



Contexte TiersLieux

TiersLieux, est une association régionale qui gère des Espaces de Travail Partagés (ETP) mis à disposition par des communes auprès de leurs administrés (entreprises et particuliers). Pour installer, déployer et administrer l'infrastructure informatique des espaces gérés par *TiersLieux*, elle fait appel à des sociétés d'infogérance prestataires de services qui répondent à des appels d'offres.

L'Espace de Travail Partagé

L'Espace de Travail Partagé (ETP) tel que défini par *TiersLieux*, a pour vocation d'accueillir les indépendants, les télétravailleurs, les TPE et les jeunes pousses dans un même lieu tout en favorisant la communication et la convivialité entre les résidents. Il s'agit également de créer des synergies permettant à chacun de gagner en efficacité, en performance et en qualité de vie. L'ETP s'appuie sur des solutions numériques qui permettent d'offrir un outil moderne, performant et d'une grande souplesse d'utilisation. Les réservations des espaces de bureau modulaires s'effectuent en ligne grâce à un portail numérique sécurisé offrant la possibilité au résident de choisir son emplacement de travail via son ordinateur ou son téléphone portable. Les entreprises peuvent louer au mois des bureaux fermés pouvant accueillir 4 personnes maximum. Les résidents disposent également du Wi-Fi haut débit sécurisé pour l'accès à Internet et à leurs ressources partagées, d'un accès personnalisé et sécurisé à la photocopieuse et, pour ceux qui le souhaitent, d'une place de stationnement dans un parking sécurisé. Chaque ETP est accessible et fonctionnel 24/24 heures et 7/7 jours grâce à la sécurisation et l'automatisation des accès via un pass numérique. Enfin, des conseils et des formations, dispensés par des spécialistes, sont régulièrement proposés aux résidents selon leurs besoins.

Projet ETP

Le projet **ETP** permet à *TiersLieux* de proposer à ses résidents (individuels ou entreprises) un ensemble de services identiques sur chaque site :

- Les espaces loués (salles et bureaux) sont tous reliés avec la salle « serveur ».
- Chaque résident dispose d'un compte d'utilisateur sur le domaine Active Directory de l'ETP.
- Les salles de réunion ont une capacité de 12 personnes avec accès Wi-Fi à Internet et au réseau local pour les utilisateurs authentifiés sur le domaine.
- Un service d'annuaire Active Directory permet à tous les résidents d'un ETP, les employés et responsables de se connecter aux services proposés par *TiersLieux* ;
- Un site WEB (portail internet accessible en ligne) permet la réservation de services et l'accès aux ressources pour les résidents et une présentation des services proposés par *TiersLieux* ;
- Un tableau de bord proposant de visualiser un ensemble de statistiques à l'attention des dirigeants et des décideurs ;
- Les sauvegardes et les fichiers de données (base de données comprise) seront stockés sur place pour des raisons d'efficacité.
- Des formations au numérique en ligne et en présentiel dispensées par des entreprises locales sous-traitantes.
- Les formations en présentiel se déroulent dans la salle libre-service située dans l'ETP. Chaque salle libre-service est équipée de 16 postes « stagiaires », 1 poste « formateur », une imprimante et un commutateur.

Toute l'organisation repose sur un portail web. Avec leur téléphone ou une tablette, les résidents font leur réservation d'espace et de ressources, choisissent leur emplacement et un QR code leur est délivré pour accéder à l'Espace de Travail Partagé 7j/7, 24h/24.

Description des locaux

Chaque bâtiment possède une « salle serveurs » située dans un local technique sécurisé, une ou deux salles de réunion équipées d'un écran multifonctions (dont la vidéoconférence), une salle libre-service, un espace détente-caféteria, des bureaux fermés et des espaces modulables de type bureau dans un plateau open space pour les résidents. Chaque résident peut louer des modules permettant d'accueillir de 1 à 4 personnes selon l'espace demandé (1 espace=1 personne=1bureau, 1 prise réseau, 1 prise ToIP, 4 prises électriques).

