

Collection
Certifications

Préparation au 2^e module ICND1 de la certification **CCNA 200-125**

CISCO

Routage et Commutation

2^e édition

20 travaux pratiques
191 questions réponses

OFFERT :
UN EXAMEN BLANC en ligne
avec réponses commentées et détaillées



eni

Fichiers complémentaires
à télécharger



Laurent **SCHALKWIJK**

Les éléments à télécharger sont disponibles à l'adresse suivante :

<http://www.editions-eni.fr>

Saisissez la référence ENI du livre CE22M2CIS dans la zone de recherche et validez.

Cliquez sur le titre du livre puis sur le bouton de téléchargement.



Introduction

A. Objectifs de l'ouvrage	14
B. Les certifications Cisco	14
C. La formation CCNA R&S NetAcad	16
D. La certification	17
E. Les outils importants	18
F. Organisation de l'ouvrage	18
1. Guide	18
a. Principes de base du réseau (20 % des points)	18
b. Les fondamentaux de la commutation LAN (26 % des points)	19
c. Les fondements du routage (25 % des points)	20
d. Les services d'infrastructure (15 % des points)	21
e. Maintenance de l'infrastructure (14 % des points)	21
2. Organisation des chapitres	22

Chapitre 1

Les réseaux commutés

A. Conception d'un réseau local	25
1. Notions de réseaux convergents	25
2. Évolution	25
3. Hiérarchisation	26
4. Rôle des réseaux commutés	28
5. Types de commutateurs	28
B. L'environnement commuté	30
1. Mécanisme de transfert de trames	30
a. CSMA/CD	30
b. Concept général	31
c. Commutation store and forward	36
d. Commutation cut-through	37

2. Domaines de commutation	37
a. Domaines de collision	38
b. Domaines de diffusion	38
c. Facteurs d'encombrement	39
C. Validation des acquis : questions/réponses	40

Chapitre 2

Concepts et configuration de base de la commutation

A. Configuration de base d'un commutateur	45
1. Rappel sur les mémoires	45
2. Configuration d'un commutateur vierge	47
a. Informations fournies par les LED.	47
b. Connexion au commutateur	48
c. Séquence de démarrage	50
d. Sources de configuration, fichiers de configuration	52
e. Interface en ligne de commande (ILC/CLI)	53
f. Modes du commutateur	53
3. Aide	56
a. Aide contextuelle	56
b. Historique de commandes.	57
c. Aide en ligne	58
4. Configuration des paramètres globaux	60
a. Configurer l'invite de commandes	60
b. Configurer un nom d'hôte	60
c. Configurer une bannière	61
5. Configuration de l'accès de gestion à distance	63
a. Principes	63
b. Configuration de l'interface de gestion du commutateur en IPv4	64
6. Limitation de l'accès par mot de passe	67
a. Protection de l'accès via le port console	67
b. Protection de l'accès via Telnet	68
c. Protection du mode privilégié	69
d. Lisibilité des mots de passe	71
e. Combien de ports VTY ?	72
f. Synchronisation et affichage des messages	73
7. Résolution de noms	76
a. Résolution statique	78
b. Résolution dynamique	79
8. Date, heure et NTP	81

9.	Mode de récupération	85
a.	Connexion au commutateur	86
b.	Procédure de récupération des mots de passe d'un commutateur	86
10.	Configuration des ports de commutateur	87
a.	Communications bidirectionnelles simultanées (full-duplex)	87
b.	Auto-MDIX	89
c.	Vérification de la configuration des ports de commutateur	89
11.	Travaux pratiques : configuration des paramètres de base du commutateur	92
B.	Sécurité du commutateur	102
1.	Les bases du chiffrement	102
a.	Les objectifs du chiffrement	102
b.	Les algorithmes de chiffrement	102
c.	L'attaque "Man in the middle"	106
d.	Les certificats	106
2.	Le protocole SSH	108
a.	SSHv1	108
b.	SSHv2	111
c.	Mise en œuvre de SSH	114
3.	Problèmes de sécurité dans les LAN	121
a.	L'inondation d'adresses MAC (MAC Address Flooding)	121
b.	L'usurpation de DHCP	122
c.	Reconnaissance via CDP	122
d.	Reconnaissance via LLDP	125
e.	Les attaques Telnet	127
f.	Attaque de mot de passe par force brute	127
4.	Pratiques de sécurité	128
5.	Mise en place de la sécurité des ports	128
a.	Désactivation des ports inutilisés	128
b.	Surveillance DHCPv4 (DHCPv4 snooping)	129
c.	Fonctionnement de port-security	131
d.	Limitation des attaques Telnet/SSH	134
C.	Travaux pratiques : configuration et sécurisation d'un commutateur dans un réseau local	135
D.	Travaux pratiques : découverte d'un réseau avec CDP	143
E.	Validation des acquis : questions/réponses	146

