République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. MIRA de Béjaia

Faculté des Sciences Exactes

Département d'Informatique

Module : Administration des Réseaux

Préparé par Dr. Mohand YAZID

Année Universitaire 2021-2022

Préface

Ce manuel de cours et de travaux pratiques, intitulé *Administration des Réseaux*, à vocation professionnelle est destiné en premier lieu aux étudiants de deuxième année Master *Administration et Sécurité des Réseaux*. Il peut être également consulté par tout étudiant de fin de cycle ayant suivi un parcours qui relève des domaines réseaux et télécommunications, et souhaitant être recruté dans une entreprise pour faire une carrière professionnelle. En effet, ce manuel englobe et résume l'essentiel des connaissances et compétences requises pour qu'un nouveau diplômé puisse rejoindre une entreprise et réussir ses tâches d'administrateur réseau. La pédagogie suivie pour rédiger, présenter et organiser ce manuel est adaptée pour un enseignement hybrid ou à distance. En effet, ce manuel offre à l'étudiant la possibilité d'acquérir des connaissances, développer des compétences , et s'auto-évaluer sans présence de l'enseignant, i.e., de façon complètement libre et autonome. Ce manuel à caractère pédagogique est le fruit de trois années d'expérience professionnelle dans le poste *Administrateur Réseau* dans le complexe Agro-Industrie CEVITAL SPA (2008-2011) et cinq années d'enseignement du module *Administration des Réseaux* dans le département d'Informatique de la faculté des Sciences Exactes de l'université de Bejaia (2017-2022). Ce manuel est scindé en trois partie :

1. La première partie, intitulée *Théorie*, fournit à l'étudiant l'ensemble des connaissances théoriques à acquérir sur le domaine de l'administration des réseaux. Cette partie à son tour est scindée en quatre chapitres :

   (a) Le premier chapitre, intitulé *Les Réseaux et Leurs Caractéristiques*, présente l'ensemble des caractéristiques qu'un administrateur réseau doit recenser sur son réseau pour pouvoir le gérer à distance.

(b) Le deuxième chapitre, intitulé *Les Domaines Fonctionnels de l'Administration des Réseaux*, présente également l'ensemble des activités qu'un administrateur réseau peut réaliser à distance sur le réseau géré.

(c) Le troisième chapitre, intitulé *Les Environnements d'Administration de Réseau*, présente d'une part un panorama de solutions logicielles pour l'administration de réseau, et d'autre part propose une démarche à suivre pour effectuer un choix optimal.

(d) Le quatrième chapitre, intitulé *L'Environnement d'Administration SNMP*, est dédié à la présentation de l'environnement d'administration des réseaux Internet le plus connu et le plus utilisé qui est SNMP.

2. La deuxième partie, intitulée *Pratique*, propose à l'étudiant cinq travaux pratiques à réaliser qui devront lui permettre de développer les compétences essentielles requises pour s'engager dans le monde de d'administration de réseau :

(a) Le premier TP, intitulé *Configuration de Base et Outils d'Accès à Distance*, a pour objectif de permettre à l'étudiant de comprendre, apprendre et maîtriser les étapes de configuration de base des équipements d'interconnexion d'un réseau.

(b) Le deuxième TP, intitulé *Conception d'un Schéma d'Adressage IP*, a pour objectif de permettre à l'étudiant de maîtriser les différentes méthodes de conception de schémas d'adressages, et apprendre surtout les bonnes pratiques à suivre pour attribuer les adresses IP.

(c) Le troisième TP, intitulé *Routage et Tests de Connectivité*, a pour objectif de permettre à l'étudiant de connaître, apprendre et maîtriser les différents tests existants pour vérifier la bonne configuration du routage, ou détecter, localiser et corriger des erreurs de configuration de ce dernier.

(d) Le quatrième TP, intitulé *Construction d'une Cartographie Réseau*, a pour objectif de permettre à l'étudiant d'être capable de construire à l'aide du protocole CDP (CISCO Discovery Protocol) la cartographie de son réseau.

(e) Le cinquième TP, intitulé *Gestion du système IOS et des Fichiers de Configuration*, a pour objectif de permettre à l'étudiant d'être capable de sauve-

garder/restaurer à l'aide du protocole TFTP le système IOS et les fichiers de configuration des équipements d'interconnexion de son réseau.

3. La troisième et dernière partie, intitulée *Sujets d'Examen avec Corrigés*, a pour objectif de tester et évaluer le niveau de compréhension et d'assimilation de l'étudiant par rapport aux savoir et savoir-faire présentés tout en long de ce manuel.

Table des matières

Table des figures

Liste des tableaux

Première partie

Théorie

Chapitre 1

Les réseaux et leurs caractéristiques

1.1 Introduction et définitions

Dans ce chapitre, nous chercherons à établir les principales caractéristiques qui permettront à l'étudiant de reconnaître l'environnement de réseau qu'il veut gérer.

Un réseau peut être caractérisé selon différents critères. Nous proposons les critères suivants :

1. **la typologie (ou la finalité)**,
2. **l'étendue**,
3. **les architectures technologiques**,
4. **les équipements**,
5. **les applications distribuées**,
6. **les usagers**.

Mais tout d'abord, définissons le concept de réseau en se basant sur la Figure 1.1.

Définition 1

Un **réseau** peut être vu comme un **ensemble de stations** (hôtes) reliées entre elles par des **noeuds** de communication et des **liens** de communication (supports). La principale fonction des noeuds de communication est de **relayer** les paquets d'information

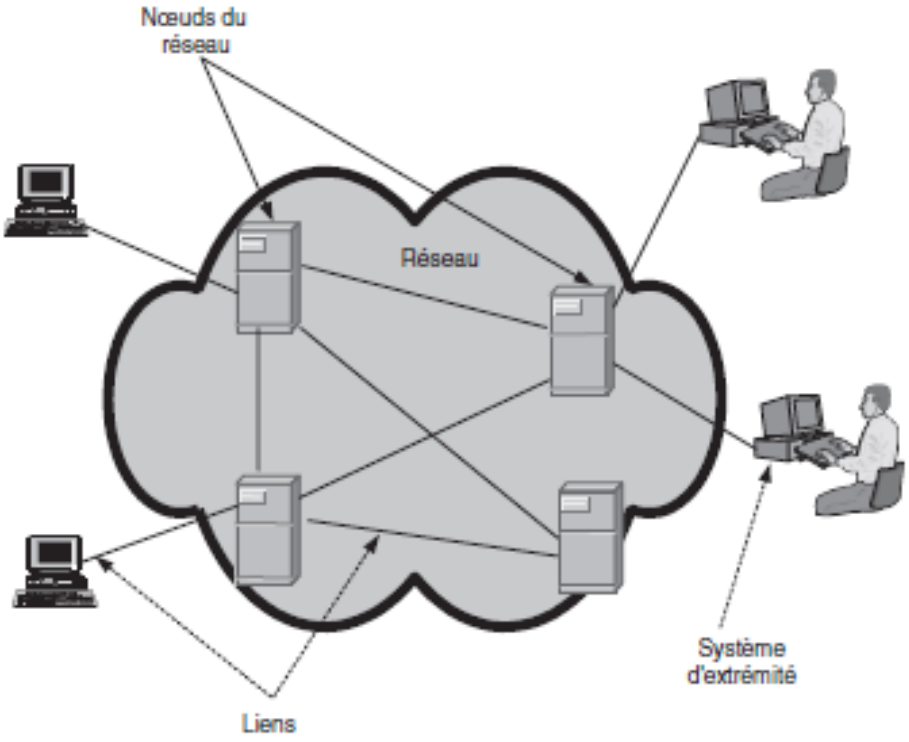


FIGURE 1.1: *Les Réseaux Informatiques*

vers les autres noeuds (routeur, pont, commutateur, etc.). Les liens de communication assurent le **transfert** des paquets entre deux noeuds.

Définition 2

À plus grande échelle, le **réseau** peut être vu comme un ensemble de noeuds **géographiquement distribués** et reliés entre eux par des liens. Les liens sont les supports de transmission, tels que le câble coaxial, la fibre optique ou la paire torsadée. Les unités rattachées aux noeuds sont très variées. Il peut s'agir d'un terminal, d'un ordinateur, d'une imprimante ou d'un réseau local. Les noeuds sont en réalité des ordinateurs dont l'une des fonctions est le **routage** des informations circulant sur le réseau.

1.2 Caractéristiques des réseaux

1.2.1 Selon la typologie

Un **réseau** peut en fait avoir **deux finalités** : celle de *servir d'autres réseaux* ou alors celle de *servir directement les utilisateurs finaux*.

1. Les **réseaux informatiques** ont principalement pour finalité de fournir des services réseaux aux membres de la même organisation.
2. Les **réseaux de télécommunication** sont quant à eux mis en place pour servir d'autres réseaux et des usagers.

Exemples :

- les réseaux **Algérie Télécom**, **France Télécom** ou **Bell Canada** fournissent des services réseaux autant à des usagers qu'à d'autres réseaux appartenant à d'autres organisations. Ces réseaux sont donc dits des réseaux de télécommunication.
- Dans cette catégorie, nous retrouverons également des réseaux **ISP** (Internet services providers). En effet, un ISP est un organisme offrant une connexion à Internet.

1.2.2 Selon l'étendue

Les réseaux peuvent être classés en fonction de **l'éloignement maximal** entre stations. On peut alors distinguer trois types de réseau : le réseau **local**, le réseau **étendu** et le réseau **métropolitain**.

Le réseau local :

- Lorsque deux stations peuvent être séparées au **maximum de quelques kilomètres**, le réseau sera dit local (LAN). Généralement, le réseau local est la propriété de la **même organisation**. C'est le type de réseau que l'on rencontre le plus souvent dans les organisations.
- Étant donné la proximité des stations, le taux de transmission des données est relativement élevé. Il est au **minimum de 10 Mbits/s** (millions de bits par seconde).

– On peut utiliser les trois types de support de transmission : **la paire torsadée**, **le câble coaxial** et **la fibre optique**. En général, la paire torsadée est la plus fréquemment utilisée.

Le réseau étendu :

– Lorsque la distance entre deux stations situées dans des lieux différents atteint au **maximum quelques centaines de kilomètres**, le réseau est dit étendu.
– Les compagnies disposant de plusieurs sites **éloignés géographiquement**, tels que les systèmes de réservation de places d'avion et les systèmes bancaires, utilisent ce genre de réseau.
– Les vitesses de transmission d'un réseau étendu sont généralement **moins grandes** que celles d'un réseau local et, par conséquent, le réseau étendu demande un **plus long** délai de transmission qu'un réseau local.

Le réseau métropolitain :

– Le réseau métropolitain se situe à **mi-chemin** entre le réseau local et le réseau étendu. Il couvre habituellement les stations d'une **même ville**.
– Le support de transmission utilisé est le **câble coaxial** ou la **fibre optique**. Cette catégorie de réseau a été conçue pour supporter le transport des données à une vitesse supérieure à 1 Mbits/s.

1.2.3 Selon les architectures de protocoles

– Les réseaux peuvent être différenciés par **les suites de protocoles** qu'ils mettent en oeuvre.
– Le fonctionnement de ces protocoles implique **une organisation architecturale du réseau**.
– Nous retrouvons des architectures de protocoles **synchrones** ou **asynchrones** :

Communication synchrone :

Elle se base sur le principe **des échanges en temps réel**. Il s'agit d'une **communication directe** entre deux interlocuteurs ou plus (Multicast) qui participent de **manière effective** à un échange d'information durant la **même session** de communication.

Communication asynchrone :

Elle se caractérise par le mécanisme des échanges **en mode différé**, i.e., lorsque les participants y contribuent **à différents moments** sans qu'il soit nécessaire que tous soient connectés au système de communication utilisé.

Nous retrouvons également différents types de commutation de données, à savoir :

Commutation de circuits :

Elle consiste à créer dans le réseau un **circuit particulier** entre l'émetteur et le récepteur avant que ceux-ci ne commencent à échanger des informations. Ce circuit sera propre aux deux entités communiquant et il sera libéré lorsque l'un des deux coupera sa communication.

Commutation de messages :

Elle consiste à envoyer un **message** de l'émetteur jusqu'au récepteur en passant de noeud de commutation en noeud de commutation. Chaque noeud attend d'avoir reçu **complètement** le message avant de le réexpédier au noeud suivant. Cette technique nécessite de prévoir de **grandes zones tampon** dans chaque noeud du réseau, et aussi prévoir un **contrôle de flux** des messages pour éviter la saturation du réseau.

Commutation de paquets :

Un **message** émis est découpé en **paquets** et par la suite chaque paquet est **commuté** à travers le réseau comme dans le cas des messages. Les paquets sont envoyés **indépen-**

damment les uns des autres et sur une **même liaison** on pourra trouver les uns derrière les autres des paquets appartenant à différents messages. Chaque noeud redirige chaque paquet vers la bonne liaison grâce à une **table de routage**.

Commutation de cellules :

Une **cellule** est un paquet particulier dont la **taille** est toujours fixée à **53 octets**. C'est la technique de base des réseaux hauts débits ATM où avant toute émission de cellules, un **chemin virtuel** est établi par lequel passeront toutes les cellules. Cette technique **mixe** donc la commutation de circuits et la commutation de paquets de taille fixe.

Les principales architectures de protocoles émergentes sont les suivantes :

- L'architecture **WDM/DWDM** (**W**avelength-**D**ivision **M**ultiplexing/**D**ense **WDM**),
- L'architecture **SONET/SDH** (**S**ynchronous **O**ptical **NET**work/**S**ynchronous **D**igital **H**ierarchy),
- L'architecture Internet **TCP/IP** (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol),
- L'architecture **IPX/SPX** (**I**nternetwork **P**acket e**X**change/**S**equenced **P**acket e**X**change),
- L'architecture **X.25**,
- L'architecture **FR** (**F**rame **R**elay),
- L'architecture **ISDN** (**I**ntegrated **S**ervices **D**igital **N**etwork),
- L'architecture **ATM** (**A**synchronous **T**ransfer **M**ode).

Dans ce qui suit, nous donnerons une brève définition pour chacune des architectures citées ci-dessus :

WDM/DWDM :

Le multiplexage en longueur d'onde est une technique utilisée en **communication optique** qui permet d'augmenter le débit sur une fibre optique en faisant circuler **plusieurs signaux** de longueurs d'onde différentes sur **une seule fibre**, en les mélangeant à l'entrée à l'aide d'un multiplexeur et en les séparant à la sortie au moyen d'un démultiplexeur. Exemple d'application : **câbles sous-marins internationaux**.

SONET/SDH :

SONET est un modèle de norme de **transmission optique**. C'est un protocole de la **couche 1** du modèle OSI utilisé principalement aux États-Unis. Son équivalent international est la norme **SDH** avec laquelle il a progressivement convergé. Initialement, SONET était normalisé pour des **transmissions téléphoniques**. Ensuite, SONET et SDH ont été modifiés pour s'adapter aux protocoles IP, ATM et Ethernet.

TCP/IP :

La suite TCP/IP est l'ensemble des protocoles utilisés pour **le transfert des données** sur Internet. Elle est souvent appelée TCP/IP, d'après le nom de ses deux premiers protocoles : **TCP** (Transmission Control Protocol) et **IP** (Internet Protocol).

IPX/SPX :

Elle fait référence aux deux protocoles propriétaires basés sur **XNS** (Xerox Network System) qu'a conçus **Novell** pour ses réseaux **NetWare**. IPX, qui correspond au protocole IP dans TCP/IP, s'exécute sur **la couche Réseau** du modèle de référence ISO/OSI. SPX, qui correspond au protocole TCP dans TCP/IP, s'exécute sur **la couche Transport**.

X.25 :

C'est un protocole pour réseaux à **commutation de paquets**. La norme X.25 correspond aux trois premiers niveaux du modèle **OSI** (Open Systems Interconnection), à savoir : le niveau **physique**, le niveau du **lien** (qui assure la fiabilité d'une communication), et le niveau des **paquets** (qui décrit le protocole de transfert de données).

FR :

C'est un protocole à **commutation de paquets** situé au niveau de la couche de **liaison** (niveau 2) du modèle OSI, utilisé pour les échanges **intersites** (WAN). Sur le plan technique, il peut être vu : comme un **successeur** de X.25.

ISDN :

C'est un réseau de **télécommunications** constitué de liaisons numériques autorisant une meilleure qualité et des vitesses pouvant atteindre **2 Mbit/s** contre 56 kbit/s pour un modem classique. On peut voir l'architecture ISDN comme une évolution **entièrement numérique** des réseaux **téléphoniques** plus anciens, conçue pour associer la **voix**, les **données**, la **vidéo** et toute autre application ou service.

ATM :

C'est un standard de **télécommunications** proposé pour le ISDN Large Bande (BISDN). C'est une amélioration de la **commutation de paquets** permettant de mieux exploiter les liens à haut débit et de s'adapter aux exigences des nouvelles applications. ATM veut permettre de véhiculer tout type d'information : **voix**, **vidéo**, **données**, i.e., être un réseau multimédia.

1.2.4 Selon les éléments physiques du réseau : les équipements

Dans les réseaux, nous retrouvons différents types d'équipements. Afin de faciliter leurs descriptions respectives, nous allons les présenter selon leur appartenance : les **équipements réseaux**, les **postes de travail** et les **serveurs**.

Les équipements réseaux :

Nous retrouverons principalement dans les équipements suivants :

Répéteur :

C'est un équipement électronique simple permettant d'**amplifier** un signal et d'**augmenter** la taille d'un réseau.

Concentrateur (Hub) :

Il permet de **concentrer** le trafic réseau provenant de plusieurs hôtes, il agit au niveau de la couche physique du modèle OSI.

Ponts (bridges) :

Il permet de relier des réseaux travaillant avec le même protocole. Ils travaillent au niveau de la couche 2 du modèle OSI (couche liaison).

Commutateur (Switch) :

C'est un pont multiport c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau de la couche 2 du modèle OSI.

Passerelle (Gateway) :

C'est un système matériel et logiciel permettant de faire la liaison entre deux réseaux afin de faire l'interface avec le protocole du réseau différent.

Routeur :

C'est un dispositif d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

Vsat :

Les réseaux de communications par satellite utilisent une station relais dans l'espace (le satellite) servant à relier (au moins) deux émetteurs/récepteurs hertziens au sol, communément appelés stations terrestres ou stations au sol.

Les postes de travail :

On peut considérer les postes de travail suivants :

Station Microsoft Windows :

Windows est actuellement préinstallé sur plus de 91 % des ordinateurs personnels.

Station GNU/Linux :

C'est un système d'exploitation libre s'appuyant sur le noyau Linux et les outils GNU.

Station Mac OS X et iOS :

C'est des systèmes pré-installés sur la majorité des ordinateurs et appareils mobiles vendus par Apple.

Les Serveurs :

Nous distinguons les types de serveurs suivants :

Serveur web :

Chaque fois que vous demandez une page web, vous passez par un réseau Internet à partir d'un serveur web.

Serveur de fichiers :

Il conserve les fichiers partagés par plusieurs ordinateurs dans un emplacement commun. Un utilisateur peut extraire un document depuis son ordinateur, le traiter et l'enregistrer de nouveau sur le serveur.

Serveur d'applications :

Il stocke et permet de partager des données (commerciales, comptabilité, etc.) accessibles depuis tous les postes reliés au serveur informatique. Il peut traiter les informations de manière à n'en extraire que les données souhaitées par l'ordinateur.

Serveur d'impression :

Il permet de partager une ou plusieurs imprimantes.

Serveur de messagerie :

Il gère les messages en distribuant le courrier électronique aux ordinateurs et en les stockant de manière à permettre un accès à distance.

1.2.5 Selon les éléments logiciels du réseau : les applications distribuées

Les services offerts aux utilisateurs finaux sont de plus en plus sophistiqués. Ils ont largement évolué ces dernières années et vont certainement encore progresser dans le futur pour laisser apparaître des services bien plus interactifs et utilisant à la base les technologies multimédias.

Parmi les services actuellement offerts, on retrouve :

- les services d'accès aux bases de données ;
- les services de transferts de fichiers ;
- les services de messagerie ;
- les services de Workgroup ;
- les services de téléphonie, etc.

Remarques :

- Les services cités précédemment sont mis à la disposition des usagers de **manière sélective**.
- En effet, en fonction de leur **position** et **rôle** dans l'entreprise, les utilisateurs peuvent accéder à des **services différenciés**, avec également **différents droits d'accès** aux serveurs, applications, etc.
- Un ensemble de **règles d'utilisation** est mis en place pour **contrôler** les accès au **système d'information** et aux **ressources de l'entreprise** et/ou **rendre disponibles** certains services à un groupe bien déterminé d'utilisateurs.

1.2.6 Selon les usagers

- Les organisations des grandes entreprises sont de plus en plus structurées. Leurs activités deviennent davantage centrées sur un système d'information qui constitue la clé de voûte du fonctionnement global de l'entreprise.
- Ce système d'information constitue également le maillon faible du système car il doit être disponible à tout moment sans quoi l'activité de l'entreprise ne peut plus être effective.
- On accède à ce système d'information via les différentes composantes du réseau identifiées dans les sections précédentes.
- Le personnel de l'entreprise qui tient un rôle différencié dans la structure globale ne peut ou ne veut pas être concerné par certains aspects techniques du fonctionnement global du réseau.
- Certains départements vont se positionner comme client vis-à-vis d'autres départements qui auront la charge du bon fonctionnement et de la disponibilité du réseau.
- On peut dès lors répertorier, sans souci d'exhaustivité toutefois, un ensemble de profils d'usagers identifiés par leur rôle dans l'entreprise :

  1. Les administrateurs de réseau qui bénéficient de privilèges importants ;
  2. Les ingénieurs qui ont des droits étendus sur certaines parties techniques du réseau ;
  3. Les dirigeants qui ont des droits étendus sur le système d'information ;
  4. Le personnel administratif avec des droits très limités.

1.3 Que veut-on gérer

Plusieurs niveaux de gestion (administration) doivent être distingués, dont il est nécessaire de comprendre l'utilité. À titre d'exemple :

La gestion de l'infrastructure réseau :

Elle concerne la gestion de tous les **éléments du réseau** et des **logiciels embarqués** qui constituent les différents réseaux de l'entreprise. On désigne par **élément du réseau** chacun des équipements qui sont branchés au réseau, ainsi que les logiciels y résidant. Les routeurs, les concentrateurs, les répéteurs, les passerelles, les modems, sont les éléments qui constituent l'infrastructure du réseau.

La gestion des desktops :

Elle concerne tous les aspects relatifs à la gestion des points d'accès au réseau. Elle englobe la gestion des stations terminales, ainsi que de tous les logiciels supportés par ces stations : système d'exploitation réseau, les applications et les services de communication mis à la disposition des usagers.

Chapitre 2

Les Domaines fonctionnels de l'administration des réseaux

2.1 Définition

- La **gestion** (**administration**) **de réseau** a trait à l'ensemble des activités permettant d'assurer le **fonctionnement du réseau** afin qu'il livre les **services attendus**.
- Ces activités peuvent être regroupées selon leurs fonctionnalités. La **décomposition fonctionnelle** établie par l'OSI a arrêté cinq domaines de gestion : la gestion de **configuration**, des **fautes**, des **performances**, des **coûts** et de la **sécurité**.
- Pour chacun de ces domaines, l'administrateur réalisera la **collecte** des données de gestion, leur **interprétation** et le **contrôle** des éléments de réseaux. Ces activités sont réalisées **à distance** sur les éléments de son réseau.

2.2 La gestion de la configuration

- La gestion de la configuration (comme illustré dans la Figure 2.1) permet de **désigner** et de **paramétrer** différents objets.
- Les procédures requises pour gérer une configuration sont :

  1. la **collecte** d'informations,

2. le **contrôle** de l'état du système,

3. la **sauvegarde** de l'état dans un historique.

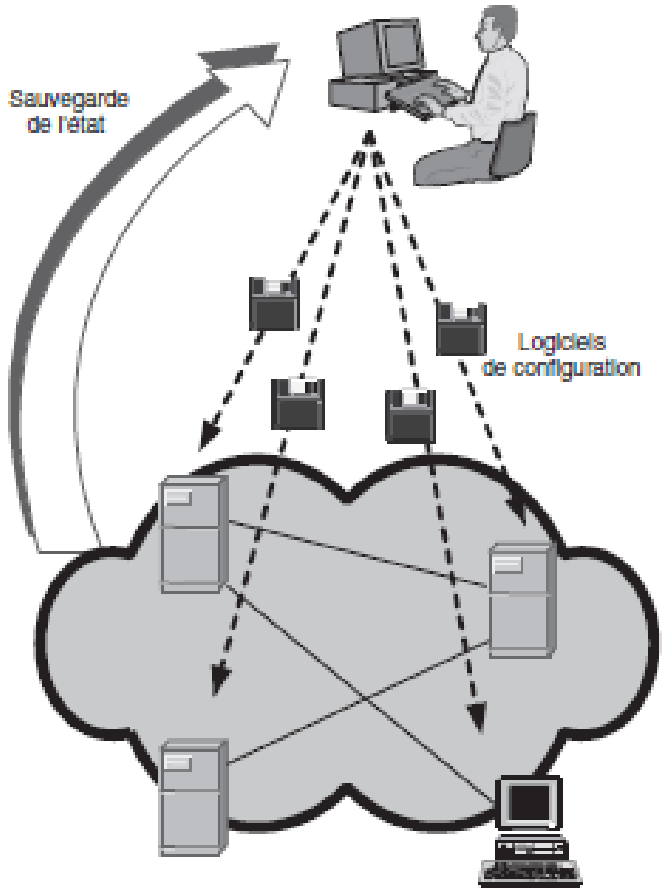


FIGURE 2.1: *La gestion de la configuration*

La gestion de la configuration couvre l'ensemble des fonctionnalités suivantes :

- Démarrage, initialisation des équipements ;
- Positionnement des paramètres ;
- Cueillette des informations d'état et intervention dans les paramètres ;
- Modification de la configuration du système ;
- Association des noms aux objets gérés ;
- Changement de l'adresse IP d'une machine ;
- Changement de l'adresse IP d'un routeur ;
- Changement de la table de routage.

2.3 La gestion des fautes

Comme illustré dans la Figure 2.2, la gestion des **fautes** permet :

1. La **détection** des pannes,
2. La **localisation** des pannes,
3. La **réparation** des pannes,
4. Le **rétablissement** du service.

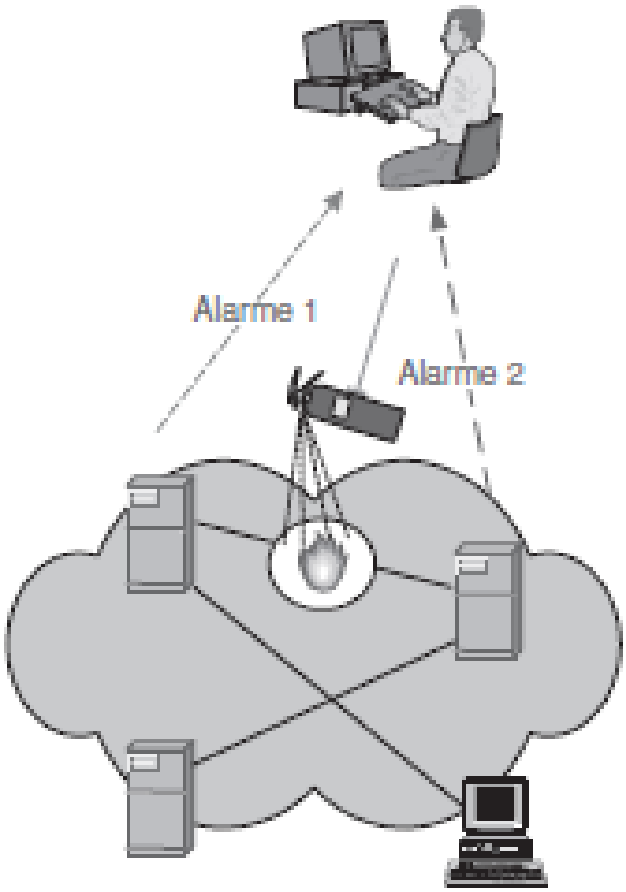


FIGURE 2.2: *La gestion des fautes*

La **gestion des fautes** couvre l'ensemble des fonctionnalités suivantes :

2.3.1 La détection des fautes

Elle comprend la préparation de rapports d'incidents de fonctionnement, la gestion de compteurs ou des seuils d'alarme, le filtrage d'événements par filtrage en amont des informations, l'affichage des dysfonctionnements.