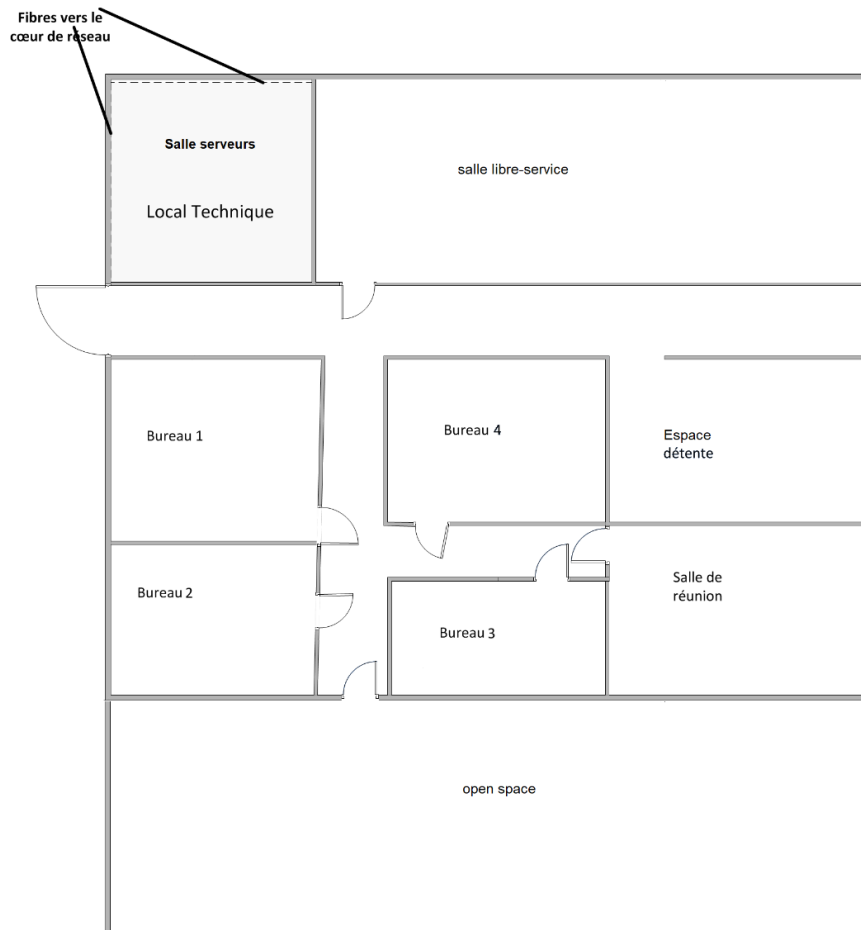
Les bureaux fermés permettent d'accueillir les jeunes pousses et les TPE de 4 personnes maximum (6 prises réseaux) avec équipement informatique fixe ou portable, 1 poste téléphonique, 1 imprimante.

Les locaux de l'ETP



Schéma des locaux de l'ETP

Le schéma ci-après présente l'étage qui abritera le nouvel Espace de Travail Partagé à implanter.



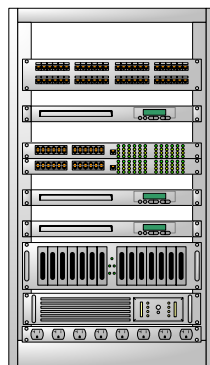
Équipement informatique et de sécurité des locaux

Le réseau informatique est basé sur un protocole unique : TCP/IP v4. Le réseau local utilise une technologie Ethernet commuté à 1Gb/s pour la connexion des solutions techniques d'accès et à 10Gb/s pour les liaisons inter-commutateurs et serveurs. Les accès à Internet et au réseau de l'ETP sont également possibles par connexion Wi-Fi sécurisée depuis tous les espaces. Les accès au réseau via une connexion Wi-Fi sont possibles pour les TPE avec un SSID et un VLAN dédié à chaque entreprise.

