Configuration des Switchs
VLAN & IEEE 802.1d, q et x
sur
Catalyst 2950 CISCO

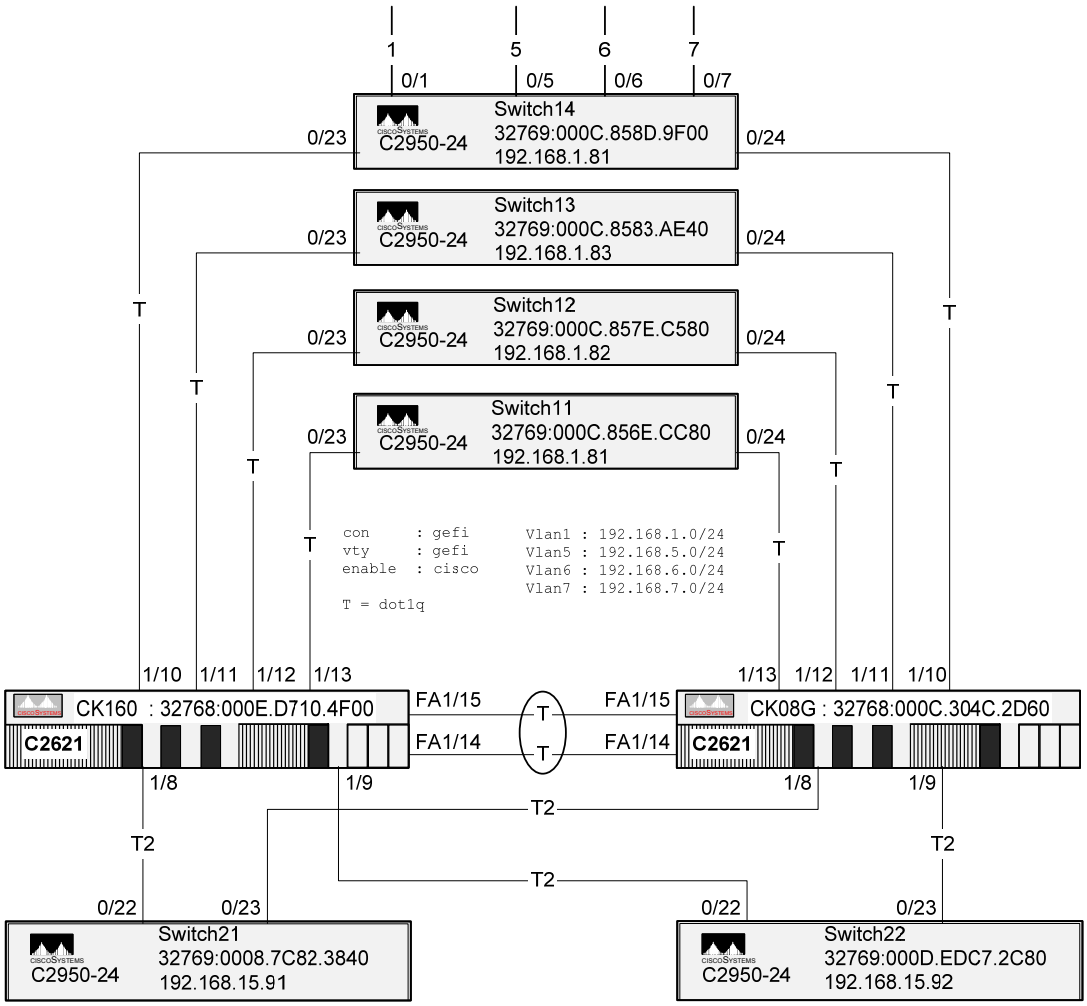


Table des matières

I. OBJECTIFS DU COURS 1

II. RAPPEL DES ACQUIS 2

II.A LE TRANSPARENT BRIDGING 2
II.B LES SWITCHS OU COMMUTATEURS 3
II.B.1 Présentation 3
II.B.2 Modes de commutation 4
II.B.3 Fonctionnement 4
II.B.4 Caractéristiques 5
II.B.5 Intérêts des VLAN 5
II.C IP : INTERNET PROTOCOL 6
II.D LA SEGMENTATION D'UN RESEAU 8
II.D.1 Par Switch 8
II.D.2 Par Routeur 8
II.E SYNTHÈSE 8

III. PRÉSENTATION DES SWITCHS CISCO 10

III.A PRÉSENTATION 10
III.B CATALYST 2900 11
III.C CATALYST 2950 12
III.D CATALYST 3500 13
III.E CATALYST 5000 14
III.F CATALYST 6000 14
III.G CATALYST 2900 15
III.G.1 Catalyst 2900 Series XL Switches 15
III.G.2 Catalyst 2950 Series Switches 15
III.G.3 Description 16
III.H CISCO 2621 17
III.H.1 Connexion au Port Console 18
III.I LE BOUTON MODE 19
III.I.1 Stat 20
III.I.2 UTL 20
III.J POWERING ON THE SWITCH AND RUNNING POST 21

IV. PROCEDURE DE CONFIGURATION PAR CLI 22

IV.A LE CLI 22
IV.B LES MODES DE CONFIGURATION 22
IV.C SVI : SWITCH VIRTUAL INTERFACE 23
IV.D AFFECTATION D'UN PORT 24
IV.E POUR CONNECTER UN ORDINATEUR A UN PORT 25
IV.F CONFIGURATION IP 26
IV.G LES MOTS DE PASSE 27
IV.H GESTION DES ADRESSES MAC 29
IV.I APPLICATION 30
IV.I.1 Block Switch 1 30
IV.I.2 Block Switch 2 31
IV.I.3 Configuration Type 32

V. LE SPANNING TREE PROTOCOL 33

V.A PRESENTATION 33
V.B PROBLEMES DES BOUCLES 34
V.C OPTIMISATION 34
V.D PONTAGE VS COMMUTATION 35
V.E HALF-SUPLEX VS FULL-DUPLEX 35
V.F STP TIEBREAKERS 35
V.G DESCRIPTION DE FONCTIONNEMENT 36
V.H PARAMETRES DE FONCTIONNEMENT 37
V.I FORMAT DES BPDU 38
V.J ELECTION DU ROOT BRIDGE 40
V.K CALCUL DU ROOT PATH COST 41
V.L ÉLECTION DU ROOT PORT 42
V.M ÉLECTION DU DESIGNATED PORT 43
V.N LES BOUCLES DE NIVEAU DEUX SONT SUPPRIMEES 45
V.O SYNTHESE 46
V.P EXERCICES 47
V.Q ÉTAT DES PORTS EN STP 48
V.R ÉTUDE DE CAS 50
V.S RECALCUL DE L'ARBRE SPANNING TREE 55
V.T RÉSUMÉ 56
V.U ACTION DU 'PORT COST' 58
V.V ROOT SWITCH & SECONDARY ROOT SWITCH 61
V.W CONFIGURATION 62
V.W.1 Présentation 62
V.W.2 Les commandes 63
V.W.3 Exemple 64
V.X APPLICATION DU STP 65
V.X.1 Application 1 65
V.X.2 Application 2 66
V.X.2.a Block Switch 1 66
V.X.2.b Block Switch 2 67
V.X.3 Application 3 68
V.X.3.a Block Switch 1 68
V.X.3.b Block Switch 2 69

VI. LES VLANS 70

VI.A PRESENTATION 70
VI.B TRANSPORT DES VLANS OU TRUNK 72
VI.B.1 Présentation 72
VI.B.2 ISL 73
VI.B.3 IEEE 802.1Q ou Dot1q 74
VI.C INTERCONNEXION 75
VI.D CONFIGURATION 76
VI.D.1 Déclaration des VLAN 76
VI.D.2 Le port en mode Multi-VLAN 77
VI.D.3 Le port en mode TRUNK 78
VI.D.4 Creating EtherChannel Port Groups 79
VI.D.5 Application 80
VI.E APPLICATION 82
VI.E.1 Block Switch 1 82
VI.E.2 Block Switch 2 83
VI.F OBSERVATIONS 84

VII. LE ROUTAGE INTER VLAN 85

VII.A PAR ROUTEUR INDEPENDANT 85
VII.B PAR UN COMMUTATEUR DE NIVEAU 3 86
VII.B.1 Méthodes 86
VII.B.2 Commandes 86

VII.C APPLICATION 1 87
VII.C.1 Block Switch 1 ..... *87*
VII.C.2 Block Switch 2 ..... *88*
VII.D APPLICATION 2 89

VIII. SPAN & RSPAN 91

VIII.A SPAN 91
VIII.A.1 Catalyst 2900 ..... *91*
VIII.A.2 Catalyst 2950 ..... *92*
VIII.B RSPAN 93
VIII.B.1 Création de la session source *93*
VIII.B.2 Création de la session destination *93*

IX. LE VTP 94

IX.A FONCTIONNEMENT 94
IX.B VTP MODES AND MODE TRANSITIONS 95
IX.C CONFIGURATION SUR C2900 & C3500 SERIES 96
IX.C.1 Les commandes *96*
IX.C.2 Configuration VTP serveur *97*
IX.C.3 Ajout d'un VLAN *97*
IX.C.4 Visualisation d'un Vlan *97*
IX.C.5 Configuration VTP Client *98*
IX.D CONFIGURATION CATALYST 5000 SERIES 98
IX.D.1 Configuration VTP serveur *98*
IX.D.2 Configuration VTP client *98*

X. CDP 99

X.A PRESENTATION 99
X.B LES COMMANDES 99

XI. CVMS 101

XII. LE CLUSTER 102

XII.A CRÉATION 102

XIII. IEEE 802.1X 103

XIII.A PRESENTATION DE L'AUTHENTIFICATION 802.1X 103
XIII.B RADIUS 104
XIII.B.1 Présentation *104*
XIII.B.2 Présentation de Freeradius *105*
XIII.B.3 Configuration de Freeradius *106*
XIII.B.3.a /etc/raddb/radiusd.conf 106
XIII.B.3.b /etc/raddb/clients.conf 107
XIII.B.3.c /etc/raddb/users 107
XIII.C CISCO 109
XIII.C.1 Configuration Guidelines *109*
XIII.C.2 Enabling 802.1X Authentication *110*
XIII.C.3 Configuring the Switch-to-RADIUS-Server Communication *112*
XIII.D EAP MD5-CHALLENGE 114
XIII.D.1 Configure the Catalyst for 802.1x *114*
XIII.D.2 Freeradius *117*
XIII.D.3 Windows XP Pro *118*
XIII.D.3.a Configuration de l'interface réseau. 118
XIII.D.3.b Verify the 802.1x Operation 119
XIII.D.3.c Vérification : après connexion au port FA0/7 du switch. 121

XIV. EXERCICE DE SYNTHÈSE 122

ANNEXE A. BRIDGE ID, SWITCH PRIORITY, AND EXTENDED SYSTEM ID 124

ANNEXE B. ICMP 125

ANNEXE C. MISE A JOUR D'IOS 126

ANNEXE D. PASSWORD RECOVERY PROCEDURE 128

ANNEXE E. CORRECTION 129

ANNEXE F. MPLS 130

F.I PRESENTATION 130
F.II TERMINOLOGIE 130

ANNEXE G. MLS 131

G.I TERMINOLOGY 131
G.II INTRODUCTION TO MLS 131
G.III KEY MLS FEATURES 132
G.IV MLS IMPLEMENTATION 133
G.V CONFIGURING MLS ON A ROUTER 135
G.VI MONITORING MLS 136
G.VII MONITORING MLS FOR AN INTERFACE 137
G.VIII MONITORING MLS INTERFACES FOR VTP DOMAINS 137

ANNEXE H. SNMP 138

ANNEXE I. ALGORITHME DE IP 139

ANNEXE J. *CONSOLE PORT SIGNALS AND PINOUTS* 140

ANNEXE K. GLOSSAIRE 141

ANNEXE L. BIBLIOGRAPHIE CISCO 142

I. Objectifs du cours

- **Mise en pratique des cours :**
  - Concepts et technologies des réseaux
  - Les réseaux locaux : *Ethernet & Transparent Bridging*
  - TCP/IP : *Adressage IP & Routage*
  - Interconnexion des réseaux (ITR1)

- **Installation, utilisation et**

- **Configuration d'équipements CISCO : Switchs Catalyst 2950 & Routeurs C2621**
  - Le Spanning Tree : IEEE 802.1D
  - Les VLANs : IEEE 802.1Q
  - Authentification : IEEE 802.1X

- **Configuration de commutateurs de niveau 3**
  - Routage inter VLAN

- **Méthode de dépannage**

Planning	1° jour	2° jour	3° jour	4° jour	5° jour
Matin	Présentation du cours & Rappel des acquis	Installation matériel & Configuration initiale	Spanning Tree (Mise en oeuvre)	Les VLAN (Mise en oeuvre)	802.1X & Synthèse
Après-midi	Présentation des Switchs & Procédures de configuration	Spanning Tree (théorie)	Les VLAN (théorie)	Routage inter VLAN & Analyse de trames	Test d'évaluation

II. Rappel des acquis

II.A Le Transparent Bridging

- les ponts et switchs Ethernet fonctionnent en '*Transparent Bridging*' :
  - par auto apprentissage (*Self Learning Process*) des addresses MAC,
  - les stations (stations de travail, serveurs, routeurs, etc.) en communication ignorent que leurs trames sont pontées.

- Les interfaces fonctionnant en mode '*Promiscuous*' (sans discrimination), un pont reçoit tout le trafic émis par les machines environnantes. Lorsqu'un équipement réseau émet, sa trame est capturée par le pont qui réalise les actions suivantes :
  - Il mémorise l'adresse MAC …
  - Puis il scrute sa FDB (*Forwarding Data Base*) pour vérifier la présence de l'adresse MAC …
    - Si l'adresse MAC Destination est …
    - Sinon
  - Il réarme le '`Aging-Time`', si l'adresse MAC Source existe déjà : durée de vie d'une adresse MAC dans la FDB. La valeur prédéfinie entre 10 secondes et 11 ans (par défaut 300 secondes).
  - Il inonde les réseaux à la réception d'une trame en broadcast.

- Les Broadcast physiques : trames ayant une adresse de Broadcast dans le champ adresse MAC destination.
  - Effet sur le réseau :
  - Effet sur les systèmes :

- Le Spanning Tree Protocol ou IEEE802.1d
  - Évite les boucles de niveau __ dans une architecture _____.

II.B Les Switchs ou Commutateurs

II.B.1 Présentation

- C'est un **concentrateur commutateur** de niveau 2 qui dirige directement le message vers le destinataire.

- Il fonctionne comme un pont, par auto apprentissage des adresses MAC sur ses ports.
  - Au départ, les tables du Switch sont vides.
  - Le Switch apprend l'adresse MAC de la machine source connectée à son port, lorsque celle-ci émet une trame.
  - Puis le Switch recherche dans ses tables l'adresse MAC destination, si l'adresse existe une seule trame sera émise à destination du poste destinataire, sinon la trame sera émise sur tous les autres ports.
  - Lorsqu'un Switch reçoit une trame en Broadcast ou en Multicast, il **inondera** le réseau de cette trame.

- Les Switchs ne filtrants pas les diffusions générales (Broadcast) et les diffusions restreintes à des groupes (Multicast), ils provoquent dans les réseaux modernes des tempêtes de diffusion ou **'Broadcast Storm'**.

- Inconvénients :
  - Sur les grands réseaux, les Switchs (comme les ponts) **laissent passer** les ***'Broadcasts physiques'***, ce qui peut générer des ***'Broadcast Storm***'. Les 'Broadcasts' détériorent les performances des systèmes (ordinateurs) en consommant du temps CPU pour désencapsuler les messages. Pour éviter cet inconvénient, il faut segmenter le réseau par des routeurs.
  - Et ils introduisent des temps de latence (temps d'exécution du pontage).
  - Comme les Switchs fonctionnent en Transparent Bridging, il y a obligation de mettre en œuvre le STP (*Spanning Tree Protocol*) lors d'architecture redondante de niveau deux.

- Avantages :
  - Les Switchs Ethernet (`Transparent Bridging`) **bloquent** les **collisions**, ce qui permet d'améliorer débit réel.
  - Les Switchs évitent les collisions, ce qui supprime le domaine de collision donc le RTD (`Round Trip Delay`), ainsi on peut réaliser des architectures MAN avec la technologie Ethernet.
  - Ils permettent également la mise en œuvre du Full Duplex pour améliorer encore le débit effectif du réseau.

II.B.2 Modes de commutation

- Le **'Store and Forward'**, commutation différée, dispose d'une mémoire tampon (buffer) qui lui permet de stocker le message entier, d'en vérifier l'intégrité (CRC) ou non, puis de l'envoyer vers son destinataire.

- Le **'Cut Through'**, commutation directe, ne dispose pas de mémoire tampon et commute le message à la volée dés réception de l'adresse MAC de destination et est donc plus rapide mais moins sécurisant. Cela ne permet pas au Switch de supprimer une trame avec une erreur de CRC.

- Le **'Fragment Free'**, commutation sans fragment, comme le 'Cut Through' la commutation est réalisée à la volée mais après les 512 premiers bits ce qui évite de transmettre les trames erronées par une collision.

- Les Switchs ont deux modes d'utilisation :
  - ***'Port Switching'*** : un port ⇒ une machine (un serveur par exemple).
  - ***'Segment Switching'*** : un port ⇒ un réseau (un HUB ou un autre SWITCH par exemple).

II.B.3 Fonctionnement

TB : Transparent Bridging

- Les réseaux **Ethernet utilisent des ponts fonctionnant en Transparent Bridging**.
- Les Switchs ou concentrateurs commutateur utilisés en 10BaseT, 100BaseTx ou 1000BaseT se conforment à la norme IEEE 802.1d (Spanning Tree).

- Le pont maintient une base de données pour commuter les trames : '`Forwarding Data Base`' ou FDB.
- Cette table se remplit par auto apprentissage (`Self Learning`). La connaissance de la position des machines est réalisée par le mode de fonctionnement 'promiscuous' des ponts, ils prennent copie de toutes les trames circulant sur les réseaux.
  - A la mise sous tension la table FDB est vide.
  - A la réception d'une trame, l'adresse MAC source et le port sur lequel le paquet a été reçu, sont mémorisés dans la FDB.
  - Pour chaque trame reçue, le pont recherche dans sa FDB (*Forwarding Data Base*) l'adresse MAC Destination :
    - Si l'adresse MAC de destination est connue, le pont émet la trame sur le port spécifié dans la FDB.
    - Si l'adresse MAC de destination est inconnue, le pont émet la trame sur tous les autres ports (mécanisme de ***flooding***/inondation).

- Par son mode de fonctionnement (TB) le switch a obligation de propager (inondation) les trames en Broadcast.

- La table comporte également pour chaque entrée, la date et l'heure du dernier accès (*Aging-Time*). Ce time-out permet de supprimer les entrées qui ne sont plus utilisées (par défaut 15 minutes) pour éviter d'encombrer inutilement la mémoire et le processeur du switch.

II.B.4 Caractéristiques

- Meilleur accès au média
  - Bande Passante dédiée (le trafic est dirigé directement vers la station spécifiée),
  - Moins de conflits d'accès, si le FDX est actif il n'y a plus de collisions
  - Les distances entre machines sont augmentées car on peut supprimer le RTD.

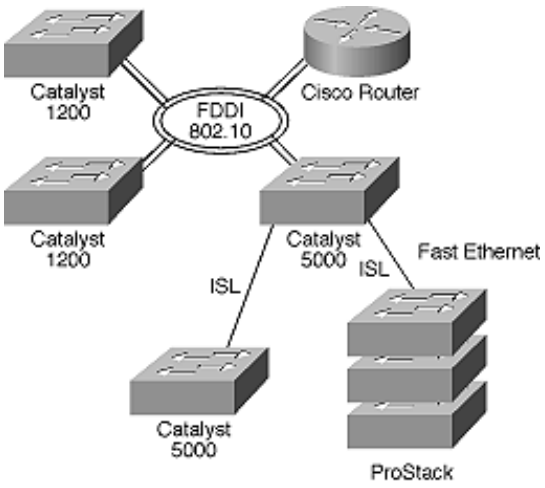
- **Ils peuvent travailler en Full Duplex**
- **Suppression du RTD (*Round Trip Delay*)**

- Avantages des switchs :
  - **Débit amélioré** par la bande passante dédiée et la suppression des collisions
  - **Périmètre du réseau agrandi** par la suppression du RTD (Round Trip Delay)
  - **Sécurité** contre l'écoute du trafic car la bande passante est dédiée.

II.B.5 Intérêts des VLAN

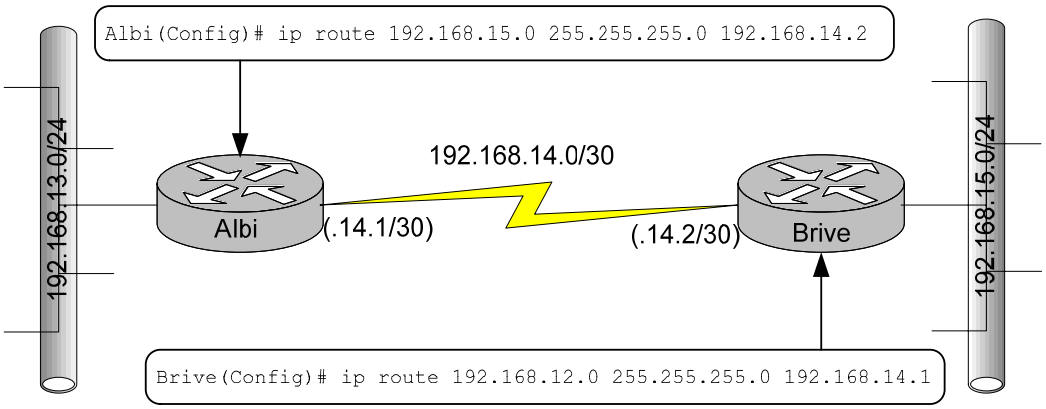
- Limiter les domaines de broadcast
- Garantir la sécurité
- Permettre la mobilité des utilisateurs

- Nouvelle manière d'exploiter la commutation pour une meilleure flexibilité des réseaux locaux.



II.C IP : Internet Protocol

- Une route : désigne l'accessibilité d'un réseau cible par l'adresse du prochain routeur (Next Hop Gateway), le réseau cible est représenté par une adresse IP et un SubNet Mask.



- Une table de routage est une base de données constituée d'enregistrements. Chaque enregistrement désigne une route qui contient cinq champs :

Target_Address	*Subnet Mask*	*Next_Hop_Gateway*	*Flags*	*Interface*

  - Le champ '*Target_Address*' (Adresse cible*)* contient l'adresse IP cible d'un réseau (ou sous réseau) ou d'une machine (host).
  - Le champ '*Subnet Mask*' contient le subnet mask associé à l'adresse cible.
  - Quand le Flag G est présent, le champ *Next_Hop_Gateway* contient l'adresse IP du prochain routeur.
    - Attention le Next Hop Gateway doit être accessible en routage direct.
    - Une machine IP (routeur ou host) connaît uniquement le prochain routeur pour atteindre la destination finale.
  - Le champ *Flags* contient :
    - U : la route est en service (Up)
    - G : la route utilise un routeur (*Gateway*). Ce Flag permet de différencier le routage direct du routage indirect.
    - H : La route fait référence à une autre machine (Host). Si ce Flag n'est pas positionné la route point vers un réseau.
    - D : La route a été créée par une redirection (*ICMP Redirect*).
    - M : La route a été modifiée par une redirection.
  - Le champ *Interface* contient le nom de l'interface réseau qui émet le datagramme.

- L'acquisition des routes par une machine IP s'effectue de quatre manières possibles.

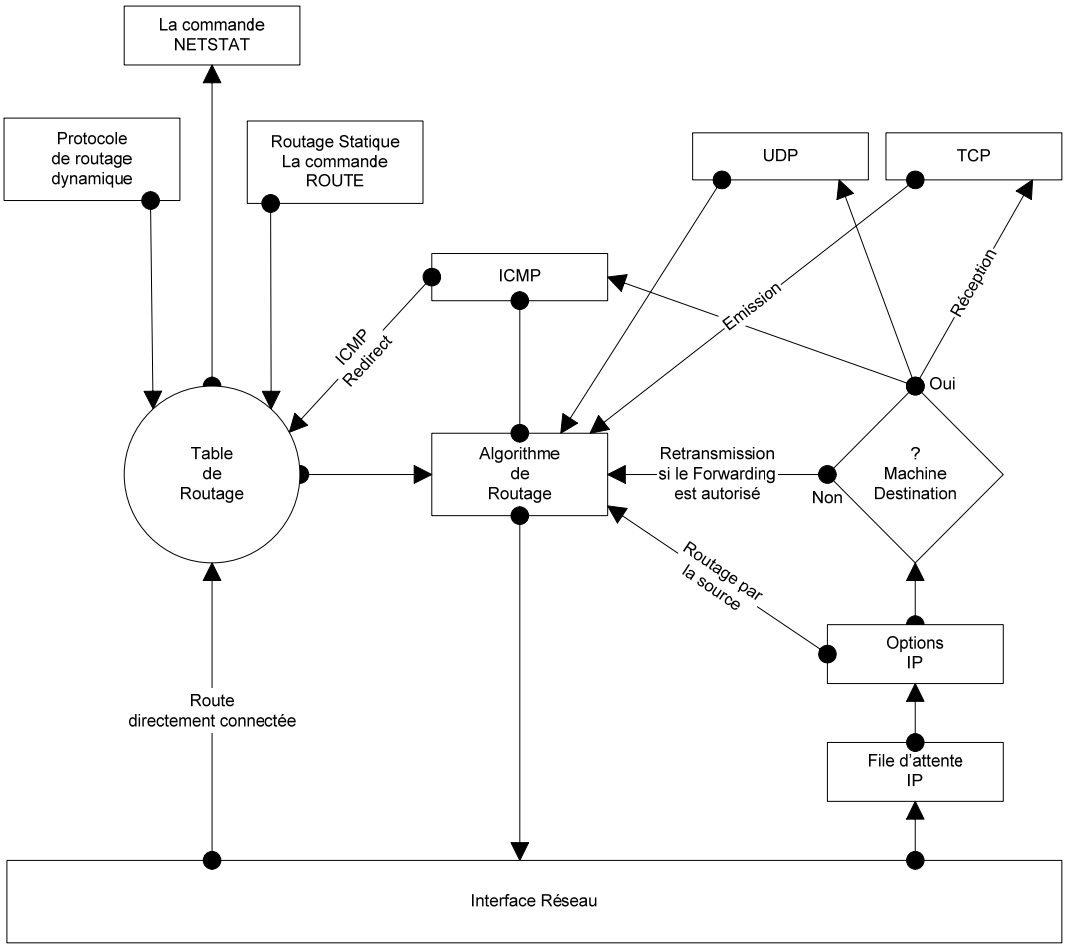
  a. Les **routes directement connectées** : ces routes sont automatiquement créées lors de la configuration des interfaces.
  b. Les **routes statiques** : ces routes doivent être déclarées manuellement ou par des fichiers statiques par la commandes '`Route`'.
  c. Les **routes dynamiques** : ces routes sont créées par des protocoles de routages dynamiques (RIP, OSPF).
  d. Par **ICMP Redirect**

- Algorithme de routage

  - Les routes de la table de routage sont classées dans l'ordre suivant :
    - Les routes des réseaux qui sont directement connectés à la plateforme
    - Les routes vers les machines (host)
    - Les routes vers les réseaux (par routage statique et dynamique)
    - La '`Default Gateway`' [route statique optionnelle].

  - Chaque route de la table de routage est évaluée dans l'ordre précisé ci-dessus :
    - Réalisez la fonction logique ET entre l'adresse IP destination et le Subnet Mask de la route
    - Si le résultat est identique à l'adresse cible de la route
      - Alors : Appliquer la route
      - Sinon : passer à la ligne suivante

  - Quand toutes les routes de la table de routage ont été évaluées et qu'aucune correspondance n'a été trouvé, IP informe d'une erreur par un message ICMP : `Destination Unreachable`.



II.D La Segmentation d'un réseau

Pont/Switch	Routeur
Couche 2	Couche 3
Adresse MAC	Adresse logique
Transparent	Route

II.D.1 Par Switch

- Amélioration le débit : bande passante dédiée et suppression de collisions.
- Diamètre du réseau beaucoup plus important, car le RTD est supprimé.
- Sécurité : bande passante dédiée.

II.D.2 Par Routeur

- Évite le Broadcast Storm (tempête de broadcast). Tout routeur bloque les broadcast physiques mais également les broadcast logiques (par défaut sur les routeurs CISCO).
- Sécurité : par la mise en place d'Access List (ACL).

II.E Synthèse

- le switch supprime le principal inconvénient d'Ethernet : la collision.

- Avantages des Switchs,

  - Débit amélioré
    - par la suppression des collisions.
    - circuit dédié

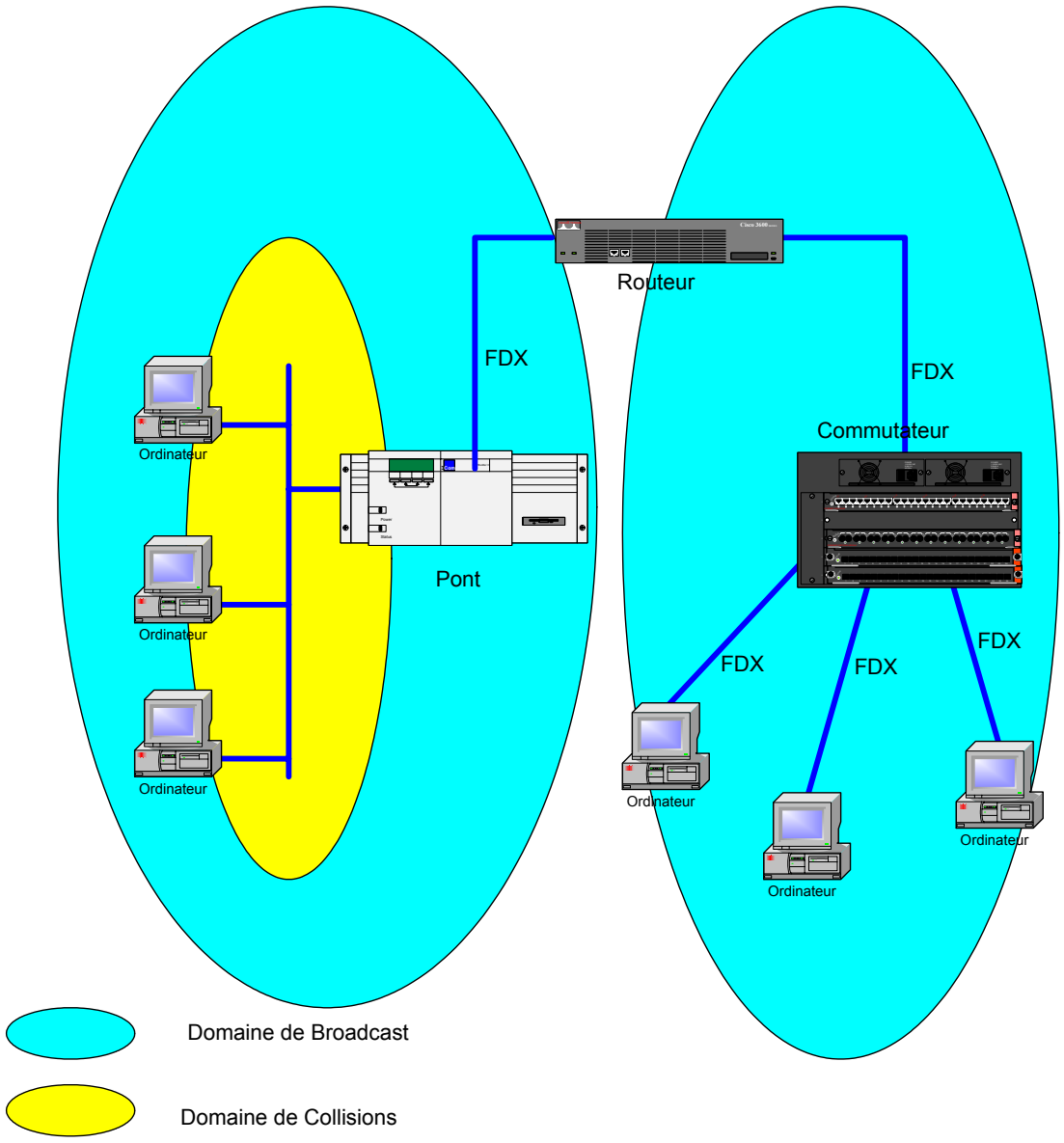
  - Distance améliorée (MAN) :
    - par la suppression des collisions donc du RTD (Round Trip Delay) ce qui permet **de** s'affranchir des distances.

  - **Sécurité**
    - circuit dédié

- Avantages des Routeurs :

  - Contrôle du trafic en Broadcast : Limitation des Broadcast Storm.
  - Interconnexion de réseaux physiques hétérogènes.

  - Contrôle du trafic Multicast
  - Détermination optimale des routes : routage statique et/ou dynamique.
  - Adressage logique indépendant des réseaux physiques.
  - Sécurité de niveau 3 : Access List.


Routeur
FDX
FDX
Commutateur
Ordinateur
Ordinateur
Ordinateur
Pont
FDX
FDX
FDX
Ordinateur
Ordinateur
Ordinateur
Domaine de Broadcast
Domaine de Collisions

III. Présentation des Switchs CISCO

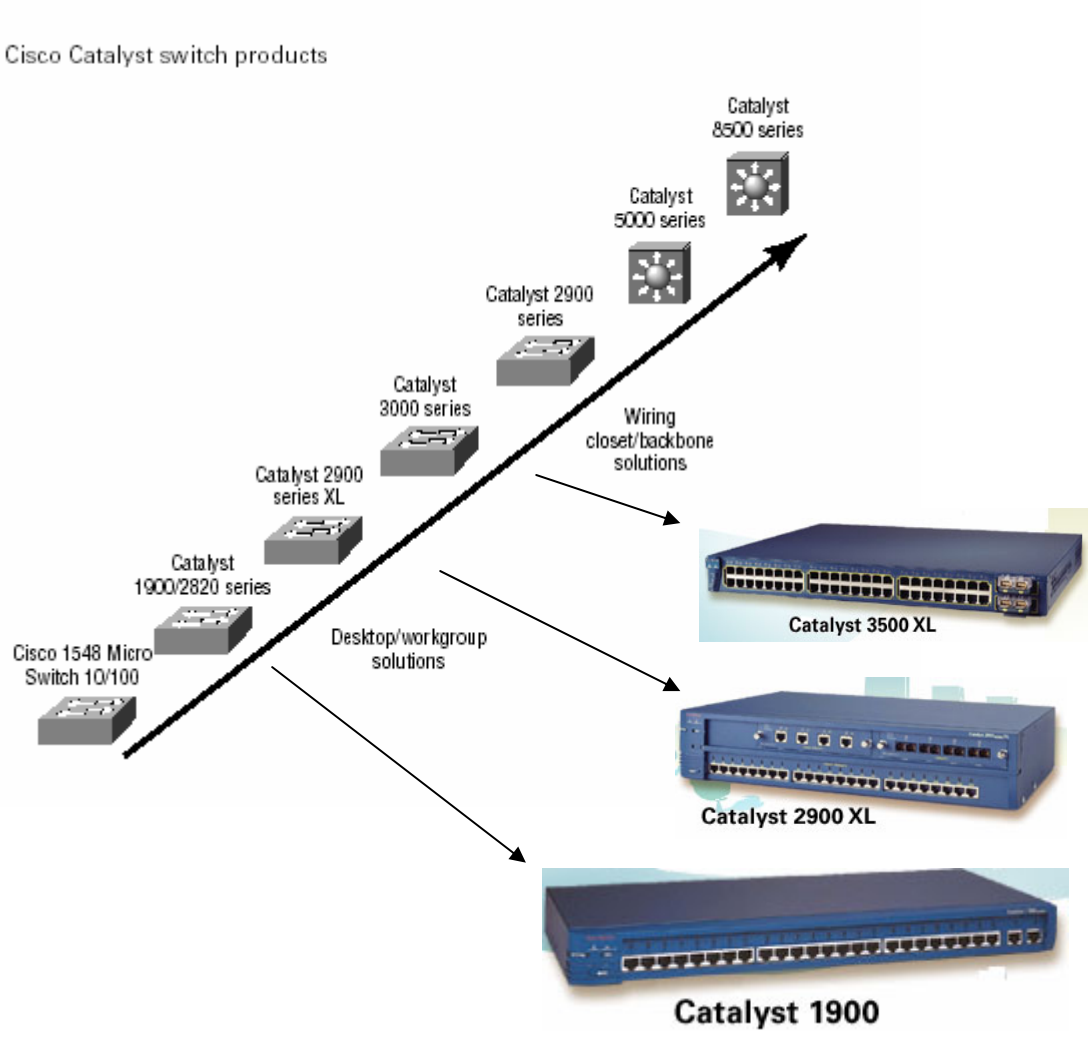
III.A Présentation

CISCO classe ses équipements dans trois catégories : '*Core layer*', '*Distribution layer*' et '*Access layer*'. Cette classification permet aux concepteurs de réseaux de choisir les équipements nécessaires.

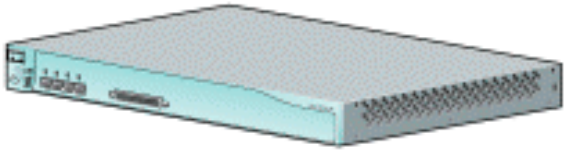
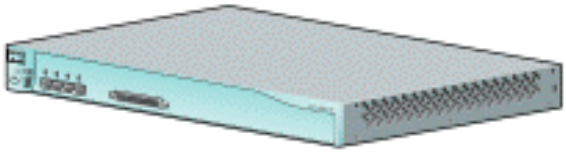
	Fonctionnalités	**Type de matériels**
Core layer		Catalyst 6000
Distribution layer		Catalyst 4000 et 5000
Access layer	Point de connexion au réseau des stations utilisateurs	Catalyst 1900, 2900

La couche d'accès réseau (*Access layer*) est l'endroit où les utilisateurs finaux se connecteront pour accéder aux ressources partagées.