2.3.2 La localisation

On y procède au moyen de rapports d'alarme, de mesures et de tests.

2.3.3 La réparation

Elle consiste à prendre des mesures correctives (réaffectation de ressources, " reroutage ", limitation du trafic par filtrage, maintenance), et à rétablir le service (tests de fonctionnement, gestion de systèmes de secours, etc.).

2.3.4 L'enregistrement des historiques d'incidents et statistiques

la gestion des fautes ne peut se limiter à ces actions ponctuelles, nécessaires mais insuffisantes pour donner le service attendu. C'est la raison pour laquelle elle comporte aussi,

1. D'une part, **l'enregistrement d'historiques d'incidents** et la **compilation de statistiques** qui peuvent porter sur la probabilité des pannes, leur durée, les délais de réparation et,
2. D'autre part, un **rôle d'interface avec les usagers** qui consiste à les informer des problèmes réseau et à leur donner la possibilité de signaler eux-mêmes des incidents tels que :
   - La déconnexion d'un câble ;
   - Une mauvaise configuration d'un équipement ;
   - Une interface défectueuse d'un routeur ;
   - La réinitialisation accidentelle.

2.4 La gestion de la performance

– Comme illustré dans la Figure 2.3, **la gestion de la performance** comprend les procédures de **collecte de données** et d'**analyse statistique** devant aboutir à la production de **tableaux de bord**.

– Elle fournit des fonctions qui permettent à des fins de **planification des ressources** du réseau :

1. de **recueillir** des données statistiques (taux d'erreurs, temps de transit, débit, etc.) ;
2. de **maintenir** et d'**analyser** des journaux sur l'historique de l'état du système (événements).

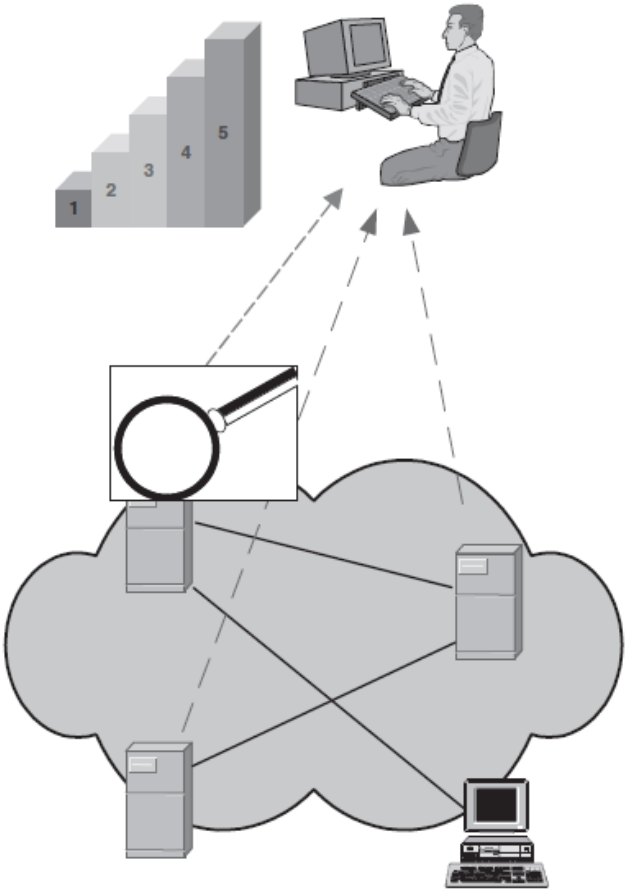


FIGURE 2.3: *La gestion des performances*

- Les informations obtenues (les journaux sur l'état du système) serviront à l'**analyse** et à la **planification** du réseau.
- On peut diviser cette partie en deux : l'une traitant de la gestion de la performance en **temps réel** et l'autre en **temps différé**.
- Pour gérer la performance d'un réseau en temps réel, il faut mettre en place les fonctionnalités suivantes :
  1. Enregistrements des **mesures** de performance ;
  2. **Surveillance** de l'activité du réseau ;
  3. Changement de configuration **proactive** et **réactive**.

2.4.1 L'enregistrements des mesures de performance

Cela passe par :

1. L'établissement et la mise à jour des critères et des conditions de mesure,
2. La gestion de la collecte d'informations,
3. Le filtrage,
4. La compilation de statistiques,
5. L'adoption de mesures à la demande,
6. Ou encore la gestion des fichiers de collecte.

2.4.2 La surveillance de l'activité du réseau

- **Visualisation** de l'utilisation des ressources,
- **Signalement** des dépassements de seuils,
- **Analyse** de la performance.

Cela implique :

- Une visualisation du fonctionnement du réseau (avec comme variables pertinentes par exemple la répartition de la charge, les différents débits, les temps de réponse ou encore la disponibilité),
- et une analyse des causes possibles de dépassement de seuil par corrélation avec les pannes d'équipements, au moyen de divers indicateurs.

2.4.3 Le changement de configuration proactive et réactive

Le fait de gérer la performance en temps réel suppose que l'on soit capable de prendre des mesures **correctives** (ou réactives) et **préventives** (ou proactives).

La gestion réactive :

Elle vise à établir lors de la détection d'un problème de performance des mesures de réaffectation des ressources par modification des paramètres de configuration ou par redistribution du trafic. Ces mesures, de par leurs natures, sont prises afin de répondre à un problème déjà **existant**.

La gestion proactive :

Elle consiste à prendre des mesures initiales permettant d'éviter d'arriver à une situation critique. Cette tâche est effectuée en temps différé et comporte quant à elle un ensemble de sous-tâches :

1. L'analyse des informations par la compilation de statistiques, d'historiques ou encore d'indicateurs de qualité du service ;
2. L'édition de tableaux de bord et de rapports, qu'ils soient périodiques ou qu'ils soient effectués à la demande ;
3. Une certaine forme d'analyse prévisionnelle par la constitution de matrices de trafic, par la détection de risques de saturation ou d'engorgement, par des simulations de scénarios, par le suivi de la gestion corrective, et enfin par la planification et le dimensionnement du réseau.

2.5 La gestion de la comptabilité

– Comme illustré dans la Figure 2.4, la **gestion de la comptabilité** permet de connaître les **charges** des objets gérés, les coûts de communication, etc.
– Cette évaluation est établie en fonction du **volume** et de la **durée** de la transmission.

La gestion de comptabilité couvre l'ensemble des fonctionnalités suivantes :

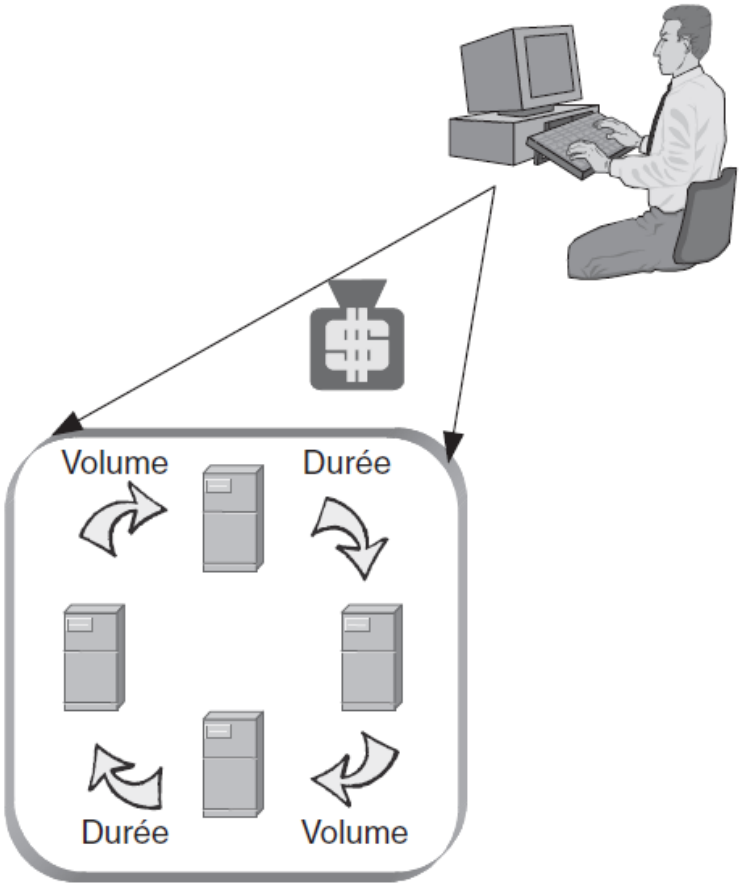


FIGURE 2.4: *La gestion des coûts*

2.5.1 Les mesures sur l'utilisation des ressources

Les **mesures** sur l'utilisation des ressources, et leur **enregistrement** en vue d'obtenir des historiques.

2.5.2 Le contrôle des quotas

Le **contrôle des quotas** par utilisateur en faisant des mises à jour des consommations courantes et en vérifiant les autorisations de consommation.

2.5.3 Le suivi des dépenses

Le **suivi** et le **contrôle** des dépenses par stockage et mise à jour des tarifs des opérateurs, par évaluation en temps réel de la consommation courante, par vérification des

factures, et enfin par suivi des coûts d'exploitation et de matériels (investissement, amortissement et maintenance).

2.5.4 La gestion financière

Bien évidemment, on retrouve dans la gestion comptable une partie financière qui consiste à ventiler les coûts (par service, par utilisateur ou encore par application), à analyser et prévoir les dépenses et enfin à étudier les possibilités de réduction des coûts.

2.5.5 La facturation

Finalement, l'activité de gestion comptable aboutit à une facturation interne, ce qui implique la gestion des clients et des trafics, la production de factures, le contrôle de la facturation et enfin le stockage des historiques.

2.6 La gestion de la sécurité

- Comme illustré dans la Figure 2.5, la **gestion de la sécurité** est une fonction de gestion qui concerne le **contrôle** et la **distribution** des informations utilisées pour la sécurité.
- Elle englobe le **cryptage** et la liste des **droits d'accès**.

Voici les fonctionnalités qui doivent être mises en oeuvre :

2.6.1 La sécurité relative à l'administration de réseau elle-même

Il faut dans un premier temps assurer la **sécurité relative à l'administration de réseau elle-même**, c'est-à-dire :

- Gérer les droits d'accès aux postes de travail,
- Gérer les droits liés aux attentes des opérateurs,
- et enfin les autorisations d'accès aux informations de gestion.

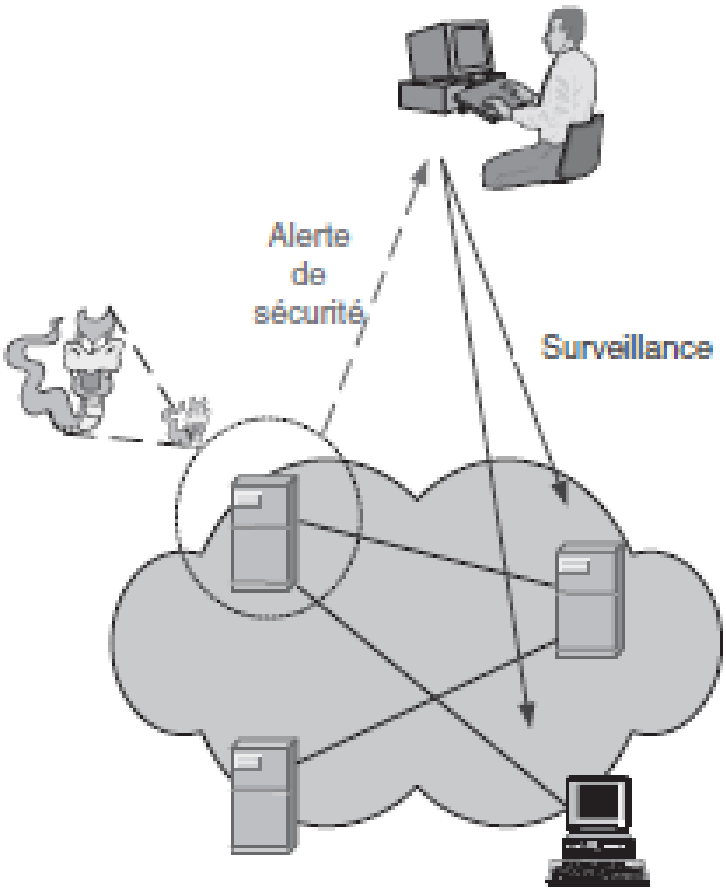


FIGURE 2.5: *La gestion de la sécurité*

2.6.2 La sécurité des accès au réseau géré

Ensuite, il faut garantir la **sécurité des accès au réseau géré** ; pour cela, il faut mettre en place des mécanismes qui impliquent des fonctions telles que :

- La définition des conditions d'utilisation,
- L'activation ou la désactivisation des mécanismes,
- La modification de certains paramètres, ou encore la gestion des listes d'autorisation (aux machines, à différents services ou à divers éléments de réseau),
- Il faut évidemment en outre effectuer un contrôle des accès (identités, horaires, temps de connexion, destination) et une détection des tentatives d'accès frauduleuses (enregistrement, compilation de statistiques et déclenchement d'alarmes si nécessaire).

2.6.3 La sécurité de l'information

Enfin, il faut garantir la **sécurité de l'information** par la gestion de mécanismes de protection, de cryptage et de décryptage, et par la détection d'incidents et de tentatives de fraude.

Chapitre 3

Les environnements d'administration des réseaux

3.1 Introduction et définitions

- Un **environnement d'administration** est un **ensemble d'outils** qui permet de mettre en place les **objectifs de gestion** de l'entreprise.
- Il existe deux catégories d'environnements d'administration : **standards** et **propriétaires**.

    1. Les **environnements propriétaires** sont basés sur des protocoles de communication **non standards** et n'autorisent en général que la gestion des équipements particuliers d'un équipementier (un propriètaire).

    2. En revanche, les **environnements standards** sont basés sur une **architecture ouverte** et des **protocoles standardisés** qui permettent de gérer **tous les équipements** qui mettent en oeuvre des fonctionnalités de gestion standards.

- Dans ce module, nous mettrons l'accent sur les environnements d'administration standards.

3.2 Environnements d'administration standards

- De nombreuses organisations se sont intéressées au problème de la gestion de réseau et de service.
- Il n'est pas possible de les énumérer toutes mais il est important de présenter celles qui ont eu le plus grand impact dans ce domaine.
- Voici sous forme de tableau (3.1) les principaux environnements d'administration disponibles sur le marché :

Environnements de gestion	**Organismes et consortiums initiateurs**
SNMP	**IETF**
TMN/CMIP	**UIT-T** & **ISO**
DMI/CIM/WBEM	**DMTF**
OMA	**OMG** & **TMF**
JMX	**Consortium Java**
DME	**OSF**

TABLE 3.1: *Les environnements d'administration standards*

3.2.1 Organismes et consortium de normalisation

Les organismes et consortiums initiateurs des environnements d'administration des réseaux sont :

3.2.1.1 IETF

Internet **E**ngineering **T**ask **F**orce est un groupe international, ouvert à tout individu, qui participe à l'élaboration des standards Internet. L'IETF produit la plupart des nouveaux standards d'Internet.

3.2.1.2 UIT-T

Union **I**nternationale des **T**élécommunications est chargée de la réglementation et de la planification des télécommunications dans le monde, elle établit les normes de ce secteur

et diffuse toutes les informations techniques nécessaires pour permettre l'exploitation des services mondiaux de télécommunications.

3.2.1.3 ISO

International **S**tandardization **O**rganization ou l'organisation internationale de normalisation est une fédération mondiale d'organismes nationaux de normalisation. Elle a pour but de produire des normes internationales dans les domaines industriels et commerciaux appelées normes ISO.

3.2.1.4 DMTF

Distributed **M**anagement **T**ask **F**orce est une organisation qui développe et maintient des standards pour l'administration de systèmes informatiques d'entreprises ou connectés à internet. Ces standards permettent de développer des composants systèmes d'administration d'infrastructures de telles façon qu'ils soient indépendants de la plateforme et neutres par rapport à la technologie employée.

3.2.1.5 OMG

Object **M**anagement **G**roup est une association américaine dont l'objectif est de standardiser et promouvoir le modèle objet sous toutes ses formes. L'OMG est notamment à la base des standards UML (Unified Modeling Language), CORBA (Common Object Request Broker Architecture), etc.

3.2.1.6 TMF

Telecommunication **M**anagement **F**orum est une association internationale d'entreprises du secteur des télécommunications et du numérique. Elle vise par des programmes de coopération à conduire des recherches, développer de bonnes pratiques et des normes, à définir des API ouvertes, et à faciliter la transition au numérique.

3.2.1.7 Consortium Java

C'est une organisation créée par Sun en 1998. Son but est de coordonner l'évolution du langage Java et des technologies qui lui sont associées.

3.2.1.8 OSF

Open **S**oftware **F**oundation fut une organisation fondée en 1988 en vue de créer un standard ouvert pour une implémentation du système d'exploitation Unix. Il fournit une implémentation de référence (code source) sur laquelle sont basés tous les produits du Distributed Management Environment (DME).

3.2.2 Principaux environnements standards

Les organismes de normalisation et les consortiums internationaux ont proposé plus d'une dizaine de solutions dont les plus populaires sont :

3.2.2.1 SNMP

- **S**imple **N**etwork **M**anagement **P**rotocol est proposé par l'**IETF** en 1988 pour la gestion des réseaux **TCP/IP**.
- SNMP est devenu le protocole de gestion de référence en raison du succès des protocoles de l'IETF (tels que : IP, TCP).
- Cet environnement est actuellement le plus déployé et utilisé.

3.2.2.2 TMN/CMIP

- **T**elecommunication **M**anagement **N**etwork / **C**ommon **M**anagement **I**nformation **P**rotocol sont proposés respectivement par l'**UIT-T** et **l'ISO**.
- L'architecture TMN et le protocole CMIP constituent la norme dans le domaine de la gestion de **réseau de télécommunication**.
- CMIP présente une version améliorée de SNMP tandis que TMN introduit un cadre de travail pour planifier, installer, maintenir, utiliser et administrer un réseau de télécommunication et les services associés.

– La complexité de ces deux entités a été un frein à leur expansion dans les petits réseaux et ils sont quasi exclusivement utilisés dans les réseaux opérateurs.

3.2.2.3 DMI/CIM/WBEM

– Ils sont proposés par les fabricants des **postes de travail** et des **serveurs**, et ils sont regroupés dans le consortium **DMTF**.
– Leur objectif est de pousser les aspects d'administration des réseaux jusqu'aux postes de travail et des serveurs incluant ainsi tous les éléments du système d'information de l'entreprise.
– Différents environnements ont été proposés :
  – **DMI** (**D**esktop **M**anagement **I**nterface),
  – **CIM** (**C**ommon **I**nformation **M**odel),
  – **WBEM** (**W**eb-**B**ased **E**nterprise **M**anagement).

DMI :

– Il fournit un Framework logiciel standard afin de gérer et de suivre les modifications de composants sur un ordinateur, qu'il soit un ordinateur portable, un ordinateur de bureau, ou un serveur.
– Pour les dispositifs gérés, DMI fait abstraction des logiciels qui les gèrent.
– Avant l'introduction de DMI, il n'existait aucune source d'information standardisée qui puisse fournir le détail des composants d'un ordinateur.

CIM :

– **CIM** est un standard ouvert qui définit comment des éléments administrés dans un environnement informatique peuvent être représentés sous forme d'un ensemble d'objets cohérents et d'un ensemble de relations entre ces objets.
– Le but du CIM est d'avoir une administration système cohérente et unifiée des éléments gérés, et cela de façon totalement indépendante de leurs fabricants ou fournisseurs.

WBEM :

- C'est un ensemble de techniques et de standards Internet de gestion servant à unifier la gestion des environnements d'informatique distribuée.
- WBEM s'appuie sur des standards Internet et sur les standards ouverts publiés par l'organisme DMTF.

3.2.2.4 DME

- **D**istributed **M**anagement **E**nvironment est proposé par les fabricants de logiciels regroupés dans l'**OSF** (**O**pen **S**oftware **F**oundation).
- Cette architecture dite DME est orientée vers la gestion exclusive des postes Unix.
- Elle ne prend pas en compte la gestion des équipements réseaux.

3.2.2.5 OMA

- **O**bject **M**anagement **A**rchitecture est proposée par le consortium **OMG**.
- Il s'agit d'une architecture d'administration orientée objets distribués.
- Elle est basée sur **CORBA** (**C**ommon **O**bjet **R**equest **B**roker **A**rchitecture).
- Elle se propose d'apporter une solution de gestion distribuée intégrant les différentes approches suscitées.

3.2.2.6 JMX

- **J**ava **M**anagement e**X**tensions est proposée par le **consortium Java**.
- Il s'agit d'un ensemble de spécifications et d'**API** (**A**pplication **P**rogramming **I**nterface) pour l'administration de réseau, faisant partie de la solution **J2EE** (**J**ava **E**nterprise **E**dition).
- Elle se propose également de fournir une solution unifiée par rapport aux solutions SNMP/TMN/WEBM.

3.3 Conception d'un environnement d'administration

- La **conception** d'un environnement d'administration de réseau est le **processus** qui permet d'aboutir à une solution **architecturale** et **technologique** du système d'administration.
- Cela suppose impérativement une grande rigueur dans les choix qui président à la réalisation d'un tel environnement afin d'éviter des échecs en termes de réalisation des objectifs et/ou des coûts.
- Il est donc extrêmement important de définir une **démarche** sur laquelle les administrateurs de réseau pourront s'appuyer pour faire les bons choix architecturaux et technologiques qui répondent aux besoins de l'entreprise.
- La démarche proposée passe par l'**identification** préalable des besoins, puis la **détermination** et la **sélection** des services nécessaires, un **choix technologique** de plate-forme et enfin l'**établissement** d'une formule d'exploitation.
- Ce processus qui comporte cinq étapes est décrit dans la Figure 3.1. Pour pouvoir effectuer ces différentes étapes, l'administrateur réseau doit acquérir un savoir-faire qui lui permette de maîtriser la technologie, de savoir dans quels cas il convient de l'utiliser, et enfin pour être à même de faire des choix optimaux en termes d'outils et de plates-formes pour mettre en place sa solution.

3.4 Elements de réseaux Vs Environnements d'administration

- L'**administration de réseau** consiste à gérer à distance les éléments de réseau.
- Pour cela, il est nécessaire d'associer aux éléments du réseau l'environnement d'administration qui est capable de les gérer à distance.
- À titre d'exemple, les **concentrateurs Ethernet** et les **routeurs** peuvent généralement être gérés par l'environnement de gestion **SNMP**.
- De même que l'administration des équipements d'interconnexion de réseau, il est possible de gérer des **serveurs**, des **bases de données** ou des **applications**.

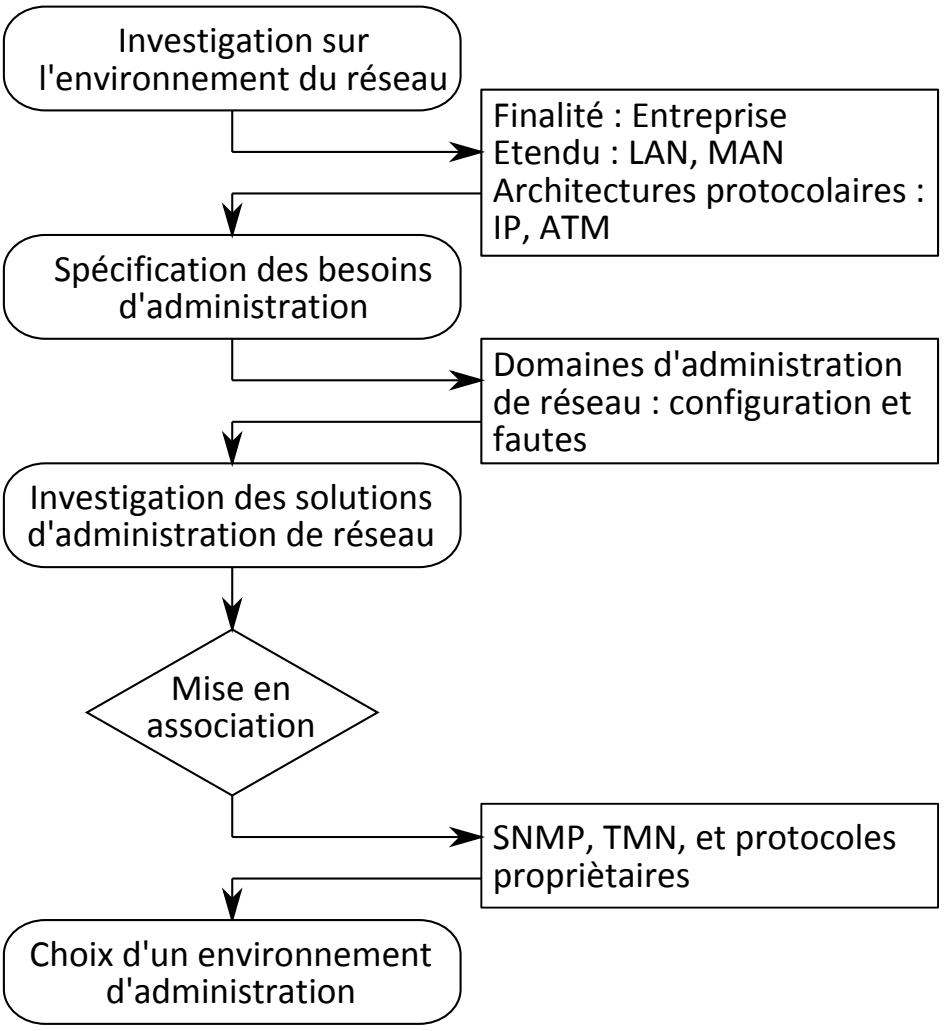


FIGURE 3.1: *Choix d'un environnement d'administration*

- En pratique, l'environnement d'administration **SNMP** peut gérer tout équipement connecté au réseau qui dispose d'un **processus**, dénommé **agent SNMP**, capable d'exécuter les **fonctions de surveillance**.
- La plupart des équipements connectés au réseau supportent un **agent SNMP** et peuvent être **administrés à distance**.
- Ces équipements vont être décrits par un **ensemble de variables** qui représente leur **état**, ainsi que leurs **paramètres de configuration**.
- Néanmoins, certains équipements ne disposent pas nécessairement de cet agent SNMP mais peuvent être dotés d'autres types d'agents (Agent Q3) voire d'aucun agent.

- Dans ce dernier cas, il n'est pas aisé de gérer ces équipements ; à titre d'exemple, la grande majorité des concentrateurs passifs (hubs passifs) ne peut être gérée à distance.
- Il est donc impératif dans un premier temps que l'administrateur de réseau puisse identifier ses équipements et déterminer s'ils peuvent être gérés ou pas.

Nous donnons dans la liste présentée ci-après un aperçu des composants logiciels et matériels qui sont généralement gérables ou non.

- Les modems **ne disposent que très rarement** d'agents SNMP.
- Les concentrateurs (hubs) passifs **ne disposent pas** d'agents SNMP **en général**.
- Les commutateurs (switchs) et les concentrateurs actifs **disposent plus souvent** d'agents SNMP.
- Les ponts (bridge) **disposent généralement** d'agents SNMP.
- Les routeurs **disposent dans leur majorité** d'agents SNMP.
- Les multiplexeurs **ne disposeront que très rarement** d'agents SNMP.
- Les passerelles (gateways) **disposent pour la plupart** d'agents SNMP.
- Les autocommutateurs téléphoniques **disposent dans leur majorité** d'agents de gestion TMN.
- Les commutateurs optiques **disposent dans leur majorité** d'agents TMN.
- Les serveurs **disposent généralement** d'agents SNMP mais on les gère principalement via l'environnement OSF dans le cas d'Unix.
- Certaines applications telles que les bases de données **disposent de leur propre** agent SNMP.

Une fois que les **caractéristiques des équipements** ont été identifiées, il est nécessaire de mettre **en association** les **types d'équipement** et **les environnements d'administration** qui peuvent les gérer (voir Tableau 3.2).

