



# **Security and the Mitel Networks 6010 Teleworker Solution**

---

White Paper

Release 1

March 2003

## Table of Contents

<b>INTRODUCTION .....</b>	<b>1</b>
<b>SOLUTION ARCHITECTURE .....</b>	<b>2</b>
<b>VOICE NETWORKING .....</b>	<b>5</b>
RTP .....	6
SECURE RTP .....	6
CAST-128 .....	7
MAC ADDRESS RESTRICTION.....	7
RESOURCES.....	8
<b>DATA SECURITY .....</b>	<b>9</b>
BACKGROUND ON PPTP .....	9
RESOURCES.....	10



## **Introduction**

The Mitel Networks 6010 Teleworker Solution enables remote workers to connect securely and conveniently to the corporate voice and data network.

This document provides an overview of the solution architecture and describes the protocols used to ensure the confidentiality of voice and data communications.

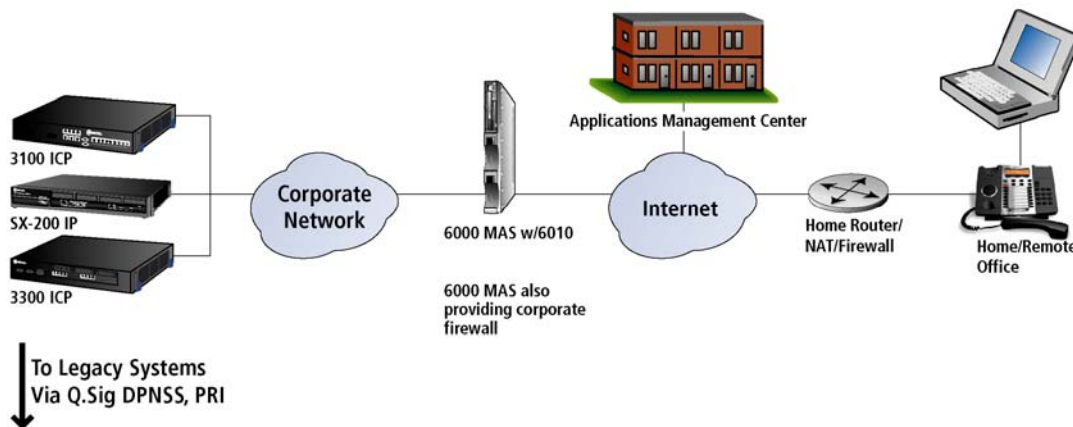
## Solution Architecture

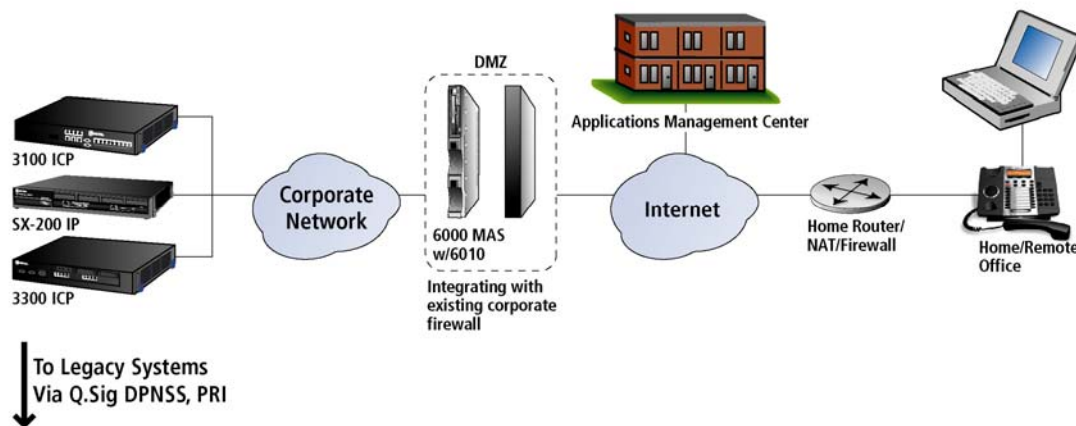
The 6010 Teleworker Solution is one in a series of applications developed for the Mitel Networks 6000 Managed Application Server (MAS) and designed to take advantage of that platform's simplicity, security and reliability. The specific purpose of the 6010 Teleworker Solution is to support remote connections to any network employing Mitel Networks' proprietary MiNET signaling protocol for Voice-over-IP. In practice, this means any network using the Mitel Networks 3100 or 3300 Integrated Communications Platform or the IP Node for the SX-200 PBX.

