LAB\_SECURITY

Table des matières

[1. Introduction : 3](#_Toc156756437)

[Contexte et Objectifs : 3](#_Toc156756438)

[2. Conception de la Topologie du Réseau : 3](#_Toc156756439)

[Équipements et Rôle : 3](#_Toc156756440)

[Liaisons et Organisation : 5](#_Toc156756441)

[3. Modèle d'Adressage du Réseau : 7](#_Toc156756442)

[Choix de la Plage d'Adresses IPv4 : 7](#_Toc156756443)

[Plan d’adressage avec VLSM : 7](#_Toc156756444)

[Adresses Publiques et Privées FAI : 8](#_Toc156756445)

[4. Représentation de l'Infrastructure avec Packet Tracer : 9](#_Toc156756446)

[Présentation Visuelle : 9](#_Toc156756447)

[Documentation des Équipements et Configurations : 11](#_Toc156756448)

[Mise en Avant des Fonctionnalités Clés : 11](#_Toc156756449)

[5. Plan de Sécurité : 11](#_Toc156756450)

[Analyse des Besoins en Sécurité et Proposition d'un Plan de Sécurité: 11](#_Toc156756451)

[Mise en place du Plan de Sécurité : 13](#_Toc156756452)

[Application de Mesures par Couche OSI: 13](#_Toc156756453)

[6. Conclusions : 13](#_Toc156756454)

[Récapitulation des Étapes : 13](#_Toc156756455)

[Points Forts de la Conception : 14](#_Toc156756456)

[Perspectives pour des Améliorations Futures : 14](#_Toc156756457)

# 1. Introduction :

## Contexte et Objectifs :

LAB\_Security, en tant que société d'audit et de sécurité logicielle, a besoin d'une infrastructure réseau robuste pour connecter ses agences, centraliser ses services au siège social, et assurer une connexion sécurisée à Internet via un FAI.

Le projet consiste à concevoir une infrastructure réseau sécurisée pour LAB\_Security. L'objectif est de créer un réseau IPv4 avec une configuration dynamique des machines et un routage OSPF pour quatre agences (Rennes, Strasbourg, Grenoble, Bordeaux) connectées à Paris. Le siège, au cœur du système d'information, est composé de 850 hôtes et 152 serveurs physiques et virtuels organisés en VLAN. L'accès internet se fait via un routeur opérateur.

# 2. Conception de la Topologie du Réseau :

## Équipements et Rôle :

La topologie du réseau est conçue pour répondre aux besoins spécifiques de LAB\_Security, en assurant la redondance, la sécurité, et une gestion efficace des connexions. Les équipements utilisés comprennent des routeurs et des switches, distribués entre le siège social à Paris et les agences à Rennes, Bordeaux, Grenoble, et Strasbourg.

1. **Paris :**

* **Routeurs** : Paris (Principal), Paris2 (Redondance pour Paris), Paris3 (Redondance pour Paris2)

Paris assure la connectivité entre le siège et interagit avec les FAI.

Paris2 et Paris3 servent de routeurs de secours pour garantir la disponibilité en cas de panne pour les agences.

Paris 3 sert de redondance vers le FAIs

* **Switches** :

Gèrent les connexions locales au siège.

Segmentent le trafic en VLANs pour différents services (DSI, Compta, Invités, etc.).

1. **Agences :**

* **Routeurs** : Deux par agence

Configurés avec le protocole HSRP pour assurer la redondance de la gateway.

Connectés à Paris2 et Paris3 pour divers chemins de sortie en cas de panne.

* **Switches** : Deux par agence

Connectent les périphériques locaux.

Les switches sont attribués à des VLANs correspondant aux différents services.

1. **Découpage des Agences et LAN :**

* **Rennes :**

Routeurs Rennes1/2 connectés à Paris2/Paris3.

Switches pour connecter les lans RennesA composé de 500 hôtes et RennesC composé de 200 hôtes

* **Bordeaux :**

Routeurs Bordeaux1/2 connectés respectivement à Paris2/Paris3.