La salle serveur est équipée du matériel suivant :

- Accès sécurisé par code et empreinte digitale
- Sondes de température et d'humidité
- Système d'extinction automatique de feu par gaz inertes
- Onduleur de 10 à 40 KVA et groupe électrogène de secours sur les sites de plus de 100 personnes
- Câblage des rocade en fibre optique entre les répartiteurs des salles et la salle serveur
- Une armoire de brassage 42 U
- Deux serveurs physiques qui hébergent des serveurs virtualisés en cluster
- Une baie SAN avec 10 disques de 2 To en RAID5 pour le stockage des données
- Deux commutateurs cœur de réseau de niveau 3, 24 ports, stackés
- Un routeur pare-feu WAN
- Une ligne Internet professionnelle via la fibre optique.

Baie de Brassage LT



- Tableaux de connexion
- Routeur-parefeu-WAN
- SW-CORE1
- SW-CORE2
- SRV-ESX1
- SRV-ESX2
- SAN-RAID5
- Onduleur

Schéma de la baie de brassage du local technique

Pour chaque salle libre-service :

- Câblage de la rocade fibre entre la salle et la salle serveur
- Câblage de 20 prises réseaux murales
- Un onduleur 1500 VA
- Une armoire de brassage 12 U
- Un commutateur de périphérie, 24 ports
- Une borne Wi-Fi 802.11ac avec authentification WPA2
- Un photocopieur multi-fonctions

Pour chaque salle de réunion et l'espace détente :

- Câblage de 12 prises réseaux murales reliées à l'open space
- Une borne Wi-Fi 802.11ac avec authentification WPA2
- Une imprimante

Pour l'open space :

- Câblage de la rocade fibre entre l'open space et la salle serveur
- Câblage de 24 (ou 48) prises réseaux murales
- Un onduleur 1500 VA
- Une armoire de brassage 12 U
- Plusieurs commutateurs de périphérie, 24 ports
- Une borne Wi-Fi 802.11ac avec authentification WPA2
- Un photocopieur multi-fonctions
- Une imprimante 3D

