Les commandes en ligne du commutateur de niveau 2 et 3 summit X460e

- Démarrer +programme+accessoire +Communication + Hyperterminal:
  - oNom = nom du switch +OK
  - oPort Com = l + OK
  - oVitesse = 9600 bauds + Appliquer + *OK*
  - oMot de passe admin password aucun

Les commandes générales

* X460-24t # **unconfigure switch** (pour effacer la configuration effet immédiat)
* X460-24t # **save configuration** (sauvegarder la configuration)
* X460-24t # **reboot** (pour redémarrer)
* X460-24t# **show configuration** (visualiser la configuration du commutateur)
* X460-24t# **show ports** <numero du port> (visualiser la configuration du port)
* X460-24t# **show ports** <numero du port> info detail (avec plus d'information)
* X460-24t # **show switch** (visualiser la configuration du switche)
* X460-24t **#show license**
* X460-24t **#show version**
* X460-24t **#create account admin** cin (pour la création d'un compte admin)
* X460-24t **#show management** (pour voir les services ouverts au management)
* X460-24t **#enable ssh** (pour valider le service ssh)
* X460-24t **#configure vlan mgmt ipaddress** <ipaddress> <mask> (pour créer une interface pour le port de management attention prise RJ45 à part)

Les opérations de sauvegarde

Pour charger un nouvel IOS sur un poste serveur TFTP

* X460-24t # **download image** <ip> <filename> **vr** <vrname> {**pri**|**sec**}
Exemple: **download image 172.16.41.1 summitX-12.6.1.3.xos vr vr-default secondary**

Pour sélectionner l'IOS à charger au démarrage sur la partition primaire ou secondaire
* X460-24t # **use image** {**pri**|**sec**}
Exemple : use image secondary

Pour sélectionner le fichier de configuration à charger au démarrage sur la partition primaire ou secondaire

* X460-24t # **use configuration** {**pri**|**sec**}

use config primary

Pour sauvegarder le fichier de configuration

* X460-24t # **save configuration** (sauvegarder la configuration)

Pour télécharger un fichier de configuration à partir d'un serveur tftp

* X460-24t # **tftp get** <ip> **-vr** <vrname> <filename.cfg>
Exemple :
tftp get 192.9.200.53 vr VR-Default primary.cfg
Dites oui pour écraser le fichier primary.cfg (lors du reboot **dites non** lorsqu'il demande de sauvegarder la configuration config actuelle et non celle téléchargée).

Pour sauvegarder un fichier de configuration vers un serveur tftp

* X460-24t # **tftp put** <ip> <filename.cfg>
Exemple
tftp put 192.9.200.53 vr vr-default primary.cfg

On peut créer un VLAN de niveau 2 mais aussi un VLAN de niveau 3 qui nous permettra d'associer sur ce VLAN de niveau 3 une interface virtuelle

Création de VLAN (Virtual Local Area Network) :

- X460-24t # **config vlan default delete port all** (effacer les ports sur un VLAN)
- * X460-24t # **create vlan** <name>
  * X460-24t # **config vlan** <name> **tag** <numero>
- * X460-24t# **config vlan** <name> **add port** <numero> **untagged**
- * X460-24t# **config vlan** <name> **add port** <numero> **tagged**

Exemple :
* X460-24t# config vlan cin1 add port 10,11 untagged

Création d'une interface virtuelle sur un VLAN de niveau 3

- X460-24t# **configure vlan** <name> **ipaddress** <ipadress> <netmask>

Association d'une interface virtuelle au VLAN

* X460-24t# configure vlan cin2 ipaddress 10.0.0.1 255.0.0.0

- * X460-24t# **enable ipforwarding vlan** <name> (valide la commutation niveau 3)

Pour effacer une interface virtuelle

* X460-24t# **unconfigure vlan** <name> **ipaddress**(désactive la commutation niveau 3)

Suppression d'un VLAN :

- * X460-24t # **delete vlan** <name> (pour effacer un VLAN)

Configuration du Routage:

Il faut au préalable créer une interface virtuelle vers un VLAN de niveau 3 vues précédemment