Switches pour connecter les lans BordeauxD composé de 80 hôtes et BordeauxE composé de 60 hôtes.

* **Grenoble :**

Routeurs Grenoble1/2 connectés respectivement à Paris2/Paris3.

Switches pour connecter les lans GrenobleA composé de 500 hôtes et GrenobleB composé de 120 hôtes.

* **Strasbourg :**

Routeurs Strasbourg1/2 connectés respectivement à Paris2/Paris3.

Switches pour connecter les lans StrasbourgD composé de 80 hôtes et StrasbourgF composé de 27 hôtes.

1. **Connexion avec le FAI :**

Routeur de FAI distant : Connecté au siège de LAB\_Security, plus précisément au routeur Paris et au routeur Paris2.

Assure la connectivité au réseau Internet.

Permet une centralisation, traçabilité, et sécurité des connexions.

Cette topologie assure une connectivité robuste et redondante. Chaque agence est connectée à deux routeurs pour garantir la disponibilité, tandis que les VLANs sur les switches permettent une segmentation efficace du trafic. Les connexions entre Paris, Paris2, et Paris3, ainsi que les connexions entre les agences, sont planifiées pour répondre aux exigences de disponibilité et de sécurité du réseau

## Liaisons et Organisation :

Les liaisons entre les équipements réseau peuvent être établies avec différents types de câbles en fonction des besoins spécifiques et des technologies utilisées. Voici une proposition basée sur les informations fournies :

1. **Liaisons au Siège (Paris)**

* **Entre les Routeurs à Paris (Paris, Paris2, Paris3)**

Câbles croisés : Utilisés pour connecter les ports Ethernet des routeurs entre eux et former un réseau OSPF interne au siège.

* **Entre le Routeur Principal Paris et le FAI distant**

Câble série DCE : Utilisé pour établir la connexion entre le routeur principal de Paris (Paris) et le FAI distant, assurant l'accès à Internet.

* **Entre les Routeurs et les Switches au Siège**

Câbles droits : Utilisés pour connecter les ports des routeurs aux ports des switches, formant ainsi les connexions entre le réseau interne du siège.

1. **Liaisons avec les Agences**

* **Entre les Routeurs et le Switch à l'Agence de Rennes**

Câbles droits : Utilisés pour connecter les ports des routeurs RennesA et RennesB aux ports du switch local, établissant ainsi la connectivité entre les routeurs et les équipements locaux.

* **Entre les Routeurs des Agences**

Câbles croisés : Utilisés pour connecter les ports Ethernet des deux routeurs d'une agence, établissant un réseau redondant au sein de l'agence.

* **Liaisons entre les Routeurs des Agences et Paris (Paris2, Paris3)**

Câbles série DCE : Utilisés pour connecter les routeurs des agences aux routeurs Paris2 et Paris3 au siège, permettant la redondance et l'accès à Internet.

* **Entre le Switch et les Périphériques Locaux**

Câbles droit : Utilisés pour connecter les ports du switch aux équipements locaux (ordinateurs, serveurs, etc.).

1. **Liaisons avec le FAI distant**

* **Entre le Routeur de FAI Distant et les Routeurs de Paris (Paris et Paris2)**

Câble série DCE : Utilisé pour connecter le routeur de FAI distant au routeur principal de Paris, assurant l'accès global à Internet.

En résumé, des câbles croisés ou droit sont utilisés pour les liaisons locales entre les routeurs, tandis que certains câbles série DCE sont employés pour les connexions entre les routeurs et le FAI distant, principalement pour des liaisons longue distance. Les connexions avec les switches et les équipements locaux peuvent, quant à elles, utiliser des câbles droits. Ces choix sont déterminés en fonction des technologies spécifiques et des besoins de distances propres à chaque liaison au sein de l'infrastructure réseau.

