31 Avenue Maurice Berteaux 78300 Poissy

https://www.h3campus.fr/campus/poissy

Téléphone. 01 30 06 33 06

Epreuve E5

« Conception et maintenance de solutions informatiques»

Dossier technique de l'infrastructure du réseau M2L

Session 2021

V06062021

Introduction :

Les Projets Personnels Encadrés (PPE) ont été développés autour d'un contexte qui est la Maison des Ligues de Lorraine (M2L). Cet environnement a permis à l'étudiant de réaliser un ensemble de projets autour de différentes situations professionnelles (les missions) et acquérir ainsi les compétences en conformité avec le référentiel.

Rappel du contexte :

La Maison des Ligues de Lorraine (M2L) a pour mission de fournir des espaces d'hébergement et des services aux différentes ligues sportives régionales et à d'autres structures hébergées. La M2L est une structure financée par le Conseil Régional de Lorraine dont l'administration est déléguée au Comité Régional Olympique et Sportif de Lorraine (CROSL).

Pour fournir ses prestations de service, la M2L s'appuie sur un réseau et une infrastructure informatique qui couvre un ensemble de besoins répondant ainsi au cahier des charges de la région et aux exigences de ses clients, les ligues.

L'infrastructure informatique et réseau est prise en charge par le service informatique de la M2L qui se charge de l'exploitation de l'ensemble des équipements du parc ainsi que de la réalisation des projets informatiques.

Présentation Générale de l'infrastructure :

L'infrastructure (schéma Annexe 1) est découpée en 3 parties comprenant le réseau de l'association M2L et ses services, le réseau des ligues et le réseau d'accès à Internet. La M2L est responsable de l'administration de l'infrastructure, de la fourniture de services à ses clients, les ligues sportives, et de la sécurisation des données et des opérations de l'administration plus généralement de son système d'information.

L'infrastructure générale est hébergée dans le domaine m2l.lan. Un serveur d'annuaire et contrôleur de domaine Active Directory assure la gestion et l'administration du réseau.

L'Infrastructure système

L'infrastructure comporte plusieurs périmètres de sécurité. Les services de la M2L et les ligues sont organisés en Unités d'organisation dans un environnement réglementé par le système de gestion d'annuaire Active Directory.

Le système d'information comprend les serveurs chargés de gérer les services internes (Active Directory, Services de stockage, sauvegarde, fichiers, gestion de parc, supervision réseau, etc.) et les services externes (site Web, Ftp, etc). L'ensemble de ces serveurs sont virtualisés dans des machines en baie (ProxMox pour la plupart) dans la salle informatique.

Les serveurs physiques se trouvent donc dans le sous réseau INFORMATIQUE du réseau de la M2L. La virtualisation est assurée par KVM avec ProxMox. Les serveurs virtualisés sont des serveurs Windows Server 2019, Debian 11, un serveur EON/Nagios, ainsi qu'un client virtuel Windows 10 et une machine Kali Linux.

La description technique de chaque serveur est donnée en annexe.

L'Infrastructure réseau

La structure générale du réseau comprend :

- Les sous réseaux de l'association M2L
- Les sous réseaux des ligues
- La DMZ
- Le réseau d'accès à Internet

Le réseau M2L héberge tous les serveurs dans un réseau composé du sous réseau Informatique et la DMZ. Les serveurs hébergent les applications (base de données, WEB, Sauvegarde etc…), les services réseau et les services de gestion et de supervision du parc informatique.

Plan d'adressage IP

Le réseau général est construit autour de l'adresse 172.16.0.0 avec un masque de 19 bits. Ceci permet de couvrir l'ensemble du plan d'adressage de l'association pour les ligues, M2L mais aussi pour les évolutions. L'administrateur a réservé un masque de 26 bits par sous réseau. Les sous réseaux couvrent les départements de M2L et les ligues. Le plan d'adressage IP 192.168.16.0 /28 est attribué à la DMZ. Les services et les ligues sont liés à un sous réseau VLAN 172.16.x.0 où x=N° Vlan.

Les tableaux en Annexe décrivent le plan d'adressage IP de l'ensemble du réseau. Ce plan d'adressage tient compte d'une exploitation des adresses IP en mode dynamique par 2 serveurs DHCP en redondance chaude.