* X460-24t # **configure vlan** <name> **ipaddress** <@IP> <Netmask>

* X460-24t # configure vlan cin1 ipaddress 192.9.200.1 255.255.255.0

* X460-24t # **enable ipforwarding vlan** <name> (activer la commutation au niveau 3)

- Routage dynamique :

- * X460-24t#**configure rip add vlan** <name>
- * X460-24t **#enable rip**
- * X460-24t **#show rip**
- * X460-24t **#show rip interface**
- * X460-24t **#show rip interface vlan** <name>

- **Port mirroring :**

Le port mirroring est très utile il permet de faire une image du flux binaire qui arrive sur un port et de renvoyer cette image (miroir) vers un autre port

Port-mirroring sur port(s) source.

- * X460-24t # **enable mirroring to port** <numero 1> (port numero1 récupère le flux binaire montant et sortant du port numero2)

  On définit le port source dont le trafic sera copié :

- * X460-24t# **config mirroring add port** <numero2> (port numero 2 est miroir le vlan est supprimé sur le port numero2)

On peut faire du port mirroring sur un VLAN entier :

config mirroring add vlan <name>

L'agrégation de liens au niveau 2

Validation de l'agrégation de lien dynamique

***** X460-24t **# enable sharing** <numero_group> **grouping** <portlist> **algorithm address-based L2 lacp**

Exemple: enable sharing 5 grouping 5,6 algorithm address-based L2 lacp

Le numéro du groupe correspondra toujours au numéro du premier port impair inscrit (ici 5)

La désignation <port> ou LAG (Link agregation group) représente un port logique qui contient un groupe de port entier <portlist>. Le premier port dans le groupe <portlist> est configuré comme étant le port logique.

Pour vérifier l'agrégation de lien

***** X460-24t **#show lacp**
***** X460-24t **#show lacp lag** <port>

Pour désactiver l'agrégation de lien

***** X460-24t **#disable sharing** <port>
***** X460-24t **#configure sharing** <port> **delete ports** <portlist>
***** X460-24t **#clear lacp counters**

Sécuriser un port sur le commutateur grâce au FDB

Pour des raisons de sécurité il est possible de sécuriser c'est-à-dire associer une ou plusieurs adresses MAC possibles à un port.
Sur les commutateurs Extreme network la gestion des ports se fait grâce à une base de données d'acheminement appelée FDB (forwarding database).

Pour associer une adresse MAC à un port dans un premier temps, il faut créer une ligne dans la FDB :

* X460-24t **#create fdbentry** <mac_addr> **vlan** <vlan_name> **ports** <portlist>

Exemple :

Create fdbentry 00:01:02:03:04:05 vlan cin port 3,4

Dans un deuxième temps il faut désactiver l'apprentissage de l'adresse MAC sur un port:

* X460-24t # **Configure port** <portlist> **vlan** <vlan_name> **limit-learning** <number> **action stop-learning**

Exemple:

Configure port 3,4 vlan cin limit-learning 0 action stop-learning

Pour vérifier le résultat dans la base de données FDB:

* X460-24t **#show fdb**

Pour effacer une adresse MAC associé à un port dans la FDB

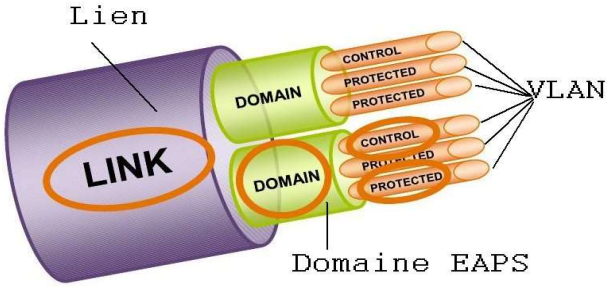
* X460-24t **#delete fdbentry** <mac_addr> **vlan** <vlan_name>

Pour effacer la désactivation de l'apprentissage de l'adresse MAC sur un port:

