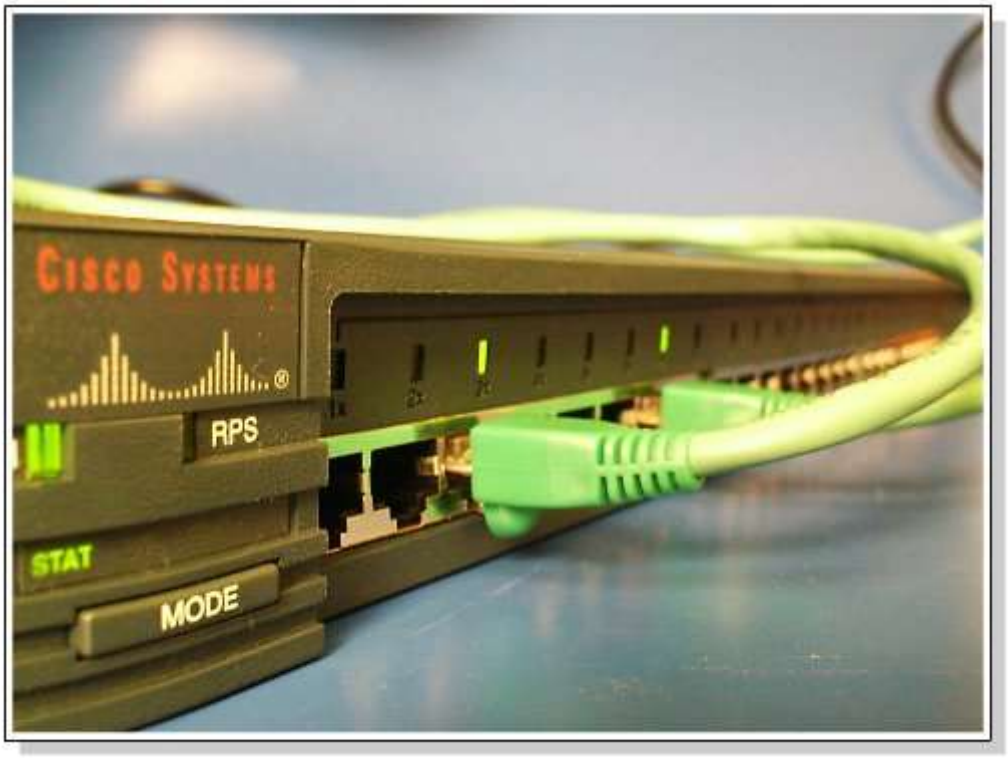
TP : Réseau embarqué



TP Mise en place d'un LAN

1) Objectifs

L'étudiant devra être capable :

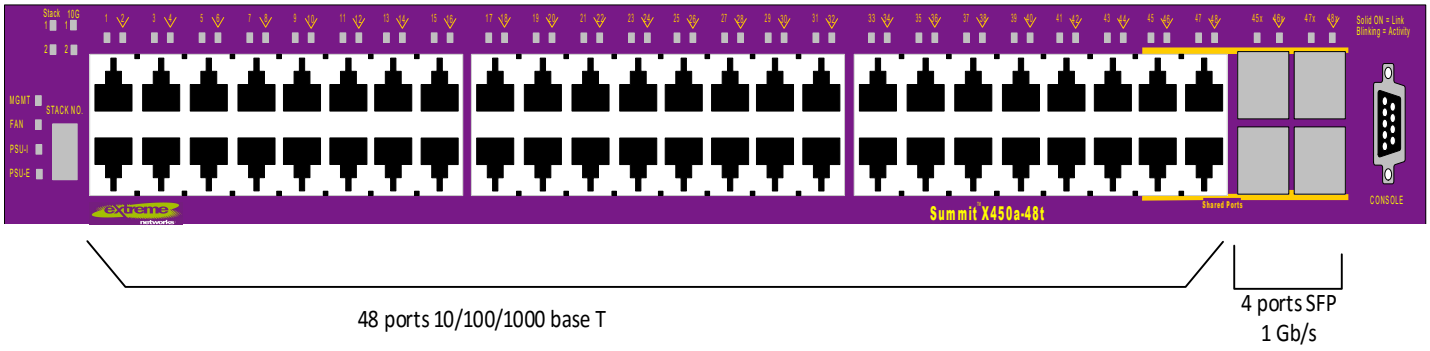
- ✓ D'identifier les différents matériels dans le réseau (routeur, switch, hub, PC, etc....)
- ✓ De câbler les différents matériels suivant une architecture réseau
- ✓ De configurer les commutateurs face aux exigences de sécurité et de configuration
- ✓ De vérifier par des tests élémentaires la conformité de l'architecture du réseau local

2) Pré-requis

Cours sur les réseaux à technologie TCP-IP.

3) Configuration des commutateurs au niveau 2

Les commutateurs utilisés sont des Extreme network X460e dotés de 24 ou 48 ports 10/100/1000 base T Et de 4 ports 1000base FX. La face arrière est constituée de la prise secteur et de modules optionnels. Les commutateurs sont déconfigurés au démarrage



Les commutateurs sont des Extreme Networks de type X460 proposant 48 ou 24 ports cuivre 10/100/1000 Mb/s. Quatre ports ont la capacité d'être « convertis », via leurs ports dédiés mini-Gbic, en ports optiques 1 Gb/s par l'adjonction de connecteurs SFP. Ils répondent aux fonctions suivantes :

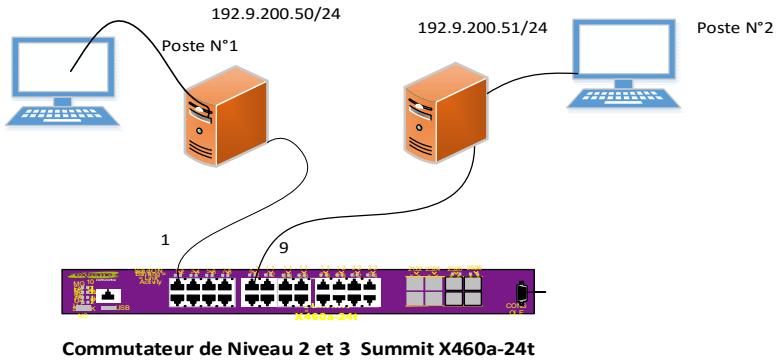
- ➢ Permettre l'accès au réseau pour les différents abonnés
- ➢ Concentrer les flux vers le coeur de réseau (backbone) via les liens redondés

Un réseau Backbone (ou réseau cœur) est la partie centrale d'un réseau de télécommunications qui fournit divers services

à des clients qui sont connectés par le réseau d'accès. Le backbone (cœur de réseau, littéralement épine dorsale) est le cœur de réseau, qui est également appelé réseau général.

3.1) Utilisation d'un commutateur sans paramétrage du commutateur

Réalisez le câblage suivant en configurant Poste N°1 et poste N°2:



Commutateur de Niveau 2 et 3 Summit X460a-24t

3.1.1) Pingez les 2 machines que constatez-vous, interprétez les résultats.

3.2) Création d'un VLAN de niveau 2

On souhaite configurer ce commutateur de niveau 2 en utilisant le principe des VLAN

La configuration pour le VLAN N°1 est la suivante :

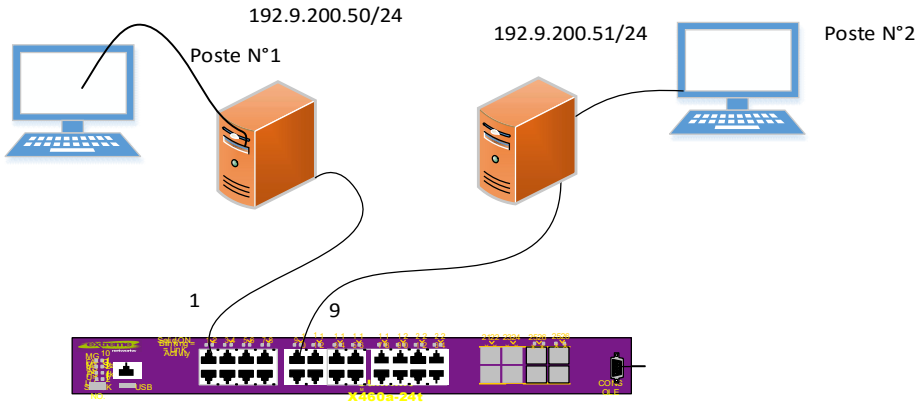
Nom du VLAN	Numéro du VLAN	Ports affectés	
Dom1	10	9,10,11,12,13,14,15,16	Untagged

La configuration pour VLAN N°2 est la suivante :

Nom du VLAN	Numéro du VLAN	Ports affectés	
Dom2	11	1,2,3,4,5,6,7,8	Untagged

A partir de la configuration précédente et de la notice d'explication de configuration du commutateur page N°32 paramétrez le commutateur summit X460e.