The 6010 Teleworker Solution consists of two elements. The first is an application (or "software blade") that is downloaded to the on-premises 6000 MAS from the Mitel Networks Applications Management Center (AMC). Once installed and configured, the application allows the 6000 MAS to function as a proxy for remote phones requiring access to the corporate voice network. The solution offers several features that are designed both to improve voice quality over the Internet and to reduce bandwidth requirements between the corporate office and remote locations.

The second element of the solution is the remote set. This is a standard, dual-port Mitel Networks 5020 or 5220 IP Phone that is configured to operate in teleworker mode.

The following diagrams illustrate the two supported deployment options:





In the first, the 6010 Teleworker Solution server is configured to function as the corporate firewall and gateway. This is a typical scenario in a small business setting and allows the customer to take advantage of the built-in firewalling capabilities of the 6000 MAS. (For more information on these capabilities, please refer to the document titled “Security and the Mitel Networks 6000 Managed Application Server.”) The second option is intended for situations where there is an existing corporate firewall. If this is the case, the 6010 Teleworker Solution server can be installed in the corporate DMZ.

As illustrated above, the recommended configuration at the remote location is to plug the Internet connection into a standard cable/DSL router capable of providing Network Address Translation (NAT) and DHCP. The phone is then connected to the router and the teleworker’s PC is connected to the second port on the back of the phone. Note that when the PC accesses the Internet via the phone, the phone does not interfere in any way with the data stream. The phone does, however, provide prioritization of the voice packets, ensuring better voice quality with minimal or no impact to the data connection.

Installation of the 6010 Teleworker Solution is simple and is typically accomplished in less than 45 minutes. The technician begins by loading the 6000 MAS software, which includes the Linux operating system, on a standard Intel-compatible computer. Installation is fully automatic and requires no Linux knowledge. Next, the technician logs into the Mitel Networks Applications Management Center (<https://www.mitel-amc.com/>), registers the server and purchases the 6010 Teleworker Solution product. Finally, the installer accesses the server’s web-based management interface (the “server manager”), enters the service account ID number assigned to this machine by the AMC, and downloads the 6010 Teleworker Solution software blade.

To configure the blade, the technician clicks on “6010 Teleworker Solution” in the server manager and enters the following settings:

- 6010 Teleworker Solution Status: set to “enabled”.
- Mitel Networks ICP Address: specifies the IP address of the ICP that will accept connections from remote IP sets.
- Enable G.729 transcoding: If the ICP provides support for G.729a transcoding, this option should be left at “no” (the default setting). Otherwise, it can be set to “yes” to reduce bandwidth requirements.

## Configure 6010 Teleworker Solution

The options below will configure your 6010 Teleworker Solution.

6010 Teleworker Solution Status

Enter the address of the Mitel Networks Integrated Communications Platform (3100/3300 ICP or SX-200 with IP Node) supported by this 6010 Teleworker Solution. If you are not sure of this address, contact your local administrator.

Mitel Networks ICP address:

Choose whether you wish to support G.729 transcoding from the teleworker sets. This is a form of compression that will reduce the amount of bandwidth used during calls. If the selected Mitel Networks ICP supports G.729 directly, you should disable this option.

Enable G.729 transcoding?

The following information is captured from the 6010 Teleworker Solution log files on the SME server. Here you can find the status of the 6010 Teleworker Solution application itself.

Log Information Connection Attempts: 0  
Active Connections: 0

To configure the IP Phone, the administrator powers up the set, holds down the “7” key and, when prompted, enters the Internet-routable IP address of the 6010 Teleworker Solution server. This information is stored by the phone in NVRAM (Non-Volatile Random Access Memory).

At this point, the phone can be taken off-site and plugged into any broadband Internet connection via a cable/DSL router, as described above. When powered up, the phone will first obtain a local IP address from the cable/DSL router and then download its software from the 6010 Teleworker Solution server at the corporate office. When the download completes (generally in less than a minute), the phone again connects to the 6010 Teleworker Solution server and the server in turn connects to the Mitel Networks ICP whose address was entered on the blade web panel. Under normal circumstances, this entire process is automatic and requires no special configuration at the remote location.

