Introduction à TCP/IP et aux routeurs de type IOS (Cisco)

Alexandre Dulaunoy (alex@thinkingsecure.com)

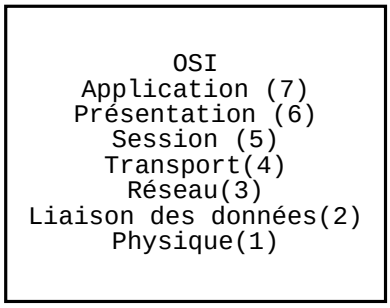
Version 0.1b/PDF

Table des matières

1 Introduction

1.1 Modèle OSI

Le but de l'OSI(ISO) est de créer un modèle idéal ou chaque couche effectue une tâche définie et dépend des services de la couche inférieure. Chaque couche donc fournit ses propres services à la couche supérieure.



Couche physique (1) La couche physique transfère les bits à travers un canal de communication. Ses bits encodés peuvent être en numérique mais aussi en analogique. Cette couche transmet les bits venant de la couche de données à l'interface physique et inversément. (support physique : Paire torsadée, coaxial, FO...)

Couche liaison de données (2) La couche liaison de données prend les données de la couche physique et fournit ses services à la couche réseau. Les bits reçus sont assemblés en trames[1]. (liaison possible : Ethernet, Frame Relay, X.25, PPP...)

Couche réseau (3) La couche réseau gère les connexions entre les noeuds du réseau. Un routeur, par exemple, travaille au minimum dans cette couche. Dans le modèle TCP/IP, la fonction de la couche réseau est assurée par IP[2]. (IPv4 ou IPv6)

Couche transport (4) La couche de transport offre des services supplémentaires par rapport à la couche réseau. Cette couche garantit l'intégrité des données. Son travail consiste à relier un sous-réseau non fiable à un réseau plus fiable. Dans le modèle TCP/IP, la fonction de la couche transport est assurée par TCP[3] et par le protocole UDP[4].

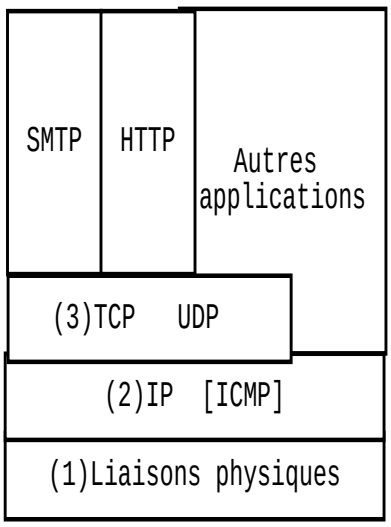
[1] Unité logique de bits assemblés.
[2] Internet Protocol
[3] Transmission Control Protocol
[4] User Datagram Protocol

Couche session (5) La couche de session gère les connexions entre les applications coopérantes. Le modèle TCP/IP ne possède pas de couche de session car TCP fournit une grande partie des fonctionnalités de session. Mais le service NFS, par exemple, peut utiliser le protocole RPC qui lui, est dans la couche de session. Beaucoup d'applications TCP n'utilisent pas les services de la couche session.

Couche présentation (6) La couche de présentation gère la représentation des données. Pour représenter les données, il existe ASCII, EBCDIC... Un langage commun doit être utilisé pour une bonne compréhension entre les différents noeuds du réseau. Par exemple, il existe le langage ASN.1 pour la représentation des données en SNMP (XDR pour NFS, Base64 pour SMTP...). Plusieurs applications TCP n'utilisent pas les services de cette couche.

Couche d'application (7) La couche d'application fournit les protocoles et les fonctions nécessaires pour les applications clients. Il existe un nombre important de services fournis par la couche d'application. Dans le modèle TCP/IP, on peut citer comme services : FTP,SMTP,POP3,HTTP[5].

1.2 Modèle TCP/IP



1.2.1 TCP / UDP

TCP et UDP sont les deux protocoles principaux dans la couche de transport. TCP et UDP utilisent IP comme couche réseau. TCP procure une couche de transport fiable, même si le service qu'il (IP) utilise ne l'est pas. TCP est orienté connexion, c'est-à-dire qu'il réalise une communication complète entre 2 points. Cela permet d'effectuer une communication client/serveur, par exemple, sans se préoccuper du chemin emprunté.

UDP émet et reçoit des datagrammes[6]. Cependant, contrairement à TCP, UDP n'est pas fiable et n'est pas orienté connexion. Il est utilisé pour les résolutions DNS et aussi pour TFTP.

[5] Nous montrerons des exemples d'intéraction avec ces services, un peu plus loin.
[6] unité d'information

1.2.2 IP

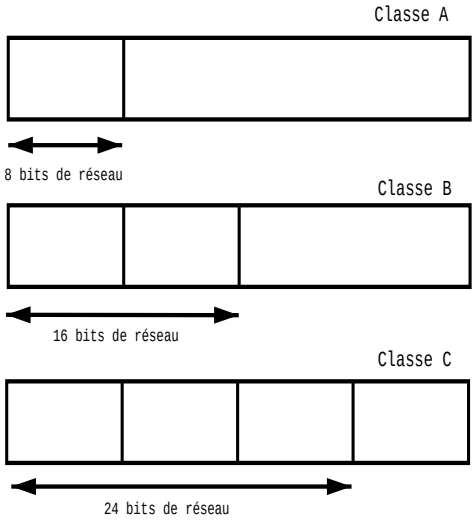
IP est le protocole principal de la couche réseau. Il est utilisé à la fois par TCP et UDP. Chaque bloc de données TCP,UDP, ICMP et IGMP qui circule est **encapsulé dans de l'IP**. IP est non fiable et n'est pas orienté connexion (contrairement à SNA par exemple).

Par non fiable, nous voulons dire qu'il n'existe aucune garantie pour que le datagramme IP arrive à la destination. Si, par exemple, un datagramme IP arrive à un routeur saturé, le routeur efface le paquet et envoie un message ICMP "unreachable" à la source. La fiabilité d'une connexion doit être maintenue par TCP.

