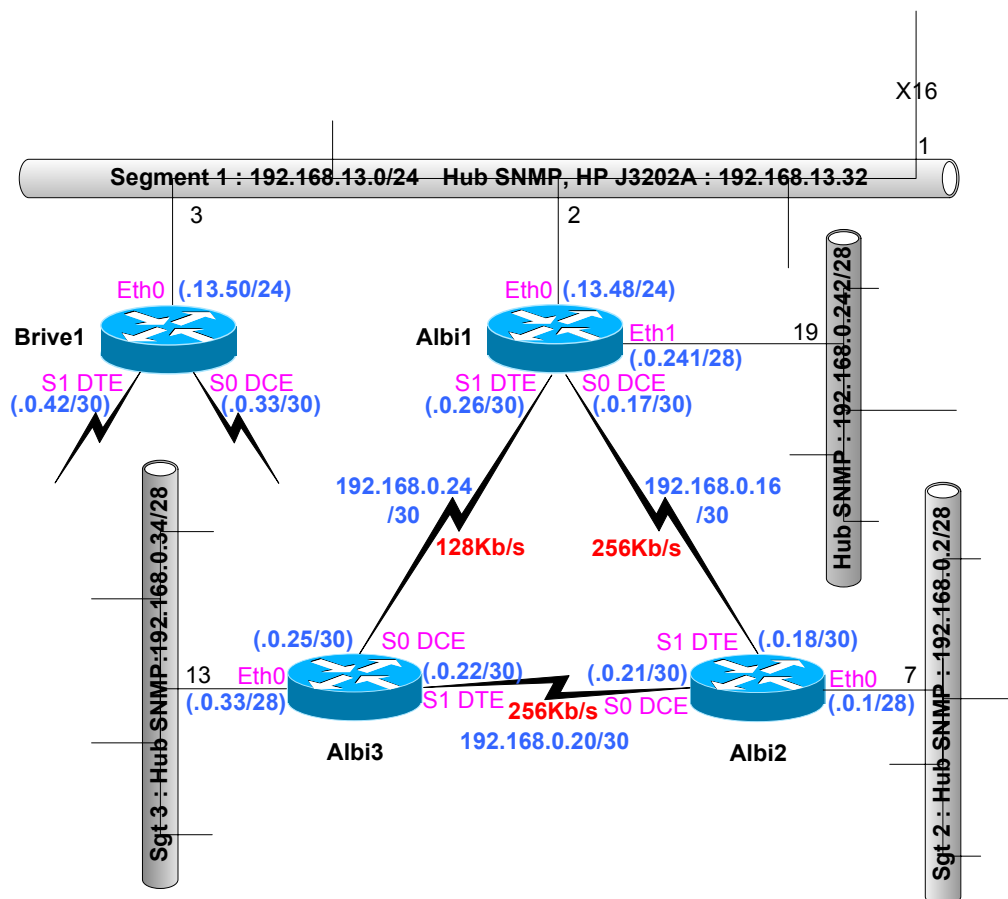


Interconnexion Réseaux III

Configuration évoluée de Routeurs CISCO



Préambule :

- ❑ Ce manuel est le support de cours ayant pour objet de finaliser une session de formation sur l'interconnexion de réseaux à base de matériels Cisco.
- ❑ Ce module doit de vous permettre de savoir construire un réseau d'entreprise à base d'équipements Cisco.
- ❑ Ce réseau s'appuyant essentiellement sur la technologie :
 - Ethernet/Fast/Giga Ethernet pour la partie LAN,
 - sur les technologies LS et Numéris pour la partie WAN.
 - Vous apprendrez également à gérer la sécurité de ce réseau.
- ❑ Le but n'est pas d'apprendre toutes les commandes possibles de l'IOS Cisco (il faudrait des mois voir des années...) mais de vous donner un état d'esprit, une méthodologie d'approche de la richesse de cet IOS.
- ❑ Vous trouverez en annexe des compléments vous permettant d'aller plus loin comme la configuration de frame Relay ou du pontage.
- ❑ Vous trouverez de nombreux exemples sur le lien :
 - http://www.cisco.com/public/products_tech.shtml

Table des matières

I.	OBJECTIFS DU COURS.....	1
II.	RAPPEL DES ACQUIS.....	2
II.A	LA PILE TCP/IP.....	2
II.B	ENCAPSULATION.....	3
II.C	IP : INTERNET PROTOCOL.....	4
III.	MATERIELS.....	7
IV.	UTILISATION CONSOLE.....	9
IV.A	INTERFACE EN LIGNE DE COMMANDE : CLI.....	9
IV.B	LES MESSAGES SYSLOG.....	11
IV.C	TELNET ET SUSPEND.....	11
IV.D	COPY/TFTP.....	12
IV.E	NTP : NETWORK TIME PROTOCOL.....	12
IV.F	RAPPEL : CONFIGURATION.....	14
V.	ROUTAGE IP.....	17
V.A	DEFINITION.....	17
V.B	DISTANCE ADMINISTRATIVE.....	17
V.C	LA METRIQUE.....	18
V.C.1	<i>Présentation</i>	18
V.C.2	<i>RIP</i>	18
V.C.3	<i>IGRP</i>	18
V.C.4	<i>EIGRP</i>	19
V.C.5	<i>OSPF</i>	19
V.C.6	<i>Changement de métrique RIP</i>	19
V.D	REGLES DE ROUTAGE.....	20
V.E	SYNTHESE AUTOMATIQUE ET AGREGATION DE ROUTES.....	21
V.E.1	<i>La synthèse automatique / autosummarization</i>	21
V.E.2	<i>L'agrégation de routes / route aggregation</i>	22
V.E.3	<i>CIDR</i>	23
V.F	SYNTHESE DES PROTOCOLES DE ROUTAGE DYNAMIQUES.....	24
VI.	RIP.....	25
VI.A	RIP v1.....	25
VI.B	RIP v2.....	25
VI.C	FONCTIONNEMENT.....	26
VI.D	CONFIGURATION.....	27
VI.D.1	<i>La commande NETWORK</i>	28
VI.D.2	<i>Spécification de la version</i>	28
VI.D.3	<i>Boucles de routage</i>	29
VI.D.4	<i>Changement de métrique</i>	30
VI.D.5	<i>Filtrage de mises à jour</i>	31
VI.D.6	<i>Authentification RIP</i>	32
VI.E	VERIFICATION.....	33
VI.E.1	<i>Configuration RIP</i>	33
VI.E.2	<i>Visualisation des routes RIP</i>	33

VI.E.3	Table de routage	34
VI.E.4	Les mises à jour	36
VI.F	EXERCICE #1	37
VI.G	EXERCICE #2	39
VI.H	EXERCICE #3	40
VI.I	EXERCICE #4	41
VII.	IGRP.....	42
VII.A	PRESENTATION.....	42
VII.B	LES TEMPORISATEURS.....	43
VII.C	CALCUL DU METRIQUE	44
VII.D	APPLICATION : CALCUL DU METRIQUE	45
VII.E	CONFIGURATION	46
VII.F	RESULTAT	48
VII.G	L'EQUILIBRAGE ET LE PARTAGE DE CHARGE	49
VII.H	DEBUG	49
VII.I	EXERCICE.....	50
VIII.	EIGRP	51
VIII.A	PRESENTATION.....	51
VIII.B	CONFIGURATION	52
VIII.C	AUTHENTIFICATION.....	54
VIII.D	RESULTAT	55
VIII.E	EXERCICE.....	56
VIII.F	CORRECTION.....	57
VIII.G	COMMANDES DE DEPANNAGE	59
IX.	OSPF	61
IX.A	PRESENTATION.....	61
IX.B	FONCTIONNEMENT	62
IX.B.1	Catégories de routeurs.....	62
IX.B.2	Les LSA	63
IX.B.3	Routeur désigné.....	63
IX.B.4	Nature hiérarchique.....	64
IX.B.5	Les liens virtuels.....	65
IX.B.6	Synthèse de routes	66
IX.C	CONFIGURATION	67
IX.D	RESULTAT	69
IX.E	EXERCICE #1	70
IX.F	EXERCICE #2.....	71
IX.G	CORRECTION.....	72
IX.H	COMMANDES DE DEPANNAGE	74
IX.I	VISUALISATION DES INTERFACES OSPF	75
IX.J	ÉTUDE DE CAS : UNE BOUCLE.....	76
IX.K	ELECTION DU ROUTEUR DESIGNÉ (DR & BDR).....	78
IX.L	AUTHENTIFICATION OSPF	79
IX.L.1	Authentification texte	79
IX.L.2	Authentification MD5.....	79
IX.M	ÉQUILIBRAGE DE CHARGE	80
IX.N	SYNTHESE RIP/OSPF	80
X.	LA REDISTRIBUTION	81
X.A	PRESENTATION.....	81
X.B	REDISTRIBUTION DANS RIP	82
X.B.1	Problèmes liés à RIP.....	82
X.B.2	Redistribution de routes statiques	82
X.B.3	Redistribution de EIGRP.....	82
X.B.4	Redistribution d'OSPF.....	83
X.C	REDISTRIBUTION DANS EIGRP	84

X.C.1	<i>Redistribution de RIP</i>	84
X.C.2	<i>Redistribution de OSPF</i>	84
X.D	REDISTRIBUTION DANS OSPF.....	85
X.D.1	<i>Redistribution d'une route statique</i>	85
X.D.2	<i>Redistribution de RIP</i>	85
X.D.3	<i>Redistribution de EIGRP</i>	85
X.E	REDISTRIBUTION MUTUELLE RIP-OSPF.....	86
X.F	EXERCICE.....	87
X.G	CORRECTION.....	88
X.H	COMMANDES DE DEPANNAGE.....	89
XI.	CONFIGURATION DHCP.....	90
XI.A	RELAJ DHCP.....	90
XI.B	SERVEUR DHCP.....	92
XII.	NAT/PAT.....	93
XII.A	PRESENTATION.....	93
XII.B	TERMINOLOGIE :.....	94
XII.C	FONCTIONNEMENT.....	97
XII.D	CONFIGURATION DU NAT STATIQUE :.....	99
XII.D.1	<i>Les commandes :</i>	99
XII.D.2	<i>Exemple :</i>	99
XII.D.3	<i>Configuration SNAT</i>	100
XII.D.4	<i>Application du SNAT</i>	101
XII.D.5	<i>Configuration du DNAT</i>	104
XII.D.6	<i>Configuration d'un Extranet</i>	105
XII.E	CONFIGURATION DU NAT DYNAMIQUE.....	106
XII.E.1	<i>Description</i>	106
XII.E.2	<i>Application</i>	107
XII.F	MAQUETTE DES EXERCICES.....	108
XII.G	TEST ET TROUBLESHOOTING.....	109
XII.H	PARTAGE DE CHARGE TCP.....	110
XII.H.1	<i>Description</i>	110
XII.H.2	<i>Configuration</i>	111
XII.H.3	<i>Exemple CISCO</i>	112
XII.I	OVERLOAD AN INSIDE GLOBAL ADDRESS.....	113
XII.J	OVERLAPPING.....	115
XII.J.1	<i>Static</i>	116
XII.J.2	<i>Dynamic</i>	116
XII.J.3	<i>Translating Overlapping Address Example</i>	117
XII.K	ROUTAGE.....	118
XII.K.1	<i>Statique</i>	118
XII.K.2	<i>RIP</i>	118
XII.K.3	<i>EIGRP</i>	119
XII.K.4	<i>OSPF</i>	119
XIII.	HSRP.....	120
XIII.A	PRESENTATION.....	120
XIII.B	PRINCIPE DE FONCTIONNEMENT :.....	120
XIII.C	CONFIGURATION.....	121
XIII.D	PARTAGE DE CHARGE.....	122
XIII.E	APPLICATION.....	123
XIII.F	EXERCICE.....	124
XIII.G	VRRP.....	125
XIII.G.1	<i>Présentation</i>	125
XIV.	SECURITE.....	126
XIV.A	DEMARCHE DE SECURITE.....	126
XIV.B	AAA.....	127

<i>XIV.B.1</i>	<i>Présentation</i>	127
<i>XIV.B.2</i>	<i>Overview of the AAA Configuration Process</i>	129
<i>XIV.B.3</i>	<i>Enable AAA</i>	130
<i>XIV.B.4</i>	<i>Disable AAA</i>	130
<i>XIV.B.5</i>	<i>Authentication</i>	131
XIV.B.5.a	AAA Authentication General Configuration Procedure.....	131
XIV.B.5.b	Configure Login Authentication Using AAA.....	132
XIV.B.5.b.One	Login Authentication Using Local Password.....	133
XIV.B.5.b.Two	Login Authentication Using Line Password.....	133
XIV.B.5.b.Trois	Login Authentication Using Enable Password.....	133
XIV.B.5.b.Quatre	Login Authentication Using RADIUS.....	134
XIV.B.5.b.Cinq	Login Authentication Using TACACS+.....	134
XIV.B.5.b.Six	Login Authentication Using Kerberos.....	134
<i>XIV.B.6</i>	<i>Authorization</i>	135
XIV.B.6.a	Configure Authorization.....	135
XIV.B.6.a.Un	TACACS+ Authorization.....	135
XIV.B.6.a.Deux	If-Authenticated Authorization.....	135
XIV.B.6.a.Trois	None Authorization.....	136
XIV.B.6.a.Quatre	Local Authorization.....	136
XIV.B.6.a.Cinq	RADIUS Authorization.....	136
XIV.B.6.a.Six	Kerberos Authorization.....	136
XIV.B.6.b	Disable Authorization for Global Configuration Commands.....	136
<i>XIV.B.7</i>	<i>Accounting</i>	137
XIV.B.7.a	Enable Accounting.....	137
XIV.B.7.a.One	Suppress Generation of Accounting Records for Null Username Sessions.....	137
XIV.B.7.a.Deux	Generate Interim Accounting Records.....	138
XIV.B.7.b	Monitor Accounting.....	139
XIV.B.7.b.Un	Accounting Attribute-Value Pairs.....	139
XIV.B.7.b.Deux	Accounting Configuration Example.....	139
XIV.C	CONFIGURATION DE L'ACCES	140
<i>XIV.C.1</i>	<i>Configuration par défaut</i>	140
<i>XIV.C.2</i>	<i>Chiffrement du mot de passe</i>	141
<i>XIV.C.3</i>	<i>Authentification locale</i>	142
<i>XIV.C.4</i>	<i>Utilisation d'un serveur d'Authentification</i>	143
<i>XIV.C.5</i>	<i>Configuration du serveur TACACS+ Freeware</i>	145
XIV.C.5.a	Présentation.....	145
XIV.C.5.b	Installation	145
XIV.C.5.c	Configuration	146
XIV.C.5.d	Lancement.....	148
XIV.C.5.e	Accounting.....	148
XIV.D	TACACS+ FREWARE FOR FIRST-TIME USERS	150
<i>XIV.D.1</i>	<i>Introduction</i>	150
<i>XIV.D.2</i>	<i>Authentication</i>	151
<i>XIV.D.3</i>	<i>Adding Authorization</i>	154
<i>XIV.D.4</i>	<i>Adding Accounting</i>	155
<i>XIV.D.5</i>	<i>test_file</i>	156
<i>XIV.D.6</i>	<i>Related Information</i>	157
<i>XIV.D.7</i>	<i>Application</i>	158
XIV.E	RADIUS	160
XIV.F	PROTECTION ANTI SPOOFING	161
XIV.G	DESACTIVER LES SERVICES INUTILES	162
XIV.H	LES TABLES ARP	163
XIV.I	CONTROLLER LES ACCES HTTP	164
XIV.J	EXERCICE	164
XV.	LES ACL	165
XV.A	PRESENTATION	165
XV.B	FONCTIONNEMENT	166
XV.C	LES COMMANDES	168
XV.D	TYPES ET IDENTIFICATION	168
XV.E	LES WILCARD MASK	169
XV.E.1	Présentation	169

XV.E.2	Exemples :	169
XV.F	LES ACL STANDARDS NUMEROTEES	170
XV.F.1	Les commandes :	170
XV.F.2	Exemple :	171
XV.G	LES ACL ETENDUES NUMEROTEES	172
XV.H	LES ACL STANDARDS NOMMEES	173
XV.H.1	Les commandes :	173
XV.H.2	Exemple :	173
XV.I	LES ACL ETENDUES NOMMEES	174
XV.I.1	Les commandes :	174
XV.I.2	Exemple :	174
XV.J	LES ACL DYNAMIQUES	175
XV.J.1	Exemple :	175
XV.K	LES ACL BASEES SUR LE TEMPS.....	176
XV.L	LES ACL REFLECTIVES	177
XV.L.1	Les commandes :	177
XV.L.2	Exemple #1 :	177
XV.L.3	Exemple #2 :	178
XVI.	IOS FIREWALL	180
XVI.A	PRESENTATION.....	180
XVII.	IPSEC.....	181
XVII.A	PRESENTATION.....	181
XVII.B	CONFIGURATION EN PSK NET-TO-NET.....	183
XVII.B.1	Configuration IKE.....	183
XVII.B.2	Configuration IPSEC	184
XVII.B.3	Application.....	185
XVII.B.4	Test et vérification.....	187
XVIII.	CBAC : CONTROLE D'ACCES BASES CONTENU	188
XVIII.A	PRESENTATION.....	188
XVIII.B	CONFIGURATION	189
XVIII.C	VERIFYING CBAC.....	191
XVIII.D	ETHERNET INTERFACE CONFIGURATION EXAMPLE	192
XVIII.E	APPLICATION #1	193
XVIII.E.1	Example #1- Without CBAC.....	193
XVIII.E.2	Example #2 - Using CBAC.....	194
XVIII.F	APPLICATION #2.....	195
XVIII.G	APPLICATION #3.....	196
XIX.	SNMP.....	197
XIX.A	ARCHITECTURE	197
XIX.B	LES REFERENCES.....	197
XIX.C	LE FORMAT D'UN MESSAGE SNMP	198
XIX.D	SNMPv1, v2 ET v3.....	200
XIX.E	LA MIB.....	201
XIX.E.1	Présentation	201
XIX.E.2	Identification des objets :	201
XIX.E.3	MIB normalisées et propriétaires.....	203
XIX.E.4	MIB II	204
XIX.E.5	RMON	209
XIX.F	CONFIGURATION DES AGENTS	210
XIX.G	NMS	212
XX.	LA JOURNALISATION.....	213
XX.A	PRESENTATION.....	213
XX.B	SYSLOG.....	213
XX.C	CONFIGURATION CISCO.....	214

XX.D	CONFIGURATION SYSLOG SOUS LINUX.....	215
XXI.	LE POLICY-BASED ROUTING.....	216
XXI.A	PRESENTATION.....	216
XXI.B	APPLICATION.....	216
XXII.	RNIS.....	217
XXII.A	PRESENTATION.....	217
XXII.B	CONFIGURATION DE RNIS.....	218
XXII.C	PROTOCOLES PAP ET CHAP.....	220
XXII.D	CONFIGURATIONS.....	221
XXII.D.1	<i>Multilink PPP.....</i>	<i>221</i>
XXII.D.2	<i>Secours et débordement.....</i>	<i>222</i>
XXII.D.3	<i>Contrôle du numéro appelant.....</i>	<i>223</i>
XXII.D.4	<i>Interface dialer.....</i>	<i>223</i>
XXII.D.5	<i>Configuration d'un client Microsoft RAS.....</i>	<i>224</i>
XXII.D.6	<i>Exemple de configuration d'un routeur RNIS.....</i>	<i>225</i>
XXIII.	CDP.....	227
XXIII.A	PRESENTATION.....	227
XXIII.B	CONFIGURATION.....	227
XXIV.	CONFIG MAKER.....	228
XXIV.A	PRESENTATION.....	228
XXIV.B	UTILISATION.....	228
XXV.	QOS.....	241
XXV.A	PRESENTATION.....	241
XXV.B	FIFO.....	242
XXV.C	WEIGHTED FAIR QUEUE.....	243
XXV.D	PRIORITY QUEUEING.....	244
XXV.D.1	<i>Principe de fonctionnement.....</i>	<i>244</i>
XXV.D.2	<i>Configuration.....</i>	<i>245</i>
XXV.E	CUSTOM QUEUEING.....	246
XXV.E.1	<i>Présentation.....</i>	<i>246</i>
XXV.E.2	<i>Principe de fonctionnement.....</i>	<i>246</i>
XXV.E.3	<i>Configuration.....</i>	<i>247</i>
XXVI.	FRAME RELAY.....	248
XXVI.A	RAPPELS.....	248
XXVI.B	CONFIGURATION.....	249
XXVII.	LE PONTAGE.....	253
XXVII.A	FONCTIONNEMENT DU PONTAGE.....	253
XXVII.B	TRANSPARENT BRIDGING.....	253
XXVII.C	IRB & CRB.....	254
XXVII.C.1	<i>Présentation.....</i>	<i>254</i>
XXVII.C.2	<i>Le routeur se comporte de la façon suivante :.....</i>	<i>255</i>
XXVII.D	CONFIGURATION DU TRANSPARENT BRIDGING.....	256
XXVII.D.1	<i>Configuration.....</i>	<i>257</i>
XXVII.E	COMMANDES.....	258
ANNEXE A.	MAQUETTE D'EXERCICES.....	259
A.I	MAQUETTE SANS VLSM.....	259
A.II	MAQUETTE AVEC VLSM.....	260
ANNEXE B.	LA COMMANDE PING.....	261
ANNEXE C.	LE REGISTRE.....	262

C.I	ROLES DU 'BOOT FIELD'	262
C.II	DEBIT DU PORT CONSOLE	263
C.III	ADRESSE DE BROADCAST	263
ANNEXE D.	ROUTEUR 2621 PLUS NM-16ESW	264
ANNEXE E.	COMPARAISON DES PROTOCOLES DE ROUTAGES	265
ANNEXE F.	PROCEDURE DE RECUPERATION D'UN MOT DE PASSE PERDU	266
ANNEXE G.	CISCO 2600	268
G.I	SAUVEGARDE IOS.....	268
G.II	MISE A JOUR DE L'IOS	269
ANNEXE H.	LAN NAMAGER	270
ANNEXE I.	LES PROTOCOLES.....	270
ANNEXE J.	LES NUMEROS DE PORT	271
ANNEXE K.	CONSOLE PORT SIGNALS AND PINOUTS.....	272
ANNEXE L.	LES RFC	273
ANNEXE M.	GLOSSAIRE.....	273
ANNEXE N.	BIBLIOGRAPHIE CISCO.....	274

I. Objectifs du cours

- ❑ **Rappel des fondamentaux**
 - OSI d'ISO : Protocole, PDU, Encapsulation
 - Ethernet / IEEE 802.3
 - IP

- ❑ **Mise en pratique des cours :**
 - Les réseaux locaux (Ethernet),
 - Les réseaux étendus (émulation par câble '*Null Modem*')
 - TCP/IP
 - ITR I

- ❑ **Configuration de deuxième niveau des Routeurs CISCO**
 - Routage dynamique : RIP et OSPF
 - La redistribution : Routage statique, RIP et OSPF
 - NAT/PAT (*Network Address Translation / Port Address Translation*)
 - HSRP (*Hot Standby Routing Protocol*)
 - SNMP
 - Sécurité : ACL, AAA et VPN IP

- ❑ **Méthode de dépannage**

Planning	1° jour	2° jour	3° jour	4° jour	5° jour
Matin	Présentation du Cours & Rappel des fondamentaux	RIP (Pratique) & OSPF (Théorie)	Redistribution & Synthèse sur le routage	NAT (Pratique)	Sécurité : AAA, ACL, TACACS, VPN IP
Après-midi	Installation et test de la maquette & RIP (Théorie)	OSPF (Pratique)	NAT (Théorie)	SNMP	Synthèse

II. Rappel des acquis

II.A La pile TCP/IP

La pile protocolaire de communication TCP/IP tire son nom des deux principaux protocoles qu'elle contient : TCP (*Transmission Control Protocol*) et IP (*Internet Protocol*).

TCP/IP est un synonyme pour '*Internet Protocol Suite*' terme désignant tous les protocoles constituant la pile TCP/IP. Il peut être aussi utilisé pour les communication d'un réseau privé (Intranet ou Extranet).

IP (le protocole) propose une méthode d'interconnexion logique des réseaux physiques. TCP/IP définit un ensemble de conventions permettant des échanges de données entre ordinateurs. Il a été développé entre les années 1977 et 1979 par la DARPA / ARPA (*Defense Advanced Research Projects Agency*) du DoD (*Department of Defense*) qui l'a mis en oeuvre sur ARPANET. Puis ce premier réseau expérimental a été subdivisé en deux : MILNET et Internet. MILNET étant réservé au DoD, tandis que le réseau Internet qui est un réseau (réseau logique) de taille mondiale fédérant les réseaux d'universités, d'institutions de recherche, de nombreuses entreprises et les particuliers.

TCP/IP est un terme générique qui renvoie à une vaste famille de protocoles et de services que l'on peut regrouper en trois grandes catégories :

- ❖ Des programmes d'applications : telnet, ftp, tftp, nfs, http, dns, dhcp, snmp, smtp etc.
- ❖ Les protocoles assurant un transport de bout en bout : tcp et udp.
- ❖ Les protocoles acheminant les données dans le réseau : ip.

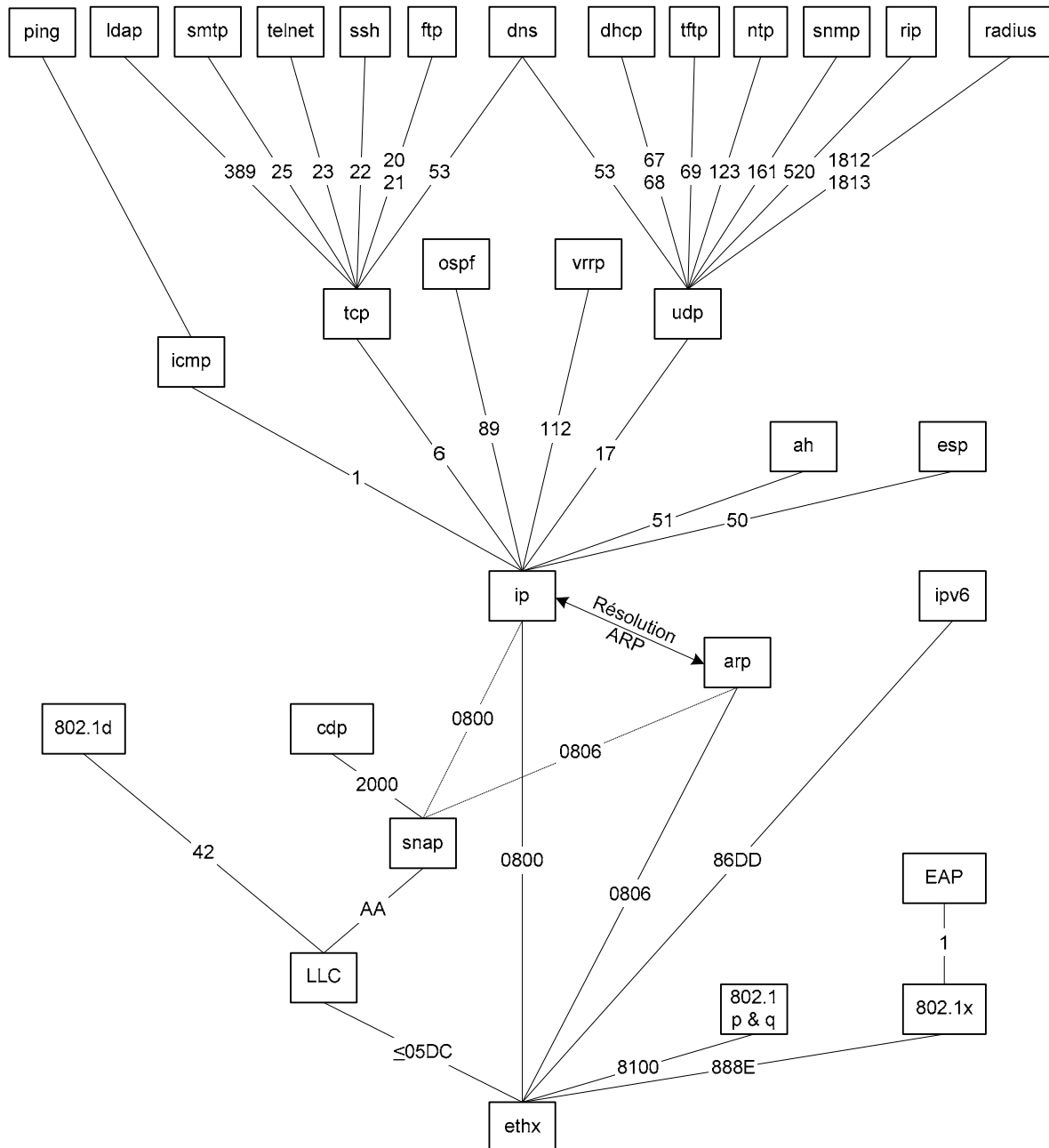
Le tableau ci-dessous donne le nom des principaux protocoles ou services de TCP/IP, avec l'indication de la couche correspondante dans le modèle OSI de l'ISO.

OSI	Stack TCP/IP							
7	Application Layer	ftp	telnet	smtp	tftp	dns	nfs	
6							xdr	
5							rpc	
4	Transmission Layer	tcp			udp			
3	Internet Layer	icmp		ip			arp	rarp
2	Network Layer	réseaux physiques : Ethernet, X25, FR, ATM, PPP (RTC, RNIS), etc.						
1								

Notons que les informations décrivant TCP/IP peuvent être trouvées dans une série de documents connue sous le nom de RFC (*Request for Comments*). Les RFC sont disponibles notamment par courrier électronique auprès du NIC (*Network Information Center*). Voir liste et modalités d'obtention de ces documents dans "*Internetworking with TCP/IP*", pages 441 et 475.

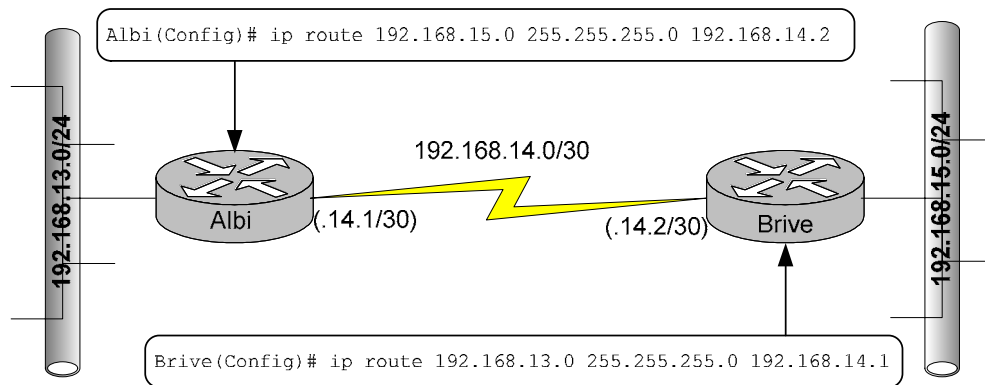
II.B Encapsulation

- ❑ Encapsulation non exhaustive, mais les principaux protocoles sont indiqués (vue d'un administrateur réseau).
- ❑ Ici, une seule interface LAN est présentée : 'ethx', mais plusieurs interfaces LAN et/ou WAN peuvent être présentes.



II.C IP : Internet Protocol

- Une route : désigne l'accessibilité d'un réseau cible par l'adresse du prochain routeur (*Next Hop Gateway*), le réseau cible est représenté par une adresse IP et son masque de sous réseau (*SubNet Mask*). Il est fortement préconisé que l'adresse du prochain routeur (*Next Hop Gateway*) appartienne à une route directement connectée.



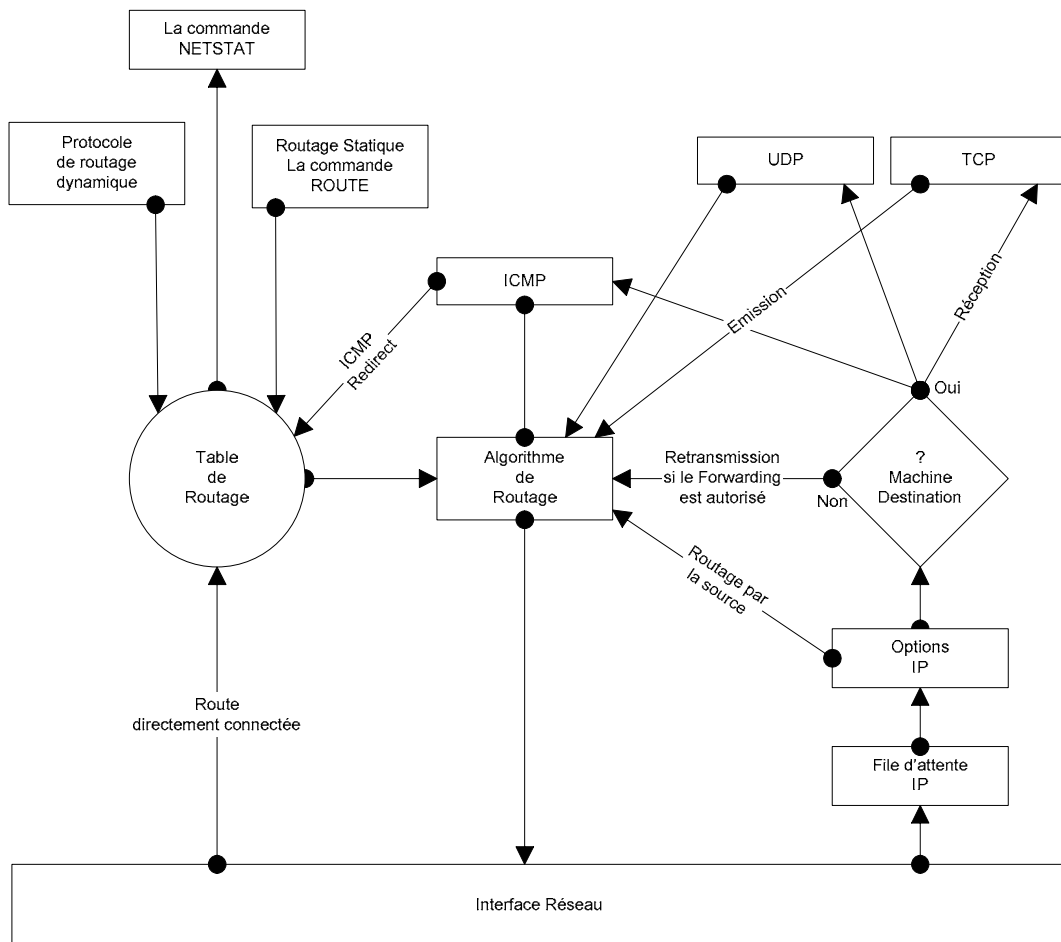
- Une table de routage est une base de données constituée d'enregistrements. Chaque enregistrement désigne une route qui contient cinq champs :

<i>Target Address</i>	<i>Subnet Mask</i>	<i>Next Hop Gateway</i>	<i>Flags</i>	<i>Interface</i>
-----------------------	--------------------	-------------------------	--------------	------------------

- Le champ '*Target Address*' (Adresse cible) contient l'adresse IP cible d'un réseau (ou sous réseau) ou d'une machine (host).
 - Le champ '*Subnet Mask*' contient le subnet mask associé à *Address_cible*. Quand ce champ contient '255.255.255.255', ceci indique une route vers une machine (host).
 - Quand le Flag 'G' est présent, le champ *Next_Hop_Gateway* contient l'adresse IP du prochain routeur (*Next Hop Gateway*).
 - Attention : le '*Next Hop Gateway*' doit être accessible en routage direct.
 - Une machine IP (routeur ou host) connaît uniquement le prochain routeur pour atteindre la destination finale.
 - Le champ *Flags* contient :
 - U comme '*Up*' : la route est en service.
 - G comme '*Gateway*' : la route désigne une route vers un réseau. Ce Flag permet de différencier le routage direct du routage indirect.
 - H comme '*Host*' : La route désigne une route vers une machine. Si ce Flag n'est pas positionné la route désigne un réseau. Dans ce cas le champ '*Subnet Mask*' contient la valeur : 255.255.255.255.
 - D : La route a été créée par une redirection (ICMP Redirect).
 - M : La route a été modifiée par une redirection.
 - Le champ *Interface* contient le nom de l'interface réseau qui émet le datagramme.
- L'acquisition des routes par une machine IP s'effectue de quatre manières possibles.
 - a. Les **routes directement connectées** : ces routes sont automatiquement créées lors de la configuration des interfaces et que le '*link*' soit présent.
 - b. Les **routes statiques** : ces routes doivent être déclarées manuellement ou par des fichiers statiques par la commandes '*Route*'.
 - c. Les **routes dynamiques** : ces routes sont créées par des protocoles de routages dynamiques (RIP, OSPF).
 - d. Par **ICMP Redirect**

□ Algorithme de routage

- Les routes de la table de routage sont classées dans l'ordre suivant :
 - Les routes des réseaux qui sont directement connectés à la plateforme,
 - Les routes vers les machines (host),
 - Les routes vers les réseaux (par routage statique et/ou dynamique) et
 - La 'Default Gateway' [route statique optionnelle].
- Chaque route de la table de routage est évaluée dans l'ordre précisé ci-dessus :
 - Réalisez la fonction logique ET entre l'adresse IP destination et le Subnet Mask de la route
 - Si le résultat est identique à l'adresse cible de la route
 - Alors : Appliquer la route
 - Sinon : passer à la ligne suivante
- Quand toutes les routes de la table de routage ont été évaluées et qu'aucune correspondance n'a été trouvée, IP informe d'une erreur par un message ICMP : Destination Unreachable.



III. Matériels

Figure 4. Cisco IOS VPN Security Portfolio

Teleworkers /SOHO	Small Branch	Medium-Sized Branch	Enterprise Branch	Enterprise Edge	Enterprise Headquarters Data Center
 Cisco 830	 Cisco 1760	 Cisco 2600XM Cisco 2691	 Cisco 3700	 Cisco 7301	 Cisco Catalyst 6500 Cisco 7600
 Cisco SOHO 90	 Cisco 1700			 Cisco 7200	
 Cisco 800 Series ISR	 Cisco Series 1800 ISR	 Cisco 2800 Series ISR	 Cisco 3800 Series ISR		

Note: The figure above provides general guidelines

Table 5. VPN Performance of Cisco IOS Routers

Cisco VPN Security Router	Maximum Tunnels	Maximum 3DES Throughput	Maximum AES Throughput
Cisco SOHO 90	8	1 Mbps	-
Cisco 830	10	7 Mbps	2 Mbps
Cisco 1700 with VPNSM	100	15 Mbps	-
Cisco 1841 with onboard VPN	100	45 Mbps	45 Mbps
Cisco 1841 with AIM-VPN/BPII-PLUS	800	95 Mbps	95 Mbps
Cisco 2600XM with AIM-VPN/EPII-PLUS	800	22 Mbps	22 Mbps
Cisco 2691 with AIM-VPN/EPII-PLUS	800	150 Mbps	150 Mbps
Cisco 2800 with Onboard VPN	300	66 Mbps	66 Mbps
Cisco 2800 with AIM-VPN/EPII-PLUS	1500	145 Mbps	145 Mbps
Cisco 3700 with AIM-VPN/HPPII-PLUS	2000	190 Mbps	190 Mbps
Cisco 3800 with Onboard VPN	700	180 Mbps	180 Mbps
Cisco 3800 with AIM-VPN/HPPII-PLUS	2500	185 Mbps	185 Mbps
Cisco 7200VXR NPE-G1 with a Single SA-VAM2+	5000	280 Mbps	280 Mbps
Cisco 7301 with SA-VAM2+	5000	379 Mbps	379 Mbps
Cisco Catalyst 6500/7600 with a Single VPNSM	8000	1.9 Gbps	-

* Up to 10 VPNSMs can be installed in the same chassis, providing an unmatched 14 Gbps of VPN capacity per chassis.

Cisco IOS VPN security routers and Cisco Catalyst switches can be managed using a convenient CLI through a variety of methods, including Telnet, SSH v2.0, or out-of-band via a console port. Alternatively, Cisco IOS routers can be configured and monitored using Cisco SDM, an intuitive and secure Web-based device management tool embedded within Cisco IOS access routers. Cisco SDM simplifies device and security configuration through smart wizards to enable customers to quickly and easily deploy, configure, and monitor VPNs without requiring extensive knowledge of the Cisco IOS CLI. Cisco IOS routers can also be configured and monitored using tools available from Cisco AVVID partners.