Un certain nombre de switchs Catalyst sont capable de router en fond de panier, pour implémenter cette fonctionnalité, il faut rajouter une carte RSM (Route Switch Module). Maintenant on peut également intégrer un switch dans un routeur, par exemple un module ESW (Ethernet Switch Module pour les Cisco 2600, 3600 et 3700 series).

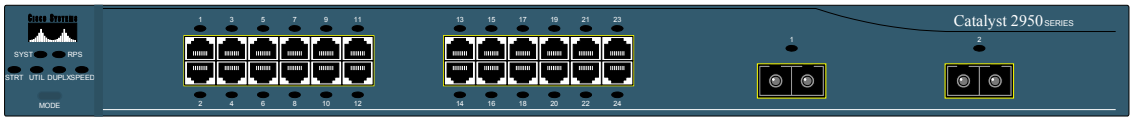


III.B Catalyst 2900

Version Number	Description	
WS-C2912-LRE-XL	4 fixed autosensing 10/100 ports 12 LRE ports	
WS-C2924-LRE-XL	4 fixed autosensing 10/100 ports 24 LRE ports	
WS-C2912-XL	12 fixed autosensing 10/100 ports	
WS-C2924C-XL	22 fixed autosensing 10/100 ports 2 100BASE-FX ports	
WS-C2924-XL	24 fixed autosensing 10/100 ports	
WS-C2912MF-XL	12 100BASE-FX ports 2 expansion slots	
WS-C2924M-XL	24 fixed autosensing 10/100 ports 2 expansion slots	

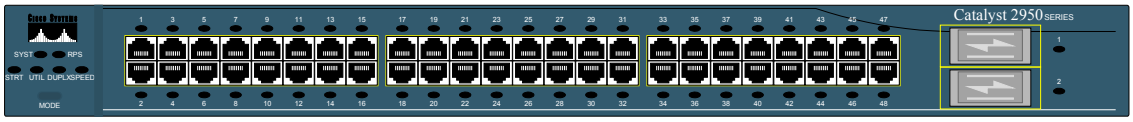
III.C Catalyst 2950

WS-C2950SX-24



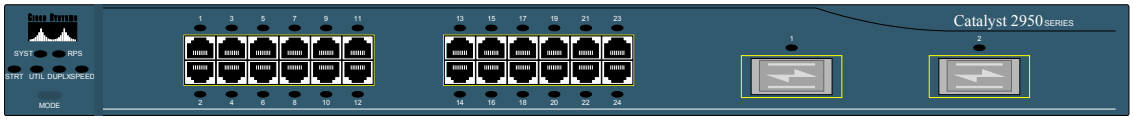
24 10/100 ports w/2 1000BASE-SX ports, Standard Image only

WS-C2950G-48-EI



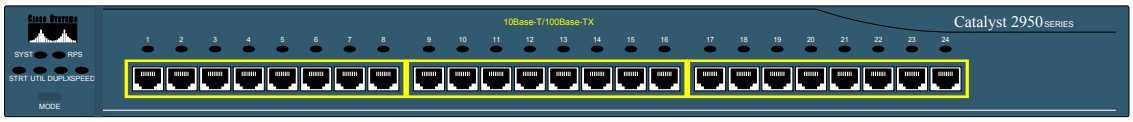
Catalyst 2950, 48 10/100 with 2 GBIC slots, Enhanced Image

WS-C2950G-24-EI



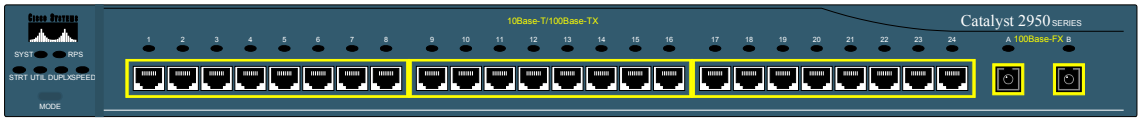
Catalyst 2950, 24 10/100 with 2GBIC slots, Enhanced Image

WS-C2950-24



24 port, 10/100 Catalyst Switch, Standard Image only

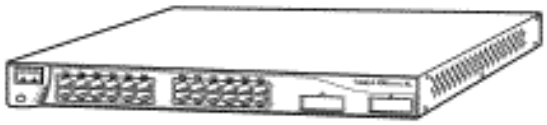
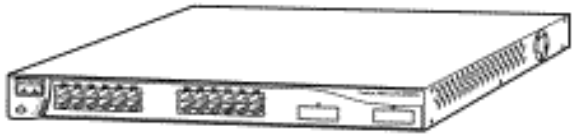
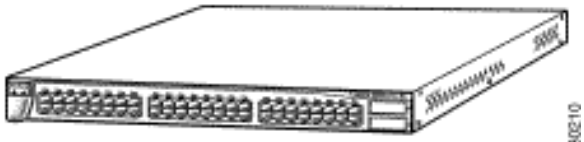
WS-C2950C-24



24 10/100 ports with 2 100BASE-FX uplinks, Enhanced Image

III.D Catalyst 3500

Catalyst 3500 Series XL Switches

Switch	Description	
WS-C3508G-XL	8 GBIC[1]-based gigabit module slots	
WS-C3512-XL	12 autosensing10/100 Ethernet ports 2 GBIC-based gigabit module slots	
WS-C3524-XL	24 autosensing 10/100 Ethernet ports 2 fixed GBIC-based gigabit module slots	
WS-C3524-PWR-XL	24 autosensing 10/100 inline-power Ethernet ports 2 GBIC-based gigabit module slots	
WS-C3548-XL	48 autosensing 10/100 Ethernet ports 2 GBIC-based gigabit module slots	

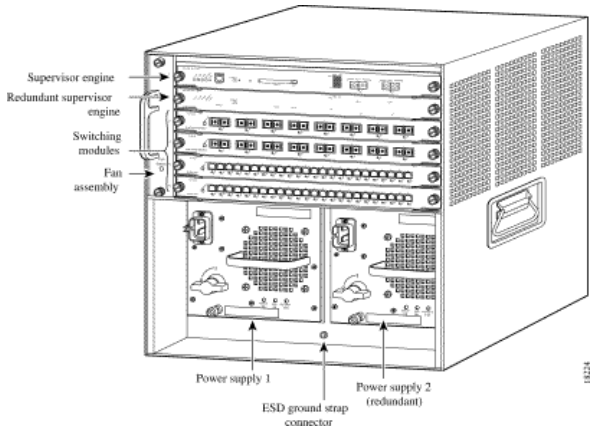
30210

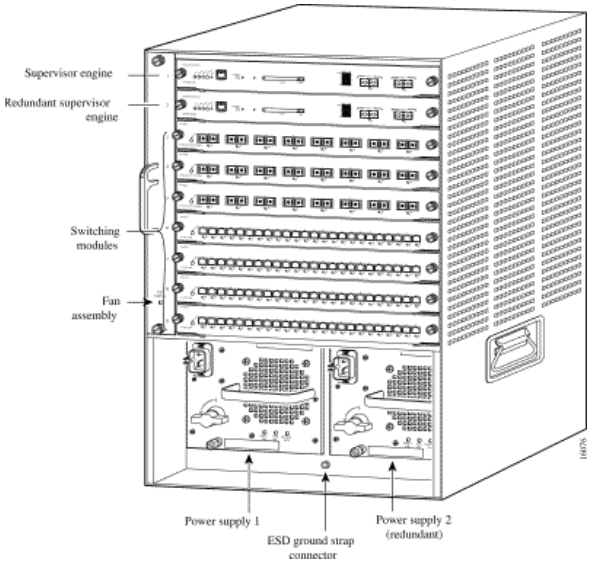
1. GBIC = Gigabit Interface Converter

III.E Catalyst 5000

III.F Catalyst 6000

6006 et 6009





III.G Catalyst 2900

III.G.1 Catalyst 2900 Series XL Switches

Nombre maximum d'adresses MAC supportées par Switch	
Modèle de Switch	**Nombre d'adresses MAC**
Catalyst 2924 XL, 2924C XL, and 2912 XL	2048
Catalyst 2924M XL and 2912MF XL	8192
Catalyst 2900 LRE XL	8192
Catalyst 3500 XL	8192

- Différentes versions :
  - WS-C2912-XL : 12 ports autosensing 10/100 Mbps
  - WS-C2924-XL : 24 ports autosensing 10/100 Mbps
  - WS-C2924C-XL : 22 ports autosensing 10/100 Mbps & 2 ports 100BaseFX
  - WS-C2912MF-XL : 12 ports 100BaseFX & 2 slots d'extensions haute débit (Gigabit Ethernet ou ATM).
  - WS-C2924MF-XL : 24 ports autosensing 10/100 Mbps & 2 slots d'extensions haute débit.

- Performance et caractéristiques :
  - Auto négociation du débit et Half/Full Duplex des ports.
  - Supporte jusqu'à 64 VLANs, car il ne peut gérer que 64 instances STP (IEEE 802.1d)
  - Tous les ports supportent le Trunking ISL & dot1q
  - Des connexions EtherChannel (agrégation de ports) entre switchs et serveurs.

III.G.2 Catalyst 2950 Series Switches

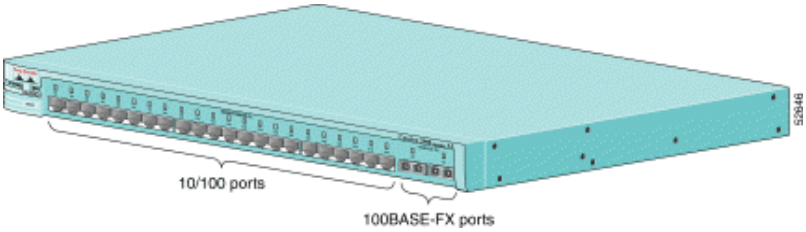
- Différentes versions :
  - WS-C2950-12 : 12 ports autosensing 10/100 Mbps
  - WS-C2950-24 : 24 ports autosensing 10/100 Mbps
  - WS-C2950C-24 : 24 ports autosensing 10/100 Mbps & 2 ports 100BaseFX
  - WS-C2950T-24 : 24 ports autosensing 10/100 Mbps & 2 ports autosensing 10/100/1000 Mbps

- Performance et caractéristiques :
  - Auto négociation du débit et Half/Full Duplex des ports.
  - Supporte 8192 adresses MAC
  - Supporte jusqu'à 64 VLANs, car il ne peut gérer que 64 instances STP (IEEE 802.1D)
  - Tous les ports supportent le Trunking dot1q (IEEE 801.1Q)
  - Des connexions EtherChannel (agrégation de ports) entre switchs et serveurs.

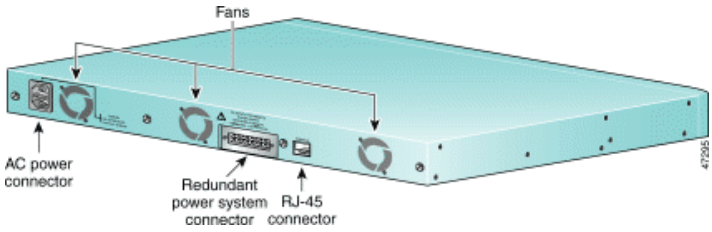
III.G.3 Description

- En fonction du modèle un Switch peut avoir:
  - Jusqu'à 24 ports 10/100 Mbps,
  - Jusqu'à 12 ports 100Base-FX,
  - 2 Slots d'extension,
  - et jusqu'à 24 ports Long-Reach Ethernet (LRE).
  - Tous les Switchs possèdent un ensemble de LEDs et d'un bouton de MODE.

Catalyst 2900 XL Front-Panel 10/100 Ports



Catalyst 2912 XL, 2924 XL, and 2924C XL Rear Panel



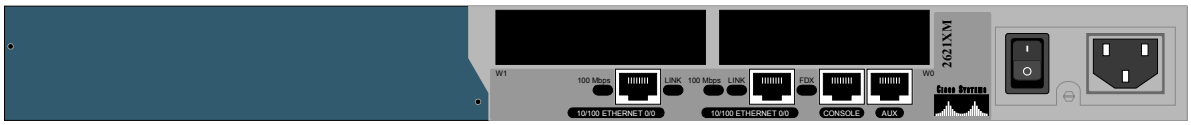
III.H Cisco 2621

- Cette génération de routeur offre de nombreux avantages par rapport à la génération précédente (Cisco 2500). L'avantage principal est sa modularité par l'adjonction de modules NM (*Network Module*) et WIC (*WAN Interface Card*).
  - Le Cisco 2600 possède un emplacement NM. Ici un module NM-16ESW qui est un switch 16 ports sur lequel on peut rajoute un port Giga Ethernet.
  - Et deux emplacements WIC.
  - Etc.

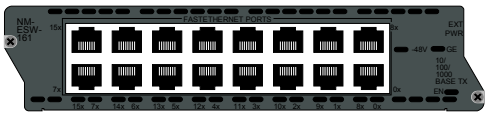
- Question : que représente comme équipement réseau un Cisco 2621 avec un module NM-16ESW ?
  - Un switch :
  - Un routeur :
  - Un commutateur de niveau 2 et 3 :

- Attention, dans cette configuration (C2621 plus ESW) les ports Ethernet n'ont pas la même connectique :
  - Les ports du routeur ont une connectique de type Host, c'est-à-dire que les broches une et deux représentent la paire émission.
  - Tandis que les ports du module NM-16ESW ont une connectique de type HUB, c'est-à-dire que les broches une et deux représentent la paire réception.

Routeur CISCO 2621XM

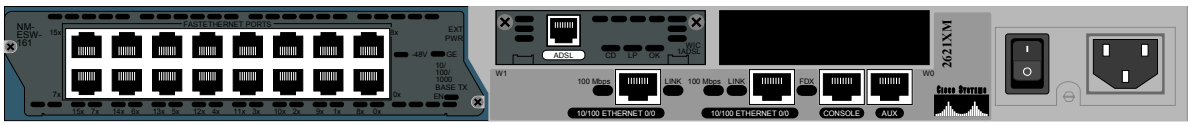


NM-16ESW

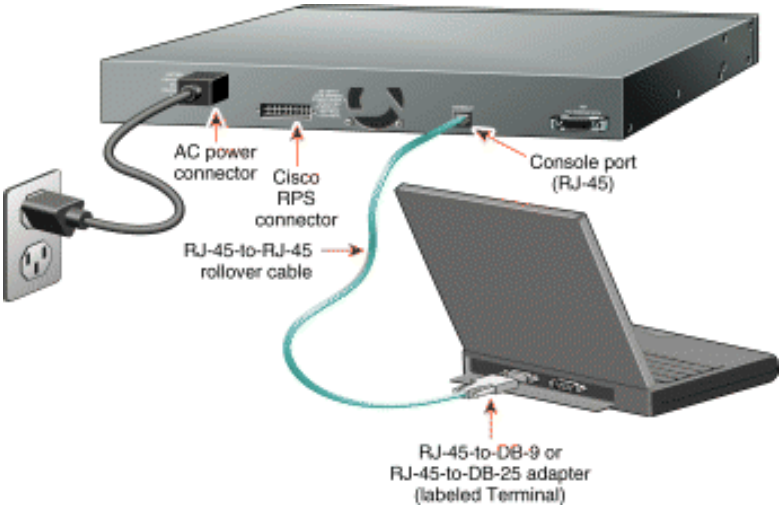


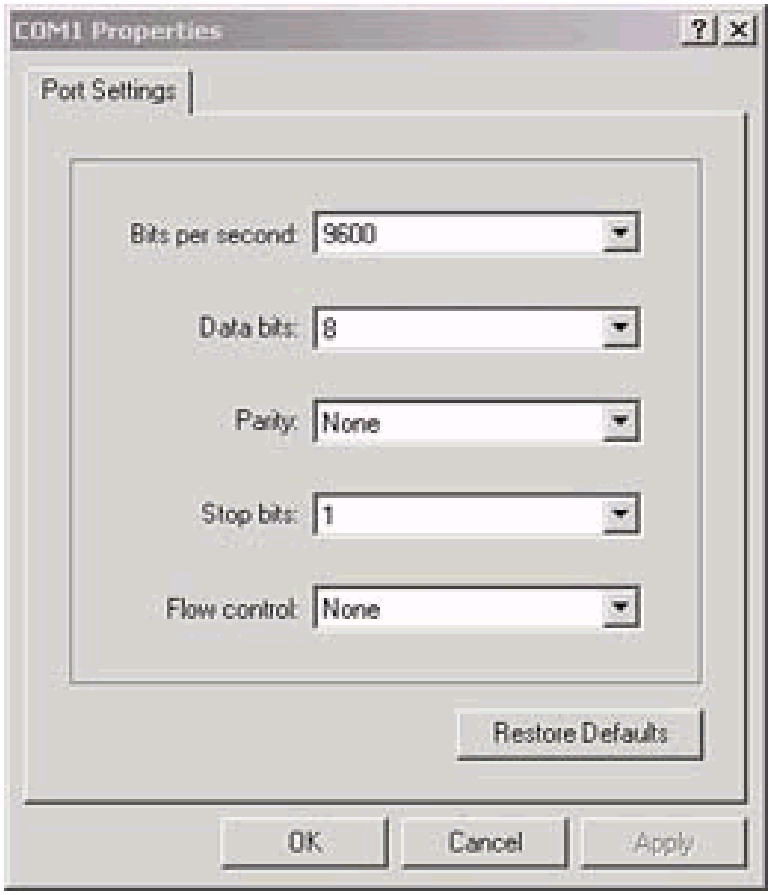
WIC-1ADSL

Commutateur de niveau 2 & 3



III.H.1 Connexion au Port Console



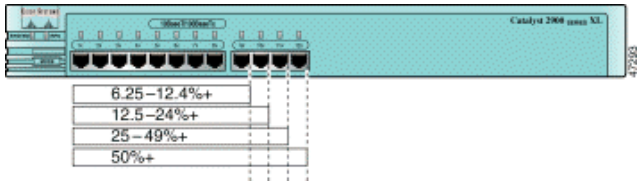


III.I Le bouton Mode

Port Mode LEDs on the Catalyst 2912 XL, 2924C XL, 2924 XL, 2924MF XL, and 2924M XL Switches

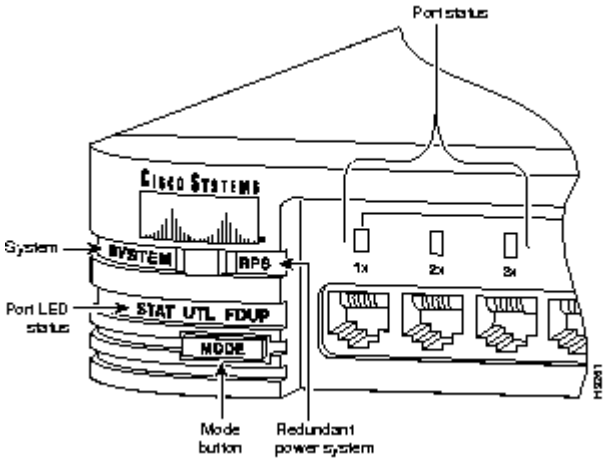
Mode LED	Port Mode	Description
STAT	Port Status	L'état du port : le mode par défaut
UTL	Switch utilization	La bande passante utilisée par le Switch
FDUP	Port duplex mode	Le mode duplex du port : Full Duplex ou Half Duplex
100	Port speed	Le débit du port : 10, 100 ou 1000 Mbps

Indication de la bande passante



Un système de lumières vertes apparaît si le commutateur est opérationnel. Il sera de couleur ambré si une défaillance système est détectée. Le RPS est une lumière d'alimentation d'énergie redondante qui est « ON » si un problème est détecté dans le commutateur. Le seul bouton sur le commutateur 1900 est le bouton de mode.

Catalyst 1900 LEDs



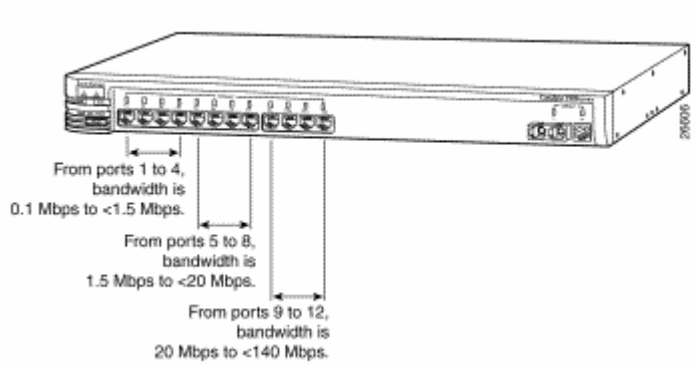
En appuyant le bouton de mode, vous pouvez voir trois lumières d'états différentes sur le commutateur :

III.I.1 Stat

Cette lumière montre l'état des ports. Si c'est vert, cela indique qu'un dispositif est branché sur le commutateur. Vert => actif et une lumière verte clignotante => activité sur le port. Si le port est de couleur ambré, il y a eu un problème de liaison.

III.I.2 UTL

Cette lumière indique la largeur de bande du commutateur. Quand vous pressez le bouton de mode sur un commutateur 1912 et les LEDs pour les ports 1 à 4 s'activent, cela signifie que l'utilisation de largeur de bande du commutateur est quelque part entre 0.1 et 1.5 Mbps.



Si les LEDs 5 à 8 s'activent, cela indique que l'utilisation est entre 1.5 et 20 Mbps alors que pour les LEDs de 9 à 12 indiquent la largeur de bande est entre 20 et 120 Mbps.

III.J Powering On the Switch and Running POST

To power on the switch after you install it, follow these steps:

Step 1 Connect one end of the AC power cord to the AC power connector on the switch.

Step 2 Connect the other end of the power cord to an AC power outlet.

As the switch powers on, it begins POST, a series of eight tests that run automatically to ensure that the switch functions properly. When the switch begins POST, the port LEDs turn amber for 2 seconds, and then they turn green. The System LED flashes green, and the RPS LED turns off. As each test runs, the port LEDs, starting with number 1, turn off. The port LEDs for ports 2 to 8 each turn off in turn as the system completes a test.

When POST completes successfully, the port LEDs return to the status mode display, indicating that the switch is operational. If a test fails, the port LED associated with the test turns amber, and the system LED turns amber. If POST fails, refer to "Troubleshooting," to determine a course of action.

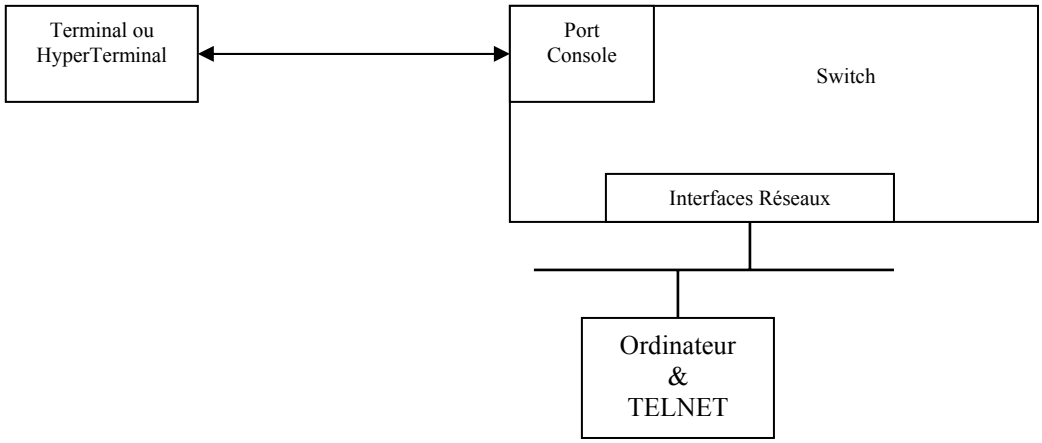
POST failures are usually fatal. Call Cisco Systems immediately if your switch does not pass POST.

POST Test Descriptions Switch LED	
1	DRAM
2	Flash memory
3	Switch CPU
4	System board
5	CPU interface ASIC
6	Switch core ASIC
7	Ethernet controller ASIC
8	Ethernet interfaces

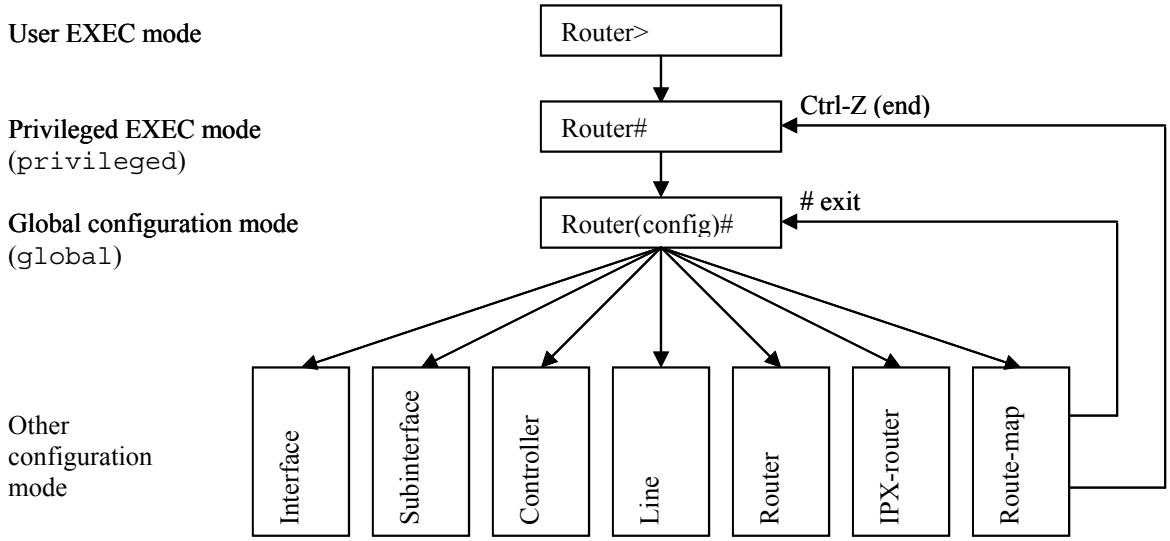
IV. Procédure de Configuration par CLI

IV.A Le CLI

- CLI (*Command-Line Interface*) est le terme qui désigne l'interface en ligne de commande du terminal pour l'IOS.
- Pour accéder au CLI on emploie ; un terminal, ou une émulation de terminal (*HyperTerminal*) sur le port console, ou une connexion TELNET par le réseau.



IV.B Les modes de configuration



Autres Modes de configuration	Invite	Configuration
(interface)	Router(config-if)#	Des interfaces
(subinterface)	Router(config-subif)#	Des interfaces virtuelles
(line)	Router(config-line)#	D'accès à partir d'un terminal
(router)	Router(config-router)#	Des protocoles de routage IP

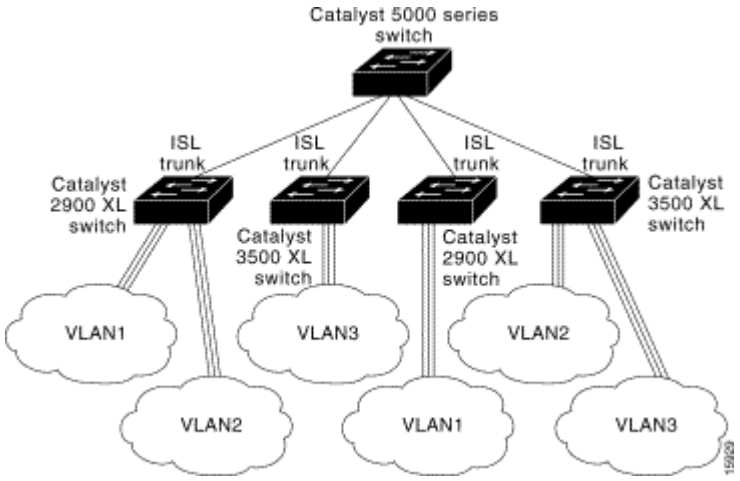
Sommaire des Modes de Commande				
		switch>		❍
		Switch#		
		Switch(config)#		
		Switch(vlan)#		
		Switch(config-if)#		
		switch(config-line)#		

IV.C SVI : Switch Virtual Interface

- Vous pouvez observer qu'il est impossible d'affecter une adresse IP à une interface d'un switch ('`no ip address`' sur chaque interface). Ceci est tout à fait normal, car les interfaces sont vues uniquement an niveau 2 (pontage) mais surtout pas au niveau 3 (routage).
- Comme une adresse IP est affectée sur une interface, il faut donc créer une interface virtuelle qui représente le réseau de niveau 2.
- Celle-ci s'appelle :
  - BVI : '*Bridge Virtual Interface*' sur un pont,
  - SVI : '*Switch Virtual Interface*' sur un switch.

IV.D Affectation d'un port

Mode	Caractéristiques
Static-access	Dans ce mode les ports sont affectés manuellement à un seul VLAN. Par défaut tous les ports sont configurés en '*static-access* et assignés au VLAN 1. Mais également, le VLAN peut être affecté par un serveur Radius via 802.1x et la commande '`(config-if)dot1x port-control auto`'. Référence Chapitre XIII, page 103
Multi-VLAN	Dans ce mode un port peut appartenir jusqu'à 250 VLANs par configuration manuelle. Ce mode interdit le Trunk dans un même Switch. Le trafic n'est pas encapsulé dans un Multi-VLAN.
Trunk (ISL ou dot1q)	Un trunk est membre de tous les VLANs dans la base de données VLAN (VLAN Database) par défaut, mais l'appartenance peut-être limitée par la configuration de la liste des '*allowed-VLAN*'.
Dynamic-access	En '*dynamic-access*' les ports appartiennent à un VLAN et sont assignés dynamiquement à un VLAN par un '*VLAN Membership Policy Server*' (VMPS). Le VMPS peut-être hébergé sur un Catalyst de la série 5000, mais pas sur des switchs des séries 2900XL et 3500XL.



Commandes générales	
Commandes	**signification**
`Switch# erase startup-config`	Effacement du fichier `Startup-config`
`Switch# reload`	Arrête et redémarre le Switch
`Switch# terminal monitor`	Active l'affichage des messages d'erreur système et de DEBUG sur la console
`Switch# terminal no monitor`	Désactive l'affichage des messages d'erreur système et de DEBUG sur la console
`Switch# undebug all`	Arrête le debug (analyseur réseau)

IV.E Pour connecter un ordinateur à un port

Commandes	Signification
() configure terminal	Entrez en mode configuration globale
(global) interface fastethernet *0/4* ou (global) interface range fastethernet *0/4 - 8*	Choix du port à configurer
shutdown	Désactivez l'interface avant de la configurer
description Server WEB	Adjoindre une description pour faciliter l'administration
speed {10 | 100 | auto}	Configuration du débit
duplex {full | half | auto}	Configuration du mode DUPLEX
spanning-tree portfast	Arrêt de la négociation STP sur le port pour une connexion plus rapide de la machine au réseau.
switchport mode access	Configuration par défaut du port en Static-access
switchport access vlan *3*	Affectation statique d'un port à un VLAN, ici au '*VLAN3*'
switchport nonegotiate	Evite de propager les VLAN (trou de sécurité des switchs CISCO)
no shutdown	Activez l'interface
end	Retour en mode privileged EXEC
() show interfaces status	Visualisation complète de la configuration des interfaces
() show running-config	Vérifiez votre configuration
() copy running-config startup-config	[optionnel] sauvegardez la configuration pour le prochain redémarrage.

- Éviter les auto-négociations sur le débit et le Duplex, car cela génère une perte de bande passante.
- Le '`spanning-tree portfast`' permet de raccorder plus rapidement un routeur, une station de travail ou un serveur au réseau, mais si vous raccorder un HUB ou un Switch : DANGER aux boucles de niveau deux.

- **Note** : Le mode par défaut des interfaces de niveau 2 est '***switchport mode dynamic desirable***'. Si l'interface la plus proche supporte le trunking et configurée pour, la connexion entre les deux switchs sera un lien Trunk.

- Si vous avez besoin de configurer plusieurs fois des groupes d'interfaces { `ethernet` | `fastethernet` | `gigabitethernet` | `tengigabitethernet` | `vlan` }, pour pouvez définir des macros.
  - La commande '`interface range`' peut être utilisée pour configurer les interfaces suivantes '`interface range`' est '`type slot/first-port – last-port [,type slot/first-port – last-port]`', où jusqu'à cinq différents espaces (`range`) peuvent être définies.
  - Le caractère '`,`' (*comma*) énumére les interfaces constituant la macro. Par exemple, l'expression '**`fa1/1 , fa1/4`**' désigne uniquement les deux interfaces FA1/1 et FA1/4.
  - Le caractère '`-`' (*hyphen*) borne une liste d'interfaces. Par exemple, l'expression '**`fa1/1 – 4`**' désigne les quatre interfaces de FA 1/1 à FA1/4.

```
(global) interface range fa 1/1 – 4, fa 6/1 – 3
 speed auto
OR
(global) define interface-range Host-Ports fa 1/1 – 4, fa 6/1 – 3
(global) interface range macro Host-Ports
 speed auto
```

IV.F Configuration IP

- Sur un Switch, un Catalyst 2900 par exemple, une seule interface VLAN peut posséder une adresse IP **active** : par défaut le VLAN 1. Vous pouvez affecter une adresse IP à plusieurs VLAN (SVI), mais seule la dernière adresse IP saisie sera effectivement active.
- Par contre, sur les commutateurs de niveau 3 chaque VLAN aura une adresse IP qui permettra de réaliser le routage entre ces différents réseaux (que sont les VLAN).

Configuration générale IP :	
Commandes	**signification**
`() configure terminal`	Entrez en mode globale configuration
`(global) hostname` *`Switch1`*	Définir le nom machine
`(global) ip default-gateway` *`192.168.15.5`*	Définir la route par défaut (Default Gateway)
`(global) ntp server` *`192.168.13.4`*	Définir le serveur de temps
`(global) ip domain-name` *`gefi.home`*	Définir le suffixe DNS
`(global) ip name-server` *`192.168.13.4`*	Définir les adresses des serveurs DNS
`(global) ip host` *`nms.gefi.home 192.168.13.4`*	Définition locale d'une adresse IP en un nom symbolique. Voir CMD : '`show hosts`'
`(global) ip subnet-zero`	Lors de subnetting, cette commande autorise l'utilisation du premier et dernier sous réseau, pour la configuration des interfaces et la mise à jour des tables de routage (RFC 1812 & 1878).
`(global) end`	Retour en mode '*privileged EXEC*'
`() show running-config`	Vérifiez votre configuration
`() show hosts`	Visualisation : IP domain-name, lookup style, nameservers, and host table. Voir CMD '`ip host`'.
`() copy running-config startup-config`	[optionnel] sauvegarde la configuration pour le prochain redémarrage.
`() copy running-config startup-config`	[optionnel] sauvegarde la configuration pour le prochain redémarrage.

Configuration IP d'une interface SVI :	
Commandes	**signification**
`(global) Interface vlan` *`1`*	Choix du VLAN à configurer par défaut le VLAN1 qui est le VLAN natif.
`ip address` *`192.168.3.61 255.255.255.0`*	Configuration de l'adresse IP
`clear ip address` *`192.168.3.61 255.255.255.0`*	Suppression de l'adresse IP
`no shutdown`	Active l'interface
`end`	Retour en mode '*privileged EXEC*'
`() show running-config`	Vérifiez votre configuration
`() copy running-config startup-config`	[optionnel] sauvegardez la configuration pour le prochain redémarrage.
`() show ip interface brief | include` *`Vlan`*	Visualisation de la configuration IP des interfaces Vlan. Attention, respectez la casse.

