<b>ABOUT THIS DOCUMENT .....</b>	<b>1</b>
Overview .....	1
Prerequisites .....	1
About the Teleworker Documentation Set .....	1
What's New for Release 4.5 .....	1
Quality of Service and the Teleworker Solution .....	2
A Note About Security .....	2
<b>ENTERPRISE SITE REQUIREMENTS .....</b>	<b>3</b>
ICP .....	3
Hardware/Software .....	4
Bandwidth .....	4
Sample Calculations for Voice Use .....	6
Your Assistant Requirements .....	6
Mitel Contact Center Softphone .....	7
<b>REMOTE SITE REQUIREMENTS .....</b>	<b>9</b>
Generic Configuration .....	9
Router/Internet Gateway .....	9
Router Gateway Requirements .....	9
VPN Connectivity .....	10
Bandwidth Requirements (Remote Site) .....	10
IP Phones .....	12
Configuring a Corporate Firewall to Host a Remote Phone .....	13
<b>SUPPORTED CONFIGURATIONS .....</b>	<b>15</b>
Teleworker Solution as Internet Gateway (Server-Gateway Mode) .....	15
Teleworker Solution Deployed in DMZ (Server Only Mode) .....	17
Significant Firewall Characteristics .....	18
Known Issues .....	19
Port-forwarding Firewalls .....	19
<b>FIREWALL CONFIGURATION .....</b>	<b>20</b>
<b>PERFORMANCE GUIDELINES .....</b>	<b>22</b>
Teleworker .....	22
Teleworker Deployed on APC .....	22

<b>GLOSSARY .....</b>	<b>23</b>
<b>APPENDIX A – SUPPORTED ROUTERS .....</b>	<b>25</b>

## List of Tables

<b>Table 1. Hardware and Software Requirements .....</b>	<b>4</b>
<b>Table 2. Bandwidth Requirements at the Enterprise Site .....</b>	<b>5</b>
<b>Table 3. YA Collaboration Bandwidth Requirements .....</b>	<b>7</b>
<b>Table 4: Database transfer costs (1 client) .....</b>	<b>8</b>
<b>Table 5: Bandwidth requirements for typical Contact Center client use.....</b>	<b>8</b>
<b>Table 7. Generic Router Requirements .....</b>	<b>9</b>
<b>Table 7. Remote Site Bandwidth Requirements.....</b>	<b>11</b>
<b>Table 10. Bandwidth Usage vs Time for a 5020/5220 IP Phone .....</b>	<b>11</b>
<b>Table 9. IP Address Requirements: Teleworker Solution as Gateway.....</b>	<b>16</b>
<b>Table 10. IP Addresses: Teleworker Gateway Deployed in DMZ.....</b>	<b>18</b>
<b>Table 11. Protocols and Ports used by the Teleworker Solution .....</b>	<b>20</b>

## List of Figures

<b>Figure 1. Remote Site Block Diagram .....</b>	<b>9</b>
<b>Figure 2. Teleworker phone behind a corporate firewall.....</b>	<b>13</b>
<b>Figure 3. Teleworker Solution as Internet Gateway (Example 1).....</b>	<b>15</b>
<b>Figure 5. Teleworker Solution as Internet Gateway (Example 2).....</b>	<b>16</b>
<b>Figure 5. Teleworker Deployed in DMZ .....</b>	<b>17</b>



## About this Document

### Overview

The purpose of this document is to describe configuration rules for the Mitel Teleworker Solution® in order to assist in sales and support of this product. This information is intended for Training, Sales and Product support staff and complements other sales material and product documentation.

### Prerequisites

As the scope of these Engineering Guidelines is to cover the Teleworker Solution application, which runs on the Mitel Standard Linux Server (MSL), the reader should first see the *MSL Installation and Administration Guide* and the *MSL Qualified Hardware* document. These are available from <http://edocs.mitel.com>.

### About the Teleworker Documentation Set

For easy access to the various Mitel documentation suites, go to <http://edocs.mitel.com>.

**Note:** You require a Mitel OnLine user name and password to access this site.

The following guides provide complete information about Teleworker:

- The *Teleworker Engineering Guidelines* (this document).
- The *Teleworker Solution Blade Guide* provides information about system requirements, installation of Teleworker and configuration Teleworker options and firewalls.
- The *Remote IP Phones Configuration Guide* provides information about configuring remote phones.

Visit [Mitel on Line](#) (MOL) for the latest updated Technical Bulletins, Release Notes and Knowledge Base articles.

### What's New for Release 4.5

- Support for up to 1000 connected sets
- Support for the Mitel 5560 IPT
- Port to Mitel Standard Linux 8.2 platform
- Simple resiliency
- Integration with Mitel Applications Suite Release 1.0
- User interface improvements
- New traceroute diagnostic
- Mitel Contact Center softphone support

## Quality of Service and the Teleworker Solution

A number of factors can degrade the quality of voice experienced by users. Proper provisioning and configuration can control some of these factors.

The impact of congestion at peak times is not always apparent on applications such as web browsing, however congestion can noticeably degrade voice. Bandwidth at the enterprise and at the remote site must be sufficient to handle the peak traffic of all Internet activities. Refer to the appropriate sections in this document for guidelines in provisioning the Teleworker Solution components.

Within the enterprise, the number of hops between the firewall, Teleworker server and ICP should be kept to a minimum – no more than 3 hops per segment (firewall to Teleworker server, Teleworker server to ICP). Congestion levels in the Internet can vary widely, impacted by factors such as:

- Time of day
- News stories such as catastrophes, sporting events, elections
- Viruses
- Service failures

The Internet transport between a remote phone and the enterprise may introduce a significant amount of delay, depending on the number of hops. If it is possible for the remote locations to use the same Internet Service Provider as the corporate office, this should increase the quality of service as the traffic will usually remain on the ISP's extended network and not traverse the public Internet.

Applications running on the PCs at the remote site may also affect voice quality. In particular, “bursty” and streaming traffic such as streaming audio and automated system updates (for example, virus pattern downloads and mailbox synchronization) may have a noticeable effect on voice quality.

## A Note About Security

Due to the broad range of application types that can be deployed on the Mitel Standard Linux operating system (formerly Managed Application Server), we suggest that you read the Security section of the *Mitel Standard Linux Installation and Administration Guide* before installing this application in co-residency with other applications

## Enterprise Site Requirements

Components at the enterprise include

- ICP
- MSL with Teleworker Solution blade installed
- Firewall.

The MSL server may provide the firewall function. See Supported Configurations for supported configurations.

### ICP

The table below lists the minimum version of ICP required for compatibility with the Teleworker Solution, and the supported variants of IP Phone. Before deploying a set as a teleworker, please be sure it has the latest set load applied by booting it from an up-to-date ICP.

