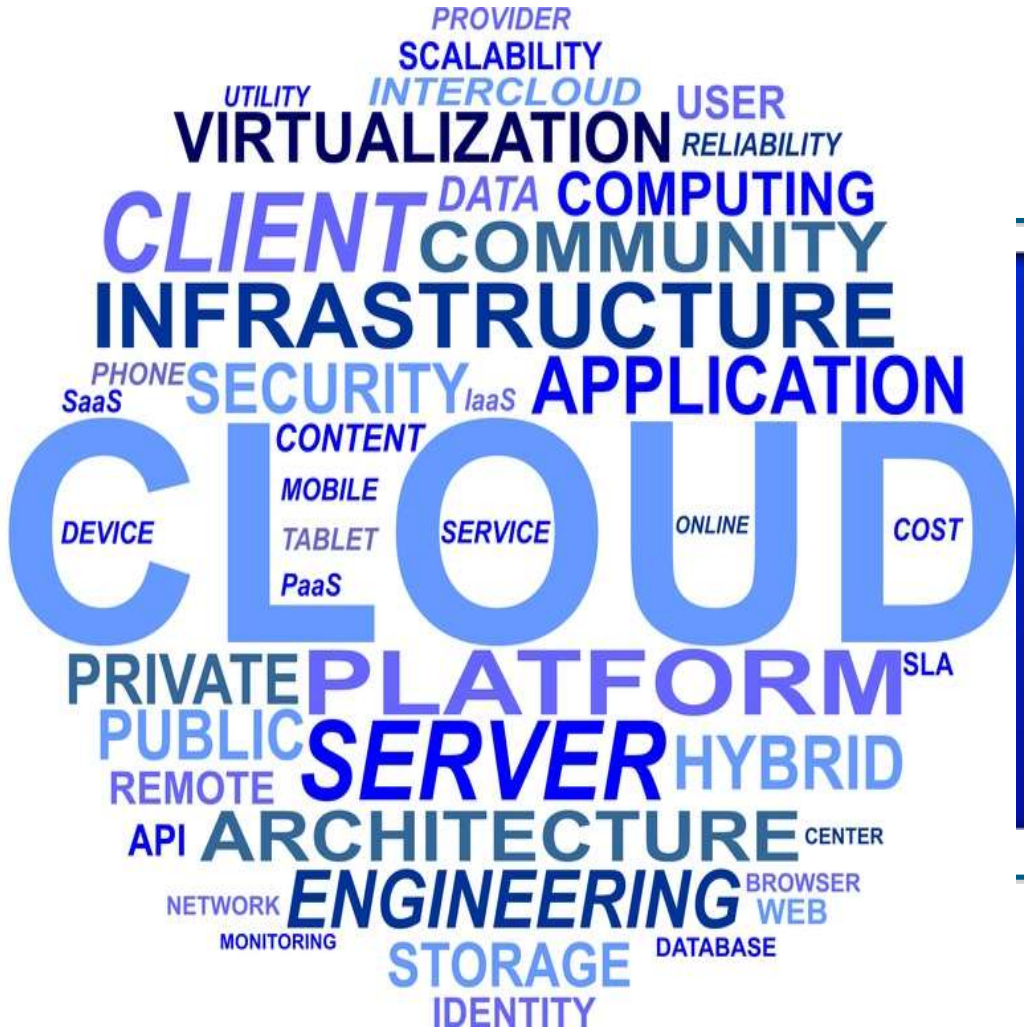


Infrastructure Réseau
Conception et Déploiement

Conception et Déploiement d'Infrastructure Réseaux

Master 2 Réseaux et Systèmes Distribués

Mr A. Dekhinet
Université de BATNA 2
Département d'Informatique

Contenu de la matière

Chapitre 1 : Identification des exigences

- Performances, Disponibilité, Fiabilité, Adaptabilité, Extensibilité, Convergence, …
- Exigences des applications : Capacité, Débit, Delai, Securité, Qualité de service,…
- Application temps réel
- Cas des services : VoIP, Streaming, …

Chapitre 2 : Modèle de conception Hiérarchique

- Introduction
- Couche Accès
- Couche Distribution
- Couche Cœur
- Dimensionnement : Support, Brassage, ...

Chapitre 3 : Couche Accès

- Technologies des réseaux d'accès
- Segmentation des réseaux
- Les commutateurs
- Les VLANs
- Les accès Distants

Chapitre 4 : Couche Distribution

- Technologie des réseaux de distribution
- Debits : Fast, Giga, 10 Giga
- Les VLANS : Trunking
- Commutation de niveau 3
- MLS : Multilayer Switch
- Spanning tree

Contenu de la matière

Chapitre 5 : Couche Coeur

- Technologie des réseaux de Cœur
- Performances, Redondance, …
- Commutation de niveau 3 et Routage
- VPN

Chapitre 6 : Adressage et Routage

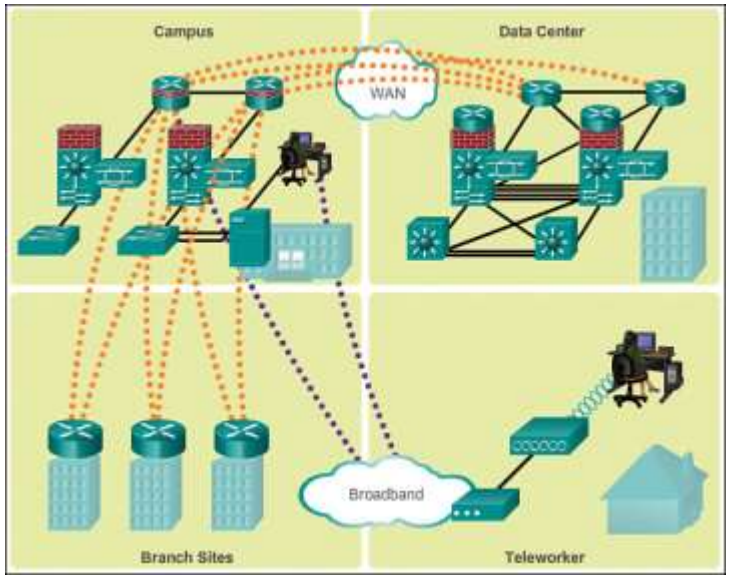
- Plan d'adressage
- Adressage IP publique et privé
- VLSM
- Protocoles de Routage Interne : RIP, OSPF
- Protocoles de Routage Externe : BGP

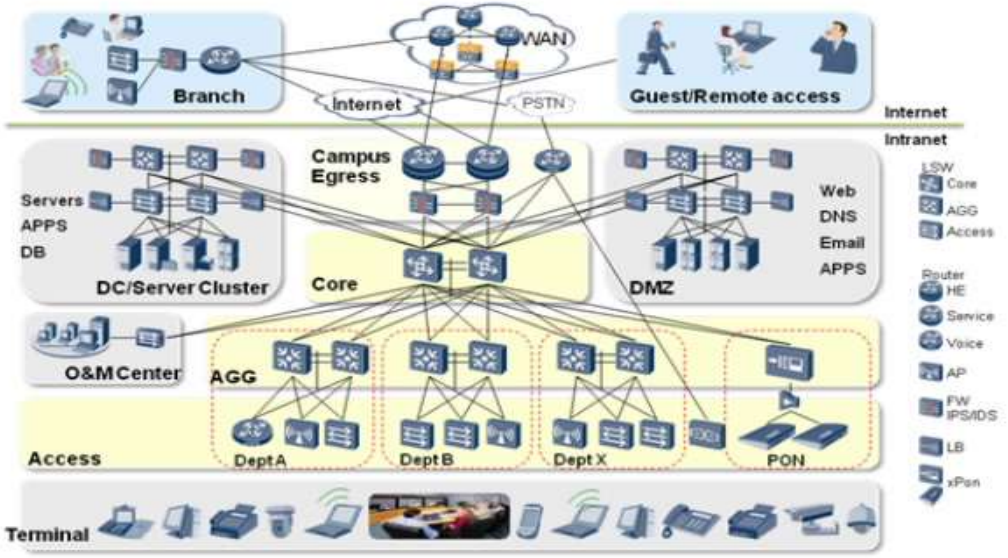
Chapitre 7 : Sécurité et Monitoring

- Sécurité du perimètre : Firewall, IPS, NAT, Web, …
- Sécurité de l'accès au réseau : NAC
- Sécurité physique
- Monitoring : Accès, Performance, Disponibilité, …