- Exemple :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#ip address 192.168.3.59 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#^Z
Switch#
```

IV.G Les mots de passe

Console password / le mot de passe pour le port console :	
Commandes	**signification**
	Attachez un terminal ou un ordinateur en émulation de terminal su le port console du switch.
`configure terminal`	Entrez en mode Configuration Global
`line console 0`	Entrez en mode de configuration d'interface pour l'accès au port console
`password` *gefi*	Le mot de passe n'est pas chiffré
`login`	Active la vérification du mot de passe
`exec-timeout 5 30`	Déconnection au bout de 5 minutes et 30 secondes.
`Logging synchronous`	Affichage correct des commandes malgré les messages système.
`Escape-character 27`	La touche ESC permet de réaliser une séquence de break.
`end`	

- Si le '*VTY Password*' n'est pas déclaré, vous ne pourrez pas accéder à l'équipement via le réseau par telnet.

VTY Password / le mot de passe pour l'accès Telnet :	
Commandes	**Signification**
`enable`	Entrez en mode '*Privileged EXEC*'
`configure terminal`	Entrez en mode Configuration Global
`line vty 0 15`	Entrez en mode de configuration d'interface pour l'accès du telnet
`password` *gefi*	Entrez le mot de passe pour l'ouverture du session telnet
`login`	Active la vérification du mot de passe
`exec-timeout 0 0`	Plus de déconnection automatique.
`Logging synchronous`	Affichage correct des commandes malgré les messages système.
`Escape-character 27`	La touche ESC permet de réaliser une séquence de break.
`access-class 1 in`	L'*access-class* uniquement pour le trafic telnet. Ici j'autorise uniquement l'adresse IP dans l'*access-list* à entrer.
`end`	Retour au mode '*Privileged EXEC*'
`show running-config`	Visualisation de la configuration active.
`copy running-config startup-config`	Sauvegarde de la '*running-config*' dans la '*startup-config*'.

Access List sur les VTY	
`Albi1(config)#` **`Access-list 1 permit 192.168.1.32 0.0.0.31`** `Albi1(config)#` **`Line vty 0 4`** `Albi1(config-line)#` **`Access-class 1 in`**	Sécurisé un accès Telnet par une ACL standard

- Déclaration du mot de passe de l'administrateur de l'équipement.

Enable password/ le mot de passe pour le compte 'enable' :	
Commandes	**signification**
`configure terminal`	Entrez en mode Configuration Global
`enable secret` *gefi*	Le mot de passe est chiffré (**recommandé**)
`enable password` *gefi*	Le mot de passe n'est pas chiffré
`end`	Retour au menu principal.
`show running-config`	Visualisation de la configuration active.
`copy running-config startup-config`	Sauvegarde de la '*running-config*' dans la '*startup-config*'.

Commandes complémentaires	**signification**
`# no enable secret`	Suppression du mot de passe '`Enable secret`'
`# no enable password`	Suppression du mot de passe '`Enable password`'

Syntaxe :

```
# enable password [level level] {password}
ou
# enable secret [level level] {password}
```

- 'level 1' est le mode normal utilisateur (*EXEC-Mode*)
- 'level 15' est le mode d'administration (*Privileged EXEC-Mode*)

Affectation et activation de mots de passe pour : le compte Enable et les VTY

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable secret cisco
Switch(config)#line vty 0 15
Switch(config-line)#password gefi
Switch(config-line)#login
Switch(config-line)#^Z
Switch#
00:30:25: %SYS-5-CONFIG_I: Configured from console by console
Switch#
```

Syntaxe pour définir un 'level'

```
Switch(config)#privileged mode level level command
Switch(config)#enable secret level level password
```

Mode	Description
configuration	Global configuration
controller	Controller configuration
exec	EXEC
hub	Hub configuration
interface	Interface configuration
ipx-router	IPX router configuration
line	Line configuration
map-class	Map Class configuration
map-list	Map List configuration
route-map	Route map configuration
router	Router configuration

Exemple :

```
Switch(config)#enable secret level 3 gedev
Switch(config)# enable secret gefi
Switch(config)#username student password cisco
…
Switch#exit
…
Username: student
Password: cisco
Switch>enable 3
Password: gedev
Switch# show privilege
Current privilege level is 3
```

IV.H Gestion des adresses MAC

- Les commutateurs utilisent la table d'adresses MAC pour relayer le trafic entre les ports. La table MAC contient des adresses dynamiques, permanentes et statiques.
  - Les **adresses dynamiques** sont des adresses MAC que le commutateur apprend, puis qu'il supprime lorsqu'elles ne sont plus utilisées.
  - Les **adresses permanentes** sont des adresses MAC affectées par l'administrateur à un port.
  - Une **adresse statique** permet de restreindre le trafic à une adresse MAC donnée à partir d'une interface source particulière.

Gestion des adresses MAC	
Commandes	**signification**
`()conf t`	Entrez en mode de configuration global
`(global) mac-address-table aging-time` *`seconds`*	Déclaration de la durée de vie d'une Adresses MAC dans la FDB.
`(global) end`	Retour au mode EXEC privilégié
`# show mac-address-table`	Visualisation des Adresses MAC dans la FDB
`# show mac-address-table aging-time`	Valeur de la durée de vie d'une adresse MAC
`# show mac-address-table address 000C.1234.5678`	Localisation d'une adresse MAC
`# show mac-address-table dynamic interface gig 0/1`	Visualisation des adresses MAC découvertes sur un port
`# clear mac-address-table`	Effacement total de la FDB
`# clear mac-address-table dynamic`	Effacement des Adresses MAC acquises par le pont
`# clear mac-address-table static`	Effacement des Adresses MAC déclarées par l'administrateur.

Adresses MAC permanentes	
`(global) MAC-ADDRESS-TABLE PERMANENT` ***`add-mac type module/port`***	
Arguments	**signification**
`add-mac`	Adresse MAC unicast
`type`	Le type d'interface : *ethernet*, *fastethernet* ou *port-channel*
`module/port`	Identifiant du port. Par exemple : 0/1
`Sw(config)# mac-address-table permanent` ***`2222.2222.2222`*** **`fastethernet`** ***`0/1`***	

- Le commutateur n'autorise le trafic destiné à l'adresse statique '*`2222.2222.2222`*' sur l'interface '`fa`*`0/1`*' qu'à partir de l'interface '`fa`*`0/2`*'.

Adresses MAC statiques	
`(global) MAC-ADDRESS-TABLE RESTRICTED STATIC` ***`add-mac type module/port src-if-list`***	
Arguments	**signification**
`add-mac`	Adresse MAC unicast
`type`	Le type d'interface : ***e****thernet*, ***fa****stethernet* ou *port-channel*
`module/port`	Identifiant du port. Par exemple : 0/1
`src-if-list`	Liste des interfaces acceptables sont séparées par des espaces
`Sw(config)# mac-address-table restricted static` ***`2222.2222.2222 fa0/1 fa0/2`***	

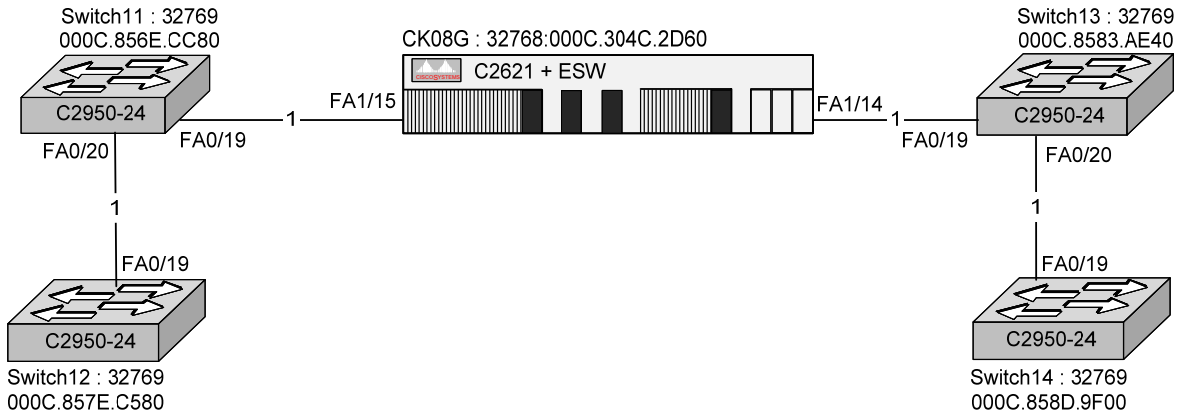
- Précédemment, Cisco utilisé le terme CAM (*Content-Adressable Memory*) pour désigner la '*Forwarding Data Base*' d'un pont ou d'un switch.

IV.I Application

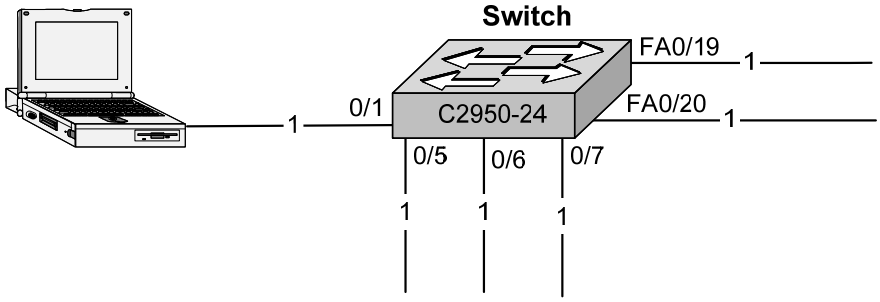
IV.I.1 Block Switch 1

	CK08G	Switch11	Switch12	Switch13	Switch14
Add IP	192.168.1.80	192.168.1.82	192.168.1.84	192.168.1.86	192.168.1.88
Subnet Mask	255.255.255.255				
Default Gateway	192.168.15.5	192.168.1.80			
Domain Name	gefi.home				
Name Server	192.168.15.9				
Serveur NTP	192.168.15.9				
Password Con	gefi	néant			
Password VTY	gefi				
P. Enable Secret	cisco				

- Installation et configuration des commutateurs



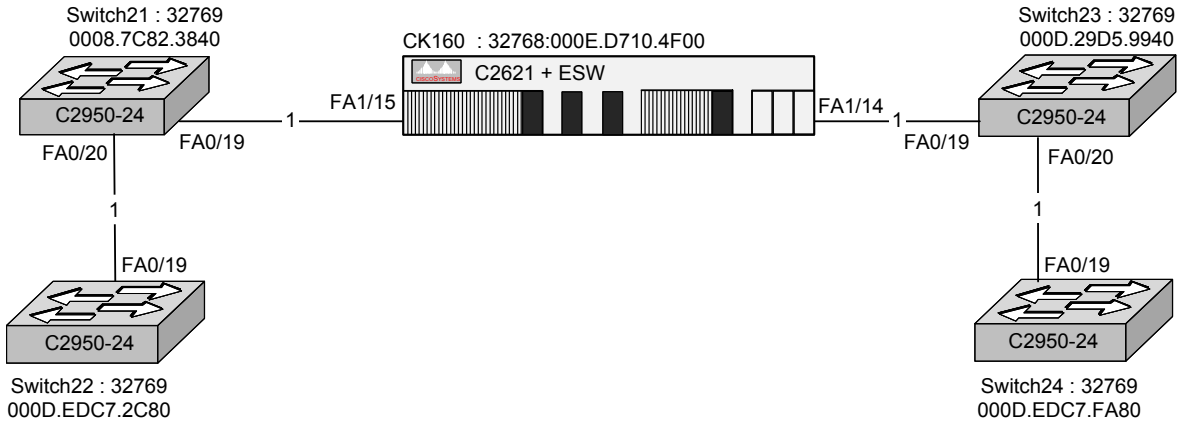
- Installation et configuration des ordinateurs
  - L'adresse IP des ordinateurs est l'adresse IP de l'équipement de raccordement plus un.
  - Le port de connexion est '`FA0/1`' sur le siwtch et '`FA1/0`' sur le routeur.



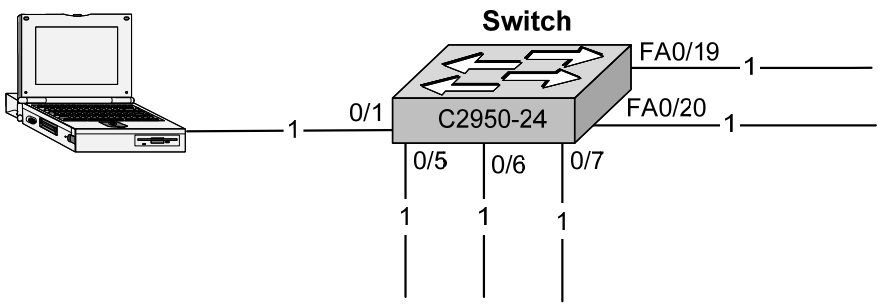
IV.I.2 Block Switch 2

	CK160	Switch21	Switch22	Switch23	Switch24
Add IP	192.168.1.96	192.168.1.98	192.168.1.100	192.168.1.102	192.168.1.104
Subnet Mask	255.255.255.255				
Default Gateway	192.168.15.5	192.168.1.96			
Domain Name	gefi.home				
Name Server	192.168.15.9				
Serveur NTP	192.168.15.9				
Password Con	gefi	néant			
Password VTY	gefi				
P. Enable Secret	cisco				

- Installation et configuration des commutateurs



- Installation et configuration des ordinateurs
  - L'adresse IP des ordinateurs est l'adresse IP de l'équipement de raccordement plus un.
  - Le port de connexion est '`FA0/1`' sur le siwtch et '`FA1/0`' sur le routeur.



IV.I.3 Configuration Type

- Voici deux configurations initiales types :
  - A gauche, la configuration du routeur/switch '`CK08G`'. Pour l'instant, on s'intéresse uniquement à son niveau 2 (commutation).
  - A droite, la configuration du switch '`Switch21`'. Pour adapter cette configuration aux autres switchs, il suffit seulement de modifier l'adresse IP du VLAN1 (Add IP du SVI).

- Attention : Si les configurations semblent ici identiques, il en reste pas moins que la déclaration de la '*Default Gateway*' est totalement différent :
  - Le switch est un équipement de niveau deux, donc la commande définissant la '*Default Gateway*' est : '`ip default-gateway 192.168.1.80`'.
  - Le routeur est un équipement de niveau trois, donc la commande définissant la '*Default Gateway*' est : '`ip route 0.0.0.0 0.0.0.0 192.168.15.5`'.

Configuration Type

Routeur : `CK08G`

```
conf t
!
hostname CK08G
ip route 0.0.0.0 0.0.0.0 192.168.15.5
ip domain-name gefi.home
ip name-server 192.168.15.9
ntp server 192.168.15.9
!
interface range  fastethernet 1/0 - 15
switchport mode access
!
no shutdown
exit
!
interface vlan 1
description Vlan d'administration
ip address 192.168.1.80 255.255.255.0
no shutdown
exit
!
line console 0
password gefi
login
escape-character 27
logging synchronous
exec-timeout 0 0
exit
!
line vty 0 4
password gefi
login
escape-character 27
logging synchronous
exec-timeout 0 0
exit
!
enable secret cisco
!
end
wr
!
```

Switch : `Switch21`

```
conf t
!
hostname Switch21
ip default-gateway 192.168.1.80
ip domain-name gefi.home
ip name-server 192.168.15.9
ntp server 192.168.15.9
!
interface range  fastethernet 0/1 - 24
switchport mode access
switchport nonegotiate
no shutdown
exit
!
interface vlan 1
description Vlan d'administration
ip address 192.168.1.81 255.255.255.0
no shutdown
exit
!
line console 0
password gefi
login
escape-character 27
logging synchronous
exec-timeout 0 0
exit
!
line vty 0 15
password gefi
login
escape-character 27
logging synchronous
exec-timeout 0 0
exit
!
enable secret cisco
!
end
wr
!
```

- La commande '`switchport nonegotiate`' n'existe pas sur l'IOS des routeurs.

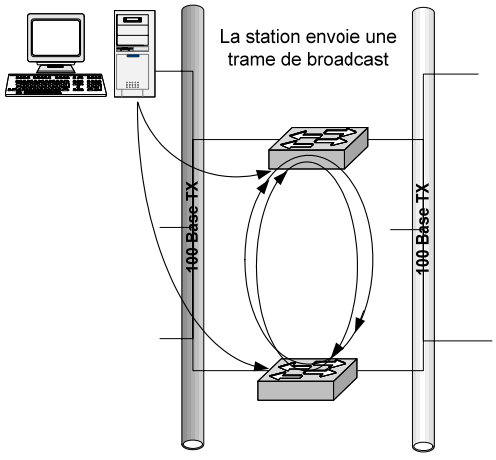
V. Le Spanning Tree Protocol

Spanning Tree	arbre recouvrant
STP	Spanning Tree Protocol
STA	Spanning Tree Algorithm

- l'algorithme du *Spanning Tree* consiste à construire un arbre définissant un chemin unique entre commutateurs et sa racine.
- Le STP (*Spanning Tree Protocol*) est un **protocole pour éviter les boucles de niveau 2 dans une architecture redondante**, et a été développé par DEC (Digital Equipment Corporation).
- L'algorithme du Spanning Tree de DEC a été normalisé par le comité 802 de l'IEEE et publié dans la spécification **IEEE 802.1d**, mais leurs fonctionnements sont différents.
- Le STP de DEC et l'IEEE 802.1d sont incompatibles entre eux. Les commutateurs CATALYST CISCO mettent en œuvre le protocole IEEE 802.1d.

V.A Présentation

- Ce protocole est nécessaire pour les ponts (*Bridge*) et les commutateurs (*Switch*) Ethernet fonctionnant en '*Transparent Bridging*'.
- Une **architecture redondante** engendre des **boucles de niveau 2** où les informations envoyées risquent de circuler indéfiniment sur votre réseau, occupant inutilement de la bande passante et pouvant rapidement saturer le réseau. Une telle architecture élimine les points de défaillance uniques qui mettraient en panne l'ensemble du réseau.
- Le but de cet algorithme (STA) est de créer dynamiquement un seul chemin de **niveau deux** entre deux LAN ou VLAN. Le fonctionnement de cet algorithme repose sur la théorie des graphes.
- La mise en œuvre de ce protocole n'est pas nécessaire, si un seul chemin de niveau 2 est présent entre segments LAN.



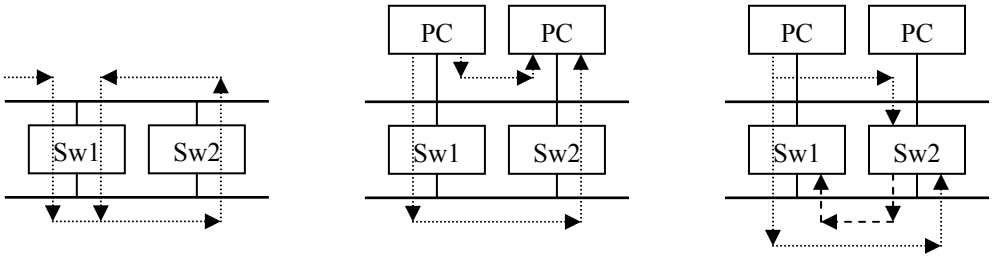
- Le STP (*Spanning Tree Protocol*) permet de mettre en « *Standby* » certaines connections en s'échangeant des **CBPDU** (*Configuration Bridge Protocol Data Unit* : **Message de configuration** des ponts).
- Attention au délai de convergence, il est très important (50 secondes par défaut).
- La répartition de charge est impossible entre ponts, mais possible sur des switchs en alternant les '*Root Switch*' entre VLAN.

- Le STP explore continuellement le réseau afin de détecter rapidement la défaillance ou l'ajout d'une liaison, d'un commutateur ou d'un pont. Lorsque la topologie du réseau change, le STP reconfigure les ports du pont ou du commutateur pour éviter une perte totale de connectivité ou la création de nouvelles boucles.

V.B Problèmes des boucles

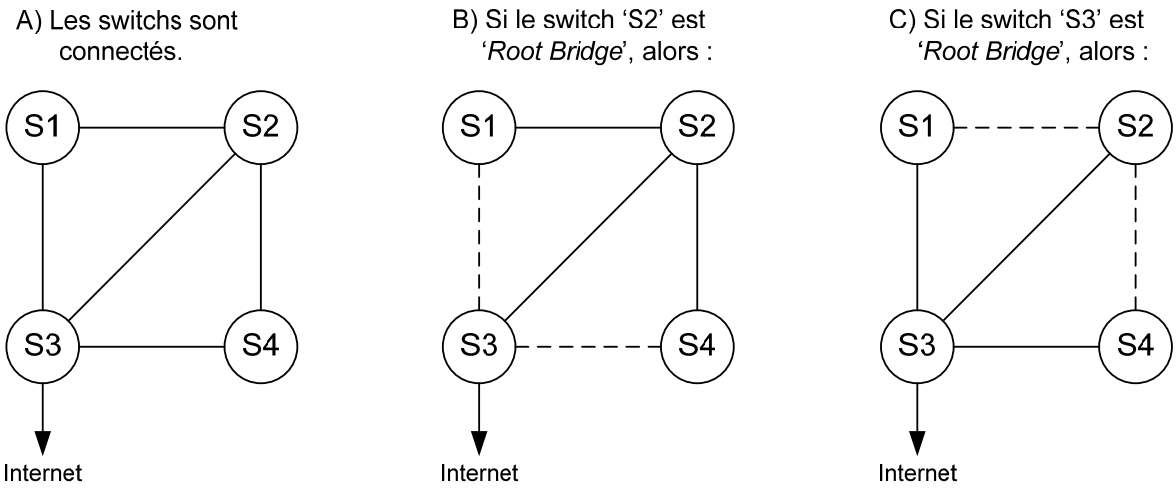
- Les problèmes des boucles de niveau 2 :

1. Lors d'un Broadcast (trame donc l'adresse MAC destination : FFFF-FFFF-FFFF) ou d'un Multicast, les ponts inondent (flood) les réseaux en dupliquant les trames.
2. Lors d'un Unicast, les ponts dupliquent les trames ce qui donne de multiple copies à l'arrivée.
3. Lors d'un Unicast, les tables (FDB : Forwarding Data Base) sont instables car le pont voit une adresse MAC source sur ses différentes interfaces.



V.C Optimisation

- Le choix du '*Root Bridge*' est fondamental dans une architecture switchée, car il déterminera la circulation optimale des trames dans un réseau redondant.



V.D Pontage vs commutation

Pontage	Commutation
Principalement basé sur le logiciel	Principalement basé sur du hardware (ASIC)
Une instance de STP par pont	Plusieurs instances de STP par commutateur
Généralement un maximum de 16 ports par pont	Ports plus nombreux sur un commutateur

V.E Half-suplex vs Full-duplex

Half-duplex (HDX)	Full-duplex (FDX)
Flot de données unidirectionnel	Flot de données bidirectionnel
Présence de collision (LAN)	Absence de collision (MAN)
Respect total du CSMA/CD	Circuit de détection des collisions désactivé
	Nécessite que le Full-duplex soit pris en charge aux deux extrémités (à chaque NIC)

V.F STP Tiebreakers

Tiebreakers : départager

- Sur les équipements CISCO, quand dans une condition il y a égalité, la décision finale est basée sur la séquence de conditions suivantes :

Référence : *CISCO Field Manuel : Catalyst Switch Configuration* de *CISCO Press*, page 177		
1	The lowest BID	Le '*Bridge Id*' le plus faible (pour la désignation du 'Bridge Root' uniquement)
2	The lowest Root Path Cost	Le '*Root Path Cost*' le plus faible
3	The lowest sender BID	Le '*Bridge Id*' de l'émetteur le plus faible
4	The lowest port ID	Le '*Port ID*' le plus faible

- Attention : dans plusieurs documents traitant du STP, quand dans une condition il y a égalité, la décision finale est basée sur la séquence de conditions suivantes :

  1. le '*Root Path Cost*' le plus faible
  2. Le '*Port ID*' le plus faible
  3. Le '*Bridge Id*' de l'émetteur le plus faible

V.G Description de fonctionnement

- les commutateurs (ponts) exécutant l'algorithme '*Spanning Tree*' échangent des messages de configuration (CBPDU) avec les autres commutateurs (ponts) à intervalles réguliers via une trame multicast. Par défaut, la CBPDU est envoyée toutes les deux secondes.

- La configuration du '*Spanning Tree*' des équipements, ponts ou commutateurs, se déroule **en 4 phases** :

1. **Élection du pont racine** (*Root Bridge*) : parmi tous les ponts, un seul sera désigné pont racine. C'est le '*Bridge ID*' le plus petit qui désignera le '*Root Bridge*'.

   - le Spanning Tree définit d'abord un pont racine (***Root Bridge***) qui est le point de départ du chemin de circulation. En général, le pont racine est un commutateur possédant une bande passante importante, donc souvent localisé au cœur du réseau (*Backbone*). Tous les ports de ce pont sont placés dans un état passant (*Forwarding*) et nommés port désigné (***Designated Port***). En état passant (*Forwarding*), un port peut émettre et recevoir du trafic.

2. **Élection du port racine** (*Root Port*) : désigne le port permettant à son pont d'atteindre le pont racine au moindre coût. Dans l'ordre des priorités : le '*Root Path Cost*', le '*Bridge ID*', puis enfin le 'PortID'.

   - Après l'élection du pont racine, **sur tous les ponts non racine**, le STA (*Spanning Tree Algorithm*) calcule une valeur relative pour chaque port de chacun des ponts ou switchs. Cette valeur est une représentation numérique du chemin à parcourir entre le port concerné et le '*Root Bridge*'. Elle s'appelle '*Root Path cost*'. le port ayant le plus bas coût administratif (RPC) pour atteindre le pont racine sera désigné port racine (***Root Port***). Cette interface est placée dans l'état passant (*Forwarding*).

3. **Élection du port désigné** (*Designated Port*) : désigne le port permettant à un réseau d'atteindre le pont racine au moindre coût.

   - Un segment peut être interconnecté au pont racine par plusieurs chemins. Ces ponts annoncent au moyen de CBPDU leur coût administratif pour atteindre le pont racine. Le pont qui possède le coût administratif le plus faible sur ce segment est appelé pont désigné (***Designated Bridge***). L'interface du pont désigné à partir de laquelle cette CBPDU de plus faible coût a été envoyé, est appelée port désigné (***designated port***), et elle est placée dans un état '*Forwarding*' (passant).

4. **les boucles de niveau deux sont supprimées**

   - Tous les ports qui ne sont pas '*Root Port*' ou '*Designated Port*' sont mis dans l'état '*Blocking*'.

V.H Paramètres de fonctionnement

- Paramètres Réseau :
  - Le '*Hello time*' : fréquence à laquelle un '*Designated port*' envoie des CBPDU, 2 s par défaut.
  - Le '*Forward delay*' : passage de l'état '*Listening learning*' à l'état '*Forwarding*', 15 s par défaut.
  - Le '*Max Age*' : délai respecté par un pont avant de décider que la topologie du réseau à changer.

- Paramètres liés au pont ou switch :
  - Le '*Bridge Priority*' (per bridge), valeur par défaut : 32768 ;
  - Le '*Root Path cost*', coût total vers le '*Root Bridge*'.

- Paramètres liés au port :
  - Le '*Port cost*' (per port) : Coût de transmission d'une trame sur un segment. Par défaut 1000/débit en M bps ;
  - Le '*Root Path cost*' : coût total vers le '*Root Bridge*'. Le pont calcul son RPC en ajoutant son '*Port Cost*' au RPC reçu.
  - Le '*Port Priority*' (per port) : priorité du port, valeur par défaut 128.

Default STP Configuration	
Caractéristique	**Configuration par défaut**
Enable state	Enabled on VLAN 1. Up to 64 spanning-tree instances can be enabled.
Mode de Spanning Tree	PVST (PVRST and MSTP are disabled).
Switch Priority (Pont) 0 (high) < *Bridge Priority* < 65535 (low)	32.768
Port Priority (interface) 0 (high) < *Port Priority* < 255 (low)	128
Port cost (interface)	1000 Mbps : 4. 100 Mbps : 19. 10 Mbps : 100.
Hello time	2 seconds
Forward-delay time	15 seconds
Maximum-aging time	20 seconds

PVST Per-VLAN Spanning Tree, s'annonce en IEEE 802.3 avec LLC-SNAP (OUI : 0x00000C et Ethertype : 0x010B)
PVRST Per-VLAN Rapid Spanning Tree ou IEEE 802.1W (disponible seulement en EI)
MSTP Multiple Spanning Tree Protocol ou IEEE 802.1S (disponible seulement en EI)

EI Enhanced Software Image, disponible sur Catalyst 2950C-24
SI Standard Software Image, disponible sur Catalyst 2950-24

- L'état '*Blocking*' autorise la réception et l'émission de CBPDU, mais interdit tout autre trafic.

- Les BPDU sont encapsulées dans des trames IEEE 802.2 (LLC) de type 1 (sans connexion ni acquittement).
- Elles emploient une adresse Multicast : 01-80-C2-00-00-00 et un SAP = 0x42.
- De plus, une adresse Multicast d'administration est définie pour tous les réseaux : 01-80-C2-00-00-10.
- Pour des évolutions futurs 15 adresses sont réservées : 01-80-C2-00-00-01 à 01-80-C2-00-00-0F.

- Le temps de construction du Spanning Tree :

(Nombre_de_niveau + 1)* 'Hello Time'

V.I Format des BPDU

BPDU : Bridge Protocol Data Unit

TC : Topology Change
TCA : Topology Change Acknowledgment

- Les Configurations BPDU sont émises périodiquement par le pont racine sur ses réseaux. Les ponts qui les reçoivent, transmettent à leur tour des CBPDU sur tous les réseaux qu'ils connectent, et propagent ainsi l'identificateur du '*Root Bridge*', tout en incrémentant le 'Root *Path* Cost' en fonction du dernier réseau traversé ('*Port Cost*' du port de réception).

- Ces CBPDU partent donc de la racine et se répercutent sur chaque branche de l'arbre, jusqu'aux extrémités. Notez qu'ils transportent les paramètres imposés par le '*Root Bridge*', tels que : l'age maximum d'un message, l'intervalle HELLO, et le délai de retransmission.

- Les messages émis par la racine ont un age de 0, et sont retransmis avec ce même age le long des branches du réseau. Cependant, si un pont du réseau ne reçoit plus de CBPDU temporairement, il va continuer à émettre périodiquement le même message (toutes les 2 secondes), en faisant croître l'age du message relativement à celui dont il est déduit. Il indique ainsi que son information d'origine n'est pas parfaitement d'actualité, mais commence à vieillir. Passé le délai '*Max Age*' (20 secondes recommandé), l'information provenant de la racine à partir de laquelle sont construits ces CBPDU est supprimé, et le pont redéfinit le chemin vers la racine ('*Path Cost*' et '*Root Port*') à partir des autres informations qu'il reçoit.

Message de configuration		
Octets	**Champ**	**Description**
2	Protocol ID	Identificateur de protocole : 0x0000
1	Version	Version : 0x00
1	BPDU Type	Type de message : 0x00
1	Flags	Indicateurs : les bits TC et TCA :
8	Root ID	Identifiant du '*Root Bridge*' : cette identifiant est constitué d'une priorité sur deux octets (par défaut 0x8000 ou 32.768) puis des six premiers octets de l'adresse MAC général du pont ou Switch.
4	Root Path Cost	Valeur binaire non signée qui représente le coût total, du pont qui transmet la CBPDU au pont cité dans le champ '*Root ID*'.
8	Bridge ID	Identifiant du pont : cette identifiant est constitué d'une priorité sur deux octets (par défaut 0x8000 ou 32.768) puis des six premiers octets de l'adresse MAC général du pont ou Switch.
2	Port ID	Identificateur de port : priorité du port (de 0 à 255) puis le numéro de port.
2	Message Age	Age du message : Temps estimé, en 1/256° de secondes, qui s'est écoulé depuis que la racine a transmis, pour la première fois, son message de configuration, sur lequel repose l'information contenue dans ce message.
2	Maximum Time	Durée de vie max : Temps estimé, en 1/256° de secondes, au bout duquel un message de configuration doit être détruit.
2	Hello Time	Temps de signalisation entre deux émissions de CBPDU (2 secondes par défaut). Ce temps est donné en 1/256° de secondes.
2	Forward Delay	Retard d'acheminement : durée, en 1/256° de secondes, temps pendant lequel les ponts doivent rester dans l'état bloqué (*Blocking*) avant de passer dans l'état émission (*Forwarding*).

Notification de changement de topologie		
Octets	**Champ**	**Description**
2	Protocol ID	Identificateur de protocole : 0x0
1	Version	Version : 0x0
1	Message Type	Type de message : 0x80

Root Identifier / Bridge Identifier (8 octets)	
MSB (2 octets)	**LSB (6 octets)**
Bridge Priority (default)	Address MAC
0x8000	00:0C:30:4C:2D:60

Port Identifier (2 octets)	
MSB (1 octet)	**LSB (1 octet)**
Port Priority (default)	Numéro de port
0x80	0x01

- Les BPDU de notification de changement de topologie sont émises par un pont qui ne reçoit plus message HELLO.

- les échanges de message CBPDU provoquent :
  - L'élection du *Root Switch* pour obtenir un Spanning-Tree stable dans une topologie réseau.
  - L'élection d'un *Designated Switch* pour chaque segment switché.
  - La suppression de boucle de niveau 2.

Format des trames BPDU

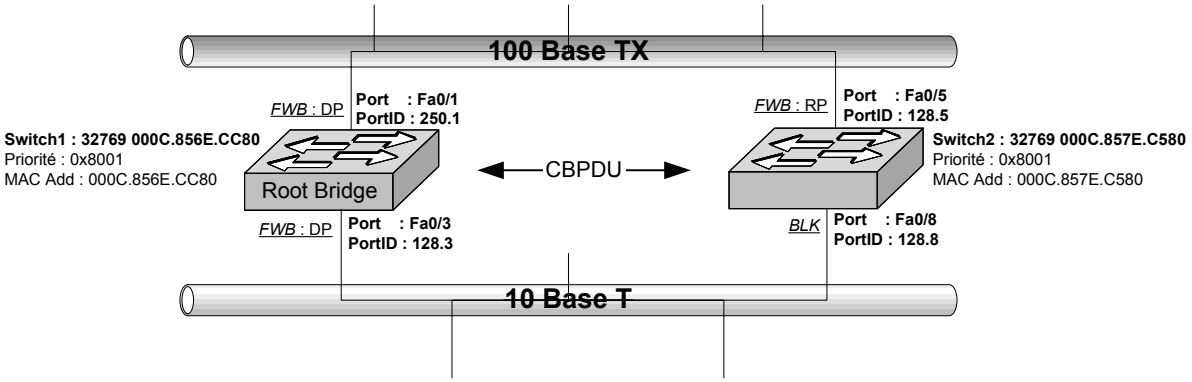
	0	15	16	31
1	Protocol ID		Version	Message type
2	Flags	n/a		
3	RootID			
4				
5	Root Path Cost			
6	BridgeID			
7				
8	PortID		Message age	
9	Max age		Hello Time	
10	Forward Delay		n/a	

V.J Election du Root Bridge

Octets	Champ
2	Protocol ID
1	Version
1	Message Type
1	Flags
8	Root ID
4	Root Path Cost
8	Bridge ID
2	Port ID
2	Message Age
2	Maximum Time
2	Hello Time
2	Forward Delay

1. Au démarrage le pont suppose qu'il est le '*Root Bridge*' et transmet des CBPDU (message de configuration) avec dans le champ '*Root ID*' son identifiant '*Bridge ID*' (Priorité et Adresse MAC).
2. Le pont, ayant le '*Bridge ID*' le plus faible, sera élu '*Root Bridge*'.
3. Par échange de CBPDU, les ponts déterminent lequel sera '*Root Bridge*'.

- Lorsqu'un pont essaie de devenir '*Root Bridge*', il émet un CBPDU toutes les (Hello Time) secondes pour poser sa candidature en tant que '*Root Bridge*' :
  - Si un pont à un '*Bridge ID*' plus petit que celui du candidat, il reste '*Root Bridge*' et émet toujours son message « Hello, i am the root bridge » toutes les (Hello Time) secondes.
  - Par contre, si son '*Bridge ID*' est plus grand que le '*Root ID*', il accepte le candidat comme '*Root Bridge*', et arrête l'émission de ses CBPDU mais propage les CBPDU du '*Root Bridge*' toutes les (Hello Time) secondes.



- Le pont et le Switch ont une adresse MAC générale affectée.
- L'adresse MAC d'un port est égale à l'adresse MAC général du pont plus le numéro du port.

- Le '*Root Bridge*' est '*Designated Bridge*' sur les LAN auxquels il est connecté.

- Le Switch avec la plus grande priorité (la plus faible valeur numérique : Switch Priority / Add MAC) est élu Root Switch par échanges de CBPDU. Si tous les switchs sont configurés avec la priorité par défaut (32768 ou 0x8000), c'est le switch avec l'adresse MAC la plus petite sur le réseau de niveau 2 qui devient Root Switch.
- Le '*Root Switch*' est le centre logique d'une topologie Spanning-Tree dans un réseau switché.

V.K Calcul du Root Path Cost

Octets	Champ
2	Protocol ID
1	Version
1	Message Type
1	Flags
8	Root ID
4	Root Path Cost
8	Bridge ID
2	Port ID
2	Message Age
2	Maximum Time
2	Hello Time
2	Forward Delay

- Le RPC : le '*Root Path Cost*' (coût du chemin racine) est un coût cumulé basé sur la bande passante de toutes les liaisons du chemin.

- Le '*Port Identifier*' : priorité du port (de 0 à 255) puis le numéro de port.

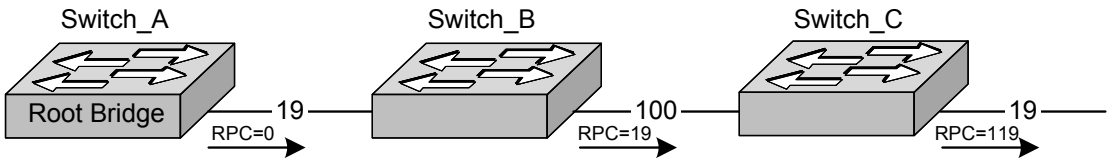
Coût par défaut des interfaces :		
Débit de la liaison	**Coût (spécification IEEE révisée)**	**Coût (ancienne spécification IEEE)**
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

- La spécification IEEE 802.1d a été révisée. Au départ, le coût était calculé sur la base de 10^9 divisé par la bande passante de la liaison en bps. Actuellement les coûts s'ajustent pour s'adapter aux interfaces à plus haut débit (1 Gbps et 10 Gbps).

Info

Pour les Catalyst 1900, l'IOS applique l'ancien calcul pour les coûts Spanning Tree. Sur les Catalyst 2900, l'IOS tient compte des calculs révisés.

- Le '*Root Path Cost*' : coût total cumulé vers le '*root bridge*'. Lors de l'envoi d'une BPDU, le '*Port Cost*' du port qui a reçu la BPDU est ajouté au '*Root Path Cost*' du pont précédent.



- Le '*Port Cost*' est fonction de la bande passante du port mais il peut être modifié manuellement par l'administrateur réseau.