Environnements de gestion	SNMP	TMN/CMIP	DMI/CIM/WBEM
Les modems	×		
Les commutateurs	×		
Les ponts (bridge)	×		
Les routeurs	×		
Les multiplexeurs	×		
Les passerelles (gateways)	×		×
Les autocommutateurs téléphoniques		×	
Les commutateurs optiques		×	
Les serveurs			×
Les applications	×		×
Les postes de travail			×

TABLE 3.2: *Mise en association éléments réseaux & environnements d'administration*

3.5 Architectures technologiques Vs Environnements d'administration

- Avant de choisir un environnement d'administration, on doit être capable de reconnaître les architectures technologiques du réseau que l'on veut gérer.
- Tous les environnements d'administration ne gèrent pas tous les types d'architecture technologique.
- On associe alors les environnements de gestion aux architectures technologiques.
- Le tableau (3.3) ci-après montre les différentes associations entre les environnements d'administration et les architectures technologiques.
- L'**environnement d'administration SNMP** est utilisé dans la majorité des cas avec l'**architecture IP**, en raison de la popularité des protocoles IP.
- L'**environnement d'administration TMN** est majoritairement utilisé avec l'architecture **Sonet**, le réseau voix **PSTN** (**P**ublic **S**ervice **T**elephony network pour réseau téléphonique public commuté) ainsi que l'architecture **ATM**.

Environnements de gestion	**SNMP**	**TMN/CMIP**	**Propriétaires**
Architecture IP	×		×
Architecture ATM	×	×	×
Architecture Frame Relay	×		×
Architecture X.25		×	×
Architecture Sonet		×	×
Réseau téléphonique		×	×
Architecture IPX	×		×

TABLE 3.3: *Mise en association architecture technologique & environnements d'administration*

Chapitre 4

L'environnement d'administration SNMP

4.1 Introduction

- **SNMP** est un protocole de la famille **TCP/IP**, et peut donc être utilisé sur tous les réseaux de type **Internet**.
- Il exploite les capacités du protocole de transport **UDP**, à savoir :
  1. Chaque trame possède une **adresse source** et une **adresse destination** qui permettent aux protocoles de niveaux supérieurs comme SNMP de pouvoir adresser leurs requêtes.
  2. Le protocole UDP peut utiliser un **checksum optionnel** qui couvre l'en-tête et les données de la trame. En cas d'erreur, la trame UDP reçue est ignorée.
  3. Le protocole UDP fonctionne **en mode non connecté**, c'est-à-dire qu'il n'existe pas de **lien persistant** entre la **station d'administration** et l'**agent administré**. Cela oblige les deux parties à s'assurer que leurs messages sont bien arrivés à destination.
- Deux ports sont désignés pour l'utilisation de SNMP, à savoir :
  1. **Port 161** pour les **requêtes** à un **agent SNMP**.

2. **Port 162** pour l'écoute des **alarmes** destinées à la **station d'administration**.

4.2 Principe de fonctionnement

- Le protocole SNMP se base sur le fait qu'il existe une **station de gestion** réseau, le **manageur**, dont le rôle est de **contrôler** le réseau et de **communiquer** via ce protocole avec un **agent**.
- L'**agent** est de manière générale une **interface SNMP** embarquée sur le matériel destiné à être administré à distance.
- La Figure 4.1 illustre le principe de fonctionnement du protocole SNMP.

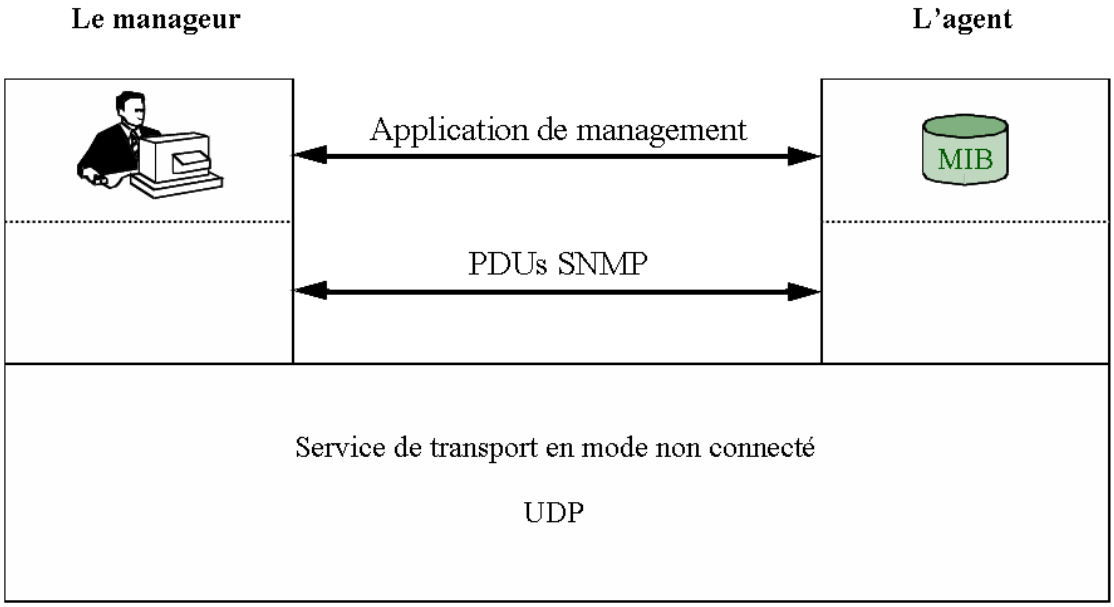


FIGURE 4.1: *Principe de fonctionnement SNMP.*

Comme illustré dans la Figure 4.2, le protocole SNMP est constitué de **plusieurs commandes différentes**. Dans les sous-sections suivantes, nous citons et définissons les principales commandes SNMP.

4.2.1 La commande Get

Cette commande, envoyée par le manageur à l'agent, a pour objectif de **demander une information** à l'agent. Celui-ci, dans le cas où la validité de la requête est confirmée,

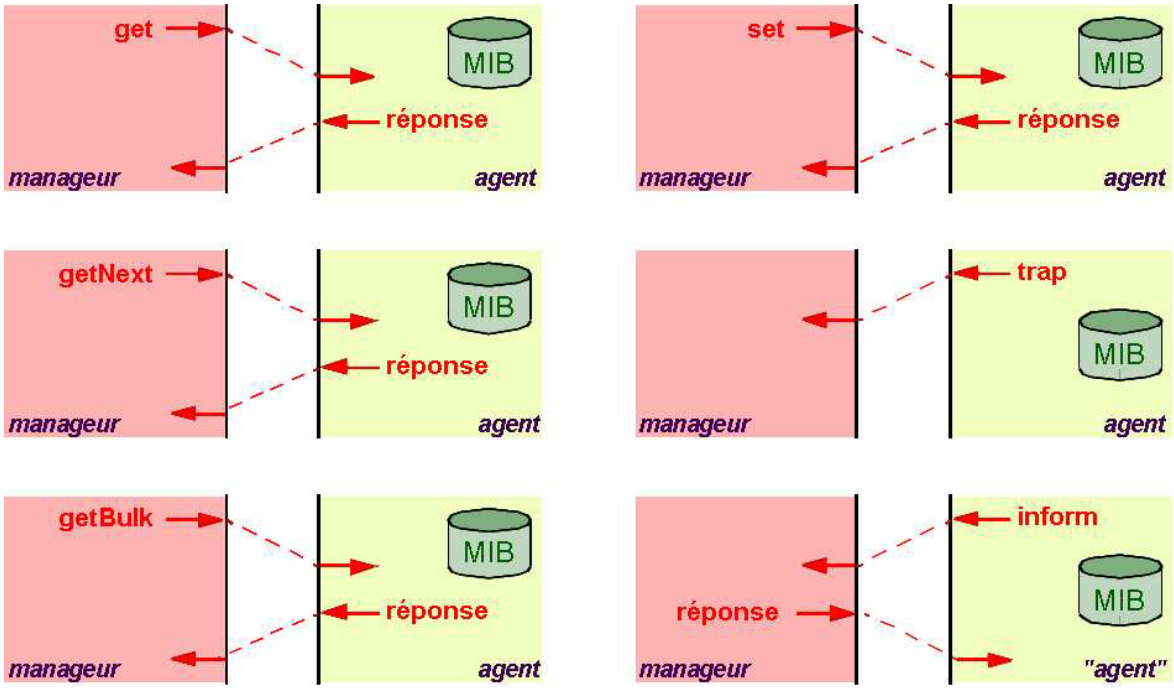


FIGURE 4.2: *Illustration des commandes SNMP.*

renvoie au manageur la **valeur** correspondant à l'information demandée.

4.2.2 La commande Getnext

Cette commande, envoyée par le manageur à l'agent, a pour objectif de **demander l'information suivante** à l'agent : il arrive qu'il soit nécessaire de parcourir toute une liste de variables de l'agent. On utilise alors cette commande, à la suite d'une requête **get**, afin d'obtenir directement le **contenu de la variable suivante**.

4.2.3 La commande Getbulk

Cette commande est envoyée par la manageur à l'agent pour **connaître la valeur de plusieurs variables** : cela évite d'effectuer plusieurs requêtes **Get** en série, améliorant ainsi les performances (implémenté dans SNMPv2).

4.2.4 La commande Set

Cette commande, envoyée par le manageur à l'agent, a pour objectif de **définir la valeur d'une variable** de l'agent administré. Cela permet d'effectuer des modifications sur le matériel.

4.2.5 La commande Trap

Lorsqu'un **événement particulier survient** chez l'agent (connexion, modification de la valeur d'une variable donnée, etc.), celui-ci est susceptible d'envoyer ce que l'on appelle une **Trap**, à savoir un message d'information destiné à la station d'administration : celle-ci pourra alors la traiter et éventuellement agir en conséquence. S'il s'agit par exemple de la coupure d'un lien réseau, cela permet à l'administrateur réseau d'en être immédiatement informé.

4.2.6 La commande Inform

Dans certains cas, il peut être intéressant pour l'agent d'**obtenir une réponse à une Trap** qu'il a émise, afin d'obtenir confirmation que celle-ci a bien été reçue et analysée : c'est l'objectif d'une commande **Inform**. (Implémenté dans SNMPv2).

4.3 Variables SNMP et le modèle SMI

- L'**objectif** de SNMP est donc d'**obtenir** ou de **modifier** la valeur d'une ou plusieurs **variables du matériel** : Il peut s'agir par exemple de l'état d'une interface réseau (allumé/éteint).
- Les **variables** SNMP exploitent le modèle **SMI** (**S**tructure of **M**anagement **I**nformation) qui définit un **modèle hiérarchique des variables**.
- Dans ce modèle, les **variables** sont répertoriées dans une **hiérarchie d'objets**.
- Chaque **objet** est identifié par ce que l'on appelle un **OID** (**O**bject **ID**entifier).
- La hiérarchie de ces objets se représente sous la forme d'un **arbre**.
- Les **branches** constituent les différents **OIDs** et les **feuilles** les **variables**.

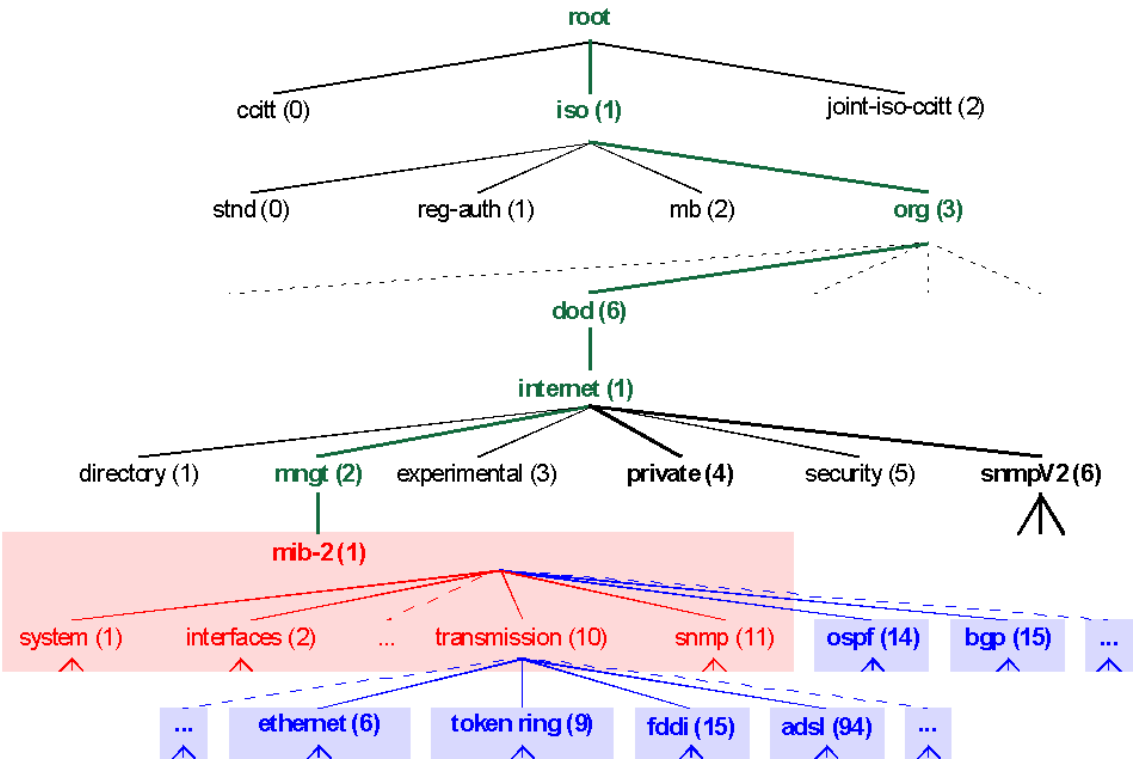


FIGURE 4.3: *Arborescence des OIDs en SNMP.*

- Une variable peut donc être référencée par la **liste ordonnée des différents OIDs** parcourus à partir de la racine de l'arbre.
- Le modèle SMI définit également les **types de données** utilisables pour les variables : entier, réel, durée, compteur, etc.
- **Un ensemble d'objets** d'un **même module** est appelé une **MIB** (**M**odule **I**nformation **B**ases).
- Il s'agit d'une base de données référençant la liste des **objets** et des **variables** associées, des **types de données** utilisés pour chaque variable et d'un **descriptif** de cette variable.
- La base contient éventuellement des **types de données personnalisés**.
- La Figure 4.3 présente l'arborescence des **OIDs**, constituant les **MIBs**. En SNMP, on utilise communément deux branches :

  1. **iso.org.dod.internet.mngt.mib-2** (**1.3.6.1.2.1**) : il s'agit de la branche contenant tous les **objets standards**, définis précisément dans les RFC. Ainsi, **tout agent SNMP** doit pouvoir **reconnaître** cette branche et les variables qui y

sont définies.

2. **iso.org.dod.internet.private.enterprises** (**1.3.6.1.4.1**) : cette branche est l'origine de tous les **objets propres** au matériel et définis par le constructeur. Ainsi, chaque constructeur se voit attribué un **identifiant** (VendorID), qui lui fournit un **espace de données** au sein de l'arbre des MIBs. Si nous prenons l'exemple de **Cisco**, dont l'identifiant est **9**, toutes les variables propres à Cisco ont une clé débutant par **1.3.6.1.4.1.9**.

4.4 Fichiers MIBs

- Les **fichiers MIBs** décrivent précisément **chaque chiffre** (**OID**) de la liste identifiant une **variable** (la clé), et sa signification.
- Prenons l'exemple simple de la variable contenant le **nom du matériel interrogé**.
- Il s'agit d'une **propriété** de l'objet standard "**system**" que nous pouvons voir dans l'arborescence donnée précédemment.
- La propriété s'appelle "**sysName**". On en déduit que la variable s'appelle alors : **iso.org.dod.internet.mngt.mib-2.system.sysName**.
- Analysons le fichier MIB décrivant l'objet " system " (RFC 1213). Le fichier fournit toutes les informations relatives à la propriété "**sysName**" (voir Figure 4.4) :
  1. **Syntaxe** : il s'agit d'une chaîne de caractères de taille variant entre 0 et 255.
  2. **Accès** : l'accès à cette variable se fait en lecture ou en écriture.
  3. **Etat** : cette variable existe et est toujours utilisable.
  4. **Description** : il s'agit du nom complet du noeud.
  5. **Sa place dans l'arborescence** : **5ième** propriété de l'objet "**system**" : On en déduit que cette variable a pour clé la valeur **1.3.6.1.2.1.1.5**.
- Ainsi, nous avons la **description** de toutes les variables, leur **méthode d'accès** et la **clé** que nous devons utiliser pour lire ou écrire sa valeur.
- La majorité des constructeurs fournit des fichiers MIBs contenant des informations sur les variables propres à leur matériel, ne faisant pas partie des informations standards.

– Il existe un grand nombre d'outils permettant de visualiser l'arbre des MIBs et de rechercher une variable au sein de celui-ci. L'exemple de la Figure 4.5 est tiré du site **www.snmplink.org**.

```
sysName OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION
            "An administratively-assigned name for this
            managed node.  By convention, this is the node's
            fully-qualified domain name."
    ::= { system 5 }
```

FIGURE 4.4: *La propriété SysName de l'objet sytem.*

4.5 Sécurité

– Sous **SNMPv1** et **SNMPv2**, la sécurité est assurée par deux choses :

1. Dans sa requête, il faut envoyer une **chaîne de communauté**, qui correspond en quelque sorte à un mot de passe, et dont les droits varient suivant cette chaîne : il est ainsi possible d'autoriser certaines personnes un accès en lecture seule, et à d'autres personnes un accès complet suivant la communauté qu'ils utilisent.
2. L'agent peut vérifier et contrôler l'origine des données, afin de vérifier que la personne en question a accès aux informations. Il s'agit généralement d'une vérification basée sur l'**adresse IP source**.

– Nous constatons toutefois que la sécurité est particulièrement lacunaire pour deux raisons : le contenu de la transaction n'est pas crypté, et il suffit que la communauté soit connue de n'importe qui pour que cette personne puisse lire les informations.

– Ces différents problèmes ont été résolus dans **SNMPv3**. En effet, celui-ci propose plusieurs modèles de sécurités différents :

1. Le premier modèle est dépourvu de sécurités et est comparable à SNMPv1/v2.

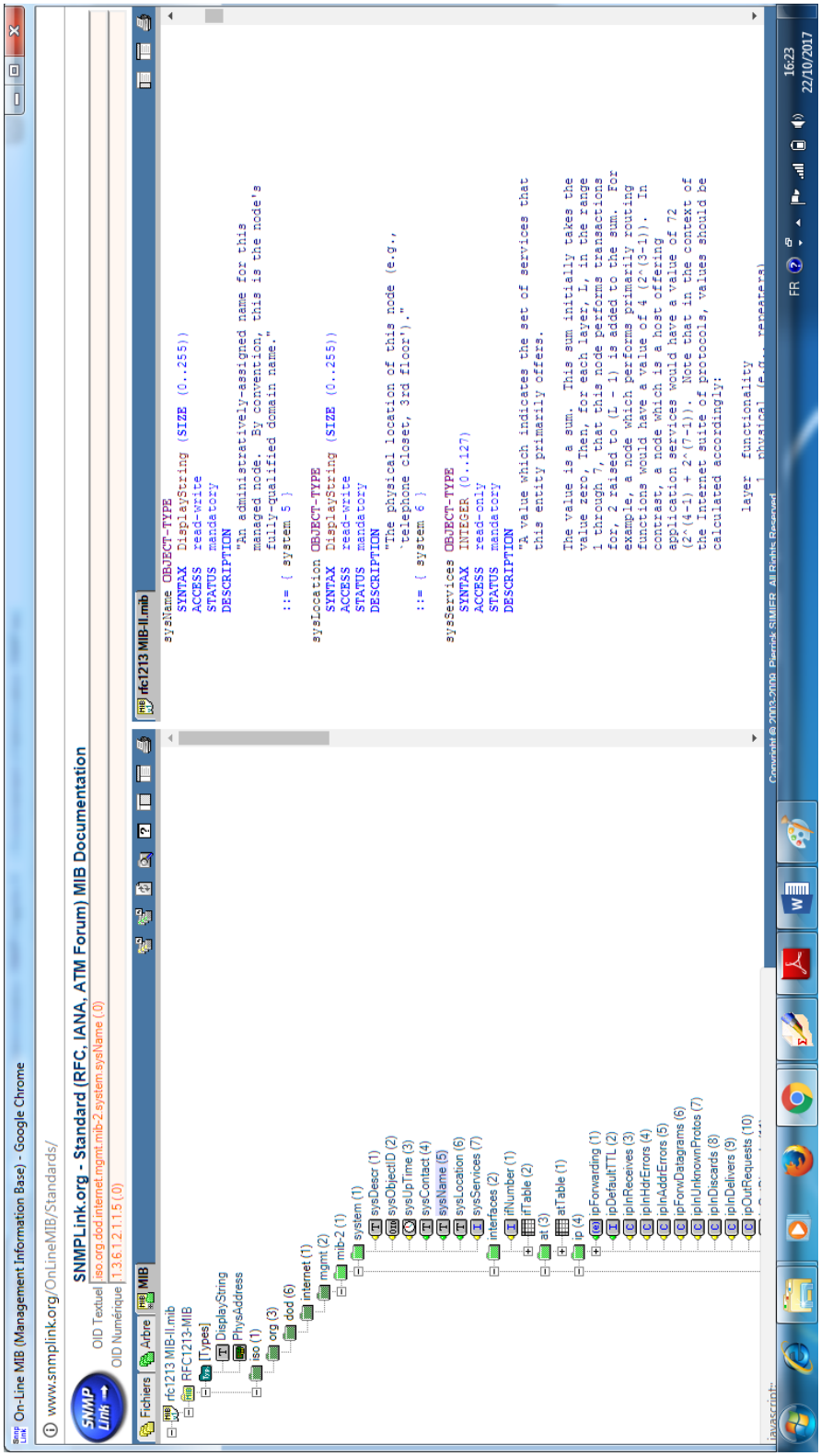


FIGURE 4.5: *Explorateur de MIBs.*

2. Le second modèle offre des capacités d'authentification par utilisateur, c'est-à-dire que chaque utilisateur dispose d'un mot de passe d'accès, ainsi que d'une clé de cryptage permettant de sécuriser le contenu de la transaction.
3. Le troisième modèle ajoute au précédent un niveau de cryptage supplémentaire en utilisant le principe d'échange des clés : le contenu des paquets est ainsi totalement crypté mais ce modèle n'est applicable.

– Lorsqu'une commande est expédiée à un agent, on attend de celui-ci une réponse. Plusieurs cas peuvent se produire :

1. **Aucune réponse** (Temps d'attente dépassé),
2. **Erreur dans la requête**,
3. **La requête a réussi**.

Aucune réponse :

Plusieurs cas sont susceptibles de produire une absence de réponse de la part du matériel interrogé :

1. SNMP est basé sur UDP et il peut arriver que les paquets n'arrivent pas à destination. Dans ce cas, le temps d'attente de réponse finit par s'écouler et il convient alors de réémettre la requête.
2. Suivant l'implémentation des agents et la version de SNMP utilisée, si l'authentification échoue (mauvaise communauté, mot de passe incorrect), l'agent peut ne pas répondre à la requête.
3. Le temps d'attente de réponse peut être paramétré dynamiquement et il est possible que le temps défini soit trop court pour permettre à la réponse de revenir.
4. Enfin, dans le pire des cas, il est possible qu'il n'y ait pas d'agent SNMP disponible sur le matériel interrogé. Nous ne pouvons en conséquence avoir de réponse à notre requête.

Erreur :

Plusieurs cas sont susceptibles de conduire au renvoi d'une erreur :

1. Lorsque l'on essaie d'écrire sur une variable en lecture seule.
2. Lorsque l'on essaie de définir la valeur d'une variable avec un type de données incorrect (si l'on essaie d'écrire une chaîne de caractères dans une variable de type entier par exemple).
3. Lorsque la variable n'existe pas.
4. Lorsque la trame SNMP est incorrecte (corruption, longueur non valide, etc.).
5. Lorsque l'authentification SNMPv3 a échoué.

Réussite :

Lorsque la requête à l'agent SNMP réussit, celui-ci nous envoie la valeur de la variable à laquelle on a accédé (que ce soit en lecture ou en écriture).

Deuxième partie

Pratique

Chapitre 5

Configuration de base et outils d'accès à distance

5.1 L'énoncé du TP

- Le but de ce TP est d'apprendre les bonnes pratiques à suivre pour effectuer la configuration de base d'un équipement d'interconnexion réseau CISCO, ainsi que les outils d'accès à distance (TELNET et SSH) à ce dernier.
- Pour cela, nous proposons la topologie de réseau représentée par la Figure 5.1. Il s'agit deux réseaux LANs interconnectés par un routeur.
- Les tâches demandées sont les suivantes :

  1. Sécuriser le port console de chacun des équipements du réseau.
  2. Sécuriser le mode d'exécution ENABLE sur chacun des équipements du réseau.
  3. Sécuriser les lignes virtuelles de chacun des équipements du réseau.
  4. Attribuer un nom à chacun des équipements du réseau.
  5. Configurer l'adressage IP de chacun des équipements du réseau.
  6. Configurer les outils d'accès à distance sur chacun des équipements du réseau.
  7. Configurer une bannière sur chacun des équipements du réseau.

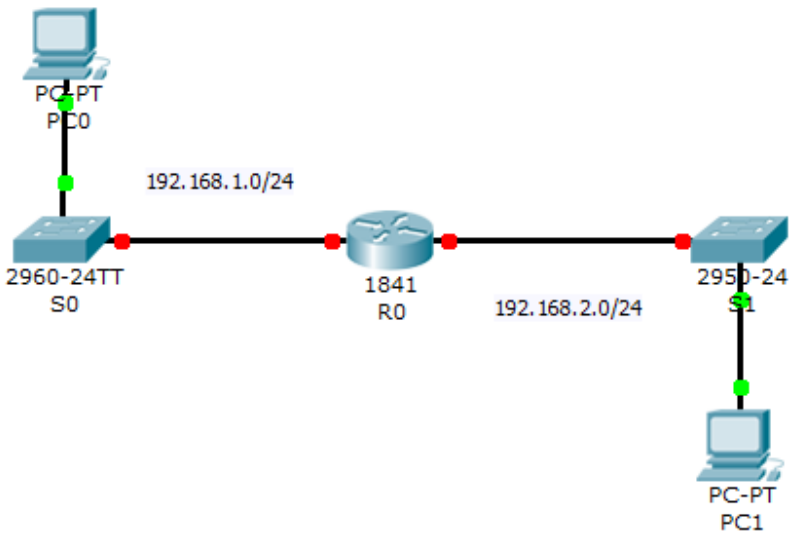


FIGURE 5.1: *TP 1 : Topologie du réseau.*

5.2 Les étapes de configuration

- La configuration de base d'un équipement d'interconnexion réseau CISCO concerne généralement des équipements vierges qui n'ont jamais été utilisés ou qui viennent juste d'être achetés.
- Ces équipements ne contiennent que des configurations par défaut, et par conséquent ils ne peuvent pas être déployés tels quels.
- La configuration de base consiste donc à paramétrer les objets importants de ces équipements de telle façon à ce qu'ils soient prêts pour être installés dans des armoires de brassage.
- Pour effectuer la configuration de base d'un équipement CISCO, l'utilisation d'un câble console pour relier ce dernier directement avec la machine d'administration est inévitable.
- Une fois la configuration de base est effectuée grâce à un câble console, l'équipement en question peut désormais être installé dans l'endroit prévu. Dorénavant, tout changement de configuration devrait être fait à distance grâce entre autres aux outils d'accès à distance TELNET et SSH.

– Pour effectuer la configuration de base, on procède comme suivant :

5.2.1 Sécurisation du port console d'un équipement CISCO

– Le port console d'un équipement CISCO sert à relier directement ce dernier à une station d'administration en utilisant un câble console pour effectuer sa configuration de base.

– Donc, il est très important de sécuriser le port console d'un équipement CISCO pour empêcher tout accès à ce dernier, évidemment lorsqu'il est définitivement installé dans une armoire de brassage.

