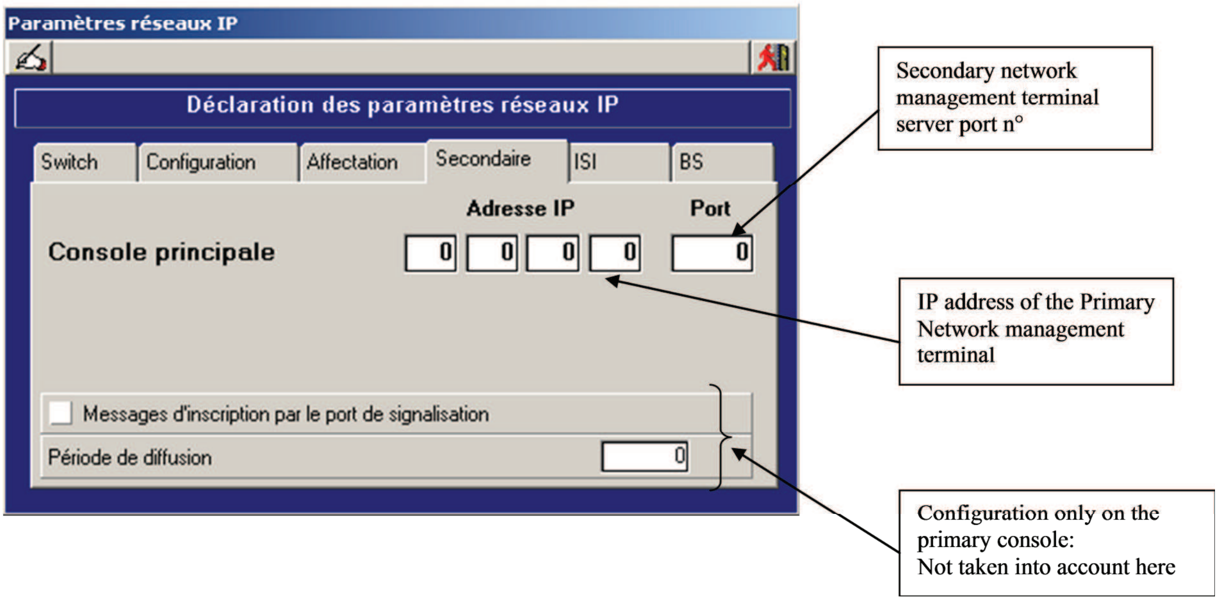
### 8.3.7.4 Network management terminal configuration



Déclaration des paramètres réseaux IP

Console principale — Adresse IP: 0 . 0 . 0 . 0 — Port: 0

□ Messages d'inscription par le port de signalisation

Période de diffusion: 0

Secondary network management terminal server port n°

IP address of the Primary Network management terminal

Configuration only on the primary console:
Not taken into account here

## *8.4 Multi-site and multi network management terminal*

### *8.4.1 PRESENTATION*

Our networks can have N independent sites interconnected using IP (Attention, here we are not talking about ISI protocol interconnection).
Each site has its own SWITCH and the sites are linked together using IP.
Each site has its own primary network management terminal connected using RS232 to the site SWITCH.
The diagram representing this is shown below:

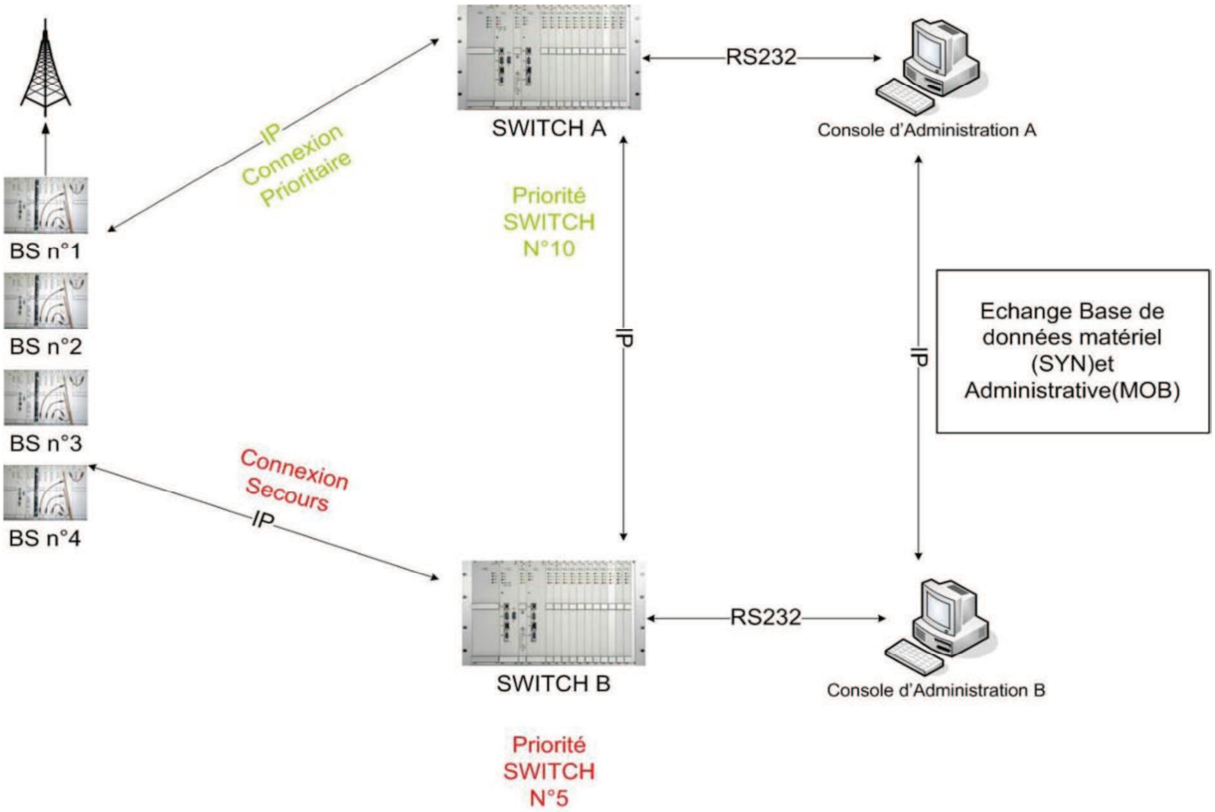


Fig 1

SWITCHES have a priority n° and the two SWITCHES are always active on the network.
This priority level is broadcast over the identification channel (see §9.3.4.1).
The highest priority SWITCH always manages the network. The others are secondary and backup.

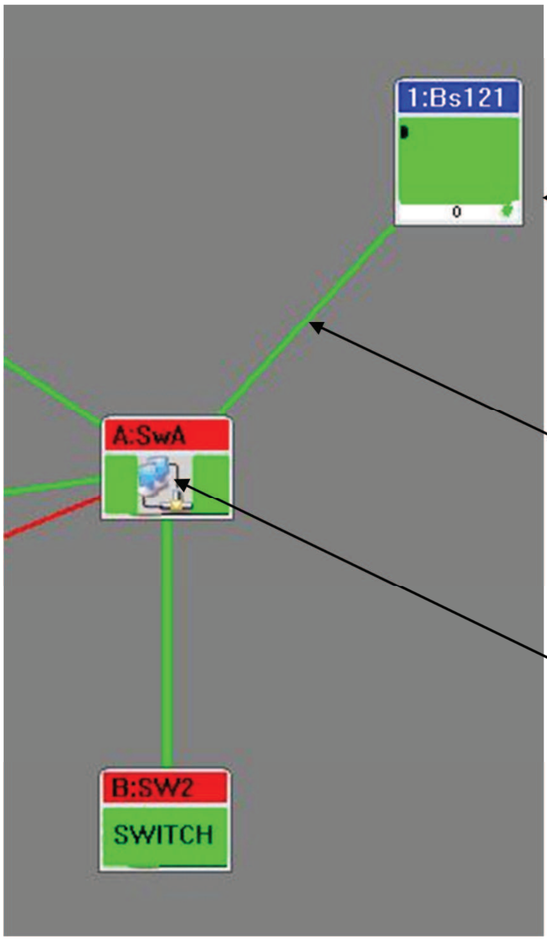
The interest is that if the link between the two sites is cut, both sites will operate independently.
This architecture also allows for a remote refresh of the technical and administrative databases on each site using a basic download.

Example: We modify the SWA-CSA site, we can either refresh the CSB or update the CSB-SWB set.

### *8.4.2 NETWORK SETTING*

We are going to parameter the network shown in Fig1.

The network management terminal synopsis will be the same whatever the site.
Below is shown the synopsis for network management terminal



The Console A synopsis shows:

SWICTH A called SwA
SWITCH B called Sw2
1 BS called Bs121

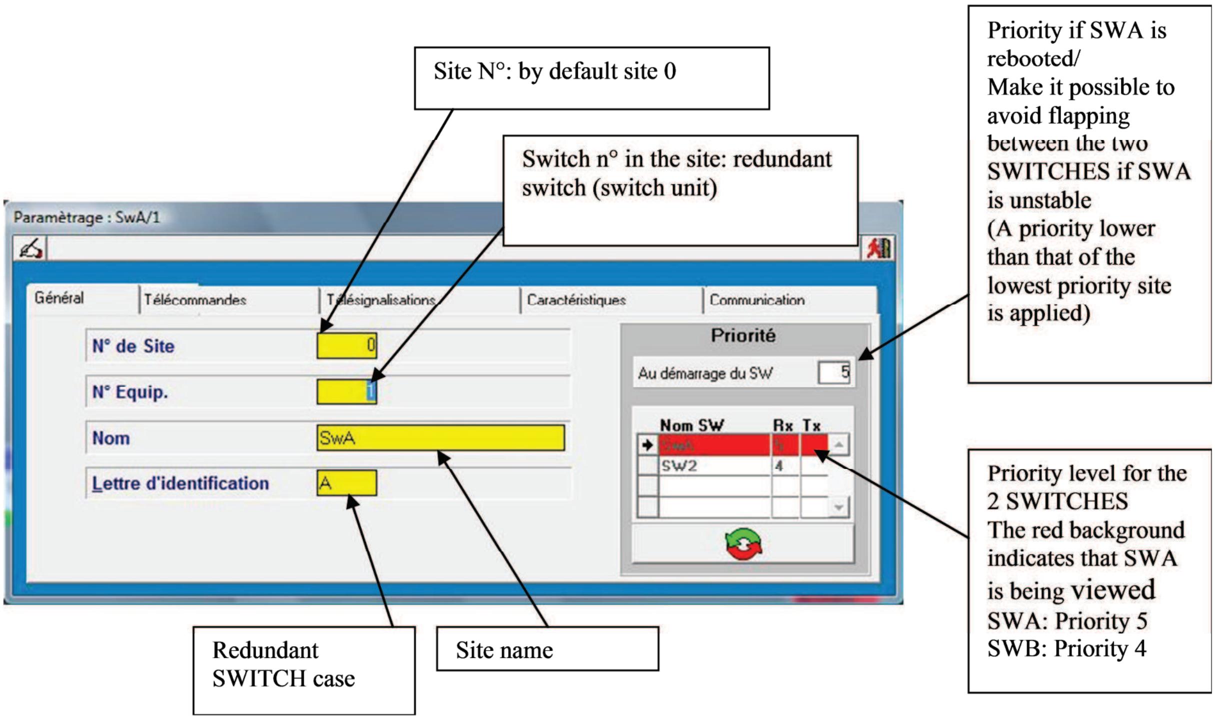
All these elements are connected using IP