Chapitre 3	Les VLAN
A. Vue d'ensemble des VLAN	153
1. Définition	153
2. Les types de VLAN	155
a. VLAN de données	155
b. VLAN voix	156
c. VLAN de gestion	158
3. Agrégation de VLAN (trunk)	158
a. Contrôle des domaines de diffusion à l'aide de réseaux locaux virtuels ..	160
b. Étiquetage IEEE 802.1q	161
B. Implémentation de VLAN	162
1. Création d'un VLAN	162
2. Affectation de ports à des VLAN	163
3. Configuration des liaisons trunk	167
4. Le protocole DTP	169
5. Travaux pratiques : configuration d'agrégation (trunk) et de VLAN (version 1) ..	171
6. Dépannage des VLAN et des trunks	178
a. Problème d'adresse IP sur le VLAN	178
b. Problèmes de VLAN manquants	178
c. Problèmes de trunks	179
C. Sécurité des VLAN	180
1. Attaques de VLAN	180
a. Attaque par usurpation de commutateur	180
b. Attaque par saut de VLAN (double tagging)	181
2. Périphérie PVLAN	182
3. Bonnes pratiques	183
D. Travaux pratiques : configuration d'agrégation (trunk) et de VLAN (version 2) ...	183
E. Validation des acquis : questions/réponses	190
Chapitre 4	Les bases des routeurs
A. Configuration initiale d'un routeur	198
1. Fonctions d'un routeur	198
2. Connecter le routeur à son environnement	200
a. Informations fournies par les LED	200
b. Connexion au routeur	201
c. L'interface en ligne de commande (ILC/CLI)	203
d. Les modes du routeur	203

e. L'aide	205
3. Le routeur, un ordinateur spécialisé	206
a. Architecture d'un ordinateur	206
b. Le processus de démarrage d'un ordinateur	206
c. Architecture d'un routeur.	207
d. Le processus de démarrage d'un routeur.	210
e. Le registre de configuration	212
f. Sources de configuration, fichiers de configuration	215
g. Gestion des IOS, des fichiers de configuration et des licences	216
4. Les interfaces	220
a. Les interfaces LAN.	221
b. Les interfaces WAN	222
c. Les interfaces de configuration	228
5. Mécanismes de transfert des paquets	228
a. La commutation de base	228
b. La commutation rapide	229
c. Cisco Express Forwarding (CEF).	229
6. Configuration des paramètres globaux	230
a. Configurer l'invite de commandes	230
b. Configurer un nom d'hôte	230
c. Configurer une bannière	230
7. Configuration de l'accès à distance de gestion IPv4	231
a. Configuration de l'interface LAN du routeur en IPv4	232
b. Vérification des paramètres d'interface IPv4	236
c. Configuration d'une interface de bouclage IPv4	241
8. Configuration de l'accès à distance de gestion IPv6	242
a. Configuration de l'interface LAN du routeur en IPv6	242
b. Vérification des paramètres d'interface IPv6	245
9. Limitation de l'accès par mot de passe	247
a. Protection du mode privilégié	248
b. Protection de l'accès via le port console	248
c. Protection de l'accès via le port auxiliaire.	248
d. Protection de l'accès via Telnet	249
e. Lisibilité des mots de passe.	249
f. Synchronisation et affichage des messages	249
10. Résolution de noms	249
11. Date, heure et NTP	249
12. Filtrage des résultats de commande show.	249

