



Tip Technique

Fiches techniques, FAQ, Conseils

✉ tip@sphinxfrance.fr

maj 14/01/2020

ACCESS ENTRANT : PASSERELLES SIERRA AIRLINK



ACCÉDER À L'ÉQUIPEMENT CONNECTÉ À VOTRE PASSERELLE

Pourquoi ?

- Accéder à des équipements distants (caméras, serveurs, capteurs, automates...)
- Remontée ou mises à jour d'informations (panneaux d'affichage, panneaux solaires...)

Comment ?

Votre abonnement opérateur avec carte SIM vous attribue une adresse IP. Elle peut être soit **privée** ou **publique**.

Cette **adresse est dite privée** si elle n'est **pas accessible directement depuis l'Internet**, ceci renforce la sécurité mais rend impossible toute connexion directe.

Inversement, **une IP publique est directement accessible** et l'accès à votre équipement est possible depuis l'internet. En raison du nombre limité d'adresses publiques, par défaut les opérateurs affectent des IP privées. **Demandez à votre opérateur une option "IP PUBLIQUE"**.

Repérez rapidement si votre IP est privée ? et donc accessible ou non depuis l'Internet...

Le tableau ci dessous indique les adresses IP privées ou réservées, si votre IP est dans cette catégorie, vous devez contacter votre opérateur pour qu'il active l'option IP publique ou qu'il vous indique le bon nom d'APN.

Bloc	Usage	Référence
0.0.0.0/8	Adresse réseau par défaut	RFC 1700
10.0.0.0/8	Adresses privées	RFC 1918
100.64.0.0/10	Espace partagé pour Carrier Grade NAT	RFC 6598
127.0.0.0/8	adresse de bouclage (localhost)	RFC 1122
169.254.0.0/16	adresses locales autoconfigurées (APIPA)	RFC 3927
172.16.0.0/12	Adresses privées	RFC 1918
192.0.0.0/24	Réservé par l'IETF	RFC 5736
192.0.2.0/24	Réseau de test TEST-NET-1	RFC 5737
192.88.99.0/24	6to4 anycast	RFC 3068
192.168.0.0/16	Adresses privées	RFC 1918
198.18.0.0/15	Tests de performance	RFC 2544
198.51.100.0/24	Réseau de test TEST-NET-2	RFC 5737
203.0.113.0/24	Réseau de test TEST-NET-3	RFC 5737
224.0.0.0/4	Multicast	RFC 5771
240.0.0.0/4	Réservé à un usage ultérieur non précisé	RFC 1112
255.255.255.255/32	broadcast limité	RFC 919

CONNEXION

La page "status" permet de visualiser l'adresse IP. Dans notre exemple, l'APN "orange.m2m" nous donne une IP publique.

Status WAN/Cellular LAN VPN Security Services Events Reporting Serial Applications I/O Admin

Last updated time : 22/6/2015 16:55:02

Apply Refresh Cancel

Home	AT Phone Number	NA
WAN/Cellular	AT Active WAN IP Address	90.117.80.182
LAN	AT Network State	Network Ready
VPN	AT Cell Info	CellInfo: TCH: 6400 RSSI: -71 LAC: 13825 CellID: 15481350
Security	AT Current Network Operator	Orange F
Services	AT Radio Technology	LTE
Serial	Network Service Type	4G
Applications	AT Signal Strength (RSSI)	-71
About	LTE Signal Strength (RSRP)	-96
	LTE Signal Quality (RSRQ)	-8
	LTE Signal Interference (SINR)	15.8
	AT Channel	6400
	WAN/Cellular Bytes Sent	680
	WAN/Cellular Bytes Rcvd	2219
	Persisted WAN/Cellular Bytes Sent	1479
	Persisted WAN/Cellular Bytes Rcvd	16371
	ALEOS Software Version	4.4.1
	AT Customer Device Name	HF33740072001001

Vérifiez que l'adresse IP Publique est joignable depuis un PC avec connexion internet.

```
>ping 90.117.80.182
Envoi d'une requête 'Ping' 90.117.80.182 avec 32 octets de données :
Réponse de 90.117.80.182 : octets=32 temps=1343 ms TTL=49
Réponse de 90.117.80.182 : octets=32 temps=59 ms TTL=49
Réponse de 90.117.80.182 : octets=32 temps=66 ms TTL=49
Réponse de 90.117.80.182 : octets=32 temps=66 ms TTL=49

Statistiques Ping pour 90.117.80.182:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 59ms, Maximum = 1343ms, Moyenne = 383ms

C:\Users\sergeb>
```

Bien qu'ayant une IP publique, **celle ci reste dynamique sur les réseaux cellulaire** donc attribuée pour une période de temps limitée.