# 3. Modèle d'Adressage du Réseau :

## Choix de la Plage d'Adresses IPv4 :

L'adresse **172.16.0.0/20** semble une option appropriée pour répondre aux besoins spécifiés. Cette plage d'adresses offre une grande flexibilité en termes d'hôtes, et elle peut être subdivisée efficacement pour répondre aux différentes tailles de LANs dans chaque agence et au siège social.

## Plan d’adressage avec VLSM :

#### VLAN par cœur de métier

DSI : ADRESSE :172.16.0.0/23 PLAGE : 0.1 - 1.254

COMPTA : ADRESSE :172.16.4.0/24 PLAGE : 4.1 - 4.254

INVITES : ADRESSE : 172.16.5.0/24 PLAGE : 5.1 - 5.254

DIRECTION : ADRESSE : 172.16.6.0/25 PLAGE : 6.1 - 6.126

RH : ADRESSE :172.16.6.128 /25 PLAGE : 6.129 - 6.254

DNS : ADRESSE 172.16.8.253

#### LAN

RennesA : ADRESSE 172.16.10.0/23 PLAGE : 10.1 - 11.254

GrenobleA : ADRESSE : 172.16.12.0/23 PLAGE : 12.1 - 13.254

RennesC : ADRESSE : 172.16.15.0/24 PLAGE : 15.1 - 15.254

GrenobleB : ADRESSE 172.16.16.0/25 PLAGE : 16.1 - 16.126

BordeauxD : ADRESSE : 172.16.16.128/25 PLAGE : 16.129 - 16.254

StrasbourgD : ADRESSE : 172.16.17.0/25 PLAGE : 17.1 - 17.126

BordeauxE : ADRESSE 172.16.17.128/26 PLAGE : 17.129 - 17.190

StrasbourgF : ADRESSE 172.16.17.192/27 PLAGE : 17.193 - 17.222  
  
La plage 172.16.0.0/20 offre suffisamment d'adresses pour accommoder le nombre d'hôtes requis tout en permettant une subdivision efficace avec VLSM.

Les réseaux d'agence sont organisés de manière logique avec une adresse de réseau facile à comprendre, renforçant la gestion et la traçabilité des connexions.

Le réseau du siège social occupe une plage plus large pour tenir compte du grand nombre de serveurs et d'hôtes.

Le réseau du FAI utilise une plage distincte pour la connectivité Internet ou de télécommunication aux serveurs, améliorant la gestion et la sécurité, en accord avec nos discussions sur la sécurité du réseau.

Ce plan offre une structure claire, permettant une gestion efficace des adresses et une évolutivité future, tout en répondant aux exigences spécifiées dans notre conversation.

#### Connectivité entre Paris2 et les agences

* Rennes: SR 172.16.18.12/30 Plage: 18.13-18.14
* Strasbourg: SR 172.16.18.20/30 Plage: 18.21-18.22
* Bordeaux: SR 172.16.18.28/30 Plage: 18.29-18.30
* Grenoble: SR 172.16.18.36/30 plage: 18.37-18.38

#### Connectivité entre Paris3 et les agences

* Rennes: SR 172.16.18.16/30 Plage: 18.17-18.18
* Strasbourg: SR 172.16.18.24/30 Plage: 18.25-18.26
* Bordeaux: SR 172.16.18.32/30 Plage: 18.33-18.34
* Grenoble: SR 172.16.18.40/30 plage: 18.41-18.42