ADDITIONAL INFORMATION

For more information, please visit the following links:

Cisco router security: <http://www.cisco.com/go/routersecurity>

Cisco router security bundles: <http://www.cisco.com/go/securitybundles>

Cisco IPsec VPN: <http://www.cisco.com/go/ipsec>

Cisco VPN 3000 Series concentrators: http://www.cisco.com/warp/public/cc/pd/hb/vp3000/prodlit/vpn3k_ov.pdf

Cisco IPsec VPN services modules:

http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/ps4221/prodlit/vpnsmds_ds.pdf

Cisco ASA 5500 Series adaptive security appliances: <http://www.cisco.com/go/asa>

Cisco PIX Security Appliances: <http://www.cisco.com/go/pix>

Cisco Security Device Manager: <http://www.cisco.com/go/sdm>

CiscoWorks VPN/Security Management Solution:

<http://www.cisco.com/en/US/products/sw/cscowork/ps2330/index.html>

Cisco IP Solution Center: <http://www.cisco.com/en/US/products/sw/netmgts/ps4748/index.html>

CiscoWorks Security Information Management Solution:

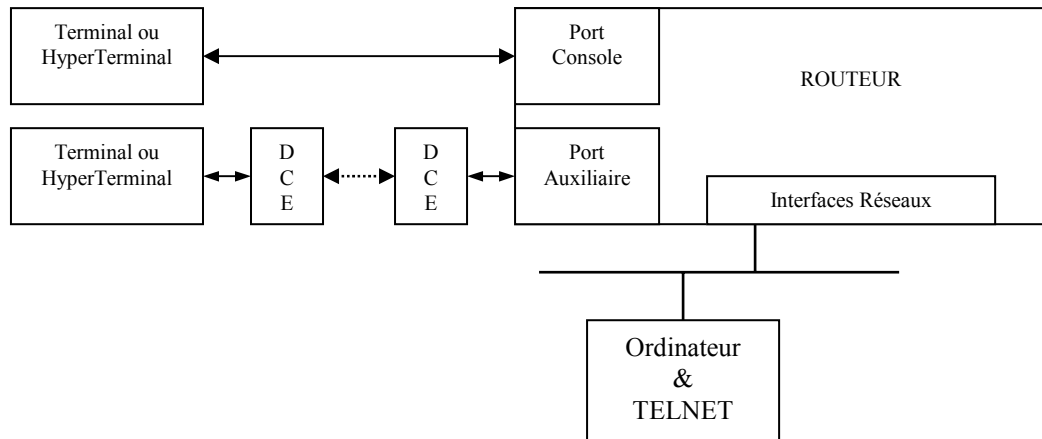
<http://www.cisco.com/en/US/products/sw/cscowork/ps5209/index.html>

SAFE Blueprint from Cisco: <http://www.cisco.com/go/safe>

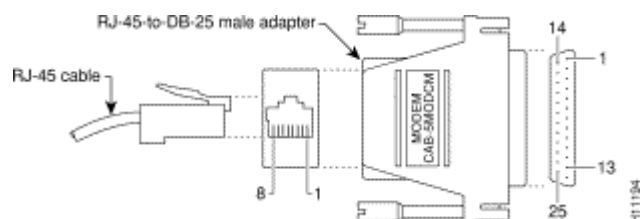
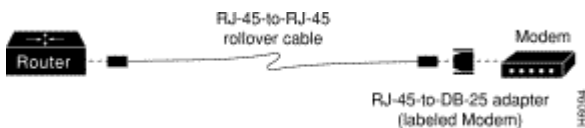
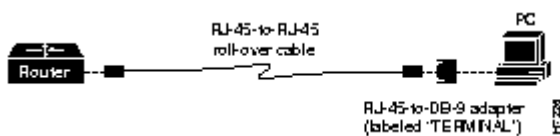
IV. Utilisation console

IV.A Interface en ligne de commande : CLI

- CLI (Command-Line Interface) est le terme qui désigne l'interface en ligne de commande du terminal pour l'IOS. Pour accéder au CLI on emploie ; un terminal, une émulation de terminal (*HyperTerminal*) sur le port console, une connexion TELNET par le réseau.



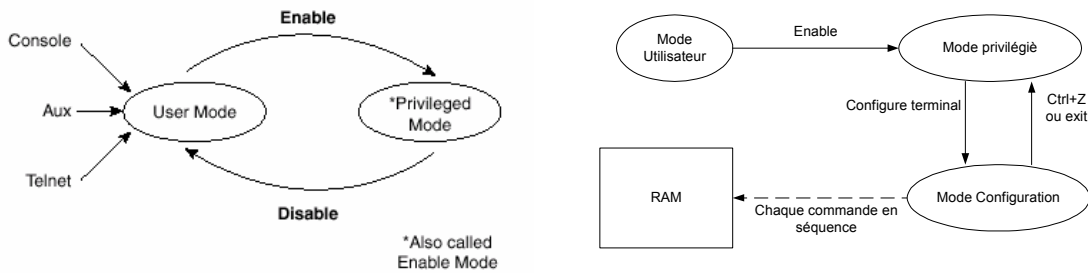
- Quand vous désirez relier le routeur à un terminal, vous devez d'abord les connecter avec le câble fournit par CISCO. Si vous connectez le routeur directement au terminal il faut utiliser l'adaptateur RJ-45 à DB-9 marqué 'TERMINAL' sinon l'adaptateur RJ-45 à DB-9 marqué 'MODEM'. Puis configurez le terminal avec les paramètres suivants ; **9600 bps, 8 bits de données, pas de parité, et 2 bits stop.**



- Toutes les commandes saisies en mode CLI sont immédiatement exécutées (mode EXEC, ainsi que certains messages de réponses sont visualisées sur le terminal. Pour que l'exécution des commandes soit différée il faut les placer dans un fichier de configuration : '*Startup-Config*' ou '*Running-Config*'.
- Une aide est présente en permanence en appuyant sur la touche '?'. 'Context-setting'. L'IOS dispose de deux niveaux principaux EXEC ; le mode **EXEC utilisateur** (symbole : >) qui permet uniquement de consulter les paramètres et le mode **EXEC privilégié** ou mode Enable (symbole : #) qui permet de configurer le routeur.

Aide pour les commandes CLI	
Instruction	Description
?	Aide pour toutes les commandes disponibles dans mode.
Help	Texte décrivant les détails listés dans ce tableau. Aucune aide réelle au sujet des commandes n'est fournie.
Commande ?	Aide textuelle décrivant toutes les premières options de paramètres pour la commande.
Comm?	Affiche la liste des commandes commençant par <COM>.
Commande parm?	Ce type d'aide liste tous les paramètres commençant par les lettres <PARM>. Notez qu'il n'y a pas d'espace entre ' parm ' et '?'. Exemple : Commande parm1 ?
Commande parm<TAB> Ou Comm<TAB>	Si l'utilisateur appuie sur la touche de tabulation au milieu d'un mot, l'interface CLI donne la fin du mot clé sur la ligne de commande ou n'exécute aucune action si ce mot n'existe pas ou plusieurs possibilités se présentent.
Commande parm1 ?	Quand le point d'interrogation est séparé de plusieurs espace après le dernier paramètre, le CLI affiche tous les sous paramètres et donne une brève explication.

Séquences de touches pour le rappel et la modification de commandes :	
Combinaison de touches	Effet
Flèche vers le haut ou Ctrl+P	Affiche la dernière commande utilisée. Plusieurs pressions permettent de remonter dans le tampon d'historique. (P comme Previous)
Flèche vers le bas ou Ctrl+N	Permet de redescendre dans les commandes. (N comme Next)
Flèche vers la gauche ou Ctrl+B	Déplace le curseur vers la gauche dans la commande, sans suppression de caractère.
Flèche vers la droite ou Ctrl+F	Déplace le curseur vers la droite dans la commande, sans suppression de caractère
Retour arrière	Déplace le curseur vers la gauche dans la commande, en supprimant le caractère.
Ctrl+A	Place le curseur au début de la commande.
Ctrl+E	Place le curseur en fin de commande.
Ctrl+R	En mode terminal moniteur, affiche correctement la ligne de commande en cours de saisit après la présentation d'un message système.
Echap+B	Déplace le curseur d'un mot vers la droite.
Echap+F	Déplace le curseur d'un mot vers la gauche.



Commandes complémentaires	Commentaires
Albil (config) # line vty 0 4	Configuration pour les accès Telnet.
Albil (config-line) # escape-character 27	Remplace CTRL-MAJ-9 (le caractère '^' sur les claviers US QVERTY) par ESC pour la séquence de 'Break'.
Albil (config-line) # logging synchronous	évite le mélange des commandes avec les messages systèmes
Albil (config-line) # exec-timeout 1 30	Indique le délai d'expiration d'une session, ici de une minute et trente secondes.
Albil (config) # line con 0	Configuration pour les accès Console
Albil (config-line) # escape-character 27	Remplace CTRL-MAJ-9 (le caractère '^' sur les claviers US QVERTY) par ESC pour la séquence de 'Break'.
Albil (config-line) # logging synchronous	évite le mélange des commandes avec les messages systèmes
Albil (config-line) # exec-timeout 0 0	Plus de déconnection automatique

IV.B Les messages Syslog

- ❑ Le système IOS génère des messages en réponse à différents événements et les envoie par défaut vers la console ; ces messages sont appelés syslog.
- ❑ Ces messages ne sont pas visibles lorsque vous vous connectez via Telnet, à moins de saisir la commande 'terminal monitor'.
- ❑ Un autre moyen d'obtenir ces messages est de faire en sorte que le système les mémorise dans un buffer mémoire RAM par la commande 'logging buffered' en mode de configuration global, puis d'utiliser la commande 'show logging' pour les afficher.

IV.C Telnet et Suspend

- ❑ la commande exec Telnet de l'IOS permet de connecter un équipement Cisco à un autre via Telnet.
- ❑ Mais comme souvent, lorsque l'on travaille sur un équipement, on souhaite modifier la configuration sur un autre équipement sans quitter la session Telnet existante.
- ❑ À partir d'une machine Cisco (Routeur ou Switch) on peut suspendre la session Telnet par la commande 'Ctrl+Maj+6 puis x' (sur clavier US 'Maj+6' correspond au caractère '^' sur le clavier FR).

Commande	Description
Ctrl-Maj+6 puis x	Cette commande suspend la session Telnet et replace l'utilisateur dans le shell initial.
# show sessions	Cette commande liste les sessions Telnet suspendues.
# where	Cette commande liste les sessions Telnet suspendues.
# resume 1	Reprend la session '1' de la liste fournit par la commande 'where'
# disconnect 1	Arrête la session Telnet '1' sur une machine distante depuis la machine initiale.

IV.D COPY/TFTP

Copie sur et à partir d'un seveur TFTP	
Commandes	Commentaires
Copy tftp: flash:	La destination ou la source peut-être : <ul style="list-style-type: none"> ○ 'flash': En mémoire flash interne du routeur. ○ 'slot0': Carte flash PCMCIA installé dans le premier connecteur ou dans l'unique connecteur du routeur. ○ 'slot1': Carte flash PCMCIA installé dans le second connecteur du routeur. ○ 'tftp': Indique un transfert vers ou depuis un serveur TFTP.

Configuration TFTP	
Commandes	Commentaires
tftp-server flash:	
ip tftp source-interface e0	

IV.E NTP : Network Time Protocol

- ❑ le protocole NTP utilise le port 123 TCP et UDP.
- ❑ La configuration d'un serveur NTP est importante pour :
 - Le 'syslog' et
 - Le protocole d'authentification Kerberos.

Configuration de l'horloge 'time-of-day'	
Commandes	Commentaires
ntp server 192.168.13.4	'192.168.13.4' est l'adresse IP du serveur NTP
clock time-zone tz-name offset	Configuration du fuseau horaire :
clock time-zone PARIS 1	<ul style="list-style-type: none"> ○ 'tz-name' nom désignant votre fuseau horaire ○ 'offset' décalage par rapport à l'UTC
clock summertime met recurring last sun mar 02:00 last sun oct 02:00	Passage de l'heure d'hivers à l'heure d'été puis de l'heure d'été à l'heure d'hivers. 'last sun mar' signifie le dernier lundi du mois de mars.
clock set 17:21:00 1 april 2004	Définition du 'time of day'
ntp master [stratum value]	Configuration d'un routeur Cisco en serveur NTP. La valeur du 'stratum' est de 1 à 15, la meilleure source a un stratum de 1.
ntp authentication-key key-number	
show clock	Affichage de la date et de l'heure du 'Time of Day'
show ntp associations detail	

- ❑ Exemple.

```
Albil#clock set 17:21:00 1 april 2004
Albil#show clock
17:21:17.511 cet Thu Apr 1 2004
```

Configuration serveur NTP	
Commandes	Commentaires
clock set 17:21:00 1 april 2004	Configuration manuelle de l'heure sur un routeur Cisco
clock time-zone <i>paris 1</i>	Définition du fuseau horaire
! outbound interface interface serial 0 ntp broadcast	
! Global configuration	
ntp authentication-key 1 md5 <i>GEFI</i>	Définition de la clé et du mot de passe d'authentification
ntp authenticate	Activation de l'authentification
ntp trusted-key 1	
ntp trusted-key 2	
ntp master 2	
ntp peer 192.168.1.1 key 1	

Configuration client NTP	
Commandes	Commentaires
! inbound interface interface serial 0 ntp broadcast client	
! Global configuration	
ntp authentication-key 1 md5 <i>GEFI</i>	
ntp authenticate	Activation de l'authentification
ntp trusted-key 1	
ntp trusted-key	
ntp peer 192.168.1.1 key 1	

Commande de configuration 'ntp peer'	
ntp peer <i>ip-address version number key keyid source interface prefer</i>	
<i>ip-address</i>	
<i>version number</i>	(optionnel)
<i>key keyid</i>	(optionnel)
<i>source interface</i>	(optionnel)
<i>prefer</i>	(optionnel)
Exemple	
# ntp peer	

IV.F Rappel : configuration

Configuration générale	
Commandes	Commentaires
Routeur# erase startup-config	Effacement de la configuration initial
Routeur# reload	Reboot du router
Routeur # show flash:	Visualise les différents IOS contenus en mémoire Flash
Routeur # show version	Visualise : La version d'IOS, Le nombre et le type d'interfaces, La quantité et le type de mémoire (RAM & Flash) Le Config-Register
Router(config)# config-register 0x2102	Réinitialisation du registre à sa valeur par défaut.
Routeur# show startup-config	Visualisation du fichier de configuration qui initialise l'IOS au boot.
Routeur# show running-config	Visualisation de la configuration (courante) dynamique.
Routeur# copy running-config startup-config Ou Routeur# wr	Sauvegarde de la configuration dynamique en NVRAM
Routeur# configure terminal Router(config)# hostname Albil Albil(config)#	Entrer dans le mode global de configuration Définir le nom du routeur, très utile lors d'un telnet.
Routeur# show history	Visualisation des dernières commandes.
Routeur# show hosts	Visualisation : Nslookup et table des hosts (équi. /etc/hosts).
Routeur# terminal monitor	Active l'affichage des messages d'erreur système et de DEBUG sur la console
Routeur# terminal no monitor	Désactive l'affichage des messages d'erreur système et de DEBUG sur la console
Routeur# undebug all	Arrête debug
Albil(config)# ip default-gateway A.B.C.D	Il faut définir un 'Default Gateway' pour le RXBOOT ou lorsqu'un routeur est utilisé en pont ou que 'Ip Routing' est désactivé'.
Routeur# configure terminal Router(config)# ip subnet-zero	Autorise l'utilisation du premier et dernier sous réseau pour la configuration des interfaces et la mise à jour des tables de routage (RFC 1812 & 1878).
Router(config)# no ip subnet-zero	Interdit l'utilisation du premier et dernier sous réseau
Albil(config)# banner motd \$ Enter TEXT message. End with the character '\$'. Bonjour, ALBI_1 \$ Albil(config)#	Création d'une bannière d'accueil
Albil# show user all	Visualisation des utilisateurs connectés.

Configuration d'une interface Ethernet	
Commandes	Commentaires
Routeur# configure terminal	Entrer dans le mode global de configuration
Routeur(config)# interface ethernet 0	Spécifier l'interface à configurer : <ul style="list-style-type: none"> o 'ethernet' pour les NIC à 10 M bps. o 'fastethernet' pour les NIC à 10/100 M bps.
Routeur(config-if)# shutdown	Désactiver l'interface
Routeur(config-if)# description Network Salle Y	Description de la connexion.
Routeur(config-if)# ip address 192.168.2.1 255.255.255.0	Affecter à l'interface son adresse IP et son Subnet Mask
Routeur(config-if)# bandwidth 10000000	(optionnel) paramètre, indiquant le débit de l'interface, utilisé par certains protocoles de routage dynamiques (IGRP, EIGRP et OSPF)
Routeur(config-if)# mtu 1522	Cette commande définit la MTU pour tous les protocoles de niveau 3. C'est la commande généralement utilisée, pour assigner une valeur différente uniquement à IP on emploie la commande 'ip mtu'.
Routeur(config-if)# ip mtu 1522	Cette commande définit la MTU pour le protocole IP uniquement.
Routeur(config-if)# no shutdown	Activer l'interface

Configuration d'une interface Série	
Commandes	Commentaires
Routeur# configure terminal	Entrer dans le mode global de configuration
Routeur(config)# interface serial 1	Spécifier l'interface à configurer.
Routeur(config-if)# shutdown	Désactiver l'interface
Routeur(config-if)# description To Albi2	Description de la connexion.
Routeur(config-if)# ip address 192.168.1.1 255.255.255.0	Affecter à l'interface son adresse IP et son Subnet Mask
Routeur(config-if)# encapsulation ppp # ppp chap ... # ppp pap ...	Les interfaces 'Serial' peuvent être configurées en : <ul style="list-style-type: none"> o 'HDLC' attention, ici HDLC est propriétaire CISCO car un champ Ethertype a été rajouté. o 'PPP' protocole standard avec authentification.
Routeur(config-if)# clock rate 56000	(optionnel) clockrate configure l'interface en DCE, en fonction de la position du câble Back to Back.
Routeur(config-if)# bandwidth 56	(optionnel) paramètre, indiquant le débit de l'interface, utilisé par certains protocoles de routage dynamiques (IGRP, EIGRP et OSPF). La valeur par défaut est de 1.544, ce qui correspond à un lien T1 de 1,544 Mbps.
Routeur(config-if)# no shutdown	Activer l'interface

Commande de configuration du routage Statique	
ip route A.B.C.D E.F.G.H I.J.K.L	
ip route	Identifie la déclaration d'une route statique / Forwarding router's address
A.B.C.D	Spécification du réseau destination (Adresse cible) / destination prefix
E.F.G.H	Subnet Mask associé à l'adresse ci-dessus / destination prefix mask
I.J.K.L	Adresse IP du (Next-Hop Gateway) routeur vers le réseau de cible / Forwarding router's address
Exemple	
Routeur(Config)# ip route 192.168.7.0 255.255.255.0 192.168.67.2	

Console password	
Commandes	signification
	Attachez un terminal ou un ordinateur en émulation de terminal su le port console du switch.
config terminal	Entrez en mode Configuration Global
line console 0	Entrez en mode de configuration d'interface pour l'accès au port console
password <i>gefi</i>	Le mot de passe n'est pas chiffré
login	Active la vérification du mot de passe
exec-timeout 5 30	Déconnection au bout de 5 minutes et 30 secondes.
logging synchronous	Affichage correct des commandes malgré les messages système.
escape-character 27	La touche ESC permet de réaliser une séquence de break.
end	

VTY Password : accès Telnet	
Commandes	Signification
enable	Entrez en mode ' <i>Privileged EXEC</i> '
config terminal	Entrez en mode Configuration Global
line vty 0 4	Entrez en mode de configuration d'interface pour l'accès du telnet
password <i>gefi</i>	Entrez le mot de passe pour l'ouverture du session telnet
login	Active la vérification du mot de passe
exec-timeout 0 0	Plus de déconnection automatique.
logging synchronous	Affichage correct des commandes malgré les messages système.
escape-character 27	La touche ESC permet de réaliser une séquence de break.
access-class 1 in	L' <i>access-class</i> uniquement pour le trafic telnet. Ici j'autorise uniquement l'adresse IP dans l' <i>access-list</i> à entrer.
end	
show running-config	
copy running-config startup-config	

Access List sur les VTY	
Albil(config)# Access-list 1 permit 192.168.1.32 0.0.0.31	Sécurité sur un accès Telnet
Albil(config)# Line vty 0 4	
Albil(config-line)# Access-class 1 in	

Enable password	
Commandes	signification
config terminal	
enable secret <i>cisco</i>	Le mot de passe est chiffré (recommandé)
enable password <i>cisco</i>	Le mot de passe n'est pas chiffré
end	Retour au menu principal.
show running-config	Visualisation de la configuration active.
copy running-config startup-config	Sauvegarde de la ' <i>running-config</i> ' dans la ' <i>startup-config</i> '.

V. Routage IP

V.A Définition

- Un **protocole de routage enregistre dans la table de routage des informations de routage**. RIP, IGRP, EIGRP et OSPF sont des exemples de protocoles de routage.
- Un **protocole routé est un protocole pour lequel il existe une spécification de niveau 3**, ou équivalente, **définissant l'adressage logique et le routage**. IP et IPX sont des exemples de protocoles routés.

V.B Distance administrative

- ❑ Lorsque **plusieurs protocoles de routage** dynamique et de **routes statiques** sont utilisés en même temps, une distance administrative est utilisée pour évaluer **la pertinence de chaque route**. L'IOS pourra alors, pour chaque route acquise, sélectionner **la route ayant la plus petite distance administrative**.
- ❑ Une **distance administrative est un entier sur huit bits** (de 0 à 255). En général, **plus la valeur** de la distance administrative fournie par un protocole de routage **est faible**, et **plus les chances de celui-ci d'être utilisé sont importantes**.
- ❑ Valeurs standard par défaut

Origine de la Route	Distance administrative
Route directement connectée	0
Route statique	1
Route IGRP de synthèse	5
Route BGP externe	20
Route IGRP avancé interne	90
Route IGRP	100
Route OSPF	110
Route IS-IS	115
Route RIP	120
Route EGP	140
Route EIGRP	170
Route BGP interne	200
Route Inconnu	255

- ❑ La distance administrative des routes statiques peut être changée par la commande `ip route` en renseignant son dernier paramètre optionnel [`distance`] avec la valeur voulue.
- ❑ La distance administrative des routes directement connectées et des routes agrégées de EIGRP ne peuvent pas être modifiées.

V.C La métrique

V.C.1 Présentation

- ❑ **Une métrique représente une distance.** Les métriques permettent de choisir le meilleur chemin de routage. Chaque algorithme de routage interprète la table de routage et génère un nombre (valeur métrique) pour chaque chemin du réseau. La plus petite valeur représente le meilleur chemin.
- ❑ Les métriques peuvent être calculées à partir d'une seule caractéristique du chemin, mais des métriques complexes sont employées, elles combinent plusieurs caractéristiques. Parmi les métriques les plus utilisées :
 - Nombre de sauts (hop count) :
 - Tops (ticks) :
 - Coût (cost) :
 - Bande passante (bandwidth) :
 - Durée (delay) :
 - Fiabilité (reliability) : le taux d'erreur d'un lien réseau.
 - Charge (loading)
 - MTU

V.C.2 RIP

- ❑ Dans ce protocole la métrique d'une route se calcule en nombre de sauts. Une fois celle-ci apprise via ses voisins, le routeur l'annonce à son tour avec une métrique incrémentée de 1.
- ❑ Le '*HOP Count*' (nombre de sauts) sert de métrique pour sélectionner le plus court chemin et indique le nombre de routeurs à traverser.
 - Un '*HOP Count*' de 0 indique un réseau connecté directement au routeur
 - La valeur maximum du HOP Count est 15,
 - un HOP Count de 16 indique une route infinie.

V.C.3 IGRP

- ❑ IGRP utilise une métrique de routage composite. Cette métrique comprend les composants suivants
 - Bande passante (*bandwidth*) :
 - Durée (*delay*) :
 - Fiabilité (*reliability*) :
 - Charge (*loading*)
 - MTU

➤ La formule que IGRP utilise pour calculer la métrique de chaque route est la suivante :

$$M_{IGRP} = \left[(k1 \times B_{IGRP}) + \left(\frac{k2 * B_{IGRP}}{256 - L} \right) + (k3 \times D_{IGRP}) \right] \times \frac{k5}{R + k4}$$

V.C.4 EIGRP

- ❑ la métrique calculée par EIGRP est basée sur la même formule que celle de IGRP, avec une multiplication du résultat par 256, ce qui donne :

$$\circ \quad M_{EIGRP} = M_{IGRP} * 256$$

V.C.5 OSPF

- ❑ Le protocole OSPF calcule la métrique d'une route en cumulant le coût de tous les segments qui la constituent, selon la formule : $C = \frac{10^8}{B}$. B désigne le débit de l'interface mesuré en bits par seconde (bps).

V.C.6 Changement de métrique RIP

- ❑ Quand plusieurs routes existent, il peut être nécessaire de contraindre RIP à choisir une route plutôt qu'une autre, surtout si deux liaisons parallèles entre deux routeurs ont des débits différents. Dans cette architecture, il faut que RIP choisisse la liaison ayant le débit supérieur.
- ❑ Comme le métrique de RIP est le nombre de saut, l'IOS offre une commande permettant de modifier le métrique de RIP.

Format de la commande :

```
offset-list <liste d'accès> {in|out} <valeur de majoration> [<interface>]
```

```
Routeur# configure terminal
Router(config)# router rip
Router(config-router)# offset-list 0 in 3 serial0
Router(config-router)# network 192.168.16.0
```

Commande	Description
off-list	Commande
<liste d'accès>	Si '0' la majoration s'applique à toutes les routes. Si numéro d'une liste d'accès, la majoration s'applique aux routes correspondantes.
{in out}	Cet argument indique si la commande s'applique en entrée ou en sortie des mises à jour.
<valeur de majoration>	Incrément.
[<interface>]	Argument optionnel. Si ce champ est absent, le changement de métrique est appliqué sur toutes les interfaces en conformité avec les autres arguments.

Ici la distance administrative est de '110', car la route a été acquise par OSPF

```
Castres1#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, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

C    192.168.15.0/24 is directly connected, Ethernet0
O IA 192.168.20.0/24 [110/820] via 192.168.15.48, 00:09:51, Ethernet0
O IA 192.168.36.0/24 [110/820] via 192.168.15.50, 00:09:51, Ethernet0
R    192.168.52.0/24 [120/1] via 192.168.50.1, 00:00:20, Serial1
O IA 192.168.17.0/24 [110/810] via 192.168.15.48, 00:09:51, Ethernet0
C    192.168.50.0/24 is directly connected, Serial1
O IA 192.168.35.0/24 [110/420] via 192.168.15.50, 00:09:51, Ethernet0
O IA 192.168.16.0/24 [110/410] via 192.168.15.48, 00:09:51, Ethernet0
O IA 192.168.32.0/24 [110/410] via 192.168.15.50, 00:09:51, Ethernet0
R    192.168.49.0/24 [120/1] via 192.168.50.1, 00:00:20, Serial1
O IA 192.168.18.0/24 [110/810] via 192.168.15.48, 00:09:51, Ethernet0
C    192.168.48.0/24 is directly connected, Serial0
O IA 192.168.33.0/24 [110/810] via 192.168.15.50, 00:09:51, Ethernet0
Castres1#
```

Ici la distance administrative est de '120', car la route a été acquise par RIP

V.D Règles de routage

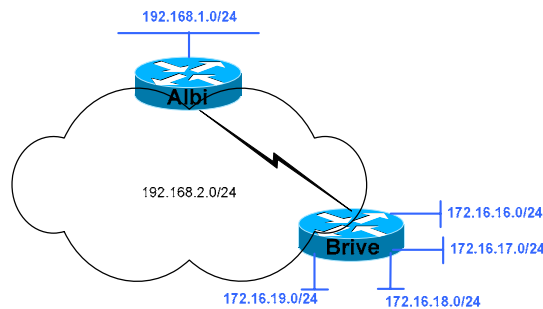
- ❑ Le routeur n'utilise les métriques que dans le cadre d'un protocole de routage particulier. Si un protocole à vecteur distance reçoit plusieurs messages de mise à jour pour le même préfixe, la route à la meilleure métrique prévaut sur les autres pour être inscrite dans la table de routage.
- ❑ Si l'information de routage provient de plusieurs origines (par exemples, les protocoles de routage dynamique, les routes statiques et les routes directement connectées) pour la même destination, la route installée dans la table sera celle dont l'origine possède la plus petite valeur administrative au détriment des autres.
- ❑ Le routeur utilise l'algorithme de recherche par la correspondance la plus longue (Subnet Mask) pour trouver la meilleure route vers une destination, dans sa table de routage (voir classement des routes dans la table de routage).
- ❑ Un protocole à vecteur distance n'annonce pas une route qu'il n'a pas installée dans la table de routage.
- ❑ Dans un protocole à état de liens, le déroulement de l'algorithme de Dijkstra, pour le calcul du plus court chemin, permet de remplir la table de routage.

V.E Synthèse automatique et agrégation de routes

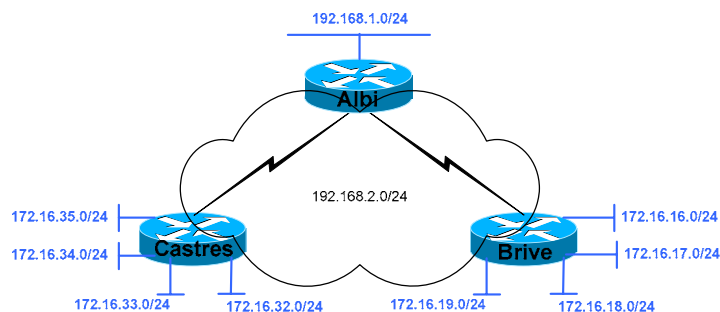
- ❑ l'IOS a été optimisé pour assurer un routage aussi rapide que possible pour diminuer la latence. Il n'en reste pas moins vrai que n'importe quel algorithme qui doit effectuer une recherche dans une liste fonctionnera plus rapidement si la liste est courte.

V.E.1 La synthèse automatique / *autosummarization*

- ❑ Sur RIP et IGRP, la synthèse automatique ne peut être désactivée.
- ❑ Sur RIP v2 et EIGRP, elle peut par contre être activée ou désactivée.
- ❑ La conception de sous réseaux IP n'autorise traditionnellement pas les réseaux discontinus.
 - Le terme *continu* désigne un réseau de classe A, B ou C sur lequel toutes les routes vers des sous réseaux de ce réseau passent uniquement par d'autres sous réseaux de ce même réseau.

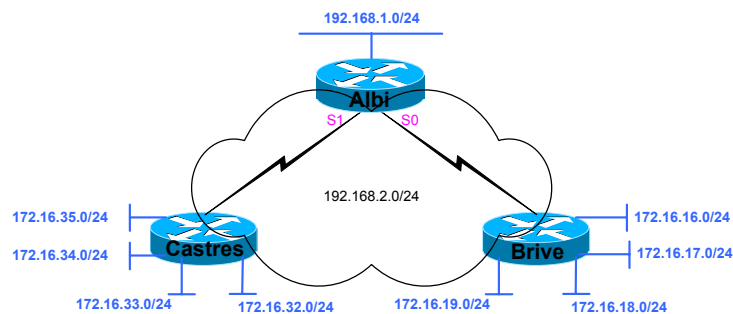


- Le terme *discontinu* qualifie un réseau de classe A, B ou C pour lequel les routes vers au moins un sous réseau de ce réseau passent par des sous réseaux d'un réseau différent.



V.E.2 L'agrégation de routes / route aggregation

- ❑ Également appelée synthèse de routes (route summarization).
- ❑ CIDR (*Classless Interdomain Routing*-routing interdomaine sans classe) est une convention définie dans la RFC 1817 (www.ietf.org/rfc/rfc1817.TXT) qui demande l'agrégation de plusieurs adresses réseaux en une seule route. L'objectif du CIDR est de simplifier les tables de routages des routeurs de l'Internet : imaginez un routeur dont la table de routage devrait contenir les routes vers tous les réseaux de classe A, B et C ($[2^{7-1}-2]+[2^{16-2}]+[2^{24-3}]$). Voir BGP.
- ❑ RIP v2, EIGRP et OSPF supportent l'agrégation de routes.
- ❑ L'agrégation de routes sert simplement à indiquer à un protocole de routage dynamique qu'il doit annoncer une seule route plutôt que plusieurs.



Configuration d'Albi :

```
Router eigrp 1
 network 192.168.1.0
 network 192.168.2.0
 no auto-summary
!
interface serial 0
 ip address 192.168.2.1 255.255.255.252
 ip summary-address eigrp 1 172.16.16.0 255.255.240.0
!
interface serial 1
 ip address 192.168.2.5 255.255.255.252
 ip summary-address eigrp 1 172.16.32.0 255.255.240.0
```

Configuration de Brive ou de Castres :

```
Router eigrp 1
 network 172.16.0.0
 network 192.168.2.0
 no auto-summary
```

- ❑ La commande 'ip summary-address' depuis le menu de configuration de l'interface n'existe que pour EIGRP. On peut également synthétiser les routes OSPF.

V.E.3 CIDR

CIDR : *Classless Interdomain Routing* - routage interdomaine sans classe

- ❑ CIDR (*Classless Interdomain Routing*-routage interdomaine sans classe) est une convention définie dans la RFC 1817 (www.ietf.org/rfc/rfc1817.TXT) qui demande l'agrégation de plusieurs adresses réseaux en une seule route. L'objectif du CIDR est de simplifier les tables de routages des routeurs de l'Internet : imaginez un routeur dont la table de routage devrait contenir les routes vers tous les réseaux de classe A, B et C ($[2^{31-2}] + [2^{16-2}] + [2^{24-3}]$). Voir BGP.
- ❑ La RFC 1466 [Gerich 1993] recommande que les nouvelles adresses de classe C en Europe soient dans la plage de 194.0.0.0 à 195.255.255.255. Ce qui permet aux pays en dehors de l'Europe de posséder une seule route 194.0.0.0/7 (194.0.0.0 mask 254.0.0.0) pour atteindre une machine sur notre continent.

In particular, the top level block allocation be designated as follows:

Multi-regional	192.0.0.0 - 193.255.255.255
Europe	194.0.0.0 - 195.255.255.255
Others	196.0.0.0 - 197.255.255.255
North America Central/South America	198.0.0.0 - 199.255.255.255
Pacific Rim	200.0.0.0 - 201.255.255.255
Others	202.0.0.0 - 203.255.255.255
Others	204.0.0.0 - 205.255.255.255
Others	206.0.0.0 - 207.255.255.255

V.F Synthèse des protocoles de routage dynamiques

Fonctionnalités	RIP (par défaut)	IGRP (par défaut)	EIGRP	OSPF
Temporisateur de mise à jour	30 secondes	90 secondes		
Type	Vecteur de distance	Vecteur de distance	Hybride équilibré	Etat de lien
Métrique	Compte de sauts	Métrique composée qui prend en compte la bande passante, le délai (par défaut), mais aussi la fiabilité, la charge et la valeur MTU.	Métrique composée qui prend en compte la bande passante, le délai (par défaut), mais aussi la fiabilité, la charge et la valeur MTU.	Coût
Valeur de métrique infinie	16	4.294.967.295		
Mécanisme de prévention des boucles	Temporisateur Holddown, Split-horizon	Temporisateur Holddown, Split-horizon	DUAL	Algorithme SPF et connaissance complète de la topologie
Temporisateur Holddown	180	280		
Mises à jour flash	Oui	Oui		
Masque de sous réseau envoyé dans la mise à jour	Non, pour RIP V1 Oui, pour RIP V2	non	Oui	oui
Encapsulé dans	UDP/520	IP, protocole 09 (0x09)	IP, protocole 88 (0x58)	IP, protocole 89 (0x59)
Adressage	Broadcast IP en RIPv1 Multicast IP en RIPv2 (224.0.0.9)	Broadcast IP	Multicast IP (224.0.0.10)	Multicast IP (224.0.0.5)

- ✓ En RIP, la métrique maximale est de 16 HOP (métrique infinie)
- ✓ Le coût **OSPF** : il est inversement proportionnel à la bande passante de l'interface. Une bande passante élevée signifie un coût faible. **Coût = 100.000.000 / Bande passante en bps.**
 - Une ligne Ethernet à 10Mbps coûtera : $10^8 / 10^7 = 10$,
 - Une ligne T1 coûtera : $10^8 / 154400 = 64$.

Protocole de routage	Synthèse automatique activée	Synthèse automatique désactivable	Supporte l'agrégation de routes
RIP v1	Oui, par défaut	Non	Non
RIP v2	Oui, par défaut	Oui	Oui
IGRP	Oui, par défaut	Non	Non
EIGRP	Oui, par défaut	Oui	Oui
OSPF	Non, mais l'agrégation peut remplir la même fonction	Non applicable	Oui

Protocole de routage	Type	Prévention des boucles	Masques envoyés
RIP v1	Vecteur distance	Temporisateur Hold-down et Split-horizon	Non
RIP v2	Vecteur distance	Temporisateur Hold-down et Split-horizon	Oui
IGRP	Vecteur distance	Temporisateur Hold-down et Split-horizon	Non
EIGRP	Hybride équilibré	DUAL et successeur possible	Oui
OSPF	Etat de lien	Algorithme SPF ou Dijkstra et carte topologique complète	Oui

DUAL : Diffusing Update Algorithm

SPF : Shortest Path First

VI. RIP

RIP : Routing Information Protocol

- ❑ Le protocole RIP est également connu sous le nom d'un programme qui le met en œuvre : 'routed'.
- ❑ Le programme 'routed' a été réalisé à l'université de Californie, à Berkeley.
- ❑ RIP peut réaliser un équilibrage de charge sur jusqu'à six chemins aux coûts identiques (quatre chemins par défaut).

VI.A RIP v1

- ❑ RIP v1 repose sur la RFC 1058 de l'IETF,
- ❑ RIP est un algorithme de type 'Distance Vector'
- ❑ RIP v1 utilise la diffusion (Broadcast) de paquet de données UDP/520 (Port : 520) pour échanger ses tables de routage toutes les 30 secondes dans leurs intégralités.
- ❑ Le HOP Count (nombre de sauts) sert de métrique pour sélectionner le plus court chemin et indique le nombre de routeurs à traverser.
 - Un HOP Count de 0 indique un réseau connecté directement au routeur
 - La valeur maximum du HOP Count est 15,
 - un HOP Count de 16 indique une route infinie.
- ❑ RIP v1 travaille en 'Classful', donc il ne peut pas fonctionner avec les VLSM (*Variable Length Subnet Mask*).
 - Ses annonces sont réalisées en Broadcast (logique et physique) sur le Port 520 (source et destination) toutes les 30 secondes par défaut.

VI.B RIP v2

- ❑ RIP v2 repose sur la RFC 1721, 1722 et 1723 de l'IETF.
- ❑ RIP v2 émet ses annonces en **Multicast** (adresse IP : 224.0.0.9) sur le port UDP/520 pour échanger ses tables de routage.
- ❑ RIP v2 apporte en plus :
 - **CIDR** (Classless Internet Domain routing) ou 'Classless',
 - Les mises à jour déclenchées (flash),
 - L'**authentification** : texte en clair pour la RFC et MD5 pour la solution propriétaire CISCO,
 - Transmission du masque de sous réseau
 - ✓ La synthèse de route (route **summarization**) : synthèse automatique (auto summarization) actif par défaut et l'agrégation de routes (route aggregation),
 - ✓ Les **VLSM** : Variable Length Subnet Mask / masques de sous réseau à longueur variable

Protocole de routage	Synthèse automatique activée	Synthèse automatique désactivable	Supporte l'agrégation de routes
RIP v1	Oui, par défaut	Non	Non
RIP v2	Oui, par défaut	Oui	Oui
IGRP	Oui, par défaut	Non	Non
EIGRP	Oui, par défaut	Oui	Oui
OSPF	Non, mais l'agrégation peut remplir la même fonction	Non applicable	Oui

VI.C Fonctionnement

- ❑ Lorsque des routeurs apprennent des modifications de l'inter réseau, ils actualisent leurs tables de routages avec ces changements et les envoient à leurs voisins.
- ❑ A la réception d'une table de routage, le routeur l'intègre dans ses propres tables de routage, exécute l'algorithme de BELLMAN-FORD puis émet les tables de routage actualisées. Ce processus n'est achevé que lorsque tous les routeurs ont convergé.
- ❑ S'il n'y a pas de changement dans l'inter réseau, chaque routeur envoie ses tables de routage à ses voisins toutes les 30 secondes.
- ❑ Les temporisateurs :
 - Le temporisateur d'Actualisation de routage (*advertising* / publication) est généralement configuré sur 30 secondes, ce qui assure que chaque routeur émet une copie complète de sa table de routage vers tous ses voisins.
 - Le temporisateur de Route invalide détermine la durée qui doit s'écouler sans recevoir d'actualisation sur une route pour considérer celle-ci comme invalide. Lorsqu'une route est marquée invalide, les voisins sont informés. T= 180secondes
 - Le temporisateur Abandon de route (Flush Route) indique le délai avant suppression d'une route invalide. T= 240secondes

Les temporisations RIP		
timers basic Interval Invalid holddown flush [sleep]		
Temporisation	Par défaut	Signification
'Update' Intervalle de mise à jour	30s	Temps entre chaque mise à jour de routage. Cette valeur peut être configurée, mais elle doit être identique sur tous les routeurs RIP.
'Invalid' Intervalle d'invalidation	180s	Si un routeur ne reçoit plus les mises à jour d'un autre routeur, il marque les routes de cet autre routeur comme invalides après 180s de silence.
'holddown' Intervalle de retenue	180s	La mise à jour d'une route redevenue active, suite à une période d'inaccessibilité, ne sera effective qu'après expiration des 180s de temporisation.
'flush' Intervalle d'élimination	240s	Si aucune mise à jour n'a toujours pas été reçue après 240s, le routeur supprime toutes les entrées de la table de routage relative au routeur devenu silencieux.
'sleep'		

- ❑ RIP classe les participants en machines « actives / passive » et « passives / silent » :
 - Un routeur actif propage les routes qu'il connaît vers les autres machines.
 - Une machine passive écoute uniquement les machines actives et met à jour leur table de routage en fonction des informations reçues.