B. CIDR et VLSM	251
1. Adressage par classe	251
2. Utilisation de CIDR et de VLSM	252
C. Travaux pratiques : configuration des paramètres de base du routeur en ligne de commande	253
D. Travaux pratiques : récupération de mot de passe	258
E. Travaux pratiques : sauvegarde et restauration d'un IOS	260
F. Validation des acquis : questions/réponses	262

Chapitre 5

Routage statique

A. Décision de routage IPv4	269
1. Commutation des paquets IPv4 entre les réseaux	269
2. Routage statique en IPv4	272
a. Pourquoi utiliser le routage statique ?	272
b. Quand utiliser les routes statiques ?	272
c. Configuration des routes statiques IPv4	273
d. La commande ip route	276
3. La table de routage IPv4	278
a. Structure de la table de routage	278
b. Hiérarchisation de la table de routage	279
c. Recherche d'une route dans la table de routage	280
4. Types de routes statiques	281
a. Route statique standard	281
b. Route statique par défaut ou de dernier recours	283
c. Route statique résumée	284
d. Route statique flottante	285
e. Route vers un hôte	286
5. Vérification et dépannage de route statique IPv4	287
6. La détermination du meilleur chemin	287
a. Le nombre de sauts ou la bande passante	290
b. Équilibrage de charge	291
c. Les distances administratives	292
7. Analyse de la table de routage en IPv4	292
a. La table de routage en IPv4	292
b. Les réseaux IPv4 directement connectés et les réseaux distants	293

B. Décision de routage IPv6	295
1. Commutation des paquets en IPv6 entre les réseaux	295
2. Les routes statiques et par défaut en IPv6.	297
3. Vérification et dépannage de route statique IPv6	300
4. Analyse de la table de routage en IPv6	300
a. La table de routage en IPv6	300
b. Configuration des interfaces IPv6 directement connectées.	300
C. Travaux pratiques : configuration de routes statiques IPv4	302
D. Travaux pratiques : configuration de routes statiques IPv6	310
E. Validation des acquis : questions/réponses	318

Chapitre 6**Routage inter-VLAN**

A. Configuration initiale d'un routage inter-VLAN	325
1. Fonctionnement du routage inter-VLAN	325
2. Le routage inter-VLAN existant.	325
a. Principe du routage inter-VLAN existant.	325
b. Configuration du routage inter-VLAN existant	325
3. Routage inter-VLAN avec la méthode router-on-a-stick	330
a. Principe du routage inter-VLAN router-on-a-stick.	330
b. Configuration du routage inter-VLAN router-on-a-stick	330
B. Dépannage du routage inter-VLAN	333
1. Problèmes de configuration liés au commutateur	333
a. Configuration des ports d'accès.	333
b. Configuration des ports trunk	335
2. Problèmes de configuration liés au routeur et au client	336
C. Commutation de couche 3	336
1. Routage inter-VLAN avec des commutateurs multicouches (L3)	336
a. Principe du routage inter-VLAN avec des commutateurs multicouches	336
b. Configuration du routage inter-VLAN avec des commutateurs multicouches	338
c. Routage inter-VLAN au moyen de ports routés	342
d. Configuration de routes statiques sur un commutateur de couche 3	344
e. Configuration d'un Catalyst 2960 comme commutateur L3 basique	344
2. Dépannage de la commutation de couche 3	345
D. Travaux pratiques : mise en œuvre d'un routage inter-VLAN	346
E. Validation des acquis : questions/réponses	359

