

MiVoice 5000 Séparation des Flux Téléphonie et Administration

09/2021

AMT/PTD/PBX/0101/5/0/FR

MANUEL DE MISE EN ŒUVRE



Avertissement

Bien que les informations contenues dans ce document soient considérées comme pertinentes, Mitel Networks Corporation (MITEL ®) ne peut en garantir l'exactitude.

Les informations sont susceptibles d'être modifiées sans préavis et ne doivent pas être interprétées de quelque façon que ce soit comme un engagement de Mitel, de ses entreprises affiliées ou de ses filiales.

Mitel, ses entreprises affiliées et ses filiales ne sauraient être tenus responsables des erreurs ou omissions que pourrait comporter ce document. Celui-ci peut être revu ou réédité à tout moment afin d'y apporter des modifications.

Aucune partie de ce document ne peut être reproduite ou transmise sous une forme quelconque ou par n'importe quel moyen - électronique ou mécanique – quel qu'en soit le but, sans l'accord écrit de Mitel Networks Corporation.

© Copyright 2021, Mitel Networks Corporation. Tous droits réservés.

Mitel ® est une marque déposée de Mitel Networks Corporation.

Toute référence à des marques tierces est fournie à titre indicatif et Mitel n'en garantit pas la propriété.

SOMMAIRE

1	AVANT PROPOS	2
1.1	TERMINOLOGIE	2
1.1.1	TERMES ET EXPRESSIONS	2
1.1.2	ABREVIATIONS	2
1.2	DOCUMENTS DE RÉFÉRENCE	3
2	INTRODUCTION	4
2.1	PRINCIPE	4
2.2	PRE-REQUIS ET PRECONISATION	4
2.3	RÈGLES ET RESTRICTIONS	4
2.4	PRÉSENTATION DE L'ARCHITECTURE	5
3	CAS D'UNE NOUVELLE INSTALLATION	6
3.1	PRE-REQUIS	6
3.2	PRINCIPALES ETAPES DE LA MISE EN ŒUVRE DE LA SEPARATION DE FLUX	6
3.3	CONFIGURATION DES PARAMETRES IP DES RESEAUX TELEPHONIE ET ADMINISTRATION POUR UNE PREMIERE INSTALLATION MITEL 5000 GATEWAYS ET MITEL 500	7
3.5	CONFIGURATION DES PARAMETRES IP DES RESEAUX TELEPHONIE ET ADMINISTRATION POUR UNE PREMIERE INSTALLATION MIVOICE 5000 SERVER	10
3.5.1	PRE-REQUIS	10
3.5.2	CONFIGURATION DES PARAMETRES IP DES RESEAUX TÉLÉPHONIE ET ADMINISTRATION	10
3.5.3	CONFIGURATION DU FIREWALL	10
4	CAS D'UNE INSTALLATION EXISTANTE	11
4.1	PRE-REQUIS	11
4.2	PRINCIPALES ETAPES DE LA MISE EN ŒUVRE DE LA SEPARATION DE FLUX	11
4.3	CONFIGURATION DES PARAMETRES IP DES RESEAUX TELEPHONIE ET ADMINISTRATION SUR UNE INSTALLATION EXISTANTE MITEL 5000 GATEWAYS ET MITEL 500	12
4.4	CONFIGURATION DU FIREWALL	12
5	CONFIGURATION DES ROUTES IP DU RESEAU ADMINISTRATION	13
5.1	CONFIGURATION DES ROUTES SUR LES MITEL 5000 GATEWAYS ET MITEL 500	13
5.2	CONFIGURATION DES ROUTES SUR LE MIVOICE 5000 SERVER	14
6	ANNEXES	15
6.1	FLUX DE DONNEES POUR LA SOLUTION MIVOICE 5000	15
6.1.1	FLUX DE DONNEES CONCERNANT LES EQUIPEMENTS RELIES AU RESEAU DE TÉLÉPHONIE	15
6.1.2	FLUX DE DONNEES CONCERNANT LES EQUIPEMENTS RELIES AU RÉSEAU ADMINISTRATION	17
6.2	PROTOCOLES SUPPORTES	20
6.2.1	PROTOCOLES EN ENTREE SUPPORTES PAR LE RESEAU TÉLÉPHONIE	20
6.2.2	PROTOCOLES EN ENTREE SUPPORTES PAR LE RÉSEAU ADMINISTRATION	21
6.2.3	PROTOCOLES AUTORISES DEPUIS LE RESEAU ENTREPRISE VERS LE RÉSEAU ADMIN	21

1 AVANT PROPOS

1.1 TERMINOLOGIE

1.1.1 TERMES ET EXPRESSIONS

Mitel 5000 Gateways	Ce terme regroupe l'ensemble des systèmes, XS, XL et XD
MiVoice 5000 ou MiVoice 5000 Server	Système de commutation téléphonique hébergé sur un PC Linux Redhat
XS, XL, XD	Gateways physiques de la gamme MiVoice 5000
XS	Ce terme regroupe les systèmes XS, XS12 et XS6
Mitel 500	Ce terme regroupe les systèmes Mitel 500, 500x et 50x
MitelMiVoice 5000 Manager	Centre de gestion d'un parc

1.1.2 ABREVIATIONS

Web Admin	Mitel 5000 Contact Center
DHCP	Dynamic Host Configuration Protocol.
FTP	File Transfer Protocol
GSI	Gateway SIP
https	Hypertext Transfer Protocol Secure
LDAP	Light Directory Access Protocol
IAE	Interface Application Externe
IP	Internet Protocol
MOVACS	Multiswitch Original Virtual Addressing Communication System
PBX	Private Branch eXchange
PPP	Point to Point Protocol
RTP	Real Time Protocol
SBC	Session Border Controller
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
TAPI	Telephony Application Programming Interface
TCP	Transport Control Protocol
TLS	Transport Layer Security, previously SSL (secure socket layer)
TMA	Terminal Management Application
TWP	Telephony Web Portal
UCP	Unified Communication Platform
VLAN	Virtual Local Area Network
VTI	Virtual Terminal Interface
XML	eXtended Markup Language

1.2 **DOCUMENTS DE RÉFÉRENCE**

Se référer à la documentation fournie sur le site Mitel.com.

