



SERVICES CULTURE ÉDITIONS
RESSOURCES POUR
L'ÉDUCATION NATIONALE

**Ce document a été numérisé par le CRDP de Montpellier pour la
Base Nationale des Sujets d'Examens de l'enseignement professionnel**

Ce fichier numérique ne peut être reproduit, représenté, adapté ou traduit sans autorisation.

BACCALAURÉAT PROFESSIONNEL
MICRO-INFORMATIQUE ET RÉSEAUX :
INSTALLATION ET MAINTENANCE

ÉPREUVE E2

Épreuve de technologie

Analyse fonctionnelle et structurelle d'un réseau ou
d'un système de communication

Ce dossier comprend 35 pages numérotées de 1/35 à 35/35, dont :

Page de garde : Page 1/35
Barème : Page 2/35
Sujet : Pages 3 à 17/35
Annexes : Pages 18 à 35/35

Vous devrez répondre directement sur les documents du dossier sujet dans les espaces prévus.

Vous devrez rendre l'intégralité du dossier à l'issue de l'épreuve.

Vous ne devrez pas noter vos noms ou prénoms sur ce dossier.

Vous devrez rendre ce dossier dans une copie d'examen anonyme que vous complèterez.

CODE ÉPREUVE :		EXAMEN : BCP	SPÉCIALITÉ : MICRO INFORMATIQUE ET RÉSEAUX : INSTALLATION ET MAINTENANCE	
SESSION 2011	SUJET	ÉPREUVE : E2 Analyse fonctionnelle et structurelle d'un réseau ou d'un système de communication		Calculatrice autorisée
Durée : 4 HEURES		Coefficient : 3	Code sujet : 01-E2MRIM-10	Page : 1/35

BARÈME

<u>Partie A</u> : Étude de certaines fonctions du réseau de l'UTC :	/ 16
<u>Partie B</u> : Étude des commutateurs Cisco 3750G-24TS :	/ 20
<u>Partie C</u> : Étude à partir du commutateur 6509 :	/ 17
<u>Partie D</u> : Étude des VLAN :	/ 25
<u>Partie E</u> : Étude du routage et du filtrage :	/ 22
TOTAL :	/ 100

PRÉSENTATION

L'Université de Technologie de Compiègne est une école d'ingénieur française qui délivre un enseignement de niveau Bac +5 (ingénieur) à Bac +8 (école doctorale).

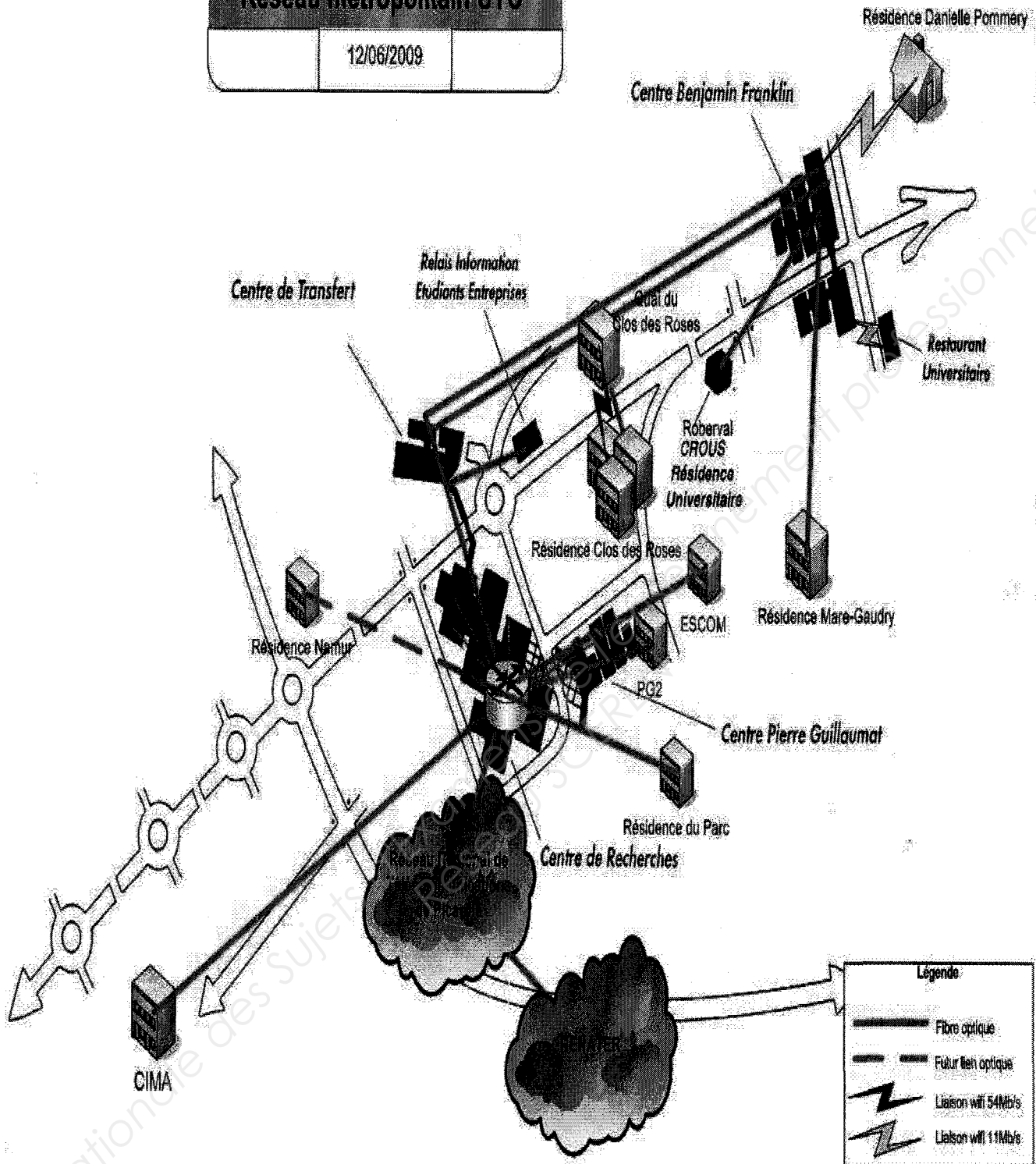
- Génie Biologique
- Génie des procédés (anciennement Génie chimique)
- Génie informatique
- Génie mécanique
- Génie des systèmes mécaniques
- Génie des systèmes urbains

L'UTC en chiffres

<u>Étudiants</u> : Étudiants : 4200 Ingénieurs : 3600 Masters : 300 Doctorants : 300 Diplômés : plus de 15 000 Diplômés (/an) : 650	<u>Formation</u> : Masters spécialisés : 2 Formations d'ingénieurs : 6 Spécialités de Master : 9 Unités de valeurs : 400 Stagiaires en entreprise (/an) : 1500
<u>Recherche</u> : Spécialités de doctorat en Sciences et Technologies : 6 Laboratoires : 10 Thèmes de recherche : 9 Pôles de compétitivité : 2 (i-Trans, Agro-ressources)	<u>International</u> : Double-diplômes (Asie, Europe, Amériques) : 9 Campus à l'étranger : 2 (Chine et Chili) Universités partenaires à l'étranger : 140 Diplômés à l'étranger : 15 % Étudiants étrangers : 15 %
<u>Personnel</u> : Personnels administratifs et techniques : 300 Personnels enseignants et enseignants-chercheurs : 350	<u>Divers</u> : Associations étudiantes : 60 Durée moyenne de recherche d'emploi : 1,3 mois Surface locaux : 65 000 m ² sur 3 sites

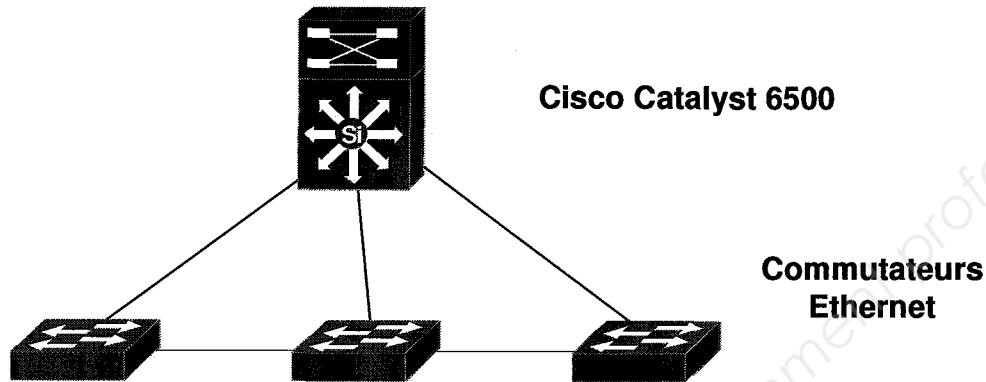
Réseau métropolitain UTC

12/06/2009



Organisation principale du réseau de l'UTC

- Les serveurs les plus importants sont connectés directement sur l'équipement central ou sur des commutateurs Ethernet dédiés en salle informatique.
- Les postes clients se connectent sur les commutateurs Ethernet.
- Le réseau UTC est entièrement Ethernet, à des débits de 100 et 1000 Mb/s (1 Gb/s).
- La majeure partie du réseau est constituée de commutateurs Ethernet reliés entre eux par des liaisons fibres 1 Gb/s.