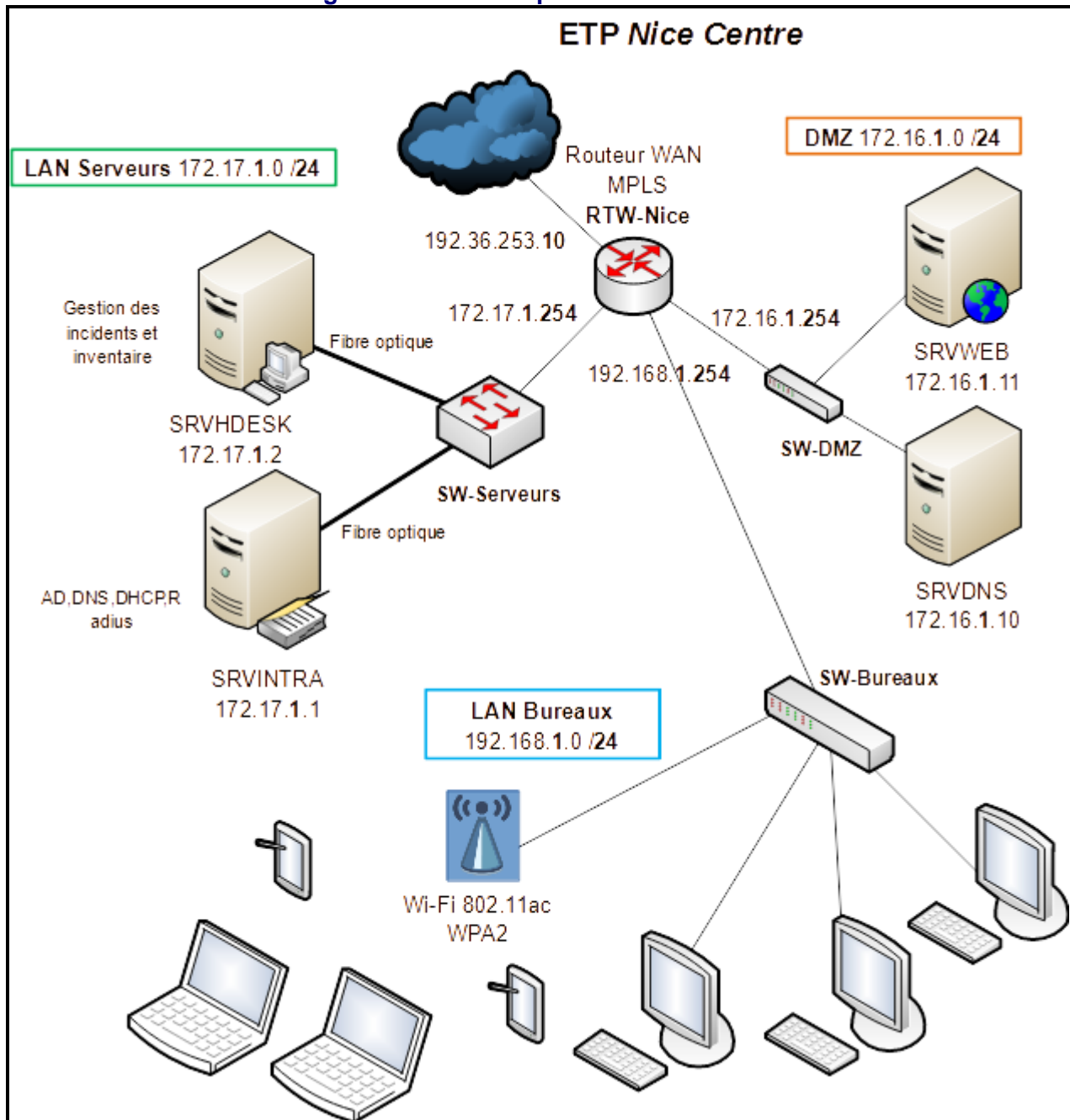
Pour chaque bureau fermé :

- Câblage de 10 prises réseaux murales reliées à l'open space
- Accès en Wi-Fi

Un système de Climatisation réversible et régulée est installé dans chaque salle/bureau.

Infrastructure réseau d'un ETP et accès à Internet

Tous les ETP ont une configuration similaire pour l'accès au réseau et à l'internet



Adresses de sous-réseaux	Adresses IP du routeur WAN
<p>Réseau interne : 192.168.v.0 /24 Passerelle par défaut : 192.168.v.254 ID Vlan réseau interne : v01 DMZ : 172.16.v.0 /24 Passerelle par défaut : 172.16.v.254 Avec v : ville (1 à 250) ID Vlan DMZ : v09 Réseau serveurs : 172.17.v.0 /24 Passerelle par défaut : 172.17.v.254 ID Vlan Serveur : v00 ID Vlan administration : v99</p>	<p>Nom : RTW-VILLE Interne : 192.168.v.254 DMZ : 172.16.v.254 Serveurs : 172.17.v.254 Externe (Out) : 192.36.253.v0</p>

Les VLAN v02 à v08 sont libres en fonction des besoins de chaque ETP	
Nom domaine AD : TiersLieux <i>dd</i> -VILLE Nom FQDN : <i>local.ville.tierslieuxdd.fr</i> Avec <i>dd</i> : numéro département	Plage d'adresses IP pour le réseau filaire : de 192.168.v.10 à 192.168.v.99 Plage d'adresses IP pour le réseau Wi-Fi : de 192.168.v.100 à 192.168.v.250 Passerelle par défaut : 192.168.v.254 DNS interne : 172.17.v.1 DNS externe : 172.16.v.10
Domaine DNS	
Domaine DNS siège : tierslieux <i>dd</i> .fr Domaine DNS agence : <i>ville.tierslieuxdd.fr</i>	DNS : 192.36.253.1 (siège) DNS : 172.16.v.10

