

**E5R : ÉTUDE DE CAS****Durée : 4 heures****Coefficient : 5****CAS XONI**

Ce sujet comporte 23 pages dont 18 pages de documentation.

Le candidat est invité à vérifier qu'il est en possession d'un sujet complet.

**Matériels et documents autorisés**

- Aucun document n'est autorisé
- Seul le matériel de composition (feuilles, stylo, gomme, règle, effaceur...) est autorisé

**Aucun appareil électronique n'est autorisé****Barème**

Mission 1 – gestion de l'architecture et de la sécurité	65 points
Mission 2 – Résolution d'incidents	35 points
Total	100 points

# 1 Présentation de la société Xoni

La société Xoni est le leader dans la fabrication et la distribution de tubes en acier inoxydable sans soudure destinés à une industrie à forte contrainte de sécurité tels que les centrales nucléaires.

Elle utilise deux principes de fabrication :

- le filage ;
- l'étirage.

La production est réalisée sur deux sites, l'un situé à Dijon et l'autre à Rouen. Le siège social, situé à Paris, gère toutes les transactions commerciales de la société ainsi que les différents aspects informatiques de la société. Dans chaque usine se trouve un responsable informatique qui est l'interlocuteur privilégié de la Direction des Services Informatique.

## 1.1 Le site de Dijon

L'usine conçoit des tubes de diamètre compris entre 25 et 50 mm. De l'acier fondu dans des fourneaux à 1 000°C passe dans des filières de diamètre variable. À sa sortie, le tube est plongé dans un bain d'acide afin d'évacuer toute aspérité.

## 1.2 Le site de Rouen

L'usine est spécialisée dans la conception des tubes fins ayant un diamètre inférieur à 25 mm. Pour les réaliser, la technique de l'étirage est utilisée. Elle nécessite des tubes plus épais produits par le site de Dijon. Ces tubes sont tirés à froid et passent dans des goulottes de plus en plus étroites jusqu'à l'obtention du diamètre désiré.

## 1.3 Le contrôle qualité

Chaque tube doit être contrôlé minutieusement. Toute imperfection pourrait avoir des conséquences désastreuses. Ces vérifications sont effectuées par des scanners. Un tube ne correspondant pas aux critères de sélection est mis au rebut et envoyé à la fonte.

## 1.4 Le service commercial

Le service commercial est composé majoritairement d'ingénieurs spécialisés dans les transactions commerciales. Ces ingénieurs négocient aussi bien avec des compagnies françaises qu'étrangères et sont sous la responsabilité du Directeur Commercial de Xoni.

Les ingénieurs commerciaux doivent à tout moment et en tout lieu pouvoir accéder aux informations commerciales et technique des produits. Ces données étant sensibles et hautement confidentielles, chaque ingénieur doit disposer d'une liaison sécurisée.

## 1.5 Votre place dans la société

Vous avez été embauché par la société Xoni en tant que technicien réseau « Junior ». Vous êtes placé directement sous la responsabilité du Directeur des Services Informatiques de la société. Votre poste est basé à Paris, au siège social.

## 2 Mission 1

### Gestion de l'architecture réseau et de la sécurité

Un audit de sécurité a été réalisé par une société extérieure à la demande du directeur des services informatiques. Un résumé du rapport d'audit, concernant le site de Dijon vous a été remis. Votre responsable a, à partir de ce document, étudié une solution modifiant l'architecture du site de Dijon. Il vous a communiqué les documents relatifs à cette modification. Une réunion avec la Direction Générale est prévue prochainement pour discuter, entre autre, du bien fondé de cette solution et son adéquation avec les préconisations du rapport d'audit.

Votre responsable souhaite présenter un argumentaire technique pour justifier le choix de la solution retenue. Habitué à ce genre de réunion, il se doute des questions qui vont lui être posées et vous demande de rédiger les principaux éléments de réponse. Vous rédigerez donc, en quelques phrases, des réponses argumentées pour chacune des questions suivantes :

<b>Q-1.1.</b>	<b><i>En quoi le découpage en VLAN correspond-il aux objectifs d'amélioration de performance et de sécurité définis dans les préconisation du rapport d'audit ?</i></b>
<b>Q-1.2.</b>	<b><i>Pourquoi chaque VLAN doit-il correspondre à un sous-réseaux différent ?</i></b>
<b>Q-1.3.</b>	<b><i>Chaque VLAN pourra-t-il accueillir le nombre de postes nécessaire ?</i></b>
<b>Q-1.4.</b>	<b><i>Pourquoi est-il intéressant que le commutateur SW1 puisse faire du routage inter-vlan ?</i></b>
<b>Q-1.5.</b>	<b><i>Pouvait-on obtenir la même architecture avec un commutateur ne supportant pas le routage inter-vlan ? Si oui, comment ?</i></b>
<b>Q-1.6.</b>	<b><i>Pourquoi n'est-il pas gênant que les commutateurs du réseau administratif ne supportent pas les VLAN ?</i></b>
<b>Q-1.7.</b>	<b><i>Le protocole Spanning Tree doit-il être activé sur tous les commutateurs, seulement sur certains ou sur aucun ?</i></b>

Pour empêcher la connexion des ordinateurs personnels des salariés, différentes procédures de contrôles d'accès ont été listées par le chef de projet.

<b>Q-1.8.</b>	<b><i>Évaluer chaque solution en indiquant si elle est envisageable avec le matériel dont on dispose et si elle répond ou pas au besoins de sécurité exprimé. Chaque réponse devra être argumentée.</i></b>
<b>Q-1.9.</b>	<b><i>Proposer la solution qui vous semble la plus appropriée en justifiant ce choix.</i></b>

Un appel d'offre a été lancé pour la réalisation des sauvegardes du site de Dijon sur les serveurs d'une entreprise spécialisée dans les sauvegardes, indépendante de la société Xoni. Il vous est demandé d'étudier les deux offres qui ont été reçues et de rédiger une note répondant précisément et de manière argumentée, aux questions :

<b>Q-1.10.</b>	<b><i>Quel est le volume à sauvegarder à partir duquel l'offre BeNeo sera, d'un point de vue tarifaire, plus intéressante ?</i></b>
<b>Q-1.11.</b>	<b><i>Les deux prestataires n'autorisent pas le même type de sauvegarde. Quelle est l'incidence des « types de sauvegardes autorisés » sur une restauration complète en fin de période de sauvegarde ?</i></b>
<b>Q-1.12.</b>	<b><i>Quels sont les autres critères qui diffèrent entre les deux prestataires et qui ont une importance dans le choix de l'offre ?</i></b>
<b>Q-1.13.</b>	<b><i>Quelle est, de votre point de vue, l'offre à retenir ?</i></b>

Sans attendre la réunion, votre responsable vous charge de préparer la configuration des commutateurs sw1, sw2, sw3 et sw4.