Un bloc d'adresse est réservé pour les équipements en adressage fixe et ceci pour chaque sous réseau. Des règles d'ingénierie ont été définies plaçant les plages d'adresse fixe sur les adresses les plus hautes de chaque sous réseau.

Ce tableau est présenté à l'ANNEXE 2.

Les éléments du réseau

Ce réseau regroupe les fonctions suivantes :

- Les VLAN sont identifiés dans le plan d'adressage IP par le troisième octet qui prend pour valeur le N° du VLAN, ainsi le service INFORMATIQUE est placé à l'adresse 172.16.2.0 /26 qui représente le VLAN 2 ou encore le VLAN de la ligue de Tennis (VLAN 10) 172.16.10.0 /26.

- Le routage des VLAN est assuré par 1 routeur (RM2L).

- Les serveurs DHCP et serveur de nom DNS assurent la gestion des machines, il n'y a pas de délégations DNS. Le service DHCP 1 (Windows) cohabite avec le serveur-contrôleur de domaine hébergeant l'annuaire Active Directory.

Infrastructure M2L

L'association M2L comporte plusieurs départements (VLAN) dont le service INFORMATIQUE. Ce service assure la gestion et l'administration du réseau et du parc informatique.
Les ressources informatiques (serveurs, bases de données, systèmes de supervision…) sont situées dans une baie de serveurs.
Parmi ces serveurs on trouve le serveur DHCP, serveur d'annuaire, serveur de déploiement WDS, serveur de déploiement d'applications RDS, RDP, le serveur Proxy qui se charge des requêtes http des personnels des ligues et M2L.

Nota : La maquette n'intègre que les 2 premiers VLAN de l'association M2L (Vlan informatique et administratif) et les 3 premières ligues (Tennis, Basket et Athlétisme).

Infrastructure des ligues

Chaque ligue est intégrée à un sous réseau dans un VLAN. Le plan d'adressage des ligues est donné dans le tableau Annexe 1.

La maquette comprend les ligues Tennis, Athlétisme et Basket avec 1 poste informatique par ligue au titre de poste client. Les postes clients utilisent les services des serveurs installés dans le sous réseau informatique.

Ces ligues sont réparties sur des commutateurs d'accès. Un commutateur de distribution assure le lien entre les commutateurs d'accès et le reste du réseau. Les commutateurs d'accès sont reliés au commutateur de distribution configurés en STP. Cette structure de réseau de commutateurs à chemin redondant garantit la continuité du service sur la transmission des données par les 3 commutateurs connectés en boucle. Le spanning-tree (STP) a été configuré pour privilégier le trafic sur les liaisons Etherchannel en phase opérationnelle (haute disponibilité).

Accès Internet et DMZ

Cette partie représente le périmètre de sécurité pour l'accès à Internet. Une zone DMZ est présente dans le réseau M2L qui réglemente les échanges et l'accès à Internet. La DMZ est connecté à un switch (switch SWDMZ) qui est relié par le switch SW1Ligue au routeur. Ce dernier assure la gestion des sous réseaux dont la DMZ qui renferme les services WEB et FTP, ainsi l'interconnexion au réseau privé et Internet.

Les 2 services FTP et WEB de la DMZ sont intégrés dans une machine physique Debian 11. Cela a pour but d'héberger le site WEB de M2L et des ligues et le serveur de téléchargement. Ces services sont accessibles depuis l'Internet et le réseau interne sous certaines conditions.

Règles de contrôle d'accès :

1/ Les postes clients du réseau privé ne peuvent accéder à Internet que par le serveur Proxy.
2/ Les internautes peuvent accéder à la DMZ mais pas au réseau privé.
3/ Les sous réseaux M2L et ligues peuvent accéder aux ressources de la DMZ.
4/ Le trafic ICMP est autorisé pour les postes fixes du service Informatique.
5/ Le trafic ICMP provenant de l'Internet est interdit.

Gestion de Parc informatique

La gestion de parc informatique est réalisée par l'application GLPI associée à l'outil d'inventaire Fusion Inventory.

Une synchronisation LDAP permet de remonter les utilisateurs de l'AD dans GLPI. La machine qui héberge ce service est sous Debian 11.