Platform	Release	Compatible Sets							
		5215 5220	DM 5215/ 5220	5235	5212 5224	Navi- gator	YA 3.2	5330 5340	5560 IPT <sup>4</sup>
3300 ICP	6.0	Yes	Yes	Yes	No	No	No	No	No
	6.1	Yes	Yes	Yes	Yes	Yes <sup>1</sup>	No	No	No
	7.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes <sup>3</sup>	No
	7.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes <sup>5</sup>
	8.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SX-200 ICP	2.0	Yes	Yes	No	No	No	Yes <sup>2</sup>	No	No
	3.0	Yes	Yes	No	Yes	No	Yes	No	No
	4.0	Yes	Yes	No	Yes	No	Yes	Yes <sup>6</sup>	No

1. Release 6.1 UR 1 or later

2. YA Desk phone support only

3. Release 7.0 UR2 or later

4. 5560 IPT Release 1.0 sets count as two devices when provisioning for Teleworker

5. Release 7.1 UR2 or later

6. Release 4.0 UR1 or later

**Note:** Teleworker Release 4.5 also supports Contact Center Release 5.3 softphones.

## Hardware/Software

**Table 1. Hardware and Software Requirements**

Item	Requirements	Notes
Hardware	PC compatible See the MSL hardware recommendations at <a href="http://edocs.mitel.com">http://edocs.mitel.com</a> .	At least 1.8 GHz P4 CPU 256MB RAM 10GB hard drive CDROM Dual Ethernet interfaces (for server-gateway deployment); or Single Ethernet interface (for DMZ deployment)
Software	MSL release 8.2 or later	Server must be registered at the Applications Management Center for the Teleworker Solution product.

Please note that the above numbers indicate the absolute minimum requirements, and using the maximum number of users on a low-end server will result in difficulty in administration via the web interface.

## Bandwidth

This section analyzes bandwidth requirements for the Teleworker Solution only. Typically, there will be other requirements for Internet access, and these requirements (such as e-mail, web browsing, e-commerce) must be provisioned as well.

In coverage of Your Assistant, this document will be covering the bandwidth requirements for the Enterprise and Remote sites, and the firewall configuration, nothing more. Please reference The Your Assistant Engineering Guidelines for full information regarding YA.

**Failure to provide sufficient bandwidth for all Internet activities may compromise the quality of service of the Teleworker Solution.**

Bandwidth requirements for individual phones are provided in Bandwidth Requirements (Remote Site).

The table below shows the bandwidth requirements at the enterprise for up to 1000 teleworker phones.

### Assumptions:

- Internet Service Providers specify bandwidth available to the user. i.e. PPPoE overhead does not need to be included in the provisioning of DSL bandwidth, but IP overhead does need to be included
- Erlang Compensation can be used to predict required bandwidth to achieve desired blocking levels when the number of remote phones exceeds 6. For less than 6 remote users, 99% non-blocking is achievable by provisioning for all users simultaneously.
- The table below assumes the remote phone user is busy approx 14 minutes per hour, with roughly 6 calls per hour. Heavier usage will necessitate more bandwidth at the enterprise.
- RTP Bandwidth Requirement is 80 Kbps for G.711 and 24 Kbps for G.729 at 6 calls per hour
- Control stream bandwidth requirement is 20 Kbps peak and 1 Kbps idle
- For fewer than 12 remotes, provision for 1 peak on control stream, provision for 2 if more than 12 remote phones

- The table below does not include bandwidth required for features such as paging. If group paging is enabled for teleworkers, an additional RTP stream should be provisioned for each remote member of the paging group
- Whenever possible, transcoding should be performed by the ICP rather than the Teleworker Solution, as this typically provides improved voice quality.
- CPH = Calls Per Hour
- .167e = For simplicity we use 100 second call hold time, so 6 CPH = 600 seconds. 1 Erlang (1e) is 100% of one busy hour. So 600 seconds = 1/6 hour (600/3600) = 0.167e.
- GOS = grade of service and relates to how many calls we would expect to be blocked due to limited resource. P.001 is the normal standard for internal calls and means 1 in 1000 calls are blocked.

**Table 2. Bandwidth Requirements at the Enterprise Site**

Number of Remote Phones (6CPH, 0.167e)	Simultaneous Calls (GOS P.0.0.1)	Bandwidth Required	
		G.711	G.729
1	1	100 kbps	50 kbps
2	2	180 kbps	75 kbps
3	3	260 kbps	100 kbps
4	4	340 kbps	125 kbps
5	5	420 kbps	150 kbps
6,7	6	500 kbps	175 kbps
8,9	8	670 kbps	230 kbps
10-12	10	840 kbps	280 kbps
13	11	910 kbps	300 kbps
14-18	13	1100 kbps	370 kbps
19-25	16	1350 kbps	450 kbps
50	25	2100 kbps	690 kbps
100	41	3420 kbps	1130 kbps
150	57	4800 kbps	1600 kbps
200	71	5950 kbps	2000 kbps
250	86	7200 kbps	2400 kbps
300	100	8350 kbps	2750 kbps
400	128	10700 kbps	3550 kbps
500	156	13100 kbps	4300 kbps
600	183	15300 kbps	5100 kbps
700	211	17700 kbps	5900 kbps

Number of Remote Phones (6CPH, 0.167e)	Simultaneous Calls (GOS P.0.0.1)	Bandwidth Required	
		G.711	G.729
800	238	19900 kbps	6600 kbps
900	265183	22200 kbps	7300 kbps
1000	291	24400 kbps	8100 kbps

## Sample Calculations for Voice Use

### G.729a configuration

The value for a site configured for G.729a with 12 users is derived using the following formula:

Bandwidth = number of users \* idle control stream requirement + number of calls \* RTP requirement (24Kbps) + 1 \* peak control stream bandwidth

$$= 12*1 + 8*24 + 1*20$$

$$= 224 \text{ (rounded to 225 Kbps)}$$

### G.711 configuration

The equivalent calculation for a site configured with G.711 is:

Bandwidth = number of users \* idle control stream requirement + number of calls \* RTP requirement (80Kbps) + 1 \* peak control stream bandwidth

$$= 12*1 + 8*80 + 1*20$$

$$= 672 \text{ (rounded to 670 Kbps)}$$

## Your Assistant Requirements

A YA client, version 3.2+, with Softphone module counts as a remote set in Table 2, with additional bandwidth required for its login, presence and collaboration connections.

The login and presence connections use negligible bandwidth, and do not require real-time priority, so as long as there is a small amount of bandwidth remaining, they should function without difficulty.

The collaboration connection can require considerable bandwidth, based on the feature used, the number of presenters, and the number of participants. Table 3 provides a typical use-case by number of presenters and participants, with the estimated bandwidth required. Note that this table assumes the following settings:

- PowerPoint sharing: enabled
- Desktop/App sharing: disabled
- Audio setting: good
- Video setting: low

For full details, consult the Your Assistant Engineering Guidelines.