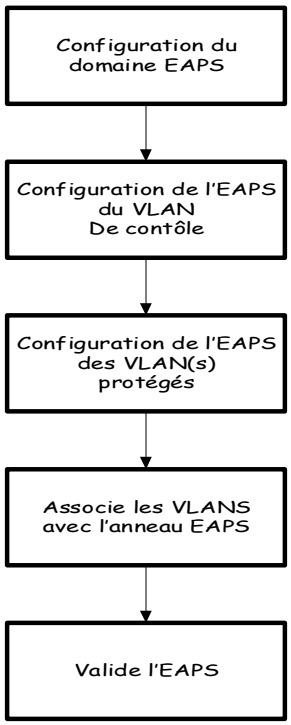
* X460-24t # **Configure port** <portlist> **vlan** <vlan_name> **unlimited-learning**

Configuration de la redondance de lien par le protocole EAPS

Le protocole EAPS (Ethernet automatic protocol switching) est constitué d'un anneau de paire de fibre optique. Ce protocole va permettre de faire passer sur un lien de pair de fibre optique plusieurs domaines EAPS. Chaque domaine EAPS dispose d'un VLAN de contrôle pour faire passer les informations de signalisation (Traffic de contrôle de l'EAPS) et d'un ou plusieurs VLAN protégés.



Tout le trafic sur la fibre optique issu des VLAN contrôle ou protégé doit être tagués.
Aucun Traffic utilisateur ne doit passer par le VLAN de contrôle.
Un Vlan de contrôle ne peut être assigné à une adresse IP.
La mise place d'une boucle EAPS s'effectue en quatre étapes :



Configuration du VLAN de contrôle

Si le VLAN de contrôle n'a pas été créé auparavant

Création du VLAN

* X460-24t # **create vlan** <name_control>

Assigne un tag au VLAN

* X460-24t # **config vlan** <name_control> **tag** <numero>

Additionne un port primaire et secondaire au VLAN de contrôle

X460-24t # **configure vlan** <name_control> **add port** <primary_port> **tagged**
* X460-24t # **configure vlan** <name_control> **add port** <secondary_port> **tagged**

Configuration d'un anneau EAPS

Création d'un domaine EAPS sur un switche

* X460-24t **#create EAPS** <name_domain>

Configuration d'un switche dans le mode maître EAPS

* X460-24t **#configure EAPS** <name_domain> **mode master**

Configuration d'un switche dans le mode transit EAPS

* X460-24t **#configure EAPS** <name_domain> **mode transit**

Configuration des ports primaires et secondaires de l'anneau

* X460-24t # **configure EAPS** <name_domain> **primary port** <port number >
* X460-24t # **configure EAPS** <name_domain> **secondary port** <port number >

Configuration du ou des VLANS protégés

Si les VLANS n'ont pas été créés auparavant

Création du VLAN

** X460-24t # **create vlan** <name_protected>*

Assigne un tag au VLAN

** X460-24t # **config vlan** <name_protected> **tag** <numero>*

Additionne un port primaire et secondaire au VLAN protégé (toujours taggé)

***** X460-24t # **configure vlan** <name_protected> **add port** <primary_port> **tagged**

***** X460-24t# **configure vlan** <name_protected> **add port** <secondary_port> **tagged**

Association des VLAN à l'anneau EAPS

Additionne un VLAN de contrôle à l'anneau EAPS

***** X460-24t **#configure EAPS** <name_domain> **add control vlan** <name_vlan_contrôle>

Additionne un VLAN protégé à l'anneau EAPS

***** X460-24t **#configure EAPS** <name_domain> **add protect vlan** <name_vlan_protégé>

Validation de l'EAPS

***** X460-24t **#enable eaps**
***** X460-24t **#enable eaps** <name_domain>

Pour voir la configuration EAPS du commutateur

***** X460-24t **#show eaps**
***** X460-24t **#show eaps** <name_domain>

Désactiver effacer et renommer des domaines EAPS

* X460-24t **#disable eaps** <name_domain>
* X460-24t **#delete eaps** <name_domain>
* X460-24t **#unconfigure eaps** <name_domain> **primary|secondary port**
* X460-24t **#configure eaps** <name_domain> **name** <new_name_domain>