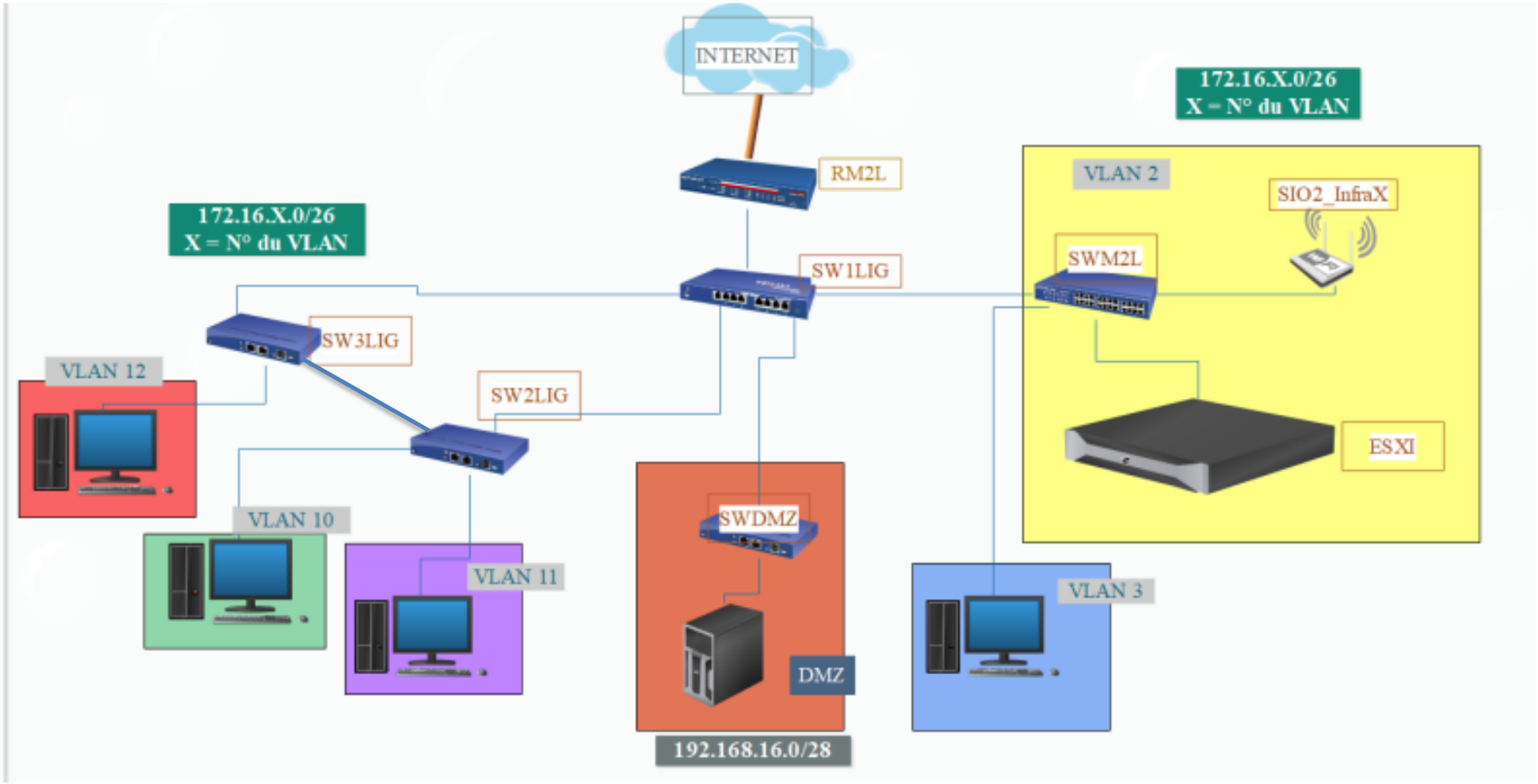
Supervision de réseau, Maintenance

En cas de panne l'analyse de problème réseau s'effectue via l'outil d'analyse de trame Wireshark qui permettra de vérifier les anomalies de fonctionnement du réseau pour la validation, les tests ou la mise en service mais aussi le dépannage de situation en cas de blocage.

Les équipements de réseau sont accessibles en SNMP pour permettre l'exploitation du réseau par le superviseur NAGIOS sous la distribution Eyes Of Network (distribution CENTOS). On utilise la communauté ¨M2L¨ pour les relations agent/serveur avec les droits en lecture. On utilisera les Traps ou notifications SNMP définies par Cisco pour surveiller les équipements Switch et routeurs, les ruptures de liens et les pannes et redémarrages des équipements.