Le réseau UTC comporte 200 switches :

Voici quelques exemples de commutateurs :

C6500,

Cisco 2924C-XL,

série Cisco 2950,

série Cisco 2960,

série Cisco 3550,

série Cisco 3560,

Cisco 3750G-24TS : switchs en cluster et Cisco CBS3120G-S

Partie A : Étude de certaines fonctions du réseau de l'UTC

Question A.1 : Traduire les acronymes et expliquer le rôle des fonctions suivantes :

DHCP :

DNS :

Question A.2 : Expliquer le rôle des fonctions suivantes :

Gateway (dans la configuration d'un ordinateur) :

Proxy :

Question A.3 : Exemple d'adresses utilisées dans le réseau de l'UTC :

Nom	ID	Adresses IP	Rôle
VLAN_SI	3	172.22.0.0 à 172.22.255.255 193.51.117.0 à 193.51.117.255 195.81.155.0 à 195.81.155.255	Centre de Recherches - Bat A /B

L'exemple précédent fait apparaître des adresses publiques et privées dans le réseau de l'UTC. Expliquer la différence entre ces deux types d'adresses.

Question A.4 : Donner les trois plages d'adresses privées
(adresse de début-adresse de fin).

Question A.5 : Quel intérêt cela présente-t-il de connaître la classe d'une adresse IP ?

Question A.6 : La plage d'adresses suivante est réservée à l'ESCOM (Ecole Supérieure de Chimie)

Nom	ID	Adresses IP	Rôle
ESCOM	43	172.27.192.0 à 172.27.207.255	ESCOM

Déterminer le nombre **d'adresses machines** disponibles dans cette plage.
Énoncer vos calculs.

Question A.7 : Le réseau de l'UTC utilise des adresses IPV4 et IPV6.
Donner le format de chacune de ces versions.

Partie B : Étude des commutateurs Cisco 3750G-24TS

Question B.1 : Énoncer le nom et le numéro de la couche du modèle OSI, lorsque cet appareil est utilisé en tant que commutateur simple.

Question B.2 : Les commutateurs ont remplacé les vieux HUB dans le réseau de l'UTC. Énoncer « le problème » de communication que les commutateurs ont supprimé.

Question B.3 : À l'aide de la documentation constructeur (**annexe 1**), énoncer le nombre et le débit des ports du commutateur **3750G-24TS**.

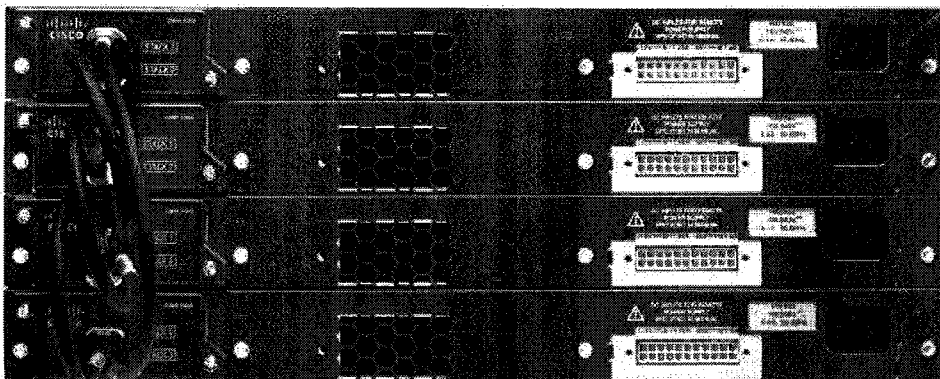
Question B.4 : Le commutateur **3750G-24TS** possède des ports Gigabit Ethernet pour Fibre Optique.

Ces ports sont utilisés notamment pour **relier les commutateurs entre eux**.

À l'aide de la documentation constructeur (annexes 1 et 1 bis), proposer les dénominations et les références d'un module enfichable et d'une jarretière optique pour un débit de 1 Gb/s et une longueur d'onde de 850 nm :

Empilement :

Comme le montre la figure suivante, les commutateurs sont empilables (stack).



Question B.5 : Donner l'avantage de l'empilement par rapport au chaînage de commutateurs :

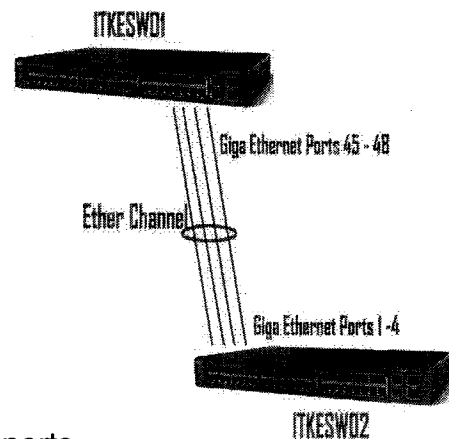
Question B.6 : À l'aide de la documentation constructeur du commutateur étudié, déterminer le nombre maximum de commutateurs par pile.

Question B.7 : Donner le débit du « moteur de commutation ».

Question B.8 : Dans une même baie, **cinq** commutateurs sont placés les uns au-dessus des autres. On désire créer un empilement de l'ensemble de ceux-ci.
Donner le nombre et la référence des câbles nécessaires. Choisir les plus adaptés.

Certains commutateurs sont reliés entre eux par des groupements de ports. On appelle cette technique l'agrégation de liens.

Ce mécanisme est appelé **Etherchannel** chez CISCO ou trunk chez d'autres constructeurs.



Question B.9 : Citer deux avantages du groupement de ports.

Question B.10 : À l'aide du document **annexe 2**, donner la norme correspondant au mécanisme **Etherchannel**.

Question B.11 : Les commutateurs sont reliés au cœur du réseau mais aussi entre eux. Citer le protocole qui détecte et traite les boucles dans le réseau.

Base Nationale des Sujets d'Examens de l'enseignement professionnel
Réseau SCEREN

Partie C : Étude à partir du commutateur 6509
Documentation annexe 3

Question C.1 : Décrire les caractéristiques du commutateur 6509 :

Préciser les 2 principales fonctions réalisées.

Préciser le nombre maximal et les caractéristiques des ports **LAN cuivre**.

Question C.2 : Les routeurs CISCO sont équipés de différents types de mémoires.
Pour chaque type, compléter le tableau suivant :

	Lecture	Ecriture	Signification	Contenu
ROM				
NVRAM				
FLASH				
RAM				

Question C.3 : Donner les protocoles WAN gérés par le commutateur 6509 lorsqu'il est équipé du module FlexWAN :

Question C.4 : Afin de prévoir les dimensions de la baie d'accueil, déterminer en cm la hauteur minimale du système Cisco 6509. (Consulter la documentation du commutateur 6509).
On rappelle que l'unité 1U= 1,72 pouces.

Question C.5 : Il est nécessaire de dimensionner l'alimentation du 6509.

Pour un système 6509 constitué comme suit :

- 1 châssis ventilé,
- 2 cartes superviseur,
- 4 modules 48 ports Ethernet,
- 1 module 16 ports GBic multimode fiber.

À l'aide de la documentation sur le commutateur 6500 (annexe 3) :

Déterminer la puissance de l'alimentation nécessaire à ce système.

Question C.6 : Donner la référence de l'alimentation à placer dans notre système.

Question C.7 : Le châssis 6509 peut accueillir deux blocs d'alimentation. En vous aidant de l'annexe 3, donner deux avantages qu'offre cette possibilité.

Partie D : Étude des VLAN.

Le réseau UTC est constitué d'une cinquantaine de VLAN. En voici quelques exemples :

Nom	ID	Adresses IP	Rôle
VLAN_SI	3	172.22.0.0 à 172.22.255.255 193.51.117.0 à 193.51.117.255 195.81.155.0 à 195.81.155.255	Centre de Recherches - Bat A /B
VLAN_ETU	7	172.26.0.0 à 172.26.255.255	Réseau Etudiant Filaire et Hertzien
VLAN_HZ_PERS	17	172.27.128.0 à 172.27.143.255	Réseau Hertzien Personnel UTC
VLAN_VOICE	22	172.28.0.0 à 172.28.255.255	Téléphonie IP
ESCOM	43	172.27.192.0 à 172.27.207.255	ESCOM

Question D.1 : Donner le nombre d'adresses machines disponibles pour les étudiants.

Préciser votre calcul :

Question D.2 : Donner la signification de l'acronyme VLAN et le rôle de celui-ci :

Question D.3 : Énoncer les différents types de VLAN réalisables sur les commutateurs habituels.

Question D.4 : L'introduction des réseaux logiques a limité le trafic des informations.
Comment appelle-t-on ce domaine où tous les postes peuvent communiquer ?

Question D.5 : Il est possible de transmettre des données de différents VLAN sur un même lien.
Donner le nom utilisé pour désigner ce type de lien et le protocole correspondant à ce type de communication :

Question D.6 : À l'aide de l'annexe 4, donner le numéro du port qui utilise ce type de Communication.

Question D.7 : Donner la commande permettant de paramétrer ce port.