IT Infrastructure

- IT Infrastructure = Data Center (Servers, Storage) + Network Infrastructure





Principes de Conception

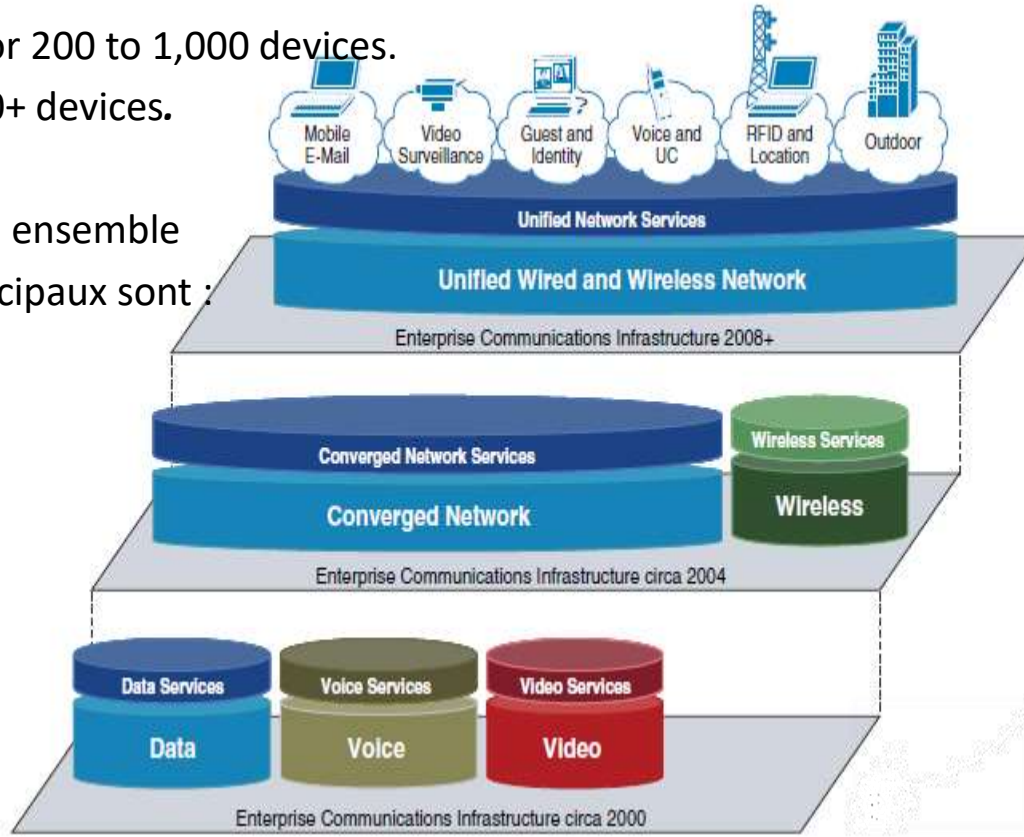
- Le déploiement d'une infrastructure doit être basé sur des principes de conception solides
- Une infrastructure réseau ou infrastructure de communication doit répondre aux besoins actuels de l'entreprise et être capable de supporter les technologies émergentes
- L'infrastructure réseau doit être convergente est unifiée : Une infrastructure pour tous les services (Data, Video, Audio, RFID, …)
- La conception doit prendre en considération la taille du réseau :

  Small network: Provides services for up to 200 devices.

  Medium-size network: Provides services for 200 to 1,000 devices.

  Large network: Provides services for 1,000+ devices.

- La conception de réseau est fondée sur un ensemble de principes fondamentales, dont les principaux sont :
  - Hierarchy
  - Modularity
  - Resiliency et High availability
  - Flexibility et Scalability



Principes de Conception

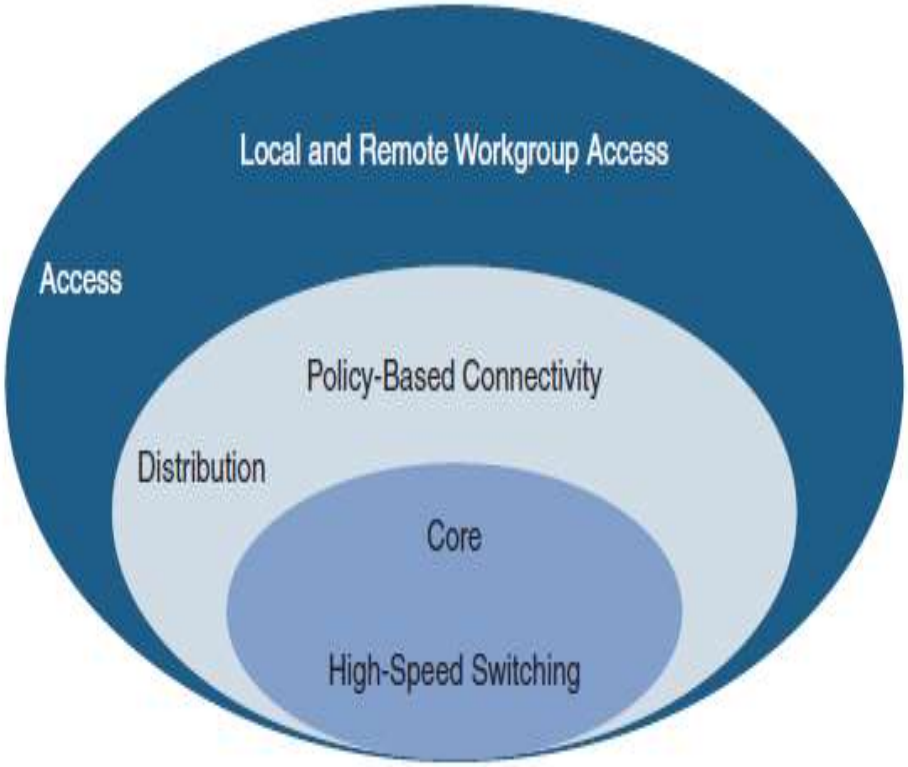
- **Hierarchy:** A *hierarchical network model* is a useful high-level tool for designing a reliable network infrastructure. It breaks the complex problem of network design into smaller and more manageable areas.
- **Modularity:** By separating the various functions that exist on a network into modules, the network is easier to design. For example Cisco has identified several modules, including the enterprise campus, services block, data center, and Internet edge.
- **Resiliency and High availability :** The network must remain available for use under both normal and abnormal conditions. Normal conditions include normal or expected traffic flows and traffic patterns. Abnormal conditions include hardware or software failures, extreme traffic loads, unusual traffic patterns, denial-of-service (DoS) events, whether intentional or unintentional, and other unplanned events.
- **Flexibility and Scalability:** The ability to modify portions of the network, add new services, or increase capacity without going through a major upgrade (i.e., replacing or adding network devices, adding new network segments, …).

Principes de Conception

- **Hiérarchie** : Le modèle de réseau hiérarchique est un moyen de haut niveau utile pour concevoir une infrastructure réseau fiable. Il permet de maitriser la complexité du problème de conception et de déploiement, en le découpant en parties maitrisables et gérables.
- **Modularité** : En séparant et en isolant les différentes fonctions qui peuvent exister dans un réseau en modules, le réseau est alors plus facile à concevoir. Plusieurs modules ou blocs sont identifiés, y compris le campus de l'organisme, le bloc des services, le data center, le WAN, Internet ou bloc publique.
- **Haute disponibilité** : Le réseau doit être disponible et fonctionnel dans les conditions normales et anormales. Les conditions anormales inclus les pannes matérielles et logiciels, la surcharge, le trafic anormal, le DoS, ...
- **Flexibilité et scallabilité** : L'infrastructure doit être apte à s'adapter et à supporter les éventuelles changements et extensions. Ces dernières peuvent inclure des extensions d'équipements réseautiques, des segments de réseaux (VLAN), des services, ...