## Voice Networking

To ensure the confidentiality of communications, all voice packets passed between the remote IP phone and the 6010 Teleworker Solution server are encrypted using the Secure Real-time Transport Protocol, a security profile for RTP.

### ***RTP***

The Real-Time Transport Protocol (RTP) is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data such as voice or video. Originally specified in an Internet Engineering Task Force (IETF) Request for Comments (RFC1889), RTP is commonly used in Internet telephony applications. RTP does not in itself guarantee real-time delivery of multimedia data, since this is dependent on network characteristics. It does, however, provide tools to help manage the data as it arrives to best effect. (For example, an application can be configured to drop voice packets that are seriously delayed since audio dropouts tend to be less disruptive to human perception than echo or delay.)

### ***Secure RTP***

Secure RTP is a security profile for RTP that adds confidentiality, message authentication and replay protection to that protocol. Specifically, Secure RTP defines a set of default cryptographic transforms and allows new transforms to be introduced in the future.

The security benefits of Secure RTP include:

- confidentiality of the RTP payloads, as well as protection against replayed packets.
- low bandwidth cost, i.e., a framework preserving RTP header compression efficiency, and limited packet expansion
- low computational cost,
- high tolerance to packet loss and re-ordering, and robustness to transmission bit-errors in the encrypted payload.

Secure RTP is ideal for protecting Voice-over-IP traffic because it can be used in conjunction with header compression and has no effect on IP Quality of Service. These attributes provide significant advantages, especially for voice traffic using low-bitrate voice codecs such as G.729.

## **CAST-128**

Secure RTP allows for the fast encryption of a voice stream using one of a number of encryption algorithms. The specific algorithm used by the Mitel Networks 6010 Teleworker Solution to encrypt both the voice stream and MiNET signaling is the CAST-128 algorithm, documented in RFC2144.

Belonging to the class of encryption algorithms known as Feistel ciphers, CAST-128 is operationally similar to the Data Encryption Standard (DES) but uses a newer, larger key size. In a Feistel cipher, the input is broken into two blocks of equal size, generally called left and right, which are then repeatedly cycled through the algorithm. At each cycle, a hash function is applied to the right block and a randomly generated key, and the result of the hash is XOR-ed into the left block (using the Boolean algebra function Exclusive-OR). The blocks are then swapped. The XOR-ed result becomes the new right block and the unaltered right block becomes the left block. The process is then repeated a number of times (rounds). Exclusive-OR encryption requires that both the encryptor and the decryptor have access to the encryption key, but the encryption algorithm, while extremely simple, is also extremely secure.

The CAST-128 encryption algorithm is designed to use a key size that can vary from 40 bits to a maximum of 128 bits. The longer the encryption key, the more difficult it is to decrypt the file. (Every bit added to the length of the key doubles the number of tries that would be required to break the encryption through brute force.) The 6010 Teleworker Solution uses the most secure method of CAST-128 encryption, with 16 rounds and a 128-bit key (also known as CAST5-128). Using a computer capable of one million calculations per second, it would take roughly 12 days to crack a 40-bit encrypted message by brute force but  $10^{25}$  years to crack a message encrypted with a 128-bit key.

## **MAC Address Restriction**

In addition to protecting the confidentiality of the voice stream and the MiNET signaling, the 6010 Teleworker Solution is designed to prevent unauthorized remote phone users from gaining access to corporate voice resources. This is accomplished by restricting access to specified Mitel Networks 5020 or 5220 IP Phones, based on a unique identifier sent by the phone to the 6010 Teleworker Solution server in a MiNET control message. That unique identifier is the MAC (Media Access Control) address of the phone.

The first time a 5020 or 5220 phone attempts to send a registration message to the 6010 Teleworker Solution, its MAC address is automatically logged and entered into a table that is displayed on the solution's web interface. By default, the phone is *disabled* and therefore will not be able to connect to the ICP. To allow access, the administrator must set the phone's entry to *enabled* by placing a check mark in the box next to the MAC address and clicking the "Update" button. It is also possible to enable specific phones by manually adding their MAC addresses to the table. Each phone's MAC address is printed on a label on the back of the set.