VI.D Configuration

Commandes	Commentaires
Router# configure terminal Router(config)# router rip Router(config-router)#	Initialisation de RIP
Router(config-router)# network 192.168.3.0	Ajoute le réseau spécifié
Router(config-router)# no network 192.168.3.0	Supprime le réseau spécifié
Router(config-router)# version 2	Activation de RIP 2. Par défaut RIP fonctionne en Version 1
Router(config-router)# passive-interface ethernet 0	Suppression des annonces RIP sur ce réseau (eth0) seulement, si aucun routeur n'existe sur celui-ci.
Router(config-router)# no auto-summary	Evite l'agrégation de routes. <ul style="list-style-type: none"> o Lors du déploiement o Si le plan d'adressage IP n'est pas cohérent.
# timers basic Update Invalid holdown flush sleep	Les temporisateurs RIP : <ul style="list-style-type: none"> o 'Update' Actualisation : publication de la table de routage, par défaut toutes les 30 secondes. o 'Invalid' Invalide (temporisateur de route invalide) : durée par défaut 180 secondes. o 'holdown' Conservation : durée par défaut 180 secondes o 'flush' Suppression (abandon de route) : durée par défaut 240 secondes o 'sleep'
Router(config-router)# no timers basic	Restaure les valeurs par défaut des temporisateurs
Router(config-router)# exit	
Router(config)# no router rip	Arrêt de RIP et suppression de sa configuration. Cette commande peut être saisie avant une nouvelle configuration.

Commandes	Commentaires
Router(config)# router rip	A partir du mode configuration global.
Router(config-router)# version 2	Définition de RIP en version 2
Router(config-router)# network 192.168.0.0	Définition des réseaux pour les annonces
Router(config-router)# passive-interface default	Suppress routing updates on all interfaces
Router(config-router)# passive-interface ? Ethernet IEEE 802.3 Null Null interface Serial Serial default Suppress routing updates on all interfaces <cr>	
#	
# no passive-interface serial 0	Active routing update on interface Serial 0 et 1
# no passive-interface serial 1	Mais ici l'interface Ethernet 0 (Cisco2500) n'émet pas d'Update RIP.
#	

Commandes complémentaires	Commentaires
Router# show ip route [sous réseau]	Affiche la totalité de la table de routage, ou une entrée si le sous réseau est spécifié.
Router# show ip protocol	Paramètres des protocoles de routage, valeurs courantes des temporisateurs
Router# debug ip rip	Génère des messages de journalisation pour chaque mise à jour RIP.
Router# no debug ip rip	Arrêt du Debug
Router# configure terminal Router(config)# ip subnet-zero	Autorise l'utilisation du premier sous réseau pour la configuration des interfaces et la mise à jour des tables de routage (RFC 1812 & 1878).
Router# configure terminal Router(config)# no ip subnet-zero	Interdit l'utilisation du premier et dernier sous réseau.

VI.D.1 La commande NETWORK

- Cette commande définit :
 - les réseaux présents dans la table de routage RIP
 - et les interfaces, correspondant au réseau déclaré, où le protocole RIP envoie les mises à jour de routage

VI.D.2 Spécification de la version

- L'utilisation de RIP v2 est préconisée pour :
 - Ces annonces en Multicast, évitent l'émission de trames en broadcast,
 - Les VLSM, l'emploi optimum de l'espace adressable IP,
 - Le CIDR qui permet de réduire le nombre de routes dans la table de routage IP et
 - L'authentification.

Commandes	Paquets RIP
# router rip	Réception des versions 1 et 2, émission de la version 1
# router rip version 1	Réception et émission de la version 1
# router rip version 2	Réception et émission de la version 2

Commandes	Fonctions
# ip rip send version 1	Seuls les paquets RIP de version 1 sont émis
# ip rip receive version 1	Seuls les paquets RIP de version 1 sont reçus
# ip rip send version 2	Seuls les paquets RIP de version 2 sont émis
# ip rip receive version 2	Seuls les paquets RIP de version 2 sont reçus
# ip rip send version 1 2	Tous les paquets RIP sont émis
# ip rip receive version 1 2	Tous les paquets RIP sont reçus

VI.D.3 Boucles de routage

- ❑ les boucles de routage peuvent se produire lors de l'utilisation de protocoles de routage par vecteur de distance en raison de la propagation d'informations erronées.
- **Split-horizon/horizon éclaté**: cette fonction est utile à la prévention des boucles de routage, **car elle empêche un routeur d'annoncer une route sur l'interface par laquelle l'information de route a été apprise**. Cette technique, associée à celle du Poison Reverse permet de s'attaquer aux topologies les plus complexes. En fait, les routes découvertes via une interface ne doivent pas être annoncées de nouveau par la même interface, puisque les autres routeurs partageant cette liaison devraient déjà en avoir pris connaissance à partir de la mise à jour initiale.

Commandes	Description
# ip split-horizon	Activation de Split Horizon par défaut.
# no ip split-horizon	Désactivation de Split Horizon

- **Holdown** : délai de retenue indiquant que lorsqu'une route est retirée, les nouvelles routes vers cette destination ne sont pas acceptées. Cette technique est particulièrement efficace sur des réseaux ayant des liens redondants.
- **Poison Reverse** : permet d'éviter les boucles de routage et d'améliorer la vitesse de convergence. Le Poison Reverse annonce une route avec une métrique infinie lorsque celle-ci n'est plus utilisable.

Problème	Solution
Plusieurs routes de même métrique vers le même sous réseau	Les options d'implémentation peuvent entraîner l'intégration dans la table de routage de la première route apprise, ou de toutes les routes.
Des boucles de routage se produisent en raison des mises à jour se croisant sur une même ligne.	Split-horizon . Le protocole de routage annonce une route sur une interface de sortie uniquement si cette route n'a pas été découverte au moyen d'une mise à jour reçue sur cette même interface. Split-horizon avec Poison-reverse . Le protocole de routage utilise les règles de la fonction Split-horizon sauf en cas de panne d'une liaison. Dans ce cas, la route affectée est annoncée sur toutes les interfaces avec une métrique signifiant une distance infinie.
Les boucles de routage se produisent en raison de mises à jour se croisant sur des voies différentes.	Route-poisoning . Lorsqu'une route vers un sous réseau est indisponible, le sous-réseau est annoncé avec une métrique indiquant une distance infinie.
Comptage à l'infini.	Temporisation de retenue Hold-down . Après avoir pris connaissance de l'indisponibilité d'une route vers un sous réseau, un routeur attend un certain temps avant de prendre en compte (ou de croire) toute information de routage de ce sous réseau. Mises à jour déclenchées (Flash) . Lorsqu'une route est inutilisable, une mise à jour est immédiatement expédiée au lieu d'attendre l'expiration du temporisateur de mise à jour. L'association de cette fonction et de la fonction Route-poisoning garantit que tous les routeurs prennent connaissance de l'indisponibilité d'un chemin avant expiration d'un temporisateur Hold-down.

VI.D.4 Changement de métrique

- ❑ Quand plusieurs routes existent, il peut être nécessaire de contraindre RIP à choisir une route plutôt qu'une autre, surtout si deux liaisons parallèles entre deux routeurs ont des débits différents. Dans cette architecture, il faut que RIP choisisse la liaison ayant le débit supérieur.
- ❑ Comme le métrique de RIP est le nombre de saut, l'IOS offre une commande permettant de modifier le métrique de RIP.
- ❑ Dans l'exemple ci-dessous, toutes les routes RIP reçues par l'interface 'Serial0' ont leur HOP augmenté de trois.

Exemple :

```
Routeur# configure terminal
Router(config)# router rip
Router(config-router)# offset-list 0 in 3 serial0
Router(config-router)# network 192.168.16.0
```

Commande de changement de métrique

`offset-list Access-list-Number {in|out} <valeur de majoration> [Interface-name]`

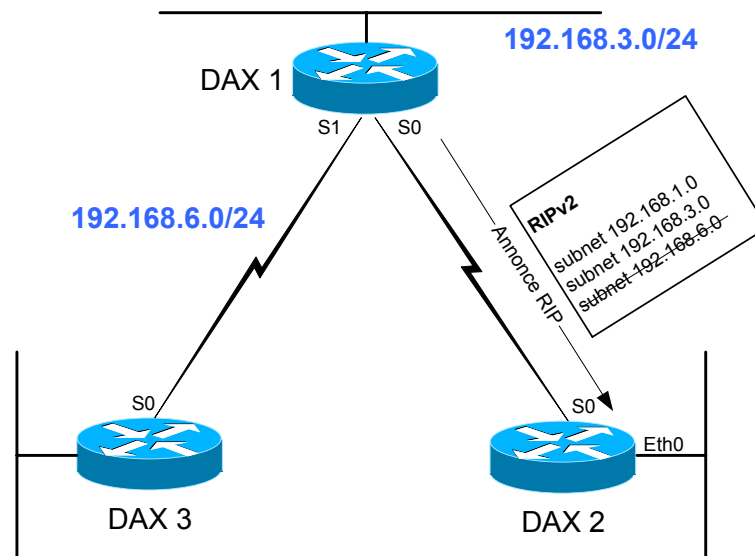
<code>off-list</code>	Commande
<code>access-list-Number</code>	Si '0' la majoration s'applique à toutes les routes. Si numéro d'une liste d'accès, la majoration s'applique aux routes correspondantes.
<code>{in out}</code>	Cet argument indique si la commande s'applique en entrée ou en sortie d'une interface.
<code><valeur de majoration></code>	Incrément.
<code>[Interface-name]</code>	Argument optionnel. Si ce champ est absent, le changement de métrique est appliqué sur toutes les interfaces en conformité avec les autres arguments.

Exemple :

```
offset-list 0 in 3 serial0
```


VI.D.5 Filtrage de mises à jour

- Dans cet exemple le Routeur 'Dax2' refuse les 'Update' RIP du réseau '192.168.6.0 0.0.0.255' en entrée de son interface 'Serial 0'.

**Format de la commande :**

```
distribute-list Access-list-Number {in|out} [Interface-name|routing-process|as-number]
```

```
Dax2# configure terminal
```

```
Dax2 (config)# router rip
```

```
Dax2 (config-router)# network 192.168.5.0
```

```
Dax2 (config-router)# distribute-list 16 in S0
```

```
Dax2 (config)# access-list 16 deny 192.168.6.0 0.0.0.255
```

```
Dax2 (config)# access-list 16 permit any
```

VI.D.6 Authentification RIP

- ❑ RIPv2 permet la mise en oeuvre de l'authentification, mais celle-ci est réalisée à partir d'un secret émis en clair sur le réseau.
- ❑ CISCO propose de l'authentification propriétaire avec le mot de passe (secret) chiffré MD5.
- ❑ Seul le mot de passe est chiffré, les informations de routage reste en clair.

Commandes	Commentaires
R# conf t	
R(config)# key chain gefi	Création du groupe de clés (keychain) nommé 'gefi'
R(config-keychain)# key 1	Identification de la clé N°1. <ul style="list-style-type: none"> ○ L'intervalle de la clé est de 0 à 2147483647. ○ L'identification des clés doit être consécutive.
R(config-keychain-key)# key-string password_A	Définition du mot de passe, suite de caractères alphanumériques (de 1 à 80) excepté le premier caractère qui ne peut pas être un caractère numérique.
# accept-lifetime 00:00:00 jan 1 2004 infinite	Durée pendant laquelle la clé peut être reçue.
R(config-keychain-key)# exit	
R(config-keychain)# key 2	Identification de la clé N°2
R(config-keychain-key)# key-string password_B	Définition du mot de passe, suite de caractères alphanumériques (de 1 à 80) excepté le premier caractère qui ne peut pas être un caractère numérique.
# accept-lifetime 13:30:00 jan 25 2000 duration 7200	Durée pendant laquelle la clé peut être reçue.
# send-lifetime 14:00:00 jan 25 2000 duration 3600	Durée pendant laquelle la clé peut être émise.
R(config-keychain-key)# exit	
R(config-keychain)# key 3	Identification de la clé N°3
R(config-keychain-key)# key-string password_C	Définition du mot de passe
# accept-lifetime 14:30:00 jan 25 2000 duration 7200	Durée pendant laquelle la clé peut être reçue.
# send-lifetime 15:00:00 jan 25 2000 duration 3600	Durée pendant laquelle la clé peut être émise.
R(config-keychain-key)# exit	
R(config-keychain)# exit	
R(config)# interface eth 0	
# ip add 192.168.0.1 255.255.255.0	
# ip rip authentication key-chain gefi	
# ip rip authentication mode md5	

- ❑ Attention : Veuillez à initialiser l'heure et la date sur les routeurs si vous utilisez les commandes 'accept-lifetime' et 'send-lifetime'. La meilleure solution pour la synchronisation des horloges est la mise en oeuvre d'un serveur NTP.

```

Albil#clock ?
  set  Set the time and date

Albil#clock set ?
  hh:mm:ss  Current Time

Albil#clock set 17:21:00 ?
  <1-31>  Day of the month
  MONTH  Month of the year

Albil#clock set 17:21:00 1 april 2004
Albil#clock set 17:21:00 1 april ?
  <1993-2035>  Year

Albil#clock set 17:21:00 1 april 2004
Albil#show clock
17:21:17.511 cet Thu Apr 1 2004
Albil#

```

VI.E Vérification

VI.E.1 Configuration RIP

- ❑ Cette commande affiche la valeur les temporisateurs et les informations réseau du routeur.

```
Albi2>show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 10 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface        Send  Recv  Key-chain
    Ethernet0        1     1 2
    Serial0           1     1 2
    Serial1          1     1 2
  Routing for Networks:
    192.168.16.0
    192.168.17.0
    192.168.19.0
  Routing Information Sources:
    Gateway         Distance   Last Update
    192.168.16.1     120       00:00:12
    192.168.17.2     120       00:00:13
  Distance: (default is 120)

Albi2>
```

VI.E.2 Visualisation des routes RIP

```
Albi2>show ip route rip
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 not set

R    192.168.20.0/24 [120/1] via 192.168.17.2, 00:00:07, Serial0
R    192.168.36.0/24 [120/3] via 192.168.16.1, 00:00:07, Serial1
R    192.168.34.0/24 [120/2] via 192.168.16.1, 00:00:07, Serial1
R    192.168.1.0/24 [120/1] via 192.168.16.1, 00:00:07, Serial1
R    192.168.18.0/24 [120/1] via 192.168.16.1, 00:00:07, Serial1
                                     [120/1] via 192.168.17.2, 00:00:07, Serial0
R    192.168.3.0/24 [120/1] via 192.168.16.1, 00:00:07, Serial1
Albi2>
```

VI.E.3 Table de routage

- ❑ Attention : Lorsqu'un routeur perd le link sur l'une de ses interfaces, l'IOS supprimera toutes les routes ayant comme '*Next Hop Gateway*' la route directement connectée à cette interface.

Les champs de sortie de la commande 'show ip route'	
Sortie	Description
C, S ou R	Identifie l'origine de la route : <ul style="list-style-type: none"> ○ 'C' : route directement connectée ○ 'S' : route statique ○ 'R' : route dynamique acquise par RIP
192.168.20.0/24	Indique le réseau cible, adresse IP avec son 'Subnet Mask'.
[120/1]	Distance administrative de la source de l'information; puis la métrique associée à la route.
via 192.168.17.2	Le ' <i>Next Hop Gateway</i> ' : adresse IP du prochain saut permettant d'atteindre le réseau cible.
00:00:07	Indique le temps écoulé depuis la dernière mise à jour de la route, au format ' <i>heures:minutes:secondes</i> '.
Serial0	Indique l'interface à travers laquelle le réseau cible peut être atteint.

- ❑ Cette commande affiche la table de routage du routeur Albi2 (voir Annexe A.I Maquette sans VLSM page 259)

```

Albi2>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, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

R    192.168.20.0/24 [120/1] via 192.168.17.2, 00:00:07, Serial0
R    192.168.36.0/24 [120/3] via 192.168.16.1, 00:00:07, Serial1
R    192.168.34.0/24 [120/2] via 192.168.16.1, 00:00:07, Serial1
C    192.168.17.0/24 is directly connected, Serial0
C    192.168.16.0/24 is directly connected, Serial1
R    192.168.1.0/24 [120/1] via 192.168.16.1, 00:00:07, Serial1
C    192.168.19.0/24 is directly connected, Ethernet0
R    192.168.18.0/24 [120/1] via 192.168.16.1, 00:00:07, Serial1
R    192.168.18.0/24 [120/1] via 192.168.17.2, 00:00:07, Serial0
R    192.168.3.0/24 [120/1] via 192.168.16.1, 00:00:07, Serial1
Albi2>

```

- ❑ Cette ligne indique qu'il faut passer trois routeurs (HOP) pour atteindre le réseau 192.168.36.0/24 avec une distance administrative de 120 (RIP).

```
R 192.168.36.0/24 [120/3] via 192.168.16.1, 00:00:07, Serial1
```

- 'R' : code indiquant l'origine de la route, ici R ⇒ RIP.
 - '192.168.36.0/24' : champ indiquant le réseau destination : adresse réseau IP et son Subnet Mask
 - '[120/3]' : Distance administrative / métrique.
 - Ici la distance administrative vaut '120' pour RIP
 - Avec un métrique de 3, signifiant la traversée de trois routeurs pour atteindre le réseau 12.168.36.0/24.
 - '192.168.16.1' : le Next-Hop Gateway
-
- ❑ Cette ligne indique deux routes pour atteindre le réseau 192.168.18.0/24.

```
R 192.168.18.0/24 [120/1] via 192.168.16.1, 00:00:07, Serial1  
[120/1] via 192.168.17.2, 00:00:07, Serial0
```

- ❑ Cette ligne indique qu'aucune 'Default Gateway' n'est configurée pour le Mini IOS

```
Gateway of last resort is not set
```

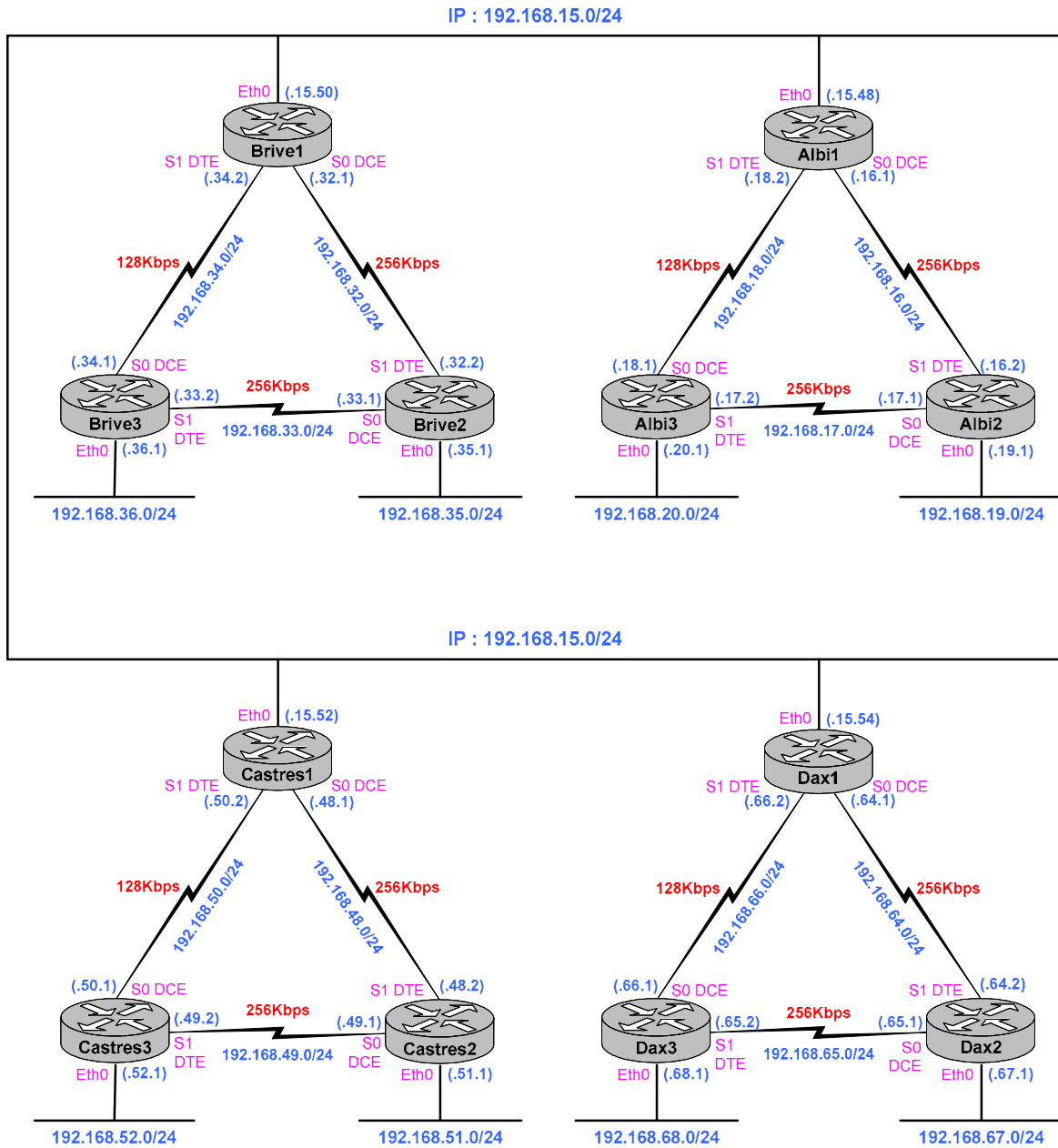
VI.E.4 Les mises à jour

- ✓ Cette commande affiche les mises à jour RIP reçues et émises
- ✓ #Term monitor & #Debug ip rip

```
Albi2#debug ip rip
RIP protocol debugging is on
Albi2#
00:29:18: RIP: sending v1 update to 255.255.255.255 via Ethernet0 (192.168.19.1)
00:29:18:     network 192.168.20.0, metric 2
00:29:18:     network 192.168.36.0, metric 4
00:29:18:     network 192.168.34.0, metric 3
00:29:18:     network 192.168.17.0, metric 1
00:29:18:     network 192.168.16.0, metric 1
00:29:18:     network 192.168.1.0, metric 2
00:29:18:     network 192.168.18.0, metric 2
00:29:18:     network 192.168.3.0, metric 2
00:29:18: RIP: sending v1 update to 255.255.255.255 via Serial0 (192.168.17.1)
00:29:18:     network 192.168.36.0, metric 4
00:29:18:     network 192.168.34.0, metric 3
00:29:18:     network 192.168.16.0, metric 1
00:29:18:     network 192.168.1.0, metric 2
00:29:18:     network 192.168.19.0, metric 1
00:29:18:     network 192.168.3.0, metric 2
00:29:18: RIP: sending v1 update to 255.255.255.255 via Serial1 (192.168.16.2)
00:29:18:     network 192.168.20.0, metric 2
00:29:18:     network 192.168.17.0, metric 1
00:29:18:     network 192.168.19.0, metric 1
00:29:24: RIP: received v1 update from 192.168.16.1 on Serial1
00:29:24:     192.168.20.0 in 2 hops
00:29:24:     192.168.36.0 in 3 hops
00:29:24:     192.168.34.0 in 2 hops
00:29:24:     192.168.1.0 in 1 hops
00:29:24:     192.168.18.0 in 1 hops
00:29:24:     192.168.3.0 in 1 hops
00:29:29: RIP: received v1 update from 192.168.17.2 on Serial0
00:29:29:     192.168.20.0 in 1 hops
00:29:29:     192.168.36.0 in 4 hops
00:29:29:     192.168.34.0 in 3 hops
00:29:29:     192.168.1.0 in 2 hops
00:29:29:     192.168.18.0 in 1 hops
00:29:29:     192.168.3.0 in 2 hops
Albi2#und a1
```

VI.F Exercice #1

- Configurez les routeurs pour réaliser un routage RIPv2.
 - Dans un plan d'adressage IP sans VLSM,

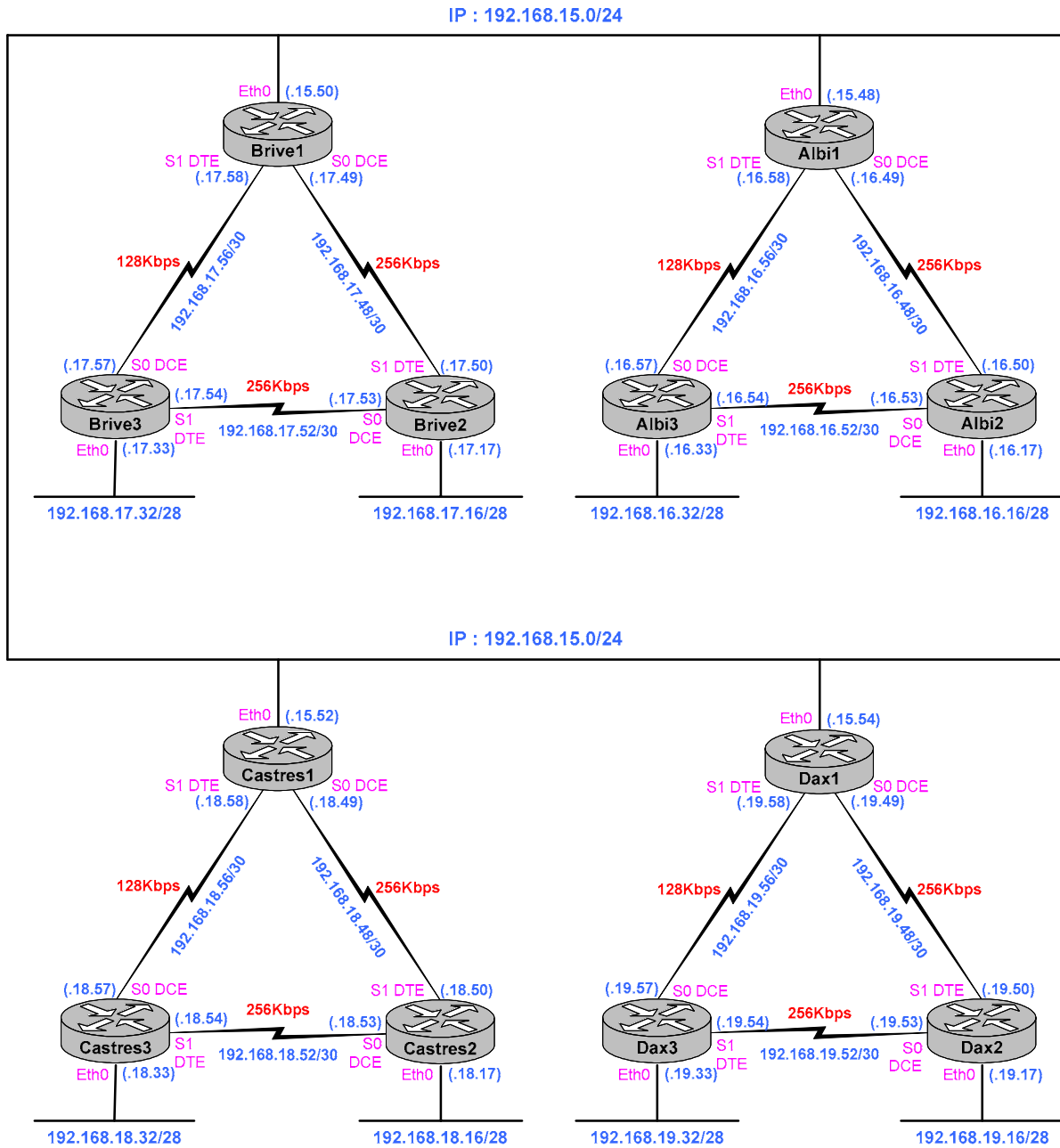


- ❑ Attention : les zones en grisées indiquent des données variables en fonction des routeurs.

Configuration Type des Routeurs	
Albi1	Albi2
<pre> conf t ! hostname Albi1 ip domain-name gefi.home ip name-server 192.168.15.9 ntp server 192.168.15.9 ! interface ethernet 0 ip address 192.168.15.48 255.255.255.0 bandwidth 10000 no shutdown exit ! interface serial 0 description Vers Albi2 ip address 192.168.16.1 255.255.255.0 clock rate 250000 bandwidth 250 no shutdown exit ! ! interface serial 1 description Vers Albi3 ip address 192.168.18.2 255.255.255.0 bandwidth 125 no shutdown exit ! no router rip router rip network 192.168.15.0 network 192.168.16.0 network 192.168.18.0 version 2 ! line console 0 escape-character 27 exec-timeout 0 0 logging synchronous login password gefi exit ! line aux 0 login password gefi exit ! line vty 0 4 escape-character 27 exec-timeout 0 0 logging synchronous login password gefi exit ! enable secret cisco ! end wr ! </pre>	<pre> conf t ! hostname Albi2 ip domain-name gefi.home ip name-server 192.168.15.9 ntp server 192.168.15.9 ! interface ethernet 0 ip address 192.168.19.1 255.255.255.0 bandwidth 10000 no shutdown exit ! interface serial 0 description Vers Albi3 ip address 192.168.65.1 255.255.255.0 clock rate 250000 bandwidth 250 no shutdown exit ! ! interface serial 1 description Vers Albi1 ip address 192.168.64.2 255.255.255.0 bandwidth 250 no shutdown exit ! no router rip router rip network 192.168.19.0 network 192.168.16.0 network 192.168.17.0 version 2 ! line console 0 escape-character 27 exec-timeout 0 0 logging synchronous login password gefi exit ! line aux 0 login password gefi exit ! line vty 0 4 escape-character 27 exec-timeout 0 0 logging synchronous login password gefi exit ! enable secret cisco ! end wr ! </pre>

VI.G Exercice #2

- Maintenant, configurez les routeurs pour réaliser un routage RIPv2.
 - Dans un plan d'adressage IP avec VLSM,



VI.H Exercice #3

- Quand le routage RIPv2 sera vérifié, Mise en œuvre du changement de métrique sur le Routeur1 et 2.

VI.I Exercice #4

- Enfin, après vérification des tables de routage en RIPv2, mettez en œuvre de l'authentification MD5 avec le mot de passe : gedev.

VII. IGRP

IGRP : Interior Gateway Routing Protocol

VII.A Présentation

- ❑ IGRP est un protocole de routage par vecteur de distance évolué, développé au milieu des années 1980 par CISCO.
- ❑ Le fonctionnement d'IGRP est proche de celui de RIP, cependant il existe quelques différences, la métrique utilisée par IGRP est plus sophistiquée, elle utilise un algorithme de calcul qui s'appuie sur les paramètres de Bande Passante et de Délai de l'interface via laquelle la mise à jour a été reçue. La valeur du métrique est plus significative. Les routes comportant plus de sauts mais plus rapides peuvent être considérées comme plus intéressantes.
- ❑ Les masques de sous réseau de longueur variable (**VLSM** : Variable-Length Subnet Mask) **ne peuvent pas être utilisés avec IGRP**.
- ❑ Le protocole IGRP est propriétaire Cisco, sauf cas particulier, il ne fonctionne pas sur les équipements des autres constructeurs.
- ❑ IGRP supplante RIP avantageusement avec une valeur maximale de 100 sauts par défaut, valeur qui peut être étendue par configuration jusqu'à 255 sauts.
- ❑ IGRP utilise une métrique composite (bande passante et délai) qui fournit une plus grande flexibilité que RIP.

Delay IGRP	
Bandwith	$\frac{10^7}{Bandwith_{Kbps}}$
125 Kbps	80.000
250 Kbps	40.000
500 Kbps	20.000
10 Mbps	1.000

VII.B Les temporisateurs

Les temporisateurs IGRP		
timers basic Update Invalid holdown flush		
Temporisateur	Par défaut	Signification
'Update' Intervalle de mise à jour	90s	Temps entre chaque mise à jour de routage. Ce temps peut être redéfini pour des réseaux ayant de débit important : Ethernet.
'Invalid' Intervalle d'invalidation	270s	Trois fois l'intervalle de mise à jour. Le temporisateur d'invalidation spécifie le temps d'attente du routeur avant de déclarer une route spécifique invalide en l'absence de messages de mise à jour pour cette route.
'holdown' Intervalle de retenue	280s	Trois fois l'intervalle de mise à jour plus 10 secondes. Le temporisateur de retenue spécifie l'intervalle pendant lequel le routeur doit retenir les changements concernant une route précédemment marquée comme invalide. Ce temporisateur doit être configuré de telle manière que les informations de routage aient le temps de se propager vers tous les routeurs, ce qui veut dire que la convergence dure au moins aussi longtemps. Le routeur place une route en retenue après l'avoir invalidée suite à une mise à jour l'annonçant comme inaccessible. Une telle route redevient valide à expiration du temporisateur ou bien lorsque le routeur reçoit une mise à jour annonçant une distance administrative inférieure. A noter également que lorsqu'une route est marquée comme invalide puis placée en retenue, elle continue à être utilisée pour router les datagrammes. Cette fonction évite simplement qu'elle ne soit mise à jour tant que la convergence n'est pas terminée.
'flush' Intervalle d'élimination	630	Sept fois l'intervalle de mise à jour. Le temporisateur d'élimination spécifie l'intervalle qui doit s'écouler avant qu'une route marquée comme invalide ne soit supprimée de la table de routage.

VII.C Calcul du métrique

- Les paramètres suivants entrent dans le calcul du métrique affecté à une liaison :
 - La **bande passante**. C'est le débit le plus faible rencontré sur le chemin. Ce paramètre peut prendre des valeurs reflétant des débits allant de 1200 bps à 10 G bps.
 - Le **delay**. Cumul des délais induits par les réseaux le long du chemin. Chaque type de média comporte un délai de propagation qui lui est associé. La modification de délai est très utile pour optimiser le routage (lien par satellites par exemple). Le retard peut être modifié avec la commande 'delay'. Le délai peut prendre une valeur de 1 à 2×10^{23} .
 - La **fiabilité**. La fiabilité est calculée dynamiquement sous la forme d'une moyenne pondérée continue toutes les 5 secondes. Cette valeur est représentée sur huit bits (de 0 à 255).
 - La **charge**. La charge est calculée dynamiquement sous la forme d'une moyenne pondérée continue toutes les 5 secondes. Cette valeur est représentée sur huit bits (de 0 à 255).
 - La formule de calcul standard de la métrique :

$$M_{IGRP} = \left[(k1 \times B_{IGRP}) + \left(\frac{k2 * B_{IGRP}}{256 - L} \right) + (k3 \times D_{IGRP}) \right]$$

- B_{IGRP} , codé BW, est le débit IGRP du chemin, calculé selon la formule : $B_{IGRP} = \frac{10^7}{B_{MIN}} \cdot B_{MIN}$
est le débit logique minimal du chemin exprimé en K bps. Ce paramètre statique est défini par la commande 'bandwidth kbps' en mode de configuration d'interface. Il faut noter cependant que cette valeur devient B_{MIN} pour un chemin spécifique, uniquement si ce débit logique est le minimum parmi ceux de tous les segments qui constituent ce chemin.
- D_{IGRP} , codé DLY, représente le délai (ou retard) du chemin qui est égal à la somme des délais de tous les segments qui le constituent. D_{IGRP} est exprimé en unités de 10 μ s, c'est-à-dire que la somme de tous les délais en microseconde est divisée par 10.
- L , codé load, est la charge de l'interface correspondante par un chiffre de 1 (minimum) à 255 (100%).

- Si $K5 \neq 0$, alors :

$$M_{IGRP} = \left[(k1 \times B_{IGRP}) + \left(\frac{k2 * B_{IGRP}}{256 - L} \right) + (k3 \times D_{IGRP}) \right] \times \frac{k5}{R + k4}$$

- R (*Reliability*), codé rely, le degré de fiabilité du segment auquel est relié l'interface, dont la valeur est exprimée dans la même fourchette que L .

- **Par défaut**, $K1=K3=1$ et $K2=K4=K5=0$, la formule devient donc :

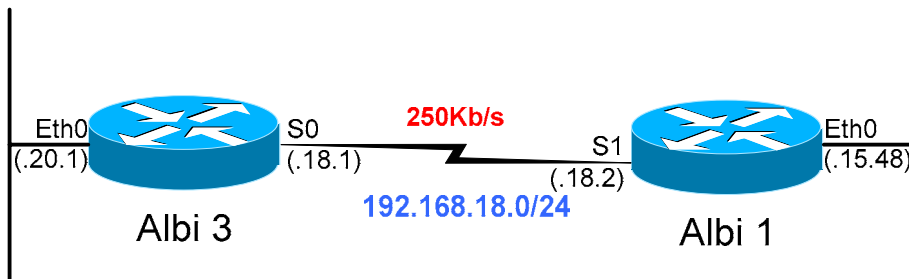
$$M_{IGRP} = \frac{10^7}{B_{MIN}} + \frac{\sum Delay_{\mu s}}{10}$$

VII.D Application : Calcul du métrique

- ❑ les paramètres ; ‘Bandwidth’, ‘Delay’, ‘Reliability’ et ‘Load’ sont donnés par la commande ‘show int’.
- ❑ Chaque incrément de retard représente 39,1 nanosecondes (39,1 10⁻⁹ x 25600 = 1 ms).
- ❑ Vous remarquerez que toutes les interfaces WAN ont le même retard.

1 ms

Valeurs de retard d’interface typiques			
Interface	Bande passante	Incrément	Retard
Ethernet	10 Mbps	25.600	1.000 µs
Série T1	1,544 Mbps	512.000	20.000 µs
Série DS0	64 Kbps	512.000	20.000 µs
Série DS0	56 Kbps	512.000	20.000 µs



- Calcul du métrique ‘Albi3’ vers le réseau 192.168.15.0/24. Ce calcul prend en compte le débit du lien WAN (250Kbps) et des retards apportés par une interface WAN (20.000) et d’une interface Ethernet (1.000) :

$$M_{IGRP} = \frac{10^7}{250 \cdot 10^3} + \frac{(20.000 + 1.000)}{10} = 40.000 + 2.100 = 42.100$$

```
Albi3#sh ip route igrp
I   192.168.15.0/24 [100/42100] via 192.168.18.2, 00:00:56, Serial0
I   192.168.16.0/24 [100/44000] via 192.168.17.1, 00:00:09, Serial1
                                   [100/44000] via 192.168.18.2, 00:00:56, Serial0
I   192.168.19.0/24 [100/42100] via 192.168.17.1, 00:00:09, Serial1
Albi3#sh ip route 192.168.15.48
Routing entry for 192.168.15.0/24

  Known via "igrp 1", distance 100, metric 42100
  Redistributing via igmp 1
  Advertised by igmp 1 (self originated)
  Last update from 192.168.18.2 on Serial0, 00:01:02 ago
  Routing Descriptor Blocks:
  * 192.168.18.2, from 192.168.18.2, 00:01:02 ago, via Serial0
    Route metric is 42100, traffic share count is 1
    Total delay is 21000 microseconds, minimum bandwidth is 250 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 0

Albi3#
```

VII.E Configuration

- ❑ Il convient dans un premier temps de définir un protocole IGRP en lui donnant un numéro d' «autonomous system».

<code>routeur IGRP id_SA</code>	'ID_SA' est le numéro d'autonomous system
---------------------------------	---

- ❑ Le routeur passe en mode configuration IGRP, on doit ensuite définir les réseaux participant à la négociation du routage avec la commande `network` :

<code>network A.B.C.D</code>	'A.B.C.D' : l'adresse du réseau participant à la négociation du routage.
------------------------------	--

- ❑ Ces deux commandes suffisent à initialiser le processus IGRP, cependant l'algorithme de calcul du métrique IGRP utilise la valeur de la bande passante.

- ❑ Sur un routeur Cisco la valeur par défaut de la bande passante d'une interface série est 1 536 Kbps soit la bande passante d'un accès T1 (accès primaire US). Cette valeur n'est jamais valable en France. La commande `bandwidth` permet d'indiquer la bande passante d'une interface mais pas de la définir. C'est une sous commande d'interface.

<code>bandwidth kbps</code>	'kbps' : la bande passante en Kbps
-----------------------------	------------------------------------

- ❑ Il n'est pas utile de diffuser les trames de mise à jour IGRP au niveau de certaines interfaces, par exemple si aucun autre routeur n'est connecté au réseau d'une interface.

- ❑ La commande, de configuration IGRP, `passive interface` permet d'interdire la diffusion des trames IGRP sur une interface.

<code>passive interface type numéro</code>	'Type' : le type d'interface, serial, Ethernet, token ... 'Numéro' : le numéro d'interface (0, 0/2...).
--	--

- ❑ Lorsque vous souhaitez diffuser les annonces IGRP sur un réseau NBMA, la commande `'neighbor'` permet de spécifier l'adresse IP d'un routeur voisin.

