

**Institut Universitaire de Technologie,  
Aix-Marseille Université**

**RAPPORT DE STAGE  
Diplôme Universitaire de Technologie  
Spécialité Réseaux et Télécommunications**

Projet de supervision et déploiement d'outils de  
télécommunication

Jérémy GUERIN

Sprint Telecom

Responsable entreprise : Thomas Boss

Responsable académique : Arnaud Février

**2021**



## Table des matières

1	Introduction.....	1
2	Présentation de l'entreprise.....	2
2.1	Organisation et personnel.....	2
2.2	Le matériel.....	3
3	Cadre général.....	4
4	Mise en place d'un outil de supervision.....	5
4.1	Les différents outils disponibles.....	5
4.2	Mise en place d'un serveur Nagios.....	7
4.2.1	Mise en place du Serveur.....	7
4.2.2	Installation de Nagios.....	7
5	Configuration d'un PBX.....	12
5.1	Prise en main avec un serveur Issabel.....	12
5.2	Mise en pratique sur Alcatel.....	15
6	Conclusion.....	17
7	Remerciements.....	19
8	Glossaire.....	21
9	Bibliographie.....	23



# 1 Introduction

Le DUT\* Réseaux et Télécommunications permet de développer des connaissances ainsi que des compétences sur différents domaines. Étant plus attiré par les matières télécoms à savoir la téléphonie d'entreprise ainsi que les cours d'infrastructure sans fil, c'est dans cette spécialité que j'ai décidé de réaliser mon stage de fin d'études, d'une durée de dix semaines.

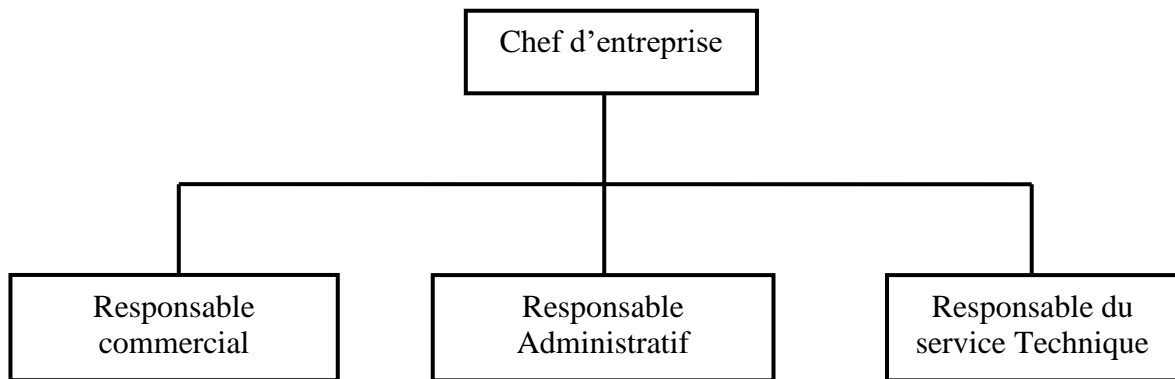
J'ai effectué mon stage au sein de l'entreprise Sprint Telecom, du 26 avril au 09 juillet 2021 avec pour tuteur Thomas BOSS, le chef d'entreprise. Mon stage avait pour objectif la mise en place de services de télécommunications pour d'autres entreprises ainsi que leur maintien en fonction et leur supervision.

Mes missions consistaient en la mise en place d'un outil de supervision pour les routeurs installés chez les clients, la configuration de PBX\* en vue de l'installation d'un service téléphonique chez les clients, la configuration de routeurs et aussi la mise en place de matériel chez les clients.

Après une présentation de l'entreprise Sprint Telecom, j'aborderai le cadre général dans lequel s'est déroulé mon stage, puis je présenterai les différentes missions que l'on m'a confiées.

## 2 Présentation de l'entreprise

### 2.1 Organisation et personnel



**Figure 1 : Organigramme du personnel**

Sprint Telecom est un opérateur global en télécommunication, fournissant des services complets sur la téléphonie filaire, cellulaire, accès Internet haut débit, voix sur IP et messagerie téléphonique.

Sprint Telecom a également une spécialité dans l'installation de système d'appel malades pour les établissements médicaux, VPN\* et sécurité par Firewall.

Ces offres sont ciblées pour des PME\*/PMI\*, TPE\*, artisans, professions libérales, collectivités et administrations. Sprint Telecom analyse les besoins adaptés à chaque profession afin d'aider les clients à optimiser le budget télécommunication et ainsi proposer un réel service télécom et informatique de proximité.

En s'adossant aux infrastructures des câblo-opérateurs majeurs tel que SFR ou Orange, mais aussi d'autres comme Altitude Infrastructure, Axione ou encore Covage, Sprint Telecom s'affranchit de toute contrainte financière liée à l'exploitation du réseau et se concentre sur le développement de services à forte valeur ajoutée adapté à ses clients.

Sprint Télécom a été fondée en 2012 par Thomas BOSS, qui avait déjà créé auparavant Axxess Telecom, vendue en 2007, ce qui lui fera signer une clause de non-concurrence de 5 ans sur ce marché.

Une fois ce délai réalisé, il décide de lancer un nouvel opérateur : Sprint Telecom. En octobre 2012, l'entreprise obtient sa licence d'opérateur puis en février 2013, un contrat est signé avec France Télécom, puis avec Alcatel en mars de la même année.

Aujourd'hui, Sprint Telecom est composée de Thomas BOSS, le chef d'entreprise, Renaud VIALE le responsable commercial, Magali PAYEN, la responsable administratif et Stéphane CAPELLE, responsable du service technique.

## 2.2 Le matériel

Sprint Télécom utilise principalement pour la partie réseau des routeurs MikroTik et TP-Link, mais aussi d'autres types comme des routeurs Netgear, Fortinet ou encore des Sonicwall. L'entreprise possède ainsi un large panel de matériel, et il en est de même pour la téléphonie. Durant mon stage, j'ai travaillé principalement avec les appareils suivants :



**Figure 2: Yealink T42S**



**Figure 3: Thomson ST2030**



**Figure 4: Gigaset C530IP**

Pour utiliser ces appareils, on utilise la Technologie de la Voix sur IP\* ou VoIP\*, permettant la communication par la voix sur des réseaux compatibles IP. En d'autres termes, les signaux analogiques audios sont transformés en données numériques puis transmis par réseaux privés, internet, WI-FI, satellite ou encore GSM\* puis sont retransmis en sons. Pour que cela fonctionne, les téléphones ont besoin d'être connectés à un PBX.