The green lines converge towards SWITCH A, it is therefore active

The display of this image on the green SWITCH A background indicates that Console A is connected to SwA

### 8.4.2.1 Sites configuration

Below SWITCH A is parametered
In conf/param right click,Name tc ts



Paramètrage : SwA/1

N° de Site: 0

N° Equip.: 1

Nom: SwA

Lettre d'identification: A

Priorité

Au démarrage du SW: 5

| Nom SW | Rx | Tx |
|---|---|---|
| SwA | 5 | |
| SW2 | 4 | |

Site N°: by default site 0

Switch n° in the site: redundant switch (switch unit)

Priority if SWA is rebooted/
Make it possible to avoid flapping between the two SWITCHES if SWA is unstable
(A priority lower than that of the lowest priority site is applied)

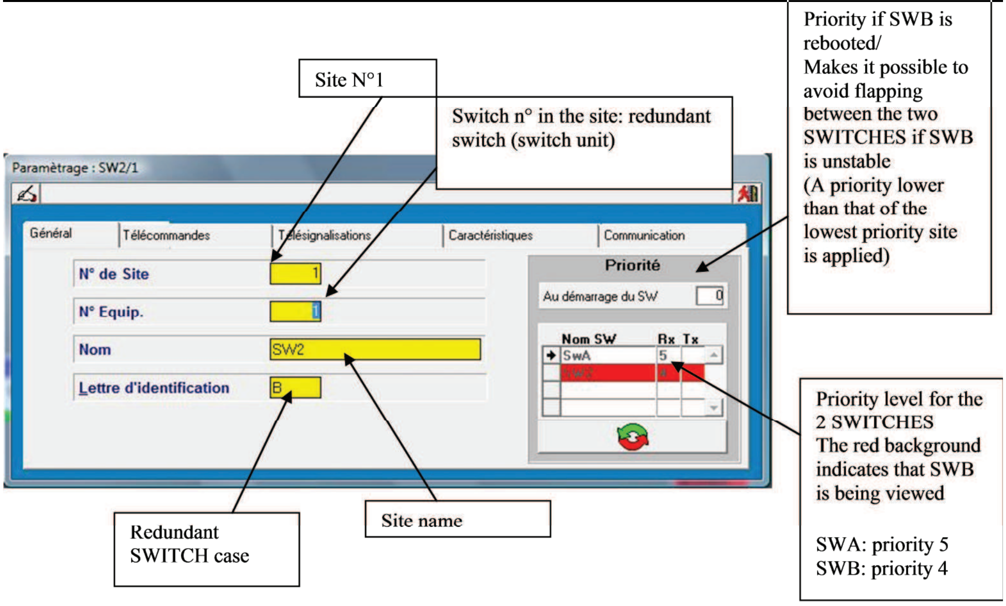
Priority level for the 2 SWITCHES
The red background indicates that SWA is being viewed
SWA: Priority 5
SWB: Priority 4

Redundant SWITCH case

Site name

Below SWITCH B is parametered
In Conf/param right click,Nom tc ts

[redacted]



Paramètrage : SW2/1

N° de Site: 1

N° Equip.: 1

Nom: SW2

Lettre d'identification: B

Priorité

Au démarrage du SW: 0

| Nom SW | Rx | Tx |
|---|---|---|
| SwA | 5 | |
| SW2 | 4 | |

Site N°1

Switch n° in the site: redundant switch (switch unit)

Priority if SWB is rebooted/
Makes it possible to avoid flapping between the two SWITCHES if SWB is unstable
(A priority lower than that of the lowest priority site is applied)

Priority level for the 2 SWITCHES
The red background indicates that SWB is being viewed

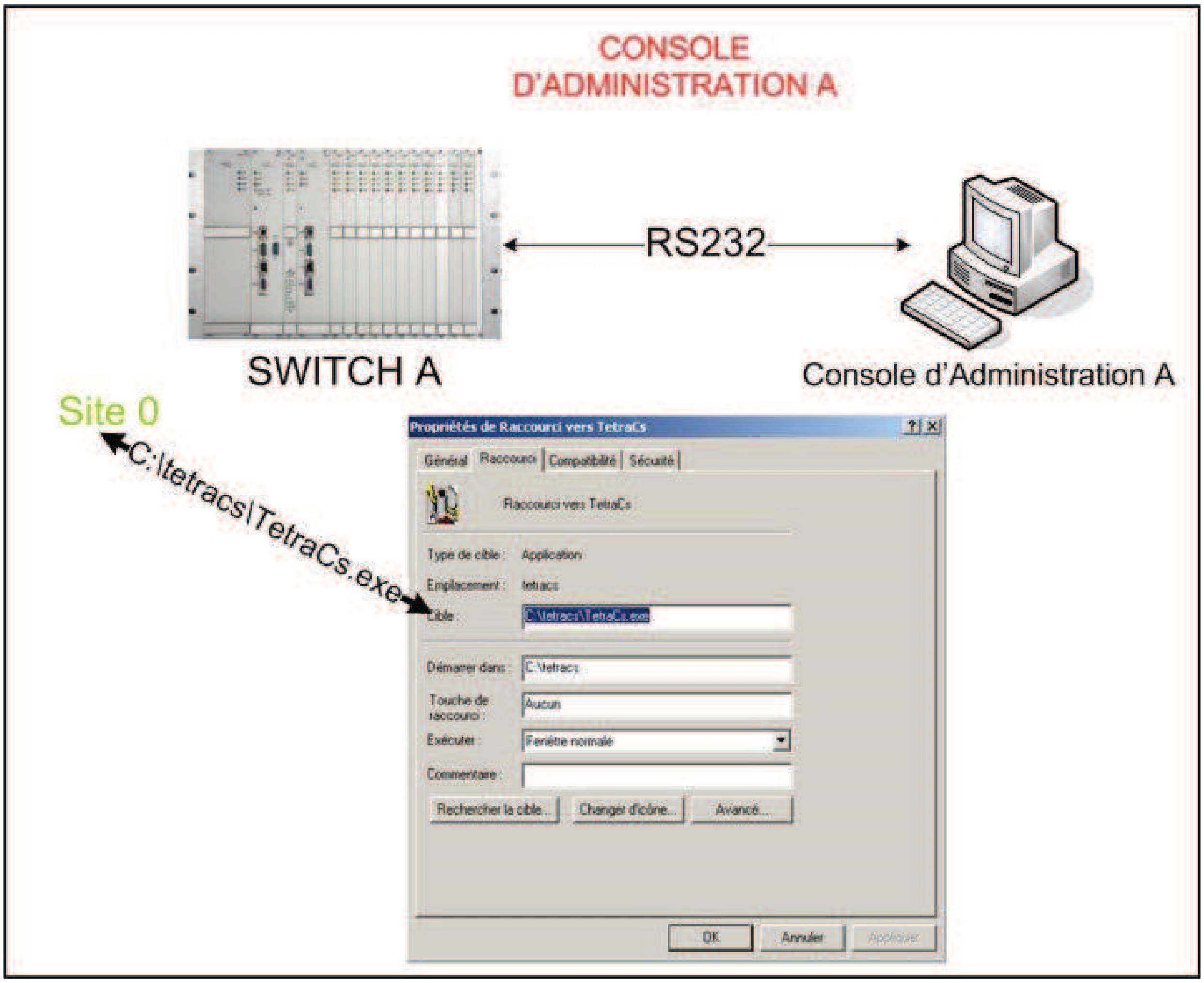
SWA: priority 5
SWB: priority 4

Redundant SWITCH case

Site name

### 8.4.2.2 Starting up the different network management terminal

Each network management terminal is started up depending on the connection site N° (see previous chapter).
The target of the Tetracs short cut properties must be modified for each site (See below).



Type de cible : Application

Emplacement : tetracs

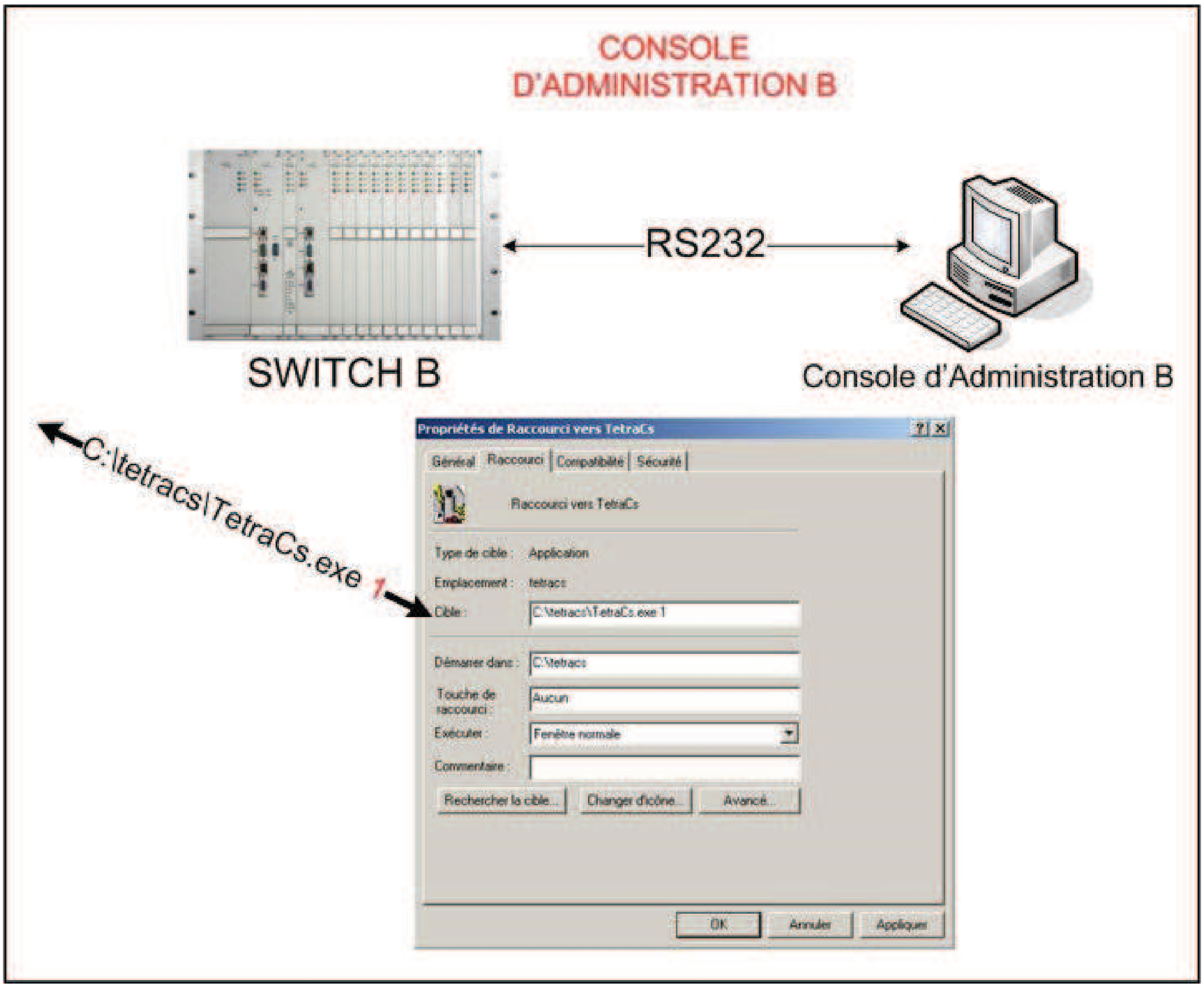
Cible : C:\tetracs\TetraCs.exe

Démarrer dans : C:\tetracs

Touche de raccourci : Aucun

Exécuter : Fenêtre normale

Commentaire :



Raccourci vers TetraCs

Type de cible : Application

Emplacement : tetracs

Cible : C:\tetracs\TetraCs.exe 1

Démarrer dans : C:\tetracs

Touche de raccourci : Aucun

Exécuter : Fenêtre normale

Commentaire :

# 9. CPUBDT SOFTWARE AUTHENTICATION (Level 2)

## 9.1 The authentication network management terminal

The authentication network management terminal is software the purpose of which is to authenticate equipment manufactured by Etelm using different means of communication. Without this authentication the equipment cannot operate correctly. It consists in the retrieval of an encrypted key by the network management terminal software and its transmission to the equipment on order to unblock it.