<code>neighbor add-IP</code>	
------------------------------	--

Lecture conseillée :

http://www.cisco.com/pcqi-bin/Support/PSP/psp_view.pl?p=Internetworking:IGRP

Configuration IGRP	
Commandes	Commentaires
Router# configure terminal Router(config)# router igrp 1 Router(config-router)#	Initialisation de IGRP avec comme identifiant d'AS '1'
Router(config-router)# network 192.168.3.0	Définition du réseau du réseau participant à la négociation du routage.
Router(config-router)# no network 192.168.3.0	Supprime le réseau spécifié
Router(config-router)# passive-interface ethernet 0	Suppression des annonces IGRP sur ce réseau, si aucun routeur n'existe sur celui-ci.
Router(config-router)# neighbor 192.168.1.1	Lorsque vous souhaitez diffusez les annonces IGRP sur un réseau NBMA, la commande 'neighbor' permet de spécifier l'adresse IP d'un routeur voisin.
Router(config-router)# metric weights tos k1 k2 k3 k4 k5	Commande de configuration des constantes IGRP : <ul style="list-style-type: none"> o 'tos' par défaut toujours à '0', o 'k1'='k3'=1, o 'k2'='k4'='k5'=0.
Router(config-if)# bandwidth 64	la bande passante (en K bps) de l'interface. Configurez le même bandwidth sur les interfaces en vis-à-vis.
Router# configure terminal Router(config)# no router igrp 1	Arrêt d'IGRP

VII.F Résultat

```

Castres2#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 not set

I    192.168.15.0/24 [100/42100] via 192.168.48.1, 00:00:11, Serial1
I    192.168.64.0/24 [100/44100] via 192.168.48.1, 00:00:11, Serial1
I    192.168.65.0/24 [100/46100] via 192.168.48.1, 00:00:11, Serial1
I    192.168.66.0/24 [100/84100] via 192.168.48.1, 00:00:11, Serial1
I    192.168.67.0/24 [100/44200] via 192.168.48.1, 00:00:11, Serial1
I    192.168.52.0/24 [100/42100] via 192.168.49.2, 00:01:14, Serial0
C    192.168.51.0/24 is directly connected, Ethernet0
I    192.168.68.0/24 [100/46200] via 192.168.48.1, 00:00:12, Serial1
I    192.168.50.0/24 [100/84000] via 192.168.49.2, 00:01:14, Serial0
                   [100/84000] via 192.168.48.1, 00:00:12, Serial1
C    192.168.49.0/24 is directly connected, Serial0
C    192.168.48.0/24 is directly connected, Serial1
Castres2#

```

```

Dax2#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 not set

I    192.168.15.0/24 [100/42100] via 192.168.64.1, 00:01:02, Serial1
C    192.168.64.0/24 is directly connected, Serial1
C    192.168.65.0/24 is directly connected, Serial0
I    192.168.66.0/24 [100/84000] via 192.168.64.1, 00:01:03, Serial1
                   [100/84000] via 192.168.65.2, 00:00:35, Serial0
C    192.168.67.0/24 is directly connected, Ethernet0
I    192.168.52.0/24 [100/46200] via 192.168.64.1, 00:01:03, Serial1
I    192.168.51.0/24 [100/44200] via 192.168.64.1, 00:01:03, Serial1
I    192.168.68.0/24 [100/42100] via 192.168.65.2, 00:00:35, Serial0
I    192.168.50.0/24 [100/84100] via 192.168.64.1, 00:01:04, Serial1
I    192.168.49.0/24 [100/46100] via 192.168.64.1, 00:01:04, Serial1
I    192.168.48.0/24 [100/44100] via 192.168.64.1, 00:01:04, Serial1
Dax2#

```

VII.G L'équilibrage et le partage de charge

- ❑ IGRP permet l'équilibrage et le partage de charge.
- ❑ La commande de configuration 'variance' permet le partage du trafic, proportionnellement au métrique des routes, en définissant la différence acceptable entre la meilleure métrique et la moins bonne.
 - Les valeurs acceptables sont des entiers positifs non nuls.
 - La valeur de variance par défaut est 1, ce qui indique un équilibrage de charge pour des routes à coûts égaux.

```
Router(config-router) # variance multiplicateur
```

- ❑ On peut utiliser la commande 'traffic-share {balanced|min}' pour contrôler la façon donc le trafic est distribué entre les différentes routes du partage de charge.
 - L'option 'balanced' précise que le trafic doit être distribué proportionnellement au poids des métriques.
 - L'option 'min' impose l'utilisation des routes de coût minimal.

```
Router(config-router) # traffic-share {balanced | min}
```

- ❑ Les commandes 'variance' et 'traffic-share' sont spécifiques aux protocoles IGRP et EIGRP.

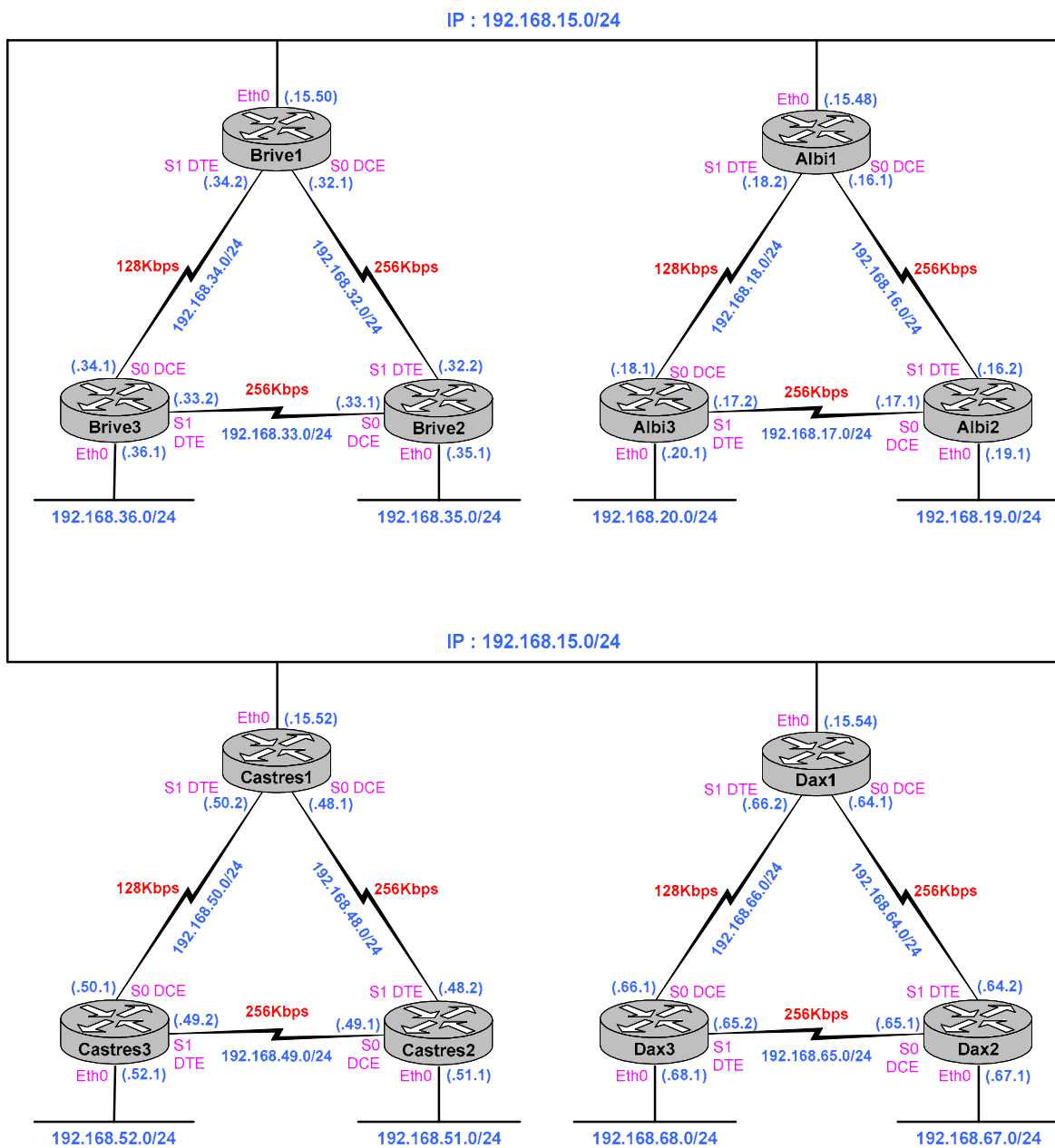
VII.H Debug

Commandes	Commentaires
Router# debug ip igrp transaction [Add-IP]	
Router# debug ip igrp events [Add-IP]	Cette commande affiche les résumés d'information de routage IGRP. Si l'adresse d'un voisin est précisée, l'affichage ne contiendra que les informations de mise à jour en provenance de ce voisin, ainsi que celles que le routeur lui destine.

VII.I Exercice

- ❑ Configurez les routeurs pour réaliser un routage IGRP.
 - Dans un plan d’adressage IP sans VLSM,
 - Sans agrégation de routes et
 - Sachant que tous les routeurs font partie de l’AS 1.

- ❑ Après la configuration des routeurs ;
 - Vérifiez le métrique dans les tables de routage.
 - Puis, désactivez le lien entre les routeurs 2 et 3 pour observer l’évolution des métriques à partir de ‘Router3’.



VIII. EIGRP

EIGRP : Enhanced Interior Gateway Routing Protocol

VIII.A Présentation

- ❑ Le protocole EIGRP est le protocole de routage dynamique propriétaire de Cisco. Il utilise la même métrique qu'IGRP, mais il applique l'algorithme DUAL (*Diffusing Update Algorithm*) pour améliorer la convergence. Cet algorithme a été conçu par SRI International, sous la direction de J.J. Garcia, dans la perspective de réaliser un protocole de routage ayant une convergence assez rapide pour garantir un réseau sans boucle de routage.
- ❑ Le mode de calcul des métriques IGRP et EIGRP sont identiques.
- ❑ Chaque routeur EIGRP mémorise les tables de routage de ses voisins, un routeur peut ainsi emprunter, s'il existe, un nouveau chemin vers un réseau donné. S'il n'en existe pas le routeur devient actif pour cette destination et envoie une requête vers chacun de ses voisins, demandant une autre route possible vers la destination. Ces requêtes se propagent jusqu'à ce qu'un autre chemin soit trouvé.
- ❑ Un routeur EIGRP reçoit une table de routage complète de ses voisins, seulement la première fois qu'il communique avec eux.

- Par défaut, la métrique EIGRP (comme IGRP) est une somme pondérée de l'inverse de la bande passante du lien ayant le débit le plus faible plus le cumul des délais des segments traversés.

$$\circ \quad M_{IGRP} = \frac{10^7}{B_{MIN}} + \frac{\sum Delay_{ms}}{10}$$

- la métrique calculée par EIGRP est basée sur la même formule que celle de IGRP, avec une multiplication du résultat par 256, ce qui donne :

$$\circ \quad M_{EIGRP} = M_{IGRP} \times 256$$

VIII.B Configuration

- La configuration d'EIGRP est identique à celle d'IGRP.

Commandes	Commentaires
Router# configure terminal Router(config)# router eigrp 1 Router(config-router)#	Initialisation de EIGRP avec comme identifiant d'AS '1'
Router(config-router)# network 192.168.3.0	Définition du réseau du réseau participant à la négociation du routage.
Router(config-router)# network all	Sert à configurer EIGRP pour tous les réseaux d'un routeur.
Router(config-router)# no network 192.168.3.0	Supprime le réseau spécifié de la gestion d'EIGRP.
Router(config-router)# passive-interface ethernet 0	Suppression des annonces IGRP sur ce réseau, si aucun routeur n'existe sur celui-ci.
Router(config-router)# neighbor 192.168.1.1	Lorsque vous souhaitez diffusez les annonces IGRP sur un réseau NBMA, la commande 'neighbor' permet de spécifier l'adresse IP d'un routeur voisin.
Router(config-if)# bandwidth 64	la bande passante (en K bps) de l'interface. Configurez le même bandwidth sur les interfaces en vis-à-vis.
Router(config-router)# no auto-summary	Evite l'agrégation de routes. <ul style="list-style-type: none"> ○ Lors du déploiement ○ Si le plan d'adressage IP n'est pas cohérent.
Router# configure terminal Router(config)# no router eigrp	Arrêt d'EIGRP

Commandes de test	Commentaires
show ip eigrp neighbors	Pour consulter la table des voisins du routeurs
show ip eigrp topology	
show ip eigrp route	

Exemple de configuration d'un routeur EIGRP :

<pre> ! version 12.0 service password-encryption ! hostname Brive3 ! enable secret 5 \$1\$lSz4\$RM0B2k.7CAtNRbV ! ip subnet-zero ! interface Ethernet0 description Reseau Ethernet ip address 192.168.36.1 255.255.255.0 no ip directed-broadcast ! interface Serial0 description LS vers Brive 1 bandwidth 128 ip address 192.168.34.1 255.255.255.0 no ip directed-broadcast clockrate 2000000 ! interface Serial1 description LS vers Brive 2 bandwidth 128 ip address 192.168.33.2 255.255.255.0 no ip directed-broadcast ! </pre>	<pre> router eigrp 1 network 192.168.33.0 network 192.168.34.0 network 192.168.36.0 no auto-summary ! ip classless ! ! line con 0 password 7 1410170D05 transport input none line aux 0 password 7 094B4B0F10 line vty 0 4 password 7 06010A254958 login ! end </pre>
--	---

- ❑ A noter la commande 'no auto-summary' :
 - Par défaut le protocole de routage va essayer de regrouper les routes. Pour un fonctionnement correct de ce regroupement **le plan d'adressage IP doit être parfaitement adapté**. Comme c'est rarement le cas et afin de faciliter les évolutions, il est conseillé dans un premier temps lors de la configuration initiale ou lors des évolutions d'inhiber cette faculté.

Lecture conseillée :

http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:EIGRP

VIII.C Authentification

- Méthode similaire à RIP v2.

Commandes	Commentaires
R# conf t	
R(config)# key chain gefi	Création du groupe de clés (keychain) nommé 'gefi'
R(config-keychain)# key 1	Identification de la clé N°1. <ul style="list-style-type: none"> ○ L'intervalle de la clé est de 0 à 2147483647. ○ L'indentification des clés doit être consécutive.
R(config-keychain-key)# key-string password_A	Définition du mot de passe, suite de caractères alphanumériques (de 1 à 80) excepté le premier caractère qui ne peut pas être un caractère numérique.
# accept-lifetime 00:00:00 jan 1 2004 infinite	Durée pendant laquelle la clé peut être reçue.
R(config-keychain-key)# exit	
R(config-keychain)# key 2	Identification de la clé N°2
R(config-keychain-key)# key-string password_B	Définition du mot de passe, suite de caractères alphanumériques (de 1 à 80) excepté le premier caractère qui ne peut pas être un caractère numérique.
# accept-lifetime 13:30:00 jan 25 2000 duration 7200	Durée pendant laquelle la clé peut être reçue.
# send-lifetime 14:00:00 jan 25 2000 duration 3600	Durée pendant laquelle la clé peut être émise.
R(config-keychain-key)# exit	
R(config-keychain)# key 3	Identification de la clé N°3
R(config-keychain-key)# key-string password_C	Définition du mot de passe
# accept-lifetime 14:30:00 jan 25 2000 duration 7200	Durée pendant laquelle la clé peut être reçue.
# send-lifetime 15:00:00 jan 25 2000 duration 3600	Durée pendant laquelle la clé peut être émise.
R(config-keychain-key)# exit	
R(config-keychain)# exit	
R(config)# interface eth 0	
# ip add 192.168.0.1 255.255.255.0	
# ip authentication mode eigrp 1 md5	
# ip authentication key-chain eigrp 1 gefi	
#	

VIII.D Résultat

- Table de routage EIGRP avec VLSM

```

Castres2#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 not set

D    192.168.15.0/24 [90/10777600] via 192.168.18.49, 00:07:44, Serial1
D    192.168.19.0/24 [90/11289600] via 192.168.18.49, 00:07:44, Serial1
     192.168.18.0/24 is variably subnetted, 5 subnets, 2 masks
D    192.168.18.56/30 [90/21504000] via 192.168.18.49, 00:04:17, Serial1
     [90/21504000] via 192.168.18.54, 00:04:17, Serial0
C    192.168.18.48/30 is directly connected, Serial1
C    192.168.18.52/30 is directly connected, Serial0
D    192.168.18.32/28 [90/10777600] via 192.168.18.54, 00:04:17, Serial0
C    192.168.18.16/28 is directly connected, Ethernet0
Castres2#

```

```

Dax2#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

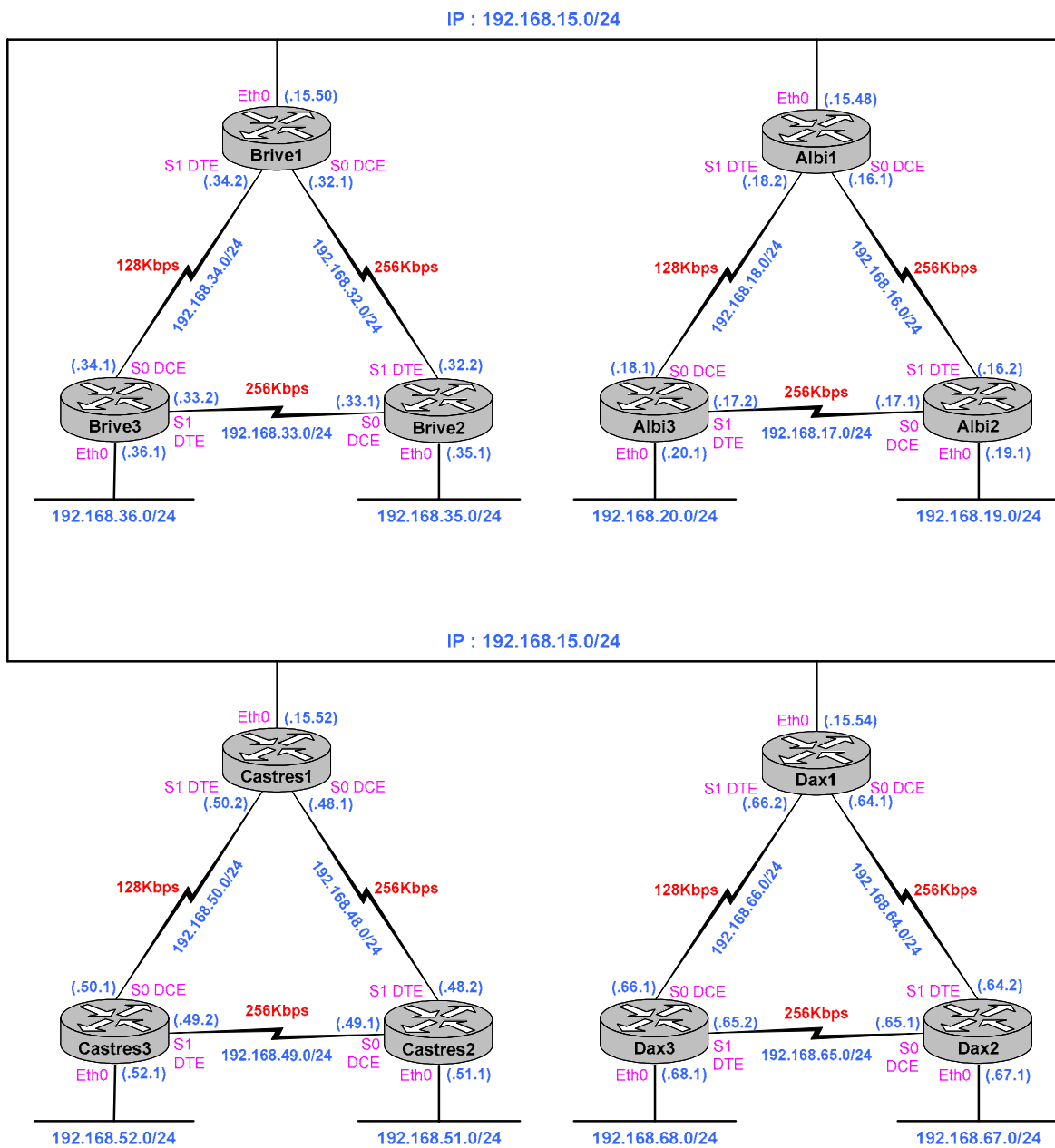
Gateway of last resort is not set

D    192.168.15.0/24 [90/10777600] via 192.168.19.49, 00:13:06, Serial1
     192.168.19.0/24 is variably subnetted, 5 subnets, 2 masks
D    192.168.19.56/30 [90/21504000] via 192.168.19.49, 00:13:08, Serial1
     [90/21504000] via 192.168.19.54, 00:13:08, Serial0
C    192.168.19.48/30 is directly connected, Serial1
C    192.168.19.52/30 is directly connected, Serial0
D    192.168.19.32/28 [90/10777600] via 192.168.19.54, 00:13:08, Serial0
C    192.168.19.16/28 is directly connected, Ethernet0
D    192.168.18.0/24 [90/11289600] via 192.168.19.49, 00:13:06, Serial1
Dax2#

```

VIII.E Exercice

- Configurez les routeurs pour réaliser un routage EIGRP.
 - Dans un plan d’adressage IP sans VLSM,
 - Sans agrégation de routes et
 - Sachant que tous les routeurs font partie de l’AS 1.



VIII.F Correction

- Les configurations des routeurs « AlbiX », « CastresX » et « DaxX » sera proche de celles des routeurs « BriveX » données en exemple, attention au plan d'adressage.

Configuration du routeur Brive 1	
<pre>! version 11.3 no service password-encryption ! hostname Brive1 enable secret 5 \$1\$lSz4\$RM0B2k.7CAtnRbVC ! ! interface Ethernet0 description Reseau Ethernet ip address 192.168.3.3 255.255.255.0 ! interface Serial0 description LS vers Brive 2 ip address 192.168.32.1 255.255.255.0 bandwidth 256 clockrate 2000000 ! interface Serial1 description LS vers Brive 3 ip address 192.168.34.2 255.255.255.0 bandwidth 128 !</pre>	<pre>! router eigrp 1 network 192.168.3.0 network 192.168.32.0 network 192.168.34.0 no auto-summary ! ip classless ! line con 0 password gefi line aux 0 password gefi line vty 0 4 password gedev login !</pre>

Configuration du routeur Brive 2	
<pre>! version 11.3 service password-encryption ! hostname Brive2 enable secret 5 \$1\$lSz4\$RM0B2k.7CAtnRbVC ! interface Ethernet0 description Reseau Ethernet ip address 192.168.35.1 255.255.255.0 ! interface Serial0 description LS vers Brive 3 ip address 192.168.33.1 255.255.255.0 bandwidth 128 clockrate 2000000 !</pre>	<pre>interface Serial1 description LS vers Brive 1 ip address 192.168.32.2 255.255.255.0 bandwidth 64 ! router eigrp 1 network 192.168.32.0 network 192.168.33.0 network 192.168.35.0 no auto-summary ! ip classless ! line con 0 password 7 06010A2745 line aux 0 password 7 1410170D05 line vty 0 4 password 7 045C0E020A37 login ! end</pre>

Configuration du routeur Brive 3

```
!
version 12.0
service password-encryption
!
hostname Brive3
!
enable secret 5 $l$lSz4$RM0B2k.7CAtNRbV
!
ip subnet-zero
!
interface Ethernet0
description Reseau Ethernet
ip address 192.168.36.1 255.255.255.0
no ip directed-broadcast
!
interface Serial0
description LS vers Brive 1
bandwidth 128
ip address 192.168.34.1 255.255.255.0
no ip directed-broadcast
clockrate 2000000
!
interface Serial1
description LS vers Brive 2
bandwidth 128
ip address 192.168.33.2 255.255.255.0
no ip directed-broadcast
!
router eigrp 1
network 192.168.33.0
network 192.168.34.0
network 192.168.36.0
no auto-summary
!
ip classless
!
!
line con 0
password 7 1410170D05
transport input none
line aux 0
password 7 094B4B0F10
line vty 0 4
password 7 06010A254958
login
!
end
```

VIII.G Commandes de dépannage

- ❑ La commande 'show ip route' permet de voir la table de routage :

```
Brive3#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 192.168.33.1 to network 0.0.0.0

C    192.168.36.0/24 is directly connected, Ethernet0
D    192.168.34.0/24 [90/41536000] via 192.168.33.1, 00:20:15, Serial1
D    192.168.35.0/24 [90/40537600] via 192.168.33.1, 00:20:43, Serial1
D    192.168.32.0/24 [90/41024000] via 192.168.33.1, 00:20:43, Serial1
D    192.168.3.0/24 [90/41049600] via 192.168.33.1, 00:20:15, Serial1
C    192.168.33.0/24 is directly connected, Serial1
Brive3#
```

- ❑ Vous pouvez modifier la valeur de la bande passante des liens séries afin de voir la conséquence sur le métrique. Cette modification est à réaliser sur chaque extrémité.
- ❑ La commande show 'ip eigrp neighbors' permet de voir les voisins EIGRP d'un routeur.

```
Brivel#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                Interface    Hold Uptime    SRTT    RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
1   192.168.34.1            Se1         14 00:00:05    105   1140 0 30
0   192.168.32.2            Se0         13 00:28:09     75    570 0 69
Brivel#
```

- ❑ La commande 'show ip eigrp interface' permet de voir les caractéristiques EIGRP d'une interface.

```
Brive3#sh ip eigrp int
IP-EIGRP interfaces for process 1

Interface    Peers    Xmit Queue    Mean    Pacing Time    Multicast    Pending
              Un/Reliable  SRTT      Un/Reliable    Flow Timer   Routes
Et0          0         0/0          0         0/10           0            0
Se1          1         0/0          17        10/380         456          0
Se0          0         0/0          0         5/10           0            0
```

- ❑ L'option détail permet d'avoir le détail d'une interface EIGRP.

```

Brive3#sh ip eigrp int detail
IP-EIGRP interfaces for process 1
Interface      Peers    Xmit Queue  Mean   Pacing Time  Multicast   Pending
Et0            0        0/0         0      0/10         0           0
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 0/0
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
Sel           1        0/0         17    10/380        456         0
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 28/29
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 1
  Retransmissions sent: 5  Out-of-sequence rcvd: 2
Se0           0        0/0         0      5/10         0           0
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 0/0
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
Brive3#

```

- ❑ Et bien sur les commandes classiques ping et traceroute en mode normal et étendu, les commandes show interfaces, show protocoles.

IX. OSPF

OSPF: Open Shortest Path First

- ❑ Le développement d'OSPF a commencé en 1997 en vue de remplacer le protocole RIP qui commençait à présenter des limitations sur de nombreux réseaux.

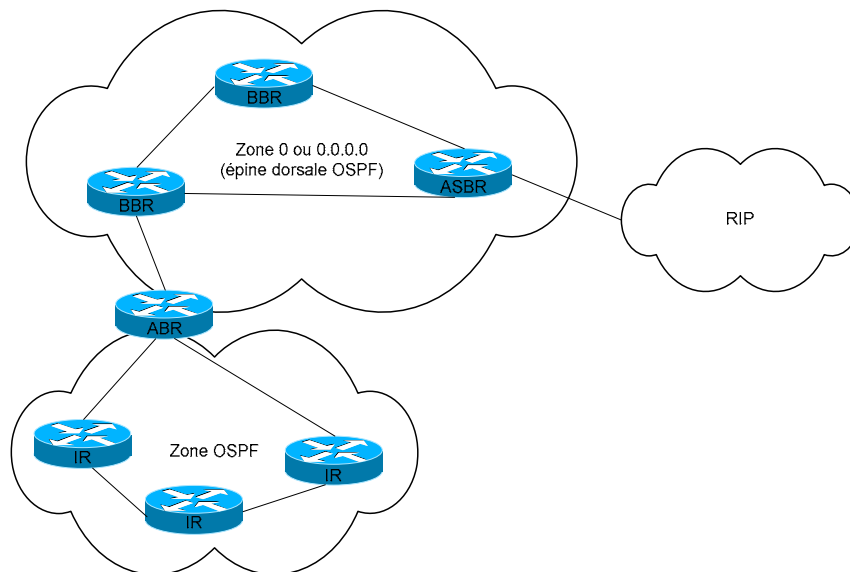
IX.A Présentation

- ❑ OSPF est un protocole de routage à état de liens, encapsulé directement dans IP (89).
- ❑ RFC : 2178, 1587 et 1793.
- ❑ La version la plus récente est OSPF Version 2, elle est décrite dans la RFC 2328.
- ❑ OSPF ne diffuse les informations de routage qu'entre les routeurs d'un même système autonome (AS, *Autonomous System*).
- ❑ OSPF supporte les VLSM (*Variable Length Subnet Masks*).
- ❑ OSPF sera utilisé de préférence pour les réseaux de grande taille, plus de 50 routeurs.
- ❑ Le réseau sera divisé en zones OSPF (OSPF AREA).
- ❑ Un routeur comportant plusieurs interfaces peut faire partie de plusieurs zones OSPF, on dira qu'il est routeur inter zone. C'est lui qui assure la liaison entre deux ou plusieurs zones OSPF.
- ❑ Une adresse de zone (par exemple area 0.0.0.1) est affectée par le NIC à chaque zone OSPF de l'Internet. Pour un réseau privé, l'administrateur peut définir son propre adressage de zone.
- ❑ Chaque zone OSPF doit être reliée soit directement soit par un lien virtuel à la zone principale (AREA 0).
- ❑ On limitera à 50 le nombre de routeurs dans une même area OSPF, si l'état des liens est instable, on diminuera la taille de la zone. On limitera également le nombre de voisins de chaque routeur à 60.
- ❑ OSPF utilise un algorithme de routage gourmand en ressources machine, si 'N' est le nombre de liens, le nombre de calculs à effectuer est $N \log N$. cependant ces calculs ne sont effectués que pour les liens dans une même zone OSPF (Area OSPF).
- ❑ Un routeur désigné (DR : *Designated Routeur*) et son backup (BDR : *Backup Designated Router*) sont élus par les routeurs d'un même segment réseau pour les représenter. Seul le DR assure les mises à jour du routage.
- ❑ L'algorithme Dijkstra (également appelé algorithme de plus court chemin ou SPF : *Shortest Path First*) est utilisé pour calculer la route à moindre coût. L'algorithme Bellman-Ford est utilisé pour calculer la route à moindre nombre de sauts.
- ❑ Le calcul de la route à moindre coût est basé sur la bande passante des liaisons.
- ❑ Le coût d'une interface : $C_{OSPF} = \frac{10^8}{Bandwidth}$, 'bandwidth' est exprimé en bits par secondes (bps).
Attention, le *bandwidth* est déclarée par la commande '*bandwidth Kbps*' dans le menu de configuration de l'interface.

IX.B Fonctionnement

IX.B.1 Catégories de routeurs

- Un système autonome OSPF est constitué de plusieurs types de routeurs OSPF.
 - **Routeur interne** ou **IR** (*Internal Router*). Routeur dont tous les réseaux directement connectés appartiennent à la même zone.
 - **Routeur interzone** ou **ABR** (*Area Border Router*). Routeur relié à plusieurs zones, incluant la zone 0 (épine dorsale). Ces routeurs peuvent aussi assurer la synthèse de routes des zones auxquelles ils sont reliés vers l'épine dorsale.
 - **Routeur d'épine dorsale** ou **BBR** (*Backbone Router*). Routeur possédant une interface avec l'épine dorsale.
 - **Routeur frontière de système autonome** ou **ASBR** (*Autonomous System Border Router*). Routeur qui échange des informations de routage avec des routeurs appartenant à d'autres systèmes autonomes. Ces routeurs peuvent aussi être configurés pour assurer la synthèse de routes de leurs liens externes vers la zone 0.



- Un routeur OSPF peut appartenir à plusieurs types à la fois. Si un routeur connecte un backbone et une zone OSPF ainsi qu'un réseau non OSPF, il est alors ABR et ASBR.

IX.B.2 Les LSA

- ❑ Les routeurs OSPF s'échangent des informations de routage au moyen d'annonces d'état de lien ou LSA (*Link-State Advertisement*). Ces annonces sont toujours acquittées et marquées d'un numéro de séquence, assurant à la fois une convergence fiable et l'intégrité de la base d'états de lien OSPF.
- ❑ Si une annonce LSA n'est pas acquittée dans un temps prédéfini, sachant que le temporisateur par défaut est de 5 secondes, le routeur source retransmet l'information.

Nom de LSA	Type	Description
Annonce de liens de routeur	1	Contient des informations sur les liens d'un routeur émetteur vers ses voisins.
Annonce de liens de réseau	2	Contient une liste des routeurs connectés à un segment réseau. Envoyée par le routeur désigné DR (<i>Designated Router</i>) de la part de tous les routeurs sur un réseau multiaccès comme Ethernet.
Annonce de liens résumés	3 & 4	Décrit les réseaux accessibles en dehors d'une zone, mais appartenant néanmoins au système autonome. Les routes vers ces réseaux sont injectées dans une zone par un routeur interzone ABR. Le type 3 correspond aux annonces émises par les routeurs ABR et le type 4 à celles émises par les routeurs ASBR.
Annonce de liens externes	5	Décrit une route vers une destination dans un autre système autonome ou processus de routage séparé.
	6	MOSPF (<i>Multicast OSPF</i>)
	7	Pour les zones NSSA (<i>Not-So-Stubby Area</i>)
	8	La RFC 2370 introduit ce type pour permettre à OSPF de supporter dans le futur d'autres informations d'applications.

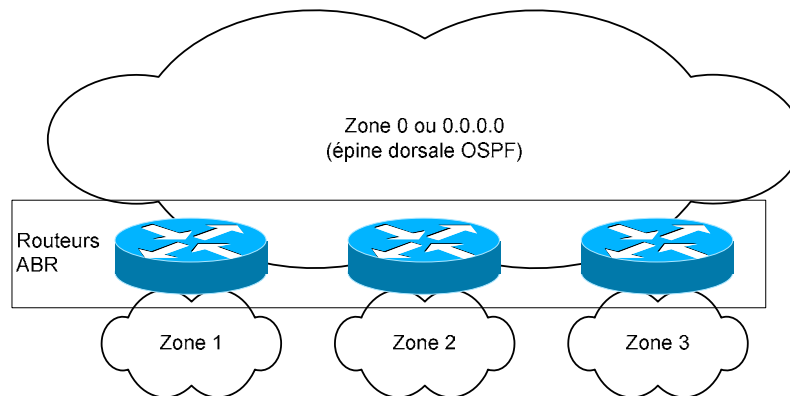
- ❑ Tous les routeurs OSPF d'une zone maintiennent la même base de données d'états de lien (LSDB : *Link-State Data Base*) contenant toutes les annonces LSA reçues.
- ❑ Lorsqu'un lien change d'état, les routeurs directement connectés envoient une annonce LSA au routeur désigné, s'il en existe un, qui transmet l'information aux autres routeurs de la zone.
- ❑ Lorsqu'un routeur reçoit une annonce LSA, il met à jour sa base de données d'états de lien puis exécute l'algorithme SPF pour recalculer les routes de sa table de routage. Une fois la nouvelle table générée, il peut l'utiliser.

IX.B.3 Routeur désigné

- ❑ Un réseau OSPF **multiaccès** (comme Ethernet) comprend un **routeur désigné** ou DR (*Designated Router*) ainsi qu'un routeur de secours ou BDR (*Backup Designated Router*). Ces routeurs sont élus au moyen du protocole *Hello* émis toutes les 10 secondes par défaut.
- ❑ Le routeur DR est chargé, entre autres choses, de générer les annonces LSA pour le réseau multiaccès tout entier. Il permet de réduire le trafic ainsi que la taille de la base de données topologique.
- ❑ **Le routeur ayant la priorité OSPF la plus élevée pour un segment donné devient DR.** Le même processus a lieu pour le BDR.

IX.B.4 Nature hiérarchique

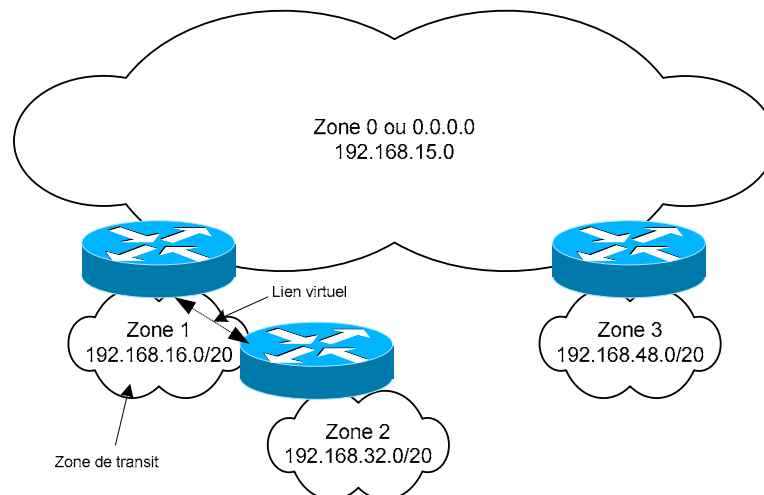
- OSPF est un protocole de routage par état de lien typique dans ce sens que les réseaux qui le supportent doivent être hiérarchiques.
 - L'épine dorsale représente la zone 0 (ou 0.0.0.0) et toutes les autres zones y sont reliées par l'intermédiaire de routeurs ABR. Tout le trafic interzone doit transiter par l'épine dorsale.
 - Un routage interzone a lieu lorsqu'un datagramme est destiné à un équipement situé dans une zone différente de celle dont il provient.



- Le concept de zones dans un réseau OSPF permet d'avoir des topologies de réseaux évolutives. L'utilisation de topologie de zones hiérarchiques OSPF répond aux problèmes d'évolutivité que nous avons rencontrés dans un seul grand réseau OSPF.
- Voici les avantages d'une topologie hiérarchique :
 - La charge CPU est réduite.
 - La table de routage est maintenue à une taille minimale.
 - La synthèse des routes réduit la charge LSU, ce qui préserve la bande passante.

IX.B.5 Les liens virtuels

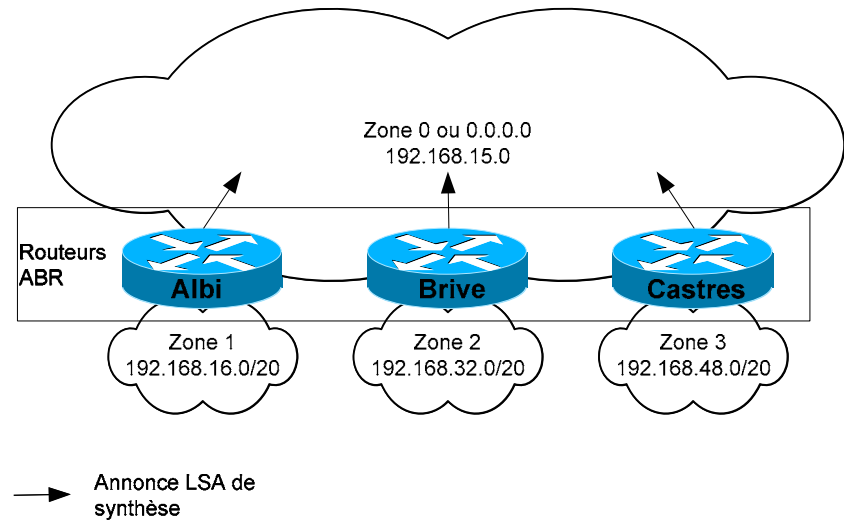
- ❑ Un lien virtuel (*virtual link*) est mis en œuvre pour relier une zone qui ne peut pas être directement connectée à l'épine dorsale par le routeur ABR le plus proche.
- ❑ Les liens virtuels fonctionnent comme des tunnels en maintenant la connectivité avec l'épine dorsale.
- ❑ L'acheminement du trafic sur un lien virtuel est plus lent que sur une liaison normale. Les liens virtuels impliquent aussi une plus grande complexité de conception et de configuration.



- ❑ De plus, ils ne sont pas bien supportés par certaines versions anciennes d'IOS qui requièrent une réinitialisation des routeurs.
- ❑ Éviter donc d'employer des liens virtuels à moins que cela soit absolument nécessaire. Par exemple, une interface de routeur ABR est en panne.

IX.B.6 Synthèse de routes

- ❑ pour obtenir des performances OSPF optimales, il faut assigner un bloc d'adresse IP contiguës à chaque zone OSPF de façon que chaque routeur ABR puisse les annoncer sous forme d'une route de synthèse.
- ❑ D'où la nécessité d'avoir un plan d'adressage IP soigné.



Commande d'agrégation de route OSPF	
<code>area id_area range A.B.C.D Mask</code>	
<code>area</code>	Depuis le menu de configuration du routage OSPF
<code>id_area</code>	l'adresse de la zone
<code>range</code>	Mot clé permettant d'agréger des routes
<code>A.B.C.D</code>	l'adresse du réseau
<code>Mask</code>	Le ' <i>Subnet Mask</i> '.
Exemple pour 'Albi'	
<code>routeur ospf 1</code>	
<code>area 0.0.0.1 range 192.168.16.0 255.255.240.0</code>	

IX.C Configuration

- ❑ La configuration d'OSPF est proche de ce que nous avons déjà vu pour les autres protocoles de routage dynamique. Cependant pour chaque réseau il est nécessaire d'indiquer le mask de sous réseau et la zone OSPF. A noter que le masque de sous réseau peut être saisi sous sa forme habituelle (par exemple 255.255.0.0) mais sera présenté sous la forme d'un wildcard mask (0.0.255.255). Lors de la configuration les deux formats sont autorisés.

Méthodologie :

- a) Il convient dans un premier temps de définir un protocole OSPF en lui donnant un numéro d' «*autonomous system*».

Commande de configuration du routage OSPF	
routeur OSPF <i>AS-id</i>	
routeur	Activation du routage dynamique, depuis le menu de configuration global.
OSPF	Ici OSPF
<i>AS-id</i>	' <i>AS-id</i> ' est le numéro d' autonomous system
Exemple	
routeur OSPF 1	

- b) Le routeur passe en mode configuration OSPF, on doit ensuite définir les réseaux participant à la négociation du routage avec la commande '*network*' :

Commande de configuration des réseaux OSPF	
network <i>A.B.C.D Mask area id_area</i>	
network	Commande définissant les réseaux sur lesquels le routage sera actif.
<i>A.B.C.D</i>	l'adresse du réseau
<i>Mask</i>	Le masque soit sous la forme ' <i>netmask</i> ' ou ' <i>wildcard mask</i> '.
<i>area</i>	Mot clé définissant la zone à configurer.
<i>id_area</i>	l'adresse de la zone
Exemple	
routeur OSPF 1 network 192.168.15.0 0.0.0.255 area 0.0.0.0	

- ❑ Les routeurs Cisco acceptent deux écritures pour désigner une zone OSPF (*OSPF area ID*) :
 - Soit sous la forme d'une adresse IP, par exemple : 0.0.0.80.
 - Soit en valeur décimale de 0 à 4.294.967.295, par exemple : 80.