– Pour sécuriser le port console, on peut procéder de deux façons : elles sont données respectivement dans les Figures 5.2 et 5.3.

```
Switch>enable
Switch#conf
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#li
Switch(config)#line co
Switch(config)#line console 0
Switch(config-line)#pass
Switch(config-line)#password cisco
Switch(config-line)#logi
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#cop
Switch#copy r
Switch#copy running-config s
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

FIGURE 5.2: *TP 1 : Sécurisation du port console (façon 1).*

5.2.2 Sécurisation du mode ENABLE d'un équipement CISCO

– Contrairement au mode d'exécution USER (représenté par le symbole >) qui est une CLI (Command Line Interface) qui ne permet d'afficher que certaines informations ordinaires sur un équipement CISCO, le mode d'exécution ENABLE (dit également PRIVILEGED, il est représenté par le symbole #) est une CLI dédiée

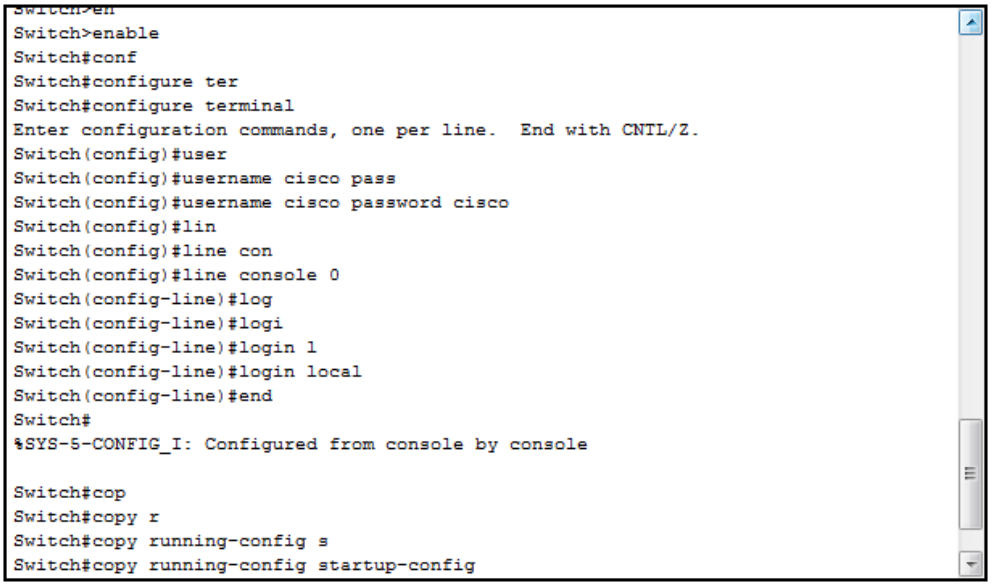


FIGURE 5.3: *TP 1 : Sécurisation du port console (façon 2).*

à l'administrateur réseau qui lui accorde des privilèges étendus sur l'équipement administré.

- Par ailleur, Le mode ENABLE sert d'un portail pour accéder à l'ensemble des modes de configuration de l'équipement CISCO géré. D'où la nécessité absolue de devoir sécuriser cette CLI pour empêcher tout affichage d'informations critiques ou tout changement de configuration de l'équipement administré.
- Pour sécuriser le mode ENABLE, on peut procéder de deux façons : elles sont données respectivement dans les Figures 5.4 et 5.5.
- La Figure 5.5 montre que la façon 2 de configurer la sécurité du mode ENABLE permet de chiffrer le mot de passe, alors que le façon 1 le laisse en clair.

5.2.3 Sécurisation des lignes virtuelles d'un équipement CISCO

- Les lignes virtuelles d'un équipements CISCO servent une fois la configuration de base est effectuée à administrer à distance ce dernier.
- Le nombre de lignes virtuelles d'un équipement CISCO représente le nombre d'accès simultané que peut supporté ce dernier. Ce nombre diffère d'un équipement à un autre, par exemple : les commutateurs sont dotés généralement de 16 lignes virtuelles

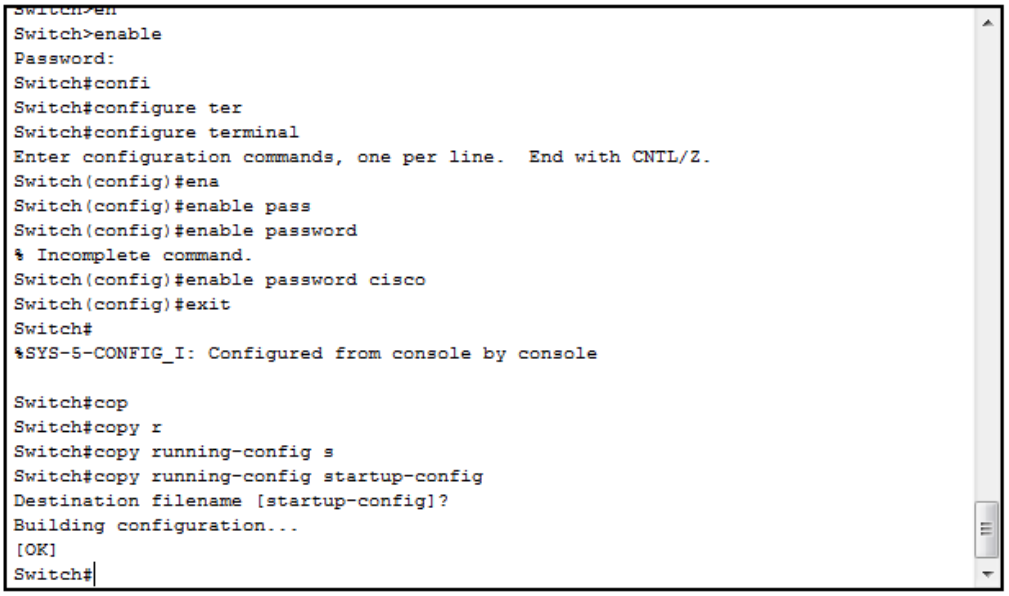


FIGURE 5.4: *TP 1 : Sécurisation du mode ENABLE (façon 1).*

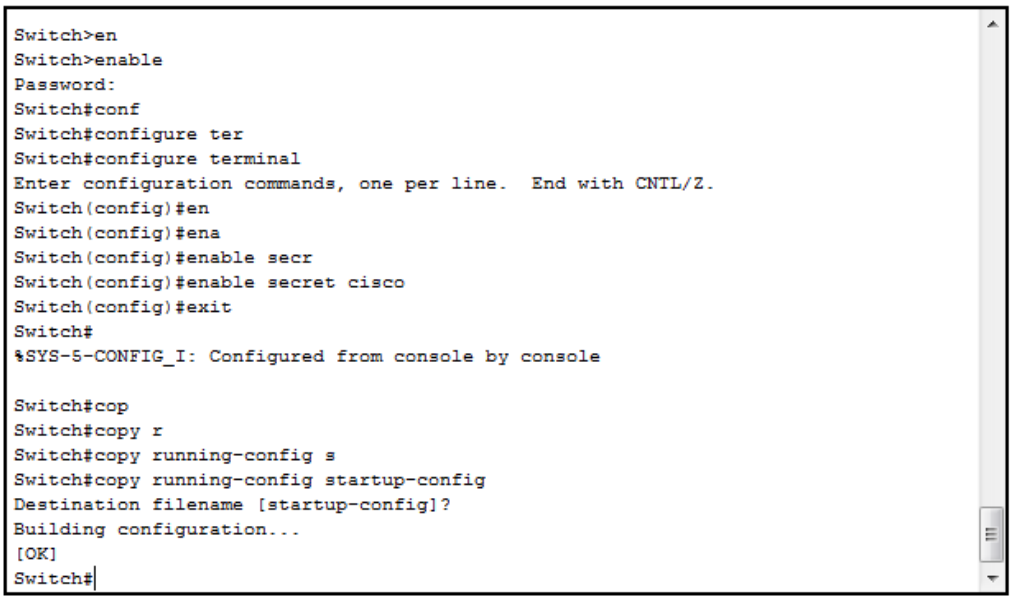


FIGURE 5.5: *TP 1 : Sécurisation du mode ENABLE (façon 2).*

(de 0 à 15), alors que les routeurs ne possèdent généralement que 5 (de 0 à 4).

– Avant qu'un équipement CISCO soit déployé, il es primordiale voire obligatoire de sécuriser ses lignes virtuelles afin d'empêcher tout accès non autorisé à distance.

– Pour sécuriser les lignes virtuelles, on peut procéder de deux façons : elles sont données respectivement dans les Figures 5.7 et 5.8.

FIGURE 5.6: *TP 1 : Sécurisation du mode ENABLE (différence entre façon 1 et façon 2).*

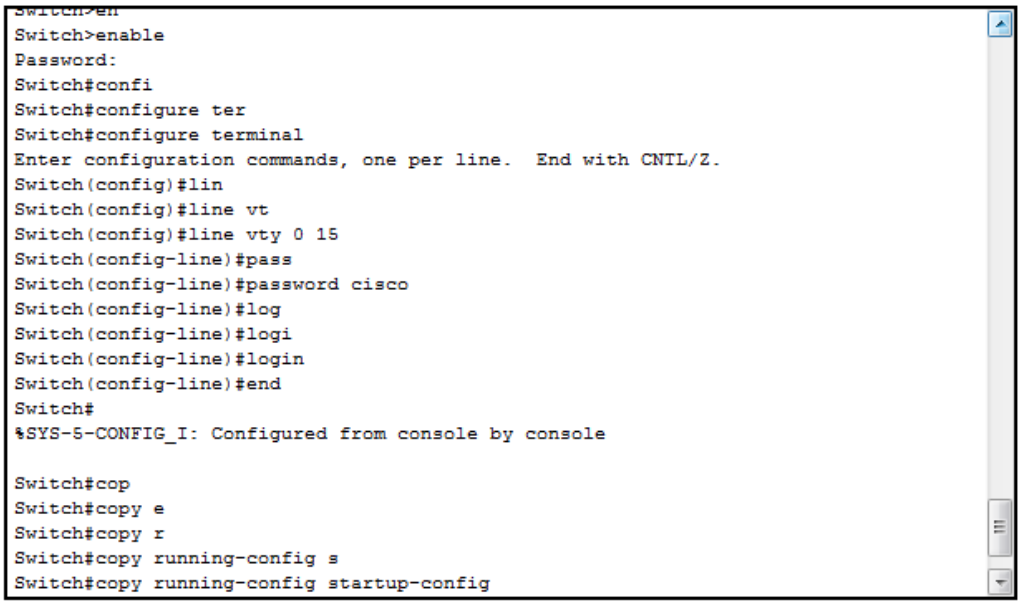


FIGURE 5.7: *TP 1 : Sécurisation des lignes virtuelles (façon 1).*

5.2.4 Attribution d'un nom à un équipement CISCO

– L'attribution d'un nom à un équipement semble être une configuration banale. Or, désigner de façon unique et significative les équipements d'interconnexion d'un réseau contribue énormément à administrer efficacement le réseau en question (no-

```
User Access Verification

Password:

Switch>en
Switch>enable
Password:
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#username cisco password cisco
Switch(config)#line vty 0 15
Switch(config-line)#login local
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy r
Switch#copy running-config s
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

FIGURE 5.8: *TP 1 : Sécurisation des lignes virtuelles (façon 2).*

tamment, réduire le temps de localisation d'une panne réseau).

- En effet, bien que les équipements réseau peuvent être identifiés grâce à leurs adresses IP, des noms uniques et significatifs sont aussi importants car ils sont facilement mémorables. Par ailleurs, certaines configurations avancées des équipements CISCO requièrent obligatoirement un nom de l'équipement pour qu'elles soient effectuées.
- La Figure 5.9 montre comment attribuer un nom à équipement CISCO.

5.2.5 Attribution d'une adresse IP à un équipement CISCO

- L'attribution des adresses IP aux équipements réseau est certainement la tâche la plus élémentaire et la plus fondamentale dans la configuration de base de ces derniers.
- Dans ce TP, nous nous focalisons sur la configuration IP de deux types d'équipements : commutateurs et routeurs. Pour cela, dans ce qui suit, nous expliquerons comment effectuer la configuration IP des équipements du réseau 192.168.1.0/24.
- Les Figures 5.10 et 5.11 montrent respectivement comment effectuer la configuration IP d'un commutateur et d'un routeur.
- Les bonnes pratiques stipulent que la dernière adresse IP est réservée pour l'in-

```
Username:
Username: cisco
Password:

Switch>en
Switch>enable
Switch#conf
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host
Switch(config)#hostname CISCO
CISCO(config)#EXIT
CISCO#
%SYS-5-CONFIG_I: Configured from console by console

CISCO#COP
CISCO#copy r
CISCO#copy running-config s
CISCO#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CISCO#
```

FIGURE 5.9: *TP 1 : Attribution d'un nom à un équipement CISCO.*

terface du routeur, ainsi que les commutateurs se voient attribuer des adresses IP décroissantes en commençant par l'avant dernière adresse IP de la plage donnée.

– Par contre, les équipements des utilisateurs se voient attribuer et façon dynamique des adresses IP croissantes en commençant par la première adresse IP de la plage donnée.

```
S0>enable
Password:
S0#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S0(config)#interface vlan 1
S0(config-if)#ip address 192.168.1.253 255.255.255.0
S0(config-if)#no shutdown

%LINK-5-CHANGED: Interface Vlan1, changed state to up


%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S0(config-if)#exit
S0(config)#ip defaul
S0(config)#ip default-gateway 192.168.1.254
S0(config)#exit
S0#
%SYS-5-CONFIG_I: Configured from console by console

S0#cop
S0#copy r
S0#copy running-config s
S0#copy running-config startup-config
```

FIGURE 5.10: *TP 1 : Attribution d'une adresse IP à un commutateur CISCO.*

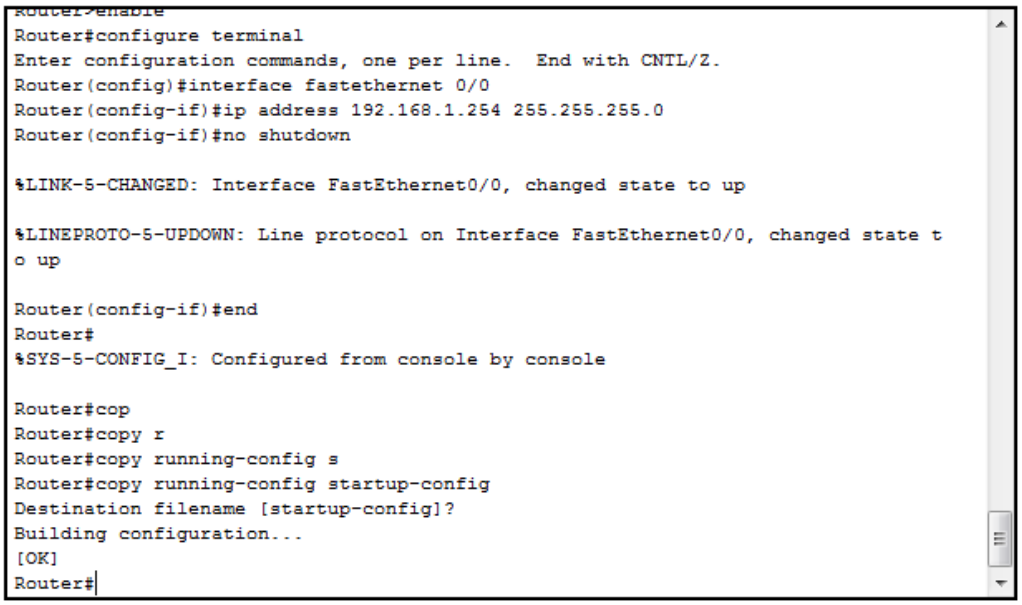


FIGURE 5.11: *TP 1 : Attribution d'une adresse IP à un routeur CISCO.*

5.2.6 Configuration des outils TELNET et SSH sur un équipement CISCO

- Sans doute, TELNET et SSH sont considérés parmi les configurations de base à effectuer sur un équipement CISCO avant de la placer dans une armoire de brassage. En effet, grâce à ces outils d'accès à distance, l'administrateur réseau pourra administrer à distance ses équipements sans être obligé de se déplacer à chaque fois.
- TELNET est un outil qui fonctionne par défaut dés lors la sécurité des lignes virtuelles de l'équipement en question est configurée. Tandis que, la configuration de SSH non seulement doit être faite de façon explicite, mais aussi plusieurs étapes sont nécessaires (voire Figure 5.12).
- Pour accéder à partir du PC0 au routeur R0 en utilisant TELNET et SSH, il suffit de saisir respectivement sur la fenêtre CMD du PC0 les commandes suivantes : telnet 192.168.1.254 et ssh -l cisco 192.168.1.254.

```
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#hostname R0
R0(config)#username cisco password cisco
R0(config)#ip domain-name cisco.com
R0(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R0(config)#crypto key generate rsa
% You already have RSA keys defined named R0.cisco.com .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: R0.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

R0(config)#line vty 0 4
*mars 1 3:51:19.205:  RSA key size needs to be at least 768 bits for ssh version
 2
*mars 1 3:51:19.205:  %SSH-5-ENABLED: SSH 1.5 has been enabled
R0(config-line)#transport input ssh
R0(config-line)#login local
```

FIGURE 5.12: *TP 1 : Configuration de l'outil d'accès à distance SSH.*

5.2.7 Configuration d'une bannière sur un équipement CISCO

- Une bannière sert, une fois elle est configurée, à afficher lors d'un accès à un équipement CISCO un message interdisant tout accès non autorisé à ce dernier.
- Certes une bannière ne constitue pas une barrière pour empêcher des accès non autorisés aux équipements CISCO, elle est tout de même utile pour rappeler à un intrus que son accès à l'équipement en question n'est pas autorisé.
- Par conséquent, cet intrus une fois détecté ne peut pas nier d'avoir été conscient de cette interdiction.
- La Figure 5.13 montre comment configurer une bannière sur un équipement CISCO.

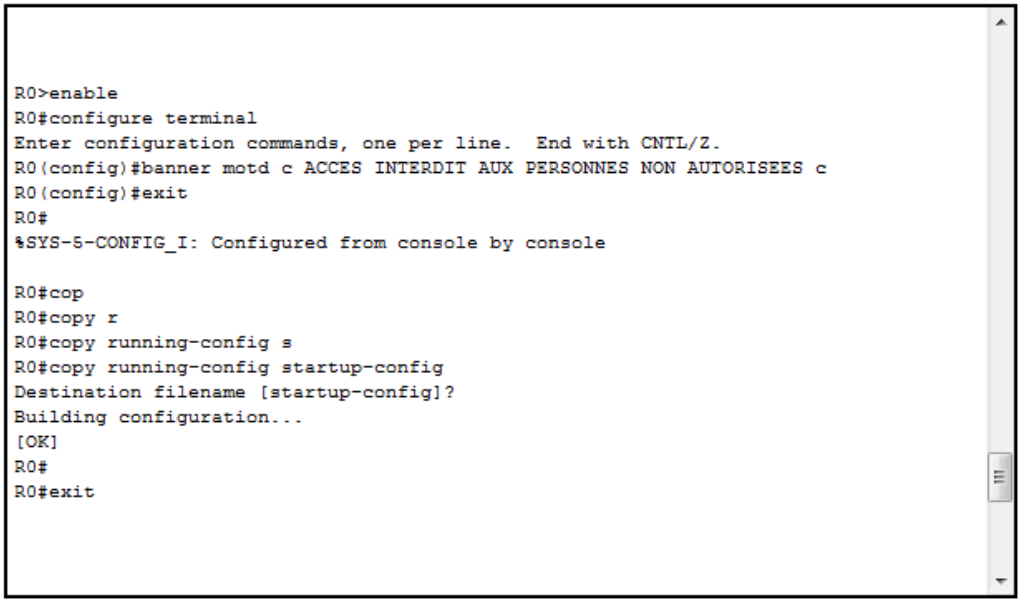


FIGURE 5.13: *TP 1 : Configuration d'une bannière sur un équipement CISCO.*

Chapitre 6

Conception d'un schéma d'adressage IPv4

6.1 L'énoncé du TP

- Le but de ce TP est d'apprendre à créer des sous-réseaux et concevoir des schémas d'adressage IP efficace, i.e., des schémas qui optimisent l'utilisation des adresses IP d'une part, et qui sont facilement extensibles d'autre part.
- Pour cela, nous proposons la topologie de réseau représentée par la Figure 6.1. Il s'agit de 03 sous-réseaux interconnectés par un routeur :
- Le sous-réseau 1 (SR1) est constitué de 6 stations (PC1-1,..., PC1-6).
- Le sous-réseau 2 est constitué de 12 stations (PC2-1,..., PC2-12).
- Le sous-réseau 3 est constitué de 18 stations (PC3-1,..., PC3-18).
- Pour chacun de ces sous-réseaux est affectée une plage d'adressage, à savoir : 192.168.5.139/27 pour le SR1, 172.16.139.46/20 pour le SR2, et 10.172.16.211/18 pour le SR3.
- Les tâches demandées sont les suivantes :

  1. Calculer pour chacune des plages d'adressages données : l'adresse IP du sous-réseau, l'adresse IP de la première machine, l'adresse IP de la dernière machine, l'adresse IP de diffusion, et l'adresse IP du prochain sous-réseau.
  2. Assigner à chacun des équipements (PCs, commutateurs, et routeur) des dif-

férents sous-réseaux une adresse IP suivant les plages d'adressages qui ont été proposées.

3. Utiliser à présent la plage d'adressage 192.168.20.0/24 pour concevoir un nouveau schéma d'adressage en se basant d'abord sur la notation CIDR (Classless Inter-Domain Routing), ensuite sur la notation VLSM (Variable-Length Subnet Mask).
4. Assigner à nouveau une nouvelle addresse IP à chacun des équipements du réseau.

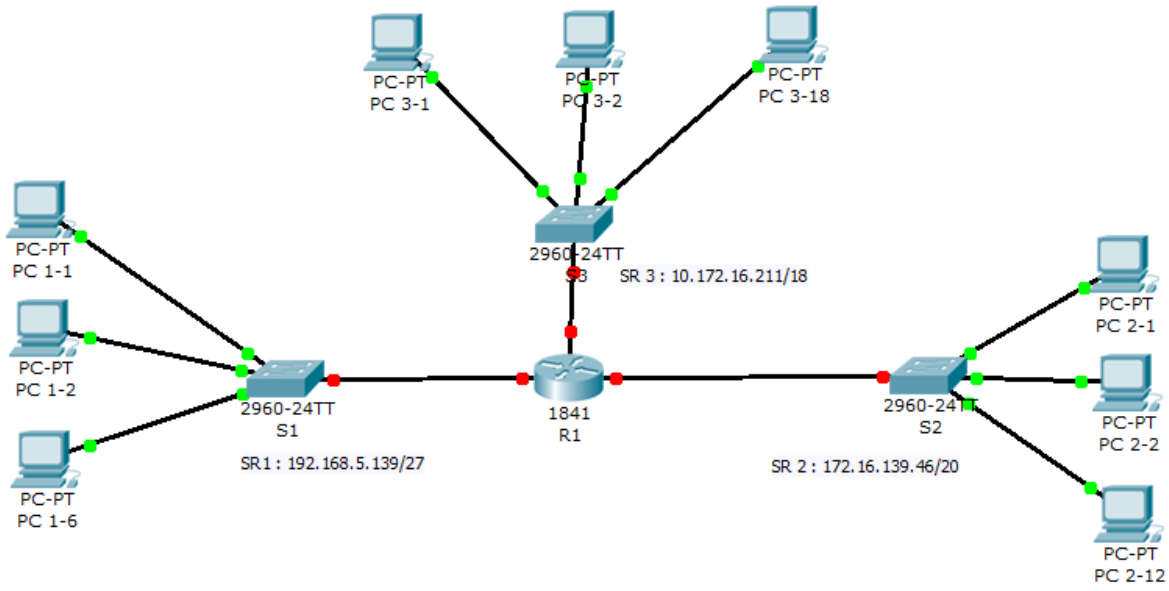


FIGURE 6.1: *TP 2 : Topologie du réseau.*

6.2 Les étapes de configuration

– La conception d'un schéma d'adressage efficace et évolutif est considérée comme l'une des tâches les plus fondamentales qu'un administrateur réseau doit maîtriser à la perfection.
– En effet, ce schéma doit à la fois éviter le gaspillage d'adresses IP et satisfaire les besoins futurs en terme d'extension du réseau.

- Par ailleurs, la conception d'un bon schéma d'adressage IP contribue énormément à faciliter la création de réseaux virtuels (VLANs : Virtual Local Area Networks) au sein d'un réseau local (LAN), mais aussi la configuration du routage sous toutes ses formes : statique, dynamique, inter VLANs, intra et inter domaines.
- Dans ce présent TP, l'étudiant va particulièrement apprendre les bonnes pratiques à suivre pour attribuer de façon logique et méthodique des adresses IP à l'ensemble des équipements (que ce soient équipements d'interconnexion ou équipements d'utilisateur final) du réseau qu'il gère, mais aussi à utiliser et comparer les deux méthodes CIDR et VLSM pour créer des sous-réseaux et concevoir des schémas d'adressages.
- A l'issue ce de TP, l'étudiant doit maîtriser de point de vue pratique l'adressage IP, et pourra surtout en fonction du réseau à administrer dans le futur effectuer un choix éclairé sur les méthodes de création des sous-réseaux et conception de schémas d'adressage.
- Dans ce qui suit, nous allons expliquer comment procéder pour répondre à chacune des tâches demandées dans ce TP :

6.2.1 Calcul des adresses IP

- Bien que le principe de calcul des adresses IP est supposé connu par les étudiants, un rappel reste tout de même très essentiel.
- En effet, l'intégralité des fonctionnalités du réseau dépend intrinsèquement de la configuration IP de ce dernier.
- De ce fait, sur la question de la configuration IP du réseau géré, il y a zéro tolérance.
- Les adresses IP du sous-réseau 1 sont obtenues comme suivant :

  1. L'adresse du réseau est : 192.168.5.128/27
  2. L'adresse de la première machine est : 192.168.5.129/27
  3. L'adresse de la dernière machine est : 192.168.5.158/27
  4. L'adresse de diffusion est : 192.168.5.159/27
  5. L'adresse du prochain réseau : 192.168.5.160/27

- Les adresses IP du sous-réseau 2 sont obtenues comme suivant :

1. L'adresse du réseau est : 172.16.128.0/20
2. L'adresse de la première machine est : 172.16.128.1/20
3. L'adresse de la dernière machine est : 172.16.143.254/20
4. L'adresse de diffusion est : 172.16.143.255/20
5. L'adresse du prochain réseau : 172.16.144.0/20

– Les adresses IP du sous-réseau 3 sont obtenues comme suivant :

1. L'adresse du réseau est : 10.172.0.0/18
2. L'adresse de la première machine est : 10.172.0.1/18
3. L'adresse de la dernière machine est : 10.172.63.254/18
4. L'adresse de diffusion est : 10.172.63.255/18
5. L'adresse du prochain réseau : 10.172.64.0/18

6.2.2 Attribution des adresses IP

– Une fois les adresses IP sont calculées pour chaque sous-réseau, il faut les attribuer de façon stratégique comme suivant :

1. Pour les équipements d'interconnexion (commutateurs et routeurs), il faut leurs attribuer des adresses IP statiques et décroissantes en commençant par la dernière adresse IP machine. En particulier, la dernière adresse machine est réservée pour l'interface du routeur, elle est dite la passerelle par défaut.
2. Pour les équipements des utilisateurs finaux, il faut leurs attribuer des adresses IP dynamique et croissantes en commençant par la première adresse machine.

– Il faut noter que les serveurs ne sont ni considérés comme des équipements d'interconnexion ni d'ailleurs comme des équipements des utilisateurs finaux. Les serveurs sont des machines très importants et leur continuité à fournir des services réseau est une question indiscutable. C'est pourquoi, des adresses doivent réservées et attribuées à ces derniers de façon statique.

6.2.3 Création de sous-réseaux : CIDR

- La méthode CIDR consiste à concevoir un schéma d'adressage en se basant uniquement sur le nombre de sous-réseaux à créer sans tenir compte du nombre d'équipements que contient chacun de ces dernier.
- Pour ce faire, la méthode CIDR consiste à ôter de la partie machine un certain nombre de bits de poids fort suivant le nombre de sous-réseaux à créer. De ce fait, l'ensemble des sous-réseaux qui seront crées vont pouvoir contenir le même nombre d'équipements.
- Dans notre cas, puisque nous avons besoin de créer 03 sous-réseaux, nous devons alors ôter 02 bits de poids fort de la partie machine.
- En appliquant la méthode CIDR sur la plage 192.168.20.0/24, les sous-plages obtenues sont les suivantes :

  1. 192.168.20.0/26 : Elle sera affectée pour le sous-réseau 1.
  2. 192.168.20.64/26 : Elle sera affectée pour le sous-réseau 2.
  3. 192.168.20.128/26 : Elle sera affectée pour le sous-réseau 3.
  4. 192.168.20.192/26 : Elle sera utilisée ultérieurement en cas d'extension du réseau.