**Figure 5: PBX**

Un PBX est composé du matériel et des logiciels qui alimentent les systèmes téléphoniques des entreprises. Les systèmes PBX acheminent les appels vers un ou plusieurs bureaux en reliant les numéros centraux d'une entreprise à plusieurs postes.

La plupart des modèles de système PBX peuvent offrir d'autres fonctions, notamment :

- conférence téléphonique
- notification de mise en attente de l'appel
- enregistrement des appels
- fonctions de mise en attente comme l'attente musicale (de la musique est diffusée pendant que les appelants sont en attente) ou de file d'attente (organise les appels entrants selon une liste d'attente).

Les fonctions des systèmes PBX peuvent être configurées à l'échelle du système ou des canaux, selon les besoins de l'entreprise.

### **3 Cadre général**

En tant qu'opérateur Télécom, Sprint Telecom est régulièrement appelée à déployer des services de téléphonie ou de réseau, et c'est notamment une partie des missions que l'on m'a confiées.

Mais surtout, l'entreprise doit s'assurer du bon fonctionnement des services délivrés à ses clients et être en mesure de réagir au plus vite en cas de dysfonctionnement.

Or, lorsqu'il y a un dysfonctionnement quelque part, il faut attendre que le client se manifeste pour le savoir, et cela peut être d'autant plus compliqué si la panne s'étend jusqu'au service téléphonique.

On m'a ainsi donné pour mission de mettre en place un outil qui permettrait de superviser les routeurs installés chez les clients afin de vérifier que tout fonctionne correctement, mais aussi d'être alerté en cas de panne pour pouvoir agir au plus vite.

## 4 Mise en place d'un outil de supervision

### 4.1 Les différents outils disponibles

Tout d'abord, il faut définir ce qu'est la supervision : il s'agit de la surveillance du bon fonctionnement des réseaux et des services informatiques qui y sont connectés.

La métrologie est le fait d'obtenir, de garder et de tracer la valeur numérique d'une charge. Par exemple le pourcentage de CPU\* utilisé sur un serveur, le nombre de personnes connectées sur un site web, le trafic entrant et sortant sur un commutateur. Bien souvent, la métrologie permet tout simplement de tracer des graphiques.

Le monitoring qui est un anglicisme de surveillance est simplement la combinaison de la métrologie et de la supervision

J'ai d'abord étudié les différents outils de monitoring :



**Figure 6 : Logo de Cacti**

Cacti, qui est un outil de métrologie OpenSource\*. Cacti permet de créer des graphs, les regrouper dans des bases de données. Il peut marcher avec des outils de supervision comme Nagios mais ne le fait pas lui-même.

The image shows the logo for Nagios, a widely used open-source monitoring system. The word "Nagios" is written in a large, bold, black, serif font. The letter 'N' has a horizontal underline, and a registered trademark symbol (®) is located at the top right of the word.

**Figure 7 : Logo de Nagios**

Nagios, un outil de supervision qui permet de surveiller les services privés. C'est un moniteur d'hôtes et de services conçu pour informer des problèmes de réseau. Il est considéré par certaines personnes comme l'outil standard dans la surveillance OpenSource, car il est le premier à être aussi complet et efficace. En revanche, sa configuration se fait sous forme de fichiers, ce qui peut être difficile d'accès.



**Figure 8 : Logo de Centreon**

Centreon, qui est un outil de monitoring, il se suffit donc à lui-même et n'a pas besoin d'être utilisé avec un outil comme Cacti. Il est assez similaire à Nagios mais est plus simple d'utilisation et dispose d'une IHM, une interface permettant de communiquer avec la machine, ce qui facilite sa configuration. Pour la métrologie, Centreon met à disposition des modèles (templates), des services et des graphiques.



**Figure 9 : Logo de Zabbix**

Zabbix est à l'instar de Centreon un outil de monitoring, qui supervise les réseaux, la santé et l'intégrité des serveurs. Il a un système d'alerte par mail en cas d'incidents techniques, est globalement assez simple à installer et à utiliser et nécessite peu de ressources mais manque de lisibilité par moments pour certains graphiques.

Finalement, notre choix se portera sur Nagios, car bien qu'il soit plus difficile d'accès que les autres, il dispose d'une grande communauté qui alimente la documentation régulièrement, informe et donne des conseils en cas de problème sur les forums et crée des plugins. Avec son large panel de plugins disponibles, Nagios est l'outil de supervision le plus complet et si on veut représenter les données dans des graphiques, on peut coupler Nagios et Cacti.

## 4.2 Mise en place d'un serveur Nagios

### 4.2.1 Mise en place du Serveur

Pour mettre en place le serveur Nagios, mon tuteur Mr Boss m'a confié un serveur physique. Je l'ai donc booté\* avec la dernière version du système d'exploitation Debian, à savoir la version 10 dit « Buster ». Je l'ai configuré de sorte que :

- Il ait un serveur SSH\* disponible
- Il soit configuré en ipv4\*
- Il ait l'adresse 192.168.0.240
- Sa passerelle par défaut soit 192.168.0.1

Une fois le serveur opérationnel, nous l'avons placé dans la baie, la salle où tous les serveurs en fonction se trouvent et sont connectés au réseau de l'entreprise. De cette manière, j'ai pu accéder au serveur par connexion SSH

### 4.2.2 Installation de Nagios

Une fois connecté au serveur, tout se fait par lignes de commandes. Pour que Nagios fonctionne il a d'abord fallu installer certains paquets : apache2\* et PHP\* sont indispensables car on y accède via le Navigateur. J'ai aussi eu à installer des bibliothèques graphiques, les outils de compilation standard (Nagios est un programme compilé en C\*, le compilateur GCC\* et ses outils associés sont donc indispensables) ainsi que Perl dont les libraires serviront à faire marcher certains plugins, notamment le SNMP.