"Pas orienté connexion", signifie que IP ne maintient aucune information d'état concernant les datagrammes successifs. Le trajet des datagrammes pour atteindre B à partir de A, n'est peut être pas le même. Les datagrammes peuvent également arriver dans le désordre par exemple. L'avantage majeur de cette technique du moindre effort, c'est la grande tolérance, notamment, vis-à-vis des pannes de l'infrastructure.

Masque de sous-réseau Outre l'adresse IP, une machine doit aussi connaître le nombre de bits attribués à l'identification du sous-réseau et à l'identificateur de machine. Ces informations sont fournies par le masque de sous-réseau (netmask). Ce masque est un masque de 32 bits (pour IPv4) contenant soit des bits à 1 pour l'identification du réseau et des bits à 0 pour l'identification de machines.

Dans la première implémentation d'IP, un militaire (? ! ?) décida de couper en plusieurs classes :



Mais ce fut une très mauvaise idée, car beaucoup de réseaux étaient trop grands pour entrer dans la classe C mais trop petits pour la classe B. Donc il y eut, au début, un gaspillage important d'adresses IP et les tables de routage devenaient de plus en plus grandes. La solution est de pouvoir attribuer exactement le nombre de bits désirés.

Maintenant, il est possible de choisir le masque réseau que l'on désire pour configurer une infrastructure réseau. Mais pourquoi s'inquiéter des classes ? parceque lorqu'un subnet n'est pas défini, il teste sur la classe.

Espace d'adressage IP privé Une entreprise qui décide d'utiliser des adresses IP ne doit pas les prendre au hasard. Il existe des classes définies par l'IANA pour l'adressage :

- 10.0.0.0 à 10.255.255.255 - 1 réseau de classe A
- 172.16.0.0 à 172.31.255.255 - 16 réseaux de classe B
- 192.168.0.0 à 192.178.255.255 - 256 réseaux de classe C

1.2.3 ICMP

ICMP est souvent considéré comme faisant partie de la couche IP. ICMP communique des messages (erreurs, modification, information). La commande “ping”, qui permet de voir si une machine répond, utilise ICMP (echo).

```
PING localhost.localdomain (127.0.0.1) from 127.0.0.1 : 56(84) bytes of data.
64 bytes from localhost.localdomain (127.0.0.1) : icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from localhost.localdomain (127.0.0.1) : icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from localhost.localdomain (127.0.0.1) : icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from localhost.localdomain (127.0.0.1) : icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from localhost.localdomain (127.0.0.1) : icmp_seq=4 ttl=255 time=0.1 ms

--- localhost.localdomain ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

Une fonctionnalité intéressante de ICMP est le “redirect”. Il est courant de n’avoir qu’un default gateway sur une workstation mais celle-ci doit atteindre plusieurs réseaux sans passer par le même gateway. La solution est de créer toutes les routes statiques sur le default gateway. Lorsque la workstation veut atteindre une destination passant par un autre gateway, le default gateway émet un ICMP redirect. Ce n’est pas le seul cas d’utilisation, il sert aussi lors de changement de la topologie (ligne down, ...).

1.3 Routage IP

1.3.1 Concept

En théorie, le routage IP est simple, particulièrement dans le cas d’une workstation. Si une machine de destination est directement connectée à une autre machine (par exemple : une liaison PPP) ou sur un réseau partagé (par exemple : Ethernet), alors le datagramme IP est envoyé sans intermédiaire à cette destination. Par contre, le routage est plus complexe sur un routeur ou sur un machine avec plusieurs interfaces.

Le routage IP est effectué sur le base de “saut à saut” (hop to hop routing). Les étapes du routage IP peuvent être découpées de cette manière :

1. Recherche, dans une table de routage, de l’entrée associée à l’adresse IP de destination. S’il trouve une correspondance entre la table de routage et l’adresse de destination, le datagramme IP est envoyé au routeur de “saut suivant”(next-hop router). Ce cas de figure est utilisé pour les liaisons point à point.
2. Recherche, dans la table de routage, de l’entrée correspondant exactement à l’indentificateur du réseau de destination. Si cette adresse est localisée, envoi du paquet au routeur de saut suivant indiqué ou à l’interface directement connecté (par exemple : si l’interface existe sur le routeur). C’est ici aussi que l’on tient compte des masques de sous-réseau.
3. Recherche, dans la table de routage, de l’entrée par défaut. Envoi du paquet au routeur “de saut suivant” si cette entrée est configurée.

Si le déroulement de ces 3 phases est correct, alors le datagramme IP est délivré au prochain routeur ou host. Par contre, si cela n’est pas le cas, un message ICMP (host unreachable ou network unreachable) est envoyé au host d’origine et le datagramme IP est jeté.

Voici une sortie de la table de routage d’un routeur CISCO :

```
lab-bt#sh 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, * - candidate
default
        U - per-user static route, o - ODR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    128.253.0.0/16 is directly connected, Ethernet0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
```