**Table 3. YA Collaboration Bandwidth Requirements**

Presenters	Participants	Bandwidth Required
1	1	192Kbps
1	2	256Kbps
1	5	448Kbps
2	2	460Kbps
2	5	736Kbps
1	10	768Kbps
2	10	1.2Mbps
2	50	4.9Mbps
5	100	18.7Mbps

**Note:** The above bandwidth requirements are in addition to those for voice, as shown in Table 2.

## Mitel Contact Center Softphone

The Teleworker 4.5 release introduces support for the Mitel Contact Center Softphone, version 5.3. This softphone has multiple components, much like Mitel Your Assistant. When using the voice component, the bandwidth requirement should be identical to any other Mitel set in a voice call, using G.711 or G.729 (compression). Mitel Contact Center Softphone supports the following additional connections through the Teleworker server:

Teleworker Server Port Used	Default Destination Port	Description
TCP port 36000	TCP port 80	HTTP authentication and user profile access
TCP port 36001	TCP port 443	HTTPS authentication and user profile access
TCP port 36002	TCP port 5024	Realtime client
TCP port 36003	TCP port 5025	Auditor connection
TCP port 36004	TCP port 5026	Telephony proxy

The “Teleworker Server Port Used” column indicates which port on the Internet side of the Teleworker is used to proxy the incoming connection, (that is, which port must be open in any firewall behind which the Teleworker server is deployed. The “Default Destination Port” is the LAN-side port to which the connection is proxied. Traffic to these ports from the Teleworker server to the ACD server must be permitted as well. Please see the Firewall Configuration section for full details.

The bandwidth use of the client depends on the purpose for which it is used. There is an initial cost in installing the client as software is downloaded and updated, and for periodic updates to upgrade the client software. These are short-term costs that are negligible in the long run.

When you open the Contact Center client and select the devices that you wish to view in a monitor, there is an initial database transfer.

As a rule devices require the following bandwidth.

1 Queue (Q) = 65 KB

1 Agent (A) = 39 KB

1 Employee (Em) = 20 KB

1 Extension (Ex) = 17 KB

1 Network Monitor (NM) (1 x 3300 ICP) = 56 KB

# of Devices	Configuration	Data size	Bandwidth (hh:mm:ss)				
			512 Kbps	1.024 Mbps (DSL)	1.54 Mbps (T1 / DSL)	2.048 Mbps	10 Mbps
5	1 Q, 1 A, 1 Ex, 1 Em, 1 NM	157.6 KB	00:00:02	00:00:01	00:00:01	00:00:00	00:00:00
50	15 Q, 11 A, 11 Ex, 12 Em, 2 NM	303.2 KB	00:00:04	00:00:02	00:00:01	00:00:01	00:00:00
100	25 Q, 25 A, 22 Ex, 25 Em, 3 NM	348.8 KB	00:00:06	00:00:03	00:00:02	00:00:01	00:00:00
500	200 Q, 100 A, 92 Ex, 100 Em, 8 NM	1.304 MB	00:00:20	00:00:10	00:00:06	00:00:05	00:00:01
1500	500 Q, 300 A, 385 Ex, 300 Em, 15 NM	3.528 MB	00:00:55	00:00:27	00:00:18	00:00:13	00:00:02
5000	2086 Q, 2379 A, 247 Ex, 322 Em, 16 NM	14.24 MB	00:03:42	00:01:51	00:01:13	00:00:55	00:00:11
8100	3036 Q, 4379 A, 247 Ex, 322 Em, 16 NM	22.72 MB	00:05:55	00:02:57	00:01:57	00:01:28	00:00:18

**Table 4: Database transfer costs (1 client)**

Table 5 illustrates the typical bandwidth requirements for a single Contact Center client.

Calls per hour (CPS)	Per ICP (KBps)	Per real-time client (KBps)
100	0.06	0.06
1000	0.61	0.59
2000	1.22	1.18
3000	1.84	1.77
4000	2.45	2.36
5000	3.06	2.95
6000	3.67	3.54

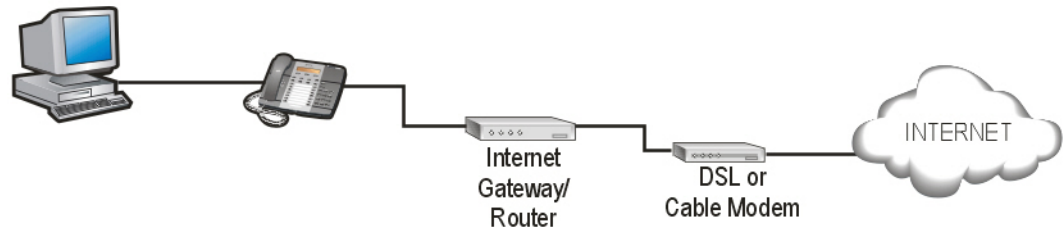
**Table 5: Bandwidth requirements for typical Contact Center client use**

*Note: This example is designed as a guideline only. Actual results may vary with each contact center configuration. The addition of Interactive Contact Center (MiTAI) will increase the bandwidth requirements.*

## Remote Site Requirements

### Generic Configuration

A generic configuration depicting the necessary elements at the teleworker site is shown in Figure 1.



**Figure 1. Remote Site Block Diagram**

**Note:** The PC is not a 'necessary' element. If there is a PC at the remote site, it may be connected via the phone, or directly to the router. Additional PCs will be connected directly to the router.

### Router/Internet Gateway

Table 6 lists the generic requirements for a router at the remote site.

**Table 6. Generic Router Requirements**

Requirement	Details	Notes
Connectivity	RJ45 10/100 Mbps	
Router Protocols	DHCP	See <a href="#">Table 8</a> for required network parameters
	NAT	Required if multiple devices (e.g. IP Phone + PC) are present
	PPPoE or PPPoA	Usually required if internet connection is DSL Router must be configured with userid and password provided by Internet Service Provider
	Authenticated DHCP	May be required for cable Internet connection. Router must be configured with userid and password provided by Internet Service Provider
	UDP	Pass through
	TFTP	Pass through

### Router Gateway Requirements

The Internet connection must be controlled/configured by the Internet Gateway/Router. This allows multiple devices to share the Internet connection. For example, the Teleworker Solution is not supported on USB PPPoE (or PPPoA) modems, as they do not provide additional ports for connection of the IP Set.

The Teleworker Solution is not supported in situations that require specific software to be loaded on the desktop PC to manage the connection. For example, the Teleworker Solution is not

supported with AOL broadband, as it requires specific software to be loaded onto the PC to allow that PC (and only that PC) to access the Internet)

A list of supported Gateway/Routers is provided in Appendix A – Supported Routers.

## VPN Connectivity

Connecting the PC to the phone does *not* provide the PC with a connection to the corporate network. That connection must still be made by the use of a VPN client installed on the PC. This ensures that existing security of the corporate network is maintained when the Teleworker Solution is deployed. A gateway to gateway VPN can be constructed in such cases to allow all client PCs to have access. However, a word of caution: routing Teleworker voice traffic across the VPN can have adverse effects on voice quality. If possible, the voice traffic should be allowed to traverse the Internet, while tunneling data traffic across the VPN.