<b>Q-1.14.</b>	<b><i>Énumérer la liste des VLAN à définir sur chaque commutateur (SW1, SW2, SW3 et SW4). Cette liste sera limitée au strict nécessaire.</i></b>
<b>Q-1.15.</b>	<b><i>Expliquer le problème posé pour la distribution des adresses par le serveur DHCP actuel sur les différents VLAN et proposer une solution.</i></b>
<b>Q-1.16.</b>	<b><i>Établir un tableau reprenant l'affectation des ports de SW1, en lui rajoutant deux colonnes :</i></b> <ul style="list-style-type: none"> <li><b><i>• Le ou les VLAN à associer à ce port ;</i></b></li> <li><b><i>• L'usage du protocole 802.1q sur ce port (oui ou non).</i></b></li> </ul>
<b>Q-1.17.</b>	<b><i>Donner la suite de commandes à réaliser pour obtenir la configuration que vous avez prévu à la question Q-1.16.</i></b>

## 3 Mission 2

### Résolution d'incidents

Votre responsable a reçu deux courriels, un de l'usine de Rouen et un du directeur du service commercial. Il vous transfère ces deux mails et vous demande prendre en charge la résolution de ces incidents.

La procédure de gestion des incidents au sein de l'entreprise Xoni, par un technicien « Junior » est toujours la même :

- Chercher la cause du problème signalé et une solution au problème ;
- Répondre par mail à celui qui a signalé l'incident en lui expliquant la cause ;
- Rédiger une courte note reprenant les symptômes et la cause technique de l'incident afin d'enrichir une base de connaissances, utile à tous les techniciens de l'entreprise ;
- Faire réaliser la solution.

Il vous est expressément rappelé, que, en tant que technicien « Junior » vous ne pouvez pas intervenir directement sur les matériels, même ceux du siège qui vous sont pourtant physiquement accessibles. Vous devez, obligatoirement par mail, proposer l'intervention à votre responsable si l'intervention concerne le siège. Il transmettra le mail à un technicien « Senior » qui réalisera l'intervention. Si l'intervention concerne une usine, vous devez proposer, toujours par mail, l'intervention au responsable informatique de l'usine concernée.

Dans les deux cas, le mail doit expliquer **très précisément** l'intervention qui doit être faite.

#### 3.1 Usine de Rouen

<b>Q-2.1.</b>	<b><i>Rédiger un mail à destination du directeur de l'usine de Rouen en lui expliquant la raison de l'incident qu'il mentionne.</i></b>
<b>Q-2.2.</b>	<b><i>Rédiger une courte note rappelant les symptômes de l'incident et sa cause technique.</i></b>
<b>Q-2.3.</b>	<b><i>Rédiger un courriel au correspondant informatique de Rouen pour lui indiquer précisément comment solutionner le problème.</i></b>

#### 3.2 Service commercial

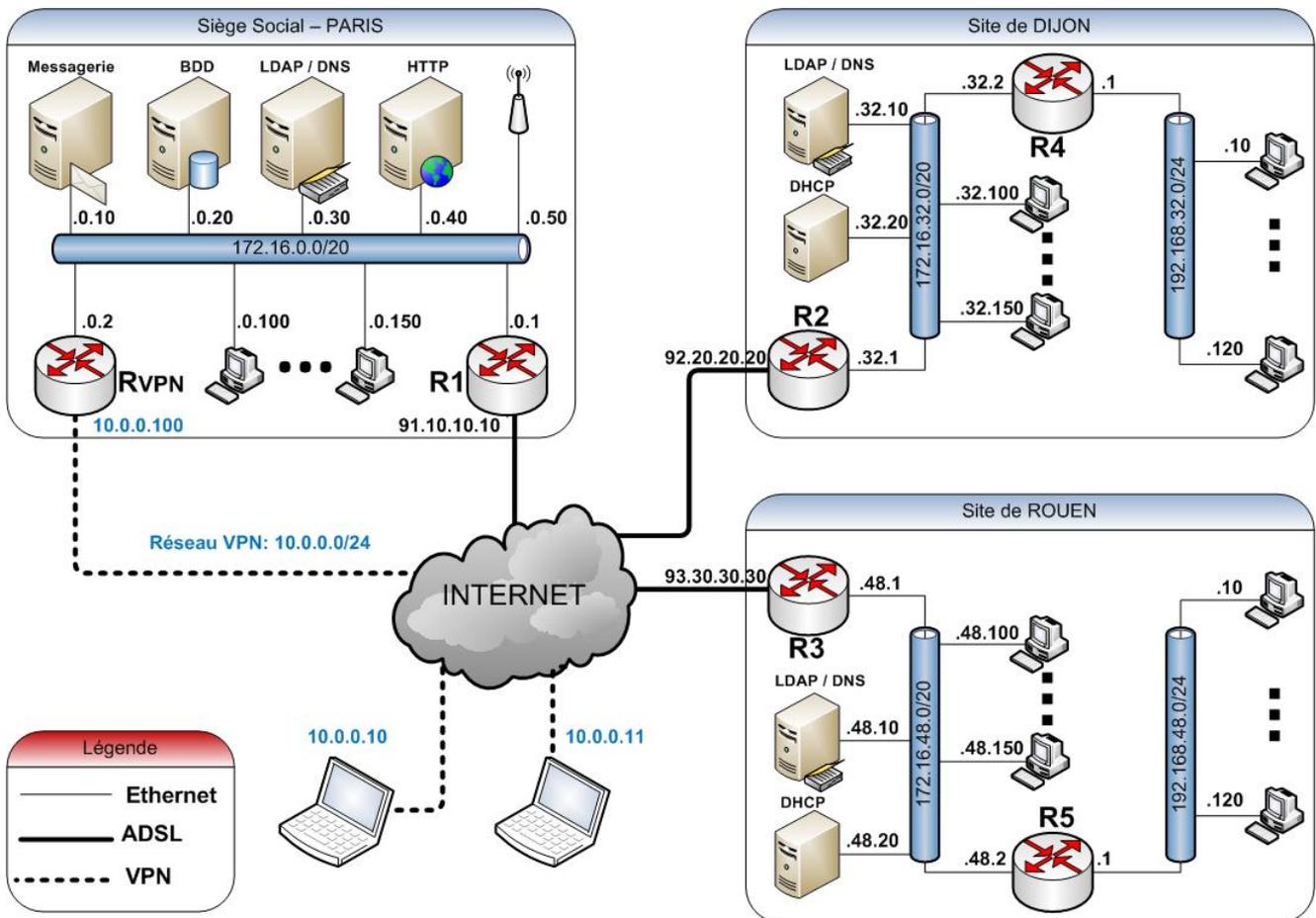
<b>Q-2.4.</b>	<b><i>Rédiger un mail à destination du directeur du service commercial en lui expliquant la raison de l'incident VPN qu'il mentionne.</i></b>
<b>Q-2.5.</b>	<b><i>Rédiger une courte note rappelant les symptômes de cet incidents VPN et précisant la cause technique.</i></b>
<b>Q-2.6.</b>	<b><i>Rédiger un e-mail à votre responsable pour proposer une solution afin de solutionner ce problème.</i></b>
<b>Q-2.7.</b>	<b><i>Expliquer, en le justifiant, quelle action il va falloir faire sur le routeur VPN afin que le vol du portable ne mette pas en danger la sécurité de l'entreprise.</i></b>
<b>Q-2.8.</b>	<b><i>Expliquer ce qu'il va falloir faire, avant d'envoyer le nouveau portable, pour que le commercial puisse accéder au VPN. Vous expliquerez les raisons de ces actions.</i></b>