Configuration du protocole de redondance de lien spanning tree STP ou PVST+

Pour la mise en place du protocole de redondance PVST+, on doit associer pour chaque VLAN que l'on souhaite propager un domaine STP. La création du domaine STP est donnée ci-dessous

On Spécifie un nouveau domaine STP

create stpd <*stpd_name*>

On doit après configurer le mode opérationnel pour le domaine STP spécifié

dot1d pour la norme 802.1d
dot1q pour la nome 802.1w

configure stpd <*stpd_name*> **mode** dot1w

La commande qui suit spécifie la priorité du domaine STP (de 0 à 61440 par pas de 4096)
Cette commande très utile pour désigner un commutateur racine via son BID. On rappelle que le commutateur dont le BID est le plus faible est élu commutateur racine

configure stpd <*stpd_name*> **priority** <value_priority>

On Configure après le mode d'encapsulation par défaut pour tous les ports associés aux domaines

configure stpd <*stpd_name*> **default-encapsulation pvst-plus**

stpd_name	Specifies an STPD name on the switch.
dot1d	Specifies the STP encapsulation mode of operation to be 802.1d.
emistp	Specifies the STP encapsulation mode of operation to be EMISTP.
pvst-plus	Specifies the STP encapsulation mode of operation to be PVST+.

On Additionne un ou des ports d'un VLAN dans un domaine STP spécifié

configure stpd <*stpd_name*> **add vlan** <Vlan_name> **ports** <port_number> **pvst-plus**

(on ne peut pas additionner les ports untagged et les ports en SRP)

On Spécifie la priorité du port dans le domaine STP spécifié (gamme de 0 à 31 pour STP)

configure stpd <*stpd_name*> **ports port-priority** <value_priority> <port_number>

On spécifie le cout du chemin dans le domaine STP spécifié **gamme de 1 à 200 000 000**

configure stpd <*stpd_name*> **ports cost** <value_cost> <port_number>

Le choix du cout va permettre de choisir les ports racines sur chaque commutateur

On Assigne un STP id à un domaine STP. En PVST+ l'identifiant STP doit correspondre au numéro de VLAN associé au domaine STP

configure stpd <*stpd_name***> tag** <numbers_vlan>

On valide au final le domaine STPD
enable stpd <*stpd_name***>**

La visualisation des informations sur le domaine STP peut s'effectuer par les trois commandes suivantes :

show stp
show stp <*stpd_name***>**
show <*stpd_name***> ports**

attention aux liens de secours associés au protocole PVST+(risque de boucle)

SRP (soft redondancy protocol) pour éviter les boucles dans le cas du SRP port redondant
configure stpd s1 mode dot1w
enable stpd s0 auto-bind vlan Default
configure stpd s1 add vlan v1 ports 9 emistp
configure stpd s1 ports mode emistp 9
configure stpd s1 ports cost auto 9
configure stpd s1 ports port-priority 128 9 /range 0 à 240 increment de 16
configure stpd s1 ports link-type edge 9
configure stpd s1 ports edge-safeguard enable 9 recovery-timeout 400
configure stpd s1 ports bpdu-restrict enable 9 recovery-timeout 400
enable stpd s1 ports 9
configure stpd s1 tag 10
enable stpd s1

edge

Spécifie un port qui n'a pas un pont attaché. Un port edge est placé et maintenu dans l'état STP forwarding tant qu'un BPDU est reçu par le port.

Pour détecter les boucles sur un port

enable elrp-client
configure elrp-client one-shot default ports 1,2 print

Cette commande s'applique à un port qui a été configuré comme un port edge. La prévention et la détection des boucles sur un port edge est configuré pour RSTP.