Chapitre 7**Routage dynamique**

A. Protocoles de routage dynamique	367
1. Évolution des protocoles de routage dynamique	367
2. Fonctionnement des protocoles de routage dynamique	367
B. Comparaison entre les routages statique et dynamique	369
C. Types de protocoles de routage dynamique	370
1. Classification des protocoles de routage	370
a. Protocoles de routage IGP et EGP	370
b. Protocoles de routage à vecteur de distance	371
c. Protocoles de routage à état de liens	372
d. Protocoles de routage par classe	372
e. Protocoles de routage sans classe	373
2. Caractéristiques des protocoles de routage	374
3. Métriques du protocole de routage	374
D. Routage dynamique à vecteur de distance	375
1. Fonctionnement des protocoles de routage à vecteur de distance	375
a. Les mises à jour	375
b. Problème de bouclage	377
2. Caractéristiques des protocoles de routage IPv4	379
E. Routage RIP et RIPng	380
1. Fonctionnement du protocole RIP	380
2. Configuration du protocole RIP	380
a. Configuration RIPv1	381
b. Annonce des réseaux	383
c. Examen des paramètres RIP par défaut	384
d. Configuration des interfaces passives	388
e. Configuration RIPv2	388
f. Récapitulation automatique et réseaux discontinus	392
g. Propagation d'une route par défaut	394
3. Travaux pratiques : mise en œuvre du protocole de routage RIPv2	395
4. Configuration du protocole RIPng	402
a. Annonce des réseaux IPv6	403
b. Configuration des interfaces passives	409
c. Propagation d'une route par défaut	409
5. Travaux pratiques : mise en œuvre du protocole de routage RIPng	410
F. Validation des acquis : questions/réponses	417

Chapitre 8**Listes de contrôle d'accès**

A. Les listes de contrôle d'accès IPv4	427
1. Objectif des listes de contrôle d'accès	427
a. Qu'est-ce qu'une liste de contrôle d'accès (ACL) ?	427
b. Filtrage des paquets	428
c. Fonctionnement des listes de contrôle d'accès	428
2. Comparaison entre ACL IPv4 standards et étendues	429
a. Fonctionnement des ACL IPv4 standards	429
b. Méthodes recommandées pour les ACL	430
3. Les ACL IPv4 standards	431
a. Les ACL IPv4 standards numérotées	431
b. Modification des ACL IPv4 standards numérotées	435
c. Les ACL IPv4 standards nommées	438
d. Modification des ACL IPv4 standards nommées	438
4. Sécurisation des ports VTY à l'aide d'une ACL IPv4	439
a. Configuration d'une ACL standard pour sécuriser un port VTY	439
b. Vérification d'ACL standard utilisée pour sécuriser un port VTY	442
5. Travaux pratiques : mise en œuvre d'ACL IPv4 standards	443
6. Les ACL IPv4 étendues	451
a. Les ACL IPv4 étendues numérotées	451
b. Les ACL IPv4 étendues nommées	454
c. Modification des ACL IPv4 étendues	455
d. Application d'ACL étendues aux interfaces	456
7. Travaux pratiques : mise en œuvre d'ACL étendues en IPv4	456
B. Les listes de contrôle d'accès IPv6	465
1. Type de listes de contrôle d'accès IPv6	465
2. Comparaison des ACL IPv4 et IPv6	465
3. Configuration des ACL IPv6	466
4. Modification des ACL IPv6	468
5. Travaux pratiques : mise en œuvre d'ACL IPv6	469
C. Validation des acquis : questions/réponses	478

Chapitre 9**DHCP (Dynamic Host Configuration Protocol)**

A. Le protocole DHCPv4	485
1. Présentation de DHCPv4	485
2. Fonctionnement de DHCPv4	486
a. Découverte des serveurs DHCP (DHCPDISCOVER)	486
b. Proposition d'adresse IP des serveurs DHCP (DHCPOFFER)	487
c. Demande de réservation du client DHCP (DHCPREQUEST)	488
d. Confirmation de réservation du serveur au client DHCP (DHCPACK)	488
e. Le renouvellement du bail DHCP	489
3. Format du message DHCPv4	490
4. Les messages DHCPv4	491
5. Configuration de base de DHCPv4	493
a. Configuration de base du routeur	494
b. Configuration des interfaces du routeur	494
c. Vérification de l'état des interfaces du routeur	495
d. Configuration de DHCPv4 sur un routeur	495
e. Vérification de DHCPv4	496
f. Relais DHCPv4	498
6. Configuration d'un routeur en tant que client DHCPv4	500
7. Dépannage de DHCPv4	501
a. Tâches de dépannage	501
b. Débogage de DHCPv4	502
8. Travaux pratiques : mise en œuvre de DHCPv4	503
B. Le protocole DHCPv6	507
1. Configuration automatique des adresses sans état (SLAAC)	507
2. Fonctionnement des SLAAC	507
3. SLAAC et DHCPv6	510
a. Option SLAAC	511
b. Option DHCPv6 sans état	511
c. Option DHCPv6 avec état	512
4. Fonctionnement du DHCPv6	513
a. Routeur en tant que serveur DHCPv6 sans état	515
b. Routeur en tant que serveur DHCPv6 avec état	517
c. Routeur en tant qu'agent de relais DHCPv6	519
5. Dépannage de DHCPv6	520
C. Validation des acquis : questions/réponses	522