Serveurs	Adresse IP interne	Adresse IP publique	Nom FQDN
Serveur interne Rôles : AD, DNS, DHCP, Radius	172.17.v.1	N	SRVINTRA. <i>ville.tierslieuxdd.fr</i>
Serveur gestion d'incident et inventaire	172.17.v.2	N	SRVHDESK. <i>ville.tierslieuxdd.fr</i>
Serveur DNS	172.16.v.10	192.36.253.v0	dns. <i>ville.tierslieuxdd.fr</i>
Serveur Web	172.16.v.11	192.36.253.v1	www. <i>ville.tierslieuxdd.fr</i>

Parmi les services offerts aux résidents, une solution logicielle de gestion d'incidents intégrée au portail web permet aux utilisateurs de créer des tickets de demande ou d'incidents.

Pour l'hébergement des entreprises ou la configuration ponctuelle d'un réseau pour l'organisation de réunions pour ses clients, TiersLieux a prévu l'utilisation de VLAN et de sous-réseaux séparés, selon la planification ci-dessous.

N° VLAN	VLAN	Service(s)	Adressage IP
vENT à v49	ENT- <i>n</i>	VLAN dédié à l'entreprise ENT (v11<ENT<v49)	172.20.1ent.0/24
vREU à v98	REU- <i>n</i>	VLAN dédié à l'événement REU (v51< REU <98)	172.20.2reu.0/24

Cette organisation permet de garantir à chaque entreprise hébergée une sécurité de leur réseau, tout en autorisant l'utilisation de moyens partagés comme la connexion internet et l'accès aux serveurs mutualisés (AD, DNS ou DHCP), grâce à des règles de filtrage définies sur le commutateur cœur de réseau (ACL Cisco) qui gèrera le routage inter-Vlan.

L'authentification des employés des « entreprises » se fera au moyen d'une authentification sur le domaine ville.etpdd.fr où sera définie une unité organisationnelle par entreprise résidente.

Exemple pour l'ETP de Nice

Adresses de sous-réseaux	DHCP	Adresses IP du routeur WAN & parefeu
Réseau interne : 192.168.1.0 /24 Passerelle : 192.168.1.254 DMZ : 172.16.1.0 /24 Passerelle : 172.16.1.254 Réseau serveurs : 172.17.1.0 /24 Passerelle par défaut : 172.17.1.254	Plage d'adresses IP pour le réseau filaire : de 192.168.1.10 à 192.168.1.99 Plage d'adresses IP pour le réseau Wi-Fi : de 192.168.1.100 à 192.168.1.250 Passerelle par défaut : 192.168.1.254 DNS interne : 172.17.1.1 DNS externe : 172.16.1.10	LAN : 192.168.1.254 LAN Serveurs : 172.17.1.254 DMZ : 172.16.1.254 Externe : 192.36.253.10

Serveurs	Adresse IP interne	Adresse IP publique	Nom FQDN
Serveur interne Rôles : AD, DNS, DHCP, Radius	172.17.v.1	N	srvintra.nice.tierslieux06.fr
Serveur gestion d'incident et inventaire	172.17.v.2	N	srvhdesk.nice.tierslieux06.fr
Serveur DNS	172.16.1.10	192.36.253.10	dns.nice.tierslieux06.fr
Serveur Web	172.16.1.11	192.36.253.11	www.nice.tierslieux06.fr

Sommaire

Contexte TiersLieux.....	1
L'Espace de Travail Partagé.....	1
Projet ETP.....	1
Les locaux de l'ETP.....	2
Schéma des locaux de l'ETP.....	2
Équipement informatique et de sécurité des locaux.....	3
Infrastructure réseau d'un ETP et accès à Internet.....	4

Contexte de la situation professionnelle : Contexte TiersLieux

La société Tiers Lieux dispose de plusieurs sites départementaux répartis sur la France.

