SAMSUNG

Enterprise IP Solutions

OfficeServ SIP Trunks

OS Software Version 4.82

(ED 01)

Introduction – PLEASE READ THIS FIRST

Welcome to the Samsung SIP Trunking manual for releases 4.6x through to 4.82. A great deal of time has gone into trying to make the information in this guide as accurate as possible, and it is mostly correct. However, some features and settings are not well documented by Samsung and their operation can unexpectedly change between patch releases; as well as the occasional appearance of "undocumented features". So if you do discover something in the manual that you feel is untrue, or find some information that we might want to include in the next edition, please send it to the guys (yes, they are all guys) at techsupport@samcom.com.au. We appreciate good feedback.

And please remember: *Although SIP is complex, programming SIP trunks in the OfficeServ isn't*. In most cases the examples at the end of the manual will get you through an install. For more complicated scenarios you can do the following: read this manual, look for additional guides on our Partner Resource Center, contact tech support. At least one of these options should get you through tricky installs.

Another worthwhile suggestion from tech support: Wireshark can save you lots of time in resolving problems. We frequently get cries for help from technicians that have spent hours on site with non-functioning SIP trunks trying to guess what is wrong; where a simple Wireshark trace could have shown them what is wrong and quickly identify the issue. A couple of hours learning Wireshark and obtaining a small LAN switch with port mirroring (the Netgear GS110TP is good) can save you from wasting lots of time, and ultimately money, at the customer site.

OfficeServ software versions

This document is based on OfficeServ software version 4.82. Many key features, such as multiple carriers, enhanced codec control, and encrypted voice, were introduced into the OfficeServ by version 4.6 and later versions. These new features are described in the following section.

SIP trunk Features in version 4.6 and 4.8

Multiple SIP provider support

As SIP trunks have become more advanced in their delivery and stability, more and more customers are using SIP as either a direct replacement for, or supplementary service to traditional analogue and ISDN services. OfficeServ V4.6 delivers the ability to simultaneously use up to four SIP providers on one OfficeServ system. The system can then be programmed to route outbound calls via each SIP provider based on the usual auto route selection criteria per call – traditionally based on cost, distance and end user extension number account details. The system can even be programmed to use alternative SIP providers as fail-over or backup routes for other providers whether they are ISDN, analogue or SIP.

Enhance MGI resources management

When the OfficeServ 7000 IP PBX series was launched, any VoIP media was controlled by the MGI (Media Gateway Interface) module and its associated channels. The MGI allows for IP devices to communicate to non-IP devices, such as TDM trunks or handsets.

V4.40 OfficeServ software delivered a new service called MPS (Media Proxy Server), which allowed IP devices to talk to IP devices without using an MGI channel. Note: MGI resources are always used to connect IP endpoints to non-IP devices. An MGI resource was also required to supply RINGBACK tone, even for IP to IP communications. MGI channels were also required to deliver music-on-hold during an IP to IP call.

Version 4.6 improves MGI allocation by providing additional resources, called RTG channels, to provide ring back tone, hold tone and music on hold. *Note: RTG channels do not pass externally sourced Music on Hold to callers; they only provide the system based tones.*

This reduces the number of MGI channels required, and in many situations decreases system cost by reducing the number of OAS/MGI64 cards and MGI licenses needed. There is 1 RTG channel in the system for every MPS channel. For example: The OAS card provides 32 RTG channels and the OS7100 has 8 inbuilt RTG channels.

Specify how many SIP Trunks can be used per ISP or SIP Peering

In prior versions of software all licensed SIP trunks were seen as one large pool for both carrier and peering calls. It was not possible to determine how many trunks could be reserved for the different route types. In version 4.6 the ability to specify the maximum number of SIP calls for SIP Peering and each SIP carrier was added.

Separation of SIP Provider trunk calls from SIP Peer trunk calls

In addition to the segregation of inbound SIP Carrier traffic, version 4.6 also enhances system Trunk Groups by adding a field to SIP Trunk Groups that determines which SIP Carrier can use the Trunk Group or if it is used for SIP Peering. This ensures a greater level of control over SIP trunks for outbound calls and call accounting by assigning which specific trunks are used for which service.

Voice Band Data (VBD) support for Fax-over-IP (FoIP)

Many of the error correction techniques used in VoIP processing are designed to ensure that voice data sounds as good as possible. As VoIP usage is increasing, more and more fax machines are being connected to SIP lines and becoming subject to these same error correction techniques. This can have a negative effect to fax transmissions. With version 4.6 it is now possible for MGIs to use the Voice Band Data (VBD) protocol. The VBD protocol disables NLP and jitter buffer processing to ensure that data transmissions (like fax or modem data) are not distorted.

Outgoing Caller ID blocking for SIP Trunks

With version 4.6 software it is now possible to block outgoing Caller ID on SIP Carrier or SIP Peering. When CLI privacy is required the OfficeServ adds a privacy request to the SIP messages for the outgoing call.

The option is also provided to allow blocking of the OfficeServ 7000 Series system host ID as well. When Caller ID is disabled the SIP Carrier or SIP Peer will receive a CID packet in the form of *<anonymous@[OfficeServ Public IP Address]>.* If the host ID is hidden as well the CID packet sent will show *<anonymous@anonymous.invalid>*.

NOTE: Some SIP Providers do not support hiding the host ID. Check with your SIP Carrier before enabling host ID masking.

Tandem trunking for SIP Peers

Tandem trunking is the ability for incoming calls on the SIP Peer trunks to be connected to an outgoing SIP Carrier or SIP Peer trunk. Prior to version 4.6 it was not possible to disable tandem trunking with SIP Peer trunks. Version 4.6 changes this by adding an option to enable or disable tandem trunking.

SIP Trunk Error Alarm

A new series of alarm indications have been added to version 4.6 relating to SIP Trunks. Any time a SIP trunk registers or loses registration it will now be logged in the system, as will any resource or allocation errors relating to SIP Trunks.
In version 4.7 the alarm indication feature was improved to show more detailed information for each alarm and not to send multiple alarms for a single fault.

Specify how the system should respond to unknown SIP traffic

Prior to version 4.6 the only way to ignore SIP traffic from unknown sources was to send a reject message. This lets a hacker know that the system exists and can lead to an increase in hacker traffic. In version 4.6 it is now possible to determine exactly how the system should respond to incoming SIP traffic from unknown sources. The new options are **No Response**, meaning that the system simply ignores the traffic as if it had not been detected. **Response**, which means that the system will send a SIP reject message.

Specify codec used for SIP Trunks

Version 4.6 adds the ability to specify the audio codec used for SIP conversations. Different codecs can be chosen for each SIP Carrier and each SIP Peer. Additionally there are four codec priority levels that can be set so that if the desired codec cannot be used the next lower priority codec will be automatically attempted.

Encrypted Voice

Version 4.6 delivers support for Secure RTP (sRTP) audio streams. sRTP is an encryption protocol developed specifically for VoIP audio streams and prevents hackers from reconstructing audio; even if the hacker has gained access to the network and captured the speech packets.

Transport Layer Security

V4.6 OfficeServ delivers SIP trunks and SIP extensions that are connected to the OS7200 and OS7400 to be secured by a data network industry - standard protocol called TLS. Transport Layer Security is a cryptography standard developed to secure company data networks from attacks.

Multiple DNS Option

Some features in the OfficeServ require it to be able to resolve URLs to IP addresses – and that means that the OfficeServ must have access to at least one Domain Name Server (DNS). There are several locations within the OfficeServ in which to program the IP addresses of Domain Name Servers – there is the *System I/O Parameters* page, and there are the *SIP Carrier Options* pages. The DNS IP addresses programmed in the *System I/O Parameters page* are used by features system wide, and that includes SIP trunks. However, some SIP carriers provide domain name servers that are specifically provided for any SIP trunks connected to their service, so these DNS IP addresses need to be put into in the *SIP Carrier Options* page set up for that carrier.

Since there are two places to configure the DNS server addresses in the OfficeServ it has option to choose which of the DNS addresses to use for the SIP trunk feature. The OfficeServ can be set to either only use the DNS IP addresses in the *System I/O Parameters* page, or to use those DNS IP addresses as well as the DNS IP addresses set in the ISP programming pages.

Overview of SIP

SIP is the acronym for Session Initiation Protocol. SIP was developed by the Internet community and is described in RFC 3261 + many others. It is used to set up interactive communication sessions over data networks: these sessions can be phone calls, video calls, transactions for instant messaging, interactive games, and so on.

SIP trunks are used by the OfficeServ to communicate with SIP carriers and SIP capable phone systems. SIP trunks have a feature set that is similar to other trunks found in the phone system – SIP station features are not available for SIP trunks.

Explanations of some of the terms used in this document

Outgoing calls: These calls are made from the OfficeServ through the SIP trunks to the SIP carrier.

Incoming calls: Incoming calls are sent from the SIP carrier through the SIP trunks to the OfficeServ.

Enterprise Indial: The term "Enterprise indial" is the name for the feature that gives the customer a range of indial numbers – without having multiple SIP accounts. Most carriers support this feature and they may give it a different name.

Registration: Registration is used by SIP devices to tell a SIP registration server (also known as a *Registrar*) where to find the equipment using that particular account. The OfficeServ *SIP trunks* in carrier mode send account registration messages to the registrar server to tell it where it should send incoming calls. If the OfficeServ cannot successfully register with the carrier it assumes that the carrier is un-contactable and does not use the trunk group for outgoing calls. *(*There is an exception to this rule. See No-Registration mode in the examples for details)*

In most cases, successful registration requires that the device attempting to register has the correct username and password for the account.

The carrier's registrar is usually at the same address as their proxy server. So the registrar address is normally left out of the SIP trunk programming in the OfficeServ.

Registration - *Representative* and *Individual* mode: The OfficeServ has two ways of performing registration – *Representative* and *Individual* mode. *Representative* mode is used when there is only a single account on the SIP carrier's network. *Individual* mode is used when the OfficeServ has multiple accounts on the SIP carrier's network.

Authorization: SIP carriers use account authorization to verify that SIP messages received from a SIP device are from the genuine holder of the SIP account, and not from a third party pretending to own that account.

Peer mode: The main purpose of Peer mode is to provide trunks between SIP capable telephone systems. SIP registration is not supported by SIP peering trunks and the IP addresses of remote systems are programmed in a dedicated table.

CLI presentation: The Calling Line ID of the station making a call is sent to the phone receiving the call. The CLI presented to the called phone can be either the SIP account number or a number from the *Enterprise Indial* range associated with the account.

CLI blocking: When CLI blocking is enforced on a call the SIP carrier does not pass the CLI to the called phone. On outgoing calls the OfficeServ can be configured to either, not send the CLI to the carrier, or request the carrier to not send the CLI to the ultimate destination of the call.

DTMF sending: There are two standard methods for sending DTMF tones through SIP trunks: *RFC2833 Inband* and *SIP INFO*. Most carriers use the *RFC2833 Inband* method.

Codec usage: Voice traffic must be encoded using a codec that both the SIP carrier and the OfficeServ can interpret. Most SIP carriers use either G.711 or G.729. G.711 gives better voice quality, but uses about 90Kbps per call. G.729 uses less bandwidth (30Kbps per call), but reduces voice quality.

Some SIP carriers support G.722, G.723 and other codecs. However, for interoperability reasons it is best not to use those codecs; unless you are confident that they will work in all call scenarios.

T.38 Fax: Faxes sent over IP networks are especially prone to transcription errors and call drop-offs; and they *cannot* be sent using the G.729 codec. T.38 is a protocol that was developed to improve the chances of a fax successfully transiting an IP network. And it allows faxes to be sent through a network using G.729 for voice. T.38 is able to carry fax and modem signals because it contains functions that allow it to check for errors and compensate for packet loss and jitter.

G.711 is an uncompressed codec that can pass fax traffic. However, for faxes to be successful it is important that the network has very little delay, jitter and packet loss.

VBD: Many of the error correction techniques used in VoIP processing are designed to ensure that voice sounds as good as possible, but they can have a negative effect on fax signalling. Since Fax machines are making calls through SIP lines they are becoming subject to these error correction techniques. From version 4.6 it is possible to use Voice Band Data (VBD) processing for faxes. VBD processing disables NLP (Non-Linear Processing) and Jitter Buffer processing to ensure that data transmissions, like fax or modem signals, are not distorted.

SIP Carrier operation and SIP Peering operation

There are two modes of operation of SIP trunks in the OfficeServ: SIP carrier mode and SIP peering mode.

Up to four separate SIP carriers are can be configured in the OfficeServ; they are designated ISP1 through to ISP4.

The key characteristics of carrier and peer mode are:

SIP carrier mode

- Designed for trunks that link to a SIP carrier.
- Can send SIP registration requests to the SIP carrier.
- Can use DNS servers to resolve a proxy URL to an IP address
- Can detect when the SIP carrier cannot be contacted and disables the trunks
- Permits call re-routing when the SIP carrier does not respond to call attempts

SIP peering mode

- Designed for SIP trunks that link to other SIP capable PBXs.
- Does not use SIP registration.
- Does not use DNS or URLs to find IP addresses of peer systems.
- Can check if a peer is available and will stop sending calls to non-responding IP addresses.
- Cannot re-route if the peer system is unavailable

Using a Single SIP account and Multiple SIP accounts

The OfficeServ must use *SIP Carrier* mode when it needs to send registration messages to a SIP carrier. Up to four ISPs (one per SIP Carrier) can be programmed in the OfficeServ, and each ISP can support single *or* multiple SIP accounts.

When a single account is used with a carrier its ISP entry should be set to *Representative* mode. When multiple SIP accounts are used with a carrier its ISP entry must be set to *Individual* mode.

These modes determine how the OfficeServ responds to requests for authorization from the carrier. In *Representative* mode a single username and password is programmed in the **SIP Carrier Options** ISP page (DM item 5.2.13) and is used for all authorization responses. In *Individual* mode the usernames and passwords are programmed in the **SIP User** tables (DM item 5.2.14) and they provide the details for the authorization responses.

In *SIP peering* mode registration messages are not sent, but outgoing calls may still need to be authorized by the SIP carrier

Individual mode operation

In *individual* mode multiple SIP accounts are setup for a carrier and the OfficeServ performs registration for every account. The SIP account details are configured in **SIP User** tables (DM item 5.2.14) and each **SIP User** table is linked to the SIP Carrier page with the same number. For example, SIP User table 1 provides the accounts for SIP Carrier 1 in **SIP Carrier Options** (DM item 5.2.13).

In *individual* mode the CLI used for an outgoing call must match a *User Name* in the **SIP User** table and the password linked to that *User Name* is used for authorization. *A call will not be made if the CLI does not match a user name in the SIP User table.*

Note: The CLI for an outgoing call can be obtained from either the **Send CLI Number** table (DM Menu 2.4.3) or the *CO number* field in the **Trunk Data** table (DM Menu: 2.6.1). A station's *Send CLI number* takes priority over a trunk's *CO number*.

Representative mode operation

In *representative* mode only one SIP account is used for each ISP. The OfficeServ uses this account for all authorization interactions with that ISP, regardless of the CLI.

Note: Some SIP carriers cannot authorize SIP calls if the CLI is different from the username of the account. In these cases the CLI of the outgoing call must be the same as the username of the account.

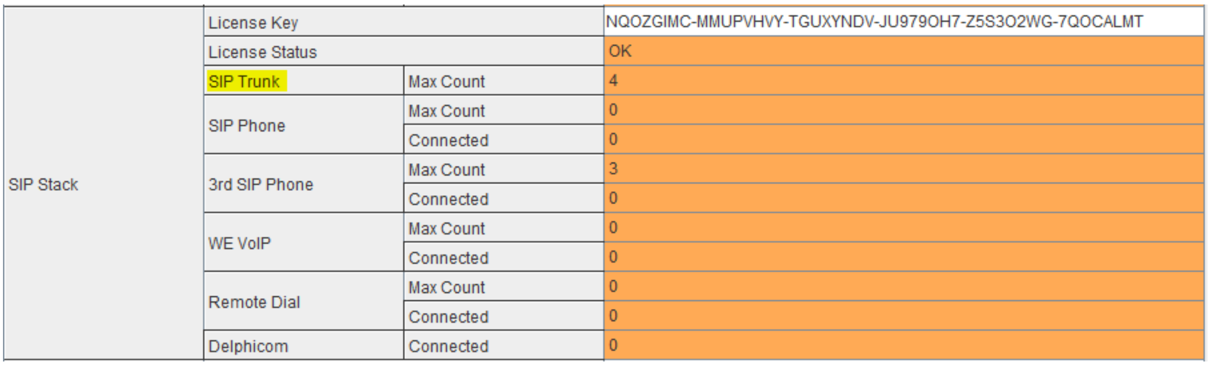
Detailed descriptions of SIP trunking commands and parameters

SIP License

The SIP trunks will not function unless a valid SIP license key has been entered.