Hiérarchie

- Le modèle de réseau hiérarchique (Three-Layers Hierarchical Internetworking design/model) est l'un des moyens et guide utilisé pour la conception d'infrastructure réseau.
- Selon le rôle et la nature des fonctions le modèle ressortis trois couches ou niveaux :
  - Cœur (Core)
  - Distribution ou Agrégation
  - Accès (Access)



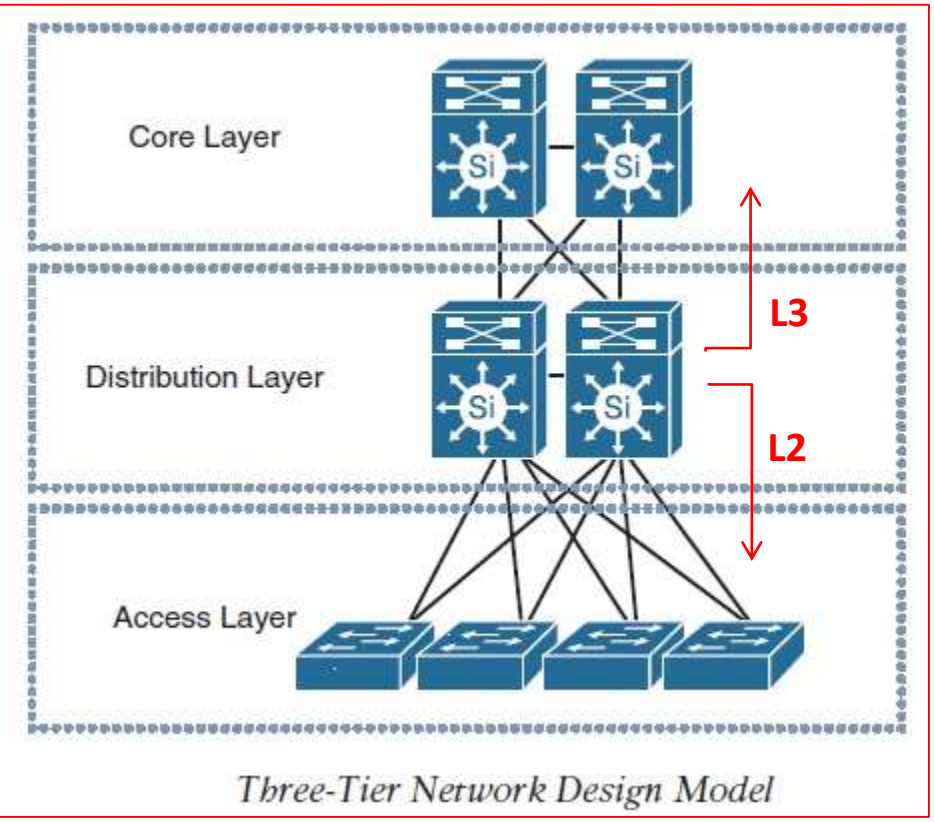
Modèle hiérarchique

- **Couche Accés** : C'est le point d'entrée qui permet aux utilisateurs finaux d'accéder au réseau. Dans les réseaux de campus, la couche accès comporte des switchs, généralement de niveau 2 (L2), dotés de fonctionnalités avancées. Les switchs fournissent la connectivité réseau à divers types d'équipements : PC, Serveurs, IP phone, Point d'accès, IP Camera. Pour les sites distants, la couche accès assure l'accès au réseau de l'entreprise en utilisant des technologies WAN.

- **Couche Distribution** : C'est la couche d'agrégation des uplinks et du traffic provenant de la couche accès à destination de la couche cœur. Elle fournit une connectivité basée sur des règles ou politiques d'accès (Policy-based connectivity). Pour assurer la segmentation du réseau et limiter les domaines de diffusion, la couche distribution comporte des routeurs ou des switchs de niveau 3.

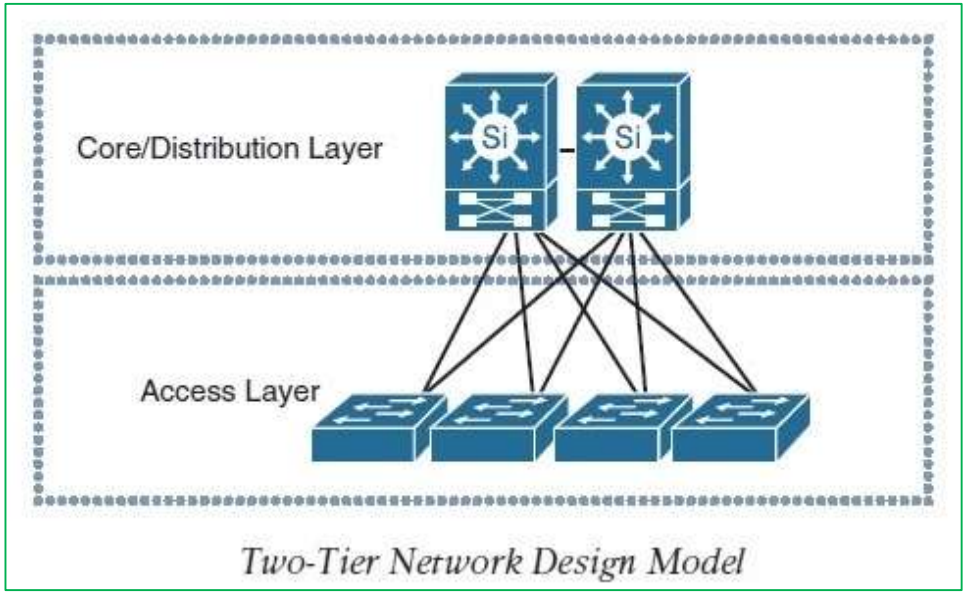
- **Couche Cœur** : C'est la couche dorsale ou backbone du réseau. Elle comporte des équipements de haute performances (High-speed network devices), tels que les switchs fédérateurs haut de gamme. Elle est conçue de tel sorte qu'elle commute les paquets le plus rapidement possible et interconnecter les différents composants de l'infrastructure : Les modules de la couche distribution, modules de service, Data Center, Sites distants (WAN).