2 INTRODUCTION

2.1 PRINCIPE

La séparation des flux de la Téléphonie et d'Administration a pour but d'améliorer la sécurité en affectant pour chacun de ces flux, un réseau IP dédié et distinct.

Cette solution consiste à définir deux réseaux IP séparés :

- Le réseau **Téléphonie** sur lequel tous les postes ou terminaux utilisateur sont connectés via les équipements correspondants. Ce réseau peut être plus généralement celui de l'entreprise,
- Le réseau **Administration** sur lequel les équipements de gestion opèrent.

Ces deux réseaux doivent être distincts et peuvent être constitués de plusieurs sous-réseaux IP.

L'architecture repose sur les principes suivants :

- Un flux de données est identifié par des adresses IP d'équipements et le protocole utilisé. Ce protocole est identifié par les ports d'UDP ou de TCP (Se référer en Annexe de ce document),
- Chaque équipement est relié à un de ces deux réseaux, excepté les iPBX (Mitel 5000 Gateways, Mitel 500 ou MiVoice 5000 Server) qui sont reliés aux deux réseaux,
- D'autres applications telles que Mitel OMM, CC, TWP et UCP sont reliées exclusivement au réseau Téléphonie, le risque de dommage des données de gestion étant moins important qu'avec un iPBX,
- Chaque réseau est dédié aux protocoles considérés,
- La communication entre les deux réseaux est réalisée au travers d'un Fire Wall externe qui filtre les flux de données,
- Les iPBXs peuvent être atteints par deux adresses IP en fonction du protocole utilisé. Un FireWall intégré aux iPBXs vérifie la cohérence entre les accès et les protocoles,
- Les accès distants via le protocole PPP ne sont pas concernés par cet environnement.

En cas de redondance et/ou de double attachement du MiVoice 5000 server, la séparation des flux est applicable à partir de R5.3 SP2.

Se référer au document AMT/PTD/PBX/0083 relativement à la version considérée (> R5.3 SP2)

2.2 PRE-REQUIS ET PRECONISATION

Pour la mise en œuvre de la séparation des flux Téléphonie/Administration sur un système Mitel 5000 gateway (y compris EX), il est nécessaire que chaque routeur raccordé respectivement sur l'interface de Téléphonie et sur l'interface d'Administration présente une adresse MAC différente.

Ceci est naturellement le cas avec des équipements de routage dédiés pour une séparation de flux complète.

Si ce n'est pas le cas et que le même Routeur soit utilisé avec simplement des VLAN dédiés, Il faut alors veiller à ce que ce Routeur utilisé puisse prendre en charge ce prérequis.

En cas de non-respect de cette préconisation, des ralentissements voire une impossibilité d'accès pourront être ressentis sur l'interface d'administration.

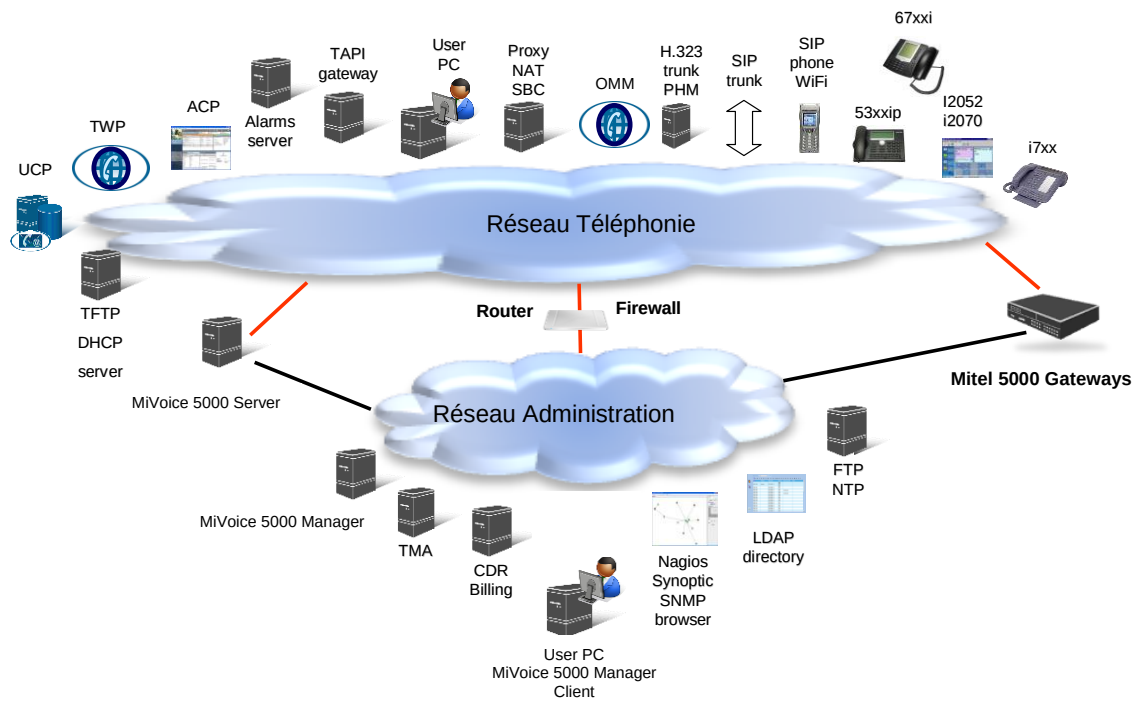
2.3 RÈGLES ET RESTRICTIONS

Tous les iPBXs de l'architecture considérée doivent être en mode Séparation de flux.