Mission 0 : Installation du Contexte TiersLieux :

Vous êtes responsable au niveau de votre département de **mettre en place l'infrastructure système et réseau** (commutateurs, routeurs, serveurs) ainsi que l'accès distant aux serveurs et équipements actifs, la sauvegarde de leur configuration.

Opérations à réaliser : obligatoire pour tous les groupes au semestre 1

Phase 1 - InfraSYS

1. Mise en place du domaine Active Directory

- Installer deux contrôleurs de domaine sur le vlan Serveur, Nom du domaine **PODx.local**
- Installer un premier contrôleur de domaine **Infra1** (+DNS+**bureau à distance**) et un second en réplification **Infra2** (+bureau à distance)
- Configurer **une VM client windows par étudiant** sur votre domaine (@IP .11 et .12 .13)
Attention avant adhésion au domaine : donner l'adresse DNS de votre serveur **Infra1** et votre nom de domaine DNS dans les propriétés avancées de IPV4 (suffixe DNS) pour les serveurs et postes à intégrer au domaine

2. Configuration du DNS AD

- Configurer la zone inverse du DNS pour les IP de TiersLieux (172.2x)
- Configurer au moins un redirecteur 1.1.1.1 sur votre serveur DNS

3. Configuration des utilisateurs du domaine Active Directory

- Mettre en place les utilisateurs et les groupes de TiersLieux dans une UO spécifique Tiers-Lieux : un groupe **IT** (Jean PEUPLUS), un groupe **Bureau** (Mélanie ZETEO), un groupe **Compta** (Lucas FRAID)

4. Intégrer le NAS au domaine AD de TiersLieux

- Créer des partages en RW sur le NAS pour chaque groupe de Tiers-Lieux, avec exclusion d'accès pour les autres groupes, avec un partage **COMMUNTL** en L/E à tous. **Ces partages ne doivent pas être visibles pour les clients de TiersLieux.**

5. Mise en place du serveur GLPI

- Installer le serveur GLPI
- Intégrer le serveur au domaine TiersLieux
- Configurer l'inventaire des VM clientes de TiersLieux
- Configurer un utilisateur du groupe **IT** avec un profil **Technicien** et un utilisateur du groupe **Bureau** qui puisse saisir les tickets mais pas les résoudre.

Phase 2 - InfraRES

- Les VLANs et le routage doivent être définis conformément au document d'architecture de Tiers-Lieux
- Configuration du **Rapid Spanning Tree**
- **L'accès SSH** aux équipements réseaux et aux serveurs Linux doit être mis en place sur le VLAN d'administration réseau (**IT x09**)
- Les configurations des équipements doivent être **sauvegardées sur le serveur NAS via FTP**
- **L'accès Internet doit être fonctionnel sur votre parefeu Stormshield (y compris DNS)**
- **Les équipements réseau doivent être administrables en SNMP avec une communauté publique en RO et une privée en RW**

Productions attendues :

- Produire la liste des tâches à réaliser, le schéma du réseau et son plan d'adressage
- Proposer un **scénario** permettant de montrer la gestion des utilisateurs et des droits sur les fichiers
- Proposer un **scénario** permettant de montrer la gestion des incidents sur GLPI
- Configurer les Vlan sur les commutateurs
- Mettre en place le routage inter vlan
- **Tous les serveurs et équipements** doivent être accessibles à distance via **SSH** ou bureau à distance
- Proposer un **scénario** permettant de montrer que la communication inter-vlan fonctionne correctement, ainsi que l'accès basique à Internet (NAT/PAT). Produire la capture de trames (éventuellement les logs) qui le prouve.

Ressources : Cours/TP Bloc 2 réseau, TP Windows