For convenience, the table also allows a description to be entered for each phone. If the entry is added through the automatic registration process, the default description is the IP address of the phone.

## Configure 6010 Teleworker Solution

### Operation status report

The new 6010 Teleworker Solution settings have been saved.

This page will permit you to configure the list of sets that are permitted to access your 6010 Teleworker Solution. This is done via the MAC address of the sets in question, configured below.

Use the following two fields if you wish to add a MAC address to the list manually. Click on the "Update" button below when done.

MAC Address  Phone Description

Alternatively, you can simply choose from the following table of addresses, which contains the MAC addresses of any remote sets that have attempted to connect, or are currently connected. Click on the "Update" button below when done.

Enabled	MAC Address	Phone Description
<input checked="" type="checkbox"/>	08:00:0f:00:89:32	Bill Smith ext 1025
<input checked="" type="checkbox"/>	08:00:0f:0e:68:f0	Jill Jones ext 2130
<input checked="" type="checkbox"/>	08:00:0f:0e:84:58	John Smith ext 3356
<input type="checkbox"/>	08:00:0f:0e:9c:3a	65.103.40.171:6900

### Resources

Secure Real-time Transport Protocol

<http://www.ietf.org/internet-drafts/draft-ietf-avt-srtp-05.txt>

RFC 2144: The CAST-128 Encryption Algorithm

<http://www.ietf.org/rfc/rfc2144.txt>

## **Data Security**

The 6010 Teleworker Solution offers several options for customers requiring a secure data connection between the remote site and the corporate office.

If the customer has an existing Virtual Private Network using IPSEC or any other encryption protocol, the 6010 Teleworker Solution can co-exist with that service. These VPN solutions may involve on-premise equipment (such as "VPN appliances") or use software installed on a desktop or laptop. In either scenario, the 6010 Teleworker Solution provides a secure voice connection while the existing equipment continues to secure the data connection.

For customers that do not have an existing VPN solution, the 6010 Teleworker Solution supports two options:

1. Using the Mitel Networks ServiceLink suite of services, the 6010 Teleworker Solution at the corporate office can be linked to a system at the remote office running the Mitel Networks 6000 Managed Application Server software in a secure IPSEC VPN. This extends the corporate network into each of the remote offices and allows for the full access of network resources by systems in the remote offices. The Mitel Networks IPSEC VPN offering includes the use of 3DES encryption and manages the exchange of IPSEC keys through the interaction of each 6010 and 6000 server with the Mitel Networks Applications Management Center (AMC). The AMC acts as a trusted broker and provides a reliable mechanism for the secure exchange of IPSEC keys between servers.
2. For offices that wish only to enable access for specific remote desktop or laptop PCs, the 6010 Teleworker Solution includes full native support for the high-encryption version of the Virtual Private Networking software included with every version of Microsoft Windows since Windows 98 (a free add-on is available for Windows 95). This software is based on the Point-to-Point Tunneling Protocol (PPTP) which was developed by a consortium of vendors led by Microsoft.

### ***Background on PPTP***

In its earliest implementation, PPTP used an authentication protocol called MS-CHAP which was found to be insecure. Microsoft corrected the deficiencies and released a new authentication protocol called MS-CHAPV2. MS-CHAPV2 operates as an encrypted mutual authentication handshake. No passwords, in either clear text or encrypted form, are passed during authentication setup.

In addition to these measures, the 6010 Teleworker Solution requires both 128-bit and stateless encryption for PPTP. These address known security issues with the original PPTP protocol release, which included:

- Clear text/encrypted password exchange during authentication
- Clear text passwords on the server
- 40-bit encryption
- Encryption state carried between packets

In summary, therefore, the 6010 Teleworker Solution will not allow connections from PPTP clients that do not support all of:

- MS-CHAPV2
- Encrypted passwords on the server
- 128-bit encryption
- Stateless encryption

There have been no reported issues with the security of PPTP when configured in this fashion.

### ***Resources***

Point-to-Point Tunneling Protocol FAQ

<http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp>

RFC 2637 - Point-to-Point Tunneling Protocol (PPTP)

<http://www.ietf.org/rfc/rfc2637.txt>

Security Architecture for the Internet Protocol (IPSEC)

<http://www.ietf.org/rfc/rfc2401.txt>