Le superviseur NAGIOS/EON assure principalement la supervision des équipements de réseau (commutateurs, routeurs, passerelles, Points d'accès) mais aussi celle des postes via le service SNMP. L'outil de gestion de parc et gestion d'incidents Fusion Inventory permet d'assurer la gestion des postes et serveurs informatiques, la gestion des demandes et des incidents, Gestion des changements et des projets.

ANNEXE 1 - SCHÉMA DE L'INFRASTRUCTURE



ANNEXE 2 - Plan d'adressage IP

VLAN M2L	VLAN 2 - INFORMATIQUE	VLAN 3 - ADMINISTRATIF	VLAN 20 - DMZ
Masque	255.255.255.192	255.255.255.192	255.255.255.240
Adresse du réseau	172.16.2.0	172.16.3.0	192.168.16.0
Adresse de diffusion	172.16.2.63	172.16.3.63	192.168.16.15
Plage d'adresses DHCP 1	172.16.2.1-25	172.16.3.1-25	
Plage d'adresses DHCP 2	172.16.2.26-50	172.16.3.26-50	
Plage fixe	172.16.2.51-62	172.16.3.51-62	
Serveurs DHCP1 Serveur DHCP 2 Borne WIFI	172.16.2.61 172.16.2.60 172.16.2.35		
Passerelle	172.16.2.62	172.16.3.62	192.168.16.14

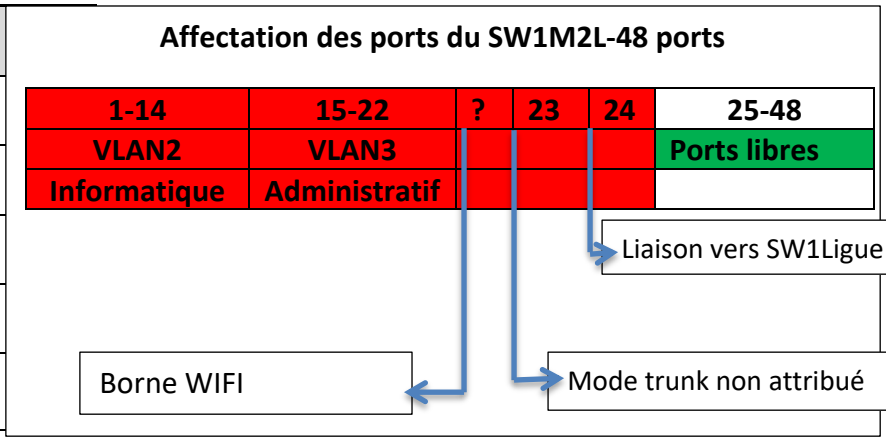
VLAN LIGUES	VLAN 10 - TENNIS	VLAN 11 - ATHLE	VLAN 12 - BASKET
Masque	255.255.255.192	255.255.255.192	255.255.255.192
Adresse du réseau	172.16.10.0	172.16.11.0	172.16.12.0
Adresse de diffusion	172.16.10.63	172.16.11.63	172.16.12.63
Plage d'adresses DHCP 1	172.16.10.1-25	172.16.11.1-25	172.16.12.1-25
Plage d'adresses DHCP 2	172.16.10.26-50	172.16.11.26-50	172.16.12.26-50
Plage fixe	172.16.10.51-62	172.16.11.51-62	172.16.12.51-62
Passerelle	172.16.10.62	172.16.11.62	172.16.12.62