Hiérarchie



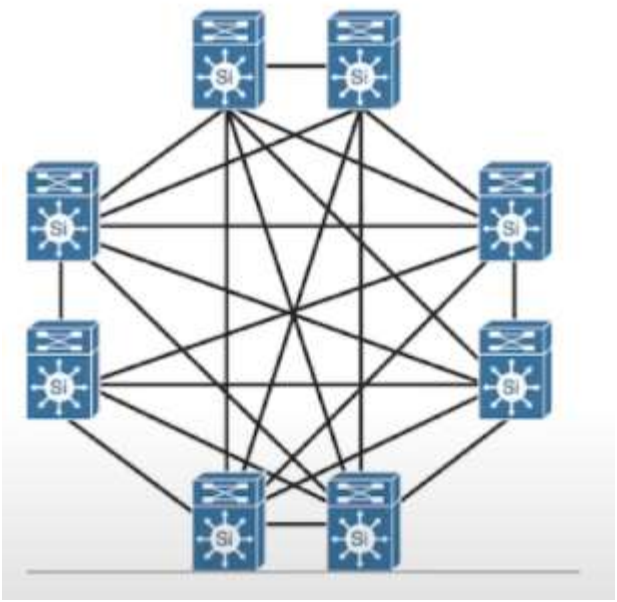
Three-Tier Network Design Model

Collapsed Core-Distribution architecture

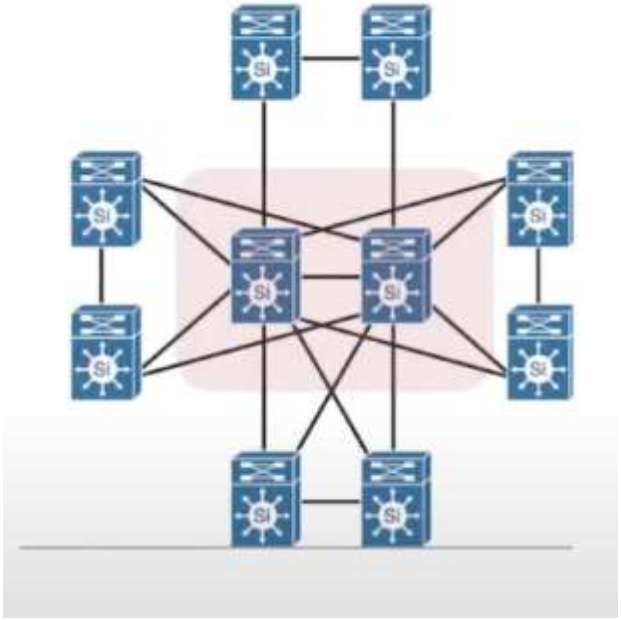


Two-Tier Network Design Model

Hiérarchie



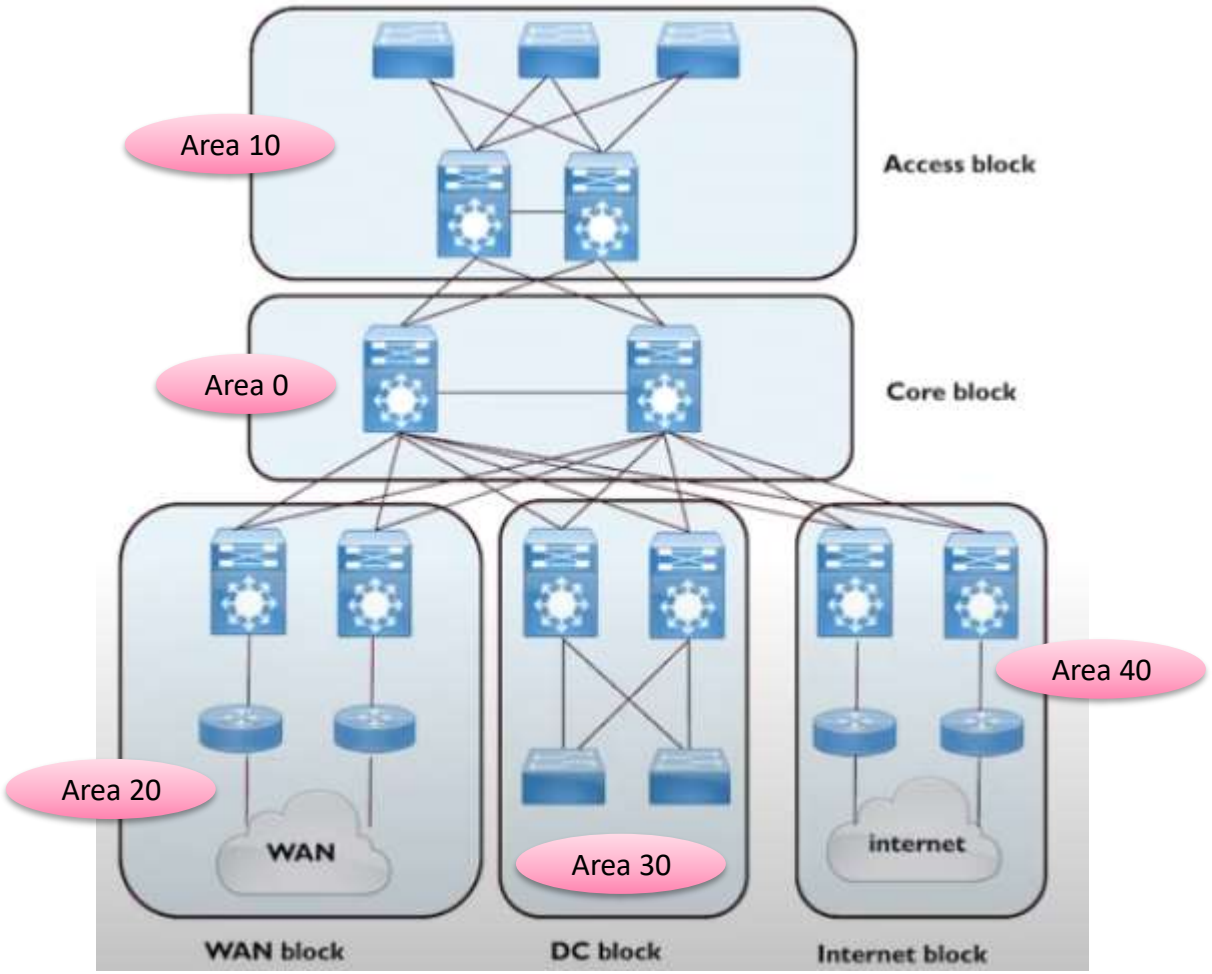
Two-Tier : Full-Mesh Distribution



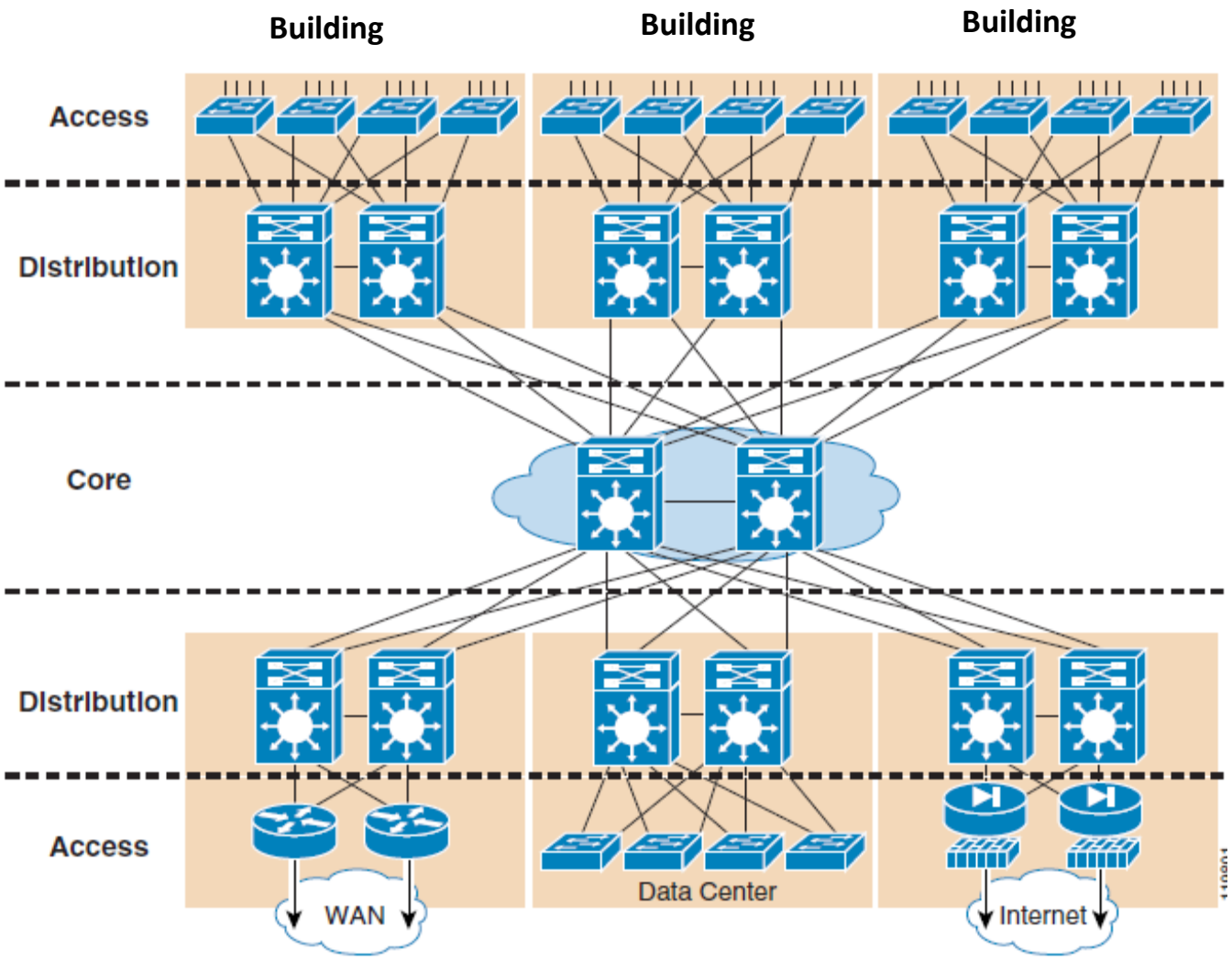
Three-Tier

Modularité

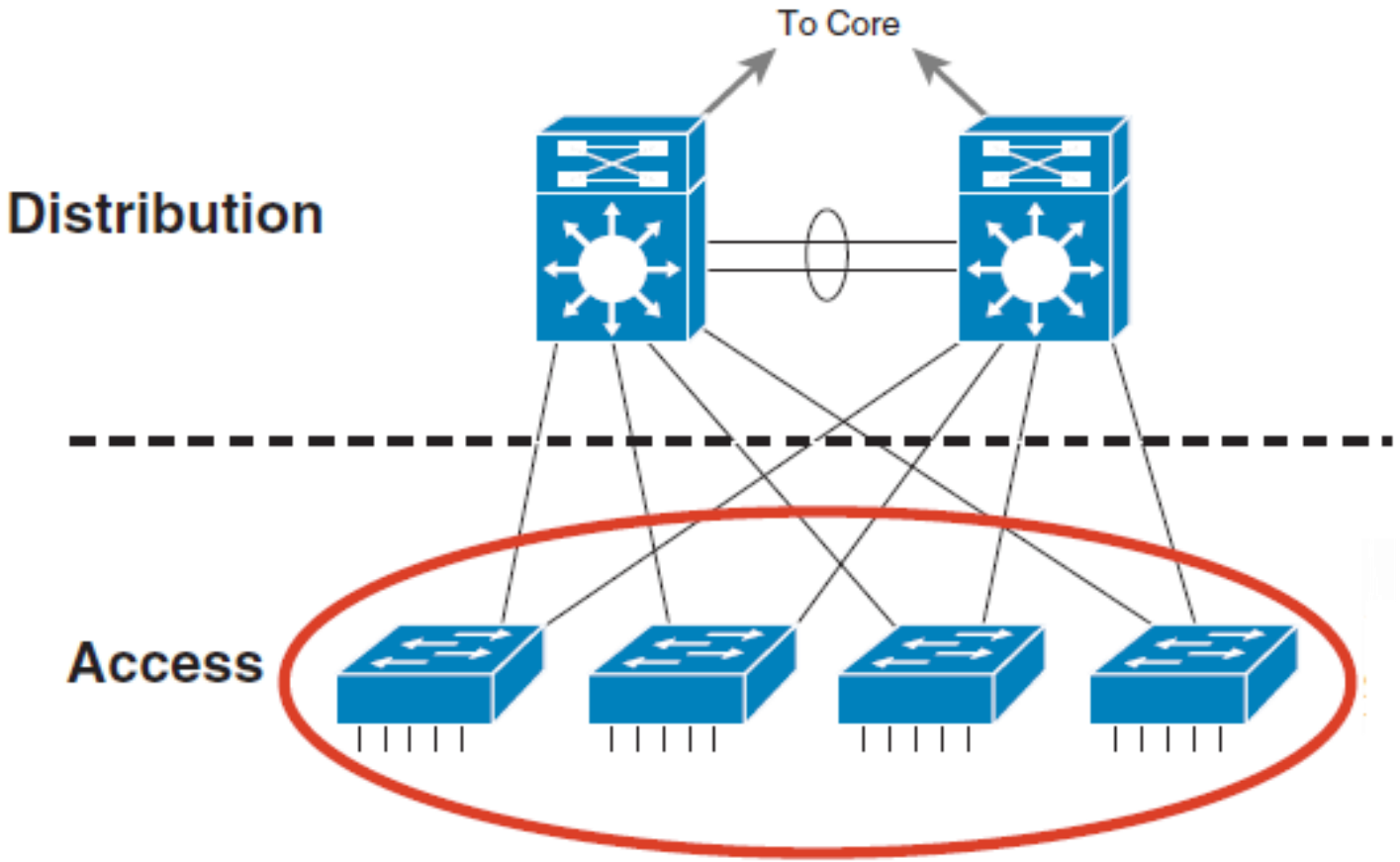
- Fault isolation
- Optimise operation
- Module replication/expansion



Modularité


Building
Building
Building
Access
Distribution
Core
Distribution
Access
WAN
Data Center
Internet

Bloc Accès-Distribution



Bloc Accès-Distribution

- **Couche Accès** : Les réseaux de campus ne peuvent, en aucun cas, perçus de manière linéaire. Au niveau accès l'étude et la conception doivent être fondées sur le principe de découpage en segment. Dans cette optique, la segmentation permet l'aboutissement à un ensemble de LAN. Le découpage en LAN peut être fonctionnelle, organisationnelle, géographique, etc… Sur le plan déploiement, les LANs sont définies sous forme de VLANs (1 Vlan = 1 Subnet).

  Data Vlans, Managment Vlan, Voice Vlans, Native Vlan, Default Vlan, Blackhole

  En général, les équipements de la couche accès, et en particuleir les switchs, doivent fournir et supporter les fonctionnalités permettant :