```
S       10.130.10.3/32 is directly connected, BRI0
S       10.130.10.0/32 [1/0] via 10.130.10.3
C       10.132.0.0/16 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, BRI0
lab-bt#
```

1.3.2 Routage dynamique

Lorsqu'un réseau atteint une taille assez importante, il est très lourd de devoir ajouter les entrées dans les tables de routage à la main. La solution est le routage dynamique. Cela permet de mettre à jour les entrées dans les différentes tables de routage de façon dynamique.

RIPv1(Routing Information Protocol) C'est le protocole (distance vector protocol) le plus vieux mais qui est toujours implanté sur beaucoup de sites. C'est un protocole de type IGP (Interior Gateway Protocol) qui utilise une algorithme permettant de trouver le chemin le plus court. Il supporte un maximum de 15 noeuds traversés (il n'est pas adapté au réseau de grande taille). Il fonctionne par envoi de messages toutes les 30 secondes. Les messages RIP permettent de dresser une table de routage.

RIPv2 (Routing Information Protocol) C'est une version améloriée pour ajouter le support des sous-réseaux (subnets), des liaisons multipoints et de l'authentification.

EIGRP Ce protocole (Hybrid link-state & distance vector protocol) de routage a été developpé par Cisco pour améliorer RIP et le rendre plus stable. Il fonctionne très bien mais il est bien sûr uniquement compatible avec les produits Cisco.

OSPF(Open Shortest Path First) C'est la deuxième génération de protocole de routage (Link-state protocol). Il est beaucoup plus complexe que RIP mais ses performances et sa stabilité sont supérieures. Le protocole OSPF utilise une base de données distribuées, qui garde en mémoire l'état des liaisons. Ces informations forment une description de la topologie du réseau et de l'état de l'infrastructure. Le protocole RIP est adapté pour des réseaux de taille raisonnable par contre OSPF est de meilleure facture pour les réseaux de taille importante (par exemple ISP).

BGP (Border Gateway Protocol) BGP est utilisé sur Internet pour le routage entre, par exemple, les différents systèmes autonomes OSPF. Ce protocole a été créé pour des besoins propres à Internet suite à la grande taille du réseau lui-même.

IDRP (Interdomain Routing Protocol - IPv6)

1.4 Services UDP

1.4.1 DNS

DNS permet d'utiliser des noms symboliques pour accéder aux hôtes. DNS est utilisé dans la majorité des cas lors de l'utilisation d'un protocole TCP. Il est même utilisé indirectement pour des vérifications d'hôtes distants.

DNS utilise une méthode requête/réponse et s'appuie sur le protocole de transport UDP. Il a été choisi car il est rapide et efficace. DNS utilise un système de nommage hiérarchique à structure arborescente.

1.5 Services TCP

1.5.1 SMTP

SMTP fournit un mécanisme d'échanges et de transports pour le courrier électronique entre 2 hosts. Le protocole utilisé est très simple et existe depuis de nombreuses années. Il a évolué pour suivre les évolutions du courrier électronique.

Voici un exemple de session SMTP :

```
[root@localhost /]# telnet unix.be.EU.org 25
Trying 195.207.52.100...
Connected to unix.be.EU.org.
Escape character is '^]'.
220 ns.synoptic.be ESMTP Sendmail 8.9.1/8.9.1; Fri, 19 May 2000 11 :58 :46
+0200
HELO .
250 ns.synoptic.be Hello [195.74.211.67], pleased to meet you
MAIL FROM :<alexandre.dulaunoy@ibt.be>
250 <alexandre.dulaunoy@ibt.be>... Sender ok
RCPT TO :>^[[D
553 ... Unbalanced '>'
RCPT TO :<adulau@be.linux.org>
250 <adulau@be.linux.org>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
test
.
250 LAA10999 Message accepted for delivery
QUIT
221 ns.synoptic.be closing connection
Connection closed by foreign host.
```

Nous utiliserons telnet pour essayer une connexion sur un serveur smtp (port 25). La commande telnet permet de définir le port de connexion (par défaut c'est 23 (telnet)).

HELO .

Cette commande permet de réaliser le "handshake" entre le serveur et le client. La réponse du serveur est positive (code 250).

MAIL FROM :<alexandre.dulaunoy@ibt.be>

Le "mail from" définit l'origine du message. Il est à noter que la majorité des serveurs SMTP demande un domain valide (cf. SPAM).

RCPT TO :<adulau@be.linux.org>

Comme pour le "mail from", le "rcpt to" définit le (ou les) destinataire(s) du message.

Ensuite, le "DATA" définit le début du message (encodé ou pas). le "." termine le contenu du message. Ensuite le serveur SMTP confirme l'acception du message. Vous pouvez ensuite faire la même chose ou faire un "QUIT" pour quitter la session TCP.

1.5.2 POP3

2 Router CISCO

2.1 Hardware

2.1.1 Structure

Unité centrale (CPU) L'unité centrale, ou le microprocesseur, est responsable de l'exécution du système d'exploitation (chez Cisco, c'est IOS) du routeur. Le système d'exploitation prend aussi bien en charge les protocoles que l'interface de commande via une session telnet. La puissance du microprocesseur est directement liée à la puissance de traitement du routeur .

Mémoire Flash La flash représente une sorte de ROM effaçable et programmable. Sur beaucoup de routeurs, la flash est utilisé pour maintenir une image d'un ou plusieurs systèmes d'exploitation. Il est tout à fait possible de maintenir plusieurs images sur la même flash (suivant la taille de la flash). La mémoire flash est pratique car elle permet une mise à jour de la mémoire sans changer des "chips". La flash peut se présenter sous forme de barette mais aussi sous forme de carte.

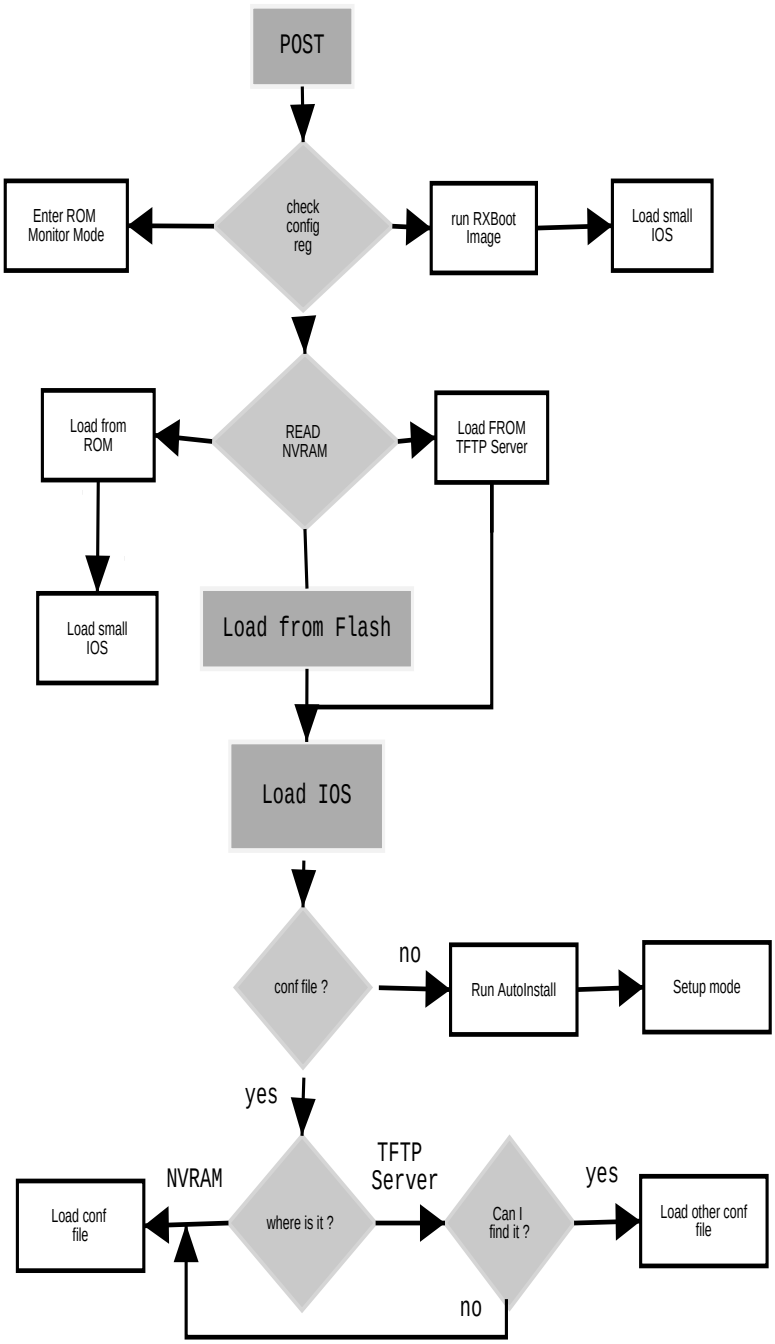
ROM La ROM contient le code pour réaliser les diagnostics de démarrage (POST : Power On Self Test). En plus, la ROM permet le démarrage et le chargement du système d'exploitation contenu sur la flash. On change rarement la ROM. Si on la change, on doit souvent enlever des "chips" et les remplacer.

RAM La RAM est utilisé par le système d'exploitation pour maintenir les informations durant le fonctionnement. Elle peut contenir les tampons (buffer), les tables de routage, la table ARP, la configuration mémoire et un nombre important d'autres choses. Et comme c'est de la RAM, lors de la coupure de l'alimentation, elle est effacée.

NVRAM (RAM non volatile) Le problème de la RAM est la non-conservation des données après la coupure de l'alimentation. La NVRAM solutionne le problème, puisque les données sont conservées même après la coupure de l'alimentation. L'utilisation de la NVRAM permet de ne pas avoir de mémoire de masse (Disques Durs, Floppy). Cela évite donc les pannes dues à une partie mécanique. La configuration est maintenue dans la NVRAM.

Portes I/O La structure même d'un routeur est l'ouverture donc l'interfaçage vers le monde extérieur est important. Il existe un nombre impressionant d'interfaces possibles pour un routeur (Liaison série asynchrone, synchrone, ethernet, tokenring, ATM, Sonet, FO, ...). La vitesse du bus qui interconnecte les I/O avec les différents composants du routeur marque aussi la puissance de traitement du routeur.

2.1.2 Processus de démarrage



2.2 Software (IOS)

2.2.1 Porte console

La configuration de base d'un routeur Cisco (et des autres aussi) se fait en général via la porte console. La porte console, sur un routeur, est configurée comme une interface DTE (Data Terminal Equipment). Mais la porte RS232 d'un PC est aussi une interface

DTE[7], c'est pour cela que vous ne pouvez connecter un cable série directement sur la porte console. La solution est d'utiliser un cable croisé (entre le fil 2 & 3) avec les différents fils de signaux. Le cable de console est souvent fourni en standard avec les routeurs Cisco.

La connexion s'effectue, en standard, à 9600bauds avec 8 bits de data, 1 bit stop et pas de parité. Vous pouvez utiliser votre émulateur de terminal favori[8].

2.2.2 Interpreteur de commande (CLI exec)

L'interpreteur de commande, comme son nom l'indique, est responsable de l'interprétation des commandes que vous tapez. La commande interprétée, si elle est correcte, réalise l'opération demandée.