DNS DYNAMIQUE SIERRA : IP MANAGER

RAPPEL

Une adresse peut changer à tout moment. Et ceci dépend de votre fournisseur d'accès. Elle peut changer toutes les 24 heures, toutes les heures, à chaque redémarrage, etc. Dans ce cas, joindre l'IP devient pratiquement impossible. Il faut donc que votre produit soit identifié par un nom. Ce nom (domaine) sera alors géré par un serveur capable de mettre à jour l'IP en face du nom choisi. **C'est le serveur dns dynamique.**

Votre passerelle intègre :

- Un client dns dynamique propriétaire sans inscription préalable qui fonctionne avec les serveurs de sierra (ip manager)
- Des clients dynamique DNS de tierce partie >> dyndns, no-ip, ods.org, regfish.com, tzo.com

Nous allons ici décrire le paramétrage du client SIERRA IP manager.

Accédez à l'interface web (<http://192.168.13.31:9191>)

User Name: user

Password: 12345

(Paramètres usine)

- 1 - Ouvrez l'onglet < Services >
- 2 - Cliquez sur le lien < Dynamic DNS >
- 3 - En face de "Service < IP Manager >

The screenshot shows the SIERRA IP Manager web interface. The 'Services' tab is selected, and the 'Dynamic DNS' link is highlighted. The 'Service' dropdown is set to 'IP Manager'. The 'Device Name' field contains 'HF33740072001001'. Other fields include 'Domain', 'IP Manager Server 1', 'IP Manager Server1 Update' (set to 'Only on Change'), 'IP Manager Server1 Update (minutes)' (set to '255'), 'IP Manager Server1 Key', 'IP Manager Server 2', 'IP Manager Server1 Update' (set to 'Only on Change'), 'IP Manager Server2 Update (minutes)' (set to '255'), and 'IP Manager Server2 Key'.

- 1 - En face de "Device Name" (par défaut, le nom correspond au numéro de série du produit). Il n'y a pas de vérification de doublons, donc mettez un nom **unique mais simple à se rappeler, nom de votre société suivi par exemple d'un numéro (pas d'espace et < à 20 caractères).**

- 2 - En face de "Domain", tapez **eairlink.com** (nom du domaine utilisé par sierra)
- 3 - En face de " IP Manager Server 1", tapez **edns1.eairlink.com**
- 4 - En face de " IP Manager Server 2", tapez **edns2.eairlink.com**

(Attention: ne pas modifier les autres champs, il s'agit des clés d'authentification du serveur distant)

"Apply" puis "Reboot" pour la prise en compte

Attendez le redémarrage de votre passerelle (2 minutes pour la série LS300).

Votre passerelle est désormais joignable sur son nom de domaine depuis n'importe quel accès internet (ex: <http://monentreprise003.eairlink.com:9191>) et même si l'adresse change.

vérification par la commande "ping" :

```
C:\Users\sergeb>ping monentreprise001.eairlink.com

Envoi d'une requête 'ping' sur monentreprise001.eairlink.com [90.117.102.146] avec 32 octets de données :
Réponse de 90.117.102.146 : octets=32 temps=1326 ms TTL=49
Réponse de 90.117.102.146 : octets=32 temps=78 ms TTL=49
Réponse de 90.117.102.146 : octets=32 temps=57 ms TTL=49
Réponse de 90.117.102.146 : octets=32 temps=55 ms TTL=49

Statistiques Ping pour 90.117.102.146:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 55ms, Maximum = 1326ms, Moyenne = 379ms

C:\Users\sergeb>
```

Services / Acemanager

Par défaut l'accès remote est désactivé sur le produit, pensez à l'activer via HTTPS only , ou both (HTTP+HTTPS)

The screenshot shows the 'Services' configuration page in the Acemanager interface. The top navigation bar includes tabs for Status, WAN/Cellular, LAN, VPN, Security, Services (selected), Location, Events Reporting, Serial, Applications, I/O, and Admin. Below the navigation bar, there are buttons for Software and Firmware, Template, Refresh All, Reboot, Help, and Logout. The main content area is titled 'ALMS' and 'Acemanager'. It features a sidebar with various configuration categories: Power Management, Dynamic DNS, SMS, AT (Telnet/SSH), Email (SMTP), Management (SNMP), Time (SNTP), Authentication, and Device Status Screen. The main configuration area is divided into two sections: 'General' and 'Advanced'. The 'General' section includes settings for Remote Access (set to 'Disable'), Local Access (set to 'Both HTTP and HTTPS'), HTTP Port (9191), HTTPS Port (9443), Session Idle Timeout (15 minutes), Maximum Login Attempts (3), and Unlock Time (120 seconds). The 'Advanced' section is currently collapsed.