- Les adresses IP du sous-réseau 1 sont obtenues comme suivant :

  1. L'adresse du réseau est : 192.168.20.0/26
  2. L'adresse de la première machine est : 192.168.20.1/26
  3. L'adresse de la dernière machine est : 192.168.20.62/26
  4. L'adresse de diffusion est : 192.168.20.63/26
  5. L'adresse du prochain réseau : 192.168.20.64

- Les adresses IP du sous-réseau 2 sont obtenues comme suivant :

  1. L'adresse du réseau est : 192.168.20.64/26
  2. L'adresse de la première machine est : 192.168.20.65/26
  3. L'adresse de la dernière machine est : 192.168.20.126/26

4. L'adresse de diffusion est : 192.168.20.127/26
5. L'adresse du prochain réseau : 192.168.20.128/26

– Les adresses IP du sous-réseau 3 sont obtenues comme suivant :

1. L'adresse du réseau est : 192.168.20.128/26
2. L'adresse de la première machine est : 192.168.20.129/26
3. L'adresse de la dernière machine est : 192.168.20.190/26
4. L'adresse de diffusion est : 192.168.20.191/26
5. L'adresse du prochain réseau : 192.168.20.192/26

– Comme nous l'avons certainement remarqué, bien que la méthode CIDR est simple à appliquer, elle ne tient pas en compte des besoins des sous-réseaux à créer, et elle n'offre pas beaucoup de possibilités d'extension du réseau.

6.2.4 Création de sous-réseaux : VLSM

– La méthode VLSM consiste quant à elle à créer des sous-réseaux en prenant en considération le nombre d'équipements que contient chacun de ces derniers.
– Cela se fait de façon progressive en commençant d'abord par créer le sous-réseau de plus grande taille et en terminant par le sous-réseau de plus petite taille.
– Pour ce faire, nous allons compter à partir du bit de poids faible le nombre de bits nécessaire pour créer le premier sous-réseau. Le reste des bits seront ôtés pour créer des sous-réseaux de même taille.
– La première sous-plage d'adresses obtenue sera automatiquement attribuée pour le premier sous-réseau car elle satisfait sur mesure ses besoins.
– La deuxième sous-plage d'adresses sera à nouveau scindée en plusieurs sous-plages de telle façon à satisfaire encore une fois sur mesure les besoins du deuxième sous-réseau.
– Ce processus sera à chaque fois réitéré jusqu'à ce que chaque sous-réseau se voit attribuer une plage d'adresses qui lui convient sur mesure.
– Dans notre cas, le sous-réseau de plus grande taille est le sous-réseau 3. Ce dernier comporte 20 équipements, nous avons alors besoin au moins de 05 bits de poids

faible de la partie machine. Les 03 bits restants de poids fort de la partie machine seront alors utilisés pour créer 08 sous-réseaux chacun comportant 30 équipements.

– La première itération de la méthode VLSM sur la plage 192.168.20.0/24 aboutira aux sous-plages d'adresses suivantes :

  1. 192.168.20.0/27 : Elle sera affectée pour le sous-réseau 1.
  2. 192.168.20.32/27 : Elle subira une deuxième itération de la méthode VLSM pour créer sur mesure une plage d'adresses pour le sous-réseau 2.
  3. 192.168.20.64/27 : Elle sera utilisée ultérieurement en cas d'extension du réseau.
  4. 192.168.20.96/27 : Elle sera utilisée ultérieurement en cas d'extension du réseau.
  5. 192.168.20.128/27 : Elle sera utilisée ultérieurement en cas d'extension du réseau.
  6. 192.168.20.160/27 : Elle sera utilisée ultérieurement en cas d'extension du réseau.
  7. 192.168.20.192/27 : Elle sera utilisée ultérieurement en cas d'extension du réseau.
  8. 192.168.20.224/27 : Elle sera utilisée ultérieurement en cas d'extension du réseau.

– Le deuxième sous-réseau de plus grande taille est le sous-réseau 2. Ce dernier comporte 14 équipements, nous avons alors besoin au moins de 4 bits de poids faible de la partie machine de la plage 192.168.20.32/27. Le bit restant de poids fort de la partie machine sera alors utilisé pour créer 02 sous-réseaux chacun comportant 14 équipements.

– La deuxième itération de la méthode VLSM sur la plage 192.168.20.32/27 aboutira aux sous-plages d'adresses suivantes :

  1. 192.168.20.32/2 : Elle sera affectée pour le sous-réseau 2.
  2. 192.168.20.48/27 : Elle subira une troisième itération de la méthode VLSM pour créer sur mesure une plage d'adresses pour le sous-réseau 1.

– Le sous-réseau de plus petite taille est le sous-réseau 1. Ce dernier comporte 8 équipements, nous avons alors besoin au moins de 4 bits de poids faible de la partie

machine de la plage 192.168.20.48/28. La totalité des bits de la partie machine seront utilisées, c'est pourquoi cette plage d'adresses ne sera scindée. Elle sera affectée telle quelle pour le sous-réseau 1.

- Les adresses IP du sous-réseau 1 sont obtenues comme suivant :
  1. L'adresse du réseau est : 192.168.20.48/28
  2. L'adresse de la première machine est : 192.168.20.49/28
  3. L'adresse de la dernière machine est : 192.168.20.62/28
  4. L'adresse de diffusion est : 192.168.20.63/28
  5. L'adresse du prochain réseau : il n'existe pas de prochain sous-réseau.
- Les adresses IP du sous-réseau 2 sont obtenues comme suivant :
  1. L'adresse du réseau est : 192.168.20.32/28
  2. L'adresse de la première machine est : 192.168.20.33/28
  3. L'adresse de la dernière machine est : 192.168.20.46/28
  4. L'adresse de diffusion est : 192.168.20.47/28
  5. L'adresse du prochain réseau : 192.168.20.48/28
- Les adresses IP du sous-réseau 3 sont obtenues comme suivant :
  1. L'adresse du réseau est : 192.168.20.0/27
  2. L'adresse de la première machine est : 192.168.20.1/28
  3. L'adresse de la dernière machine est : 192.168.20.30/27
  4. L'adresse de diffusion est : 192.168.20.31/27
  5. L'adresse du prochain réseau : 192.168.20.32/27
- Comme nous l'avons certainement remarqué, bien que la méthode VLSM permet de créer des sous-réseaux sur mesure et ne pose aucun problème sur l'évolution du réseau, elle reste tout de même complexe car elle nécessite plusieurs itérations de calcul.

Chapitre 7

Routage et tests de connectivité

7.1 L'énoncé du TP

- L'objectif ultime de ce TP est d'apprendre à l'étudiant comment réaliser des tests de connectivité afin de s'assurer de la bonne configuration du routage, ou dans le cas échéant détecter, localiser et corriger des erreurs de configuration de ce dernier.
- Pour cela, nous proposons la topologie de réseau représentée par la Figure 7.1. Il s'agit de réseaux locaux (chacun est composé de deux sous-réseaux) interconnectés via des réseaux WANs.
- Les tâches demandées sont les suivantes :
  1. Configurer pour chaque équipement du réseau ci-dessous une @IP selon les plages d'adressages qui ont été données.
  2. Effectuer un test de connectivité pour s'assurer que les équipements qui appartiennent au même réseau communiquent.
  3. Configurer le routage statique à l'aide de la commande " IP ROUTE NETWORK-NUMBER INTERFACE-NUMBER ".
  4. Configurer à nouveau le routage statique à l'aide de la commande " IP ROUTE NETWORK-NUMBER NEXT-HOP-NUMBER".
  5. Réduire au maximum possible le nombre de routes statiques que vous avez configurées en les remplaçants par des routes par défaut.

6. Utiliser la commande " SHOW IP ROUTE " pour afficher et vérifier la table de routage. Ensuite, utiliser la commande " PING @IP " pour tester la connectivité du réseau.
7. Configurer le routage dynamique à l'aide du protocole RIP.
8. Utiliser la commande " SHOW IP PROTOCOLS " pour s'assurer de la bonne configuration du protocole RIP.
9. Utiliser la commande " SHOW IP ROUTE " pour afficher et vérifier la table de routage.
10. Utiliser la commande " PING @IP " pour tester la connectivité du réseau.
11. Utiliser la commande " DEBUG IP RIP " pour visualiser les mises à jour de routage échangées entre les différents routeurs.

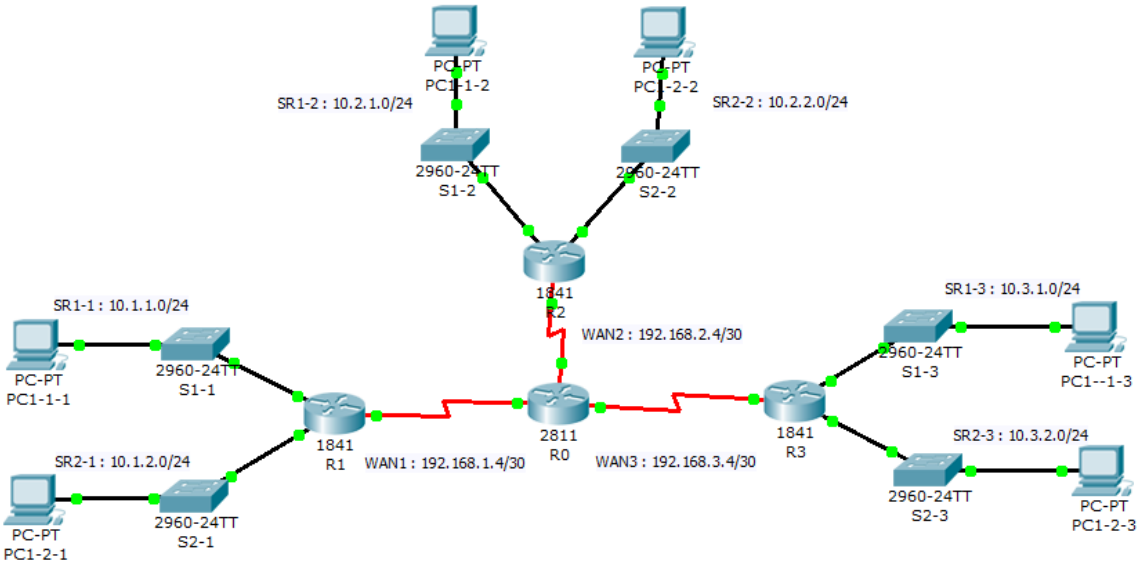


FIGURE 7.1: *TP 3 : Topologie du réseau.*

7.2 Les étapes de configuration

– Le bon fonctionnement d'une infrastructure réseau dépend non seulement d'une bonne conception d'un schéma d'adressage, mais aussi d'une bonne configuration

du routage. En effet, nous distinguons deux façons de faire le routage : le routage statique et le routage dynamique.

- Le routage statique est à la charge de l'administrateur réseau, i.e., c'est à lui de veiller à configurer des routes statiques pour assurer une connectivité entre n'importe quels deux équipements du réseau. Certes le routage statique offre à l'administrateur réseau la possibilité de contrôler entièrement l'acheminement des données dans son réseau, il n'est pas recommandé dans le cas de grands réseaux car le temps de configuration et de maintenance est excessivement grand.
- Le routage dynamique est par contre délégué à un protocole de routage qui doit être évidemment configuré préalablement par l'administrateur réseau. Dans le routage dynamique, le protocole configuré se charge de découvrir des routes et mettre à jour des tables de routage.
- Pour réussir le routage d'un réseau, il ne suffit pas d'apprendre à configurer des routes statiques (dans le cas d'un routage statique) ou un protocole de routage (dans le cas d'un routage dynamique), mais surtout il faut apprendre à réaliser les tests de connectivité une fois le routage est configuré.
- En effet, grâce à ces tests de connectivité, on pourra montrer la bonne configuration du routage, ou dans le cas échéant détecter, localiser et corriger des erreurs de configuration de ce dernier.
- A l'issue de ce TP, l'étudiant sera en mesure d'appliquer et interpréter les résultats de chacun des tests de connectivité suivants : PING @IP, TRACERT @IP, SHOW IP ROUTE, SHOW IP PROTOCOLS, DEBUG IP RIP, etc.
- Dans ce qui suit, nous allons expliquer comment procéder pour répondre à chacune des tâches demandées dans ce TP :

7.2.1 Configuration du routage statique

- Pour configurer le routage statique, l'administrateur réseau doit introduire dans chaque routeur constituant le réseau des routes statiques qui vont permettre ce dernier d'atteindre n'importe quelle destination du réseau.
- Il existe deux manières pour configurer des routes statiques : soit en utilisant l'in-

terface de sortie ou l'adresse IP du prochain saut.

– Pour montrer comment faire, nous proposons de configurer une route statique sur le routeur "R0" pour rejoindre le réseau 10.1.1.0/24.

– Les commandes à saisir sont données respectivement dans les Figures 7.2 et 7.3.

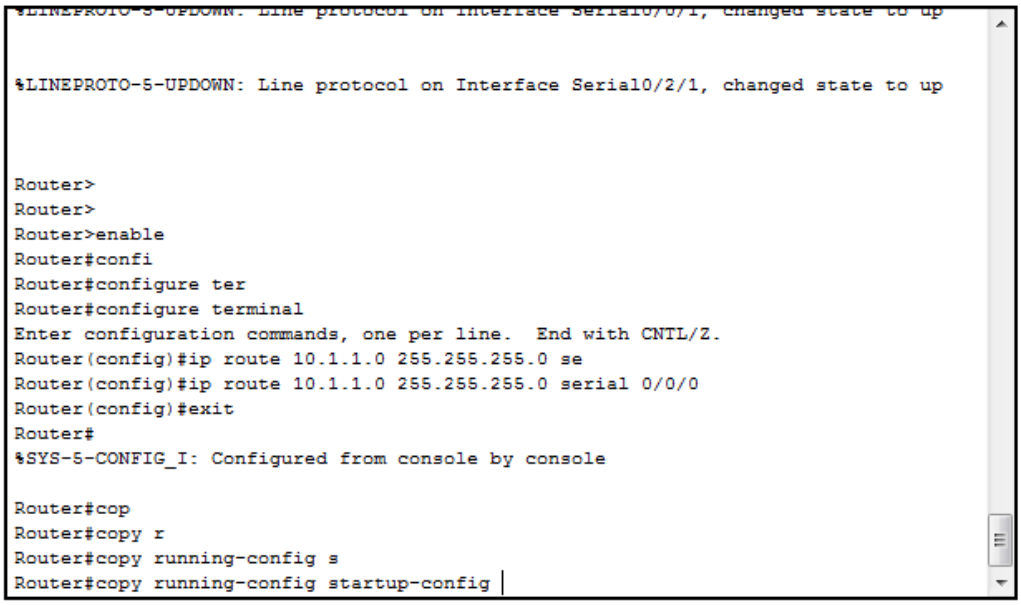


FIGURE 7.2: *TP 3 : Routage statique (en utilisant l'interface de sortie).*

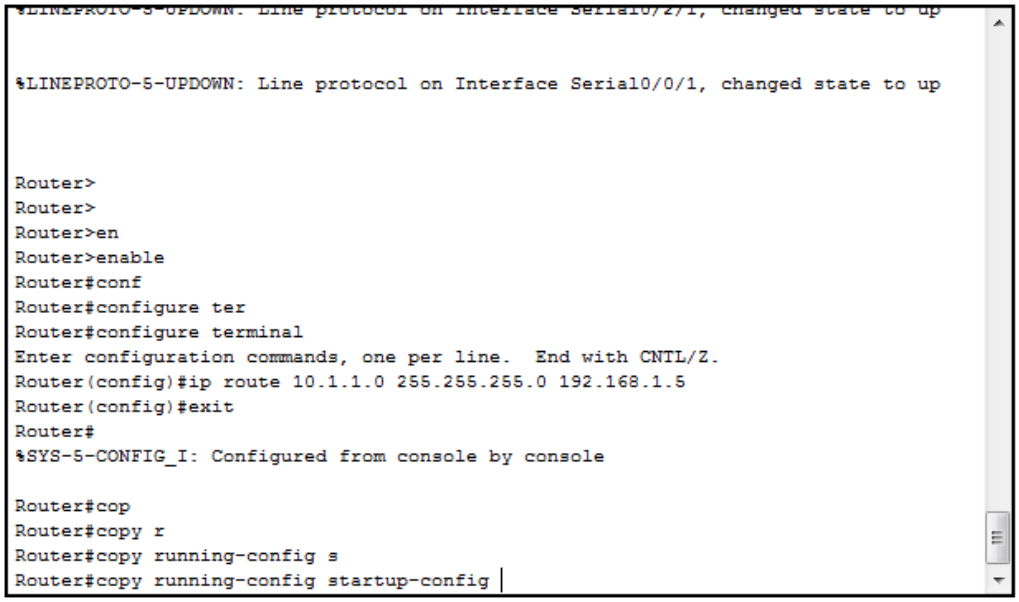


FIGURE 7.3: *TP 3 : Routage statique (en utilisant l'@ du prochain saut).*

7.2.2 Configuration du routage dynamique

– Pour configurer le routage dynamique, l'administrateur réseau doit configurer un protocole de routage. Dans ce TP, nous allons utiliser le protocole RIP (Routing Information Protocol).

– La Figure 7.4 montre comment configurer le protocole RIP sur le routeur "R0".

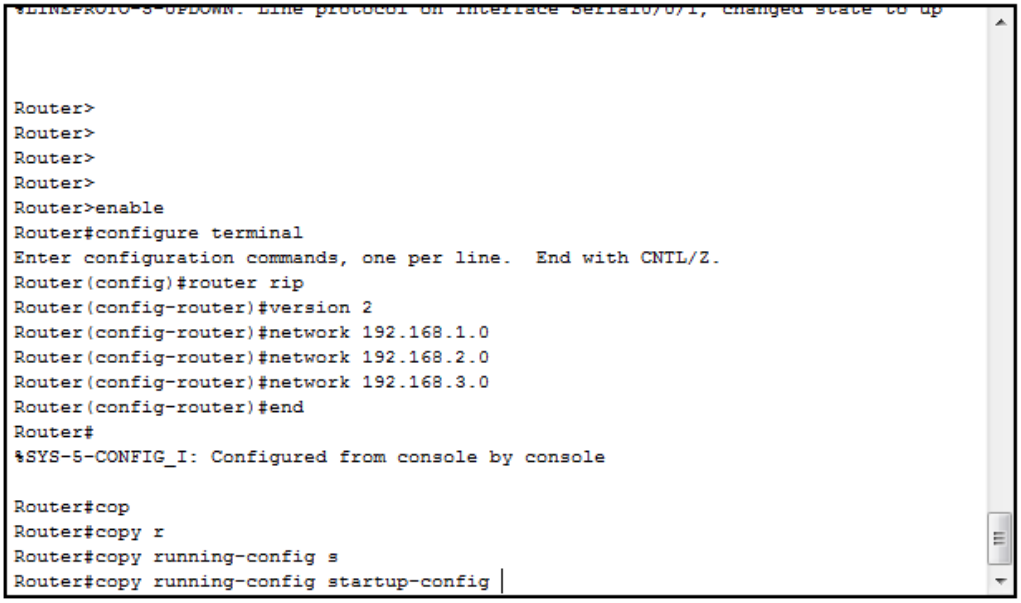


FIGURE 7.4: *TP 3 : Routage dynamique (en utilisant le protocole RIP).*

7.2.3 Tests de connectivité

– Suivant le type de routage utilisé (statique ou dynamique), il existe plusieurs tests de connectivité qu'un administrateur réseau peut réaliser pour s'assurer qu'il existe au moins une route optimale (à moindre coût) allant de n'importe quelle source vers n'importe quelle destination.

– C'est pourquoi, pour effectuer une bonne configuration du routage d'un réseau, il ne suffit pas seulement de connaître et d'appliquer les commandes qui permettent d'y parvenir, mais aussi il faut connaître, apprendre, et maîtriser les tests de connectivité qui permettent de montrer le bon acheminement des données.

– Il existe plusieurs tests de connectivité à effectuer pendant et après la configuration

du routage. Certaines tests sont commun entre le routage statique et dynamique, et d'autres sont dédiés pour le routage dynamique.

– Dans ce qui suit, nous allons tenter d'expliquer chacun de ces tests :

7.2.3.1 La commande PING @IP

– Bien que la commande PING @IP est un test de connectivité usuel connu par tous les étudiants, beaucoup d'autres eux ne savent lire et interpréter les messages retournés par ce test.

– Le nombre de messages ainsi que leurs contenus retournés par le test de connectivité PING @IP dépend du type des équipements source et destination concernés par ce test :

1. Quand l'équipement interrogeant et l'équipement interrogé sont des stations Windows (voir la Figure 7.5), les paramètres retournés par défaut sont les suivants : le nombre de messages ICMP est de 4, la taille d'un message ICMP est de 32 octets, le nombre maximum de saut (TTL) est de 128.
2. Quand l'équipement interrogeant est une station windows et l'équipement interrogé est un équipement IOS (voir la Figure 7.6), les paramètres retournés par défaut sont les suivants : le nombre de messages ICMP est de 4, la taille d'un message ICMP est de 32 octets, le nombre maximum de saut (TTL) est de 255.
3. Quand l'équipement interrogeant est IOS, indépendamment de l'équipement interrogé (voir les Figures 7.7 et 7.8), les paramètres retournés par défaut sont les suivants : le nombre de messages ICMP est de 5, la taille d'un message ICMP est de 100 octets.

– Pour résumer, le test de connectivité PING @IP permet surtout de retourner deux informations : si l'équipement de destination est joignable depuis un équipement source et après combien de sauts (routeurs).

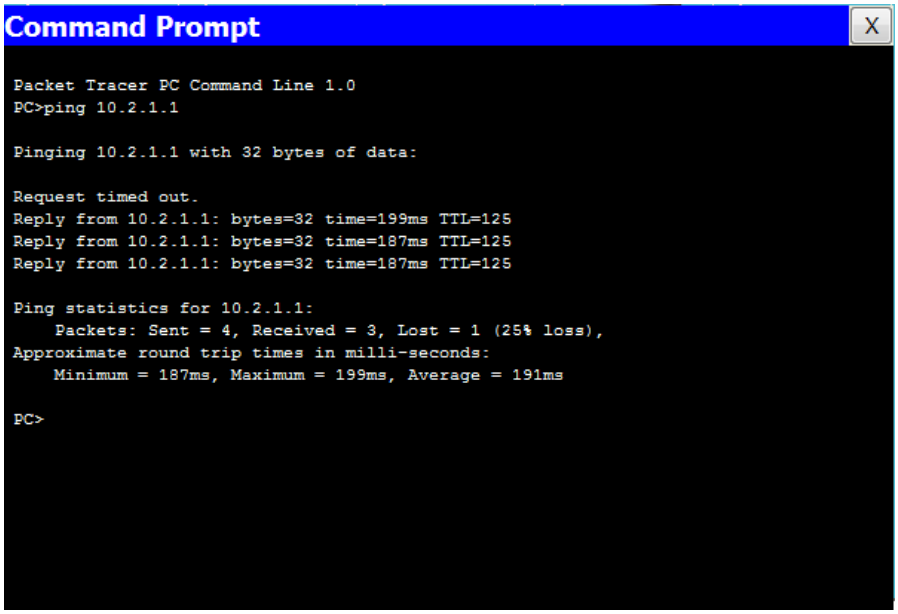


FIGURE 7.5: *TP 3 : La commande PING @IP (From PC1-1-1 To PC1-1-2).*

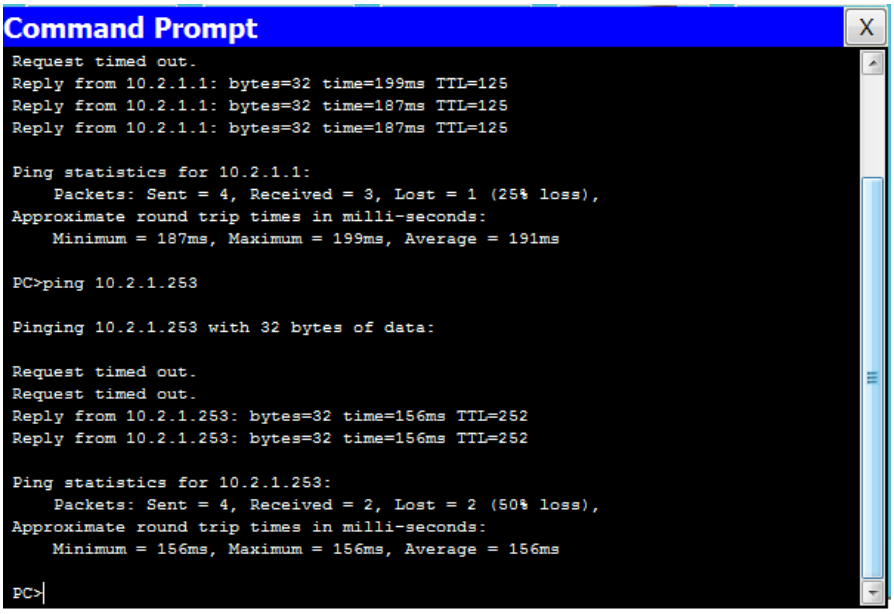


FIGURE 7.6: *TP 3 : La commande PING @IP (From PC1-1-1 To S1-2).*

7.2.3.2 La commande TRACERT/TRACEROUTE @IP

– La commande TRACERT @IP (sur un équipement Windows, voir la Figure 7.9) ou la commande TRACEROUTE @IP (sur un équipement IOS, voir la Figure 7.10) permettent de retourner exactement les mêmes informations.

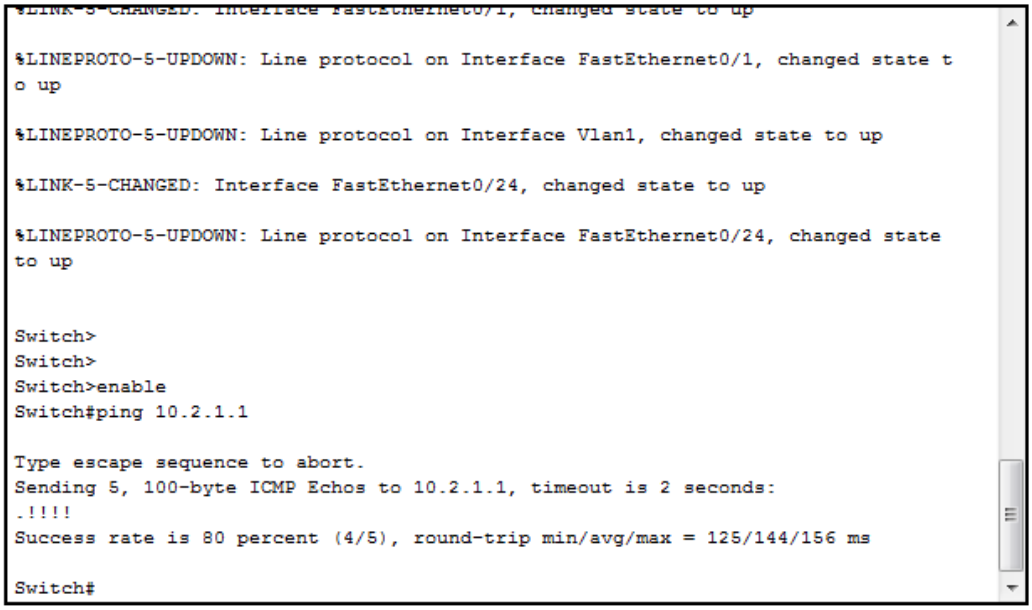


FIGURE 7.7: *TP 3 : La commande PING @IP (From S1-1 To PC1-1-2).*

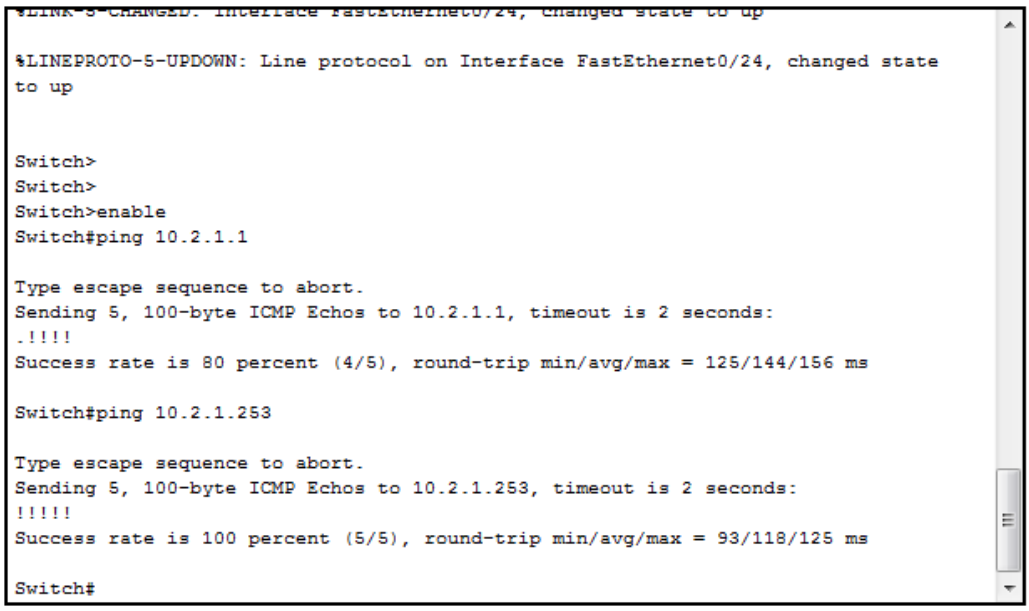


FIGURE 7.8: *TP 3 : La commande PING @IP (From S1-1 To S1-2).*

– En effet, le rôle de ces commandes est de raffiner l'information retournée par la commande PING @IP sur le nombre de saut à effectuer pour atteindre une destination. Ces deux commandes consistent donc à tracer l'itinéraire à emprunter d'une source à une destination en affichant l'ensemble des routeurs ayant participé dans cette opération.