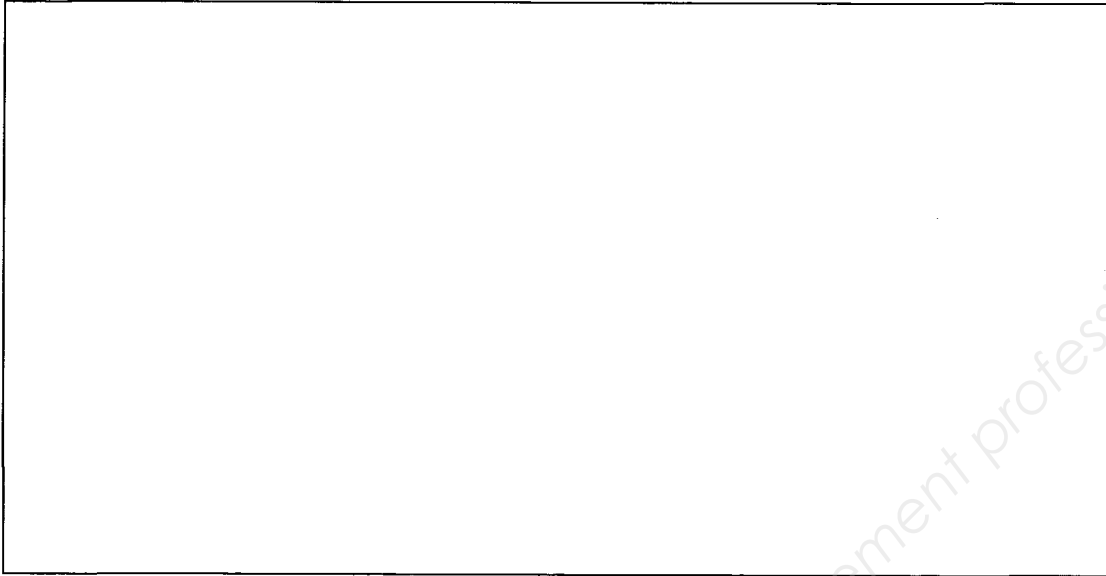
Question D.8 : Ce mode de communication introduit une modification du format de la trame Ethernet. Préciser cette modification.

Dans le réseau de l'UTC les VLAN sont gérés comme le décrit la présentation suivante :

- Les commutateurs Cisco utilisés à l'UTC disposent d'une fonctionnalité très importante : **l'affectation de VLAN par adresse MAC** (Adresse physique de la carte Réseau d'un équipement).
- Au lieu d'indiquer de manière figée dans la configuration des équipements l'affectation des VLAN, le commutateur interroge un serveur qui donne pour une adresse MAC le VLAN à utiliser.
- Le protocole utilisé entre le commutateur et le serveur d'authentification se nomme **VMPS (VLAN Management Policy Server)** (norme propriétaire Cisco).
- Ce système est par exemple utilisé dans le cas des connexions des étudiants et du personnel : pour pouvoir se connecter, il faut avoir **une adresse MAC référencée** sur le serveur.

Question D.9 : Un étudiant connecte un ordinateur portable sur le réseau de l'UTC.

À l'aide de l'annexe 5, décrire en quatre étapes le processus d'affectation au VLAN concerné.



Question D10 : Est-il possible d'utiliser ce système avec un commutateur d'une autre marque que Cisco (HP, 3Com,...) ? Justifier votre réponse.




Partie E : Étude du routage et du filtrage


Le trafic réseau entre les VLAN et l'extérieur de l'UTC, est routé et filtré par deux cartes du système « 6509 » central.

- Carte de routage (Sup-720) :
 - Filtrage peu sophistiqué (adresses IP / ports) et peu souple
 - Travail au niveau des paquets (pas de suivi de connexion automatique)
 - Très rapide (plusieurs dizaines de Gb/s)
- Carte firewall (FWSM) :
 - Filtrage très sophistiqué (filtrage applicatif, filtrage URL)
 - Travail au niveau des sessions (suivi de connexion automatique)
 - Débit max : environ 5 Gb/s, suivi d'1 million de connexions simultanées
 - Carte à rajouter dans le châssis (n'est pas incluse d'office)

Question E.1 : Énoncer le rôle du Pare-Feu dans un réseau et préciser si cette fonction peut jouer le rôle d'Anti-Virus.



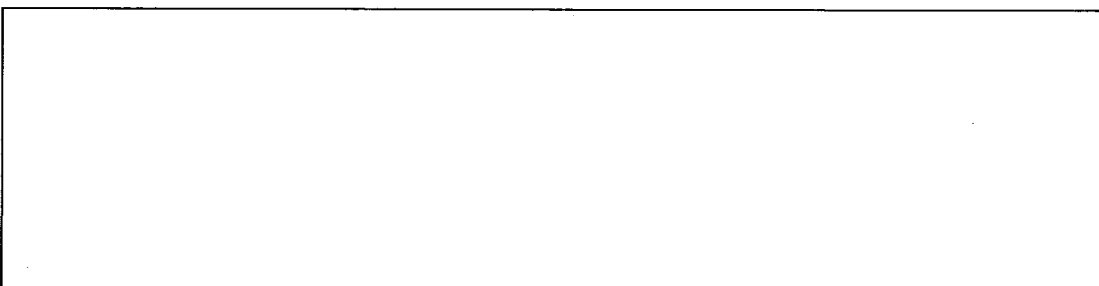
Question E.2 : Dans un réseau LAN Ethernet, préciser quand la fonction routage est nécessaire.



Question E.3 : Énoncer le nom de l'élément d'information analysé par un routeur.



Question E.4 : En vous aidant de l'annexe 6, énoncer les deux types de liste d'accès (ACL) sur les routeurs de la marque CISCO. Préciser la différence entre ces deux types d'ACL.



Question E.5 : Dans une ACL, préciser l'action de la dernière règle (implicite).

Question E.6 : Commenter le filtrage effectué en sortie du routeur par l'ACL suivante :
permit 172.26.0.0 0.0.255.255

Question E.7 : Commenter le filtrage effectué par l'ACL suivante :
ip access-list extended ext-vers-utc
permit tcp any gt 1023 host 195.81.155.22 eq 443

Question E.8 : En fonction des deux exemples suivants, qui réalisent la même fonction, préciser sur quelle carte il est **préférable** d'effectuer du filtrage. Justifier votre choix.

Autorisation de sortie de trafic FTP pour la machine d'adresse IP 195.81.155.55

• Sur carte Sup-720 :

```
ip access-list extended utc-vers-ext
permit tcp host 195.81.155.55 any eq 20
permit tcp host 195.81.155.55 any eq 21
```

```
ip access-list extended ext-vers-utc
permit tcp any eq 20 host 195.81.155.55 gt 1023 established
permit tcp any eq 21 host 195.81.155.55 gt 1023 established
```

• Sur carte FWSM :

```
access-list FR-OUTSIDE-ACL extended
permit tcp host 195.81.155.55 any eq ftp
```

Question E.9 : On désire bloquer l'accès à un certain nombre de sites Web. Sur quelle carte doit-on effectuer le filtrage ? Justifier votre réponse.

Annexe 1

Extrait de la documentation des Commutateurs 3750



Fiche Produit

Commutateurs Cisco Catalyst 3750

La gamme Cisco® Catalyst® 3750 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWise™, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité, vu comme un simple commutateur virtuel.

Figure 1. Commutateurs d'accès Cisco Catalyst 3750 10/100 et 10/100/1000

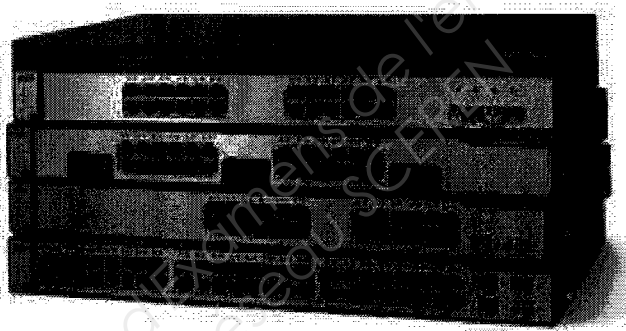
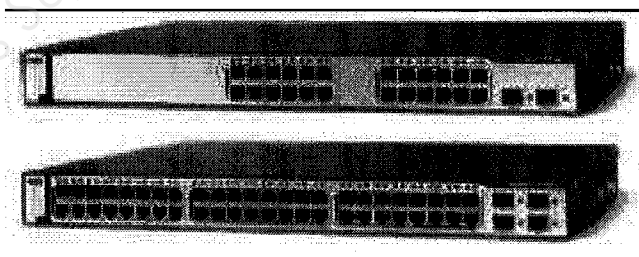


Figure 2. Commutateurs Cisco Catalyst 3750 de 24 et 48 ports 10/100 avec PoE IEEE 802.3af



CONFIGURATIONS

Le tableau 1 montre les configurations des commutateurs de la gamme Cisco Catalyst 3750.