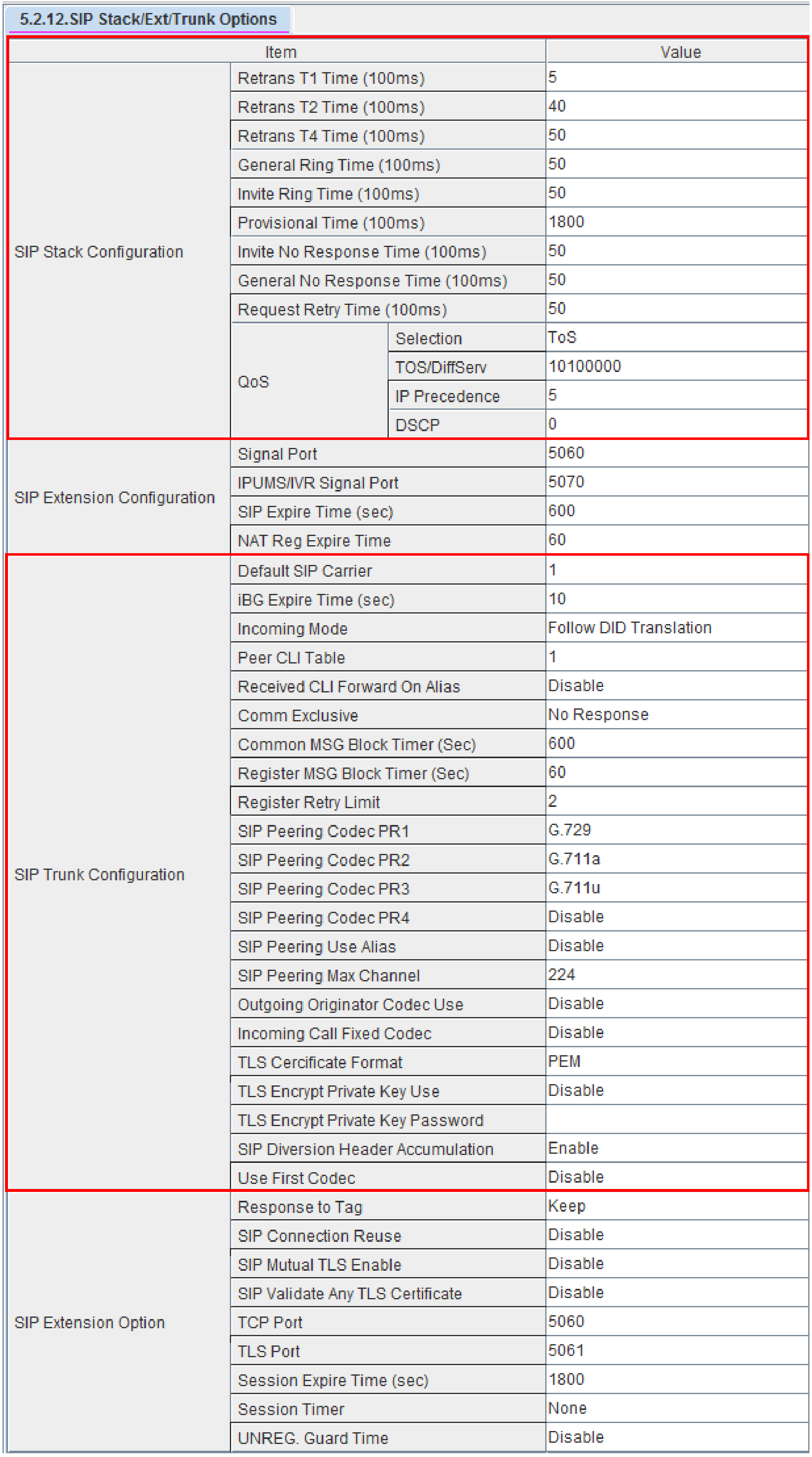
The license screen displayed below is taken from an OS7200 and shows that a valid license key has been entered and that four SIP trunks are available.

The License Key screen (DM item 2.1.4)



SIP Stack	License Key		NQOZGIMC-MMUPVHVY-TGUXYNDV-JU979OH7-Z5S3O2WG-7QOCALMT
	License Status		OK
	SIP Trunk	Max Count	4
	SIP Phone	Max Count	0
		Connected	0
	3rd SIP Phone	Max Count	3
		Connected	0
	WE VoIP	Max Count	0
		Connected	0
	Remote Dial	Max Count	0
		Connected	0
	Delphicom	Connected	0

SIP Stack/Ext/Trunk Options (DM Menu 5.2.12)



Item			Value
SIP Stack Configuration	Retrans T1 Time (100ms)		5
	Retrans T2 Time (100ms)		40
	Retrans T4 Time (100ms)		50
	General Ring Time (100ms)		50
	Invite Ring Time (100ms)		50
	Provisional Time (100ms)		1800
	Invite No Response Time (100ms)		50
	General No Response Time (100ms)		50
	Request Retry Time (100ms)		50
	QoS	Selection	ToS
		TOS/DiffServ	10100000
		IP Precedence	5
		DSCP	0
SIP Extension Configuration	Signal Port		5060
	IPUMS/IVR Signal Port		5070
	SIP Expire Time (sec)		600
	NAT Reg Expire Time		60
SIP Trunk Configuration	Default SIP Carrier		1
	iBG Expire Time (sec)		10
	Incoming Mode		Follow DID Translation
	Peer CLI Table		1
	Received CLI Forward On Alias		Disable
	Comm Exclusive		No Response
	Common MSG Block Timer (Sec)		600
	Register MSG Block Timer (Sec)		60
	Register Retry Limit		2
	SIP Peering Codec PR1		G.729
	SIP Peering Codec PR2		G.711a
	SIP Peering Codec PR3		G.711u
	SIP Peering Codec PR4		Disable
	SIP Peering Use Alias		Disable
	SIP Peering Max Channel		224
	Outgoing Originator Codec Use		Disable
	Incoming Call Fixed Codec		Disable
	TLS Cercificate Format		PEM
	TLS Encrypt Private Key Use		Disable
	TLS Encrypt Private Key Password		
	SIP Diversion Header Accumulation		Enable
	Use First Codec		Disable
SIP Extension Option	Response to Tag		Keep
	SIP Connection Reuse		Disable
	SIP Mutual TLS Enable		Disable
	SIP Validate Any TLS Certificate		Disable
	TCP Port		5060
	TLS Port		5061
	Session Expire Time (sec)		1800
	Session Timer		None
	UNREG. Guard Time		Disable

SIP Stack Configuration

The SIP timers in this section are set to values recommended in the SIP RFCs. They should not be changed from their default values. *The Samsung SIP engineers have given the following explanation for each timer.*

Retrans T1 Time (100mS): The initial re-transmission time if there is no answer, based on the RFC2543 specification.

Retrans T2 Time (100mS): The maximum re-transmission time if there is no answer, based on the RFC2543 specification.

Retrans T4 Time (100mS): The time the User Agent Server waits after receiving the ACK message. It is based on the RFC2543 specification.

General Ring Time (100mS): The server retransmits the response for this length of time until the requested retransmission is received. For example, the wait time after sending 200 OK for INFO.

Invite Ring Time (100mS): After the client sends ACK for the INVITE Final Response, the client cannot confirm if the server received the ACK message. The client waits for this length of time after sending ACK for the Final Response.
Provisional Time (1800mS): After receiving the Provisional Response, the User Agent waits for this length of time until Timeout ends.

INVITE No Response Time (100mS): Before sending CANCEL for the INVITE Request, the User Agent waits for this length of time.

General No Response Time (100mS): Before sending CANCEL for General Request, the User Agent waits for this length of time.

Request Retry Time (100mS): After sending General Request, the User Agent waits for the Final Response for this length of time.

QoS

In every IP packet there is an 8 bit “Type of Service” field that can be used to designate the priority of the packet. When a congested data link is causing packets to queue up this field may be used by the networking equipment to help it decide what priority each packet should have in relation to other packets.

The network does not have to use the “Type of Service” value; it is up to the network designer to program the network to use this value to help it make decisions about packet priority.

SIP signalling packets may need to receive special treatment in a network, so the OfficeServ can set the bit pattern in this field to any value required by the network designers.

The *Selection* field decides which one of three settings to use to set the ToS byte value. The options are: *ToS/DiffServ*, *IP Precedence* and *DSCP*.

The *ToS*, *IP Precedence* and *DSCP* options are provided because the network designer may define the 8 bit value based on any one of those three methods.

*Note: This setting only affects SIP signalling packets and it is not used to set the 8 bit field in the voice packets. The equivalent setting for voice packets is found in **MGI Options** (DM Menu 5.2.16).*

SIP Trunk Configuration

Default SIP Carrier

This option is not used in 4.6 and later software.

Comm Exclusive

Sets the method the system uses to respond to SIP traffic from unknown sources.

The carrier exclusive feature provides additional security for the OfficeServ system. When it is enabled it rejects incoming call attempts from SIP devices with an unknown source IP address.

- **No Response**, meaning that the system will **ignore** all SIP messages from unknown IP addresses. The OfficeServ system does not send back any response message.

- **Response**, meaning that the system will system will respond with a deny message (403 forbidden) for calls from unknown IP addresses.

Valid SIP traffic comprises SIP messages that come from *known* IP addresses. The system recognises the following IP addresses as valid.

1. Registered SIP Station IP Addresses (DM Menu 6.2.3)
2. VoIP Peering IP Addresses (DM Menu 5.2.17)
3. The ISP IP Addresses (DM Menu 5.2.13) – these are the IP addresses in the *Outbound Proxy* and *Alternative Outbound Proxy fields*. There are four ISPs, so four *Outbound Proxy* addresses can be assigned. The system will reject calls from a carrier if it sends SIP messages from a server with an unlisted IP address. Therefore, it is preferable to put a URL in the “Outbound Proxy” field, because IP addresses obtained from the Domain Name Servers are more likely to be correct.

This feature affects incoming calls in both *Carrier* and *Peer* mode. It has does not affect outgoing calls.

Note: IP addresses can be put in the VoIP Peering table just to prevent the source IP address being blocked, even when they are not needed for outgoing calls.

Common MSG Block Timer (Sec): This timer specifies duration the sending IP address will be blocked. It is applied to all SIP messages, except the REGISTER message.

Register MSG Block Timer (Sec): *This is for SIP Phones.* This timer specifies the duration the sending IP address will be blocked. It is only applied to REGISTER message failures.

Register Retry Limit: *This is for SIP Phones.* This is the number of failed attempts that a SIP phone can make to register with the OfficeServ before being blocked. A failed attempt is generally caused by an incorrect User ID or Password in the REGISTER message.

iBG Expire Time (sec)

The iBG product is not currently available in Australia, so this setting is not used. It should remain at its default value.

Incoming Mode

There are three options for the handling of calls coming in via SIP trunks.

Follow Trunk Ring – Uses the settings in DM Menu item 3.2.1 Trunk Ringing (MMC 406) command to find the destination for incoming calls.

Follow Incoming Digits – Uses the received digits and the *Tel number* field in **Numbering Plan** (DM item 2.8.0) to find the destination for incoming calls.

Follow DID translations – This compares the destination number to the *Incoming Digits* field in **DID Ringing** (DM Menu item 3.2.3) to find the destination for incoming calls. *Be aware that the destination number sent by the SIP carrier may vary depending on the source of the SIP call. Some carriers do not provide the full national number when the source of the call is another user of their SIP services.*

Peer CLI table

This parameter is used for SIP peering only. The *Peer CLI Table* parameter contains the ID number of the CLIP table used for outgoing calls made using the **SIP peering** feature. The CLIP tables are configured in **Send CLI Number** (DM Menu item 2.4.3).

Received CLI Forward on Alias

Incoming trunks (such as ISDN or SIP) can provide the calling line Identification (CLI) number of the calling party for display on the phone receiving the call. If an incoming trunk call is forwarded to an external destination by the OfficeServ the CLI of the calling party can be sent in the outgoing INVITE message. *This feature is described in detail below.*

Operation of Received CLI Forward on Alias

When a station forwards the incoming trunk call to an external destination through the SIP trunks the OfficeServ will put the *station* CLI programmed in **Send CLI Number** (DM Menu item 2.4.3) in the *From:* header in the outgoing SIP INVITE message. This means that the party receiving the call will see the CLI of the OfficeServ station forwarding the call, not the CLI of the original calling party.

The *Received CLI Forward on Alias* feature adds the option to send the CLI of the original calling party as well as the CLI of the forwarding station.

When this option is 'Enabled' the *From:* line in the SIP INVITE message includes the CLI of both the station that forwarded the call and the CLI of the external calling party.

When this option is 'Disabled' the *From:* line only contains the CLI of the station that forwarded the call.

The example below shows a SIP INVITE message sent when the feature is 'Enabled'.

Station 207 is set to forward all calls through the SIP trunks.

The CLI of the calling party is **0398722900** and the CLI of the phone is **207**.

```
From: "0398722900"<SIP:207@192.168.1.230:5060;user=phone;tag=10525f8\r\n
```

SIP Peering Codec PR1 ~ 4

This sets the audio codec prioritisation to use when establishing a SIP Peering call. The codec set in PR1 will be attempted first, and if that codec is not accepted, PR2 will be tried, followed by PR3 and PR4.

SIP Peering Use Alias

When the *SIP Trunking Use Alias* parameter is enabled the contents of the *Send SIP Alias Name* field configured in **Send CLI Number** (DM menu 2.4.3) is added to the front of the caller URI in the From: header in the INVITE message.

For example, when the *Send SIP Alias Name* field name field contains "MyAliasName" and the CLI is 0386828546. The `From:` field in the INVITE message appears as follows.

```
From: "MyAliasName"sip:0386828546@voice.mibroadband.com.au;tag=1c34456
```

SIP Peering Max Channel

This sets the maximum number simultaneous inbound and outbound calls for peering trunks. Call attempts beyond this limit receive a busy signal.

Outgoing Originator Codec Use

When *Outgoing Originator Codec Use* is enabled the OfficeServ will use the codec assigned to the calling phone as the highest priority for outgoing calls. If the call is from an analog or digital phone the MGI codec will be used.

Incoming Call Fixed Codec

When *Incoming Call Fixed Codec* is set to “Disable” the OfficeServ uses the codec preferred by the calling SIP peer system.

When *Incoming Call Fixed Codec* is set to “Enable” the OfficeServ uses the codecs defined in the PR1 to PR4 fields. The codec in PR1 is the preferred option.

TLS Certification Format

Please see the **OfficeServ V4.6x – V4.7x Software Feature Guide** for information about programming the TLS/sRTP feature.

TLS Encrypt Private Key Password

Please see the **OfficeServ V4.6x – V4.7x Software Feature Guide** for information about programming the TLS/sRTP feature.

SIP Diversion Header Accumulation

SIP Carriers may put diversion information in INVITE messages sent to the OfficeServ when the call has already been diverted within the carrier network. If the OfficeServ then re-diverts this call to an external destination it can add its own diversion information to the existing information.

Set the *SIP Diversion Header Accumulation* option to “Enable” to make the OfficeServ add its diversion details to the carrier’s diversion information. Note: The outgoing call with multiple diversion headers may fail if the carrier cannot process multiple diversion records in the INVITE message.

Use First Codec

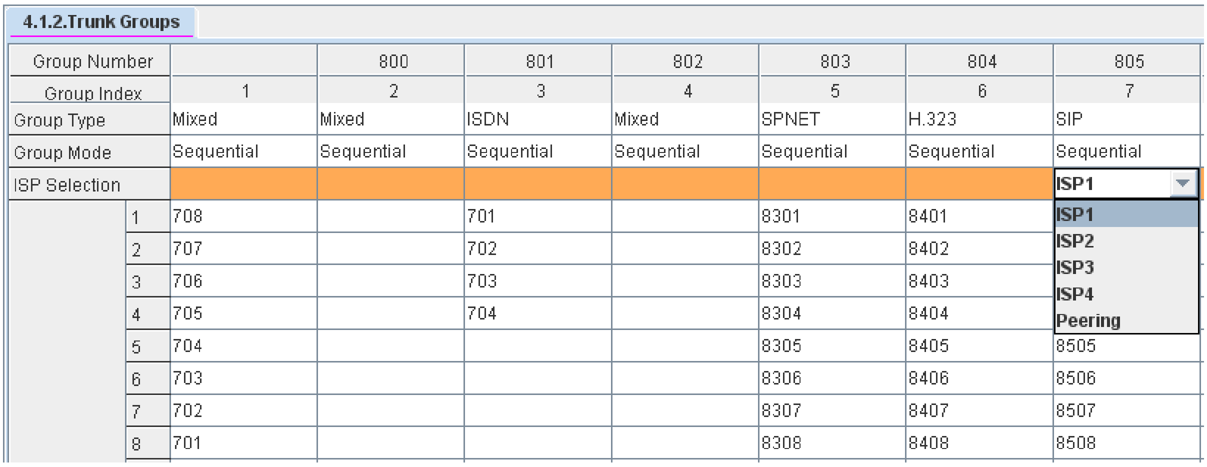
Sometimes a peer system will put multiple codecs in its response to a call setup request from the OfficeServ. The OfficeServ normally expects the peer to choose a single codec from the list it provided in its INVITE message; and therefore it re-sends the INVITE message to try and resolve this problem. If the peer’s response to this re-INVITE also contains multiple codecs the OfficeServ will send yet another INVITE message, and if this cycle continues voice problems can occur.