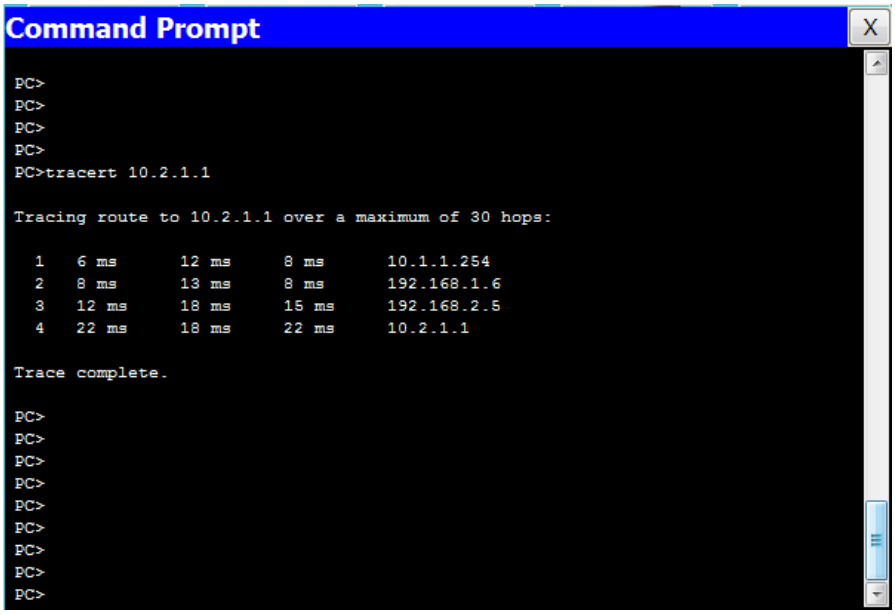


FIGURE 7.9: *TP 3 : La commande TRACERT @IP (From PC1-1-1 To PC1-1-2).*

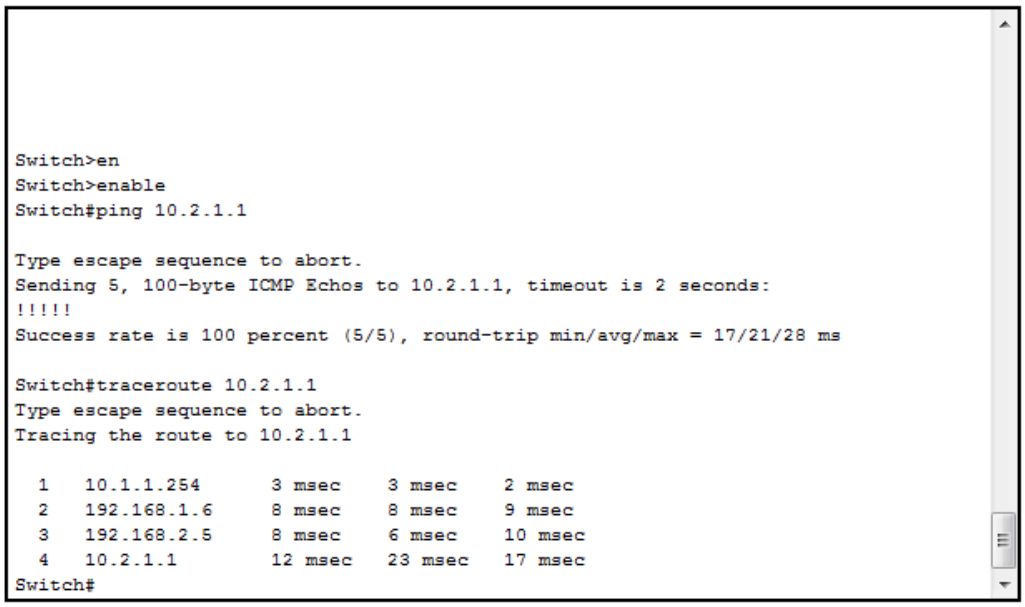


FIGURE 7.10: *TP 3 : La commande TRACEROUTE @IP (From S1-1 To PC1-1-2).*

7.2.3.3 La commande SHOW IP ROUTE

– Cette commande est exécuté sur l'interface CLI d'un routeur pour afficher sa table de routage. Elle est évidemment applicable que ce soit dans le cas d'un routage statique ou dynamique.

– Grâce à cette commande, l'administrateur réseau pourra vérifier si les routes statiques introduites ont été bien configurées (voir la Figure 7.11), ou le protocole de routage configuré permet bien de découvrir des routes et mettre à jour la table de routage (voir la Figure 7.12).

```
Router#sh
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 6 subnets
S       10.1.1.0 is directly connected, Serial0/0/0
S       10.1.2.0 is directly connected, Serial0/0/0
S       10.2.1.0 is directly connected, Serial0/0/1
S       10.2.2.0 is directly connected, Serial0/0/1
S       10.3.1.0 is directly connected, Serial0/2/1
S       10.3.2.0 is directly connected, Serial0/2/1
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.4 is directly connected, Serial0/0/0
     192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.4 is directly connected, Serial0/0/1
     192.168.3.0/30 is subnetted, 1 subnets
```

FIGURE 7.11: *TP 3 : La commande SHOW IP ROUTE (routage statique).*

```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 6 subnets
R       10.1.1.0 [120/1] via 192.168.1.5, 00:00:08, Serial0/0/0
R       10.1.2.0 [120/1] via 192.168.1.5, 00:00:08, Serial0/0/0
R       10.2.1.0 [120/1] via 192.168.2.5, 00:00:25, Serial0/0/1
R       10.2.2.0 [120/1] via 192.168.2.5, 00:00:25, Serial0/0/1
R       10.3.1.0 [120/1] via 192.168.3.5, 00:00:02, Serial0/2/1
R       10.3.2.0 [120/1] via 192.168.3.5, 00:00:02, Serial0/2/1
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.4 is directly connected, Serial0/0/0
     192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.4 is directly connected, Serial0/0/1
     192.168.3.0/30 is subnetted, 1 subnets
```

FIGURE 7.12: *TP 3 : La commande SHOW IP ROUTE (routage dynamique).*

7.2.3.4 La commande SHOW IP PROTOCOLS

- La commande SHOW IP PROTOCOLS est également applicable uniquement sur l'interface CLI d'un routeur, et encore dans le cas d'un routage dynamique.
- Cette commande une fois exécutée permet à l'administrateur réseau de vérifier si le protocole de routage utilisé (dans notre cas, à titre illustratif, il s'agit du protocole RIP, voir la Figure 7.13) a été bien configuré.

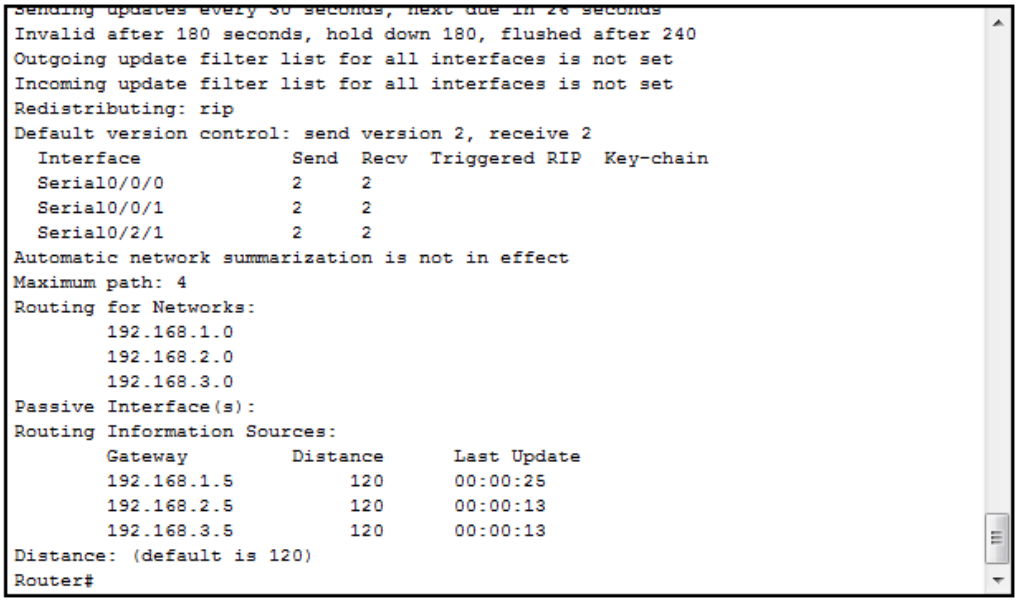


FIGURE 7.13: *TP 3 : La commande SHOW IP PROTOCOLS.*

7.2.3.5 La commande DEBUG IP RIP

- Il arrive parfois que les tests présentés et discutés précédemment ne permettent pas de détecter l'origine d'un dysfonctionnement du routage dans un réseau.
- C'est pourquoi, on fait recours à la commande DEBUG IP *ROUTING-PROTOCOL-NAME* (dans notre cas c'est le protocole RIP) pour analyser le problème et trouver une solution.
- Cette commande consiste donc à afficher en temps réel les informations de routage échangées entre les routeurs (voir la Figure 7.14).
- Bien que cette commande aide énormément l'administrateur réseau à comprendre le fonctionnement de son réseau, elle entraîne une activité supplémentaire au routeur.

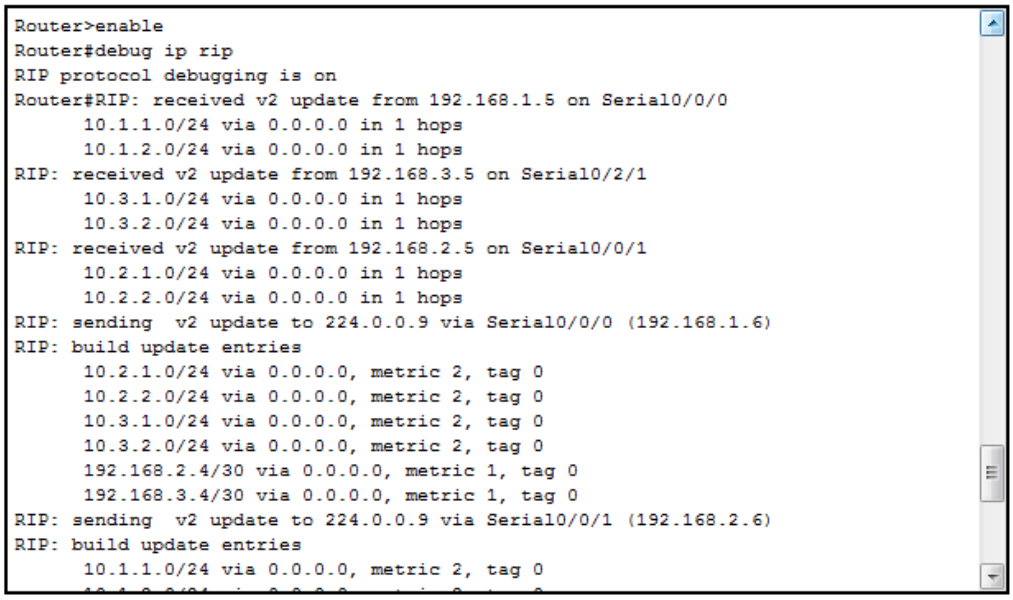


FIGURE 7.14: *TP 3 : La commande DEBUG IP RIP.*

Chapitre 8

Construction d'une cartographie réseau

8.1 L'énoncé du TP

- Le but de ce TP est d'apprendre à utiliser le protocole CDP (CISCO Discovery Protocol) pour construire une cartographie réseau.
- Pour cela, nous proposons la topologie de réseau représentée par la Figure 8.1.
- Le fichier source de cette topologie est disponible sur l'adresse https ://elearning.univ-bejaia.dz/course/view.php ?id=10372.
- Les mots de passe et les noms utilisateur sont tous " cisco ".
- Le travail demandé est suivant :
- Utiliser les commandes suivantes :
  1. IPCONFIG,
  2. PING,
  3. TELNET,
  4. SHOW CDP NEIGHBORS,
  5. SHOW CDP ENTRY.
- Pour construire la cartographie du réseau ci-dessous. En d'autres termes, identifier

les informations suivantes pour chacun des équipements d'interconnexion :

1. Nom,
2. Type,
3. Plateforme,
4. Ports d'interconnexion,
5. @IP.

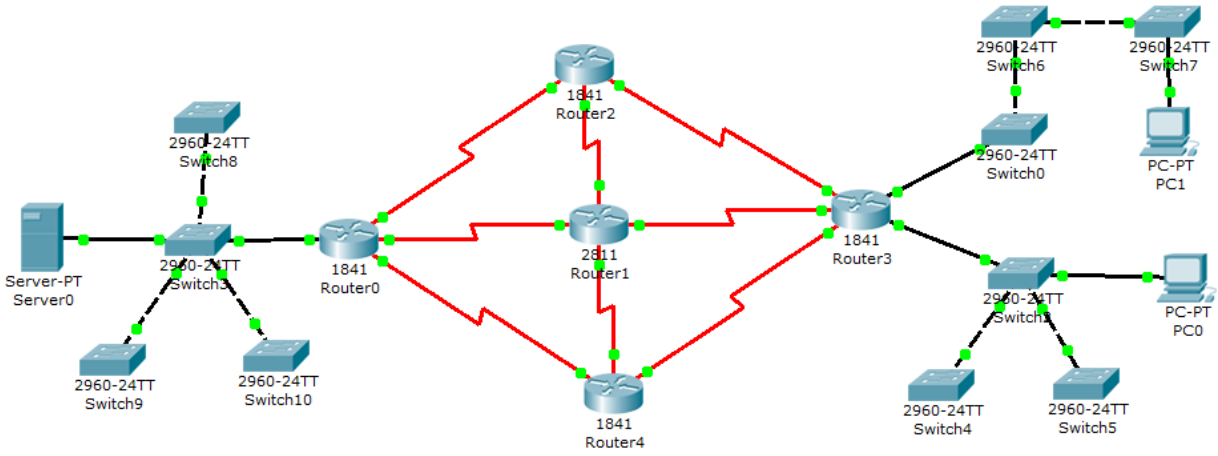


FIGURE 8.1: *TP 4 : Topologie du réseau.*

8.2 Les étapes de configuration

– Tout administrateur réseau doit connaître la cartographie de son réseau. Cette dernière doit être imprimée sur papier et toujours disponible dans la poche de l'administrateur réseau.
– En effet, la cartographie réseau contient l'ensemble des informations utiles sur l'interconnexion des équipements du réseau.
– Grâce à cette dernière, les pannes réseau sont facilement et rapidement détectables, localisables et réparables.
– Dans le cadre des réseaux CISCO, le protocole utilisé pour construire la cartographie réseau est dit CDP.

– Dans ce présent, l'étudiant va apprendre à utiliser différentes commandes pour parvenir à construire la cartographie de son réseau.
– Supposant que la station d'administration et le PC0, les étapes à suivre sont les suivantes :

8.2.1 La commande IPCONFIG

– Lorsqu'un administrateur réseau est installé pour la première fois dans son poste, il n'a à portée de main que son ordinateur pour construire la cartographie du réseau dont il a la charge.
– Pour commencer alors à construire la cartographie de son réseau, il va s'en servir de la commande IPCONFIG sur la fenêtre CMD de son ordinateur (voir la Figure 8.2).
– Cette commande permettra donc à l'administrateur réseau de recenser le premier équipement d'interconnexion de son réseau qui est la passerelle par défaut.

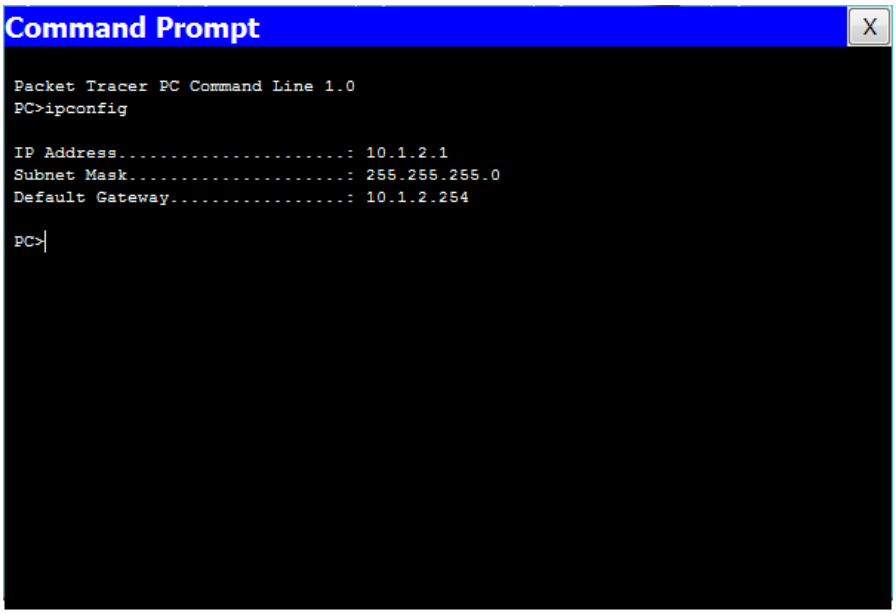


FIGURE 8.2: *TP 4 : La commande IPCONFIG.*

8.2.2 La commande PING @IP

– A chaque fois qu'un nouvel équipement est recensé, il est recommandé voire nécessaire d'effectuer le test de connectivité PING @IP avant de tenter d'y accéder à distance (voir la Figure 8.3).

– Ce test permettra à l'administrateur réseau de distinguer le cas d'un équipement qui ne répond pas et celui d'un équipement qui n'accepte pas une connexion à distance.

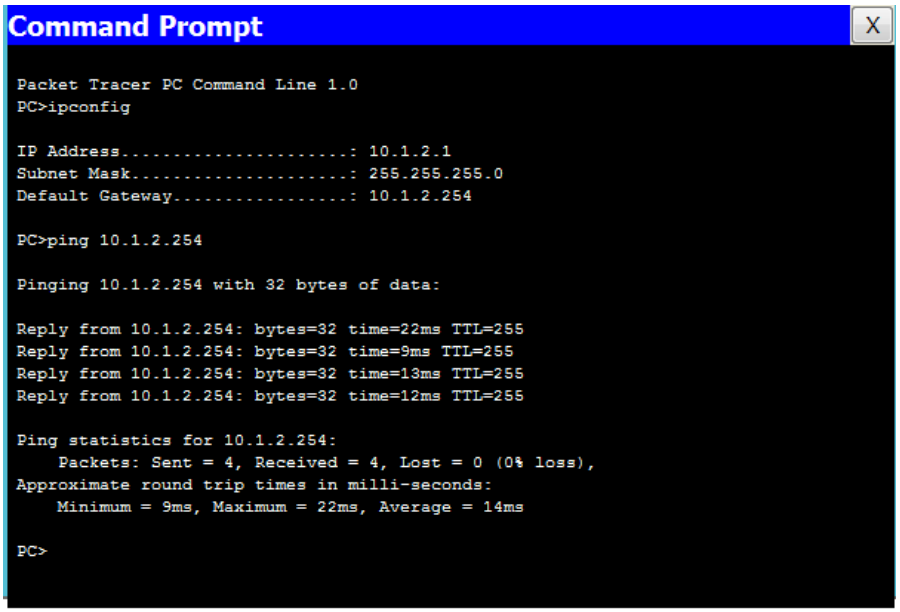


FIGURE 8.3: *TP 4 : La commande PING @IP.*

8.2.3 La commande TELNET @IP

– Lorsqu'un équipement répond avec succès au test de connectivité PING @ IP, l'administrateur réseau pourra utiliser un outil d'accès à distance tel que TELNET @IP pour y accéder.

– Bien évidemment, l'administrateur réseau va utiliser les mots de passe et les noms utilisateur qui lui ont été remis par sa hiérarchie le jour de son installation dans le poste.

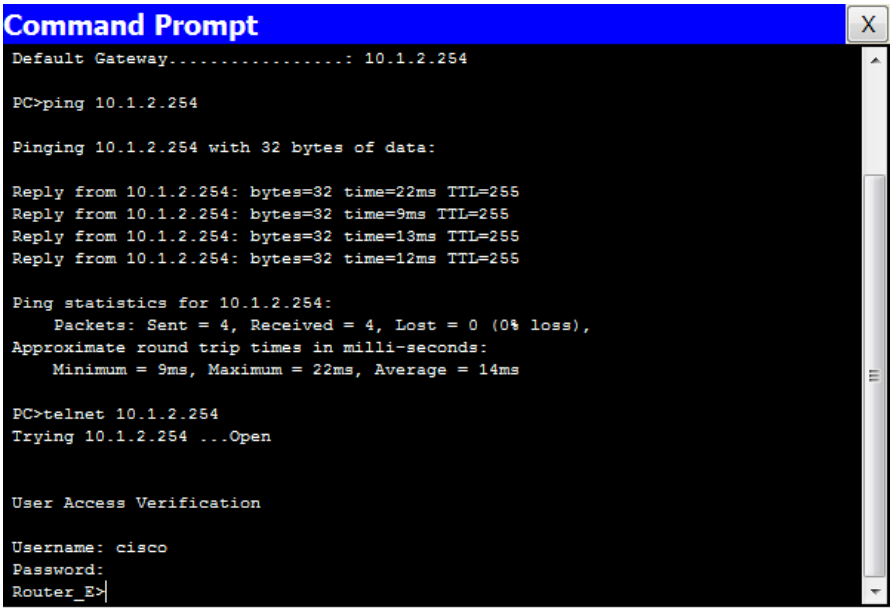


FIGURE 8.4: *TP 4 : La commande TELNET @IP.*

8.2.4 La commande SHOW CDP NEIGHBORS

- Une fois l'accès à distance à un équipement d'interconnexion s'est produit avec succès, l'administrateur pourra passer à la prochaine étape qui consiste à découvrir les voisins directs de l'équipement en question, et ce en utilisant la commande SHOW CDP NEIGHBORS.
- Cette commande permet d'afficher pour chaque voisin directement connecté les informations indiquées dans la Figure 8.5.

8.2.5 La commande SHOW CDP ENTRY

- L'unique information pertinente que la commande SHOW CDP NEIGHBORS ne permet pas d'afficher et celle de l'adresse IP des équipements voisins.
- Cette information est obtenue en utilisant la commande SHOW CDP ENTRY (voir la Figure 8.6).

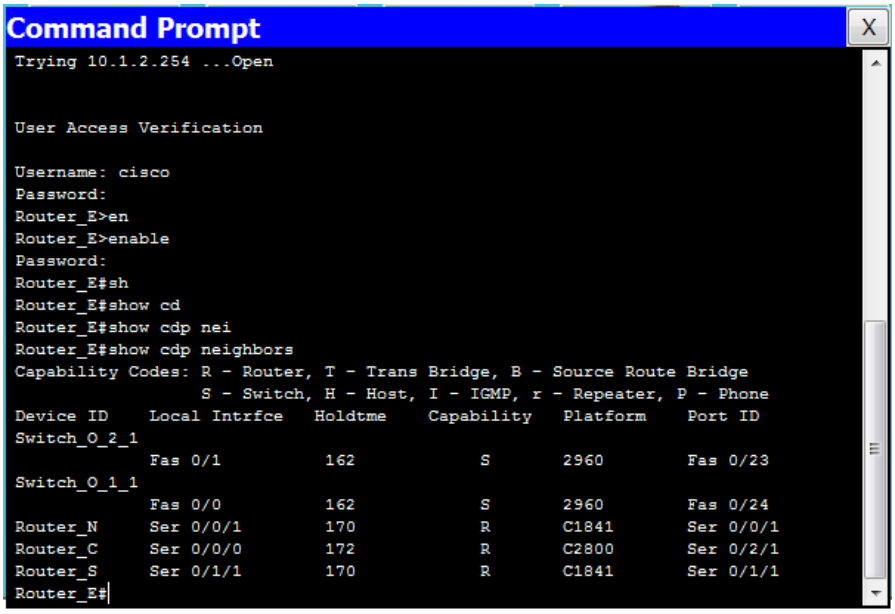


FIGURE 8.5: *TP 4 : La commande SHOW CDP NEIGHBORS.*

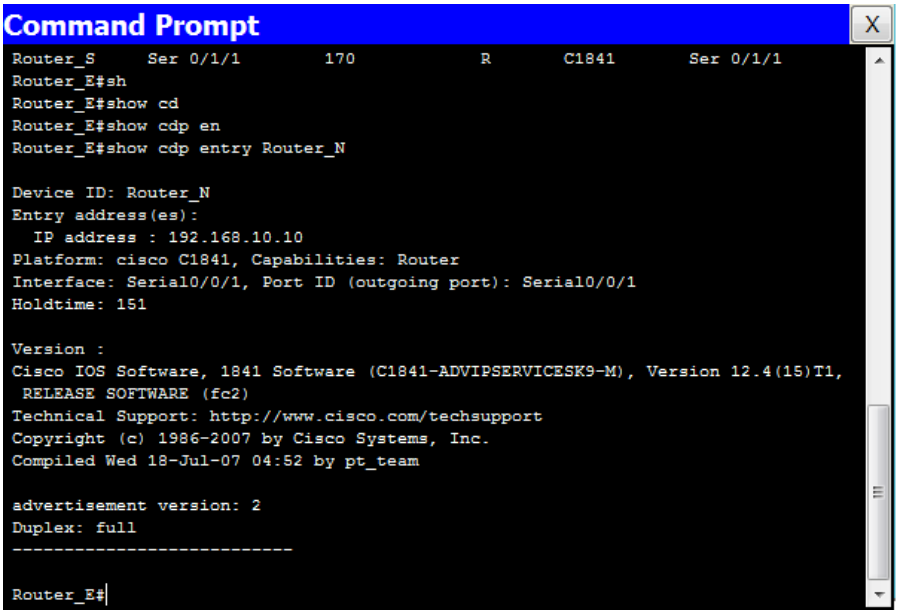


FIGURE 8.6: *TP 4 : La commande SHOW CDP ENTRY.*

Chapitre 9

Gestion du système IOS et des fichiers de configuration

9.1 L'énoncé du TP

- Le but de ce TP est d'apprendre à l'étudiant comment sauvegarder et restaurer le système IOS et les fichiers de configuration d'un équipement CISCO en utilisant le protocole TFTP.
- Pour cela, nous proposons la topologie de réseau représentée par la Figure 9.1.
- Le fichier source de cette topologie est disponible sur l'adresse https ://elearning.univ-bejaia.dz/course/view.php ?id=10372.
- Les mots de passe et les noms utilisateur sont tous "cisco".
- Le travail demandé est le suivant : (il doit se faire à partir de la station d'administration "PC-A")

A. En utilisant les commandes du protocole CDP (déjà présentées dans le chapitre précédent), construisez la cartographie du réseau ci-dessous.

B. En utilisant les commandes du protocole TFTP, effectuez les tâches suivantes :

1. Sauvegarder le système IOS de chacun des commutateurs et routeurs du réseau ci-dessous dans le serveur "Server-B". Nommer les copies des systèmes IOS sur

le serveur "Server-B" de la manière suivante : "**IOS**_*HOSTNAME-DEVICE_IP-ADDRESS-DEVICE_PLATFORM*.**bin**".