J'ai ensuite créé l'environnement Nagios c'est-à-dire son utilisateur, son groupe et son répertoire de travail, ainsi que l'utilisateur qui fera tourner les processus du serveur web apache2. Une fois toutes ces étapes de préparation effectuées, j'ai téléchargé l'archive des sources de Nagios, je l'ai décompressée et l'ai compilée. J'ai par la suite mis en place l'arborescence Nagios, installé les composants nécessaires au démarrage de Nagios. Une fois toutes ces étapes effectuées, j'ai démarré les services apache2 et Nagios et depuis le navigateur de l'ordinateur en allant à l'adresse <http://192.168.0.240/nagios>, on accède à l'interface de base.

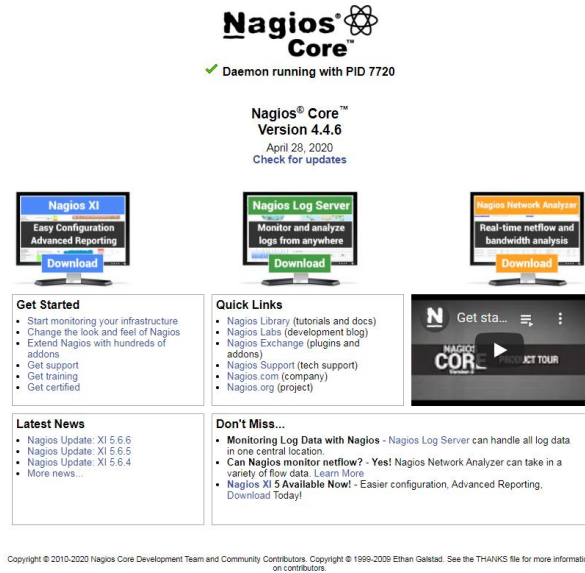


Figure 10 : l'interface Nagios

Nagios est donc installé, mais pour l'instant rien n'est configuré. J'ai donc téléchargé les plugins qui serviront à superviser différents services, puis j'ai commencé à modifier les fichiers de configuration :

```
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg
cfg_file=/usr/local/nagios/etc/objects/hostclients.cfg
cfg_file=/usr/local/nagios/etc/objects/hostgroups.cfg
cfg_file=/usr/local/nagios/etc/objects/notifications.cfg
```

Figure 11 : fichier nagios.cfg

Dans le fichier de configuration principal, j'ai écrit l'emplacement de tous les autres fichiers de configuration de Nagios, puis j'ai créé ces fichiers pour qu'ils aient chacun un rôle. Je vais donc vous les expliquer un par un.

```
define command {
    command_name    check_snmp
    command_line    $USER1$/check_snmp -H $HOSTADDRESS$ $ARG1$
}

define command {
    command_name    check_http
    command_line    $USER1$/check_http -I $HOSTADDRESS$ $ARG1$
}
```

Figure 12 : configuration des commandes dans le fichier commands.cfg

Le fichier `commands.cfg` sert à définir les commandes que l'on pourra utiliser pour vérifier les services que l'on veut. Certaines sont configurées de base, de mon côté j'ai ajouté les deux commandes `snmp_load` car c'est ce que l'on va utiliser pour vérifier le protocole SNMP.

Le fichier `contacts.cfg` sert à définir à quelle adresse seront envoyés les mails de notification. Pour que l'envoi des mails fonctionne, j'ai configuré le serveur de messagerie « Postfix » en lui assignant le relai SMTP de l'entreprise

```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = Nagios.sprint-telecom.fr
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $myhostname, Nagios.sprint-telecom.fr, localhost.localdomain, , localhost
relayhost = smtp.sprint-telecom.fr
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

**Figure 13 : fichier de configuration de Postfix**

Le fichier `timeperiods.cfg` définit les différentes plages horaires possibles pour l'envoi des notifications : de base les notifications sont réglées sur un système 24h/24, 7j/7 mais sont définies dans ce fichier d'autres possibilités comme les horaires de travail (du lundi au vendredi de 9 à 17h), du 24x7 sans les vacances. On peut dans ce fichier créer d'autres possibilités, mais dans notre cas j'ai préféré rester sur la configuration par défaut.

Le fichier `templates.cfg` sert à indiquer le modèle à suivre pour définir chaque objet dans les autres fichiers.

Le fichier `notifications.cfg` définit la commande qui permettra d'envoyer les mails à l'aide de Postfix.

Les fichiers `hostclients` et `hostgroups` servent à définir les hôtes que l'on va remplir ainsi que le groupe auquel ils appartiennent :

```
define hostgroup {
    hostgroup_name    adsl
    alias             ADSL
}

define hostgroup {
    hostgroup_name    vdsl
    alias             VDSL
}
```

**Figure 14 : définition des groupes dans le fichier `hostgroups.cfg`**

Une fois tous groupes définis, j'ai rentré les hôtes dans le fichier `hostgroups`, en choisissant les services à vérifier et les paramètres de notification :

```

#GIE R2 SECURITE
define host{
    use network-host
    host_name          gie_r2_securité
    alias              GIE R2 Sécurité
    address            85.  .111.38
    hostgroups         mesclients,TP_Link,adsl
    check_interval     1
    notification_interval 60
}

define service{
    use                generic-service
    host_name          gie_r2_securité
    service_description PING
    check_command      check_ping!100.0,20%!500.0,60%
    notifications_enabled 0
}