The MSL server on which the Teleworker Solution runs can optionally provide data VPN services, however a VPN is not required for the Teleworker Solution. Details can be found in the Managed Application Server Installation and Administration Guide, available at <http://edocs.mitel.com/>

### Use of an existing corporate VPN

The Teleworker Solution does not affect any existing VPN client software server (e.g. IPSEC road warrior connection) installed on the remote PC. The PC should be connected to either the second Ethernet port of the IP phone or directly to the router and the existing software should be used as before.

**Note:** To activate the second Ethernet port on sets connected to an SX-200 ICP, the appropriate system option must be purchased and the phone's class of service must be changed.

**Note:** VPN (e.g. IPSEC) pass-through must be supported by the router at the remote site.

### Corporate firewall/network configuration for VPN access

The corporate office firewall may need to be reconfigured to allow other traffic from the MSL to the internal network if the MSL is used as a VPN server. The ports and protocols required will depend on the applications used by the client PCs and this configuration is outside the scope of this document.

More information on firewall configuration guidelines can be found in Figure 4 – Teleworker Deployed in DMZ and in Firewall Configuration.

## Bandwidth Requirements (Remote Site)

This section analyzes bandwidth requirements for the Teleworker Solution only. Typically, there will be other requirements for Internet access, and these requirements (such as e-mail, web browsing, e-commerce) must be provisioned as well. Failure to provide sufficient bandwidth for all Internet activities may compromise the quality of service of the Teleworker Solution

The table below details the bandwidth required by a teleworker phone, including voice stream, peak control stream utilization, and IP header overhead.

**Table 7. Remote Site Bandwidth Requirements**

Requirement	Bandwidth	Notes
Internet Access Bandwidth required for each Teleworker phone *see Note 3	50 Kbps (bi-directional) *see Note 1	if G.729a compression is enabled at enterprise
	100 Kbps (bi-directional) *see Note 1	if G.729a compression is not enabled
YA Collaboration	192 Kbps (bi-directional) *see Note 2	

**Note 1:** If the remote phone user is a member of a paging group, or if off hook call announce is enabled, additional bandwidth will be needed. An additional 50 kbps per phone needs to be provided for G.729 paging, 100 kbps for G.711.

**Note 2:** This bandwidth requirement assumes that audio quality is set to “good”, video quality is set to “low”, and Powerpoint sharing is enabled, with desktop/app sharing disabled. Please refer to the Your Assistant Engineering Guidelines for full details.

**Note3:** Internet access bandwidth requirements include IP overhead, and possibly more depending on your access technology. Speak with your Internet Service Provider.

Table 7 does not consider bandwidth requirements for PCs or other devices, which must be provisioned in addition to the IP Phone. If there is insufficient bandwidth, symptoms experienced by the IP phone user may include degraded voice quality, slow response, service interruption or loss of service.

### Bandwidth Usage and ISP Quotas

Many Internet Service Providers set quotas on the amount of IP bandwidth per month. As an aid in predicting whether a specific quota will be exceeded, this section provides the necessary data and a sample calculation.

Assumptions:

- Signaling channel requires 1 KByte per minute (average), based on 6 calls per hour, business usage, 15 minutes per hour
- G.711 voice stream requires 10 kBytes per second (IP)
- G.729A voice stream requires 3 kBytes per second (IP)
- IP header is counted as user information

**Table 8. Bandwidth Usage vs Time for a 5020/5220 IP Phone**

	Bandwidth Required	Hourly Bandwidth Usage (100%)	Monthly Bandwidth Usage (100%)
<b>Signaling Stream</b>	1 kByte per minute	60 kByte	43.2 MB
<b>G.711 Voice Stream (IP), 20ms</b>	80 kbps	36 MB	25.92 GB
<b>G.729a Voice Stream (IP), 20ms</b>	24 kbps	10.8 MB	7.78 GB

**Note:** 20ms RTP packets is the default, but is configurable by set in the Teleworker solution administration panel in the server-manager.

The data in Table 8 can be used in different ways:

- Estimate the available call time given a quota

- Estimate the monthly bandwidth requirement given a call profile.

**Estimating Available Call Time**

**Example:** ISP Quota is 2 GBytes per month, use is continuous

Call hours of G.729a =  $(2000 \text{ MBytes} - 43.2 \text{ Mbytes}) / 10.8 \text{ MBytes per hour} = 181 \text{ hours}$

Call hours of G.711 =  $(2000 \text{ MBytes} - 43.2 \text{ MBytes}) / 36 \text{ MBytes per hour} = 54 \text{ hours}$

**Example:** ISP Quota is 2 GBytes per month, use is 15min per hour, 12 hours per day, 7 days per week

Call hours of G.729a =  $(1448 \text{ hours or more than 1 month})$

Call hours of G.711 =  $(432 \text{ hours or roughly 18 days})$

**Estimating Monthly Bandwidth Requirement**

**Example:** A user that averages 4 hours of phone calls per day, for 22 workdays in a month.

Bandwidth Usage for G.729a =  $43.2 \text{ MBytes} + (10.8 \text{ MBytes} \times 4 \text{ hr per day} \times 22 \text{ days}) = 994 \text{ MBytes}$

Bandwidth Usage for G.711 =  $43.2 \text{ MBytes} + (36 \text{ MBytes} \times 4 \text{ hr per day} \times 22 \text{ days}) = 3200 \text{ MBytes or } 3.2 \text{ GBytes}$

**IP Phones**

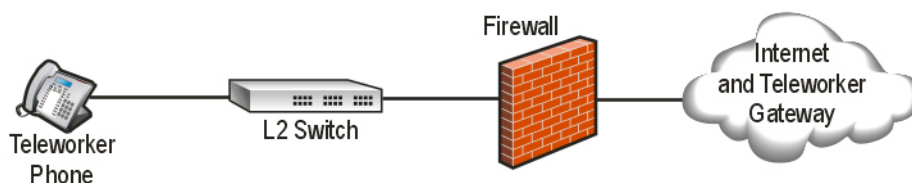
The remote location must meet the following IP Phone requirements:

Component	Details	Notes
Supported IP Phones	Mitel 5020 IP Phone Mitel 5212 IP Phone Mitel 5215 IP Phone Mitel 5220 IP Phone Mitel 5224 IP Phone Mitel Dual Mode 5215 IP Phone Mitel Dual Mode 5220 IP Phone Mitel 5235 IP Phone Mitel 5330 IP Phone Mitel 5340 IP Phone Mitel 5560 IPT Mitel Navigator Your Assistant Softphone (3.2 or higher) Contact Center 5.3 Softphone	
Supported peripherals	5305 IP Conference Unit 5310 IP Conference Unit Line Interface Module	<b>Note:</b> 5422 PKM is <u>not</u> supported
Required Network Parameters	IP Address	Provided by the Internet
	Subnet Mask	

Component	Details	Notes
	Default Gateway IP Address	Gateway
	Teleworker Gateway IP Address	Manually programmed into the IP Phone (see <i>Remote IP Phones Configuration Guide for Teleworker</i> available at Mitel OnLine)
Voice Encryption Algorithm	AES	
Maximum IP Phones per Remote Site	20	Bandwidth must be provisioned for all Internet traffic, including applications other than the Teleworker Solution application.  <b>NOTE:</b> Maximum number of sets per remote site may be adversely affected by router performance.