```
Reply to request 4 from 128.253.154.110, 4 ms
Reply to request 4 from 128.253.154.204, 1 ms
lab-bt#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  128.253.154.204         0   0080.c723.989f  ARPA   Ethernet0
Internet  128.253.154.110         0   0040.951a.24c4  ARPA   Ethernet0
Internet  128.253.154.116         -   0010.7bc2.07cf  ARPA   Ethernet0
Internet  128.253.154.2           0   0000.4d21.8405  ARPA   Ethernet0
Internet  128.253.154.9           0   0040.055a.9476  ARPA   Ethernet0
lab-bt#
```

Si lors de la configuration initiale un (ou des) password a été configuré, vous devez introduire ce password pour accéder à l'interpreteur de commande.

Il y a 2 modes d'execution sur un routeur Cisco :

1. Le mode utilisateur (prompt : >)
2. Le mode privilégié (prompt : #)

Lors de la connexion initiale avec le routeur, vous arrivez dans le mode utilisateur. Pour passer au mode privilégié, vous devez introduire la commande `enable` et ensuite introduire un mot de passe. Le mode utilisateur sert uniquement à la visualisation des paramètres (pas de la configuration) et des différents status du routeur. Par contre, le mode privilégié permet, en plus de la visualisation des paramètres, la configuration du routeur et le changement de paramètres dans la configuration.

L'interpreteur de commande des routeurs Cisco est très souple et vous permet de demander les commandes disponibles. Vous désirez savoir les commandes qui commencent par "ho", rien de plus simple, `ho? <enter>`. Il est aussi possible d'utiliser l'expansion de commande comme sous Unix (avec la touche de tabulation). Si il n'y pas de confusions possibles, vous pouvez utiliser les abbréviations de commande. Par exemple, `sh ip int brie` au lieux de `show ip interface brief`. Cela permet de gagner du temps et de rendre la vie un peu plus facile.

2.2.3 Les fichiers de configuration

Dans un routeur cisco (en général), il existe différents fichiers de configuration. Il y a un fichier de configuration dans la nvram (startup-config), qui est lu au démarrage du routeur et copié en mémoire. Il y a un autre fichier de configuration dans la mémoire vive (running-config).

La "startup-config" est conservée dans la nvram sous forme ASCII. Tandis que la "running-config" est dans la ram sous forme binaire.

[7] Un équipement de terminal est souvent DTE, c'est-à-dire qu'il reçoit un signal d'horloge et se synchronise dessus. Le DCE donne un signal. Il est possible de configurer une interface série asynchrone pour qu'elle devienne DCE (clock rate 64000 par exemple).

[8] Hyperterminal (win32), cu (Unix), minicom, reflection...

2.2.4 Images IOS

2.2.5 Configuration générale

Lorsque vous désirez passer en mode configuration, vous devez taper (en mode enable) :