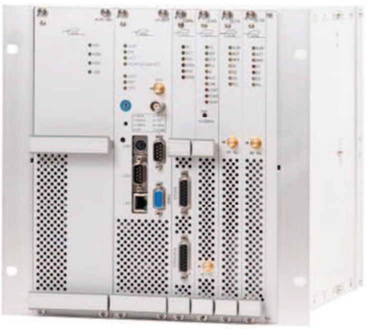
There are two authentication methods which are: automatic and manual. One uses internet and is automatic, the other involves calling Etelm and manually entering the encryption key. Once the software key is in the software network management terminal, it must be sent to the equipment to be identified either via a network cable or by a crossed serial cable.

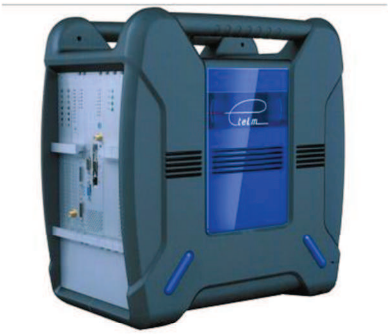
## 9.2 Use

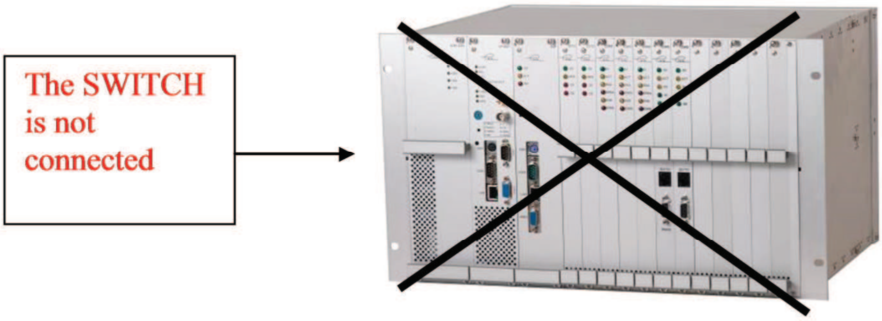
The Etelm equipment authentication is needed in several situations:

- New equipment
- Expired validity date
- Major upgrade

The authentication procedure only concerns the equipment below.





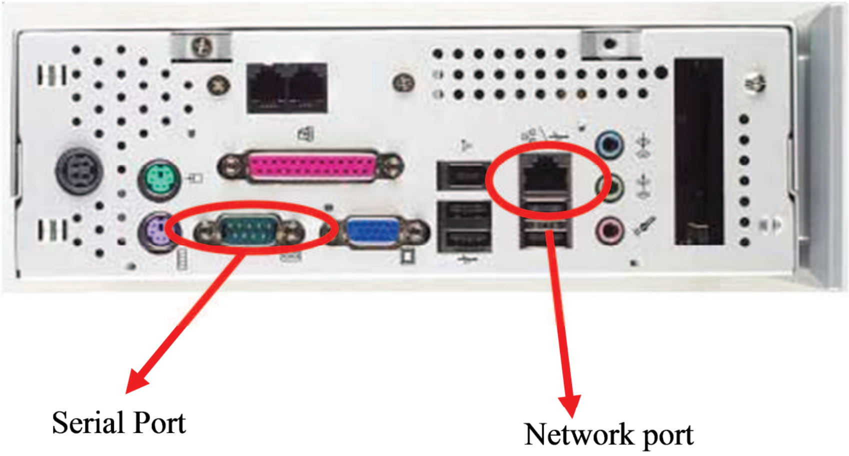


The SWITCH is not connected

# 9.3 Integration

## 9.3.1 Equipment

The software is installed on any PC, preferably a laptop, so that it can be used close to the equipment to be authenticated (especially if a direct connection is to be made). The PC must have either a serial port or a network port (which is true for the majority of PCs, even older ones, see images) or, of course, both.



Physical locations of the network and serial ports

## 9.3.2 Software

The authentication network management terminal software is compatible Windows 2000, XP, Vista and 7. It can be installed in any directory. It contains an executable (which must be authorised to dialogue on the network by the firewall) and a mandatory library file.

# 9.4 Presentation

## 9.4.1 Why authenticated?

The authentication of Etelm equipment is used to protect them from any unauthorised product copy. The referencing makes it possible to better control the distributed software especially with regards to quantities, versions, validity periods, sites... which brings special help for maintenance. To do this each appliance and software must be recognised and identified before operation becomes possible.

## 9.4.2 What is authenticated?

Authentication only applies to base stations. Only recent versions are concerned.

## 9.4.3 When to authenticate?

As explained above, authentication is needed for all new equipment, in order to renew a key or to carry out a major upgrade.

## 9.4.4 New equipment

Equipment can be delivered authenticated or not depending on the case. If an Etelm appliance has never operated and never been referenced it must be authenticated and unblocked in order to be fully and correctly operational. To do this the appliance must be installed in its environment and configured. Next the procedure should be launched using the authentication network management terminal using the correct settings.

## 9.4.5 Validity period

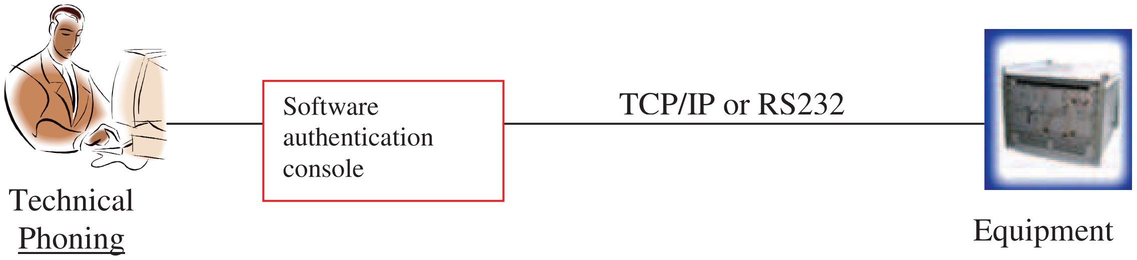
Etelm An installed Etelm appliance which is operational and referenced has an associated validity date key. When the date expires the equipment is blocked. The equipment must be re-authenticated in order to be used again. To do this, run the procedure as if new equipment were being installed after having contacted Etelm to extend the expiry date.

## 9.4.6 Upgrade

When an upgrade is available its installation invalidates the authentication. A procedure must therefore be launched from the authentication network management terminal in order to unblock the equipment again (after the upgrade).

# 9.5 How to authenticate?

## 9.5.1 Authentication by phone

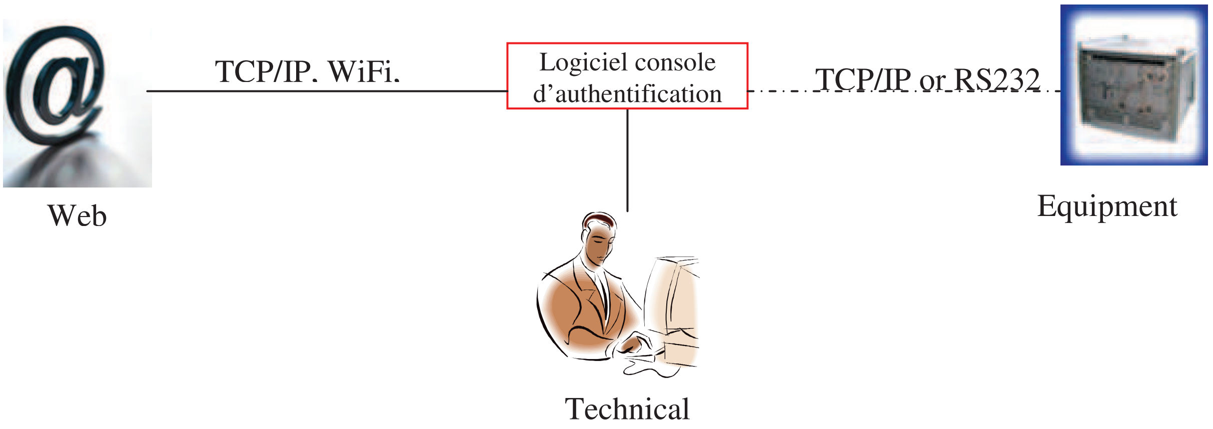


Architecture of phone authentication

As can be seen here, the authentication will be carried out by a technician in the authentication centre or at the customer site who, in exchange for a first software number supplied by the equipment to be authenticated, will receive a new number depending on the unblocking authorisation managed by Etelm.

Compared to Internet authentication the procedure is exactly the same except that the serial number is supplied orally and not via internet. This liberates from network and router issues.

## 9.5.2 Internet authentication



Internet authentication architecture

As above, authentication is carried out by a technician from the authentication centre or the customer who will use another menu on the authentication network management terminal. It must be connected to Internet and the equipment at the same time. If this is not possible the new software key can be retrieved directly from the Internet and the equipment authenticated using the technique described in the previous paragraph.