Tableau 1. Modèles de commutateur Cisco Catalyst 3750

Modèle	Description
Cisco Catalyst 3750-24TS	24 ports Ethernet 10/100 et 2 ports Gigabit Ethernet SFP
Cisco Catalyst 3750-48TS	48 ports Ethernet 10/100 et 2 ports Gigabit Ethernet SFP
Cisco Catalyst 3750-24PS	24 ports Ethernet 10/100 PoE et 2 ports Gigabit Ethernet SFP
Cisco Catalyst 3750-48PS	48 ports Ethernet 10/100 PoE et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3575G-24T	24 ports Ethernet 10/100/1000
Cisco Catalyst 3750G-24TS	24 ports Ethernet 10/100/1000 et 4 ports Gigabit Ethernet SFP ; 1,5U
Cisco Catalyst 3750G-24TS-1U	24 ports Ethernet 10/100/1000 et 4 ports Gigabit Ethernet SFP ; 1U
Cisco Catalyst 3750G-48TS	48 ports Ethernet 10/100/1000 et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-16TD	16 ports Ethernet 10/100/1000 et 1 port 10GE Xenpak
Cisco Catalyst 3560G-48PS	48 ports Ethernet 10/100/1000 PoE et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-24PS	24 ports Ethernet 10/100/1000 PoE et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-48PS	48 ports Ethernet 10/100/1000 PoE et 4 ports Gigabit Ethernet SFP
Cisco Catalyst 3750-24FS	24 ports Ethernet 100BASE-FX et 2 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-12S	12 ports Gigabit Ethernet SFP
Cisco Catalyst 3750G-24WS	24 ports Ethernet 10/100/1000 PoE et 2 ports Gigabit Ethernet SFP ; Contrôleur WLAN intégré ; 2U

Technologie Cisco StackWise - un nouveau standard pour la résilience de pile de commutateurs

La technologie Cisco StackWise est une architecture d'empilement de commutateurs optimisée pour les réseaux Gigabit Ethernet. Elle a été conçue pour favoriser les ajouts, les suppressions et le redéploiement de commutateurs dans une pile tout en maintenant des performances constantes en son sein. La technologie Cisco StackWise assemble jusqu'à neuf commutateurs individuels dans une simple unité logique, en utilisant des câbles spécifiques d'empilement et un logiciel de gestion intelligente de la pile. Tous les commutateurs de la gamme Cisco Catalyst 3750 et de la nouvelle gamme Catalyst 3750-E sont empilables ensemble dans une même pile. Une pile fonctionne comme une unité de commutation unique gérée par un commutateur maître, élu parmi les commutateurs membres de la pile. Le commutateur maître crée et met à jour automatiquement toutes les tables de commutation et de routage. Une pile en fonctionnement peut accepter de nouveaux membres ou supprimer des membres existants sans interruption de service.

FONCTIONNALITÉS PRINCIPALES ET AVANTAGES

Facilité d'utilisation : Configuration « Plug-and-Play »

Une pile en fonctionnement se gère et se configure automatiquement. Lors de l'ajout ou de la suppression de commutateurs, le commutateur maître charge automatiquement dans le nouveau commutateur la version logicielle Cisco IOS® utilisé par la pile, charge les paramètres de configuration globale, et met à jour toute les tables de routage pour prendre en compte les changements. Les mises à jour sont appliquées simultanément à tous les commutateurs de la pile.

La gamme Cisco Catalyst 3750 permet d'empiler jusqu'à 9 commutateurs comme seule unité logique pour un total de 468 ports Ethernet 10/100, 10/100/1000, PoE ou non, ou 9 ports 10 Gigabit Ethernet. Les commutateurs 10/100, 10/100/1000, et 10 Gigabit Ethernet peuvent être regroupés au sein d'une même pile dans toutes les combinaisons possible pour évoluer avec les besoins du réseau.

Gestion simplifiée – Plusieurs commutateurs, une seule adresse IP d'administration

Chaque pile de la gamme Cisco Catalyst 3750 est gérée en tant qu'objet unique avec une seule adresse IP. La gestion IP unique est supportée pour les activités telles que la détection de défaillances, la création et la modification de réseaux locaux virtuels (VLAN), la sécurité, et la QoS.

SPÉCIFICATIONS TECHNIQUES

Le tableau suivant décrit les fonctionnalités de la gamme Cisco Catalyst 3750 et leurs bénéfices.

Fonctionnalité	Bénéfices
Empilement évolutif	<ul style="list-style-type: none">• La technologie Cisco StackWise crée une interconnexion des commutateurs à 32 Gb/s au sein d'une pile. Jusqu'à 9 commutateurs peuvent être empilés ensemble pour un maximum de 468 ports 10/100, 468 ports 10/100/1000, 108 ports Gigabit Ethernet fibre, 9 ports 10 Gigabit Ethernet, ou un mixte de ces ports. Des combinaisons de ports supplémentaires peuvent être créées en empilant ensemble des commutateurs des gammes Cisco Catalyst 3750 et 3750-E.

Le tableau suivant indique les spécifications matérielles des commutateurs Cisco Catalyst 3750.

Tableau 1. Spécifications matérielles

Description	Spécifications
Performances	<ul style="list-style-type: none">• Matrice de commutation de 32 Gbps• 38,7 Mpps de taux de transfert à travers la pile (paquets de 64 octets)• Taux de transfert (paquets de 64 octets) :<ul style="list-style-type: none">- 38,7 Mpps (Catalyst 3750G-24TS, 3750G-24TS-1U, 3750G-48TS, 3750G-24PS, 3750G-48PS, 3750G-24WS)- 35,7 Mpps (Catalyst 3750G-24T, 3750G-16TD)- 17,8 Mpps (Catalyst 3750G-12S)- 13,1 Mpps (Catalyst 3750-48TS, 3750-48PS)- 6,5 Mpps (Catalyst 3750-24TS, 3750-24PS, 3750-24FS)• 128 Mo de DRAM

	<ul style="list-style-type: none"> • Mémoire Flash : <ul style="list-style-type: none"> - 32 Mo (Catalyst 3750G-48TS-1U, 3750G-48TS, 3750G-24PS, 3750G-48PS, 3750G-24WS et 3750-24FS) - 16 Mo (Catalyst 3750-24TS, 3750-48TS, 3750-24PS, 3750-48PS, 3750G-24T, 3750G-24TS, 3750G-24WS, 3750G-12S, 3750G-16TD) • 12 000 adresses MAC configurables • 20 000 routes unicast configurables pour le Catalyst 3750G-12S et 11 000 routes pour tous les autres modèles. • 1 000 groupes IGMP et routes multicast configurables • MTU (Maximum Transmission Unit) configurable jusqu'à 9000 octets, avec une longueur maximale de la trame Ethernet de 9018 octets (trames Jumbo) pour la commutation niveau 2 sur les ports Gigabit Ethernet, et jusqu'à 1546 octets pour la commutation de trames labellisées avec le protocole MPLS (Multiprotocol Label Switching) sur les ports Fast Ethernet
Connecteurs et câblage	<ul style="list-style-type: none"> • Ports 10BASE-T : connecteurs RJ-45, câblage UTP (paire torsadée non blindée) catégorie 3, 4, ou 5 de deux paires • Ports 10BASE-T PoE : connecteurs RJ-45, câblage UTP (paire torsadée non blindée) catégorie 3, 4, ou 5 de deux paires, alimentation sur les broches 1, 2 (négatif) et 3,6 (positif) • Ports 100BASE-TX : connecteurs RJ-45, câblage UTP catégorie 5 de deux paires • Ports 100BASE-TX PoE : connecteurs RJ-45, câblage UTP catégorie 5 de deux paires, alimentation sur les broches 1, 2 (négatif) et 3,6 (positif) • Ports 100Base-FX : connecteurs MT-RJ, fibre multimode 50/125 ou 62.5/125 • Ports 1000BASE-T : connecteurs RJ-45, câblage UTP catégorie 5 de quatre paires • Ports 1000BASE-TX PoE : connecteurs RJ-45, câblage UTP catégorie 5 de quatre paires, alimentation sur les broches 1, 2 (négatif) et 3,6 (positif) • Ports SFP 1000BASE-T : connecteurs RJ-45, câblage UTP catégorie 5 de quatre paires • Ports SFP 1000BASE-SX, -LX/LH, -ZX, et CWDM : connecteurs fibre LC (fibre monomode ou multimode) • Ports XENPAK 10GBASE-ER (monomode) • Ports XENPAK 10GBASE-LR (monomode) • Ports StackWise d'empilement : câblage cuivre spécifique Cisco StackWise compatible également avec la technologie StackWise Plus des commutateurs de la gamme Cisco Catalyst 3750-E. • Port console de gestion : câble RJ-45 vers DB9 pour connexion à un PC ; pour la connexion d'un terminal, utiliser un adaptateur RJ-45 / DB-25 femelle de type DTE (data-terminal equipment) qui peut être commandé séparément (référence ACS-DSBUASYN=).