Chapitre 10**Traduction d'adresse réseau pour IP (NAT)**

A. Fonctionnement de la NAT	529
1. Caractéristiques de la NAT	529
a. Espace d'adressage privé IPv4	530
b. NAT, terminologie et principe	530
2. Types de NAT	532
a. NAT statique	532
b. NAT dynamique	532
c. Traduction d'adresses de port (PAT)	533
3. Avantages et inconvénients de la NAT	534
a. Les avantages	534
b. Les inconvénients	534
B. Configuration de la NAT	535
1. La NAT statique	535
a. Configuration de la NAT statique	535
b. Vérification de la NAT statique	536
2. La NAT dynamique	537
a. Configuration de la NAT dynamique	537
b. Vérification de la NAT dynamique	538
3. La PAT	542
a. Configuration de la PAT : pool d'adresses	542
b. Configuration de la PAT : adresse unique	544
c. Vérification de la PAT	544
4. Redirection de port	546
a. Principe de la redirection de port	546
b. Configuration de la redirection de port	546
c. Vérification de la redirection de port	547
5. NAT et IPv6	548
a. NAT pour IPv6 ?	548
b. Adresse unique locale IPv6	548
c. NAT64	549
C. Travaux pratiques : mise en œuvre de la NAT et de la PAT	550
D. Validation des acquis : questions/réponses	555

Chapitre 11

Intégration des compétences

A. Travaux pratiques : intégration des compétences (version 1).560
B. Travaux pratiques : intégration des compétences (version 2).580

Tableau des objectifs609
Index613



Chapitre 3

A. Vue d'ensemble des VLAN	153
B. Implémentation de VLAN	162
C. Sécurité des VLAN	180
D. Travaux pratiques : configuration d'agrégation (trunk) et de VLAN (version 2) . . .	183
E. Validation des acquis : questions/réponses	190

Prérequis

Le modèle OSI et notamment le rôle de la couche liaison de données et de la couche réseau sont à connaître, ainsi que la notion de trame, de protocole Ethernet et de protocole IP. Toutes ces notions sont abordées dans le livre "Cisco - Notions de base sur les réseaux" dans la collection Certifications aux Éditions ENI.

Les chapitres précédents sont également des prérequis.

Objectifs

À la fin de ce chapitre, vous serez en mesure de :

- Expliquer la notion de VLAN et de trunk (agrégation).
- Expliquer les meilleures pratiques et leurs conceptions.
- Mettre en place des VLAN et des trunk.
- Expliquer les types d'attaques et les méthodes de contre-mesures.
- Dépanner les problèmes de VLAN et de trunk.
- Dépanner les problèmes de configuration de base des VLAN.

Au regard du cahier des charges de la certification ICND1, vous serez capable de :

- Reconnaître le but et les fonctionnalités de divers périphériques réseau (compétence transversale).
- Sélectionner les composants requis pour rencontrer une spécification réseau donnée (compétence transversale).
- Identifier les applications courantes et leurs impacts sur le réseau (compétence transversale).
- Prédire le flux de données entre deux hôtes à travers le réseau (compétence transversale).
- Dépanner et corriger les problèmes communs associés à l'adressage IP et à la configuration des hôtes (compétence transversale).
- Configurer et vérifier les VLAN.
- Configurer et vérifier l'agrégation des commutateurs Cisco, ce qui inclut :
 - le protocole DTP ;
 - l'auto-négociation.
- Assigner des ports non utilisés dans un VLAN non utilisé.
- Placer le VLAN natif dans un autre VLAN que le VLAN 1.
- Dépanner et résoudre les problèmes d'agrégation (trunk) sur un commutateur Cisco.
 - vérifier l'état d'une agrégation ;
 - vérifier l'encapsulation d'une agrégation ;
 - vérifier et corriger l'appartenance d'un VLAN à une agrégation (*VLAN allowed*).