Réalisez le câblage suivant :

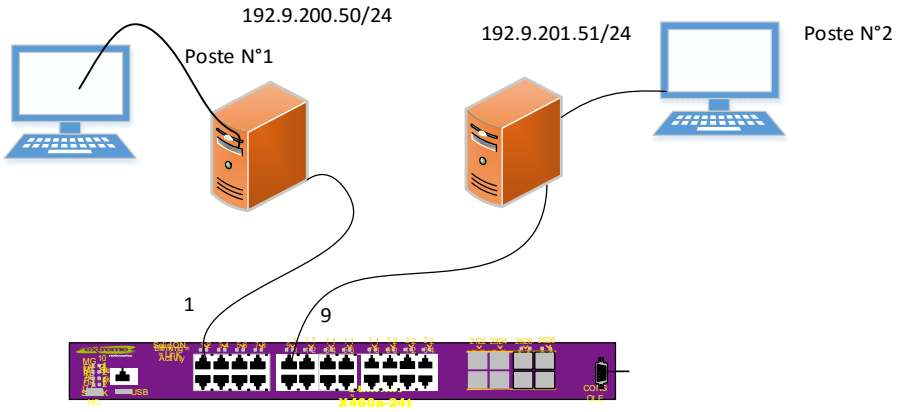


Commutateur de Niveau 2 et 3 Summit X460a-24t

Pingez les 2 machines que constatez-vous, interprétez les résultats.

Modifiez le câblage afin que les deux postes se voient

Modifiez la configuration du Poste N°2 voir schéma ci-dessous :

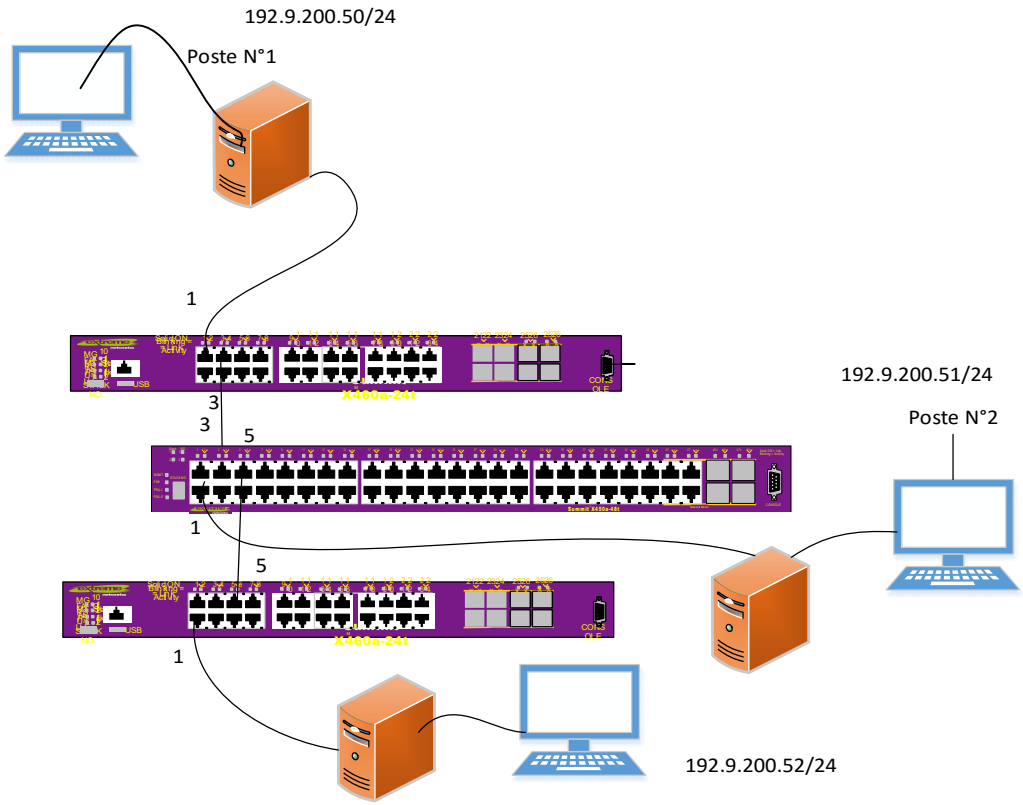


Commutateur de Niveau 2 et 3 Summit X460a-24t

Pingez les 2 machines, conclure.

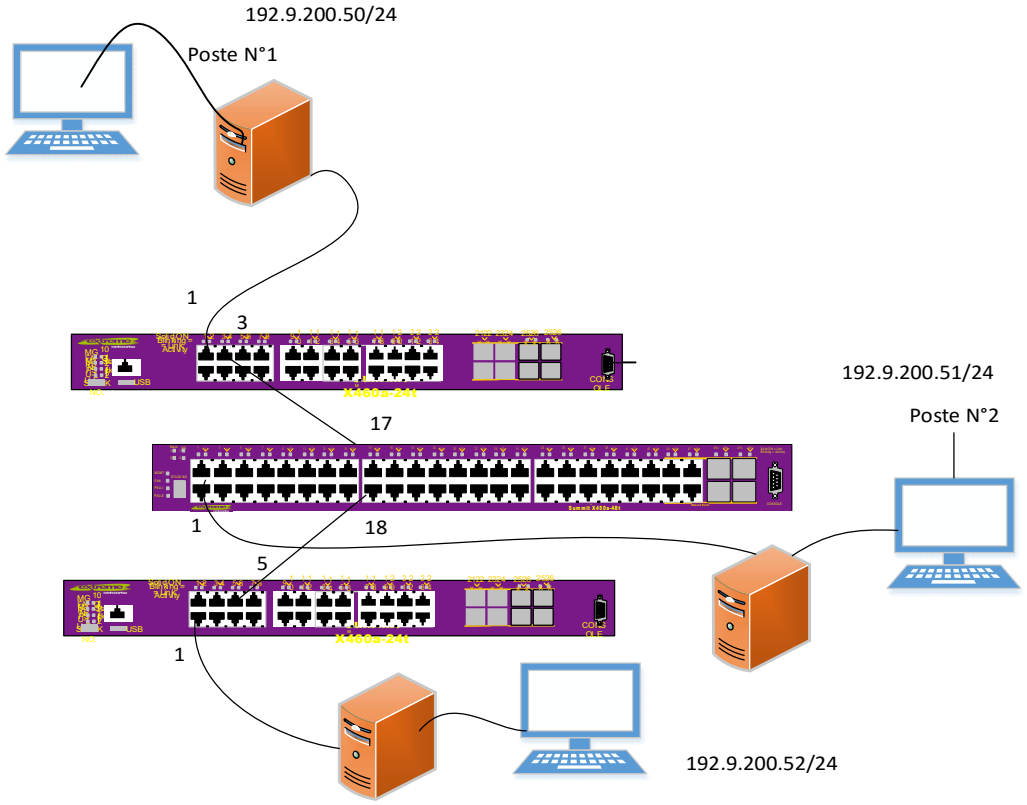
3.3) Propagation de VLAN sur les commutateurs au niveau 2

Réalisez le câblage suivant :



Pingez les 2 machines que constatez-vous, interprétez les résultats.

Modifiez le câblage suivant



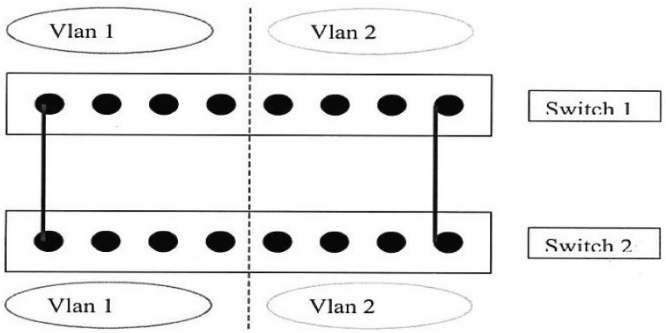
Pingez les 2 machines que constatez-vous, interprétez les résultats.

En vous servant du dossier sur les lignes de commande, sauvegardez la configuration et restaurez la configuration par la suite.

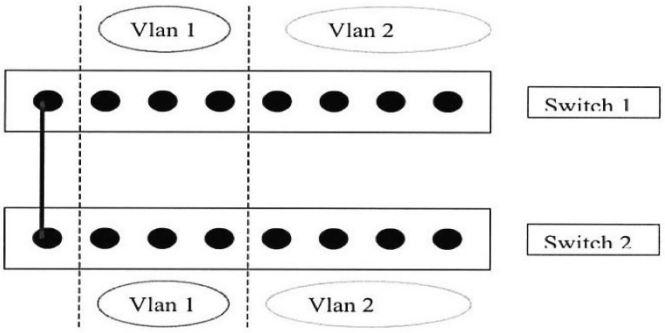
3.4) La propagation de VLAN

Si vous désirez propager plusieurs VLAN sur un même lien physique, il faut tagger les trames afin de respecter la norme 802.1Q. Pour cela il faudra que vos paquets qui circulent entre commutateurs soit taggués, c'est-à-dire qu'ils contiennent dans leurs en têtes le numéro du VLAN (VLAN ID) pour lequel ils sont destinés.

