Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Interventions au service de la commune

Alexandre BATTISTELLA

MAIRIE DE CABRIÈS

Responsable entreprise : Maxime BRUNET

Responsable académique : Sébastien SANCHEZ

2024

Table des matières :

I – Introduction : [↑]

1 – Règles : [↑]

Règle 1) Tout acronyme est littéralement détaillé dans la page « **3 - Glossaire des Acronymes** », dans leur ordre d'apparition.

Règle 2) Tout acronyme écrit dans ce document l'est en **gras** ; quand un acronyme apparaît pour la première fois, il est également **souligné** et parfois littéralement détaillé.

Règle 3) Tout terme à expliquer (selon moi) l'est dans la partie « **4 - Glossaire des Compléments** », dans leur ordre d'apparition.

Règle 4) Tout terme à expliquer est écrit en **vert gras** la première fois qu'il apparaît.

Règle 5) Tout acronyme qui est également un terme à expliquer sera écrit, la première fois qu'il apparaît, en **vert gras souligné**.

Exemples :

PC est un acronyme qui apparaît pour la première fois.

PC est un acronyme qui n'apparaît pas pour la première fois.

image disque est un terme à expliquer qui apparaît pour la première fois.

image disque est un terme à expliquer qui n'apparaît pas pour la première fois.

OSI est un acronyme qui est également est un terme à expliquer qui apparaît pour la première fois.

Règle 6) Tout acronyme ou terme à expliquer qui apparaît pour la première fois est cliquable via **[CTRL + CLIC GAUCHE]** ou **[CLIC GAUCHE]**. Cliquer dessus vous redirigera vers la partie glossaire, où il est possible de naviguer via des icônes intuitives (**[↓]** **[↑]** **[↑]**).

Règle 7) Tout titre de partie, sous-partie et sous-sous-partie visible dans la table des matières est cliquable via la même combinaison qu'au-dessus. Cliquer dessus vous amènera à la partie du document correspondante. Il est possible de revenir, depuis une partie, sous-partie ou sous-sous-partie à la table des matières via ( ).

Règle 8) Toute photographie utilisée dans ce document provient de moi. Certaines captures d'écrans proviennent de moi ou du **SIGV** (encadrées en **vert foncé**), d'autres non (encadrées en **rouge foncé**).

Règle 9) Toute commande utilisable dans une console de commande et qui aurait pu être utilisée ou qui fut utilisée dans le cadre de mon travail sera citée en **marron gras**.

Règle 10) Les règles précédentes ne s'appliquent plus forcément dans la partie **IV**.

2 – Contexte :

J'ai donc réalisé mon stage dans une collectivité qu'est la mairie de Cabriès. Pour ce qui est de la gestion côté réseau, la collectivité est en fait rattachée à un organisme : le **SIGV** (**S**yndicat **I**ntercommunal **G**rand **V**allat).

Le **SIGV** est le garant des connexions réseaux, de la téléphonie **IP**, de l'administration, de la maintenance et globalement du bon fonctionnement de toute l'infrastructure informatique liée aux **3** communes qui lui sont rattachées : Cabriès, Bouc-Bel-Air et Simiane-Collongue (des communes très proches géographiquement).

Chaque commune contient un certain nombre de **sites**. Ainsi, on distingue **11** sites sur Cabriès, **19** sites sur Bouc-Bel-Air et **11** sites sur Simiane-Collongue.

Mon tuteur, ***Maxime BRUNET***, est chargé de la partie « Communication » de la commune de Cabriès. Ainsi, je fus (physiquement) par défaut à ses côtés, c'est-à-dire sur le site intitulé « Mairie Centrale », situé donc dans la commune de Cabriès (il s'agit bien sûr d'un des sites gérés par le **SIGV**).

Cela dit, je prépare actuellement un **BUT** Réseaux & Télécommunications parcours Cybersécurité, donc ce qui fut le plus intéressant pour moi dans ce cadre était de passer la plupart de mon temps auprès du **SIGV**, qui s'occupe comme énoncé plus tôt du côté administration réseau de tous les sites auxquels il est affilié. C'est là que je rencontrai ***Gabriel PRATI***, membre du **SIGV**. C'est auprès de lui que j'effectuai toutes les tâches qui suivirent.

Il est également important de savoir que j'arrivais ici en tant que stagiaire dans une période dite de « post-migration » de l'ensemble des trois communes. En fait, le projet commun de ces trois communes eut été de centraliser les équipements informatiques et les services liés à ces équipements, afin que le tout soit entre les mains du **SIGV** pour la gestion. Ainsi, chaque site fut devenu dépendant du **SIGV** du point de vue réseau. Grâce à ça, la gestion administrative de l'infrastructure réseau des trois communes s'en est retrouvée simplifiée.

Je précise pour la suite que lorsque je parle de configuration réseau mise en place par le **SIGV**, il peut s'agir soit d'une configuration actuelle et effective, soit d'une configuration cible (visée, voulue) qui n'est pas effective uniquement par manque de temps de configuration (c'est pour cela que je la considère en formulant de cette manière comme effective au fond). Il ne faut pas omettre que le **SIGV** est à l'heure où j'écris ce texte composé de trois personnes au total.

3 – Objectifs du stage :

Au-delà de l'objectif implicite qui fut de découvrir ce qu'est le monde professionnel, ou en tout cas le monde professionnel en collectivité, mes objectifs furent d'aider la commune à finaliser sa phase de migration ; il restait en effet quelques tâches à réaliser pour compléter la migration des équipements informatiques (formatage de **PCs** & Serveurs, déploiement de **PCs** portables/fixes, déploiement de bornes **WIFI**, déploiement de téléphones **IP**, mise à jour de l'Active Directory (**AD**) de la commune, résolution de problèmes divers, …).

Il y eut parmi ces missions des tâches que je pus réaliser seul, mais certaines nécessitèrent l'intervention de M. Prati (puisqu'il y eut besoin de modifier des configurations de Switches sur lesquels il avait la main notamment). Globalement, j'accompagnai souvent Gabriel lors de ses différentes interventions sur des sites affiliés au **SIGV**.

II – Le contexte architectural

I – Introduction ::

1 – L’architecture générale :

Voici ci-dessous un plan d’architecture générale du **SIGV** et ce à quoi il est rattaché (**Figure 1**) :

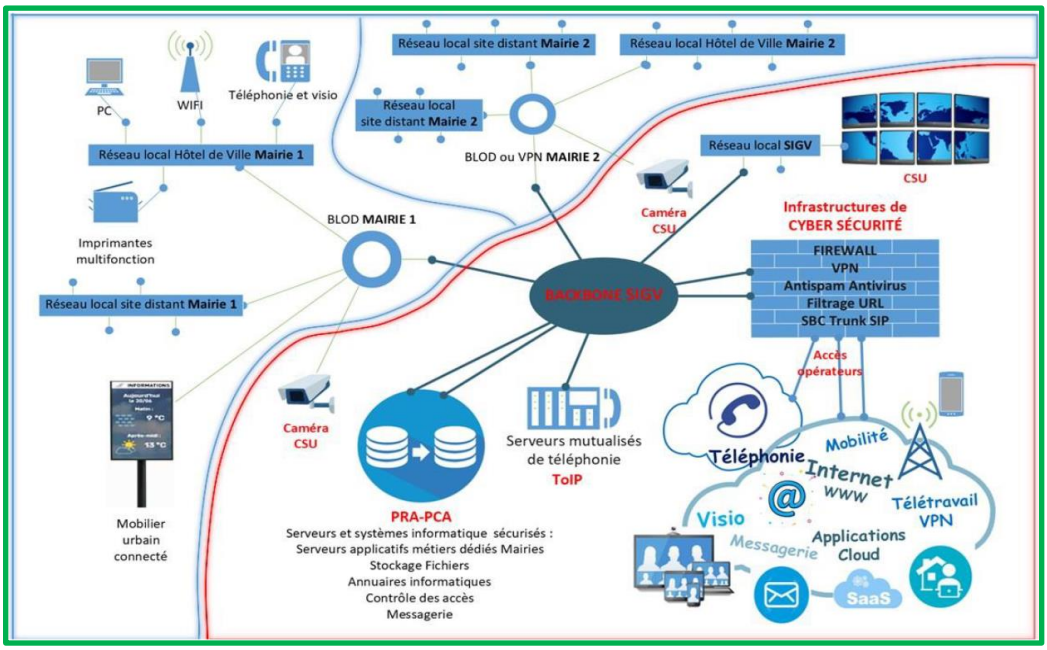

Figure 1

On voit tout d'abord que le **SIGV** est l'élément central de toute l'architecture regroupant les trois communes, jusque-là rien de surprenant. Le **SIGV** est ici représenté par le nom « **BACKBONE SIGV** » sur le schéma. Une zone de backbone peut être associée au cœur de réseau dans l'architecture générique des réseaux **LAN**, à savoir la couche qui assure un transport optimal des informations entre les sites.

Le **SIGV** est relié à plusieurs services :

- **Serveurs mutualisés de téléphonie (ToIP) :** la téléphonie, au sein des sites affiliés au **SIGV**, est gérée en **ToIP** (**T**elephony **o**ver **I**nternet **P**rotocol), ce qui signifie que tout le système de téléphonie des trois communes fonctionne en **IP** depuis chaque téléphone ; ainsi, en plus de la voix, c'est bien tout le système de téléphonie qui va transiter et fonctionner sur le réseau **IP**. Cela s'effectue grâce à un [IPBX. Concrètement, chaque téléphone est branché directement sur le réseau informatique voulu, à la manière d'un ordinateur (en réalité, sur des postes pourvus de téléphones **IP**, c'est le boîtier téléphonique qui est relié au réseau interne, et le **PC** qui est relié au boîtier téléphonique en tant qu'équipement final). Cela permet un pilotage optimal de la téléphonie. Ces serveurs mutualisés permettent logiquement un accès au ***CallManager*** (logiciel de gestion édité par Cisco permettant de traiter et configurer le système d'appels dans un certain environnement).

- **PRA-PCA :** ces deux acronymes signifient respectivement « **Plan de Reprise d'Activité** » et « **Plan de Continuité d'Activité** ». Le « **Plan de Reprise d'Activité** » désigne toutes les procédures qui seront mises en place, le jour où une panne survient, pour rendre à nouveau opérationnel un système d'informations, et ce le plus rapidement possible. Le « **Plan de Continuité d'Activité** » quant à lui, désigne toutes les procédures qui sont actuellement mises en place pour que, le jour où une panne survient, toutes les applications critiques nécessaires au bon fonctionnement d'un système d'informations soient quand même disponibles (cette stratégie est généralement plus coûteuse que le **PRA**, qui assume une coupure temporaire). Ainsi, ce qu'on voit sur le schéma et ce qu'on doit en comprendre, c'est que tous les serveurs (sécurisés, applicatifs métiers), stockages fichiers, annuaires informatiques, contrôle des accès et messagerie sont dupliqués et sauvegardés autre part que dans leurs emplacements initiaux, afin de pouvoir garantir et appliquer les plans de **PRA** ou **PCA** selon les cas de figures (grâce à de la **redondance**).

- **Infrastructures de CYBER SÉCURITÉ :** elles constituent l'ensemble des infrastructures de cyber sécurité mises en place entre l'extérieur et le cœur de réseau représenté par le **SIGV**. Le Firewall pour le filtrage, le [VPN pour les connexions à distance, l'Antispam Antivirus pour éviter les requêtes frauduleuses, le Filtrage **URL** pour bloquer/autoriser l'accès à certaines pages WEB, ou encore le [SBC [↑]Trunk SIP permettant d'établir le lien entre l'**IPBX** du **SIGV** (opérateur interne du point de vue des

agents, en fait) et l'extérieur (réseau du fournisseur de services télécom, ici Orange) pour ce qui est de la téléphonie **IP**.

- **BLOD MAIRIE 1 & 2 :** ce qu'on entend ici par « **BLOD MAIRIE 1 & 2** », c'est « un point d'accès à toute l'infrastructure réseau d'une certaine mairie/commune ». Ce schéma ayant été réalisé avant l'incorporation de la commune de Cabriès à l'infrastructure réseau gérée par le **SIGV**, seulement les deux autres mairies apparaissent. Au-delà de ces points d'accès, du point de vue du **SIGV**, on retrouve tous les sites affiliés aux différentes communes, avec les infrastructures qui s'en suivent et les différents services liés auxdites communes (**WIFI**, téléphonie et visio, **PCs**, imprimantes, ...).
  Il est important de comprendre que chaque **BLOD** de MAIRIE (qui constituent donc l'ensemble des sites affiliés à une certaine commune) possède en son sein un site qui fait office de **site centralisateur** ; c'est donc par ce site qu'on peut au final relier deux sites d'un même **BLOD** ensemble, tout comme c'est depuis ce site qu'est établie la liaison vers le **SIGV**. Voici un schéma complémentaire pour comprendre (**Figure 2**) :

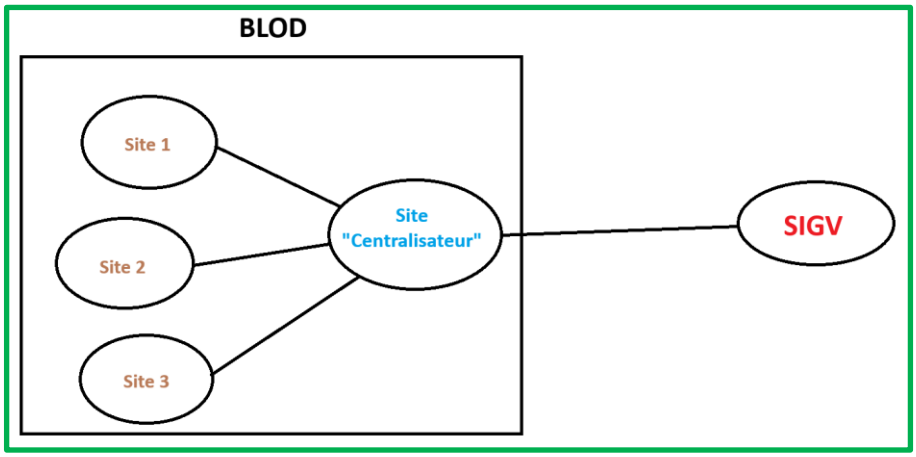

Figure 2

Dans le cas de la commune de Cabriès par exemple, le site centralisateur est le site de la Mairie Centrale ; c'est donc de là que part la liaison en direction du **SIGV**.