L'utilisation d'un serveur de téléchargement externe est impérative dans l'environnement actuel proposé. Ce serveur doit être déclaré pour la gestion des postes (TMA).

En conséquence, Le serveur de téléchargement embarqué pour les Mitel 5000 Gateways n'est pas utilisable dans cet environnement.

2.4 PRÉSENTATION DE L'ARCHITECTURE



3 CAS D'UNE NOUVELLE INSTALLATION

3.1 PRE-REQUIS

Deux réseaux distincts sont opérationnels et communiquent via un ensemble Routeur/FireWall.

Se référer également au paragraphe 2.2 - Pré-requis et Préconisation.



ATTENTION : Le serveur de téléchargement embarqué n'est pas utilisable dans cet environnement. Un serveur de téléchargement externe doit être déclaré pour la gestion des postes (TMA). Se référer au Manuel Installation des Postes - AMT/PTD/TR/0014.

3.2 PRINCIPALES ETAPES DE LA MISE EN ŒUVRE DE LA SEPARATION DE FLUX

Raccorder et configurer les différents équipements sur leur réseau respectif,

Sur le MiVoice 5000 Manager

Le MiVoice 5000 Manager étant relié au réseau Administration, aucune configuration particulière n'est requise pour l'environnement Séparation de flux.

Sur les Mitel 5000 Gateways et Mitel 500

La définition des différents paramètres réseaux est à définir lors de la phase Ctrl + i,

Le Firewall intégré aux Mitel 5000 Gateways est configuré automatiquement à l'issue de cette phase

Sur Le MiVoice 5000 Server,

Les deux cartes réseaux sont opérationnelles relativement aux deux réseaux.

La déclaration de l'adresse IP du réseau Administration est à effectuer à partir de Web Admin.

La Configuration du Firewall interne est effectuée en se référant à l'annexe



Note : Concernant les Mitel 5000 Gateways, Mitel 500 et le MiVoice 5000 server, dans le cas où le réseau Administration est constitué de plusieurs sous-réseaux, définir les routes correspondantes (se référer au paragraphe 5 - Configuration des routes IP du réseau administration).

Sur le Routeur/Firewall d'interconnexion

Configurer le filtrage pour laisser passer les flux qui apparaissent surlignés dans le tableau en Annexe.

Dans le cas où le réseau Administration est constitué de plusieurs sous-réseaux, définir les routes correspondantes (se référer au paragraphe 5 - Configuration des routes IP du réseau administration).

3.3 CONFIGURATION DES PARAMETRES IP DES RESEAUX TELEPHONIE ET ADMINISTRATION POUR UNE PREMIERE INSTALLATION MITEL 5000 GATEWAYS ET MITEL 500

Dans le cas d'une première installation, la configuration de la séparation des flux est à réaliser lors de la phase du Ctrl +i.

L'accès est réalisé localement sur le port COM de la carte mère en utilisant un câble NULL MODEM (réf. :BHG0024A) relié entre le port COM de la carte mère et le port COM du PC d'administration.

Procédure

Sur le PC raccordé au port COM

- Ouvrir une fenêtre "Hyperterminal" et paramétrer la connexion comme indiqué :
- Bits par seconde : 115200 b/s
- Bits de données : 8
- Parité : aucun
- Bits d'arrêt : 1
- Contrôle de flux : Aucun
- Mettre sous tension le coffret et sur le PC, visualiser le déroulement du démarrage,
- A l'affichage "**Identification starting**"
- Tapez la commande **Ctrl + I**

L'écran affiche ensuite les différents modes de configuration :

```
Configuration mode (F/T/S/P/E)
- F: Factory mode
- T: Total mode
- S: Standard mode
- P: Password reset
- U: USB provisioning mode
- E: for Exit
```

Sélectionner le mode "**S**" (mode standard) et valider par la touche "**Return**" pour entrer dans le menu de pré-configuration réseau.

L'écran affiche ensuite la pré-configuration réseau par défaut du système.

C'est à partir de cet écran, lors d'une première installation, que l'adresse définie permet d'accéder par la suite à l'exploitation de l'iPBX via le Web Admin, l'accès étant réalisé physiquement via le port **LAN** en face avant de la carte mère.

Dans le cas de séparation des flux Administration et Téléphonie, l'adresse indiquée dans cet écran sera dédiée au réseau Téléphonie en association avec celle définie pour le réseau Administration dans le menu suivant **ADMINISTRATION NETWORK**.

Concernant les accès physiques, dans ce cas, en face avant de la carte mère :

- Le port **LAN** est dédié au réseau Téléphonie,
- Le port **ETH2** est dédié au réseau Administration,

```
CONFIGURATION / NETWORK
*-----*

| ENTER IP ADDRESS: 192.168.65.1
| ENTER NETWORK MASK: 255.255.255.0
| ENTER GATEWAY: 192.168.65.254
*-----*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O)? Y
```

Répondre "**y**" et valider par la touche "**Return**" pour accéder aux différents champs.