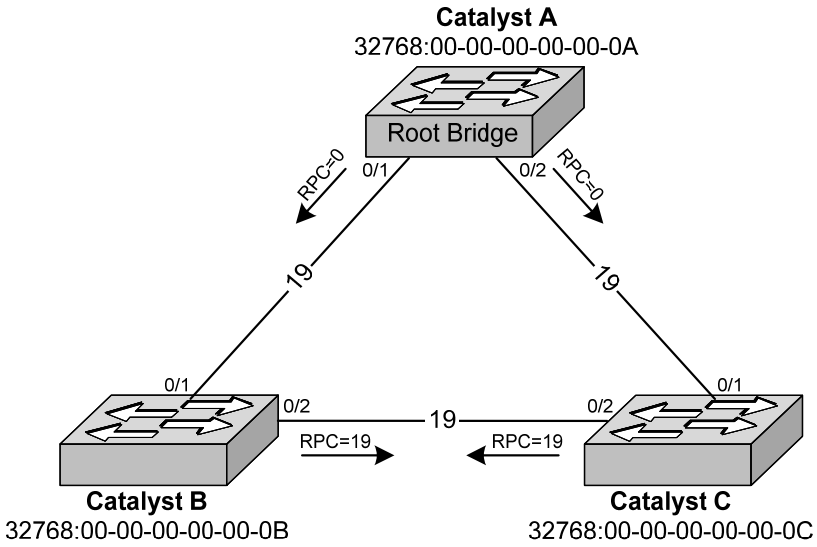
V.L Élection du Root Port

- **Élection du port racine** (`Root Port`) : désigne le port permettant à son pont d'atteindre le pont racine au moindre coût pour tous les ponts non '`Root Bridge`'. Dans l'ordre des priorités :

  - Le '`Root Path Cost`' le plus faible. Ici le port 0/1 du Catalyst B a un RPC de 19 contre un RPC de 38 pour le port 0/2. Idem pour le catalyst C.

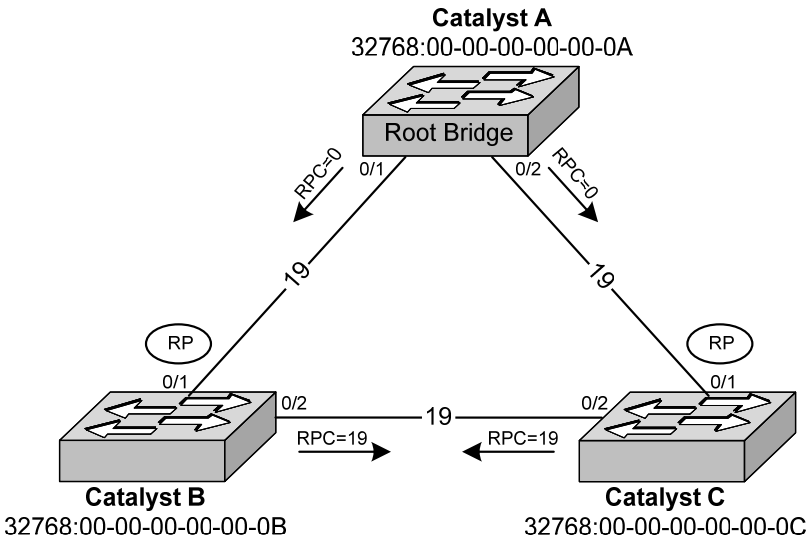
  - Le '`Bridge ID`' le plus faible reçu du switch qui émet la CBPDU.

  - Le '`PortID`'. Le port qui reçoit le plus faible '`PortID`' contenu dans les CBPDU émis par les switchs voisins, devient '`Root Port`'.



V.M Élection du Designated Port

- **Élection du port désigné** (`Designated Port`) : désigne le port permettant à un réseau d'atteindre le pont racine au moindre coût.
    - Le '`Root Path Cost`' le plus faible. Ici les ports 0/2 des deux Catalyst B et C ont le même RPC (38).
    - Le '`Bridge ID`' du switch émetteur le plus faible. Ici le port 0/2 du Catalyst B est '`Designated Port`' car le '`Bridge ID`' du 'Catalyst B' est inférieur à celui du 'Catalyst C'.
    - Le '`PortID`' : C'est le '`PortID`' le plus faible de tous les '`PortID`' contenu dans les CBPDU émis par les switchs voisins.



Info

Tous les ports d'un '`Root Bridge`' sont '`Designated Port`'.

- Sur Catalyst 2950

```
Switch1# show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     000c.304c.2d60
              Cost        100
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000c.856e.cc80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Port ID                    Designated                 Port ID
Name             Prio.Nbr      Cost Sts     Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1            128.1          100 FWD         0 32768 000c.304c.2d60 128.43
Fa0/2            128.2          100 FWD       100 32769 000c.856e.cc80 128.2

Switch1#
```

Root Path Cost

Le port FA0/2 du Switch 'Switch1' a comme caractéristiques :
- Actif (FWD)
- Son '*Port Priority*' = 128.2
- Avec un coût de 100 (10BaseT)

Cette zone indique où est connecté le port FA0/2 du 'Switch1' :
- Le Switch '000C.856ECC80'
- avec un '*Bridge Priority*' de 32769
- et sur son port FA0/2 avec un '*Port Priority*' de 128.2
- Le Switch1 a un coût de 100 pour atteindre le '*Root Bridge*' via son port FA0/1.

- Sur C2621 + ESW

```
CK160#show spanning-tree active brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     000e.d710.4f00
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     000e.d710.4f00
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 0

Interface                                  Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/8      128.49   128    19 FWD     0 32768 000e.d710.4f00 128.49

CK160#
```

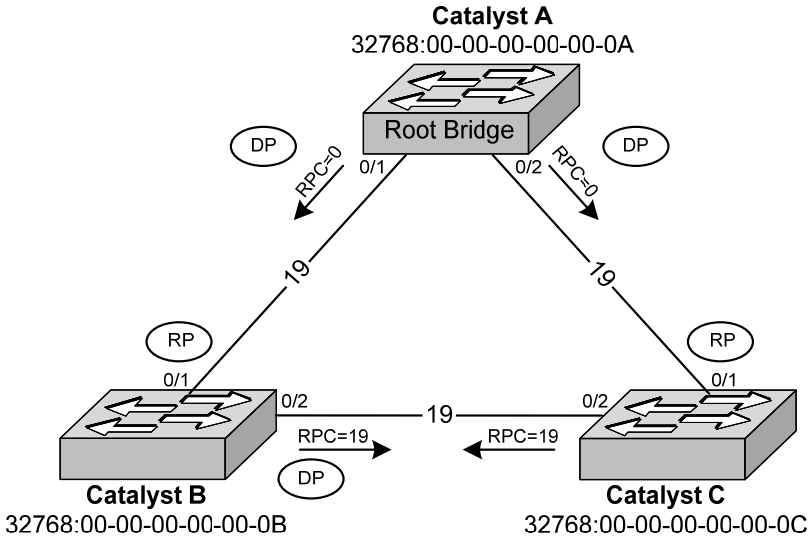
V.N Les boucles de niveau deux sont supprimées

- Sur chaque réseau éloigné du '*Root Bridge*', c'est le pont qui propose le plus faible coût du chemin vers la racine, est nommé '*Designated Bridge*' (pont désigné).

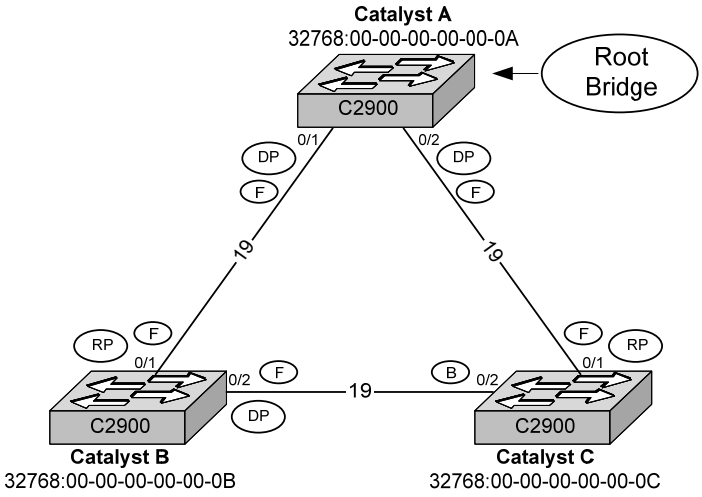
- De même, chaque '*Designated Bridge*' à un '*Root Port*' (Port Racine) qui mène au '*Root Bridge*',

  - les autres ports, offrants cet accès à des réseaux plus éloignés, sont déclarés '*Designated Ports*' (Ports désignés).
  - Les ports qui participent à créer des boucles sont mis en mode '*Blocking*' (Bloqué), à l'exception de l'écoute des paquets CBPDU.

- Notez qu'avant que la configuration ne soit stabilisée, les ponts s'échangent des informations mais ne retransmettent pas les trames des trafics réels qu'ils reçoivent, et n'apprennent pas encore les adresses MAC.



V.O Synthèse



1. Election du '*Root Bridge*' :
   - Tous les switchs ont la même priorité (32768, valeur par défaut).
   - Toutefois, le 'Catalyst A' a l'adresse MAC la moins élevée (00-00-00-00-00-0A), ce qui lui permet de devenir le '*Root Bridge*'.

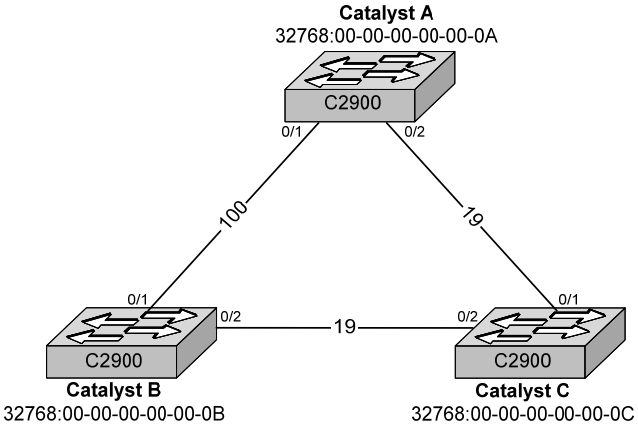
2. Election des '*Root Ports*' :
   - Les switchs calculent les RPC pour atteindre le '*Root Bridge*'.
   - Comme les ports 0/1 des 'Catalyst B' et 'Catalyst C' ont le plus petit RPC (0 + 19) pour atteindre le '*Root Bridge*', ils deviennent '*Root Port'*.

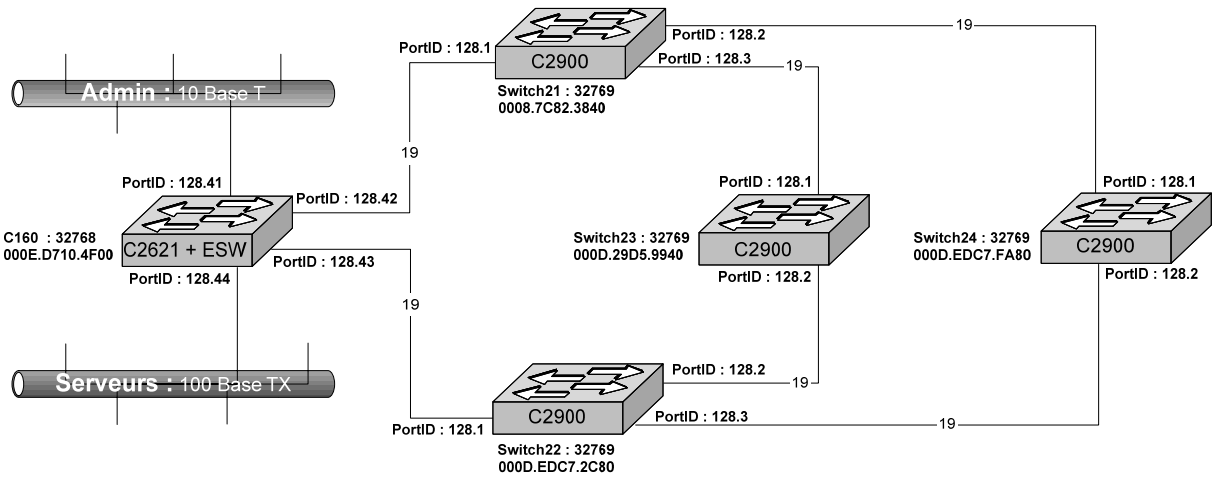
3. Election des 'Designated Ports' :
   - Par définition, tous les ports d'un '*Root Bridge*' sont '*Designated Port*'.
   - Comme le segment entre les switchs 'Catalyst B' et 'Catalyst C' a le même RPC par le 'Catalyst B' ou par le 'Catalyst C', c'est le '*Bridge ID*' le plus faible qui désigne le '*Designated Port*' du segment. Ici le 'Catalyst B' a un '*Bridge ID*' plus faible que celui du 'Catalyst C' donc c'est le ports 0/2 du 'Catalyst B' qui devient 'Designated *Port'*.

4. Tous les ports qui ne sont pas '*Root Ports*' ou '*Designated Ports*' sont mis dans l'état '*Blocking*'.
   - Comme le port 0/2 du 'Catalyst C' est ni '*Root Port*' et ni '*Designated Port*', alors le STA le met dans l'état '*Blocking*'.

V.P Exercices

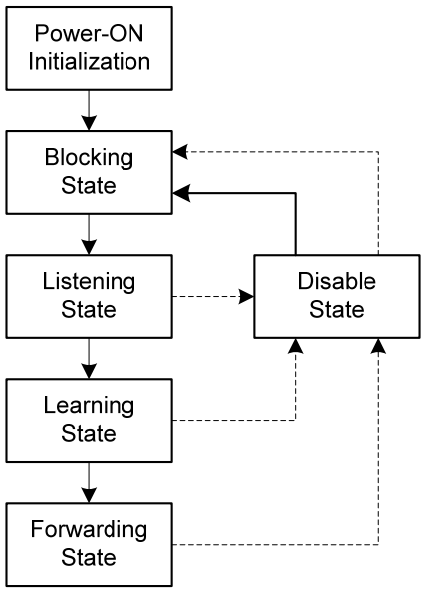
- Pour les deux schémas ci-dessous, indiquez :
  - le switch '*Root Bridge*', et
  - les ports '*Root Port*' et '*Blocking Port*'.



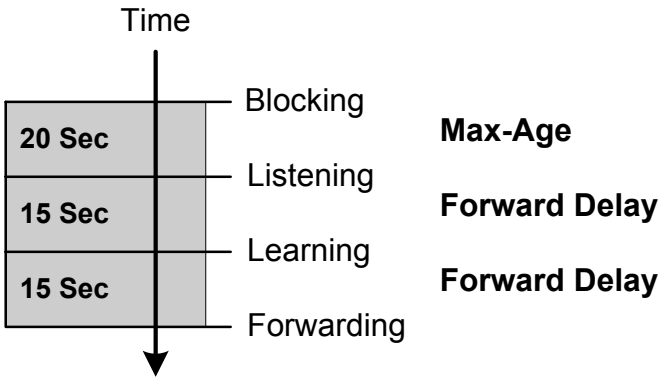


V.Q État des ports en STP

- Each Layer 2 interface on a switch using spanning tree exists in one of these states:
  - Blocking : The interface does not participate in frame forwarding.
  - Listening : The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
  - Learning : The interface prepares to participate in frame forwarding.
  - Forwarding : The interface forwards frames.
  - Disabled : The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.



- Blocking/bloquant : pas de trafic à travers ce port, reçoit seulement les CBPDU
- Listening/écoute : pas de trafic à travers ce port, stoppent les CBPDU
- Learning/découverte : pas de trafic à travers ce port, construit sa FDB
- Forwarding/transmission : trafic utilisateur, transmission et réception de CBPDU
- Disable/désactivé : l'interface est arrêtée



Ports	État des ports	Commentaires
Tous les ports d'un pont racine	Passant (*Forwarding*)	Le pont racine est le pont désigné pour l'ensemble des segments
Port racine (*Root Port*)	Passant (*Forwarding*)	Le port racine est celui qui reçoit les CBPDU de plus faible coût de la part du pont racine.
Port désigné (*Designated Port*)	Passant (*Forwarding*)	Le pont désigné est celui qui envoie les CBPDU de plus faible coût sur chaque segment.
Autres ports	Bloquant (*Blocking*)	Les autres ports ne peuvent ni envoyer ni recevoir de trames autres que les CBPDU.

- **Blocking State**. A Layer 2 interface in the blocking state does not participate in frame forwarding. After initialization, a BPDU is sent to each interface in the switch. A switch initially functions as the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is the root or root switch. If there is only one switch in the network, no exchange occurs, the forward-delay timer expires, and the interfaces move to the listening state. An interface always enters the blocking state after switch initialization. An interface in the blocking state performs as follows:

  - Discards frames received on the port
  - Discards frames switched from another interface for forwarding
  - Does not learn addresses
  - Receives BPDUs

- **Listening State**. The listening state is the first state a Layer 2 interface enters after the blocking state. The interface enters this state when the spanning tree determines that the interface should participate in frame forwarding. An interface in the listening state performs as follows:

  - Discards frames received on the port
  - Discards frames switched from another interface for forwarding
  - Does not learn addresses
  - Receives BPDUs

- **Learning State**. A Layer 2 interface in the learning state prepares to participate in frame forwarding. The interface enters the learning state from the listening state. An interface in the learning state performs as follows:

  - Discards frames received on the port
  - Discards frames switched from another interface for forwarding
  - Learns addresses
  - Receives BPDUs

- **Forwarding State**. A Layer 2 interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state. An interface in the forwarding state performs as follows:

  - Receives and forwards frames received on the port
  - Forwards frames switched from another port
  - Learns addresses
  - Receives BPDUs

- **Disabled State**. A Layer 2 interface in the disabled state does not participate in frame forwarding or in the spanning tree. An interface in the disabled state is nonoperational. A disabled interface performs as follows:

  - Discards frames received on the port
  - Discards frames switched from another interface for forwarding
  - Does not learn addresses

V.R Étude de cas

1. Conditions initiales

```
Switch1#show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.856e.cc80
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.856e.cc80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1            128.1          100 FWD         0 32769 000c.856e.cc80 128.1
Fa0/3            128.3          100 FWD         0 32769 000c.856e.cc80 128.3

Switch1#
```

```
Switch2#show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.856e.cc80
             Cost        100
             Port        5 (FastEthernet0/5)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.857e.c580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/5            128.5          100 FWD         0 32769 000c.856e.cc80 128.1
Fa0/8            128.8          100 BLK         0 32769 000c.856e.cc80 128.3

Switch2#
```

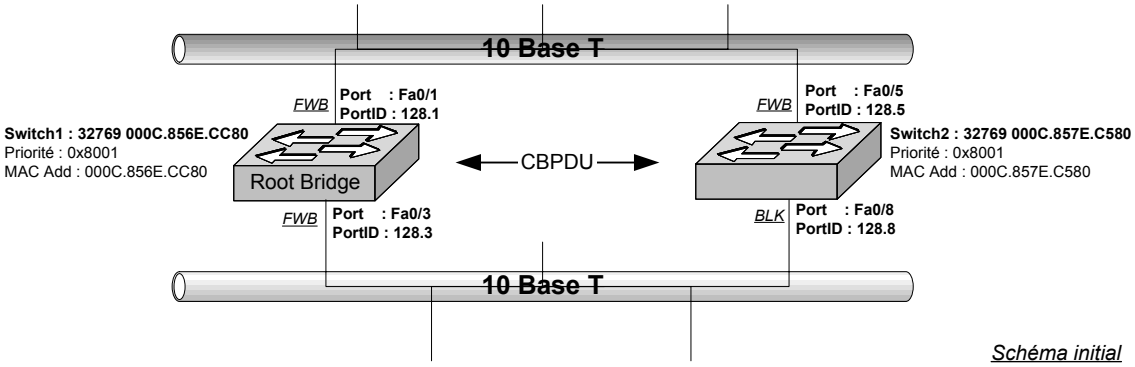


Schéma initial

2. Modification du numéro de port

   - Déconnectez de la prise mâle RJ45 en '*Switch1 Fa0/1*' pour la brancher en '*Switch1 Fa0/5*'
   - Observez le port '*Switch2 Fa0/5*' qui passe de l'état FWD (orange) en BLK (vert).

```
Switch2#show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000c.856e.cc80
              Cost        100
              Port        8 (FastEthernet0/8)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000c.857e.c580
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 15

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/5            128.5          100 BLK         0 32769 000c.856e.cc80 128.5
Fa0/8            128.8          100 FWD         0 32769 000c.856e.cc80 128.3

Switch2#
```

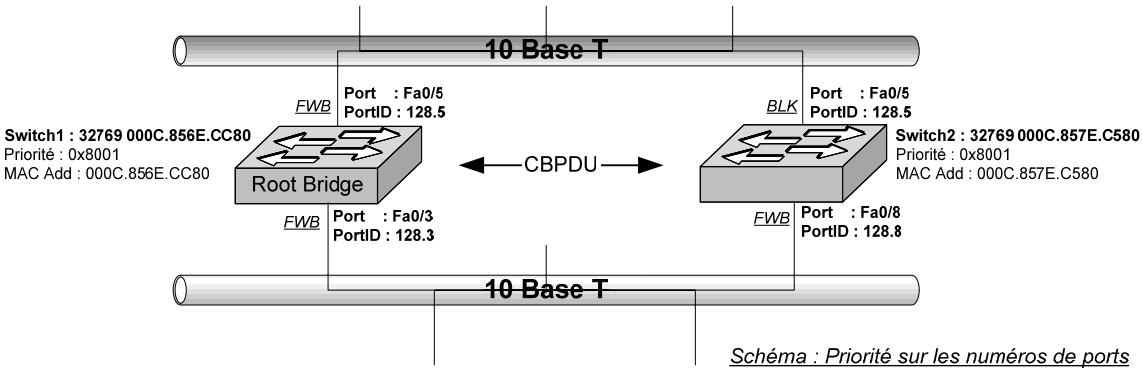


Schéma : Priorité sur les numéros de ports

- **Attention** : lorsque le RPC (*Root Path Cost*) est identique le choix du meilleur chemin est calculé à partir des éléments du pont de niveau supérieur.

3. Augmentation de la priorité

   - Augmentatez de la priorité du port '*Switch1 Fa0/1*' de 128 à 1
   - Le port '*Switch2 Fa0/5*' reste dans l'état FWD.

```
Switch1 #conf t
Switch1(config)#int fa0/1
Switch1(config-if)#spanning-tree port-priority ?
  <0-255>  port priority

Switch1(config-if)#spanning-tree port-priority 1
Switch1(config-if)#
```

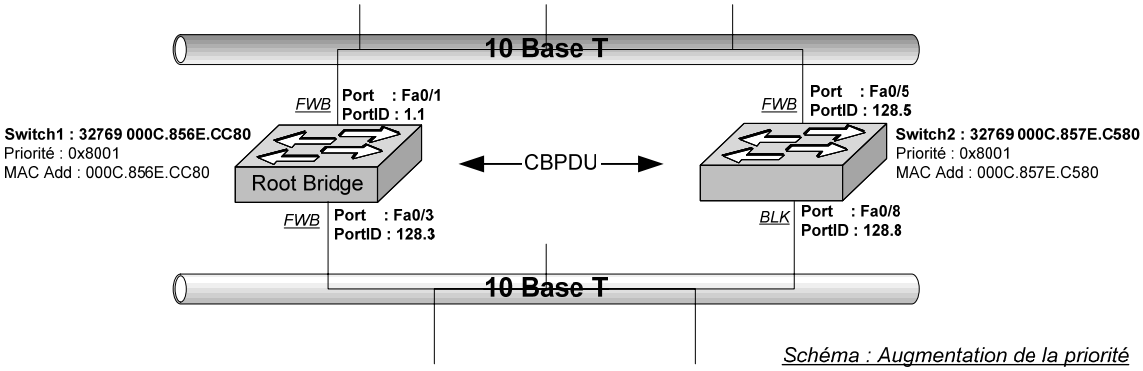


Schéma : Augmentation de la priorité

```
Switch2#sh spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000c.856e.cc80
              Cost        100
              Port        5 (FastEthernet0/5)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000c.857e.c580
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/5            128.5          100 FWD         0 32769 000c.856e.cc80   1.1
Fa0/8            128.8          100 BLK         0 32769 000c.856e.cc80 128.3

Switch2#
```

4. Diminution de la priorité

   - Diminuez de la priorité du port '*Switch1 Fa0/1*' de 128 à 250
   - Le port '*Switch2 Fa0/5*' passe de l'état FWD à l'état BLK.

```
Switch1 #conf t
Switch1(config)#int fa0/1
Switch1(config-if)#spanning-tree port-priority ?
  <0-255>  port priority

Switch1(config-if)#spanning-tree port-priority 250
Switch1(config-if)#
```

```
Switch2# show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000c.856e.cc80
              Cost        100
              Port        8 (FastEthernet0/8)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000c.857e.c580
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Port ID                    Designated                 Port ID
Name             Prio.Nbr      Cost Sts     Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/5            128.5          100 BLK         0 32769 000c.856e.cc80 250.1
Fa0/8            128.8          100 FWD         0 32769 000c.856e.cc80 128.3

Switch2#
```

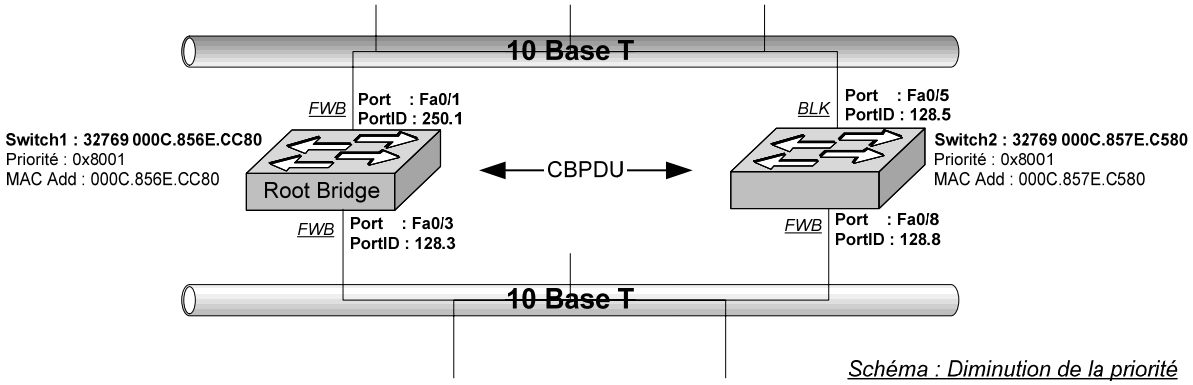


Schéma : Diminution de la priorité

5. Modification du débit

```
Switch2#show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000c.856e.cc80
              Cost        19
              Port        5 (FastEthernet0/5)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000c.857e.c580
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 15

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/5            128.5           19 FWD          0 32769 000c.856e.cc80 250.1
Fa0/8            128.8          100 BLK          0 32769 000c.856e.cc80 128.3

Switch2#
```

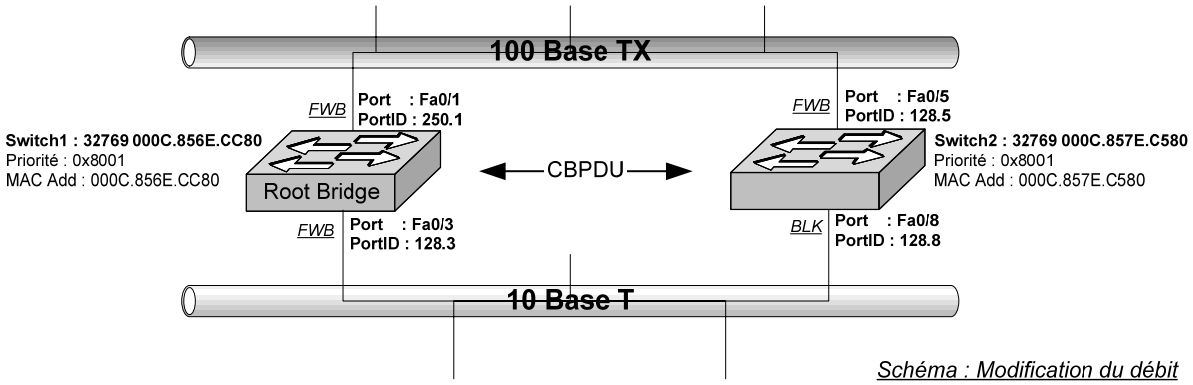


Schéma : Modification du débit

V.S Recalcul de l'arbre Spanning Tree

- Le moindre changement affectant le réseau (ajout ou panne d'un équipement) déclenche un nouveau calcul de chemin. Ce changement peut obliger certains ports qui étaient en mode '*Blocking*' à passer en mode 'Forwarding'.

- Un port en mode '*Blocking*' ne passe pas directement en mode 'Forwarding' : il passe par deux états intermédiaires avant de prendre le relais d'un port défaillant. D'abord il écoute (mode '*Listening*'), puis il apprend (mode '*Learning*').

    - La phase d'écoute permet au port de vérifier qu'il peut devenir 'Forwarding', tandis que
    - La phase d'apprentissage permet au port de construire sa table de commutation.

    - Ces différentes étapes augmentent considérablement la durée de transition du mode '*Blocking*' au mode 'Forwarding'.

- Chaque fois que la topologie du réseau change (lien brisé par exemple) l'algorithme du STP doit être recalculé. Typiquement, le temps de recalcul du chemin, appelé encore temps de convergence, prend environ 50 secondes, ce qui représente une durée extrêmement longue dans le monde des réseaux. Afin de réduire cette durée entre 2 et 5 secondes, CISCO apporte plusieurs améliorations au protocole Spanning Tree : UplinkFast et PortFast.

    - UplinkFast est particulièrement utile sur les switchs d'accès. Il ramène le temps de convergence à environ 2 secondes, en prédéfinissant un '*uplink*' primaire et un '*uplink*' redondant. Grâce à la technologie '*UplinkFast*', le switch se connecte rapidement au nouveau 'Bridge Root' : l'uplink redondant passe immédiatement du mode '*Blocking*' au mode 'Forwarding', sans avoir à passer par les deux états intermédiaires. Il retransmet ensuite l'information du changement de topologie à tous les autres switchs qu'il peut atteindre.

    - PortFast est dédié à la connexion des ordinateurs (station de travail, serveurs, etc.). lorsque PortFast est activé, les ports commutent directement du mode '*Blocking*' au mode 'Forwarding'.

- Enfin, le standard précise que le diamètre maximum recommandé de l'architecture est de 7 ponts. Cela signifie qu'au plus 7 ponts peuvent être traversés lors du passage entre deux réseaux distincts, soit aussi un diamètre maximum de 8 réseaux.

V.T Résumé

1) Toutes les interfaces d'un pont sont **stabilisées** dans un état de **transmission** ou **bloquant**. Les interfaces dans un état de transmission participent à l'arbre recouvrant.

2) Un des Switchs est élu comme pont racine (*Root Bridge*) de l'arbre. Ce processus d'élection implique tous les Switchs jusqu'à ce que l'un d'eux soit désigné. Toutes les interfaces du pont racine sont dans un état de transmission car le '*Root Bridge*' est le '*Designated Bridge*' des réseaux qu'il connecte.

3) Chaque Switch reçoit des CBPDU de la part du pont racine, soit directement, soit par l'intermédiaire d'un autre pont. Chaque pont peut en recevoir plusieurs sur ses interfaces, mais le port sur lequel la CBPDU de plus faible coût est reçue devient son port racine (*Root Port*) et son interface est placée dans un état de transmission.

4) Pour chaque segment LAN, un pont transmet la CBPDU possédant le plus faible coût.

5) Ce Switch est le pont désigné ('*Designated Bridge*') pour ce segment. L'interface du Switch de ce segment est placée dans un état de transmission.

6) Toutes les autres interfaces du Switch sont placées dans un état bloquant.

7) Les temporisateurs :

   - Le pont racine envoie des CBPDU selon un intervalle exprimé en secondes, donné par le temporisateur **HELLO**. Les autres ponts s'attendent à recevoir des copies retransmises de ces CBPDU, confirmant que rien n'a changé. La durée HELLO étant définie dans la CBPDU, tous les ponts utilisent la même valeur.

   - Si un pont ne reçoit pas de CBPDU alors que la durée **MAXAGE** a expiré, il débute le processus de changement de l'arbre recouvrant. La réaction peut varier selon la topologie. La durée MAXAGE étant définie dans la CBPDU, tous les ponts utilisent la même valeur.

   - Un ou plusieurs ponts décident alors de modifier l'état de leurs interfaces, de bloquant à celui de transmission, ou vice versa, selon la modification intervenue sur le réseau. Par exemple, avant de passer d'un état bloquant à un état de transmission, une interface est placée dans un état transitoire d'écoute. Après expiration du temporisateur **Forward Delay**, elle entre dans un état de découverte. Après une autre expiration de ce temporisateur, elle est alors placée dans un état de transmission.

   - Le protocole Spanning Tree prévoit ces temporisateurs pour éviter tout risque de boucles temporaires.

8) Le '*Root Bridge*' :
   a. Un par réseau (domaine de Broadcast Physique)
   b. Processus d'élection : '*Bridge ID*' le plus faible
   c. Confirmé élu à intervalle régulier ('*Hello Time*' toutes les 2 secondes)
   d. Configure les Timers des autres ports
   e. Tous les autres ports calculent le chemin le plus court vers le 'Root Bridge' ('*least Root Path Cost*')

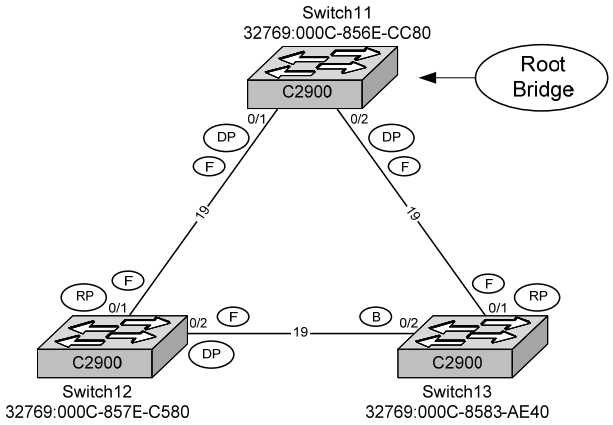
9) Le '*Root Port*' :
   a. Un par pont
   b. Port au '*least Root Path Cost*'
   c. Il reçoit toutes les BPDU envoyées par le '*Root Bridge*'
   d. État du port jamais bloquant

10) Le '*Designated Port*' :
   a. Port connectant le '*Designated Bridge*' au segment choisi
   b. Tous les trafics qui sortent du segment
   c. Transmission de BPDU vers les autres ponts
   d. Jamais dans état bloquant

11) Le '*Designated Bridge'*
   a. Au moins un par segment : il transmet les trames sur chaque segment
   b. Le 'Root Bridge' est toujours '*Designated Bridge*' pour le segment qu'il connecte
   c. Toujours le pont avec le plus court chemin vers le '*Root Bridge*'

V.U Action du 'Port Cost'

1. Conditions initiales :




```
Switch11#show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.856e.cc80
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.856e.cc80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1            128.1           19 FWD         0 32769 000c.856e.cc80 128.1
Fa0/2            128.2           19 FWD         0 32769 000c.856e.cc80 128.2

Switch11#
```

```
Switch12#show spanning-tree active

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1            128.1           19 FWD         0 32769 000c.856e.cc80 128.1
Fa0/2            128.2           19 FWD        19 32769 000c.857e.c580 128.2

Switch12#
```

```
Switch13#show spanning-tree active

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1            128.1           19 FWD         0 32769 000c.856e.cc80 128.2
Fa0/2            128.2           19 BLK        19 32769 000c.857e.c580 128.2

Switch13#
```

2. Modification du '*Port Cost*' sur le port 'FA0/1' du 'Switch11'

- Affectation d'un coût de 100 à l'interface 'FA0/1' du 'Switch11'

```
Switch11#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch11(config)#interface fastEthernet 0/1
Switch11(config-if)#spanning-tree vlan 1 ?
  cost           Change an interface's per VLAN spanning tree path cost
  port-priority  Change an interface's spanning tree port priority

Switch11(config-if)#spanning-tree vlan 1 cost 100
```

- Vérification sur le 'Switch12' et 'Switch13' : aucune modification

```
Switch12#show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.856e.cc80
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.857e.c580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1            128.1           19 FWD         0 32769 000c.856e.cc80 128.1
Fa0/2            128.2           19 FWD        19 32769 000c.857e.c580 128.2

Switch12#
```

- Cette configuration n'apporte aucune modification sur l'état des ports des switchs 'Switch11', 'Switch12' et 'Switch13'.

3. Modification du '*Port Cost*' sur le port 'FA0/1' du 'Switch12'

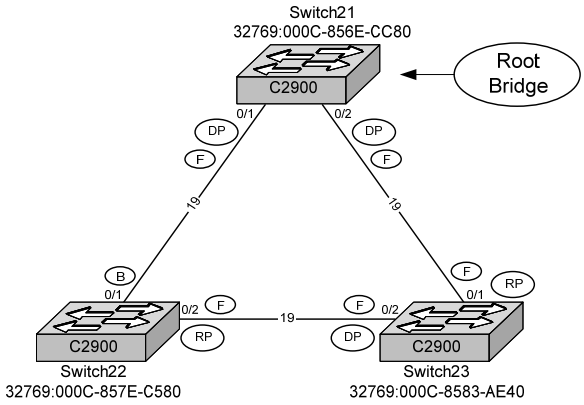
   - Affectation d'un coût de 100 à l'interface 'FA0/1' du 'Switch12'

```
Switch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch12(config)#int fastEthernet 0/1
Switch12(config-if)#spanning-tree vlan 1 cost 100
Switch12(config-if)#
```

   - Vérification sur le 'Switch12' et 'Switch13' :
     1. Le 'Root Switch' n'a pas changé, c'est toujours 'Switc11'.
     2. Mais, le port 'FA0/1' du 'Switch12' est passé en 'Blocking' au profit du port 'FA0/2' du 'Switch12'.