Tableau 2. Références des commutateurs Cisco Catalyst 3750

Référence	Description
WS-C3750G-24T-S	<ul style="list-style-type: none"> • 24 ports Ethernet 10/100/1000 • 32 Gb/s, bus d'empilage haut débit • Technologie d'empilement innovante • Commutateur multi-niveaux empilable de 1U • Services intelligents de classe entreprise pour la périphérie du réseau • Image logicielle IP Base installée • Routage Basique : statique, RIP, EIGRP stub, PIM stub, évolutif en IP Services pour bénéficier d'un routage dynamique IP complet
Modules Transceiver SFP	
GLC-SX-MM=	Module SFP 1000BASE-SX, connecteur LC
GLC-LH-SM=	Module SFP 1000BASE-LX/LH, connecteur LC
GLC-ZX-SM=	Module SFP 1000BASE-ZX, connecteur LC
GLC-T=	Module SFP 10/100/1000BASE-T, connecteur RJ-45
GLC-BX-D=	Module SFP 1000BASE-BX, IEEE 802.3ah, 1490 nm
GLC-BX-U=	Module SFP 1000BASE-BX, IEEE 802.3ah, 1310 nm
GLC-GE-100FX=	Module SFP 100BASE-FX pour emplacement SFP GE des 3750
CWDM-SFP-1470=	Module SFP CWDM 1470 nm, Gigabit Ethernet et FC 1G/2G (gris)
CWDM-SFP-1490=	Module SFP CWDM 1490 nm, Gigabit Ethernet et FC 1G/2G (violet)
CWDM-SFP-1510=	Module SFP CWDM 1510 nm, Gigabit Ethernet et FC 1G/2G (bleu)
CWDM-SFP-1530=	Module SFP CWDM 1530 nm, Gigabit Ethernet et FC 1G/2G (vert)
CWDM-SFP-1550=	Module SFP CWDM 1550 nm, Gigabit Ethernet et FC 1G/2G (jaune)
CWDM-SFP-1570=	Module SFP CWDM 1570 nm, Gigabit Ethernet et FC 1G/2G (orange)
CWDM-SFP-1590=	Module SFP CWDM 1590 nm, Gigabit Ethernet et FC 1G/2G (rouge)
CWDM-SFP-1610=	Module SFP CWDM 1610 nm, Gigabit Ethernet et FC 1G/2G (marron)
Modules Xenpak pour Catalyst 3750G-16TD	
C3-XENPAK-10GB-LR=	10GBASE-LR, fibre monomode de 10 km max.
XENPAK-10GB-ER	10GBASE-ER, fibre monomode de 40 km max.
Jarretières optiques	
CSS5-CABSX-LC=	Jarretière optique multimode de 10m, SX connecteurs LC-LC
CSS5-CABSX-LCSC=	Jarretière optique multimode de 10m, SX connecteurs LC-SC
CSS5-CABLX-LCSC=	Jarretière optique monomode de 10 m, LX connecteurs LC-SC
CAB-SM-LCSC-5M	Jarretière optique monomode de 5m, connecteurs LC-SC
CAB-SM-LCSC-1M	Jarretière optique monomode de 1m, connecteurs LC-SC
Câbles d'empilement StackWise pour Catalyst 3750	
CAB-STACK-50CM=	Câble d'empilement Cisco StackWise de 50 cm
CAB-STACK-1M=	Câble d'empilement Cisco StackWise de 1m
CAB-STACK-3M=	Câble d'empilement Cisco StackWise de 3m
Kits de montage en rack	
RCKMNT-1RU=	Kit de montage en rack pour les Catalyst 3750 de 1U
RCKMNT-3550-1.5RU=	Kit de montage en rack pour les Catalyst 3750 de 1,5U
RCKMNT-REC-1RU=	Kit de montage en rack en renforcement pour les Catalyst 3750 de 1U
RCKMNT-REC-1.5RU=	Kit de montage en rack en renforcement pour les Catalyst 3750 de 1,5U

Annexe 1bis

Gigabit Ethernet

There are five different physical layer standards for gigabit Ethernet using optical fiber (1000BASE-X), twisted pair cable (1000BASE-T), or balanced copper cable (1000BASE-CX).

The IEEE 802.3z standard includes 1000BASE-SX for transmission over multi-mode fiber, 1000BASE-LX for transmission over single-mode fiber, and the nearly obsolete 1000BASE-CX for transmission over balanced copper cabling. These standards use 8b/10b encoding, which inflates the line rate by 25%, from 1,000–1,250 Mbit/s to ensure a DC balanced signal. The symbols are then sent using NRZ.

IEEE 802.3ab, which defines the widely used 1000BASE-T interface type, uses a different encoding scheme in order to keep the symbol rate as low as possible, allowing transmission over twisted pair.

Name	Medium	Specified distance
1000BASE-CX	<u>Twinaxial cabling</u>	25 meters
1000BASE-SX	Multi-mode fiber	220 to 550 meters dependent on fiber diameter and bandwidth ^[2]
1000BASE-LX	Multi-mode fiber	550 meters ^[3]
1000BASE-LX	Single-mode fiber	5 km ^[3]
1000BASE-LX10	Single-mode fiber using 1,310 nm wavelength	10 km
1000BASE-ZX	Single-mode fiber at 1,550 nm wavelength	~ 70 km
1000BASE-BX10	Single-mode fiber, over single-strand fiber: 1,490 nm downstream 1,310 nm upstream	10 km
1000BASE-T	Twisted-pair cabling (Cat-5, Cat-5e, Cat-6, or Cat-7)	100 meters
1000BASE-TX	Twisted-pair cabling (Cat-6, Cat-7)	100 meters

1000BASE-X is used in industry to refer to gigabit Ethernet transmission over fiber, where options include 1000BASE-CX, 1000BASE-LX, and 1000BASE-SX, 1000BASE-LX10, 1000BASE-BX10 or the non-standard -ZX implementations.

1000BASE-CX is an initial standard for gigabit Ethernet connections over twinaxial cabling with maximum distances of 25 meters using balanced shielded twisted pair and either DE-9 or 8P8C connector. The short segment length is due to very high signal transmission rate. Although, it is still used for specific applications where cabling is done by IT professionals, for instance the IBM BladeCenter uses 1000BASE-CX for the Ethernet connections between the blade servers and the switch modules, 1000BASE-T has succeeded it for general copper wiring use.

1000BASE-SX is a fiber optic gigabit Ethernet standard for operation over multi-mode fiber using a 770 to 860 nanometer, near infrared (NIR) light wavelength. The standard specifies a distance capability between 220 metres (62.5/125 μm fiber with low modal bandwidth) and 550 metres (50/125 μm fiber with high modal bandwidth). In practice, with good quality fiber and terminations, 1000BASE-SX will usually work over significantly longer distances.

1000BASE-LX is a fiber optic gigabit Ethernet standard specified in IEEE 802.3 Clause 38 which uses a long wavelength laser (1,270–1,355 nm). 1000BASE-LX is specified to work over a distance of up to 5 km over 10 μ m single-mode fiber.

1000BASE-LX can also run over all common types of multi-mode fiber with a maximum segment length of 550 m. For link distances greater than 300 m, the use of a special launch conditioning patch cord may be required.^[5] This launches the laser at a precise offset from the center of the fiber which causes it to spread across the diameter of the fiber core, reducing the effect known as differential mode delay which occurs when the laser couples onto only a small number of available modes in multi-mode fiber.

1000BASE-BX10 is capable of up to 10 km over a single strand of single-mode fiber, with a different wavelength going in each direction. The terminals on each side of the fibre are not equal, as the one transmitting downstream (from the center of the network to the outside) uses the 1,490 nm wavelength, and the one transmitting upstream uses the 1,310 nm wavelength.

1000BASE-ZX is a non-standard but industry accepted^[citation needed] term to refer to gigabit Ethernet transmission using 1,550 nm wavelength to achieve distances of at least 70 km over single-mode fiber.

Annexe 2

IEEE 802.3 et standards

IEEE 802.3 est composée de différents standards dont voici la liste (non exhaustive) ci-dessous :

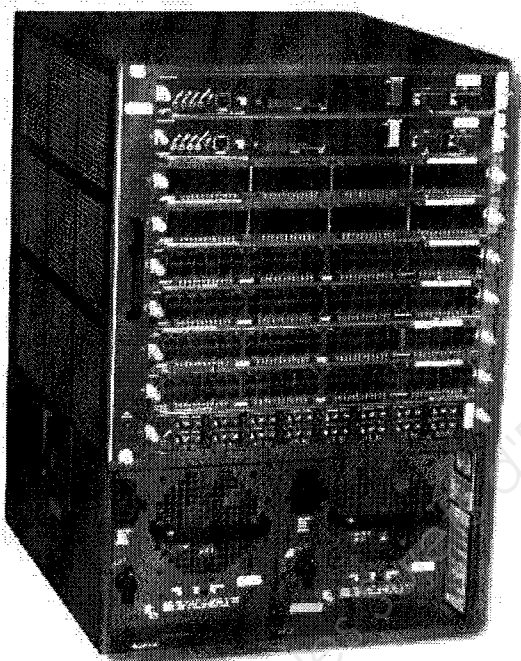
Norme	Date	Description
IEEE 802.3	1983	10BASE5 sur câble coaxial
IEEE 802.3a	1983	10BASE2 sur câble coaxial fin
IEEE 802.3b	1985	10BROAD36
IEEE 802.3c	1985	10 Mbits/s
IEEE 802.3d	1987	FOIRL -Fiber-Optic Inter-Repeater Link
IEEE 802.3e	1987	1BASE5
IEEE 802.3i	1990	10BASE-T sur paires torsadées
IEEE 802.3j	1993	10 Mbits/s sur fibre optique (d)
IEEE 802.3q	1993	Agrégation de VLAN
IEEE 802.3u	1995	Fast Ethernet à 100 Mbits/s (d)
IEEE 802.3y	1998	100BASE-T2
IEEE 802.3z	1998	Gigabit Ethernet à 1000 Mbits/s (d)
IEEE 802.3ab	1999	1000BASE-T
IEEE 802.3ac	1998	VLAN TAG
IEEE 802.3ad	2000	Link Aggregation
IEEE 802.3ae	2002	10GBASE-F
IEEE 802.3af	2003	DTE Power via MDI
IEEE 802.3ah	2004	Ethernet in the First Mile (d)
IEEE 802.3ak	2004	10GBASE-CX4
IEEE 802.3an	2006	10GBASE-T
IEEE 802.3ap	2007	Backplane Ethernet
IEEE 802.3aq	2006	10GBASE-LRM
IEEE 802.3ar	En cours	Gestion des embouteillages
IEEE 802.3as	2006	Extension de la trame
IEEE 802.3at	2008	Amélioration de Power over Ethernet
IEEE 802.3av	2009	10 Gbits/s PHY EPON
IEEE 802.3ay	2008	Amélioration du standard de base 802.3
IEEE 802.3ba	2009	Ethernet 40 et 100 Gbits/s

Annexe 3

Les routeurs CISCO sont généralement équipés des types suivants de mémoires :

- **ROM** (Read Only Memory) contenant : le programme auto-test de mise sous tension (**POST** = Power-On Self-Test), le programme d'amorçage du routeur, tout ou partie du système d'exploitation appelé **IOS** (Internetworking Operating System).
- **NVRAM** (Non-Volatile Random Access Memory) contenant : le fichier de configuration du routeur tel qu'il sera au démarrage (configuration de démarrage, aussi appelée **Start-Up Configuration** ou **START**).
- **RAM Flash** (type spécial de ROM pouvant être effacée et reprogrammée) contenant : une ou plusieurs versions d'IOS. (La RAM Flash est couramment appelée la **FLASH**)
- **RAM** (Random Access Memory) contenant : la configuration active du routeur (configuration en cours aussi appelée **Running Configuration** ou **RUN**), la table de routage, les paquets à router, ...