When the *Use First Codec* feature is enabled the OfficeServ chooses the first codec in the response from the peer and does not resend the INVITE messages.

Set *Use First Codec to “Enable”* if the SIP trunks are having the problem described above.

Trunk Groups

The multiple ISP feature requires that the OfficeServ be able to identify which ISP to use for a call. In **4.1.2 Trunk Groups** there is a field for each group called ***ISP Selection*****;** this setting identifies the ISP to be used for the call. “Peering” is selected if the call is to be sent through the SIP peering trunks. The default SIP trunk group is assigned to ISP 1, but ISP number for the default group can be changed.

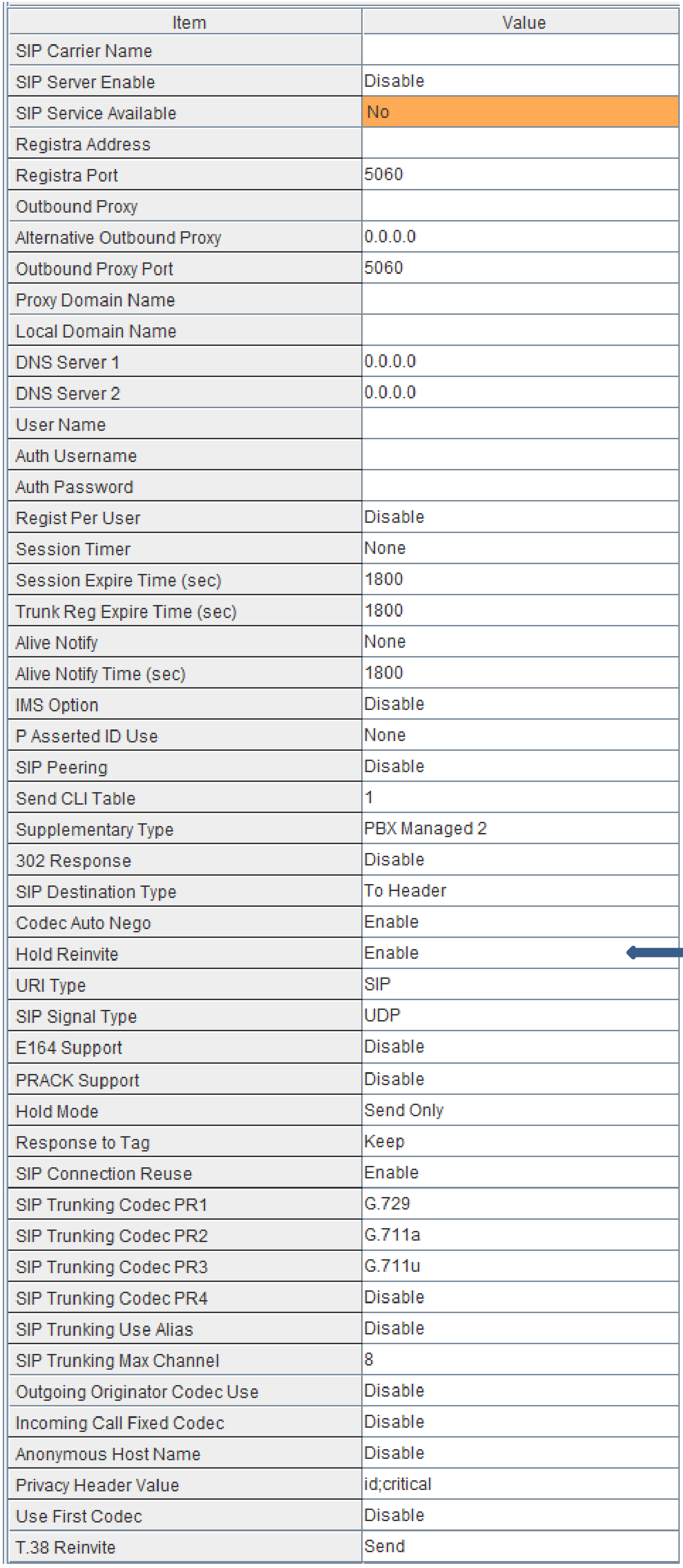


4.1.2.Trunk Groups

Group Number			800	801	802	803	804	805
Group Index		1	2	3	4	5	6	7
Group Type		Mixed	Mixed	ISDN	Mixed	SPNET	H.323	SIP
Group Mode		Sequential	Sequential	Sequential	Sequential	Sequential	Sequential	Sequential
ISP Selection								ISP1
	1	708		701		8301	8401	
	2	707		702		8302	8402	
	3	706		703		8303	8403	
	4	705		704		8304	8404	
	5	704				8305	8405	8505
	6	703				8306	8406	8506
	7	702				8307	8407	8507
	8	701				8308	8408	8508

SIP Carrier Options

The SIP Carrier Option page (DM item 5.2.13)



Item	Value
SIP Carrier Name	
SIP Server Enable	Disable
SIP Service Available	No
Registra Address	
Registra Port	5060
Outbound Proxy	
Alternative Outbound Proxy	0.0.0.0
Outbound Proxy Port	5060
Proxy Domain Name	
Local Domain Name	
DNS Server 1	0.0.0.0
DNS Server 2	0.0.0.0
User Name	
Auth Username	
Auth Password	
Regist Per User	Disable
Session Timer	None
Session Expire Time (sec)	1800
Trunk Reg Expire Time (sec)	1800
Alive Notify	None
Alive Notify Time (sec)	1800
IMS Option	Disable
P Asserted ID Use	None
SIP Peering	Disable
Send CLI Table	1
Supplementary Type	PBX Managed 2
302 Response	Disable
SIP Destination Type	To Header
Codec Auto Nego	Enable
Hold Reinvite	Enable
URI Type	SIP
SIP Signal Type	UDP
E164 Support	Disable
PRACK Support	Disable
Hold Mode	Send Only
Response to Tag	Keep
SIP Connection Reuse	Enable
SIP Trunking Codec PR1	G.729
SIP Trunking Codec PR2	G.711a
SIP Trunking Codec PR3	G.711u
SIP Trunking Codec PR4	Disable
SIP Trunking Use Alias	Disable
SIP Trunking Max Channel	8
Outgoing Originator Codec Use	Disable
Incoming Call Fixed Codec	Disable
Anonymous Host Name	Disable
Privacy Header Value	id;critical
Use First Codec	Disable
T.38 Reinvite	Send

The **HOLD REINVITE** parameter is not shown when *MPS Service* is "ON" in **2.1.5 System Options**

SIP Mutual TLS and **SIP Validate Any TLS Certificate** parameters are not shown in this image because TLS is not available in the OS7030, OS7100 or OS7200S

Use the SIP carrier options page to configure the OfficeServ to communicate with SIP carriers.
Up to four carriers can be configured in the SIP Carrier Options screens: they are labelled ISP1, ISP2, ISP3 and ISP 4. And the default configuration in the OfficeServ uses ISP 1 for all outgoing SIP calls.

SIP Carrier Name

This is a text label that can be used to identify the carrier. It is only provided for display purposes and information is not required in this field.

SIP Server Enable

This parameter determines if this SIP carrier configuration is active. If it is set to disable the carrier configuration in this table is not used.

SIP Service Available

This field shows the SIP trunk registration status of the OfficeServ. “Yes” is displayed when the OfficeServ has successfully registered with the SIP carrier. When this field shows “No” registration has not been successful and it may not be possible to make outgoing calls. The effects of registration on the *SIP Service Available* field in *Representative* and *Individual* mode are described below.

Be aware that when the OfficeServ is not able to register with the SIP carrier the SIP carrier may assume that the OfficeServ is offline. Consequently, it does not send incoming calls to the OfficeServ.

Representative mode. When the OfficeServ is in *representative* mode (*Regist Per User* is ‘Disabled’) the *SIP Service Available* field shows the registration status of the single account programmed in the **SIP Carrier Option** page**.** If *SIP Service Available* is “No” the account has not been registered successfully with the carrier and OfficeServ will not use this ISP for outgoing calls.

The OfficeServ will not attempt registration if the *Username* field in the **SIP Carrier Option page** is empty.

Individual mode. When the OfficeServ is in individual mode (*Regist Per User* is ‘Enabled’) the *SIP Service Available* field shows the status of *all* of SIP accounts programmed in the **SIP Users** table (DM menu 5.2.14) that is linked to that ISP page. All of the SIP accounts must register successfully with the SIP carrier before the *SIP Service Available* field shows “Yes”.

If *any* SIP account fails to register the *SIP Service Available* field shows “No” and SIP accounts that fail to register cannot be used to make outgoing calls. However, outgoing calls can be made using any SIP accounts that were able to register successfully.

Registra address

Some SIP carriers have their SIP registration server on a different IP address to their SIP proxy server. The *Registra Address* parameter (should be "Registrar", but let just live with it) was provided to allow the OfficeServ to register with one address and make outgoing calls to another address.

The *Registra Address* parameter contains the IP address of the SIP carrier's registration server. **In most cases this feature is not required and the *Registra address* field is left blank.**

Note: Even if the Registra Address field contains an invalid address the OfficeServ will still try and use it. Therefore, you should leave the Registra Address field blank when the carrier's SIP registrar address is the same as the Outbound Proxy Server address.

Registra Port

This is the transport layer port number that will be used for registration attempts. The default is 5060 and it should be left at this value, unless the carrier specifies another port number.

Outbound Proxy

The Outbound Proxy address is the destination address for both SIP registration attempts and outgoing calls. It can be a programmed as a URL or an IP address. The *Outbound Proxy* address is only used for registration when the *Registra Address* parameter is blank.

When the *Outbound Proxy* field is in URL format the OfficeServ must use a Domain Name Server (DNS) to resolve the URL address to an IP address. There are two advantages to using URL format. The first is that the SIP trunk provider can change the IP address of their SIP Proxy server without being forced to have their customer's SIP devices re-programmed. The second is that they can configure their DNS information to provide list of backup SIP servers to use if the primary server fails. (This list is called an SRV record.) *Note: Not all SIP trunk providers use SRV records, so the benefits of this feature will vary between SIP carriers.*

In addition, when the *Proxy Domain Name* field is blank the address in the *Outbound Proxy* field is used in the authorization details. In many cases the *Outbound Proxy* address and the *Proxy Domain Name* are the same, so this functionality reduces the complexity of the OfficeServ programming.

Alternative Outbound Proxy

The *Alternate Outbound Proxy* address is used when the outbound proxy server is not contactable.

The OfficeServ tries several times to contact the *Outbound Proxy Server* on the programmed address, or addresses if DNS SRV records are used. If these attempts fail it will try the *Alternative Outbound Proxy.*

Outbound Proxy Port

This is the transport layer port number that will be used for outgoing call attempts. The default is 5060 and it should remain at this value, unless the carrier specifies another port number.

Proxy Domain Name

The proxy domain name is used in SIP registration messages and outgoing calls as part of the authorization name. When this field is empty the value in the 'Outbound Proxy' field is used instead.

Local Domain Name

The OfficeServ uses the *Local Domain Name* instead of the *Proxy Domain Name* in the `From:` header in outbound SIP messages. This modification is required by some overseas SIP carriers that are not using SIP Registration. *It is highly recommended that this field remain blank, unless this specific modification to the SIP messages is requested by the SIP carrier.*

DNS Server 1 and DNS Server 2

A domain name server is required when a URL address is programmed in either the *Outbound Proxy* field or the *Registra Address* field. The domain name server converts the URL to an IP address and may also provide the addresses of backup servers. The ISP providing the broadband link will usually specify DNS server addresses for their broadband service. A DNS server address is not required when the *Outbound Proxy* and the *Registra Address* are both IP addresses.

NOTE: If the *Multi DNS Server* option in **System Options (DM2.1.5)** is "Disabled" the main system DNS IP addresses in the **System I/O Parameters (DM 5.6.1)** page are used instead of these IP addresses.

Username

The username field contains the SIP account name that the OfficeServ uses with the SIP carrier. If the *Auth User* parameter (described below) is blank the *Username* is sent to the SIP carrier when performing authorization in *representative* mode.

- In *representative* mode *(Register per User* is "Disabled"): SIP registration messages are not sent when this parameter is blank.
- In *individual* mode *(Register per User* is "Enabled"): The *Username* parameter is not used.
- The *Username* field supports alphanumeric characters.

Auth Username

Auth User is only required when performing SIP registration in *representative* mode. The SIP trunks will use the *Auth Username* instead of the *Username* in response to any authorization requests from

the SIP carrier. The *Auth Username* feature is provided because the username that is used to *identify* the service is sometimes different to the username used to *authorize* the service.
Important: In most cases the *Username* and *Auth Username* are the same, so the *Auth Username* parameter is not required. Alphanumeric characters can be used in this field.

Auth Password

This is the password used when the SIP carrier feature is configured in *representative* mode (*Register per User* is disabled). When representative mode is used all outgoing calls and registration messages will use this password for authorization.

Register per user

When *Register per User* is set to 'Enable' the SIP registration and authorization features operate in *individual* mode. In individual mode the account numbers and passwords are configured in the **SIP User** t**able (DM item 5.2.14)**. There is one *SIP User table* per carrier and up to 100 accounts can be programmed in each *SIP User table*.

Session Timer

SIP recommendation RFC 4028 describes a method of periodically determining the status of an active SIP session. This feature allows both SIP user agents and proxies to determine whether the SIP session is still active. In most cases it is the SIP carrier that performs this operation and therefore the OfficeServ does not need to use it.

When the OfficeServ is programmed to use this feature it will periodically send UPDATE requests to the SIP carrier during a SIP call. The *Session Timer* parameter has three options: NONE, INVITE and UPDATE.

The session timer interval is specified in the *Session Expire Time* parameter. For more information about how this feature works please read RFC 4028.

It is recommended that the *Session Timer* parameter is set to "None" – unless the SIP carrier specifies that this feature is required.

Session Expire Time (sec)

This parameter is configured in conjunction with the Session Timer feature. Please see the Session Timer description for details on how to use this parameter.

Trunk Registration expire time (sec)

The trunk registration expire timer determines how often SIP registration messages are sent to maintain registration with the SIP carrier. The carrier often changes this value by specifying a new value when acknowledging registration from the OfficeServ. If the carrier does specify a new registration expiry time the value programmed in this field is ignored and the carrier's value is used instead.

Alive Notify

Alive Notify is used to inform the carrier that the OfficeServ SIP trunks are available. It is also used by the OfficeServ to find out if the carrier is available.

When the *Alive Notify* feature is activated the OfficeServ repeatedly sends OPTIONS messages to the SIP carrier. The *Alive Notify Time* field determines how often the OPTIONs messages are sent.

The OfficeServ expects the SIP carrier to respond to the OPTIONS messages, so it also uses this feature to find out if the SIP Carrier's proxy server is contactable. The OfficeServ assumes that the SIP trunks are out of service if there are no responses to its OPTIONS messages.

Other uses of the Alive Notify feature

No Registration mode.

In *no-registration* mode the OfficeServ does not send registration messages to the carrier, since the carrier does not support SIP registration. However, registration is also used by the OfficeServ to determine if the carrier is available, and it blocks the SIP trunks if there are no responses. The *Alive Notify* feature gets around this problem by sending OPTIONs messages instead of registration messages. If the OfficeServ gets a response to the OPTIONs messages it assumes that the carrier is available and unblocks the trunks.

Router NAT table problems

If the SIP re-registration time is longer than the refresh time in a router's Network Address Table (NAT), the router may flush the dynamic port translation it created for the SIP packets. This blocks incoming calls because incoming SIP messages cannot pass from the carrier through the router to the OfficeServ.

The *Alive Notify* feature can be setup to repetitively send SIP packets at a time interval that is shorter than the NAT re-fresh time in the router; this stops the router flushing the NAT table.

Alive Notify Time

The *Alive Notify Time* field sets the time interval between sending SIP OPTIONS messages for the *Alive Notify* feature.

IMS Option

When the *IMS Option* enabled the special SIP headers that are commonly used in an IMS environment are automatically applied. S*et to disabled unless otherwise informed*.

P-Asserted-ID Use

P-Asserted-ID is a feature that adds a header to the INVITE message and it is used to provide addition information about the originator of the SIP call. It is most commonly used when the OfficeServ is connected to a SIP carrier that is providing **Enterprise Indial** trunks. Enterprise Indial trunks use a primary account number with secondary indial numbers. *The operation of this feature is shown below.*

In the example:
Username = "0386828547", *Auth Username* = "0386828546", *Station CLI* = "3211"

Headers from the INVITE messages
P-Asserted-ID Use set to: Primary

```
From: <sip:3211@apollo.engin.com.au:5060;user=phone>;tag=5b21bf0
P-Asserted-Identity: "0386828547" sip:0386828547@apollo.engin.com.au
Authorization: Digest username="0386828546" . . . . .
```

P-Asserted-ID Use set to: Alternate

```
From: <sip:0386828547@apollo.engin.com.au:5060;user=phone>;tag=5ac4170
P-Asserted-Identity: "3211" <sip:3211@apollo.engin.com.au>
Authorization: Digest username="0386828546". . . . . .
```

When *P-Asserted-ID Use* is set to 'Primary' the *From:* header in the outbound message contains the station CLI, and the *P-Asserted-Identity:* header contains the *Username* that is configured in the SIP carrier screen.