Table de noms DNS

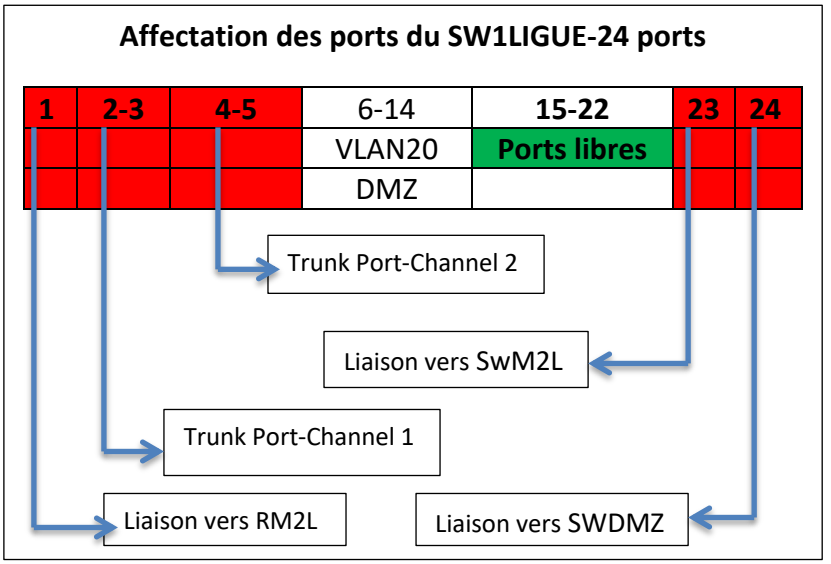
Équipement	Nom	Adresse IP
Serveur DNS	Srv-ad-dhcp1-dns	172.16.2.61
Serveur Web	web	http://192.168.16.1
Serveur FTP	ftp	ftp://192.168.16.1
Serveur RDS	rds	172.16.2.58

ANNEXE 3 - PLAN DE BRASSAGE

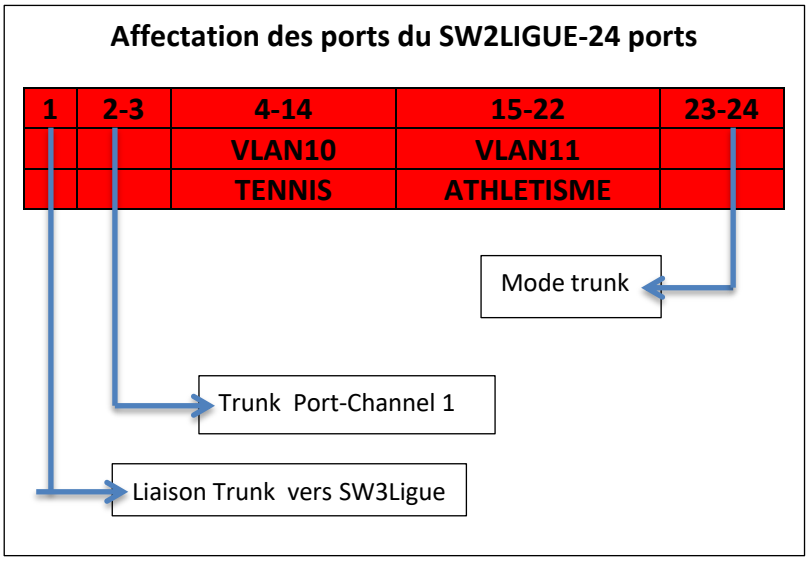
SWM2L (C2950)	Ports
VLAN 2 (INFO)	Ports 1 à 14
VLAN 3 (ADMIN)	Ports 15 à 22
Mode trunk non attribué	Port 23
Liaison vers SW1Ligue	Port 24
Borne WIFI	Port



SW1LIGUE 2960/2950	Ports
Liaison vers RM2L	Port 1
Trunk Port-Channel 1	Ports 2 et 3
Trunk Port-Channel 2	Ports 4 et 5
VLAN 20 (DMZ)	Ports 6 à 14
Non attribué	Ports 15 à 22
Liaison vers SwM2L	Port 23
Liaison vers SWDMZ	Port 24