```
conf terminal
```

Cela siginifie que vous configurer le routeur en mode terminal. Il est tout à fait possible de configurer via TFTP par exemple. A ce moment le prompt change en :

```
router(config)#
```

Donc vous êtes dans la racine de la configuration du routeur et vous pouvez configurer les paramètres généraux.

2.2.6 Configuration des interfaces

Mais lors de la configuration d'un routeur, vous configurez souvent des interfaces. Il est donc nécessaire de passer du mode configuration générale vers le configuration de l'interface. Voici un exemple :

```
router> enable
password :
router#configure terminal
router(config)#interface ethernet 0
router(config-if)#ip address 10.1.1.1 255.255.255.0
router(config-if)#exit
router(config)#exit
router#copy running-config startup-config
```

Dans cet exemple, on peut voir la configuration de l'interface ethernet 0[9] avec son addresse IP et son masque réseau. Lors de ce genre de configuration, nous modifions la configuration "running" et donc nous réalisons un `copy running-config startup-config` pour sauver la configuration dans la nvram.

2.2.7 Configuration des lignes VTY

Il existe aussi différent types d'interfaces à configurer. Par exemple, la configuration des interfaces vituelles (pour l'accès via telnet du cli-exec) se fait de la même manière que les interfaces.

```
gw-int>enable
password :
gw-int#configure terminal
gw-int(config)#line vty 0 6
gw-int(config-line)#password MonSuperPasswordd
gw-int(config-line)#exec-timeout 15 0
gw-int(config-line)#exit
gw-int(config)#exit
gw-int#
```

Dans ce cas, on configure le password pour 7 sessions possibles via telnet sur le routeur. On spécifie le password (sinon on ne sait pas se connecter à distance) ainsi que le timeout d'utilisation pour fermer les sessions quand elles ne sont plus utilisées.

[9] La notation des interfaces, sur un routeur Cisco, est importante. La notation 4/0 signifie l'interface 0 du slot 4. Les cartes, qui possèdent plusieurs interfaces, sont numérotées de façon séquentielles. Dans l'exemple, on spécifie l'interface 0 c'est donc un modèle avec une seule interface Ethernet (comme le Cisco-1601 par exemple)

2.2.8 Configuration des interfaces routages

La configuration des protocoles de routage est réalisé de la même manière que les interfaces.

```
router leprotocolederoutage
```

Protocole de routage	Description
bgp	Border gateway protocol
egp	Exterior gateway protocol
igrp	Interior gateway protocol
isis	ISO IS-IS
iso-igrp	IGRP pour les réseaux OSI
ospf	Open shortest path first
rip	Routing information protocol
static	Static CLNS routing

```
ip-int-gw>enable
password :
ip-int-gw#configure terminal
ip-int-gw(config)#router ospf 303
ip-int-gw(config-router)#network 145.30.6.0
ip-int-gw(config-router)#exit
ip-int-gw(config)#exit
ip-int-gw#
```

2.3 Les “access lists”

Les routeurs Cisco fournissent la possibilité de faire du filtering. Les “access lists” peuvent être configurées pour tous les protocoles routables (IP, IPX, AppleTalk, ...).

Vous pouvez configurer les “access lists” sur chaque routeur de façon indépendante. Les “access lists” permettent de prévenir l’accès sur votre réseau. Les “access lists” ne sont pas uniquement destinées à la sécurité mais peuvent être utilisées dans le cadre de contrôles d’ouverture de ligne (DDR, ...).

2.3.1 Utilisation des “access lists”

Les “access list” filtrent le traffic réseau en contrôlant si des paquets routés sont transférés ou bloqués sur le(les) interface(s) du routeur. Un routeur peut examiner chaque paquet suivant ce que vous avez spécifié dans les “access lists”. Il est à noter que la sécurité est minimum, un utilisateur averti pourrait contourner les “access lists”.

Les critères d’une “access list” sont l’adresse de source du traffic, la destination du traffic, le niveau de protocole ou d’autres informations.

Pourquoi utiliser des “access lists” Il y a beaucoup de raisons pour configurer des “access lists” :

- Restreindre la mise à jour des tables de routage
- Contrôler le flux du réseau (pour les route-map par exemple)
- Et bien sûr limiter les accès aux réseaux ou à des services spéficiques du routeur

Vous pouvez utiliser les “access lists” pour fournir un niveau minimum de sécurité. Si aucune “acess lists” n’est configurée, le traffic passe sans aucune restriction à travers le routeur.

2.3.2 Création d'"access lists"

Il y a 2 étapes pour la création de listes de contrôle. La première est de créer l'access list et la seconde étape est de l'appliquer sur l'interface. Lors de la création de l'"acess list", il faut lui assigner un identificateur unique. Dans la majorité des cas, vous devrez utiliser un numéro (suivant le type de protocole à filtrer). Il est aussi possible d'utiliser une "access list" basée un nom mais uniquement avec certains protocoles.

Protocole	espace
IP	1 à 99
Extended IP	100 à 199
Ethernet type code	200 à 299
Ethernet address	700 à 799
Transparent bridging (protocol type)	200 à 299
Transparent bridging (vendor code)	700 à 799
Extended transparent bridging	1100 à 1199
DECnet & extended DECnet	300 à 399
XNS	400 à 499
Extended XNS	500 à 599
Appletalk	600 à 699
Source-route bridging (protocol type)	200 à 299
Source-route bridging (vendor code)	700 à 799
IPX	800 à 899
Extended IPX	900 à 999
IPX SAP	1000 à 1099
VINES	1 à 100

La création d'une "access list" est une suite de critères avec les paramètres sources, destinations, ou types de protocole. Pour une "access list" donnée (un numéro unique ou un nom unique) vous pouvez avoir plusieurs entrées. Vous n'êtes pas limité dans la taille de la liste (juste par la mémoire) . Par contre, plus la liste est longue, plus elle prend du temps à être parcourue (! !).

exemple :