Extrait de la documentation des Commutateurs 6500



Exemple of Cisco Catalyst 6509 NEB:

The 9-slot Cisco Catalyst 6509 offers scalable port densities, ideal for many wiring-closet, core and data-center deployments. When equipped with a single Catalyst 6500 Series supervisor engine, eight payload slots are available to support a wide range of interface or services modules. Redundant supervisor engine configurations using fast 1-3 second failover are also supported for maximum network uptime.

The 100% Genuine CISCO chassis includes:

- (1) WS-C6509 - Chassis
- (1) WS-C6K-9SLOT-FAN - Fan
- (2) WS-X6K-SUP2-2GE - Supervisor 2 Engines
- (2) WS-X6148-GE-TX - 48 Port 10/100/1000 Modules
- (4) WS-X6348-RJ-45 - 48 Port 10/100 Modules
- (1) WS-X6416-GBIC - 16 GBIC Port Module
- (20) WS-G5484= - Multimode Fiber GBICs
- (2) WS-CAC-2500W - 2500W Power Supply

Services de commutation de niveau 2 à 7 orientés contenu et applications

- Le module CSM (Content Switching Module) intégré apporte une option de répartition de charge du serveur et du pare-feu haute performance et riche en fonctionnalités à la gamme Cisco Catalyst 6500, pour une infrastructure mieux protégée et plus facile à gérer, garantissant en outre un contrôle sans précédent.
- L'accélération SSL multigigabit intégrée combinée au module CSM crée une solution de commerce électronique très performante.
- L'intégration du pare-feu multigigabit et du module CSM forme une solution de centre de données sécurisée haute performance.
- Des fonctionnalités logicielles telles que NBAR (Network Based Application Recognition) optimisent l'administration du réseau et la gestion de l'utilisation de la bande passante.

Performances évolutives

- La gamme Cisco Catalyst 6500 fournit les meilleures performances de commutation LAN du marché (400 Mpps) grâce à la plate-forme Distributed Cisco Express Forwarding (DCEF720).
- Elle supporte les débits CEF (Cisco Express Forwarding) et de matrice de commutation pour un déploiement optimal dans les postes techniques, au niveau des coeurs de réseau, dans les centres de données et sur extrémités WAN ainsi que sur les réseaux des fournisseurs de services.

Richesse des services de niveau 3

- Le routage multiprotocole de niveau 3 supporte les besoins de réseau classiques et offre un mécanisme de transition en douceur dans l'entreprise
- Support matériel des tables de routage, tant au niveau des entreprises que des fournisseurs de services
- Support matériel d'IPv6 (à l'aide de Supervisor Engine 720) grâce à une suite de services haute performance sans équivalent.
- Support matériel des tables de routage étendues des entreprises et des fournisseurs de services.
- Support matériel de MPLS pour activer les services VPN dans l'entreprise et faciliter l'intégration en douceur avec les nouvelles infrastructures centrales haut débit des fournisseurs de service et les déploiements d'accès optique Ethernet.

Services avancés de données, de voix et de vidéo

- Communications IP intégrées au travers de toutes les plates-formes de la gamme Cisco Catalyst 6500.
- Cartes d'interface 10/100 et 10/100/1000 améliorables en clientèle, dotées d'une alimentation en ligne utilisant une carte fille et garantissant le support ultérieur de la norme IEEE 802.3af pour la protection des investissements actuels.
- Interfaces denses T1/E1 et passerelle VoIP (voice-over-IP) FXS (Foreign Exchange Station) pour les connexions d'accès RTPC (Réseau Téléphonique Public Commuté) et de téléphonie classique, de télécopie et PBX (Private Branch Exchange).
- Prise en charge d'applications IP multicast vidéo et audio haute performance.
- Administration intégrée indispensable pour déployer efficacement un réseau d'entreprise intégré évolutif.

Modules d'interface WAN

Les gammes Cisco Catalyst 6500 et Cisco 7600 supportent plusieurs interfaces WAN reposant sur deux technologies :

- *Module FlexWAN* — accepte jusqu'à deux cartes de port plug-in offrant de nombreux protocoles et caractéristiques WAN/MAN
- *Module de services optiques (OSM)* — carte d'interface de ligne dédiée fournissant plusieurs interfaces, dont OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, T3 fractionné, PoS OC-12/STM-4 fractionné, Gigabit Ethernet, ATM OC-12/STM-4 et DPT (Dynamic Packet Transport) OC-48/STM-16.

Module FlexWAN

Le module FlexWAN s'adapte aux systèmes des gammes Cisco Catalyst 6500 et Cisco 7600 et utilise les cartes de port des gammes Cisco 7200 et 7500 pour de nombreux protocoles WAN/MAN, dont Frame Relay, ATM, PoS, PPP (Point-to-Point Protocol) et HDLC (High-Level Data Link Control). De plus, le module FlexWAN offre des options de média telles que ClearChannel et T1/E1 fractionné, T3/E3, HSSI (High-Speed Service Interface), PoS OC-3 et ATM.

Modules de services optiques (OSM)

Les modules OSM sont des cartes d'interface qui fournissent une connectivité WAN haut débit avec des processeurs de réseau embarqués pour les applications de service IP à débit distribué. Pour en savoir plus sur les modules OSM, consulter les fiches techniques sur le site CISCO.

Tableau 1 Gamme Catalyst 6500 en bref

Configurations de châssis	3 emplacements 6 emplacements 9 emplacements 9 emplacements verticaux 13 emplacements
Bande passante du fond de panier	Bus partagé de 32 Gbits/s Matrice de commutation de 256 Gbits/s Matrice de commutation de 720 Gbits/s
Performances de transmission de niveau 3	Supervisor 1 MSFC : 15 Mpps Supervisor 2 MSFC : jusqu'à 210 Mpps Supervisor 720 : jusqu'à 400 Mpps
Système d'exploitation	Catalyst OS (CatOS) Cisco IOS Configuration hybride CatOS/IOS
Modules de supervision redondants	Oui, avec correction automatique sans changement d'état en cas de panne
Composants redondants	Alimentations (1+1) Matrice de commutation (1+1) Horloge remplaçable Ventilateur remplaçable
Fonctionnalités de haute disponibilité	Protocole GLBP (Gateway Load Balancing Protocol) Protocole HSRP (Hot Standby Router Protocol) EtherChannel multimodule Rapid Spanning Tree Multiple Spanning Tree Rapid Spanning Tree par VLAN Protocoles Rapid Convergence de niveau 3

Tableau 2 Densités de ports maximales sur le système

Modules LAN	
10/100/1000 Ethernet	576 ports, prenant tous en charge Inline Power
10/100 Fast Ethernet	576 ports, prenant tous en charge Inline Power
100-Base-FX	288 ports
Gigabit Ethernet (GBIC)	194 ports (2 ports fournis sur le module de supervision)
10 Gigabit Ethernet (XENPAK)	32 ports
Modules WAN intégrés	
FlexWAN (DS0 à OC-3)	12 modules avec 24 cartes de port
Ports OC-3 POS	192
Ports OC-12 POS 48	48
Ports OC-12 ATM	24
Ports OC-48 POS/DPT	24

Tableau 3 Power Requirements and Heat Dissipation

Model Number/Module Type	Module Current (A)	Module Power (Watts)	AC	
			AC-InputPower (Watts)	Heat Diss.(BTU/HR)
WS-C6K-9SLOT-FAN fan tray	1.10	46.00	58.00	196.00
WS-C6509 Catalyst 6509 chassis	5.00	210.00	262.50	896.44
WS-X6K-SUP2-2GE Supervisor Engine 1A with PFC and MSFC2 daughter cards	2.90	121.80	152.25	519.93
WS-X6348-RJ21V48-port 10/100 Ethernet module with WS-F6K-VPWR PoE daughter card	4.78	200.76	250.96	856.50
WS-X6416-GBIC16-port 1000BASE-X Gigabit Ethernet module	2.81	118.02	147.53	503.8

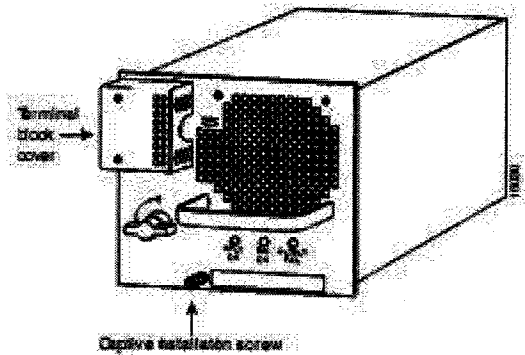
Tableau 4 Tension d'alimentation VCA et VCC requise