define service{
    use                generic-service
    host_name          gie_r2_securité
    service_description CPU load One Minute Interval
    check_command      snmp_load_1m!-C public
    notifications_enabled 0
}

```

**Figure 15 : définition d'un hôte dans hostclients.cfg**

Ici on peut voir les paramètres utilisés pour définir ce client :

- host\_name : identifiant de l'hôte
- alias : nom complet de l'hôte
- address : adresse IP de l'hôte
- hostgroups : groupes auquel l'hôte appartient (mesclients pour tous, suivi de la marque et du type de connexion)
- check\_interval : nombre d'unités de temps entre chaque check vers l'hôte en minutes. Je l'ai mis à un pour avoir une vérification régulière.
- notification\_interval : nombre d'unités de temps entre deux envois de mail en cas d'alerte. Si ce routeur cesse de fonctionner, on recevra un mail toutes les heures le signalant jusqu'à ce que le problème soit réglé.

Il y a ensuite les services :

Le premier va checker le ping, afficher l'état du service en « warning » si les paquets mettent plus de 100ms pour arriver ou s'il y a une perte de 20% des paquets, en « critical » pour un délai de 500ms ou plus de 60% de perte des paquets. J'ai désactivé les notifications car elles seraient redondantes avec celles de l'hôte en cas de panne.

Le second va vérifier toutes les minutes que le protocole SNMP fonctionne bien. J'ai aussi désactivé les notifications pour celui-là. Pour qu'il fonctionne, il a fallu accéder à chacun des routeurs pour activer SNMP.

Ainsi, j'ai rentré par ce procédé les 83 routeurs installés chez les différents clients de Sprint Telecom en spécifiant à chaque fois le type de routeur et le type de connexion, pour que lorsque l'on retourne sur Nagios via le navigateur, on observe tous nos hôtes classés par groupes avec leur état ainsi que celui de leur service.

Host Status Totals			
Up	Down	Unreachable	Pending
75	8	0	0
All Problems		All Types	
6		83	

Service Status Totals				
Ok	Warning	Unknown	Critical	Pending
101	1	46	23	0
All Problems		All Types		
70		171		

Service Overview For All Host Groups

Fibre SFR (FFTH_SFR)			
Host	Status	Services	Actions
AD_Services	UP	1 OK 1 UNKNOWN	
Hotel_Modernisme	UP	1 OK 1 UNKNOWN	
Kallisto_Bureau	UP	1 OK 1 UNKNOWN	
Kallisto_Résidents	UP	1 OK 1 UNKNOWN	
Maison_Posture_Velivoy	UP	1 OK 1 CRITICAL	

TP Link (TP_Link)			
Host	Status	Services	Actions
Azurdom_Aubagne	UP	1 OK	
Capstan_Pythées_TP	UP	2 OK	
Despy_Blancarde_2	UP	1 OK	
Etude_de_provence_Chateau	UP	2 OK	
Etude_de_provence_Vente_30	UP	1 OK 1 UNKNOWN	
Hexo_Tradition	UP	1 OK	
JLD_Paradis	UP	2 OK	
Maitre_Barbis	UP	2 OK	
Ollier_et_Associés_TP	UP	2 OK	
Pharmacie_Aurore	UP	2 OK	
alicanta_doussiere_2	DOWN	2 CRITICAL	
alicanta_hotel_doussiere	UP	2 OK	
archimbaud_docks	UP	1 OK	
auto_service_martegaux	UP	1 CRITICAL	
cardinetta	UP	2 OK	
chateau_martegaux	UP	2 OK	
franchi	UP	2 OK	
hoig	UP	1 OK	
les_ramons	UP	2 OK	
maitre_bdt	DOWN	2 CRITICAL	
pharmacie_rossero	DOWN	2 CRITICAL	
rdgises_sotus_servants	UP	2 OK	
syndical_pharmaciens_ver	UP	2 OK	

ADSL (adsl)			
Host	Status	Services	Actions
Cabaret_Jauffret	DOWN	2 CRITICAL	
Capstan_Pythées_Netgear	DOWN	2 CRITICAL	
Capstan_Pythées_TP	UP	1 OK	