SECURITY - PORT FORWARDING (redirection de port)

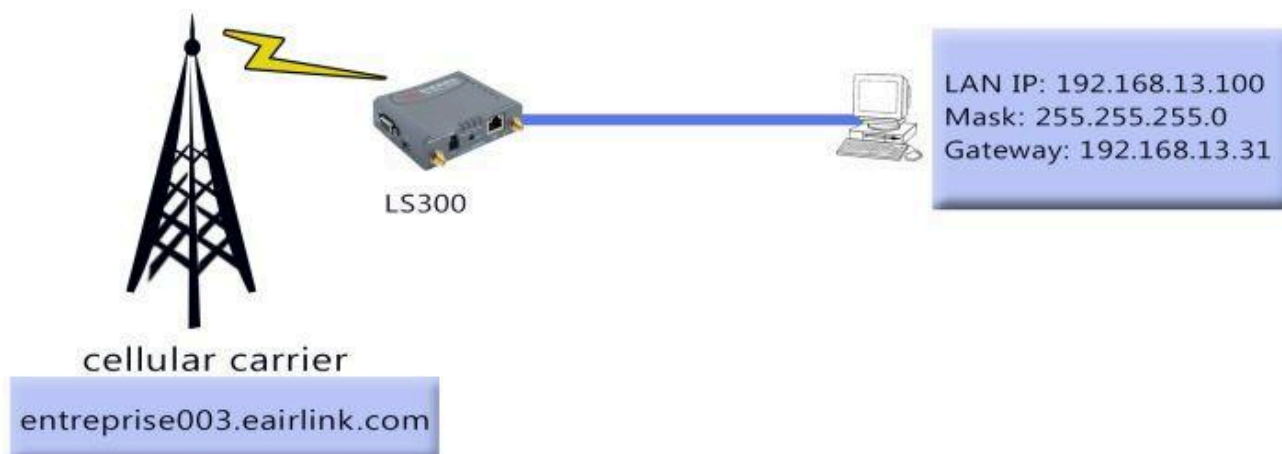
Pour accéder à vos équipements distants, il faut configurer le produit pour qu'il "redirige" les paquets vers le ou les équipements de votre réseau privé.

- 1 - Cliquez sur l'onglet "Security"
- 2 - Choisissez "Port Forwarding"

The screenshot shows the 'Security' configuration page in the Acemanager interface. The top navigation bar includes tabs for Status, WAN/Cellular, LAN, VPN, Security (selected), Services, Events Reporting, Serial, Applications, I/O, and Admin. Below the navigation bar, there are buttons for Apply, Refresh, and Cancel. The main content area is titled 'Port Forwarding'. It features a sidebar with various configuration categories: Port Filtering - Inbound, Port Filtering - Outbound, Trusted IPs - Inbound (Friends), Trusted IPs - Outbound, and MAC Filtering. The main configuration area includes settings for DMZ Enabled (set to 'Automatic'), DMZ IP in use (192.168.13.100), and Port Forwarding (set to 'Disable'). Below these settings is a table for Port Forwarding rules. The table has columns for Public Start Port, Public End Port, Protocol, Host IP, and Private Start Port. An 'Add More' button is located at the bottom right of the table.

DMZ : Zone Démilitarisée, elle correspond à l'ouverture de tous les ports de la passerelle vers une adresse ip du réseau local.

Les ports entrants sont mappés à l'identique sur l'adresse DMZ, une connexion sur le port 80 protocole TCP vers nomentreprise001 sera redirigé vers l'équipement 192.168.13.100 sur le port 80 protocole TCP



Attention par défaut, une DMZ est active et redirige les données vers l'adresse 192.168.13.100 (1ère adresse IP fournie par le serveur DHCP de votre passerelle)

Port Forwarding: permet de rediriger un port ou une plage de ports vers une adresse IP précise et vers un port précis. Vous pouvez donc avoir plusieurs équipements (automates, serveurs, caméras...) en réception de l'adresse publique en précisant des ports différents.