Alimentation	Tension/Intensité (CA)	Tension/Intensité (CC)
950 W WS-CAC-950W	100 à 240 VCA (10 % pour la gamme complète) ; 15 A	- 48 VCC à - 60 VCC en continu ; 38 A à - 48 VCC, 30 A à - 60 VCC
1000 W WS-CAC-1000W	100 à 240 VCA (10 % pour la gamme complète) ; 12 A à 100 VCA, 6 A à 240 VCA	Non supporté
1300 W WS-CAC-1300W	100 à 240 VCA (10 % pour la gamme complète) ; 17,25 A à 100 VCA, 8 A à 200 VCA	- 48 VCC à - 60 VCC en continu ; 38 A à - 48 VCC, 30 A à - 60 VCC
2500 W WS-CAC-2500W	100 à 240 VCA 200 à 240 VCA (10 % pour la gamme complète) ; 17 A maximum à 200/240 VCA avec une puissance de sortie de 2500 W ; 16 A maximum à 100/120 VCA avec une puissance de sortie de 1300 W	- 48 VCC à - 60 VCC en continu ; 80 A à - 40,5 VCC, 70 A à - 48 VCC, 55 A à - 60 VCC
4000 W WS-CAC-4000W	100 à 240 VCA (10 % pour la gamme complète) ; 23 A	Non supporté

Tableau 5 Dimensions des châssis de la gamme Catalyst 6500

Dimensions	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
Unités de rack	4 U	12 U	15 U	20 U	20 U

Cisco 6500 Power Supply Specifications : Power Supply Redundancy



Catalyst 6500 series switching modules have different power requirements. Depending upon the wattage of the power supply, certain switch configurations might require more power than a single power supply can provide. Although the power management feature allows you to supply power to all installed modules with two power supplies, redundancy is not supported in this configuration. Redundant and combined power configurations are summarized in Table A-42.

Note For proper load-sharing operation in a redundant power supply configuration, you must install two modules in the chassis. If you fail to install two modules, you might receive spurious OUTPUT FAIL indications on the power supply.

Note In systems that have two different sized power supplies installed, you may not have true redundancy. If the larger wattage power supply fails, the smaller wattage power supply might not be able to handle the entire load by itself.

Table A-42 Power Supply Redundancy

If you have two power supplies of	and redundancy is	Then
Equal wattage	Enabled	The total power drawn from both supplies is never greater than the capability of one supply. If one supply malfunctions, the other supply can take over the entire system load. Each power supply provides approximately half of the required power to the system. Load sharing and redundancy are enabled automatically; no software configuration is required.
Unequal wattage	Enabled	Both power supplies initially come online. For the Catalyst operating system, if the difference between the two power supply's output wattage is less than 10 percent of the higher output wattage power supply, redundancy is enabled. If the difference is greater than 10 percent, the lesser wattage power supply is disabled. For Cisco IOS, both power supplies come on. The total available wattage is the output wattage of the higher wattage power supply.
Equal or unequal wattage	Disabled	The total power available to the system is approximately 167 percent of the lower-wattage power supply. The system powers up as many modules as the combined capacity allows. If the higher-wattage power supply fails, the lower-wattage supply might also shut down due to overcurrent protection to prevent damage to the lower-wattage power supply.

Annexe 4

Configuration des VLAN sur un switch Cisco

1. Création des VLAN

```
Switch> enable  
Switch# vlan database  
Switch(vlan)# vlan 3 name VLAN_SI  
Switch(vlan)# vlan 43 name ESCOM  
Switch(vlan)# exit
```

Passer en mode privilégié
Crée le VLAN nommé VLAN_SI avec le numéro (VID) 3.
Crée le VLAN nommé ESCOM avec le numéro (VID) 43.

2. Affectation des ports (ports 1 à 4 : VLAN 3 - ports 9 à 12 VLAN 43)

```
Switch# configure terminal  
Switch(config)# interface fastEthernet 0/1  
Switch(config-if)# switchport mode access  
Switch(config-if)# switchport access vlan 3  
Switch(config-if)# exit
```

paramétrage du port n°1
pas de tag sur ce port (access)
affectation du port au vlan 3

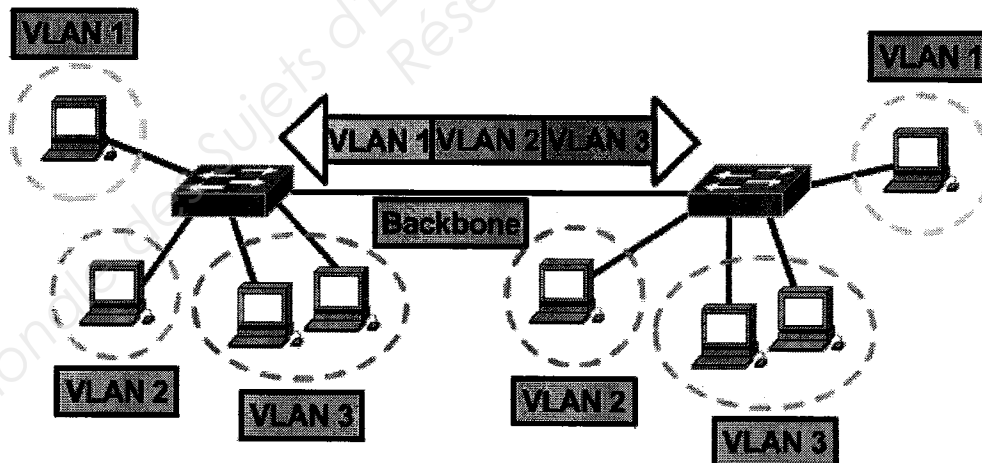
```
Switch(config)# interface fastEthernet 0/9  
Switch(config-if)# switchport mode access  
Switch(config-if)# switchport access vlan 43  
Switch(config-if)# exit
```

paramétrage du port n°9
pas de tag sur ce port (access)
affectation du port au vlan 43

3. Création du lien taggé ou trunk (port 24)

```
Switch(config)# interface fastEthernet 0/24  
Switch(config-if)# switchport mode trunk  
Switch(config-if)# switchport trunk encapsulation dot1q  
Switch(config-if)# exit
```

paramétrage du port n°24
ce lien sera taggé (trunk)...
...au format 802.1Q



Annexe 5

VMPS (VLAN Membership Policy Server)

Qu'est-ce-que le VMPS ?

La gestion de VLAN est devenue fastidieuse et rébarbative sur un grand site hétérogène, il a alors fallu trouver une solution pour automatiser cette gestion. Le VMPS est un service, créé par Cisco, chargé de faire correspondre un Vlan à une (ou plusieurs) adresse Mac et s'impose donc comme la solution.

Comprendre le VMPS

La gestion dynamique des VLAN passe tout d'abord par la compréhension d'une architecture réseau basée sur les Vlan de niveau 2, du protocole VTP (Vlan Trunking Protocol), puis par l'étude du protocole VQP (Vlan Query Protocol).

Le protocole VTP (Vlan Trunking Protocol)

L'utilisation du protocole VTP est obligatoire sur le réseau sur lequel on veut déployer une solution VMPS. En effet, ce dernier utilisera le nom de domaine VTP lors de l'échange de paquets entre le serveur VMPS et les commutateurs clients.

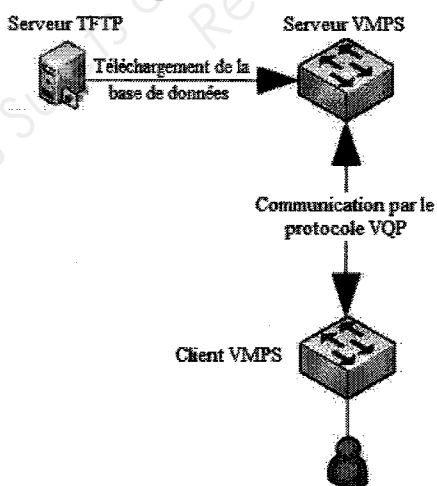
Le protocole VQP

Le protocole VQP est un protocole qui permet au switch client d'interroger un serveur VMPS avec des informations sur les stations enregistrées et leur Vlan associé. Ainsi le switch client pourra associer le port avec le bon VLAN. Le serveur VMPS est le plus souvent un switch ou un routeur Cisco, mais il existe également des serveurs " libres " (dont le code source est consultable et modifiable) destinés aux machines Unix (Linux et Solaris).

Le VMPS est donc basé sur une architecture client/serveur et permet de gérer dynamiquement les assignations de Vlan en fonction d'adresses MAC (Media Access Control). Lorsqu'une machine se connecte à un port, le switch récupère son adresse MAC et se connecte au serveur VMPS afin de vérifier le droit d'accès de cette machine. Lorsque celle-ci est autorisée, le serveur envoie au client le Vlan dans lequel cette machine doit se connecter. Le switch place donc le port dans le bon Vlan et la machine a donc accès au réseau.

Si le Vlan n'est pas autorisé sur le port, il y a 2 solutions :

- le serveur VMPS est en mode open, il renvoie un message avertissant que l'accès au réseau est refusé,
- le serveur VMPS est en mode secure, le port du switch est alors refermé.



Le serveur VMPS peut être accompagné de serveurs secondaires pour prendre le relais en cas de panne ou pour simplement équilibrer la charge (load-balancing). Le serveur utilise une base de données contenant les adresses MAC des clients, le Vlan correspondant et d'autres règles permettant de donner le droit à un utilisateur de se connecter. Normalement cette base de données est téléchargée par le serveur VMPS à partir d'un serveur TFTP (Trivial File Transfert Protocol), qui peut être situé n'importe où sur le réseau. Cette base de données est chargée dans le serveur à chaque démarrage/redémarrage de celui-ci.