Comer_Food	UP	1 UNKNOWN	
Etude_de_provence_Vente_30	UP	1 OK 1 UNKNOWN	
Etal	UP	2 OK	
KC_Vitrolles	UP	2 OK	
La_Pagerie_Sonicwall	UP	1 OK	
Oasis_13006	UP	1 OK 1 UNKNOWN	
Oasis_Aubagne	UP	1 UNKNOWN	
padding_Bat	DOWN	2 CRITICAL	
Pharmacie_Aurore	UP	1 OK	
Pharmacie_Midi	UP	1 UNKNOWN	
Pharmacie_Perrier	UP	1 OK 1 CRITICAL	
Tacos_Aix	UP	1 OK 1 UNKNOWN	
Tacos_Marseille	UP	1 OK	
alicanta_doussiere_2	DOWN	2 CRITICAL	
alicanta_hotel_doussiere	UP	2 OK	
enapl_ver_adsl	UP	1 CRITICAL	
archimbaud_docks	UP	1 OK	
auto_service_martegaux	UP	1 OK 1 CRITICAL	

Figure 16 : interface de Nagios après configuration complète

En cliquant sur n'importe quel Hôte, on aura accès à ses informations, à savoir son nom complet, son adresse IP, son statut, les groupes auquel il appartient ainsi que les actions réalisables depuis Nagios, c'est-à-dire les paramètres de checks et de notifications pour l'hôte et ses services.

Host State Information

Host Status:	UP (for 1d 8h 25m 24s)
Status Information:	PING OK - Packet loss = 0%, RTA = 30.24 ms
Performance Data:	rta=30.243999ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0
Current Attempt:	1/10 (HARD state)
Last Check Time:	06-26-2021 12:27:52
Check Type:	ACTIVE
Check Latency / Duration:	0,000 / 4,000 seconds
Next Scheduled Active Check:	06-26-2021 12:28:52
Last State Change:	06-25-2021 04:32:52
Last Notification:	N/A (notification 0)
Is This Host Flapping?	NO (0,00% state change)
In Scheduled Downtime?	NO
Last Update:	06-26-2021 12:28:10 ( 0d 0h 0m 6s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

Host Commands

- Locate host on map
- Disable active checks of this host
- Re-schedule the next check of this host
- Submit passive check result for this host
- Stop accepting passive checks for this host
- Stop obsessing over this host
- Disable notifications for this host
- Send custom host notification
- Schedule downtime for this host
- Schedule downtime for all services on this host
- Disable notifications for all services on this host
- Enable notifications for all services on this host
- Schedule a check of all services on this host
- Disable checks of all services on this host
- Enable checks of all services on this host
- Disable event handler for this host
- Disable flap detection for this host
- Clear flapping state for this host

Host Comments

Add a new comment Delete all comments  
 Entry Time Author Comment Comment ID Persistent Type Expires Actions  
 This host has no comments associated with it

Figure 17 : Détail d'un hôte sur Nagios

Pour finir, à chaque changement d'état d'un hôte, on aura une notification sur la boîte mail créée dans ce but. Cela va ainsi permettre de réagir au plus vite en cas de panne, mais aussi d'être alerté si le routeur est remis en état.

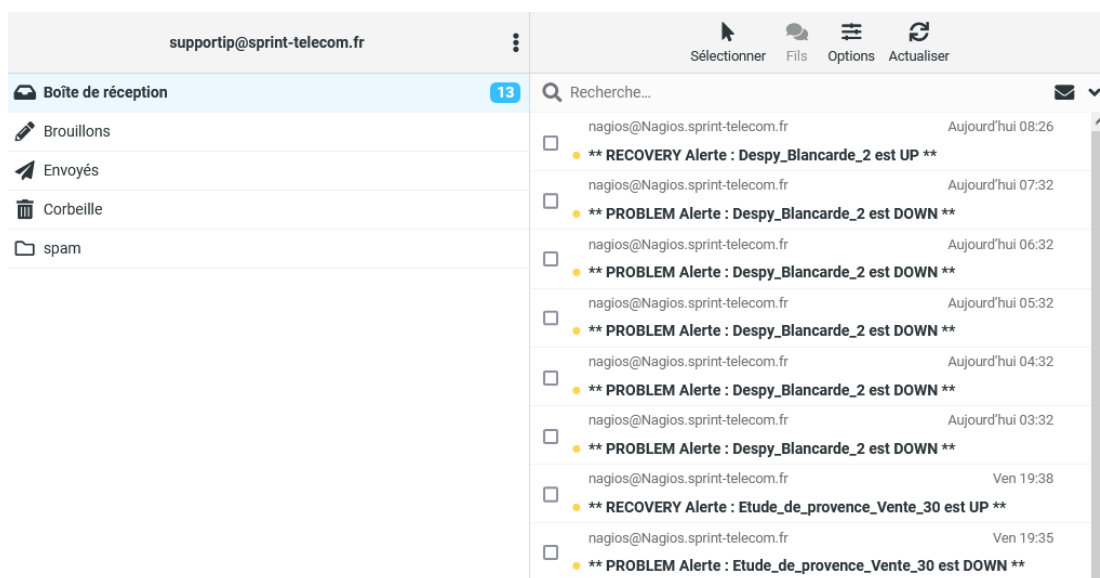


Figure 18 : notifications envoyées par Nagios

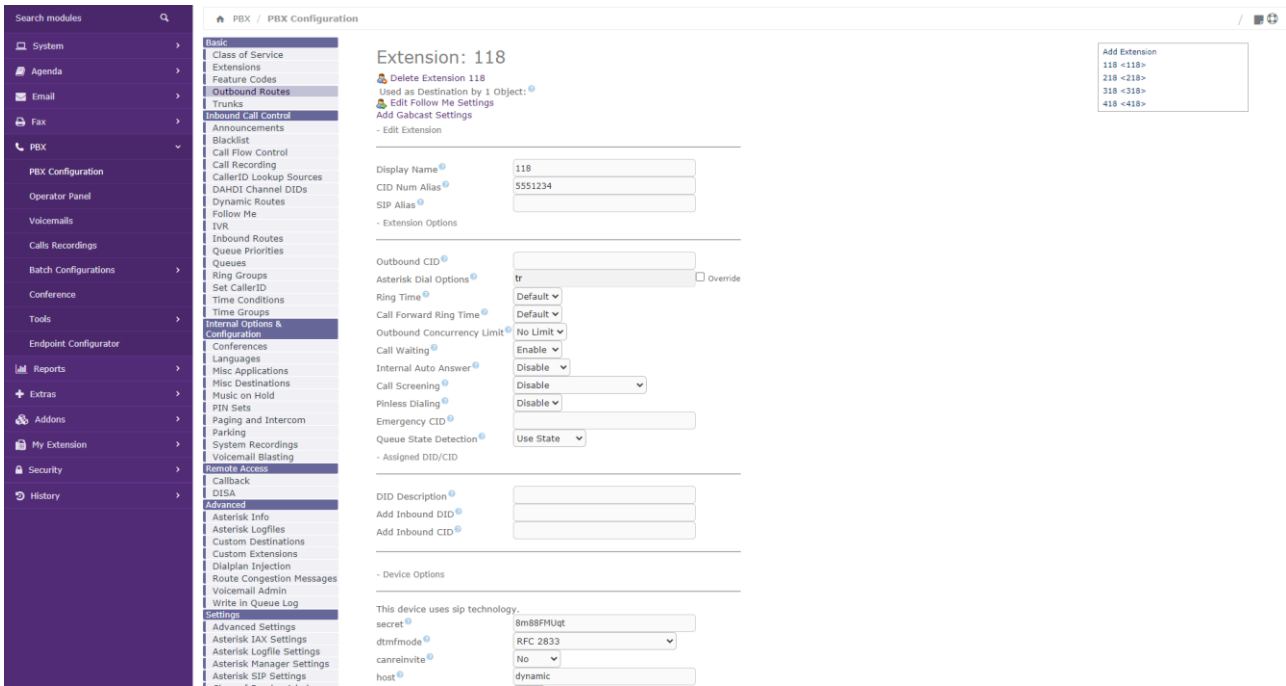
## 5 Configuration d'un PBX

### 5.1 Prise en main avec un serveur Issabel

Afin de me familiariser avec la configuration de la VoIP, on m'a chargé de configurer plusieurs Téléphones avec un serveur Issabel, qui est un logiciel PBX de communications unifiées OpenSource, offrant une configuration, une gestion et des rapports conviviaux basés sur le Web pour la téléphonie.