## Configuring a Corporate Firewall to Host a Remote Phone

In the event it is necessary to operate a Teleworker phone behind a corporate firewall, as depicted in Figure 2 below, one of two approaches can be used.



**Figure 2. Teleworker phone behind a corporate firewall**


1. The firewall can be configured to allow all connections to and all responses from the Teleworker Gateway IP address.
2. Alternatively, a more restrictive approach would be to configure the firewall with the following:
  - Allow a bi-directional TCP connection to destination port 6801 and 6802 on Teleworker Solution IP address
  - Allow bi-directional TCP connections to destination ports 3998 and 6880 on the Teleworker Solution IP address (for 5235, 5330, 5340 and Navigator set features)
  - Allow incoming UDP from source ports 20000 to 23000 on Teleworker Solution IP address
  - Allow outgoing UDP to destination ports 20000 to 23000 on Teleworker Solution IP address


- Allow bi-directional TCP connections to destination ports 2114, 2116, 35000 and 37000 on the Teleworker Solution IP address, if using Your Assistant

## Supported Configurations


There are two supported configurations for the Teleworker Solution:

- Teleworker as Internet Gateway
- Teleworker Solution Deployed in DMZ

 **Note:** For deployment as an Internet gateway, the external address **must** be dedicated to the Teleworker Solution, publicly routable, and reachable from both the Internet and the **internal** network.

 For deployment in a DMZ, the external address **should** be dedicated to the Teleworker Solution (see Note below), **must** be publicly routable and reachable from both the Internet and the **internal** network.

**NOTE: Failure to follow these guidelines will result in one-way or no audio.**

 **Note:** Some firewalls which use port-forwarding to simulate a DMZ are. (see Port-forwarding Firewalls.)

### Teleworker Solution as Internet Gateway (Server-Gateway Mode)

If an enterprise does not have an existing firewall, Mitel recommends deploying the Mitel Standard Linux (MSL) server as the Teleworker Solution, Internet gateway and firewall.

Figure 3 shows an example of this configuration using the Teleworker Solution and a Mitel 3300 ICP. The same configuration can be used when deploying the Teleworker Solution with an SX-200 ICP.

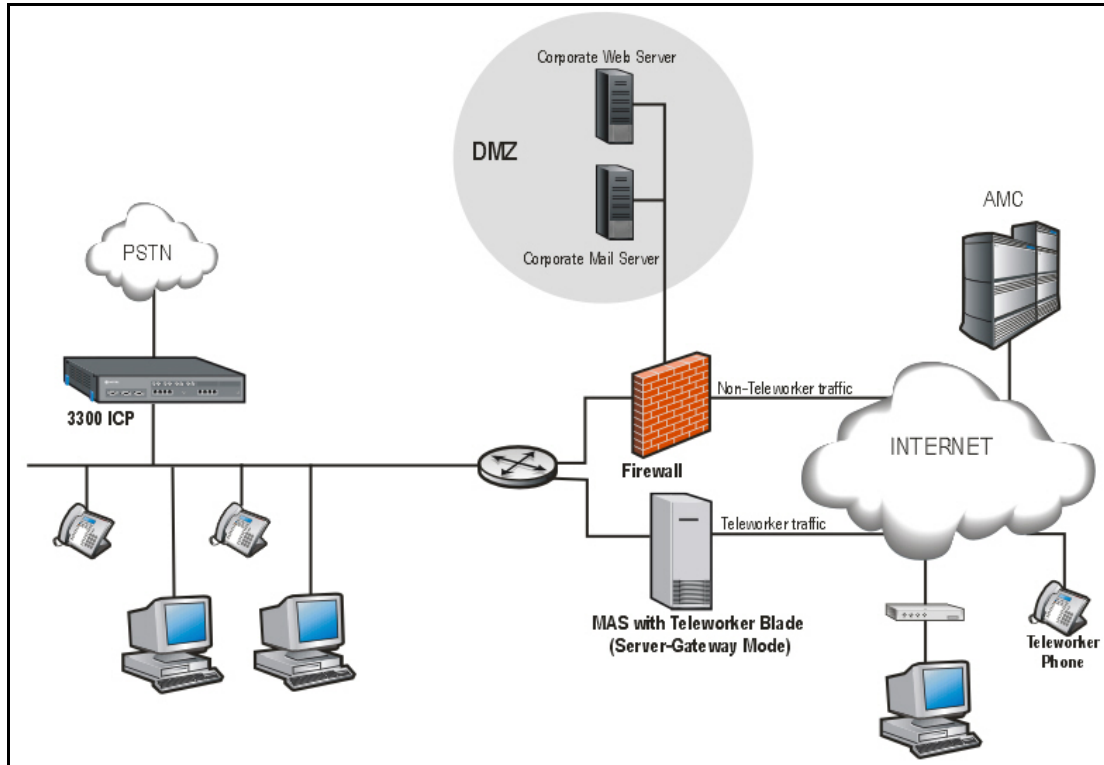


Figure 3. Teleworker Solution as Internet Gateway (Example 1)

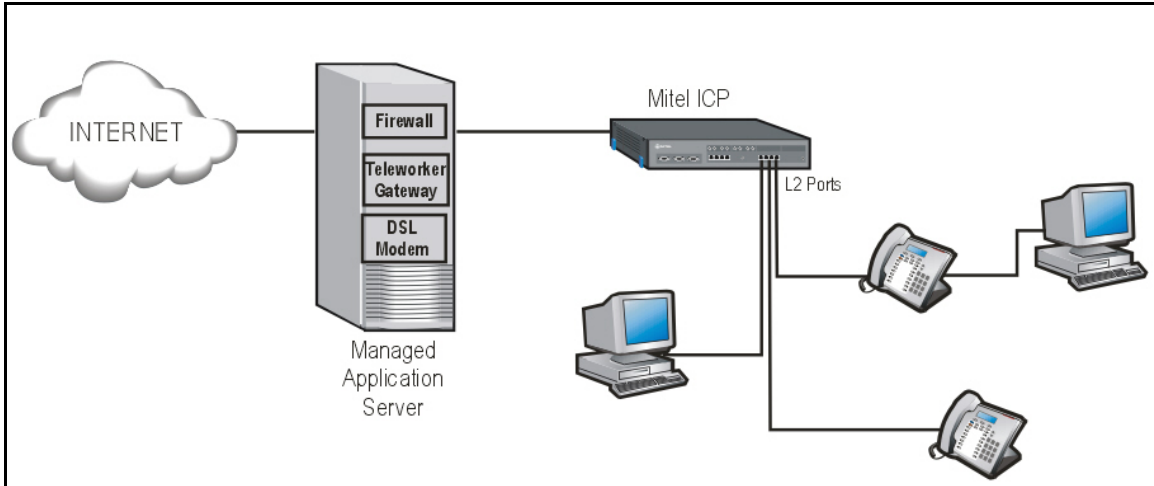



Figure 4. Teleworker Solution as Internet Gateway (Example 2)