Commandes	Commentaires
configure terminal router ospf 1	Initialisation d'OSPF avec comme identifiant l'AS '1'
network 192.168.15.0 0.0.0.255 area 0	Définition du réseau participant à la négociation du routage.
network 192.168.16.0 0.0.15.255 area 0.0.0.1 Summary-address 192.168.0.0 255.255.0.0	Agrégation de routes pour un routeur ASBR : pour synthétiser les routes entre AS (<i>Autonomous System</i>)
area 0.0.0.1 range 192.168.16.0 255.255.240.0	Agrégation de routes pour un routeur ABR : pour synthétiser les routes d'une zone
area 0 authentication [message-digest]	Activation de l'authentification
area zone-id stub	Définit la 'zone-id' comme étant terminal, zone dans laquelle les informations sur les routes externes ne sont pas envoyées.
area zone-id default-cost cost	Définit le 'cost' à la route principale
area zone-id virtual-link A.B.C.D	Définition d'un lien virtuel
passive-interface {default serial eth Dialer BRI} Interface	Suppression des mises à jour de routage <ul style="list-style-type: none"> o 'default' sur toutes les interfaces o 'serial' sur l'interface série (précisez quelle interface) o 'eth 0' sur l'interface Ethernet o 'Interface' interface en particulier
Distance 200	Redéfinition de la distance administrative. Par défaut 110.
configure terminal interface eth 0	Menu de configuration de l'interface
ip ospf priority <0-255>	Priorité pour élire le DR et le BDR. C'est la valeur la plus élevée qui désigne le DR (<i>Designated Router</i>)
ip ospf cost <1-65535>	Coût OSPF d'une interface. Ce paramètre remplace 'Bandwith'.
ip ospf hello-interval <1-65535>	'hello-interval' délai (par défaut 10s) pour l'émission des messages Hello qui permettent : <ul style="list-style-type: none"> o de signaler l'existence du routeur et o l'élection du DR et BDR.
ip ospf dead-interval <1-65535>	'dead-interval' indique l'intervalle à l'issue duquel un routeur n'ayant pas reçu de message HELLO de son voisin le considère comme défaillant.

Exemple de configuration d'un routeur OSPF

<pre> version 12.0 service password-encryption ! hostname Dax3 ! enable secret 5 \$l\$lSz4\$RM0B2k.7CAtnRb ! ip subnet-zero ! interface Ethernet0 description Reseau Ethernet ip address 192.168.68.1 255.255.255.0 no ip directed-broadcast ! interface Serial0 description LS vers Brive 1 bandwidth 256 ip address 192.168.66.1 255.255.255.0 no ip directed-broadcast clockrate 2000000 </pre>	<pre> ! interface Serial1 description LS vers Brive 2 bandwidth 512 ip address 192.168.65.2 255.255.255.0 no ip directed-broadcast ! router ospf 1 network 192.168.65.0 0.0.0.255 area 0.0.0.0 network 192.168.66.0 0.0.0.255 area 0.0.0.0 network 192.168.68.0 0.0.0.255 area 0.0.0.0 ! ip classless ! line con 0 password 7 1410170D05 transport input none line aux 0 password 7 094B4B0F10 line vty 0 4 password 7 06010A254958 login ! end </pre>
--	--

Lecture conseillée :

http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Internetworking:OSPF

IX.D Résultat

```

Castres2#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 not set

O IA 192.168.15.0/24 [110/410] via 192.168.18.49, 00:08:00, Serial1
    192.168.19.0/24 is variably subnetted, 5 subnets, 2 masks
O IA 192.168.19.56/30 [110/1210] via 192.168.18.49, 00:08:01, Serial1
O IA 192.168.19.48/30 [110/810] via 192.168.18.49, 00:08:01, Serial1
O IA 192.168.19.52/30 [110/1210] via 192.168.18.49, 00:08:01, Serial1
O IA 192.168.19.32/28 [110/1220] via 192.168.18.49, 00:03:25, Serial1
O IA 192.168.19.16/28 [110/820] via 192.168.18.49, 00:08:01, Serial1
    192.168.18.0/24 is variably subnetted, 5 subnets, 2 masks
O    192.168.18.56/30 [110/1200] via 192.168.18.49, 00:09:49, Serial1
    [110/1200] via 192.168.18.54, 00:09:49, Serial0
C    192.168.18.48/30 is directly connected, Serial1
C    192.168.18.52/30 is directly connected, Serial0
O    192.168.18.32/28 [110/410] via 192.168.18.54, 00:09:49, Serial0
C    192.168.18.16/28 is directly connected, Ethernet0
Castres2#

```

```

Dax2#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 not set

O IA 192.168.15.0/24 [110/410] via 192.168.19.49, 00:01:57, Serial1
    192.168.19.0/24 is variably subnetted, 5 subnets, 2 masks
O    192.168.19.56/30 [110/1200] via 192.168.19.49, 00:01:58, Serial1
    [110/1200] via 192.168.19.54, 00:01:58, Serial0
C    192.168.19.48/30 is directly connected, Serial1
C    192.168.19.52/30 is directly connected, Serial0
O    192.168.19.32/28 [110/410] via 192.168.19.54, 00:01:58, Serial0
C    192.168.19.16/28 is directly connected, Ethernet0
    192.168.18.0/24 is variably subnetted, 5 subnets, 2 masks
O IA 192.168.18.56/30 [110/1210] via 192.168.19.49, 00:01:59, Serial1
O IA 192.168.18.48/30 [110/810] via 192.168.19.49, 00:01:59, Serial1
O IA 192.168.18.52/30 [110/1210] via 192.168.19.49, 00:01:59, Serial1
O IA 192.168.18.32/28 [110/1220] via 192.168.19.49, 00:01:59, Serial1
O IA 192.168.18.16/28 [110/820] via 192.168.19.49, 00:01:59, Serial1
Dax2#

```

IX.E Exercice #1

- À partir du schéma réseau sans VLSM, configurez simplement le routage OSPF sur vos routeurs avec les paramètres suivants :
 - Les routeurs Albi1, Brive1, Castres1 et DAX1 réalisent la zone '0.0.0.0' par leur interface sur le réseau 192.168.15.0/24.
 - Les routeurs Albi font partie de la zone '0.0.0.1'.
 - Les routeurs Brive font partie de la zone '0.0.0.2'.
 - Les routeurs Castres font partie de la zone '0.0.0.3'.
 - Les routeurs Dax font partie de la zone '0.0.0.4'.

IX.F Exercice #2

- Quand la configuration initiale est réalisée et testée, mettez en œuvre l'agrégation de route sur les routeurs ABR. Puis vérifiez la simplification de vos tables de routage.

IX.G Correction

- ❑ La configuration de l'ensemble des routeurs est comparable à celles données en exemple au plan d'adressage et aux zones OSPF prêt.
- ❑ Attention aux routeurs « X.1 », ce sont des routeurs inters area, ils ont des interfaces dans des zones différentes.

CONFIGURATION DU ROUTEUR DAX 3	
<pre> version 12.0 service password-encryption ! hostname Dax3 ! enable secret 5 \$1\$lSz4\$RM0B2k.7CAtnRbVCr ! ip subnet-zero ! interface Ethernet0 description Reseau Ethernet ip address 192.168.68.1 255.255.255.0 no ip directed-broadcast ! interface Serial0 description LS vers Brive 1 bandwidth 256 ip address 192.168.66.1 255.255.255.0 no ip directed-broadcast ip ospf cost 380 clockrate 2000000 ! interface Serial1 description LS vers Brive 2 bandwidth 512 ip address 192.168.65.2 255.255.255.0 no ip directed-broadcast </pre>	<pre> ! router ospf 1 network 192.168.65.0 0.0.0.255 area 0.0.0.4 network 192.168.66.0 0.0.0.255 area 0.0.0.4 network 192.168.68.0 0.0.0.255 area 0.0.0.4 ! ip classless ! snmp-server community public RO snmp-server community private RW ! line con 0 password 7 1410170D05 transport input none line aux 0 password 7 094B4B0F10 line vty 0 4 password 7 06010A254958 login ! end </pre>

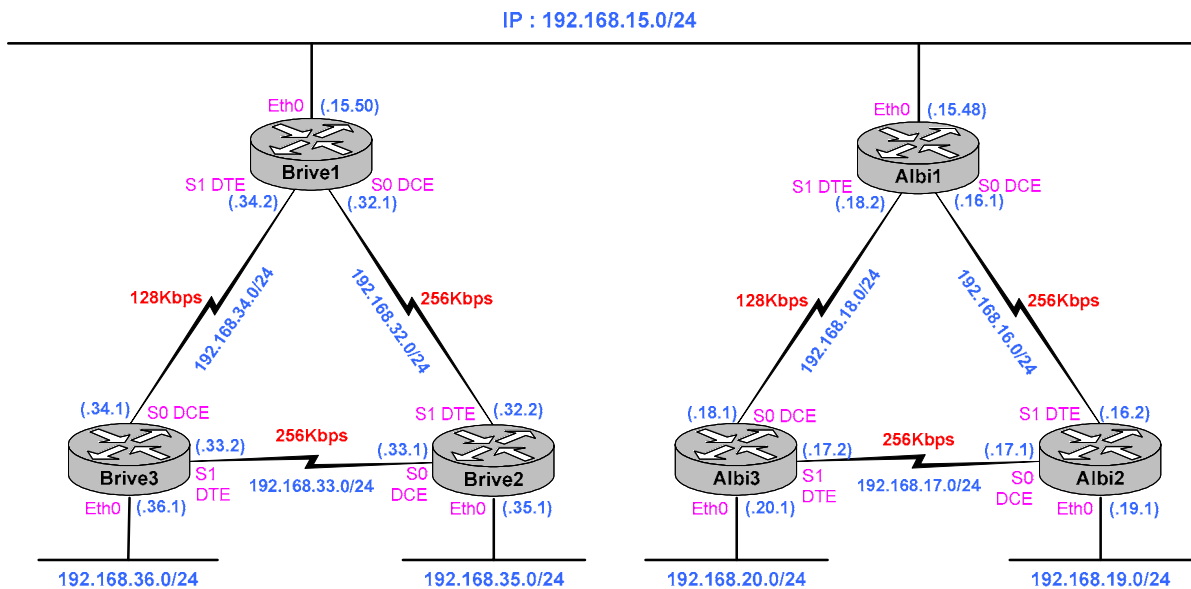
CONFIGURATION DU ROUTEUR DAX 1

<pre> ! version 12.0 no service password-encryption ! hostname DAX1 ! enable secret 5 \$1\$lSz4\$RM0B2k. ! ip subnet-zero ! ! interface Ethernet0 description Reseau Ethernet ip address 192.168.3.7 255.255.255.0 no ip directed-broadcast ! interface Serial0 description LS vers Dax 2 bandwidth 512 ip address 192.168.64.1 255.255.255.0 no ip directed-broadcast clockrate 2000000 ! interface Serial1 description LS vers Dax 3 bandwidth 256 ip address 192.168.66.2 255.255.255.0 no ip directed-broadcast ip ospf cost 380 </pre>	<pre> ! router ospf 1 network 192.168.3.0 0.0.0.255 area 0.0.0.0 network 192.168.64.0 0.0.0.255 area 0.0.0.4 network 192.168.66.0 0.0.0.255 area 0.0.0.4 ! ip classless ! snmp-server community public RO snmp-server community private RW ! line con 0 password gefi transport input none line aux 0 password gefi line vty 0 4 password gedev login ! end </pre>
---	--

IX.H Commandes de dépannage

- ❑ Maintenant, essayez les commandes bien connues :
 - 'ping',
 - 'traceroute',
 - 'show ip route',
 - 'show interfaces',
 - 'show protocoles'.
- ❑ Ces commandes sont semblables à celles vu lors de l'étude d'EIGRP.

- ❑ Exemple :



- La commande 'show ip ospf Neighbor' pour visualiser les voisins OSPF.

```
Albi1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address        Interface
192.168.34.2    1     FULL/DR         00:00:32   192.168.15.50 Ethernet1
192.168.19.1    1     FULL/-          00:00:36   192.168.16.2  Serial0
192.168.20.1    1     FULL/-          00:00:33   192.168.18.1  Serial1
Albi1#
```

- On peut également obtenir le détail.

```

Albil#show ip ospf neighbor detail
Neighbor 192.168.34.2, interface address 192.168.15.50
  In the area 0.0.0.0 via interface Ethernet1
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 192.168.15.50 BDR is 192.168.15.48
  Options 2
  Dead timer due in 00:00:36
Neighbor 192.168.19.1, interface address 192.168.16.2
  In the area 0.0.0.1 via interface Serial0
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 0.0.0.0 BDR is 0.0.0.0
  Options 2
  Dead timer due in 00:00:30
Neighbor 192.168.20.1, interface address 192.168.18.1
  In the area 0.0.0.1 via interface Serial1
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 0.0.0.0 BDR is 0.0.0.0
  Options 2
  Dead timer due in 00:00:38
Albil#

```

IX.I Visualisation des interfaces OSPF

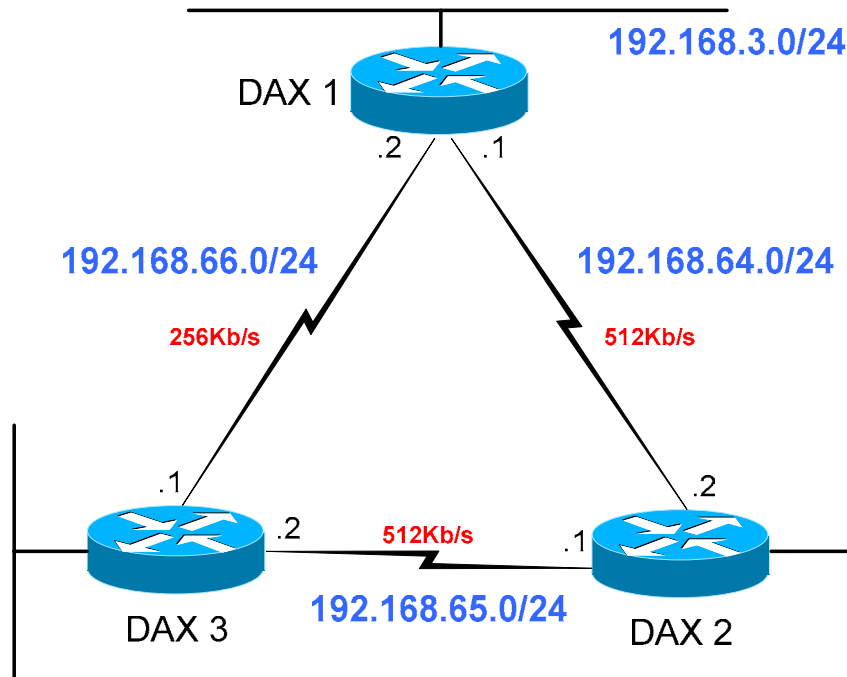
```

Albil#show ip ospf interface
Ethernet1 is up, line protocol is up
  Internet Address 192.168.15.48/24, Area 0.0.0.0
  Process ID 1, Router ID 192.168.18.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 192.168.34.2, Interface address 192.168.15.50
  Backup Designated router (ID) 192.168.18.2, Interface address 192.168.15.48
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.34.2 (Designated Router)
  Suppress hello for 0 neighbor(s)
Serial0 is up, line protocol is up
  Internet Address 192.168.16.1/24, Area 0.0.0.1
  Process ID 1, Router ID 192.168.18.2, Network Type POINT_TO_POINT, Cost: 400
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.19.1
  Suppress hello for 0 neighbor(s)
Serial1 is up, line protocol is up
  Internet Address 192.168.18.2/24, Area 0.0.0.1
  Process ID 1, Router ID 192.168.18.2, Network Type POINT_TO_POINT, Cost: 800
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.20.1
  Suppress hello for 0 neighbor(s)
Albil#

```

- ❑ Notez l'ID du routeur et le coût des interfaces.
- ❑ Calculez le coût pour chaque liaison série et comparez avec celui calculé par le routeur.

IX.J Étude de cas : une boucle



- ❑ A partir du routeur DAX3 nous pouvons atteindre le réseau 192.168.3.0 directement par le lien 192.168.66.0 ou par le lien 192.168.65.0 passer par le routeur DAX2 puis le lien 192.168.64.0.
- ❑ La commande 'show ip route 192.168.3.0' nous donne le résultat suivant :

```

O   192.168.3.0/24 [110/400] via 192.168.66.2, 00:00:20, Serial0
    [110/400] via 192.168.65.1, 00:00:20, Serial1
    
```

- ❑ Nous avons deux routes dont le métrique identique est de 400.
 - En effet :

Débit	Calcul	Coût
Deux liens 512 Mbps	$10^8/512\ 000 + 10^8/512\ 000$	390
Un lien 256 Mbps	$10^8/256\ 000$	390
 - En ajoutant le coût de l'interface Ethernet ($10^8/10\ 000\ 000 = 10$) on obtient bien un métrique de 400.
- ❑ Dans ce cas le routeur va envoyer successivement un paquet sur chaque interface, comme c'est le cas lorsque l'on veut faire du partage de charge sur deux liens.

- ❑ Nous pouvons modifier le coût d'une des interfaces afin de choisir la route.
- ❑ La Commande 'ip ospf cost' va permettre de modifier le coût d'une interface.

Exemple :

DAX1(config)# int serial 1 DAX1(config if)#ip ospf cost 380	On fixe le coût de l'interface S0 à une valeur moindre : 380.
--	---

- ❑ La commande 'sh ip route 192.168.3.0' nous donne le résultat suivant :

O 192.168.3.0/24 [110/390] via 192.168.66.2, 00:00:02, Serial0
--

- ❑ Afin de rester cohérent, cette modification doit être effectuée sur chaque extrémité du lien.

Exemple de métrique :

Métrique OSPF	
Bandwith	$\frac{10^8}{\textit{Bandwith}}$
128 Kbps	781
256 Kbps	390
512 Kbps	195
10 Mbps	10

IX.K Election du routeur désigné (DR & BDR)

DR : Designated Router

BDR : Backup DR

- ❑ OSPF élit un DR et un BRD sur chaque segment multiaccès. L'objectif est de fournir aux autres routeurs un point de contact central pour l'échange d'informations, ce qui permet de réduire le trafic émis.
- ❑ L'élection des routeurs DR et BDR se fait par échange de messages HELLO. Ces paquets HELLO sont émis en multicast IP sur chaque segment et le routeur possédant la priorité OSPF la plus forte devient DR. Le même processus se déroule pour élire le BDR. En cas d'égalité, le routeur possédant le RID (*Router Identifier*) le plus élevé gagne l'élection. Le RID est l'adresse IP la plus forte d'un routeur OSPF.
- ❑ La configuration de la priorité OSPF est réalisée au niveau de l'interface.
 - La valeur par défaut de la priorité est de '1', tandis que sa valeur maximum est de 255.
 - Si 'ip ospf priority 0', alors le routeur n'est pas éligible DR ou BDR.

```
Conf t
interface Serial 1
 ip address 192.168.66.2 255.255.255.0
 ip ospf priority 2
```

- ❑ Pour forcer l'élection du DR, on peut aussi créer une interface virtuelle avec une adresse IP qui sera la plus élevée du réseau, ce qui permettra à ce router de devinir DR pour tous les LAN qui lui sont connectés

```
Conf t
interface loopback 0
 ip address 192.168.255.254 255.255.255.0
```

- ❑ Si le DR (routeur R1) tombe en panne alors le BDR (routeur R2) rend la relève. Dès que l'ancien DR redevient opérationnel XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
- ❑ Une priorité de '0' désigne une interface qui ne peut pas concourir à l'élection du DR et BDR. Son état est '*DROTHER*'.
- ❑ Les annonces LSA ne sont délivrées qu'aux routeurs DR et BDR.
- ❑ Le choix du DR est déterminant dans une architecture OSPF, car ce protocole exige d'importante capacité CPU pour ses calculs. Utiliser des routeurs OSPF internes (IR : *Internal Router*) en DR et BDR et les routeurs ABR ou ABSR pour diffuser les tables de routages

IX.L Authentification OSPF

- ❑ Sous OSPF, il est possible d’authentifier les paquets (PDU). Par défaut, un routeur n’applique aucun mécanisme d’authentification.
- ❑ Deux méthodes d’authentification sont disponibles :
 - Authentification simple par mot de passe ou
 - Authentification MD5 (Message Digest 5).

IX.L.1 Authentification texte

- ❑ Cette méthode permet de configurer un mot de passe ou clé (key) par zone. Pour permettre aux routeurs d’une même zone de participer au processus de routage, ils doivent être configurés avec le même mot de passe.
- ❑ L’inconvénient de cette solution est qu’elle sujette aux attaques passives, c’est-à-dire qu’un analyseur réseau (sniffer) peut visualiser le mot de passe.

Authentification simple par mot de passe	
Commandes	Commentaires
# router ospf 100	
# network 10.10.0.0 0.0.255.255 area 0	
# area 0 authentication	Activation de l’authentification dans la zone 0.
# interface eth 0	
# ip add 10.10.10.1 255.255.255.0	
# ip ospf authentication-key <i>password</i>	Déclaration du mot de passe qui sera échangé en clair (dans l’entête du message OSPF) sur le réseau.

IX.L.2 Authentification MD5

Authentification par condensé de message (MD5)	
Commandes	Commentaires
# router ospf 100	
# network 10.10.0.0 0.0.255.255 area 0	
# area 0 authentication message-digest	
# interface eth 0	
# ip add 10.10.10.1 255.255.255.0	
# ip ospf message-digest-key 10 md5 <i>password</i>	Déclaration du mot de passe qui sera échangé chiffré sur le réseau.

# ip ospf message-digest-key <Key-ID> md5 [0-7] <i>password</i>	

IX.M Équilibrage de charge

- ❑ l'option ECMP (*Equal Cost Multi-Path*), décrite dans la RFC 2178 permet l'équilibrage de charge.

IX.N Synthèse RIP/OSPF

- ❑ OSPF a été conçu pour pallier les limitations du protocole RIP qui manque d'évolutivité, converge lentement et est sujet aux boucles de routage.
- ❑ OSPF apporte :
 - Vitesse de convergence : la convergence est plus rapide car les modifications de routage sont transmises immédiatement et calculées en parallèle.
 - Support du VLSM : supporte les masques de sous réseau et le VLSM.
 - Utilisation de la bande passante : OSPF utilise la multi diffusion (*multicast*) lors de l'actualisation de routage et effectue un envoi uniquement en cas de changement dans le réseau.
 - Méthode de sélection de chemin : OSPF utilise une valeur de coût basée sur la vitesse de la connexion.
- ❑ Mais OSPF est extrêmement sensible à l'instabilité de liens série. Cette condition désignée par le terme instabilité de route (*route flapping*) peut générer une série d'annonces LSA, conduisant le routeur à recalculer sa table de routage à plusieurs reprises et gênant la convergence.

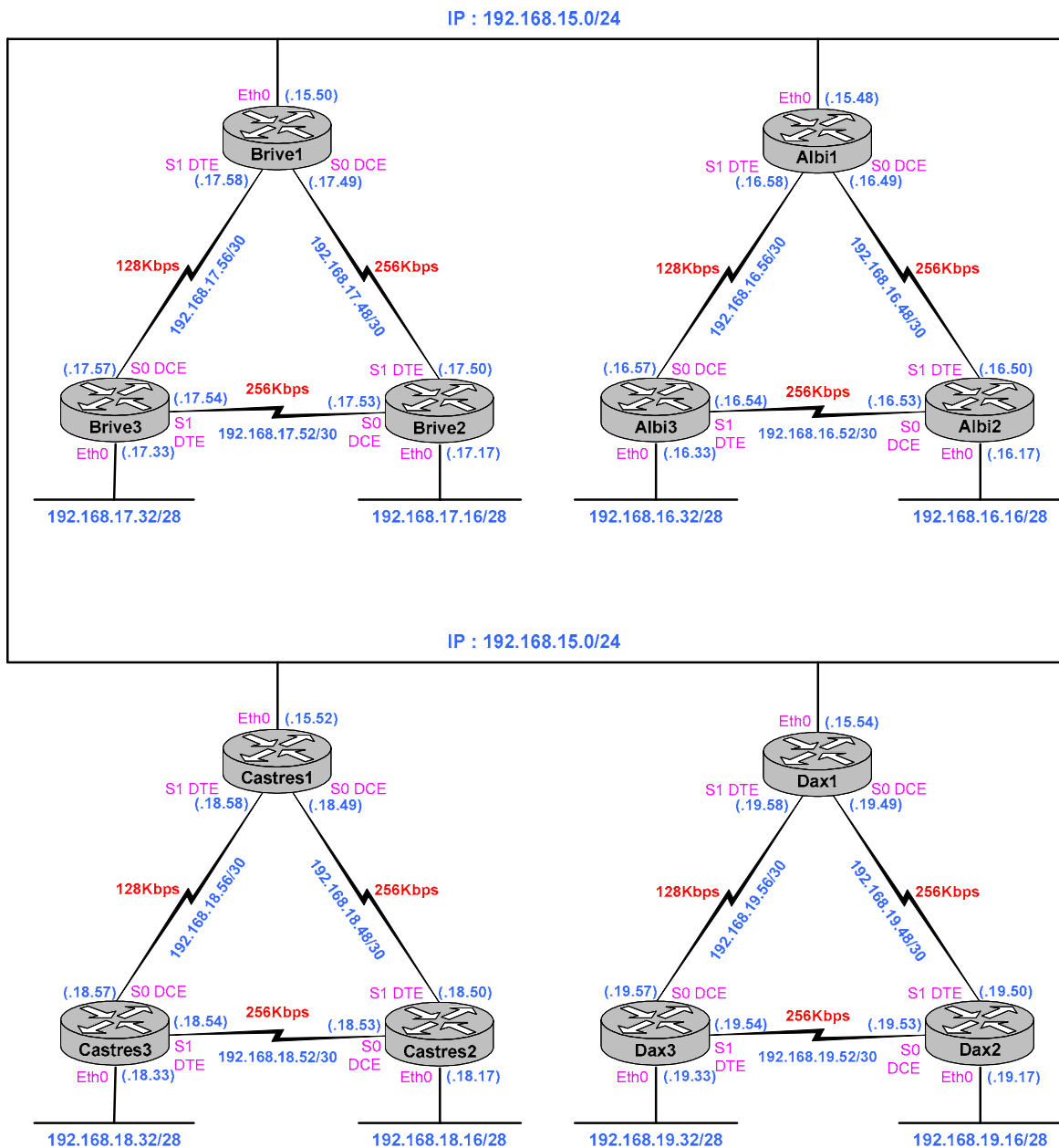
Commandes	Commentaires
<code>timers spf delay retenue</code>	<p>Cette commande a été introduite pour empêcher que les routeurs ne recalculent trop souvent leur table de routage. Les valeurs acceptées se situent entre 0 et 65535 pour les deux temporisateurs.</p> <ul style="list-style-type: none"> ○ Le temporisateur '<i>delay</i>' définit le délai en secondes qui s'écoule entre la prise de connaissance d'un changement de topologie et le début du processus de calcul SPF. Le délai par défaut est de 5 secondes. La valeur '0' indique l'absence de délai, c'est-à-dire que le processus de calcul débute immédiatement. ○ Le temporisateur '<i>retenue</i>' spécifie l'intervalle qui doit s'écouler entre deux processus de calcul SPF.

- ❑ Le routage OSPF est fiable, car toutes les annonces LSA sont acquittées par un ACK.

X. La redistribution

X.A Présentation

- La redistribution va permettre de faire cohabiter sur un routeur deux ou plusieurs protocoles de routage. Cette option lorsqu'elle est appliquée permet de faire passer les informations de routage d'un protocole vers un autre.



X.B Redistribution dans RIP

X.B.1 Problèmes liés à RIP

- ❑ La métrique de RIP est le nombre de sauts, ce nombre est limité à 15.
- ❑ La métrique EIGRP ou OSPF par exemple seront généralement supérieurs à 15, ce qui aura pour effet que les routes EIGRP ou OSPF ne seront pas prises en compte.
- ❑ La solution est de fixer la métrique au niveau de la redistribution.

X.B.2 Redistribution de routes statiques

- ❑ On peut par exemple redistribuer dans un protocole de routage dynamique des informations de routage statique.
- ❑ La commande 'redistribute static':

Exemple :

```
Routeur rip
network 172.16.16.0
network 192.168.16.0
redistribute static
passive interface ethernet 0
```

X.B.3 Redistribution de EIGRP

- ❑ La métrique de RIP est le nombre de sauts, ce nombre est limité à 15.
- ❑ La métrique EIGRP ou OSPF par exemple seront généralement supérieurs à 15, ce qui aura pour effet que les routes EIGRP ou OSPF ne seront pas prises en compte.
- ❑ La solution est de fixer la métrique au niveau de la redistribution.
- ❑ Dans l'exemple suivant les routes EIGRP seront redistribuées dans RIP avec un métrique de 3.

```
router rip
version 2
redistribute eigrp 1 metric 3
network 192.168.3.0
network 192.168.32.0
network 192.168.34.0
```

X.B.4 Redistribution d'OSPF

- ❑ La métrique de RIP est le nombre de sauts, ce nombre est limité à 15.
- ❑ La métrique d'une route OSPF est généralement supérieure à 15, ce qui aura pour effet que les routes OSPF ne seront pas prises en compte. La solution est de fixer la métrique au niveau de la redistribution.

- ❑ Dans l'exemple suivant les routes OSPF seront redistribuées dans RIP avec un métrique de 3.

```
router rip
version 2
redistribute ospf 1 metric 3
network 192.168.3.0
network 192.168.32.0
network 192.168.34.0
```

- ❑ Exemple à voir :
 - La commande '**redistribute**' utilise le mot clé '**ospf**' pour indiquer que les routes OSPF doivent être redistribuées dans RIP. Le mot clé '**internal**' spécifie les zones intrazones et interzones OSPF ; à savoir '**external 1**' pour la route externe de type 1 et '**external 2**' pour la route externe de type 2. Comme la commande de l'exemple utilise le comportement par défaut, il se peut que ces commandes ne soient pas visualisées dans les fichiers de configurations du routeur.

```
router rip
version 2
redistribute ospf 1 match internal external 1 external 2
default-metric 10
network 192.168.3.0
network 192.168.32.0
network 192.168.34.0
```

X.C Redistribution dans EIGRP

X.C.1 Redistribution de RIP

- ❑ Pour que EIGRP fonctionne il convient de connaître les valeurs du tableau suivant entrant dans le calcul du métrique.

Métrique	Valeur
bandwidth	10000 for Ethernet. Minimum bandwidth of the route may be 9.6.
delay	100 x 10 microseconds = 1 ms.
reliability	255 for 100% reliability.
load	Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
MTU	Minimum MTU of the router usually equals the Ethernet bandwidth.

- ❑ La commande 'default-metric' permet de fixer ces valeurs :

```
default-metric bandwidth delay reliability load MTU
```

```
router eigrp 1
 redistribute rip
 network 192.168.3.0
 network 192.168.32.0
 network 192.168.34.0
 default-metric 10000 100 255 1 1500
 no auto-summary
```

X.C.2 Redistribution de OSPF

```
router eigrp 1
 redistribute ospf 1
 network 192.168.19.0
 default-metric 10000 100 255 1 1500
 no auto-summary
```

- ❑ Si la commande 'default-metric' n'est pas saisie EIGRP ne redistribue pas les routes OSPF.

X.D Redistribution dans OSPF

```
router ospf 1
 redistribute static
 default-information originate
 redistribute rip subnets
 redistribute eigrp 1 subnets
 network 192.168.15.0 0.0.0.255 area 0.0.0.0
```

- ❑ les routeurs ASBR redistribuent automatiquement les routes statiques.

X.D.1 Redistribution d'une route statique

- ❑ Pour qu'OSPF redistribue le routage statique, il suffit de rajouter la commande 'redistribute static'.

```
redistribute static
```

- ❑ Pour qu'OSPF redistribue une 'Default Gateway', il faut rajouter la commande 'default-information originate'. Il n'est pas nécessaire de mettre la commande 'redistribute static', si la seule route statique déclarée dans le routeur est une 'Default Gateway' (bien que une 'Default Gateway' soit une route statique).

```
default-information originate
```

X.D.2 Redistribution de RIP

- ❑ Attention par défaut OSPF redistribue seulement les réseaux non 'subnettés' :
 - 'Only classful networks will be redistributed'.

```
redistribute rip
```

- ❑ Pour qu'OSPF redistribue des réseaux 'subnettés', il faut rajouter l'argument 'subnets'.

```
redistribute rip subnets
```

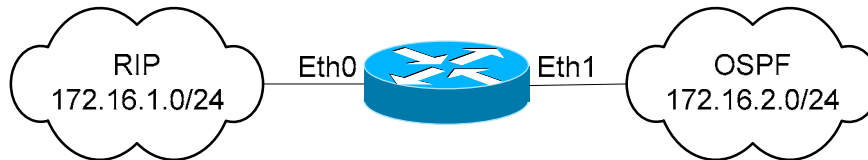
X.D.3 Redistribution de EIGRP

- ❑ Pour qu'OSPF redistribue des réseaux 'subnettés', il faut rajouter l'argument 'subnets' comme pour RIP.

```
redistribute eigrp 1 subnets
```

X.E Redistribution mutuelle RIP-OSPF

- Il est parfois nécessaire d'intégrer des topologies de réseau plus complexes, telles que des nuages RIP et OSPF indépendants, qui doivent effectuer une redistribution mutuelle. Dans cette architecture, il est capital d'éviter des boucles de routage en filtrant les routes. Le routeur exécute RIP et OSPF.

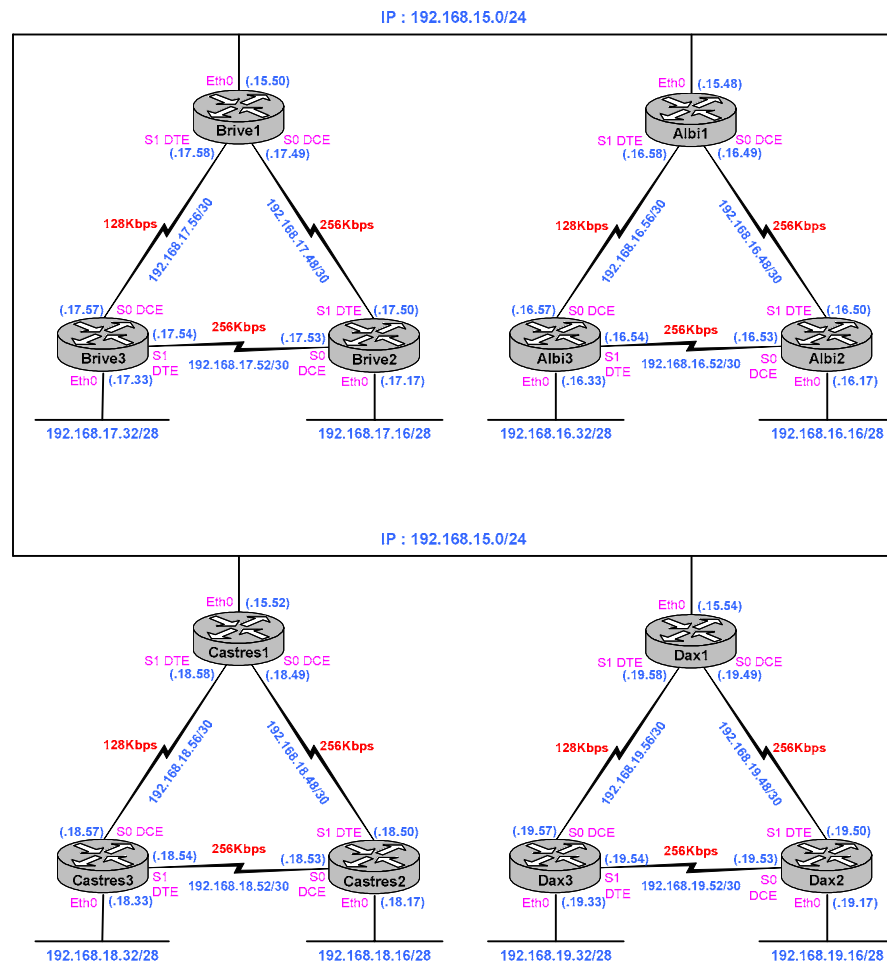


```
!  
interface Ethernet0  
description Routage RIP  
ip address 172.16.1.1 255.255.255.0  
!  
interface Ethernet1  
description Routage OSPF  
ip address 172.16.2.1 255.255.255.0  
!  
router rip  
version 2  
network 172.16.0.0  
passive-interface eth1  
redistribute ospf 1 metric 5  
distribute-list 10 out ospf 1  
!  
router ospf 1  
network 172.16.2.0 0.0.0.255 area 0.0.0.0  
redistribute rip subnets  
distribute-list 11 out rip  
!  
access-list 10 deny 172.16.1.0 0.0.0.255  
access-list 10 permit 0.0.0.0 255.255.255.255  
access-list 11 permit 172.16.1.0 0.0.0.255  
access-list 11 deny 0.0.0.0 255.255.255.255  
!
```


X.F Exercice

- ❑ Dans une architecture VLSM, configurez les routeurs comme suit :
 - Albi1, Brive1, Castres1 et Dax1 : OSPF area 0
 - Albi : OSPF area 1,
 - Brive : OSPF area 2
 - Castres : RIPv2
 - Dax : EIGRP

- ❑ Les deux routeurs, le C2621 et le C2503, sont à la charge du formateur :
 - Le C2621 et le C2503 seront configurés dans ‘OSPF area 0’.
 - De plus pour sortir sur Internet, le routeur C2503 redistribue dans ‘OSPF area 0’ une route par défaut (Default Gateway).



X.G Correction**Configuration du routeur Brivel**

```

!
version 11.3
no service password-encryption
!
hostname Brivel
!
enable secret 5 $1$lSz4$RMOB2k.7CAtnRbV
!
!
interface Ethernet0
description Reseau Ethernet
ip address 192.168.3.3 255.255.255.0
!
interface Serial0
description LS vers Brive 2
ip address 192.168.32.1 255.255.255.0
bandwidth 256
clockrate 2000000
!
interface Serial1
description LS vers Brive 3
ip address 192.168.34.2 255.255.255.0
bandwidth 128
!
!
router eigrp 1
 redistribute rip
 redistribute ospf 1
 redistribute static
 network 192.168.3.0
 network 192.168.32.0
 network 192.168.34.0
 default-metric 10000 100 255 1 1500
 no auto-summary
!
router ospf 1
 redistribute static
 redistribute rip
 redistribute eigrp 1
 network 192.168.3.0 0.0.0.255 area 0.0.0.0
!
router rip
 version 2
 redistribute static
 redistribute eigrp 1 metric 3
 redistribute ospf 1 metric 5
 network 192.168.3.0
 network 192.168.32.0
 network 192.168.34.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.30
!
line con 0
 password gefi
line aux 0
 password gefi
line vty 0 4
 password gedev
 login
!
end

```

X.H Commandes de dépannage

- ❑ Essayez les commandes habituelles pour vous assurer du bon fonctionnement de l'ensemble de la maquette.
- ❑ Notez que nous voyons des routes redistribuées OSPF, EIGRP :

```
Dax3#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 not set

O   192.168.64.0/24 [110/390] via 192.168.65.1, 00:02:28, Serial1
C   192.168.65.0/24 is directly connected, Serial1
O E2 192.168.20.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
C   192.168.66.0/24 is directly connected, Serial0
O E2 192.168.36.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
O   192.168.67.0/24 [110/205] via 192.168.65.1, 00:02:28, Serial1
O E2 192.168.34.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
O E2 192.168.17.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
C   192.168.68.0/24 is directly connected, Ethernet0
O E2 192.168.35.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
O E2 192.168.16.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
O E2 192.168.19.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
O E2 192.168.32.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
O E2 192.168.18.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
O   192.168.3.0/24 [110/390] via 192.168.66.2, 00:02:29, Serial0
O E2 192.168.33.0/24 [110/20] via 192.168.66.2, 00:02:28, Serial0
Dax3#
```

XI. Configuration DHCP

- ❑ Le service DHCP (Dynamic Host Configuration Protocol) nécessite pour fonctionner une configuration particulière au niveau des routeurs.
- ❑ DHCP est une extension de BOOTP (Bootstrap Protocol).
- ❑ DHCP utilise UDP (port 67 pour le serveur, 68 pour le client).
- ❑ Le routeur Cisco peut être un relai DHCP mais aussi un serveur DHCP.

XI.A Relai DHCP

- ❑ Lorsqu'un host veut obtenir sa configuration IP à l'aide de DHCP, il envoie une requête DHCP en broadcast on l'appelle DHCPDISCOVER.
- ❑ Le serveur répond avec un message DHCP OFFER contenant entre autres les adresses IP et MAC.
- ❑ La station envoie toujours en broadcast un message DHCPREQUEST, ce afin de préciser le serveur retenu.
- ❑ Le serveur accuse réception avec un message DHCPACK.
- ❑ Pour que cela fonctionne sur un réseau « routé » (le serveur DHCP n'est pas sur le même LAN que le client, le routeur qui reçoit la requête en broadcast, doit la transmettre en unicast au serveur DHCP).
- ❑ La commande 'ip helper-address' précise l'adresse vers laquelle sont routées les trames de broadcast.