- Renseigner successivement les paramètres réseau du système en utilisant la touche **Return** pour changer de ligne.

```
CONFIGURATION / NETWORK
*-----*

| ENTER IP ADDRESS: 10.100.40.150 |
| ENTER NETWORK MASK: 255.255.255.192 |
| ENTER GATEWAY: 10.100.40.129 |
*-----*
```

Suite à la validation de la dernière ligne, le résumé des paramètres réseau est ensuite affiché pour confirmation.

```
CONFIGURATION / NETWORK
*-----*

| RESUME |
| IPADR = 10.100.40.150 |
| NETWORKMASK = 255.255.255.192 |
| GATEWAY = 10.100.40.129 |
| NETWORKADR = 10.100.40.128 |
| BROADCAST = 10.100.40.191 |
*-----*
DO YOU CONFIRM (Y/N)? Y
```

Si le résumé n'est pas correct :

- Taper "**n**" pour recommencer la préconfiguration réseau

Si le résumé est correct :

- Taper "**y**" et valider par la touche "**Return**".

L'écran suivant permet la configuration d'un réseau supplémentaire et distinct pour les flux Administration.

```
DO YOU WANT TO CONFIGURE MANAGEMENT IP NETWORK? Y/[N]
```



Note : La configuration de séparation des réseaux peut être néanmoins réalisée ultérieurement à partir de Web Admin, Menu **SYSTEME>Configuration>Cartes>Parametres des cartes IP**.
Se référer au paragraphe 4.3

Dans le cas de Séparation des flux, répondre "**y**" et valider par la touche "**Return**".

L'écran affiche la configuration de séparation de flux pour l'accès réseau Administration au travers du connecteur ETH2 en face avant de la carte mère :

```
CONFIGURATION / ADMINISTRATION NETWORK
| ENTER ADMIN IP ADDRESS:
| ENTER ADMIN NETWORK MASK: |
| ENTER ADMIN GATEWAY: |
| ENTER ADMIN STATE (0/1):
*-----*
```

Renseigner successivement les paramètres du réseau dédié Administration en utilisant la touche Return pour changer de ligne.

Concernant la ligne **ENTER ADMIN STATE**:

- Le choix (1) permet une activation immédiate de la séparation de flux,
- Le choix (0) supprime la configuration renseignée précédemment.

Suite à la validation de la dernière ligne, le résumé des paramètres réseau est ensuite affiché pour confirmation.

```
CONFIGURATION / ADMINISTRATION NETWORK
| ADMIN IPADR = 20.100.42.121 |
| ADMIN NETWORKMASK = 255.255.255.192 |
| ADMIN GATEWAY = 20.100.42.65 |
| ADMIN NETWORKADR = 20.100.42.64 |
| ADMIN BROADCAST = 20.100.42.127
DO YOU CONFIRM (Y/N)? Y
```

Si le résumé n'est pas correct :

- Taper "**n**" pour recommencer la préconfiguration réseau.

Si le résumé est correct :

- Taper "**y**" et valider par la touche "**Return**".

Les étapes suivantes permettent de finaliser l'installation et ne concernent pas la séparation des flux (Se reporter au Manuel d'installation AMT/PTD/PBX/0058).

A la fin de la configuration par Ctrl + i, le système redémarre

- Raccorder le port **LAN** au réseau Téléphonie,
- Raccorder le port **ETH2** au réseau Administration

L'accès à le Web Admin s'effectuera donc à partir de l'URL (https://) définie pour l'Administration. L'accès sur le port LAN ne permet plus l'exploitation qui s'effectue désormais sur ETH2.



ATTENTION : Dans le cas ou le switch de raccordement au réseau Administration ne gère pas le cross-over (négociation émission/réception), il est impératif d'utiliser un câble croisé entre le Mitel 5000 Gateways ou Mitel 500 et ce switch.

Concernant le FireWall intégré au Mitel 5000 Gateways

Suite à cette configuration lors de la phase de Ctrl + i, le firewall sera configuré automatiquement pour le Mitel 5000 Gateways.

3.5 CONFIGURATION DES PARAMETRES IP DES RESEAUX TELEPHONIE ET ADMINISTRATION POUR UNE PREMIERE INSTALLATION MIVOICE 5000 SERVER

3.5.1 PRE-REQUIS

Le PC hébergeant le MiVoice 5000 server doit disposer de deux accès réseaux (un pour le réseau Administration, un pour le réseau Téléphonie).

Le MiVoice 5000 est installé et accessible par le Web Admin.

3.5.2 CONFIGURATION DES PARAMETRES IP DES RESEAUX TÉLÉPHONIE ET ADMINISTRATION

A partir de Web Admin, sélectionner le Menu **SYSTEME>Configuration>Cartes>Parametres des cartes IP**.

La liste des cartes IP déclarées s'affiche (dans le cas du MiVoice 5000 Server, il n'y a qu'une ligne).

- Sélectionner la ligne **0-00**,
- Dans l'écran suivant, cocher la case **Utilisation d'un reseau admin**,
- Entrer ensuite l'adresse IP du réseau Téléphonie dans le champ **Adresse IP** du haut (choix sur liste),
- Sous la ligne **Utilisation d'un reseau admin**, renseigner l'adresse IP du réseau Admin (champ – **adresse IP**),
- Cliquer sur **Confirmation**



Note : La configuration des autres champs n'est pas spécifique à la séparation des flux ; Se reporter au manuel d'exploitation du Web Admin (AMT/PTD/PBX/0080).

3.5.3 CONFIGURATION DU FIREWALL

Un Firewall est intégré à l'OS du MiVoice 5000 Server afin de répartir les flux de données.

Ce Firewall n'est pas configurable à partir de Web Admin.

La configuration du Firewall est sous la responsabilité de l'administrateur.

Vérifier que tous les ports nécessaires sont ouverts en se référant au paragraphe 6.2.