2 – Les réseaux :

Pour des raisons de confidentialité, je n'utiliserai pas de valeurs précises concrètes réelles pour expliquer l'adressage utilisé dans le cadre de l'architecture complète gérée par le SIGV pour les trois communes impliquées. Aussi, les valeurs que je prends pour expliquer sont purement aléatoires à chaque fois.

Au sein de toute l'infrastructure gérée par le **SIGV**, de nombreux réseaux existent. Ce sont évidemment des réseaux privés. Parmi ces réseaux privés, on distingue les réseaux réservés aux serveurs (tels que des **NAS** ou des Switches par exemple), des réseaux **VLAN** réservés à différents services et appareils tel que les bornes **WIFI**, les imprimantes, les **PCs** et leurs téléphones, etc.

Concernant la nomenclature des **@IP** des réseaux réservés aux serveurs, elle est de la forme « **P . X . Y . Z /24 »**, où :

P = **10** ou **172** ou **192** (adressage privé oblige).

X,**Y**,**Z** = une valeur quelconque non essentielle à la compréhension bien que représentant une certaine logique.

Maintenant, concernant la nomenclature des **@IP** des réseaux **VLAN** réservés à différents services et appareils, elle est de la forme « **P- . α . β . γ /24 »**, où :

P- = 10 ou **172** ou **192** ET pas la même valeur que **P**.

α = un chiffre allant de **1** à **9** qui représente le type de service ou d'appareils auxquels est lié le réseau VLAN (ex : **1** correspond aux **imprimantes**, **2** aux **bornes WIFI**, **3** aux **PCs**, etc.). Ces correspondances sont établies et connues du **SIGV** pour la configuration des différents réseaux voulus.

β = un nombre allant potentiellement de **1** à **41** (pour **41** sites au total) qui représente le site auquel un certain réseau est affilié (ex : **1** correspond au site de la **mairie centrale de Cabriès**, **2** à **l'office du tourisme de Cabriès**, **3** à une **certaine école de Bouc-Bel-Air**, **4** à la **mairie centrale de Simiane-Collongue**, **5** au **service des sports de Bouc-Bel-Air**, etc.). Ces correspondances sont établies et connues du **SIGV** pour la configuration des différents réseaux voulus.

γ = un nombre quelconque allant de **1** à **254**, différenciant chaque hôte sur un réseau considéré (le masque étant en **/24**, c'est bien cet octet qui va différencier les différents hôtes sur un réseau donné).

Ainsi par exemple, si on considère que tout ce que je dis depuis tout à l'heure est vrai, la machine qui a pour **@IP 10.2.5.88** est une **borne WIFI** appartenant au site du **service des sports de Bouc-Bel-Air** et qui se distingue des autres bornes affiliées à ce site par la valeur « **88** ». Elle appartient alors au réseau **VLAN 10.2.5.0/24**.

Autre exemple, la machine qui a pour **@IP 10.1.1.143** est une **imprimante** appartenant au site de la **mairie centrale de Cabriès** et qui se distingue des autres bornes affiliées à ce site par la valeur « **143** ». Elle appartient alors au réseau **VLAN 10.1.1.0/24**.

J'ai détaillé là les **VLANs** auxquels étaient rattachés des équipements finaux tels que les téléphones **IP**, les **PCs**, les bornes **WIFI** et les imprimantes mais il n'est pas à omettre que ce ne sont pas les seuls **VLANs** présents dans l'architecture générale et qu'il en existe bien plus encore qui contiennent notamment divers serveurs différents selon les sites (**BDD**, **proxies**, serveurs applicatifs métiers, serveurs **DHCP** à part, **NAS**, …). Il existe plus de **250 VLANs** utilisés au sein de l'architecture gérée par le **SIGV**.

Pour ce qui est du **routage inter-VLANs** (puisqu'il est bien nécessaire afin de faire communiquer ensemble tous ces appareils dans tous ces **VLANs** différents), il donc réalisé au niveau **3**, directement dans le cœur de réseau, par le **SIGV**.

3 – L'Active Directory (AD) :

Pour des raisons de confidentialité, je ne montrerai pas dans le détail la composition exacte de l'AD parmi ce que je veux montrer (nom des groupes, nom des utilisateurs, adresses des utilisateurs, ...).

Nous allons dans cette partie expliquer ce qu'est l'**AD** et comment il est structuré au sein des trois communes gérées par le **SIGV**.

Tout d'abord, une infrastructure **AD** est comparable à une

forêt.

Chaque forêt contient au moins un **domaine**.

Chaque domaine possède des **ressources**.

Chaque domaine peut posséder des **groupes**.

Chaque domaine peut également posséder des **UO**. Sur chaque **UO** (ou bien **OU**) peut être appliquée une **GPO**.

Chaque domaine possède au moins deux **contrôleurs de domaine** .

Pour communiquer à l'intérieur d'un domaine, les machines peuvent utiliser le protocole [NetBIOS] (c'est le cas pour les machines appartenant aux trois communes). Pour communiquer à l'extérieur d'un domaine, les machines utilisent logiquement le protocole **IP** ici.

Appliquons ces principes à la configuration actuelle administrée par le **SIGV** (les trois communes).

Premièrement, il existe une forêt s'intitulant « **sigv.lan** ». Chaque commune affiliée au **SIGV** utilise un domaine spécifique qui lui est propre. Ainsi, **Cabriès** a pour nom de domaine « **cab.sigv.lan** », **Bouc-Bel-Air** a pour nom de domaine « **bbr.sigv.lan** » et **Simiane-Collongue** a pour nom de domaine « **sim.sigv.lan** ». Ainsi, à cette forêt sont rattachés et inclus ces trois domaines (**Figure 3**) :

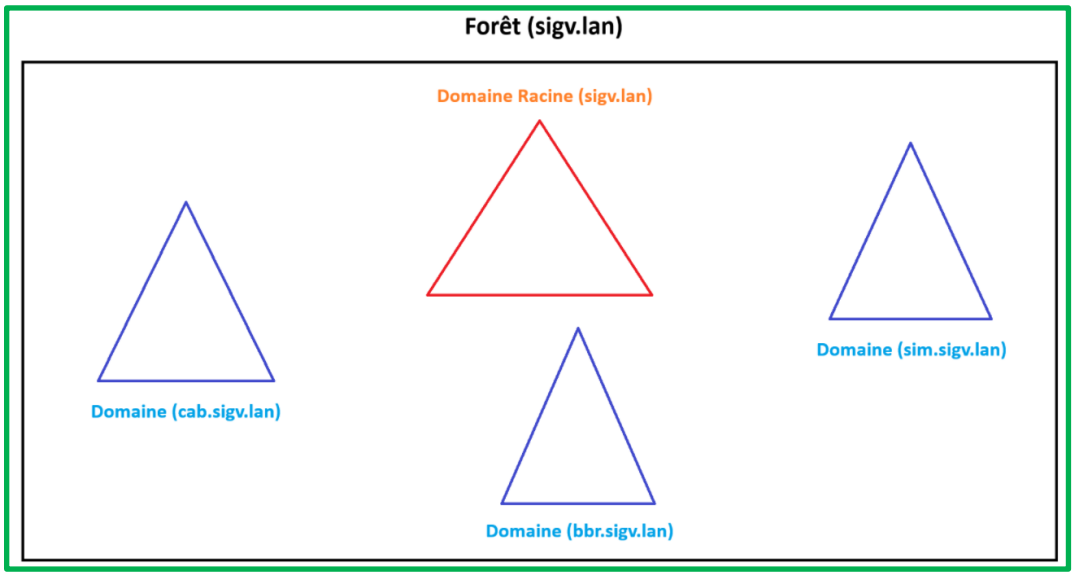

Figure 3

Dans ce cas, on peut également dire que la forêt « **sigv.lan** » est le **domaine racine** (principal) et « **cab/bbr/sim.sigv.lan** » les domaines enfants du domaine racine « **sigv.lan** ». D'où la représentation, en rouge, d'un domaine « **sigv.lan** ».

Par la suite, je vais décrire et expliquer comment est structuré le domaine de Cabriès « **cab.sigv.lan** » (en guise d'exemple). Cela aurait été sensiblement la même chose si j'avais décrit le domaine de Bouc-Bel-Air « **bbr.sigv.lan** » ou celui de Simiane-Collongue « **sim.sigv.lan** », puisque la logique d'infrastructure **intra-domaine** ne varie presque pas entre domaines. Pour des raisons de sécurité, je n'ai eu accès qu'à la partie listant les utilisateurs et les ordinateurs du domaine (et pas à la partie s'occupant des **GPO** par exemple). Je vais donc expliquer seulement ce que j'ai pu consulter.

Voici ce que l'on voit lorsqu'on visualise le contenu de l'**AD** pour le domaine « **cab.sigv.lan** » (**Figure 4**) :

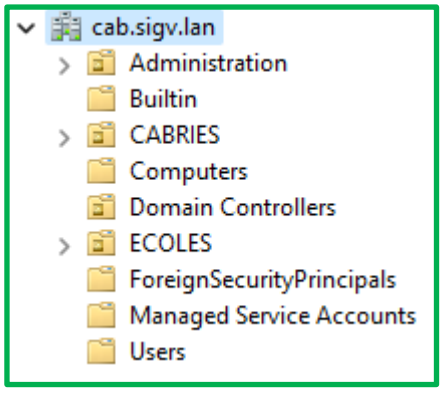

Figure 4

Dans ce domaine, on peut constater l'existence de neuf **OU**. Celles qui sont précédées d'une petite flèche grise contiennent elles-mêmes des **OU**, les autres non. Décortiquons-les unes-à-unes :

Premièrement, l'**OU** « **Administration** » : elle contient tous les comptes (donc tous les utilisateurs) administrateurs ainsi que tous les comptes liés aux différents **services** (**LDAP**, **VPN**, **ToIP**, sauvegarde, ...) du domaine (**Figure 5**).

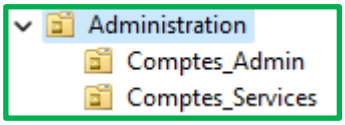

Figure 5

Deuxièmement, l'**OU** « **Builtin** » : elle contient tout un ensemble de **groupes de sécurité** nécessaires au bon fonctionnement des services installés dans le domaine.

Troisièmement, l'**OU** « **CABRIES** » : elle contient tout un ensemble d'**OU**, qui correspondent à chaque fois à un **site** (comme Mairie Centrale, Mairie Annexe Calas, Police Municipale, ...) ou à une **catégorie** plus spécifique et précise (comme **DGS**, Elus, Ressources Humaines, ...). Dans ces différentes **OU** se trouvent donc les utilisateurs et groupes d'utilisateurs associés au **site** et/ou à la **catégorie** dont ils font partie (**Figure 6**).

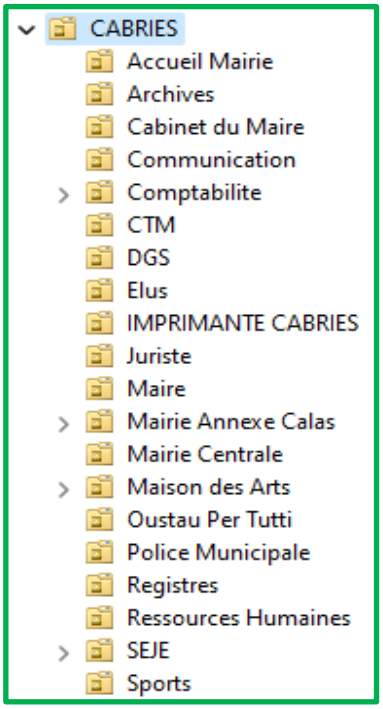

Figure 6

Quatrièmement, l'**OU** « **Computers** » : sont renseignés dedans tous les ordinateurs (leurs noms donc) appartenant au domaine de Cabriès, que ce soient des postes de travail ou des serveurs hébergeant un certain service (comme le **DHCP** par exemple, qui est un service associé à un serveur en particulier ici).

Cinquièmement, l'**OU** « **Domain Controllers** » : elle contient tous les contrôleurs de domaine du domaine de Cabriès. Il y en a comme dit précédemment au moins deux, pour assurer une redondance. Concrètement, un contrôleur de domaine est considéré comme un ordinateur par l'**AD**.

Sixièmement, l'**OU** « **ECOLES** » : se situent dedans trois autres **OU**, qui correspondent aux trois écoles présentes dans la commune de Cabriès. Chacune de ces « sous-**OU** » contient tous les utilisateurs et groupes d'utilisateurs affiliés à leur lieu de travail respectifs (**Figure 7**).

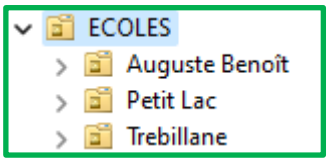

Figure 7

On voit là que, pour des questions d'administration **AD**, l'**OU** « **ECOLES** » n'est pas contenue dans l'**OU** « **CABRIES** » de tout à l'heure. En effet, de façon générale, les écoles n'ont pas les mêmes besoins que les sites situés dans l'**OU** « **CABRIES** » qui sont des sites entièrement affiliés à la mairie. Les écoles, elles, dépendant aussi de l'académie d'Aix-Marseille, le **SIGV** ne constitue pas 100 % de la gestion de ces cas.