Le déploiement d'une infrastructure unifiée et convergente

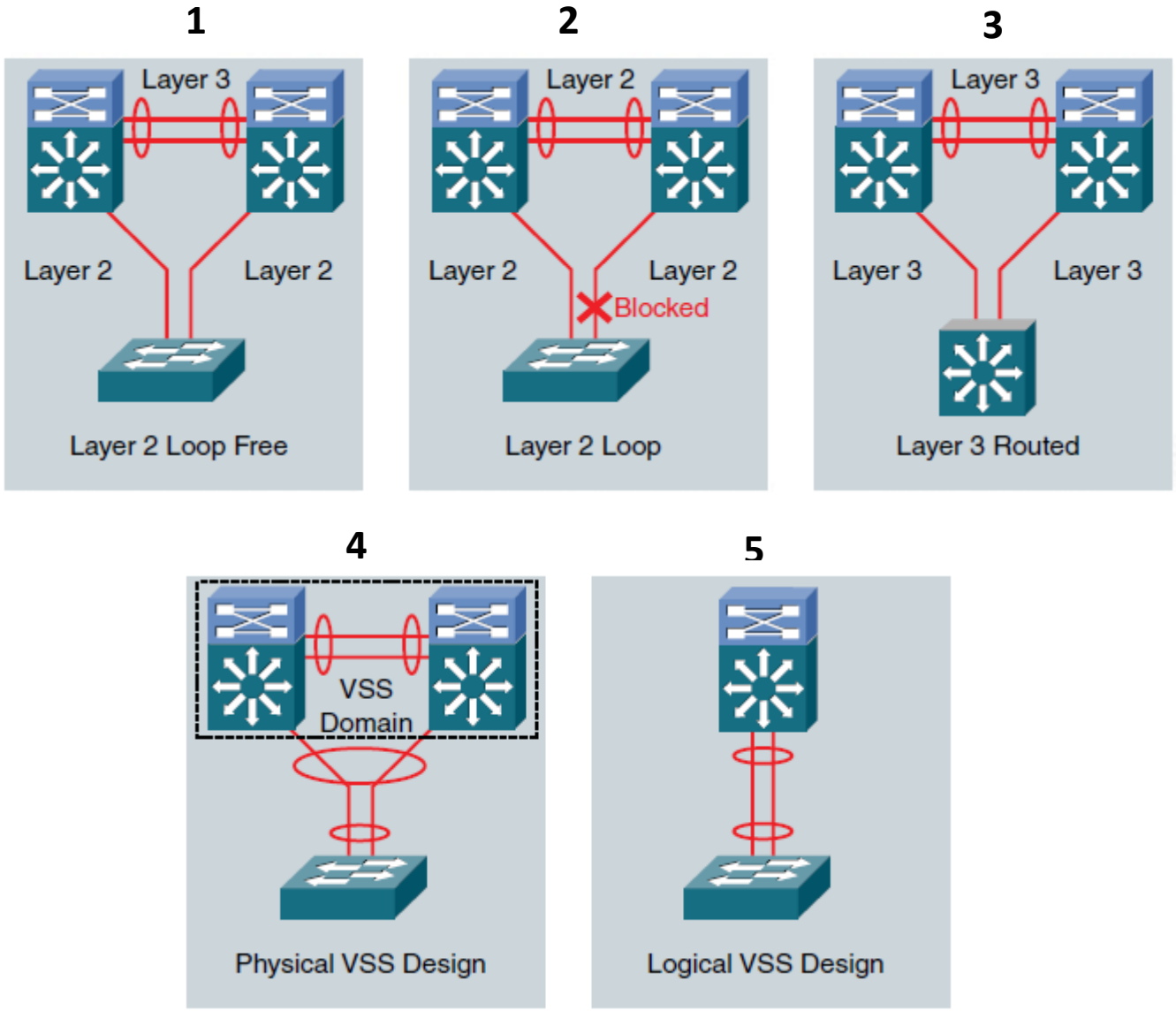
- **Fonctionnalités supportées**
  - Switching ou commutation de niveau 2 (MAC switching)
  - Convergence : Power Over Ethernet (PoE), VLAN auxiliaires (IP Phone), …
  - VLAN, Trunk, 802.1y (y=d,p,q,w,x,…), Cisco VTP, …
  - Agrégation de Lien : EtherChannel, LACP, PAgP, …
  - Haute disponibilité : STP, FHRP(HSRP, VRRP, GLBP), EtherChannel, …
  - Security : Port Security, Storm control, DHCP Snooping, ARP inspection, IP source guard, Port-Based Authentication (802.1x), Etc …
  - Mécanisme pour Quality of Service (QoS) : Classification, Marquage, …
  - Etc …

Bloc Accès-Distribution

- **Bloc Accès-Distribution** : On ne peut appréhender l'importance et la nécessité des fonctionnalités de la couche accès, sans la traiter conjointement avec la couche distribution. On peut distinguer trois modèles de conception et de déploiement du bloc Accès-Distribution :
  - Modèle Multi-Tiers : 1 et 2
  - Modèle a couche accès routé (Routed Access) : 3
  - Modèle a Switch Virtuelle (Virtual Switch : VSS, vPC) : 4 et 5

  Sur le plan topologie physique les trois modèles sont similaires, les différences peuvent être dans les éléments suivants :
  - Ou se situe la frontière entre le Niveau 2 et le Niveau 3 (Layer-2 and Layer-3)
  - Comment implémenter la topologie de redondance
  - Comment fonctionne la haute disponibilité

Bloc Accès-Distribution



- **Conception sans boucle L2 (Layer 2 Loop Free Design)** : Dans cette conception, les switchs d'accès sont L2. Les liens entre la couche accès et distribution sont L2 trunk. Le lien entre les switchs de distribution est L3.

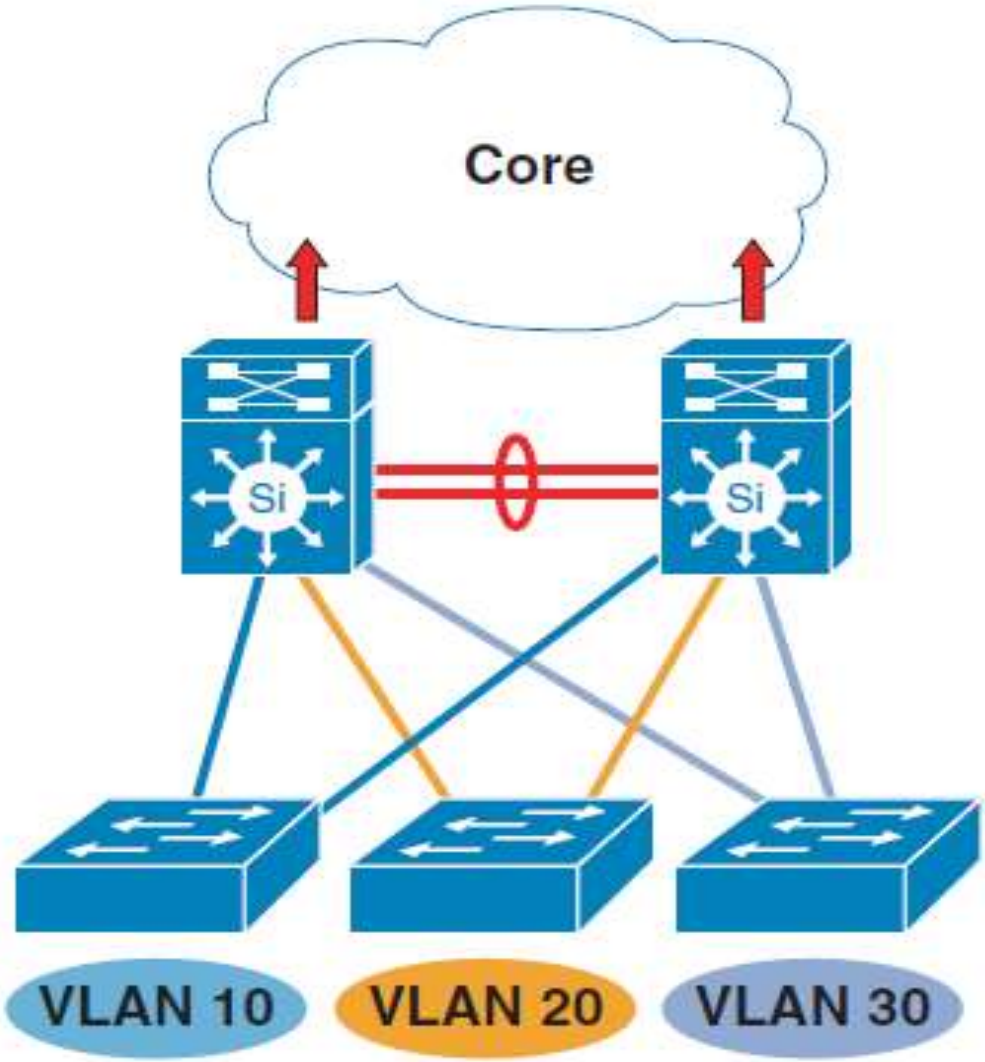
  En général les liens sont Etherchannel dont les avantages sont :

  - Accroissement de la bande passante
  - Haute disponobilité
  - Equilibrage de charge
  - Simplification de la topologie du réseau

  Ce modèle est caractérisé par l'absence de boucle L2 dans le bloc Accès-Distribution, ainsi le STP ne s'implique pas dans la convergence du réseau et l'équilibrage de charge (Load Balancing : LB). Le LB du trafic Accès Distribution peut utiliser le FHRP (First Hop Router Protocol).

  Ce modèle de conception est idéal dans le cas où chaque VLAN n'utilise qu'un seul switch. Cette conception n'est pas recommandée dans le cas ou un VLAN est étendu sur plusieurs switchs.