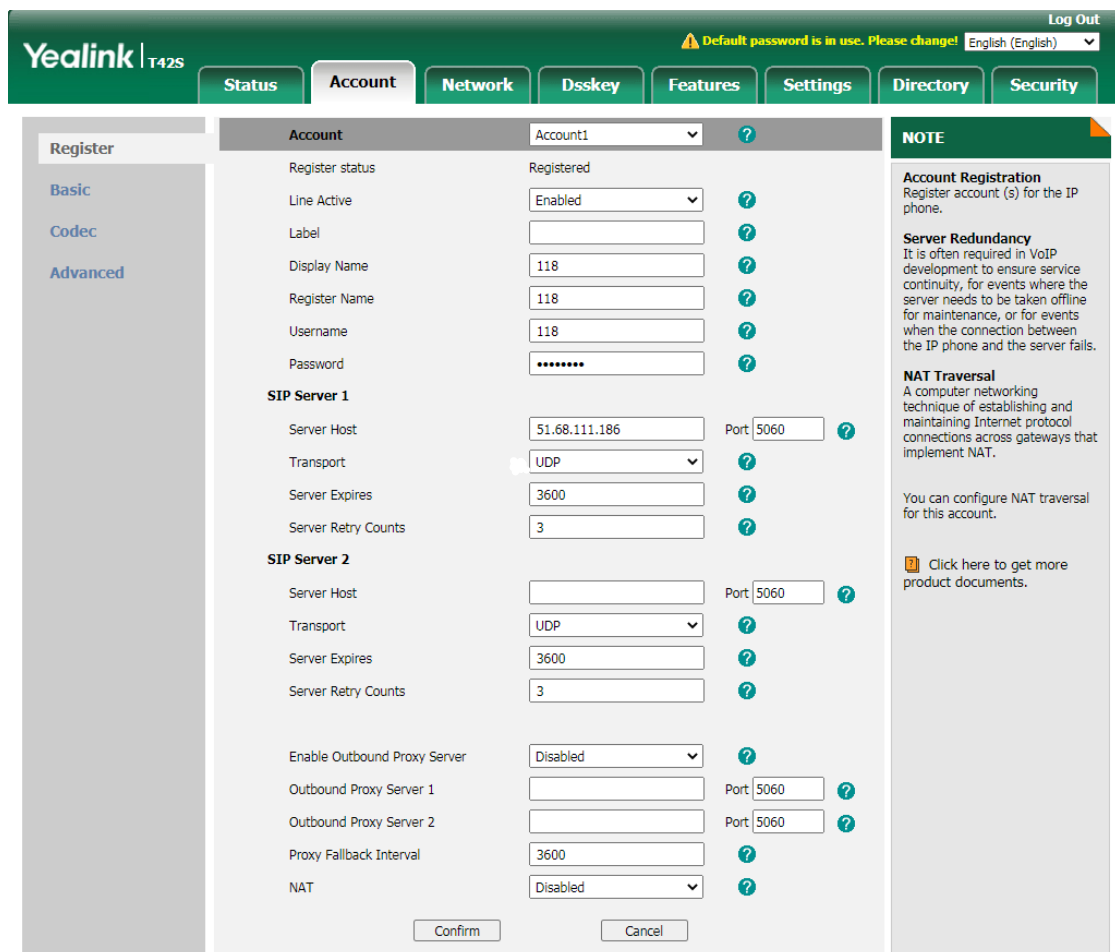
Issabel est basé sur des versions open-source d'Elastix, Asterisk, FreePBX, HylaFAX, Openfire et Postfix et fournit des fonctionnalités de PBX, fax, messagerie instantanée et serveur de messagerie. Issabel utilise le protocole SIP\*, qui permet d'établir une session entre plusieurs participants, la modifier ou la terminer. SIP est le protocole le plus utilisé en VoIP

J'avais donc à ma disposition un Thomson ST2030, un Yealink T42S, un Gigaset C530IP et mon propre téléphone portable. La première étape est d'accéder au serveur Issabel et de créer les « extensions », qui permettront la connexion avec les téléphones.



**Figure 19 : création d'extensions sur Issabel**

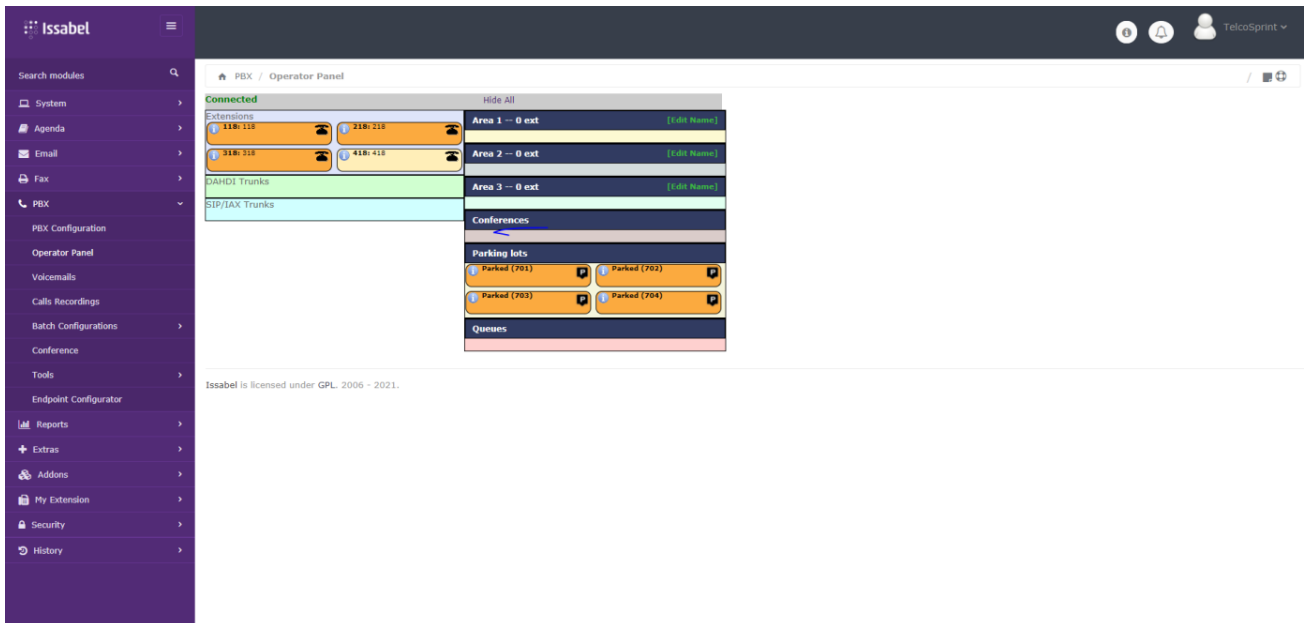
Pour chaque extension, j'ai choisi un nom correspondant au numéro du téléphone ainsi que le mot de passe qui servira à l'authentification via le protocole SIP. J'ai par la suite connecté chacun des téléphones au réseau afin qu'ils obtiennent une adresse IP grâce au DHCP\* pour pouvoir les paramétrer en accédant à leur configuration, en tapant leur adresse dans le navigateur.



Copyright © 2021 Yealink Inc. All rights reserved.

**Figure 20 : interface de configuration du Yealink**

Sur le téléphone, j'ai rempli de sorte que les informations correspondent à celles rentrées dans Issabel. L'adresse dans le champ « Server Host » est celle du serveur Issabel et le mot de passe est celui que l'on a choisi plus tôt pour l'extension. De cette manière, l'authentification se fera et permettra la connexion. Le protocole SIP se fait par défaut sur le port 5060. Une fois toutes ces informations rentrées, lorsqu'on vérifie dans le panel opérateur sur Issabel, on voit que le téléphone est connecté. J'ai répété cette opération avec les deux autres téléphones ainsi que mon portable via une application gratuite, et j'ai pu passer des appels.



**Figure 21 : Le panel opérateur avec les quatre extensions configurées**

J'ai essayé d'imaginer le plus de scénarii possibles, essayé des transferts d'appels et j'ai créé des groupes d'appels avec différentes stratégies :

- Les téléphones sonnent tous en même temps
- Les téléphones sonnent l'un après l'autre mais un à la fois
- Un premier téléphone sonne, puis après quelques secondes le deuxième sonne aussi, puis le troisième
- Le premier téléphone disponible sonne

## 5.2 Mise en pratique sur Alcatel

Une fois l'outil pris en main, j'ai pu passer à la pratique en configurant avec mon tuteur Mr BOSS un PBX en vue de le placer chez un client. Dans cette situation, le client envoie à Sprint Telecom un document spécifiant les besoins téléphoniques, à savoir le nombre de postes à installer, le nom qu'il faut leur attribuer et le type d'appareil et l'entreprise se charge de répondre à cette demande. Pour configurer le PBX, nous avons utilisé le logiciel OMC.

OMC est l'outil de configuration et d'administration des appareils d'Alcatel Lucent. C'est un logiciel permettant de mettre en place sur le PBX

- Les touches programmables des postes
- Les plages horaires
- Le réseau
- L'accès internet
- Les fonctions voix du système
- Les groupements d'appels