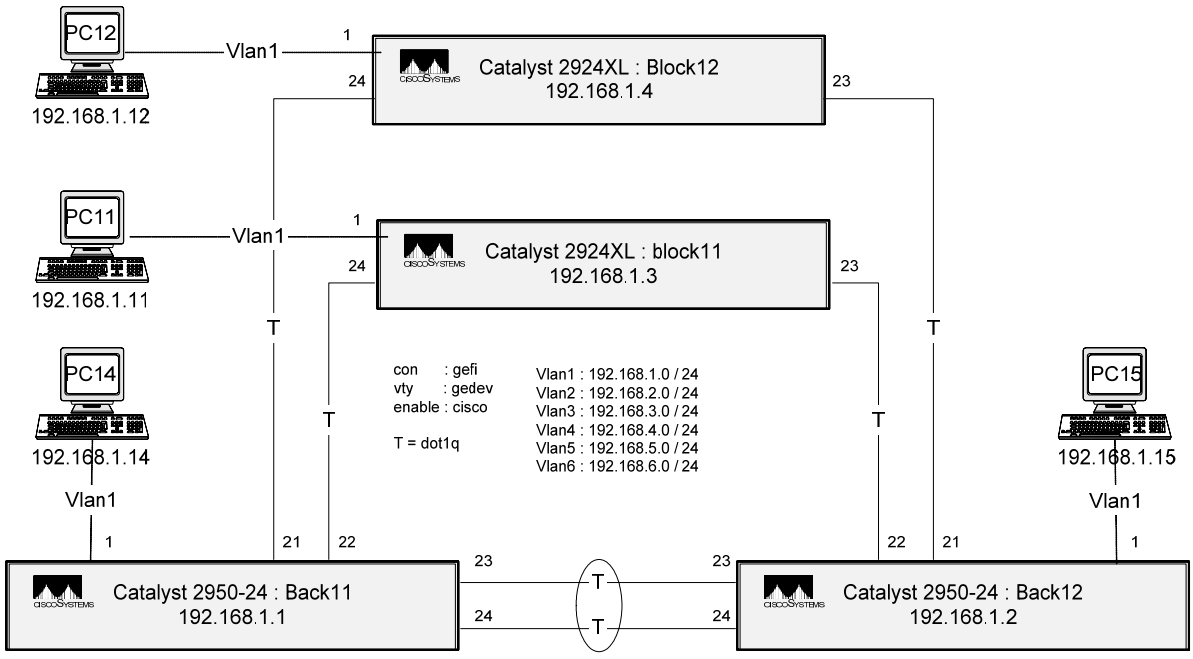
```
Switch12#show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000c.856e.cc80
              Cost        38
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000c.857e.c580
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1            128.1          100 BLK         0 32769 000c.856e.cc80 128.1
Fa0/2            128.2           19 FWD        19 32769 000c.8583.ae40 128.2

Switch12#
```

   - Cette configuration modifie les flux dans cette architecture.



V.V Root Switch & Secondary Root Switch

- Dans une solution redondante, on souhaite garder la maîtrise de la gestion des flux : si le '*Root Bridge*' (RB) tombe en panne, le switch qui le remplacera, aura été désigné auparavant.
- Pour cela, il faut prévoir un '*Secondary Root Bridge*' (SRB). Le SRB a une priorité intermédiaire entre le '*Root Bridge*' et la priorité par défaut (0x8000 ou 32768).



V.W Configuration

- Paramètres Réseau :
  - Hello time : fréquence à laquelle un 'Designated port' envoie des CBPDU, 2 s par défaut.
  - Forward delay : passage de l'état 'Listening learning' à l'état 'Forwarding', 15 s par défaut.
  - Max Age : délai respecté par un pont avant de décider que la topologie du réseau à changer.
  - Bridge Priority (per bridge) : intervalle codé sur 2 octets, de 1 à 65535 (32768_{10} ou Ox8000 par défaut).

- Paramètres liés au port
  - Port cost : Coût de transmission d'une trame sur un segment. Par défaut 1000/débit en M bps (exemple ; en 10 Base T = 100, en 100 Base FX, FDDI = 10, ATM = 6).
  - Path cost : coût total vers le 'root bridge'. Lors de l'envoi d'une BPDU, le 'port cost' du port précédent qui a reçu la BPDU est ajouté.
  - Port priority :

V.W.1 Présentation

- CISCO et le comité IEEE 802.1Q ont des approches très différentes concernant le Spanning Tree et les VLANS.

Les instances STP sur les VLANs :		
Protocole	**Méthode**	**Description**
ISL		Une instance par VLAN
802.1Q	CST : Common Spanning Tree	Une instance pour tous les VLANs. Le CST est la solution de l'IEEE 802.1Q pour le Spanning Tree et les VLANS.
	PVST : Per-VLAN Spanning Tree	Une instance par VLAN. Le PVST est une solution propriétaire CISCO
	PVST+	Le PVST+ est une solution propriétaire CISCO qui permet une compatibilité ascendante du CST dans PVST+.
802.1W	PVRST Per-VLAN Rapid Spanning Tree	
802.1S	MSTP Multiple Spanning Tree Protocol	

Le CST : Common Spanning Tree	
Avantages	**Inconvénients**
Moins de bande passante consommée	Un seul Root Bridge, pas d'optimisation réseau et switchs
Moins d'overhead processeur	Complexité de la topologie STP lorsque le réseau s'accroît

Catalyst	**Instance STP**	**VLAN**
2912 XL, 2924 XL, 2924C XL	64	64
2950-24	64	64
3500 XL	64	250

V.W.2 Les commandes

Spanning Tree Protocol	
Commandes	**signification**
(global) no spanning-tree vlan *vlan-id*	Désactivation du STP d'un VLAN
(global) spanning-tree vlan *vlan-id*	Activation du STP sur un VLAN
(global) spanning-tree [vlan *vlan-id*] protocol {ieee|ibm}	Spécification de l'implémentation STP utilisée pour l'instance STP. Actuellement cette commande est supprimée car on utilise le protocole IEEE 802.1Q par défaut.
(global) spanning-tree vlan *vlan-id* priority *bridge-priority*	**Switch Priority**. Configuration de la priorité du switch pour l'instance STP spécifiée. Entrez une valeur entre 0 et 65535 ; la valeur la plus faible donne au switch la plus grande chance d'être choisi comme 'root switch'.
(global) spanning-tree vlan *vlan-id* root primary	**Switch Priority**. Configuration de ce switch comme root switch primaire pour cette instance STP (PVST) : 0x2000
(global) spanning-tree vlan *vlan-id* root secondary	**Switch Priority**. Configuration de ce switch comme root switch secondaire en cas de disfonctionnement du root switch primary pour cette instance STP (PVST) : 0x4000
spanning-tree portfast	Désactive le STP sur le port '0/X'.
() conf t (global) int fa x/y spanning-tree [vlan *vlan-id*] cost *port-cost* end	**Path Cost**. Configuration du 'Path Cost' pour l'instance STP spécifiée, de 1 à 65535. valeur donnée en fonction du débit du port (9 en 100 BaseTX), mais paramétrable.
() conf t (global) int fa x/y (spanning-tree [vlan *vlan-id*] port-priority *port-priority* end	**Port Priority**, configuration de la priorité du port, puis pour l'instance STP spécifiée. Entrez une valeur de 0 à 255. La valeur la plus faible donne la priorité la plus forte.
() copy run start	Sauvegarde la configuration
() show spanning-tree bridge	État et configuration du STP
() show spanning-tree active	Visualisation de la config STP C2900
() show spanning-tree brief	Visualisation de la config STP sur C2621+ ESW
() show spanning-tree vlan 1 brief	Visualisation de la config STP
() show spanning-tree vlan *Vlan_ID*	
() show running-config	

- Le switch fonctionnant en PVST, on doit préciser le VLAN pour déclarer le '*Bridge Priority*'.
- Par contre, la déclaration du '*Port Cost*' et du '*Port Priority*' peut se faire de manière globale ou par VLAN.
    - Si vous précisez le 'Vlan-ID' dans la commande, le '*Port Cost*' et le '*Port Priority*' seront valides uniquement pour le VLAN spécifié, sinon ils actifs pour tous les VLAN de l'interface.

Définition de la priorité du port	
(interface) spanning-tree [vlan *vlan-id*] port-priority *Port-priority*	
Arguments	**Signification**
[vlan *vlan-id*]	Si le Vlan est spécifié, l'affectation ne concerne que ce Vlan. Sinon, la priorité est modifiée pour tous les Vlans de cette interface.
Port-priority	Valeur de la priorité : de 0 à 255. La valeur la plus faible donne la priorité la plus forte.
(interface) spanning-tree port-priority *2*	

Définition du coût du port	
(interface) spanning-tree [vlan *vlan-id*] cost *Port-cost*	
Arguments	**Signification**
[vlan *vlan-id*]	Si le Vlan est spécifié, l'affectation ne concerne que ce Vlan. Sinon, la priorité est modifiée pour tous les Vlans de cette interface.
Port-cost	Valeur du coût : 9 par défaut en 100BaseTX.
(interface) spanning-tree cost *2*	

V.W.3 Exemple

- Sur C2621+ESW :

```
CK160#show spanning-tree active brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     000e.d710.4f00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     000e.d710.4f00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 0

Interface                                  Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/8      128.49   128    19 FWD     0 32768 000e.d710.4f00 128.49

CK160#
```

- Sur Catalyst 2900 :

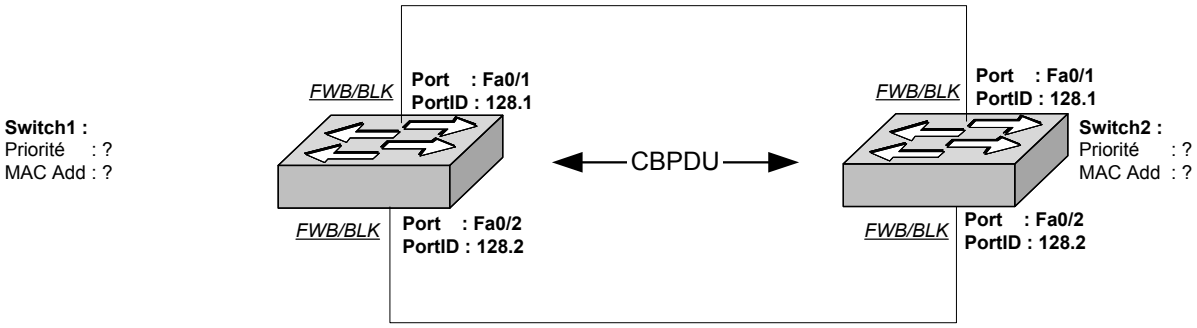
```
Sw4#show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.856e.cc80
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.856e.cc80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Port ID                    Designated               Port ID
Name             Prio.Nbr      Cost Sts     Cost Bridge ID           Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/1            128.1           19 FWD         0 32769 000c.856e.cc80 128.1
Fa0/2            128.2           19 FWD         0 32769 000c.856e.cc80 128.2
Fa0/4            128.4           19 FWD         0 32769 000c.856e.cc80 128.4
```

Spanning-tree Port Cost (configurable on a per-interface basis)	1000 Mbps 4 100 Mbps 19 10 Mbps 100

V.X Application du STP

V.X.1 Application 1

- Réalisez le montage suivant, puis
- Renseignez le schéma



- Après avoir déterminez et vérifiez le 'Root Bridge' par défaut, rendez l'autre switch 'Root Bridge'.

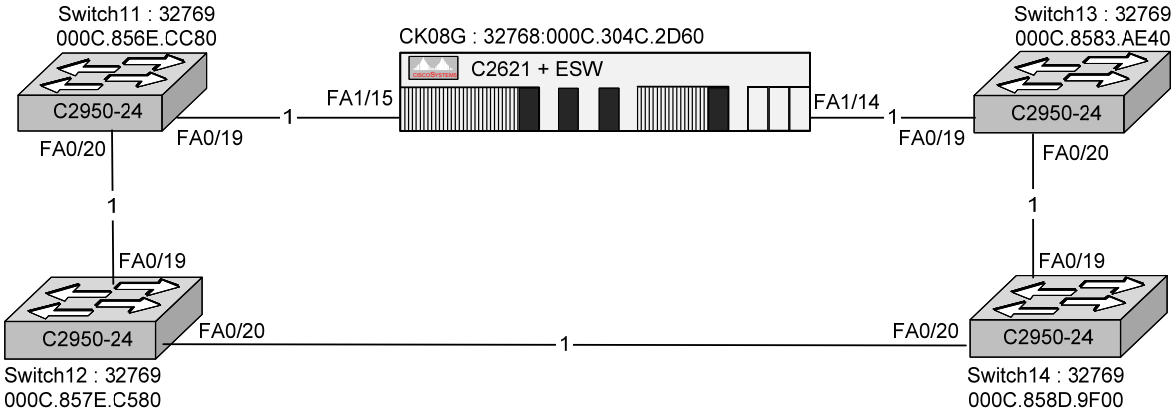
- Modifier le 'Port Priority' de chacune des interfaces des switchs, en observant les modifications apportées.

V.X.2 Application 2

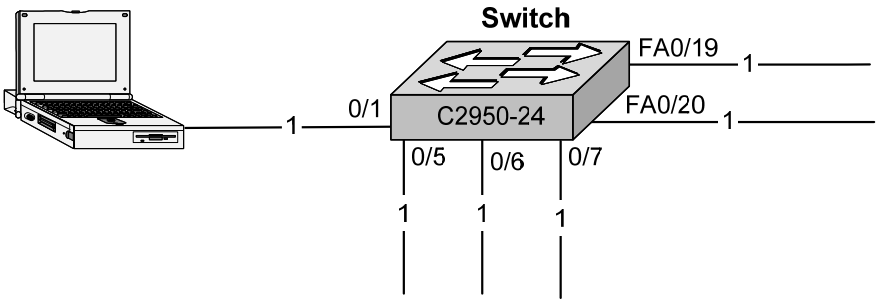
V.X.2.a Block Switch 1

- Pour éviter la configuration des ports en TRUNK, configurez ceux-ci en :
  - ‘#switchport mode access’
  - ‘#switchport nonegotiate’

- Installation et configuration des commutateurs



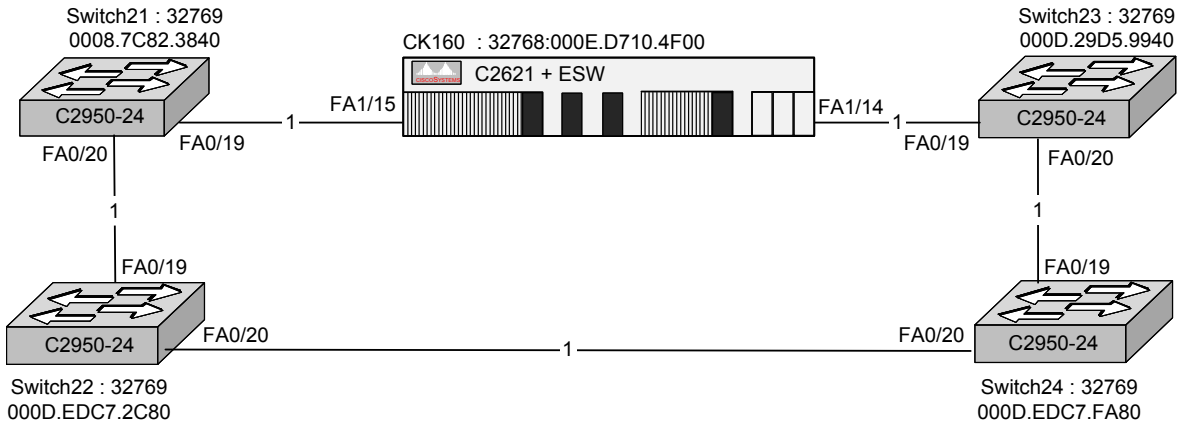
- Installation et configuration des ordinateurs



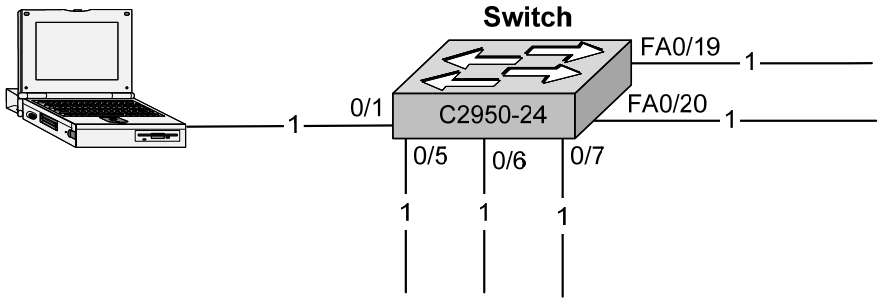
V.X.2.b Block Switch 2

- Pour éviter la configuration des ports en TRUNK, configurez ceux-ci en :
  - ‘#switchport mode access’
  - ‘#switchport nonegotiate’

- Installation et configuration des commutateurs



- Installation et configuration des ordinateurs



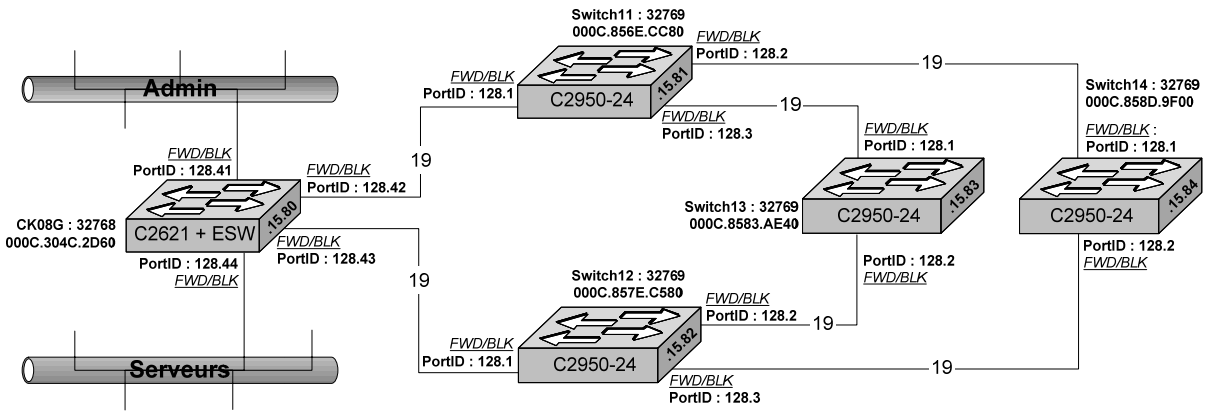
V.X.3 Application 3

V.X.3.a Block Switch 1

- Pour éviter la configuration des ports en TRUNK, configurez ceux-ci en :
  - '#switchport mode access'
  - '#switchport nonegotiate'

- Exercice :
  1. Renseignez le schéma suivant :

     - Le RB (Root Switch)
     - Le RPC (Root Path Cost) de chaque switch
     - L'état des ports



  2. Rendez le Switch1 '*Primary Root Bridge*' ; vérifiez.

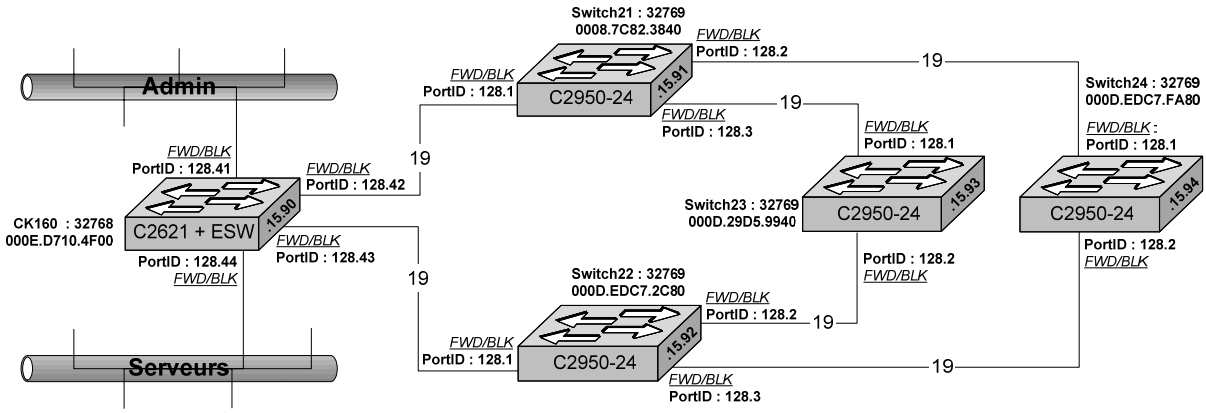
  3. Rendez le Switch2 '*Secondary Root Bridge*' ; vérifiez.

V.X.3.b Block Switch 2

- Pour éviter la configuration des ports en TRUNK, configurez ceux-ci en :
  - '#switchport mode access'
  - '#switchport nonegotiate'

- Exercice :
  1. Renseignez le schéma suivant :

     - Le RB (Root Switch)
     - Le RPC (Root Path Cost) de chaque switch
     - L'état des ports



  2. Rendez le Switch21 '*Primary Root Bridge*' ; vérifiez.

  3. Rendez le Switch22 '*Secondary Root Bridge*' ; vérifiez.

VI. Les VLANs

VLAN: Virtual LAN

VI.A Présentation

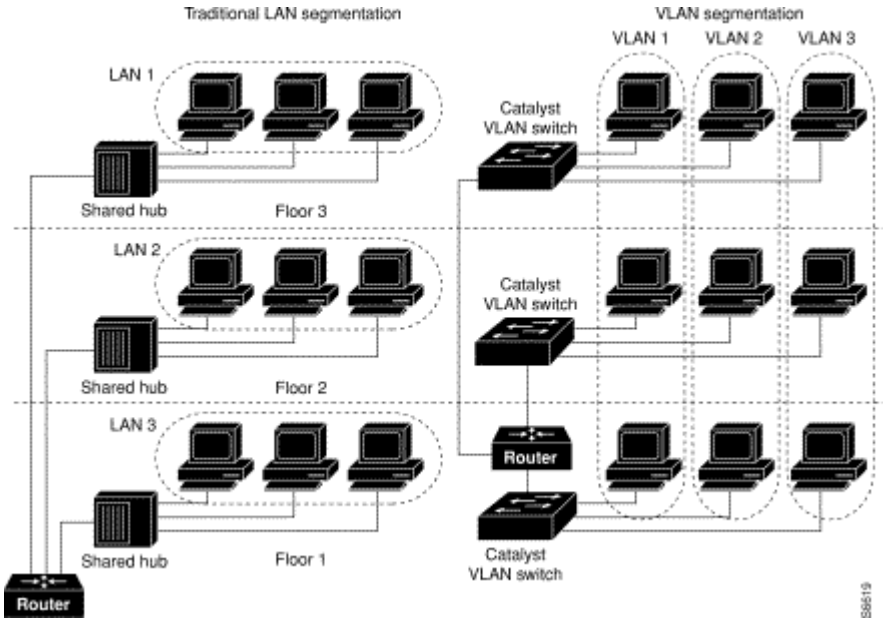
- L'objectif initial des VLAN est une segmentation fonctionnelle du réseau destinée
  - A limiter les domaines de *broadcast*,
  - Faciliter le raccordement des utilisateurs lors d'un déménagement de bureau, et à
  - Sécuriser les utilisateurs.

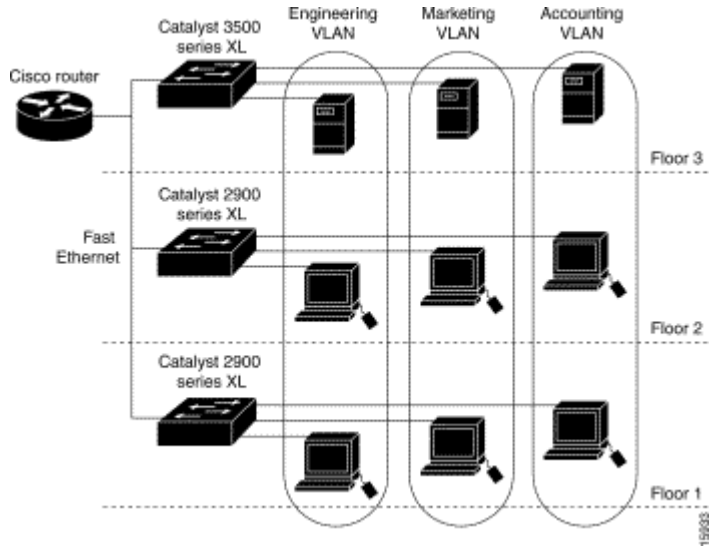
- Un VLAN est un réseau, c'est-à-dire un **domaine de Broadcast**.

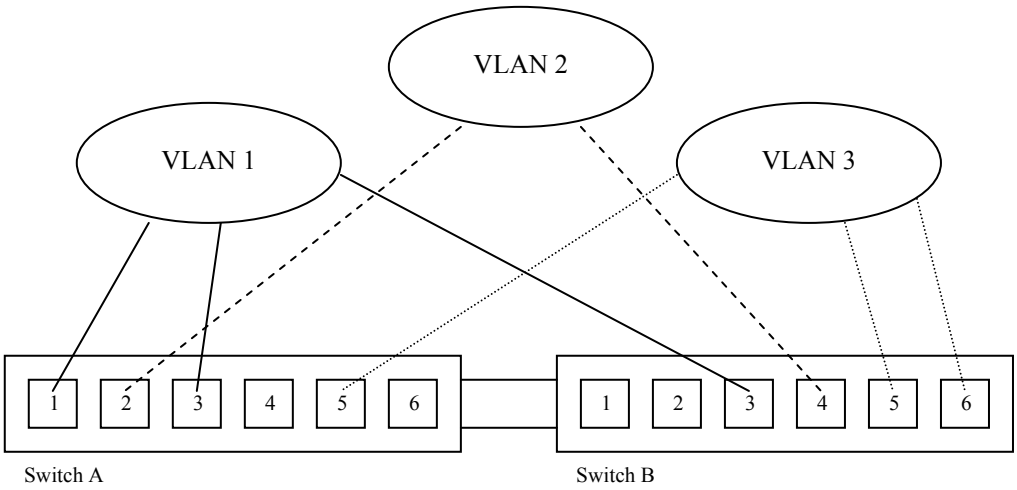
- Il existe plusieurs approches pour constituer les VLAN

  - *Static VLAN* : par l'assignation d'un port (*port-based membership*) à un numéro de VLAN (VLAN ID) ou par un serveur Radius après authentification de l'utilisateur par 802.1x.

  - *Dynamic VLAN* : par assignation d'une adresse MAC (*membership based on MAC address*) à un numéro de VLAN (VLAN ID). Dans cette méthode, il faut disposer d'une base de données qui donnera l'identification du VLAN en fonction de l'adresse MAC : VMPS sur Catalyst 5000 & 6000 ou CiscoWorks 2000 ou CiscoWorks for Switched Internetworks (CWSI).







- Cette architecture fournit trois VLAN totalement indépendants les uns des autres donc trois domaines de broadcast en Ethernet.
- L'interconnexion des VLAN sera réalisé par un routeur avec des ACL, pour sécuriser les communications.

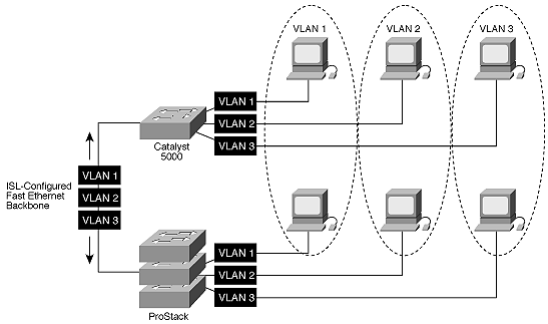
VI.B Transport des VLANs ou Trunk

VI.B.1 Présentation

- Un trunk est une liaison point à point qui transmet et reçoit le trafic entre deux switchs (cas général) ou entre un switch et un routeur ou entre switch et un ordinateur (serveur).
- Ce lien transporte le trafic de plusieurs VLANs et peut les étendre à travers tout le réseau via d'autres switchs. Attention la gestion des VLANs est réalisée au niveau 2, donc ils ne passent les routeurs (plus exactement la couche 3).

- Il existe deux protocoles d'encapsulation des VLANs : ISL et dot1q (IEEE 802.1q). Le protocole propriétaire Cisco, ISL, est maintenant abandonné sur les IOS modernes.
- Le transport des VLANs s'effectue via des ports **FastEthernet** ou **Gigabit Ethernet**.

- Le TRUNKING permet aussi l'agrégation de plusieurs liens 100BaseTX entre commutateur ou switch, moyen économique pour augmenter le débit entre switchs et éviter les points de congestion.
  - Le MLT, MultiLink Trunking, chez BAY
  - Le Prot Trunking chez 3COM
  - L'EtherChannel chez CISCO



➢ **Note** : Le mode par défaut des interfaces de niveau 2 est '***switchport mode dynamic desirable***'. Si l'interface la plus proche supporte le trunking et configurée pour, la connexion entre les deux switchs sera un lien Trunk.

➢ **Note** : Le DTP (Dynamic Trunking Protocol), protocole point à point, gère la négociation des liens Trunk entre switchs. Durant cette négociation le port ne participe pas au STP. Ce protocole est un **trou de sécurité**, car on pourra récupérer tous les VLANs en connectant un switch à un port non protégé

```
(interface) switchport nonegotiate
```

VI.B.2 ISL

ISL : Inter-Switch Link

- Protocole propriétaire CISCO. Sur les IOS récents, ce protocole est abandonné au profit de 802.1Q.

- Une instance STP par VLAN

ISL Header	Encapsulation Frame	**FCS**

# of bits	40	4	4	48	16	24	24	15	1	16	16	8 to 196600	32
Frame field	**DA**	**Type**	**User**	**SA**	**LEN**	**AAAA03**	**HAS**	**VLAN**	**BPDU**	**Index**	**RES**	Encap. Frame	**FCS**

- DA - Destination Address, cette adresse est de type Multicast (0x01-00-0C-00-00 ou 0x03-00-0C-00-00), elle signale au récepteur que le paquet est une trame ISL.
- Type - pour Ethernet 0000, pour ATM 0011
- User - Type Extension
- SA - Source Address, adresse MAC de l'émetteur
- LEN - Length, indique la longueur du paquet ISL de DA à FCS.
- AAAA03 - Subnetwork Access Protocol (SNAP) et Logical Link Control (LLC)
- HSA – High Bits of Source Address, adresse OUI.
- VLAN – Destination Virtual LAN ID, identification du VLAN.
- BPDU – Bridge Protocol Data Unit et Cisco Discovery Protocol (CDP) Indicator, ce bit indique l'encapsulation d'une trame BPDU ou CDP.
- Index, utilisé pour les diagnostique et ignoré par le récepteur.
- RES – Reserved for Token Ring and FDDI.
- Encap. Frame – Trame Ethernet encapsulée en transit dans un lien Trunk.
- FCS – champ CRC de la trame ISL.

VI.B.3 IEEE 802.1Q ou Dot1q

- The EtherType and VLAN ID are inserted after the MAC source address, but before the original Ethertype/Length or Logical Link Control (LLC). The 1-bit CFI included a T-R Encapsulation bit so that Token Ring frames can be carried across Ethernet backbones without using 802.1H translation.

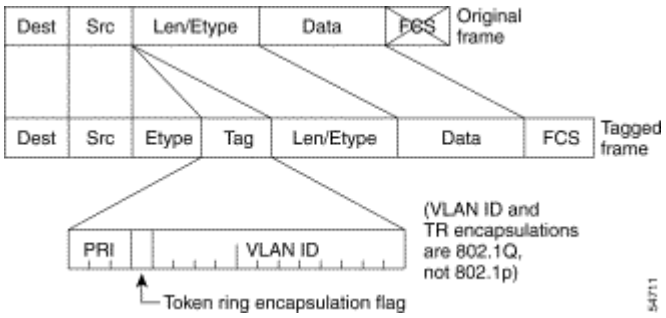
- Draft Standard P802.1Q/D11 pour *Standard for Virtual Bridged Local Area Network*.
- La norme 802.1Q consiste à ajouter un champ dans l'entête de la trame Ethernet initial à la fois pour gérer les VLAN et des classes de service (802.1P)
- Ces trames sont véhiculées entre les commutateurs et/ou routeurs.

Ethernet V2 / IEEE 802.3

8 octets	6 octets	6 octets	**2 octets**	**2 octets**	2 o	46 à 1500 octets	4 o
Préambule	@ MAC DST	@ MAC SRC	TPID 0x8100	TCI	T/Long.	Données	CRC

TPID : Tag Protocol Identifier
Le champ TPID correspond au champ Type d'une trame Ethernet V2 Si champ TPID = 0x8100 alors 802.1Q/802.1P

TCI: Tag Control Information			
COS	Class Of Service	3 bits	Utilisé par la norme 802.1p
CFI	Common Format Identifier	1 bit	0 ⇒ Format normal 1 ⇒ champ RIF présent
VID	VLAN Identifier	12 bits	4096 identificateurs de VLAN



- **Note** : Les trames Ethernet originales ne peuvent pas excéder une longueur maximale de 1518 octets (hors préambule). Si une trame de longueur maximale est marquée (tagged) par 802.1Q, il en résulte une trame de **1522 octets**. Ce type de trame est nommé '**Baby Giant Frame**'. Normalement le switch traite une trame de 1522 octets sans problème, bien qu'il puisse enregistrer une erreur.

VI.C Interconnexion

- Pour interconnecter les VLANs, il faut utiliser le routage ; deux solutions

  - Par un routeur externe via un lien Trunk. Mais attention, dans ce cas les VLAN ne se propagent pas au-delà du routeur (voir schéma de la page de garde).

  - Par une carte de routage intégrée au switch (on parle ici de commutateur niveau 3). Ici il faudra plutôt restreindre les VLAN dans les liens TRUNK (ex. C2600 plus une carte d'extension ESW).

VI.D Configuration

VI.D.1 Déclaration des VLAN

- **Important** : il faut absolument créer le VLAN dans le VLAN Database avant l'affectation d'un port dans un VLAN. En réalité, cette commande crée une SVI (*Switch Virtual Interface*), cette interface virtuelle représente le lien entre le protocole de niveau trois (ici IP) et le VLAN (c'est à dire le réseau).

- **Trois opérations sont nécessaires pour obtenir le LINK**
  - Création d'une SVI (*Switch Virtual Interface*)
  - Activation
  - Application

Commandes	Signification
C2621# **vlan database**	
C2621(vlan)# **vlan 16**	Création de l'interface SVI 16
C2621(vlan)# **no vlan 16**	Suppression d'une interface virtuelle
C2621(vlan)# **vlan 16 state active**	Activation de l'interface
C2621(vlan)# **apply**	Application et activation des modifications
C2621(vlan)# **exit**	Application et activation des modifications, puis sortie du menu VLAN DATABASE
C2621(vlan)# **abort**	Sortie du menu VLAN DATABASE sans appliquer les modifications
C2621(vlan)# **show**	Visualisation des VLAN existants.

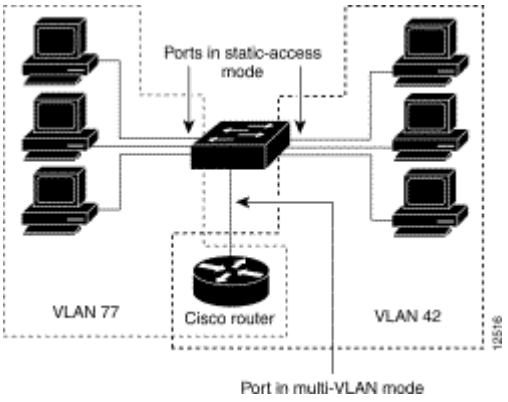
```
C2621#vlan database
C2621(vlan)#
C2621(vlan)#vlan ?
  <1-1005>  ISL VLAN index

C2621(vlan)#vlan 16 ?
  are        Maximum number of All Route Explorer hops for this VLAN
  backupcrf  Backup CRF mode of the VLAN
  bridge     Bridging characteristics of the VLAN
  media      Media type of the VLAN
  mtu        VLAN Maximum Transmission Unit
  name       Ascii name of the VLAN
  parent     ID number of the Parent VLAN of FDDI or Token Ring type VLANs
  ring       Ring number of FDDI or Token Ring type VLANs
  said       IEEE 802.10 SAID
  state      Operational state of the VLAN
  ste        Maximum number of Spanning Tree Explorer hops for this VLAN
  stp        Spanning tree characteristics of the VLAN
  <cr>

C2621(vlan)#vlan 16
VLAN 16 added:
    Name: VLAN0016
C2621(vlan)#vlan 16 state ?
  active   VLAN Active State
  suspend  VLAN Suspended State

C2621(vlan)#vlan 16 state active
VLAN 16 modified:
    State ACTIVE
C2621(vlan)#apply
APPLY completed.
C2621(vlan)#exit
APPLY completed.
Existing….
C2621#
```

VI.D.2 Le port en mode Multi-VLAN

- Par défaut tous les ports sont affectés sur le VLAN 1 (d'administration) en Static-access.

- Emploi : Deux VLANs se partageant un même routeur ou serveur tout en étant isolés.
- Un Switch **ne peut pas effectuer du Multi-Vlan et du Trunk**.
- Ne pas connecter un port configuré en Multi-VLAN à un HUB ou à un Switch. (You cannot have multi-VLAN and trunk ports configured on the same switch.)

Commandes	signification
`() configure terminal`	Entrez en mode configuration global
`(global) interface` *`fastethernet 0/4`*	Choix de l'interface à configurer
`(interface) switchport mode multi`	Mettre le port en mode Multi-VLAN
`(interface) switchport multi vlan` *`42,77`*	Affectation du port aux VLANs 1 et 2
`(interface) switchport multi vlan add` *`2`*	Rajoute le VLAN 2 dans la liste
`(interface) switchport multi vlan remove` *`2`*	Supprime le VLAN 2 de la liste
`(interface) end`	Retour en mode privileged EXEC
`() show interfaces` *`fa0/4`* `switchport`	Vérifier vos entrées



- Activation du Multi Vlan sur un port

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/2
Switch(config-if)#switchport multi vlan 1,2
Switch(config-if)#^Z
Switch#
```

- Désactivation du Multi Vlan sur un port

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/2
Switch(config-if)#no switchport multi vlan 1,2
Switch(config-if)#no  switchport mode multi
Switch(config-if)#^Z
Switch#
```

VI.D.3 Le port en mode TRUNK

- Un TRUNK n'existe qu'entre Switchs qui s'échangent des VLANs.

