



Conseils pour raccordement en IP

Installateurs et télésurveilleurs

1. CONTENU DE CETTE DOCUMENTATION	2
2. CONNEXION AU RÉSEAU LOCAL	2
2.1. Connexion automatique : DHCP	2
2.2. Connexion manuelle	2
2.3. Communication locale	3
3. ACCÈS À INTERNET	3
3.1. Passerelle	3
3.2. Serveurs DNS	3
3.3. Schéma du réseau local	4
3.4. Internet mobile	4
4. ESSAIS DE RACCORDEMENT EN IP	5
4.1. Test de l'accès à internet	5
A. Réseau local (filaire ou Wifi)	5
B. Internet mobile (3G, 4G, 5G...)	5
C. Test accès internet	5
4.2. Internet HS : tests	5
A. Réseau local	5
B. Accès mobile	5
4.3. Internet OK : vérifications	6
5. TESTS DE FRONTAUX	7
5.1. Test local	7
A. Connexion au réseau local	7
B. Paramétrage du frontal	7
C. Test de réception	7
5.2. Test depuis l'extérieur	8
5.3. Schéma de réception du frontal	8

1. CONTENU DE CETTE DOCUMENTATION

Cette documentation explique les principes de l'IP et d'internet et donne des conseils pour diagnostiquer et résoudre les problèmes de raccordement d'une centrale d'alarme sur un frontal de télésurveillance. Elle est utile aux installateurs et aux télésurveilleurs qui manqueraient de connaissances sur certains principes de communication d'internet.

2. CONNEXION AU RÉSEAU LOCAL

Un équipement se connecte sur le réseau local essentiellement via deux moyens :

1. un câble Ethernet (prise RJ45)
2. une borne Wifi

Quel que soit le moyen de connexion, l'équipement doit disposer de deux paramètres :

- Une adresse IP locale
- Un masque de sous-réseau

Les adresses IP locales sont formatées selon le masque de sous-réseau :

- Masque 255.255.255.0 (longueur 24 bits) : 192.168.xxx.xxx
- Masque 255.255.0.0 (longueur 16 bits) : 10.xxx.xxx.xxx (ou 172.16.xxx.xxx à 172.31.xxx.xxx)

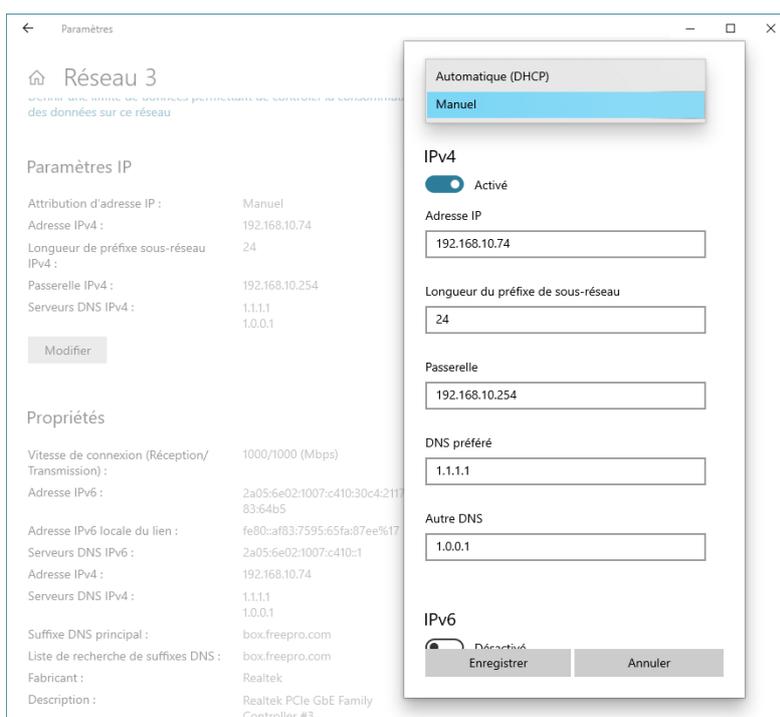
Ces deux données peuvent être obtenues automatiquement ou saisies manuellement.