- Les discriminations téléphoniques

Pour s'y connecter, nous avons mis l'adresse du PBX en 192.168.1.246, celle de l'ordinateur en 192.168.1.1 avec l'adresse du PBX en passerelle et nous avons utilisé la version d'OMC adaptée au PBX. Nous avons branché le téléphone opérateur sur un port digital (DC in) et nous avons commencé la configuration du PBX.

La première étape était de changer les mots de passe par défaut et de vérifier la date et l'heure du PBX. Nous avons ensuite rentré chaque poste avec le nom et le numéro correspondant. Il a ensuite fallu configurer chaque poste afin qu'ils aient des touches d'appels rapides avec un ordre précis pour chaque poste, des droits ou non de transfert et d'interception d'appels et un renvoi dynamique avec un délai approprié.

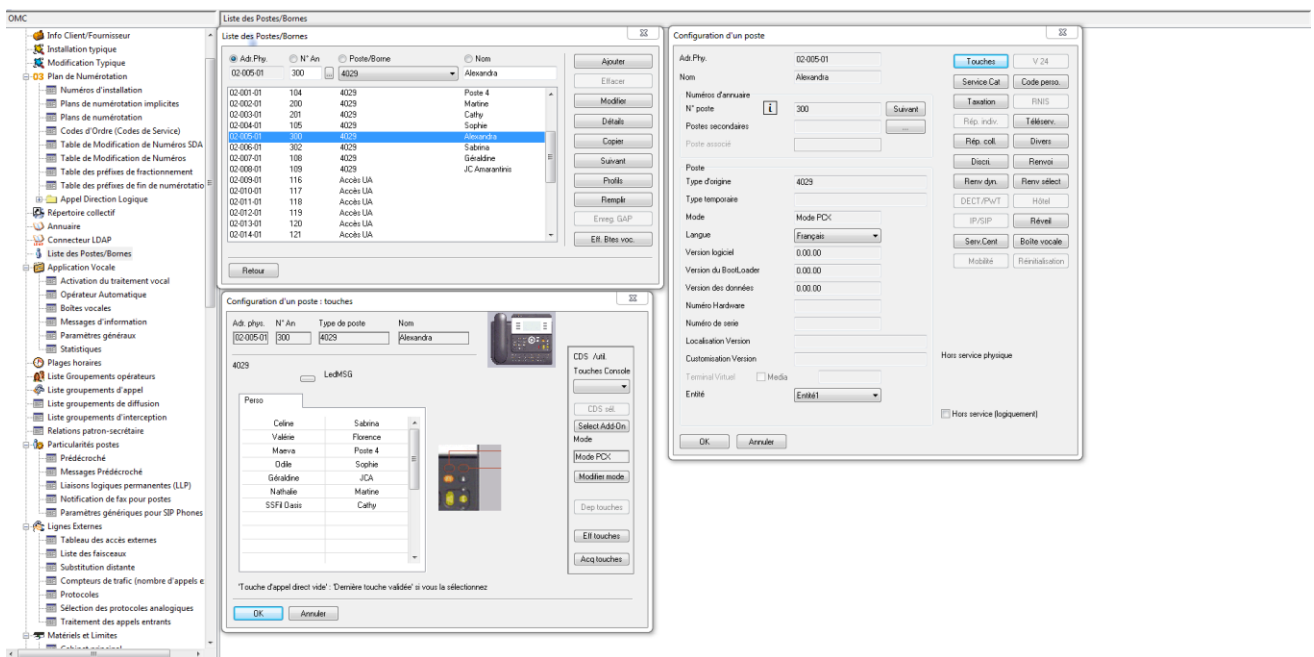


Figure 22 : Configuration du PBX à l'aide d'OMC

## 6 Conclusion

Ce stage de dix semaines au sein de l'entreprise Sprint Telecom m'a fortement épanoui et m'a beaucoup apporté.

Tout d'abord, j'ai eu la responsabilité d'une mission que je devais mener en autonomie. Mettre en pratique mes connaissances acquises à l'IUT m'a permis de progresser fortement en Administration système, en téléphonie, de beaucoup mieux comprendre et maîtriser le système d'exploitation Debian et de progresser en télécommunications en général, mais cela m'a aussi entraîné à chercher par moi-même. Et lorsque j'étais bloqué, je pouvais toujours compter sur Mr Boss ou Mr Capelle pour qu'ils m'apportent leurs connaissances.

Ce stage m'a aussi permis d'élargir ma conception du travail en général, ayant beaucoup d'interactions avec les membres de Sprint Telecom, que ce soit avec Mr Boss mais aussi avec Mr Viale ou Mme Payen ou encore avec les clients que j'ai pu rencontrer.

J'ai aussi pu travailler mes compétences d'écoute, de compréhension et de travail d'équipe que ce soit pour appliquer les consignes que chacun d'entre eux pouvaient me donner lorsqu'ils avaient besoin de mon aide, ou encore pour rédiger une documentation afin d'expliquer comment Nagios fonctionne, pour que tout le monde puisse l'utiliser ou ajouter des hôtes.

J'ai appris d'autre part la vie en entreprise, les relations avec les clients, le respect entre collègues ou encore celui de l'espace de travail.

Enfin, ce stage rentrant totalement dans le domaine d'activité qui m'intéresse professionnellement parlant, j'ai pu commencer à maîtriser des outils et des technologies qui me serviront ultérieurement en tant qu'ingénieur.



## 7 Remerciements

Je tiens à témoigner de ma plus profonde et sincère gratitude à toutes les personnes qui ont permis à ce stage de se dérouler.

Tout d'abord, je tiens à remercier mon tuteur Thomas BOSS, qui m'a accueilli dans son entreprise et m'a accompagné tout le long de mon stage, toujours avec beaucoup de bienveillance et de pédagogie. Il m'a accordé sa confiance et n'a pas hésité à me confier du matériel ou me laisser faire des essais dans le but de me faire progresser.

Je remercie toute l'équipe de Sprint Telecom, Renaud VIALE et Magali PAYEN pour leur gentillesse, leur patience et leur bonne humeur ainsi que Stéphane CAPELLE qui, malgré la distance, a su trouver du temps pour m'aider lorsque je rencontrais certains problèmes dans mon travail que je n'aurais pu résoudre seul.