## Adresses Publiques et Privées FAI :

**Réseau local FAI** : ADRESSE : 172.16.30.0/24 PLAGE : 30.1 - 30.254

**Réseau Paris-FAI avec une adresse publique :** ADRESSE : 203.0.113.4/30 plage 113.5 -113.6

**Réseau Paris3 - FAI avec une adresse publique :** ADRESSE : 203.0.113.0/30 plage 113.1 -113.2

# 4. Représentation de l'Infrastructure avec Packet Tracer :

## Présentation Visuelle :

Une image contenant texte, capture d’écran, diagramme, ligne

Description générée automatiquement

**Siège de Paris**

**Une image contenant diagramme, capture d’écran, ligne, Tracé

Description générée automatiquementAgence de Rennes**

**Une image contenant diagramme, capture d’écran, ligne, cercle

Description générée automatiquement**

**Agence de Strasbourg  
  
Une image contenant diagramme, capture d’écran, ligne, Tracé

Description générée automatiquement**

**Agence de Bordeaux  
  
Une image contenant diagramme, cercle, ligne, capture d’écran

Description générée automatiquement**

**Agence de Grenoble**

**Une image contenant diagramme, ligne

Description générée automatiquement  
FAI**

## Documentation des Équipements et Configurations :

Configuration des interfaces, des VLANs, et des connexions dans Packet Tracer.

## Mise en Avant des Fonctionnalités Clés :

Configuration des routeurs pour le routage OSPF.

Configuration des commutateurs pour les VLANs.

# 5. Plan de Sécurité :

## Analyse des Besoins en Sécurité et Proposition d'un Plan de Sécurité :

Les besoins de sécurité de l'infrastructure réseau de LAB\_Security, en conformité avec le modèle OSI (Open Systems Interconnection), peuvent être définis comme suit, en prenant en compte chaque couche du modèle :

1. **Sécurisation des Ports des Switches (Couche Physique) :**

Objectif : Prévenir les accès non autorisés aux équipements réseau physiques.

Mesures : Configurer des mécanismes de sécurisation des ports, tels que le Port Security, pour limiter l'accès aux appareils autorisés uniquement.

1. **Redondance de la Gateway avec HSRP (Couche Liaison de Données) :**

Objectif : Assurer une continuité de service en cas de panne d'un équipement.

Mesures : Implémenter le protocole HSRP (Hot Standby Router Protocol) pour la redondance des passerelles, permettant une bascule transparente en cas de défaillance de l'équipement principal.

1. **Utilisation de VLANs pour la Sécurité des Réseaux (Couche Liaison de Données) :**

Objectif : Isoler logiquement les segments de réseau pour améliorer la sécurité et la gestion.

Mesures : Configurer des VLANs (Virtual Local Area Networks) pour segmenter les réseaux en fonction de critères tels que les départements, les fonctions ou les équipes. Cela permet de limiter la visibilité et l'accès entre les différentes parties du réseau.

1. **Configuration OSPF sur Paris avec Zones Multiples (Couche Réseau) :**

Objectif : Assurer une connectivité efficace et sécurisée entre les réseaux.

Mesures : Configurer OSPF (Open Shortest Path First) avec une conception de zones multiples pour optimiser le routage, améliorer la stabilité, et garantir la confidentialité des informations de routage.

1. **Mise en Place d'ACL pour le Filtrage du Trafic (Couche Réseau) :**

Objectif : Contrôler sélectivement le flux de trafic entre les réseaux.

Mesures : Utiliser des Listes de Contrôle d'Accès (ACL) pour définir des politiques de filtrage, autorisant ou refusant le trafic en fonction de critères spécifiques tels que les adresses IP, les protocoles, ou les ports.

1. **Chiffrement des Communications entre Réseaux Locaux (Couche Transport) :**

Objectif : Protéger la confidentialité des données transitant entre les réseaux.

Mesures : Implémenter des mécanismes de chiffrement, comme l'utilisation de protocoles VPN (Virtual Private Network) pour sécuriser les communications entre sites distants.

1. **Verrouillage de l'Accès aux Modes Console, Utilisateur et Privilégié par Mot de Passe (Couche Application) :**

Objectif : Prévenir l'accès non autorisé aux équipements réseau et aux configurations sensibles.

Mesures : Configurer des mots de passe robustes pour l'accès à la console, aux modes utilisateur (mode EXEC) et privilégié (mode Enable) des équipements réseau.