This command applies only to ports that have already been configured as edge ports.
Loop prevention and detection on an edge port configured for RSTP or MSTP is called edge safeguard.
You configure edge safeguard on RSTP or MSTP edge ports to prevent accidental or deliberate misconfigurations (loops) resulting from connecting two edge ports together or by connecting a hub or other non-STP switch to an edge port. Edge safeguard also limits the impact of broadcast storms that might occur on edge ports.
An edge port configured with edge safeguard immediately enters the forwarding state and transmits BPDUs. This advanced loop prevention mechanism improves network resiliency but does not interfere with the rapid convergence of edge ports.
Recovery time starts as soon as the port becomes disabled. If no recovery-timeout is specified, the port is permanently disabled.

Configuration d'un lien de secours contrôlé logiciellement

Le protocole SRP (software redundant protocol) permet de créer un port redondant contrôlé logiciellement.
Un port redondant contrôlé logiciellement est configuré afin d'associer un chemin de secours à un port primaire (les ports doivent être sur le même système). Le port redondant surveille l'état du lien du port primaire et si ce lien tombe, le port redondant établie un nouveau lien qui devient actif. Tu configures le lien redondant de façon à ce qu'il soit toujours monté mais logiquement bloqué. Tu peux seulement associer un seul port redondant à un port primaire. Le port primaire et le port secondaire doivent avoir les mêmes VLAN.

configure ports <*primaryPort*> **redundant** <*secondaryPort*> {**link** [**on** | **off**]}

Le premier port doit spécifier le port primaire. Le second port spécifie le port redondant.

primaryPort	Specifies one primary port or slot and port.
redundantPort *secondaryPort*	Specifies one or redundant port or slot and port.
link	Specifies state of link: on—Specifies keeping the redundant port active, but block trafficoff—Specifies forcing the link down on the redundant port  Note The default value is off.

Si link est on le traffic de niveau 2 circule mais le traffic vlan est coupé pendant le blocage
Si link est off le traffic est complétement coupé pendant le blocage

Pour visualiser la redondance de port

show ports redundant

Pour désactiver la redondance de port

unconfigure ports 3 **redundant**

Les ACCESS LIST (ACL)

Les listes d'accès (access list) sont des instructions qui expriment une liste de règle, imposée par l'opérateur, donnant un contrôle supplémentaire sur les paquets reçus et transmis par le commutateur.
Les listes d'accès sont capables d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie vers une destination.
Les listes de contrôle d'accès (ACL) IP permettent donc de filtrer le trafic sur le réseau. Les ACL peuvent être appliqués sur les paquets entrants ou sortants du commutateur.
Une ACL est un ensemble de règle qui définit une action spécifique sur les paquets entrants ou sortants

Ils existent deux types d'ACL :

- Les ACLs statiques qui sont créées à partir d'un fichier séparé (policy)
- Les ACLs dynamiques qui sont créées directement par une ligne de commande

Les ACLS statiques

La syntaxe du langage utilisée (script shell) pour définir un ensemble de règle ne sera pas abordée durant ce TP.
Pour créer le fichier comportant les règles de filtrage on utilisera l'éditeur vi implanté sur le switche

Création d'un fichier pour les ACL

* X460-24t.4 **#edit policy** <nom du fichier>

Exemple :

edit policy denyserveurweb

Ce fichier aura par la suite comme extension .pol

Vous rentrez sous l'emblématique éditeur vi de LINUX. La lettre s sous vi permet de passer en mode édition. Pour sortir du mode édition tapez sur la touche echap puis :wq

Exemple de fichier d'ACL

```
entry noweb{
if{
destination-address 192.9.200.112/24;
source-address 192.9.201.53/24;
protocol tcp;
destination-port 80;
}
then{
deny;
}
}
```

Vérification de la syntaxe des ACL du fichier

* X460-24t.4 **#check policy** <nom du fichier >

Appliquez la ou les règles à un VLAN

* X460-24t.4 **#configure access-list** <nom du fichier> **vlan** <nom du VLAN>

Pour visualiser les access list en cours

* X460-24t.4 **#show policy**

Pour visualiser les access list du fichier

* X460-24t.4 **#show policy** <nom du fichier >

Pour visualiser toutes les access list

* X460-24t.4 **#show access-list**

Pour supprimer une ACCESS LIST

* X460-24t.4 **#unconfigure access-list** <nom du fichier >