4 CAS D'UNE INSTALLATION EXISTANTE

4.1 PRE-REQUIS

Deux réseaux distincts sont opérationnels et communiquent via un ensemble Routeur/Firewall.

Si un serveur de téléchargement interne est actuellement utilisé, il ne doit plus être utilisé. Il doit être remplacé par un serveur de téléchargement externe pour la gestion des postes (TMA). Se référer au Manuel Installation des Postes - AMT/PTD/TR/0014.

4.2 PRINCIPALES ETAPES DE LA MISE EN ŒUVRE DE LA SEPARATION DE FLUX

Laisser dans cette première phase, le Firewall d'interconnexion, transparent.

Déplacer les équipements dédiés Administration du réseau TEL actuel vers le réseau Administration.

Les adresses doivent également être réaffectées (MiVoice 5000 Manager, DHCP, FTP, Annuaire LDAP, etc..).

Durant cette phase, l'administration et la Gestion des postes sont indisponibles.

Sur l'AX ou Mitel 500

Configurer la séparation des flux à partir de Web Admin (se référer au paragraphe 4.3-).

Sur Le MiVoice 5000 Server,

Deux accès réseaux doivent être opérationnels relativement aux deux réseaux.

La déclaration de l'adresse IP du réseau Administration est à effectuer à partir de Web Admin.

La Configuration du Firewall interne est effectuée en se référant à l'annexe.



Note : Concernant les Mitel 5000 Gateways, Mitel 500 et le MiVoice 5000 server, dans le cas où le réseau Administration est constitué de plusieurs sous-réseaux, définir les routes correspondantes (se référer au paragraphe 5 - Configuration des routes IP du réseau administration).

Sur le MiVoice 5000 Manager

Reconfigurer les adresses des sites. Se référer au document AMT/PTD/NMA/0040.

Sur le Routeur/Firewall d'interconnexion

Configurer le filtrage pour laisser passer les flux qui apparaissent surlignés dans le tableau 5.3.

Dans le cas où le réseau Administration est constitué de plusieurs sous-réseaux, définir les routes correspondantes (se référer au paragraphe 5).

4.3 CONFIGURATION DES PARAMETRES IP DES RESEAUX TELEPHONIE ET ADMINISTRATION SUR UNE INSTALLATION EXISTANTE MITEL 5000 GATEWAYS ET MITEL 500

A partir de Web Admin, sélectionner le Menu **SYSTEME>Configuration>Cartes>Parametres des cartes IP**.

La liste des cartes IP déclarées s'affiche (dans le cas du MiVoice 5000 Server, il n'y a qu'une ligne).

- Sélectionner la ligne 0-04
- Dans l'écran suivant, cocher la case **Utilisation d'un reseau admin**
- Entrer ensuite l'adresse IP du réseau Téléphonie dans le champ **Adresse IP** du haut,
- Sous la ligne **Utilisation d'un reseau admin**, renseigner l'adresse IP du réseau Admin (champs – **adresse IP/Masque/routeur**)
- Cliquer sur **Confirmation**.



Note : La configuration des autres champs n'est pas spécifique à la séparation des flux ; Se reporter au manuel d'exploitation du Web Admin (AMT/PTD/PBX/0080).

Suite à la configuration à partir du Web Admin

- Raccorder le réseau Téléphonie sur le port **LAN** en face avant de la carte mère,
- Raccorder le réseau Admin sur le port **ETH2** en face avant de la carte mère. Cette liaison permettra d'accéder au Web Admin.

4.4 CONFIGURATION DU FIREWALL

Un Firewall est intégré à l'OS du MiVoice 5000 Server afin de répartir les flux de données.

Ce Firewall n'est pas configurable à partir de Web Admin.

La configuration du Firewall est sous la responsabilité de l'administrateur.

Vérifier que tous les ports nécessaires sont ouverts en se référant au paragraphe 6.2.

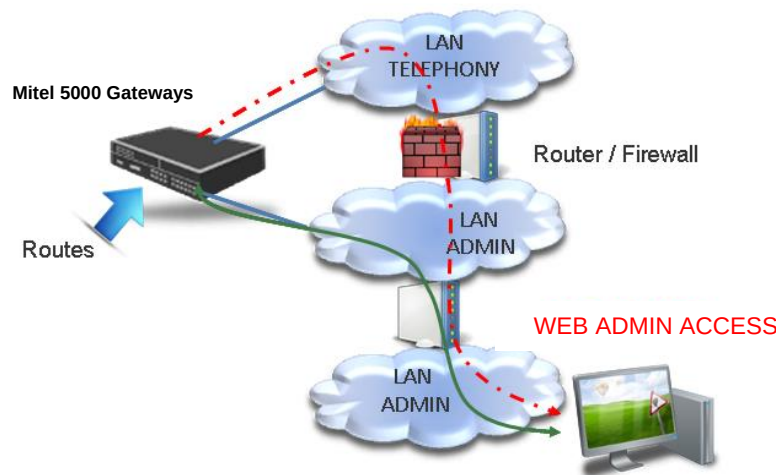
5 CONFIGURATION DES ROUTES IP DU RESEAU ADMINISTRATION

Lorsque le réseau Administration contient plusieurs sous réseaux, un poste client peut atteindre le Mitel 5000 Gateways ou le Mitel 500 sur le réseau d'administration par différentes routes (pour accéder à le Web Admin par exemple).

Il est donc nécessaire de définir une route pour atteindre ce client sinon le Mitel 5000 Gateways peut établir une route par le réseau de téléphonie. Parce qu'il ne sait pas que cette adresse de sous réseau (et la passerelle par défaut) utilisée est la passerelle de défaut du réseau de téléphonie.