Annexe 6

ACL, PRINCIPE DE FONCTIONNEMENT

Les ACL, ou Access Control List permettent de filtrer ce qui entre ou sort par les interfaces d'un routeur, en fonction :

- de l'IP Source,
- de l'IP de destination,
- du port source,
- du port de destination,
- du protocole (IP, TCP, UDP, ICMP).

Il est possible d'autoriser ou d'interdire les paquets IP. Une ACL contient plusieurs règles qui sont lues séquentiellement jusqu'à ce que l'une d'elles corresponde au paquet traité. La lecture de la liste s'arrête alors.

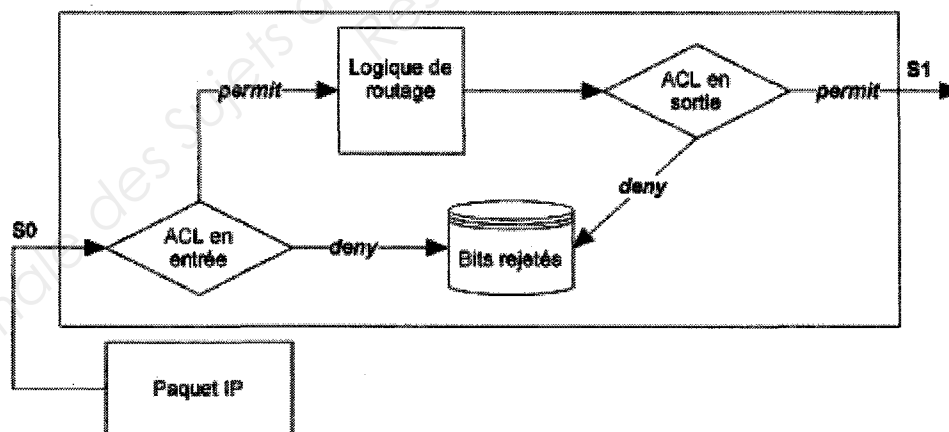
Exemple de liste :

1. Interdire l'adresse IP source 192.168.1.1
2. Interdire le réseau IP source 194.45.0.0 /16
3. Autoriser le réseau IP source 10.0.0.0 /8
4. Interdire tout.

Un paquet avec IP Src 10.0.0.3 sera traité par la règle 3.

Un paquet avec IP Src 192.168.1.2 sera traité par la règle 4.

La dernière règle est implicite (on n'est pas obligé de la préciser).



Comme indiqué par le schéma ci-dessus, un paquet peut être traité lorsqu'il entre dans le routeur ou lorsqu'il sort.

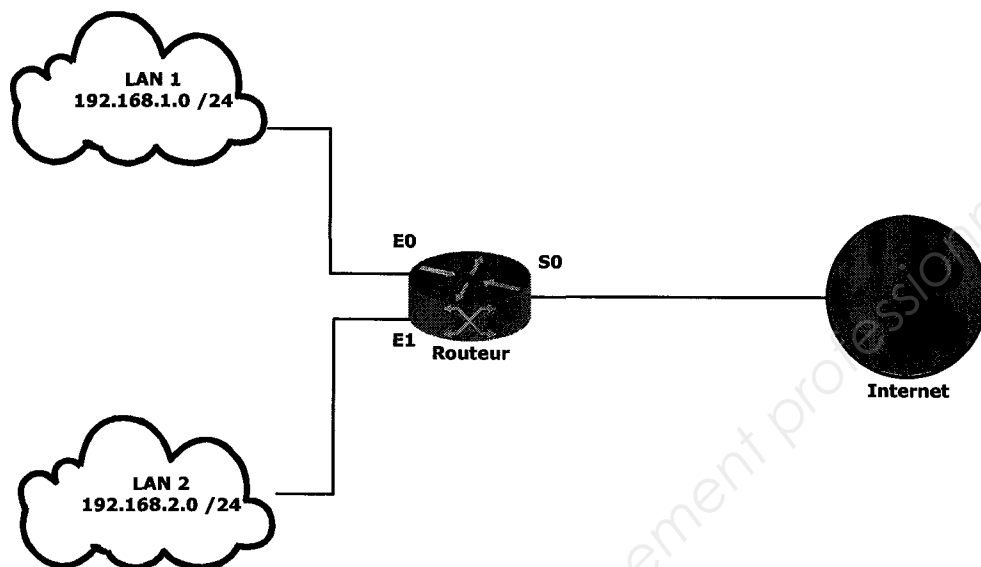
Les mots utilisés pour autoriser ou interdire sont : **permit deny**

Il existe deux types d'ACL : Les ACLs simples et les ACLs étendues.

ACL SIMPLE

Avec ces règles simples, le routeur ne regarde que l'IP Source.

Exemple :



```
Router(config) # access-list 5 permit 192.168.1.0 0.0.0.255  
Router(config) # access-list 5 deny any
```

Liste des « filtres »...

```
Router(config) # interface S0  
Router(config-if) # ip access-group 5 out
```

...à appliquer en sortie de l'interface S0 (out)

En français : « les paquets en provenance du LAN 1 pourront sortir vers le réseau Internet »
« tous les autres paquets seront interdits de sortie vers Internet »

Nomenclature d'une ACL simple.

```
Router(config) # access list {1-99} {permit | deny} [source address] [source mask]
```

{1-99} → numéro de l'access-list, toujours **entre 1 et 99 pour une liste standard.**

{permit | deny} → **autorise ou interdit** le paquet.

[source address] → **adresse ip du réseau (ou de la machine)** concernée.

[source mask] → **masque générique** : C'est l'inverse d'un masque de sous-réseau habituel.

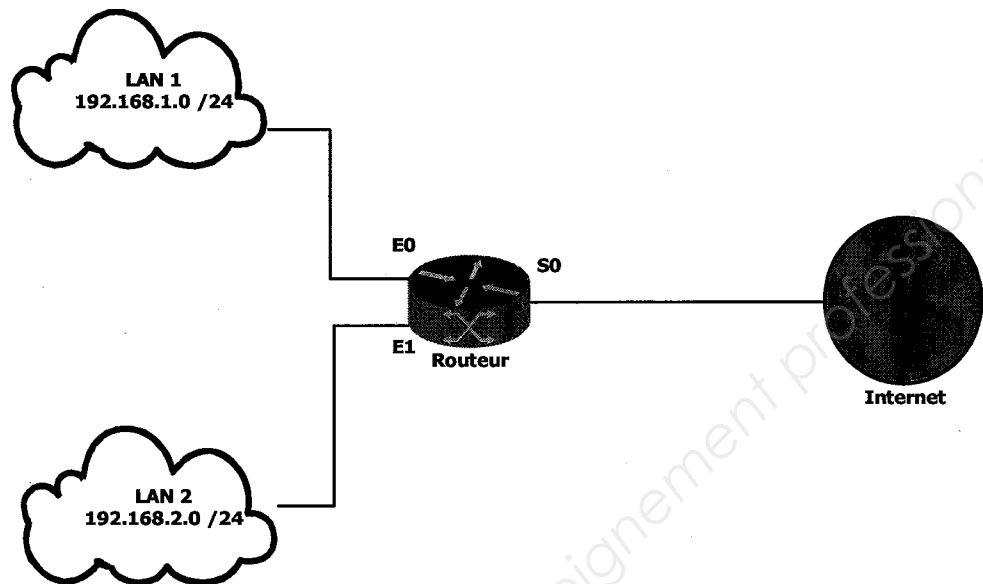
Lorsque tous les bits d'une @IP doivent être comparés, on peut utiliser le mot clé **host**.

Pour qu'une instruction deny ou permit s'applique à toutes les @IP qui ne sont pas indiquées dans les instructions de la liste, il est possible d'utiliser le mot clé **any**.

ACL ÉTENDUE

Une ACL étendue s'intéresse à l'IP source mais aussi l'IP de destination ainsi que les ports (source et dest) et le protocole (IP, ICMP, TCP, UDP).

Exemple :



```
Router(config) # access-list 101 deny icmp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config) # access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80
Router(config) # access-list 101 deny any
```

```
Router(config) # interface E0
Router(config-if) # ip access-group 101 in
```

...à appliquer en entrée de l'interface E0 (in)

En français : « les paquets icmp (ping) en provenance du LAN 1 vers LAN 2 ne pourront pas entrer dans l'interface E0 ».
« Les paquets en provenance de LAN 1 vers tous les réseaux (any) sur le port TCP 80 (http) pourront entrer dans l'interface E0 ».
« Tous les autres paquets seront interdits d'entrer dans E0 ».

Nomenclature d'une ACL étendue.

```
Router(config) # access-list {100-199} {permit | deny} [protocol] [source address] [source mask]
[destination address] [destination mask] [operator operand]
```

- | | |
|------------------------------|--|
| {100-199} | → numéro de l'access-list, toujours entre 100 et 199 pour une liste IP étendue. |
| {permit deny} | → autorise ou interdit le paquet. |
| [protocol] | → protocole sur lequel agit l'access-list (IP, TCP, UDP, ICMP) |
| [source address] | → adresse ip du réseau (ou de la machine) source. |
| [source mask] | → masque générique : c'est l'inverse d'un masque de sous-réseau habituel |
| [destination address] | → adresse ip du réseau (ou de la machine) destination. |
| [destination mask] | → masque générique : c'est l'inverse d'un masque de sous-réseau habituel |
| [operator operand] | → opérateur suivi, en opérant du numéro de port spécifique concerné
(eq = equal , gt = greather than) |