2.1. Connexion automatique : DHCP

La grande majorité des réseaux locaux comporte un serveur DHCP qui va fournir les données de connexion aux équipements qui le demande. Dans de nombreuses installations, la box internet assure le rôle de serveur DHCP.

2.2. Connexion manuelle

Les paramètres de connexion sont entrés manuellement - d'après les indications d'un responsable.



2.3. Communication locale

Disposer d'une adresse locale et d'un masque de sous-réseau permet de communiquer avec les autres équipements de ce sous-réseau, si les 2 ou 3 premiers chiffres de leurs adresses sont identiques. Exemples :

- 192.168.10.74 du sous-réseau 255.255.255.0 (/24) communique avec toutes les adresses débutant par les 3 premiers chiffres "192.168.10." mais pas (exemple) "192.168.83.".
- 10.16.231.29 du sous-réseau 255.255.0.0 (/16) communique avec toutes les adresses débutant par les 2 premiers chiffres "10.16." mais pas (exemple) "10.18.".

3. ACCÈS À INTERNET

Une adresse IP *locale*, comme son nom l'indique, ne peut accéder qu'aux équipements *locaux*. Un équipement spécial du réseau local est chargé de transmettre les connexions vers l'extérieur : la passerelle. Dans de nombreuses installations, c'est la box internet qui remplit ce rôle.

La passerelle, en relayant les demandes de connexions vers l'extérieur, permet aux équipements du réseau local d'accéder aux adresses IP d'internet dans le monde entier.

3.1. Passerelle

La passerelle doit avoir une adresse locale accessible à l'équipement qui veut se connecter à l'extérieur. Exemple : 192.168.10.74 (255.255.255.0, /24) peut se connecter sur la passerelle "192.168.10.254" mais pas "192.168.83.1".

Généralement, les passerelles ont le dernier chiffre de leur adresse égal à 1 (mini) ou 254 (maxi).

3.2. Serveurs DNS

Avoir accès aux adresses IP mondiales ne suffit pas pour de nombreux usages. Souvent, les adresses IP "directes" ne sont pas connues mais obtenues via un nom de domaine.

Exemple : le nom de domaine "logetel.fr" donne l'adresse IP : 213.186.33.19.

Un nom de domaine offre 2 avantages importants :

- La facilité de mémorisation par rapport à des chiffres.
- La modification possible de l'adresse désignée par le nom de domaine en cas de réorganisation (changement d'adresse IP, déménagement, urgence...).

Pour "traduire" un nom de domaine en adresse IP, l'équipement doit disposer de l'adresse d'un serveur DNS (Domain Name System). Souvent, le paramétrage par défaut désigne la box internet comme serveur DNS. Cette dernière se chargera alors de relayer les demandes aux "vrais" serveurs DNS.