## 4 Documentation fournie

<b>1</b>	<b>Documentation technique fournie par Xoni.....</b>	<b>7</b>
1.1	Architecture réseau de la société Xoni.....	7
1.2	Infrastructure des usines de Dijon et Rouen.....	8
1.3	Fonctionnement des échanges inter-sites.....	8
1.4	Paramétrages Routeur R1.....	9
1.4.1	Table de routage du routeur R1.....	9
1.4.2	Table de DNAT du routeur R1.....	9
1.4.3	Règles de filtrage du routeur R1.....	9
1.4.4	Contenu du fichier « /etc/firewall/rules » du routeur R1.....	10
1.5	Paramétrage du routeur R2.....	11
1.5.1	Table de routage du routeur R2.....	11
1.5.2	Table de DNAT du routeur R2.....	11
1.5.3	Règles de filtrage du routeur R2.....	11
1.5.4	Contenu du fichier « /etc/firewall/rules » du routeur R2.....	11
1.6	Paramétrage du routeur R3.....	12
1.6.1	Table de routage du routeur R3.....	12
1.6.2	Table de DNAT du routeur R3.....	12
1.6.3	Règles de filtrage du routeur R3.....	12
1.6.4	Contenu du fichier « /etc/firewall/rules » du routeur R3.....	12
1.7	Paramétrage du routeur RVPN.....	13
1.7.1	Table de routage du routeur Rvpn.....	13
1.7.2	Table de filtrage du routeur Rvpn.....	13
1.8	Paramétrage des serveurs du siège à Paris.....	13
1.8.1	Tables de routages des serveurs du réseau de Paris.....	13
1.8.2	Table de filtrage des serveurs de Paris.....	13
1.9	Extrait de la liste des ports standardisés.....	14
<b>2</b>	<b>Dossier technique d'évolution du site de Dijon.....</b>	<b>15</b>
2.1	Résumé du rapport d'audit.....	15
2.2	Architecture proposée pour le site de Dijon.....	16
2.3	Segmentation prévue pour le site de Dijon.....	16
2.4	Procédures de contrôle d'accès envisagées pour le site de Dijon.....	17
2.5	Affectation des ports sur le commutateurs SW1.....	17
<b>3</b>	<b>Documentation technique du matériel de Dijon.....</b>	<b>18</b>
3.1	Extrait de la documentation relative à SW1.....	18
3.2	Extrait de la liste des commandes acceptées par SW1.....	19
3.3	Extrait de la documentation relative à SW2/SW3/SW4.....	20
<b>4</b>	<b>Réponse à l'appel d'offre.....</b>	<b>21</b>
4.1	Données techniques.....	21
4.2	Offres de solutions de sauvegarde en ligne.....	21
<b>5</b>	<b>Extraits de Wikipédia « Les sauvegardes ».....</b>	<b>22</b>
5.1	Méthodes (types) de sauvegarde les plus courantes.....	22
5.2	Mécanisme.....	22
5.3	Sauvegarde complète.....	22
5.4	Sauvegarde différentielle.....	22
5.5	Sauvegarde incrémentielle ou incrémentale.....	22
<b>6</b>	<b>Mails reçu par la DSI.....</b>	<b>23</b>
6.1	Mail1.....	23
6.2	Mail2.....	23

# 1 Documentation technique fournie par Xoni

## 1.1 Architecture réseau de la société Xoni



La société comporte 3 sites reliés entre eux par des lignes ADSL. Les routeurs R1, R2 et R3 prennent en charge les protocoles SNAT, DNAT et PAT.

Il existe un deuxième routeur (RVPN) au siège social de Paris qui permet à divers ingénieurs commerciaux de se connecter directement, en VPN, afin de bénéficier des services de réalisations de devis, de consultation de tarifs spécifiques et de consultations des données techniques liées aux fabrications.

Les ingénieurs commerciaux de la société XONI peuvent donc se connecter à partir du réseau internet sur le réseau du siège social en utilisant ce VPN.

Le principe du VPN mis en place est le suivant :

- Chaque ordinateur portable d'un ingénieur commercial va se connecter au réseau du siège social en utilisant une adresse IP publique et une connexion internet vers le routeur RVPN ;
- Le routeur va d'abord authentifier le portable de façon certaine, puis il va initialiser un tunnel sécurisé entre lui-même (RVPN) et l'ordinateur portable concerné. Il attribuera une adresse IP privée dans le tunnel sur le réseau 10.0.0.0/24 à l'ordinateur portable.

## 1.2 Infrastructure des usines de Dijon et Rouen

L'infrastructure des sites de Dijon et de Rouen est composée de 2 réseaux distincts :

- Le réseau administratif est composé des serveurs et d'une cinquantaine de postes ;
- Le réseau de production est composé d'environ 100 postes répartis sur les trois ateliers à raison de 30 à 40 postes par atelier.

Sur les sites de Dijon et de Rouen les différents postes informatiques sont reliés, au sein du même réseau, par des commutateurs 100Mbps non managés, qui ne sont pas représentés sur le schéma général.

En plus des serveurs représentés sur les sites de Dijon et de Rouen, il existe, dans chaque usine, une dizaine de serveurs de production, non représentés sur ce schéma et qui sont tous placés dans le réseau administratif, comme les serveurs LDAP/DNS et DHCP.

## 1.3 Fonctionnement des échanges inter-sites

Dans le réseau de la société XONI, un certain nombre de services sont centralisés au siège social de la société à Paris. Il s'agit principalement des services de messagerie, ainsi que des services d'annuaire. L'annuaire LDAP présent au siège est répliqué automatiquement sur les sites de Dijon et de Rouen, du moins pour la partie qui les concerne. Ceci signifie que les changements apportés dans l'annuaire (créations de comptes, modifications de comptes ou effacements de comptes) à Paris sont appliqués sur les sites de Rouen et de Dijon, en général au bout d'une heure. Cette réplication s'effectue au travers des différents ports utilisés par LDAP.

L'infrastructure DNS est la suivante :

- la zone xoni.fr est gérée par un serveur DNS principal situé à PARIS ;
- la zone dijon.xoni.fr est gérée par un serveur principal à DIJON ;
- la zone rouen.xoni.fr est gérée par un serveur principal à ROUEN ;
- Chaque serveur DNS sert aussi de serveur secondaire pour les autres zones. Ainsi, le serveur DNS de PARIS est serveur secondaire de la zone dijon.xoni.fr et rouen.xoni.fr. De même le serveur DNS de DIJON est serveur secondaire de la zone xoni.fr et rouen.xoni.fr.

En conséquence, les ports nécessaires à la réplication des serveurs DNS et des serveurs LDAP sont ouverts sur le site de Paris ainsi que les ports nécessaires à la messagerie.

Sur les autres sites, seuls sont ouverts les ports nécessaires à la réplication des serveurs LDAP.