2. Vérifier si les copies des systèmes IOS ont été correctement sauvegardées sur le serveur "Server-B".
3. Remplacer les systèmes IOS existants sur les différents commutateurs et routeurs par les copies sauvegardées dans le serveur "Server-B".
4. Redémarrer les différents commutateurs et routeurs à chaque fois qu'une copie du système IOS est chargée.

C. En utilisant toujours les commandes TFTP, effectuez les tâches suivantes :

1. Sauvegarder le fichier de configuration "STARTUP-CONFIG" de chacun des commutateurs et routeurs du réseau ci-dessous dans le serveur "Server-C". Nommer les copies des fichiers de configuration sur le serveur "Server-C" de la manière suivante : "**STARTUP-CONFIG**_*HOSTNAME-DEVICE_IP-ADDRESS-DEVICE_PLATFORM*".
2. Vérifier si les copies des fichiers de configuration ont été correctement sauvegardées sur le serveur "Server-C".
3. Utiliser la commande "DESCRIPTION" du mode de configuration d'interface dans chacune des interfaces des commutateurs et routeurs identifiées dans la partie "A", afin de décrire les différentes interconnexions existantes entre les différents commutateurs et routeurs. La description doit de se faire de la manière suivante : "**FROM** *LOCAL-DEVICE* **TO** *REMOTE-DEVICE*". Il ne faudrait pas oublier de faire la commande "COPY RUNNING-CONFIG STARTUP-CONFIG"
4. Sauvegarder le fichier de configuration "RUNNING-CONFIG" de chacun des commutateurs et routeurs du réseau ci-dessous dans le serveur "Server-A". Nommer les copies des fichiers de configuration sur le serveur "Server-A" de la manière suivante : "**RUNNING-CONFIG**_*HOSTNAME-DEVICE_IP-ADDRESS-DEVICE_PLATFORM*".

5. Charger les copies des fichiers de configuration ”STARTUP-CONFIG” sauvegardées dans le serveur ”Server-C” dans leurs équipements respectifs. Il faudrait recopier ces dernières à la fois dans la mémoire RAM et dans la mémoire NVRAM (Non Volatil RAM).
6. Afficher et comparer les fichiers de configuration ”RUNNING-CONFIG” et ”STARTUP-CONFIG” de chacun des commutateurs et routeurs. Qu’est-ce que vous remarquez ? Qu’est-ce que vous en déduisez ?

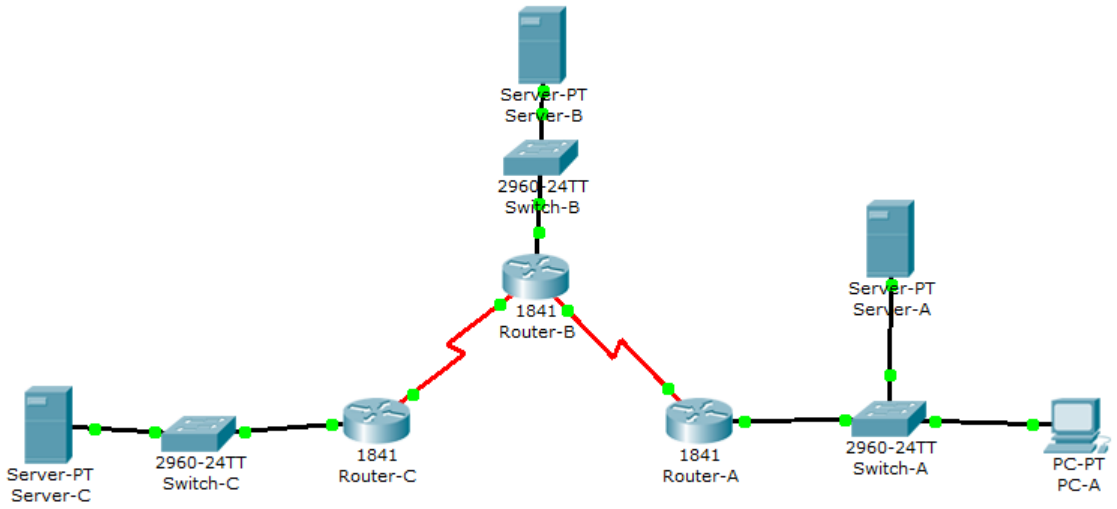


FIGURE 9.1: *TP 5 : Topologie du réseau.*

9.2 Les étapes de configuration

– La gestion du système IOS et des fichiers de configuration des équipements d’interconnexion d’un réseau est l’une des tâches les plus importantes d’un administrateur réseau.
– Cette tâche consiste à sauvegarder dans un serveur distant une copie du système IOS et des fichiers de configuration de chaque équipement d’interconnexion, et de les restaurer en cas de besoin (panne d’un équipement par exemple).
– La sauvegarde et la restauration du système IOS et des fichiers de configuration que l’administrateur réseau doit maîtriser à la perfection devraient réduire l’impact des pannes réseau sur le fonctionnement du réseau.

- Dans ce présent TP, nous allons expliquer à l'étudiant comment utiliser le protocole TFTP pour effectuer la sauvegarde et la restauration du système IOS et des fichiers de configuration d'un équipement d'interconnexion CISCO.
- à l'issue de ce TP, l'étudiant va devoir maîtriser les commandes du protocole TFTP pour gérer rapidement et efficacement le système IOS et les fichiers de configuration des équipements d'interconnexion de son réseau.
- Les étapes à suivre sont les suivantes :

9.2.1 Sauvegarde du système IOS

- La sauvegarde du système IOS d'un équipement d'interconnexion CISCO consiste à exporter une copie de de dernier dans un serveur distant.
- Le système IOS qui fait fonctionner les équipements CISCO se trouve dans une mémoire particulière dite FLASH.
- La Figure 9.2 montre comment utiliser les commandes du protocole TFTP pour sauvegarder une copie du système IOS du routeur ROUTEUR-A dans le serveur SERVEUR-B.
- La Figure 9.3 confirme que l'opération de sauvegarde s'est déroulée avec succès.

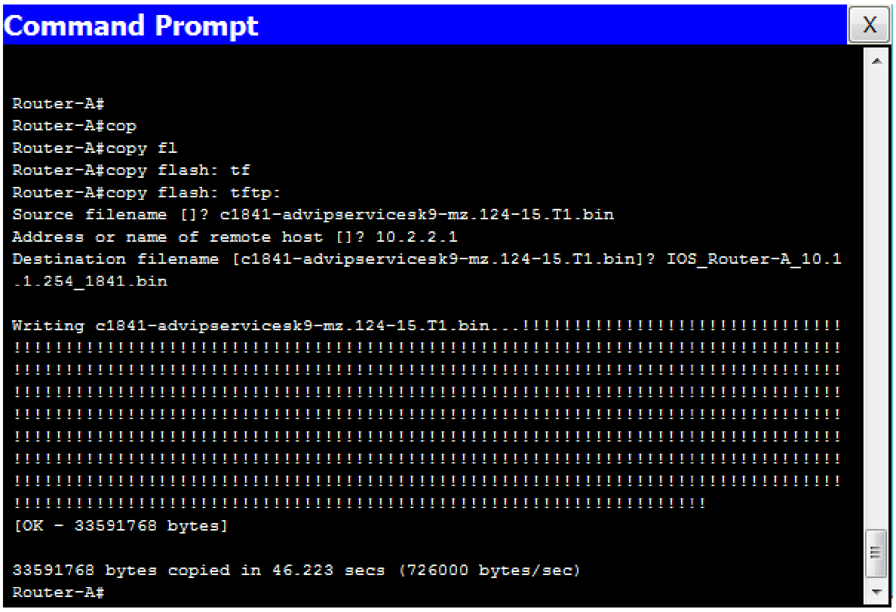


FIGURE 9.2: *TP 5 : Sauvegarde du système IOS.*

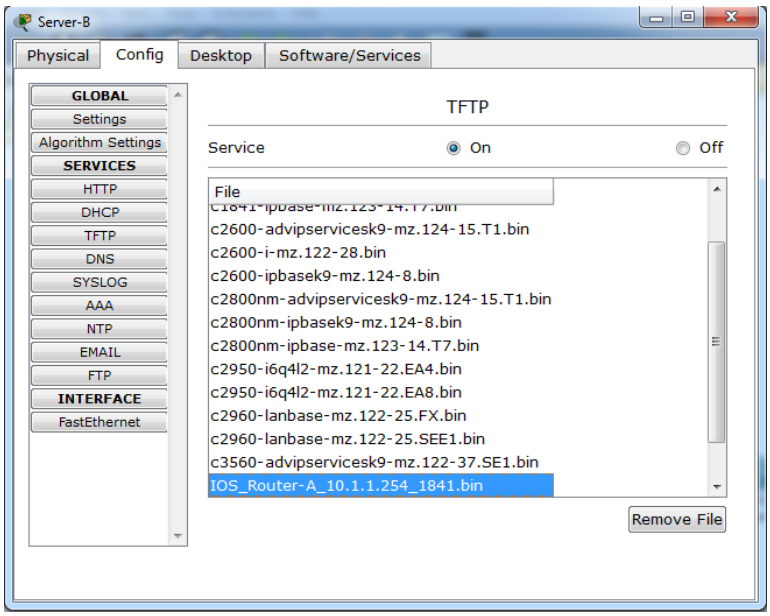


FIGURE 9.3: *TP 5 : Vérification de la sauvegarde du système IOS.*

9.2.2 Restauration du système IOS

- La restauration ou simplement la mise à jour d'un système IOS d'un équipement d'interconnexion CISCO consiste à importer depuis un serveur distant une version du système IOS autre que celle utilisée par l'équipement en question.
- Justement, avant de commencer l'opération de mise à jour, il est nécessaire de supprimer d'abord la version actuelle du système IOS.
- La Figure 9.4 montre comment supprimer le système IOS du routeur ROUTEUR-A.
- La Figure 9.5 montre comment utiliser les commandes du protocole TFTP pour restaurer le système IOS du routeur ROUTEUR-A à partir du serveur SERVEUR-B.
- La Figure 9.6 confirme que l'opération de restauration s'est déroulée avec succès.
- Bien évidemment, il ne faut pas oublier de redémarrer l'équipement en question afin qu'il applique la mise à jour effectuée.

9.2.3 Sauvegarde du fichier STARTUP-CONFIG

- La sauvegarde du fichier de configuration STARTUP-CONFIG d'un équipement d'interconnexion CISCO consiste à exporter une copie de ce dernier dans un serveur

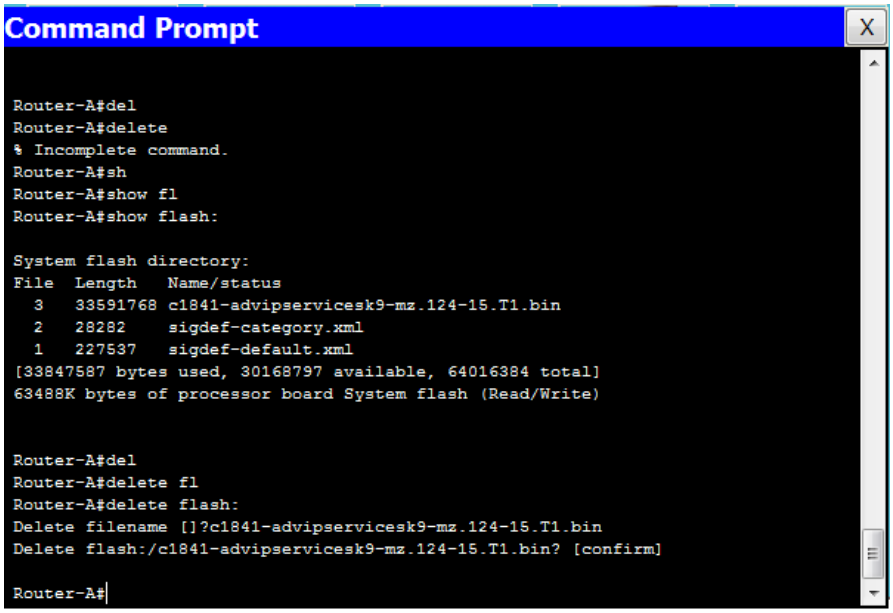


FIGURE 9.4: *TP 5 : Restauration du système IOS (étape 1).*

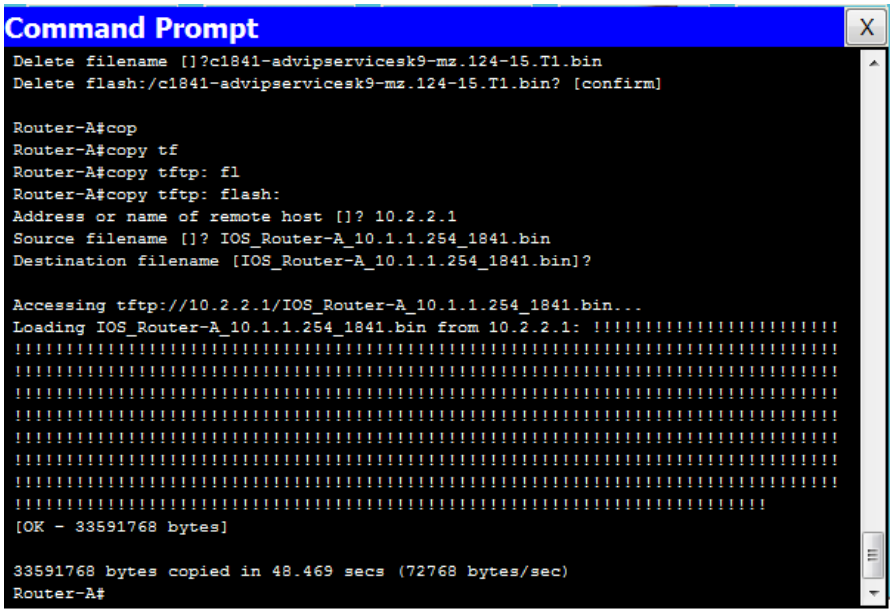


FIGURE 9.5: *TP 5 : Restauration du système IOS (étape 2).*

distant.

– Le fichier de configuration STARTUP-CONFIG contient la configuration enregistrée (permanente) de l'équipement en question. Ce fichier se trouve dans une mémoire spéciale appelée NVRAM.

– La Figure 9.7 montre comment utiliser les commandes du protocole TFTP pour

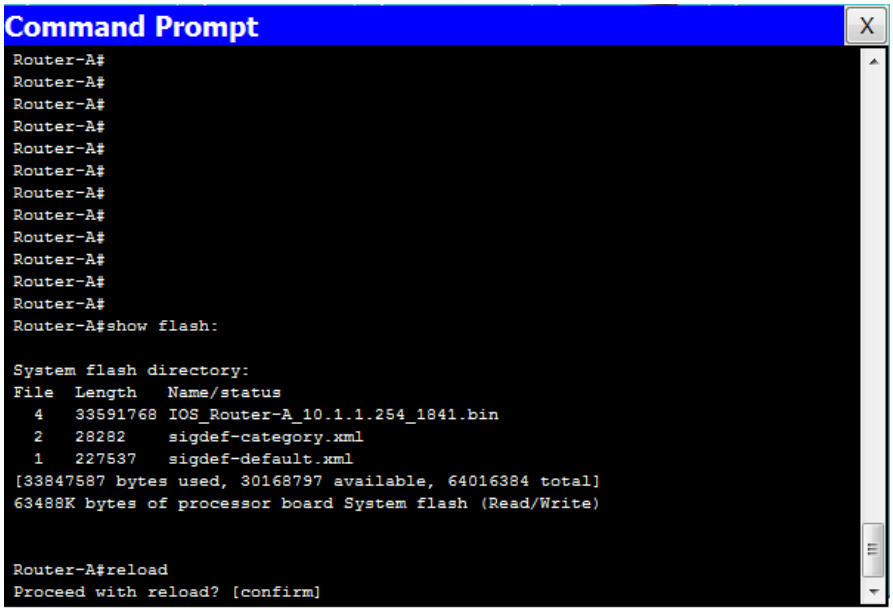


FIGURE 9.6: *TP 5 : Restauration du système IOS (étape 3).*

sauvegarder une copie du fichier STARTUP-CONFIG du routeur ROUTEUR-A dans le serveur SERVEUR-C.

– La Figure 9.8 confirme que l'opération de sauvegarde s'est déroulée avec succès.

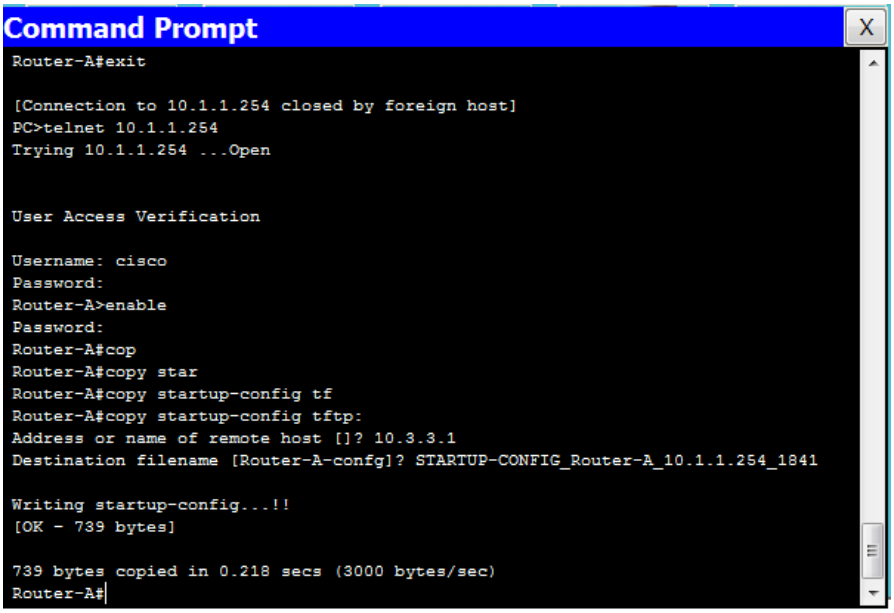


FIGURE 9.7: *TP 5 : Sauvegarde du fichier STARTUP-CONFIG.*

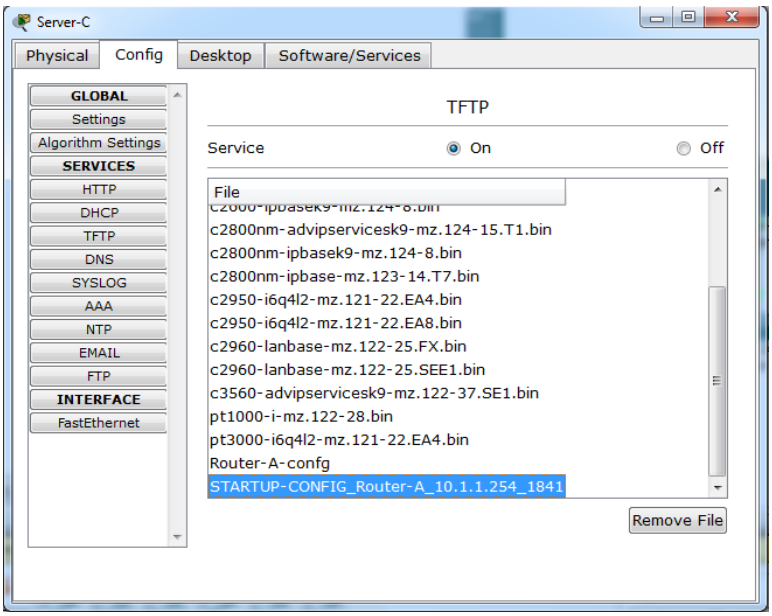


FIGURE 9.8: *TP 5 : Vérification de la sauvegarde du fichier STARTUP-CONFIG.*

9.2.4 Sauvegarde du fichier RUNNING-CONFIG

- La sauvegarde du fichier de configuration RUNNING-CONFIG d'un équipement d'interconnexion CISCO consiste à exporter une copie de ce dernier dans un serveur distant.
- Le fichier de configuration RUNNING-CONFIG contient la configuration non enregistrée (en cours) de l'équipement en question. Ce fichier se trouve dans une mémoire spéciale appelée RAM.
- La Figure 9.9 montre comment configurer la description de l'interface FastEthernet0/0 du routeur ROUTEUR-A. Évidemment, pour que cette modification du fichier RUNNING-CONFIG soit enregistrée de façon permanente, il faudrait utiliser la commande COPY RUNNING-CONFIG STARTUP-CONFIG.
- La Figure 9.10 montre comment utiliser les commandes du protocole TFTP pour sauvegarder une copie du fichier RUNNING-CONFIG du routeur ROUTEUR-A dans le serveur SERVEUR-A.
- La Figure 9.11 confirme que l'opération de sauvegarde s'est déroulée avec succès.

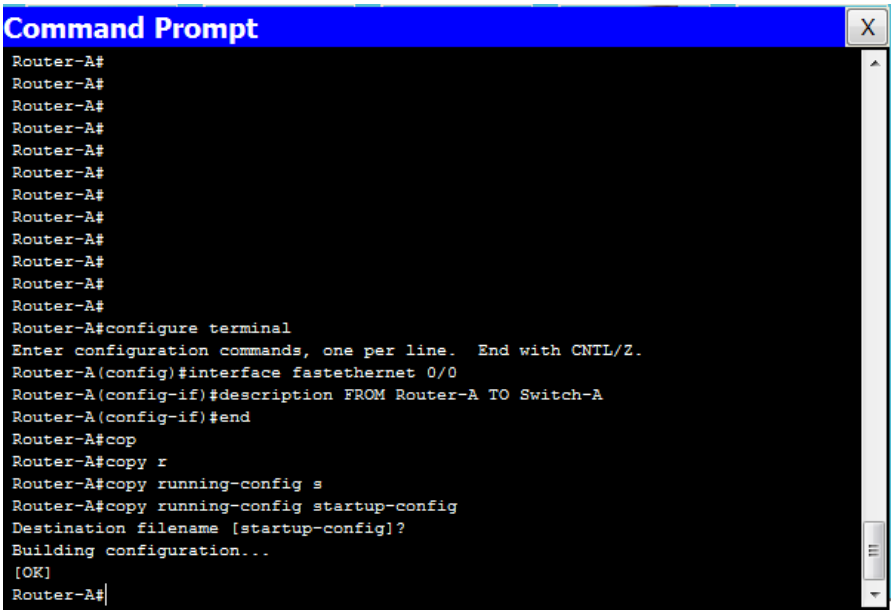


FIGURE 9.9: *TP 5 : Modification d'un fichier RUNNING-CONFIG.*

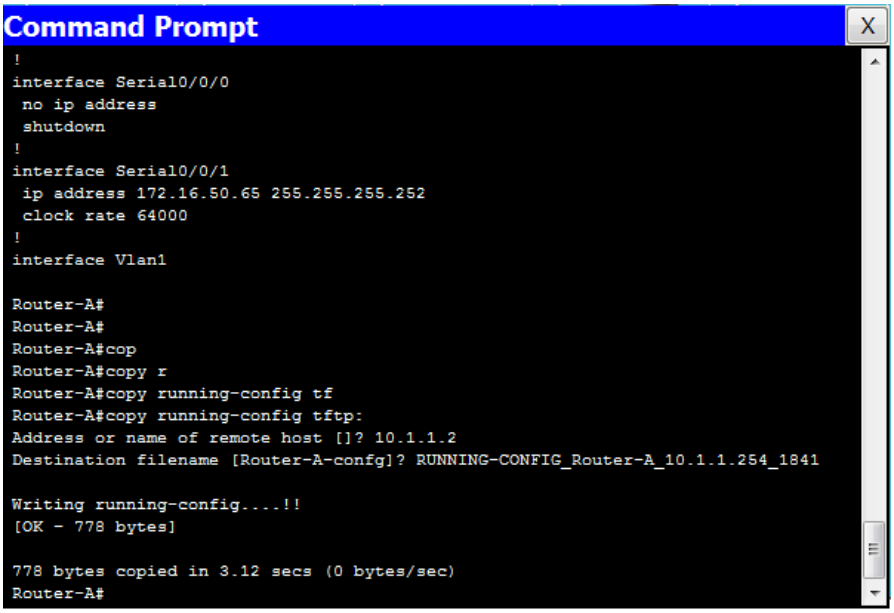


FIGURE 9.10: *TP 5 : Sauvegarde du fichier RUNNING-CONFIG.*

9.2.5 Restauration du fichier STARTUP-CONFIG dans la RAM

– La restauration dans la mémoire RAM du fichier STARTUP-CONFIG d'un équipement d'interconnexion CISCO consiste à importer depuis un serveur distant une version ultérieure de ce fichier dans la mémoire RAM de l'équipement en question.

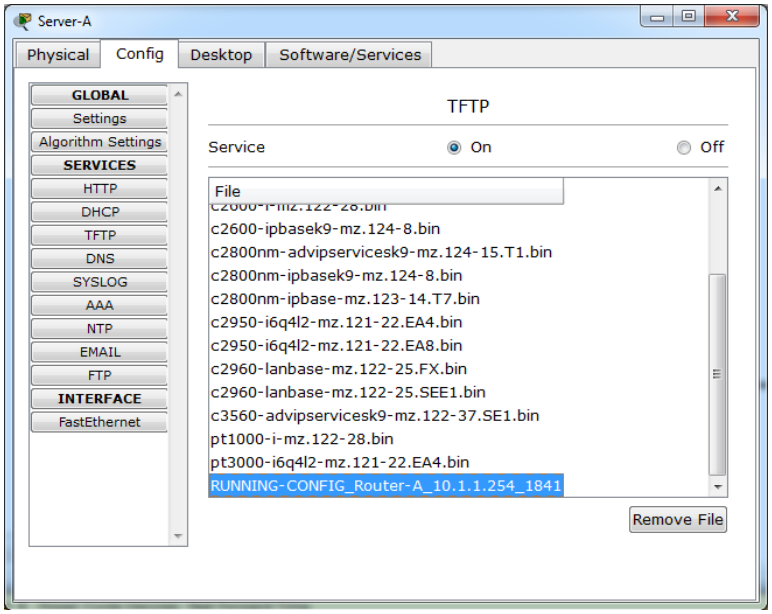


FIGURE 9.11: *TP 5 : Vérification de la sauvegarde du fichier RUNNING-CONFIG.*

– La Figure 9.12 montre comment utiliser les commandes du protocole TFTP pour restaurer dans la mémoire RAM du routeur ROUTEUR-A le fichier de configuration STARTUP-CONFIG à partir du serveur SERVEUR-C.

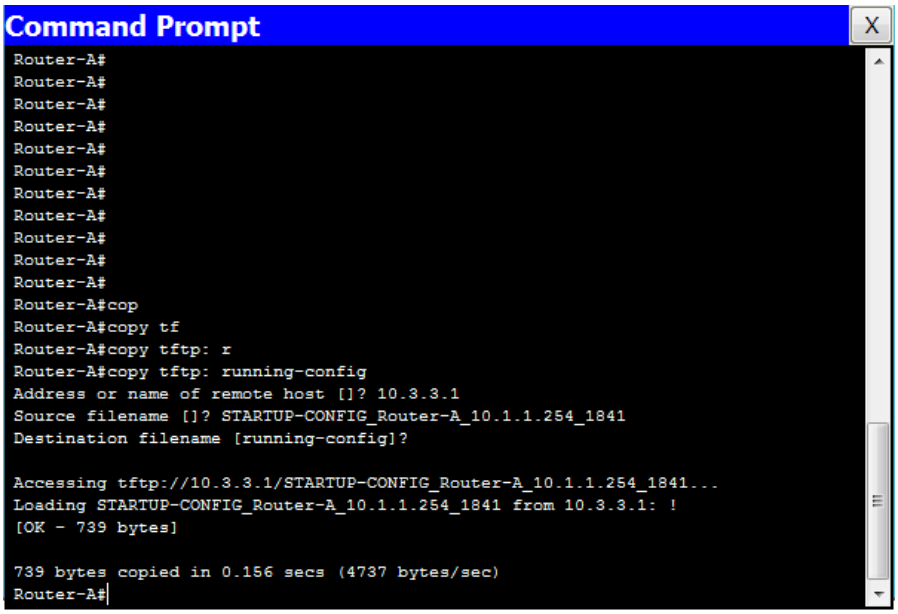


FIGURE 9.12: *TP 5 : Restauration du fichier STARTUP-CONFIG dans la RAM.*

9.2.6 Restauration du fichier STARTUP-CONFIG dans la NVRAM

– La restauration dans la mémoire NVRAM du fichier STARTUP-CONFIG d'un équipement d'interconnexion CISCO consiste à importer depuis un serveur distant une version ultérieure de ce fichier dans la mémoire NVRAM de l'équipement en question.