Septièmement & Huitièmement, les **OU** « **ForeignSecurityPrincipals** » et « **Managed Service Accounts** » : ces **OU** ne contiennent rien.

« **ForeignSecurityPrincipals** » est censée être une **OU** où sont stockés des objets venant de domaines certifiés qui seraient extérieurs à la forêt dans laquelle est l'**OU** « **ForeignSecurityPrincipals** », or ici, la forêt gérée par le **SIGV** n'étant pas affiliée à une autre forêt extérieure par une **relation d'approbation** , ou plutôt dans ce cas par une **relation d'approbation de forêts** , aucun objet ne doit apparaître ici (et c'est bien le cas).

« **Managed Service Accounts** » est censée être l'**OU** contenant tous les comptes de services administrés autonomes, à savoir des comptes fournissant une gestion automatique des mots de passe, une gestion simplifiée des **noms principaux de service** (**SPN**) et la possibilité de déléguer la gestion à d'autres administrateurs. Dans cette **OU**, il n'y a donc pas de comptes de services administrés autonomes, cependant ces comptes se situent en réalité dans l'**OU** « **Administration** », puis « **Comptes_Services** » vue plus haut.

Neuvièmement, l'**OU** « **Users** » : on observe dedans tous les utilisateurs et groupes de sécurité liés aux services présents dans le domaine de Cabriès (**DHCP**, **DNS**, certificats, ...).

4 – La téléphonie IP :

Pour des raisons de confidentialité, je n'utiliserai pas de valeurs précises concrètes réelles pour expliquer la nomenclature des numéros de téléphonie IP utilisée dans le cadre de l'architecture complète gérée par le SIGV pour les trois communes impliquées. Aussi, les valeurs que je prends pour expliquer sont purement aléatoires à chaque fois.

Le système de téléphonie **IP** est, comme vu auparavant, entièrement géré par le **SIGV** (en tout cas pour ce qui touche à l'interne). Pour pouvoir passer des appels à l'**extérieur**, le **SIGV** utilise **Orange** comme opérateur téléphonique. Ainsi, chaque appel initié depuis un certain site passe par le **Trunk SIP** (lien entre le cœur de réseau qu'est le **SIGV** et l'opérateur) et est finalement acheminé vers l'extérieur grâce à l'opérateur et à ses réseaux d'accès.

Il existe, à la manière des réseaux, une nomenclature spécifique pour chaque site concernant la téléphonie **IP**. De nos jours, la plupart des numéros qu'on compose sont composés de dix chiffres et les numéros associés aux différents agents gérés par le **SIGV** sont justement, eux-aussi composés de dix chiffres.

Pour expliquer la suite, penchons-nous déjà sur la composition générique d'un numéro de téléphone **IP** dans le cadre de l'infrastructure actuelle gérée par le **SIGV** :

- Les **deux premiers chiffres** correspondent, selon une norme nationale, à une certaine zone géographique vaste. En **France**, en région sud-est (comme c'est notre cas ici) les deux premiers chiffres sont forcément « **04** » en entreprise.

- Les **deux prochains chiffres** correspondent, selon une norme nationale, à un indicatif départemental (on gagne alors en précision). Dans le département des Bouches-du-Rhône (comme c'est le cas ici), il existe plusieurs combinaisons de chiffres possibles : 13, 42, 65, 84, etc. Prenons pour exemple et vérité que c'est le « **42** » qui est utilisé dans ce cas.

- Les **cinquième & sixième chiffres** sont, eux, fournis par l'opérateur de l'infrastructure (ici Orange) selon l'architecture téléphonique (par exemple « **91** »). Ce chiffre peut varier selon les sites, mais simplifions ici en disant qu'il est tout le temps fixe.

- Les **deux chiffres suivants**, personnalisables par le **SIGV**, sont le fruit d'une appartenance à un certain site. D'ailleurs, si deux sites s'occupent en réalité du même service (en clair réalisent un travail similaire), il est tout à fait possible d'avoir ces deux chiffres similaires pour ces deux sites (ex : **00** pour **mairie centrale**, **01** pour **maison des arts**, **01** pour **bibliothèque**, **18** pour une **école**, ...).

- Enfin, les **deux derniers chiffres** désignent un hôte en particulier (ex : **05** pour **François DUPONT**, **22** pour **Pierre DELAQUEDUC**, **40** pour **Jean DUVIADUC**, ...).

Ainsi, par exemple (si on considère que tous les exemples que j'ai donnés sont vrais), si je suis **François DUPONT,** agent travaillant dans la **maison des arts**, mon numéro de téléphonie **IP** attribué sera le **04 42 91 01 22**.

Autre exemple, si je suis **Jean DUVIADUC**, agent travaillant en **mairie centrale**, mon numéro de téléphonie **IP** attribué sera le **04 42 91 00 40**.

Cela permet donc aux agents d'appeler l'**intérieur** et de se faire appeler depuis l'intérieur ainsi qu'appeler l'extérieur et de se faire appeler depuis l'extérieur (grâce au fournisseur Orange). Par ailleurs, par convention/norme de téléphonie d'entreprise, si un agent interne de **l'effectif** souhaite appeler une personne à l'extérieur, il doit renseigner avant de composer le numéro de la personne externe un « **0** ». Ainsi, si **François DUPONT** veut appeler le numéro de son père « **06 11 22 33 44** », il devra composer sur son poste téléphonique le « **0 06 11 22 33 44** » pour le joindre.

Aussi, la technologie des téléphones **IP** permet, au sein de l'infrastructure gérée par le **SIGV** (donc en interne), d'appeler les autres agents uniquement grâce aux quatre derniers numéros d'un numéro de téléphone **IP** complet.

Ainsi, par exemple, si **François DUPONT** souhaite appeler **Jean DUVIADUC**, il peut, soit composer son numéro complet (donc le **04 42 91 00 40**), soit composer les quatre derniers chiffres de son numéro complet (donc le **00 40**) ; dans les deux cas, il pourra atteindre **Jean DUVIADUC**. En revanche, si je cherche à appeler **Jean DUVIADUC**, n'étant pas officiellement membre de l'effectif, je ne pourrai l'appeler qu'à l'aide de son numéro complet.

Il est également intéressant de noter que chaque numéro de téléphone **IP** de membre de l'effectif est renseigné dans l'**AD**, en tant que descriptif d'un profil d'utilisateur (autrement dit, un utilisateur dans l'**AD** possède un champ « **téléphonie IP** » le définissant en partie, sous réserve que l'agent ait bien un téléphone **IP** en physique bien sûr). C'est une valeur à renseigner manuellement, tout comme l'adresse mail qui, elle aussi, peut quelque part définir un utilisateur dans l'**AD**.

D'ailleurs, dans la commune de Cabriès, tout agent possède une adresse e-mail de la forme ***blabla@cabries.fr***. Pour le système de mails, le **SIGV** se repose sur la « **Gsuite** » (de nos jours « **Workspace** » de chez **Google**, qui est donc leur hébergeur de serveur mail (utilisant d'ailleurs le protocole [**SMTPS** pour fonctionner).

III – Les différentes tâches :

1 – Le grand nettoyage physique :

Quand j'arrivai sur le site de la Mairie Centrale (où je fus par défaut tout le long de mon stage), je fus confronté au premier problème qui s'est avéré être la première tâche de mon stage et qui était dû au caractère post-migratoire de tous les sites de toutes les communes affiliées au **SIGV** : le **rangement**.

En effet, le fait d'avoir centralisé quasiment tous les équipements et services informatiques de tous ces sites a fait que ceux-ci demeuraient pourvus, inutilement, d'équipements tel que des serveurs de sauvegarde ou de sécurité.

La majorité des sites étaient déjà dépourvus de ces équipements inutiles, mais le site de la Mairie Centrale en fut un où ce rangement n'avait pas encore été effectué. J'ai donc, durant la première semaine de mon stage, dû m'occuper de ça en faisant bien attention à mon agilité pour ne rien débrancher dans la salle de brassage (ce qui fut presque entièrement respecté, puisque lors du **2ème** jour de rangement, j'ai involontairement débranché une prise électrique qui alimentait un **boîtier fibre** , coupant la connexion à Internet et la téléphonie **IP** de plusieurs sites, générant quelques vagues d'inquiétude provenant d'agents du site de la Mairie Centrale, notamment d'agents du service comptabilité, qui fut à ce moment-là en plein jour de paye).
Je ne fus pas fier de ça, mais après la présentation de mes excuses, je me suis rapidement remis au travail en essayant de ne pas reproduire ce genre d'erreurs. Ce jour-là, ça n'a duré que quelques minutes, mais c'est aussi là où je me suis rendu compte d'à quel point il faut être précautionneux dès qu'on entre dans une salle de brassage : couper momentanément un service réseau peut mener à une perte de temps précieuse du côté de ceux qui travaillent. Quelque part, quand on travaille dans ça, que ce soit à n'importe quelle couche du [↑] [↓], on est garant de l'accès à Internet des agents, accès aujourd'hui indispensable en entreprise ou en collectivité. Une panne de ce service primordial peut entraîner des retards aux conséquences qui peuvent s'avérer graves. Ce métier implique une très grande responsabilité, et nécessite un grand sérieux ainsi qu'une vigilance permanente.

Après une semaine d'efforts physiques (entre autres), j'avais enfin terminé de nettoyer cette salle de brassage ! Ci-dessous (**Figure 8**) une photo de la baie de brassage une fois mon intervention terminée (il faut imaginer une armoire complètement remplie de serveurs initialement) :

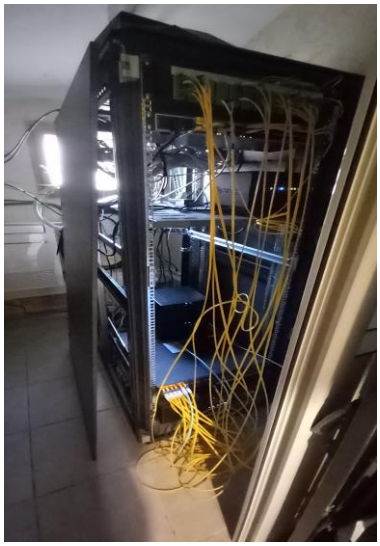

Figure 8

Au final, ce nettoyage m'aura permis de récupérer :

- **4** serveurs de sauvegarde inutiles à présent, puisque les données étaient déjà sauvegardées du côté du **SIGV**.
- **1** Firewall **Stormshield** (sécurité), **1** routeur **KEYYO**, entre autres.
- Plus de **50** câbles qui traînaient et/ou étaient désormais inutiles.

J'avais donc pu récupérer pas mal de choses, mais il fallait maintenant les ranger proprement. C'est là que j'appris l'existence d'un espace de stockage réservé au matériel informatique (que j'appellerai « **E**space de **S**tockage du **M**atériel **I**nformatique », **ESMI**).

J'estime que le tri des équipements réseau dont on dispose est une étape à ne pas négliger en entreprise ou en collectivité : être conscient de ce qu'on a à disposition peut éviter les achats inutiles ou plus généralement les pertes de temps (puisqu'on sait ce qu'on a, et où c'est rangé). Tout cela m'a motivé à réorganiser l'**ESMI** qui était visiblement laissé à l'abandon ou presque, en plus d'être mal rangé ; en rangeant proprement ce qu'il y avait déjà avec ce que j'avais pu récupérer, je suis donc parvenu à un résultat satisfaisant (**Figure 9**), sachant qu'à côté, je conservais un inventaire de tout ce qu'il y avait dans cet **ESMI**, et la quantité de chaque item (voir **ANNEXES – A**).

Figure 9

*à gauche **pendant** le rangement (début)*
*à droite **après** le rangement*

Je fus également envoyé à un moment sur le site de la Police Municipale de Cabriès afin de réaliser la même chose, mais avec là moins d'équipements à enlever de la baie de brassage, bien que suivant la même logique. Je récupérai d'ailleurs un serveur de sauvegarde de vidéosurveillance là-bas, ce qui élevait le total de serveurs inutiles entre mes mains à cinq.

Une fois de retour (d'une petite intervention) en Mairie Centrale, je triais à chaque fois ce que je venais de récupérer directement dans l'**ESMI** (majoritairement des câbles, parfois des boîtiers aux services divers), et je mettais à jour mon inventaire en conséquence ! D'ailleurs, cela fut bénéfique puisque lors d'interventions futures nécessitant du matériel spécifique, je fus capable de dire si tel ou tel équipement était disponible ou non dans l'**ESMI**, nous faisant gagner du temps sur ces interventions diverses.

Après avoir réalisé ce ménage nécessaire, je récupérai deux autres serveurs de sauvegarde qui eurent déjà été ramenés en Mairie Centrale depuis d'autres sites. Au final, j'avais sept serveurs de sauvegarde à présent inutilisés. En plus de ça, je pus récupérer cinq **PCs** fixes et quatre **PCs** portables qui, eux aussi, furent ramenés d'autres sites ou simplement mis hors service en Mairie Centrale.

Au final, en récapitulant ce que j'avais pu récupérer d'intéressant pour la suite, on trouve :

- **7** serveurs de sauvegarde
- **5 PCs** fixes
- **4 PCs** portables

À présent, le but fut de complètement formater ces appareils (configuration usine + suppression totale des données conservées par les appareils). C'est l'objet de la prochaine sous-partie !

2 – Formatage :

2.1 – Serveurs :

Lors de ma deuxième semaine de stage, je me suis donc attelé au formatage de tous les équipements cités en fin de sous-partie précédente. Mon but fut tout d'abord de m'occuper des sept serveurs de sauvegarde : je devais les remettre en configuration usine tout en faisant attention de bien supprimer toutes les **données extra-système** présentes à l'intérieur et qui étaient au final devenues superflues. En plus de ça, il fallait que je prenne des notes sur la configuration physique de ces équipements (processeur, **RAM**, stockage, alimentation, …), afin de garder une trace des caractéristiques physiques de chaque serveur, dans le but final de les vendre. Les informations recueillies pour ces sept serveurs de sauvegarde sont inscrites dans sept fichiers différents que je place en annexe (voir **ANNEXES – B**).