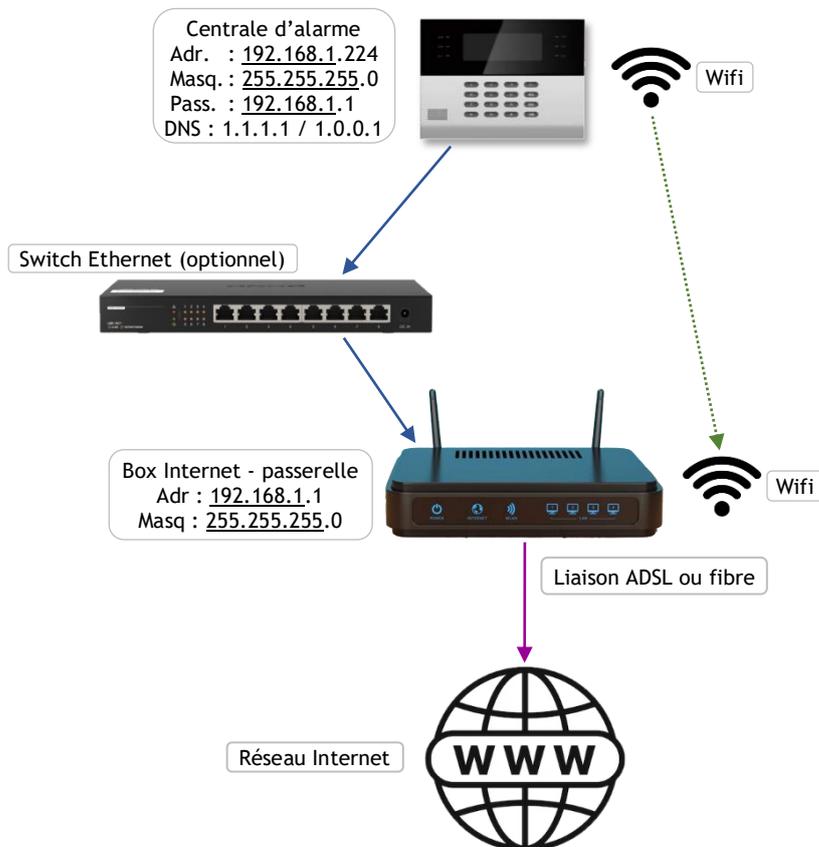
Au besoin, il est possible de paramétrer un serveur DNS public.

Exemples de DNS publics - adresse principale et secours :

- Cloudflare : 1.1.1.1 et 1.0.0.1
- Quad9 : 9.9.9.9 et 149.112.112.112
- Google : 8.8.8.8 et 8.8.4.4

3.3. Schéma du réseau local

Voici un schéma général de connexion au réseau local en filaire ou en Wifi, ainsi que l'accès extérieur via la passerelle :



3.4. Internet mobile

Le paramétrage de l'accès à internet mobile (GSM 3G, 4G, 5G...) est bien plus simple qu'en filaire ou Wifi car les paramètres de connexion sont fournis directement par l'opérateur de téléphonie lors de l'activation de la carte SIM sur son réseau.

De plus, il n'y a pas de distinction entre adresses locales et publiques : l'accès mobile est directement en relation avec l'internet mondial.

4. ESSAIS DE RACCORDEMENT EN IP

En cas de problème de communication entre une centrale d'alarme et un frontal chez un télésurveilleur, de multiples points sont à vérifier.

4.1. Test de l'accès à internet

A. Réseau local (filaire ou Wifi)

Filaire : débrancher le câble RJ45 de la centrale et connectez-le sur un PC portable.

Wifi : éteindre la centrale et se connecter sur la box en wifi.

Filaire et Wifi : si les paramètres de connexion de la centrale au réseau local sont manuels, les reprendre sur le PC portable. Sinon activer les paramètres automatiques (DHCP).

B. Internet mobile (3G, 4G, 5G...)

Prendre la carte SIM de la centrale et l'insérer dans un smartphone.

C. Test accès internet

Lancer un navigateur internet sur le PC portable ou le smartphone : les sites web sont-ils accessibles ?

4.2. Internet HS : tests

A. Réseau local

Si l'accès à internet n'est pas OK, il faut tester l'accès au réseau local en filaire ou wifi.

Un autre poste du réseau local a-t-il, lui, accès à internet ?

Si non, vérifier l'état de la connexion internet de la box : se connecter sur l'interface d'administration et consulter l'état internet.

Si oui, vérifier :

- Si en paramètres manuels, les vérifier (adresse, masque, passerelle, DNS)
- Si en automatique, vérifier que le serveur DHCP a bien attribué une adresse valide :
Filaire : Paramètres / Réseau et internet / Ethernet / cliquer sur l'icône du réseau.
Wifi : Paramètres / Réseau et internet / Wifi / Propriétés du matériel.