– La Figure 9.13 montre comment utiliser les commandes du protocole TFTP pour restaurer dans la mémoire NVRAM le fichier de configuration STARTUP-CONFIG du routeur ROUTEUR-A à partir du serveur SERVEUR-C.

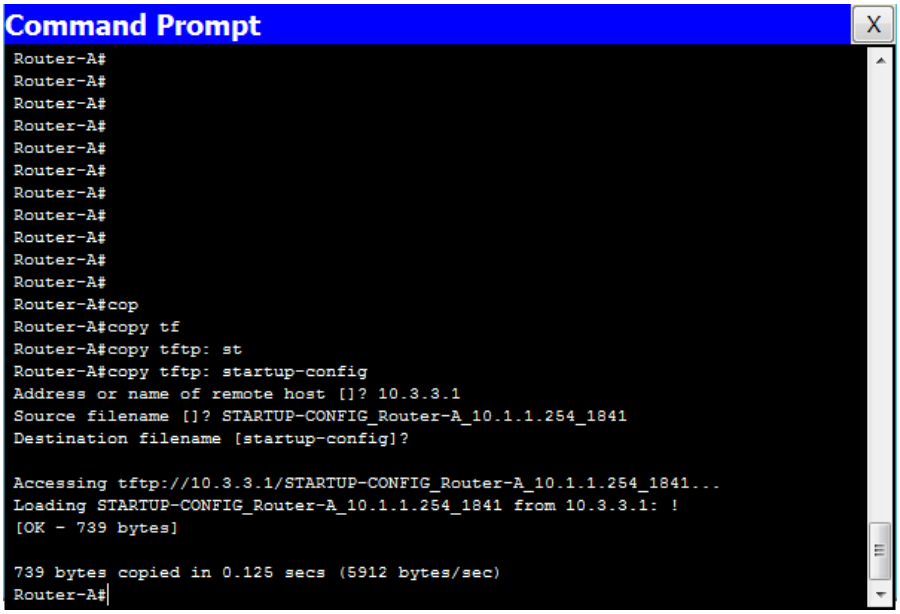


FIGURE 9.13: *TP 5 : Restauration du fichier STARTUP-CONFIG dans la NVRAM.*

9.2.7 Comparaison des fichiers RUNNING-CONFIG et STARTUP-CONFIG

– Les Figures 9.14 et 9.15 montrent clairement que lorsque la restauration d'un fichier de configuration se fait dans la mémoire RAM, seules les commandes configurées dans les deux fichiers source et destination sont écrasées et remplacées par les nouvelles lignes du fichier source.

– Par contre, lorsque la restauration se fait dans la mémoire NVRAM, le fichier

de configuration de destination est écrasé et complètement remplacé par le fichier source.

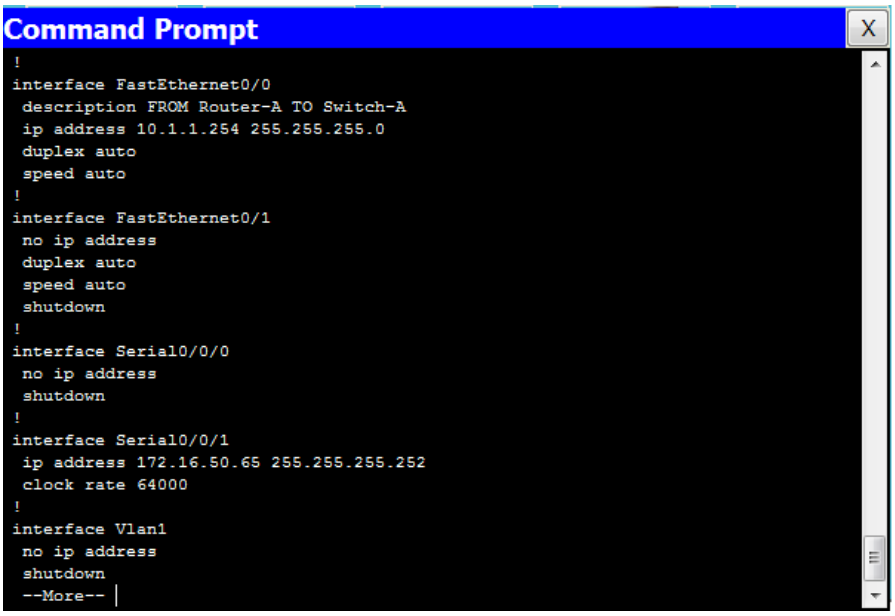


FIGURE 9.14: *TP 5 : Le fichier STARTUP-CONFIG.*

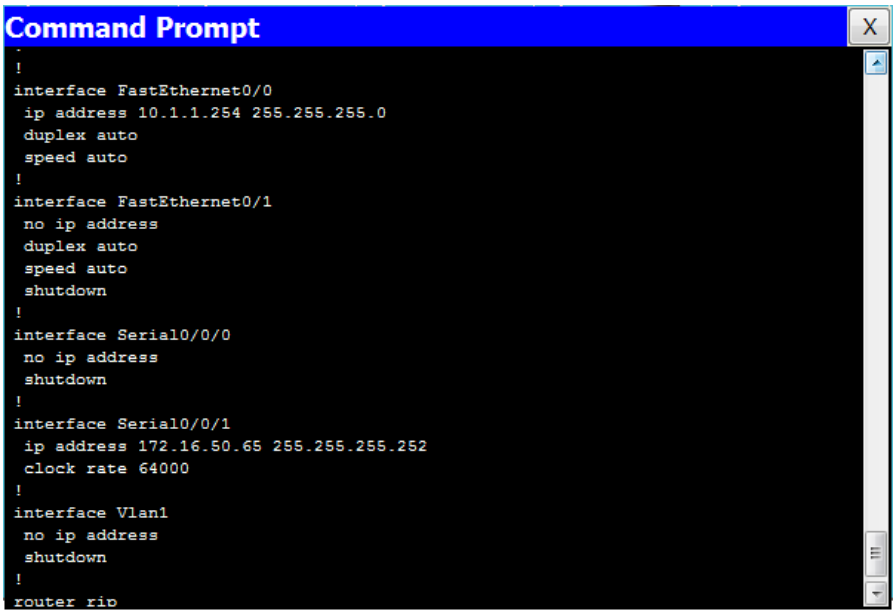


FIGURE 9.15: *TP 5 : Le fichier RUNNING-CONFIG.*

Troisième partie

Sujets d'examen avec corrigés

Chapitre A

Sujet d'examen 2017-2018 avec corrigé

A.1 Sujet d'examen

A.1.1 Partie théorique

1. Citer les caractéristiques que l'administrateur de réseaux doit recenser sur son réseau afin qu'il puisse l'administrer efficacement. Présenter brièvement la caractéristique la plus fondamentale et la plus critique. (02 pts)
2. Donner deux niveaux d'administration de réseaux avec une brève définition. (01 pts)
3. Quel est l'objectif global et le concept de base de l'administration des réseaux ? (0.5 pts)
4. Citer les tâches que l'administrateur de réseaux peut réaliser à travers l'administration des réseaux. Expliquer brièvement les deux tâches les plus élémentaires. (01.75 pts)
5. Donner les deux catégories d'environnements d'administration de réseaux. Quelle est la principale différence qui existe entre ces deux dernières ? (01 pts)
6. Compléter le tableau suivant (01 pts) :

Réseau, Equipement, ou Système à administrer	L'environnement d'administration le plus approprié
Réseaux Informatiques	
Réseaux de Télécommunication	
Applications et Bases de Données	
Serveurs Unix	

7. Quels sont les deux environnements d'administration de réseaux qui permettent d'unifier l'ensemble des environnements existants ? Justifier brièvement votre réponse. (0.75 pts)
8. Quelles sont les deux entités qui interviennent dans une communication SNMP. Quelle est la différence entre ses deux commandes TRAP et INFORM. (0 1 pts)
9. De quelle façon les variables SNMP sont-elles décrites ? Qu'est-ce qu'elles représentent ? Qu'est-ce qu'elles forment ? L'ensemble formé est-il unique ? (01 pts)

A.1.2 Partie pratique

1. Quels sont les ports de configuration et les outils d'accès à distance des équipements CISCO ? (01 pts)
2. Quelles sont les deux touches du clavier qui facilitent à l'administrateur de réseaux de se rappeler des commandes de configuration CISCO ? Quel est le rôle de chacune ? (01 pts)
3. Quelle est l'interface à utiliser et les commandes à saisir pour configurer l'@ IP de management d'un commutateur CISCO ? (01 pts)
4. Quelle est la similarité et les différences entre TELNET, SSH et SNMP ? (01 pts)
5. Quel est le rôle de chacune de ces commandes CISCO : SHOW IP PROTOCOLS, SHOW IP ROUTE, DEBUG IP RIP ? (01.5 pts)
6. Quel est le protocole CISCO et la commande principale de ce dernier qui aident l'administrateur de réseaux à construire la cartographie de son réseau ? (01 pts)
7. Donner les trois composants matériels les plus importants d'un routeur CISCO. Donner également le logiciel contenu dans ces composants. (03 pts)

8. Rayer les commandes qui peuvent engendrer des incohérences lors de la gestion du fichier de configuration : COPY RUN START, COPY START RUN, COPY RUN TFTP, COPY TFTP RUN, COPY START TFTP, COPY TFTP START. (0.5 pts)

A.2 Corrigé type

A.2.1 Partie théorique

1. – La typologie (ou la finalité), l'étendu, les architectures de protocoles, les équipements, les applications, les usagers. (1.5 pts)
   – Un réseau peut avoir deux finalités : celle de servir d'autres réseaux et celle de servir directement les utilisateurs finaux. (0.5 pts)
2. – L'administration de l'infrastructure réseau : elle concerne l'administration des équipements d'interconnexion du réseau. (0.5 pts)
   – L'administration des desktops : elle concerne l'administration des points d'accès au réseau. (0.5 pts)
3. – Assurer le fonctionnement du réseau (0.25 pts)
   – à distance (0.25 pts)
4. – Gestion de la configuration, gestion des fautes, gestion des performances, gestion des coûts et gestion de la sécurité. (01.25 pts)
   – Gestion de la configuration : désigner et paramétrer les différents équipements du réseau. (0.25 pts)
   – Gestion des fautes : détecter, localiser et réparer les pannes. (0.25 pts)
5. – Environnements d'administration standards et environnements d'administration propriétaires. (0.5 pts)
   – Un environnement d'administration standard permet des gérer tous types d'équipements qui met en œuvre des fonctions de gestion standard. (0.25 pts)
   – Un environnement d'administration propriétaire ne permet de gérer que les équipements du propriétaire. (0.25 pts)
6. Compléter le tableau suivant (01 pts) :

Réseau, Equipement, ou Système à administrer	L'environnement d'administration le plus approprié
Réseaux Informatiques	SNMP (0.25 pts)
Réseaux de Télécommunication	TMN/CMIP (0.25 pts)
Applications et Bases de Données	DMI/CIM/WBEM (0.25 pts)
Serveurs Unix	DME (0.25 pts)

7. – OMA et JMX. (0.5 pts)
   – Ils sont basés sur le principe " Objet distribué " (0.25 pts)
8. – La station de gestion et l'agent SNMP. (0,5 pts)
   – TRAP permet de signaler un évènement. (0,25 pts)
   – INFORM permet d'obtenir une réponse à une TRAP. (0,25 pts)
9. – Une série de numéros. (0,25 pts)
   – Un ensemble d'objets. (0,25 pts)
   – MIB. (0,25 pts)
   – N'est pas unique. (0,25 pts)

A.2.2 Partie pratique

1. – Le port console et le port auxiliaire. (0,5 pts)
   – TELNET et SSH. (0,5 pts)
2. – La touche point d'interrogation : elle permet d'enlever l'ambiguïté sur une commande. (0,5 pts)
   – La touche tabulation : elle permet d'écrire entièrement une commande. (0,5 pts)
3. – VLAN 1. (0,25 pts)
   – Interface vlan 1, ip address @IP mask, no shutdown. (0,75 pts)
4. – C'est des outils d'accès à distance. (0,25 pts)
   – TELNET est un outil non sécurisé. (0,25 pts)
   – SSH est un outil sécurisé. (0,25 pts)
   – SNMP gère tous les équipements de la même façon. (0,25 pts)

5. – SHOW IP PROTOCOLS : affiche des informations sur le protocole de routage configuré. (0,5 pts)
   – SHOW IP ROUTE : affiche la table de routage. (0,5 pts)
   – DEBUG IP RIP : affiche en temps réel les mises à jour de routage. (0,5 pts)
6. – CDP. (0,5 pts)
   – Sh cdp neighbors. (0,5 pts)
7. – RAM (0,5 pts) -> Running-config (0,5 pts)
   – NVRAM (0,5 pts) -> Startup-config (0,5 pts)
   – Flash (0,5 pts) -> IOS software (0,5 pts)
8. – COPY START RUN (0.25 pts)
   – COPY TFTP RUN (0.25 pts)

Chapitre B

Sujet d'examen 2018-2019 avec corrigé

B.1 Sujet d'examen

B.1.1 Partie théorique

1. Citer les différents types de commutation de données existants. Spécifier le type de commutation utilisé dans les réseaux suivants : INTERNET et ATM. (01.50 pts)
2. Quelle est la pile protocolaire qui ressemble plus à TCP/IP ? Dites pourquoi ? (0.75 pts)
3. Donner par ordre les activités communes d'un administrateur de réseaux par rapport à n'importe quel domaine fonctionnel de l'administration de réseaux. (0.75 pts)
4. Pour gérer les pannes d'un réseau, l'administrateur de réseaux suit une procédure bien spécifique. Citer les quatre étapes de cette procédure. (01 pts)
5. Parmi les tâches de l'administrateur de réseaux, nous distinguons la gestion de la comptabilité. Donner un exemple simple et concret de cette tâche de gestion. (0.50 pts)
6. Pourquoi SNMP est l'environnement d'administration le plus déployé. (0.50 pts)

7. Citer les trois environnements d'administration proposés par le consortium DMTF. Quelle est la particularité de ces derniers ? (01 pts)
8. Expliquer à l'aide d'un organigramme la méthode à suivre pour choisir un environnement d'administration de réseaux. (02 pts)
9. Citer les deux ports désignés pour l'utilisation de SNMP. Quel est le rôle de chacun de ces ports ? (01 pts)
10. Expliquer brièvement le principe d'une variable SNMP. (0.50 pts)
11. SNMP propose-t-il réellement un environnement d'administration sécurisé ? Justifier votre réponse. (0.50 pts)

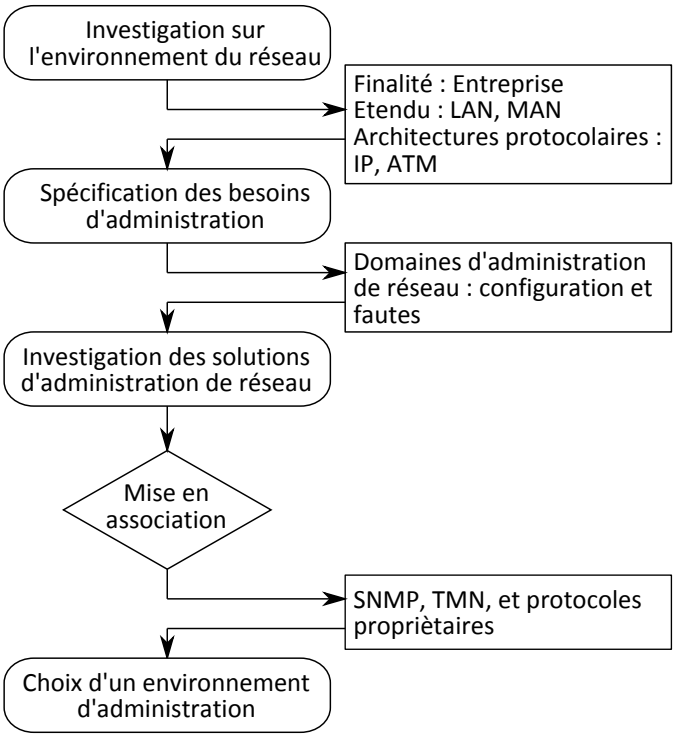
B.1.2 Partie pratique

1. Est-il obligatoire de configurer le nom d'un équipement CISCO pour que certaines fonctionnalités de ce dernier puissent être réalisées ? Si la réponse est négative, il faudra alors donner un exemple. (01 pts)
2. Pendant les séances de TPs, les étudiants ont tendance à oublier de configurer la passerelle par défaut des commutateurs. Elle sert à quoi cette dernière et donner les commandes permettant de la configurer. (01 pts)
3. Quelles sont les deux méthodes permettant de construire des sous-réseaux ? Quel est l'avantage de chacune ? (01 pts)
4. Une table de routage est composée d'un ensemble de routes. Quelles sont les informations fournies par une route ? (01 pts)
5. Cisco propose le protocole CDP pour construire la cartographie du réseau. Expliquer les étapes d'utilisation de ce protocole. (02 pts)
6. Citer les cinq mémoires que comporte un équipement CISCO. Donner le contenu de chacune de ces dernières. (02.50 pts)
7. Pour gérer la partie logicielle d'un équipement CISCO, nous faisons généralement recours au protocole TFTP. Donner les différentes façons (à l'aide de commandes) permettant d'utiliser ce protocole. (01.50 pts)

B.2 Corrigé type

B.2.1 Partie théorique

1. – Circuit, Message, Paquet, Cellule. (01 pts)
   – Internet -> Paquet, ATM -> Cellule. (0.50 pts)
2. – IPX/SPX. (0.25 pts)
   – IPX -> IP, SPX -> TCP. (0.50 pts)
3. – Collecte de données de gestion. (0.25 pts)
   – Interprétation de ces données. (0.25 pts)
   – Contrôle des éléments du réseau. (0.25 pts)
4. – Détection des pannes. (0.25 pts)
   – Localisation des pannes. (0.25 pts)
   – Réparation des pannes. (0.25 pts)
   – Rétablissement du service. (0.25 pts)
5. La gestion des abonnements téléphoniques. (0.50 pts)
6. SNMP fait partie de la pile protocolaire TCP/IP. (0.50 pts)
7. – DMI/CIM/WBEM. (0.75 pts)
   – Gestion des postes de travail. (0.25 pts)
8. (02 pts)
9. – 161 -> Requêtes à un agent SNMP. (0.50 pts)
   – 162 -> Alarmes à une station d'administration. (0.50 pts)
10. – Une variable SNMP est une suite d'objets. (0.25 pts)
    – Chacun object est identifié par un numéro appelé OID. (0.25 pts)
11. – SNMP ne propose pas réellement un environnement sécurisé. (0.25 pts)
    – SNMPv1 et SNMPv2 ne sont pas vraiment sécurisés. SNMPv3 n'est pas complètement implémenté. (0.25 pts)



B.2.2 Partie pratique

1. – Oui. (0.250 pts)
   – SSH. (0.250 pts)
2. – La passerelle par défaut permet aux commutateurs de communiquer avec des d'autres équipements qui ne sont pas dans le même réseau. (0.50 pts)
   – ip default getway @IP. (0.50 pts)
3. – CIDR -> facile à utilizer. (0.50 pts)
   – VLSM -> gère efficacement les @IP. (0.50 pts)
4. – @IP du réseau de destination. (0.25 pts)
   – @IP du prochain saut/ Interface de sortie. (0.25 pts)
   – Type de la route : directement connecté/ Statique/ Type du protocole de routage. (0.25 pts)
   – Métrique de performance. (0.25 pts)
5. – ipconfig -> obtenir @IP de la station d'administration et celle de la passerelle par défaut. (0.50 pts)

- Telnet -> se connecter à la passerelle par défaut. (0.50 pts)
- Show cdp neighbors -> obtenir nom, plateforme, interfaces de connexion. (0.50 pts)
- Show cdp entry -> obtenir @IP des équipements directement connetctés à la passerelle par défaut. (0.50 pts)

6. – Flash -> Système IOS. (0.50 pts)
   - NVRAM -> Stratup Config. (0.50 pts)
   - RAM -> Running Config. (0.50 pts)
   - ROM -> Bootstrap + POST. (0.50 pts)
   - Registre de configuration -> Numéro indiquant le type de sémarrage de l'équipement. (0.50 pts)
7. – Copy run TFTP. (0.25 pts)
   - Copy start TFTP. (0.25 pts)
   - Copy flash TFTP. (0.25 pts)
   - Copy TFTP run. (0.25 pts)
   - Copy TFTP start. (0.25 pts)
   - Copy TFTP flash. (0.25 pts)

Chapitre C

Sujet d'examen 2019-2020 avec corrigé

C.1 Sujet d'examen

C.1.1 Partie théorique

1. Citer les trois versions existantes du protocole SNMP. Comparer ces trois versions par rapport au niveau de sécurité assuré. (01.75 pts)
2. Citer les trois réponses SNMP pouvant se produire lorsqu'une requête SNMP est expédiée à un agent SNMP. Donner pour chacun de ces cas un exemple permettant de le produire. (01.50 pts)
3. Expliquer le rôle du site www.snmplink.org . (0.50 pts)
4. Quel est l'environnement d'administration standard le plus répandu ? Pourquoi ? (0.50 pts)
5. CiscoWorks est-il un environnement d'administration standard ? pourrait-il gérer des équipements basés sur la pile protocolaire TCP/IP ? (0.50 pts)
6. Quels sont les deux éléments essentiels du réseau à prendre en considération lorsqu'on choisit un environnement d'administration. (0.50 pts)

7. Est-il possible qu'un équipement réseau soit administré par un environnement standard et un autre propriétaire ? Justifier votre réponse. (0.75 pts)
8. Quelle est la configuration minimale à effectuer sur un équipement réseau avant de le placer dans une armoire de brassage ? (0.75 pts)
9. Quel est le but de la gestion de performance ? Quels sont ses types ? Donner leur principe de base. (01.50 pts)
10. Dans la gestion des pannes, faudrait-il faire participer les utilisateurs ? Comment ? (0.75 pts)
11. Citer les quatre types de commutation existants accompagnés d'une brève définition ? (02 pts)

C.1.2 Partie pratique

1. Quel est l'objectif du protocole CDP ? Donner la procédure à suivre étape par étape pour atteindre cet objectif. (02.25 pts)
2. Donner la procédure à suivre pour mettre à jour le système IOS d'un équipement CISCO à partir d'un serveur TFTP. (01 pts)
3. Donner la procédure à suivre pour restaurer la configuration d'un équipement CISCO à partir d'un serveur TFTP. (01 pts)
4. Quelle est la différence entre les deux commandes SHOW et DEGUG ? (01 pts)
5. Dans quel cas est-il obligatoire de configurer la commande NO AUTO-SUMMARY avec le protocole RIPv2 ? Pourquoi ? (01 pts)
6. Quelles sont les deux informations les plus importantes retournées par la commande SHOW IP PROTOCOLS ? (01 pts)
7. Quelle est le but principal dernier la subdivision d'un réseau en sous-réseau ? Comment cet objectif est-il atteint dans la pratique ? (01 pts)
8. Quel est le rôle de la commande PORT SECURITY ? Quand est-ce qu'elle est généralement utilisée ? (0.75 pts)

C.2 Corrigé type

C.2.1 Partie théorique

1. – SNMPv1, SNMPv2, et SNMPv3 (0.75 pts)
   – SNMPV1 et SNMPv2 utilisent une chaine de communauté (0.25 pts)
   – SNMPv3 a trois modèles de sécurité :
   – Modèle 1 utilise une chaine de communauté. (0.25 pts)
   – Modèle 2 possède des capacités d'authentification. (0.25 pts)
   – Modèle 3 rajoute au modèle 2 un niveau de cryptage supplémentaire. (0.25 pts)
2. – Aucune réponse (0.25 pts) : absence d'un agent SNMP. (0.25 pts)
   – Requête avec échec (0.25 pts) : la variable spécifiée n'existe pas. (0.25 pts)
   – Requête avec succès (0.25 pts) : retour de la valeur demandée. (0.25 pts)
3. www.snmplink.org permet de visualiser l'arbre des MIBs (0.25 pts) et de rechercher une variable au sein de celui-ci (0.25 pts).
4. SNMP (0.25 pts) car il est fait partie de la pile protocolaire TCP/IP (0.25 pts).
5. – NON. (0.25 pts)
   – OUI. (0.25 pts)
6. Les équipements d'interconnexion (0.25 pts), et la pile protocolaire (0.25 pts).
7. – OUI. (0.25 pts)
   – Pour utiliser un environnement standard, il faut que l'équipement autorise la gestion standard. (0.25 pts)
   – Pour utiliser un environnement propriétaire, il faut que l'équipement appartienne au même propriétaire que celui de l'environnement. (0.25 pts)
8. – Sécuriser les ports d'accès (physiques et virtuels). (0.25 pts)
   – Configurer une @IP de gestion. (0.25 pts)
   – Configurer l'accès à distance. (0.25 pts)
9. – Gestion de performance : son but final est la planification des ressources réseaux. (0.25 pts)
   – Il existe deux types : gestion proactive (0.25 pts) et gestion réactive. (0.25 pts)

- Gestion proactive : consiste à prendre des mesures initiales pour ne pas arriver à un état critique. (0.25 pts)
- Gestion réactive : vise à établir lors de la détection d'un problème des mesures correctives. (0.25 pts)

10. – OUI. (0.25 pts)
    – En les formant sur les éventuelles pannes que les utilisateurs peuvent signaler sans que le personnel réseau puisse intervenir directement. (0.50 pts)
11. – Commutation de circuit (0.25 pts) : un circuit physique est établi entre la source et la destination (0.25 pts).
    – Commutation de messages (0.25 pts) : des messages entiers sont transférés d'un nœud à un autre jusqu'à atteindre la destination (0.25 pts).
    – Commutation de paquets (0.25 pts) : un message est découpé en paquets qui sont transférés indépendamment les uns des autres jusqu'à atteindre la destination (0.25 pts).
    – Commutation de cellules (0.25 pts) : un message est découpé en cellules de tailles fixes sont toutes transférés sur le même circuit virtuel (0.25 pts).

C.2.2 Partie pratique

1. – Construire la cartographie du réseau. (0.25 pts)
   – Les étapes sont :
   (a) Ipconfig sur la station d'administration (0.25 pts) : obtenir l'@IP de la passerelle par défaut (0.25 pts).
   (b) Telnet @IP passerelle (0.25 pts) : accéder au premier équipement du réseau (0.25 pts).
   (c) Show CDP neibghbors (0.25 pts) : afficher les voisins directs du premier équipement (passerelle) (0.25 pts).
   (d) Show CDP entry + nom d'un voisin (0.25 pts) : afficher son @IP (0.25 pts).
2. – Telnet @IP équipement à mettre à jour. (0.25 pts)
   – Copy TFTP Flash. (0.25 pts)

- Introduire @ IP du serveur TFTP. (0.25 pts)
- Préciser le nom du système à charger. (0.25 pts)

3. - Telnet @IP équipement à restaurer. (0.25 pts)
   - Copy TFTP STARTUP. (0.25 pts)
   - Introduire @ IP du serveur TFTP. (0.25 pts)
   - Reload. (0.25 pts)
4. - SHOW : afficher des données statiques. (0.50 pts)
   - DEBUG : afficher des données dynamiques. (0.50 pts)
5. - Dans le cas des réseaux dont les plages d'@ appartiennent à la même classe. (0.50 pts)
   - Pour éviter que les routes soient résumées. (0.50 pts)
6. - Afficher les réseaux à diffuser. (0.50 pts)
   - Afficher les sources des mises à jour de routage. (0.50 pts)
7. - Avoir plusieurs domaines de diffusion. (0.50 pts)
   - VLANs. (0.50 pts)
8. - Protéger les prises réseaux des utilisateurs. (0.50 pts)
   - Dans le cas des VLANs (sous-réseaux). (0.25 pts)

Bibliographie

Uyless Black. *Network Management Standards : Snmp, Cmip, Tmn, Mibs, and Object Libraries*. McGraw-Hill Inc.,US, 1995.

Pierre Cabantous. *Les réseaux informatiques - Guide pratique pour l'administration et la supervision*. Editions ENI, 2019.

José Dordoigne. *Les réseaux : Entraînez-vous à l'administration d'un réseau*. Editions ENI, 2004.

Craig Hunt. *TCP/IP Network Administration*. O'Reilly, 2002.