Note : Donc, lors de la création des routes, on utilisera toujours la gateway du réseau d'administration. Dans le cas où les serveurs Web Admin, SNMP, ANNUAIRE EXT, SYSLOG, DATE&HEURE ne se trouvent pas dans le même réseau local (Admin), il faut déclarer les routes pour les atteindre.



- Le trait mixte rouge correspond à la route par défaut,
- Le trait continu vert correspond à la route une fois configurée.

5.1 CONFIGURATION DES ROUTES SUR LES MITEL 5000 GATEWAYS ET MITEL 500

Menu **SYSTEME>Configuration>Cartes>Routes ip du reseau admin**

- Cette commande n'est pas disponible pour le MiVoice 5000 Server.

ROUTE X : ADDRESS IP

X: 1 to 120.

Cette ligne permet de saisir l'adresse IP du sous réseau à joindre avec cette route.

Le système contrôle la syntaxe et présente le diagnostic d'erreur 'ERREUR SYNTAXE' si la valeur saisie n'est pas de la forme w.x.y.z, ou si 0.0.0.0 ou 255.255.255.255 est saisi.

Lors de la première saisie d'une adresse IP, le masque associé est forcé à 255.255.255.0.

Lors de l'effacement d'une adresse IP, le masque associé est effacé.

MASQUE

Cette ligne n'est présentée que si une adresse IP a été saisie pour cette route.

Cette ligne permet de saisir le masque qui définit la zone à joindre avec cette route.

Le système contrôle la syntaxe et présente le diagnostic d'erreur 'ERREUR SYNTAXE' si la valeur saisie n'est pas de la forme w.x.y.z, ou si 0.0.0.0 est saisi. De plus, la RHM contrôle que la valeur saisie est un masque de sous réseau, c'est-à-dire que les bits significatifs sont contigus et que le bit de poids

fort est à 1. Si ce n'est pas le cas, ou si le masque est effacé, le diagnostic d'erreur 'VALEUR INCORRECTE' est affiché.



Note : Le système, dans ce menu, ne contrôle pas si des plusieurs routes accèdent à la même zone (cas d'inclusions de réseau). Par contre le système supprimera les 'doublons' pour ne configurer que les routes nécessaires.

Jusqu'à 120 routes peuvent être créées (adresse IP et masque).

Les modifications sont prises en compte à la sortie du menu.

5.2 CONFIGURATION DES ROUTES SUR LE MIVOICE 5000 SERVER

Il faut être administrateur du serveur Linux.

La programmation du routage du réseau administration est à réaliser en utilisant la commande :

```
# route add -net xxx.xxx.xxx.xxx mask mmm.mmm.mmm gw ggg.gggg.ggg.ggg
```


6 ANNEXES

6.1 FLUX DE DONNEES POUR LA SOLUTION MIVOICE 5000

6.1.1 FLUX DE DONNEES CONCERNANT LES EQUIPEMENTS RELIES AU RESEAU DE TÉLÉPHONIE

Ce tableau donne la liste de flux de données dans la solution MiVoice 5000 R5.2 et relativement aux demandes effectuées par des équipements reliés au réseau de téléphonie.

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
i7xx	signalling	PBX/MiVoice 5000 Server (SERVIP)	I over IP (port 3199)	Tel
	configuration	DHCP server	DHCP	Tel
	software download	Download tool	TFTP	Tel
	voice flow	End points	RTP	Tel
Download tool	software download	i7xx	Proprietary (port 9410)	Tel
i2052 or i2070	Signaling i2052	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
	Signalling i2070	PBX/MiVoice 5000 Server (SERV-POWIN)	Gateway TCP/X.25	Tel
	configuration	PBX/MiVoice 5000 Server (EAI)	Gateway TCP/X.25	Admin
	directory	LDAP directory	LDAP read only	Admin
	date & time	PBX/MiVoice 5000 Server (NTP server)	NTP	Tel
	voice flow (i2052 only)	End points	RTP	Tel
MiVoice 5300 IP Phone	signalling	PBX/MiVoice 5000 Server(GSI or proxy)	extended SIP (18060)	Tel
	software download	FTP server	FTP	Admin
	configuration	DHCP server	DHCP	Tel
	voice flow	End points	RTP	Tel
Mitel 6700 SIP Phone	signalling	PBX/MiVoice 5000 Server(GSI or proxy)	SIP (5060)	Tel
	software download	FTP - TFTP server	FTP – TFTP	Admin and Tel
	configuration	DHCP server	DHCP	Tel
	telephony services	PBX/MiVoice 5000 Server (XML proxy)	Proprietary http / https	Tel
	date & time	PBX/MiVoice 5000 Server (NTP server)	NTP	Tel
	voice flow	End points	RTP	Tel
SIP phone & WiFi	signalling	PBX/MiVoice 5000 Server (GSI)	SIP (5060)	Tel
	voice flow	End points	RTP	Tel