Table 9. IP Address Requirements: Teleworker Solution as Gateway

<p><b>External: 1 Static Address</b></p> <p>(This address must be directly attached to the MSL server and not subject to NAT or behind another firewall)</p> <p> <b>Note:</b> If this address changes, all deployed Teleworker sets must be reprogrammed with the new address.</p>	<p>This address must be:</p> <ul style="list-style-type: none"> <li>• static</li> <li>• publicly/Internet routable</li> <li>• reachable from the customer network</li> </ul> <p>The interface may optionally be configured through DHCP, PPPoE, or PPPoA, but the address assigned must be static. Remote sets will lose connectivity to the Teleworker Gateway if the address changes.</p>
<p><b>Internal: 1 Static Address</b></p>	<p>This address is allocated from the customer's internal network range.</p>

An enterprise can take advantage of the DSL, authenticated DHCP and ISDN capabilities of the MSL server.

Key points of this configuration:

- MSL provides:
  - Teleworker Solution blade
  - NAT for all devices at the enterprise
  - Firewall

PPPoE or PPPoA<sup>1</sup> for DSL, authenticated DHCP for cable modems, ISDN, etc.

**Additional local networks**

Additional internal networks or subnets that require access to the Teleworker Solution can

<sup>1</sup> PPPoA support is limited in the current release. Mitel UK Product Support recommends the use of a D-Link DSL 300T modem at the enterprise site if PPPoA connectivity is required in gateway mode. Configure the modem to provide DHCP on the internal interface, and use DHCP on the MSL server to configure the public interface. The modem acts as a bridge. Note that PPPoA 'routers' that provide NAT will not work here.

be added via the "Local Networks" panel of the server manager. This access can be limited to individual hosts, or large network blocks can be used. In all cases, the "Router" property should be set to the address of the router on the subnet attached to the MSL server internal interface.

- To allow access from the single subnet 192.168.12.0/24, you would enter 192.168.12.0/255.255.255.0 in the "Local Networks" panel.
- If the customer's network has multiple subnets, with a common prefix, you can allow access from the prefix. For example, if the customer uses various subnets within the 192.168.0.0/16 network, you would enter 192.168.0.0/255.255.0.0 in the "Local Networks" panel, and allow the local router to determine the routing to the individual subnets.

It is worth noting that unless these networks are added via the Local networks panel, they will be unable to use the Teleworker server.

## Teleworker Solution Deployed in DMZ (Server Only Mode)

The Teleworker Solution can also be deployed behind a customer-provided or customer-managed firewall as shown in Figure 4. This firewall **must** have 3 network interfaces (ports): WAN, LAN, and DMZ. Two-port firewalls are **not supported**.

It should also be noted that some "DSL routers" with port forwarding are simply two-port NAT devices and should be treated as any other two-port firewall. Deployment of the Teleworker Solution behind such devices is not supported.

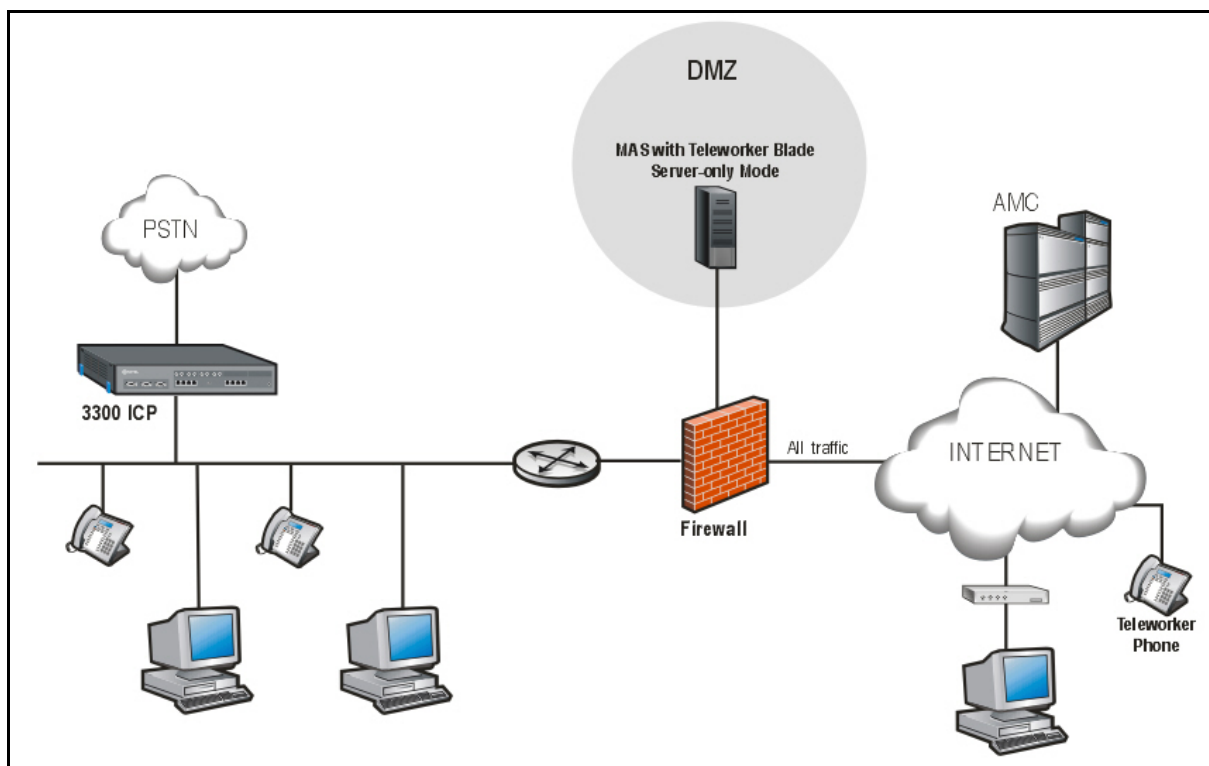


Figure 5. Teleworker Deployed in DMZ

**Table 10. IP Addresses: Teleworker Gateway Deployed in DMZ**

<p><b>External: 1 Static Address</b> (Address of the MSL server <i>prior</i> to DMZ network address translation)</p> <p>If this address changes, all deployed teleworker sets must be reprogrammed with the new address.</p>	<p>This address must be:</p> <ul style="list-style-type: none"> <li>• static</li> <li>• publicly/Internet routable</li> <li>• reachable from the customer network</li> <li>• able to reach the customer network</li> </ul> <p>preferably dedicated to the Teleworker Solution, but see also Port-forwarding Firewalls.</p>
<p><b>DMZ: 1 Static Address</b> (Address of the MSL <i>after</i> DMZ network address translation)</p>	<p>This address is allocated from the customer's DMZ network range, typically a private (RFC1918) address.</p>