## 1.4 Paramétrages Routeur R1

### 1.4.1 Table de routage du routeur R1

Réseau	Masque	Passerelle	Interface
172.16.0.0	255.255.240.0	-	172.16.0.1
91.10.10.0	255.255.255.0	-	91.10.10.10
0.0.0.0	0.0.0.0	Passerelle FAI	91.10.10.10

### 1.4.2 Table de DNAT du routeur R1

Interface d'arrivée	Adresse publique	Port public	Adresse privée de redirection	Port privé de redirection
eth0	91.10.10.10	53	172.16.0.30	53
eth0	91.10.10.10	25	172.16.0.10	25
eth0	91.10.10.10	110	172.16.0.10	110
eth0	91.10.10.10	143	172.16.0.10	143
eth0	91.10.10.10	389	172.16.0.30	389
eth0	91.10.10.10	636	172.16.0.30	636
eth0	91.10.10.10	3268	172.16.0.30	3268
eth0	91.10.10.10	88	172.16.0.30	88

### 1.4.3 Extrait des règles de filtrage du routeur R1

Ces règles s'appliquent en entrée de l'interface eth0 du routeur R1

No de règle	Adresse Source	Port source	Adresse Destination	Port Dest.	Protocole	Action
1	92.20.20.20/32	*	172.16.0.30/32	53	udp	Accepte
2	92.20.20.20/32	*	172.16.0.10/32	25	tcp	Accepte
3	92.20.20.20/32	*	172.16.0.10/32	110	tcp	Accepte
4	92.20.20.20/32	*	172.16.0.10/32	143	tcp	Accepte
5	92.20.20.20/32	*	172.16.0.30/32	389	tcp	Accepte
6	92.20.20.20/32	*	172.16.0.30/32	636	tcp	Accepte
7	92.20.20.20/32	*	172.16.0.30/32	3268	tcp	Accepte
8	92.20.20.20/32	*	172.16.0.30/32	88	tcp	Accepte
9	93.30.30.30/32	*	172.16.0.30/32	53	udp	Accepte
10	93.30.30.30/32	*	172.16.0.10/32	25	tcp	Accepte
11	93.30.30.30/32	*	172.16.0.10/32	110	tcp	Accepte
12	93.30.30.30/32	*	172.16.0.10/32	143	tcp	Accepte
13	93.30.30.30/32	*	172.16.0.30/32	389	tcp	Accepte
14	93.30.30.30/32	*	172.16.0.30/32	636	tcp	Accepte
15	93.30.30.30/32	*	172.16.0.30/32	3268	tcp	Accepte
16	93.30.30.30/32	*	172.16.0.30/32	88	tcp	Accepte
défaut	*	*	*	*	*	Refuse

**Nota :** Les règles de filtrage sont évaluées après les règles de redirection.

#### 1.4.4 Extrait du contenu du fichier « /etc/firewall/rules » du routeur R1

```
#!/bin/bash
iptables -F
iptables -t nat -F
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

iptables -t nat -A PREROUTING -i eth0 -p udp --dport 53 -j DNAT --to 172.16.0.30:53
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25 -j DNAT --to 172.16.0.10:25
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 110 -j DNAT --to 172.16.0.10:110
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 143 -j DNAT --to 172.16.0.10:143
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 389 -j DNAT --to 172.16.0.30:389
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 636 -j DNAT --to 172.16.0.30:636
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 3268 -j DNAT --to 172.16.0.30:3268
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 88 -j DNAT --to 172.16.0.30:88
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

iptables -A FORWARD -i eth0 -s 92.20.20.20/32 -d 192.16.0.30/32 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i eth0 -s 92.20.20.20/32 -d 192.16.0.10/32 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -i eth0 -s 92.20.20.20/32 -d 192.16.0.10/32 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -i eth0 -s 92.20.20.20/32 -d 192.16.0.10/32 -p tcp --dport 143 -j ACCEPT
iptables -A FORWARD -i eth0 -s 92.20.20.20/32 -d 192.16.0.30/32 -p tcp --dport 389 -j ACCEPT
iptables -A FORWARD -i eth0 -s 92.20.20.20/32 -d 192.16.0.30/32 -p tcp --dport 636 -j ACCEPT
iptables -A FORWARD -i eth0 -s 92.20.20.20/32 -d 192.16.0.30/32 -p tcp --dport 3268 -j ACCEPT
iptables -A FORWARD -i eth0 -s 92.20.20.20/32 -d 192.16.0.30/32 -p tcp --dport 88 -j ACCEPT
iptables -A FORWARD -i eth0 -s 93.30.30.30/32 -d 192.16.0.30/32 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i eth0 -s 93.30.30.30/32 -d 192.16.0.10/32 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -i eth0 -s 93.30.30.30/32 -d 192.16.0.10/32 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -i eth0 -s 93.30.30.30/32 -d 192.16.0.10/32 -p tcp --dport 143 -j ACCEPT
iptables -A FORWARD -i eth0 -s 93.30.30.30/32 -d 192.16.0.30/32 -p tcp --dport 389 -j ACCEPT
iptables -A FORWARD -i eth0 -s 93.30.30.30/32 -d 192.16.0.30/32 -p tcp --dport 636 -j ACCEPT
iptables -A FORWARD -i eth0 -s 93.30.30.30/32 -d 192.16.0.30/32 -p tcp --dport 3268 -j ACCEPT
iptables -A FORWARD -i eth0 -s 93.30.30.30/32 -d 192.16.0.30/32 -p tcp --dport 88 -j ACCEPT

iptables -A FORWARD -o eth0 -d 92.20.20.20/32 -j ACCEPT
iptables -A FORWARD -o eth0 -d 93.30.30.30/32 -j ACCEPT
```

## 1.5 Paramétrage du routeur R2

### 1.5.1 Table de routage du routeur R2

Réseau	Masque	Passerelle	Interface
172.16.32.0	255.255.240.0	-	172.16.0.1
92.20.20.0	255.255.255.0	-	92.20.20.20
0.0.0.0	0.0.0.0	Passerelle FAI	92.20.20.20

### 1.5.2 Table de DNAT du routeur R2

Interface d'arrivée	Adresse publique	Port public	Adresse privée de redirection	Port privé de redirection
eth0	92.20.20.20	53	172.16.32.10	53
eth0	92.20.20.20	389	172.16.32.10	389
eth0	92.20.20.20	636	172.16.32.10	636
eth0	92.20.20.20	3268	172.16.32.10	3268
eth0	92.20.20.20	88	172.16.32.10	88

### 1.5.3 Règles de filtrage du routeur R2

Ces règles s'appliquent en entrée de l'interface eth0 du routeur R2

No de règle	Adresse Source	Port source	Adresse Destination	Port Dest.	Protocole	Action
1	91.10.10.10/32	*	172.16.32.10/32	53	*	Accepte
2	91.10.10.10/32	*	172.16.32.10/32	389	*	Accepte
3	91.10.10.10/32	*	172.16.32.10/32	636	*	Accepte
4	91.10.10.10/32	*	172.16.32.10/32	3268	*	Accepte
5	91.10.10.10/32	*	172.16.32.10/32	88	*	Accepte
défaut	*	*	*	*	*	Refuse

**Nota** : Les règles de filtrage sont évaluées après les règles de redirection.

### 1.5.4 Contenu du fichier « /etc/firewall/rules » du routeur R2

```
#!/bin/bash
```

```
iptables -F
```

```
iptables -t nat -F
```

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

```
iptables -P FORWARD DROP
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p udp --dport 53 -j DNAT --to 172.16.32.10:53
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p tcp --dport 389 -j DNAT --to 172.16.32.10:389
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p tcp --dport 636 -j DNAT --to 172.16.32.10:636
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p tcp --dport 3268 -j DNAT --to 172.16.32.10:3268
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p tcp --dport 88 -j DNAT --to 172.16.32.10:88
```