Parmi ces sept serveurs à formater, six pouvaient l'être via une interface WEB, et un n'admettait pas d'interface WEB pour faciliter le travail ; j'ai donc dû le faire via la console de commandes incluse dans le serveur. Commençons par les six serveurs que j'ai pu formater via une interface WEB (je vais parler là d'un serveur en particulier, mais la description ci-après de la tâche effectuée s'applique aux cinq autres).

Après avoir alimenté le serveur, je branchai un câble sur un port (**VGA**, **HDMI**, **DP**) du serveur, relié à un port (**VGA**, **HDMI**, **DP**) de l'écran sur lequel j'allais visualiser les informations.

Ensuite, après avoir branché un clavier quelconque sur un port **USB** du serveur, j'ai pu allumer mon premier serveur à formater et commencer réellement ma mission. Un fois le serveur démarré, on arrive sur une page fixe (**Figure 10**) :

Figure 10

Décortiquons les éléments de cette page pour comprendre :

Ligne 1 : on apprend là que ce serveur utilise un **hyperviseur de type 1** « **VMware ESXi** », version **6.7.0** pour fonctionner. Est aussi renseigné la version de mise en production du modèle « **8169922** ».

Ligne 2 : on apprend que la société de logiciels « **VMware** » est derrière ce modèle (on l'avait deviné).

Ligne 3 : est inscrit ici le processeur qu'utilise le serveur pour fonctionner.

Ligne 4 : est indiquée ici la quantité de **RAM** possédée par le serveur (**4** Go dans ce cas).

Les autres lignes : ce sont les plus intéressantes. Elles nous indiquent comment pouvoir accéder à l'hôte (ça tombe bien, c'est ce que je veux) : ainsi, on voit qu'il est possible d'accéder à l'hôte via trois **URL** différentes utilisant respectivement un **nom de domaine** , une **@IPv4** , et une **@IPv6** .

Cependant, il faut remarquer que c'est illusoire et dénué de sens ici : en effet, comme on le voit, ces paramètres réseaux eurent été définis statiquement, et donc en accord avec l'emplacement et la configuration du serveur, au moment où il était fonctionnel ! L'ayant complètement détaché du **réseau privé** auquel il appartenait (pour ne citer que l'exemple de l'**@IPv4**), l'adresse **IP** « **10.1.149.200** » n'est plus joignable (tout comme le serveur) !

C'est donc embêtant, nous qui voulions y accéder via le WEB ne pouvions donc pas à ce moment-là. Je me suis donc naturellement dirigé vers les paramètres du serveur, afin de voir ce que je pouvais y faire. Je suis ensuite tombé sur une page d'authentification (**Figure 11**) :

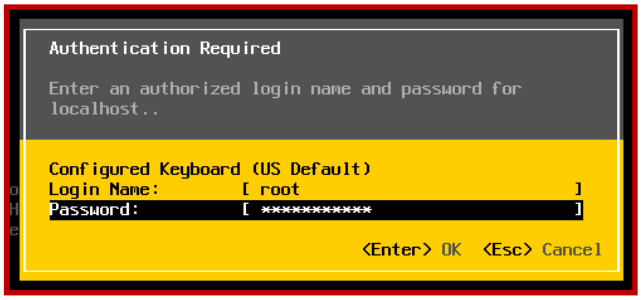

Figure 11

Ne connaissant ni l'identifiant, ni le mot de passe associés à un ancien super-utilisateur utilisé pour configurer ce serveur, j'ai donc dû demander à M. Brunet de me les fournir ; il a contacté le **SIGV** qui a pu lui fournir les informations nécessaires. Je me suis donc connecté au serveur via ce compte administrateur, et j'ai enfin pu accéder aux paramètres de celui-ci (**Figure 12**) :

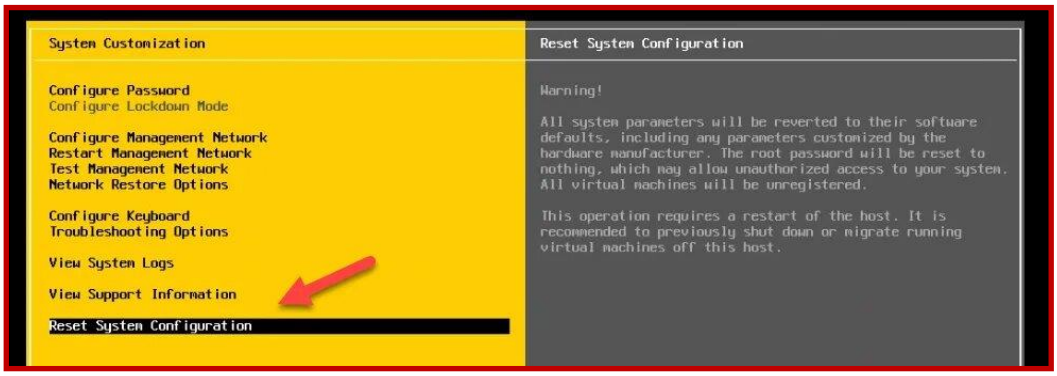

Figure 12

J'ai donc ici scrupuleusement fait le tour de tous les paramètres qui m'étaient proposés afin de choisir celui qui serait le plus optimal à utiliser dans mon cas. Ainsi, comme indiqué dans cette capture d'écran, le paramètre qui va m'intéresser ici est « **Reset System Configuration** ». En lisant la description de ce paramètre à droite, on apprend globalement que tous les paramètres systèmes courants vont être réinitialisés en configuration usine (bingo) et que le mot de passe de l'administrateur va également être réinitialisé à « **rien** ». Cela sous-entend aussi que les paramètres réseau du serveur vont être réinitialisés, ce qui ne peut qu'être bon puisque le serveur est pour l'instant inaccessible.

Après sélection du paramètre et un redémarrage forcé du serveur, on retombe sur la page d'accueil, mais cette fois-ci, quelque chose a changé au niveau des dernières lignes (**Figure 13**) :

Figure 13

Effectivement, maintenant pour accéder et configurer le serveur, il faut joindre l'**@IPv4** « **0.0.0.0** ». Ici, il faut comprendre que le serveur n'est toujours pas joignable (ce qui est normal, il n'a certes plus d'**@IPv4** fixe injoignable, mais le fait est qu'il n'a plus du tout d'**@IPv4** actuellement, donc il reste inatteignable).

Cela dit, le principal problème fut réglé et je n'étais là qu'à un pas de la solution à laquelle j'avais réfléchi : brancher, grâce à un câble Ethernet, un **PC** quelconque au serveur, afin de créer un réseau local (entre le **PC** et le serveur), afin de joindre le serveur sur le réseau local ainsi créé, depuis mon **PC**. Cette méthode est réalisable grâce au mécanisme **[APIPA** (**A**utomatic **P**rivate **I**nternet **P**rotocol **A**ddressing).

Au bout d'un moment, sur le serveur (**Figure 14**) et au niveau de la carte réseau Ethernet de mon **PC** (**Figure 15**), les deux **@IPv4 APIPA** sont apparues.

Figure 14

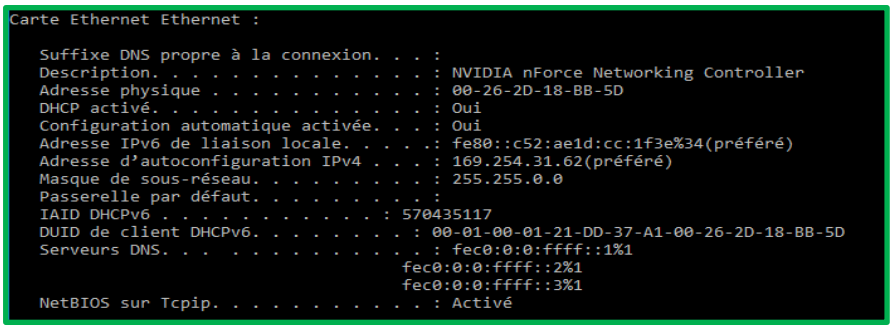

Figure 15

J'ai donc pu, grâce à un navigateur WEB, accéder à l'**@IP** du serveur et à son interface WEB (**Figure 16**).

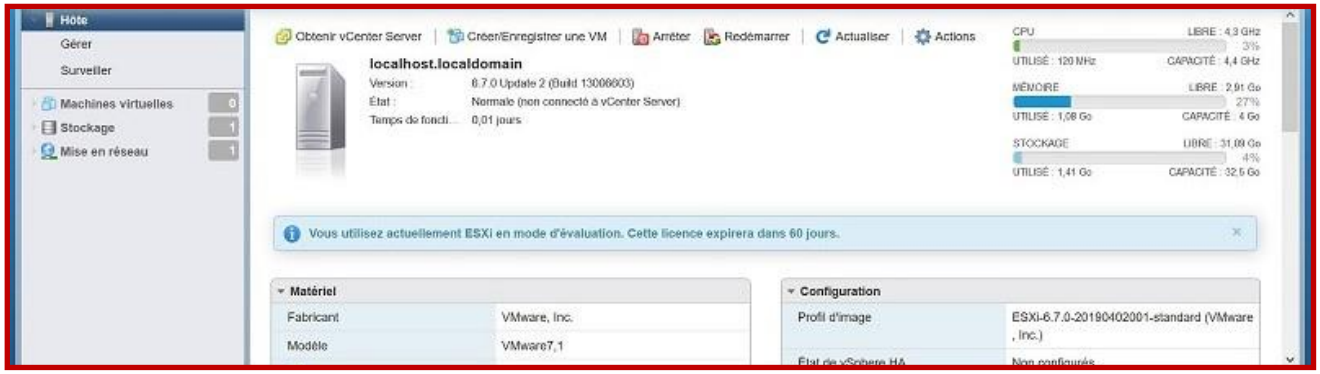

Figure 16

Dans le menu de gauche, on peut voir trois catégories d'éléments dont le serveur dispose : le nombre de **machines virtuelles** montées et gérées par le serveur, le nombre d'espaces de stockage configurés sur le serveur, et le nombre de moyens utilisés par le serveur pour communiquer avec d'autres hôtes (dans notre cas un seul, par câble Ethernet). Dans le cas de ce serveur, ce qui nous intéresse est la partie « **Stockage** » du menu de gauche.

Quand on sélectionne l'onglet « Stockage » nous sont montrées les différentes **BDD** (**B**ase(s) **D**e **D**onnées) contenues dans le serveur qui sont affiliées à une certaine **partition de disque** . Dans ce serveur : de disques durs on crée des partitions, dans lesquelles on crée des **BDD** diverses, et ce sont justement ces **BDD** diverses que je vais chercher à supprimer définitivement. Je ne m'attarderai pas plus longtemps sur ça ; pour supprimer lesdites **BDD**, il suffisait donc de se rendre dans l'onglet « **Stockage** » et de sélectionner l'action « Supprimer », pour toute **BDD** existante. Concernant les partitions, je les ai par la suite également supprimées, quasiment de la même façon que pour la suppression des **BDD**, via une action de suppression. Voici comment je suis arrivé à formater les six premiers serveurs de sauvegarde !

Il ne me restait donc qu'un serveur à formater, mais comme dit dans l'introduction de cette sous-partie, c'était cette fois différent puisque je n'avais pas d'interface WEB à disposition pour réaliser ma tâche : j'ai donc dû passer par une console de commandes intégrée au serveur restant (« **Shell ESXi** »). Il était d'ailleurs possible de se connecter via **[SSH** au serveur, ce qui se serait effectué dans ce cas avec la commande suivante depuis le **PC** relié au serveur, via un terminal de commandes : **ssh root@[@IPv4 serveur]**.

Le **Shell ESXi** me convenait parfaitement, alors j'ai réalisé le formatage grâce à celui-ci. En faisant des recherches sur l'Internet, je suis tombé sur une page WEB contenant les informations que je cherchais (voir **ANNEXES – C** pour le lien de la page ainsi que la sitographie).

La commande à utiliser avait la syntaxe suivante :

partedUtil delete "/vmfs/devices/disks/[nom_du_disque]" [numéro_de_la_partition_à_supprimer]

En faisant un « **ls** » dans le répertoire « **/vmfs/devices/disks/** », il fut facile de déterminer le nom du disque dur présent dans le serveur (puisqu'il n'y en avait qu'un), ainsi que les partitions existantes créées à partir dudit disque. Ainsi, il ne me restait plus qu'à appliquer la commande du dessus pour chaque partition présente formée à partir de l'unique disque dur du serveur. Certaines partitions ne pouvaient être supprimées (certainement des partitions où résident des données utiles au bon fonctionnement du système), les autres furent supprimées avec succès. La suppression des partitions a entraîné la suppression des données contenues dedans, donc typiquement les potentielles **BDD** qu'il pouvait y avoir. Mon devoir fut alors de nouveau accompli !

2.2 – PCs :

Une fois tous ces serveurs formatés correctement, je les rangeai dans la salle de brassage, et ils furent prêts à être vendus. Ensuite, il me resta donc les cinq **PCs** fixes et les quatre **PCs** portables à formater.

Ici, je ne vais pas séparer cet ensemble de **PCs** en deux groupes qui seraient « les **PCs** portables » et « les **PCs** fixes », puisque ça n'a que peu de sens étant donné que ce n'est pas le caractère « fixe » ou « portable » qui a changé la façon de réaliser la tâche par la suite, mais plus le **[SE** (**S**ystème d'**E**xploitation) utilisé par les **PCs** ; en effet, parmi les neuf **PCs** que j'eus à disposition, sept furent sous Windows 10 « Professionnel », et deux sous Linux.