- **Propagation de VLAN :**



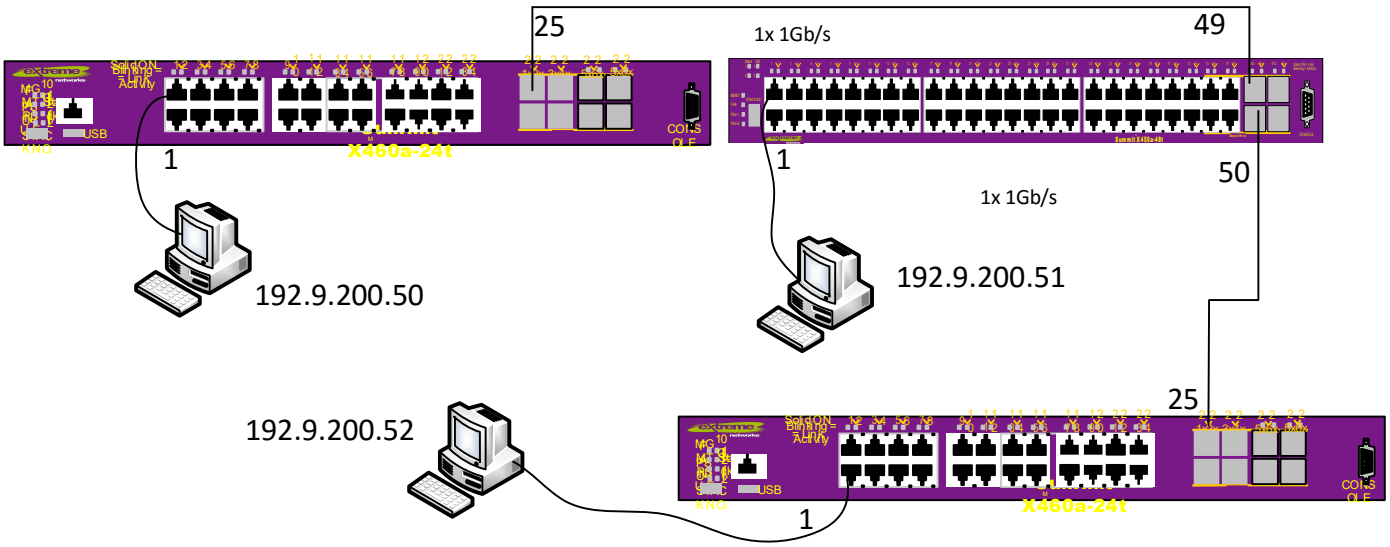
- On est obligé de tirer deux câbles pour relier les deux vlan ensemble .
- Pour éviter cela, on fait de la propagation de vlan ce qui permet de ne tirer qu'un seul câble .



Proposez une modification de la configuration du switche afin de tagger les trames entres les deux commutateurs ;

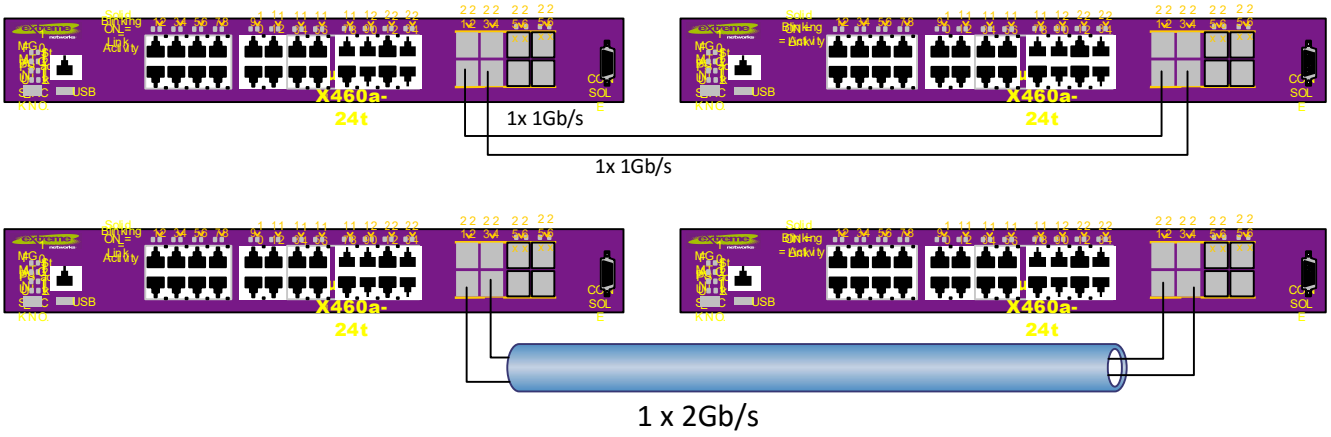
Vérifiez le bon fonctionnement

Câblez de la façon suivante et configurez les switches pour assurer un trunk entre les deux commutateurs.



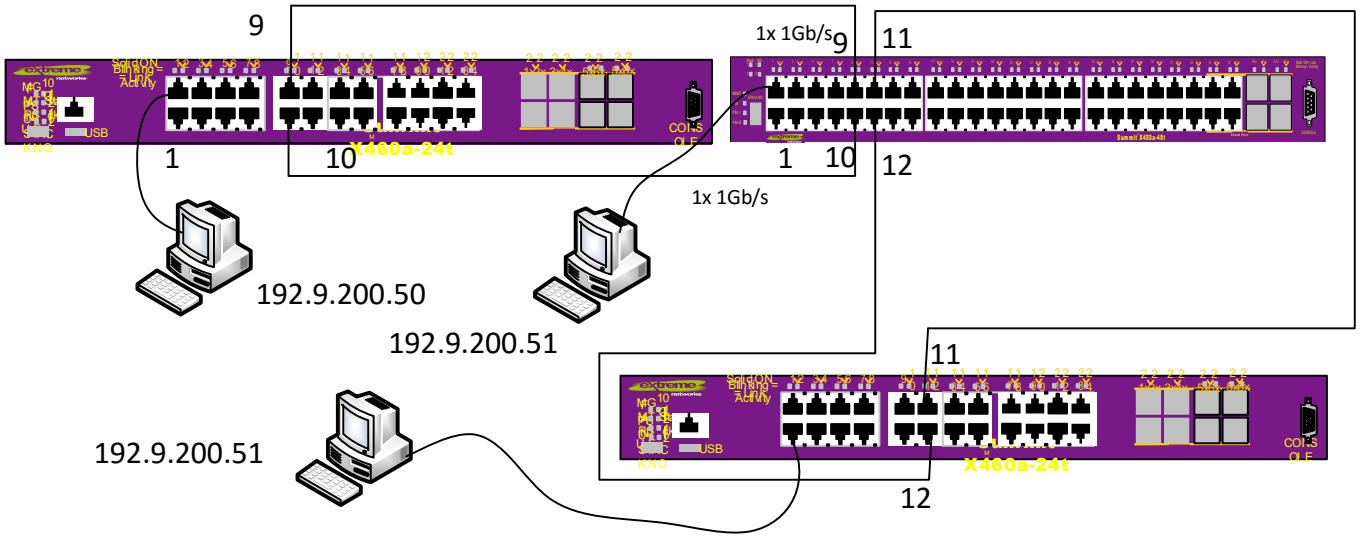
3.5) L'agrégation de liens

L'agrégation de liens est une notion de réseau informatique décrivant le regroupement de plusieurs liens réseau comme s'il s'agissait d'un seul lien réseau. Le but est d'accroitre le débit au-delà des limites d'un seul lien, et éventuellement de faire en sorte que les autres liens prennent le relai si un lien tombe en panne (redondance).
L'agrégation de liens est le plus souvent mise en place entre les ports de commutateurs Ethernet mais on peut la rencontrer entre serveurs et commutateurs.
Le commutateur utilise de multiple port comme un simple port logique ce qui permet d'augmenter les débits



Le trafic reçu est recombiné et vu comme un simple flux de trafic. Le protocole utilisé est le LACP (link agregation control protocol) IEEE802.3ad.

En vous servant des lignes de commande (voir dossier cli) réalisez une agrégation de lien à partir du schéma suivant :

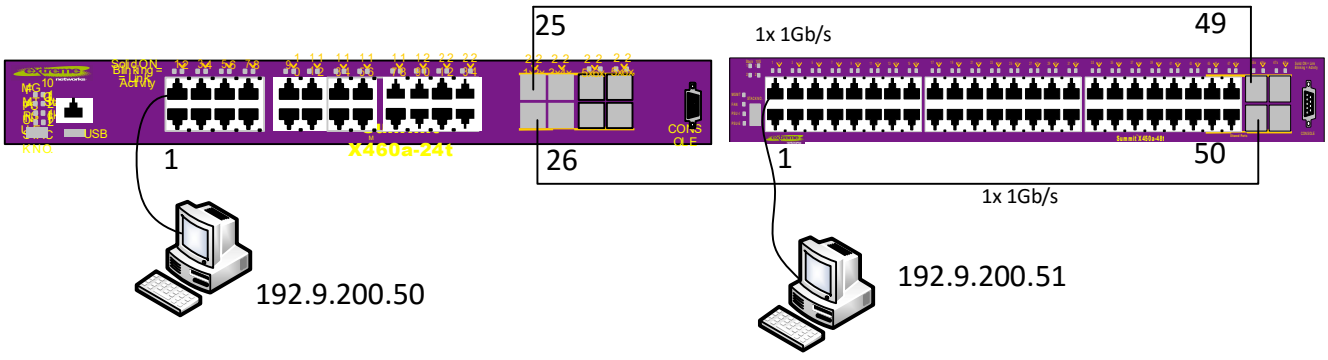


Désactivez le port 9 et vérifiez le bon fonctionnement de l'agrégation de liens

Attention les ports physiques ne peuvent être regroupés que par paire ou par 4 commençants toujours par un chiffre impair.