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.32.10/32 -p udp --dport 53 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.32.10/32 -p tcp --dport 389 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.32.10/32 -p tcp --dport 636 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.32.10/32 -p tcp --dport 3268 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.32.10/32 -p tcp --dport 88 -j ACCEPT
```

```
iptables -A FORWARD -o eth0 -d 91.10.10.10/32 -j ACCEPT
```

## 1.6 Paramétrage du routeur R3

### 1.6.1 Table de routage du routeur R3

Réseau	Masque	Passerelle	Interface
172.16.48.0	255.255.240.0	-	172.16.0.1
93.30.30.0	255.255.255.0	-	93.30.30.30
0.0.0.0	0.0.0.0	Passerelle FAI	93.30.30.30

### 1.6.2 Table de DNAT du routeur R3

Interface d'arrivée	Adresse publique	Port public	Adresse privée de redirection	Port privé de redirection
eth0	93.30.30.30	53	172.16.48.10	53
eth0	93.30.30.30	389	172.16.48.10	389
eth0	93.30.30.30	636	172.16.48.10	636
eth0	93.30.30.30	3268	172.16.48.20	3268
eth0	93.30.30.30	88	172.16.48.10	88

### 1.6.3 Règles de filtrage du routeur R3

Ces règles s'appliquent en entrée de l'interface eth0 du routeur R3

No de règle	Adresse Source	Port source	Adresse Destination	Port Dest.	Protocole	Action
1	91.10.10.10/32	*	172.16.48.10/32	53	udp	Accepte
2	91.10.10.10/32	*	172.16.48.10/32	389	tcp	Accepte
3	91.10.10.10/32	*	172.16.48.10/32	636	tcp	Accepte
4	91.10.10.10/32	*	172.16.48.20/32	3268	tcp	Accepte
5	91.10.10.10/32	*	172.16.48.10/32	88	tcp	Accepte
défaut	*	*	*	*	*	Refuse

**Nota** : Les règles de filtrage sont évaluées après les règles de redirection.

### 1.6.4 Contenu du fichier « /etc/firewall/rules » du routeur R3

```
#!/bin/bash
```

```
iptables -F
```

```
iptables -t nat -F
```

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

```
iptables -P FORWARD DROP
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p udp --dport 53 -j DNAT --to 172.16.48.10:53
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p tcp --dport 389 -j DNAT --to 172.16.48.10:389
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p tcp --dport 636 -j DNAT --to 172.16.48.10:636
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p tcp --dport 3268 -j DNAT --to 172.16.48.10:3268
```

```
iptables -t nat -A PREROUTING -i eth0 -s 91.10.10.10/32 -p tcp --dport 88 -j DNAT --to 172.16.48.10:88
```

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.48.10/32 -p udp --dport 53 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.48.10/32 -p tcp --dport 389 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.48.10/32 -p tcp --dport 636 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.48.20/32 -p tcp --dport 3268 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -s 91.10.10.10/32 -d 192.16.48.10/32 -p tcp --dport 88 -j ACCEPT
```

```
iptables -A FORWARD -o eth0 -d 91.10.10.10/32 -j ACCEPT
```

## 1.7 Paramétrage du routeur RVPN

### 1.7.1 Table de routage du routeur Rvpn

Réseau	Masque	Passerelle	Interface
172.16.0.0	255.255.240.0	-	172.16.0.2
10.0.0.0	255.255.255.0	-	10.0.0.100
0.0.0.0	0.0.0.0	172.16.0.1	176.16.0.2

### 1.7.2 Table de filtrage du routeur Rvpn

Le routeur Rvpn ne contient pas de table de filtrage. Tous les échanges entre le VPN et le réseau de Paris sont autorisés dans les deux sens.

## 1.8 Paramétrage des serveurs du siège à Paris

### 1.8.1 Tables de routages des serveurs du réseau de Paris

#### SERVEUR MESSAGERIE

Réseau	Masque	Passerelle	Interface
172.16.0.0	255.255.240.0	-	172.16.0.10
0.0.0.0	0.0.0.0	172.16.0.1	176.16.0.10

#### SERVEUR BDD

Réseau	Masque	Passerelle	Interface
172.16.0.0	255.255.240.0	-	172.16.0.20
10.0.0.0	255.255.255.0	172.16.0.2	172.16.0.20
0.0.0.0	0.0.0.0	172.16.0.1	176.16.0.20

#### SERVEUR LDAP / DNS

Réseau	Masque	Passerelle	Interface
172.16.0.0	255.255.240.0	-	172.16.0.30
10.0.0.0	255.255.255.0	172.16.0.2	172.16.0.30
0.0.0.0	0.0.0.0	172.16.0.1	176.16.0.30

#### SERVEUR HTTP

Réseau	Masque	Passerelle	Interface
172.16.0.0	255.255.240.0	-	172.16.0.40
0.0.0.0	0.0.0.0	172.16.0.1	176.16.0.40

### 1.8.2 Table de filtrage des serveurs de Paris

Les serveurs de Paris ne contiennent pas de table de filtrage. Tous les échanges sont autorisés dans les deux sens.

## 1.9 Extrait de la liste des ports standardisés

La société Xoni utilise les ports et protocoles standardisés par l'ICANN (Well-Known-Ports). Voici un extrait de cette liste concernant notamment les ports utilisés au sein de Xoni.

Protocole/application	Port utilisé	Protocole
SSH	22	TCP
Telnet	23	TCP
SMTP	25	TCP
DNS	53	UDP
HTTP	80	TCP
KERBEROS (auth. LDAP)	88	TCP
POP3	110	TCP
IMAP	143	TCP
LDAP	389	TCP
HTTPS	443	TCP
LDAP over SSL	636	TCP
Global Catalog LDAP	3268	TCP

## **2 Dossier technique d'évolution du site de Dijon**

### **2.1 Résumé du rapport d'audit**

Ce rapport d'audit a été rédigé suite à la constitution d'un groupe de pilotage de l'informatique de production du site de Dijon, composé d'un membre de la Direction Générale de XONI, de représentants de la DSI (Direction des Services Informatiques) et des représentants de l'usine, pour la plupart cadres ou agents de maîtrise de chacun des ateliers.

Il en ressort que le site de Dijon est composé d'un ensemble administratif et de l'usine de production, elle-même subdivisée en 3 ateliers. Dans chaque atelier, il existe des ordinateurs spécifiquement dédiés à la production : réglage des fourneaux, vitesses d'écoulement de l'acier fondu, calage des filières, etc... Dans les ateliers 1 et 3, il existe aussi une vingtaine d'autres postes qui servent à la gestion de production : planification, enregistrement de la main d'œuvre, sorties de pièces, mesure de la production.

L'organisation actuelle du réseau est le résultat d'une mise en place réalisée au fur et à mesure que les besoins s'exprimaient mais sans aucun pilotage ni réflexion d'ensemble.