- You cannot have multi-VLAN and trunk ports configured on the same switch.

Activation du mode Trunk	
Commandes	**signification**
`Switch# configure terminal`	Entrez en mode global configuration
`Switch(config)# interface fastethernet 0/4`	Choix de l'interface à configurer
`Switch(config-if)# switchport mode trunk`	Configuration du port en mode trunk
`Switch(config-if)# switchport mode dynamic desirable`	Configuration par défaut des ports : attention trou de sécurité car cette configuration permet de projeter les VLANs sur un autre switch.
`Switch(config-if)# switchport trunk encapsulation {isl|dot1q}`	Configuration du trunk en ISL ou Dot1q.
`Switch(config-if)# switchport trunk allowed vlan remove vlan-list`	Définition de la liste des VLANs qui ne sont pas autorisés à être émis et reçus sur ce port
`Switch(config-if)# end`	Retour en mode privileged EXEC
`# show interfaces trunk`	Visualisation de la configuration des liens Trunk
`# show interface fa mod-id/if-id switchport`	Vérifiez vos entrées. Dans l'affichage, vérifiez les champs : Operational Mode et Operational Trunking Encapsulation
`# show interfaces status`	Visualisation complète de la configuration des interfaces
`# show interface fa mod-id/if-id switchport allowed-vlan`	Vérifiez vos entrées.
`# copy running-config startup-config`	[optionnel] sauvegardez la configuration pour le prochain redémarrage.

Désactivation du mode Trunk	
Commandes	**signification**
`() configure terminal`	Entrez en mode global configuration
`(global) interface fastethernet 0/4`	Choix de l'interface à configurer
`(interface) no switchport mode`	Retour en mode static-access (mode par défaut)
`(interface) end`	Retour en mode privileged EXEC
`() show interface fa mod-id/if-id switchport`	Vérifiez vos entrées. Dans l'affichage, vérifiez les champs : Operational Mode et Operational Trunking Encapsulation

- L'IEEE 802.1Q impose quelques limitations :
  - Le VLAN Natif (par défaut VLAN 1) doit être identique à chaque extrémité.
  - La désactivation du STP du VLAN natif sans désactivation du STP de chaque VLAN peut potentiellement provoquer des boucles de niveau 2.
  - Un port TRUNK ne peut pas servir de port monitor

VI.D.4 Creating EtherChannel Port Groups

- La norme IEEE 802.3ad définit l'agrégation de liens.

- La configuration de plusieurs liens Trunk par agrégation permet d'augmenter le débit entre équipements.

Commandes IOS Release 12.0	Signification
() configure terminal	Entrez en mode configuration global
(global) interface *fastethernet 0/23*	Entrez en mode configuration interface, et spécifier une interface physique à configurer. Jusqu'à huit interfaces de même type et de même débit peuvent être configurées pour un même groupe.
(interface) port group 1 distribution destination	Assign the port to group 1 with destination-based forwarding.
(interface) exit	Retour en mode global configuration
(global) interface *fastethernet 0/24*	Enter the second port to be added to the group
(interface) port group 1 distribution destination	Assign the port to group 1 with destination-based forwarding
(interface) end	Retour en mode privileged EXEC
() show running-config	Vérifiez votre configuration
() copy running-config startup-config	[optionnel] sauvegardez la configuration pour le prochain redémarrage.
() show etherchannel 1 summary	État de EtherChannel Groupe 1
() show interfaces status	Visualisation complète de la configuration des interfaces

Commandes IOS Release 12.2	Signification
() configure terminal	Entrez en mode configuration global
(global)interface fastethernet *0/23* (global)interface range fastethernet *0/20 - 21*	Entrez en mode configuration interface, et spécifier une interface physique à configurer. Jusqu'à huit interfaces de même type et de même débit peuvent être configurées pour un même groupe.
(interface)channel-group 1 mode on	Assign the port to group 1. Assignation du port dans le 'po1' (portchannel 1)
(interface)end	Retour en mode privileged EXEC
# show running-config	Vérifiez votre configuration
# copy running-config startup-config	[optionnel] sauvegardez la configuration pour le prochain redémarrage.
# show etherchannel 1 summary	État de EtherChannel Groupe 1
# show interface portchannel *1* status	
# show interface portchannel *1* summary	
# show interface portchannel *1* etherchannel	
# show interfaces status	Visualisation complète de la configuration des interfaces

VI.D.5 Application

□ Configuration

```
Ck160(config-if)#switchport trunk allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  remove  remove VLANs from the current list

Ck160(config-if)#
```

□ Configuration des ports en mode Trunk

```
conf t
int range fa 1/8 - 15
 switchport mode trunk
 no shut
 exit
```

□ Agrégation de liens : Etherchannel

```
int range fa 1/12 - 13
 shut
 channel-group 1 mode on
 no shut
 exit
```

□ Suppression de VLAN dans un Trunk

```
int range fa1/8 - 9
switchport trunk allowed vlan remove 3
switchport trunk allowed vlan remove 4
switchport trunk allowed vlan remove 5
```

```
int port-channel 1
 switchport trunk allowed vlan remove 10
 switchport trunk allowed vlan remove 11
 exit
```

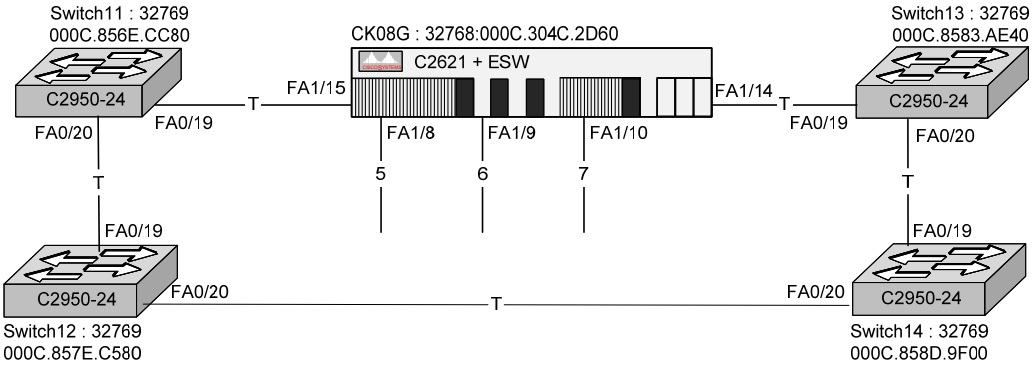
□ Contrôle

```
Ck160#sh etherchannel 1 summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        R - Layer3      S - Layer2
        U - in use
Group Port-channel  Ports
------+------------+-----------------------------------------------------------
1     Po1(SU)     Fa1/8(P)   Fa1/9(P)

Ck160#sh int po1 status

Port    Name               Status       Vlan       Duplex Speed Type
Po1                        connected    trunk      a-full   a-100 unknown

Ck160#sh int po1 summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface          IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS  TRTL
------------------------------------------------------------------------------
* Port-channel1         0     0    0     0  2000    5  6000   10   0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown

Ck160#sh int po1 etherchannel
Age of the Port-channel   = 00d:00h:29m:51s
Logical slot/port   = 3/0           Number of ports = 2
GC                  = 0x00010001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse

Ports in the Port-channel:

Index   Port   EC state
------+------+------------
  0     Fa1/8    on
  1     Fa1/9    on

Time since last port bundled:    00d:00h:29m:46s    Fa1/9

Ck160#
```

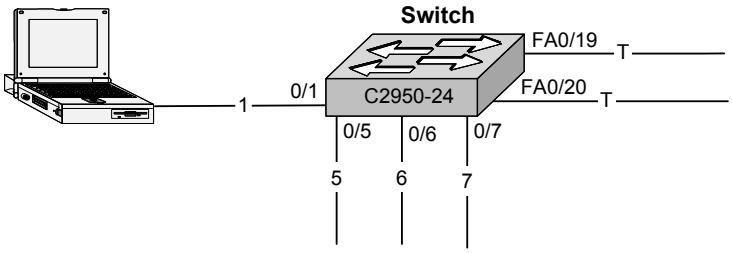
VI.E Application

VI.E.1 Block Switch 1

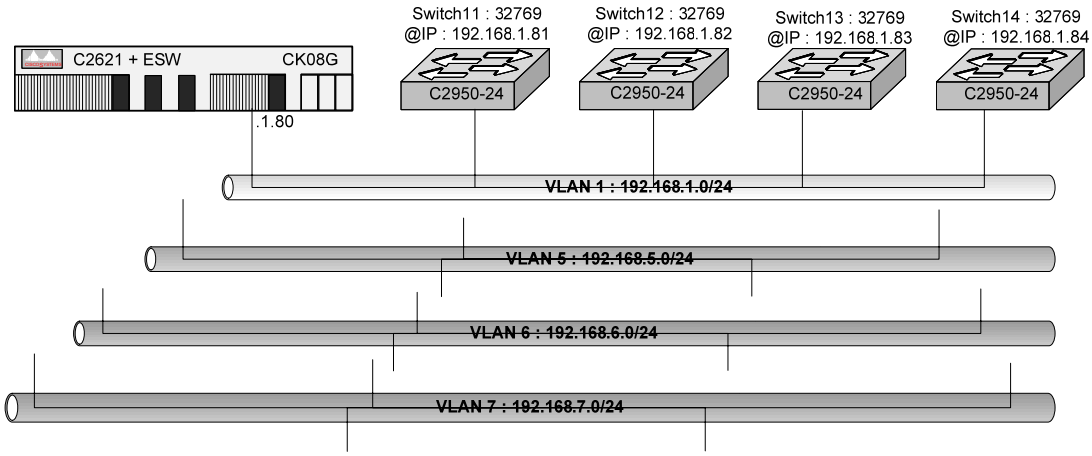
- Installation et configuration des commutateurs



- Installation et configuration des ordinateurs

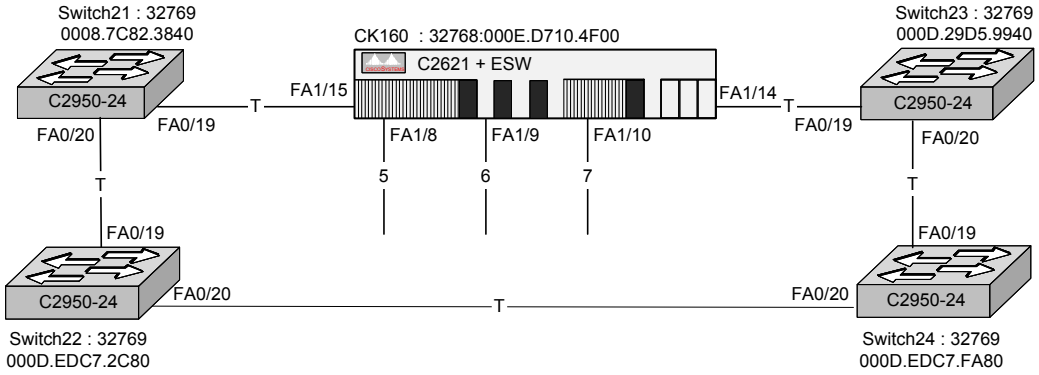


- Vue virtuelle des réseaux

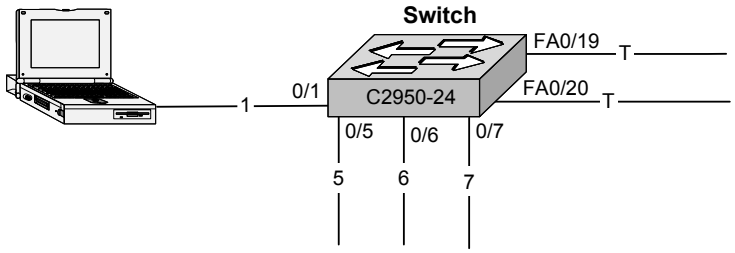


VI.E.2 Block Switch 2

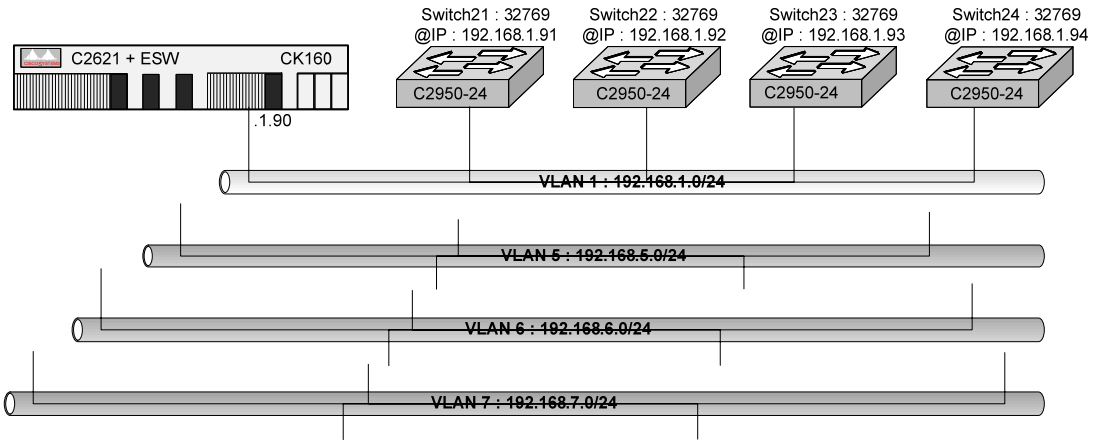
- Installation et configuration des commutateurs



- Installation et configuration des ordinateurs



- Vue virtuelle des réseaux



VI.F Observations

- Sur un lien TRUNK (par défaut 802.1Q) :

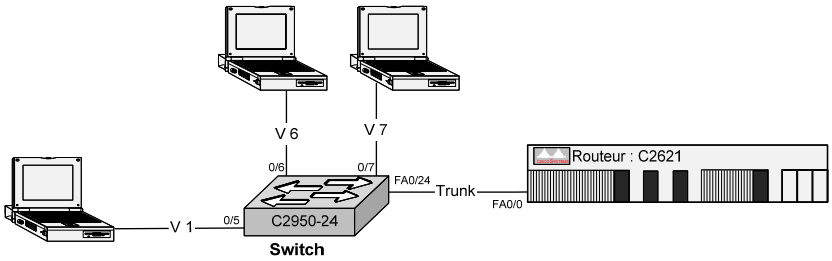
  - Les trames du VLAN natif ne sont pas taguées sur un lien trunk.
  - Par contre le trafic correspondant aux autres VLAN est tagué par le protocole IEEE 802.1Q par défaut.

  - Les BPDU STP sont encapsulées dans LLC (ou IEEE 802.2) puis directement dans IEEE 802.3.
  - Par contre les annonces PVSTP sont :
    - Non taguées sur le '`native VLAN`' (par défaut le VLAN 1),
    - Taguées par VLAN.

VII. Le routage inter VLAN

VII.A Par routeur indépendant

- Le routeur CISCO doit disposer d'un IOS IP Plus, pour gérer le protocole dot1q (802.1Q).
- Le trunking ne peut pas être réalisé sur un port '`Ethernet`', il faut obligatoirement disposer de ports '`Fastethernet`' au minimum.



- Sur le routeur,
  l'interface physique '`fastEthernet 0/0`' est utilisée pour supporter des interfaces virtuelles (également appelées sous interfaces) pour router le trafic entre ces trois machines qui sont connectées sur trois VLAN différents.
- La sous-interface '`FastEthernet 0/0.1`' est configurée par l'interface principale 'FA0/0'.

Routage via un port trunk :	
Commandes	**Signification**
(global) interface fastethernet *slot/port.subif-number*	Spécifiez la sous interface à configurer. La sous interface est représentée par '*subif-number*'.
(interface) encapsulation dot1q *vlanid*	Définition du type d'encapsulation et de l'identification du VLAN d'affectation pour cette interface physique.
(sub-interface) ip address *ip-address sub-net-mask*	Assignation de l'adresse IP à cette sous interface

```
C2621#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
C2621(config)#int fa 0/0
C2621(config-if)# ip address 192.168.1.20 255.255.255.0
C2621(config-if)#no shut
C2621(config-if)#exit
C2621(config)#int fa 0/0.2
C2621(config-subif)#encapsulation dot1Q 2
C2621(config-subif)#ip address 192.168.2.20 255.255.255.0
C2621(config-subif)#no shut
C2621(config-subif)#exit
C2621(config)#int fa 0/0.3
C2621(config-subif)#encapsulation dot1Q 3
C2621(config-subif)#ip address 192.168.3.20 255.255.255.0
C2621(config-subif)#no shut
C2621(config-subif)#exit
C2621(config)#
```

- A la place du routeur CISCO, vous pouvez câbler tout autre système gérant 802.1Q.
  - Sous Linux, vous n'avez aucun problème car le protocole 802.1Q est géré par le système Linux lui-même.
  - Tandis que sous Windows, c'est le Device Driver fournit avec l'interface qui offre la possibilité ou non de gérer le protocole 802.1Q.

VII.B Par un commutateur de niveau 3

- Les Catalyst 3500, 4000(*), 5000 (**) et 6000 disposent de carte de routage (routage en fond de panier).
- Maintenant des cartes d'extension ESW sont disponibles pour les routeurs ; C2600 et C3600. Ces cartes ESW sont des switch (attention à la connectique différentes des ports intégrés au routeurs).

(*) Avec une carte superviseur 3 ou 4
(**) Avec une carte RSM

VII.B.1 Méthodes

- La configuration s'effectue en trois étapes :

1. Création du VLAN dans la 'Data Base'
2. Affectation du port à un VLAN
3. Affectation d'une adresse IP et de son Subnet Mask à l'interface VLAN

VII.B.2 Commandes

Création d'un VLAN :	
Commandes	**Signification**
`C2621#vlan database`	
`C2621(vlan)#vlan 16 state active`	Création et Activation de l'interface SVI VLAN 16
`C2621(vlan)#exit`	Application dans la base de données et activation du VLAN physiquement

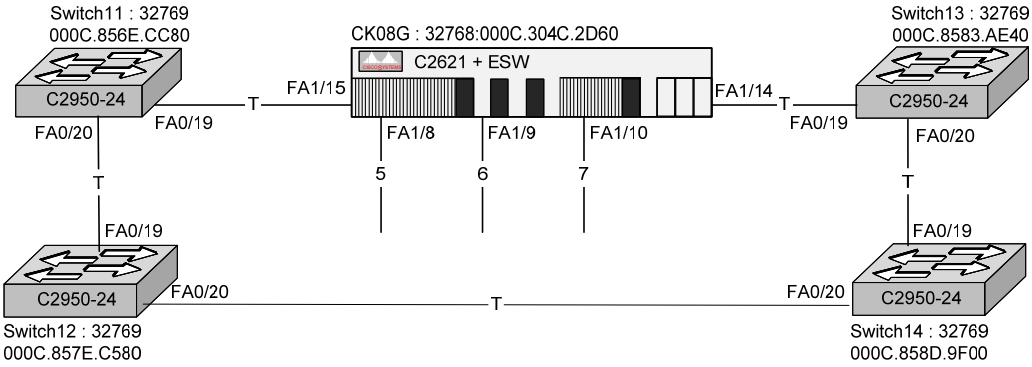
Affection d'un port à un VLAN	
Commandes	**Signification**
`() configure terminal`	Entrez en mode global configuration
`(global) interface` *`fastethernet 0/4`*	Choix du port à configurer
`(interface) shutdown`	Désactive l'interface SVI VLAN 4
`(interface) switchport access vlan` *`3`*	Affectation statique du port au VLAN 3 ici
`(interface) no shutdown`	Active l'interface SVI VLAN 3
`(interface) end`	Retour en mode privileged EXEC

Affectation d'une adresse IP	
Commandes	**Signification**
`() configure terminal`	Entrez en mode global configuration
`(global) interface vlan 1`	Choix du VLAN à configurer par défaut le VLAN1 qui est le VLAN natif.
`(interface) ip address` *`192.168.3.61 255.255.255.0`*	Affectation de l'adresse IP
`(interface) no shutdown`	Optionnel
`(interface) end`	Retour en mode privileged EXEC
`() copy running-config startup-config`	[optionnel] sauvegardez la configuration pour le prochain redémarrage.

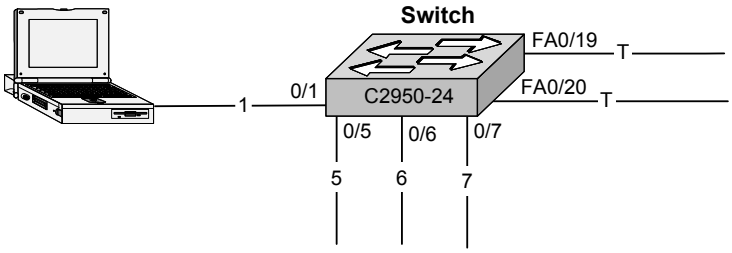
VII.C Application 1

VII.C.1 Block Switch 1

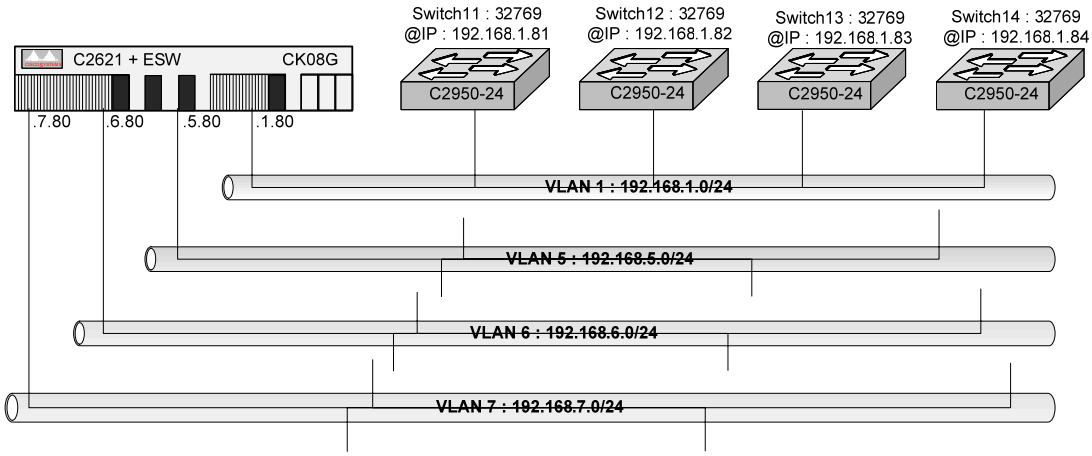
- Installation et configuration des commutateurs



- Installation et configuration des ordinateurs

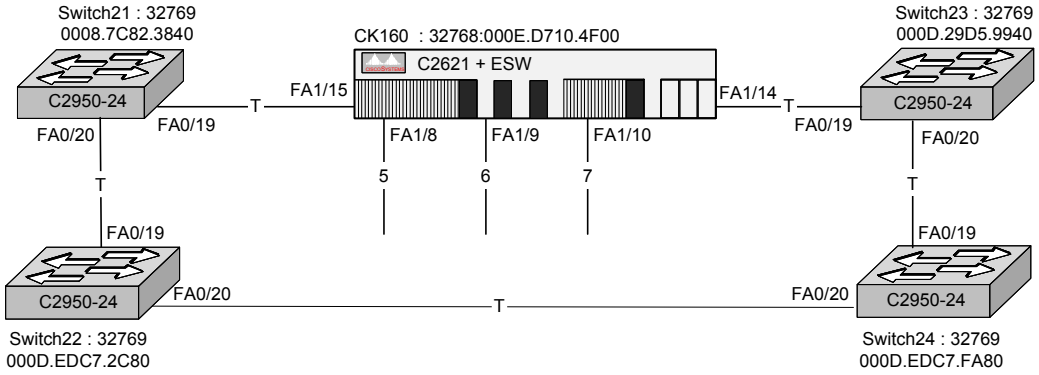


- Vue virtuelle des réseaux

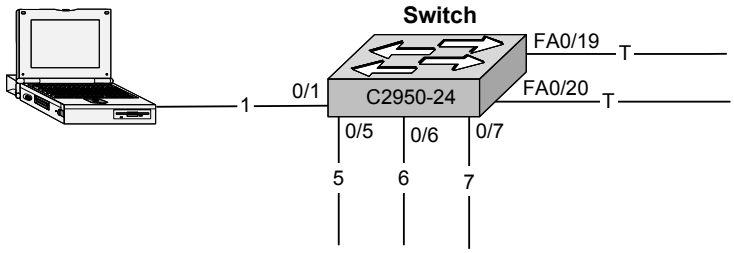


VII.C.2 Block Switch 2

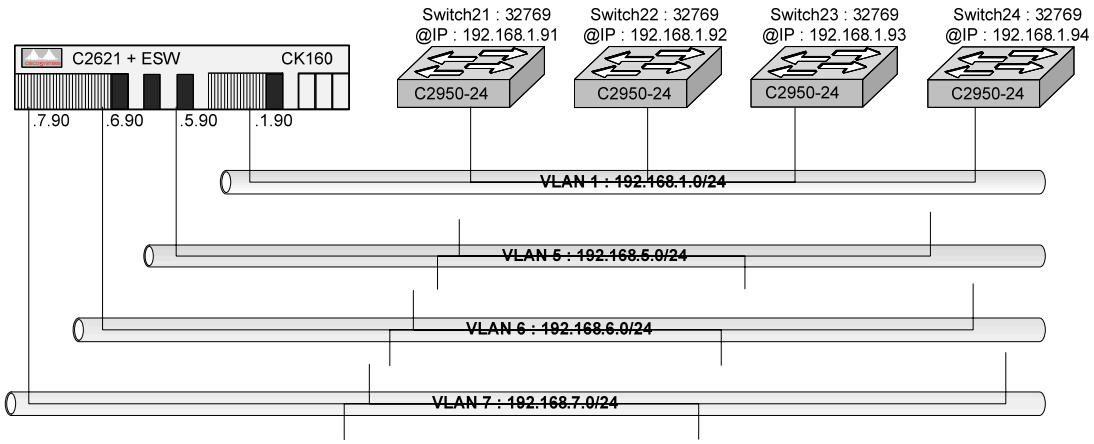
- Installation et configuration des commutateurs



- Installation et configuration des ordinateurs

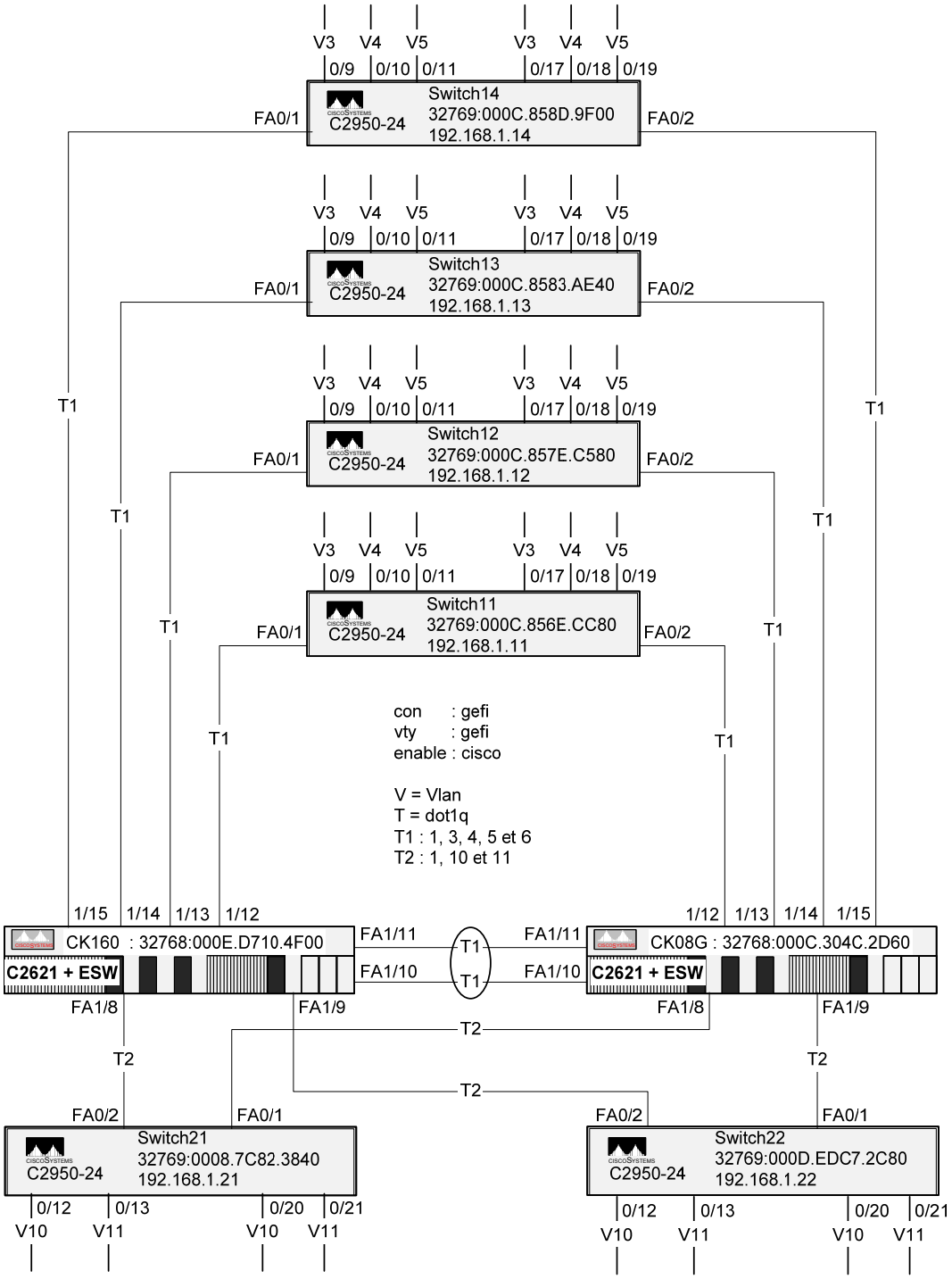


- Vue virtuelle des réseaux

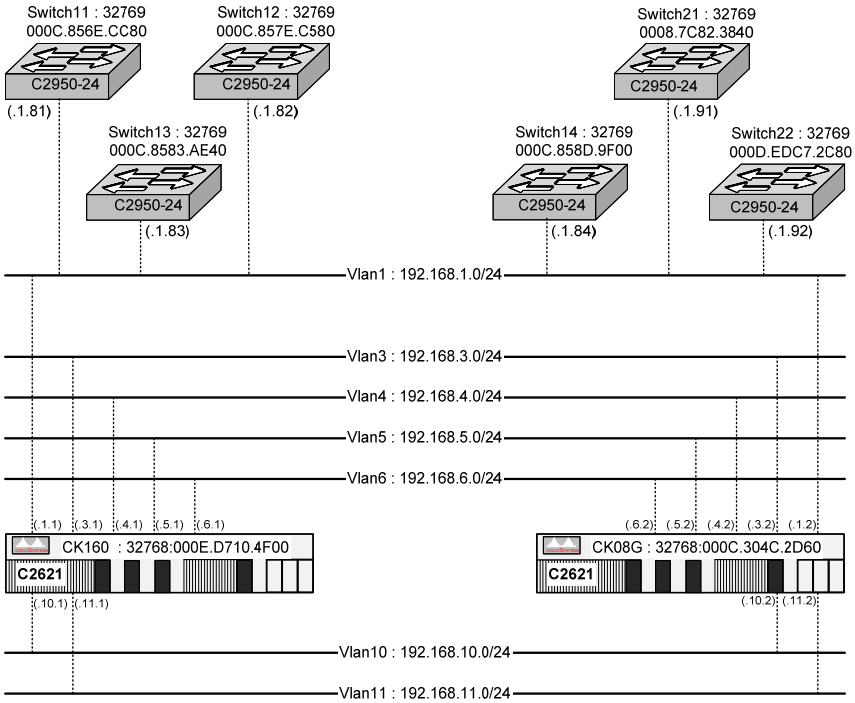


VII.D Application 2

- Réalisez le câblage de cette maquette



- Réalisez la configuration en fonction de ces deux schémas
  - Le schéma de la page précédente fournit les éléments de Niveau 1 et 2.
  - Le schéma de cette page fournit les éléments de configuration IP.



VIII. SPAN & RSPAN

SPAN : Switch Port Analyser
RSPAN: Remote SPAN

You can use Switch Port Analyzer (SPAN) to monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. A SPAN port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. You can define any number of ports as SPAN ports, and any combination of ports can be monitored.

- Vous pouvez utiliser le Switch Port Analyser pour analyser le trafic d'un autre port.
- Les deux ports doivent faire partie d'un même VLAN.
- Le port SPAN est configuré en **Static-access**

VIII.A SPAN

VIII.A.1 Catalyst 2900

Cisco IOS 12.0		
Etapes	**Commandes**	**signification**
1	`configure terminal`	Entrez en mode globale configuration
2	`interface fastethernet 0/4`	Choix de l'interface à configurer
3	`port monitor interface`	Autorise le monitoring sur le port spécifié
3'	`no port monitor interface`	Arrête le monitoring sur le port spécifié
5	`end`	Retour en mode privileged EXEC
6	`show running-config`	Vérifiez votre configuration
7	`copy running-config startup-config`	[optionnel] sauvegardez la configuration pour le prochain redémarrage.

VIII.A.2 Catalyst 2950

Cisco IOS 12.1		
	Commandes	**signification**
1	# **configure terminal**	Entrez en mode globale configuration
2	# **no monitor session** {*session-number* | **all** | **local** | **remote**}	Efface toute configuration SPAN et RSPAN o 'all' supprime toutes les sessions SPAN et RSPAN o 'local' supprime toutes les sessions locales SPAN. o 'remote' supprime toutes les sessions distantes RSPAN
3	# **monitor session** *session-number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	Spécifie une session SPAN et le port source (monitored port) o '*session-number*' crée une nouvelle session SPAN, pour lancer la première session spécifiez '*1*'. o '*interface-id*' spécifie le port source, où le trafic est capturé. o '**both** ' capture le trafic reçu (rx) et émis (tx) o '[**,** | **-**]' spécifie une liste ou un pool d'interfaces.
4	# **monitor session** *session-number* **destination interface** *interface-id* [**encapsulation** {**dot1q**}] [**ingress vlan** *vlan-id*]	Spécifie une session SPAN et le port destination où sera connecté un analyseur réseau (sniffer)
5	# **end**	Retour en mode '*privileged EXEC*'
3'	# **show monitor** [**session** *session-number*]	
6	# **show running-config**	Vérifiez votre configuration
7	# **copy running-config startup-config**	[optionnel] sauvegardez la configuration pour le prochain redémarrage.