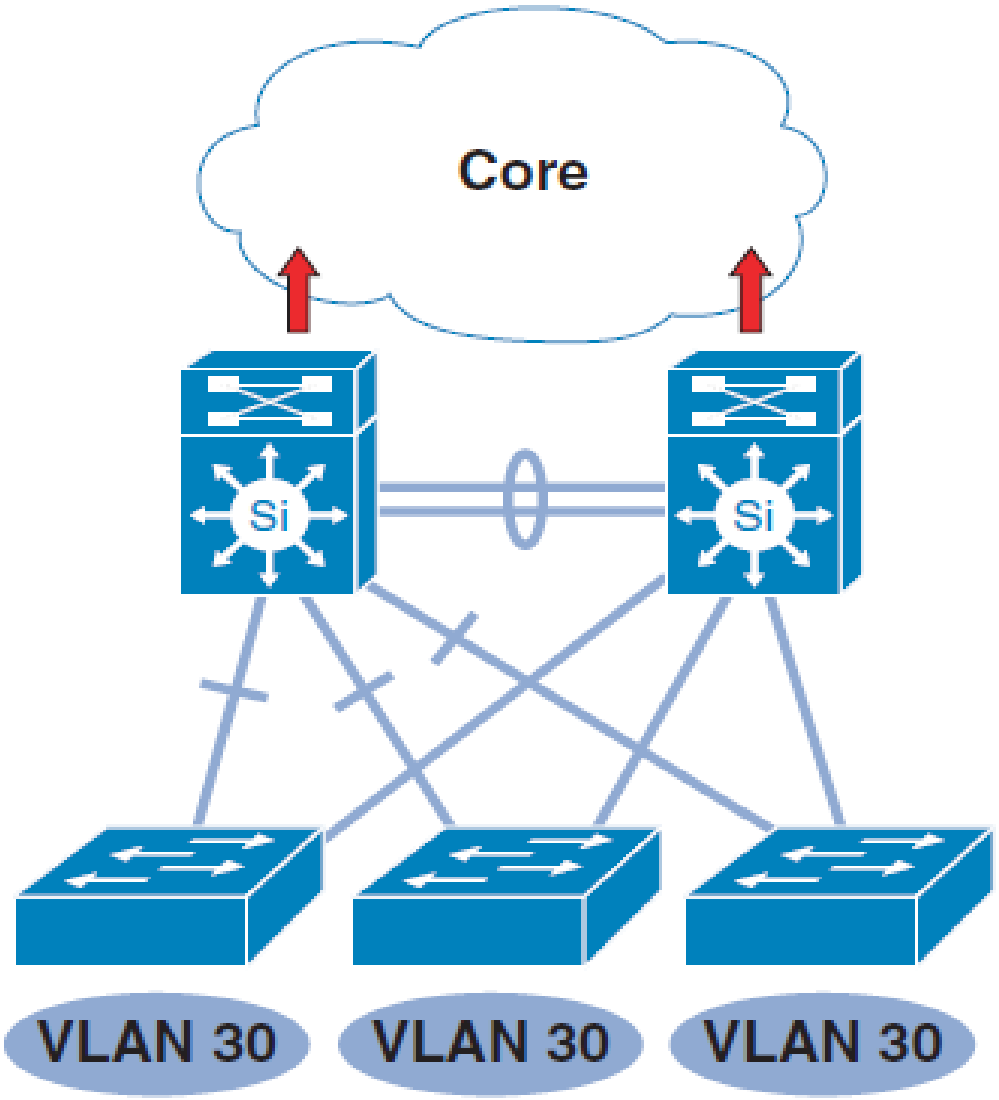
Bloc Accès-Distribution



- **Conception avec boucle L2 (Layer 2 Looped Design)** : Dans cette conception, les switchs d'accès sont L2. Les liens entre la couche accès et distribution sont L2 trunk. Le lien entre les switchs de distribution est L2 trunk. Ce modèle introduit une boucle L2 entre les switchs de distribution et ceux de l'accès. Pour éliminer la boucle, le STP bloque un lien uplink entre le switch d'accès et celui de distribution. Ce modèle de conception est recommandé dans le cas où les VLANs sont étendus sur plusieurs switchs.

  Il faut mentionner que dans le cas ou le switch d'accès est relié à un seul switch de distribution, la haute disponibilité peut être assurée par l'Etherchannel. Et dans ce cas il est inutile d'activer le STP, et les liens sources de la boucle peuvent être agrégées.

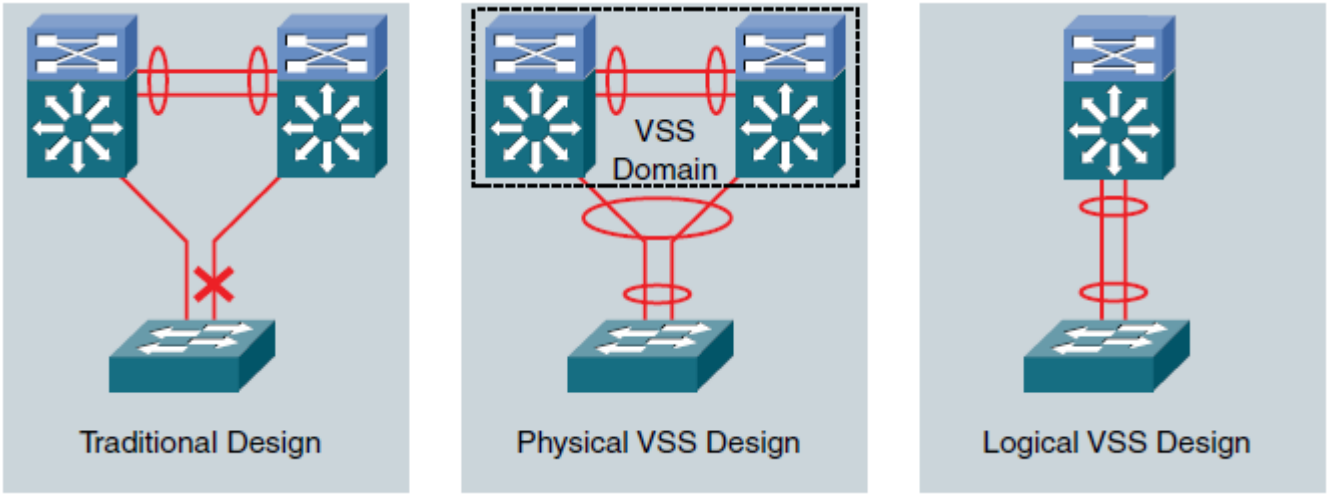
Bloc Accès-Distribution

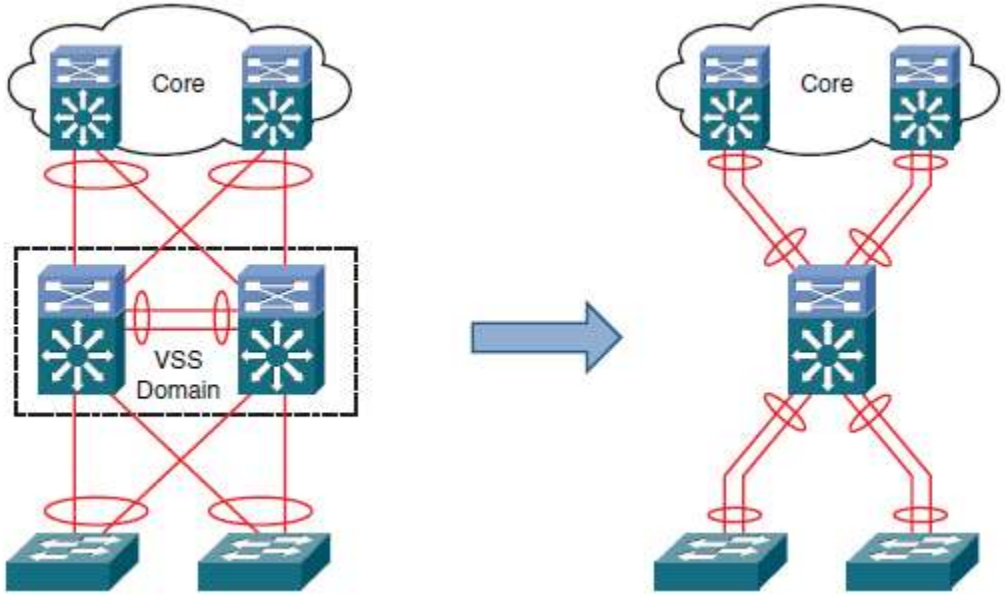


- **Conception L3 routé (Layer 3 Routed Design)** : Ce modèle de conception se base sur le routage L3 dans les switchs d'accès. Tous les liens entre les switchs sont de type L3. L'avantage majeur de cette conception est l'élimination du STP des liens inter-switchs. FHRP est aussi inutilisé, car la passerelle par défaut pour les End Devices réside dans le switch d'accès au lieu du switch de distribution. La contrainte sur les VLANs est similaire à l'approche 1.