When *P-Asserted-ID Use* is set to 'Alternate" the *From:* header in the outbound message contains the *Username* configured in the SIP carrier screen, and the *P-Asserted-Identity:* header contains the station CLI.

In both cases authorisation is performed using the *Auth Username* parameter. When the *Auth Username* field is blank the number in the *Username* is used for authorisation instead.

The *P-Asserted-ID* functionality is fully described in RFC 3325.

SIP Peering

When the *SIP Peering* parameter is enabled, the *From:* header line in the SIP messages contains the *IP address* of the OfficeServ system instead of the URL, or IP address, of the SIP carrier's proxy server. This option is normally disabled.

Send CLI table

In the **Send CLI Number** table (DM Menu 5.2.13) there are four CLI entries for each port. The *Send CLI Table* parameter defines which entry to use for outgoing calls made via this ISP.

Supplementary Type

Supplementary SIP messages are proprietary extensions to the SIP RFCs. The default value ‘PBX Managed 2’ should be used, unless the OfficeServ is connected to a system that supports these extensions.

302 Response

The OfficeServ it is able to send `302 Moved Temporarily` messages to a SIP carrier when the *302 Response* feature is enabled in programming for an ISP.

The `302 Moved Temporarily` message tells the carrier to re-direct a call that was sent to the OfficeServ to a new destination number and clears the call from the OfficeServ trunk group. The benefit of this feature is that SIP trunks and other resources in the OfficeServ are not used for the duration of the forwarded call.

This feature is used when a station registers ‘Call Forward All’ to an external destination via the same SIP trunk group that received the call.

When this feature is *disabled* the OfficeServ will link the incoming and outgoing calls internally. This requires the use of two SIP trunks in the OfficeServ.

WARNING: The SIP carrier must support the ‘302 Moved Temporarily’ message. Call forward All to external will fail if the ‘302 Moved Temporarily’ message is not supported by the carrier. Most carriers DO NOT support this feature, so it is best that it disabled, unless otherwise informed.

SIP Destination Type

In the INVITE SIP message for incoming calls the destination number can be put into either the **Request URI** or the **To:** header lines. This option tells the OfficeServ which header line to look for the destination number. The default value is **To:** and it is normally left as such.

Codec Auto Nego

This option is not used, as the new 4.60 codec control features are now used instead.

Hold Reinvite

The *Hold Reinvite* option is only provided when the MPS feature is disabled in **System Options** (DM 2.1.5). When the MPS feature is disabled the SIP trunks do not have to send *Hold Re-Invite* messages when a call is put on hold. The option to disable *Hold Re-Invite* messages is provided because that message can cause problems with hold tones on some carriers.

The **Hold Mode** option (described later) is used when the MPS feature is enabled or the MPS feature is disabled and *Hold Reinvite* is enabled.

URI type

This feature allows the OfficeServ to use an alternative addressing method in the header lines in the SIP messages. Most carriers do not support the **Tel** URI type, so it should only be changed to **Tel** upon request of the SIP carrier.

SIP Signal Type

UDP is normally used as the transport layer protocol for SIP. This option allows the system to use TCP instead. UDP is the default value and is used unless TCP is required by the SIP carrier.

E.164 Support

When enabled the SIP trunks support the E.164 dialling rules.

PRACK Support

There is a SIP message called **PRACK** (PRovisional ACKnowledgement). This message is used to provide an enhanced level of reliability for the transmission of SIP messages during the setup of a call through a PSTN network.

Not all SIP carriers support PRACK functionality. So it is recommended that it remain at the default value (disabled) unless otherwise advised.

Hold Mode

When a call is put on hold the OfficeServ sends a message to the SIP carrier to indicate that there is a change to the call, this is called a *Hold Re-Invite*.

Hold tones are sent by the OfficeServ when a call is in progress and the user presses hold or transfer. The MPS feature cannot send hold tones, so MGI and RTG ports are used to send the tone. Therefore, the OfficeServ must send a SIP message to the carrier to tell it to change the UDP port number from the MPS range to the MGI or RTG range. And when the call is taken off hold the OfficeServ must do the reverse operation. The SIP message used for this operation is a standard *Invite* message that changes the media address values.

In this *Invite* message there is a field that can be either: ***Send-Only, Receive-Only, or Inactive***. These options are described below.

Send-only and Inactive tell the SIP carrier that it is not necessary to send the RTP traffic stream to the OfficeServ, this is because the OfficeServ is not listening to incoming RTP packets (it is only sending them). Some carriers incorrectly interpret this message as a request for them to send their own hold tone to the other party in the call.

The OfficeServ sends ***send-receive*** to indicate that it is listening to the RTP stream from the SIP carrier.

The *Hold Mode* option chooses whether ***send-only, Inactive*** or ***receive-only*** is used in the *Invite* message.

It is recommended that this parameter be set to SendRecv to ensure that hold tones generated by the OfficeServ are heard by the other party.

Response to Tag

Tags are additional unique code strings appended to TO: headers sent in SIP 18x and 200 OK messages. These messages are sent in response to INVITEs from the carrier and uniquely identify the dialog. Normally, tags are not changed when SIP messages are sent due to a change in an existing call, but there are occasions where the carrier requires that the tag change when media settings change.

The option “Keep” does not change the tag during a call, the option “Change” forces the OfficeServ to renew the tag when SIP messages are sent during a call.

SIP Connection Re-use

This option selects whether TLS certification must happen on every call, or only once during registration. Please see the **OfficeServ V4.6x – V4.7x Software Feature Guide** for information about programming the TLS/sRTP feature.

SIP Mutual TLS(Only in OS7200 and OS7400)

Please see the **OfficeServ V4.6x – V4.7x Software Feature Guide** for information about programming the TLS/sRTP feature.

SIP Validate Any TSL Certificate (Only in OS7200 and OS7400)

Sets whether the system will reject (Disable) or accept (enable) unknown certificates during the TLS handshake process. Please see the **OfficeServ V4.6x – V4.7x Software Feature Guide** for information about programming the TLS/sRTP feature.

SIP Trunking Codec PR1 ~ 4

This sets the audio codec prioritisation to use when establishing a call using this carrier. The codec set in PR1 will be attempted first, and if that codec is not accepted, PR2 will be tried, followed by PR3 and PR4.

SIP Trunking Use Alias

When the *SIP Trunking Use Alias* parameter is enabled the contents of the *Send SIP Alias Name* field configured in **Send CLI Number** (DM menu 2.4.3) is added to the front of the caller URI in the From: header in the INVITE message.

For example, when the *Send SIP Alias Name* field name field contains “MyAliasName” and the CLI is 0386828546. The `From:` field in the INVITE message appears as follows.

```
From: “MyAliasName”sip:0386828546@voice.mibroadband.com.au;tag=1c34456
```

SIP Trunking Max Channel

This sets the maximum number of simultaneous inbound and outbound calls that can be made through this SIP Carrier. Call attempts beyond this limit receive a busy signal.

Outgoing Originator Codec Use

When *Outgoing Originator Codec Use* is enabled the OfficeServ will use the codec assigned to the calling phone as the highest priority for outgoing calls. If the call is from an analog or digital phone the MGI codec will be used.

Incoming Call Fixed Codec

When *Incoming Call Fixed Codec* is set to “Enable” the OfficeServ uses the codecs defined in the PR1 to PR4 fields. The codec in PR1 is the preferred option.

For incoming calls, the source address of the call is matched to an outbound proxy address (obtained by DNS lookup if the proxy address is a URI) to identify which ISP configuration applies to the incoming call, and if there is no matching address, the SIP peering configuration is used.

When this option is set to “Disable” the OfficeServ uses the codec preferred by the calling SIP Carrier.

Anonymous Host Name

This feature is only used when calling line ID blocking is enabled on an outgoing call.

When *Anonymous Host Name* is “Enabled” outbound calls for this SIP Carrier will have an anonymous host name *and* URL, so the Caller ID information sent will be in the form:
`<anonymous@anonymous.invalid>`

When *Anonymous Host Name* is “Disabled” outbound calls for this SIP Carrier will have an anonymous host name, so the Caller ID information will be in the form:
`<anonymous@yoursipcarrier.com.au>`

Privacy Header Value

When CLI privacy is required for an outgoing call the OfficeServ puts a privacy request in the SIP INVITE message. Privacy is requested when CLI is blocked for the call and there are three ways to block CLI:
1) Set *CID Send* in **Station Data (DM 2.5.1)** to “No”.
2) Press a feature button programmed as NOCLIP.
3) Dial the NOCLIP feature access code.

The default value in this field is “id;critical”, and it can be changed if necessary. However, you should not change it unless instructed to do so.

Use First Codec

Sometimes a carrier will put multiple codecs in its response to a call setup request from the OfficeServ. This causes a problem, because the OfficeServ expects the carrier to choose a single codec from the list that it provided in its INVITE message. To try and resolve this issue the OfficeServ sends the INVITE message again. If the carrier continues to put multiple codecs in its responses the OfficeServ will keep sending INVITE messages, and voice problems can occur.

When the *Use First Codec* feature is enabled the OfficeServ chooses the first codec in the response from the carrier and does not resend the INVITE message.

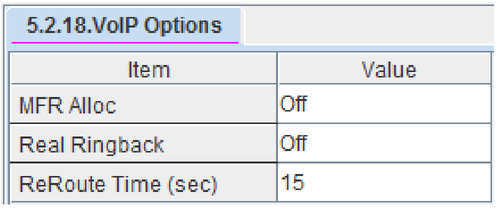
Set *Use First Codec to “Enable”* if the SIP trunks are having the problem described above.

T.38 Reinvite

When a fax is detected on an incoming call the OfficeServ can be configured to either send a re-INVITE to request T.38, or not. In early software the option to use T.38 for fax was applied on a system wide basis. This new option is provided on a per-ISP basis to allow greater flexibility in the OfficeServ.

VoIP Options

There are two parameters in the **VoIP Options** (DM 5.2.18) screen that affect SIP trunk calls.



5.2.18.VoIP Options

Item	Value
MFR Alloc	Off
Real Ringback	Off
ReRoute Time (sec)	15

Real Ringback

During the setup of an outgoing call the SIP carrier sends back SIP messages to indicate the call status. When the call is in the ringing state the SIP carrier can send either `180 RINGING` or `183 SESSION PROGRESS`. The `180 RINGING` message tells the OfficeServ to send local ring tone to the calling station or trunk. The `183 SESSION PROGRESS` message tells the OfficeServ that inband tones are being sent by the carrier, which is usually ring tone, and these tones should be sent to the calling station or trunk.

When *Real Ringback* is "Off" and the OfficeServ receives a `183 SESSION PROGRESS` message, it interprets the message as a request to send locally generated ring tone to the calling party. This may result in the calling party getting the wrong tones, as the SIP carrier may not be sending ring tone in its audio stream. For example: it could be playing a voice message to indicate that the called number is vacant.

When *Real Ringback* is "On" and the OfficeServ receives the 183 SESSION PROGRESS message, the audio sent by the SIP carrier is passed directly through to the calling party.

It is recommended that this setting be changed to "On".

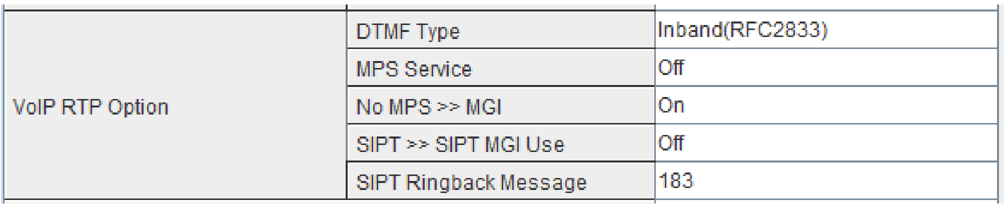
RE-Route Time (sec)

The OfficeServ will try another route if an outgoing call does not get any responses from the SIP carrier before this time expires.

This feature is only available in carrier mode – it does not work in peer mode.

Additional SIP settings

To improve the interoperability of the Samsung SIP trunks with some SIP carriers, call control options have been added in **System Options** (DM menu item 2.1.5) → **VoIP RTP Option**.



VoIP RTP Option	DTMF Type	Inband(RFC2833)
	MPS Service	Off
	No MPS >> MGI	On
	SIPT >> SIPT MGI Use	Off
	SIPT Ringback Message	183

DTMF Type

There are three ways in which DTMF digits can be sent through SIP trunks. **Inband(RFC2833)** is the most commonly used method.

Outband – The DTMF digits are sent in SIP INFO messages. The SIP carrier must be able to understand and process SIP INFO messages and pass these digits on through the network to a device that converts them into DTMF tones. Most SIP carriers do not support Outband DTMF.

Inband(In Voice) – The DTMF digits are sent as tones in voice packets. This works okay with G.711, but G.729 compression adversely affects the tones and makes it difficult for the receiving device to interpret them correctly.

Inband(RFC2833) – RFC 2833 is a protocol that specially encodes DTMF digits before putting them into VoIP packets. Most SIP carriers use this method as it is the most efficient and reliable way of passing DTMF through VoIP links.

MPS Service

When the MPS service is enabled the OfficeServ uses the MPS feature for conversations between SIP trunks and other VoIP endpoints, such as IP Phones.

NOTE: The MPS feature is only used when the two VoIP endpoints are the conversation state. MGI channels are still used during call setup and hold.

No MPS -> MGI

This feature is checked when a VoIP call is made while there are insufficient MPS channels to handle the call. In this situation, when *No MPS -> MGI* option is “On”, the OfficeServ uses MGI channels instead.

SIP-T -> SIP-T MGI Use

When the MPS feature is enabled all SIP trunk to SIP trunk calls will use MPS channels. When the *SIP-T -> SIP-T MGI Use* option is “On”, SIP trunk to SIP trunk calls *do not* use MPS channels and MGI channels are used instead.

The reason that this feature is required is that some SIP carriers lose voice when MPS mode is used for SIP trunk to SIP trunk calls. This problem usually occurs when an incoming SIP trunk call is immediately forwarded back out through the SIP trunks. Therefore, to prevent voice problems on SIP Trunk to SIP trunks calls, the *SIP-T -> SIP-T MGI Use* setting should be “ON”.

SIP-T Ringback Message

After the OfficeServ receives an incoming call and puts it into the ring state it informs the carrier of the status of the call. There are two different SIP messages that can be sent to the carrier when a call is in the ringing state: *183 Session Progress* and *180 Ringing*. When *183 Session Progress* is used, the OfficeServ sends ring tone to the carrier. When *180 Ringing* is used, the carrier generates ring tone to send to the caller.

For carrier compatibility purposes, the OfficeServ SIP trunks can be set to send either message. This setting is system wide and affects all SIP trunk calls for all ISPs.

SIP Peering

SIP peering is used to connect the OfficeServ to other SIP capable phone systems. SIP Peering is a trunk to trunk relationship; it does not support SIP registration or provide station features.

SIP peering uses the **VoIP Peering** page (DM item 5.2.17) to configure the settings for the links to other SIP systems. The addresses in this table are also used by the *Carrier Exclusive* feature to identify the trusted IP addresses of SIP peers.

VoIP Peering (DM item 5.2.17)

There are 250 tables and each table contains the settings for a single destination device, or system.

The settings and fields for each table are*: IP Address, Protocol, Alive Check, User Information, Remote Port, Check Timer, Alive Status, SIP Signalling Type, SIP Response to Tag, VoIP Tandem, SIP Connection Time Out(sec),* and *VoIP Peering Title.*

These settings are described below.

Table number

The SIP peering page can store up to 250 tables. The *Table Number* field in **VoIP Outgoing Digits** (DM item 5.2.3) is linked to this field. The digit plan in **VoIP Outgoing Digits** is used to choose the table number to use for an outgoing call.

IP Address

This is the IP address of the peer system.

Protocol

This parameter is not currently used. Dialling the trunk *Group Number* in **Trunk Groups** (DM 4.1.2) selects the trunk group, and the *Group Type* field chooses the signalling protocol to be used for the call.

Alive Check

When this feature is set to ‘Option’ the OfficeServ periodically sends SIP OPTIONS messages to the peer IP address. If the peer does not respond to the Options message the OfficeServ assumes that it is not able to receive calls, and sets the table *Alive Status* to “*No”.* And when the Alive Status is “No”, calls are not sent to the peer IP address.

When the *Alive Check* option is enabled for a peering table, the OfficeServ will periodically send SIP OPTIONs messages the peer systems to find out if they are responding to SIP OPTIONS messages. If a peer IP address does not respond to the OPTIONS message the OfficeServ will not make calls to that IP address.