```
interface serial 0/4
ip addresse 192.168.1.254 255.255.255.0
ip access-group 1 in
!
!
access-list 1 permit 192.168.1.1
access-list 1 deny 192.168.2.0 0.0.0.255
```

A la fin de chaque "access lists", il y a la règle implicite **"deny all traffic".** Ce qui signifie que ce qui n'est pas spécifié est interdit.

L'ordre des entrées dans l'"access-list" est important et c'est la première règle qui satisfait qui est prise en compte.

Lors de la modification d'une "access list", il est difficile de la modifier. Il vous est impossible d'insérer une règle dans l'"acces list". La seule solution est d'effacer la liste et de la recréer (même si vous avez 300 entrées 8-). Vous pouvez aussi copier la liste en TFTP et ensuite la recharger en TFTP.

2.4 Les “dialer list”

2.5 ISDN

ISDN utilise un nombre important de protocoles.

2.5.1 ISDN couche 1

Le layer 1 est la couche physique responsable pour la connexion au switch. Il supporte la connexion à un TA/NT1 ou à des “devices” multiples. Les canaux B et D partagent le même interface physique.

Canal D	Canal B
(layer 3) DSS1 (Q.931)	IP/IPX...
(layer 2) LAPD (Q.921)	HDLC/PPP/FR/...

(layer 1) I.430/I.431/ANSI T1.601

Le canal D est gouverné par DDR (Dial on Demand Routing). DDR est le mécanisme pour réaliser des connexions “Dial On Demand”. Le canal B est utilisé pour la transmission des données (IP,IPX...).

2.5.2 ISDN couche 2 (Q.921)

Un numéro de TEI est assigné par le switch ISDN. Cela permet de donner une identification à votre connexion sur le NT1/TA.

2.5.3 ISDN couche 3 (Q.931)

Un protocole DSS1 (Digital Subscriber Signalling System N°1) est utilisé pour la gestion des appels, des connexions & des alertes.

Suivant le pays, les techniques de “signalling” ne sont pas les mêmes entre le switch & le NT1.

Lors de l’utilisation d’ISDN, vous devez spécifier le type de switch :

```
isdn switch-type basic-net3
```

! Attention lors de la modification du switch-type, dans la majorité des cas, vous devez redémarrer le router !

2.6 NAT

2.7 Gestion des problèmes

2.7.1 Commande Debug

ISDN et Dial on Demand

```
show interface bri 0
show isdn status
show ppp multilink
debug dialer
debug isdn q921
debug isdn q931
debug isdn events
debug isdn active
debug isdn history
```

PPP

```
debug ppp negotiation
debug ppp authentification
```

2.8 Example de configuration

2.8.1 Dialup vers Internet (sans NAT)

```
Current configuration :
!
version 11.2
no service finger
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname di100334
!
enable secret 5 $1$wWjV$iTqcdHeE/iTkwNF.IIKrE1
enable password 7 1420230805172924
!
ip subnet-zero
no ip source-route
ip name-server 193.74.208.135
ip name-server 193.74.208.65
ip name-server 193.121.171.135
isdn switch-type basic-net3
isdn tei-negotiation first-call
!
!
interface Ethernet0
 ip address 193.74.140.254 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface BRI0
 ip unnumbered Ethernet0
 ip access-group 111 in
 ip access-group 112 out
 no ip redirects
 encapsulation ppp
 bandwidth 64
 dialer idle-timeout 300
 dialer string 042246011
 dialer hold-queue 5
 dialer-group 1
```

```
 ppp chap hostname diXXXXXX
 ppp chap password 7 XXXXXXXXXXXXXXXXX
!
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 BRI0
ip route 10.0.0.0 255.0.0.0 Null0
ip route 172.16.0.0 255.240.0.0 Null0
ip route 192.168.0.0 255.255.0.0 Null0
ip route 193.74.147.0 255.255.255.0 BRI0
access-list 10 permit 192.92.130.4
access-list 10 permit 193.74.208.188
access-list 10 permit 193.74.140.0 0.0.0.255
access-list 10 deny   any
access-list 11 deny   any
access-list 101 deny   ip any host 255.255.255.255
access-list 101 deny   udp any any range netbios-ns 139
access-list 101 permit ip 193.74.140.0 0.0.0.255 any
access-list 101 deny   ip any any
access-list 111 deny   ip 193.74.140.0 0.0.0.255 any
access-list 111 deny   ip any host 193.74.140.255
access-list 111 deny   udp any 193.74.140.0 0.0.0.255 eq 135
access-list 111 deny   tcp any 193.74.140.0 0.0.0.255 eq 12345
access-list 111 deny   tcp any 193.74.140.0 0.0.0.255 eq 12346
access-list 111 deny   udp any 193.74.140.0 0.0.0.255 eq 31337
access-list 111 deny   tcp any 193.74.140.0 0.0.0.255 eq 31337
access-list 111 permit ip any 193.74.140.0 0.0.0.255
access-list 111 deny   ip any any
access-list 112 deny   tcp 193.74.140.0 0.0.0.255 any eq 12345
access-list 112 deny   tcp 193.74.140.0 0.0.0.255 any eq 12346
access-list 112 deny   udp 193.74.140.0 0.0.0.255 any eq 31337
dialer-list 1 protocol ip list 101
!
line con 0
 login
 transport preferred none
line vty 0 4
 access-class 10 in
 access-class 11 out
 password 7 110A1016141D
 login
 length 23
 transport preferred none
!
end
```

2.8.2 Dialup vers Internet (avec NAT / sans easy IP)

```
Current configuration :
!
version 11.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname lanburodep
!
enable password 7 12100703
!
username lieg-cs1 password 7 XXXXXXXXXX
username bru-cs1 password 7 XXXXXXXXXX
username lanburodep password 7 XXXXXXXXXXX
ip subnet-zero
ip nat pool lanburodep-natpool-0 194.78.144.163 194.78.144.165 netmask 255.255.8
ip nat inside source list 2 pool lanburodep-natpool-0 overload
ip nat inside source static 200.0.0.100 194.78.144.162
no ip domain-lookup
isdn switch-type basic-net3
isdn tei-negotiation first-call
!
interface Ethernet0
 description connected to Internet
 ip address 200.0.0.4 255.255.255.0 secondary
 ip address 194.78.144.161 255.255.255.248
 ip nat inside
!
interface BRI0
 description connected to Internet
 no ip address
 encapsulation ppp
 dialer pool-member 1
!
interface Dialer1
 ip address 192.168.3.68 255.255.255.0
 ip nat outside
 encapsulation ppp
 no ip split-horizon
 bandwidth 64
 dialer remote-name lieg-cs1
 dialer string 2302911
 dialer hold-queue 10
```