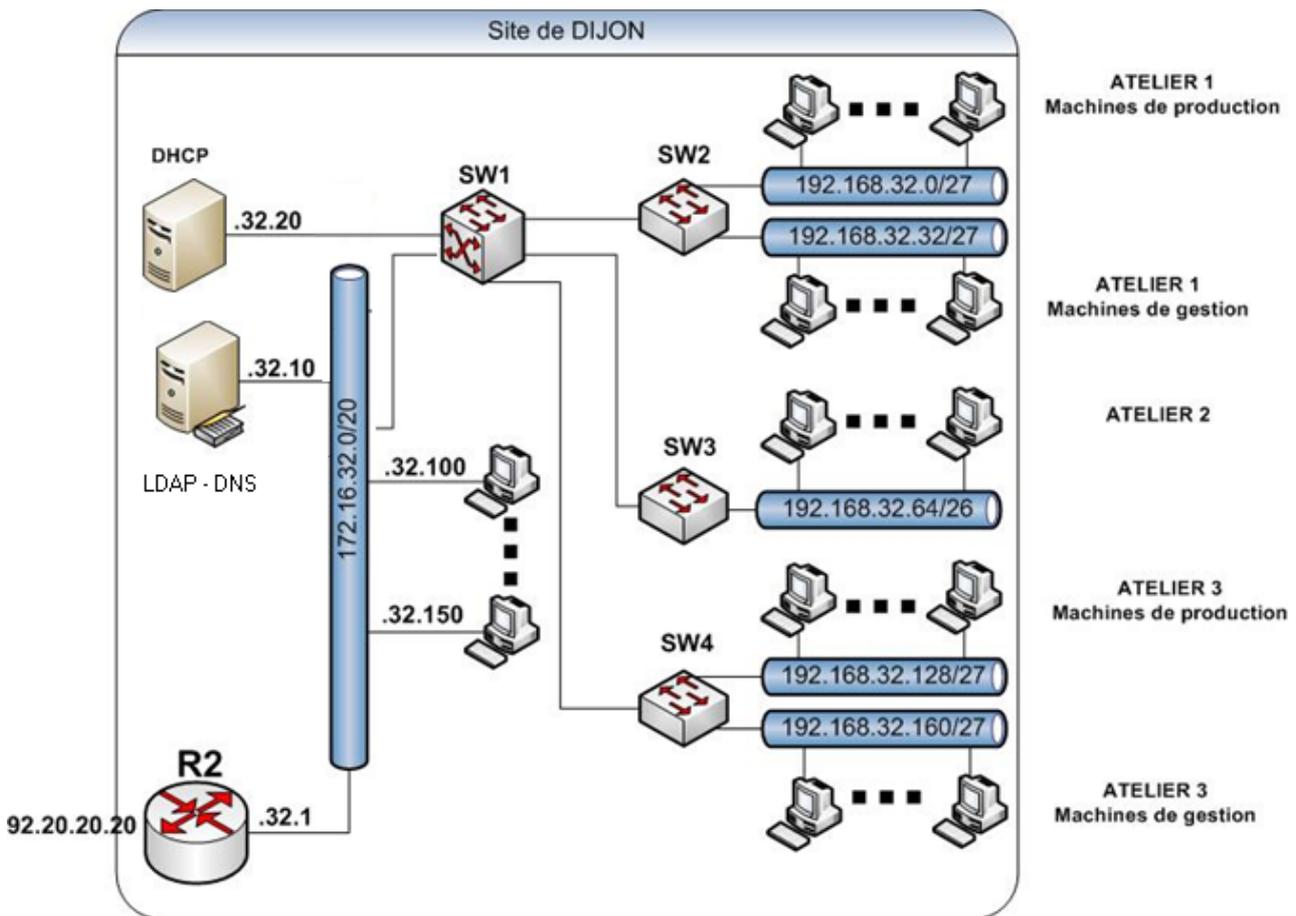
De nombreuses failles de sécurité ont été relevées, notamment :

- Les ateliers peuvent communiquer entre eux et échanger des données sans aucun contrôle. Des mélanges peuvent ainsi se produire dans les données de réglage de la production ou dans celles relatives à son contrôle ;
- N'importe quel ordinateur peut se connecter au réseau de production et récupérer ainsi n'importe quelle donnée sur l'ensemble du réseau ;
- Bien que soumise à une exigence de traçabilité et de sécurisation des données, en raison du caractère particulier des usages des produits fabriqués, la société XONI n'a pas mis en place de solution de sauvegarde des données de production.

En conséquence, ce rapport d'audit suggère comme interventions prioritaires :

- Améliorer la performance du réseau de production ;
- Améliorer la sécurité du réseau de production ;
- Mettre en place une solution de sauvegarde des données.

## 2.2 Architecture proposée pour le site de Dijon



Les postes du réseau administratif, ainsi que les serveurs de production ne sont pas concernés par ces modifications. Ils resteront raccordés au réseau administratif par les deux commutateurs non-manageables actuels.

Les adresses IPv4 seront fournies aux différents VLAN de manière dynamique par le serveur DHCP raccordé au commutateur SW1.

## 2.3 Segmentation prévue pour le site de Dijon

Le réseau de production sera découpé en 6 VLANS, numérotés de 2 à 7. Le réseau administratif, contenant les serveurs de DIJON, serait associé au VLAN 2.

Numéro de Vlan	Nom du vlan	Masque
1	Default (non utilisé)	255.0.0.0
2	Administration	255.255.240.0
3	Production-1	255.255.255.224
4	Gestion-1	255.255.255.224
5	Production-2	255.255.225.192
6	Production-3	255.255.255.224
7	Gestion-3	255.255.255.224

## 2.4 Procédures de contrôle d'accès envisagées pour le site de Dijon

Les différentes procédures envisagées de contrôle d'accès des postes sont les suivantes :

1. Règles de filtrage de niveau deux à partir des adresses MAC, à mettre en place sur les ports d'interconnexion des commutateurs, ou sur les ports d'accès aux serveurs ;
2. Règles de filtrage de type firewall sur le commutateur-routeur SW1, à partir des adresses IP ;
3. Contrôle d'accès basé sur les adresses MAC autorisées à se connecter sur chaque port, fixées manuellement par l'administrateur ;
4. Limitation du nombre d'hôtes (adresses MAC) qui peuvent accéder sur chaque port ;
5. Mise en place de VLAN privés qui peuvent interdire la communication entre certains ports d'un même VLAN ;

## 2.5 Affectation des ports sur le commutateurs SW1

Port	Périphérique connecté
1	R2
2	Serveur DHCP
3	SW2
4	SW3
5	SW4
6	Ancien switch1 48 ports réseau administratif
7	Ancien switch2 48 ports réseau administratif et serveurs
8	Non connecté
SUP 1	Non équipé
SUP 2	Non équipé

## 3 Documentation technique du matériel de Dijon

### 3.1 Extrait de la documentation relative à SW1

Le modèle SW1 est un commutateur 10/100/1000 à 8 ports entièrement géré avec 2 ports supplémentaires Gigabit double fonction pour une connectivité cuivre ou SFP. Associé à un routage statique et RIP IPv4, à des fonctions de gestion et de sécurité robustes et professionnelles, à une garantie gratuite à vie et à des mises à jour logicielles gratuites, le commutateur SW1 constitue une solution performante et économique.