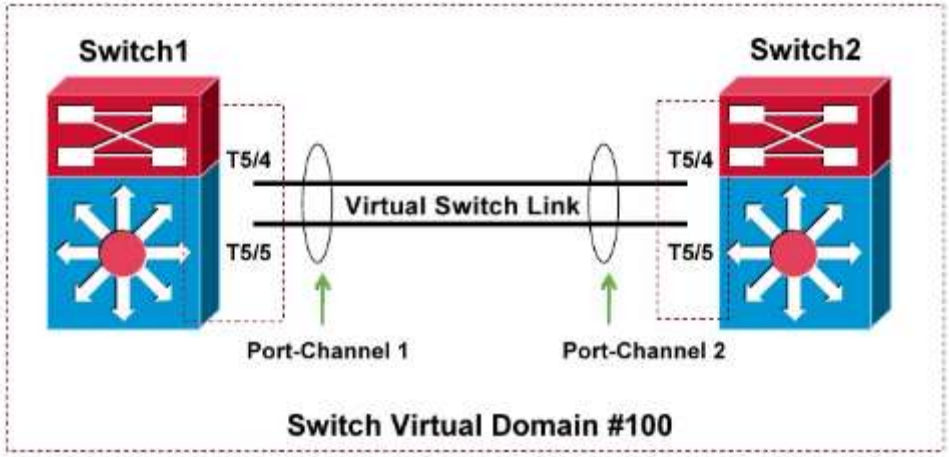
- **VSS (Virtual Switching System) :** VSS est une technologie de virtualisation réseau propriétaire de CISCO, qui combine deux switchs physique en un seule entité logique. Les deux switchs forment un seul switch virtuel, et par conséquent une seule entité a administrer. Les deux switchs sont interconnectés par un Etherchannel spécifique nommé VSL (Virtual Switch Link), qui doit contenir, au moins, deux liens 10 Gbps. De l'autre coté, le switch de la couche accès est connecté au switch VSS via un Etherchannel Multichassis MEC (Multichassis EtherChannel). Le modèle de déploiement VSS élimine le STP, FHRP, etc… Les figures qui suivent illustrent le principe du VSS et donnent un aperçu sur l'activation et la configuration des switchs.

Virtual Switching System





Virtual Switching System



Switch1

```
Router(config)#host VSS
VSS(config)#switch virtual domain 100

Domain ID 10 config will take effect only
after the exec command 'switch convert mode
virtual' is issued

VSS(config-vs-domain)#switch 1
VSS(config-vs-domain)#exit

VSS(config)#interface port-channel 1
VSS(config-if)#switch virtual link 1

VSS(config-if)#interface range tenG 5/4 - 5
VSS(config-if-range)#channel-group 1 mode on
```

Switch2

```
Router(config)#host VSS
VSS(config)#switch virtual domain 100

Domain ID 10 config will take effect only
after the exec command 'switch convert mode
virtual' is issued

VSS(config-vs-domain)#switch 2
VSS(config-vs-domain)#exit

VSS(config)#interface port-channel 2
VSS(config-if)#switch virtual link 2

VSS(config-if)#interface range tenG 5/4 - 5
VSS(config-if-range)#channel-group 2 mode on
```

Couche Accès

Switch1

```
vss#switch convert mode virtual
```

4

```
This command will convert all interface
names to naming convention "interface-type
switch-number/slot/port", save the running
config to startup-config and reload the
switch.
Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
[OK]
Saving converted configuration to bootflash:
...
Destination filename [startup-
config.converted_vs-20071031-150039]?
```

AT THIS POINT THE SWITCH WILL REBOOT

Switch2

```
vss#switch convert mode virtual

This command will convert all interface
names to naming convention "interface-type
switch-number/slot/port", save the running
config to startup-config and reload the
switch.
Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
[OK]
Saving converted configuration to bootflash:
...
Destination filename [startup-
config.converted_vs-20071031-150039]?
```

AT THIS POINT THE SWITCH WILL REBOOT

Switch1

SWITCH CONSOLE OUTPUT

```
<…snip…>
System detected Virtual Switch configuration...
 Interface TenGigabitEthernet 1/5/4 is member of
PortChannel 1
 Interface TenGigabitEthernet 1/5/5 is member of
PortChannel 1

<…snip…>
00:00:26: %PFREDUN-6-ACTIVE: Initializing as
ACTIVE processor for this switch
Initializing as Virtual Switch ACTIVE
processor

<…snip…>
00:01:19: %VSLP-5-RRP_ROLE_RESOLVED: Role
resolved as ACTIVE  by VSLP

00:01:19: %VSL-5-VSL_CNTRL_LINK:  New VSL
Control Link  5/4
```

Switch2

SWITCH CONSOLE OUTPUT

```
<…snip…>
System detected Virtual Switch configuration...
 Interface TenGigabitEthernet 2/5/4 is member
of PortChannel 2
 Interface TenGigabitEthernet 2/5/5 is member
of PortChannel 2

<…snip…>
00:00:26: %PFREDUN-6-ACTIVE: Initializing as
ACTIVE processor for this switch
Initializing as Virtual Switch STANDBY
processor

<…snip…>
00:01:02: %VSLP-5-RRP_ROLE_RESOLVED: Role
resolved as STANDBY by VSLP

00:01:02: %VSL-5-VSL_CNTRL_LINK:  New VSL
Control Link  5/4
```

Couche Accès

SWITCH CONSOLE OUTPUT — Switch1

```
<…snip…>
vss-demo# switch accept mode virtual
interface Port-channel2
 switch virtual link 2
 no shutdown
interface TenGigabitEthernet2/5/4
 channel-group 2 mode on
 no shutdown
interface TenGigabitEthernet2/5/5
 channel-group 2 mode on
 no shutdown

This command will populate the above VSL configuration
from the standby switch into the running
configuration.
The startup configuration will also be updated with
the new merged configuration if merging is successful.
Do you want to proceed? [yes/no]: yes
Merging the standby VSL configuration...

Building configuration...

00:11:33: %PFINIT-SW1_SP-5-CONFIG_SYNC: Sync'ing the
startup configuration to the standby Router. [O
```

5

SWITCH CONSOLE OUTPUT — Switch2

```
<…snip…>

Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 10-Oct-07 01:02 by chrisvan
00:02:42: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:02:42: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
vss-sdby>
Standby console disabled

vss-sdby>
```

Switch1

```
vss# sh switch virtual
Switch mode                   :
Virtual Switch
Virtual switch domain number : 10
Local switch number           : 1
Local switch operational role:
Virtual Switch Active
Peer switch number            : 2
Peer switch operational role :
Virtual Switch Standby
vss#
```

Switch2

```
vss-sdby>enable
Standby console disabled

vss-sdby>
```

Both switches are now converted with
Switch1 - VSS Active
Switch2 - VSS Hot standby

Switch 2 console is now disabled for normal console activity…