# *9.6 Handling*

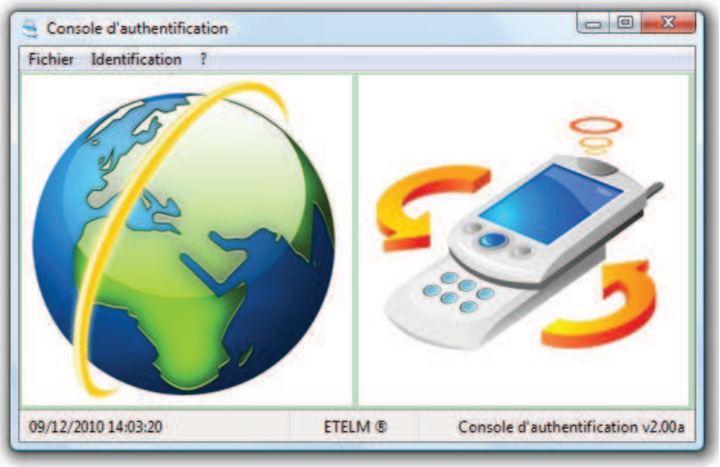
## *9.6.1 General*

### 9.6.1.1 Introduction

The authentication network management terminal is used to authenticate via internet i.e. to reference and unblock equipment manufactured by Etelm. After having entered the parameters, either the network management terminal connects to the authentication centre and downloads a new key to replace the old one, or the new key is entered manually after having been exchanged for the old key by phone. The network management terminal then sends the key to the equipment via the network or the RS232 port (serial) depending on the user's choice.

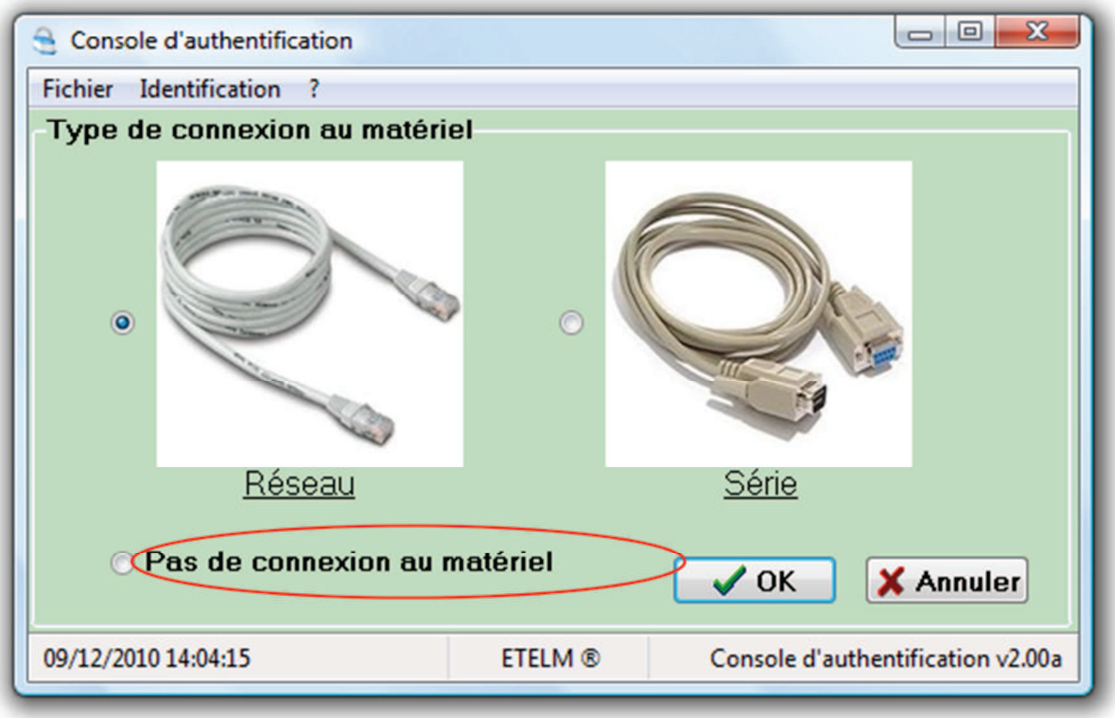
### 9.6.1.2 Procedure

When the network management terminal is launched the following window appears. A menu gives access to a few settings such as the language, help or the choice of the authentication technique. Clicking on the image either launches automatic authentication (the globe) or manual authentication (the telephone).



Automatic or manual authentication choice menu

Whatever the previous selection, the following window is displayed (except for what is outlined in red which only appears for automatic authentication):



Console d'authentification
Fichier
Identification
?
Type de connexion au matériel
Réseau
Série
Pas de connexion au matériel
OK
Annuler
09/12/2010 14:04:15
ETELM ®
Console d'authentification v2.00a

Menu to select the communications protocol between the network management terminal and equipment.

The media used to communicate with the new equipment must be selected. The choice is made by clicking on the image and validating using OK. Cancel returns to the previous menu. Next, depending on the automatic or manual authentication choice, a different window appears.

The "no connection to the equipment" menu specific to automatic authentication is used to retrieve a new key via internet in exchange for the old key without necessarily being connected to the equipment. The procedure is divided into several steps.

## 9.7 Manual authentication (by phone)

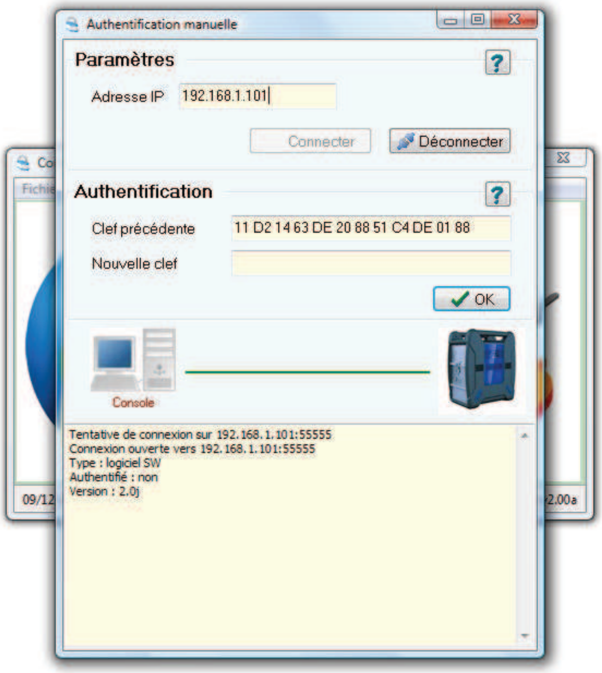
### 9.7.1.1 Network connection to the equipment

This software will therefore make it possible to authenticate equipment by phoning Etelm (or downloading a key via internet). First the parameters must be configured. To do this, enter the equipment IP address (which should belong to the same sub-network as the authentication network management terminal if using a switch or a router...) and the communications port.

To finish click on the "connect" button and the network management terminal attempts to retrieve the key.

A small window shows the status of events (connection, disconnection and error). The diagram shows a network management terminal and a BS connected by a cable. The cable is green when connected and red otherwise. In the following case the connection succeeded (in the window and the cable is green) and the old key is shown in the "previous key" field. Typically the authentication network management terminal waits for the new key in order to send it to the equipment.

In the progress window (at the bottom) there are several items that can be very useful. The type of software that can be used to make sure there is no error, the version is used to know if the software is up to date and finally if the equipment is already authenticated. In the example below a TETRA version 2.0j switch has already been authenticated.



Adresse IP 192.168.1.101

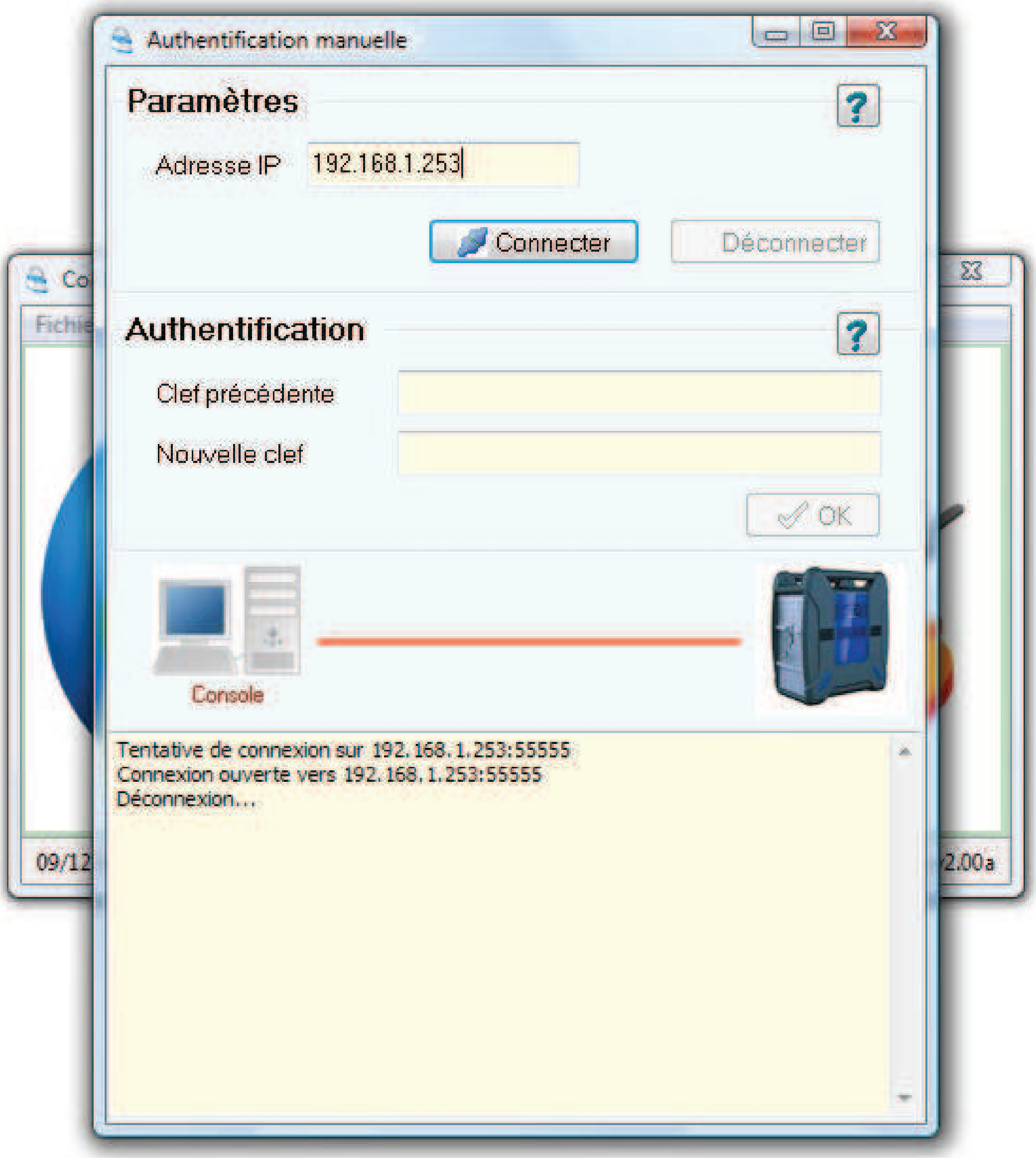
Clef précédente 11 D2 14 63 DE 20 88 51 C4 DE 01 88

Nouvelle clef

```
Tentative de connexion sur 192.168.1.101:55555
Connexion ouverte vers 192.168.1.101:55555
Type : logiciel SW
Authentifié : non
Version : 2.0j
```

Manual authentication menu using a network cable

In the following case the connection attempt has failed because the equipment has not responded at address 192.168.1.253:

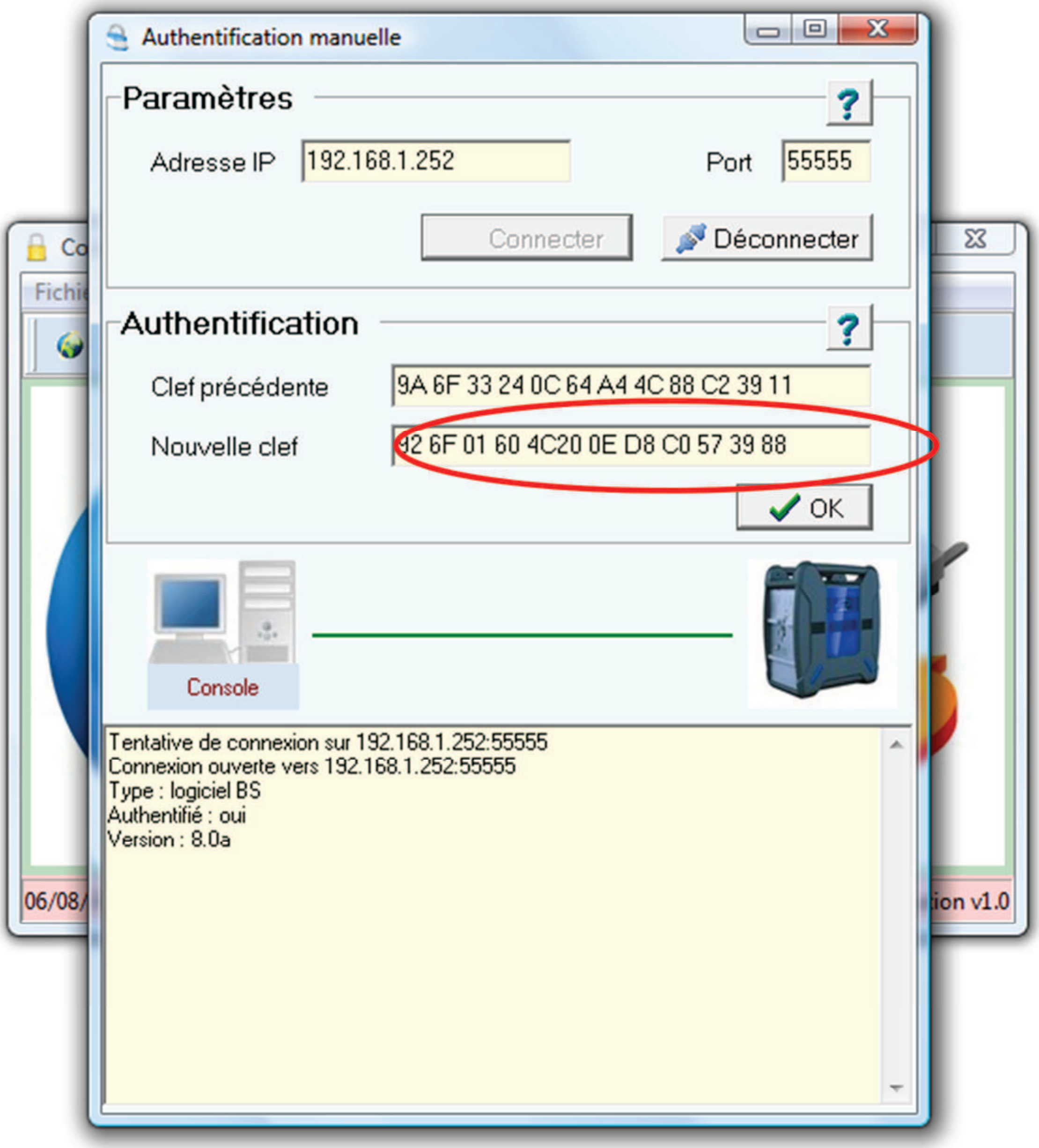


```
Tentative de connexion sur 192.168.1.253:55555
Connexion ouverte vers 192.168.1.253:55555
Déconnexion...
```

Connection failed

Once the old software key has been obtained either:

- Communicate it (with the corresponding customer identifiers) by phone to the authentication centre (Etelm) which will supply a new key corresponding to the customer's remaining credit.
- Or send it via the automatic authentication menu without connecting to the equipment (with the supplied customer identifiers).



Adresse IP 192.168.1.252

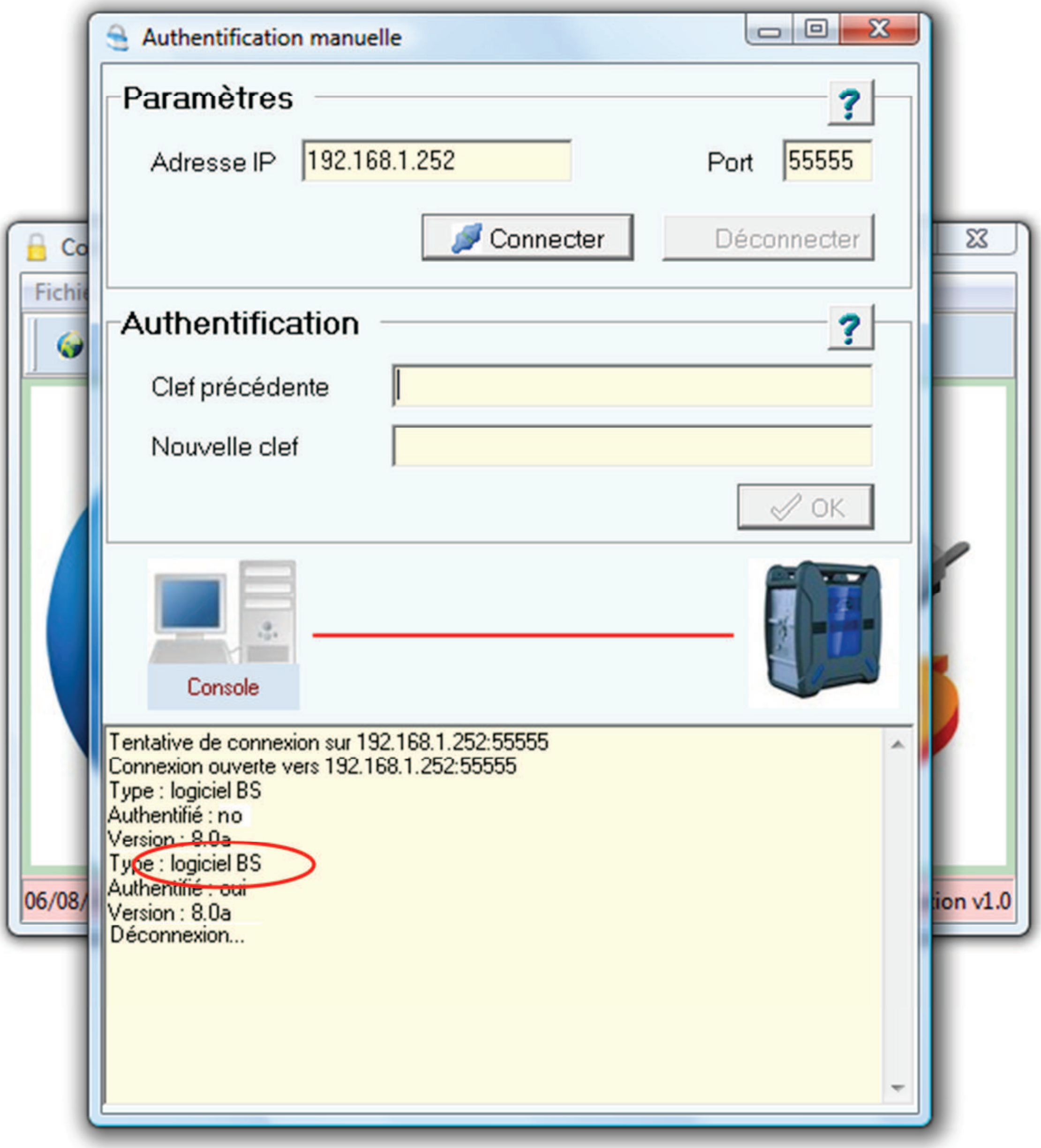
Port 55555

Clef précédente 9A 6F 33 24 0C 64 A4 4C 88 C2 39 11

Nouvelle clef 92 6F 01 60 4C20 0E D8 C0 57 39 88

```
Tentative de connexion sur 192.168.1.252:55555
Connexion ouverte vers 192.168.1.252:55555
Type : logiciel BS
Authentifié : oui
Version : 8.0a
```

Enter the new key



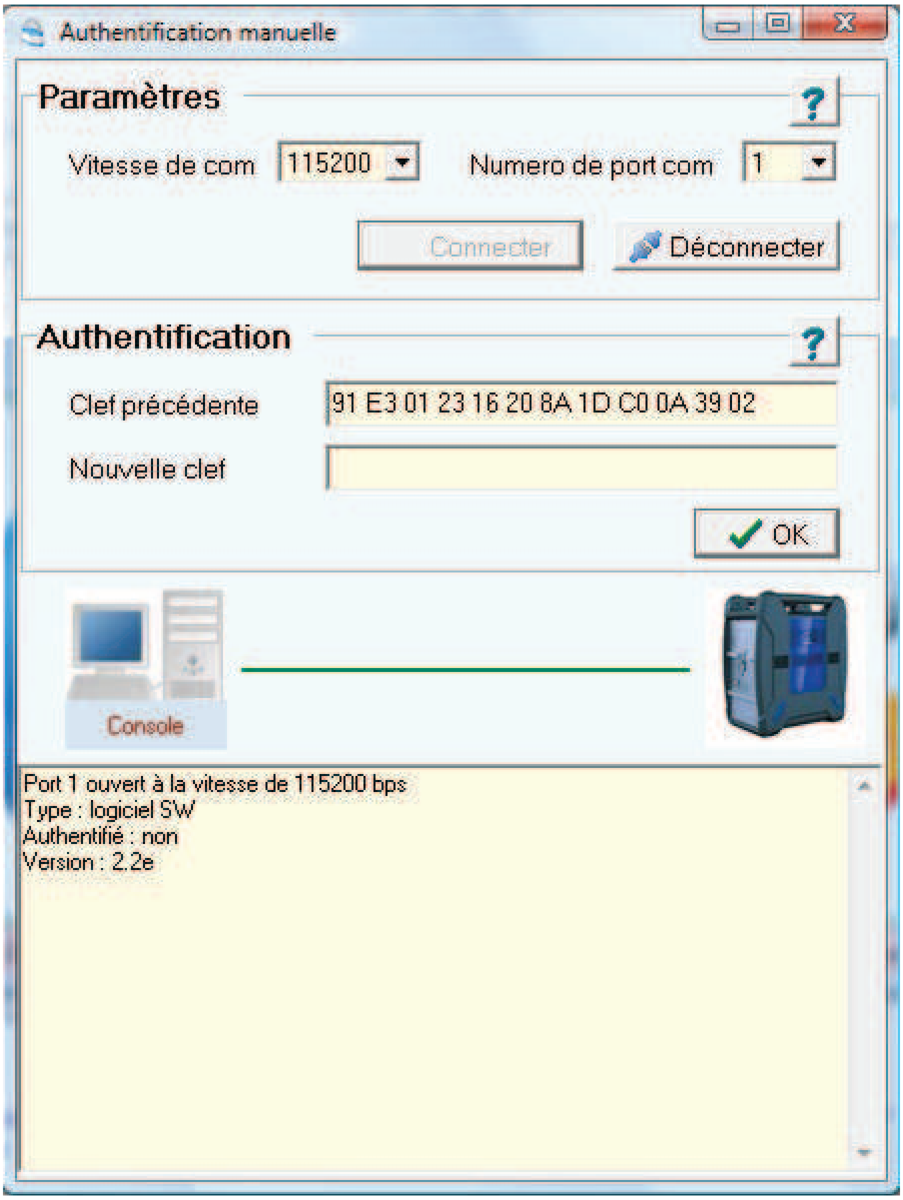
```
Tentative de connexion sur 192.168.1.252:55555
Connexion ouverte vers 192.168.1.252:55555
Type : logiciel BS
Authentifié : no
Version : 8.0a
Type : logiciel BS
Authentifié : oui
Version : 8.0a
Déconnexion...
```

Confirm success

Once the new key is entered (red circle figure 8), validate, and the network management terminal automatically disconnects. To check its success just test the equipment functions, look at the programme return in the window (red circle figure 9) or check the 'ACT' LED on the equipment. The LED should flash slowly (frequency of 2 or 4 seconds).