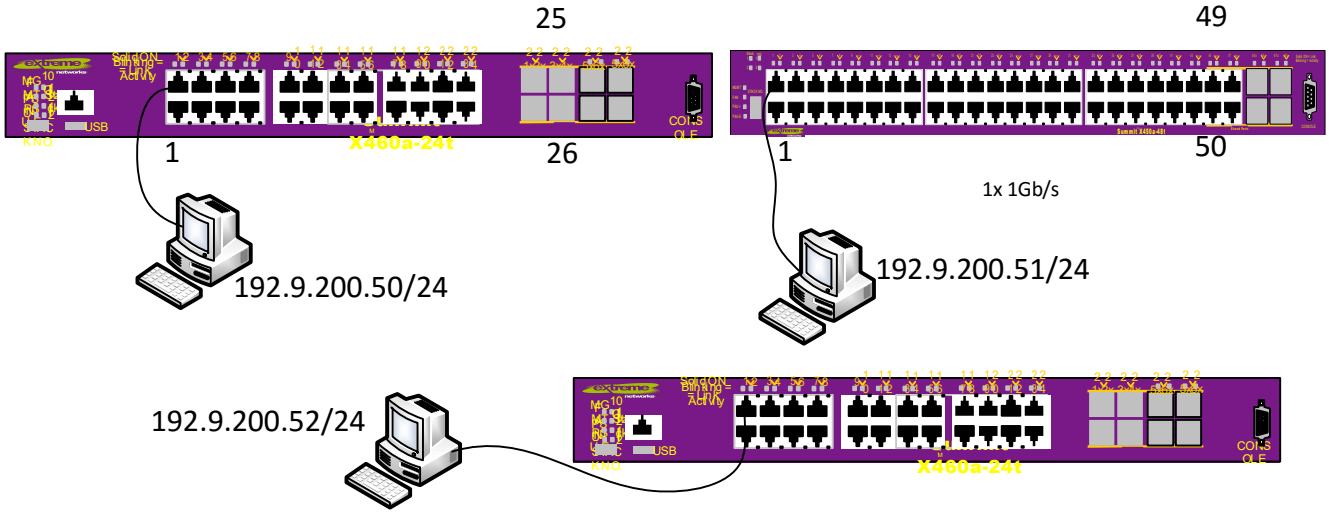
Load-Sharing Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
4-port groups	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
2-port groups	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

En vous servant des lignes de commande (voir dossier cli) réalisez une agrégation de lien à partir du schéma suivant :



Sécurisation des ports

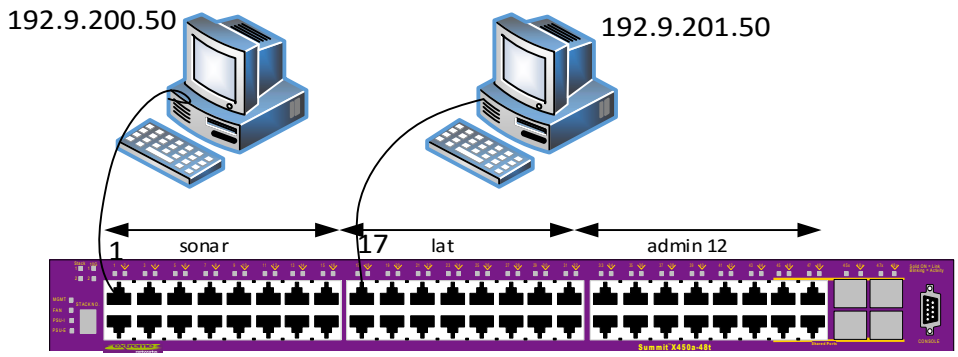
On souhaite sécuriser les ports N°1 de chaque switche avec l'adresse MAC de chaque ordinateur. En vous servant des commandes en ligne mettez en place cette sécurisation



Vérifiez le bon fonctionnement de cette sécurisation

4) Configuration des commutateurs au niveau 3

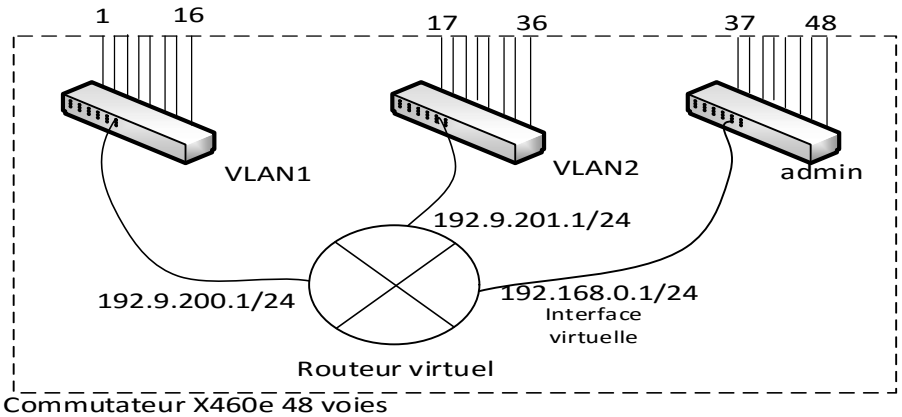
Ce modèle de commutateur peut travailler comme un routeur virtuel en utilisant une commutation sur les adresses IP. Le schéma de câblage est le suivant pour le commutateur du type X460a-48t :



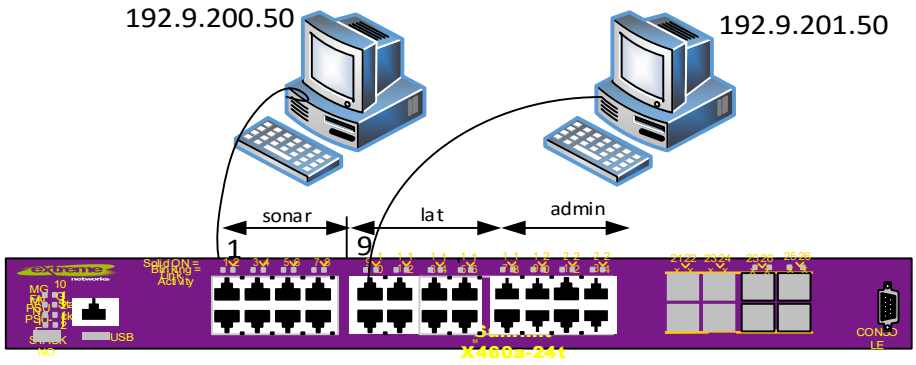
La configuration est la suivante :

Nom du VLAN	Numéro du VLAN	Ports affectés		@IP interface
VLAN1	10	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	Untagged	192.9.200.1/24
VLAN2	11	17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32	Untagged	192.9.201.1/24
admin	12	33,34,35,36,37,38,39,40,41,42,42,44,45,46,47,48	Untagged	192.168.0.1/24

Le commutateur va créer des interfaces virtuelles pour chaque VLAN de la manière suivante :



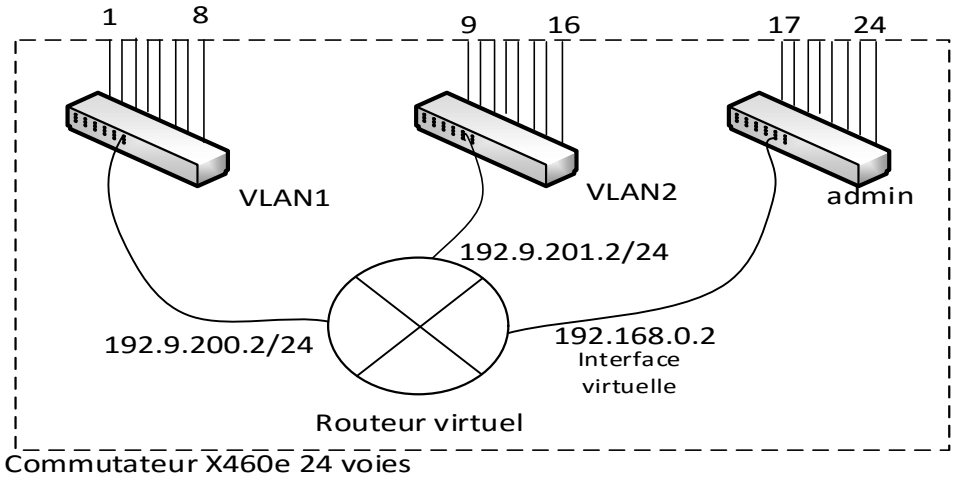
Le schéma de câblage est le suivant pour le commutateur du type X460a-24t :



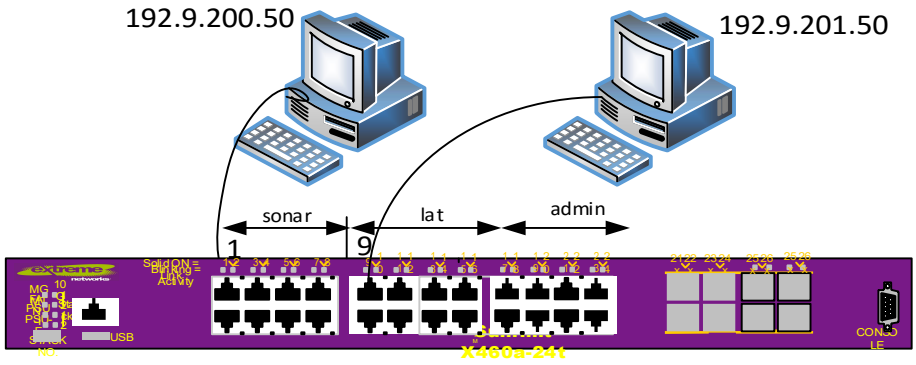
La configuration est la suivante :

Nom du VLAN	Numéro du VLAN	Ports affectés		@IP interface
VLAN1	10	1,2,3,4,5,6,7,8	Untagged	192.9.200.2/24
VLAN2	11	9,10,11,12,13,14,15,16	Untagged	192.9.201.2/24
admin	12	17,18,19,20,21,22,23,24	Untagged	192.168.0.2/24