User Information

This is an alphanumeric username that is put into the *To:* and *From:* lines in the OPTIONS message. The system only sends OPTIONS messages on peering trunks when there is data entered into this field. It can also use the *User Information* to verify the source of an incoming SIP OPTIONS message. If the OPTIONS message from a peer system does not have matching user information field in the local peer table the OfficeServ may ignore the message or send back an error reply message (depending on the *Comms Exclusive* setting).

Remote port

This is the transport layer port number on which the remote peer expects to receive SIP signalling traffic. SIP traffic is normally sent to port 5060.

Check Timer

When the *Alive Check* feature is enabled, the value in this field determines the interval between sending OPTIONS messages.

Alive Status

This field displays the status of the link. If it is “Yes”, the OfficeServ will try and use the link for calls.

Note: ‘Yes’ is always displayed when *Alive Check* is “None”. And, as a result, the OfficeServ always regards the link as being available for outgoing calls.

SIP Signal Type

Use this parameter to choose the transport mode for SIP signalling. The choices are ‘UDP’ and ‘TCP’. UDP is most commonly used, and is the default setting.

SIP Response to Tag

Tags are additional unique code strings appended to TO: headers sent in SIP 18x and 200 OK messages. These messages are sent in response to INVITEs from the carrier and uniquely identify the dialog. Normally, tags are not changed when SIP messages are sent due to a change in an existing call, but there are occasions where the carrier requires that the tag change when media settings change.

The option “Keep” does not change the tag during a call, the option “Change” forces the OfficeServ to renew the tag when SIP messages are sent during a call.

SIP Connection Reuse

This option selects whether TLS certification must happen on every call, or only once during registration. Please see the **OfficeServ V4.6x – V4.7x Software Feature Guide** for information about programming the TLS/sRTP feature.

VoIP Tandem

This option is provided so that tandem calls between SIP peering trunks can be restricted if necessary. By default, the setting is “Enable” and this allows tandem calls.

SIP Connection Time Out (sec)

This option is only required if SIP Connection Reuse is enabled. This is the expiration time for an established connection. If the remote peer system doesn’t refresh the keep-alive before this time expires the OfficeServ will tear down the reused established connection. The value of this timer should not be less than the “Check Timer” value of the peer system.

VoIP Peering Title

This is a field for putting a description of the peering service. It is for note keeping purposes only and is not used as part of the signalling.

SIP Users

The *SIP User* tables are used for a couple of purposes. The most common purpose is to contain the list of accounts for SIP trunks using *individual* mode, and the other is to contain a list of entries for the conversion of alphanumeric names to numbers.

The *SIP user* tables store the usernames and passwords of SIP accounts used by trunks in *individual* mode. When the *Register per User* feature in **SIP Carrier Options** (DM menu 5.2.13) is enabled for an ISP the system sends SIP registration messages for every entry programmed in the *SIP User* table that is linked to the ISP.

The relationship between the *SIP Carrier* number and the *Table number* is as follows: The **Table** number (shown on the top left of the screen capture below) is linked to the *SIP carrier number* in **SIP Carrier Options** (DM menu 5.2.13). Each *Table* number corresponds to the *SIP Carrier* number. For example: Table 1 is used by SIP carrier 1.

To understand the alphanumeric name conversion feature please read the section on **Incoming Alphanumeric Username** in the **Advanced Features** section of this document.

The SIP User tables (DM item 5.2.14)

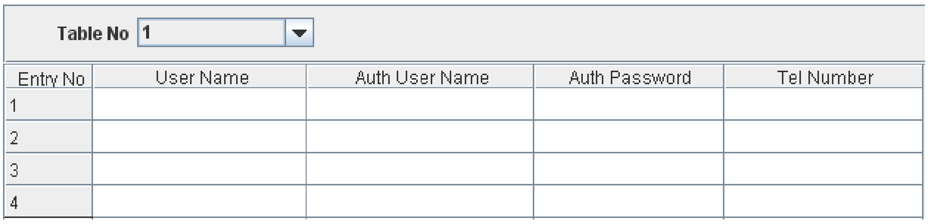


Table No 1

Entry No	User Name	Auth User Name	Auth Password	Tel Number
1				
2				
3				
4				

Entry Number

Up to 100 entries can be made per table.

Username

This is the account username sent to the SIP carrier for authorization. Alphanumeric characters can be used in this field.

Auth User Name

Sometimes the SIP carrier wants an accounts username and its authorization username to be different. The *Auth User Name* parameter allows the account name used for registration to be different to the name used for authorization. When data is entered into the *Auth User Name* field the OfficeServ uses it in the authorization header in the REGISTER messages sent to the SIP proxy. *The User Name is employed for authorization if the Auth User Name parameter is left blank.*

Auth Password

This is the password used for account authorization.

Tel Number

This number is used to match alphanumeric usernames to internal station numbers for incoming calls. To understand this option please read the section on **Incoming Alphanumeric Username** in the **Advanced SIP Features** section of this document.

VoIP outgoing digits table (DM item 5.2.3)

The **VoIP Outgoing digits** table is used by SIP peering to identify which peer table to use for a call. SIP Peering is used if the trunk group selected for the call is configured as “Peering” in *Trunk Group (4.1.2)*.

The dialled digits are checked to see if they that match an entry in the *Access Digit* field – the call fails if a match is not found.

5.2.3 VoIP Outgoing Digits table

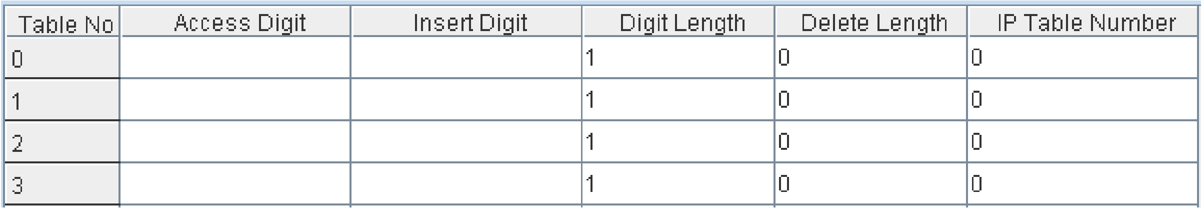


Table No	Access Digit	Insert Digit	Digit Length	Delete Length	IP Table Number
0			1	0	0
1			1	0	0
2			1	0	0
3			1	0	0

Table Number.

There can be up to 250 entries in this table.

Access Digit

These are the first digits of the number dialled by the user after dialling the VoIP trunk access code.

Insert Digits

These digits are added to the front of the dialled number. For example: if the user dials “8722900” and the *Insert digits* value is set to “9” the number sent by the OfficeServ out of the VoIP trunks would be “**9**8722900”.

Digit Length

This field identifies the number of digits that are expected to be received to make up the access code length. This equals the number of digits in the *Access Digit* field.

Delete Length

This is the amount of digits that will be deleted from the start of the dialled number.

IP Table Number

This field identifies which *Table Number* entry to use in **VoIP Peering** (DM item 5.2.17).

Server Use

Not used in 4.60 and later software. This legacy setting was used by earlier software to decide if a call should use carrier or peering mode. The trunk group selection method in the current software makes this decision instead and has made this setting redundant.

Trunk Access code

The default access code for SIP trunks in the OS7100, OS7200 and OS7400 is ‘805’, and in the OS7030 it is ‘802’. SIP trunks do not use overlap sending, so the ‘end of dialling’ code ‘#’must be used to signal end of dialling. LCR can be configured to automatically append the “#” code to a number.

Calling Line ID number

The Calling Line ID is used in a couple of ways.

1. When the SIP trunks are in *individual* mode the CLI number is used to identify which SIP account to use to authorize the call.

2. Some SIP carriers require that the CLI number in the *From:* line in the INVITE message be the same as the SIP account number. Therefore, it *may* be necessary to configure the CLI in the OfficeServ to match the account number when *representative* mode is being used.

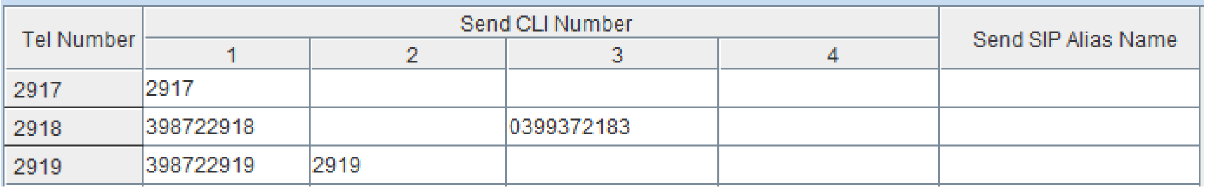
There are two ways to select the CLI for an outgoing call.

CLI Method 1

This method uses the station CLI in the **CLI Send Number** (DM 2.4.3) table. When an outgoing call is made the *Send CLI Table* parameter in the **SIP Carrier Options** (DM 5.2.13) page or the *Peer CLI Table* parameter in the **SIP Stack/Ext/Trunk Options** (DM 5.2.12) page is used to find the source entry of the CLI number.

There are four numbers columns for the CLI numbers; these correspond to the CLI Table number in the **SIP Carrier Options** and **SIP Stack/Ext/Trunk Options** pages.

2.4.3 Send CLI Number



Tel Number	Send CLI Number				Send SIP Alias Name
	1	2	3	4	
2917	2917				
2918	398722918		0399372183		
2919	398722919	2919			

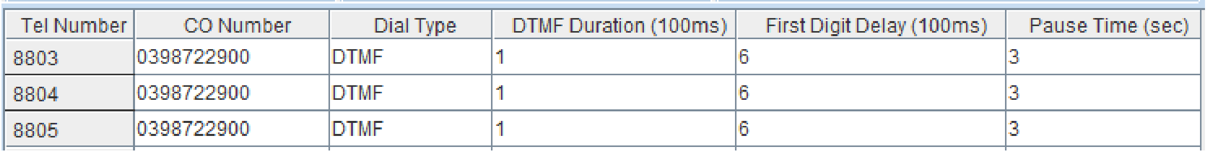
Send SIP Alias Name

This adds a name in front of the CLI in the *From:* line in the SIP INVITE message. This name can only be displayed by SIP phones and it is not used by the system when searching for account information.

CLI Method 2

Another way of sending the CLI is to assign the SIP account number to the SIP trunks in the **Trunk Data** table.

Note: The number allocated to a station in **CLI Send Number** (DM 2.4.3) is used in preference to the *CO number* in the **Trunk data** (DM 2.6.1) table. Therefore, the entry for the station in the **CLI Send Number** table must be blank for this method to work.



Tel Number	CO Number	Dial Type	DTMF Duration (100ms)	First Digit Delay (100ms)	Pause Time (sec)
8803	0398722900	DTMF	1	6	3
8804	0398722900	DTMF	1	6	3
8805	0398722900	DTMF	1	6	3

CLI Blocking (Privacy)

On outgoing calls the OfficeServ can request the carrier to not send the CLI to the called party. This is achieved by either setting the *CID Send* parameter to “No” in **Station Data** (DM Menu Item 2.5.1) or by using the NOCLIP feature, which is configured in the system **Number Plan** (DM Menu Item 2.8.0).

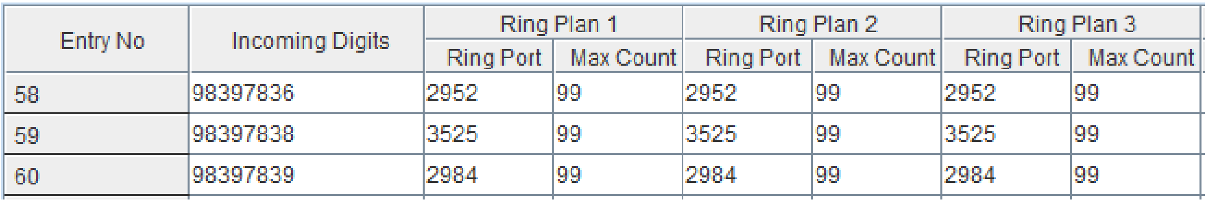
CLI blocking is a feature that needs to be supported by the carrier as well as the OfficeServ SIP trunks. If the carrier does not support this feature the call may fail, or the CLI may still be presented to the called party.

Incoming calls

The method used to decide the destination for incoming calls is defined in **SIP Stack/Ext/Trunk Options** (DM item 5.2.12) → SIP Trunk Configuration → *Incoming Mode*. There are three choices: *Follow trunk Ring*, *Following Incoming Digits*, *Follow DID Translations*.

Follow DID Translations – Use the Incoming calls are directed to the correct station number using the **DID Ringing table** (DM item 3.2.3).

The destination number sent by the SIP carrier must match an entry in this table; otherwise, the call goes to the default destination group.



Entry No	Incoming Digits	Ring Plan 1		Ring Plan 2		Ring Plan 3	
		Ring Port	Max Count	Ring Port	Max Count	Ring Port	Max Count
58	98397836	2952	99	2952	99	2952	99
59	98397838	3525	99	3525	99	3525	99
60	98397839	2984	99	2984	99	2984	99

Follow Trunk Ring – Uses the settings in **Trunk Ringing** (DM item 3.2.1) to find the destination for incoming calls.

Follow Incoming Digits – Uses the received digits and the *Tel number* field in **Numbering Plan** (DM item 2.8.0) to find the destination for incoming calls.

The most commonly used method is **DID Incoming digits**.

Advanced SIP features

Outgoing Alphanumeric Username

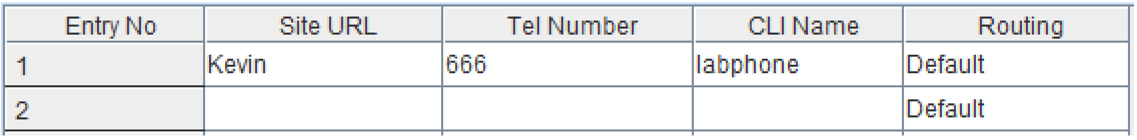
Outgoing calls to alphanumeric destinations have two important characteristics:

1. The destination address contains alpha characters.
2. The CLI may need to contain alpha characters.

Station users can only dial numeric characters, so the OfficeServ must convert the dialled number to an alphanumeric value. And the CLI sent from the OfficeServ may also be alphanumeric, so it must be able to change the CLI to an alphanumeric value.

SIP Destinations

The **SIP Destination** (DM Item 5.2.15) table is used by the alphanumeric username feature to associate dialled numbers to alphanumeric destinations.



Entry No	Site URL	Tel Number	CLI Name	Routing
1	Kevin	666	labphone	Default
2				Default

The **SIP Destination** (DM Item 5.2.15) table

Entry No

Up to 1000 entries can be put into this table.

Site URL

The *Site URL* is the alphanumeric destination address that will be contacted when the user dials the number in the *Tel Number* field. When the dialled digits match the number in the *Tel Number* field the value in *Site URL* is put into the *To:* header in the outgoing SIP INVITE message instead.

Tel Number

The number configured in this field is compared with the dialled digits to find a match.

CLI Name

The *CLI Name* is used for the calling party information when the digits dialled by the user match a number in the *Tel Number* field. The *CLI Name* is also used in the authorization of the call and must match a valid account name or number.

Note: The *CLI Name* is put into the *From:* header in outgoing SIP INVITE messages.

Routing

The *Routing* parameter is not used and should be left as ‘Default’

Incoming Alphanumeric Username

When the OfficeServ receives an incoming call to a destination with an alphanumeric identity it must convert the alphanumeric identity to a station number.

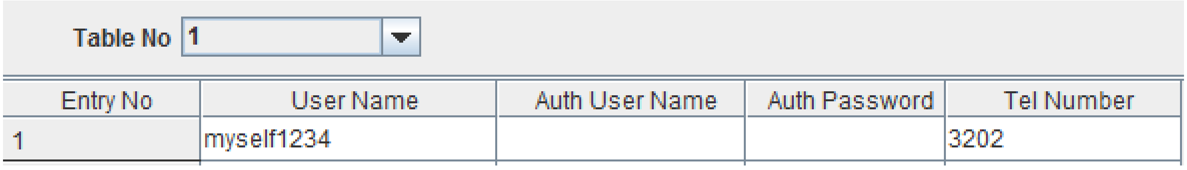


Table No 1

Entry No	User Name	Auth User Name	Auth Password	Tel Number
1	myself1234			3202

The ***SIP User*** (DM Item 5.2.14) table is used to assign an incoming alphanumeric destination name to a number.

The *User Name* field contains the alphanumeric destination name that is converted to the number provided in the *Tel Number* field. After the name has been converted to a number the system uses the indial tables to route the call to the required station.

No Registration Feature

Some carriers do not use SIP Registration and will not respond to registration messages from the OfficeServ. Therefore, the SIP Carrier functionality in the OfficeServ can be configured to not send registration messages.

Registration messages are not sent when the *Username* field in the **SIP Carrier Options** page is blank. However, since registration messages are not being sent, or replied to, the OfficeServ will not know the status of the SIP carrier's proxy server. *If the OfficeServ cannot determine the status of the SIP proxy server it will not send calls to it.*

To solve this problem the OfficeServ has a feature that enables it to find out if the SIP carrier proxy server is available – without using registration messages. This feature sends SIP OPTIONS messages to the SIP proxy server address and detects if there are any replies. If a SIP proxy server replies to the OPTIONS message the OfficeServ assumes that the proxy is available and outgoing calls can be made.