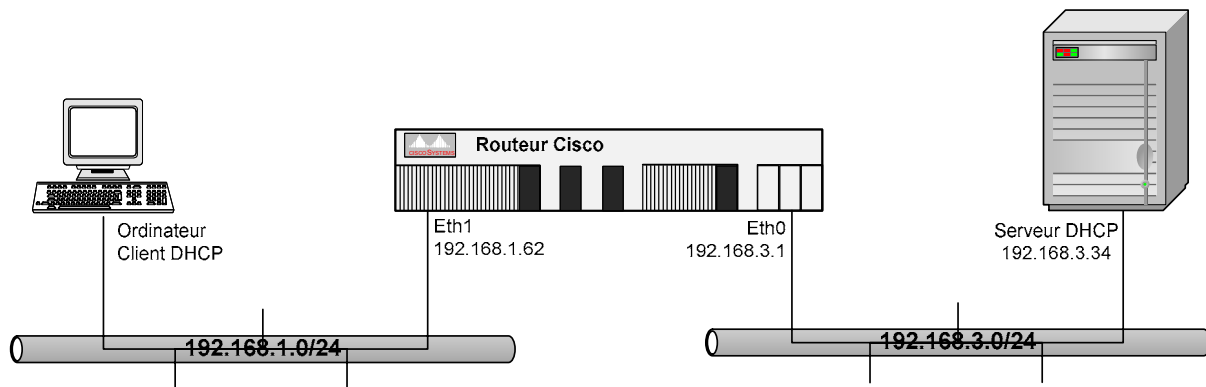
La Commande :

ip helper-address A.B.C.D	Adresse du serveur DHCP
---------------------------	-------------------------

Exemple :

```
interface ethernet 0/1
  ip helper-address 172.17.1.106
```

- ❑ Noter que pour différentes interfaces d'un même routeur, cette commande permet d'utiliser un serveur DHCP différent.
- ❑ La commande 'ip helper-address' a pour effet de transmettre en unicast à la machine indiquée, les trames reçues en broadcast (que ce soit du DHCP ou autre chose, BOOTP par exemple).



```

Router# configure terminal
Router(config)# no ip forward-protocol udp 37
Router(config)# no ip forward-protocol udp 49
Router(config)# no ip forward-protocol udp 53
Router(config)# no ip forward-protocol udp 69
Router(config)# no ip forward-protocol udp 137
Router(config)# no ip forward-protocol udp 138
Router(config)# ip forward-protocol udp 67
Router(config)# ip forward-protocol udp 68
Router(config)# interface ethernet 0
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config)# interface ethernet 1
Router(config-if)# ip address 192.168.1.62 255.255.255.0
Router(config-if)# ip helper-address 192.168.3.34
    
```

Ports	Protocoles
37	Time (timeserver)
49	Tacacs
53	DNS
69	tftp
137	NetBIOS-NS (NBNS)
138	NetBIOS-DGN (NetBIOS datagramme)
67	bootps (dhcps)
68	bootpc (dhcpc)

XI.B Serveur DHCP

- Le routeur, quoique ce ne soit pas sa fonction principale, peut assurer la fonction de serveur DHCP.

Exemple de configuration :

```
service dhcp
ip dhcp excluded-address 192.168.1.1 192.168.1.128
ip dhcp pool 1
  network 192.168.1.0 255.255.255.0
  domain-name gefi.fr
  default-router 192.168.1.1
  dns-server 210.1.24.2
```

XII. NAT/PAT

NAT : Network Address Translation, RFC 2663 et 3022

PAT : Port Address Translation

XII.A Présentation

- ❑ La translation d'adresse, appelée NAT consiste à changer l'adresse source et/ou destination des datagrammes IP traversant un routeur ou un firewall. Ce type de mécanisme peut être utilisé pour :
 - Augmenter le nombre de stations avec un nombre d'adresses IP insuffisant,
 - connecter un réseau privé à l'Internet,
 - sécuriser son Intranet en masquant le plan d'adressage,
 - interconnecter deux réseaux ayant la même adresse IP réseau.

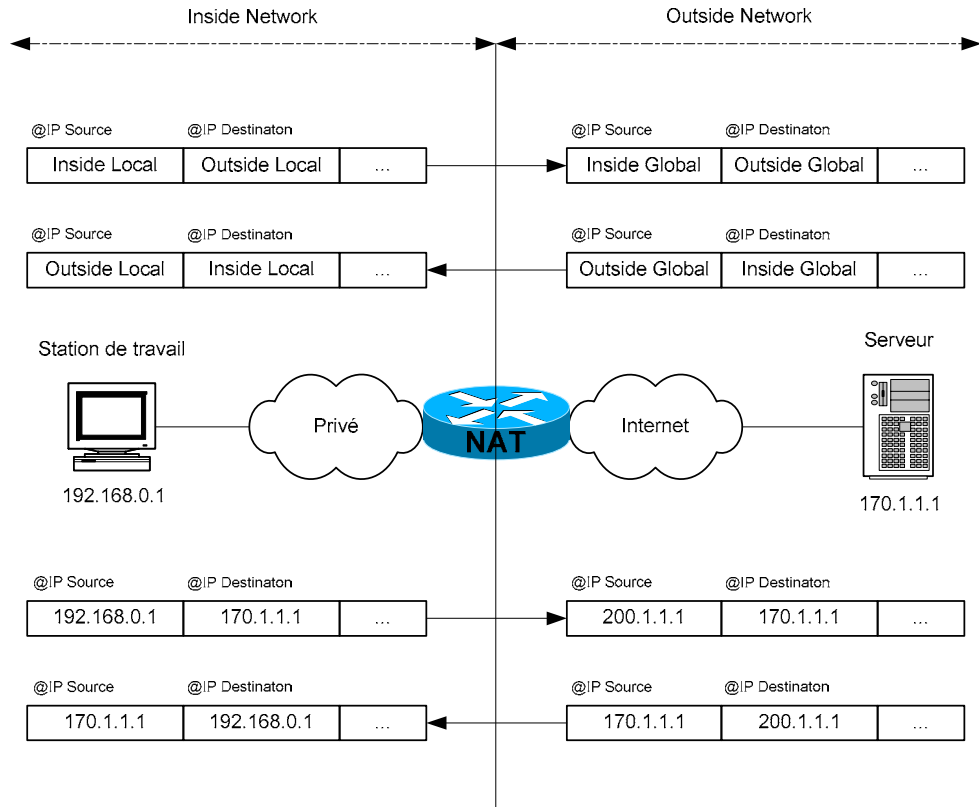
- ❑ En effet le RFC 1918 définit les tranches d'adresses utilisables pour un réseau privé et non routables sur l'Internet :

Reserved Private Network Allocation RFC 1918		
Network Class	Subnet mask	Network Addresses
A	255.0.0.0	10.0.0.0 - 10.255.255.255
B	255.255.0.0	172.16.0.0 - 172.31.255.255
C	255.255.255.0	192.168.0.0 - 192.168.255.255

- ❑ L'administrateur choisira donc les adresses de son réseau privé dans ces tranches.
- ❑ Il conviendra de traduire ces adresses privées, non routable sur l'Internet, en adresses publiques (officielles), ces dernières sont en général fournies par son ISP.
- ❑ Il existe plusieurs méthodes de translation :
 - Statique : une adresse interne correspond à une adresse externe, on parle alors de NAT (*Network Adresse Translation*).
 - Dynamique : plusieurs adresses internes peuvent éventuellement correspondre à une ou plusieurs adresses externes, on fera la différence sur le port source, on parle alors de PAT (*Port Address Translation*). Deux possibilités existent ; N pour M ($M \leq N$) et N pour 1.
- ❑ Le NAT peut être statique ou dynamique, le PAT sera forcément dynamique.
- ❑ Définition des interfaces, en règle générale :
 - Inside côté réseau privé,
 - Outside côté réseau Internet (par exemple).
- ❑ On peut définir un groupe d'adresses (*pool*), les adresses seront prises une à une dans ce groupe, lorsqu'il n'y a plus d'adresse disponible, toute nouvelle connexion devient alors impossible (NAT), l'option 'overload' permet de passer en mode PAT et ainsi de traduire un nombre d'adresses plus important que celles du groupe.
- ❑ NAT est incompatible avec un certain nombre de protocoles :
 - AH d'IPSEC,
 - FTP actif,

XII.B Terminologie :

- Exemple typique :
 - Ici, le réseau privé est le réseau ‘*Inside*’,
 - Ici ‘Internet’ est le réseau ‘*Outside*’.



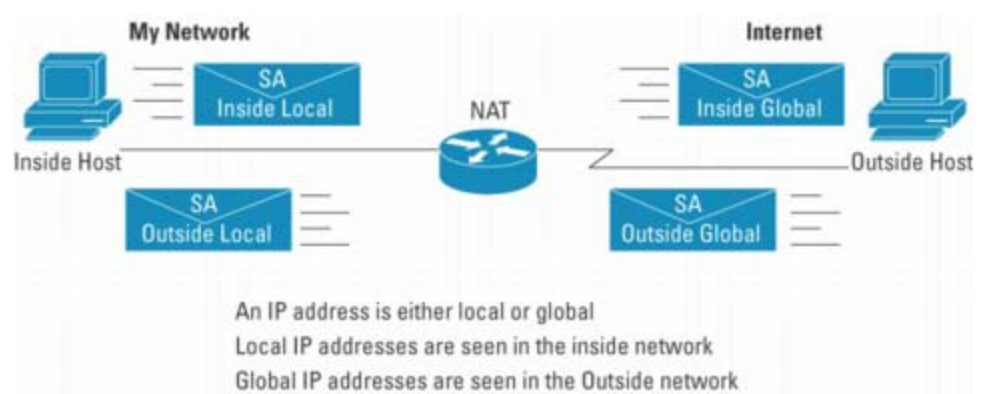
Appellation	Signification	Valeur (voir exemple)
Inside local address	C'est l'adresse IP de l'hôte de l' <i>Inside</i> dans l' <i>Inside</i> .	192.168.0.1
Inside global address	C'est l'adresse IP de l'hôte de l'Inside utilisée (vue) dans l' <i>Outside</i> .	200.1.1.1
Outside local address	C'est l'adresse IP de l'hôte de l' <i>Outside</i> mais tel qu'elle apparaît dans l' <i>Inside</i> . Ce n'est pas nécessairement une adresse IP publique, mais elle doit être routable dans l' <i>Inside</i> .	170.1.1.1
Outside global address	C'est l'adresse IP de l'hôte de l' <i>Outside</i> mais tel qu'elle apparaît dans l' <i>Outside</i> .	170.1.1.1

Appellation	Signification
Local address	C'est une adresse routable dans l' <i>Inside</i> '.
Global address	C'est une adresse routable dans l' <i>Outside</i> '.
Inside	L'inter réseau de l'inside.
Outside	L'inter réseau de l'outside.

- ❑ L'adresses IP '*Inside local address*' sera toujours une adresse privée.
- ❑ L'adresse IP '*Outside local address*' peut être :
 - une adresse publique, dans ce cas la '*Outside local address*' sera identique à la '*Outside global address*'.
 - une adresse privée, dans cette possibilité :
 - ❖ le réseau '*Outside*' possède une adresse réseau privée
 - ❖ une translation sur l'adresse destination sera réalisée (voir DNAT).

Command	Action
ip nat inside source	<ul style="list-style-type: none"> ○ Translates the source of IP packets that are traveling inside to outside. ○ Translates the destination of the IP packets that are traveling outside to inside.
ip nat outside source	<ul style="list-style-type: none"> ○ Translates the source of the IP packets that are traveling outside to inside. ○ Translates the destination of the IP packets that are traveling inside to outside.

- ❑ Le flux de session est un ensemble de paquets IP échangés entre deux instances et formant ainsi une unité, dans la mesure où ils sont traités de manière identique par un routeur NAT.
- ❑ Ce flux de session est orienté, dans le sens du premier paquet envoyé ; le sens initial et le sens inverse.
 - Une session Telnet est un exemple de flux de session : la connexion TCP correspondante étant initiée par la machine faisant office de terminal, le sens initial du flux de session correspondant est orienté du terminal vers le serveur.
 - Les flux de session basés sur les protocoles TCP/UDP peuvent être décrits de manière unique par le tuple {adresse IP source, Port source, adresse IP destination, Port destination}.
 - Dans le cas du protocole ICMP, un flux de session peut être identifié de manière analogue par le tuple {adresse IP source, adresse IP destination, type ICMP, identifiant ICMP}.
- ❑ Le routage transparent (comportement d'un routeur NAT par rapport à un routeur sans NAT) se déroule en trois phases :
 - Liaison des adresses : durant cette phase, on associe les deux adresses des deux espaces d'adressage (exemple : l'*inside local address* à l'*inside global address*). Cette phase devra être réalisée avant de pouvoir traduire les adresses. Cette liaison est faite soit de manière statique ou dynamique.
 - Traduction des adresses : durant cette phase le routeur NAT peut modifier les datagrammes IP en transit. Comme les adresses IP source et/ou destination et les numéros de ports sont modifiés le routeur NAT devra recalculer le champ CRC de l'entête IP.
 - Libération de la liaison des adresses : lorsque le dernier flux de session d'une liaison s'est terminé, cette dernière doit être libérée, dans la variante dynamique, afin de permettre une réutilisation de l'adresse externe. Dans la variante statique, la liaison est conservée.



❑ CONFIGURATION EXAMPLES

- The following sample configuration translates between inside hosts addressed from either the **192.168.1.0** or **192.168.2.0** nets to the globally-unique **171.69.233.208/28** network.

```
ip nat pool net-20 171.69.233.208 171.69.233.223 netmask 255.255.255.240
ip nat inside source list 1 pool net-20
!
interface Ethernet0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface Ethernet1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

- The next sample configuration translates between inside hosts addressed from the **9.114.11.0** net to the globally unique **171.69.233.208/28** network. Packets from outside hosts addressed from **9.114.11.0** net (the "true" **9.114.11.0** net) are translated to appear to be from net **10.0.1.0/24**.

```
ip nat pool net-20 171.69.233.208 171.69.233.223 netmask 255.255.255.240
ip nat pool net-10 10.0.1.0 10.0.1.255 netmask 255.255.255.0
ip nat inside source list 1 pool net-20
ip nat outside source list 1 pool net-10
!
interface Ethernet0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface Ethernet1
ip address 9.114.11.39 255.255.255.0
ip nat inside
!
access-list 1 permit 9.114.11.0 0.0.0.255
```

- In this example, outside-initiated connections to the SMTP port (25) will be sent to the inside host 192.168.10.1.

```
ip nat inside source static tcp 192.168.10.1 25 171.69.232.209 25
```

- The next sample configuration translates between inside hosts addressed from the **9.114.11.0** net to the globally unique **171.69.233.208/28** network. Packets from outside hosts addressed from **9.114.11.0** net (the "true" **9.114.11.0** net) are translated to appear to be from net **10.0.1.0/24**.

```
ip nat pool net-20 171.69.233.208 171.69.233.223 netmask 255.255.255.240
ip nat pool net-10 10.0.1.0 10.0.1.255 netmask 255.255.255.0
ip nat inside source list 1 pool net-20
ip nat outside source list 1 pool net-10
!
interface Ethernet0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface Ethernet1
ip address 9.114.11.39 255.255.255.0
ip nat inside
!
access-list 1 permit 9.114.11.0 0.0.0.255
```

XII.C Fonctionnement

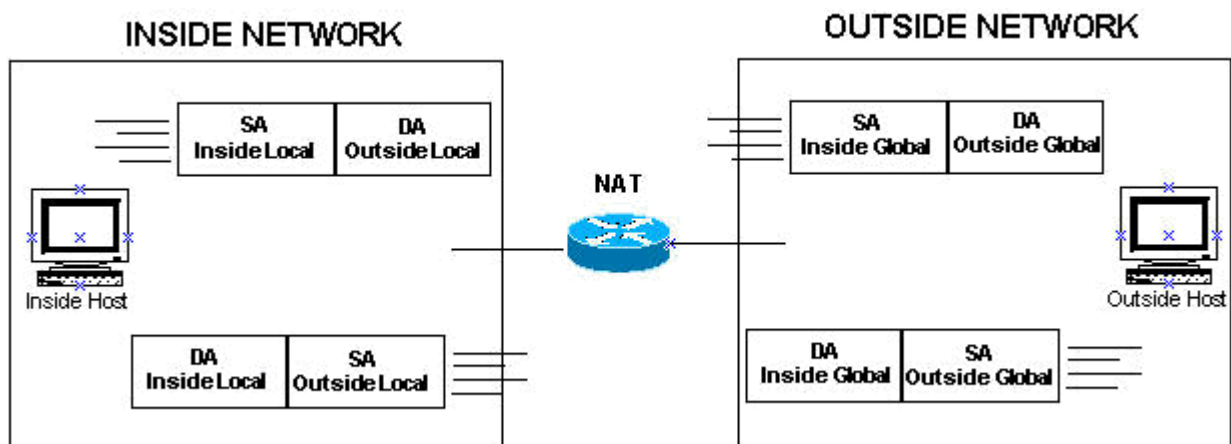
- ❑ Le NAT est implémenté au niveau d'un routeur ou d'une machine équivalente (firewall). Au moment où un datagramme traverse le routeur NAT, ce dernier modifie l'entête IP.
 - Si l'adresse IP source est modifiée, on parle de SNAT : Source NAT.
 - Si l'adresse IP destination est modifiée, on parle de DNAT : Destination NAT.

- ❑ Le Source NAT (SNAT) :
 - Le NAT statique consiste à effectuer sur les datagrammes une substitution de l'adresse IP source par une autre. Ainsi, pour chaque adresse IP du réseau interne (*Local Inside Address*), il faut disposer d'une adresse IP publique (*Global Inside Address*).
 - Le NAT dynamique consiste à effectuer sur les datagrammes une substitution N pour M de l'adresse source ($N > M$). Pour l'ensemble des N adresses IP internes du réseau, il suffira donc de disposer de M adresses IP publiques. Si $M = 1$, toutes les adresses privées (internes) utilisent une unique adresse IP publique pour sortir. Cette configuration est appelée IP masquerading (mascarade IP) puisque toutes les machines du réseau interne utilisent l'adresse (de l'interface côté FAI) du routeur NAT pour sortir.
 - Comme dans le cas du NAT statique, le routeur qui effectue du NAT dynamique substitue l'adresse IP source. Il s'agit donc également d'un mécanisme de Source NAT. Attention, lors du retour de la session un DNAT est effectué, c'est-à-dire que le routeur va substituer la '*Global Inside Address*' par '*Local Inside Address*' dans le champ Adresse IP destination du datagramme IP.
 - Dans le cas du NAT dynamique (256 vers 16 ou 16 vers 1) le routeur NAT implémente un mécanisme de translation de port ou PAT (*Port Address Translation*) pour déterminer à quelle adresse interne est destiné le datagramme.

- ❑ Le Destination NAT (DNAT) :
 - La table DNAT (Destination NAT) permet à une machine de l'Internet d'accéder à une machine d'un réseau privé.

Commande de configuration 'ip nat inside source static'	
<code>ip nat inside source {list{acl-name name} pool name [overload]} static local-ip global-ip</code>	
<code>ip nat inside source</code>	Commande de translation de l'adresse IP source de l'inside dans l'outside. Cette translation peut être effectuée de manière statique ou dynamique.
<code>list{acl-name name} pool name</code>	Ici la commande effectue une translation dynamique d'une ' <i>Inside local address</i> ' acquise à partir d'une ACL standard en ' <i>Inside global address</i> ' définit dans un groupe (<i>pool</i>) d'adresses. L'option '[overload]' permet au router d'utiliser une seule ' <i>Global Address</i> ' pour plusieurs ' <i>Inside Address</i> '.
<code>static local-ip global-ip</code>	Ici la commande effectue une translation statique d'une ' <i>Inside local address</i> ' en ' <i>Inside global address</i> '.
Exemples	
<code>ip nat inside source list 1 pool net-208 overload</code>	
<code>ip nat inside source static 10.0.1.10 192.168.19.2</code>	

Inside-to-Outside	Outside-to-Inside
check input access list input accounting inspect policy routing routing NAT inside to outside (local to global translation) check output access list inspect	check input access list input accounting inspect NAT outside to inside (global to local translation) policy routing routing check output access list inspect



- ❑ Lorsqu'un trafic est généré depuis l'inside vers l'outside :
 - A allée, un SNAT est réalisé : l'adresse IP source est tradlatée de 'Local Inside Address' en 'Global Inside Address'.
 - Au retour, un DNAT est réalisé : l'adresse IP destination est tradlatée de 'Global Inside Address' en 'Local Inside Address'. Cette translation est possible par la mémorisation des différentes adresses IP (source et destination) et des numéros de port (source et destination).
- ❑ Lorsqu'un trafic est généré depuis l'outside vers l'inside :
 - Lorsque le datagramme IP initial entre dans le routeur côté Outside

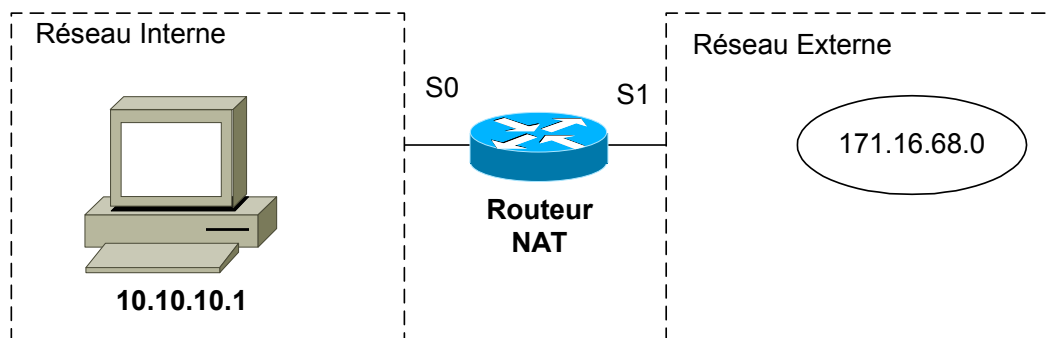
XII.D Configuration du NAT statique :

XII.D.1 Les commandes :

- En configuration statique, la table NAT est remplie manuellement par la commande 'ip nat {inside | outside} source static' donnant les correspondances entre adresses locales et globales.

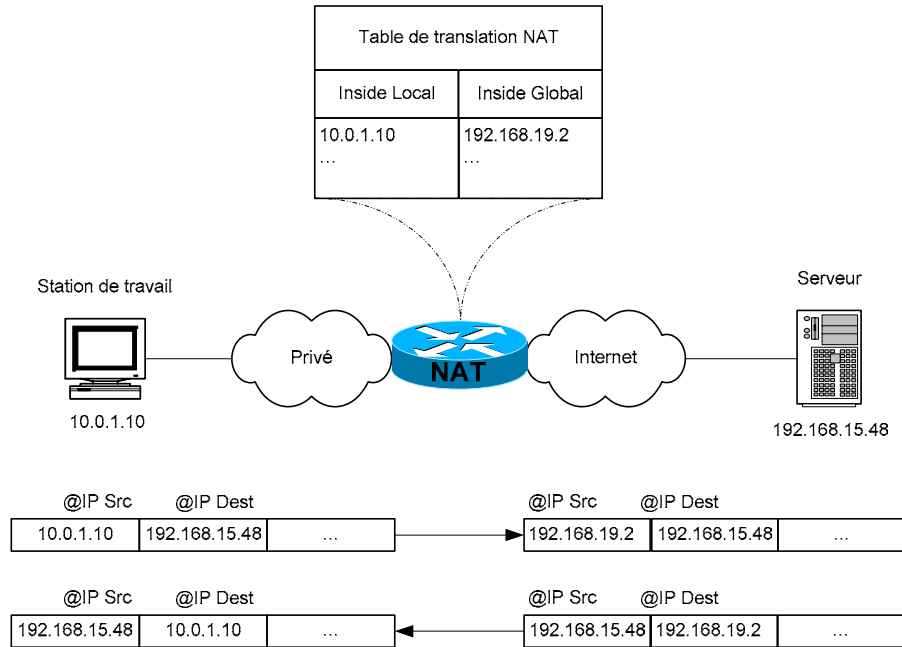
	Commande	Commentaire
1	ip nat inside source static <i>Inside-local</i> <i>Inside-global</i>	Etablir une translation statique entre une ' <i>Inside local address</i> ' et une ' <i>Inside global address</i> '.
1'	ip nat outside source static <i>Outside-local</i> <i>Outside-global</i>	Etablir une translation statique entre une ' <i>Outside local address</i> ' et une ' <i>Outside global address</i> '.
2	interface <i>type if-number</i>	Configuration de l'interface ' <i>inside</i> '
3	ip nat inside	Définir l'interface comme connectée à l'inside
4	interface <i>type if-number</i>	Configuration de l'interface ' <i>outside</i> '.
5	ip nat outside	Définir l'interface comme connectée à l'outside

XII.D.2 Exemple :



XII.D.3 Configuration SNAT

- Source NAT : translation des adresses source.



- Dans cette configuration, lorsque le routeur reçoit sur son interface 'inside' un datagramme IP avec comme adresse IP source 10.0.1.10, l'adresse IP source est modifiée en 192.168.19.2. De même si le routeur reçoit un datagramme sur son interface outside avec pour destination 192.168.19.2, l'adresse IP destination est traduite en 10.0.1.10.

```

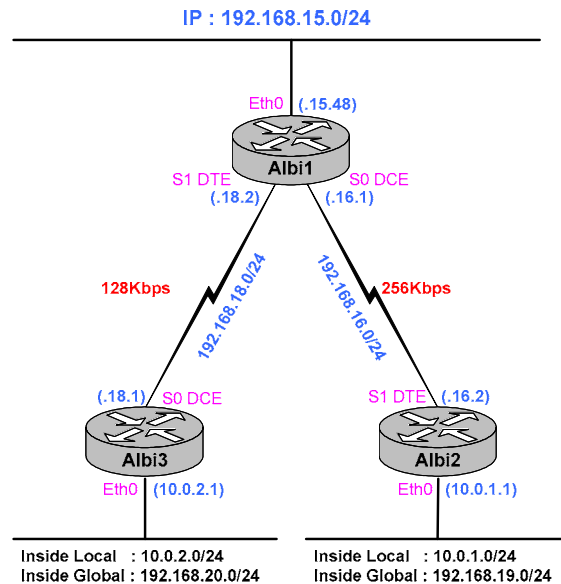
ip nat inside source static 10.1.1.10 192.168.19.2
!
interface Ethernet0
ip address 10.0.1.1 255.255.255.0
ip nat inside
!
interface Serial0
ip address 192.168.18.2 255.255.255.0
ip nat outside
    
```

Commande de configuration 'ip nat inside source static'	
<code>ip nat inside source static local-ip global-ip</code>	
<code>ip nat inside source static</code>	Commande de translation de l'adresse IP source de l'inside dans l'outside.
<code>local-ip</code>	Inside local address
<code>global-ip</code>	Inside global address
Exemple	
<code>ip nat inside source static 10.0.1.10 192.168.19.2</code>	

XII.D.4 Application du SNAT

- Cette configuration permet aux machines des réseaux 10.0.1.0/24 et 10.0.2.0/24 d'accéder au réseau 192.168.15.0 et réciproquement.

- La configuration d'Albi1 est totalement normale.



```

Albi1#sh run
Building configuration...

!
interface Ethernet0
 bandwidth 10000
 ip address 192.168.15.48 255.255.255.0
 no ip directed-broadcast
!

interface Serial0
 bandwidth 250
 ip address 192.168.16.1 255.255.255.0
 no ip directed-broadcast
 clockrate 250000
!

interface Serial1
 bandwidth 125
 ip address 192.168.18.2 255.255.255.0
 no ip directed-broadcast
!

ip route 192.168.19.0 255.255.255.0 192.168.16.2
ip route 192.168.20.0 255.255.255.0 192.168.18.1
!
end
Albi1#

```

- Contrôle : Albi1 possède les routes pour atteindre les réseaux tradatés.

```

Albi1#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, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

C    192.168.15.0/24 is directly connected, Ethernet1
S    192.168.20.0/24 [1/0] via 192.168.18.1
C    192.168.16.0/24 is directly connected, Serial0
S    192.168.19.0/24 [1/0] via 192.168.16.2
C    192.168.18.0/24 is directly connected, Serial1
Albi1#

```

- Sur Albi3 (comme sur Albi2),

```

Albi3#show running-config
Building configuration...

Current configuration:
!
interface Ethernet0
 bandwidth 10000
 ip address 10.0.2.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface Serial0
 bandwidth 125
 ip address 192.168.18.1 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 no ip mroute-cache
 no fair-queue
 clockrate 125000
!
interface Serial1
 shutdown
!
ip route 0.0.0.0 0.0.0.0 192.168.18.2!
!
ip nat inside source static 10.0.2.2 192.168.20.2
ip classless
!
!
end
Albi3#

```

```

Albi3#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 192.168.20.2       10.0.2.2          ---                ---
Albi3#

```


- ❑ Contrôle : une machine Windows 10.0.2.2 peut pinguer un serveur Linux sur le réseau 192.168.15.0/24.

```
C:\>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet:

    Suffixe DNS propre à la connexion :
    Adresse IP. . . . . : 10.0.2.2
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 10.0.2.1

C:\>ping 192.168.15.49

Envoi d'une requête 'ping' sur 192.168.15.49 avec 32 octets de données :

Réponse de 192.168.15.49 : octets=32 temps=13 ms TTL=62
Réponse de 192.168.15.49 : octets=32 temps=11 ms TTL=62
Réponse de 192.168.15.49 : octets=32 temps=13 ms TTL=62
Réponse de 192.168.15.49 : octets=32 temps=11 ms TTL=62

Statistiques Ping pour 192.168.15.49:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 11ms, Maximum = 13ms, Moyenne = 12ms

C:\>
```

- ❑ Voir le PC sur l'autre réseau traduit.

```
C:\>ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au réseau local:

    Suffixe DNS propre à la connexion :
    Adresse IP. . . . . : 10.0.2.2
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 10.0.2.1

C:\>ping 192.168.19.2

Envoi d'une requête 'ping' sur 192.168.19.2 avec 32 octets de données :

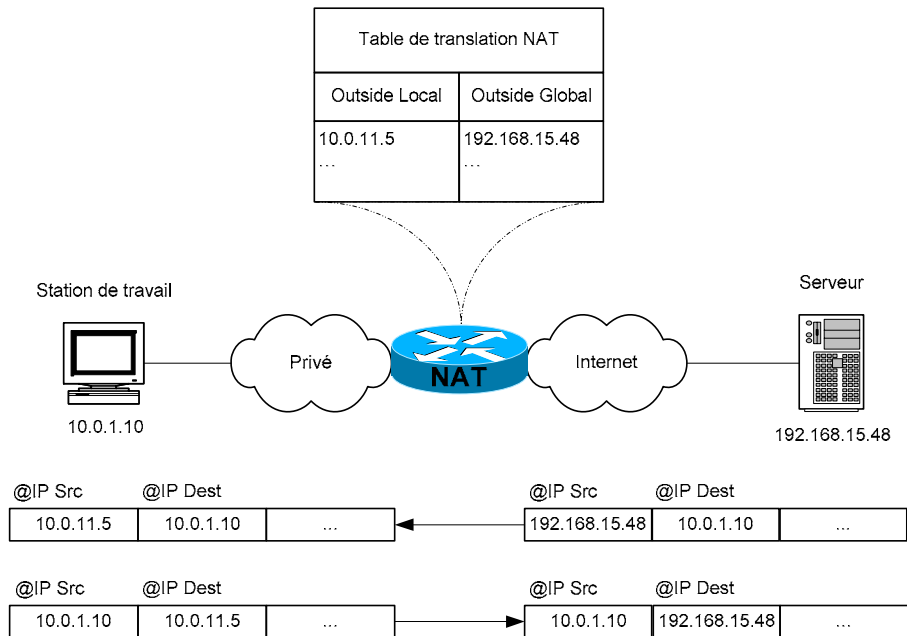
Réponse de 192.168.19.2 : octets=32 temps=16 ms TTL=61
Réponse de 192.168.19.2 : octets=32 temps=16 ms TTL=61
Réponse de 192.168.19.2 : octets=32 temps=16 ms TTL=61
Réponse de 192.168.19.2 : octets=32 temps=16 ms TTL=61

Statistiques Ping pour 192.168.19.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 16ms, Maximum = 16ms, Moyenne = 16ms

C:\>
```

XII.D.5 Configuration du DNAT

- Destination NAT : translation des adresses destination.



- Dans cette configuration, lorsque le routeur reçoit sur son interface 'outside' un datagramme avec pour adresse source 171.16.68.1, l'adresse source est modifiée en 10.10.10.5. De même s'il reçoit sur son interface inside un paquet avec pour adresses destination 10.10.10.5, il translate cette adresse en 171.16.68.1

```
ip nat outside source static 10.0.11.5 192.168.15.48
!
interface Ethernet0
ip address 10.0.1.1 255.255.255.0
ip nat inside
!
interface Serial0
ip nat outside
```

Commande de configuration 'ip nat outside source static'	
<code>ip nat outside source static local-ip global-ip</code>	
<code>ip nat outside source static</code>	Commande de translation de l'adresse IP source de l'outside dans l'inside
<code>local-ip</code>	Adresse 'outside local'
<code>global-ip</code>	Adresse 'outside global'
Exemple	
<code>ip nat outside source static 10.0.11.5 192.168.15.48</code>	

XII.D.6 Configuration d'un Extranet

```

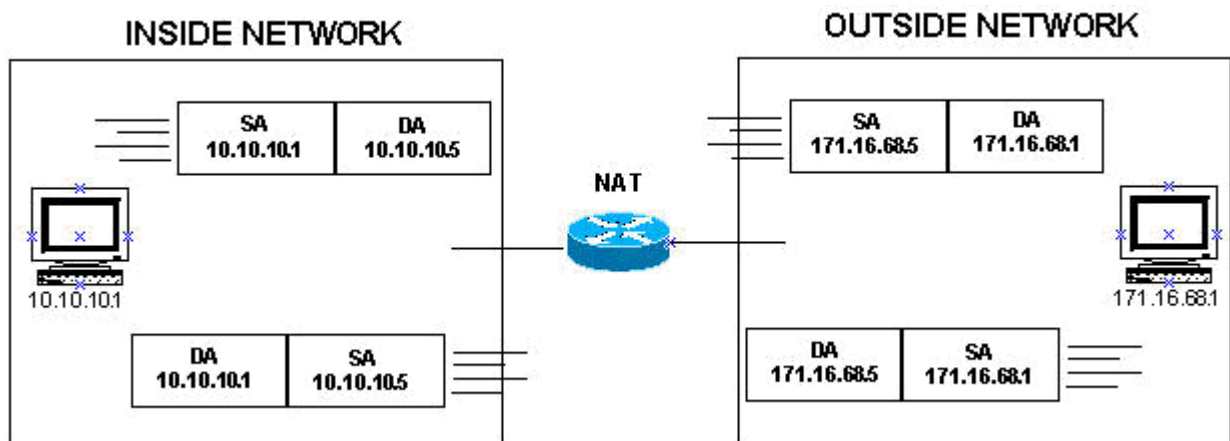
ip nat inside source static 10.10.10.1 171.16.68.5
ip nat outside source static 171.16.68.1 10.10.10.5

interface serial 0
ip nat inside

interface serial 1
ip nat outside

```

- ❑ Dans cette configuration, lorsque le routeur reçoit un paquet sur son interface inside avec comme adresse source 10.10.10.1, l'adresse source est modifiée en 171.16.68.5 et si le routeur reçoit sur son interface outside un paquet avec pour adresse source 171.16.68.1, l'adresse source est modifiée en 10.10.10.5.
- ❑ De même si le routeur reçoit un paquet sur son interface outside avec pour destination 171.16.68.5, l'adresse destination est traduite en 10.10.10.1, s'il reçoit sur son interface inside un paquet avec pour adresse destination 10.10.10.5, il traduit cette adresse en 171.16.68.1



XII.E Configuration du NAT dynamique

XII.E.1 Description

- ❑ En configuration dynamique, c'est le routeur qui crée la table NAT au fur et à mesure que les datagrammes satisfaisant à certaines règles arrivent sur l'interface '*Inside*'.
- ❑ Pour créer des entrées dans la table NAT, le routeur utilise une plage d'adresses connues de l'extérieure mise à sa disposition lors de la configuration. Pour chaque nouvelle entrée, le routeur consomme une adresse IP de la plage allouée dans un ordre croissant. Si cette plage ne contient plus d'adresse disponible, l'entrée dans la table n'est pas créée.

	Commande	Commentaire
1	<code>ip nat pool name-pool start-ip end-ip {netmask netmask prefix-length prefix-length} [type {match-host rotary}]</code>	Définir une plage (pool) d'adresses globales. Les paramètres optionnels : <ul style="list-style-type: none"> ○ [type match-host] vous permet de préserver la partie hôte de l'adresse IP (hostid) lors de l'affectation d'une adresse globale à une adresse locale interne. ○ [type rotary] : Rotary Address Pool
2	<code>access-list access-list-number permit source [source-wildcard]</code>	Création de l'access-list standard qui autorise les machines à accéder au processus NAT.
3	<code>ip nat inside source list access-list-number pool name-pool</code>	Définir la translation
4	<code>interface type number</code>	Configurer l'interface inside
5	<code>ip nat inside</code>	Définir l'interface comme connectée dans l'inside
6	<code>interface type number</code>	Configurer l'interface outside.
7	<code>ip nat outside</code>	Définir l'interface comme connectée dans l'outside

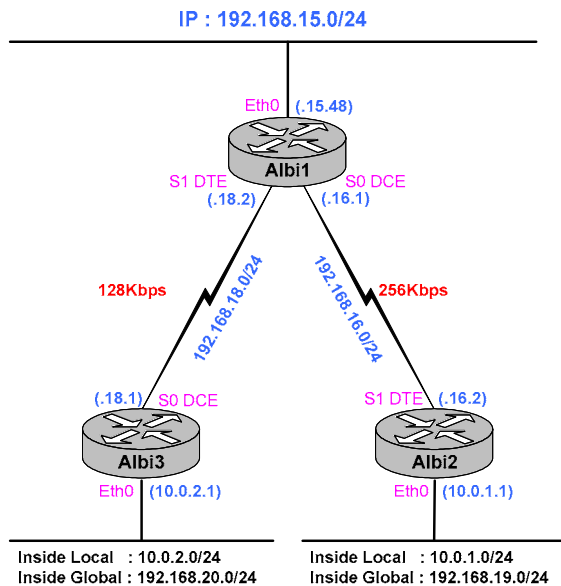
Commande de configuration 'Ip nat pool'	
<code>ip nat pool name start-ip end-ip netmask netmask prefix-length prefix-length type rotary</code>	
<code>ip nat pool name</code>	Définition du groupe d'adresses traduites.
<code>start-ip</code>	Première adresse de l'Outside Global disponible
<code>end-ip</code>	Dernière adresse de l'Outside Global disponible
<code>netmask netmask</code>	Le Subnet Mask
<code>prefix-length prefix-length</code>	Ou le préfixe du Subnet Mask
<code>[type {match-host rotary}]</code>	(option)
Exemple	
<code>ip nat pool dyn-nat 192.168.2.1 192.168.2.254 netmask 255.255.255.0</code>	

Commande de configuration 'ip nat inside source list'	
ip nat inside source list <i>access-list-number</i> <i>pool name-pool</i> [<i>overload</i>]	
ip nat inside source	Commande
list <i>access-list-number</i>	Référence à l'ACL standard qui définit les adresses IP sources a traduité.
pool <i>name-pool</i>	Référence aux adresses de l'outside
[<i>overload</i>]	Activez cette option, si vous disposez d'un nombre insuffisant d'adresses. Quand cette option est active le NAT travaille en PAT.
Exemple	
ip nat inside source list 1 pool net-208 overload	

- L' overload permet la surcharge des adresses globales.

XII.E.2 Application

- Configuration type sur Albi3 (idem sur Albi2).



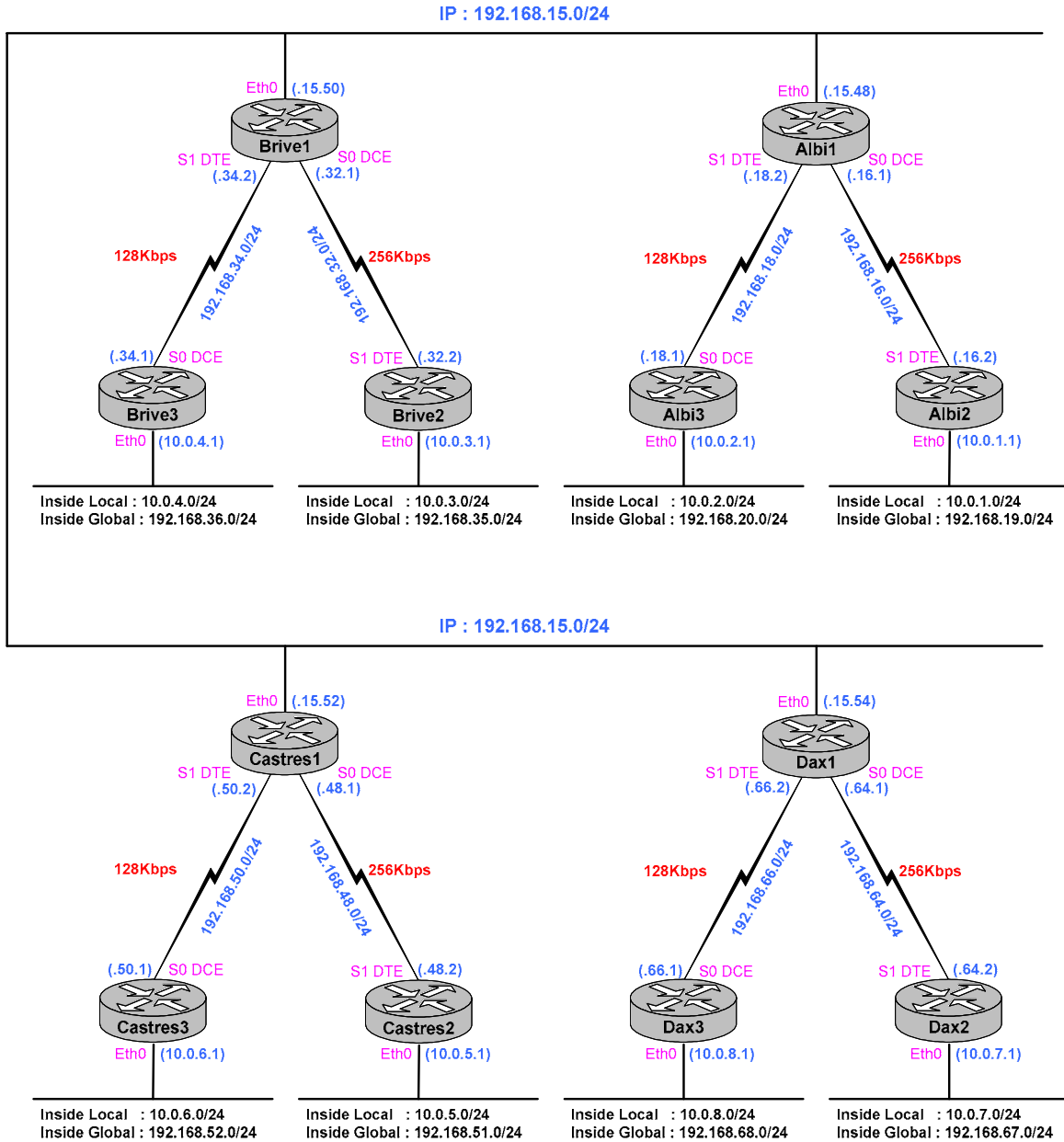
```

ip nat pool dyn-nat 192.168.19.2 192.168.19.254 netmask 255.255.255.0 type match-host
ip nat inside source list 1 pool dyn-nat
!
interface Ethernet0
ip address 10.0.1.1 255.255.255.0
ip nat inside
!
interface Serial0
ip address 192.168.16.2 255.255.255.0
ip nat outside
!
access-list 1 permit 10.0.1.0 0.0.0.255
    
```

Lecture conseillée :

http://www.cisco.com/pcqi-bin/Support/PSP/psp_view.pl?p=Internetworking:NAT

XII.F Maquette des exercices



XII.G Test et Troubleshooting

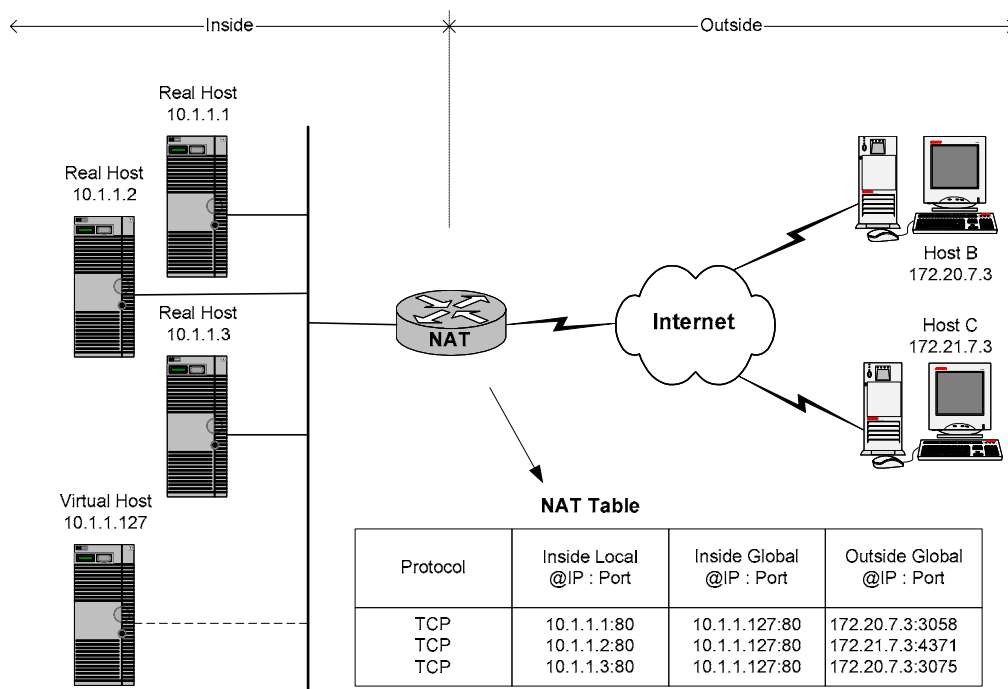
Commandes	Commentaires
Routeur# show ip nat translation [verbose]	Affichage des translations actives
Routeur# show ip nat statistics	Affichage des statistiques de translation
Routeur# debug ip nat [list detailed]	Affichage
Routeur# clear ip nat translation *	Toutes les entrées sont effacées

Effacement des entrées dans la table NAT de translation	
Commandes	Commentaires
Routeur# clear ip nat translation *	Toutes les entrées sont effacées
Routeur# clear ip nat translation inside <i>global-ip local-ip</i> [outside <i>local-ip global-ip</i>]	
Routeur# clear ip nat translation outside <i>local-ip global-ip</i>	
Routeur# clear ip nat translation protocol inside <i>global-ip global-port local-ip local-port</i> [outside <i>local-ip local-port global-ip global-port</i>]	

XII.H Partage de charge TCP

XII.H.1 Description

- ❑ Solution permettant le partage de charge sur plusieurs serveurs offrant un même service plus performant.
- ❑ L'idée pour effectuer cette distribution, les clients se réfèrent à un serveur virtuelle (adresse IP affectée à machine non existante). Le NAT translate l'adresse virtuelle (adresse IP destination) en une adresse correspond à une machine réelle parmi un groupe de serveurs.



- ❑ Cette translation est réalisée uniquement à l'ouverture de session.

XII.H.2 Configuration

- configuration du routeur NAT effectuant le partage de charge.