This example shows how to set up a SPAN session, session 1, for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is cleared, and then bidirectional traffic is mirrored from source port 1 to destination port 10.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastEthernet0/1 both
Switch(config)# monitor session 1 destination interface fastEthernet0/10 encapsulation dot1q
Switch(config)# end
```

VIII.B RSPAN

- La configuration du VLAN nécessaire au RSPAN

VIII.B.1 Création de la session source

Cisco IOS 12.1	
Commandes	**signification**
`# configure terminal`	Entrez en mode globale configuration
`# no monitor session {`*`session-number`* `| all | local | remote}`	Efface toute configuration SPAN et RSPAN o '`all`' supprime toutes les sessions SPAN et RSPAN o '`local`' supprime toutes les sessions locales SPAN. o '`remote`' supprime toutes les sessions distantes RSPAN
`# monitor session` *`session-number`* `source interface` *`interface-id`* `[ , | - ] [ both | rx | tx ]`	Spécifie une session SPAN et le port source (monitored port) o '*`session-number`*' crée une nouvelle session SPAN, pour lancer la première session spécifiez '*`1`*'. o '*`interface-id`*' spécifie le port source, où le trafic est capturé. o '**`both`** ' capture le trafic reçu (rx) et émis (tx) o '`[ , | - ]`' spécifie une liste ou un pool d'interfaces.
`# monitor session` *`session-number`* `destination remote vlan` *`vlan-id`* `reflector-port` *`interface-id`*	Spécifie une session SPAN et le port destination où sera connecté un analyseur réseau (sniffer)
`# end`	Retour en mode '*privileged EXEC*'
`# show monitor [ session` *`session-number`*`]`	
`# show running-config`	Vérifiez votre configuration
`# copy running-config startup-config`	[optionnel] sauvegardez la configuration pour le prochain redémarrage.

VIII.B.2 Création de la session destination

Cisco IOS 12.1	
Commandes	**signification**
`# configure terminal`	Entrez en mode globale configuration
`# monitor session` *`session-number`* `source remote vlan` *`vlan-id`*	Spécifie une session SPAN et le VLAN o '*`session-number`*' référence à la session RSPAN. o '**`source remote vlan`**'. o '*`vlan-id`*' spécifie la source du VLAN RSPAN a monitoré.
`# monitor session` *`session-number`* `destination interface` *`interface-id`* `[ encapsulation {dot1q} ]`	Spécifie une session RSPAN et l'interface destination où sera connecté un analyseur réseau (sniffer)
`# end`	Retour en mode '*privileged EXEC*'
`# show monitor [ session` *`session-number`*`]`	
`# show running-config`	Vérifiez votre configuration
`# copy running-config startup-config`	[optionnel] sauvegardez la configuration pour le prochain redémarrage.

IX. Le VTP

VTP : Virtual Trunking Protocol

- VTP est un protocole de transmission de messages de niveau 2, qui permet de centraliser l'addition, la suppression ou la modification des VLANs. VTP permet aux solutions de réseau commuté de changer d'échelle en réduisant les besoins de configuration manuelle. VTP réduit les erreurs ou les incohérences de configuration qui peuvent causer des problèmes, comme les noms dupliqués ou les spécifications de type de VLAN incorrects.

- Le principe est de créer un serveur VTP sur un ou plusieurs commutateurs (afin d'assurer une redondance), de paramétrer les autres commutateurs en client VTP. Toute modification apportée à un serveur VTP sera propagée au niveau des clients VTP.

IX.A Fonctionnement

- VTP est un protocole qui échange des messages de niveau 2 via des trames Trunk.
  - Échange en multicast.
  - Ne passe pas les routeurs.
  - Se propage uniquement par les ports Trunk.

- Facilite l'administration

- Les versions : les deux versions ne sont pas compatibles
  - VTP Version 1 : version par défaut,
  - VTP Version 2 : surtout pour le support de Token-Ring

IX.B VTP Modes and Mode Transitions

You can configure a supported switch to be in one of the VTP modes.

VTP Modes	Description
VTP server	In this mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links. In VTP server mode, VLAN configurations are saved in non-volatile RAM. VTP server is the default mode.
VTP client	In this mode, a VTP client behaves like a VTP server, but you cannot create, change, or delete VLANs on a VTP client. In VTP client mode, VLAN configurations are saved in nonvolatile RAM.
VTP transparent	In this mode, VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, transparent switches do forward VTP advertisements that they receive from other switches. You can create, modify, and delete VLANs on a switch in VTP transparent mode. In VTP transparent mode, VLAN configurations are saved in non-volatile RAM, but they are not advertised to other switches.

Two configurations can cause a switch to automatically change its VTP mode:

- When the network is configured with more than the maximum 250 VLANs (some models support a maximum of 64 VLANs), the switch automatically changes from VTP server or client mode to VTP transparent mode. The switch then operates with the VLAN configuration that preceded the one that sent it into transparent mode.
- When a multi-VLAN port is configured on a supported switch in VTP server mode or client mode, the switch automatically changes to transparent mode.

IX.C Configuration sur C2900 & C3500 series

IX.C.1 Les commandes

VTP Server mode :		
Etape	**Commandes**	**Signification**
1	`C2621 # vlan database`	Entrez en mode VLAN Database
2	`C2621(vlan) # vtp domain domain-name`	Définir un nom de domaine VTP (de 1 à 32 caractères)
3	`C2621(vlan) # vtp password password-name`	(Optionnel) définir un mot de passe au domaine VTP (de 8 à 64 caractères)
4	`C2621(vlan) # vtp server`	Configuration du switch en mode VTP Server (mode par défaut)
5	`C2621(vlan) # exit`	Retour en mode EXEC privilégié
6	`C2621 # show vtp status`	Vérifiez la configuration VTP

VTP Client mode :		
Etape	**Commandes**	**Signification**
1	`C2900 # vlan database`	Entrez en mode VLAN Database
2	`C2900(vlan) # vtp client`	Configuration du switch en mode VTP Client
3	`C2900(vlan) # vtp domain domain-name`	Définir un nom de domaine VTP (de 1 à 32 caractères)
4	`C2900(vlan) # vtp password password-name`	(Optionnel) définir un mot de passe au domaine VTP (de 8 à 64 caractères)
5	`C2900(vlan) # exit`	Retour en mode EXEC privilégié
6	`C2900 # show vtp status`	Vérifiez la configuration VTP

Désactivation du VTP (VTP Transparent mode) :		
Etape	**Commandes**	**Signification**
1	`C2900 # vlan database`	Entrez en mode VLAN Database
2	`C2900(vlan) # vtp transparent`	Désactivation du VTP sur le Switch
3	`C2900(vlan) # exit`	Retour en mode EXEC privilégié
4	`C2900 # show vtp status`	Vérifiez la configuration VTP

Commandes complémentaires :	
Commandes	**Signification**
`C2900 # vlan database`	Entrez en mode VLAN Database
`C2900(vlan) # vlan v2-mode`	Activation de VTP Version 2
`C2900(vlan) # no vlan v2-mode`	Désactivation de VTP Version 2
`C2900(vlan)#exit`	Application dans la base de données et activation du VLAN physiquement
`C2900(vlan) # show vtp status`	Visualisation des informations VTP
`C2900(vlan) # show vtp counters`	Affichage des compteurs VTP, nombre de messages reçus et émis.

IX.C.2 Configuration VTP serveur

```
Switch# vlan database
Switch(vlan)# vtp domain Building_A
Setting VTP domain name to Building_A
Switch(vlan)# vtp domain Building_A password LAVA
Domain name already set to Building_A .
Setting device VLAN database password to LAVA.
Switch(vlan)# vtp server
Setting device to VTP SERVER mode.
Switch(vlan)# exit
APPLY completed.
Exiting....

Switch# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 68
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : Building_A
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x09 0xF6 0x57 0x1C 0xC9 0x6F 0x75 0x16
```

IX.C.3 Ajout d'un VLAN

```
Switch# vlan database
Switch(vlan)# vlan 0003 name marketing
VLAN 3 added:
    Name: marketing
Switch(vlan)# exit
APPLY completed.
Exiting....
Switch#
```

IX.C.4 Visualisation d'un Vlan

```
Switch# show vlan name marketing
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------

3    marketing                        active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- ------ ------
3    enet  100003     1500  -      -      -        -    0      0
```

IX.C.5 Configuration VTP Client

```
Switch# vlan database
Switch(vlan)# vtp client
Setting device to VTP CLIENT mode.

Switch(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....

Switch# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 68
Number of existing VLANs        : 6
VTP Operating Mode              : Client
VTP Domain Name                 : Building_A
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x09 0xF6 0x57 0x1C 0xC9 0x6F 0x75 0x16
Configuration last modified by 172.20.130.40 at 3-5-93 22:15:25
```

IX.D Configuration Catalyst 5000 series

IX.D.1 Configuration VTP serveur

```
Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable) set vtp mode server
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
Lab_Network                    1            2           server      -
Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
10         1023             40              enabled
Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
172.20.52.70    disabled disabled 2-1000
Console> (enable)
```

IX.D.2 Configuration VTP client

```
Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable) set vtp mode client
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
Lab_Network                    1            2           client      -
Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
10         1023             40              enabled
Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
172.20.52.70    disabled disabled 2-1000
Console> (enable)
```

X. CDP

CDP : Cisco Discovery Protocol

X.A Présentation

- Protocole de niveau 2 propriété CISCO
- Auto découverte des équipements réseau (Switch & routeurs) CISCO
- CDP permet identifier :
  - Les devices
  - Les adresses IP
  - Les ports
  - Type d'équipements : pont, switch ou routeur
  - Version
  - Le type de plateforme
- Note : Certains constructeurs ont implémenté CDP (exemple : HP sur ses Switchs)

X.B Les commandes

- CDP est par défaut actif (*enable*).

Commandes complémentaires	Commentaires
`Router(config)# no cdp run`	Désactive CDP pour toutes les interfaces du routeur
`Router(config-if)# no cdp enable`	Désactive CDP pour l'interface spécifiée

```
User Access Verification

Password:
C2621>en
Password:
C2621#show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled
C2621#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Back1            Fas 0/0            138         T S       WS-C2950-2Fas 0/17
C2621#
```

```
Back1#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Albi1            Fas 0/9            139          R        2500      Eth 0
Back2            Fas 0/24           156         T S       WS-C2950-2Fas 0/24
Back2            Fas 0/23           156         T S       WS-C2950-2Fas 0/23
C2621            Fas 0/17           169          R        2621      Fas 0/0.1
C2503            Fas 0/9            147          R        2500      Eth 0
Block11          Fas 0/22           130         T S       WS-C2924-XFas 0/24
Block12          Fas 0/21           165         T S       WS-C2924-XFas 0/24
Brive1           Fas 0/9            122          R        2505      Eth 0
Back1#
```

```
Albi1#show cdp entry *
-------------------------
Device ID: Albi2
Entry address(es):
  IP address: 192.168.16.2
Platform: cisco 2500,  Capabilities: Router
Interface: Serial0,  Port ID (outgoing port): Serial1
Holdtime : 151 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

-------------------------
Device ID: Back
Entry address(es):
  IP address: 192.168.3.60
Platform: cisco WS-C2924-XL,  Capabilities: Trans-Bridge Switch
Interface: Ethernet0,  Port ID (outgoing port): FastEthernet0/1
Holdtime : 132 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5.2)XU, MAINTENANCE IN
TERIM SOFTWARE
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 17-Jul-00 17:35 by ayounes

-------------------------
Device ID: albi3
Entry address(es):
  IP address: 192.168.18.1
Platform: cisco 2505,  Capabilities: Router
Interface: Serial1,  Port ID (outgoing port): Serial0
Holdtime : 117 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Albi1#
```

XI. CVMS

CVMS : Cisco Visual Manager Software

- La configuration du switch est effectuée par un navigateur,
- Le Switch dispose d'un serveur Web embarqué (Embbebed)
- il faut que le vty 15 (privilege-level 15) est un mot de passe affecté.
  - Le 'Privilege level 15' vous fournit un accès en lecture / écriture à CVMS
  - Le 'Privilege level 1 à 14' vous fournit un accès en lecture seule à CVMS
  - Le 'Privilege level 0' vous interdit tout accès à CMS
- Installez le plug-in java xxxxxxxxxx dans votre navigateur (version : j2re.1.3.1 ou supérieure)

Modes VTP	Description
VTP Serveur	Dans ce mode, vous pouvez créer, modifier et supprimer des VLANs et spécifier d'autres paramètres de configuration (tel que la version du VTP)pour le domaine VTP.
VTP Client	
VTP Transparent	

XII. Le Cluster

- quand des switchs sont regroupés en cluster (grappe), un switch est désigné '*command switch'* et les autres sont '*member switches'*.
- L'adresse IP pour le cluster entier est assignée au '*command switch'* puis il distribue les informations de configuration et management aux autres switchs.

- Tous switchs Catalyst 2950 peut-être '*command switch'* ou '*member switches'* dans un cluster.
- Les switchs 2900 XL doivent disposés de 8 Mo de DRAM pour être '*command switch'*.
- Les switchs 2820 et 1900 ne peuvent pas être '*command switch'*.

- Un cluster est composé d'un '*command switch'* et jusqu'à 15 '*member switches'* .
- Le '*command switch'* est le seul point d'entrée du cluster.

XII.A Création

Commandes	**signification**
`# configure terminal`	
`# cluster enable cluster_name`	Active le '*command switch'* et nomme le cluster
`# end`	Retourne en mode 'Privileged Exec'
`# show cluster candidates`	Visualise la liste des candidats
`# show cluster members`	Visualise la liste courante des '*member switches*'
`# configure terminal`	
`# cluster member n mac-address hw-addr password password`	Rajoute un candidat dans le cluster ➢ '*n*' ID de 1 à 15 ➢ '*hw-addr*' son adresse MAC ➢ '*password*'
`# end`	Retourne en mode 'Privileged Exec'
`# show cluster members`	Visualise l'état du cluster
`# no cluster member n`	Supprime le switch d'ID 'n'

XIII. IEEE 802.1X

XIII.A Présentation de l'authentification 802.1x

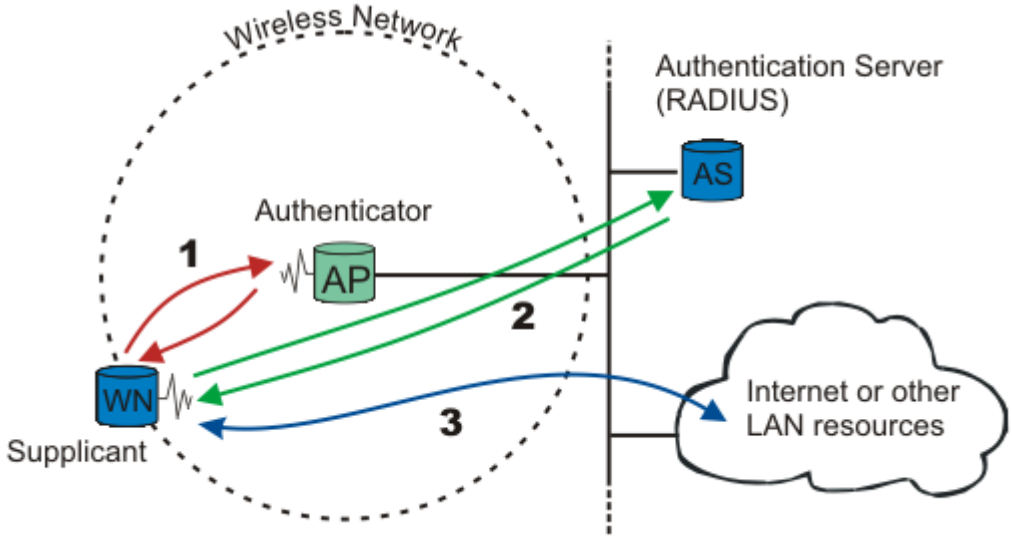
La norme IEEE 802.1x permet l'authentification sur les réseaux sans fil 802.11 et Ethernet câblés, ainsi que l'accès à ces réseaux.

Lorsqu'un utilisateur souhaite accéder à des services via un port de réseau local (LAN, *Local Area Network*) spécifique, ce port adopte l'un des deux rôles suivants : *authentificateur* ou *demandeur*. En tant qu'authentificateur, le port LAN applique l'authentification avant d'autoriser l'accès de l'utilisateur. En tant que demandeur, le port LAN demande l'accès aux services auxquels l'utilisateur souhaite accéder. Un *serveur d'authentification* vérifie les informations d'identification du demandeur, puis indique à l'authentificateur si le demandeur est autorisé à accéder aux services de l'authentificateur.

IEEE 802.1x utilise des protocoles de sécurité standard pour accorder aux utilisateurs l'accès aux ressources réseau. L'authentification, l'autorisation et la gestion des comptes des utilisateurs sont assurées par un serveur RADIUS (Remote Authentication Dial-In User Service). RADIUS est un protocole qui permet l'authentification, l'autorisation et la gestion des comptes centralisées pour l'accès réseau. Un serveur RADIUS reçoit et traite les demandes de connexion envoyées par les clients RADIUS.

En outre, IEEE 802.1x résout bon nombre des problèmes liés au cryptage WEP (Wired Equivalent Privacy) en générant, en distribuant et en gérant automatiquement les clés de cryptage.

Supplicant <=> Authenticator <=> Authenticator Server



XIII.B Radius

XIII.B.1 Présentation

- Créé par Livingston Entreprises, Radius est normalisée par les RFC 2138 et 2139 de l'IETF.
- Normalisé en janvier 1997 dans la RFC 2058 : http://www.ietf.org/rfc/rfc2058.txt , Radius avait essentiellement pour objectif de fournir aux FAI un moyen pour gérer qu'une seule base d'utilisateurs quel que soit le POP auquel ces derniers se connectaient. La principale fonction était par conséquent de transférer les informations d'authentification depuis les RAS (*Remote Access Servers*) à un mécanisme central, lui-même capable de s'interfacer avec un système d'authentification.

- Il s'est enrichi de fonctions
  - d'accounting : dans la RFC 2866 de juin 2000 : http://www.ietf.org/rfc/rfc2866.txt
  - support d'IPv6 : dans la RFC 3162 d'août 2001 : http://www.ietf.org/rfc/rfc3162.txt
  - support EAP : dans la RFC 3579 de septembre 2003 : http://www.ietf.org/rfc/rfc3579.txt

- Radius utilise le port UDP/1812

- Les attributs :
  - Un des principaux aspects de Radius est la richesse des informations transmises entre le client et le serveur, voire jusqu'au poste utilisateur.
  - Ces informations sont appelées attributs et sont positionnées à la fin du paquet selon le format suivant :
    - **Type** : un octet, correspondant au type de données de l'attribut. Les valeurs sont définis dans la RFC 1700 : http://www.ietf.org/rfc/rfc2865.txt
    - **Longueur** : un octet, taille (en octets) de l'attribut.
    - **Attribut** : valeur de l'attribut à proprement parler.

- Il gère les fonctions AAA (*Authentication, Authorization and Accounting*), c'est-à-dire l'authentification, l'autorisation et la journalisation des événements :
  - Authentification et autorisation. Il s'agit de vérifier l'identité de l'utilisateur et de lui assigner un profil d'utilisation. Pour y parvenir, Radius hérite des méthodes d'authentification du protocole PPP, c'est-à-dire PAP, CHAP et EAP, incluant pour la dernière la possibilité d'utiliser des cartes (tokens), etc. les échanges d'authentification/autorisation sont élémentaires. Ils s'appuient sur des demandes (de la part du client) et des réponses (de la part du serveur) d'authentification/autorisation. Une base de données située sur le serveur d'accès distant sur lequel s'exécute le serveur Radius gère l'ensemble des utilisateurs Radius ainsi que leurs profils. L'étape préliminaire permet d'authentifier et d'autoriser un utilisateur. Il y a donc, par rapport à Tacacs+, gain d'échange de messages entre client et serveur.
  - Accounting. Il s'agit de connaître toutes les actions menées par un utilisateur à des fins de comptabilité pour la facturation de service réseau ou à des fins d'investigation pour la gestion du réseau. Les informations disponibles sont les demandes d'authentification afin d'ouvrir et fermer une session. Si plusieurs serveurs Radius sont déployés, une consolidation des journaux de log doit être réalisée afin de corréler les événements entre eux.

XIII.B.2 Présentation de Freeradius

- Site : http://www.freeradius.org

- RPM : `freeradius-0.9.3-103.rpm`
- Freeradius supporte une grande variété de bases de données :
  - LDAP
  - MySQL

- Man :
  - `# man radius` :
  - `# man radiusd` :
  - `# man radiusd.conf` : FreeRADIUS Configuration File

- Fichiers de configuration :
  - '`/etc/raddb/radiusd.conf`' :

  - '`/etc/raddb/users`' : This file contains authentication security and configuration information for each user. Voir '`man 5 users`'

  - '`/etc/raddb/clients.conf`' :

- Démarrage du serveur : `# /etc/init.d/radiusd start`

- Fichiers complémentaires :
  - `/var/log/radacct` : Accounting Directory
  - `/var/log/radius/radacct/` :
  - `/var/log/radius/radutmp` :

```
#
#       For a list of RADIUS attributes, and links to their definitions,
#       see:
#
#       http://www.freeradius.org/rfc/attributes.html
#
```

XIII.B.3 Configuration de Freeradius

XIII.B.3.a /etc/raddb/radiusd.conf

- FreeRADIUS server configuration file.

- *radiusd.conf* file is the central location to configure most aspects of the FreeRADIUS product. It includes configuration directives as well as pointers and two other configuration files that may be located elsewhere on the machine. There are also general configuration options for the multitude of modules available now and in the future for FreeRADIUS. The modules can request generic options, and FreeRADIUS will pass those defined options to the module through its API.

- Before we begin, some explanation is needed of the operators used in the statements and directives found in these configuration files. The = operator, as you might imagine, sets the value of an attribute. The := operator sets the value of an attribute and overwrites any previous value that was set for that attribute. The == operator compares a state with a set value. It's critical to understand how these operators work in order to obtain your desired configuration.

XIII.B.3.b /etc/raddb/clients.conf

- ‘`clients.conf`’ - client configuration directive. Ce fichier définit les AP et/ou les Switchs désirant interroger un serveur Radius, ils doivent déclarer leur adresse IP leur mot de passe secret partagé.

- This file is included by default. To disable it, you will need to modify the CLIENTS CONFIGURATION section of "`radiusd.conf`".

- Exemple 1 :

```
#client some.host.org {
#       secret          = testing123
#       shortname       = localhost
#}

#
#  You can now specify one secret for a network of clients.
#  When a client request comes in, the BEST match is chosen.
#  i.e. The entry from the smallest possible network.
#
#client 192.168.0.0/24 {
#       secret          = testing123-1
#       shortname       = private-network-1
#}
#
#client 192.168.0.0/16 {
#       secret          = testing123-2
#       shortname       = private-network-2
#}


#client 10.10.10.10 {
#       # secret and password are mapped through the "secrets" file.
#       secret      = testing123
#       shortname   = liv1
#       # the following three fields are optional, but may be used by
#       # checkrad.pl for simultaneous usage checks
#       nastype     = livingston
#       login       = !root
#       password    = someadminpas
#}
```

- Exemple 2 :
  - Pour tester en local que votre serveur Radius fonctionne, rajoutez un client autorisé pour la boucle locale uniquement.

```
client 127.0.0.1 {
       secret          = test
       shortname       = localhost
}
```

  - Vous pouvez ensuite rajouter les réseaux, ou les adresses IP des clients uniquement.

```
client 192.168.1.1/24 {
       secret          = test
       shortname       = C2621
       nastype         = cisco
}
```

XIII.B.3.c /etc/raddb/users

- This file contains authentication security and configuration **information for each user**.
- Voir ‘`man 5 users`’

- Exemple 1 :

```
#
# This is a complete entry for "steve". Note that there is no Fall-Through
# entry so that no DEFAULT entry will be used, and the user will NOT
# get any attributes in addition to the ones listed here.
#
#steve  Auth-Type := Local, User-Password == "testing"
#       Service-Type = Framed-User,
#       Framed-Protocol = PPP,
#       Framed-IP-Address = 172.16.3.33,
#       Framed-IP-Netmask = 255.255.255.0,
#       Framed-Routing = Broadcast-Listen,
#       Framed-Filter-Id = "std.ppp",
#       Framed-MTU = 1500,
#       Framed-Compression = Van-Jacobsen-TCP-IP#
# The rest of this file contains the several DEFAULT entries.
# DEFAULT entries match with all login names.
# Note that DEFAULT entries can also Fall-Through (see first entry).
# A name-value pair from a DEFAULT entry will _NEVER_ override
# an already existing name-value pair.
#

#
# First setup all accounts to be checked against the UNIX /etc/passwd.
# (Unless a password was already given earlier in this file).
#
DEFAULT Auth-Type = System
        Fall-Through = 1

# Création d'un utilisateur :
"roger"  Auth-Type := Local, User-Password == "inutile"
      Reply-Message = "Bonjour %u"
```

- Exemple 2 :

```
# Création d'un utilisateur :
"mobile"  Auth-Type := EAP, User-Password == "test"
"test"  Auth-Type := Local, User-Password == "test"
```

XIII.C CISCO

XIII.C.1 Configuration Guidelines

http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00800c6ef3.html

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/12111ea1/scg/sw8021x.pdf

These are the 802.1X authentication configuration guidelines:

- When 802.1X is enabled, ports are authenticated before any other Layer 2 features are enabled.
- The 802.1X protocol is supported on Layer 2 static-access ports, but it is not supported on these port types:
    - Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
    - Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed.
    - Dynamic-access ports—If you try to enable 802.1X on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
    - EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error message appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
    - Secure port—You cannot configure a secure port as an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.
    - Switched Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

XIII.C.2 Enabling 802.1X Authentication

To enable 802.1X port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure 802.1X port-based authentication. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**aaa authentication dot1x** {**default**} *method1* [*method2...*]	Create an 802.1X authentication method list. To create a default list that is used when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. Enter at least one of these keywords: • **group radius**—Use the list of all RADIUS servers for authentication. • **none**—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.
Step 4	**interface** *interface-id*	Enter interface configuration mode, and specify the interface connected to the client that is to be enabled for 802.1X authentication.
Step 5	**dot1x port-control auto**	Enable 802.1X authentication on the interface. For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports, see the "802.1X Configuration Guidelines" section.

Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show dot1x**	Verify your entries. Check the Status column in the 802.1X Port Summary section of the display. An *enabled* status means the port-control value is set either to **auto** or to **force-unauthorized**.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable 802.1X AAA authentication, use the **no aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2*...] global configuration command. To disable 802.1X authentication, use the **dot1x port-control force-authorized** or the **no dot1x port-control** interface configuration command.

This example shows how to enable AAA and 802.1X on Fast Ethernet port 0/1:

```
Switch# configure terminal

Switch(config)# aaa new-model

Switch(config)# aaa authentication dot1x default group radius

Switch(config)# interface fastethernet0/1

Switch(config-if)# dot1x port-control auto

Switch(config-if)# end
```

XIII.C.3 Configuring the Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

Beginning in privileged EXEC mode, follow these steps to configure the RADIUS server parameters on the switch. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	Configure the RADIUS server parameters on the switch. For *hostname* | *ip-address,* specify the host name or IP address of the remote RADIUS server. For **auth-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1812. For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server. **Note** Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. If you want to use multiple RADIUS servers, re-enter this command.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete the specified RADIUS server, use the **no radius-server host** {*hostname* | *ip-address*} global configuration command.

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server, to use port 1612 as the authorization port, and to set the encryption key to *rad123*, matching the key on the RADIUS server:

```
Switch(config)# radius-server host 172.l20.39.46 auth-port 1612 key rad123
```

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, **radius-server retransmit**, and the **radius-server key** global configuration commands. For more information, see the "Configuring Settings for All RADIUS Servers" section.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, refer to the RADIUS server documentation.

XIII.D EAP MD5-Challenge

- Exemple de configuration permettant de sécuriser l'accès au réseau d'entreprise (ici Ethernet).
- Mise en œuvre comme :
  - '*Authentication Server*' : Freeradius (version 1.0.2-5) sur plateforme Linux Suse 9.3 ;
  - '*Authenticator*' : un switch Cisco Catalyst 2950 avec IOS : '*c2950-i6q4l2-mz.121-13.EA1.bin*' ;
  - '*Supplicant*' : Windows XP-Pro avec SP2.

- MD5 CHAP (*EAP-Message Digest 5 Challenge Handshake Authentication Protocol*) est un type EAP obligatoire qui utilise le même protocole de défi/réponse que CHAP PPP, mais les défis et les réponses sont envoyées sous forme de messages EAP.

- MD5-Challenge CHAP est généralement utilisé pour authentifier les informations d'identification des clients d'accès distant, à l'aide d'un système de sécurité basé sur le nom d'utilisateur et le mot de passe. Vous pouvez également utiliser MD5-Challenge CHAP pour tester l'interopérabilité de EAP.

XIII.D.1 Configure the Catalyst for 802.1x

- In this sample configuration, you enable 802.1x authentication on port fa0/7. You connect the RADIUS server to VLAN 1 behind interface fa0/6.

- **Note:** Make sure that the RADIUS server always connects behind an authorized port.

- Définition de l'état du port du supplicant
  - '`auto`': Authentification 802.1x activée …
  - '`force-authorized`': Authentification 802.1x désactivée. Le port émet et reçoit normalement le trafic sans authentification 802.1x. C'est l'état par défaut.
  - '`force-unauthorized`'

- Commandes :

```
--------------------------------------------------------------------------------
!
 aaa new-model
!--- Enable AAA.
aaa authentication login default none
!--- Use AAA for 802.1x only, which is optional.
aaa authentication dot1x default group radius
aaa authorization network default group radius
!--- You need authorization for dynamic VLAN assignment to work with RADIUS.
!
radius-server host 192.168.33.9
!--- Set the IP address of the RADIUS server.
radius-server key fred
!--- This is the RADIUS server key.
!
interface Vlan1
!--- This is the L3 interface to access the RADIUS server.
 ip address 192.168.33.2 255.255.255.0
!
interface fa0/6
!--- The RADIUS server is behind this L2 port.
 switchport mode access
 switchport access vlan 1
!
interface fa0/7
!--- Enable 802.1x on the interface.
 switchport mode access
 dot1x port-control auto
end
!
--------------------------------------------------------------------------------
```

- This example shows how to enable AAA and 802.1X on Fast Ethernet port 0/7 :

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authentication login default none
Switch(config)# radius-server host 192.168.33.9 key fred
Switch(config)# interface fastethernet0/7
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x multiple-hosts
Switch(config-if)# end
```

- Avec une EI, il faut activer 802.1x pour activer l'authentification sur le port

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
```

- Enabling 802.1x Port-Based Authentication

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# interface fastethernet0/7
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```

- Verifies your entries

```
Switch# show dot1x all
```

- Configuring Switch-to-Radius-Server Communication

```
Switch(config)# ip radius source-interface vlan1
Switch(config)# radius-server host 192.168.33.9
Switch(config)# radius-server key fred
Switch(config-if)# end
```

XIII.D.2 Freeradius

- '`/etc/raddb/radiusd.conf`' et '`/etc/raddb/eap.conf`'

```
modules {
        ...
        eap {
                default_eap_type = md5
                md5 {
                }
            ...
        }
        ...
}

# eap sets the authenticate type as EAP
authorize {
        ...
        eap
}

# eap authentication takes place.
authenticate {
        eap
}

# If you are proxying EAP-LEAP requests
# This is required to make LEAP work.
post-proxy {
        eap
}
```

- '`/etc/raddb/clients.conf`'
  - Ce fichier déclare les *Authenticators* auprès du serveur Radius, avec leur clé.

```
client 192.168.0.0/16 {
       secret          = fred
       shortname       = 192.168.33.2
       nastype         = cisco
}
```

- '`/etc/raddb/user`'
  - Ce fichier déclare les utilisateurs ayant droit d'accéder au réseau (au travers d'un switch ou d'un AP Wifi).
  - '`Auth-Type = Local`' désigne que le mot de passe est géré par le serveur Radius, c'est-à-dire dans le fichier même.

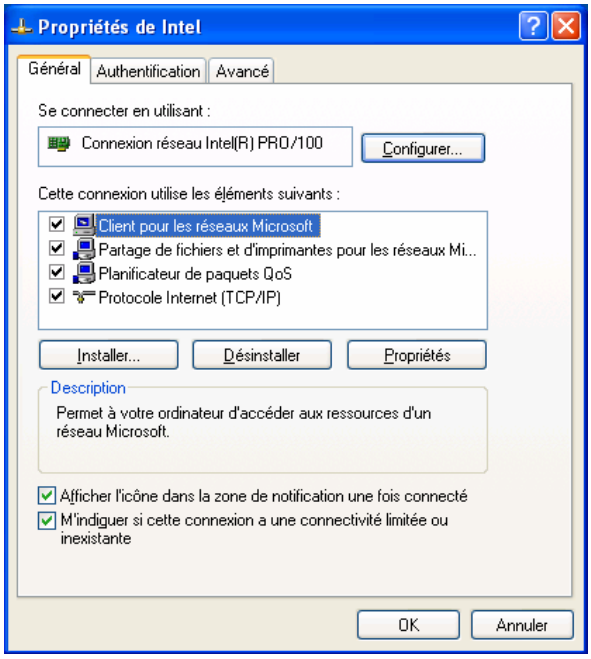
```
# file : /etc/raddb/users
#
# Création d'un utilisateur :
user  Auth-Type = Local, User-Password = "user"
```

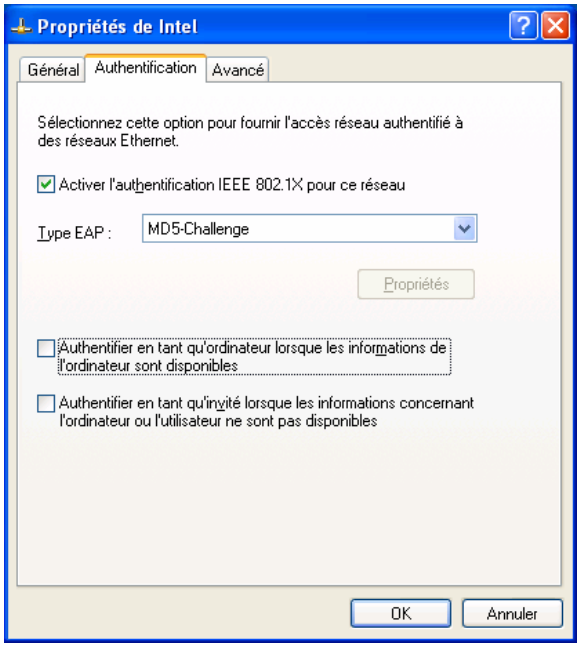
- après avoir modifié les fichiers de configuration du serveur Radius, vous devez relancez le processus par la commande : '`# /etc/rc.d/init.d/radiusd restart`'.

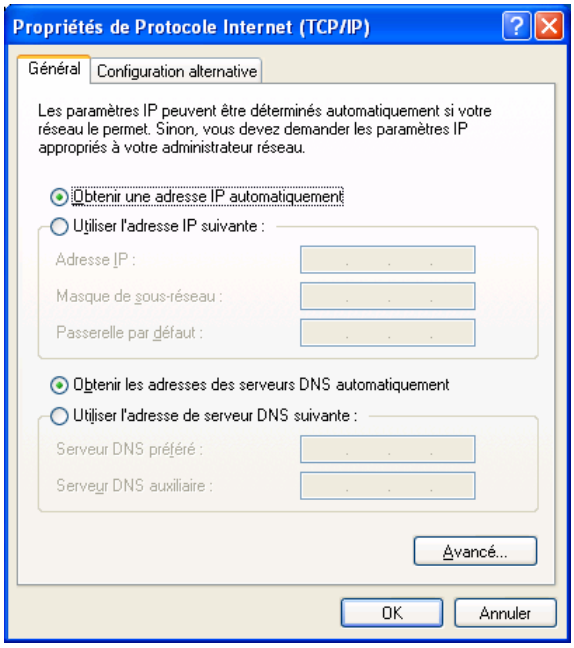
XIII.D.3 Windows XP Pro

XIII.D.3.a Configuration de l'interface réseau.

- Client DHCP.
- Authentification IEEE 802.1X en EAP MD5-Challenge, et décocher la case : '*Authentifier en tant qu'ordinateur lorsque les informations de l'ordinateur sont disponibles*'.







Avec le supplicant fourni en standard par Microsoft sous Windows 2000 ou XP il est possible d'utiliser 2 méthodes d'authentification EAP-TLS et PEAP.

L'authentification se fait au démarrage de la machine ou/et au logon de l'utilisateur. Le comportement est fixé par la valeur d'une clé dans le registre

HKEY_LOCAL_MACHINE\Software\Microsoft\EAPOL\Parameters\General\Global\AuthMode

- 0 (c'est la valeur par défaut) authentification de la machine au démarrage, en cas d'échec authentification de l'utilisateur au logon
- 1 authentification de la machine au démarrage, puis authentification de l'utilisateur au logon
- 2 uniquement authentification de la machine

XIII.D.3.b Verify the 802.1x Operation

- If you have correctly completed the configuration, the PC client displays a popup prompt to enter a user name and password.

- Follow these instructions:

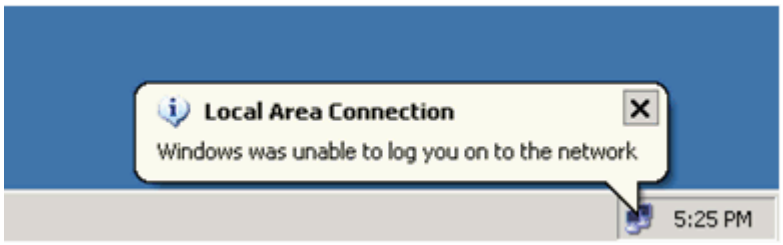
1. Click on the prompt, which this example shows:

A user name and password entry window displays.

2. Saisissez le nom d'utilisateur et son mot de passe (voir `/etc/raddb/user` du serveur Radius).

   - Nom d'utilisateur : `user`
   - Mot de passe : `user`

3. If no error messages appear, verify connectivity with the usual methods, such as through access of the network resources and with ping.



If this error appears, verify that the user name and password are correct:

4. If the password and user name appear to be correct, verify the 802.1x port state on the switch.

Look for a port status that indicates AUTHORIZED.

```
Switch22#sh dot1x statistics

FastEthernet0/7

    Rx: EAPOL     EAPOL     EAPOL     EAPOL     EAP       EAP       EAP
        Start     Logoff    Invalid   Total     Resp/Id   Resp/Oth  LenError
        1         0         0         11        5         5         0

        Last      Last
        EAPOLVer  EAPOLSrc
        1         0000.39c6.84d0

    Tx: EAPOL     EAP       EAP
        Total     Req/Id    Req/Oth
        37        19        5


Switch22#sh dot1x int fa0/7
802.1X is enabled on FastEthernet0/7
  Status                Authorized
  Port-control          Auto
  Supplicant            0000.39c6.84d0
  Multiple Hosts        Disallowed
  Current Identifier    3

  Authenticator State Machine
    State               AUTHENTICATED
    Reauth Count        0

  Backend State Machine
    State               IDLE
    Request Count       0
    Identifier (Server) 2

  Reauthentication State Machine
    State               INITIALIZE

Switch22#
```

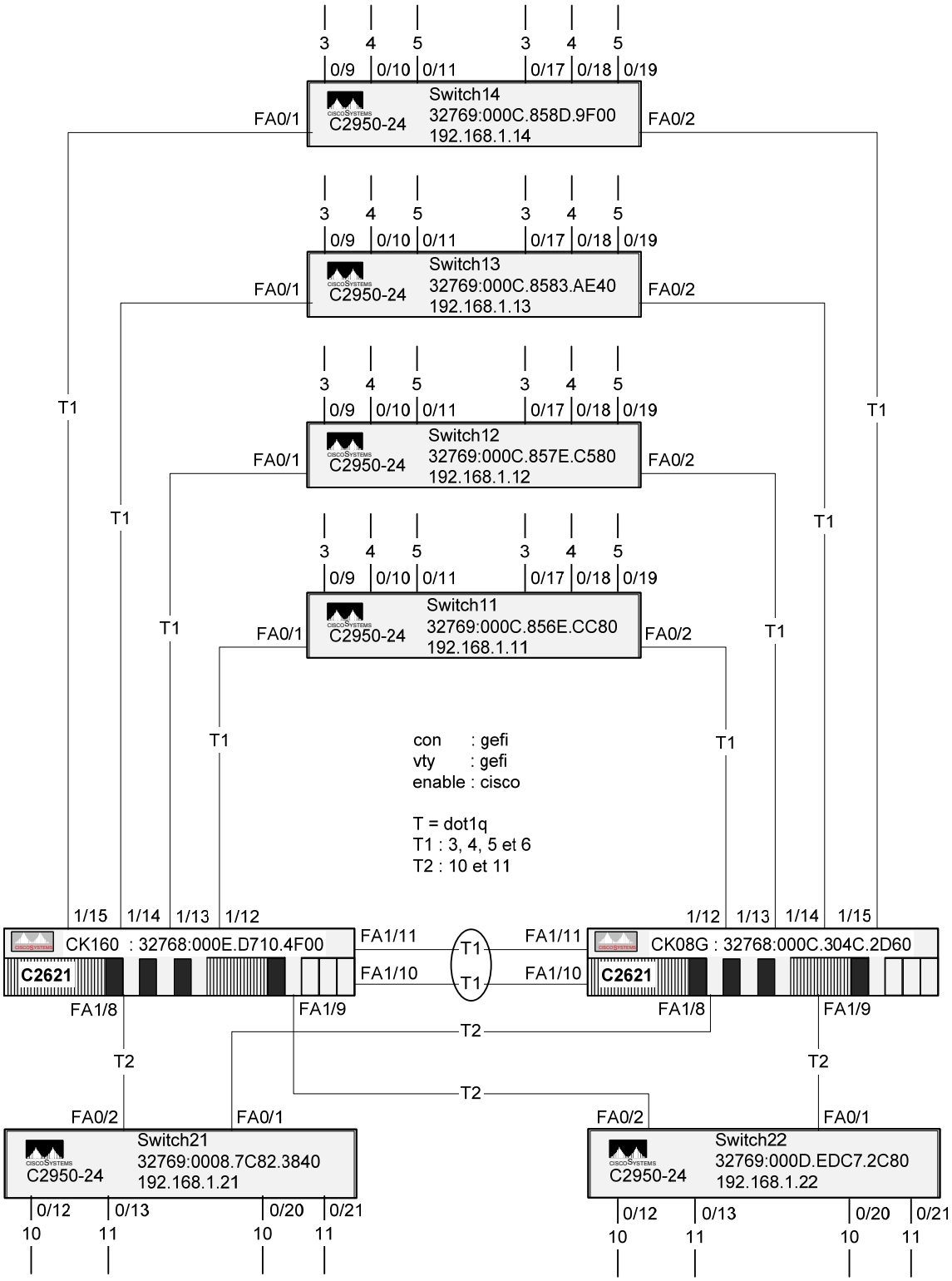
5. To troubleshoot further, collect the output of these **debug** commands:

   - **debug radius**

XIII.D.3.c Vérification : après connexion au port FA0/7 du switch.