Le commutateur va créer des interfaces virtuelles pour chaque VLAN de la manière suivante :



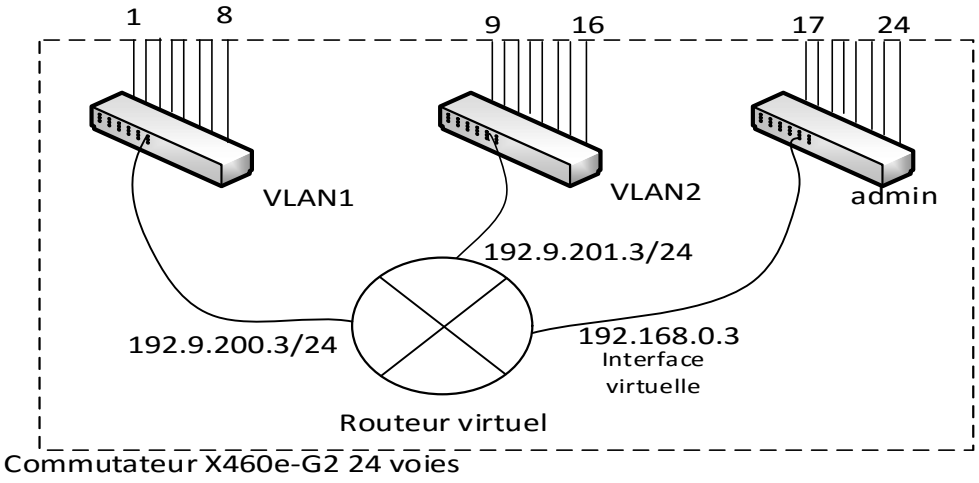
Le schéma de câblage est le suivant pour le commutateur du type X460a-24t-G2 :



La configuration est la suivante :

Nom du VLAN	Numéro du VLAN	Ports affectés		@IP interface
VLAN1	10	1,2,3,4,5,6,7,8	Untagged	192.9.200.3/ 24
VLAN2	11	9,10,11,12,13,14,15,16	Untagged	192.9.201.3/ 24
admin	12	17,18,19,20,21,22,23,24	Untagged	192.168.0.3/ 24

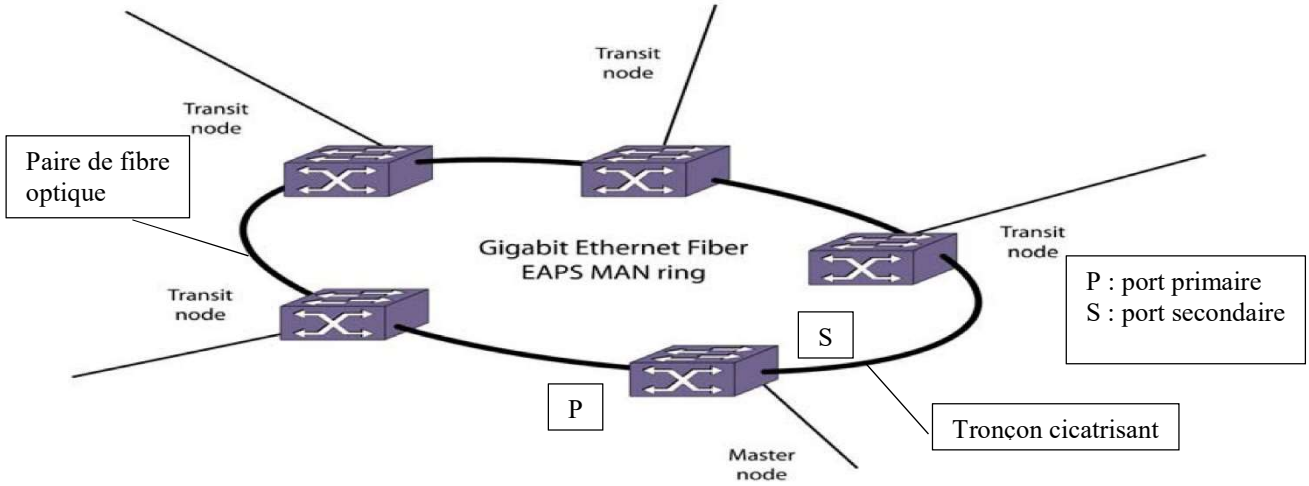
Le commutateur va créer des interfaces virtuelles pour chaque VLAN de la manière suivante :



En utilisant les commandes en ligne (voir dossier), créez les interfaces virtuelles pour chaque commutateur en respectant la configuration précédente. On prendra un protocole de routage dynamique du type RIP
Testez le bon fonctionnement

5) Mise en place d'une redondance de lien sur une boucle EAPS

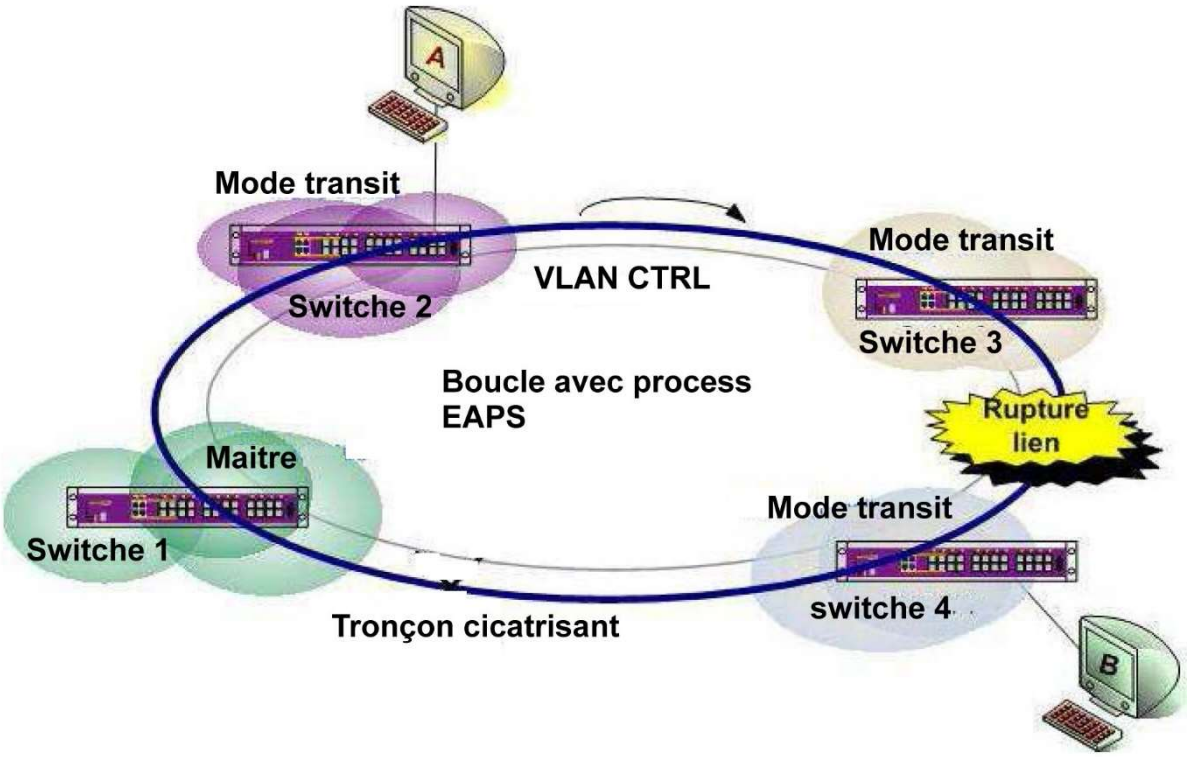
Le protocole EAPS (Ethernet automatic protocol switching) a été inventé par Extreme network pour augmenter la disponibilité des anneaux.
Le protocole EAPS, fournit une protection rapide dans la commutation au niveau 2 et 3 dans des switches interconnectés dans une topologie Ethernet en **anneau tel que les réseaux métropolitains MAN (concurrent du FDDI)**.
Dans une boucle EAPS, les commutateurs forment une architecture backbone grâce à une topologie en anneau. Une paire de fibre optique assure le lien entre chaque commutateur (liaison montante et descendante) .



Dans le principe même de la boucle, les informations échangées au sein d'une même boucle logique peuvent transiter indifféremment dans un sens comme dans l'autre. Cependant, pour que l'information ne « tourne pas indéfiniment » dans le réseau, chaque boucle est coupée logiquement en un point (i.e. port d'un commutateur membre de la boucle bloqué par logiciel). Ce point correspond aux tronçons de fibre cicatrisants sur la boucle (port secondaire du maitre).
Le mécanisme de cicatrisation retenu consiste en la fermeture du lien cicatrisant en cas de rupture d'une fibre optique sur la boucle. Le protocole de convergence EAPS (Extreme Automatic Protection Switching) permet aux commutateurs connectés en boucle de se reconfigurer rapidement en cas de panne (perte d'un lien optique ou d'un commutateur).
Le commutateur maitre EAPS contrôle en permanence l'état des boucles grâce à des trames de contrôle et peut à tout moment rétablir la partie « ouverte » d'une boucle (tronçon cicatrisant) rétablissant ainsi un chemin de commutation.