```

ip nat pool real-hosts 10.1.1.1 10.1.1.3 prefix-length 24 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
interface Serial0
ip address 192.168.18.2 255.255.255.0
ip nat outside
!
access-list 2 permit 10.1.1.127
!
    
```

Commande de configuration 'ip nat pool'	
<code>ip nat pool name start-ip end-ip prefix-length 24 type rotary</code>	
<code>ip nat</code>	Commande affectant les adresses traduites (outside)
<code>pool name</code>	Désigne les adresses a traduites (inside)
<code>start-ip end-ip</code>	Pool d'adresses traduites. Ici sont définis les machines physiques réalisant des tâches de serveurs.
<code>prefix-length 24</code>	Subnet Mask
<code>type rotary</code>	On alterne l'utilisation des différents serveurs pour effectuer le partage de charge
Exemple	
<code>ip nat pool real-hosts 10.1.1.1 10.1.1.3 prefix-length 24 type rotary</code>	

Commande de configuration 'ip nat pool'	
<code>ip nat inside destination list 2 pool name</code>	
<code>ip nat inside</code>	Commande
<code>destination</code>	Ce champ désigne que la translation se fera sur le champ adresse IP destination lors de la requête.
<code>list 2</code>	ACL standard définissant une machine virtuelle permettant le partage de charge. C'est sur cette adresse que les clients accèdent au service réparti sur plusieurs serveurs.
<code>pool name</code>	Référence au pool d'adresses traduites.
Exemple	
<code>ip nat inside destination list 2 pool real-hosts</code>	

XII.H.3 Exemple CISCO

TCP Load Distribution Example

In the following example, the goal is to define a virtual address, connections to which are distributed among a set of real hosts. The pool defines the addresses of the real hosts. The access list defines the virtual address. If a translation does not already exist, TCP packets from serial 0 (the outside interface) whose destination matches the access list are translated to an address from the pool.

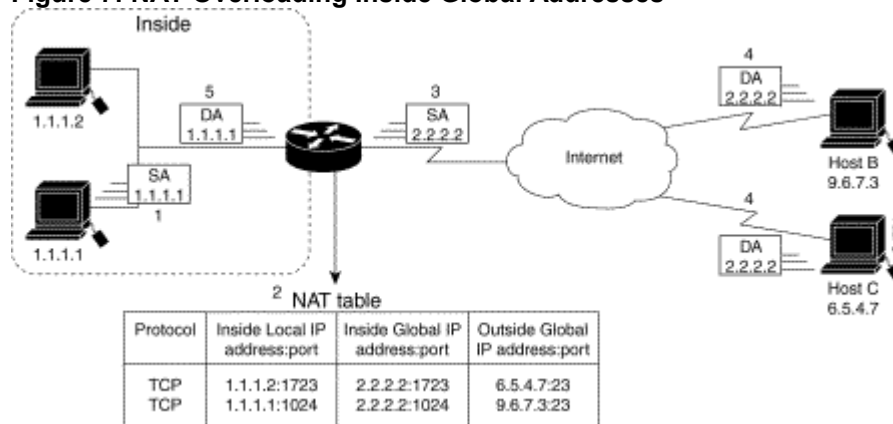
```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
access-list 2 permit 192.168.15.1
```

XII.I Overload an Inside Global Address

You can conserve addresses in the inside global address pool by allowing the router to use one global address for many local addresses. When this overloading is configured, the router maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. When multiple local addresses map to one global address, each the TCP or UDP port numbers of each inside host distinguish between the local addresses.

[Figure 7](#) illustrates NAT operation when one inside global address represents multiple inside local addresses. The TCP port numbers act as differentiators.

Figure 7: NAT Overloading Inside Global Addresses



- The following steps are taken in overloading inside global addresses, as shown in [Figure 7](#). Both Host B and Host C think they are talking to a single host at address 2.2.2.2. They are actually talking to different hosts; the port number is the differentiator. In fact, many inside hosts could share the inside global IP address by using many port numbers.
 - **Step 1** The user at Host 1.1.1.1 opens a connection to Host B.
 - **Step 2** The first packet that the router receives from Host 1.1.1.1 causes the router to check its NAT table.
 - If no translation entry exists, the router determines that address 1.1.1.1 must be translated, and sets up a translation of inside local address 1.1.1.1 to a legal global address. If overloading is enabled, and another translation is active, the router reuses the global address from that translation and saves enough information to be able to translate back. This type of entry is called an *extended entry*.
 - **Step 3** The router replaces the inside local source address 1.1.1.1 with the selected global address and forwards the packet.
 - **Step 4** Host B receives the packet and responds to Host 1.1.1.1 by using the inside global IP address 2.2.2.2.
 - **Step 5** When the router receives the packet with the inside global IP address, it performs a NAT table lookup, using the protocol, inside global address and port, and outside address and port as a key, translates the address to inside local address 1.1.1.1, and forwards the packet to Host 1.1.1.1.
 - **Step 6** Host 1.1.1.1 receives the packet and continues the conversation. The router performs Steps 2 through 5 for each packet.

To configure overloading of inside global addresses, perform the following tasks beginning in global configuration mode:

Task	Command
Define a pool of global addresses to be allocated as needed.	<code>ip nat pool name start-ip end-ip {netmask netmask prefix-length prefix-length}</code>
Define a standard access list.	<code>access-list access-list-number permit source [source-wildcard]</code>
Establish dynamic source translation, identifying the access list defined in the prior step.	<code>ip nat inside source list access-list-number pool name overload</code>
Specify the inside interface.	<code>interface type number</code>
Mark the interface as connected to the inside.	<code>ip nat inside</code>
Specify the outside interface.	<code>interface type number</code>
Mark the interface as connected to the outside.	<code>ip nat outside</code>

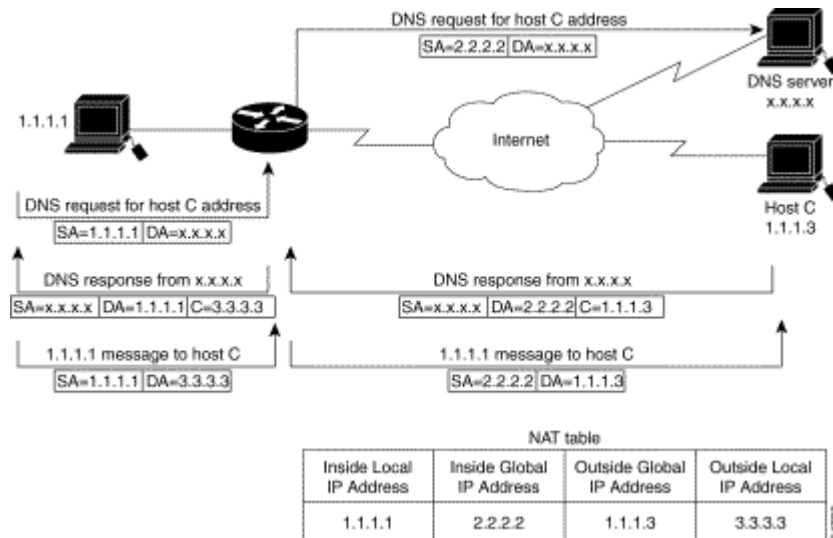
Note The access list must permit only those addresses that are to be translated. (Remember that there is an implicit "deny all" at the end of each access-list.) An access list that is too permissive can lead to unpredictable results.

See the "[Overloading Inside Global Addresses Example](#)" section at the end of this chapter for an example of overloading inside global addresses.

XII.J Overlapping

- L'Overlapping (chevauchement) permet l'interconnexion de deux réseaux ayant les mêmes adresses.

The NAT overview discusses translating IP addresses, perhaps because your IP addresses are not legal, officially assigned IP addresses. Perhaps you chose IP addresses that officially belong to another network. The case of an address used both illegally and legally is called *overlapping*. You can use NAT to translate inside addresses that overlap with outside addresses. Use this feature if your IP addresses in the stub network are legitimate IP addresses belonging to another network, and you want to communicate with those hosts or routers.



The router takes the following steps when translating overlapping addresses:

Step 1 The user at Host 1.1.1.1 opens a connection to Host C by name, requesting a name-to-address lookup from a DNS server.

Step 2 The router intercepts the DNS reply and translates the returned address if there is an overlap (that is, the resulting legal address resides illegally in the inside network). To translate the return address, the router creates a simple translation entry mapping the overlapping address 1.1.1.3 to an address from a separately configured, outside local address pool.

The router examines every DNS reply from everywhere, ensuring that the IP address is not in the stub network. If it is, the router translates the address.

Step 3 Host 1.1.1.1 opens a connection to 3.3.3.3.

Step 4 The router sets up translations mapping inside local and global addresses to each other, and outside global and local addresses to each other.

Step 5 The router replaces the source address with the inside global address, and replaces the destination address with the outside global address.

Step 6 Host C receives the packet and continues the conversation.

Step 7 The router does a lookup, replaces the destination address with the inside local address, and replaces the source address with the outside local address.

Step 8 Host 1.1.1.1 receives the packet and the conversation continues, using this translation process.

XII.J.1 Static

To configure static outside source address translation, perform the following tasks beginning in global configuration mode:

Commande	tâche
<code>ip nat outside source static <i>global-ip local-ip</i></code>	Establish static translation between an outside local address and an outside global address.
<code>interface <i>type number</i></code>	Specify the inside interface.
<code>ip nat inside</code>	Mark the interface as connected to the inside.
<code>interface <i>type number</i></code>	Specify the outside interface.
<code>ip nat outside</code>	Mark the interface as connected to the outside.

XII.J.2 Dynamic

To configure dynamic outside source address translation, perform the following tasks beginning in global configuration mode.

Commande	tâche
<code>ip nat pool <i>name start-ip end-ip</i> {<i>netmask netmask</i> <i>prefix-length prefix-length</i>}</code>	Define a pool of local addresses to be allocated as needed.
<code>access-list <i>access-list-number permit source</i> [<i>source-wildcard</i>]</code>	Define a standard access list.
<code>ip nat outside source list <i>access-list-number pool name</i></code>	Establish dynamic outside source translation, specifying the access list defined in the prior step.
<code>interface <i>type number</i></code>	Specify the inside interface.
<code>ip nat inside</code>	Mark the interface as connected to the inside.
<code>interface <i>type number</i></code>	Specify the outside interface.
<code>ip nat outside</code>	Mark the interface as connected to the outside.

Note The access list must permit only those addresses that are to be translated. (Remember that there is an implicit "deny all" at the end of each access-list.) An access list that is too permissive can lead to unpredictable results.

See the "[Translating Overlapping Address Example](#)" section at the end of this chapter for an example of translating an overlapping address.

XII.J.3 Translating Overlapping Address Example

- In the following example, the addresses in the local network are being used legitimately by someone else on the Internet. An extra translation is required to access that external network. Pool net-10 is a pool of outside local IP addresses. The statement `ip nat outside source list 1 pool net-10` translates the addresses of hosts from the outside overlapping network to addresses in that pool.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface serial 0
ip address 171.69.232.192 255.255.255.240
ip nat outside
!
interface ethernet0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

```
ip nat pool net-2 192.2.2.0 192.2.2.255 prefix-length 24
ip nat pool net-10 192.3.3.0 192.3.3.255 prefix-length 24
ip nat inside source list 1 pool net-2
ip nat outside source list 1 pool net-10

ip nat inside destination list 2 pool real-hosts
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
interface Serial0
ip address 171.69.232.2 255.255.255.0
ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
```

XII.K Routage

- ❑ L'adressage interne (*Inside*) ne doit pas être diffusé vers l'extérieure (*Outside*).
- ❑ L'adressage extérieure (*Outside*) peut être diffusé vers l'interne (*Inside*).

XII.K.1 Statique

- ❑ Aucune différence.

XII.K.2 RIP

- ❑ Pour pouvoir router, il faut créer une interface virtuelle qui représente le réseau vu de l'extérieure.
- ❑ Exemple donné ;
 - Pour Albi1 sans VLSM :

```
router rip
network 192.168.15.0
network 192.168.16.0
network 192.168.18.0
```

- Pour Albi3 sans VLSM :

```
interface Loopback0
ip address 192.168.20.1 255.255.255.0
no ip directed-broadcast
!
router rip
network 192.168.20.0
network 192.168.18.0
```


XII.K.3 EIGRP

```
router eigrp
 network "adresse du réseau externe"
 distribute-list 3 out
 distribute-list 3 in
!
# access-list 3 pour interdire les adresses du réseau interne
access-list 3 deny "adresse du réseau externe" "Subnet Mask du réseau externe"
access-list 3 permit any
```

XII.K.4 OSPF

- ❑ Pour pouvoir router, il faut créer une interface virtuelle qui représente le réseau vu de l'extérieur.

```
interface Loopback0
 ip address 192.168.20.1 255.255.255.0
 no ip directed-broadcast

interface Tunnel0
 ip address 192.168.100.1 255.255.255.0
 tunnel source 192.168.20.1
 tunnel destination 192.168.20.1
```

XIII. HSRP

HSRP : Hot Standby Routing Protocol, RFC 2281

Protocole de haute disponibilité

XIII.A Présentation

- ❑ HSRP (*Hot Standby Routing Protocol*) a été développé par Cisco afin d'améliorer la disponibilité du réseau en assurant la redondance du « prochain saut » (*Next Hop Gateway*).
- ❑ HSRP permet à un routeur A d'effectuer le travail de routage IP d'un routeur B lorsque le routeur B devient indisponible.
- ❑ HSRP est également compatible IPX, Appel Talk et Banyan Vines.

XIII.B Principe de fonctionnement :

- ❑ HSRP fonctionne au-dessus d'UDP en utilisant : le port 1985, l'adresse IP multicast 224.0.0.2 et avec un TTL fixé à 1.
- ❑ Avec HSRP l'adresse Mac et l'adresse IP d'un routeur virtuel sont utilisées. L'adresse Mac virtuelle est reconnaissable : 00:00:0C:07:AC:xx ('xx' indiquant le groupe HSRP).
- ❑ S'il existe plus de deux routeurs, on parlera de MHSRP (*Multi Hot Standby Routing Protocol*).

XIII.C Configuration

- HSRP se configure au niveau d'une interface

Commande	Description
interface ethernet 0	A partir du menu de configuration global, allez dans le menu de configuration de l'interface.
ip address A.B.C.D 255.255.X.X	Définition de l'adresse réelle de l'interface
standby X ip A.B.C.D	Standby : HSRP Interface Configuration Commands <ul style="list-style-type: none"> • 'X' : identifiant du groupe HSRP • 'ip A.B.C.D' : adresse IP du routeur virtuelle HSRP
standby X preempt [delay]	Standby : cde HSRP <ul style="list-style-type: none"> • 'X' = identifiant du groupe HSRP • 'preempt' autorise le fonctionnement HSRP • '[delay]' Wait before preempting
standby X priority Y	Priority 'Y' est le niveau de priorité de l'interface. Le routeur ayant la priorité la plus haute assurera le routage. <ul style="list-style-type: none"> • Valeur de priorité de 0 à 255 • Valeur par défaut : 100 • La valeur '0' indique la plus faible priorité
standby X authentication <i>gefi</i>	Cette commande permet de réaliser l'authentification des messages HSRP.
Standby X timer T U	Définition des « timers » pour les messages de Hello.

- **Note :**
 - La valeur des timers va définir l'intervalle entre les trames de Hello (T) et le délai (U) au bout duquel le routeur de niveau de priorité moins un assurera le routage s'il n'a pas reçu de trame de hello du routeur prioritaire.

Exemple de configuration :

<pre>hostname RouterA ! interface ethernet 0 ip address 172.16.1.2 255.255.255.0 standby 1 ip 172.16.1.1 standby 1 preempt standby 1 priority 150 standby 1 timer 5 10</pre>	<pre>hostname RouterB ! interface ethernet 0 ip address 172.16.1.3 255.255.255.0 standby 1 ip 172.16.1.1 standby 1 preempt standby 1 priority 50 standby 1 timer 5 10</pre>
--	---

- Le routeur A qui assure le routage pour le réseau 172.16.1.0, on dit que c'est le routeur actif. Sa priorité de 150 est supérieure à celle du routeur B qui ne dispose que d'une priorité de 50).
- L'adresse virtuelle est **172.16.1.1**, cette adresse est celle du « default gateway » à configurer sur les stations de ce LAN.
- Dans cet exemple, les routeurs s'échangent un message de « hello » toutes les 5 secondes, le second routeur devient actif s'il n'a pas reçu de messages de « hello » pendant 10 secondes. La commande 'standby timer' doit avoir la même valeur pour tous les routeurs participant à HSRP.
- La commande 'standby preempt' autorise le routeur à devenir actif.
- Lorsque le routeur A devient indisponible c'est le routeur B qui assurera le routage, toujours avec l'adresse IP **172.16.1.1** et l'adresse MAC 00:00:0C:07:AC:01

XIII.D Partage de charge

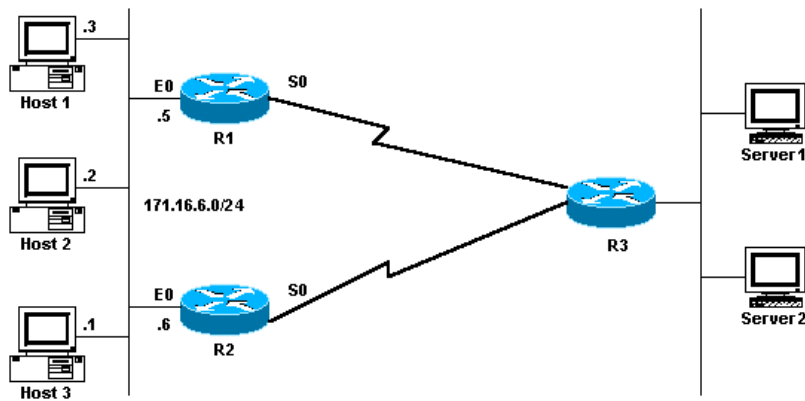
- ❑ Par son fonctionnement, HSRP peut facilement assurer le partage de charge. Il convient alors de configurer correctement deux groupes comme le montre l'exemple suivant.

<pre>hostname RouterA ! interface ethernet 0 ip address 172.16.1.1 255.255.255.0 standby 1 ip 172.16.1.3 standby 1 priority 110 standby 1 preempt standby 2 ip 172.16.1.4 standby 2 preempt</pre>	<pre>hostname RouterB ! interface ethernet 0 ip address 172.16.1.2 255.255.255.0 standby 1 ip 172.16.1.3 standby 1 preempt standby 2 ip 172.16.1.4 standby 2 priority 110 standby 2 preempt</pre>
---	---

- ❑ La moitié des stations du LAN sont configurés avec comme « default gateway » l'adresse du routeur A soit **172.16.1.3**, la seconde moitié utilise celle du routeur B soit **172.16.1.4**.
- ❑ Nous avons deux « Hot Standby Group » **le 1** et **le 2**
- ❑ Si le routeur A devient inutilisable, **le groupe 1 active le routage sur le routeur B**.
- ❑ Si le routeur B devient inutilisable, **le groupe 2 active le routage sur le routeur A**.
- ❑ La valeur par défaut de la priorité est de 100.
- ❑ Noter dans cet exemple le paramétrage de la priorité entre les deux groupes.

Lecture conseillée :

http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Internetworking:HSRP

XIII.E Application**R1 MHSRP Configuration**

Current configuration:

```
interface Ethernet0
  ip address 171.16.6.5 255.255.255.0

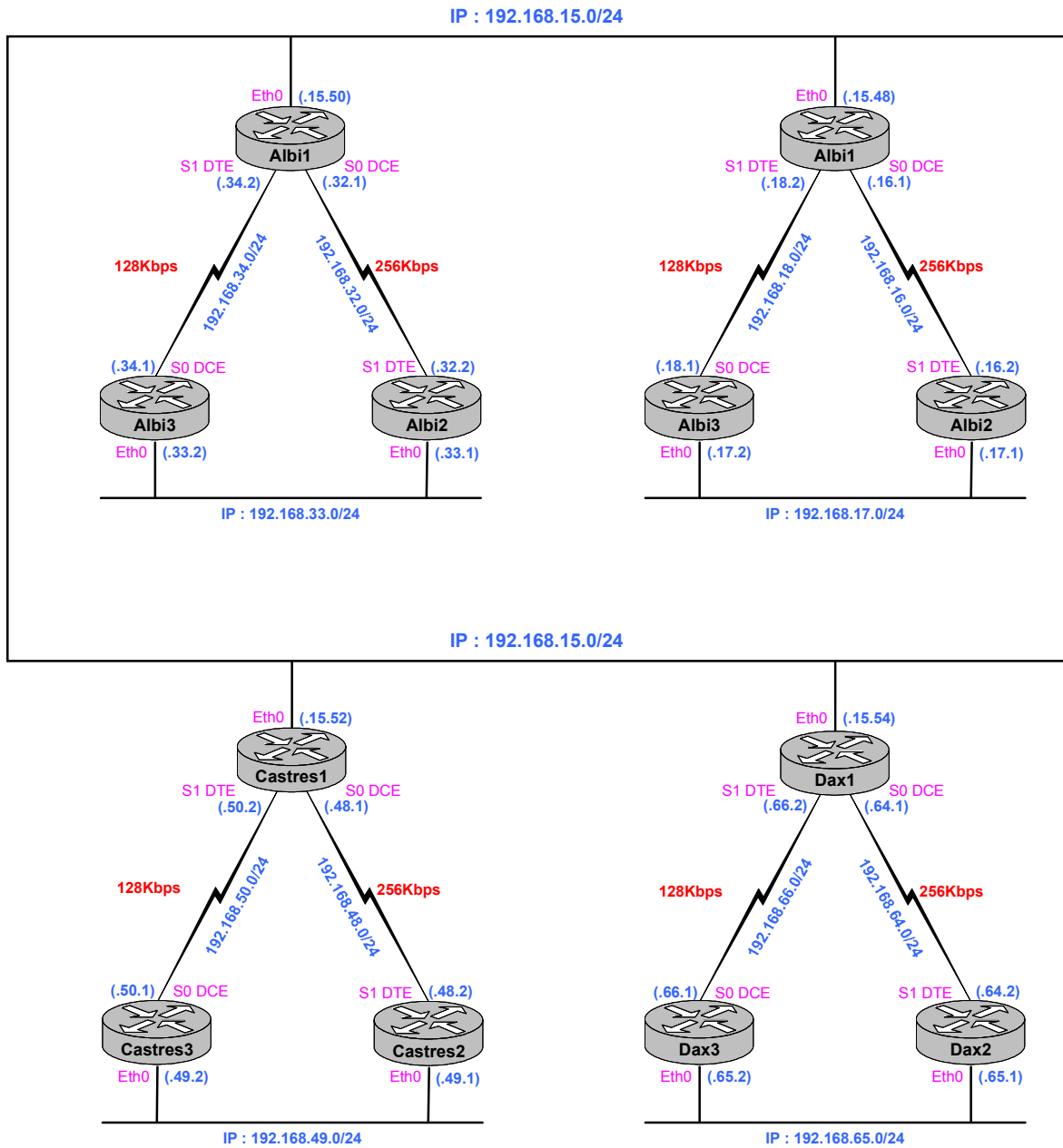
  standby 1 preempt
  standby 1 ip 171.16.6.100
  standby 1 track Serial0
  standby 2 preempt
  standby 2 ip 171.16.6.200
  standby 2 track serial 0
  standby 2 priority 95
```

R2 MHSRP Configuration

Current configuration:

```
interface Ethernet0
  ip address 171.16.6.6 255.255.255.0
  standby 1 preempt
  standby 1 ip 171.16.6.100
  standby 1 track Serial0
  standby 1 priority 95
  standby 2 preempt
  standby 2 ip 171.16.6.200
  standby 2 track serial 0
```

XIII.F Exercice



XIII.G VRRP

VRRP : *Virtual Router Redundancy Protocol*, RFC 2338

XIII.G.1 Présentation

- ❑ Le protocole VRRP reprend les principes du protocole HSRP (RFC 2281) spécifié par CISCO. Le format des paquets est différent, ce qui rend ces deux protocoles incompatibles.
- ❑ VRRP est encapsulé dans IP avec le numéro de protocole 112. Ses paquets sont émis avec l'adresse IP multicast 224.0.0.18, dont l'adresse IP source est la véritable adresse IP du routeur et dont le TTL est fixé à 255. Le tout est transmis dans une trame avec comme adresse MAC source 00-00-5E-00-01-xx où 'xx' représente le numéro d'identification du routeur virtuel (identique au champ 'n°id routeur virtuel' du paquet VRRP).
- ❑ Un même routeur peut participer à plusieurs groupes VRRP et plusieurs groupes VRRP peuvent cohabiter sur un LAN.
- ❑ VRRP intègre l'authentification des messages grâce au support d'IPSEC AH (MD5 HMAC) en plus du mode avec un mot de passe simple.

Protocoles	Encapsulation	Adresse IP	Adresse MAC	TTL
HSRP	UDP/1985	224.0.0.2	00-00-0C-07-AC-xx	1
VRRP	IP/112	224.0.0.18	00-00-5E-00-01-xx	255

XIV. Sécurité

XIV.A Démarche de sécurité

- ❑ Il semble évident de ne pas négliger l'accès physique aux équipements sensibles comme les routeurs, les switches, les serveurs, etc. L'idéal étant de placer ces équipements dans un local dont l'accès est contrôlé. Ne pas négliger les risques de coupure d'électricité, d'incendie et de dégâts des eaux.

- ❑ Il est également indispensable de protéger l'accès logique à ces équipements sensibles, par exemple protection par mot de passe, carte à puce, listes d'accès...

- ❑ Dans une entreprise, la démarche de sécurité doit se baser sur une politique de sécurité, cette politique étant établie en fonction de l'organisation, des processus et des risques.

- ❑ Cette politique va par exemple définir :
 - les moyens :
 - présence d'un serveur d'authentification (Tacacs, Radius ou Kerberos),
 - présence d'un serveur Certificate Authority (CA),
 - mise en place d'une PKI.

 - la manière :
 - par identification et authentification manuelle,
 - par une clé pré partagée (PSK) ou
 - par certificat X509.

 - la périodicité du changement des mots de passe,
 - la manière de les conserver...

XIV.B AAA

XIV.B.1 Présentation

- AAA : Authentication, Authorization and Accounting.
 - **Authentication.** L'authentification permet de vérifier l'identité d'un utilisateur.
 - **Authorization.** Après l'étape d'authentification de l'utilisateur, il s'agit d'assigner un profil d'utilisation ou de droits d'accès à la ressource accédée.
 - **Accounting.** Il s'agit de connaître toutes les actions réalisées par un utilisateur à des fins de comptabilité pour la facturation du service rendu ou à des fins de gestion d'activité.

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

• **Authentication**—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.

All authentication methods, except for local, line password, and enable authentication, must be defined through AAA. For information about configuring all authentication methods, including those implemented outside of the AAA security services, refer to the chapter "Configuring Authentication."

• **Authorization**—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. All authorization methods must be defined through AAA.

As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces. For information about configuring authorization using AAA, refer to the chapter "Configuring Authorization."

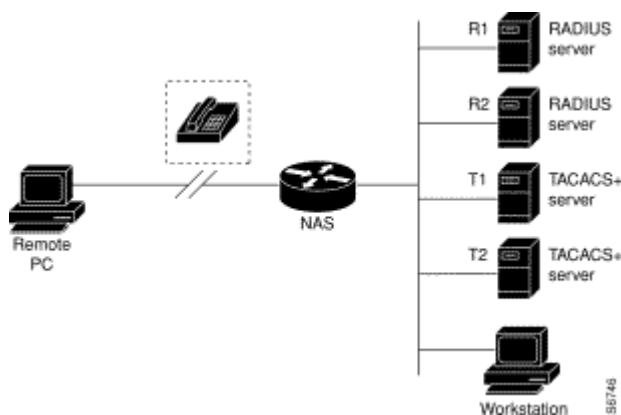
- **Accounting**—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces. For information about configuring accounting using AAA, refer to the chapter "Configuring Accounting."

In many circumstances, AAA uses protocols such as RADIUS, TACACS+, or Kerberos to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS, TACACS+, or Kerberos security server.

Although AAA is the primary (and recommended) method for access control, Cisco IOS software provides additional features for simple access control that are outside the scope of AAA, such as local username authentication, line password authentication, and enable password authentication. However, these features do not provide the same degree of access control that is possible by using AAA.

□ Typical AAA Network Configuration



XIV.B.2 Overview of the AAA Configuration Process

Configuring AAA is relatively simple after you understand the basic process involved. To configure security on a Cisco router or access server using AAA, follow this process:

1. Enable AAA by using the **aaa new-model** global configuration command.
2. If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
3. Define the method lists for authentication by using the **aaa authentication** command.
4. Apply the method lists to a particular interface or line, if required.
5. (Optional) Configure authorization using the **aaa authorization** command.
6. (Optional) Configure accounting using the **aaa accounting** command.

For a complete description of the commands used in this chapter, refer to the "Authentication Commands" chapter of the Security Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Task	Location in Security Configuration Guide	Process Step
Configure local login authentication.	Configuring Authentication	3
Control login using security server authentication.	Configuring Authentication	3
Define method lists for authentication.	Configuring Authentication	3
Apply method lists to a particular interface or line.	Configuring Authentication	3
Configure RADIUS security protocol parameters.	Configuring RADIUS	2
Configure TACACS+ security protocol parameters.	Configuring TACACS+	2
Configure Kerberos security protocol parameters.	Configuring Kerberos	2
Enable TACACS+ authorization.	Configuring Authorization	5
Enable RADIUS authorization.	Configuring Authorization	5
View supported IETF RADIUS attributes.	RADIUS Attributes	2
View supported vendor-specific RADIUS attributes.	RADIUS Attributes	2
View supported TACACS+ AV pairs.	TACACS+ AV Pairs	2
Enable accounting.	Configuring Accounting	6

XIV.B.3 Enable AAA

Before you can use any of the services AAA network security services provide, you need to enable AAA.

To enable AAA, perform the following task in global configuration mode:

Task	Command
Enable AAA.	aaa new-model

Note When you enable AAA, you can no longer access the commands to configure the older deprecated protocols, TACACS or Extended TACACS. If you decided to use TACACS or Extended TACACS in your security solution, do not enable AAA.

XIV.B.4 Disable AAA

You can disable AAA functionality with a single command if, for some reason, you decide that your security needs cannot be met by AAA but can be met by using TACACS, Extended TACACS, or a line security method that can be implemented without AAA.

To disable AAA, perform the following task in global configuration mode:

Task	Command
Disable AAA.	no aaa new-model

XIV.B.5 Authentication

- ❑ L'authentification permet aux administrateurs d'identifier les utilisateurs qui se connecte au équipements (switch & routeur). L'indentification et l'authentification sont réalisées à partir d'une base de données locale ou distante (Tacacs+, Radius ou Kerberos).
- ❑ Normalement, quand un utilisateur se connecte à un équipement Cisco par un terminal ou par Telnet, l'IOS demande uniquement un mot de passe.
- ❑ Avec une authentification AAA, chaque fois qu'un utilisateur se connecte, il doit s'identifier et s'authentifier.