A. Vue d'ensemble des VLAN

En IPv4, les réseaux locaux sont sensibles aux diffusions, en effet lors d'une diffusion (*broadcast*) toutes les machines du réseau (ou du sous-réseau) reçoivent l'information diffusée, même si cette information ne les concerne pas ! Seuls les routeurs bloquent le trafic de diffusion.

Réduire la taille d'un domaine de diffusion en découpant celui-ci en sous-domaines permet de réduire le nombre de périphériques impactés par la diffusion et d'augmenter les performances du réseau.

Les routeurs sont des appareils spécialisés dans le routage et le transfert de données à longue distance (pour les réseaux WAN) et leurs circuits intégrés gérant la commutation ne sont pas aussi performants que ceux des commutateurs. De plus, les routeurs ne disposent pas de suffisamment de cartes réseau pour autoriser le nombre de subdivisions nécessaires dans un réseau moderne.

L'accès au LAN est généralement géré par un commutateur d'accès L2 (couche 2) qui placera le périphérique dans le réseau virtuel (VLAN) adéquat.

Même si les VLAN sont principalement utilisés dans des réseaux locaux commutés, ils sont de plus en plus employés dans les réseaux étendus (WAN).

1. Définition

Les VLAN sont des regroupements logiques de périphériques au sein d'un même réseau physique, ils sont identifiés par un numéro. Un groupe de périphériques dans un VLAN communiquent comme s'ils étaient reliés au même câble. Des appareils partageant une même connexion physique, mais isolés logiquement dans des VLAN différents, se comporteront comme s'ils étaient sur des réseaux indépendants.

Les diffusions (*broadcast*) sont communiquées uniquement à des périphériques d'un même VLAN et les paquets destinés aux stations n'appartenant pas à ce VLAN doivent être transférés par un routeur (ou un appareil ayant des capacités de routage).

Un VLAN crée un domaine de diffusion logique qui peut s'étendre sur plusieurs segments de réseau local physique.

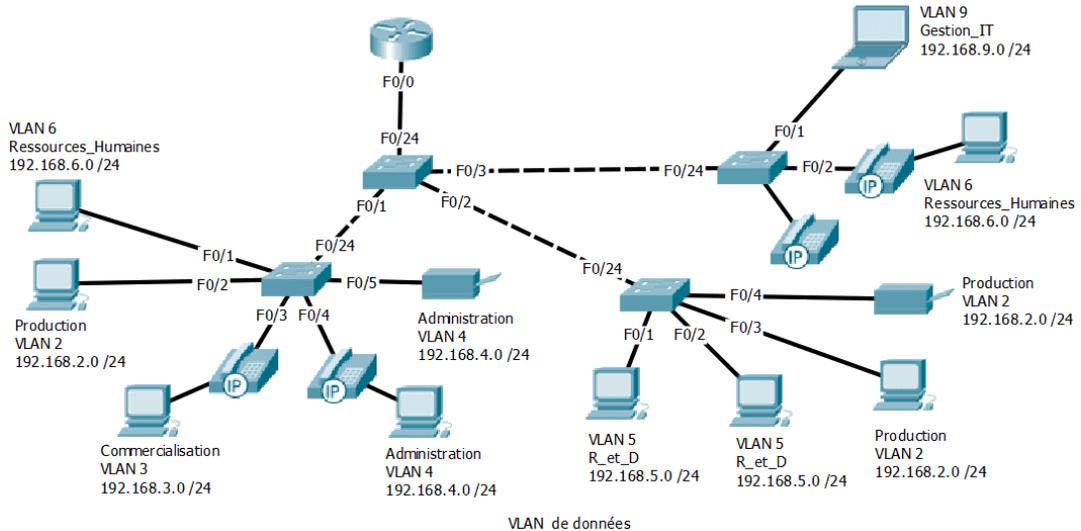
☞ *Un VLAN est donc indépendant de sa structure physique et il permet de séparer logiquement des périphériques appartenant à un même réseau physique.*