```
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication pap callin
 ppp pap sent-username XXXXXX password 7 XXXXX
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
ip route 10.0.0.0 255.0.0.0 200.0.0.3
ip route 137.0.0.0 255.255.0.0 200.0.0.254
ip route 192.0.0.0 255.255.255.0 200.0.0.3
ip route 220.1.1.0 255.255.255.0 200.0.0.254
access-list 2 permit 200.0.0.0 0.0.0.255
access-list 2 permit 192.0.0.0 0.0.0.255
access-list 2 permit 10.0.0.0 0.255.255.255
access-list 2 permit 137.0.0.0 0.0.255.255
access-list 2 permit 205.1.1.0 0.0.0.255
snmp-server community public RO
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
 login
line vty 0 3
 password 7 XXXXXXX
 login
line vty 4
 login
!
end
```

2.8.3 Dialup vers Internet (avec NAT/Easy IP)

```
Current configuration :
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable password ibt
!
ip subnet-zero
!
```

```
ip name-server 195.238.2.21
ip name-server 195.238.2.22
isdn switch-type basic-net3
!
!
!
interface Ethernet0
 ip address 10.0.1.1 255.255.255.0
no ip directed-broadcast
 ip nat inside
!
interface BRI0
 description Skynet
 ip address negotiated
 no ip directed-broadcast
 ip nat outside
 encapsulation ppp
 dialer idle-timeout 180
 dialer string 2261111
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap callin
 ppp chap hostname XXXXXXXXXX
 ppp chap password 7 XXXXXXXXXXXXXXX
 hold-queue 75 in
!
ip nat inside source list 100 interface BRI0 overload
ip nat inside source static tcp 10.0.1.2 25 194.78.223.58 25 extendable
ip classless
ip route 0.0.0.0 0.0.0.0 BRI0
!
access-list 100 permit ip any any
dialer-list 1 protocol ip list 100
!
line con 0
 password XXXX
 transport input none
 stopbits 1
line vty 0 4
 password XXXX
 login
!
end
```

2.8.4 Ligne louée (Frame Relay)

```
Current configuration :
```

```
!
version 11.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
!
!
interface Ethernet0
 ip address 172.16.30.1 255.255.0.0
!
interface Serial0
 ip address 192.168.1.2 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 17
!
interface Serial1
 no ip address
shutdown
router rip
 network 172.16.0.0
 network 192.168.1.0
!
ip classless
ip default-network 0.0.0.0
!
!
line con 0
 password ibt
line vty 0
 password ibt
 login
line vty 1 4
 login
!
end
```

2.8.5 Dial On Demand (entre site)

```
Current configuration :
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
```

```
!
hostname 3620alleur
!
!
username 3620alleur password 7 151B0918
username 1603liege password 7 151B0918
username 1603gent password 7 141E101F
username jl password 7 130A191E020201
username tw password 7 082E584F07
isdn switch-type basic-net3
!
interface BRI0/0
 ip unnumbered Ethernet1/0
 encapsulation ppp
 dialer map ip 205.1.1.254 name 1603liege 2471543
 dialer-group 1
 ppp authentication chap
!
interface BRI0/1
 ip unnumbered Ethernet1/0
 encapsulation ppp
 dialer map ip 220.1.1.254 name 1603gent 2471543
 dialer-group 1
 ppp authentication chap
!
interface BRI0/2
 no ip address
 shutdown
!
interface BRI0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 ip address 200.0.0.254 255.255.255.0
!
no ip classless
ip route 205.1.1.0 255.255.255.0 205.1.1.1
ip route 205.1.1.1 255.255.255.255 BRI0/0
ip route 220.1.1.0 255.255.255.0 220.1.1.254
ip route 220.1.1.254 255.255.255.255 BRI0/1
access-list 100 deny   ip any host 255.255.255.255
access-list 100 permit ip any any
dialer-list 1 protocol ip list 100
!
line con 0
 password ibt
```

```
line aux 0
line vty 0 4
 password ibt
 login
!
end
--- autre site

Current configuration :
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname 1603liege
!
boot system flash 1 :80269401.bin
!
username 1603liege password 0 ibt
username 1603gent password 0 ibt
username 3620alleur password 0 ibt
isdn switch-type basic-net3
!
!
interface Ethernet0
 ip address 205.1.1.254 255.255.255.0
!
interface BRI0
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer map ip 200.0.0.254 name 3620alleur 02475428
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap
 hold-queue 75 in
!
no ip classless
ip route 0.0.0.0 0.0.0.0 200.0.0.4
ip route 200.0.0.0 255.255.255.0 200.0.0.254
ip route 200.0.0.254 255.255.255.255 BRI0
access-list 100 permit ip any any
dialer-list 1 protocol ip list 100
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
end
```

2.8.6 Liaison LL (support SNA)

```
Current configuration :
!
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname Haironville
!
enable secret 5 $1$.Z0Z$QbdOQluHjLFqSMlDBi6R0/
enable password cisco
!
username Galvameuse password 0 cisco
username nerac password 0 cisco
username thouare password 0 cisco
username diemoz password 0 cisco
username MPB password 0 cisco
username PFF password 0 cisco
username Lyon password 0 cisco
username Agen password 0 cisco
username Nantes password 0 cisco
memory-size iomem 30
ip host Galvameuse 131.12.1.2
ip host Diemoz 131.14.1.2
ip host Thouare 131.15.1.2
ip host Nerac 131.16.1.2
ip host MPB 141.13.1.2
ip host PFF 131.18.1.2
ip host Lyon 151.14.1.2
ip host Agen 151.16.1.2
ip host Nantes 151.15.1.2
ipx routing 0060.8338.75c1
isdn switch-type vn3
buffers small permanent 400
buffers middle permanent 200
buffers big permanent 150
buffers verybig permanent 30
buffers large permanent 20
buffers huge permanent 20
!
interface Ethernet0/0
 ip address 130.10.1.1 255.255.0.0
 ipx network 8202 encapsulation SAP
 bridge-group 1
!
interface Serial0/0
```