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
SIP Trunk	signalling	PBX/MiVoice 5000 Server (GSI)	SIP (5060)	Tel
	voice flow	End points	RTP	Tel
H.323 Trunk	signalling	PHM	H.323 (H.225/H.245)	Tel
	voice flow	End points	RTP	Tel
PHM	PHM - signalling	PBX/MiVoice 5000 Server	TCP/X.25 (port 3208)	Tel
DECT-IP application	Mitel OMM – signalling	PBX/MiVoice 5000 Server (GSI)	Extended SIP	Tel
	Mitel OMM – resiliency	Mitel OMM	proprietary	Tel
	Mitel OMM – directory	LDAP directory	LDAP read only	Admin
	Mitel OMM – terminal list	PBX/MiVoice 5000 Server (Web Admin)	https	Admin
	Mitel RFP – configuration	DHCP server	DHCP	Tel
	Mitel RFP – voice flow	End points	RTP	Tel
NAT SBC PROXY	signalling	PBX/MiVoice 5000 Server (GSI)	Extended SIP (5060&5064)	Tel
	Mitel RFP – voice flow relay	End points	RTP	Tel
PBX/MiVoice 5000 Server	Multisite signalling	PBX/MiVoice 5000 Server (SERGIC)	Movacs (tunnel 1998)	Tel
	Multisite signalling	PBX/MiVoice 5000 Server (SERGIC)	TLS	Tel
	MiVoice 5000 Server redundancy	MiVoice 5000 Server	Heartbeat	Tel
	PBX redundancy	PBX XD	DRBD	internal
	Test	PBX/MiVoice 5000 Server (AFISER)	TCP/X.25 (port 3302)	Tel
	VOIP voice flow	End points	RTP	Tel
	E-voicemail	Mail server	SMTP/POP3/IMAP4	Tel
	TMA set configuration	Mitel 6700 SIP Phone & MiVoice 5300 IP Phone web page	HTTP	Tel
User PC	White pages	PBX/MiVoice 5000 Server	HTTP	Tel
	Self admin	MiVoice 5000 Manager	https	Admin
	Mail application	Mail server	SMTP/POP3/IMAP4	Tel
	Mitel OMM - configuration	Mitel OMM application	Telnet, HTTP, TFTP	Tel
TAPI application	signalling	TAPI gateway	Proprietary (port 5001)	Tel
TAPI gateway	TAPI gateway signalling	PBX/MiVoice 5000 Server (TAPI)	Gateway TCP/X.25	Tel

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
Alarm station	signalling	M7900 alarm server	Port com emulation	Tel
M7900 alarm server	signalling	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
CC	signalling	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
	CTI	PBX/MiVoice 5000 Server (CSTA)	Gateway TCP/X.25	Tel
	voice flow	End points	RTP	Tel
	Directory	LDAP directory	LDAP read only	Admin
	Miscellaneous Client Server relations		HTTP, DCOM, file sharing	Tel
TWP	signalling	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
	CTI	PBX/MiVoice 5000 Server (CSTA)	Gateway TCP/X.25	Tel
	media flow (voice, visio)	End points	RTP	Tel
	Directory	LDAP directory	LDAP read only	Admin
	CTI	User station	https	Tel
UCP	signalling	PBX/MiVoice 5000 Server	VTI/XML (port 3199)	Tel
	CTI	PBX/MiVoice 5000 Server (CSTA)	Gateway TCP/X.25	Tel
	voice flow	End points	RTP	Tel
	Directory	LDAP enterprise database	LDAP read only	Admin
	Fax downloading		FTP	Tel
	Miscellaneous		VPIM/SMTP/POP3 IMAP/RPC/HTTP/https	Tel
Remote user via ISDN/PPP	all	all	all	PPP
Most of the equipment	Log information	Support team equipment	Syslog (514)	Admin

6.1.2 FLUX DE DONNEES CONCERNANT LES EQUIPEMENTS RELIES AU RÉSEAU ADMINISTRATION

Ce tableau donne la liste de flux de données dans la solution MiVoice 5000 R5.2 et relativement aux demandes effectuées par des équipements reliés au réseau Administration.

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
MiVoice 5000 Manager	Directory synchro.	Active directory	LDAP	Admin
	Directory replication	MiVoice 5000 Server	LDAP	Admin
	Supervision	SNMP manager	SNMP (trap)	Administration
	Polling	PBX/MiVoice 5000 Server (agent SNMP)	SNMP (get)	Administration

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
	File transfer (CDR/billing)	PBX/MiVoice 5000 Server (Web Admin)	https	Admin
	PBX/MiVoice 5000 Server configuration	PBX/MiVoice 5000 Server (Web Admin)	https (XML)	Admin
		MiVoice 5000 Manager clients	Proprietary (44555)	Admin
	MiVoice 5000 Manager clients	PBX/MiVoice 5000 Server – VT100	Proprietary (8201)	Admin
	Date & time	NTP server	NTP	Administration
	Alarm	SMTP server	SMTP	Administration
	UCP configuration	UCP	Proprietary (13888)	Admin
MiVoice 5000 Manager client	Management	MiVoice 5000 Manager	https (apache server)	Admin
	PBX/MiVoice 5000 Server VT100&MMI	Via MiVoice 5000 Manager	proprietary(8201/8220)	Admin
	PBX/MiVoice 5000 Server configuration	Via AM7430	vnc client (5800/5809)	Admin
	Synoptic Nagios	PBX/MiVoice 5000 Server	https	Admin
	Synoptic Nagios	AM7430	HTTP	Admin
PBX/MiVoice 5000 Server	SNMP agent	MiVoice 5000 Manager & other managers	SNMP	Admin
	Maintenance	SNMP managers	PPP (via ISDN)	PPP
	MiVoice 5000 Server redundancy	MiVoice 5000 Server	Heartbeat	Admin
	MiVoice 5000 Server redundancy	MiVoice 5000 Server	DRBD	Admin
	Directory	LDAP directory	LDAP	Admin
	White pages	LDAP directory	LDAP	Admin
	Date & time	NTP server	NTP	Admin
User PC	GDB application	PBX/MiVoice 5000 Server (debug)	Proprietary (port 1005)	Admin
	Operator	PBX/MiVoice 5000 Server (Web Admin)	https	Admin
	Operator	PBX/MiVoice 5000 Server (Linux)	SSH	Admin
	White pages	PBX/MiVoice 5000 Server	HTTP	Tel
	Self admin	MiVoice 5000 Manager	https	Admin
	Mail application	Mail server	SMTP/POP3/IMAP4	Tel
	Mitel OMM - configuration	Mitel OMM application	Telnet, HTTP, TFTP	Tel
CDR/Billing	Data transfer	PBX/MiVoice 5000 Server (MUFAX or KITAXE)	Gateway TCP/X.25	Admin
	File transfer	MiVoice 5000 Manager	https	Admin
	directory	LDAP directory	LDAP read only	Admin
	configuration	PBX/MiVoice 5000 Server	Gateway TCP/X.25	Admin