The type of message sent in the reply does not matter: any response is good enough for the OfficeServ. However, if the SIP proxy does not reply to OPTIONS messages the OfficeServ does not send it calls.

The *Alive Notify* parameter in the **SIP Carrier Options** page can be set to either 'None' (which is the default) or 'Options'. OPTIONS messages are sent when it is set to "Options".

The *Alive Notify Timer* parameter determines how often the options messages will be sent, and its default value is 1800 seconds. If a SIP Proxy server does not respond to SIP messages the OfficeServ will send OPTION messages in rapid succession, until it gets a reply. This enables the OfficeServ to recover quickly from network outages.

MGI and OAS card configuration

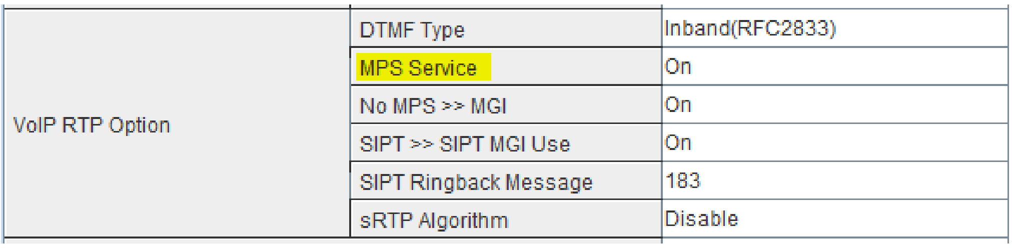
The MPS Feature

The MPS feature allows IP phones and IP trunks to send voice packets to the SIP trunks without using MGI channels.

The MPS feature sends voice traffic between IP endpoints through MPS channels in the OAS card, or built in channels available in the OS7030, OS7100, and OS7200S.

For a detailed explanation of the MPS feature and OAS card, including configuration information, please read the document titled: **The OfficeServ Media Proxy Server feature**. This document can be obtained from the Partner Resource Centre.

The MPS feature is "On" by default in the OS7030, OS7100 and OS7200S systems. The option to enable and disable it is provided in **System Options** (DM Menu item 2.1.5).



VoIP RTP Option	DTMF Type	Inband(RFC2833)
	MPS Service	On
	No MPS >> MGI	On
	SIPT >> SIPT MGI Use	On
	SIPT Ringback Message	183
	sRTP Algorithm	Disable

Like the MGI feature, the MPS feature uses UDP ports to identify the different VoIP traffic streams being received. If the customer's network has routers or firewalls with Network Address Translation (NAT) they will need to configure port/address translations in those devices to enable voice packets to get to the MPS channels.

The default port ranges for the MPS feature are shown below

Hardware	*Start UDP port*	*End UDP port*
OS7030	40000	40031
OS7100	40000	40031
OS7200S	40000	40031
OAS card	40000	40127

By default, the MGI channels on the OAS card start at UDP port 30000.

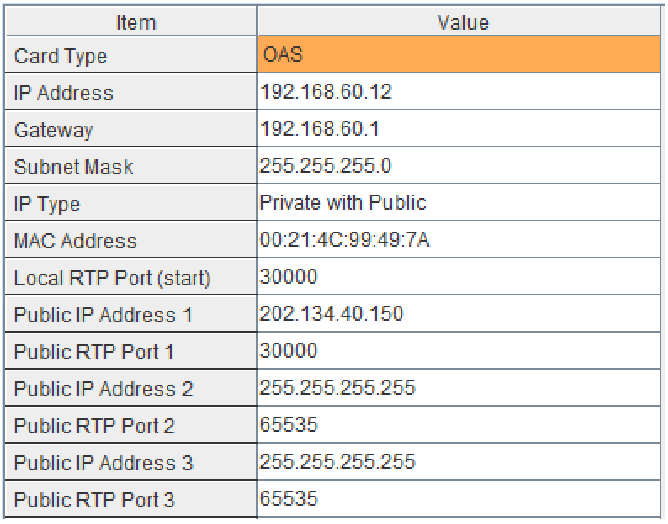
If necessary, the port ranges used by the MPS and MGI channels can be changed. This is explained in the following section: **Multiple Public IP Addresses**.

Multiple Public IP addresses

The OfficeServ has the ability to have multiple public IP addresses and flexible port ranges. The flexible port range feature is used when the NAT/firewall in the customer's network cannot use the default ports; or there are multiple MGI/OAS cards in a system that receive traffic from the Internet. Multiple public addresses are also used in complex network scenarios where the customer wants different public addresses for different VoIP devices.

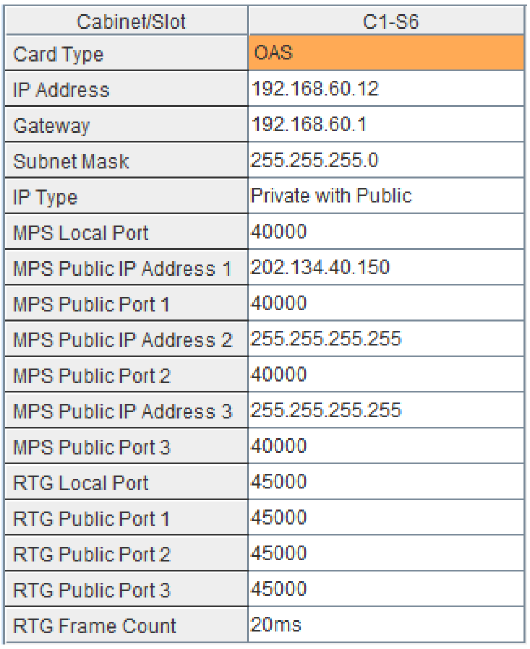
The changes to these parameters are performed in **MGI Card** (DM 2.2.2) and **MPS/RTG Card** (DM 2.2.15).

MGI Card (DM2.2.2) is for setting up the MGI Channels. *Note: The OAS card must be configured in **MPS Card** (DM 2.2.14) to provide MGI channels for them to appear in this table.*



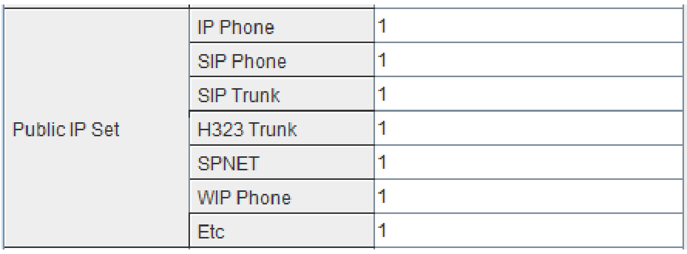
Item	Value
Card Type	OAS
IP Address	192.168.60.12
Gateway	192.168.60.1
Subnet Mask	255.255.255.0
IP Type	Private with Public
MAC Address	00:21:4C:99:49:7A
Local RTP Port (start)	30000
Public IP Address 1	202.134.40.150
Public RTP Port 1	30000
Public IP Address 2	255.255.255.255
Public RTP Port 2	65535
Public IP Address 3	255.255.255.255
Public RTP Port 3	65535

MPS/RTG Card (DM 2.2.15) is for setting up the MPS and RTG channels.



Cabinet/Slot	C1-S6
Card Type	OAS
IP Address	192.168.60.12
Gateway	192.168.60.1
Subnet Mask	255.255.255.0
IP Type	Private with Public
MPS Local Port	40000
MPS Public IP Address 1	202.134.40.150
MPS Public Port 1	40000
MPS Public IP Address 2	255.255.255.255
MPS Public Port 2	40000
MPS Public IP Address 3	255.255.255.255
MPS Public Port 3	40000
RTG Local Port	45000
RTG Public Port 1	45000
RTG Public Port 2	45000
RTG Public Port 3	45000
RTG Frame Count	20ms

The call types are allocated to public addresses and port ranges in **System IP Options** (DM 5.2.10). The fields for public addresses and ports 2 & 3 are only required if the customer wants the traffic for different types of VoIP device to use separate public addresses.



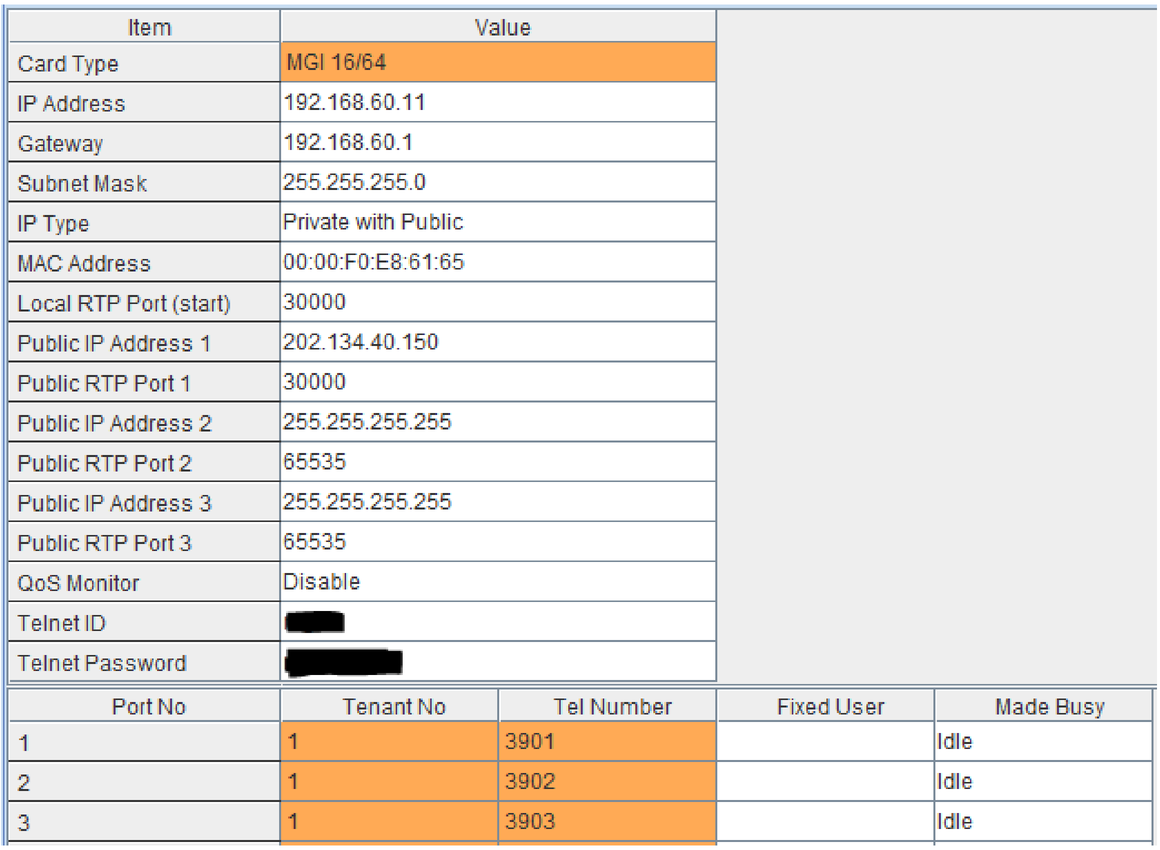
Public IP Set	IP Phone	1
	SIP Phone	1
	SIP Trunk	1
	H323 Trunk	1
	SPNET	1
	WIP Phone	1
	Etc	1

This feature is primarily used when the OfficeServ has multiple IP addresses for its MGI or MPS channels. For example: A twin cabinet OS7030 has MGI channels with two IP addresses – so the RTP port numbers must use different ranges. This is required because NAT tables in routers and firewalls cannot be programmed to forward traffic received on a single public address and port range to multiple IP addresses.

It is recommended that the *Local RTP Port(start)* and the *Public RTP Port 1* both use the same port range, as this makes the programming in the Firewall/NAT easier to implement and troubleshoot.

MGI card network configuration

The MGI card screen (DM 2.2.2)



Item	Value
Card Type	MGI 16/64
IP Address	192.168.60.11
Gateway	192.168.60.1
Subnet Mask	255.255.255.0
IP Type	Private with Public
MAC Address	00:00:F0:E8:61:65
Local RTP Port (start)	30000
Public IP Address 1	202.134.40.150
Public RTP Port 1	30000
Public IP Address 2	255.255.255.255
Public RTP Port 2	65535
Public IP Address 3	255.255.255.255
Public RTP Port 3	65535
QoS Monitor	Disable
Telnet ID	[redacted]
Telnet Password	[redacted]

Port No	Tenant No	Tel Number	Fixed User	Made Busy
1	1	3901		Idle
2	1	3902		Idle
3	1	3903		Idle

This page is used to configure the IP addresses and ports of MGI cards installed in the system. In the OS7030, OS7100 and OS7200S systems the MGI card is attached to the main processor; and in those systems the IP address settings are configured in **System Selection** (DM 2.1.0) and **LAN Parameter** (DM 2.1.2).

The MPS IP address and port settings are configured in the **MPS Card** (DM 2.2.15) page.

Understanding MGI and MPS RTP port ranges

The OfficeServ allows the UDP port numbers of the MGI and MPS channels to be changed from the default values. This may be necessary in networks that use Network Address Translation for incoming traffic.

Local RTP Port (start)

All RTP traffic uses UDP ports. The *Local RTP port* is the first port number in the range that will be used for traffic within the private network.

Public IP Address (1 to 3)

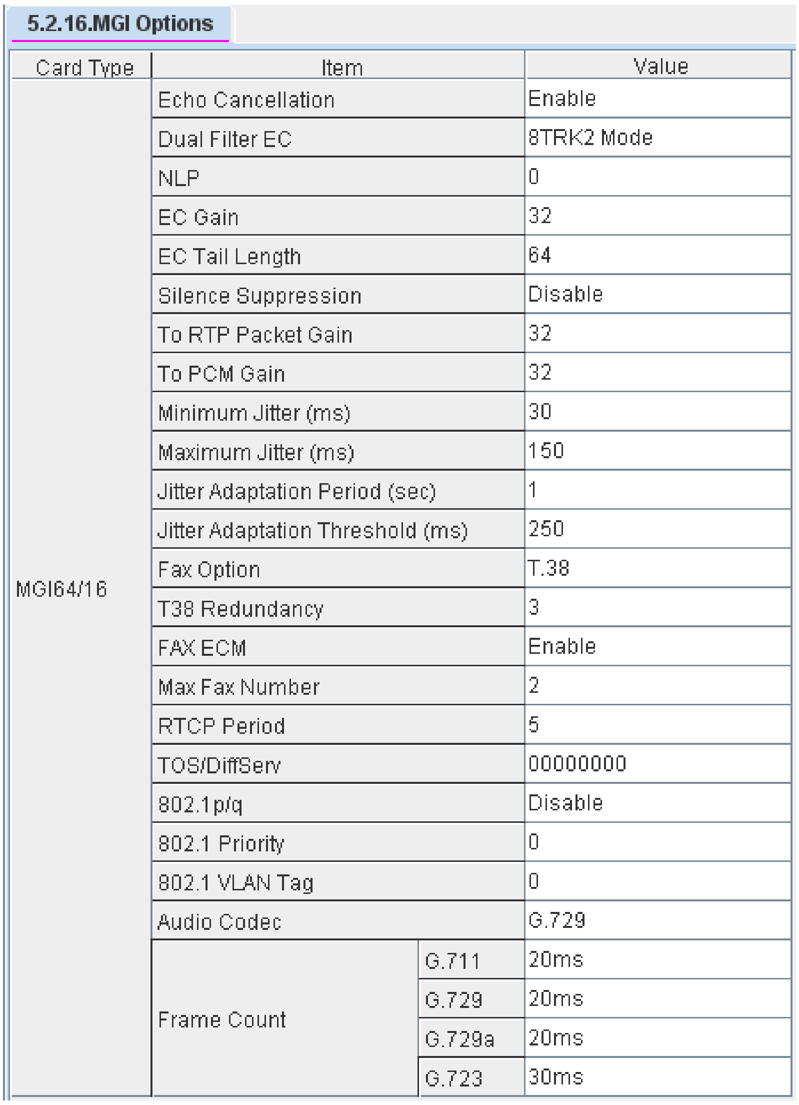
These are the public addresses used by the various types of VoIP call specified in **System IP Options** (DM 5.2.10). They are only used when the *IP Type* parameter is set to “Private with Public”.

Public RTP Port (1 to 3)

All RTP traffic uses UDP ports. The public UDP port ranges are utilized for calls that use the *Private with Public* feature. The *Public RTP port* number is the first UDP port number in the range of UDP ports used for calls.