```
ip address 131.12.1.1 255.255.0.0
 ipx network 13112
 bridge-group 1
!
interface Serial1/0
 ip address 141.13.1.1 255.255.0.0
 ipx network 14113
 bridge-group 1
!
interface Serial1/1
 ip address 131.18.1.1 255.255.0.0
 ipx network 13118
 bridge-group 1
!
interface Serial1/2
 no ip address
 bridge-group 1
!
interface Serial1/3
 ip address 131.16.1.1 255.255.0.0
 ipx network 13116
 bridge-group 1
!
interface BRI2/0
 description SECOURS GALVAMEUSE
 ip address 133.10.2.1 255.255.0.0
 encapsulation ppp
 ipx network 13312
 dialer idle-timeout 200
 dialer wait-for-carrier-time 10
 dialer map bridge name Galvameuse broadcast
 dialer map ip 133.10.1.2 name Galvameuse broadcast
 dialer map ipx 13312.0060.8338.b881 name Galvameuse broadcast
 dialer load-threshold 1 either
 dialer-group 1
 ppp authentication chap
 bridge-group 1
!
interface BRI2/1
 description SECOURS DIEMOZ
 ip address 133.10.4.1 255.255.0.0
 encapsulation ppp
 ipx network 13314
 dialer idle-timeout 200
 dialer wait-for-carrier-time 10
 dialer map bridge name diemoz broadcast
 dialer map ip 133.10.1.4 name diemoz broadcast
```

```
 dialer map ipx 13314.0000.0c3e.bb4b name diemoz broadcast
 dialer load-threshold 1 either
 dialer-group 1
 ppp authentication chap
 bridge-group 1
!
interface BRI2/2
 description SECOURS NERAC
 ip address 133.10.6.1 255.255.0.0
 encapsulation ppp
 ipx network 13316
 dialer idle-timeout 200
 dialer wait-for-carrier-time 10
 dialer map bridge name nerac broadcast
 dialer map ip 133.10.1.6 name nerac broadcast
 dialer map ipx 13316.0060.5cf4.c7a7 name nerac broadcast
 dialer load-threshold 1 either
 dialer-group 1
 ppp authentication chap
 bridge-group 1
!
!
interface BRI2/3
 description SECOURS THOUARE
 ip address 133.10.5.1 255.255.0.0
 encapsulation ppp
 ipx network 13315
 dialer idle-timeout 200
 dialer wait-for-carrier-time 10
 dialer map bridge name thouare broadcast
 dialer map ip 133.10.1.5 name thouare broadcast
 dialer map ipx 13315.0060.5cf4.ca36 name thouare broadcast
 dialer load-threshold 1 either
 dialer-group 1
 ppp authentication chap
 bridge-group 1
!
interface Serial3/0
 ip address 131.15.1.1 255.255.0.0
 ipx network 13115
 bridge-group 1
!
interface Serial3/1
 ip address 151.15.1.1 255.255.0.0
 bridge-group 1
!
interface Serial3/2
```

```
 ip address 131.14.1.1 255.255.0.0
 ipx network 13114
 bridge-group 1
!
interface Serial3/3
 no ip address
 ipx network 15114
 bridge-group 1
!
router eigrp 1
 network 131.12.0.0
 network 131.14.0.0
 network 131.15.0.0
 network 131.16.0.0
 network 130.10.0.0
 network 141.13.0.0
 network 131.18.0.0
 network 151.14.0.0
 network 151.15.0.0
 network 151.16.0.0
!
no ip classless
ip route 130.20.0.0 255.255.0.0 133.10.1.2 200
ip route 130.40.0.0 255.255.0.0 133.10.1.4 200
ip route 130.50.0.0 255.255.0.0 133.10.1.5 200
ip route 130.60.0.0 255.255.0.0 133.10.1.6 200
ip route 130.80.0.0 255.255.0.0 133.10.1.8 200
ip route 140.10.0.0 255.255.0.0 143.10.1.3 200
ip route 150.40.0.0 255.255.0.0 153.10.1.4 200
ip route 150.50.0.0 255.255.0.0 153.10.1.5 200
ip route 150.60.0.0 255.255.0.0 153.10.1.6 200
ip route 195.0.0.0 255.255.0.0 130.10.1.3 200
!
!
!
ipx router eigrp 1
 network 13112
 network 13114
 network 13115
 network 13116
 network 13118
 network 14113
 network 8202
 network 15114
!snmp-server community public RO
snmp-server chassis-id Haironville
dialer-list 1 protocol ip permit
```

```
dialer-list 1 protocol ipx permit
dialer-list 1 protocol bridge permit
bridge 1 protocol ieee
banner motd ^C


   Routeur d'HAIRONVILLE


^C
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password cisco
 login
!
```

2.8.7 Liaison Internet LL (+Backup ISDN)

```
Current configuration :
!
version 11.2
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname di100174
!
enable secret 5 $1$h7NB$kbLrXApUBxyIp8ounEJq/.
enable password dFyP311
!
username di100174 password 0 F37kGS8D
ip name-server 193.121.171.135
ip name-server 193.74.208.135
ip name-server 193.74.208.65
isdn switch-type basic-net3
isdn tei-negotiation first-call
!
interface Ethernet0
 ip address 193.121.102.14 255.255.255.248
!
interface Serial0
 backup delay 10 10
 backup interface BRI0
```

```
 ip unnumbered Ethernet0
 encapsulation ppp
!
interface BRI0
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer idle-timeout 180
 dialer string 3001111
 dialer load-threshold 100 outbound
 dialer-group 1
 no fair-queue
 ppp authentication pap callin
 ppp pap sent-username diXXXXXX password 7 XXXXXXXXX
 ppp multilink
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0 50
ip route 0.0.0.0 0.0.0.0 BRI0 100
access-list 101 deny   udp any any eq netbios-ns
access-list 101 deny   udp any any eq netbios-dgm
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
line con 0
line vty 0 4
 password dFyP311
 login
!
end
```