### 9.7.2 SERIAL EQUIPMENT CONNECTION

The use of a serial cable instead of a network cable does not change the procedure, it is strictly identical. Parameter configuration changes only.



Vitesse de com 115200

Numero de port com 1

Clef précédente 91 E3 01 23 16 20 8A 1D C0 0A 39 02

Nouvelle clef

```
Port 1 ouvert à la vitesse de 115200 bps
Type : logiciel SW
Authentifié : non
Version : 2.2e
```

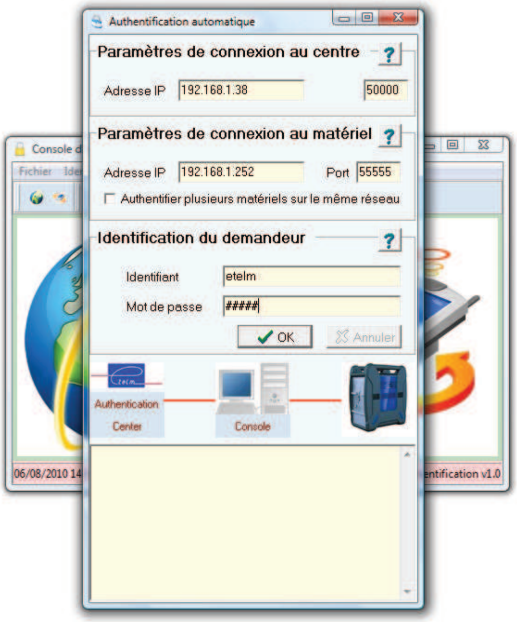
Manual authentication using a serial cable

As a parameter there is the communication speed and port number to be defined. It is preferable to leave the default configuration. If the connection fails it is possible to try again using another communications port.

# 9.8 Automatic authentication (via Internet)

## 9.8.1 Network connection to the equipment

The software will make it possible to authenticate equipment automatically via internet. First the parameters must be configured. To do this enter the IP address on the authentication centre and the communications port (choose any one that your firewall authorises). If a router is used it must be configured to accept the TCP protocol on the appropriate port.
Next the connection to the equipment should be configured. To do this, enter the equipment IP address (which should belong to the same sub-network as the authentication network management terminal if using a switch or a router...) and the communications port.
To finish enter the login and password supplied with the equipment and click on the "OK" button. The network management terminal connects to the centre and retrieves a valid key (if the customer credit is sufficient) and sends it to the equipment.



Authentification automatique

Paramètres de connexion au centre

Adresse IP: 192.168.1.38 50000

Paramètres de connexion au matériel

Adresse IP: 192.168.1.252 Port: 55555

□ Authentifier plusieurs matériels sur le même réseau

Identification du demandeur

Identifiant: etelm

Mot de passe: #####

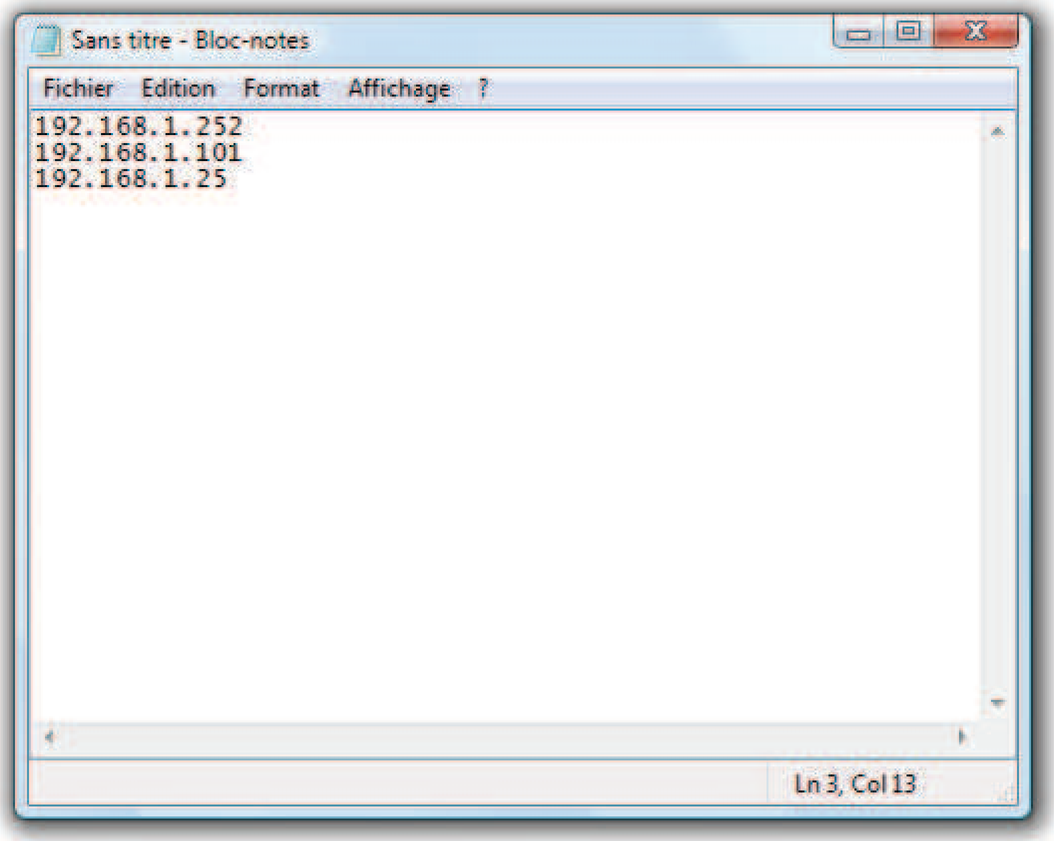
Automatic authentication using a network cable

At the end of the operation the network management terminal disconnects from the centre and the equipment should be tested to see whether the authentication was successful.

## 9.8.2 Multiple authentications (IP network)

It is possible to authenticate several appliances one after the other automatically without changing the configuration each time. To do this all the equipment must be on the same IP network and the network management terminal must have internet access.

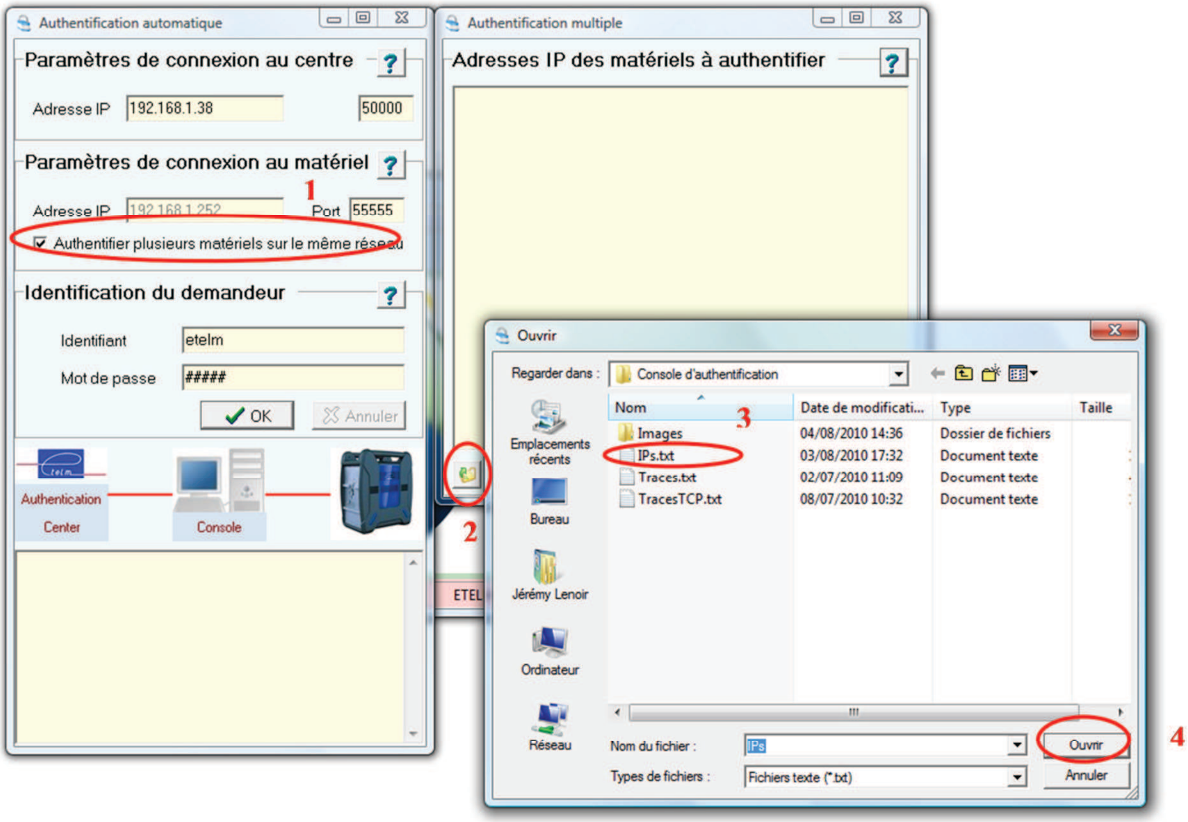
To begin with, create a text file (for example right click on the desktop, new menu, text file) containing all the IP addresses of the equipment to be authenticated as follows:



```
192.168.1.252
192.168.1.101
192.168.1.25
```

IP address entry

The IP addresses must be entered correctly and separated by carriage returns. The file is saved and closed.