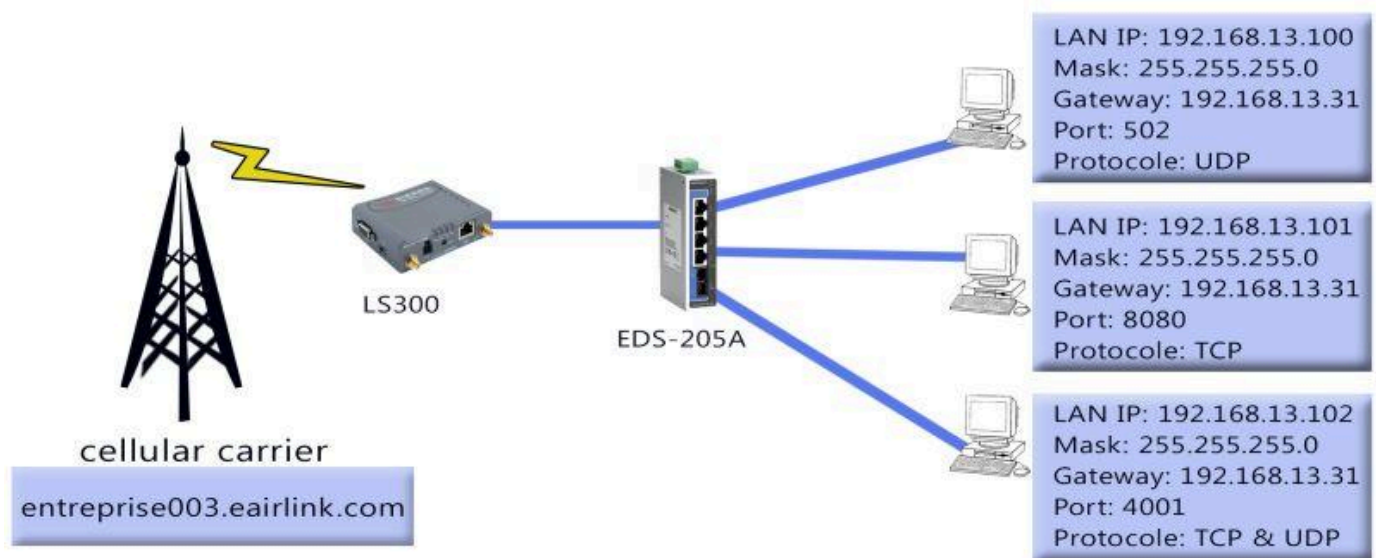
Toutes les requêtes vers l'adresse opérateur (nomentreprise001.eairlink.com) seront renvoyées en fonction de vos règles de redirection vers les équipements désirés.

Exemple de connexion sur **nomentreprise001.eairlink.com**

Une connexion sur le port 502 UDP sera redirigée vers l'équipement 192.168.13.100 port 502 UDP

Une connexion sur le port 4001 TCP et/ou UDP sera redirigée vers l'équipement 192.168.13.101 port 4001 TCP et/ou UDP

Une connexion sur le port 8080 TCP sera redirigée vers le l'équipement 192.168.13.102 port 8080 TCP



Paramétrage:

1. Désactivez la fonction DMZ : "Disable"
2. Activez le Port Forwarding: "Enable"
3. Choisissez le port de début (**Public Start Port**)
4. Choisissez le port de fin (**Public End Port**)
5. Choisissez le protocole utilisé (TCP, UDP ou les deux)
6. Choisissez l'adresse IP de destination (adresse IP de l'équipement devant être accessible)
7. Choisissez le port de début pour l'adresse de destination (**Private Start Port**)
8. Cliquez sur "Add More" pour créer d'autres règles de redirection

Last updated time : 22/6/2015 17:12:43

Apply Refresh Cancel

Port Forwarding					
		DMZ Enabled	Disable ▼		
		Port Forwarding	Enable ▼		
Port Forwarding					
	Public Start Port	Public End Port	Protocol	Host IP	Private Start Port
X	502	502	UDP ▼	192.168.13.100	502
X	4001	4001	TCP & UDP ▼	192.168.13.101	4001
X	8080	8080	TCP ▼	192.168.13.102	8080
					Add More

Cliquez sur "Apply" puis sur "Reboot" pour la prise en compte des paramètres.