Chercher si l'adresse IPv4 est bien présente et correcte.

Si non :

- Filaire : vérifier l'état du câble, essayer avec un autre câble.
Essayer avec un autre port RJ45 du switch ou de la box.
- Wifi : Le wifi est-il bien activé ?
- Essayer de redémarrer la box.

B. Accès mobile

Soit la carte SIM est HS, soit elle n'est pas activée chez l'opérateur.

4.3. Internet OK : vérifications

Si l'accès à internet est OK, alors soit :

- Un pare-feu local bloque la sortie vers le frontal du télésurveilleur. Cette situation ne se produit que dans des sites sécurisés (banques, grand magasins, hôpitaux, institutions, communes...) dans lesquels les pare-feux sont programmés pour bloquer les flux sortants non déclarés. Se rapprocher de responsables de la sécurité informatique et réseau.
- La programmation de la centrale est invalide, au niveau des paramètres, soit :
 - de connexion au réseau local
 - de connexion au frontal (adresse et N° de port du frontal, TCP ou UDP, protocole).
- Le frontal chez le télésurveilleur est inopérant. A vérifier avec le télésurveilleur. Très peu probable si ce dernier a déjà plusieurs centrales de ce type raccordées chez lui.

Un logiciel de simulation d'alarme, comme **Élixir**, peut alors être d'une grande aide pour trouver l'origine du problème d'émission des alarmes, en indiquant si la connexion TCP est OK ou non. Cette information permet de distinguer entre les problèmes de connexion IP et ceux liés au protocole et à l'acquittement.

5. TESTS DE FRONTAUX

Cette partie s'adresse aux télésurveilleurs pour tester la bonne réception d'un frontal IP de réception d'alarme.

5.1. Test local

Si le frontal n'est pas joignable de l'extérieur, un test en local permet de valider :

- La connexion au réseau local
- Le paramétrage du frontal (écoute-t-il le (ou les) bon numéro de port ?)
- L'absence de blocage d'un pare-feu système (comme Windows Defender Firewall)

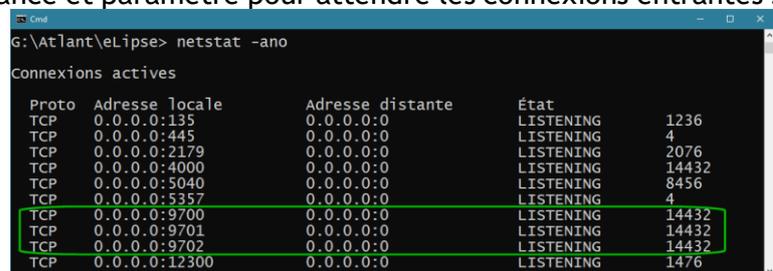
A. Connexion au réseau local

Un frontal doit avoir une adresse locale fixe, par de paramètres manuels ou un bail DHCP fixe. Ce poste est-il visible des autres postes du réseau local (via la commande PING <adresse> ?) Si non : vérifier le paramétrage de l'accès au réseau local.

B. Paramétrage du frontal

Le frontal de réception IP doit être lancé et paramétré pour attendre les connexions entrantes sur les bons numéros de ports.

Une commande utile pour vérifier :



```

G:\Atlant\elipse> netstat -ano
Connexions actives
Proto Adresse locale Adresse distante État
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1236
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:2179 0.0.0.0:0 LISTENING 2076
TCP 0.0.0.0:4000 0.0.0.0:0 LISTENING 14432
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 8456
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:9700 0.0.0.0:0 LISTENING 14432
TCP 0.0.0.0:9701 0.0.0.0:0 LISTENING 14432
TCP 0.0.0.0:9702 0.0.0.0:0 LISTENING 14432
TCP 0.0.0.0:12300 0.0.0.0:0 LISTENING 1476
  
```

La commande "**netstat -ano**" liste (entre autres) tous les numéros de ports actuellement actifs sur le poste. Dans la copie d'écran en exemple, un frontal écoute les ports TCP 9700, 9701 et 9702 (avec le numéro de processus n° 14432).