#### Qualité de service (QoS)

- Options d'interfaces d'administration : Interface graphique utilisateur Web, Interface de ligne de commande (CLI), protocole SNMP (Simple Network Management Protocol) (SNMPv2c/SNMPv3) : permet d'administrer le commutateur à l'aide de différentes applications de gestion réseau tierces.
- Gestion de priorité de trafic (IEEE 802.1p) : permet de classer, en temps réel, le trafic en huit niveaux de priorité affectés à quatre files d'attente

#### Connecteurs

- LED sur panneau avant.
- Fonctionnalité de type double fonction : deux ports 10/100/1000 ou emplacements SFP pour offrir une connectivité fibre optique en option telle que Gigabit-SX, -LX, -LH, 100-FX, 100-BX et 1000-BX
- IEEE 802.3af PoE : offre jusqu'à 15,4 W par port pour alimenter des dispositifs PoE IEEE 802.3af, tels que téléphones IP, points d'accès sans fil et caméras de sécurité
- MDIX automatique : s'ajuste automatiquement aux câbles droits ou croisés sur tous les ports 10/100/1000
- Port console série RJ-45 : permet d'accéder facilement à l'interface du commutateur en façade de l'appareil

#### Tolérance de panne et haute disponibilité

- Multiple Spanning Tree IEEE 802.1s : offre une grande disponibilité des liens dans plusieurs environnements VLAN en autorisant l'utilisation de plusieurs arborescences; permet la prise en charge des protocoles d'ancienne génération IEEE 802.1d et IEEE 802.1w
- Jonction de port et agrégation de liaisons : Jonction : prend en charge jusqu'à huit liaisons par tronçon pour accroître la bande passante et créer des connexions redondantes ; Protocole LACP (Link Aggregation Control Protocol) IEEE 802.3ad : facilite la configuration des tronçons via la configuration automatique.

#### Commutation de couche 2

- Protocole d'enregistrement VLAN GARP : permet l'apprentissage automatique et l'affectation dynamique de VLAN
- Prise en charge et marquage de VLAN : prend en charge IEEE 802.1q
- Supporte 256 VLAN simultanément

#### Routage de couche 3

- Routage IP statique : permet la configuration manuelle du routage inter-vlan ;
- Protocole RIP (Routing Information Protocol) : assure le routage RIPv1 et RIPv2

#### Sécurité

- Listes de contrôle d'accès (LCA) : permet le filtrage de la couche IP 3 en fonction de l'adresse IP du sous-réseau source/destinataire et du numéro de port TCP/UDP source/destinataire

- ACL basé sur les identités : permet la mise en œuvre d'une stratégie de sécurité d'accès à forte granularité et l'affectation VLAN spécifique à chaque utilisateur authentifié du réseau
- Filtrage du port source : permet de spécifier les ports autorisés à communiquer avec les autres
- Contrôle d'accès 802.1x liés à un serveur RADIUS Externe.
- Protocoles de cryptage : Secure Shell (SSHv2): crypte toutes les données transmises pour un accès distant CLI sécurisé sur les réseaux IP. Secure Sockets Layer (SSL): crypte tout le trafic HTTP, permettant un accès sécurisé à l'interface de gestion web du switch. Secure FTP (SFTP): crypte l'envoi et la réception de fichiers de configuration

## 3.2 Extrait de la liste des commandes acceptées par SW1

### Syntaxe

- Les [valeurs entre crochets] doivent être remplacées par une valeur correspondant à la commande. Par exemple la commande :  

```
show vlan ports [port-number]
```

 peut être utilisée de la façon suivante :  

```
show vlan ports 3
```
- Chaque commande est écrite sur une seule ligne ;
- Les listes peuvent être précisées
  - Soit par un intervalle (1-5 → de 1 à 5 inclus)
  - Soit par des valeurs indépendantes (1,5 → 1 et 5)
  - Soit par une combinaison des deux formes : (1-3,8,12-14 → 1 2 3 8 12 13 et 14)

### Commandes

- **configure host-name [name]** → Set the switch name ;
- **configure max-vlans [number]** → Set the maximum number of VLANs on the switch ;
- **configure reset factory-default** → Set switch configuration with factory default parameters (clear all user configuration like a never used switch) ;
- **configure spanning-tree [enable or disable]** → Enable or Disable STP ;
- **configure vlan [vlan-id] name [vlan-name]** → Create vlan and set a name to vlan ;
- **configure vlan [vlan-id] tagged [list-ports-number]** → Assign tagged ports to vlan ;
- **configure vlan [vlan-id] untagged [list-ports-number]** → Assign untagged ports to vlan ;
- **show vlan [vlan-id]** → Show the vlan configuration ;
- **show vlan ports [port-number]** → Show VLANs that contains the port-number ;
- **show vlans** → Show the vlan list (number and name) ;

### **3.3 Extrait de la documentation relative à SW2/SW3/SW4**

Conformes aux normes 802.3af 802.3at, ces commutateurs peuvent fournir jusqu'à 30 Watts aux périphériques. Ils incluent différentes options de gestion, notamment SNMP, interface Web, et interface CLI compacte. Toute la gamme prend également en charge le filtrage des listes de contrôle d'accès.

Fonctions complètes de niveau 2

- Équipés de toutes les fonctionnalités d'un commutateur administrable de niveau 2, vous aurez tous les outils en main pour ajuster les performances de votre réseau. Les commutateurs offrent une surveillance IGMP, mise en miroir des ports, protocole STP (Spanning Tree) et protocole LLDP (Link Layer Discovery Protocol), ainsi que le contrôle de flux IEEE 802.3x. Prise en charge et marquage de VLAN : Prise en charge IEEE 802.1Q (4094 ID VLAN) et 256 VLAN simultanément. Auto-surveillance des VLAN. Intégration des fonctions d'agrégation de liens 802.3ad.

Renforcement de la sécurité

- Les commutateurs prennent également en charge l'authentification 802.1X basée sur les ports, ce qui permet d'authentifier le réseau avec un serveur RADIUS externe. La sécurité est renforcée par une liste de contrôle d'accès (liste des adresses MAC autorisées par port). Ces commutateurs incluent en outre une fonction de détection d'usurpation ARP qui protège le réseau Ethernet d'éventuelles attaques susceptibles d'entraîner la détection des trames de données, l'altération du trafic ou son interruption par l'envoi de faux messages ARP au réseau.

## 4 Réponse à l'appel d'offre

### 4.1 Données techniques

La nécessité d'une sauvegarde est renforcée par les nouvelles obligations de XONI en matière de traçabilité. Il a été étudié le principe d'une sauvegarde en mode hébergé de type « *As a Service* » afin de mieux estimer les coûts. Pour le personnel de la DSI, la charge de travail s'en trouvera allégée.

Les données de la base de production ont été estimées à 30 Go avec un accroissement en volume annuel de l'ordre de 5%.