Commençons par les sept **PCs** sous Windows. Pour ce qui était de récupérer les informations des composants, ce fut relativement facile : on se connectait à la session de l'utilisateur qui utilisait précédemment le **PC** considéré, on se rendait dans les différents paramètres nous permettant de recueillir les informations voulues (gestion des disques, informations à propos du **PC**, carte graphique), et on les inscrivait dans sept fichiers textes différents, à la manière des sept serveurs de tout à l'heure (voir **ANNEXES – D** pour ces fichiers).

En revanche, pour les formater, ce fut une autre histoire. Ce n'était pas à moi de m'en charger directement, mais au **SIGV**. Je suis donc allé auprès d'eux pour réaliser cette tâche. Les **PCs** avaient en stockage des informations propres à chaque utilisateur, informations dont il fallait se débarrasser. Le **SIGV** préconise, pour la

réinitialisation/formatage de **PCs**, le **SE Windows 10 « Professionnel »** , et étant donné que les sept **PCs** furent déjà sous Windows 10 « Professionnel », il a simplement fallu les réinitialiser depuis la session de l'utilisateur précédant (fonction accessible directement dans les paramètres des **PCs**). Ce fut simple, rapide, efficace.

Passons maintenant au deux **PCs** qui fonctionnaient sous Linux. Tout d'abord, étant donné que ces **PCs** furent voués à être complètement modifiés et parce que je n'avais pas les accès nécessaires pour réaliser ma tâche correctement, il ne me fallait pas récupérer d'informations sur les composants physiques de ceux-ci.

Pour ce qui fut du formatage de ces deux machines, comme je l'ai dit dans le dernier paragraphe, le **SIGV** préconise Windows 10 « Professionnel » comme **SE** dans un **PC** qui serait réinitialisé, or cette fois-ci les deux **PCs** que nous avions-là n'étaient même pas sous Windows ! Le plan fut donc ici d'utiliser une **clé bootable** avec Windows 10 « Professionnel » dedans, et de choisir en option de boot du **PC** considéré la clé bootable, ce qui faisait que le **PC** allait désormais utiliser Windows 10 « Professionnel » pour booter par défaut.

Voyons maintenant les étapes par lesquelles il faut passer afin de créer une clé bootable avec le **SE** voulu dedans, étapes par lesquelles nous sommes passés pour réaliser la mission.

Tout d'abord, sur un ordinateur à part, déjà correctement configuré et intégré au domaine, on a installé le logiciel ***Rufus*** qui est un logiciel permettant de créer des clés bootables facilement, et ce pour n'importe quel **OS** (**O**perating **S**ystem).

Après installation du logiciel, lors de son exécution, on arrive sur cette page (**Figure 17**) :

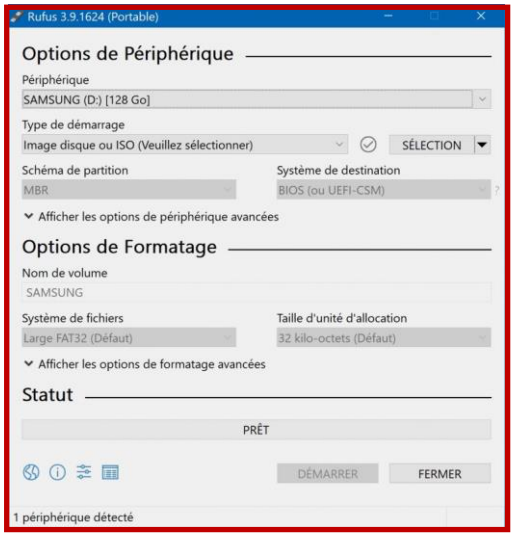

Figure 17

Cette page nous demande d'abord de sélectionner un périphérique ; ici, on choisit la clé qu'on veut transformer en clé bootable, clé préalablement branchée au **PC** bien sûr. Ensuite, on sélectionne un **fichier .iso** contenant Windows 10 et pour les options de formatage (puisque oui, la clé sur laquelle le **SE** va être mis sera tout d'abord complètement formatée par le logiciel), on laisse par défaut. On clique sur « **PRÊT »** et l'opération s'effectue.

Une fois l'opération terminée, il ne nous restait plus qu'à brancher la clé sur le **PC** Linux dont on voulait changer le **SE**, d'accéder au **BIOS** lors du démarrage de l'ordinateur, et de sélectionner notre clé bootable comme support de boot, et le tour était joué !

Maintenant, que nous avions ces neufs **PCs** complètement formatés et réinitialisés à disposition avec Windows 10 « Professionnel » dessus, l'objectif allait naturellement être de les intégrer à un domaine.

Ici, ces **PCs** allaient tous être intégrés au domaine de Cabriès, puisque c'est au sein de ce domaine (et donc de cette commune) qu'était prévue l'arrivée de nombreux nouveaux agents qui avaient donc besoin d'un ordinateur pour travailler correctement. Voyons donc maintenant par quel processus le **SIGV** est passé pour intégrer ces neuf ordinateurs au domaine de Cabriès (je vais prendre l'exemple d'un seul cas, mais c'est sensiblement la même chose pour les huit autres).

Tout d'abord, on crée dans l'**AD** le nouvel utilisateur correspondant au nouvel agent qui va arriver sur ce nouveau poste et on place ce nouvel utilisateur dans l'**OU** voulue et cohérente vis-à-vis de son poste (ou alors, dans le cas où c'est un simple changement de machine pour un utilisateur qui existe déjà bel et bien dans le domaine, on réutilise l'utilisateur déjà existant correspondant à l'agent). En créant ce nouvel utilisateur, on lui définit un nom d'utilisateur de la forme **prénom.nom** et un mot de passe (ces deux valeurs étant soumises à des règles établies par le SIGV pour le domaine).

Ensuite, on démarre un **PC** formaté grâce à notre clé bootable avec Windows 10 « Professionnel » dedans.

Une fois le **PC** démarré avec le **SE** correctement initialisé, on crée un nouvel utilisateur qui correspond à l'agent qui souhaite prochainement intégrer l'effectif (ou à l'agent déjà dans l'effectif à qui on va fournir une nouvelle machine). Appelons-le **François DUPONT** pour l'exemple.

Par la suite, on se dirige vers les paramètres Windows et on cherche celui permettant de modifier le domaine de l'ordinateur (**Figure 18**) :

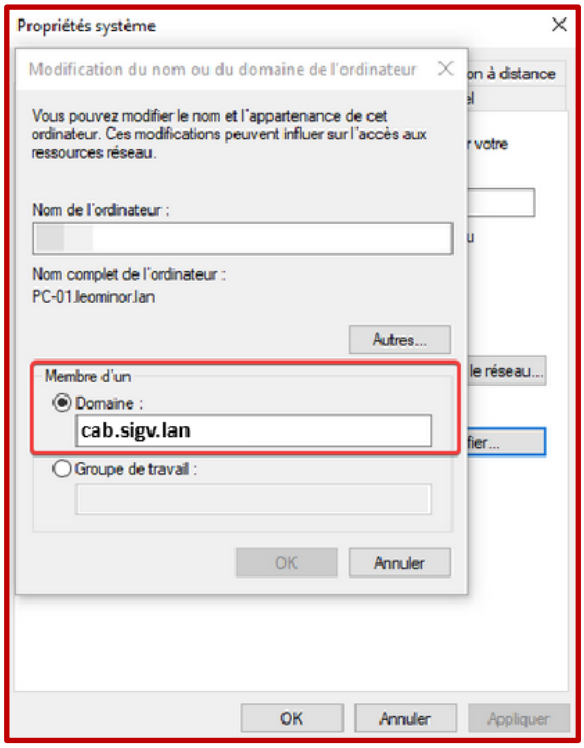

Figure 18

Comme inscrit sur la capture d'écran, on définit que le nouvel ordinateur est membre d'un domaine et que ce domaine a pour nom « **cab.sigv.lan** ».

Une fois qu'on valide cette attribution de domaine à l'ordinateur, un message apparaît (**Figure 19**) :

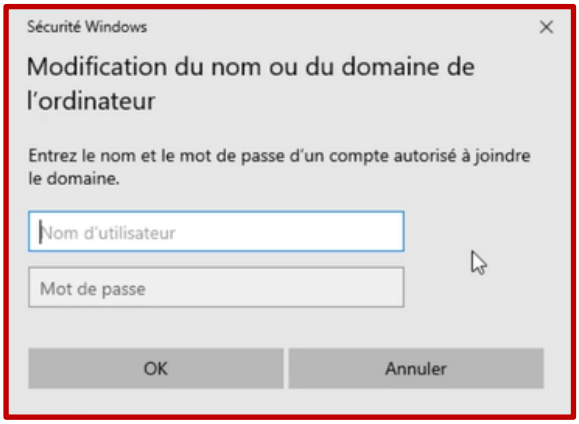

Figure 19

Ce message nous est envoyé par le contrôleur de domaine couramment actif au sein du domaine. Si on le reçoit, c'est une bonne nouvelle puisque ça veut dire que nous pouvons bel et bien communiquer avec lui (le **SIGV** s'en est assuré au moment de l'intégration au domaine du **PC**, en lui attribuant des paramètres **IP** corrects pour pouvoir communiquer avec) !

Par définition, le contrôleur de domaine est le garant de l'**AD** du domaine considéré, ici « **cab.sigv.lan** » ; par logique, il connaît alors tous les utilisateurs actuellement inscrits dans sa part de l'**AD**.

Ainsi, deux cas sont possibles : soit **François DUPONT** fait déjà partie de l'effectif et donc il souhaite simplement changer de PC, soit **François DUPONT** ne fait pas encore partie de l'effectif mais va le rejoindre bientôt.

Dans le **1er** cas, on remplira alors les champs demandés avec le nom d'utilisateur de **François DUPONT** déjà existant au sein de l'**AD** du domaine de Cabriès, ainsi qu'avec son mot de passe (qu'il devra d'ailleurs changer lors du prochain démarrage de la machine).

Dans le **2ème** cas, on remplira cette fois les champs demandés avec le nom d'utilisateur de **François DUPONT** venant d'être créé au sein de l'**AD** du domaine de Cabriès, ainsi qu'avec son mot de passe (générique, qu'il devra d'ailleurs changer lors du prochain démarrage de la machine). Ainsi par exemple, si l'agent **François DUPONT** est un agent qui souhaite intégrer l'effectif en tant qu'assistant **DGS**, on aura inscrit dans ce cas au préalable son prénom et son nom dans la partie de l'**AD** correspondant au domaine de Cabriès, dans l'**OU** « **CABRIES** » puis « **DGS** » et ce en tant que nouvel utilisateur.

Alors, si on rentre son nom d'utilisateur (qui serait donc **françois.dupont**) ainsi que le mot de passe qu'on lui a attribué lors de la création de son profil utilisateur dans l'**AD** plus tôt (ou il y a longtemps s'il fait déjà partie de l'effectif) et qu'on clique sur « **OK** », le contrôleur de domaine va, de son côté, vérifier dans la **BDD** de sa partie de l'**AD** pour voir si cet utilisateur existe bel et bien et s'il est donc bien autorisé à rejoindre le domaine considéré. Si c'est le cas, l'opération sera un succès et notre utilisateur rejoindra bien le domaine de Cabriès, et sera donc opérationnel ; il aura alors accès à toutes les différentes fonctions autorisées par le **SIGV** (grâce aux **GPOs**).

Maintenant que ces neuf **PCs** sont inclus au domaine de Cabriès, il va falloir les déployer, et ce sera l'objet de la première partie de la sous-partie suivante !

3 – Déploiement : [↑]

3.1 – Les PCs : [↑]

Parmi les neuf potentiels **PCs** déployables, nous n'en eûmes déployé que sept. Ainsi, deux **PCs** portables, intégrés au domaine, ne sont toujours pas déployé quand j'écris ce rapport.

Maintenant, parmi les sept **PCs** que nous avons déployés, trois furent des déploiements de « **remplacement** » (un **PC** en remplace un autre) et quatre des déploiements « **d'installation** » (un **PC** s'installe sans en remplacer un autre).

Commençons par parler des quatre déploiements « **d'installation** ». Dans ces cas ce fut assez simple : il suffisait d'arriver sur les lieux de l'installation muni, pour l'exemple d'un **PC**, d'un câble d'alimentation adapté au **PC**, de câbles possédant des interfaces de connexion (**VGA**/**HDMI**/**DP**), et c'est tout !

Ensuite, on branchait le **PC** correctement (électriquement, à l'écran/aux écrans, au réseau) et on pouvait le démarrer.

Ici, il fallait faire attention à la partie réseau, car en effet, ces postes étant complètement nouveaux et ne remplaçant pas d'anciens postes, nous n'avions là aucune information précise sur les **prises réseau** à notre disposition ; étaient-elles bien **brassées** ? Correctement reliées au **Switch de regroupement des différents postes** avec le bon numéro au niveau des **noyaux** ?

Dans un premier temps, on se contentait de brancher le nouveau **PC** à une prise réseau quelconque, pour voir si le signal remontait bien au **PC**. Quelques fois ça marchait, quelques fois non. Dans ces derniers cas, il fallait appeler M. Prati (puisque j'étais avec M. Brunet pour déployer les **PCs**) afin qu'il se connecte à distance (via un **VPN**) au Switch du site considéré et qu'il voie si le port du Switch correspondant à celui sur lequel on a branché le **PC** était correctement configuré (selon l'infrastructure réseau du site, j'épargnerai les détails ici).

Dans la majorité des cas, le problème ne venait pas de la configuration en soi des ports du Switch, mais bien de la non-véracité des indications des numéros inscrits à la fois sur la prise murale et son noyau qui lui était *en théorie* associé. On finissait toujours par s'en sortir cela dit, simplement qu'on perdait du temps.