MGI card codec options

The MGI Options screen (DM 5.2.16)



5.2.16.MGI Options

Card Type	Item		Value
MGI64/16	Echo Cancellation		Enable
	Dual Filter EC		8TRK2 Mode
	NLP		0
	EC Gain		32
	EC Tail Length		64
	Silence Suppression		Disable
	To RTP Packet Gain		32
	To PCM Gain		32
	Minimum Jitter (ms)		30
	Maximum Jitter (ms)		150
	Jitter Adaptation Period (sec)		1
	Jitter Adaptation Threshold (ms)		250
	Fax Option		T.38
	T38 Redundancy		3
	FAX ECM		Enable
	Max Fax Number		2
	RTCP Period		5
	TOS/DiffServ		00000000
	802.1p/q		Disable
	802.1 Priority		0
	802.1 VLAN Tag		0
	Audio Codec		G.729
	Frame Count	G.711	20ms
		G.729	20ms
		G.729a	20ms
		G.723	30ms

The MGI card operational parameters must be configured to match the voice traffic requirements of the SIP carrier. Note that the codec setting in this screen is not used for calls that use the MPS feature.

The options in this command will affect the voice quality of calls that use MGI channels. They should remain at the default value unless there is good reason to change them.

Audio Codec

The audio codec option selects the preferred codec to be used for calls. G.729 requires about 30Kbps per call and is used to preserve bandwidth on a data link. G.711 requires about 90Kbps per call, has better voice quality, and is used if there is sufficient bandwidth available. Note that even if the MGI card is configured for G.711 the SIP carrier may force the OfficeServ to use G.729 instead – it is also possible that the opposite may occur.

Frame count

Frame count defines how large the voice samples are in each voice packet, and this defines how many packets are sent every second. Most VoIP devices use a frame size of 20mS, which requires 50 packets per second. Increasing the frame size *reduces* the number of packets sent per second, and as result, less bandwidth is required. But the trade-offs are: increased voice delay experienced by the users and increased degradation in voice quality when packet loss occurs.

Silence suppression

Silence suppression reduces the amount of bandwidth used for a call. It does this by suspending the transmission of voice packets when speech is not heard from the user. This feature can reduce voice clarity, and it is only recommended when there are many concurrent calls and there isn't sufficient bandwidth.

Fax Option

The *Fax Op*tion allows you to select the type of data transmission service to use for Fax over IP calls. The Options are:

1. T.38
2. Pass Through
3. VBD

T.38

T.38 is a reliable way of sending fax and modem transmissions over packet networks. This option should be enabled if the SIP carrier offers T.38 for faxes through their network. When this feature is disabled the MGI codec setting must be G.711, as G.729 cannot carry fax data streams. Be aware that faxes sent over G.711 on packet networks can suffer problems if the network has significant jitter and packet loss; therefore, T.38 is preferred when it is supported by the carrier.

Pass Through

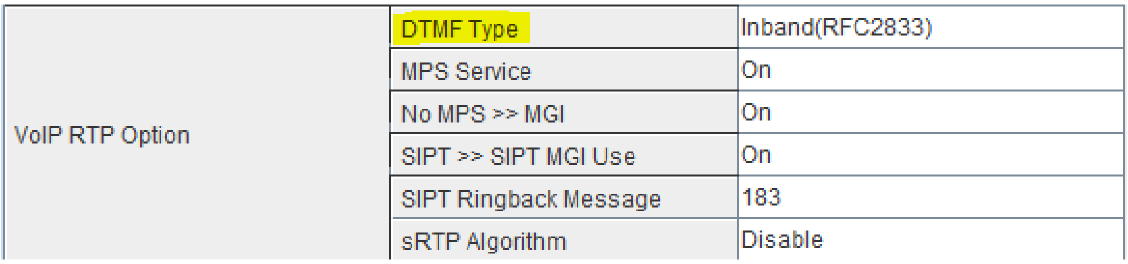
The MGI implements non-T.38 voice grade processing for fax calls when this setting is applied.

VBD

Many of the error correction techniques used in VoIP processing are designed to ensure that voice sounds as good as possible. The VBD protocol disables NLP (Non-linear Processing) and Jitter Buffer processing to ensure that fax and modem transmissions over VoIP links are not impaired by those processes.

DTMF on SIP trunks

DM menu item 2.1.5 →VoIP RTP Options.



VoIP RTP Option	DTMF Type	Inband(RFC2833)
	MPS Service	On
	No MPS >> MGI	On
	SIPT >> SIPT MGI Use	On
	SIPT Ringback Message	183
	sRTP Algorithm	Disable

There are three different methods in which DTMF digits can be sent through a VoIP link: Outband, Inband(Voice) and Inband(RFC2833), and the most commonly used method is **Inband(RFC2833)**.

Outband – The DTMF digits are sent in a SIP INFO message. The SIP carrier must be able to understand and process SIP INFO messages and then pass this on through the network to a device that converts it into DTMF tones. This is a complex task for carrier networks and most SIP carriers do not support Outband DTMF.

Inband(In Voice) – The DTMF digits are sent as tones in voice packets. This works okay with G.711 encoding, but G.729 compression may impair the receiving device's ability to detect the tones.

Inband(RFC2833) – RFC 2833 is a protocol that was developed to enable DTMF digits to reliably pass through VoIP links that compress voice. SIP carriers prefer to use this method.

Example Configurations

There are two modes of operation of SIP trunks in the OfficeServ: SIP carrier mode and SIP peering mode.

Up to four separate SIP carriers are can be configured in the OfficeServ and they are designated ISP1 through to ISP4.

The key characteristics of carrier and peer mode are:

SIP carrier mode

- Designed for trunks that link to a SIP carrier.
- Can send SIP registration requests to the SIP carrier.
- Can use DNS servers to resolve a proxy URL to an IP address
- Can detect when the SIP carrier cannot be contacted and disables the trunks
- Permits call re-routing when the SIP carrier does not respond to call attempts

SIP peering mode

- Designed for SIP trunks that link to other SIP capable PBXs.
- Does not use SIP registration.
- Does not use DNS or URLs to find the IP addresses of peer systems.
- Can check if a peer is available and will stop sending calls to non-responding IP addresses.
- Does not re-route when the peer system is unavailable

Which mode should you use?

When the OfficeServ is connected to a SIP carrier the preferred type of operation is *SIP Carrier* mode. SIP peering mode is preferred when the OfficeServ makes SIP trunk calls to another PBX.

It is possible to use both modes at the same time, which allows a system to use its SIP trunks to connect to both SIP carriers and SIP PABXs.

Some SIP carriers do not require registration, so it may be possible to use SIP peering for calls to those networks. However, it is also possible to use SIP carrier mode without sending registration messages. And, since SIP carrier mode provides more features than peering mode, it is better to use SIP carrier mode in those cases.

Least Cost Routing configuration

SIP trunks use ‘en-block’ sending for outgoing calls; which means that the OfficeServ will wait for all digits to be dialled before setting up a call. Since, by default, the system does not know how long a dialled number will be, it waits for the *ISDN Inter Digit Time* to expire before processing the call. This waiting period is unacceptable for many customers.

This delay can be eliminated by the user pressing ‘#’ to indicate the end of dialling. And the LCR feature can also be programmed to append “#” to the end of a number when it reaches a defined length (usually 8 or 10 digits), which means that users do not have to dial it themselves.

Use the following steps to program the LCR feature to add the ‘#’ digit to the end of an outgoing number. The programming described below is only a guide, as it expected that customer systems will need far more detailed numbering plans.

Step 1: In **Numbering Plan** (DM 2.8.0) program the LCR feature access code.
(This is usually set to ‘0’)

Step 2: In **LCR Options** (DM 3.1.1) set the *LCR Enable* parameter to “On”.

Step 3: In **Routing Digits** (DM 3.1.2) configure the *LCR Digit*, *Length* and *Route Table* parameters. The *Length* must be equal to the expected amount of digits that will be dialled, including the *LCR Digit*. The *Route Table* parameter contains the number of the route table that will be used in the **Routing Table** (DM 3.1.4).

Step 4: In **Routing Table** (DM 3.1.4) assign the SIP trunk group access code to the *Group* parameter. The *Modify* parameter contains the *Entry Number* that will be used in the **Modify Digits** (DM 3.1.5) table.

Step 5: In **Modify Digits** (DM 3.1.5) put the “#” code in the *Append Digits* field linked to the table entry.

A quick configuration guide for SIP trunks

For more detailed information on the use of the SIP commands please read the detailed guides in the ‘**Detailed descriptions of SIP trunking commands and parameters’** section of this document.

To prepare for an installation of SIP trunks you must:

1. Configure the IP address, Subnet mask and Gateway address on the LAN interfaces in the main processor and, if necessary, the MGI or OAS card.

2. Verify that the broadband connection provides a reliable link to the SIP provider.

3. Check that the customer’s Router/Firewall is able to pass SIP signalling and associated voice traffic.

4. Obtain and enter the SIP trunk licenses into the OfficeServ

5. When the system is an OS7030, OS7100 or an OS7200S, please check that there are a sufficient number of licensed MGI channels to handle the maximum amount of SIP trunk calls; as well as calls from other VoIP devices, such as IP Phones and Samsung soft phones. Note that when IP phones are used the MPS feature reduces the number of MGI channels needed by the system.

6. If the SIP carrier provides their proxy server address as a URL (e.g. *sip.mycarrier.com.au*) obtain the IP address of a DNS server that can be used to resolve the URL to an IP address. This address is usually provided by the Internet service provider or the customer’s IT staff.

7. Obtain the following information and SIP account details from the SIP provider.
   - The SIP Proxy server URL or IP address.
   - The Proxy domain name (usually the same as the SIP Proxy server URL).
   - The SIP account name/number.
   - The password for the SIP account (if required).

8. When the SIP carrier requires password authorization the SIP trunks must use *Representative* or *Individual* mode. When there is a single SIP account the OfficeServ uses *Representative* mode, and if there are multiple SIP accounts it uses *Individual* mode. These modes are described in more detail in the **Using a Single SIP account and Multiple SIP accounts** section of this document.

9. When the SIP carrier does not use passwords the OfficeServ should use carrier mode with the “No Registration” feature configured. (See the “No Registration Feature” section of this document for details.)

HOW TO: A quick configuration guide for SIP trunks in Carrier mode

SIP carrier mode is used to link the OfficeServ to SIP carriers using SIP trunks. SIP carriers usually require that the OfficeServ register its SIP presence and provide authorisation for outgoing calls.

The **SIP carrier options** (DM 5.2.13) page is used to configure SIP trunks in carrier mode. When the SIP carrier provides a single SIP account, the username and password information is entered into this page. When there are multiple SIP accounts the **SIP User** (DM 5.2.14) page is programmed with the usernames and passwords of all of those accounts. *The section in this document on Representative and Individual mode has more information about configuring the SIP trunks with single and multiple accounts.*

For more information on the use of the SIP trunk commands please read the detailed guides in the '**Detailed descriptions of SIP trunking commands and parameters'** section of this document.

To prepare for an installation of SIP trunks in carrier mode you must:

1. Configure the IP address, Subnet mask and Gateway address for the LAN interface in the main processor and, if necessary, the OAS/MGI card.

2. Obtain and enter the SIP trunk license into the OfficeServ.

10. When the system is an OS7030, OS7100 or an OS7200S, please check that there are a sufficient number of licensed MGI channels to handle the maximum amount of SIP trunk calls – as well as calls from other VoIP devices, such as IP Phones and Samsung soft phones. Note that when IP phones are used the MPS feature reduces the number of MGI channels needed by the system.

3. Verify that the IP network that links the OfficeServ to the SIP carrier is allowing traffic to pass unhindered.

4. Obtain the SIP account details from the SIP carrier. In the **Partner Resource Centre** there are configuration guides to help with setting up SIP trunks on some carriers; there is a guide for Telstra, for example.

5. Obtain the DNS server address from the Internet provider.

Example: Configuring the SIP trunks in Representative mode.

The following example shows the basic programming required to set up SIP trunks with a carrier that uses a single account for all calls. In this case the SIP trunks are using *Representative* mode.

Trunk Groups (DM 4.1.2)

The SIP trunks are selected by the trunk group number.

Group Number = This is the trunk group number dialled by the user or accessed by LCR.
Group Type = The type of trunk group is SIP.
ISP Selection = This the ISP in the *SIP Carrier Options table (DM 5.2.13*) that will be used by the trunk group. E.G *ISP1*
Trunk numbers. Make sure that at least one SIP trunk number is provided.

SIP Carrier Options (DM 5.2.13)

SIP Server Enable = Enable
Outbound Proxy = sipproxy.example.com.au
DNS Server 1 = 1.2.3.4 *(Use the DNS server address provided by the Internet provider)*
User Name = The account number provided by the SIP carrier
Auth Password = The password provided by the SIP carrier
Regist. Per User = Disabled
Send CLI Table = 1
Hold Mode = SendRecv
All other parameters should remain at their default values

Send CLI Number (DM 2.4.3)

Some SIP carriers do not need the CLI to match the account number. In this example the CLI must match the account number. The SIP trunks have been configured to use **Send CLI Table** = 1

Tel Num = *Station number*
Send CLI Number 1 = *SIP account number*

SIP DID Ringing (DM 3.2.3)

Incoming Digits = *The number received from the SIP carrier*
Ring Plan 1 to 6 = *The destination station number for incoming calls for the appropriate ring plan.*

System Options (DM 2.1.5)

Most SIP Carrier use *RFC2833* to send and receive DTMF digits. And make sure that the URL can be resolved using DNS.

VoIP RTP Option → DTMF Type = Inband(RFC2833)
Multi DNS Server = *Enable*

VoIP Options (DM 5.2.18)

It is preferred that the audio sent by the SIP Carrier during the ring state is passed through to the stations.

Real Ringback = *ON*

Example: Configuring the SIP trunks in Individual mode.

This example is for a customer with multiple SIP accounts with passwords. Therefore, the SIP trunks need to be in *Individual* mode. Note: the CLI of a station making an outgoing call must be the same as a SIP account number.

Trunk Groups (DM 4.1.2)

The SIP trunks are selected by the trunk group number.

Group Number = This is the trunk group number dialled by the user or accessed by LCR.
Group Type = The type of trunk group is SIP.
ISP Selection = This the ISP in the *SIP Carrier Options table (DM 5.2.13*) that will be used by the trunk group. E.G *ISP1*
Trunk numbers. Make sure that at least one SIP trunk number is provided.

SIP Carrier Options (DM 5.2.13)

SIP Server Enable = Enable
Outbound Proxy = sipproxy.example.com.au
DNS Server 1 = 1.2.3.4 *(Use the DNS server address provided by the Internet provider)*
Regist. Per User = Enable
Send CLI Table = 1 (In this example, CLI table 1 provides the CLI for the station)
Hold Mode = SendRecv
All other parameters remain at their default values

SIP Users (DM 5.2.14)

Add an entry in the *SIP User table* for *every* SIP account.

User Name = *This is the account number provided the carrier.*
Auth Password = *This is the password linked to the account.*

Send CLI Number (DM 2.4.3)

The CLI configured for the calling phone must match one of the account numbers programmed in **5.2.14 SIP Users.** The SIP trunks have been configured to use **Send CLI Table** = 1

Tel Num = *Station number*
Send CLI Number 1 = *SIP account number*

SIP DID Ringing (DM 3.2.3)

Incoming Digits = *This is the number received from the SIP carrier*
Ring Plan 1 to 6 = *This is the destination station number for incoming calls.*

System Options (DM 2.1.5)

Most SIP Carrier use *RFC2833* to send and receive DTMF digits. And make sure that the URL can be resolved using DNS.

VoIP RTP Option → DTMF Type = Inband(RFC2833)
Multi DNS Server = *Enable*

VoIP Options (DM 5.2.18)

The audio sent by the SIP Carrier during the ring state should be passed through to the stations.

Real Ringback = *ON*

HOW TO: A quick configuration guide for SIP trunks in Peer mode

SIP peering mode is used to link the OfficeServ to other systems using SIP trunks. Unlike SIP carriers these systems do not need to authorize calls or register SIP presence. SIP peering uses a number plan to permit a flexible network configuration.

For more information on the use of the SIP trunking commands please read the detailed guides in the ‘**Detailed descriptions of SIP trunking commands and parameters’** section of this document.

To prepare for an installation of SIP trunks in peering mode you must:

1. Configure the IP address, Subnet mask and Gateway address for the LAN interface in the main processor and, if necessary, the MGI card.

2. Obtain and enter the SIP trunk license into the OfficeServ.

3. When the system is an OS7030, OS7100 or OS7200S verify that there are a sufficient number of licensed MGI channels to handle the maximum amount of SIP calls and calls from any other VoIP device connected to the system: for example, IP Phones and Samsung soft phones.

4. Verify that the IP network linking the OfficeServ to the remote systems is allowing traffic to pass unhindered.

5. Obtain IP addresses of the remote systems.

6. Design the number plan that will be used to choose the routes to the other systems.

An example configuration for SIP trunks in peering mode.

The following example gives an overview of the programming required to set up SIP trunks between two systems in peer mode.

In this example:

1. The IP address if the OfficeServ is 192.168.1.230

2. The remote system's IP address is 192.168.1.108

3. The numbers dialled in the remote system are in the 2xx range

Trunk Groups (DM 4.1.2)

The SIP trunks are selected by the trunk group number.

Group Number = This is the trunk group number dialled by the user or accessed by LCR.
Group Type = The type of trunk group is SIP.
ISP Selection = This is set to "Peering".
Trunk numbers. Make sure that at least one SIP trunk number is provided.