### 4.2 Offres de solutions de sauvegarde en ligne

<i>Critères</i>	<i>Offre BeNeo</i>	<i>Offre Tecarch</i>
Tarification	60 € par mois pour un volume autorisé de 50 Go sauvegardés	500 € par an pour un volume autorisé de 20 Go sauvegardés, puis 10 € par an par Go supplémentaire
Disponibilité du service	24/24 heures, 7/7 jours, 365/365 jours	24/24 heures, 7/7 jours, 365/365 jours
Conditions techniques de l'hébergement	<ul style="list-style-type: none"> <li>• Deux centres d'hébergement Tier3 reliés par fibre optique</li> </ul> Caractéristiques : <ul style="list-style-type: none"> <li>• Norme ISO 9001</li> <li>• Sécurité d'accès physique 24x7x365 par du personnel présent sur site</li> <li>• Contrôle d'accès biométrique</li> <li>• Alimentation électrique, de grande capacité, stable et redondante</li> <li>• Double liaison télécoms et support de communication intégralement en fibre optique</li> <li>• Climatisations redondantes et protection anti-feu</li> </ul>	<ul style="list-style-type: none"> <li>• Un centre de pilotage surveille l'environnement</li> </ul>
Confidentialité	<ul style="list-style-type: none"> <li>• Cryptage des données</li> <li>• Serveurs virtuellement « privés » permettant une administration personnalisée</li> <li>• Rapport quotidien de sauvegarde par courriel</li> </ul>	<ul style="list-style-type: none"> <li>• Cryptage des données</li> <li>• Serveurs mutualisés</li> <li>• Rapport quotidien de sauvegarde par courriel</li> </ul>
Type de sauvegarde autorisée	<ul style="list-style-type: none"> <li>• <b>Totale</b> en début de période de sauvegarde, <b>différentielle</b> ensuite</li> <li>• Période de sauvegarde modulable de 5 à 20 jours</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Totale</b> en début de période de sauvegarde, <b>incrémentielle</b> ensuite</li> <li>• Période de sauvegarde hebdomadaire</li> </ul>
Restauration	<ul style="list-style-type: none"> <li>• Complète ou partielle ; accès à distance aux données sauvegardées, avant restauration</li> </ul>	<ul style="list-style-type: none"> <li>• Complète ou partielle ; accès à distance aux données sauvegardées avant restauration</li> </ul>

## 5 Extraits de Wikipédia « Les sauvegardes »

### 5.1 Méthodes (types) de sauvegarde les plus courantes

La méthode la plus simple est la **sauvegarde complète** ou totale (appelée aussi "full backup") ; elle consiste à copier toutes les données à sauvegarder que celles-ci soient récentes, anciennes, modifiées ou non.

Cette méthode est la plus fiable mais elle est longue et très coûteuse en termes d'espace disque, ce qui empêche de l'utiliser en pratique pour toutes les sauvegardes à effectuer. Afin de gagner en rapidité et en temps de sauvegarde, il existe des méthodes qui procèdent à la sauvegarde des seules données modifiées et/ou ajoutées entre deux sauvegardes totales. On en recense deux :

- La **sauvegarde différentielle**
- La **sauvegarde incrémentale**

### 5.2 Mécanisme

Pour pouvoir différencier ces différentes méthodes de sauvegarde (complète, incrémentielle, différentielle), le mécanisme mis en place est l'utilisation d'un marqueur d'archivage. Chaque fichier possède ce marqueur d'archivage, qui est positionné à "vrai" lorsque l'on crée ou modifie un fichier. On peut interpréter cette valeur comme "Je viens d'être modifié ou créé : je suis prêt à être archivé donc je positionne mon marqueur à vrai". Ce marqueur est appelé aussi attribut d'archivage (ou bit d'archivage).

### 5.3 Sauvegarde complète

Lors d'une sauvegarde complète, on va remettre à "0" l'attribut du fichier pour mémoriser le fait que le fichier a été enregistré.

Lors d'une sauvegarde complète, tous les fichiers sont sauvegardés, indépendamment de la position du marqueur (vrai ou faux). Une fois le fichier archivé, celui-ci se voit attribuer la position de son marqueur (le bit d'archive) à "faux" (ou à "0").

### 5.4 Sauvegarde différentielle

Lors d'une sauvegarde différentielle, tous les fichiers dont le marqueur est à "vrai" sont sauvegardés. Une fois le fichier archivé, celui-ci garde la position de son marqueur tel qu'il l'avait avant la sauvegarde.

La restauration faite à partir de ce type de sauvegarde nécessite la recopie sur disque de la dernière sauvegarde complète et de la sauvegarde différentielle la plus récente.

Si la restauration se porte, par exemple, sur un disque complet qui a été sauvegardé le jour J+4, on doit alors recopier sur disque la sauvegarde complète du jour J et la sauvegarde différentielle du jour J+4 afin d'avoir la dernière version des données.

### 5.5 Sauvegarde incrémentielle ou incrémentale

Lors d'une sauvegarde incrémentielle, tous les fichiers dont le marqueur est à "vrai" sont sauvegardés. Une fois le fichier archivé, celui-ci se voit attribuer la position de son marqueur à "faux". Par exemple, si une sauvegarde complète est réalisée le jour J. Le jour J+1, la sauvegarde incrémentielle est réalisée par référence au jour J. Le jour J+2, la sauvegarde incrémentielle est réalisée par référence au jour J+1. Et ainsi de suite.

Si la restauration se porte, par exemple, sur un disque complet qui a été sauvegardé le jour J+4, on doit alors recopier sur disque la sauvegarde du jour J et les sauvegardes incrémentielles des jours J+1, J+2, J+3 et J+4 afin d'obtenir la dernière version de la totalité des données.

## **6 Mails reçu par la DSI**

### **6.1 Mail1**

*Expéditeur : Directeur Usine Rouen*

*Destinataire : DSI*

*Objet : Impossibilité pour les nouveaux employés d'accéder à leur compte*

*Bonjour,*

*Un incident particulièrement gênant a été détecté lors de l'arrivée de 3 nouveaux salariés dans l'usine de Rouen. Conformément à la procédure habituelle ces nouveaux salariés ont été créés par le siège de la société, à Paris. Normalement, dans la demi-journée qui suit, ces salariés peuvent utiliser leur ordinateur à Rouen et se connecter au réseau grâce à leur compte fraîchement créé. Cela n'a pas été le cas cette fois : Deux jours après, ils ne peuvent toujours pas se connecter !*

*J'ai contacté mon homologue sur le site de Dijon où des embauches similaires ont eu lieu le même jour. Les employés de Dijon ont pu, eux, se connecter sans difficultés environ une heure après la demande de création de leur compte.*

*Il est à noter qu'il n'y a pas eu de nouveaux utilisateurs au site de Rouen depuis longtemps et que le problème est peut-être donc très ancien.*

*Espérant une solution rapide.*

*Cordialement*

*Victor Pille*

*Directeur – Usine de Rouen*

### **6.2 Mail2**

*Expéditeur : Direction commerciale*

*Destinataire : DSI*

*Objet : Dysfonctionnement dans le VPN*

*Bonjour,*

*Plusieurs incidents de même nature m'ont été signalés par nos commerciaux : Lorsqu'ils sont en déplacement à l'extérieur de l'entreprise, ils se connectent bien à leur compte et peuvent récupérer ou stocker des fichiers sur le serveur, par contre ils n'ont pas accès à leur compte de messagerie ni, semble-t-il, au serveur web.*

*D'autre part un des commerciaux, M. Jean Sérien, c'est fait voler son portable ce matin. Merci de lui en préparer un nouveau dans les plus brefs délais et de le faire porter par la navette interne de l'entreprise. Le portable volé était repéré P-COM-027.*

*Espérant une solution rapide à ces deux problèmes.*

*Cordialement*

*Bruno Future*

*Directeur commercial*