Les avantages des VLAN sont les suivants :

- Sécurité (confidentialité) : il est possible de séparer logiquement les trames et ainsi de les acheminer uniquement aux destinataires voulus. Chaque port en mode accès d'un commutateur peut être attribué à un seul VLAN (à l'exception des ports connectés à un téléphone IP, à un autre commutateur ou à un point d'accès Wi-Fi). Dans le cas particulier des téléphones IP, le port appartient à deux VLAN.
- Réduction des coûts : l'utilisation d'un réseau convergé où les données informatiques, la téléphonie, la vidéo et les flux vidéo partagent un même média, réduit fortement les coûts d'infrastructure.
- Meilleures performances : la subdivision du réseau en sous-réseaux logiques permet de diminuer les diffusions au sein d'un domaine et diminue également l'impact lors d'incident comme une tempête de diffusion (*broadcast storm*).

- Gestion accrue : la mise en place de VLAN peut sembler dans un premier temps complexe mais en réalité elle simplifie la gestion du service informatique en regroupant les périphériques non pas en fonction de leur localisation mais plutôt en fonction de critères de fonctionnalité, de type de trafic (*class*), de besoins ou de sécurité. Étant donné que les VLAN peuvent être nommés (sauf le VLAN 1), ils sont plus facilement identifiables. Il est possible également de définir des politiques de sécurité et des accès différents par VLAN.

☞ Une tempête de diffusion se produit lorsque toute la bande passante disponible est consommée en raison du nombre trop élevé de trames de diffusion prises dans une boucle de couche 2 et provoque une panne du réseau.



Exemple de VLAN dans un réseau local.

Chaque VLAN d'un réseau commuté correspond à un sous-réseau IP. L'adressage réseau appliqué aux segments réseau ou aux VLAN doit être réfléchi, cohérent. Il faut donc prendre en compte l'ensemble du réseau afin de clarifier et simplifier au maximum celui-ci !

La méthode d'implémentation des VLAN qui sera abordée est basée sur le port ou réseau local virtuel d'accès (*Access VLAN*).

2. Les types de VLAN

VLAN par défaut : le VLAN par défaut est le VLAN 1. Tous les ports deviennent membres du VLAN par défaut après le démarrage initial du commutateur. Le VLAN 1 ne peut pas être renommé ni supprimé.

```
Switch# show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active
```

Tous les ports physiques du commutateur sont dans le VLAN 1 qui est le VLAN par défaut.

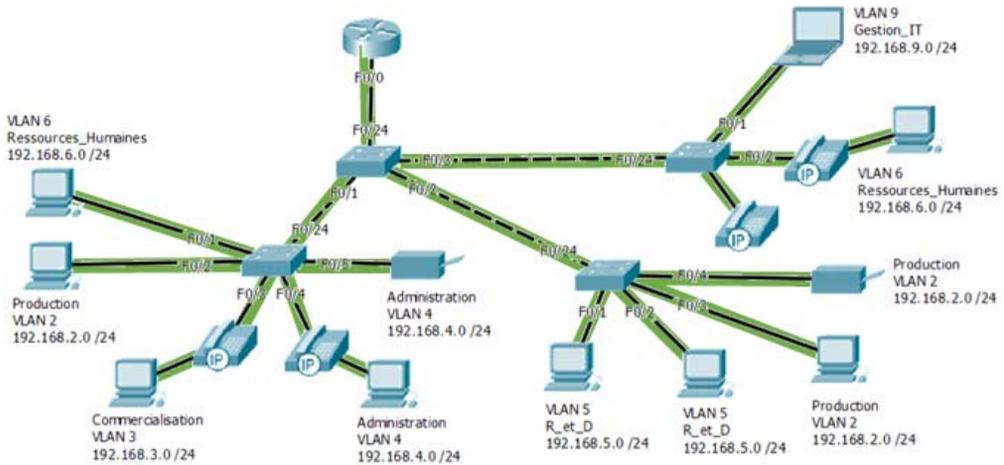
☞ Par défaut, le trafic de contrôle de couche 2, tel que le trafic des protocoles CDP et STP, est associé au VLAN 1. Pour des raisons de sécurité, il est conseillé de choisir un autre VLAN que le VLAN 1 en tant que VLAN par défaut ou en tant que VLAN natif.