SIP Stack/Ext/Options (DM 5.2.12)

In the *SIP Trunk Configuration* section of this page there are multiple settings for SIP peering: such as Codec and Max channels. For this basic example, only the *Send CLI Table* parameter is used. The *Send CLI Table* parameter must be checked to make sure that it matches the correct CLI table. The SIP trunks send the CLI in found in the *Send CLI Number (DM 2.4.3)* table to the remote system.

Send CLI Table = 1 (In this example, CLI table 1 provides the CLI for the station)

VoIP Outgoing Digits table (DM item 5.2.3)

In this example, the **VoIP Outgoing Digits** table (DM 5.2.3) has been configured to send calls for destination numbers starting with '2' to *IP Table 0* in ***VoIP Peering*** *(DM 5.2.17).*
The *Digit Length* is 1, so only the first digit will be used to decide which table to use.

Table No = 0
Access Digit = 2
Digit Length = 1
IP Table Number = 1

The IP Table Number selects the peer table in *VoIP Peering (DM 5.2.17)*

VoIP Peering table (DM item 5.2.17)

In this example, the IP address of the remote system is in table 1 of *VoIP Peering (DM 5.2.1*7).

Table No = 1
IP Address = 202.100.120.10 (This is only an example address)

By default, the *Alive Status* for the table entry is “Yes” because it assumes that the remote system is available. If you want the OfficeServ to verify that the remote site is on line you can set the *Alive Check* parameter to ‘OPTIONS’ and put a name in the *User Information* that is shared with the remote system, e.g. “LabTest”. The *Alive Check* feature gets the OfficeServ to test the link by sending OPTIONS messages to check if the remote site is available.

Troubleshooting

The following list refers to problems that have occurred on site and has describes their causes.

No SIP trunk licenses

When there are no SIP trunk licenses the OfficeServ will not make SIP calls or try to register with the SIP carrier.

The outbound proxy server address is incorrect

If the outbound proxy server address is incorrect the OfficeServ cannot contact the SIP carrier.

The DNS server IP address are incorrect or are not used

When the Outbound Proxy address is an URL the OfficeServ will attempt to resolve that URL to an IP address. If the DNS server address is not configured or is incorrect the OfficeServ cannot resolve the proxy server's IP address; and as a result, registration and outgoing calls will fail.
DNS lookup will fail if the *Multi DNS Server* setting in **System Options (DM2.1.5)** is set to "Disable" and there are no IP addresses programmed in **System I/O Parameters (DM 5.6.1)**.

Programming error in the account number or password or the SIP account is not activated at the SIP carrier

If the account number or password is incorrect the SIP carrier may reject SIP registration attempts and outgoing calls.

The CLI number does not match the account number.

Some SIP carriers require that the calling party information matches the account number. And when *Register Per User* is enabled the CLI must match one of the account numbers for outgoing calls to be made.

Broadband router and NAT-ALG issues

Some routers/firewalls do not support NAT-ALG properly. Use the OfficeServ **Private with Public** feature and static port translation entries in the router/firewall to bypass this problem.

DTMF not sent or received

Check that the DTMF setting is correct for the SIP carrier. In most cases the DTMF mode is RFC2833.

CLI is still being presented to the called party when CLI privacy is requested

The *Privacy Header Value* in **SIP Carrier Options (DM5.2.13)** may be missing or incorrect. Check that it has the right value. It is also possible that the carrier does not support CLI privacy and still sends it to the called party even if the OfficeServ SIP trunks request privacy. A Wireshark trace is needed to confirm this issue.

To diagnose problems with SIP trunks perform the following activities.

Obtain a network diagram with IP addresses

It is important that the broadband network is configured properly and that the network address details are correct. Verify that all IP addresses, as well as the subnet mask and the gateway address, are programmed correctly.

Check to see if the OfficeServ has been able to Register with the SIP server

Check the display field: **SIP Carrier Options** (DM 5.2.13): *SIP Service Available* = Yes

Check the SIP Alarm description table in Alarm History (DM 6.1.1)

Status	Alarm	Samsung Descriptions
OK	ISP1 OK REGIST	System succeeds in registering to the server with REGISTER message.
	ISP1 OK NO EXP	System succeeds in registering to the server which sends 200 OK with no expire time. In this case system uses expire time which the server offered at first.
	ISP1 OK OPTION	System succeeds in registering to the server by receiving response of OPTION message.
	DNS OUT 1 OK	System has contacted a DNS server
NOK	ISP1 NOK OPUPDT	System fails to register to the server because user changes the current setting when using OPTION message.
	ISP1 NOK UNREGI	System unregisters to the server.
	ISP1 NOK REFAIL	System tries to register to the server but it receives 4xx message.
	ISP1 NOK RE TO	System tries to register to the server but it can’t receive response message.
	ISP1 NOK REAUTH	Authentication fails.
	ISP1 NOK OP TO1	System can’t receive response message even though it sends OPTION message.
	ISP1 NOK OP TO2	System fails to register to the server even though it sends OPTION message.
	ISP1 NOK INVT01	System can’t receive response message even though is sends INVITE message. (Inviting call leg state)
	ISP1 NOK INVT02	System can’t receive response message even though it sends INVITE message. (Proceeding call leg state)
	ISP1 NOK NONAME	This alarm is shown in case of Korea.
	ISP1 NOK REGRQ	System receives 403 response whose reason includes “Register request” even though it sends INVITE message.
	DNS OUT 1 NOK	System cannot contact a DNS server

Obtain an Ethereal/Wireshark capture of call attempts.

Wireshark has a very good SIP call analysis feature in the Menu: *Telephony*→ *VoIP calls*.

Use this Wireshark feature to check that SIP messages from the OfficeServ:

- Are going to the correct destination IP address.
- Are being responded to by the SIP server
- Have the correct caller ID information
- Are not being rejected because the password is incorrect

Using Wireshark

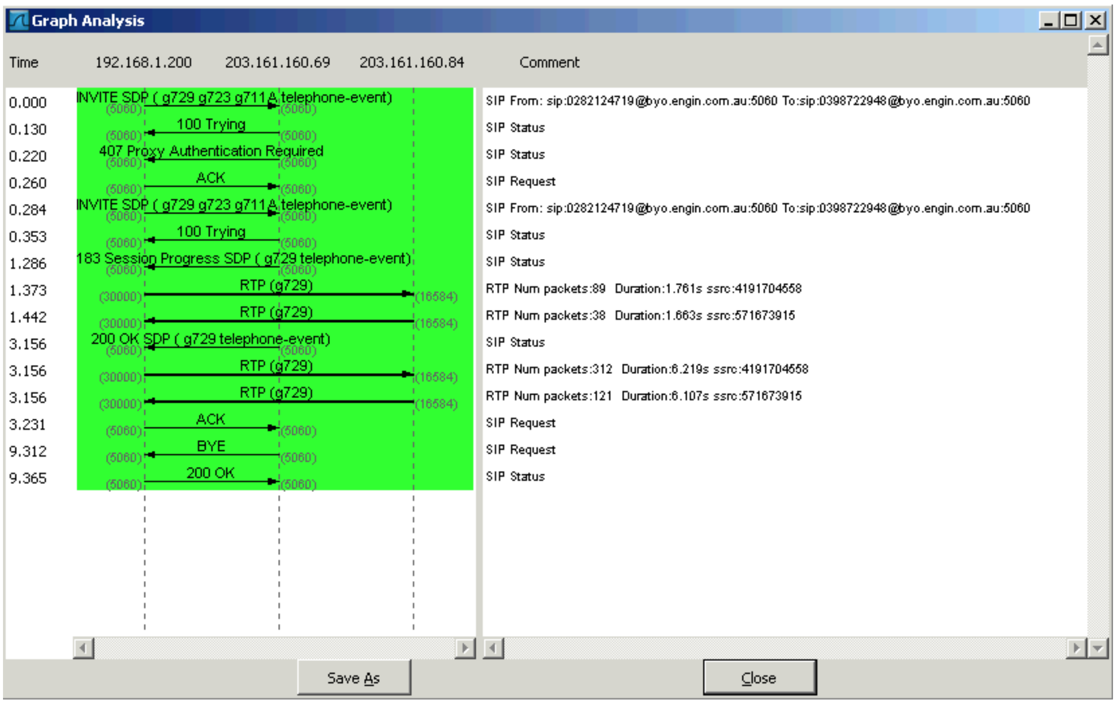
Wireshark is used to help diagnose SIP problems. There is a document available in the Partner Resource Centre titled "**How to use Wireshark to gather VoIP information**" which gives a detailed explanation of Wireshark and how to install and configure it for the analysis of VoIP calls.

Sample SIP calls in Wireshark VoIP call analysis charts.

The charts shown below were obtained from Wireshark using the VoIP analysis feature.

Successful outgoing call

The Wireshark call analysis chart below shows a successful outgoing call setup from an OfficeServ using IP address 192.168.1.200 to a SIP server at 203.161.160.69. The call was cleared by the called party after about 6 seconds.

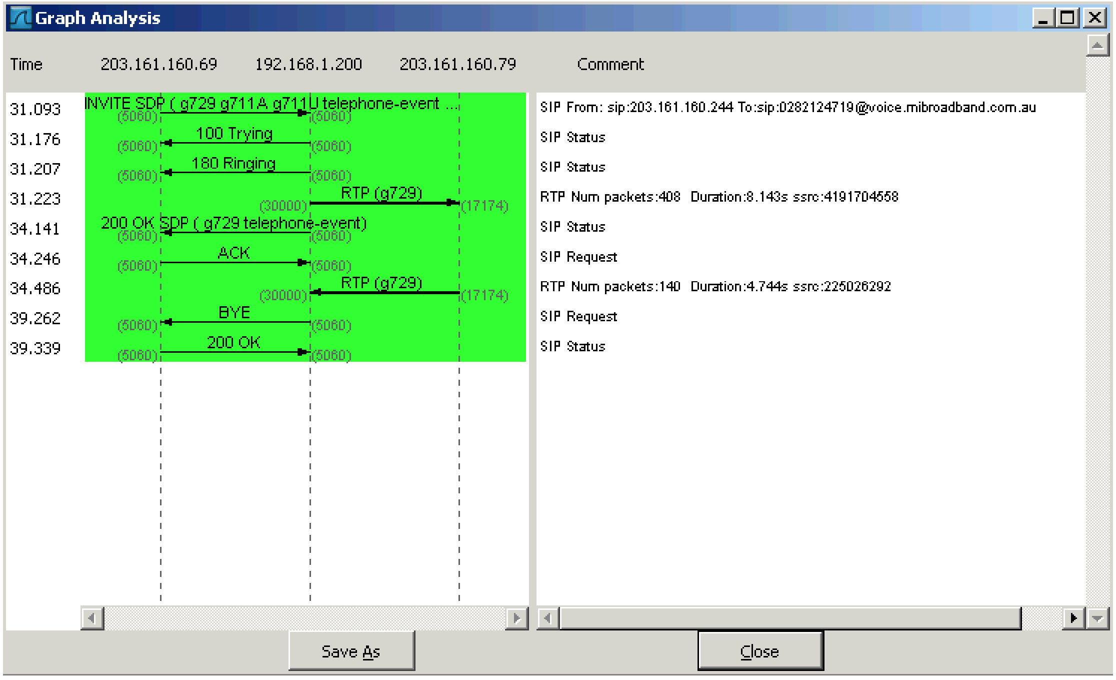


```
Time    192.168.1.200   203.161.160.69   203.161.160.84    Comment

0.000   INVITE SDP ( g729 g723 g711A telephone-event)      SIP From: sip:0282124719@byo.engin.com.au:5060 To:sip:0398722948@byo.engin.com.au:5060
        (5060) ------------------> (5060)
0.130   100 Trying                                         SIP Status
        (5060) <------------------ (5060)
0.220   407 Proxy Authentication Required                  SIP Status
        (5060) <------------------ (5060)
0.260   ACK                                                SIP Request
        (5060) ------------------> (5060)
0.284   INVITE SDP ( g729 g723 g711A telephone-event)      SIP From: sip:0282124719@byo.engin.com.au:5060 To:sip:0398722948@byo.engin.com.au:5060
        (5060) ------------------> (5060)
0.353   100 Trying                                         SIP Status
        (5060) <------------------ (5060)
1.286   183 Session Progress SDP ( g729 telephone-event)   SIP Status
        (5060) <------------------ (5060)
1.373   RTP (g729)                                         RTP Num packets:89  Duration:1.761s ssrc:4191704558
        (30000) ---------------------------------> (16584)
1.442   RTP (g729)                                         RTP Num packets:38  Duration:1.663s ssrc:571673915
        (30000) <--------------------------------- (16584)
3.156   200 OK SDP ( g729 telephone-event)                 SIP Status
        (5060) <------------------ (5060)
3.156   RTP (g729)                                         RTP Num packets:312  Duration:6.219s ssrc:4191704558
        (30000) ---------------------------------> (16584)
3.156   RTP (g729)                                         RTP Num packets:121  Duration:6.107s ssrc:571673915
        (30000) <--------------------------------- (16584)
3.231   ACK                                                SIP Request
        (5060) ------------------> (5060)
9.312   BYE                                                SIP Request
        (5060) <------------------ (5060)
9.365   200 OK                                             SIP Status
        (5060) ------------------> (5060)
```

Successful incoming call

The chart below shows a successful incoming call from a SIP server at 203.161.160.69 to the OfficeServ on IP address 192.168.1.200. The call was cleared by the called party after about 4 seconds.

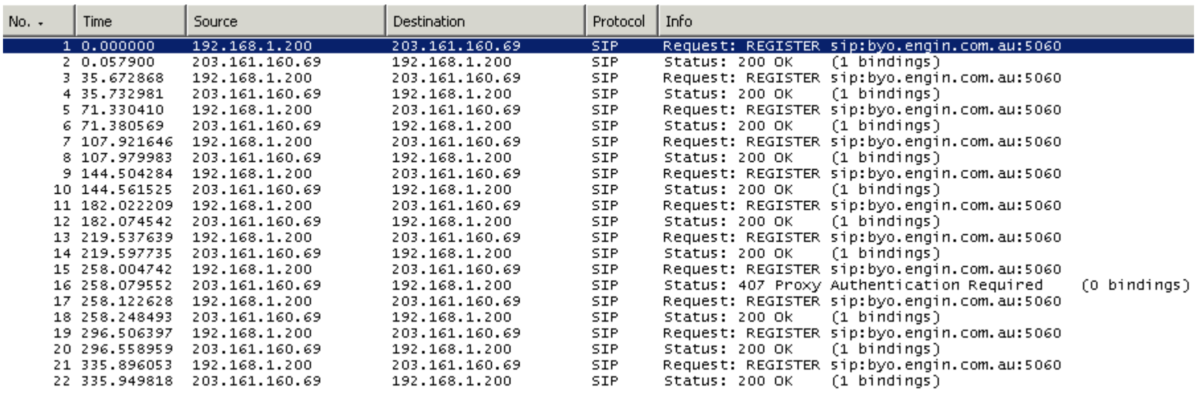


```
Time      Comment
31.093    SIP From: sip:203.161.160.244 To:sip:0282124719@voice.mibroadband.com.au
31.176    SIP Status
31.207    SIP Status
31.223    RTP Num packets:408  Duration:8.143s ssrc:4191704558
34.141    SIP Status
34.246    SIP Request
34.486    RTP Num packets:140  Duration:4.744s ssrc:225026292
39.262    SIP Request
39.339    SIP Status
```

SIP Register Messages

The following screen capture shows a Wireshark trace of the Registration messages between an OfficeServ and a SIP server. Register messages have two purposes: They are sent as keep-alive messages to the SIP server to make sure that it knows that the OfficeServ is available for incoming calls, and by the OfficeServ to verify that the SIP trunks are available for outgoing calls. Most of the REGISTER messages in the screen capture below are periodic (heartbeat type) register messages and do not contain any authorization information.

Packet number 16 is a response message from the SIP server that is asking the OfficeServ to provide authorization details. The Register message in Packet 17 contains the authorization details.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
2	0.057900	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)
3	35.672868	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
4	35.732981	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)
5	71.330410	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
6	71.380569	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)
7	107.921646	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
8	107.979983	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)
9	144.504284	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
10	144.561525	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)
11	182.022209	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
12	182.074542	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)
13	219.537639	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
14	219.597735	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)
15	258.004742	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
16	258.079552	203.161.160.69	192.168.1.200	SIP	Status: 407 Proxy Authentication Required (0 bindings)
17	258.122628	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
18	258.248493	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)
19	296.506397	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
20	296.558959	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)
21	335.896053	192.168.1.200	203.161.160.69	SIP	Request: REGISTER sip:byo.engin.com.au:5060
22	335.949818	203.161.160.69	192.168.1.200	SIP	Status: 200 OK (1 bindings)

Document Revision History

Edition	**Date**	**Author**	**Revision Details**
DRAFT	27/10/2014	Colin Elms	*Based on OfficeServ software version 4.82*
01	6/11/2014	Colin Elms	*Published version of the document*