Une fois le **PC** démarré et correctement relié au réseau interne du site, il fallait donc se connecter à la session du nouvel agent (ce que lui seul pouvait faire, étant donné qu'il devait y renseigner son mot de passe personnel lié à son utilisateur pour la première fois, comme dit dans la sous-partie précédente). En considérant qu'il l'eut fait lors de son arrivée sur le poste, il avait donc accès à sa session située dans le domaine de Cabriès !

Par ailleurs, sur les sessions des nouveaux utilisateurs étaient déjà préinstallées certaines applications (choisies par le **SIGV**, pour permettre un travail optimal des agents). Parmi elles, on peut noter ***Cisco Jabber*** (application faisant office d'annuaire, permettant donc la facilitation de la communication entre les différents membres de l'effectif), ***Keepass*** (gestionnaire de mots de passe sécurisé), ***Teamviewer Remote*** (logiciel permettant le contrôle à distance d'un ordinateur, utile à M. Prati lors d'interventions à distance), Word, Adobe Reader, ...

Pour les trois déploiements de « **remplacement** », ce fut quasiment la même chose. Seulement ici, il s'agissait de remplacer des postes de **clients légers** par ces nouveaux **PCs**. On enlevait alors ces clients légers, et toutes les données relatives aux agents qui occupèrent ces postes furent donc sauvegardées sur un serveur virtuel distant ; il n'y avait donc aucun mal à les restituer sur la nouvelle machine de l'agent.
Une fois le nouveau **PC** démarré et correctement relié au réseau interne du site, il fallait donc se connecter à la session de l'agent déjà existant (ce que lui seul pouvait faire, étant donné qu'il devait y renseigner son mot de passe personnel lié à son utilisateur). En considérant qu'il l'eut fait lors de son retour sur le poste, il avait donc accès de nouveau à sa session située dans le domaine de Cabriès (depuis un certain temps) !

Au-delà de **PCs**, j'eus l'occasion d'aider à déployer d'autres équipements. La partie d'après s'adresse aux déploiements de bornes **WIFI** sur différents sites à Cabriès, que je déployai avec M. Prati directement.

3.2 – Les bornes WIFI :

Nous avions alors quatre bornes **WIFI** « **Ubiquiti UniFi** » à déployer sur quatre différents sites de Cabriès. Ce fut à chaque fois le même processus de déploiement donc je vais, comme à mon habitude, prendre un exemple qui servira aussi à expliquer le reste.

Dans notre cas, les déploiements effectués furent des déploiements « **d'installation** » ; l'objectif était donc de couvrir une plus grande zone en **WIFI**, puisqu'il existait, avant l'installation de ces nouvelles bornes, des endroits où le signal renvoyé par la borne **WIFI** à l'appareil le demandant était plutôt faible (puisque l'appareil demandant était soit trop loin d'une borne déjà installée, soit séparé de la borne par trop de matières solides (murs, plafonds, sols, armoires, ...)).

Dans un premier temps on arrivait sur le site considéré. On repérait approximativement l'endroit où devait être placée cette borne, puis on cherchait une prise murale sur laquelle brancher ce nouvel équipement réseau.

Une fois l'appareil branché à la prise murale, on allait dans la baie de brassage au niveau de laquelle était censée arriver la liaison partant de la prise murale qu'on a considérée plus tôt, on trouvait le noyau associé à notre prise murale et on reliait ce noyau au Switch principal (si ce n'était pas déjà fait).

Par la suite, M. Prati alla sur son ordinateur, se connecta sur le Switch principal des lieux, et configura le bon port du Switch d'une certaine façon :

Il fallait tout d'abord désigner le port du Switch qui nous intéressait comme étant en **mode access** . **(config-if)# switchport mode access** sur un Switch Cisco.

Par la suite, il fallait s'assurer de le placer dans le bon **VLAN**, donc dans le **VLAN** correspondant aux bornes **WIFI** du site considéré. **(config-if)# switchport access vlan [numéro]** sur un Switch Cisco.

Ensuite, pour que le trafic passant par ce **VLAN** (donc issu de la borne) soit correctement acheminé vers le site centralisateur du **BLOD** (puis vers le **SIGV**), il fallut autoriser le **VLAN** concerné à transiter sur le lien partant du site et allant vers le site centralisateur (ce qui fut déjà fait car le **VLAN** n'est pas nouveau). Cette dernière liaison que j'énonce est une liaison en **mode trunk** .

Une fois la partie réseau configurée, il fallait se rendre sur le contrôleur de bornes **WIFI** qui se situait sur un serveur distant (accessible via **VPN**) afin de configurer la borne correctement pour qu'elle diffuse le bon réseau.

Une fois arrivé sur l'interface WEB du contrôleur de bornes **WIFI** et être allé dans l'onglet **« UniFi Devices »**, répertoriant tous les appareils **WIFI** que le contrôleur de bornes **WIFI** peut voir, on tombe sur une page telle que celle-ci (**Figure 20**) :

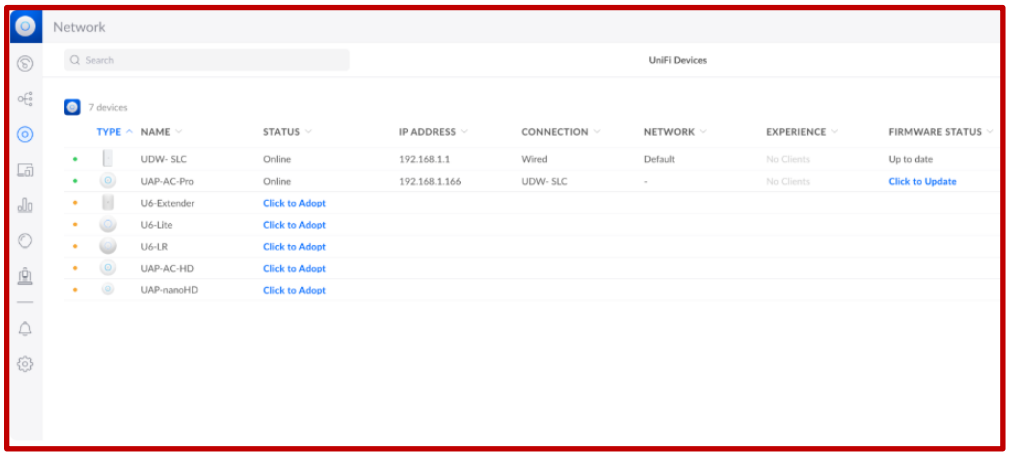

Figure 20

On y voit donc des bornes **WIFI** (U6-Extender, U6-Lite, U6-LR, ...) et le contrôleur de bornes **WIFI** lui-même (UDW-SLC). On peut ensuite voir, pour chaque élément, son statut (en ligne, pas encore configuré), son **@IP** sur le réseau, son type de connexion au réseau, le réseau auquel il appartient, une indication sur les clients de celui-ci (utilisateurs l'utilisant), et le statut de son **firmware**.

Pour la configuration générale d'une borne, plusieurs paramètres subtils peuvent être réglés, je ne vais pas m'attarder là-dessus (notamment puisque ces paramètres furent préconfigurés par M. Prati avant l'intervention sur site, donc il ne faisait pas ça avec moi). Je peux cependant souligner que parmi ces paramètres, il y en a un d'assez important, le choix de la bande de fréquences sur laquelle la borne **WIFI** va émettre (**2.4 GHz ou 5GHz**).

Une fois la configuration générale terminée, il fallait spécifier quel réseau devait diffuser et partager la nouvelle borne **WIFI**. Cela se faisait comme ça (**Figure 21**) :

Figure 21

« **Name** » : on spécifie ici le **[SSID** du « **réseau WIFI** ». Ce que j'appelle « **réseau WIFI** » ici, c'est la technologie grâce à laquelle l'utilisateur va pouvoir accéder à un certain réseau (privé ou public).

« **Password** » : on rentre là le mot de passe servant à protéger l'accès au réseau **WIFI** et donc au réseau spécifique fourni par la borne.

« **Network** » : on sélectionne ici le réseau qui sera diffusé par la borne et auquel un utilisateur possédant le mot de passe pourra accéder.

« **Broadcasting APs** » : ici on considère un groupe d'**[APs**. Ce groupe d'**APs** correspondra au groupe de bornes qui connaîtront et appliqueront les paramètres définis au-dessus.

Il faut savoir quelque chose : chaque site possède actuellement son propre **SSID** interne (c'est-à-dire son propre accès **WIFI** au réseau interne de l'entreprise), et tous les sites possèdent un **SSID** commun qui est un **SSID** permettant un simple accès à Internet (utilisé pour les invités).

Nous devions donc avec M. Prati faire en sorte que cette nouvelle borne **WIFI** partage également (comme les autres) le réseau interne de l'entreprise (via un **SSID** parlant du type « **[nom_du_site] PRIV** ») ainsi que le réseau permettant simplement l'accès à Internet (via un **SSID** parlant du type « **WIFI INVITE** »). Il est d'ailleurs prévu de créer un réseau **WIFI** avec un **SSID** du type « **SIGV LAN** » permettant à tous les sites de toutes les communes affiliées au **SIGV** de se connecter sur un même réseau **WIFI**. Cela en faciliterait la gestion (on pourrait voir qui est connecté, avec quelle **@IP** et donc en déduire le site assez facilement pour potentiellement intervenir).

Nous avons donc réalisé cette tâche pour les quatre sites de Cabriès mentionnés au début de cette partie. Cependant, la mission de déploiement ne s'arrêta pas là, puisque nous avions encore un autre type d'appareils à déployer à ce moment-là : des téléphones **IP**.

3.3 – Les téléphones IP :

Nous avions avec M. Prati cinq téléphones IP à configurer. Il s'agissait, pour les cinq cas, de déploiements de « **remplacement** ». Comme ce fut à chaque fois le même processus de déploiement, je vais, comme habituellement, prendre un exemple générique qui servira aussi à expliquer le reste.

On arrivait alors sur les lieux du site sur lequel déployer le téléphone **IP**, munis du téléphone et de deux câbles Ethernet. Pourquoi deux ? Puisque le téléphone **IP** est en fait dans toute l'infrastructure gérée par le **SIGV** un appareil intermédiaire entre le **PC** et le Switch principal de la baie de brassage, ainsi, deux câbles Ethernet sont nécessaires à l'incorporation du téléphone **IP** dans l'infrastructure générique. On peut, si on considère « ------- » comme étant un câble Ethernet, résumer la situation ainsi :

PC ------- Téléphone IP/boîtier téléphonique ------- Switch principal

Ensuite, de la même façon que les bornes **WIFI**, il a fallu s'assurer que le réseau remonte bien jusqu'au **PC** (autrement dit que le **PC** accède bien au réseau interne auquel il appartenait de base) ; cela voudrait dire que le téléphone **IP** fait correctement transiter le réseau en son sein. D'ailleurs, il est à noter que dans l'architecture générale gérée par le **SIGV**, les téléphones **IP** et les **PCs** d'agents sont, pour chaque site, dans deux **VLANs** distincts ; en réalité, le **PC** et le téléphone ne communiquent pas directement.

Ainsi pour s'assurer de cette bonne connectivité et pour correctement configurer le téléphone **IP** et les flux qui lui sont associés, M. Prati a pris la main en se connectant par **VPN** sur Switch du site concerné. À la manière des bornes **WIFI**, il fallait d'abord désigner le port du Switch qui nous intéressait (donc celui sur lequel était branché le téléphone **IP**) comme étant en mode access (je ne remets pas les commandes ici). Par la suite, il fallait s'assurer de le placer dans le bon **VLAN**, donc dans le **VLAN** correspondant aux **PCs** et téléphones **IP** du site considéré.

Ensuite, pour que le trafic passant par ce **VLAN** soit correctement acheminé vers le site centralisateur du **BLOD** (puis vers le **SIGV**), il fallut autoriser le **VLAN** concerné à transiter sur le lien partant du site et allant vers le site centralisateur (ce qui fut déjà fait car le **VLAN** n'est là non plus pas nouveau).

Une fois la configuration réseau réalisée, il fallait accéder au boîtier téléphonique en lui-même pour configurer quelques paramètres de base comme l'identité de l'agent occupant ce poste ainsi que des paramètres plus techniques que je ne vais pas détailler ici puisque je ne les ai que frôlés auprès de M. Prati lors des interventions.

Concernant la convergence en interne du nouveau téléphone **IP** déployé, ça se passe comme suit :

1) Le téléphone **IP** est reconnu par les serveurs mutualisés de téléphonie (**ToIP**) se situant sur un réseau de serveurs spécialisés. C'est depuis ces serveurs qu'on a accès au **CUCM** (CallManager Cisco) afin de visualiser tout téléphone **IP** relié au **SIGV** (annuaires) et afin de pouvoir les reconfigurer derrière.

2) On inscrit manuellement dans l'**AD** le nouveau numéro de téléphone correspondant à un utilisateur déjà existant ou à un nouvel utilisateur afin de l'identifier plus précisément.

3) Le **CUCM** se met à jour en synchronisant ses données avec l'ajout effectué dans l'**AD**.

4) ***Cisco Jabber*** se synchronise à son tour avec le **CUCM**, permettant de maintenir à jour ses annuaires au service de ses utilisateurs (agents de l'effectif).

4 – Tâches diverses :

Cette sous-partie étant différente des précédentes au sens du contenu et de la structuration, elle se situera intégralement en annexes (voir **ANNEXES – E**) !

IV – Conclusion : [↑]

1 – Résumé :

Ce stage m'aura permis beaucoup de choses : m'initier et me familiariser un peu avec le monde professionnel, mettre parfois en application ce que j'avais pu découvrir de façon théorique, ainsi que découvrir de nouvelles notions dans le domaine des réseaux informatiques.