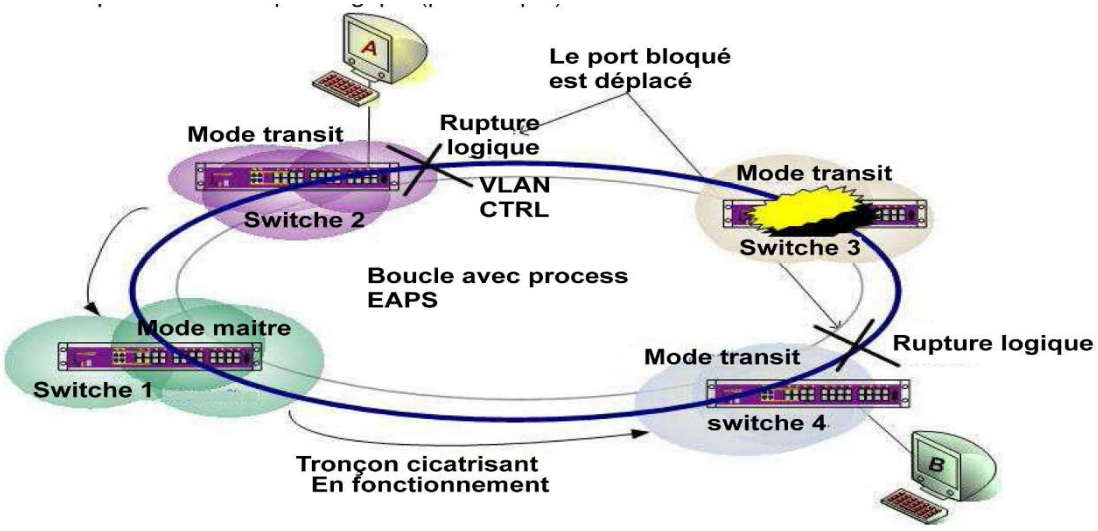
Deux cas de défaillances sont possibles :

- Rupture d'une fibre



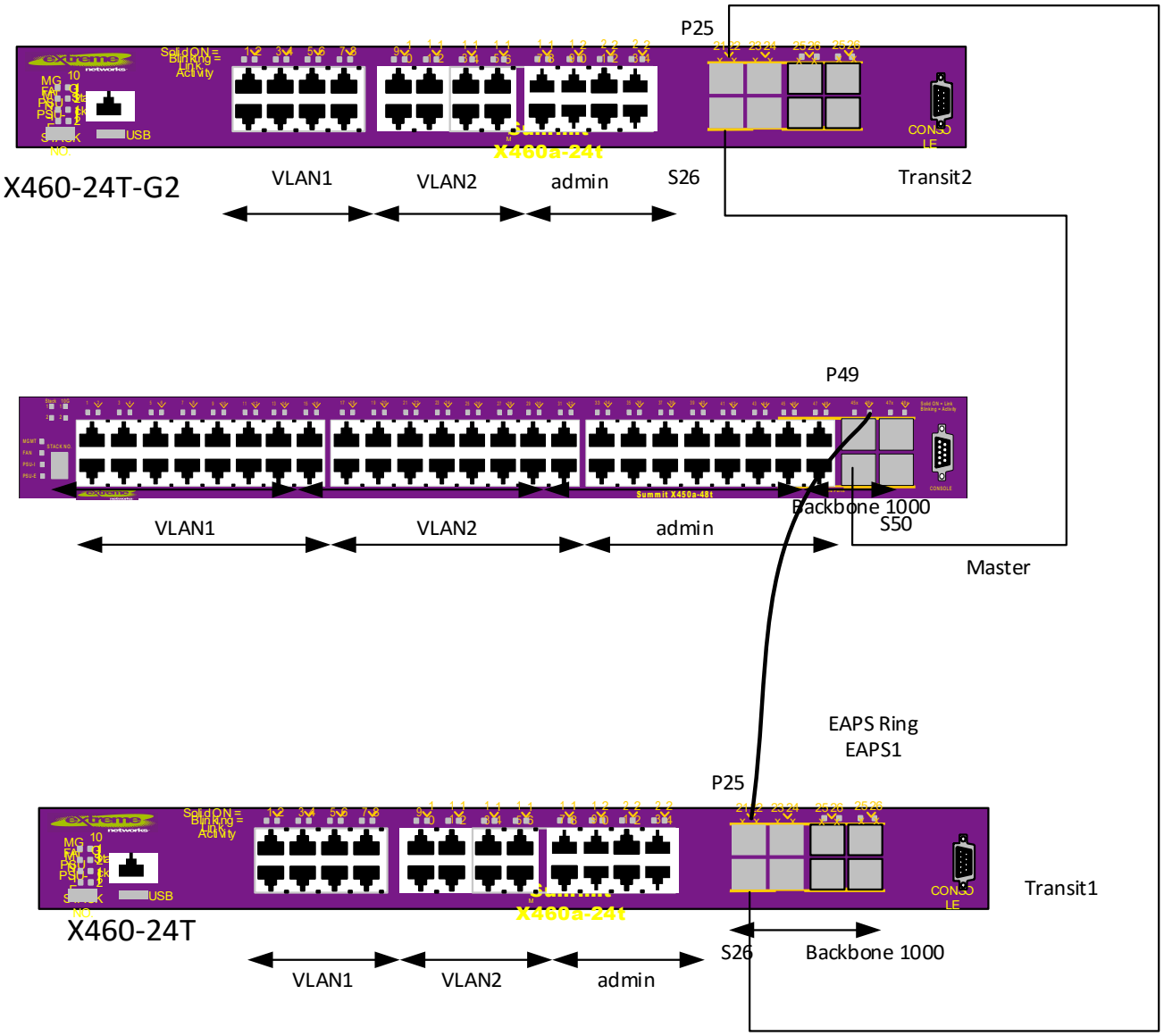
- Disfonctionnement d'un commutateur

  En cas de panne d'un commutateur (n'intégrant pas de fonction de routage), le même mécanisme s'applique, à la différence près que les deux commutateurs situés de part et d'autre du commutateur hors service placent une coupure logique (port bloqué) du côté de ce dernier.



Les systèmes informatiques du switche 3 sont alors in opérationnels sauf s'ils sont reliés par au double attachement à un autre commutateur valide

On souhaite implanter la technologie EAPS en utilisant les trois commutateurs suivants :



La configuration est la suivante pour le switche Master:

Nom du VLAN	Numéro du VLAN	Ports affectés		@IP interface
VLAN1	10	1,2,3,4,5,6,7,8	Untagged	192.9.200.1/24
VLAN2	11	9,10,11,12,13,14,15,16	Untagged	192.9.201.1/24
admin	12	17,18,19,20,21,22,23,24	untagged	192.9.202.1/24
backbone	1000	49,50	tagged	

La configuration est la suivante pour le switche transit1:

Nom du VLAN	Numéro du VLAN	Ports affectés		@IP interface
VLAN1	10	1,2,3,4,5,6,7,8	Untagged	192.9.200.2/24
VLAN2	11	9,10,11,12,13,14,15,16	Untagged	192.9.201.2/24
admin	12	17,18,19,20,21,22,23,24	untagged	192.9.202.2/24
backbone	1000	25,26	tagged	

La configuration est la suivante pour le switche transit2:

Nom du VLAN	Numéro du VLAN	Ports affectés		@IP interface
VLAN1	10	1,2,3,4,5,6,7,8	Untagged	192.9.200.3/24
VLAN2	11	9,10,11,12,13,14,15,16	Untagged	192.9.201.3/24
admin	12	17,18,19,20,21,22,23,24	untagged	192.9.202.3/24
backbone	1000	25,26	tagged	

En utilisant les commandes en ligne (voir dossier), Réalisez cette boucle EAPS.
Vérifiez son bon fonctionnement.
Désactivez le port primaire et vérifiez la redondance de lien
Disable ports <primary_ports>

6) Mise en place d'une agrégation de lien en relation avec la boucle EAPS

Comme pour l'agrégation de lien il est possible de regrouper plusieurs ports physiques et leur lien optique ou filaire dans un seul groupe. Le protocole LACP permet de répartir la charge en débit sur les différents liens du groupe. Si un lien tombe le débit est impacté mais le fonctionnement reste garanti. Afin d'éviter les problèmes de boucle cette agrégation de lien doit être associée à la boucle EAPS

La commande est alors :

enable sharing <numéro du groupe> **grouping** <numéro des ports> **algorithm address-based** <numéro du niveau OSI> **lacp**

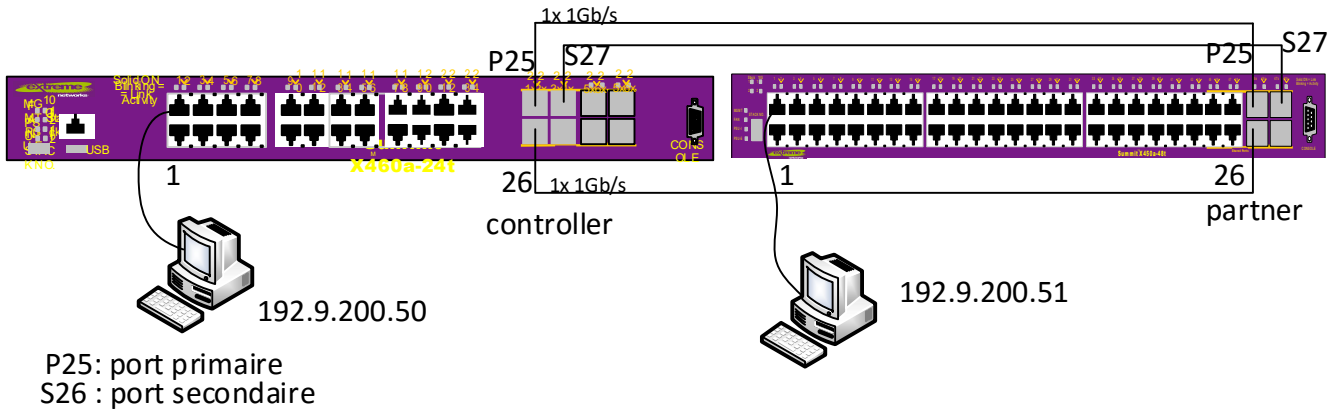
exemple pour créer un groupe à partir des ports 25 et 26 au niveau 2 en protocole LACP, on a la commande :

enable sharing 25 grouping 25,26 algorithm address-based L2 lacp

Le numéro du groupe correspondra toujours au numéro du premier port impair inscrit (ici 25).