- VLAN natif : un VLAN natif est défini sur un port d'agrégation 802.1Q (*trunk*) afin de déterminer à quel VLAN appartient le trafic non étiqueté. Un port d'agrégation est un port par lequel peuvent passer plusieurs VLAN. Le VLAN natif par défaut est le VLAN 1.
- VLAN natif non étiqueté : il n'y a pas de modification de la trame. C'est le comportement standard d'un commutateur Cisco. Il est parfois nécessaire de recourir à cette technique lorsqu'il faut faire passer le trafic d'un protocole qui vérifie l'intégrité de ses trames.
- VLAN natif étiqueté : même le VLAN natif est marqué par une étiquette. Cette technique de plus en plus courante permet de se prémunir des attaques utilisant un double étiquetage (*double tagging attack*), le but de ces attaques étant de provoquer un saut de VLAN.

☞ Le protocole STP (*Spanning Tree Protocol*) garantit l'unicité du chemin logique entre toutes les destinations sur le réseau en procédant intentionnellement au blocage des chemins redondants susceptibles d'entraîner la formation d'une boucle.

a. VLAN de données

Les VLAN de données ne transportent que le trafic généré par l'utilisateur. Il est d'usage de séparer le trafic de voix et de gestion du trafic de données car ils ne nécessitent pas le même traitement.

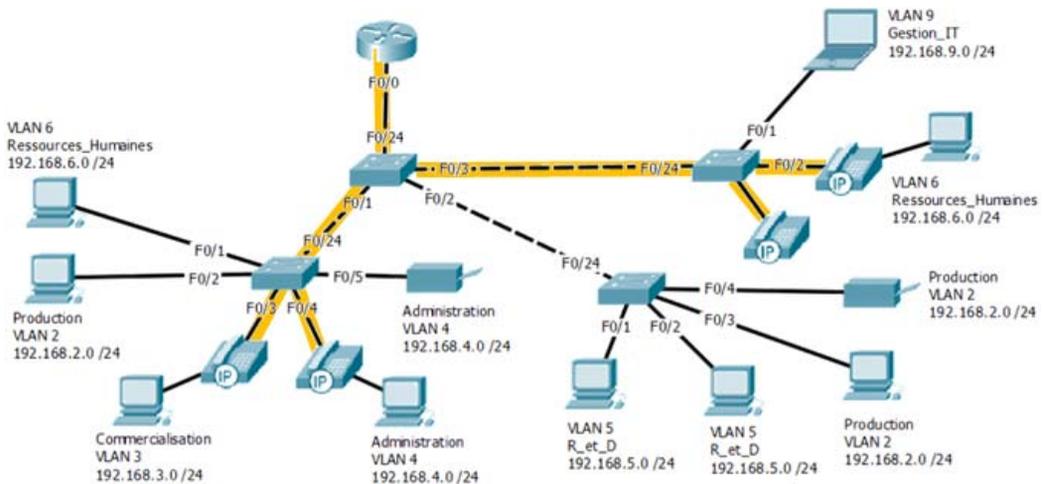


VLAN de données.

b. VLAN voix

Un VLAN spécifique est nécessaire pour prendre en charge la voix sur IP (VoIP) dont le trafic est très sensible. Ce VLAN a comme caractéristiques :

- Une bande passante consolidée pour garantir la qualité de la voix. Ce qui implique de prioriser le trafic en donnant une priorité absolue à ce VLAN.
- Un délai inférieur à 150 ms sur l'ensemble du réseau. Qu'il soit local, intersite ou VPN.



VLAN voix.