Paramètres de connexion au centre

Adresse IP 192.168.1.38 50000

Paramètres de connexion au matériel

Adresse IP 192.168.1.252 Port 55555

☑ Authentifier plusieurs matériels sur le même réseau

Identification du demandeur

Identifiant etelm

Mot de passe #####

Adresses IP des matériels à authentifier

Regarder dans : Console d'authentification

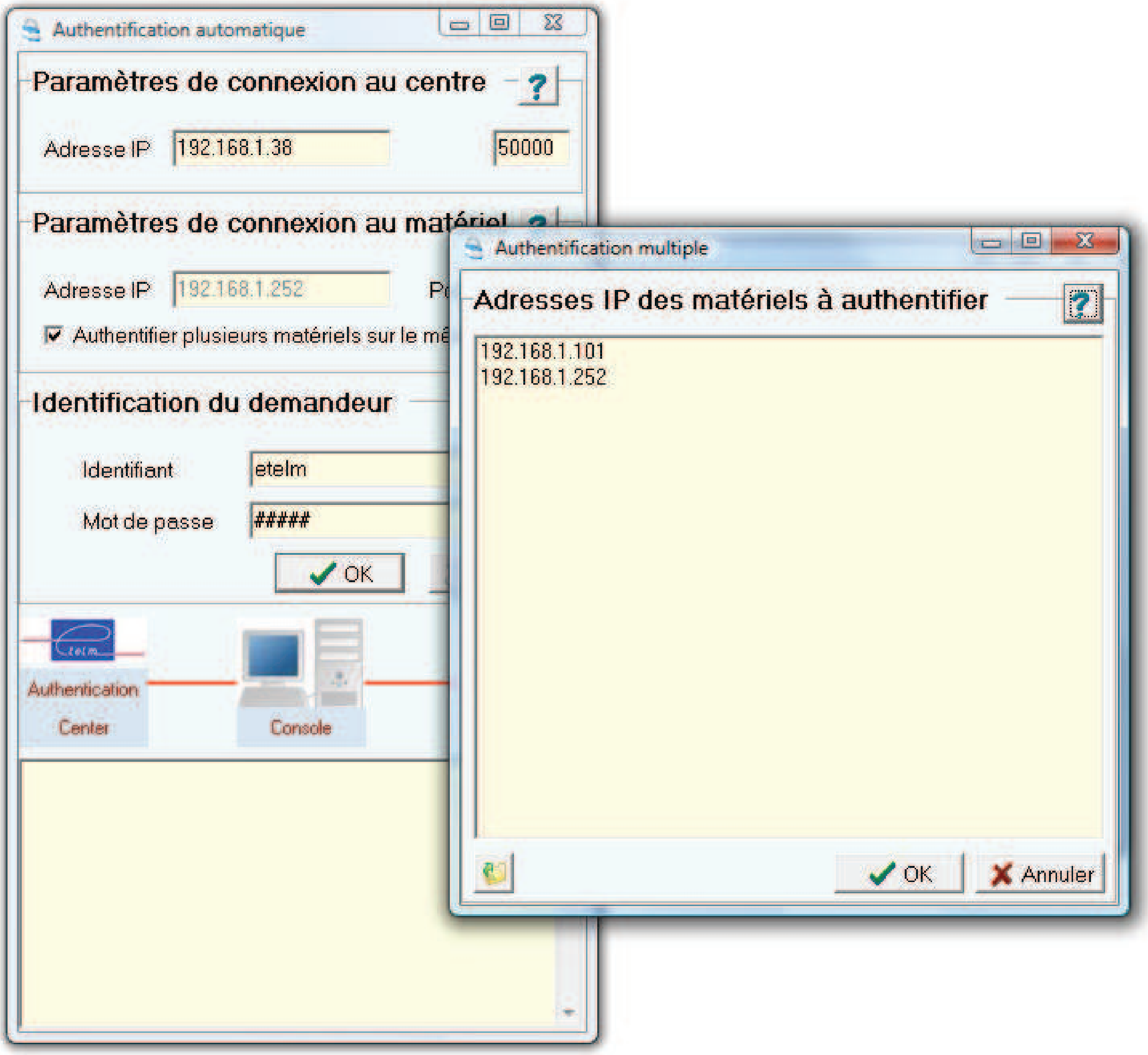
| Nom | Date de modificati... | Type | Taille |
|---|---|---|---|
| Images | 04/08/2010 14:36 | Dossier de fichiers | |
| IPs.txt | 03/08/2010 17:32 | Document texte | |
| Traces.txt | 02/07/2010 11:09 | Document texte | |
| TracesTCP.txt | 08/07/2010 10:32 | Document texte | |

Nom du fichier : IPs

Types de fichiers : Fichiers texte (*.txt)

Multiple authentications by IP network

To authenticate several appliances connected to the same network, first check the "authenticate several appliances on the same network" box (surrounded in red, N°1), next click on the button showing a file in the window that has appeared (surrounded in red N° 2), select the text file containing the IP addresses (in red N°3) and finally click on the open button (in red N° 4).
The addresses appear in the "IP addresses of equipment to authenticate" window as shown below. If an address is not shown, it is because it is not correct.



Authentification automatique

Paramètres de connexion au centre

Adresse IP: 192.168.1.38 — 50000

Paramètres de connexion au matériel

Adresse IP: 192.168.1.252

☑ Authentifier plusieurs matériels sur le mê

Identification du demandeur

Identifiant: etelm

Mot de passe: #####

Authentification multiple

Adresses IP des matériels à authentifier

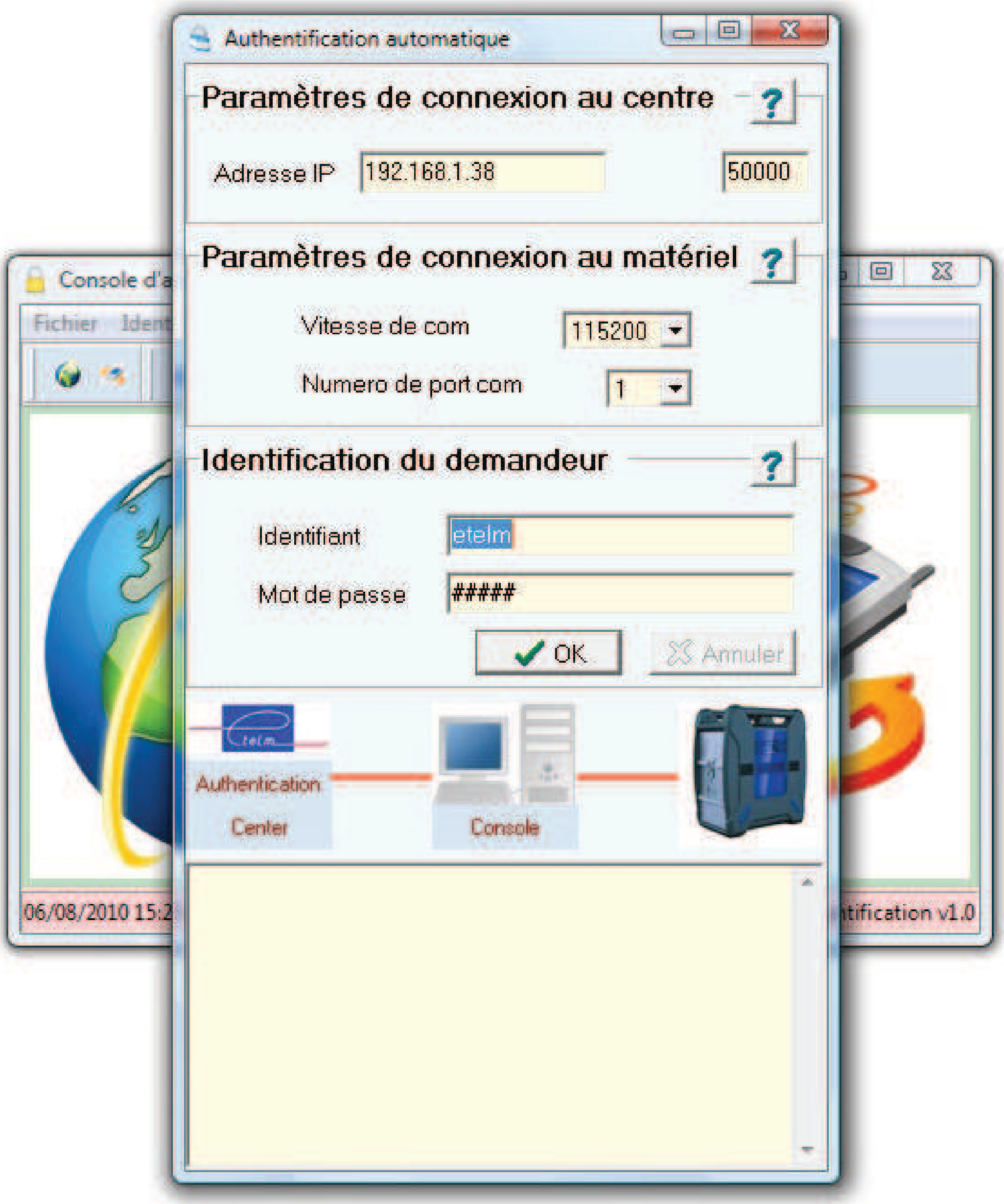
192.168.1.101
192.168.1.252

IP address validation

Validate click on the OK button. Finally, to launch the procedure, carry on as if authenticating a single appliance. The procedure is exactly the same.

### 9.8.3 SERIAL EQUIPMENT CONNECTION

The use of a serial cable instead of a network cable does not change the procedure, it is strictly identical. The parameter configuration changes only.