Pour associer ce groupe à la boucle EAPS on utilisera les commandes suivantes :

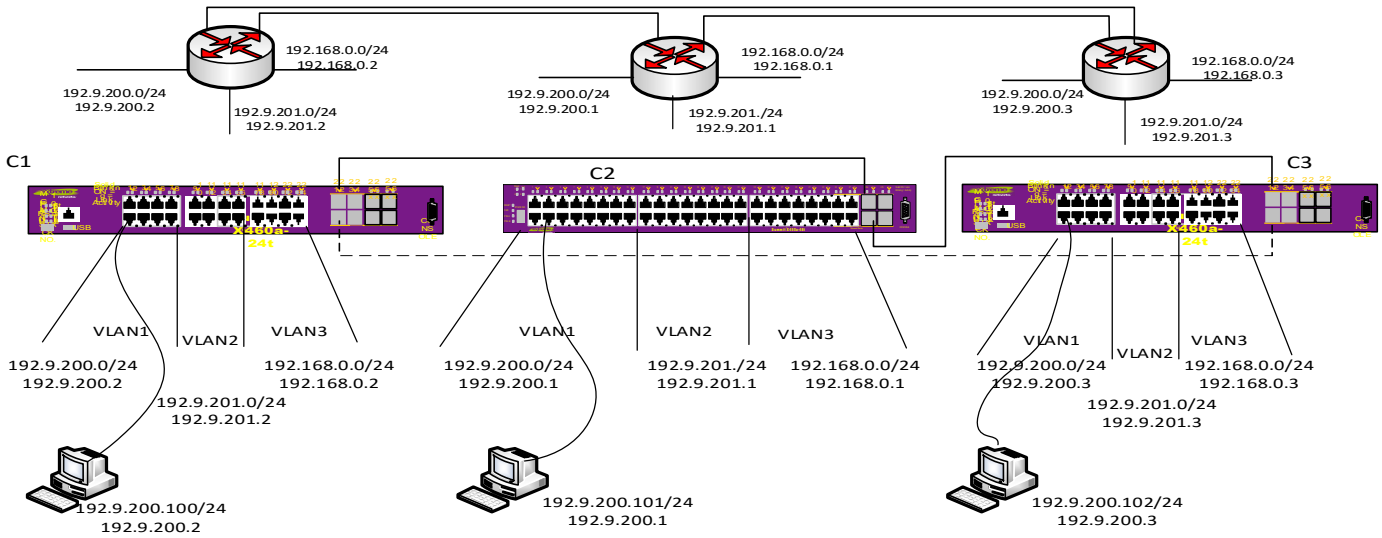
create eaps shared-port 25
configure eaps shared-port 25 mode partner
configure eaps shared-port 25 link-id 21



Un switche est configure en controller et l'autre en partner
Le numéro 21 est un numéro unique qui identifie le partage
Attention la license Core est nécessaire pour partager EAPS et agrégation de liens

7) La redondance des routeurs et le protocole VRRP

Le protocole VRRP va permettre de palier la défaillance d'un routeur primaire et de son interface passerelle en utilisant un routeur secondaire dit redondant. Ce routeur secondaire va mettre à disposition l' interface passerelle qui aurait dû disparaitre suite au disfonctionnement du routeur primaire. Prenons l'exemple suivant pour mieux comprendre ce mécanisme :



Les trois ordinateurs sont reliés à trois commutateurs différents. Chaque ordinateur a une adresse passerelle différente si une interface virtuelle vient à tomber on perd le VLAN.
Le protocole VRRP (Virtual Router Redundancy Protocol) va permettre de pallier ce problème, voici en quelques lignes son fonctionnement

Chaque commutateur possédant une interface sur le même réseau ou VLAN de niveau 3 est identifié par un numéro unique. Les VLAN sont configurés pour appartenir à un seul et même VRID, c'est-à-dire un « groupe VRRP ».

exemple la commande suivante pour le commutateur C2:

create vrrp vlan <nom du VLAN > **vrid** <numéro d'identification du vrrp>

qui nous donne :

create vrrp vlan VLAN1 vrid 1

Ce numéro ici 1 est unique pour le vlan VLAN1

Pour chaque commutateur ou routeur, on associe une priorité, le routeur ou commutateur ayant la plus haute priorité est élu maitre (routeur principal) les autres sont élus comme secondaires (standby). On peut définir pour le commutateur N°2 la priorité 255 pour le VLAN N°1

configure vrrp vlan VLAN1 vrid 1 priority 255

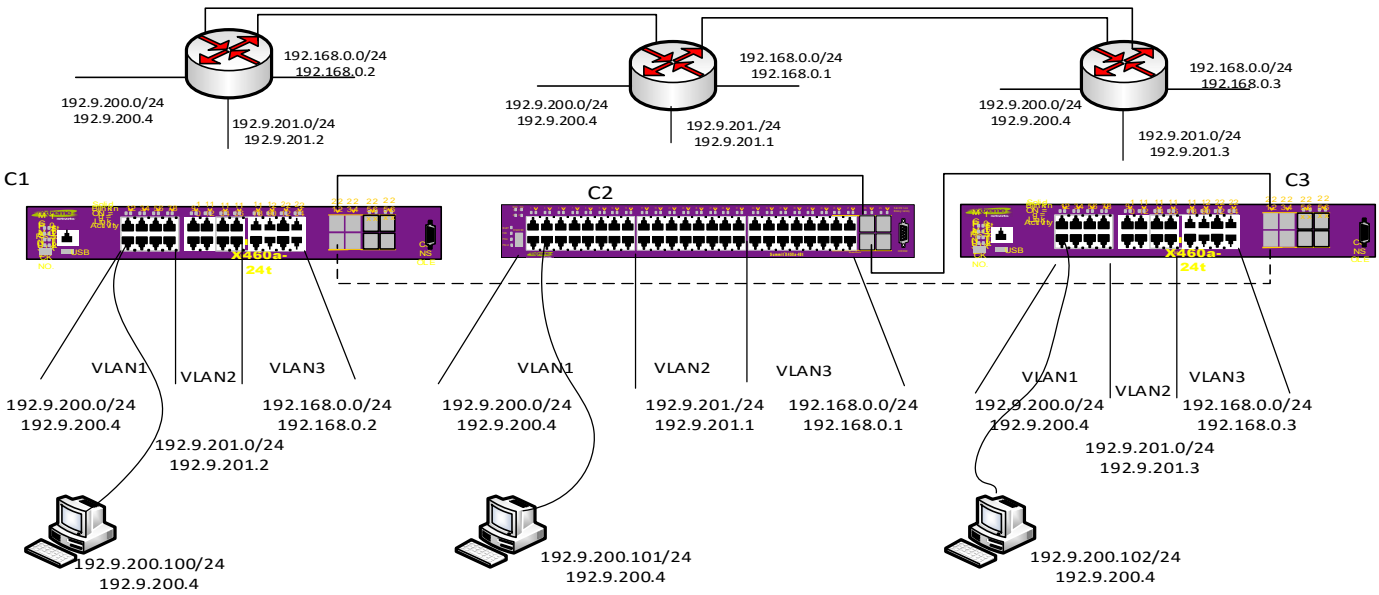
La priorité maximale est 255. Le commutateur N°2 est élu maitre ou principal pour le VLAN N°1. Les autres commutateurs C1 et C3 seront élus secondaires pour le VLAN N°1.

Une adresse IP de passerelle est attribuée pour chacun des VLANs, elle deviendra unique pour un VLAN sur tous les commutateurs.

configure vrrp vlan <nom du VLAN> **vrid** <numéro du vrid> **add** <adresse IP passerelle pour tous>

exemples
configure vrrp vlan VLAN1 vrid 1 add 192.9.200.4

En fait, cette IP est virtuelle et n'est donc qu'un « point » dans le réseau. C'est encore un routeur virtuel (ou logique si vous préférez), un « faux routeur qui n'existe pas physiquement mais seulement virtuellement.
Si les priorités changent (par exemple, lorsqu'un lien tombe, un service réduit la priorité du routeur), une élection a lieu à nouveau afin de désigner le commutateur Maitre ou principal.