## Significant Firewall Characteristics

- The firewall must have at least three physical interfaces:
  - Internal network
  - External network/Internet
  - DMZ
- The Teleworker Solution is provided by an MSL server installed in the customer's existing DMZ. In this configuration, the MSL must be installed in "server-only" mode.
- The corporate firewall provides static network address translation between an externally visible address and the DMZ address of the MSL.
- The MSL must have a static IP address visible from the external network (Internet). This should be a separate address from the external IP address of the firewall, although some firewalls that support port forwarding may allow sharing the address. It is vital that this address actually be static as any change of the address will cause remote sets to lose connectivity.
- The TCP and UDP port numbers used on the external address of the firewall must be preserved when the packets are passed to the MSL on the DMZ.
- Details of the protocols that must be configured in the firewall are provided in [Firewall Configuration](#). Particular attention should be paid to the requirement that all UDP ports >= 1024 on the LAN be permitted to reach the **public** IP of the Teleworker server.
- Failure to configure the firewall properly will result in audio problems (typically one-way audio).

## Known Issues

We have seen issues with Checkpoint NG firewalls and their use of the “Smart Connection Re-use” feature. It is apparently enabled by default, and can cause issues with a set behind it attempting to reconnect to a Teleworker server. The firewall has no knowledge of the current state of the connection endpoints, but attempts to determine that state by mangling the connection attempt of the set through the firewall. This feature should be disabled.

## Port-forwarding Firewalls

The configuration of a Teleworker server through the use of a port-forwarding firewall (where the external address of the firewall is shared between the Teleworker Solution and other applications) is **supported in version 3.0 and higher for firewall devices with 3 interfaces only**. This allows you to have a single external IP address assigned to your firewall. It does not eliminate the need for a separate DMZ network. When configuring the Teleworker Solution for this type of firewall environment, follow all the guidelines for a normal DMZ deployment with the exception that the Teleworker’s publicly-visible IP address will be the same as the firewall’s publicly-visible address (that is, the single public IP address is shared).

Firewalls (and other types of devices) with only two ports are **not supported**. While these firewalls may be able to simulate a DMZ for a simple service such as a web server, they are unable to provide the true DMZ environment required for the Teleworker Solution. The Teleworker Solution requires the coordination of multiple simultaneous connections, which cannot be achieved with simple port-forwarding.

Some two-port firewalls (for example, the SonicWall SOHO2) will allow the firewall to have multiple external IP addresses, but perform port forwarding to simulate a DMZ. These firewalls are not supported.

## Firewall Configuration

The information in this section is provided to allow configuration of a customer's firewall for the Teleworker Solution in DMZ deployment. **This configuration is automatic in the “Teleworker server as the gateway” deployment.** In all cases below, “server” refers to the Teleworker Solution server (that is, the MSL server).

The Direction column in the table below requires some explanation. The direction of the arrow indicates permission to initiate new traffic in that direction. These rules assume a stateful firewall that will permit return traffic on an existing established connection.

**Table 11. Protocols and Ports used by the Teleworker Solution**

Port Range	Direction	Purpose & Details
TCP 22 (SSH)	Server → Internet	<b>AMC communications.</b> Allow outbound packets (and replies) on TCP port 22 between the Teleworker Server and the Internet to enable server registration, software and license key downloads, alerts and reporting.
UDP 53 (DNS)	Server → Internet	<b>Domain Name System.</b> The server requires DNS to look up the IP address of the Mitel AMC. Alternatively, the server can be configured to forward all DNS requests to another DNS server. See the <i>MSL Installation and Administration Guide</i> for details.
TCP 443 (HTTPS)	Server ← Internet	<b>Remote Server Management.</b> (Optional) Allow inbound and outbound packets on TCP port 443 between the Teleworker Server and the Internet to allow remote management of the server, if required.  HTTPS access to the manager on the external interface must be also be explicitly enabled from the server manager interface.
TCP 443 (HTTPS)	Server ← LAN	<b>Local Server Management.</b> Allow inbound and outbound packets on TCP port 443 between the Teleworker Server and the LAN to allow for management of the server.  HTTPS access to the manager on the external interface must be also be explicitly enabled from the server manager interface.  <b>The firewall should be configured to limit HTTPS access to desired management hosts.</b>
TCP 6800, 6801 and 6802	Server → LAN Server → ICP(s)	<b>MiNet Call Control.</b> Allow incoming and outgoing packets for TCP ports 6801 (MiNet-SSL) and 6802 (MiNet-Secure V1) between the server and the Internet. Allow incoming and outgoing packets for TCP ports 6800 (unencrypted MiNet), 6801 and 6802 between the server and the LAN and the server and the ICP(s).  The LAN rule can be omitted if there are no IP sets on the LAN, but ensure that the ICP(s) can communicate with the server's <b>public</b> address.
TCP 6801 and 6802	Server ← Internet	
TCP 3998 and 6880	Server ← Internet	<b>SAC Connection Support.</b> Allow incoming TCP on ports 3998 and 6880 to support the applications and the web browsing, respectively, on the 5235, 5330, 5340 and Navigator sets, from the Internet to the Teleworker server. There is an additional LAN rule that follows this to complete the support.
TCP 3998, 3999 and 6880	Server → ICP(s)	<b>SAC Connection Support.</b> Allow bi-directional TCP traffic on port 3999 to the ICP(s). This is to support the applications on the 5235, 5330, 5340 and Navigator sets.  <b>Note:</b> 3998 and 6880 are dependent on an additional, internal Teleworker server that the Internet-facing server is daisy-chained to.