Enfin, je tiens à remercier l'équipe de ChronosportShop à savoir Thomas MOUREN, Nicolas PAGLIARELLA et Aurélie PEREIRA qui partageaient les locaux et qui ont toujours été sympathiques.

Travailler pendant ces dix semaines dans cette équipe a été pour moi un réel plaisir, toujours avec une ambiance rassurante et agréable



## 8 Glossaire

**DUT** : Diplôme Universitaire de Technologie

**PBX** : Private Branch Exchange ou autocommutateur téléphonique privé en français

**VPN** : Virtual Private Network ou réseau virtuel privé, système permettant de créer un lien direct entre des ordinateurs distants

**PME** : Petites ou Moyenne Entreprise

**PMI** : Petites et Moyennes entreprises Industrielles

**TPE** : Très Petite Entreprise

**IP, IPV4** : Internet Protocol, Protocole informatique de connexion qui gère la transmission des données par Internet. IPv4 en est la 4<sup>e</sup> version et la première à avoir été largement déployée

**VoIP** : Voice over IP ou voix sur IP

**Boot** : Démarrage d'un ordinateur et chargement du programme initial

**GSM** : Global System for Mobile Communications, standard numérique de 2<sup>e</sup> génération (2G)

**OpenSource** : logiciel dont le code est accessible, modifiable et distribuable par n'importe qui

**CPU** : Central Processing Unit ou Processeur en français

**IHM** : Interaction Homme Machine

**SSH** : Secure Shell, un protocole de communication sécurisé

**Apache** : logiciel de serveur web multiplateforme gratuit et open-source

**PHP** : Hypertext Preprocessor, langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur http

**C** : langage de programmation impératif généraliste, de bas niveau

**GCC** : Compilateur spécialement créé pour le C

**ADSL** : Asymmetric Digital Subscriber Line, Ligne d'abonné numérique asymétrique, c'est une technologie d'accès à Internet sur ligne téléphonique. Une partie de la bande passante est dédiée à la transmission de données multimédias et une autre à la voix

**SNMP** : Simple Network Management Protocol, protocole simple de gestion de réseau qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance

**SMTP** : Simple Mail Transfer Protocol, utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique

**SIP** : Session Initiation Protocol

**DHCP** : Dynamic Host Configuration Protocol, protocole de configuration dynamique des hôtes en français, qui permet d'obtenir automatiquement une adresse IP lorsque l'on se connecte à un réseau



## 9 Bibliographie

*XMedius, Qu'est-ce qu'un système PBX. [en ligne] Mis à jour le 28/08/18. Disponible à l'adresse :*

*<https://www.xmedius.com/fr/blogue/quest-ce-quun-systeme-pbx/>*

*3CX, Qu'est-ce que le SIP – Session Initiation Protocol ?[en ligne] Disponible à l'adresse :*

*<https://www.3cx.fr/voip-sip/sip/>*

*Thomas Mouren, Rapport de stage chez Sprint Telecom, 2014*

*Mickael Dorigny, Monitoring : supervision et métrologie [en ligne] Mis à jour le 24/09/2018,*

*Disponible à l'adresse :*

*<https://www.it-connect.fr/monitoring-supervision-et-metrologie/>*

*Dossier Présentation de Sprint Telecom*