La commande suivante autorise un commutateur à devenir maitre si sa priorité est supérieure à celle du maitre actuel, même si ce maitre fonctionne correctement.
Sans cette option, il y aura réélection si et seulement si le routeur maitre et son interface tombe.

configure vrrp vlan <numéro du VLAN> **vrid** <numéro du vrid> **preempt**

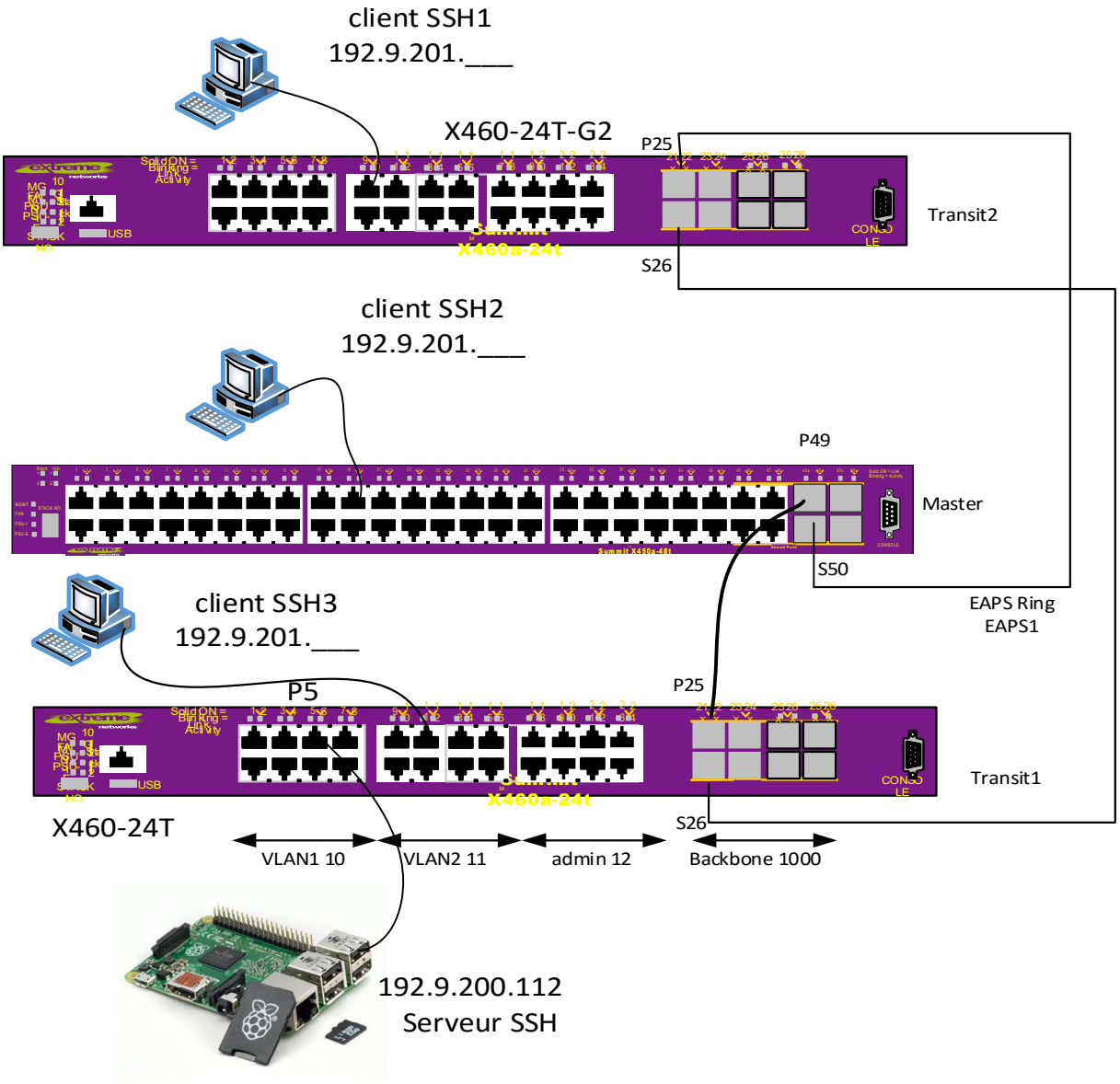
exemple :

configure vrrp vlan VLAN1 **vrid** 1 **preempt**

Dans le cas de VRRP, les commutateurs vont associer une adresse MAC particulière à l'adresse IP virtuelle sous la forme 00:00:5E:00:01:XX (où XX est le n° du groupe VRRP soit vrid).
Dés lors, pour le PC, quoi qu'il arrive, ce sera cette adresse MAC qui identifiera sa passerelle.
De leur côté les commutateurs dialoguent par multicast (224.0.0.18) afin de négocier et de savoir qui devra se charger de traiter la trame destinée à l'adresse MAC VRRP.

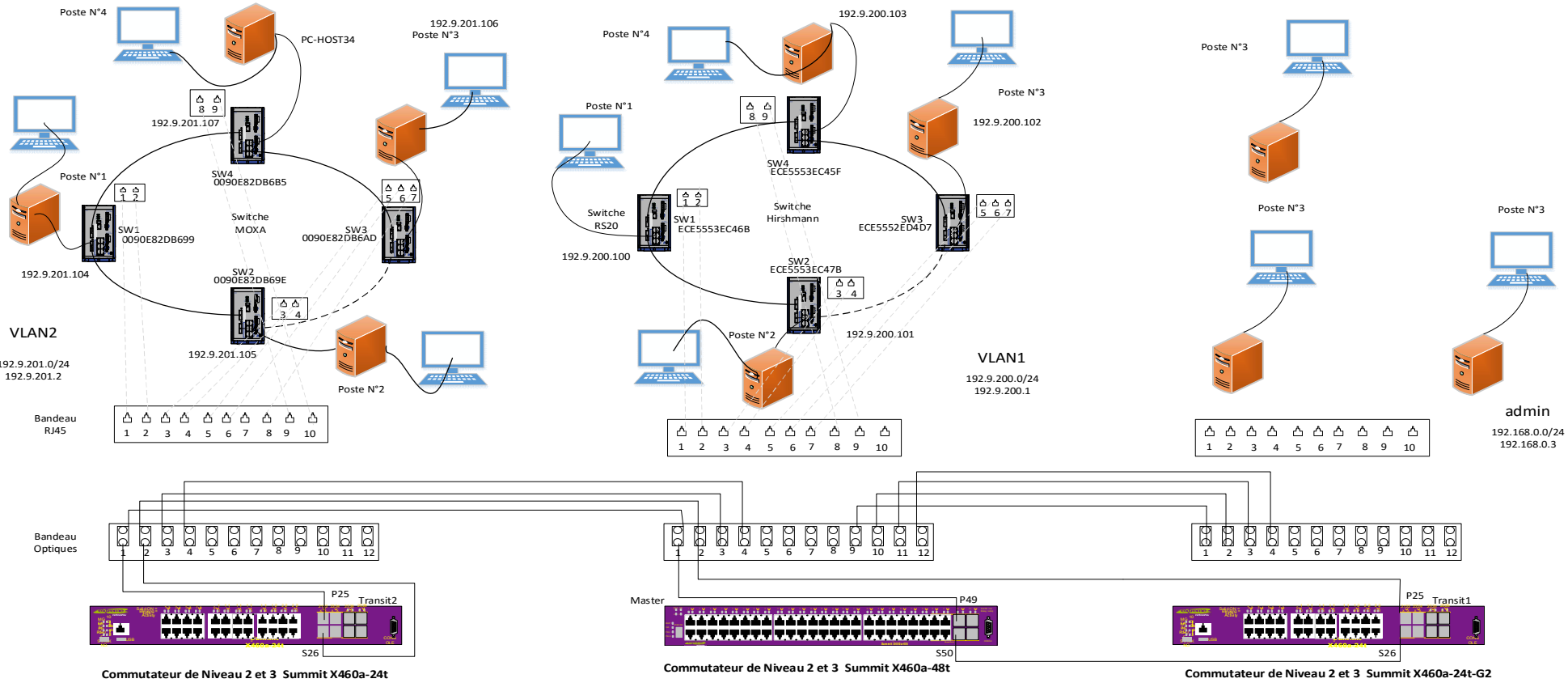
8) Mise en place d'une access list

On souhaite mettre en place une access List statique afin de filtrer le trafic SSH entre un ordinateur client SSH et une carte du type raspberry serveur SSH.



En vous aidant du dossier sur les lignes de commande (partie Access List), mettez en place ce filtrage afin de bloquer la communication entre un serveur et un client SSH. L'Access List sera créée sur le commutateur du client SSH.

La multidiffusion et sa propagation au niveau 3 du modèle OSI


Poste N°4
PC-HOST34
192.9.201.106
Poste N°3
192.9.201.107
Poste N°1
SW4
0090E82DB6B5
Switche
MOXA
SW1
0090E82DB699
SW3
0090E82DB6AD
192.9.201.104
SW2
0090E82DB69E
192.9.201.105
Poste N°2
VLAN2
192.9.201.0/24
192.9.201.2
Bandeau
RJ45
192.9.200.103
Poste N°4
Poste N°3
Poste N°1
192.9.200.102
SW4
ECE5553EC45F
Switche
RS20
SW1
ECE5553EC46B
Switche
Hirshmann
SW3
ECE5552ED4D7
192.9.200.100
SW2
ECE5553EC47B
192.9.200.101
Poste N°2
VLAN1
192.9.200.0/24
192.9.200.1
Poste N°3
Poste N°3
Poste N°3
admin
192.168.0.0/24
192.168.0.3
Bandeau
Optiques
P25
Transit2
S26
Commutateur de Niveau 2 et 3 Summit X460a-24t
Master
P49
S50
Commutateur de Niveau 2 et 3 Summit X460a-48t
P25
Transit1
S26
Commutateur de Niveau 2 et 3 Summit X460a-24t-G2