Port Range	Direction	Purpose & Details
TCP 80	Server → LAN Server → Internet	<b>SAC Connection Support (Optional).</b> Allow TCP port 80 from the server to the internet, and to the LAN, to support web browsing on the 5235, 5330, 5340 and Navigator sets. Also required to the Internet to allow browsing of the Internet from the set.
UDP 20,000 to configured upper bound* (SRTP)	Server ← Internet Server ← LAN	<b>Voice Communications.</b> Allow incoming SRTP on UDP ports 20000 – configured upper bound* from all streaming devices on the LAN and the Internet. Mis-configuration here is a common cause of one-way audio problems.
UDP 1024 to 65,535 (RTP)	Server → LAN Server → Internet	<b>Voice Communications.</b> Allow outgoing SRTP on UDP ports greater than, or equal to, 1024 from the server to all streaming devices on the LAN and the Internet. Mis-configuration here is a common cause of one-way audio problems.
TCP 3300 (VFA)	Server ← Internet Server ↔ LAN	<b>Optional VoiceFirst Communications.</b> Allow bi-directional traffic on TCP port 3300 if you have a VoiceFirst Solution installed.
TCP 2114	Server ↔ LAN Server ← Internet	<b>Your Assistant Support.</b> To permit the YA client to connect to the logon server on the LAN side, this port must be permitted. Failure to do so will result in the client being unable to logon via their YA client.
TCP 2116	Server ↔ LAN Server ← Internet	<b>Your Assistant Support.</b> To permit the YA client to connect to the telephony server on the LAN side, this port must be permitted. Failure to do so will result in the client being unable to control their set via the Mitel ICP.
TCP 35000	Server ↔ LAN Server ← Internet	<b>Your Assistant Support.</b> To permit the YA client to connect to the presence server on the LAN side, this port must be permitted. Failure to do so will result in the presence features in YA failing to function.
TCP 37000	Server ↔ LAN Server ← Internet	<b>Your Assistant Support.</b> To permit the YA client to connect to the collaboration server on the LAN side, this port must be permitted. Failure to do so will result in the collaboration features in YA failing to function.

\* Configured upper bound is controlled by a setting in the Advanced panel. You must reserve four ports per set that you wish to support. Thus, to support 1000 sets, 4000 ports are required, from 20000 to 24000, and those ports must be open in the firewall configuration of any firewall that the Teleworker server is installed behind.

## Performance Guidelines

These numbers indicate the absolute minimum requirements, and using the maximum number of users on a low-end server will result in difficulties in administration via the web interface.

### Teleworker

Device Type	Maximum number of Teleworker Phones	Simultaneous Calls WITH Transcoding
5560 IPT	500	Because of the CPU-intensive nature of G.729a transcoding, a 1.8 GHz server that supports 1000 (see Note) simultaneous users with transcoding disabled, may only support 24 simultaneous users with transcoding enabled (See <a href="#">Table 2</a> on page 5)
All other sets	1000	

### Teleworker Deployed on APC

Device Type	Maximum number of Teleworker Phones	Simultaneous Calls WITHOUT Transcoding	Simultaneous Calls WITH Transcoding
5560 IPT	20	15	2
All other sets	40	30	4

## Glossary

Acronym	Description
<b>APC</b>	Application Processor Card
<b>ATM</b>	Asynchronous Transfer Mode
<b>DHCP</b>	Dynamic Host Configuration Protocol ( <a href="#">RFC 1541</a> – Oct'93)
<b>DMZ</b>	De-Militarized Zone – A portion of a LAN, which is behind a firewall but has elements that are exposed to the internet.
<b>DSL</b>	Digital Subscriber Loop
<b>E2T</b>	Ethernet to TDM – a system component that provides a gateway function for voice samples, between the packet domain (Ethernet) and TDM domain
<b>G.711</b>	ITU-T codec audio standard, specifying an audio signal with a 3.4 KHz bandwidth (ordinary analog voice signal) over an A-law and $\mu$ -law digitized, linear PCM at 64Kbps. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs.
<b>G.729</b>	This ITU-T standard describes CELP compression where voice is coded into 8-Kbps streams. The two variations of this standard (G.729A and G.729A Annex A) differ mainly in computational complexity; both provide speech quality similar to 32-Kbps ADPCM.
<b>ICP</b>	Integrated Communications Platform
<b>IETF</b>	The official specification documents of the Internet Protocol suite are defined by the Internet Engineering Task Force ( <a href="#">IETF</a> ) and the Internet Engineering Steering Group ( <a href="#">IESG</a> ). These specifications are recorded and published as standards track RFCs. As a result, the RFC publication process plays an important role in the <a href="#">Internet standards process</a> . RFCs must first be published as <a href="#">Internet Drafts</a> .
<b>IP</b>	Internet Protocol ( <a href="#">RFC 1122</a> Section 3.)
<b>IPSec</b>	Internet Protocol Security
<b>ISP</b>	Internet Service Provider
<b>MiNet</b>	Mitel Network Layer Protocol – A layer 2 protocol used to transport messages between the PBX and all Mitel DNIC phones
<b>NAT</b>	Network Address Translation - a technique for translating one set of IP addresses, often private, to another set, often public ( <a href="#">RFC 1631</a> – May'94)
<b>PPPoE</b>	Point to Point Protocol over Ethernet
<b>PPPoA</b>	Point to Point Protocol over ATM
<b>PPTP</b>	Point-to-Point Tunneling Protocol ( <a href="#">PDF Spec</a> )
<b>QoS</b>	Quality of Service
<b>RTP</b>	Real Time Protocol ( <a href="#">RFC 1889</a> )
<b>SRTP</b>	Secure Real Time Protocol (IETF Proposed Standard: <a href="http://www.ietf.org/rfc/rfc3711.txt">http://www.ietf.org/rfc/rfc3711.txt</a> – Apr 04)
<b>SSL</b>	Secure Socket Layer
<b>TCP</b>	Transmission Control Protocol ( <a href="#">RFC 1122</a> Section 4.1)

<b>TFTP</b>	Trivial File Transfer Protocol ( <a href="#">RFC 783</a> ). A simple file transfer protocol (no password protection or user directory services) that uses UDP to transfer files across a network
<b>UDP</b>	User Datagram Protocol ( <a href="#">RFC 1122</a> Section 4.1)
<b>UI</b>	User Interface
<b>VoIP</b>	Voice over Internet Protocol
<b>VPN</b>	Virtual Private Network

## Appendix A – Supported Routers

While the remote IP Phone should work behind most routers/Internet gateways, supported router/Internet gateways include:

Manufacturer	Model	Minimum Software Version	Notes
Mitel	MAS/MSL	MAS 7.0 MSL 8.0	Refer to <a href="http://www.mitel.com/DocController?documentId=9787">http://www.mitel.com/DocController?documentId=9787</a> Note: Minimum software version 7.0
D-Link	DI-604	2.10	Refer to <a href="http://support.dlink.com/downloads/">http://support.dlink.com/downloads/</a>
	DI-614	2.10	
	DI-704	2.57b3	
	DI-524 "Air Plus G" wireless	5.0	
Netgear	MR314	3.29	Refer to <a href="http://www.netgear.com/support/main.asp">http://www.netgear.com/support/main.asp</a>
	RP614	4.11RC24	
Linksys	WRTG54GS	1.05.0	Refer to <a href="http://www.linksys.com/download/">http://www.linksys.com/download/</a>
	BEFSR41v2	2.25.2	

**NOTE:** Any supported router should be upgraded to its latest firmware/OS load before deployment.