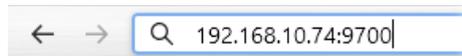
Les colonnes doivent indiquer, comme en exemple :

- Proto : **TCP** (ou plus rarement UDP)
- Adresse locale : **0.0.0.0:<N°_de_port>**
- Adresse distante : **0.0.0.0**
- État : **LISTENING** (en écoute)

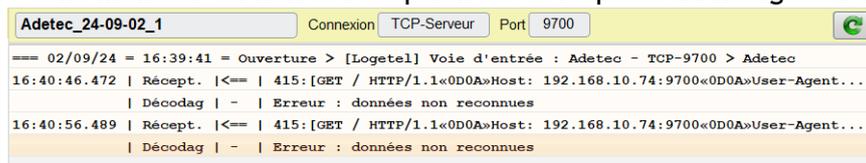
Si le numéro de port attendu ne se trouve pas dans la liste c'est qu'aucun logiciel n'est en attente de connexion sur ce port : vérifier alors l'état et la programmation du frontal.

C. Test de réception

Un test simple est d'utiliser un navigateur internet - à partir d'un autre poste - et d'entrer dans la barre d'adresse, l'adresse IP locale du frontal et le n° de port à tester :



Sur le frontal, les traces vont montrer ou non la réception de la requête du navigateur (exemple de traces sur eLipse) :



```

Adetec_24-09-02_1 Connexion TCP-Serveur Port 9700
==== 02/09/24 = 16:39:41 = Ouverture > [Logetel] Voie d'entrée : Adetec - TCP-9700 > Adetec
16:40:46.472 | Récept. |<== | 415:[GET / HTTP/1.1<0D0A>Host: 192.168.10.74:9700<0D0A>User-Agent...
| Décodag | - | Erreur : données non reconnues
16:40:56.489 | Récept. |<== | 415:[GET / HTTP/1.1<0D0A>Host: 192.168.10.74:9700<0D0A>User-Agent...
| Décodag | - | Erreur : données non reconnues
  
```

A 16:40:46, la requête HTTP-GET du navigateur est bien reçue (et la relance 10 sec. plus tard).

Si le frontal n'a pas reçu la requête du navigateur, il faut vérifier sa connexion au réseau local, son adresse IP et un blocage possible par un pare-feu système (comme Windows Defender Firewall).

Si ce test est OK, il est possible de passer au test depuis l'accès public externe.

5.2. Test depuis l'extérieur

Pour recevoir des connexions depuis l'extérieur, le routeur (la box internet) doit être programmée correctement au niveau des numéros des ports entrants. Chaque port (ou plage de ports) dédié à la réception d'alarme doit être ouvert et redirigé vers l'adresse locale du frontal IP. Consulter la documentation du fournisseur d'accès à internet pour le paramétrage.

Comme pour le test local, un navigateur peut être utilisé en entrant dans la barre d'adresse : l'adresse IP publique et le numéro de port à tester.

Attention : certains équipements d'accès internet (les box) ne permettent pas à un équipement local de se connecter sur un autre équipement local en passant par l'accès extérieur (fonction de bouclage, "loopback" ou "hairpinning" en anglais). Exemple : c'est OK chez Free mais impossible avec les LiveBox d'Orange (même en version "Pro"). Il est donc préférable de tester à partir d'un second accès internet (autre box, autre site, internet mobile...).

Un logiciel de simulation d'alarme, comme Élixir, peut tester intégralement la bonne réception en simulant l'envoi des alarmes, ce qui permet de valider l'ensemble de la chaîne des traitements :

- Accès internet publique OK
- Adresse IP publique
- Numéro de port dédié au protocole et redirigé vers le frontal
- Réception, décodage et acquittement du frontal
- Transmission au logiciel de traitement des alarmes

5.3. Schéma de réception du frontal