J'ai pris beaucoup de plaisir à réaliser ce stage ; le rythme de vie me plaisait et les personnes que j'ai pu côtoyer m'étaient très agréables et sympathiques. Cela m'a par ailleurs permis de développer encore un peu plus ma capacité à communiquer avec autrui. Au-delà de personnes que je côtoyais au quotidien, j'ai parfois dû communiquer avec des agents qui m'étaient parfaitement inconnus afin de prêter attentions aux problèmes qu'ils rencontraient, pour par la suite les régler (si j'y étais autorisé).
Les compétences indubitables de mon tuteur de stage ainsi que de M. Prati m'ont permis de me sentir impliqué et de m'intéresser d'autant plus à ce qui était fait sous mes yeux. Je n'hésitais pas à poser des questions sur les sujets qui me semblaient importants et où j'avais des doutes, et ils n'hésitaient pas à me répondre et à m'expliquer autant de fois qu'il le fallait certains principes.

Ces **10** semaines de stage m'ont permis de me donner un avant-goût de ce qui pouvait m'attendre plus tard. Cette période en tant que stagiaire m'a fait le plus grand bien, puisque le quotidien est bien différent de celui des études auquel j'ai pu être confronté depuis le début de l'année scolaire. En bref, je suis fier et heureux d'avoir pu réaliser ma première expérience quasi-professionnelle dans un cadre aussi accueillant et chaleureux que la mairie de Cabriès, et j'ai hâte de poursuivre ainsi sur la voie du professionnalisme en réalisant, sur mes résultats le permettent, ma prochaine année d'études en alternance !

2 – Remerciements :

Je tiens à remercier toutes les personnes qui m'ont m'accueilli chaleureusement au rez-de-chaussée du site de la mairie centrale : ***Maxime BRUNET*** mon tuteur, ***Christophe QUAZIZ*** son collègue, ***Mélody MALESA***, ***Valentin EFFANTIN*** ainsi qu'***Amapola VENTRON*** maire de Cabriès.

Il m'est également impossible de ne pas citer ***Gabriel PRATI***, membre du **SIGV**, avec qui j'ai passé la plupart de mon temps pour de nombreuses interventions instructives.

Merci aussi à toutes les personnes que j'ai pu croiser de près ou de loin, je ne peux pas toutes les citer ici. En plus de cette expérience pour mon futur professionnel, je retiendrai tous ces bons moments que j'ai pu passer avec les autres ; pour moi, la perspective professionnelle saine ne se construit qu'à partir d'un bien-être social personnel fondé par de solides bases humaines et relationnelles !

3 – Glossaire des Acronymes :

SIGV : Syndicat Intercommunal Grand Vallat [↑]

IP : Internet Protocol [↑]

BUT : Bachelor Universitaire de Technologie [↑]

PCs (ou PC) : Personal Computer(s) [↑]

WIFI : Wireless Fidelity [↑]

AD : Active Directory [↑] [↓]

LAN : Local Area Network .[↑

ToIP : Telephony over Internet Protocol [↑]

IPBX : Internet Protocol Private Branch Exchange [↑] [↓]

PRA : Plan de Reprise d'Activité [↑]

PCA : Plan de Continuité d'Activité [↑]

VPN : Virtual Private Network [↑] [↓]

SBC : Session Border Controller [↑] [↓]

Trunk SIP : Trunk Session Initiation Protocol [↑] [↓]

BLOD : Boucle Locale Optique Dédiée [↑]

NAS : Network-Attached Storage [↑]

VLAN : Virtual Local Area Network [↑] [↓]

DHCP : Dynamic Host Control Protocol [↑]

UO : Unité d'Organisation [↑] [↓]

OU : Organizational Unit [↑] **(UO = OU)**

GPO : Groupe Policy Object [↑] [↓]

NetBIOS : Network Basic Input/Output System [↑] [↓]

LDAP : Lightweight Directory Access Protocol [↑] [↓]

DGS : Directeur.trice Général.e des Services [↑]

SPN : Service Principal Name [↑]

DNS : Domaine Name System [↑]

SMTPS : Simple Mail Transfert Protocol Secure [↑] [↓]

OSI : Open Systems Interconnection [↑] [↓]

ESMI : Espace de Stockage du Matériel Informatique [↑]

RAM : Random Access Memory [↑]

VGA : Video Graphics Array [↑] [↓]

HDMI : High Definition Multimedia Interface [↑] [↓]

DP : DisplayPort [↑] [↓]

USB : Universal Serial Bus [↑]

URL : Uniform Resource Locator [↑]

@IPv4 : utilisé pour désigner une adresse IPv4. [↑]

@IPv6 : utilisé pour désigner une adresse IPv6. [↑]

APIPA : Automatic Private Internet Protocol Addressing [↑] [↓]

@IP : utilisé pour désigner une adresse IP (le plus souvent une adresse IPv4). [↑]

BDD : Base De Données [↑]

SSH : Secure Shell [↑] [↓]

SE : Système d'Exploitation [↑] [↓]

OS : Operating System [↑] **(SE = OS)**

BIOS : Basic Input/Output System [↑]

[

SSID : Service Set Identifier [↑] [↓]

APs (ou AP) : Access Point [↑] [↓]

CUCM : Cisco Unified Communications Manager [↑]

4 – Glossaire des Compléments :

sites : ici est appelé « site » un endroit, géré par le **SIGV**, contenant un ensemble d'équipements informatiques, de logiciels, de protocoles se connectant et communiquant entre eux et vers d'autres sites. [↑]

AD : le but de l'**AD** est de pouvoir gérer une base de données constituée d'un ensemble de services informatiques qui permettent de mettre en lien les utilisateurs avec les ressources réseau dont ils ont besoin pour réaliser convenablement leurs missions. [↑] [↑]

IPBX : l'**IPBX** est un autocommutateur téléphonique (appareil intermédiaire entre un appelant et un appelé, redirigeant le trafic au bon endroit selon des règles d'appel effectives) privé utilisant le protocole IP pour gérer les appels téléphoniques au sein d'une certaine entreprise (en interne, donc). Il assure donc dans notre cas le système téléphonique de l'ensemble des sites affiliés au **SIGV** (vous pouvez le voir comme placé au niveau de l'entité « **BACKBONE SIGV** » sur le schéma de la sous-partie d'où vous provenez, à savoir la sous-partie **1** de la partie **II**). [↑] [↑]

redondance : ce qu'on appelle redondance, c'est le processus consistant à ajouter des équipements de réseau et des lignes de communications supplémentaires afin de maintenir une connectivité (effective) si la voie principale ou empruntée par défaut venait à tomber en panne. C'est un mécanisme essentiel pour toute entreprise ou collectivité, puisqu'une panne momentanée de connectivité peut engendrer d'énormes problèmes. [↑]

VPN : l'objectif d'un **VPN** est, pour un utilisateur, de pouvoir se connecter à un réseau privé distant au travers d'Internet, via un tunnel privé et chiffré. Dans le cadre professionnel, il peut donc permettre à un agent d'entreprise par exemple d'accéder à un serveur interne d'une entreprise d'où il veut (à condition que ce soit en accord avec les potentielles règles de filtrage du **VPN**). Ce client, représenté par l'agent d'entreprise, est alors nomade. C'est une des formes pouvant être prises par une liaison **VPN** (hôte à site). Il est également possible de mettre en place une liaison **VPN** entre deux sites, on parle dans ce cas-là d'une liaison site à site. En somme, une liaison **VPN** assure la transmission des données de manière sûre et anonyme sur des réseaux publics. Dans le cadre de mon stage, j'ai pu voir Gabriel (pour rappel membre du **SIGV**) beaucoup utiliser son **VPN** de n'importe où afin d'avoir accès aux différents Switches (à des fins de configuration) situés donc dans des réseaux privés/internes. [↑] [↑]

SBC : cet équipement, installé en cœur de réseau ou en périphérie (au bord) sur un environnement de téléphonie sur **IP** (comme c'est notre cas ici), permet d'exercer un contrôle (sécurité) sur les flux multimédias auxquels il est lié. [↑] [↑]

Trunk SIP : le **Trunk SIP** est la liaison qui permet à une entreprise ou collectivité possédant un environnement de téléphonie sur **IP** (comme c'est notre cas ici) de transiter ses communications téléphoniques vers l'extérieur. D'ailleurs, le **Trunk SIP** doit être vu comme plusieurs canaux établis entre le système de téléphonie interne et l'extérieur ; ainsi, sachant que les communications transitent dans ces canaux, plus le nombre de canaux est élevé, plus le **Trunk SIP** permet de faire transiter un grand nombre de communications simultanément. **[↑] [↑]**

site centralisateur : ce que j'appelle un « site centralisateur » est un site, appartenant à un **BLOD**, permettant d'établir la connexion entre deux sites de ce même **BLOD**, et permettant aussi d'établir la connexion entre tous ces sites et l'instance du **SIGV**. **[↑]**

VLAN : un **VLAN** est un réseau **LAN** qui est virtuel et indépendant ; il permet d'améliorer la gestion d'un certain réseau, d'optimiser sa bande passante, de séparer les flux et donc par extension de renforcer la sécurité. Il n'est par défaut pas possible de communiquer entre plusieurs **VLANs**, mais le routage inter-vlan peut rendre cela possible au niveau 3 ! **[↑] [↑]**

proxies : de façon générale, un « proxy » est un serveur qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour en faciliter et/ou surveiller leurs échanges. En réseau, il est communément utilisé en tant qu'intermédiaire pour accéder à un autre réseau (souvent Internet d'ailleurs). **[↑]**

routage inter-VLANs : ce que j'appelle le « routage inter-**VLANs** » (ou routage entre **VLANs**) c'est cette capacité qu'on les différents **VLANs** à communiquer entre eux. Cela s'effectue au niveau **3** en traitant ce qu'on appelle des interfaces **VLAN**. **, par** le **SIGV**.

forêt : une forêt représente un espace, une collection composée d'au moins un domaine. **[↑]**

domaine : en informatique, un domaine constitue un ensemble d'utilisateurs qui va partager les mêmes ressources et qui va avoir les mêmes exigences de sécurité. On distingue alors le domaine principal (qui a le même nom que la forêt), des autres domaines (qui ont une même base de nom que la forêt, et qui dépendent du domaine principal). **[↑]**

ressources : une ressource, dans le cadre de l'**AD**, représente un appareil informatique (imprimante, **PC**, borne **WIFI**, commutateur, routeur, ...) ou un élément logique d'un appareil informatique (dossiers, fichiers). **[↑]**

groupes : un groupe, toujours dans le cadre de l'**AD**, permet de regrouper les différents utilisateurs d'un domaine afin de simplifier la gestion de leurs droits **NTFS*** sur les différentes ressources et afin de mieux les distinguer lors de l'application d'une **GPO**. **[↑]**

***** « **New Technology File System** » : système de fichiers utilisé par le **SE** Windows. Ici, les « droits **NTFS** » (donc les droits relatifs au système de fichiers et à son arborescence), seront appliqués sur les groupes et les utilisateurs.

UO : une unité d'organisation est un objet qui va permettre de se calquer au plus proche possible de l'organisation d'une entreprise ou collectivité en regroupant des utilisateurs et/ou des ordinateurs. **[↑] [↑]**

GPO : une **GPO** (ou stratégie de groupe) est, de façon générale, un objet qui va contenir toute la sécurité que l'on veut appliquer sur l'environnement de l'utilisateur ou de l'ordinateur. On l'appliquera alors sur une certaine **UO**, qui contient des utilisateurs et/ou des ordinateurs, afin de leur exiger des normes de sécurité choisies. Considérons une **UO** contenant une autre **UO** ; si on applique une **GPO** sur la première **UO** (**UO** parent), celle-ci sera également appliquée à la deuxième (**UO** enfant), c'est ce qu'on appelle « l'héritage ». Ainsi, la **GPO** qu'on applique sur une **UO** parent est prioritaire sur toutes les potentielles **GPO** qu'on appliquera sur les **UO** enfants de cette **UO** parent. **[↑] [↑]**

contrôleurs de domaine : on entend par « contrôleur de domaine » tout serveur Windows qui contient la **BDD** de l'**AD** et qui prend en charge toutes les fonctions liées à ce système (authentification et autorisation). S'il faut obligatoirement deux contrôleurs de domaine par domaine, c'est pour assurer la disponibilité et la continuité du service de l'**AD**, aujourd'hui essentiel au bon fonctionnement de tout une infrastructure informatique. **[↑]**

NetBIOS : c'est le protocole qui est utilisé entre les machines Windows pour communiquer. C'est un système de nommage et une interface logicielle permettant d'établir des sessions entre différents ordinateurs d'un certain réseau. Ainsi, le nom **NetBIOS** d'une machine d'écrit comme tel : « **\\nom_de_la_machine** ». Si une machine souhaite partager une ressource, le nom de partage de cette ressource (utile aux autres machines qui souhaiteraient également, en étant autorisées au préalable, accéder à la ressource) s'écrira comme ça : « **\\nom_de_la_machine_qui_partage\nom_de_partage_de_la_ressource** ». **[↑]** [↑]

domaine racine : le domaine racine d'une forêt est le premier domaine à avoir été créé dans celle-ci, c'est alors le domaine parent de tous les autres qui seront créés par la suite. Le domaine racine d'une forêt a le même nom que la forêt dans laquelle il se situe. [↑]

intra-domaine : qui est relatif à l'intérieur d'un certain domaine (« intra » pour intérieur). [↑]

services : un service, dans le cadre de l'**AD**, est une fonctionnalité, un logiciel, ou en tout cas quelque chose pouvant être utilisé par d'autres membres de l'**AD** (serveur WEB, partage réseau, service **DNS*/DHCP**, service d'impression, ...). [↑]

* « **Domain Name System** » : système associant des noms de domaine Internet avec leurs **@IP** (ou d'autres types d'enregistrements, comme du texte simple par exemple).