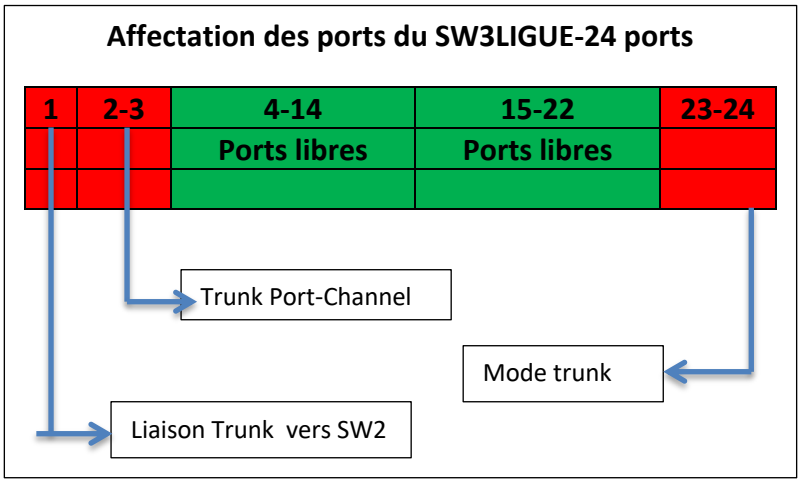


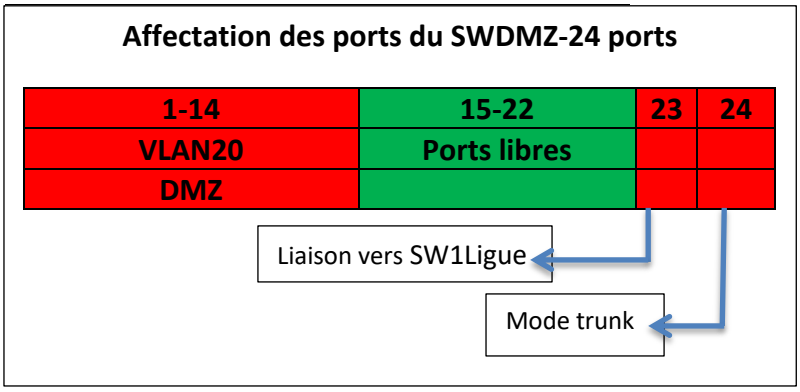
SW2LIGUE (C2950-24/48TT)	Ports
Liaison Trunk vers SW3Ligue	Port 1
Trunk Port-Channel 1	Ports 2 et 3
VLAN 10 (Tennis)	Ports 4 à 14
VLAN 11 (Athlétisme)	Ports 15 à 22
Mode trunk	Ports 23-24



ANNEXE 3 - SUITE PLAN DE BRASSAGE

SW3LIGUE (C2950-24/48TT)	Ports
Liaison Trunk vers SW2	Port 1
Trunk Port-Channel 2	Ports 2 et 3
VLAN 12 (Basket)	Ports 4 à 14
Non attribué	Ports 15 à 22
Mode trunk	Ports 23 - 24





ANNEXE 4 - IDENTIFIANTS & MOTS DE PASSES

Equipement	Adresse IP	Masque	Identifiant	Mot de passe
PROXMOX	172.16.2.51	255.255.255.192	root	BtsSIO2022
Serveur AD-DHCP1-DNS	172.16.2.61	255.255.255.192	Administrateur	123AZEqsd
Serveur RDS-WDS	172.16.2.58	255.255.255.192	Administrateur	123AZEqsd
Serveur DHCP2 (Debian)	172.16.2.60	255.255.255.192	bts | root	Bts | root
Serveur EON Nagios	172.16.2.57	255.255.255.192	root	123AZEqsd
Serveur Debian GLPI	172.16.2.56	255.255.255.192	Serveur : Bts GLPI : glpi	Root glpi
Borne Wifi	172.16.2.35	255.255.255.192	SSID :WIFI_INFRA2	admin Btssio78!
NAS	/	/	/	/
Client virtuel	IP dynamique	255.255.255.192	Administrateur	Btssio78!
Machine hôte DMZ	192.168.16.1	255.255.255.240	dmz	dmz
Serveur Web	192.168.16.1	255.255.255.240	web	web
Serveur FTP	192.168.16.1	255.255.255.240	ftp	ftp
Serveur PROXY	172.16.2.59	255.255.255.192	squid	squid
Client du domaine	Ip dynamique	255.255.255.192	bts / Administrateur	Btssio78!
SWM2L (ssh)	172.16.2.52	255.255.255.192	cisco	cisco
SW1LIG (ssh)	172.16.2.53	255.255.255.192	cisco	cisco
SW2LIG (telnet)	172.16.2.54	255.255.255.192	cisco	cisco
SW3LIG (telnet)	172.16.2.55	255.255.255.192	cisco	cisco
SWDMZ (telnet)	192.168.16.13	255.255.255.140	cisco	cisco
RM2L (ssh)	172.16.2.62	/	cisco	cisco

* Pour les postes intégrés au domaine on peut utiliser un compte présent dans l'Active Directory.
* Accès root des VM Linux : root|root
* Mdp VTP : cisco123

ANNEXE 5 - PLAN DE LA BAIE