```
C:\>ipconfig /all

Configuration IP de Windows

        Nom de l'hôte . . . . . . . . . . . : ts501
        Suffixe DNS principal . . . . . . . :
        Type de nœud . . . . . . . . . . . . : Hybride
        Routage IP activé . . . . . . . . . : Non
        Proxy WINS activé . . . . . . . . . : Non
        Liste de recherche du suffixe DNS : gefi.home


Carte Ethernet Intel:

        Suffixe DNS propre à la connexion : gefi.home
        Description . . . . . . . . . . . . : Connexion réseau Intel(R)
PRO/100
        Adresse physique . . . . . . . . . .: 00-00-39-C6-84-D0
        DHCP activé. . . . . . . . . . . . : Oui
        Configuration automatique activée . . . . : Oui
        Adresse IP. . . . . . . . . . . . . : 192.168.33.189
        Masque de sous-réseau . . . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . . . : 192.168.33.9
        Serveur DHCP. . . . . . . . . . . . : 192.168.33.9
        Serveurs DNS . . . . . . . . . . . .  : 192.168.33.9
        Serveur WINS principal. . . . . . . : 192.168.33.9
        Bail obtenu . . . . . . . . . . . . : lundi 16 mai 2005 12:46:52
        Bail expirant . . . . . . . . . . . : mardi 17 mai 2005 12:46:52

C:\>
```

XIV. Exercice de synthèse



```
       : Network          : Ck160        : Ck08g        : HSRP
-----------------------------------------------------------------------
Vlan1  : 192.168.1.0/24   : 192.168.1.1   : 192.168.1.2  : 192.168.1.3
Vlan3  : 192.168.3.0/24   : 192.168.3.1   : 192.168.3.2  : 192.168.3.3
Vlan4  : 192.168.4.0/24   : 192.168.4.1   : 192.168.4.2  : 192.168.4.3
Vlan5  : 192.168.5.0/24   : 192.168.5.1   : 192.168.5.2  : 192.168.5.3
Vlan6  : 192.168.6.0/24   : 192.168.6.1   : 192.168.6.2  : 192.168.6.3
Vlan10 : 192.168.10.0/24  : 192.168.10.1  : 192.168.10.2 : 192.168.10.3
Vlan11 : 192.168.11.0/24  : 192.168.11.1  : 192.168.11.2 : 192.168.11.3
```

Annexe A. Bridge ID, Switch Priority, and Extended System ID

The IEEE 802.1D standard requires that each switch has an unique bridge identifier (bridge ID), which determines the selection of the root switch. Because each VLAN is considered as a different *logical bridge* with PVST and PVRST, the same switch must have as many different bridge IDs as VLANs configured on it. Each VLAN on the switch has a unique 8-byte bridge ID; the two most-significant bytes are used for the switch priority, and the remaining six bytes are derived from the switch MAC address.

In Release 12.1(9)EA1 and later, Catalyst 2950 and Catalyst 2955 switches support the 802.1T spanning-tree extensions. Some of the bits previously used for the switch priority are now used as the VLAN identifier. The result is that fewer MAC addresses are reserved for the switch, and a larger range of VLAN IDs can be supported, all while maintaining the uniqueness of the bridge ID. As shown in Table 12-1, the two bytes previously used for the switch priority are reallocated into a 4-bit priority value and a 12-bit extended system ID value equal to the VLAN ID. In earlier releases, the switch priority is a 16-bit value.

Switch Priority Value and Extended System ID															
Switch Priority Value				**Extended System ID** (Set Equal to the VLAN ID)											
Bit 16	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN. With earlier releases, spanning tree used one MAC address per VLAN to make the bridge ID unique for each VLAN.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the "Configuring the Root Switch" section, "Configuring a Secondary Root Switch" section, and "Configuring the Switch Priority of a VLAN" section.

Annexe B. ICMP

Les messages ICMP, RFC 792				
Type	**Code**	**Description**	**Query**	**Error**
0	0	Echo Reply (Ping)	*	
3		Destination unreachable		*
	0	Network unreachable		*
	1	Host unreachable		*
	2	Protocol unreachable		*
	3	Port unreachable		*
	4	Fragmentation needed and « Don't fragment » bit set		*
	5	Source route failed		*
	6	Destination network unknown		*
	7	Destination host unknown		*
	8	Source host isolated (obsolete)		*
	9	Destination network administratively prohibited		*
	10	Destination host administratively prohibited		*
	11	Network unreachable for TOS		*
	12	Host unreachable for TOS		*
	13	Communication administratively prohibited by filtering		*
	14	Host precedence violation		*
	15	Precedence cut-off in effect		*
4	0	Source quench		*
5		Redirect		*
	0	Redirect datagrams for network		*
	1	Redirect datagrams for host		*
	2	Redirect datagrams for Type-Of-Service and network		*
	3	Redirect datagrams for Type-Of-Service and host		*
8	0	Echo Request (Ping)	*	
9	0	Router advertisement	*	
10	0	Router Solicitation	*	
11		Time Exceeded		*
	0	TTL equal 0 during transit		*
	1	TTL equal 0 during reassembly		*
12		Parameter problem		*
	0	IP header bad (catchall error)		*
	1	Required option missing		*
13	0	Timestamp request / marqueur temporel	*	
14	0	Timestamp reply / réponse à marqueur temporel	*	
15	0	Information request (obsolete)	*	
16	0	Information reply (obsolete)	*	
17	0	Address Mask Request	*	
18	0	Address Mask reply	*	

Annexe C. Mise à jour d'IOS

Commandes	signification
`# conf term`	
`# no ip http server`	
`# end`	
`# delete flash:html/*`	Effacement du répertoire flash:html
`# delete flash:c2900...`	Suppression de l'IOS

`# tar /x tftp://192.168.2.1/c2900...bin flash:`
ou
`# copy tftp://192.168.2.1/c2900...bin flash:`
	Transfert du nouvel IOS

`# conf term`	
`# ip http server`	
`# end`	
`# reload`	Arrêt et redémarrage

```
Block12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Block12(config)#no ip http server
Block12(config)#end
Block12#
2d10h: %SYS-5-CONFIG_I: Configured from console by consoledele
Block12#delete flash:html/*
Delete filename [html/*]?
Delete flash:html/Snmp? [confirm]
%Error deleting flash:html/Snmp (Is a directory)
Delete flash:html/ClusterBuilder.html.gz? [confirm]
Delete flash:html/ClusterManager.html.gz? [confirm]
Delete flash:html/Graph.html.gz? [confirm]
Delete flash:html/arptabl.htm.gz? [confirm]
Delete flash:html/bandwdth.htm.gz? [confirm]
Delete flash:html/baudrate.htm.gz? [confirm]
!
! ...
!
Delete flash:html/cgmpcfg.htm.gz? [confirm]
Delete flash:html/vmpscfg.htm.gz? [confirm]
Delete flash:html/vsm.htm.gz? [confirm]
Delete flash:html/vtpmgmt.htm.gz? [confirm]
Delete flash:html/clstbldr.toc? [confirm]
Delete flash:html/clstmgr.toc? [confirm]
Delete flash:html/cvsm.toc? [confirm]
Delete flash:html/ssp.toc? [confirm]
Delete flash:html/prefs.text? [confirm]
Delete flash:html/version.txt? [confirm]
Block12#delete flash:?
flash:/c2900XL-c3h2s-mz-120.5.2-XU.bin  flash:/c2900XL-diag-mz-120.5.2-XU  flash
:/config.text  flash:/env_vars  flash:/html
flash:/vlan.dat

Block12#delete flash:/c2900XL-c3h2s-mz-120.5.2-XU.bin
Delete filename [c2900XL-c3h2s-mz-120.5.2-XU.bin]?
Delete flash:/c2900XL-c3h2s-mz-120.5.2-XU.bin? [confirm]
Block12#delete flash:/c290
Block12#delete flash:/c2900XL-diag-mz-120.5.2-XU
Delete filename [c2900XL-diag-mz-120.5.2-XU]?
Delete flash:/c2900XL-diag-mz-120.5.2-XU? [confirm]
Block12#tar /x tftp://192.168.2.1/c2900xl-c3h2s-tar.120-5.WC3b.bin flash:
Loading c2900xl-c3h2s-tar.120-5.WC3b.bin from 192.168.2.1 (via VLAN1): !
extracting info (109 bytes)
extracting c2900XL-c3h2s-mz.120-5.WC3b.bin (1752223 bytes)!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

html/ (directory)
extracting html/homepage.htm (3994 bytes)!
```

```
extracting html/not_supported.html (1392 bytes)!
extracting html/common.js (9111 bytes)!
extracting html/cms_splash.gif (22062 bytes)!!!!!
extracting html/cms_12.html (911 bytes)
extracting html/cms_13.html (1010 bytes)!
extracting html/cluster.html (2823 bytes)
extracting html/CMS.jar (1280829 bytes)!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
extracting html/CiscoChartPanel.jar (74146 bytes)!!!!!!!!!!!!!!
extracting html/Redirect.jar (1958 bytes)!
extracting e2rb.bin (8192 bytes)!
extracting info.ver (109 bytes)!!
[OK - 3174400 bytes]

Block12#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Block12(config)#ip http server
Block12(config)#end
Block12#
2d10h: %SYS-5-CONFIG_I: Configured from console by console
Block12#reload

System configuration has been modified. Save? [yes/no]: y
Building configuration...

Proceed with reload? [confirm]

2d10h: %SYS-5-RELOAD: Reload requested
```

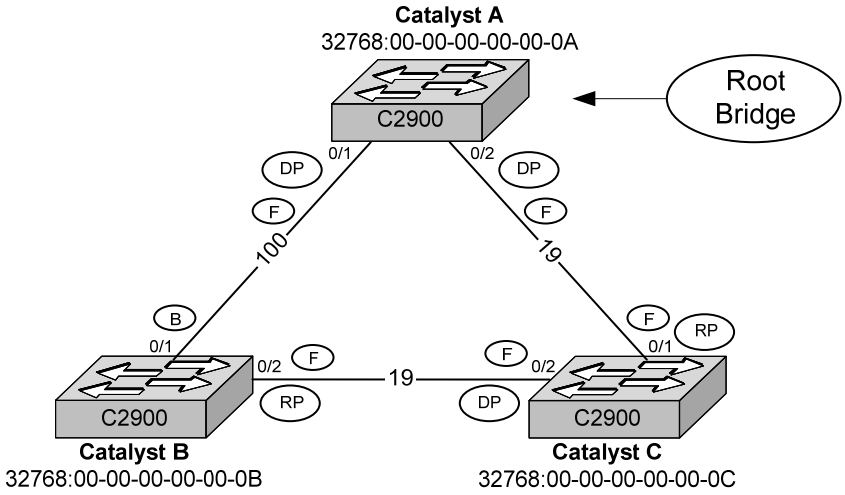
Annexe D. Password Recovery Procedure

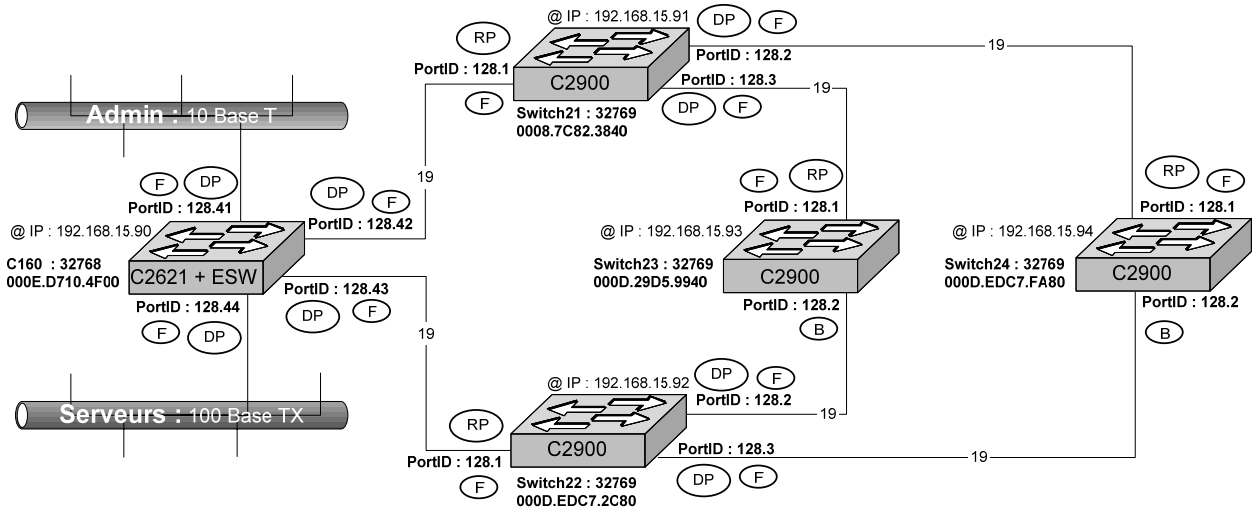
Pour switchs Catalyst 2900XL, 3500XL, 2950 et 3550 Series

1. Connectez un terminal sur le port console : 9600 bps, No parity, 8 bits data, 1 stop bit et No flow control
2. Débranchez le câble d'alimentation
3. Presser et maintenir le bouton MODE à gauche en face avant du switch puis rebranchez le câble d'alimentation. Vous pouvez relâcher le bouton MODE une à deux secondes après que la LED du port 1x soit éteinte.
4. Tapez la commande : `flash_init`
5. Tapez la commande : `load_helper`
6. Tapez la commande : `dir flash:` (ne pas oublier les deux points après *flash*)
7. Tapez la commande : `rename flash:config.text flash:config.old` pour renommez le fichier de configuration. Ce fichier contient la définition de mot de passe.
8. Tapez la commande : `boot` pour rebooter le système.
9. entrez N au prompt lors du démarrage du programme Setup :
   - `Continue with the configuration dialog? [yes/no] : N`
10. au prompt de l'IOS tapez : `enable` pour travailler en mode Enable.
11. Tapez la commande : `rename flash:config.old flash:config.text` pour renommez le fichier de configuration avec ses valeurs initialles.
12. Copiez le fichier de configuration en mémoire
    - `Switch# copy flash:config.text system:running-config`
13. changez le mot de passe
    - `Switch# configure terminal`
    - `Switch(config)# no enable secret`
    - `Switch(config)# enable password cisco`
14. Sauvegardez le nouveau fichier de configuration
    - `Switch# write memory`

Annexe E. Correction

- Correction des deux exercices sur le Spanning Tree.





Annexe F. MPLS

MPLS : Multi Protocol Label-Switching
GMPLS : Generalized MPLS

F.I Présentation

CIOA : Classical IP Over ATM
MPOA : Multi Protocol Over ATM
PNNI : Private Network Node Interface
NHRP : Next Hop Resolution Protocol

- Le protocole IP est devenu le standard de raccordement à un réseau pour tous les systèmes informatiques. De son côté, la technologie ATM incarne la solution préférée des opérateurs pour interconnecter des équipements réseau entre eux, tout en offrant de la qualité de service.
- La difficulté de cette solution se situe au niveau de l'adressage, la problématique vient de la correspondance de l'adresse IP et de l'adresse ATM (sachant que ATM est NBMA).
- On peut regrouper les solutions en trois catégories :
    - Les techniques d'émulation :
    - Le protocole CIOA (*Classical IP Over ATM*), lorsqu'il n'y a qu'un seul sous réseau ATM.
    - Les techniques de serveurs de routes MPOA, PNNI et NHRP, lorsqu'il y a plusieurs sous-réseaux ATM à traverser.

- Ces trois dernières techniques sont de plus en plus remplacées par MPLS (normalisé par l'IETF).

F.II Terminologie

Annexe G. MLS

MLS : Multilayer Switching

- Disposer d'un IOS Version 12.1 ou plus
- Le '*Multilayer switching*' combine la commutation de couche 2 et le routage de couche 3.

RP : Route Processor
SE : Switching Engine

G.I Terminology

The following terminology is used in the MLS chapters:

- Multilayer Switching-Switching Engine (MLS-SE)—A NetFlow Feature Card (NFFC)-equipped Catalyst 5000 series switch.
- Multilayer Switching-Route Processor (MLS-RP)—A Cisco router with MLS enabled.
- Multilayer Switching Protocol (MLSP)—The protocol running between the MLS-SE and MLS-RP to enable MLS**.**

G.II Introduction to MLS

- Layer 3 protocols, such as IP and Internetwork Packet Exchange (IPX), are connectionless—they deliver each packet independently of each other. However, actual network traffic consists of many end-to-end conversations, or flows, between users or applications.
- A flow is a unidirectional sequence of packets between a particular source and destination that share the same protocol and transport-layer information. Communication from a client to a server and from the server to the client is in separate flows. For example, HTTP Web packets from a particular source to a particular destination are in a separate flow from File Transfer Protocol (FTP) file transfer packets between the same pair of hosts.
- Flows can be based on only Layer 3 addresses. This feature allows IP traffic from multiple users or applications to a particular destination to be carried on a single flow if only the destination IP address is used to identify a flow.
- The NFFC maintains a Layer 3 switching table (MLS cache) for the Layer 3-switched flows. The cache also includes entries for traffic statistics that are updated in tandem with the switching of packets. After the MLS cache is created, packets identified as belonging to an existing flow can be Layer 3-switched based on the cached information. The MLS cache maintains flow information for all active flows. When the Layer 3-switching entry for a flow ages out, the flow statistics can be exported to a flow collector application.
- For information on multicast MLS, see the "Introduction to IP Multicast MLS" section in this chapter.

G.III Key MLS Features

Summary of Key Features	
Feature	Description
Ease of Use	Is autoconfigurable and autonomously sets up its Layer 3 flow cache. Its "plug-and-play" design eliminates the need for you to learn new IP switching technologies.
Transparency	Requires no end-system changes and no renumbering of subnets. It works with DHCP[1] and requires no new routing protocols.
Standards Based	Uses IETF[2] standard routing protocols such as OSPF and RIP for route determination. You can deploy MLS in a multivendor network.
Investment Protection	Provides a simple feature-card upgrade on the Catalyst 5000 series switches. You can use MLS with your existing chassis and modules. MLS also allows you to use either an integrated RSM or an external router for route processing and Cisco IOS services.
Fast Convergence	Allows you to respond to route failures and routing topology changes by performing hardware-assisted invalidation of flow entries.
Resilience	Provides the benefits of HSRP[3] without additional configuration. This feature enables the switches to transparently switch over to the Hot Standby backup router when the primary router goes offline, eliminating a single point of failure in the network.
Access Lists	Allows you to set up access lists to filter, or to prevent traffic between members of different subnets. MLS enforces multiple security levels on every packet of the flow at wire speed. It allows you to configure and enforce access control rules on the RSM. Because MLS parses the packet up to the transport layer, it enables access lists to be validated. By providing multiple security levels, MLS enables you to set up rules and control traffic based on IP addresses and transport-layer application port numbers.
Accounting and Traffic Management	Allows you to see data flows as they are switched for troubleshooting, traffic management, and accounting purposes. MLS uses NDE to export the flow statistics. Data collection of flow statistics is maintained in hardware with no impact on switching performance. The records for expired and purged flows are grouped and exported to applications such as NetSys for network planning, RMON2[4] traffic management and monitoring, and accounting applications.
Network Design Simplification	Enables you to speed up your network while retaining the existing subnet structure. It makes the number of Layer 3 hops irrelevant in campus design, enabling you to cope with increases in any-to-any traffic.
Media Speed Access to Server Farms	You do not need to centralize servers in multiple VLANs to get direct connections. By providing security on a per-flow basis, you can control access to the servers and filter traffic based on subnet numbers and transport-layer application ports without compromising Layer 3 switching performance
Faster Interworkgroup Connectivity	Addresses the need for higher-performance interworkgroup connectivity by intranet and multimedia applications. By deploying MLS, you gain the benefits of both switching and routing on the same platform.

1DHCP = Dynamic Host Configuration Protocol

2IETF = Internet Engineering Task Force

3HSRP = Hot Standby Router Protocol

4RMON2 = Remote Monitoring 2

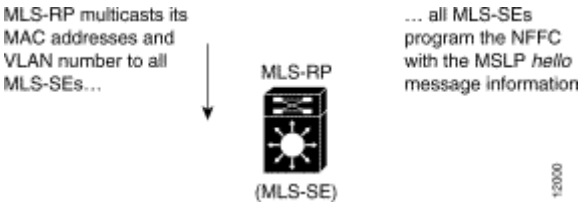
G.IV MLS Implementation

This section provides a step-by-step description of MLS implementation.

Note The MLS-RPs shown in the figures represent either a RSM or an externally attached Cisco router.

The MLSP informs the Catalyst 5000 series switch of the MLS-RP MAC addresses used on different VLANs and the MLS-RP's routing and access list changes. Through this protocol, the MLS-RP multicasts its MAC and VLAN information to all MLS-SEs. When the MLS-SE hears the MLSP *hello* message indicating an MLS initialization, the MLS-SE is programmed with the MLS-RP MAC address and its associated VLAN number (see Figure 64).

Figure 64 MLS Implementation

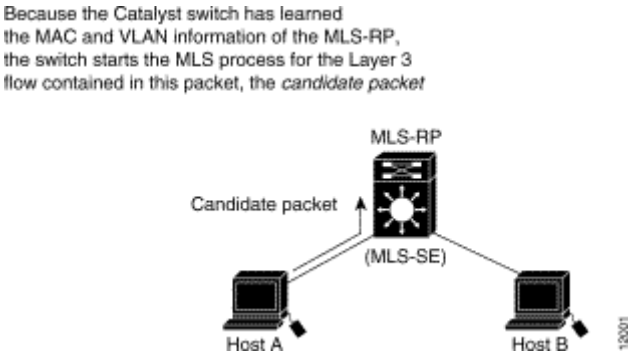


In Figure 65, Host A and Host B are located on different VLANs. Host A initiates a data transfer to Host B. When Host A sends the first packet to the MLS-RP, the MLS-SE recognizes this packet as a *candidate packet* for Layer 3 switching because the MLS-SE has learned the MLS-RP's destination MAC address and VLAN through MLSP. The MLS-SE learns the Layer 3 flow information (such as the destination address, source address, and protocol port numbers), and forwards the first packet to the MLS-RP. A partial MLS entry for this Layer 3 flow is created in the MLS cache.

The MLS-RP receives the packet, looks at its route table to determine how to forward the packet, and applies services such as Access Control Lists (ACLs) and class of service (COS) policy.

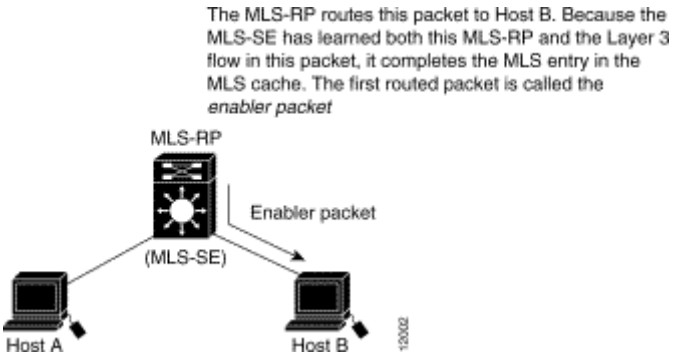
The MLS-RP rewrites the MAC header adding a new destination MAC address (Host B's) and its own MAC address as the source.

Figure 65 MLS Implementation



The MLS-RP routes the packet to Host B. When the packet appears back on the Catalyst 5000 series switch backplane, the MLS-SE recognizes the source MAC address as that of the MLS-RP, and that the packet's flow information matches the flow for which it set up a candidate entry. The MLS-SE considers this packet an *enabler packet* and completes the MLS entry (established by the candidate packet) in the MLS cache (see Figure 66).

Figure 66 MLS Implementation

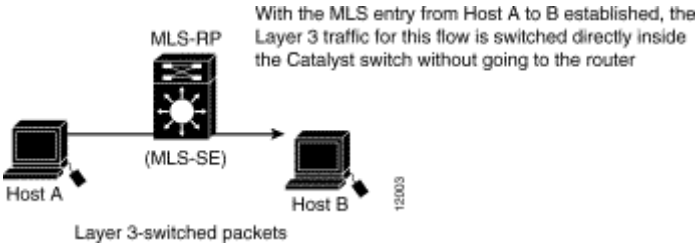


After the MLS entry has been completed, all Layer 3 packets with the same flow from Host A to Host B are Layer 3 switched directly inside the switch from Host A to Host B, bypassing the router (see Figure 67). After the Layer 3-switched path is established, the packet from Host A is rewritten by the MLS-SE before it is forwarded to Host B. The rewritten information includes the MAC addresses, encapsulations (when applicable), and some Layer 3 information.

The resultant packet format and protocol behavior is identical to that of a packet that is routed by the RSM or external Cisco router.

Note MLS is unidirectional. For Host B to communicate with Host A, another Layer 3-switched path needs to be created from Host B to Host A.

Figure 67 MLS Implementation



See the *Catalyst 5000 Series Multilayer Switching User Guide* for additional network implementation examples that include network topologies that do not support MLS.

G.V Configuring MLS on a Router

- To configure MLS on your router, use the following commands beginning in global configuration mode. Depending upon your configuration, you might not have to perform all the steps in the procedure.

Step	Command	Purpose
1	`Router(config)# mls rp ip`	Globally enables MLSP. MLSP is the protocol that runs between the MLS-SE and the MLS-RP.
2	`Router(config)# interface` *type number*	Selects a router interface.
3	`Router(config-if)# mls rp vtp-domain` [*domain-name*]	Selects the router interface to be Layer 3 switched and then adds that interface to the same VLAN Trunking Protocol (VTP) domain as the switch. This interface is referred to as the MLS interface. This command is required only if the Catalyst switch is in a VTP domain.
4	`Router(config-if)# mls rp vlan-id` [*vlan-id-num*]	Assigns a VLAN ID to the MLS interface. MLS requires that each interface has a VLAN ID. This step is not required for RSM VLAN interfaces or ISL-encapsulated interfaces.
5	`Router(config-if)# mls rp ip`	Enables each MLS interface.
6	`Router(config-if)# mls rp management-interface`	Selects one MLS interface as a management interface. MLSP packets are sent and received through this interface. This can be any MLS interface connected to the switch.
	Repeat steps 2 through 5 for each interface that will support MLS.	

Note The interface-specific commands in this section apply only to Ethernet, Fast Ethernet, VLAN, and Fast Etherchannel interfaces on the Catalyst RSM/Versatile Interface Processor 2 (VIP2) or directly attached external router.

- To globally disable MLS on the router, use the following command in global configuration mode:

Command	Purpose
`Router(config)# no mls rp ip`	Disables MLS on the router.

G.VI Monitoring MLS

To display MLS details including specifics for MLSP, use the following commands in EXEC mode, as needed:

- MLS status (enabled or disabled) for switch interfaces and subinterfaces
- Flow mask used by this MLS-enabled switch when creating Layer 3-switching entries for the router
- Current settings of the keepalive timer, retry timer, and retry count
- MLSP-ID used in MLSP messages
- List of interfaces in all VTP domains that are enabled for MLS

Command	Purpose
`Router# show mls rp`	Displays MLS details for all interfaces.

After entering this command, you see this display:

```
router# show mls rp
multilayer switching is globally enabled
mls id is 00e0.fefc.6000
mls ip address 10.20.26.64
mls flow mask is ip-flow
vlan domain name: WBU
current flow mask: ip-flow
current sequence number: 80709115
current/maximum retry count: 0/10
current domain state: no-change
current/next global purge: false/false
current/next purge count: 0/0
domain uptime: 13:03:19
keepalive timer expires in 9 seconds
retry timer not running
change timer not running
fcp subblock count = 7
1 management interface(s) currently defined:
vlan 1 on Vlan1
7 mac-vlan(s) configured for multi-layer switching:
mac 00e0.fefc.6000
vlan id(s)
1 10 91 92 93 95 100
router currently aware of following 1 switch(es):
switch id 0010.1192.b5ff
```

G.VII Monitoring MLS for an Interface

To show MLS information for a specific interface, use the following command in EXEC mode:

Command	Purpose
Router# **show mls rp** [*interface*]	Displays MLS details for a specific interface.

After entering this command, you see this display:

```
router# show mls rp int vlan 10
mls active on Vlan10, domain WBU
router#
```

G.VIII Monitoring MLS Interfaces for VTP Domains

To show MLS information for a specific VTP domain use the following command in EXEC mode:

Command	Purpose
Router# **show mls rp vtp-domain** [*domain-name*]	Displays MLS interfaces for a specific VTP domain.

After entering this command, you see this display:

```
router# show mls rp vtp-domain WBU
vlan domain name: WBU
current flow mask: ip-flow
current sequence number: 80709115
current/maximum retry count: 0/10
current domain state: no-change
current/next global purge: false/false
current/next purge count: 0/0
domain uptime: 13:07:36
keepalive timer expires in 8 seconds
retry timer not running
change timer not running
fcp subblock count = 7
1 management interface(s) currently defined:
vlan 1 on Vlan1
7 mac-vlan(s) configured for multi-layer switching:
mac 00e0.fefc.6000
vlan id(s)
1 10 91 92 93 95 100
router currently aware of following 1 switch(es):
switch id 0010.1192.b5ff
```

Annexe H. SNMP

Commandes	Commentaires
`Access-list 2 permit 192.168.3.32 0.0.0.1`	ACL qui autorise les stations à l'accès SNMP 'Public'
`Snmp-server community private RW 2`	Création de la community 'Private' en Read/Write aux stations correspondant à l'ACL 2.
`Snmp-server packetsize 4096`	La taille par défaut est de 484 octets
`Snmp-server trap-authentication`	Remonte des traps si des accès avec un nom de community incorrecte
`Snmp-server host 192.168.3.32 public`	Identification du destinataire des TRAPs

- Pour obtenir les MIB :
  - Allez sur le site ftp.cisco.com en anonymous
  - Dans le répertoire /pub/mibs/supportlists/wsc2900xl pour les Catalyst 2900 XL,
  - Dans le répertoire /pub/mibs/supportlists/wsc3500xl pour les Catalyst 3500 XL,
  - Faire la commande get MIB_Filename pour obtenir le fichier MIB souhaité.

Annexe I. Algorithme de IP

RFC 791 & 1122

- Site : http://www.infonet.fundp.ac.be/LEARN/labo-rip.

```
Procédure routageIP(données data: datagramme, Table: table de routage)
début
  adresse_passerelle := adresse colonne 'Passerelle'
  adresse_dest := l'adresse IP de la destination extraite de data;
  adresse_source := l'adresse IP de la source extraite de data;
  si adresse_dest correspond à  une des adresse IP  du routeur
    alors envoyer le paquet à destination
      sortir de la procédure;
    sinon Aller dans  table
            ' REMARQUE: LES ADRESSES IP SONT CLASSÉES PAR ORDRE DÉCROISSANT DE LEUR MASQUE'
      'recherche de la correspondance la plus longue (la plus spécifique)'
      pour chaque entrée faire:
      N := masque du sous-réseau;
      si les N  bits de tête de adresse_dest = les N  bits de tête de l'adresse de sous-reseau
           alors si on se trouve dans la partie directement connectée de la table de routage
            Alors  envoyer le paquet à destination:
                     transmettre(data, adresse_dest);
              sinon  envoyer le paquet à l'adresse passerelle:
                transmettre(data, adresse_passerelle)
                  finsi;
      finpour;

        si pas d'entrée trouvée
        alors  retourner à source un datagramme indiquant une erreur de routage
      finsi
  finsi
fin


Procédure transmettre(données data: datagramme, IP: adresse IP)
    début si reseau broadcast à accès multiple (ethernet, token ring, ...)
         alors 'obtention de l'adresse couche 2 de destination'
          Consultation de la table ARP
          si table ARP pas disponible
            alors   lancement d'une requête ARP sur le sous-reseau
                (de manière à obtenir l'adresse MAC 48 bits de la machine destination)
                      'envoi du datagramme'

           encapsulement de data dans une trame de liaison de données;
           émission de data dans une trame liaison de données à
           destination de l'adresse de destination MAC 48 bits;
           sortie de la procédure

         sinon si connexion point à point (PPP, ...)
             alors émission de data dans une trame PPP à destination de la machine passerelle
             sinon si autre type de reséau (ATM, X25, ..)
                      alors ...
```

Annexe J. *Console Port Signals and Pinouts*

Use the console RJ-45 to DB-9 serial cable to connect the access point's console port to the COM port of your PC running a terminal emulation program.

Note Both the Ethernet and console ports use RJ-45 connectors. Be careful to avoid accidently connecting the serial cable to the Ethernet port connector.

Note When your configuration changes are completed, you must remove the serial cable from the access point.

Table E-1 lists the signals and pinouts for the console RJ-45 to DB-9 serial cable.

Table E-1 Signals and Pinouts for a Console RJ-45 to DB-9 Serial Cable

Console Port		**PC COM Port**	
RJ-45		DB-9	
Pins	Signals[1, 2, 3, 4]	Pins	Signals[1, 2, 3, 4]
1	NC	-	-
2	NC	-	-
3	TXD	2	RXD
4	GND	5	GND
5	GND	5	GND
6	RXD	3	TXD
7	NC	-	-
8	NC	-	-

[1] NC indicates not connected.

[2] TXD indicates transmit data.

[3] GND indicates ground.

[4] RXD indicates receive data.

Annexe K. Glossaire

CAM — Content-Addressable Memory
Table en mémoire contenant les adresses MAC sources des trames Ethernet reçues, cette terme Cisco correspond à la 'Forwarding Data Base' des switchs actuels.

CEF — Cisco Express Forward

CPE — Customer premises Equipment

LRE — Long-Reach Ethernet
Solution permettant d'utiliser un câblage téléphonique pour transporter de l'Ethernet et de s'affranchir de la limite de 100 mètres imposée par la norme. Distances couvertes : 1525 m à 5 Mbps, 1220 m à 10 Mbps et 1067 m à 15 Mbps.

MLS — Multi layer Switching
Route le premier datagramme puis switch les autres. Voir CEF

MPLS — Multi Protocol Label-Switching

MSTP — Multiple Spanning Tree Protocol ou IEEE 802.1S

NIC — Network Interface Card
Carte d'interface réseau (ex. : carte Ethernet).

PVST — Per-VLAN Spanning Tree

PVRST — Per-VLAN Rapid Spanning Tree ou IEEE 802.1W

RPS — Redundant Power System

SAID — Security Association Identifier

VMPS — VLAN Membership Policy Server
Le VMPS peut-être hébergé sur un Catalyst de la série 5000, mais pas sur des switchs des séries 2900XL et 3500XL.

VTP — VLAN Trunking Protocol
Protocole propriétaire CISCO permettant de centraliser les informations de configuration des VLAN.

Annexe L. Bibliographie CISCO

ICND : Interconnexion des systèmes réseaux Cisco	Steve McQuerry	CISCO Press
Cisco Field Manuel Catalyst Switch Configuration	David HUCABY Steve McQUERRY	CISCO Press
Architecture réseau Linux Conception et implémentation des protocoles réseau du noyau Linux	K. Wehrle, F. Pählke, H. Ritter, D. Müller, M. Bechler	VUIBERT
Préparation à la certification CCNA	Wendell Odom	CISCO Press
Architecture de réseaux & études de cas		CISCO Press
Conception d'inter réseaux CISCO	Matthew H. BIRKNER	CISCO Press
Sécurité des réseaux	Merike KAEO	CISCO Press
Installer et configurer un routeur CISCO	Chris LEWIS	EYROLLES
Configuration IP des routeurs CISCO	Innokenty RUDENKO	EYROLLES
Dépannage des réseaux	Jonathan FELDMAN	Campus Press