Authentification automatique

Paramètres de connexion au centre

Adresse IP: 192.168.1.38 50000

Paramètres de connexion au matériel

Vitesse de com: 115200

Numero de port com: 1

Identification du demandeur

Identifiant: etelm

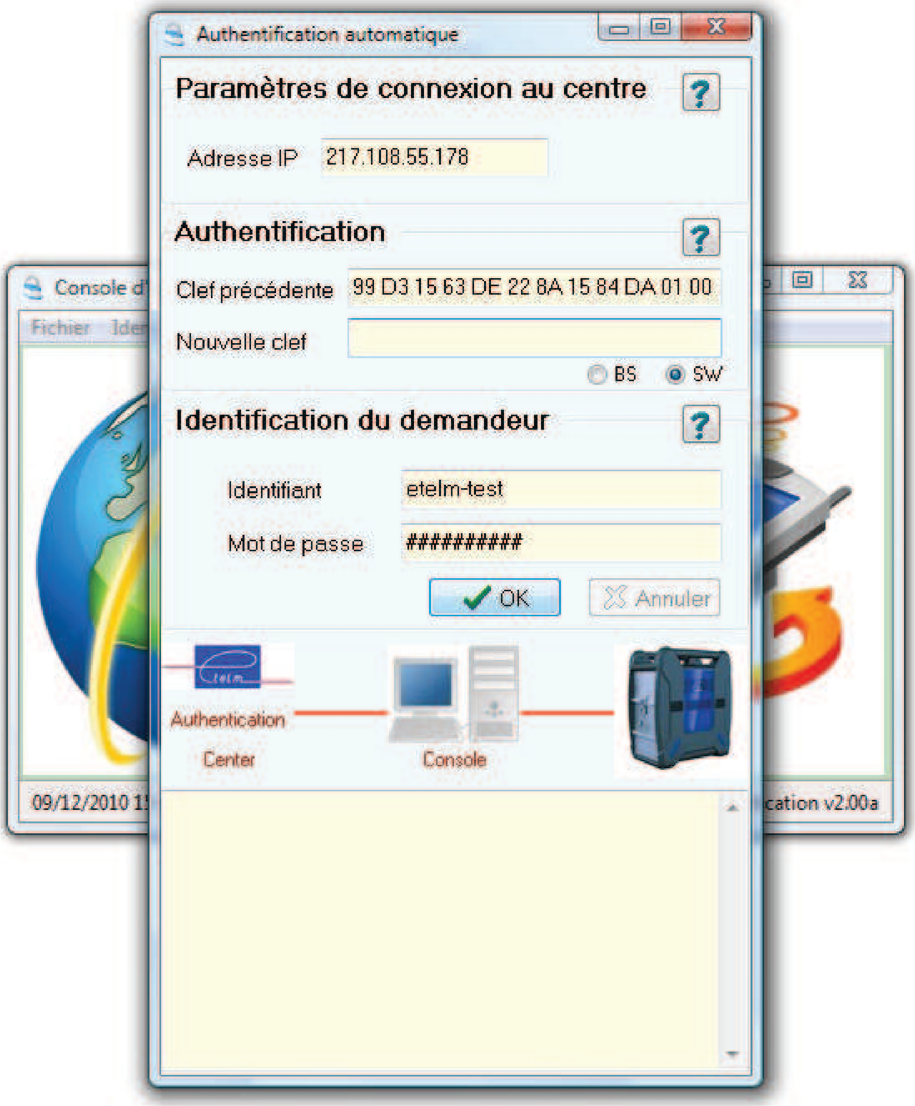
Mot de passe: #####

Automatic authentication using a serial cable

As for manual authentication, here the communications speed is set and the same steps as above are carried out. Multiple authentications are not possible because it would need a serial cable connection to all the BSs at the same time.

### 9.8.4 No connection to the equipment

It is possible to authenticate equipment via Internet without being directly connected to them. In this case start by retrieving the old key using the method in the previous paragraph (see §4.2), send it via internet as explained below, then retrieve the new key and send it to the equipment using the previous method again.



Authentification automatique

Paramètres de connexion au centre

Adresse IP: 217.108.55.178

Authentification

Clef précédente: 99 D3 15 63 DE 22 8A 15 84 DA 01 00

Nouvelle clef:

○ BS ● SW

Identification du demandeur

Identifiant: etelm-test

Mot de passe: ##########

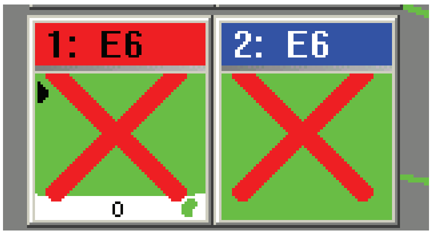
Automatic authentication without connecting to the equipment

First enter the old key, enter the identifiers that were supplied and click on OK. The new key will appear. It must then be sent to the equipment.

### 9.8.5 Diagnosing an authentication problem on a NeTIS-B

Using the TETRA network management terminal you can see whether a BS is authenticated

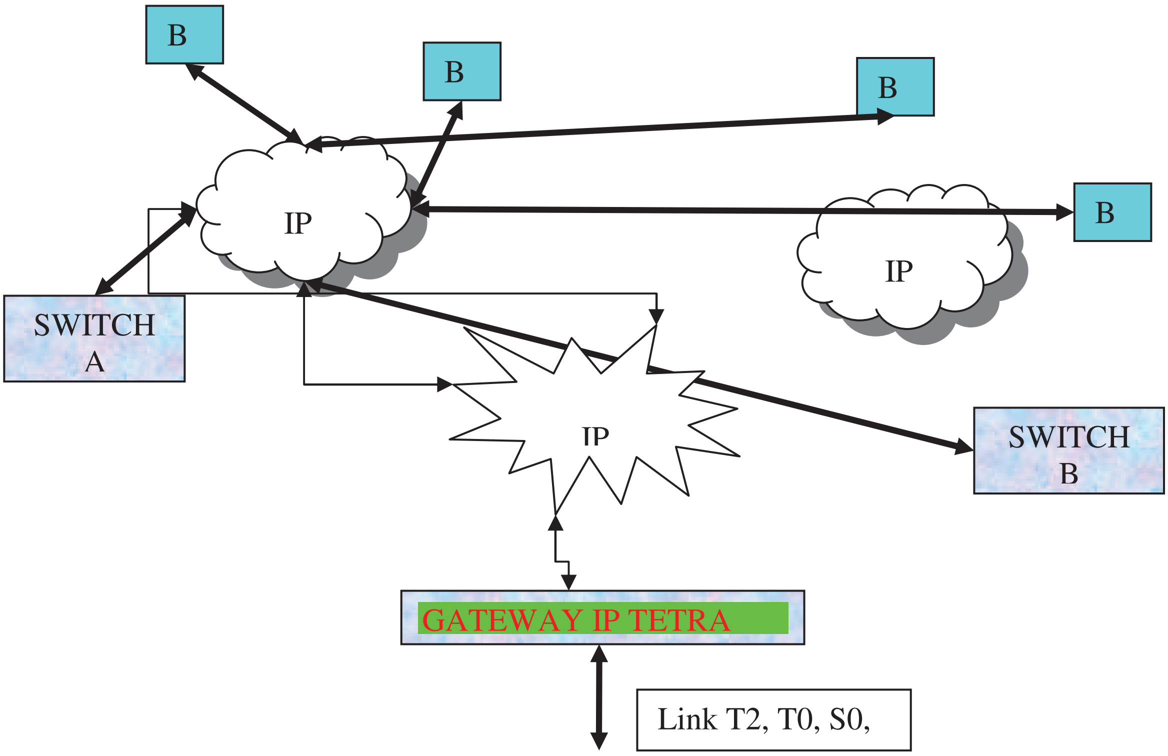
In the monitoring you will see a red cross appear on the green background of the icon as shown below if the NeTIS-B has not been authenticated:



# *10. PABX GATEWAY*

## *10.1 Introduction*

The TETRA IP Gateway for PBX (phone switchboard) is used to open up a classic phone installation to the TETRA IP radio world.



This gateway is used to interconnect a phone link to any location of an ETELM IP TETRA network having the TETRA UDP phone and signalling from the different TETRA SWITCHES.

This IP / PABX Gateway, in the case of a "full IP" TETRA network with several switches each having phone access, makes it possible to route phone calls from anywhere on the network to the TETRA SWITCH managing the network at time t, without using external inter PABX links.
And on the opposite, for a radio call to a phone, the TETRA SWITCH routes the call to the IP Gateway corresponding to the phone call.

Communications from phone sets connected to the PABX are sampled, converted to binary data using MIC decoding (modulation by impulse coding), then encapsulated in IP packets by the TETRA IP Gateway for PABX.

On the other hand, radio calls are sent to the TETRA IP Gateway for PABX which routes them to the PABX and, when the connection is made transforms the TETRA UDP IP phone blocks onto the MIC blocks needed for the phone link.

## 10.2 Equipment

This TETRA_IP for PABX Gateway is composed of:

- A BS chassis to access the UPlane and CPlane bus managing phoning and TETRA signalling from the CPU board
- A 220V or 48V power supply board
- A CPU board (need to have an 8k equipment signal)
- A BDT board (Time base)
- A COM2 or COM3 board configured with the T2 software (Version 2.05/) or a COMS board for an S0 or T0 access

## 10.3 Led signification

Led **5V** led for the CPU board:

- On if 5V power supply is present on the CPU board
- Off if the 5V power supply is absent from the CPU board

**ACT** led for the CPU board:

- Very fast flashing if the IP PABX gateway has not received a configuration from the Switch CPU board.
- Slow flashing (once per second) if the IP PABX Gateway is configured

**INT** led for the CPU board:

- On if the 125 µs interruption is supplied by the BDT board to the CPU board
- Off if the 125 µs interruption is absent

**ACT/MCCH** led for the CPU board:

- On if the IP PABX Gateway is connected to the switch (TCP connection)
- Off if the IP PABX Gateway is not connected to the switch

Add COM and BDT boards

# 10.4 Configuration

## 10.4.1 Configuration to the IP PABX Gateway

- Parameter the Gateway IP address (by modifying the file /etc/interfaces)

## 10.4.2 Configuration of the service network management terminal

- Creation of phone appliance with the IP address of the appliance and its number as the link.
- In the dialling plan, indicate the PABX type for the number range corresponding to the gateway followed by the corresponding equipment number.

# 11. MODULE DESCRIPTION

## 11.1 Power supply board:

- **INDICATORS:**

+5V+30V+12V-12V
**Normal operation**: all on

- **Role:**

The power supply provides direct current of de +5v, +12v, -12v and +30v

# 11.2 CPU-BDT board

Impossible d'afficher l'image.

# *11.3 CCT2 board*

Impossible d'afficher l'image.

# 11.4 COM board

Impossible d'afficher l'image.

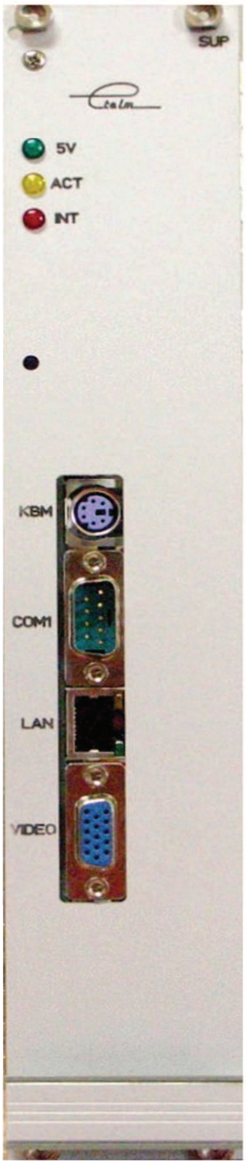
## 11.5 COM3 board

Impossible d'afficher l'image.

# 11.6 DCTR board

Impossible d'afficher l'image.

# 11.7 SUPIP board



- **INDICATORS:**

***Green indicator***: *P*ower present
***Yellow ACT indicator*:** slow flashing
***Red INT indicator:*** fast flashing (PC interruption)

- **Description**

This card is unique in a switch, it is similar to a CPU card. Its role is to ensure the mixing of the phone channels and the interfacing of IP dispatching.

Only the connection port to a local network is used; it only conveys voice over IP traffic for dispatching.

## *11.8 UCM board*

Impossible d'afficher l'image.

## *11.9 UCM2 board*

Impossible d'afficher l'image.

## *11.10 Power amplifier (PA)*

This module amplifiers the RF signals sent by the CPU module in order to deliver 10 Watts RF.
It is powered by +28 volts and can be checked on the front face of the UCM2. The PA alarms are present on the front face of the UCM2. The PA provides a set point for the regulation of its output power.

The amplifier has an internal blocking mechanism if it does not receive the transmission command from the UCM. No measurements can be made if the BS is not in TETRA transmission.

The module has an integrated circulator which protects it from accidental load disconnections and considerably minimises the risks of intermodulation with neighbouring transmitters.

Impossible d'afficher l'image.