EQUIPMENT	DEPARTMENT	REMOTE EQUIPMENT	PROTOCOL	NETWORK
(EAI)				
TMA	Terminal management	FTP server	FTP	Admin
	PBX/MiVoice 5000 Server configuration	PBX/MiVoice 5000 Server (Web Admin)	https (XML)	Admin
AM7430	PBX configuration	PBX/MiVoice 5000 Server in R4.2 or previous	Proprietary (TCP/X.25)	Tel

6.2 PROTOCOLES SUPPORTES

6.2.1 PROTOCOLES EN ENTREE SUPPORTES PAR LE RESEAU TÉLÉPHONIE

PORTS DE DESTINATION	PROTOCOLES	PROTOCOLES APPLI	SERVICES
13	TCP	DAYTIME	Mise à l'heure IPS
68	UDP	DHCP	Configuration Terminal
69	UDP	TFTP	Transfert de fichier
80	TCP	HTTP	Service Annuaire
123	UDP	NTP	Date et heure
694	UDP		Heartbeat
1998	TCP	SERGIC Tunnel	Signalisation Multisite MOVACS
2000 à 3196			Non assigné
3197	TCP	HTTP	XML Proxy
3198	TCP	CRI	
3199	TCP	CRI / VTI-XML (propriétaire)	Signalisation Terminaux
3207	TCP		Réservé
3208	TCP	TPKT	H.323 Serveur (pour H.323/MOVACS gateway)
3209	TCP	TPKT	Gateway Server pour Attendant Console et Software phone sur PC (TD/PC)
3210	TCP		Réservé
3211	TCP	CSTA	CSTA Server
3212 à 3216	TCP	CSTA	Réservé
3220 à 3283	TCP	TPKT	Serveur interne appelé par TAPI Gateway
3284 à 3287	TCP		Réservé
3292 à 3299	TCP		Reservé si plus de ports sont nécessaires pour un serveur (dans le cas d'une fournissant plusieurs CCUs)
3300	TCP		Réservé
3301	TCP	TPKT	CSTA Server (identique à 3211 mais mode TPKT)
3302	TCP	TPKT	AFISER Server (echo service)
3303	TCP	Non D	AFISER Server (echo service)
3305 à 3399	TCP	CSTA	Réservé
3600 à 7999	TCP	CSTA	Non assigné
3998	TCP	MOVACS over TLS	MOVACS Multisite signaling
4443	TCP	HTTPS	Proxy XML pour Mitel 6700 SIP Phone
5060	UDP	SIP	Signalisation SIP
5061	TCP	SIP	Signalisation SIP
5062	TCP	SIP	Signalisation SIP
5063	UDP	SIP	Signalisation SIP
5160	UDP	SIP	Signalisation SIP

PORTS DE DESTINATION	PROTOCOLES	PROTOCOLES APPLI	SERVICES
5161	UDP	SIP	Signalisation SIP
5162	UDP	SIP	Signalisation SIP
5163	UDP	SIP	Signalisation SIP
8001 à 65534	TCP		Non assigné

6.2.2 PROTOCOLES EN ENTREE SUPPORTES PAR LE RÉSEAU ADMINISTRATION

PORTS DE DESTINATION	PROTOCOLES	PROTOCOLES APPLI	SERVICES
20	TCP	FTP	
21	TCP	FTP	Transfert de fichier
22	TCP	SSH	Accès distant
80	TCP	HTTP	Pages blanches et XML Proxy
161	UDP	SNMP	Supervision et synoptique
162	UDP	SNMP	Supervision et synoptique
389	TCP	LDAP	Annuaire
636	TCP	LDAPS	Accès sécurisé à l'annuaire
443	TCP	HTTPS	Transfert de fichier et Configuration
514	UDP	SYSLOG	Log information
694	UDP		Heartbeat
1005	TCP	GDB	Application GDB (Debugger)
2222	TCP	SSH	RHM VT100
3200 à 3204	TCP	propriétaire	KITAXE
3206, 3218 et 3219	TCP	propriétaire	IAE
3217, 3288, 3291, 3304			
	TCP	propriétaire	MUFACT
3302 à 3303	TCP	propriétaire	AFISER
3400 à 3599	TCP	propriétaire	Plages réservées

6.2.3 PROTOCOLES AUTORISES DEPUIS LE RESEAU ENTREPRISE VERS LE RÉSEAU ADMIN

Le firewall externe doit laisser passer les protocoles suivants depuis le réseau Entreprise vers le réseau Admin :

Ce FireWall doit être configuré en mode d'inspection (STATEFULL).

PORTS DE DESTINATION	PROTOCOLES	ADRESSE SOURCE AUTORISEE	PROTOCOLES APPLI	SERVICES
20	TCP	Toutes	FTP	
21	TCP	Toutes	FTP	Transfert de fichier
389	TCP	Toutes	LDAP	Annuaire
636	TCP	Toutes	LDAPS	Accès sécurisé à l'annuaire
443	TCP	Adresse PC client	HTTPS	Mitel OMM
443	TCP	Adresse PC client	HTTPS	Self admin (Mitel Phone suite)
514	UDP		SYSLOG	Log Information