LDAP : **LDAP** est un protocole qui, à la base, permet l'interrogation et la modification de services d'annuaires. Il repose sur la suite de protocoles **TCP/IP** pour fonctionner. **[↑]** [↑]

groupes de sécurité : les groupes de sécurité, dans le cadre de l'**AD**, sont utilisés pour gérer les droits et les autorisations (pour les utilisateurs) sur des ressources d'un certain domaine. [↑]

relation d'approbation : une relation d'approbation est un lien qui permet d'ouvrir un certain domaine aux ressources d'un autre domaine. Une relation tirée d'un domaine **A** vers un domaine **B** donne la possibilité au domaine **A** d'accéder aux ressources du domaine **B**, mais ce à condition qu'un administrateur du domaine **B** donne la permission aux utilisateurs certifiés du domaine **A** d'accéder effectivement aux ressources de leur domaine **B**. Une relation d'approbation peut être implicite (créée automatiquement par le système) ou explicite (créée par l'administrateur système). Une relation d'approbation peut aussi être unidirectionnelle (des utilisateurs d'un domaine **A** peuvent accéder aux ressources d'un domaine **B**, mais pas l'inverse) ou bidirectionnelle (des utilisateurs d'un domaine **A** peuvent accéder aux ressources d'un domaine **B** et inversement). Les domaines enfants du domaine principal « **sigv.lan** » sont reliés à celui-ci par une relation d'approbation bidirectionnelle. [↑]

relation d'approbation de forêts : une relation d'approbation de forêts est une relation d'approbation mais se faisant entre deux domaines de deux forêts différentes. Dans ce cas, ce sont les deux domaines racine qui sont liés par une relation d'approbation de forêts. Le **SIGV** ne possède pas de relation d'approbation de forêts avec une autre forêt. [↑]

noms principaux de service : pour identifier un certain service, il est nécessaire de connaître le nom du service ainsi que la machine sur laquelle tourne le service (puisqu'il pourrait y avoir un service tournant sur plusieurs machines ou plusieurs services tournant sur une seule machine, rendant impossible la distinction d'un service seulement par le nom de service ou le nom de machine). C'est justement en combinant ces informations (nom de service + machine sur laquelle il tourne) qu'on obtient ce qu'on appelle un « nom principal de service », noté **SPN** (toujours dans le cadre de l'**AD**). [↑]

extérieur : quand je parle de « l'extérieur » de façon générale, je désigne tout réseau/hôte qui n'est pas géré par le **SIGV** (Internet, réseau opérateur Orange, ...). [↑]

intérieur : quand je parle de « l'intérieur » de façon générale, je désigne tout réseau/hôte qui est géré par le **SIGV** (sites, liens inter-sites, ...). [↑]

l'effectif : j'entends par « l'effectif » l'ensemble de toutes les personnes occupant un poste géré informatiquement par le **SIGV** (peu importe la commune parmi les trois gérées par le **SIGV**, donc). [↑]

SMTPS : c'est un protocole sécurisé permettant d'envoyer et de recevoir des messages électroniques (mails) sur Internet. [↑] [↑]

boîtier fibre : un boîtier fibre (placé sur site) permet d'accueillir une liaison fibre provenant d'un autre site et/ou de fournir une liaison fibre allant vers un autre site ou vers l'Internet (dans ce dernier cas on passe par un fournisseur/opérateur). [↑]

modèle OSI : il définit une architecture « hiérarchique » répartissant logiquement les fonctions nécessaires à la communication entre différents systèmes. Le modèle **OSI** comporte **7** couches (officieusement ***8***). [↑] [↑]

données extra-système : ce que j'appelle des « données extra-système » ici, sont des données qui ne sont pas absolument nécessaires au bon fonctionnement d'un système. [↑]

VGA, HDMI, DP : ce sont là trois interfaces de connexion. L'interface « **VGA** » est la plus ancienne, elle reste encore couramment utilisée de nos jours. L'interface « **HDMI** » est plus récente ; adaptée pour la haute résolution, elle permet de transporter le son en plus du signal vidéo (contrairement à **VGA**). L'interface « **DP** » est la plus récente des trois, et certainement la plus performante : elle propose une meilleure bande passante que l'interface « **HDMI** » et supporte parfaitement les modes 8K. [↑] [↑]

hyperviseur de type 1 : un hyperviseur est un logiciel permettant de créer et d'exécuter des machines virtuelles. Un hyperviseur de type **1** effectue sa tâche en interagissant directement avec le matériel physique de la machine (contrairement à l'hyperviseur de type **2**, qui s'exécute sur un **SE**). [↑]

nom de domaine : un nom de domaine permet de traduire une adresse **IP** en un nom qui parle plus et qui est plus facilement mémorisable. Du point de vue logique, une **@IP** peut avoir son équivalent en nom de domaine ; un nom de domaine a forcément au moins une **@IP** qui lui est associée. [↑]

réseau privé : un réseau privé utilise obligatoirement les plages d'adressage **IP** suivantes : **10.0.0.0/8**, **172.16.0.0/12**, **192.168.0.0/16**. Il permet de faire communiquer de nombreux appareils entre eux, bien que les **@IP** utilisées dans ce cadre ne soient pas routables sur l'Internet (puisqu'il pourrait en exister plus d'une dans ce milieu, rendant impossible la différenciation de deux **@IP** similaires). Ils sont majoritairement utilisés en entreprise ou en collectivité. [↑]

0.0.0.0 : l'utilisation de cette **@IP** non-routable désigne une destination invalide, inconnue, ou inatteignable. [↑]

APIPA : le mécanisme APIPA permet à une machine de s'attribuer automatiquement une **@IP** si aucune **@IP** n'est définie sur une certaine interface considérée et si les requêtes **DHCP*** effectuées ensuite par défaut échouent. Une adresse **APIPA** utilise un masque de sous-réseau en **/16**, où les deux octets de la partie réseau sont toujours les mêmes : **169.254.X.Y/16** ***(0 <= X <= 255 | 1 <= Y <= 254)***. [↑] [↑]

* « **Dynamic Host Control Protocol** » : attribue dynamiquement des **@IP** à chaque hôte autorisé le demandant.

machines virtuelles : de façon générale, une machine virtuelle est un environnement complètement virtualisé qui fonctionne sur une machine physique : c'est une émulation, une simulation d'un appareil informatique (pouvant être créée/exécutée/instanciée grâce à un hyperviseur) qui a son propre **SE** et ses propres caractéristiques physiques (processeur, **RAM**, disque dur, carte réseau, ...). Plusieurs machines virtuelles peuvent être exécutée sur une seule machine physique : c'est l'un de leurs avantages. [↑]

partition de disque : une partition de disque est une section d'un espace de stockage disque. Ainsi, pour un même disque dur (par exemple), on peut établir différentes partitions qui ont a priori chacune une attribution spécifique et donc un rôle spécifique dans le stockage des données du disque. [↑]

SSH : **SSH** est un protocole permettant d'envoyer de façon sécurisée des commandes à un ordinateur (hôte ou serveur), et ce même sur un réseau potentiellement non sécurisé. [↑] [↑]

SE : un **SE** désigne l'ensemble des programmes permettant de faire correctement fonctionner un certain appareil informatique. [↑] [↑]

Windows 10 « Professionnel » : Windows 10 est un **SE** possédant plusieurs éditions. Chaque édition est faite pour s'adapter à un certain contexte en rajoutant certaines fonctionnalités adaptées au contexte d'utilisation. Ici, Windows 10 « Professionnel » est l'une des douze éditions liées à Windows 10, et confère, en plus des fonctionnalités de l'édition de base, certaines étant orientées pour l'environnement professionnel (**AD**, Bureau à Distance, BitLocker, Hyper-V, Windows Defender Device Guard, ...). **[↑]**

clé bootable : ce que j'appelle « clé bootable » ici, est un périphérique externe (clé **USB**) contenant un système de fichiers permettant de démarrer un ordinateur (ici, notre clé bootable contient le **SE** Windows 10 « Professionnel »). Ainsi, ce n'est pas le disque dur de l'ordinateur (contenant le **SE** intégré à l'ordinateur, utilisé par défaut) qui est sollicité, mais bien le lecteur **USB** externe (contenant le **SE** qu'on veut que l'ordinateur utilise). **[↑]**

fichier .iso : j'entends par « fichier .iso » un fichier dont l'extension est « .iso ». Un fichier .iso est un format de fichier numérique reproduisant, par son contenu qui lui est strictement identique au niveau des fichiers, des dossiers et de l'arborescence, un **CD**, **DVD**, blu-ray, etc. (en clair un disque optique ou magnétique). Le fichier .iso qu'on utilise ici contient tout un **SE** Windows 10 « Professionnel », et est directement compatible avec le **PC** par la suite utilisé auquel on va vouloir intégrer le nouveau **SE** contenu dans le fichier .iso, lui-même contenu dans la clé bootable. **[↑]**

BIOS : le **BIOS** est un logiciel stocké sur la carte mère d'un ordinateur utilisé par le microprocesseur (ensemble de circuits intégrés permettant de traiter l'information) de l'ordinateur pour permettre le bon démarrage du système informatique dudit ordinateur après sa mise sous tension. **[↑ [↑]**

prises réseau : j'entends par une « prise réseau », une prise murale Ethernet qu'on trouve fréquemment dans des bâtiments, notamment de travail. Ce genre de prise sert à relier un certain équipement au réseau interne du site sur lequel elle est présente et/ou de le faire accéder [cet équipement] à l'extérieur. **[↑]**

brassées : ce que j'entends par une prise « brassée » est une prise qui est disponible à l'accueil d'un équipement informatique car elle est correctement configurée au lieu de son arrivée au niveau de la baie de brassage. **[↑]**

Switch de regroupement des différents postes : j'entends par un « Switch de regroupement de différents postes » le Switch principal, situé dans une baie de brassage, permettant d'accueillir tout équipement réseau du réseau interne du site en son sein et permettant à ces équipements d'accéder, avec plus ou moins de possibilités, à l'extérieur. **[↑]**

noyaux : entre une prise réseau/murale et un Switch de regroupement des différents postes se situe un noyau. Ainsi, si « ------- » correspond à un câble réseau, on pourrait résumer l'infrastructure énoncée comme ça :

Prise réseau/murale ------- Noyau ------- Switch de regroupement des différents postes

Un noyau est donc l'élément qui prend en entrée l'arrivée par câble de la prise réseau et propose en sortie une potentielle connexion avec le Switch de regroupement des différents postes. Il est généralement situé dans la baie de brassage, proche du Switch. Afin de faciliter le travail de brassage d'une certaine prise murale, on annote généralement un numéro proche de celle-ci, numéro qu'on reporte au noyau relié à cette prise murale pour établir une correspondance désormais connue. Ainsi, si on branche par exemple un câble correspondant à un équipement quelconque sur la prise murale annotée « **13** », on saura qu'elle est reliée par un câble au noyau également annoté « **13** » dans la salle de brassage. **[↑]**

clients légers : un client léger est un périphérique informatique basique mais qui exécute la presque totalité des services auxquels il a recours sur un serveur centralisé (gestion, stockage, session utilisateur, ...) ; il n'a presque pas de logique d'application et dépend donc surtout du serveur centralisé auquel il est rattaché pour le traitement des données. Pour ce qui est du matériel, un client léger peut se contenter d'une machine minimaliste sans problèmes (ordinateur très ancien, moderne, ou spécialisé dans la technologie du client léger). **[↑]**

mode access : configurer un port en mode access dans le cadre de **VLANs** permet à ce port d'acheminer uniquement le trafic vers et depuis le **VLAN** spécifique qui lui a été attribué. Le mode access est utilisé pour la connexion terminale d'un certain périphérique (**PC**, imprimante, serveur, ...) appartenant à un seul **VLAN**. **[↑]**

mode trunk : configurer un port en mode trunk dans le cadre de **VLANs** permet à ce port de laisser passer les trames provenant et allant vers différents **VLANs**. Cela se fait via un mécanisme de tags : chaque trame autorisée à passer dans une liaison trunk (via un port en mode trunk donc) est « taguée » avec le **VLAN** correspondant, puis « détaguée » quand elle arrive au niveau d'un port en mode access correspondant à sa destination finale. **[↑]**

firmware : de façon générale, le firmware correspond au programme intégré dans un matériel informatique pour qu'il puisse fonctionner. **[↑]**

2.4 GHz ou 5 GHz : tout d'abord, ces valeurs sont des fréquences qui correspondent à des bandes de fréquence, c'est à dire la place dont dispose un signal pour passer. Les bandes **2.4 GHz** et **5 GHz** sont les deux bandes de fréquences radio qui permettent d'émettre un signal sans fil. Le choix de la bande d'émission s'effectue selon des critères de débit et de portée. La bande **2.4 GHz** est une bande longue portée moins rapide que la bande **5 GHz** et plus sensible aux interférences (puisqu'elle offre moins de place que la bande **5 GHz** et est donc plus facilement « encombrable »). La bande **5 GHz** elle est une bande plus rapide (permettant un meilleur débit) que la bande **2.4 GHz**, moins sensible aux interférences (car plus de place), mais sa portée est plus courte que la bande **2.4 GHz**. Le choix se fait donc selon l'infrastructure effective d'un site et selon les projets qu'on a en tête, bien qu'il existe aujourd'hui des équipements capables d'émettre sur les deux bandes en même temps (d'ailleurs dans
le cas des bornes UniFi installées par le **SIGV**, les deux bandes de fréquence sont utilisés pour un même **SSID**, puisque la technologie de ces bornes le permet). **[↑]**

SSID : le **SSID** est un simple terme technique utilisé pour désigner le nom d'un réseau **WIFI** (réseau permettant un accès à un autre derrière). **[↑]** **[↑]**

APs : un **AP** est un dispositif permettant aux périphériques de se connecter à un certain réseau, via une connexion sans fil/radio. **[↑]** **[↑]**