```
Albil#telnet nonAAA-router
User Access Verification
Password: xxxxxx
nonAAA-router>enable
Password: yyyy
nonAAA-router #

Albil#telnet AAA-router
Trying AAA-router (10.1.1.1)... Open User Access Verification
Username: fred
Password: xxxxxx
AAA-router>
```

XIV.B.5.a AAA Authentication General Configuration Procedure

To configure AAA authentication, no matter what method of authentication you select, you need to perform the following tasks:

1. Enable AAA by using the **aaa new-model** global configuration command. For more information about configuring AAA, refer to the "AAA Overview" chapter.
2. Configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos, if you are using a security server. For more information about RADIUS, refer to the "Configuring RADIUS" chapter. For more information about TACACS+, refer to the "Configuring TACACS+" chapter. For more information about Kerberos, refer to the "Configuring Kerberos" chapter.
3. Define the method lists for authentication by using the **aaa authentication** command.
4. Apply the method lists to a particular interface or line, if required.

XIV.B.5.b Configure Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the **aaa authentication login** command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the **aaa authentication login** command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the **login authentication** line configuration command.

To configure login authentication by using AAA, perform the following tasks, beginning in global configuration mode:

Task	Command
Enable AAA globally.	aaa new-model
Create a local authentication list.	aaa authentication login {default list-name}method1 [method2...]
Enter line configuration mode for the lines to which you want to apply the authentication list.	line [aux console tty vty] line-number [ending-line-number]
Apply the authentication list to a line or set of lines.	login authentication {default list-name}

The keyword *list-name* is any character string used to name the list you are creating. The keyword *method* refers to the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following:

```
aaa authentication login default tacacs+ none
```

Note Because the **none** keyword enables *any* user logging in to successfully authenticate, it should be used only as a backup method of authentication.

To create a default list that is used if **no list** is specified in the **login authentication** command, use the **default** argument followed by the methods you want used in default situations. The default method list is automatically applied to all interfaces.

For example, to specify RADIUS as the default method for user authentication during login, enter the following:

```
aaa authentication login default radius
```

Table 4 lists the supported login authentication methods.	
AAA Authentication Login Methods Keyword	Description
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.

radius	Uses RADIUS authentication.
tacacs+	Uses TACACS+ authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router. If selected, this keyword must be listed as the first method in the method list.

XIV.B.5.b.One Login Authentication Using Local Password

Use the **aaa authentication login** command with the **local method** keyword to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter the following:

```
aaa authentication login default local
```

For information about adding users into the local username database, refer to the "[Establish Username Authentication](#)" section in this chapter.

XIV.B.5.b.Two Login Authentication Using Line Password

Use the **aaa authentication login** command with the **line method** keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following:

```
aaa authentication login default line
```

Before you can use a line password as the login authentication method, you need to define a line password. For more information about defining line passwords, refer to the "[Configure Line Password Protection](#)" section in this chapter.

XIV.B.5.b.Trois Login Authentication Using Enable Password

Use the **aaa authentication login** command with the **enable method** keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, enter:

```
aaa authentication login default enable
```

Before you can use the enable password as the login authentication method, you need to define the enable password. For more information about defining enable passwords, refer to the "Configuring Passwords and Privileges" chapter.

XIV.B.5.b.Quatre Login Authentication Using RADIUS

Use the **aaa authentication login** command with the **radius method** keyword to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter:

```
aaa authentication login default radius
```

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the "Configuring RADIUS" chapter.

XIV.B.5.b.Cinq Login Authentication Using TACACS+

Use the **aaa authentication login** command with the **tacacs+ method** keyword to specify TACACS+ as the login authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, enter:

```
aaa authentication login default tacacs+
```

Before you can use TACACS+ as the login authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the "Configuring TACACS+" chapter.

XIV.B.5.b.Six Login Authentication Using Kerberos

Authentication via Kerberos is different from most other authentication methods: the user's password is never sent to the remote access server. Remote users logging in to the network are prompted for a username. If the key distribution center (KDC) has an entry for that user, it creates an encrypted ticket granting ticket (TGT) with the password for that user and sends it back to the router. The user is then prompted for a password, and the router attempts to decrypt the TGT with that password. If it succeeds, the user is authenticated and the TGT is stored in the user's credential cache on the router.

A user does not need to run the KINIT program to get a TGT to authenticate to the router. This is because KINIT has been integrated into the login procedure in the Cisco IOS implementation of Kerberos.

Use the **aaa authentication login** command with the **krb5 method** keyword to specify Kerberos as the login authentication method. For example, to specify Kerberos as the method of user authentication at login when no other method list has been defined, enter:

```
aaa authentication login default krb5
```

Before you can use Kerberos as the login authentication method, you need to enable communication with the Kerberos security server. For more information about establishing communication with a Kerberos server, refer to the "Configuring Kerberos" chapter.

XIV.B.6 Authorization

For authorization configuration examples using the commands in this chapter, refer to the "TACACS+ Configuration Examples" section located at the end of the this chapter.

XIV.B.6.a Configure Authorization

The **aaa authorization** command allows you to set parameters that restrict a user's network access. To enable AAA authorization, perform the following task in global configuration mode:

Task	Command
Set parameters that restrict a user's network access.	aaa authorization { network exec command level } { tacacs+ if-authenticated none local radius krb5-instance }



Note Authorization is bypassed for authenticated users who log in using the console line, even if authorization has been configured.

To enable authorization for all network-related service requests (including SLIP, PPP, PPP NCPs, and ARA protocols), use the **network** keyword. To enable authorization to determine if a user is allowed to run an EXEC shell, use the **exec** keyword.

To enable authorization for specific, individual EXEC commands associated with a specific privilege level, use the **command** keyword. This allows you to authorize all commands associated with a specified command level from 0 to 15.

XIV.B.6.a.Un TACACS+ Authorization

To have the network access server request authorization information via a TACACS+ security server, use the **aaa authorization** command with the **tacacs+ method** keyword. For more specific information about configuring authorization using a TACACS+ security server, refer to the "Configuring TACACS" chapter. For an example of how to enable a TACACS+ server to authorize the use of network services, including PPP and ARA, see the "TACACS+ Authorization Example" section at the end of this chapter.

XIV.B.6.a.Deux If-Authenticated Authorization

To allow users to have access to the functions they request as long as they have been authenticated, use the **aaa authorization** command with the **if-authenticated method** keyword. If you select this method, all requested functions are automatically granted to authenticated users.

XIV.B.6.a.Trois None Authorization

To perform no authorization for the actions associated with a particular type of authentication, use the **aaa authorization** command with the **none method** keyword. If you select this method, authorization is disabled for all actions.

XIV.B.6.a.Quatre Local Authorization

To select local authorization, which means that the router or access server consult its local user database to determine the functions a user is permitted, use the **aaa authorization** command with the **local method** keyword. The functions associated with local authorization are defined by using the **username** global configuration command. For a list of permitted functions, refer to the "Configuring Authentication" chapter.

XIV.B.6.a.Cinq RADIUS Authorization

To have the network access server request authorization via a RADIUS security server, use the **aaa authorization** command with the **radius method** keyword. For more specific information about configuring authorization using a RADIUS security server, refer to the "Configuring RADIUS" chapter. For an example of how to enable a RADIUS server to authorize services, see the "RADIUS Authorization Example" section at the end of this chapter.

XIV.B.6.a.Six Kerberos Authorization

To run authorization to determine if a user is allowed to run an EXEC shell at a specific privilege level based on a mapped Kerberos instance, use the **krb5-instance method** keyword. For more information, refer to the "Enable Kerberos Instance Mapping" section of the "Configuring Kerberos" chapter. For an example of how to enable Kerberos instance mapping, see the "Kerberos Instance Mapping Examples" section at the end of this chapter.

XIV.B.6.b Disable Authorization for Global Configuration Commands

The **aaa authorization** command with the keyword **command** attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using **no aaa authorization config-commands** stops the network access server not from attempting configuration command authorization. To disable AAA authorization for all global configuration commands, perform the following task in global configuration mode:

Task	Command
Disable authorization for all global configuration commands.	no aaa authorization config-command

XIV.B.7 Accounting

XIV.B.7.a Enable Accounting

The **aaa accounting** command enables you to create a record for any or all of the accounting functions monitored. To enable AAA accounting, perform the following task in global configuration mode:

Task	Command
Enable accounting.	aaa accounting { system network connection exec command <i>level</i> } { start-stop wait-start stop-only } { tacacs+ radius }

For minimal accounting, use the **stop-only** keyword, which instructs the specified authentication system (RADIUS or TACACS+) to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the **start-stop** keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. You can further control access and accounting by using the **wait-start** keyword, which ensures that the RADIUS or TACACS+ security server acknowledges the start notice before granting the user's process request.

XIV.B.7.a.One Suppress Generation of Accounting Records for Null Username Sessions

When **aaa accounting** is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. An example of this is users who come in on lines where the **aaa authentication login method-list none** command is applied. To prevent accounting records from being generated for sessions that do not have usernames associated with them, perform the following task in global configuration mode:

Task	Command
Prevent accounting records from being generated for users whose username string is NULL.	aaa accounting suppress null-username

XIV.B.7.a.Deux Generate Interim Accounting Records

To enable periodic interim accounting records to be sent to the accounting server, perform the following task in global configuration mode:

Task	Command
Enable periodic interim accounting records to be sent to the accounting server.	aaa accounting update { newinfo periodic number }

When the **aaa accounting update** command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword **newinfo** is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example of this would be when IPCP completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.

When used with the keyword **periodic**, interim accounting records are sent periodically as defined by the argument number. The interim accounting record contains all of the accounting information recorded for that user up to the time the interim accounting record is sent.

Both of these keywords are mutually exclusive, meaning that whichever keyword is configured last takes precedence over the previous configuration. For example, if you configure **aaa accounting update periodic**, and then configure **aaa accounting update newinfo**, all users currently logged in will continue to generate periodic interim accounting records. All new users will generate accounting records based on the **newinfo** algorithm.



Caution Using the **aaa accounting update periodic** command can cause heavy congestion when many users are logged in to the network.

XIV.B.7.b Monitor Accounting

No specific **show** command exists for either RADIUS or TACACS+ accounting. To obtain accounting records displaying information about users currently logged in, perform the following task in Privileged EXEC mode:

Task	Command
Step through all active sessions and print all the accounting records for the actively accounted functions.	show accounting

XIV.B.7.b.Un Accounting Attribute-Value Pairs

The network access server monitors the accounting functions defined in either TACACS+ attribute/value (AV) pairs or RADIUS attributes, depending on which security method you have implemented. For a list of supported RADIUS accounting attributes, refer to the "RADIUS Attributes" appendix in the *Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the "TACACS+ AV Pairs" appendix in the *Security Configuration Guide*.

XIV.B.7.b.Deux Accounting Configuration Example

In the following sample configuration, RADIUS-style accounting is used to track all usage of EXEC commands and network services, such as SLIP, PPP, and ARAP:

```
aaa accounting exec start-stop radius
aaa accounting network start-stop radius
```

The **show accounting** command yields the following output for the above configuration:

```
Active Accounted actions on tty0, User georgef Priv 1
Task ID 2, EXEC Accounting record, 00:02:13 Elapsed
task_id=2 service=shell
Task ID 3, Connection Accounting record, 00:02:07 Elapsed
task_id=3 service=connection protocol=telnet address=172.21.14.90 cmd=synth
Active Accounted actions on tty1, User rubble Priv 1
Task ID 5, Network Accounting record, 00:00:52 Elapsed
task_id=5 service=ppp protocol=ip address=10.0.0.98
Active Accounted actions on tty10, User georgef Priv 1
Task ID 4, EXEC Accounting record, 00:00:53 Elapsed
task_id=4 service=shell
```

[Table 9](#) describes the fields contained in this example.

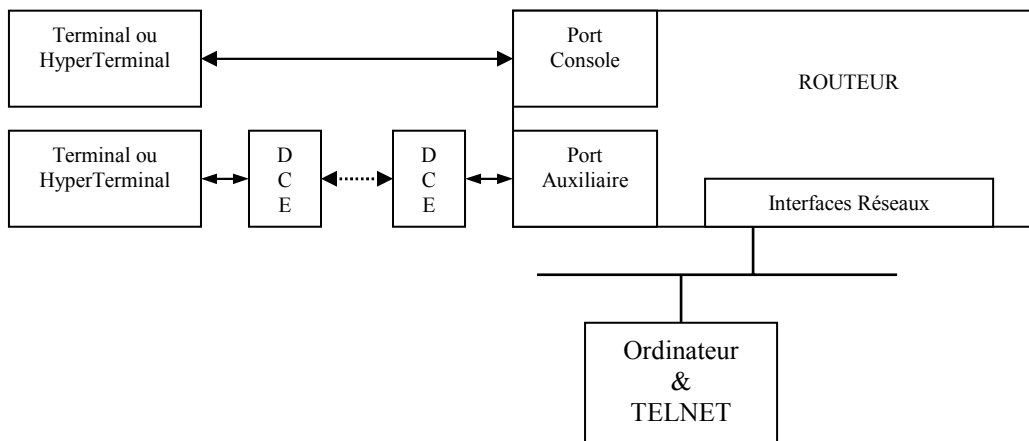
Table 9: Show Accounting Field Descriptions	
Field	Description
Active Accounted actions on	Terminal line or interface name user with which the user logged in.
User	User's ID
Priv	User's privilege level.
Task ID	Unique identifier for each accounting session.
Accounting Record	Type of accounting session.
Elapsed	Length of time (hh:mm:ss) for this session type.
attribute=value	AV pairs associated with this accounting session.

XIV.C Configuration de l'accès

- ❑ L'IOS Cisco permet à l'administrateur de choisir entre différentes solutions d'identification locales ou centralisées.

XIV.C.1 Configuration par défaut

- ❑ L'accès à l'interface CLI peut nécessiter la saisie de mots de passe. Il existe 3 modes de connexion au routeur avec éventuellement des mots de passe différents, ces mots de passe ont habituellement la même valeur.



Accès à partir	Type de mot de passe	procédure
Port Console	Mot de passe de console	C2514# conf t C2514(config)# line console 0 C2514(config-line)# login C2514(config-line)# password mot_de_passe
Port Auxiliaire	Mot de passe auxiliaire	C2514# conf t C2514(config)# line aux 0 C2514(config-line)# login C2514(config-line)# password mot_de_passe
TELNET	Mot de passe VTY	C2514# conf t C2514(config)# line vty 0 4 C2514(config-line)# login C2514(config-line)# password mot_de_passe
	Mode ENABLE (#)	C2514(config)# enable secret mot_de_passe

- ❑ *Note* : plusieurs connexions telnet sont possibles simultanément, correspondant aux terminaux virtuels (VTY) 0 à 4.
- ❑ Quelle que soit le mode de connexion l'interface utilisateur est place en mode EXEC, ce qui signifie que les commandes saisies dans ce mode sont exécutées.
- ❑ Il existe deux modes EXEC :
 - le mode utilisateur,
 - le mode privilégié ou mode « enable » en raison de la commande utilisée pour accéder à ce mode.
- ❑ Le mode privilégié permet d'accéder à des commandes plus puissantes comme, par exemple les commandes de configuration de l'équipement.
- ❑ Le mot de passe est un des moyens de contrôler l'accès aux équipements et le passage en mode 'enable'.

XIV.C.2 Chiffrement du mot de passe

- ❑ Utiliser le service 'password encryption' afin que les mots de passe n'apparaissent pas en clair dans les fichiers de configuration.

```
service password-encryption
```

- ❑ Le cryptage des mots de passe de premier niveau ou du mot de passe « enable » (Enable Password) est facilement décryptable.
- ❑ Il est conseillé d'utiliser 'enable secret' plutôt qu' 'enable password' dont le niveau de cryptages est supérieur.
- ❑ La différence entre ces deux commandes réside dans l'algorithme employé pour chiffrer le mot de passe ou le secret.
- ❑ La commande 'enable password' utilise un algorithme de cryptage réversible, signalé par le chiffre 7.
- ❑ Le secret du mode 'enable secret' est chiffré au moyen de l'algorithme MD5, signalé par le chiffre 5. Cet algorithme n'est pas réversible (hash) et offre donc une meilleure sécurité.
- ❑ Si vous configurez les deux commandes, 'enable secret' sera prioritaire.
- ❑ De plus, il est conseillé de paramétrer un 'enable password' si la version de 'boot' est trop ancienne, sinon en mode 'boot' il serait impossible de passer au niveau 'Enable'.

XIV.C.3 Authentification locale

- ❑ Cette méthode appelée « Local » permet de configurer une base utilisateurs sur le routeur.
- ❑ Elle permet également de définir le niveau (0 à 15 ou 15 correspond au « Mode Enable ») accordé à l'utilisateur. Une commande EXEC peut être prédéfinie et exécutée automatiquement après l'authentification.
- ❑ Ce type d'utilisateur est nécessaire pour les authentifications de type PAP ou CHAP, que nous étudieront PAP et CHAP plus tard.

Exemple :

```
Switch# username superuser password superpassword  
Switch# username who nopassword nohangup autocommand show users
```

- ❑ Il est déconseillé d'utiliser un login avec username de niveau « enable ». Le mot de passe est trop facilement décryptable.

XIV.C.4 Utilisation d'un serveur d'Authentification

- ❑ Il est toutefois possible de gérer les utilisateurs de façon centralisée. On utilise pour cela un serveur de type AAA (*authentification, autorisation, accounting*).
- ❑ Les équipements Cisco permettent l'utilisation de serveurs de type Tacacs, Radius et Kerberos.
- ❑ Configuration de AAA pour un équipement Cisco (type routeur ou switch (IOS)) utilisant un serveur TACACS.

Exemple de configuration :

```
tacacs-server host 192.168.3.18
tacacs-server key ciscomania

aaa new-model
aaa authentication password-prompt Local_Password:
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 15 default tacacs+ if-authenticated
aaa authorization commands 0 default tacacs+ if-authenticated
aaa accounting exec default start-stop tacacs+
aaa accounting commands 0 default start-stop tacacs+
aaa accounting commands 1 default start-stop tacacs+
aaa accounting commands 15 default start-stop tacacs+
aaa accounting connection default start-stop tacacs+
aaa accounting system default start-stop tacacs+
```

Le détail des commandes :

Commande	Description
<code>tacacs-server host 192.168.3.18</code>	Définit le host 192.168.3.18 comme serveur Tacacs.
<code>tacacs-server key ciscomania</code>	Active le chiffrement du champ donnée et définit la clé de chiffrement des messages Tacacs.
<code>aaa new-model</code>	Initialise le mode AAA. La commande <code>no aaa new-model</code> supprime toutes les commandes aaa
<code>aaa authentication password-prompt Local_Password:</code>	Définit le prompt en cas de non fonctionnement du serveur.
<code>aaa authentication login default tacacs+ enable</code>	Définit le mode d'authentification, Tacacs en premier, si le serveur ne répond pas c'est le mot de passe Enable qui doit être utilisé. En indiquant LINE on utiliserait le mot de passe des VTY.
<code>aaa authentication enable default tacacs+ enable</code>	On définit le mode d'authentification pour accéder au mode enable (comme la commande ci-dessus).
<code>aaa authorization commands 15 default tacacs+ if-authenticated</code>	L'équipement vérifiera les autorisations de l'utilisateur sur le serveur, pour les commandes du niveau 15. En cas de non réponse il acceptera les commandes d'un utilisateur authentifié.
<code>aaa accounting exec default start-stop tacacs+</code>	Les commandes «exec» seront journalisées sur le serveur.

Précautions pour la configuration :

- ❑ *La procédure de configuration conseillée est la suivante :*
 - Définir dans un premier temps le serveur et sa clé.
 - Paramétrer l'authentification, tester son fonctionnement depuis une seconde session telnet, ce afin de se prévoir un retour arrière.
 - Paramétrer les autorisations, à partir de la seconde connexion qui est authentifiée.
 - Terminer par l'accounting.
 - Enregistrer la configuration (`# copy run start`) quand tout fonctionne correctement.
- ❑ Si l'équipement n'est pas sur le même site on peut s'assurer de pouvoir reprendre la main en cas d'erreur, en paramétrant un «`reload in hh:mn`» ou un «`reload at hh:mn`» (s'assurer de la mise à l'heure de l'équipement). S'assurer cependant de ne pas perturber les utilisateurs du réseau.

XIV.C.5 Configuration du serveur TACACS+ Freeware

TACACS : Terminal Access Controller Access Control System

XIV.C.5.a Présentation

- ❑ Le protocole TACACS+ est la dernière version du protocole TACACS. Développé à l'origine par BBN pour le MILNET, puis repris par Cisco, il a été étendu une première fois avec XTACACS (eXtended TACACS), compatible avec TACACS, pour finir par TACACS+.
- ❑ TACACS est un protocole de contrôle d'accès simple.
- ❑ TACACS+ utilise le port TCP 49, contrairement à TACACS qui s'appuie sur UDP.

Différences fondamentales	
TACACS	Combine l'authentification et le processus d'autorisation
XTACACS	Sépare l'authentification, l'autorisation et la comptabilité
TACACS+	Ressemble à XTACACS avec un contrôle d'attributs et une comptabilité étendus.

- ❑ Le fichier de configuration du serveur Tacacs est le fichier `/etc/tacacs/tac_plus.cfg`.
- ❑ Les principales variables de ce fichier sont :
 - Key : la clé, une chaîne de caractères, commune au serveur et aux équipements clients.
 - Le fichier d'accounting, c'est dans ce fichier que la log sera sauvegardée (`/var/log/account.log`).
- ❑ Voir aussi :
 - Pour plus d'info utilisez `'man tac_plus'`.
 - Le User's Guide Tac_plus

XIV.C.5.b Installation

- ❑ L'exemple suivant fonctionne sous une station Linux Mandrake, le RPM Tacacs est installé à partir de : <http://rpmfind.net> sur le site <http://rpmfind.net>.
- ❑ Installation : `# rpm -ivh tac_plus-4.0.3-2.i386.rpm`.
- ❑ Les scripts de démarrage sont installés mais non vu par la commande `'chkconfig -- list'`.

XIV.C.5.c Configuration

- le fichier de configuration type : `‘/etc/tacacs/tac_plus.cfg’`

```
# On définit la clé tacacs qui doit être identique à celle du routeur
key = ciscomania

# on définit le fichier d'accounting
accounting file = /var/log/account.log

# on définit le mot de passe Enable
user = $enable$ {
    login = des E9LW72xjYH.26
    # member = 0
    name = "Do Not Delete!"
}

#on définit les utilisateurs avec les mots de passé en clair ou cryptés DES
user = dom {
    default service = permit
    login = des dfNH0QilBYqpM
}

user = student {
    default service = permit
    login = cleartext "gefi"
}

#on peut donner une date d'expiration du compte utilisateur
user=fred {
    expires = "mai 20 2001"
    login = cleartext "admin"
}
```

- Utilisez le programme `‘/usr/sbin/generate_passwd’` pour créer le mot de passe *Enable* chiffré DES dans `‘login = des E9LW72xjYH.26’`

```
[root@c18724root]$ /usr/local/sbin/generate_passwd
Password to be encrypted: cisco
E9LW72xjYH.26
```

❑ Fichier de configuration amélioré

- génération du mot de passe pour le compte Enable.

```
[root@ci18724root]$ /usr/local/sbin/generate_passwd
Password to be encrypted: cisco
E9LW72xjYH.26
```

- le fichier de configuration correspondant : '/etc/tacacs/tac_plus.cfg'

```
key = ciscomania
accounting file = /var/log/account.log

user=root {
  default service = permit
  service = exec {
    priv-lvl = 15
  }
  cmd = configure {
    deny aaa.*
    permit .*
  }
  login = des "E9LW72xjYH.26"
}
```

- 'User' : le login de l'utilisateur.
- 'Default Service' : ce qui sera permit.
- 'Service = exec{ priv-lvl = 15 }' permet de configurer le niveau de l'utilisateur 0 à 15, 15 étant le niveau 'enable'.
- Cmd, les commandes autorisées ou interdites.
- Login correspondant au mot de passe du compte, nous utiliserons un mot de passe crypté des plus sûr que le mot de passe en clair. Pour obtenir le cryptage à partir du mot de passe en clair on utilise l'utilitaire '/usr/sbin/generate_passwd' comme suit :

XIV.C.5.d Lancement

□ Démarrage du service

- Le service est démarré par le script `‘/etc/rc.d/init.d/tacacs {start | stop | restart | status}’`.
- L'option de démarrage du daemon utilisé par ce script est `‘-C /etc/tacacs/tac_plus.cfg’`, cette option précise le fichier de configuration à utiliser.
- D'autres options sont disponibles :
 - `‘-t’` pour passer en mode debug.

XIV.C.5.e Accounting

Exemple de fichier de journalisation de l'accounting :

```
[root@c18724 root]$ more /var/log/account.log
Mon Nov 5 10:22:57 2001 140.6.48.8 dom tty1 140.6.48.100 stop task_id=26 timezone=UTC
service=shell priv-lvl=15 cmd=show running-config <cr>
Mon Nov 5 10:23:11 2001 140.6.48.8 dom tty1 140.6.48.100 stop task_id=27 timezone=UTC
service=shell priv-lvl=15 cmd=configure terminal <cr>
Mon Nov 5 10:23:37 2001 140.6.48.8 dom tty1 140.6.48.100 stop task_id=28 timezone=UTC
service=shell priv-lvl=15 cmd=no tacacs-server host 172.17.48.100 <cr>
```

- ❑ La fonction 'lock & key' permet d'activer ou de désactiver des ACL dynamiques.

```
#exemple d'utilisateur pour la fonction lock & key
user = acl {
    login = cleartext "acl"
    service = exec {autocmd = "access-enable timeout 120"}
}

#exemple d'utilisateur pour l'autorisation
user=invite {
    default service = permit

# le telnet est permit à fred sauf pour les adresses 192.168.3.*
    cmd = telnet {
        deny 192\.168\.3\.[0-9]+
        permit .*
    }

#les commandes de visualisations sont permises sauf show interfaces

    cmd = show {
        deny interface
        permit .*
    }

#les commandes de configurations sont interdites
    cmd = configure {
        deny .*
    }
login = des dfNH0QilBYqpM
}
```

- ❑ Lecture conseillée :
 - http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Internetworking:Tacacs_plus

XIV.D TACACS+ Freeware for First-Time Users

- ❑ Référence : http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800946a3.shtml
- ❑ Document ID: 13865
- ❑ Cisco no longer maintains or updates this document. Though the document resides on Cisco.com, Cisco cannot guarantee the document's accuracy. Please consider this fact if you decide to use this information for support purposes.

XIV.D.1 Introduction

- ❑ The following information describes how to configure a Cisco router for authentication with the TACACS+ freeware that runs on UNIX; installing the freeware requires use of a C-compiler. As noted in the TACACS+ freeware Users' Guide, the freeware code does not come with any warranty or support. It does not offer as many features as our commercially available Cisco Secure ACS for Windows or Cisco Secure ASC UNIX.
- ❑ The TACACS+ freeware can be obtained through FTP: <ftp://anonymous@ftp-eng.cisco.com/pub/tacacs/>
- ❑ You can also obtain the freeware from the command-line interface (CLI) by anonymous ftp to ftp-eng.cisco.com.
- ❑ The router configuration below was developed on a router running Cisco IOS Software Release 11.3.3; Cisco IOS 12.0.5.T and later uses **group tacacs+** instead of **tacacs+**, so statements such as **aaa authentication login default tacacs+ enable** would appear as **aaa authentication login default group tacacs+ enable**.
- ❑ For more complete information on router commands, see the [Cisco IOS Software documentation](#).
- ❑ Tacacs+ utilise deux fichiers:
 - To see router-to-server interaction at the server, type:

```
tail -f /var/tmp/tac_plus.log
```
 - With TAC+ running on the server, to see the entries going into the **accounting** file, enter on the server:

```
tail -f /var/log/tac.log
```


XIV.D.2 Authentication

1. Make sure you have compiled TACACS+ (TAC+) code on the UNIX server. The server configurations here assume you are using the Cisco TAC+ server code; the router configurations should work whether or not the server code is Cisco's. TAC+ must be run as root; **su** to root if necessary.
2. Copy the [test file](#) at the end of this document, place it on the TAC+ server, and name it "test_file". Check to be sure the **tac_plus_executable** daemon starts with **test_file**; in the following command, the **-P** option checks for compile errors but does *not* start the daemon:

```
tac_plus_executable -P -C test_file
```

You may see the contents of test_file scroll down the screen, but you should not see messages such as "cannot find file", "cleartext expected--found cleartext", or "unexpected }". If there are errors, check paths to **test_file**, re-check your typing, and re-test before continuing.

3. On the router, start configuring TAC+.

Enter **enable** mode and type **conf t** before the command set.

The following syntax ensures that you will not be locked out of the router initially, providing the **tac_plus_executable** is not running:

```
!--- Turn on TAC+
aaa new-model
enable password whatever
!--- These are lists of authentication methods.
!--- "linmethod", "vtymethod", "conmethod", and
!--- so on are names of lists, and the methods
!--- listed on the same lines are the methods
!--- in the order to be tried. As used here, if
!--- authentication fails due to the
!--- tac_plus_executable not being started, the
!--- enable password will be accepted because
!--- it is in each list.
!
aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable
aaa authentication login conmethod tacacs+ enable
!
!--- Point the router to the server, where #.#.#.#
!--- is the server IP address.
!
tacacs-server host #.#.#.#
line con 0
password whatever
!--- No time-out to prevent being locked out
!--- during debugging.
exec-timeout 0 0
login authentication conmethod
line 1 8
login authentication linmethod
modem InOut
transport input all
rxspeed 38400
txspeed 38400
flowcontrol hardware
line vty 0 4
password whatever
!--- No time-out to prevent being locked out
!--- during debugging.
exec-timeout 0 0
login authentication vtymethod
```

4. Test to be sure you can still access the router with Telnet and through the console port before continuing. Because the **tac_plus_executable** is not running, the enable password should be accepted.

Note: Keep the console port session active and remain in **enable** mode; this session should not time out. We are starting to limit access to the router at this point, and you need to be able to make configuration changes without locking yourself out.

To see server-to-router interaction at the router, issue the following commands:

```
terminal monitor
debug aaa authentication
```

5. As root, start TAC+ on the server:

```
tac_plus_executable -C test_file -d 16
```

6. Check to be sure TAC+ started:

```
ps -aux | grep tac_plus_executable
```

Or,

```
ps -ef | grep tac_plus_executable
```

If TAC+ does not start, it is usually a problem with syntax in the `test_file`. Return to Step 1 to correct.

7. To see router-to-server interaction at the server, type:

```
tail -f /var/tmp/tac_plus.log
```

Note: The **-d 16** option in Step 5 sends output of all transactions to the **/var/tmp/tac_plus.log**.

8. Telnet (VTY) users should now have to authenticate through TAC+.

With debug going on the router and the server (steps 4 and 7), telnet into the router from another part of the network.

The router should produce a **username** and **password** prompt, to which you reply:

```
'authenuser' (username from test_file)
'admin' (password from test_file)
```

where user 'authenuser' is in group 'admin', which has password 'admin'.

Watch the server and the router where you should see the TAC+ interaction—what's being sent where, responses, requests, and so on. Correct any problems before continuing.

9. If you also want your users to authenticate through TAC+ to get into **enable** mode, make sure your console port session is still active and add the following command to the router:

```
!--- For enable mode, list 'default' looks to TAC+
!--- then enable password if TAC+ not running
aaa authentication enable default group tacacs+ enable
```

Users should now have to *enable* through TAC+.

10. With debug going on the router and the server (steps 4 and 7), telnet into the router from another part of the network. The router should produce a **username** and **password** prompt, to which you reply:

```
'authenuser' (username from test_file)
'admin' (password from test_file)
```

When entering **enable** mode, the router will request a password, to which you reply:

```
'cisco' ($enable$ password from test_file)
```

Watch the server and the router where you should see the TAC+ interaction – what's being sent where, responses, requests, and so on. Correct any problems before continuing.

11. Bring down the TAC+ process on the server while still connected to the console port to be sure that your users can still access the router if TAC+ is down:

```
ps -aux | grep tac_plus_executable  
Or,  
ps -ef | grep tac_plus_executable)  
kill -9 pid_of_tac_plus_executable
```

Repeat the Telnet and enable of the previous step. The router should realize that the TAC+ process is not responding and allow users to log in and enable with the default passwords.

12. Check for authentication of your console port users through TAC+ by bringing up the TAC+ server again (steps 5-6), and establishing a Telnet session to the router (which should authenticate through TAC+).

Remain connected through Telnet into the router in **enable** mode until you are sure you can log in to the router through the console port.

Log out of your original connection to the router through the console port, then reconnect to the console port. Console port authentication to log in and enable using userIDs and passwords (shown in step 10) should now be through TAC+.

13. While remaining connected through either a Telnet session or the console port and with debug going on the router and the server (steps 4 and 7), establish a modem connection to line 1.

Line users should now have to log in and enable through TAC+.

The router should produce a **username** and **password** prompt, to which you reply:

```
'authenuser' (username from test_file)  
'admin' (password from test_file)
```

When entering **enable** mode, the router will request a password.

Reply:

```
'cisco' ($enable$ password from test_file)
```

Watch the server and the router where you should see the TAC+ interaction – what's being sent where, responses, requests, etc. Correct any problems before continuing.

Users should now have to *enable* through TAC+.

XIV.D.3 Adding Authorization

By default, there are 3 command-levels on the router:

- privilege level 0 which includes disable, enable, exit, help, and logout
- privilege level 1 - normal level on a telnet - prompt says `router>`
- privilege level 15 - enable level - prompt says `router#`

Since commands available depend on the ios feature set, version of Cisco IOS, model of router, and so on, there is not a comprehensive list of all commands at levels 1 and 15. For example, **show ip nat trans** would not be present in an ip only feature set, **show ip nat trans** would not be in Cisco IOS 10.2.X because NAT was not introduced at the time, and **show environment** would not be present in router models without power supply and temperature monitoring. Commands available in a particular router at a particular level can be found by entering a `?` at the prompt in the router when at that privilege level.

Console port authorization was not added as a feature until CSCdi82030 was implemented. Console port authorization is off by default to lessen the likelihood of accidentally being locked out of the router. If a user has physical access to the router through the console, console port authorization is not extremely effective. However, console port authorization can be turned on under line `con 0` in an image that CSCdi82030 was implemented in with the command:

```
authorization exec default|WORD
```

1. The router can be configured to authorize commands through TAC+ at all or some levels. The following router configuration allows all users to have per-command authorization set up on the server. Here we authorize all commands through TAC+, but if the server is down, no authorization is necessary, hence the **none**.

```
aaa authorization commands 1 default tacacs+ none
aaa authorization commands 15 default tacacs+ none
```

2. While the TAC+ server is running, telnet into the router with userid **authenuser**. Because **authenuser** has **default service = permit** in `test_file`, this user should be able to perform all functions.

While in the router, enter **enable** mode, and turn on authorization debugging:

```
terminal monitor
debug aaa authorization
```

3. Telnet into the router with userid **authoruser** and password **operator**.

This user should be able to do two **show** commands: **traceroute** and **logout** (see `test_file`).

Watch the server and the router where you should see the TAC+ interaction, that is, what's being sent where, responses, requests, and so on. Correct any problems before continuing.

4. If you want to configure a user for an autocommand, eliminate the commented-out user **transient** in the `test_file`, and put a valid IP address destination in place of the `####`.

Stop and start the TAC+ server.

On the router:

```
aaa authorization exec default tacacs+
```

Telnet to the router with userid **transient** and password **transient**. The `telnet ####` will execute and user **transient** will be sent to the other location.

XIV.D.4 Adding Accounting

Adding accounting is optional.

Reference to the accounting file is in test_file – **accounting file = /var/log/tac.log**. But accounting does not take place unless configured in the router (provided the router is running a version of Cisco IOS greater than 11.0).

1. First enable accounting in the router:

```
aaa accounting exec default start-stop tacacs+
aaa accounting connection default start-stop tacacs+
aaa accounting network default start-stop tacacs+
aaa accounting system default start-stop tacacs+
```

Note: AAA accounting doesn't do per-command accounting in some versions. A workaround is to use per-command authorization and log the occurrence in the accounting file. (See Bug ID CSCdi44140.) If you are using an image in which this is fixed is being used [11.2(1.3)F, 11.2(1.2), 11.1(6.3), 11.1(6.3)AA01, 11.1(6.3)CA as of September 24, 1997] you can also enable command-accounting.

2. With TAC+ running on the server, to see the entries going into the accounting file, enter on the server:

```
tail -f /var/log/tac.log
```

Then log into and out of the router, telnet out of the router, etc.

If necessary, on the router enter:

```
terminal monitor
debug aaa accounting
```

XIV.D.5 test_file

```

- - - - - (cut here) - - - - -

# Set up accounting file if enabling accounting on NAS
accounting file = /var/log/tac.log

# Enable password setup for everyone:
user = $enable$ {
    login = cleartext "cisco"
}

# Group listings must be first:
group = admin {
# Users in group 'admin' have cleartext password
    login = cleartext "admin"
    expires = "Dec 31 1999"
}

group = operators {
# Users in group 'operators' have cleartext password
    login = cleartext "operator"
    expires = "Dec 31 1999"
}

group = transients {
# Users in group 'transient' have cleartext password
    login = cleartext "transient"
    expires = "Dec 31 1999"
}

# This user is a member of group 'admin' & uses that group's password to log
in.
# The $enable$ password is used to enter enable mode. The user can perform
all commands.
user = authenuser {
    default service = permit
    member = admin
}

# This user is limited in allowed commands when aaa authorization is
enabled:
user = telnet {
    login = cleartext "telnet"
    cmd = telnet {
        permit .*
    }
    cmd = logout {
        permit .*
    }
}

# user = transient {
#     member = transients
#     service = exec {
#         # When transient logs on to the NAS, he's immediately
#         # zipped to another site
#         autocmd = "telnet #.#.#.#"
#     }
# }

# This user is a member of group 'operators'
# & uses that group's password to log in
user = authenuser {
    member = operators
# Since this user does not have 'default service = permit' when command
# authorization through TACACS+ is on at the router, this user's commands

```

```
# are limited to:
  cmd = show {
    permit ver
    permit ip
  }
  cmd = traceroute {
    permit .*
  }
  cmd = logout {
    permit .*
  }
}
```

----- (end cut here) -----

XIV.D.6 Related Information

- [TACACS+ in IOS Documentation](#)
- [Single-User Network Access Security TACACS+](#)
- [TACACS+ Technology Support Page](#)

XIV.D.7 Application

a) Fichier de configuration du serveur Tacacs Plus

```
# /etc/tacacs/tac_plus.cfg
# Set up accounting file if enabling accounting on NAS
accounting file = /var/log/tac.log

# Active le chiffrement et définit sa clé
key = ciscomania

# Enable password setup for everyone:
user = $enable$ {
    login = cleartext "cisco"
}

# Group listings must be first:
group = admin {
# Users in group 'admin' have cleartext password
    login = cleartext "admin"
    expires = "Dec 31 2010"
}

group = operators {
# Users in group 'operators' have cleartext password
    login = cleartext "operator"
    expires = "Dec 31 2010"
}

group = transients {
# Users in group 'transient' have cleartext password
    login = cleartext "transient"
    expires = "Dec 31 2010"
}

# This user is a member of group 'admin' & uses that group's password to log in.
# The $enable$ password is used to enter enable mode. The user can perform all commands.
user = authenuser {
    default service = permit
    member = admin
}

# This user is limited in allowed commands when aaa authorization is enabled:
user = telnet {
    login = cleartext "telnet"
    cmd = telnet {
        permit .*
    }
    cmd = logout {
        permit .*
    }
}

# user = transient {
#     member = transients
#     service = exec {
#         # When transient logs on to the NAS, he's immediately
#         # zipped to another site
#         autocmd = "telnet #.#.#.#"
#     }
# }
```

- ❑ Pour activer le chiffrement des messages Tacacs, il suffit de définir une clé par la commande 'key LINE'

b) Fichier de configuration du C2621 avec IOS 12.3-6c

```

!--- Turn on TAC+
aaa new-model
enable password whatever
!--- These are lists of authentication methods.
!--- "linmethod", "vtymethod", "conmethod", and
!--- so on are names of lists, and the methods
!--- listed on the same lines are the methods
!--- in the order to be tried. As used here, if
!--- authentication fails due to the
!--- tac_plus_executable not being started, the
!--- enable password will be accepted because
!--- it is in each list.
!
aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable
aaa authentication login conmethod tacacs+ enable
!
!--- For enable mode, list 'default' looks to TAC+
!--- then enable password if TAC+ not running
aaa authentication enable default group tacacs+ enable
!
!--- Point the router to the server, where #.#.#.#
!--- is the server IP address.
!
tacacs-server host 192.168.13.9
!
! Activative le chiffrement du champ donné des messages Tacacs
! et définit la clé de cryptage.
tacacs-server key ciscomania
!
line con 0
    password whatever
    !--- No time-out to prevent being locked out
    !--- during debugging.
    exec-timeout 0 0
    login authentication conmethod
line vty 0 4
    password whatever
    !--- No time-out to prevent being locked out
    !--- during debugging.
    exec-timeout 0 0
    login authentication vtymethod
!
!--- enable accounting in the router
aaa accounting exec default start-stop tacacs+
aaa accounting connection default start-stop tacacs+
aaa accounting network default start-stop tacacs+
aaa accounting system default start-stop tacacs+
!

```

- ❑ Attention: le port AUX n'est pas sécurisé.
- ❑ Pour activer le chiffrement des messages Tacacs, il suffit de définir une clé par la commande 'tacacs-server key [0|7] LINE'

XIV.E Radius

The lines in this sample RADIUS reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default radius** command specifies RADIUS as the default method for user authentication during login.
- The **aaa authorization reverse-access radius** specifies RADIUS as the method for user authorization when trying to establish a reverse Telnet session.
- The **radius-server host** command identifies the RADIUS server.
- The **radius-server key** command defines the encryption key used for all RADIUS communications between the NAS and the RADIUS daemon.

The following example configures the RADIUS server to grant a user named "jim" reverse Telnet access at port tty2 on the NAS named godzilla:

```
Password = "goaway"  
User-Service-Type = Shell-User  
cisco-avpair = "raccess:port#1=godzilla/tty2"
```

The syntax "raccess:port=any/any" permits a user to have unconditional access to NAS ports for reverse Telnet. If no "raccess:port={nasname}/{tty number}" clause exists in the user profile, the user is denied access to reverse Telnet on all ports.

For more information about configuring RADIUS, refer to the "Configuring RADIUS" chapter.

XIV.F Protection anti spoofing

- ❑ Le principe du spoofing est d'utiliser depuis l'extérieur, une adresse IP interne afin d'atteindre un équipement, éventuellement en aveugle (pas de trame retour).
- ❑ La solution pour éviter ce type d'intrusion est d'interdire en entrée sur son réseau les adresses correspondant au réseau interne par la mise en place d'ACL correspondantes.

XIV.G Désactiver les services inutiles

- ❑ Désactiver les services UDP et TCP Small Servers, IP finger.

Commandes :

no service udp-small-servers	Interdire les services UDP.
no service tcp-small-servers	Interdire les services TCP.
no ip finger	Interdire le finger.
no service finger	Interdire le finger.

Exemple :

```
!  
service password-encryption  
no service udp-small-servers  
no service tcp-small-servers  
!  
no ip finger
```

XIV.H Les tables ARP

- ❑ Il est possible de bloquer les entrées de la table ARP.
- ❑ Ce type de configuration peut être généralisé à l'ensemble du réseau, toutefois il sera très difficile à maintenir. Cependant il est intéressant de configurer de la sorte quelques liens sensibles comme la connexion d'un pare-feu.

Exemple :

```
Router(config)#arp 172.16.1.20 ?
  H.H.H 48-bit hardware address of ARP entry
Router(config)#arp 172.16.1.20 0000.C047.1B8E ?
  arpa  ARP type ARPA

  sap   ARP type SAP (HP's ARP type)
  smds  ARP type SMDS
  snap  ARP type SNAP (FDDI and TokenRing)
Router(config)#arp 172.16.1.20 0000.C047.1B8E arpa
Router(config)#^Z

Router#sh ip arp
Protocol Address          Age (min)  Hardware Addr  Type   Interface
Internet 172.6.54.49         -          00e0.1e7f.d71a ARPA   Ethernet0
Internet 172.16.1.20         -          0000.c047.1b8e ARPA
Router#
```

XIV.I Contrôler les accès http

- ❑ Si le serveur HTTP est activé sur les routeurs, le contrôler avec une Access-List, voir un serveur AAA. Il est effectivement possible de modifier la configuration du routeur grâce à ce service.

Exemple :

```
ip http server
ip http authentication enable
ip http access-class 99
```

XIV.J Exercice

Exercice sur la sécurité :

- ❑ Configurez vos équipements Cisco pour qu'ils utilisent le serveur Tacacs+ dont l'adresse estavec la clé suivante
- ❑ Configurez un accès http Sécurisé.
- ❑ Essayez un telnet sur le port finger (tcp 79).
- ❑ Désactivez les services inutiles.
- ❑ Configurer les routeurs pour SNMP.
- ❑ La station d'administration SNMP a pour adresse :
- ❑ Utiliser pour nom de community public et private.
- ❑ Mettre en place une Access-list pour filtrer le SNMP.
- ❑ Configurez la journalisation.
- ❑ Le serveur de log a pour adresse :
- ❑ La station d'administration recevra la journalisation au niveau information, avec la facility local0.
- ❑ Familiarisez vous avec CDP.

Option :

- ❑ En fonction du temps restant, installez le produit Lorient et manager vos routeurs en SNMP.
 - <http://llecointe.com>

XV. Les ACL

XV.A Présentation

- ❑ Les routeurs Cisco disposent d'un moyen puissant de contrôle du trafic, ce sont les listes d'accès.
- ❑ Une liste d'accès (Access-List) a plusieurs fonctions possibles sur un routeur :
 - le filtrage,
 - le contrôle des mises à jour du routage,
 - la gestion de priorités,

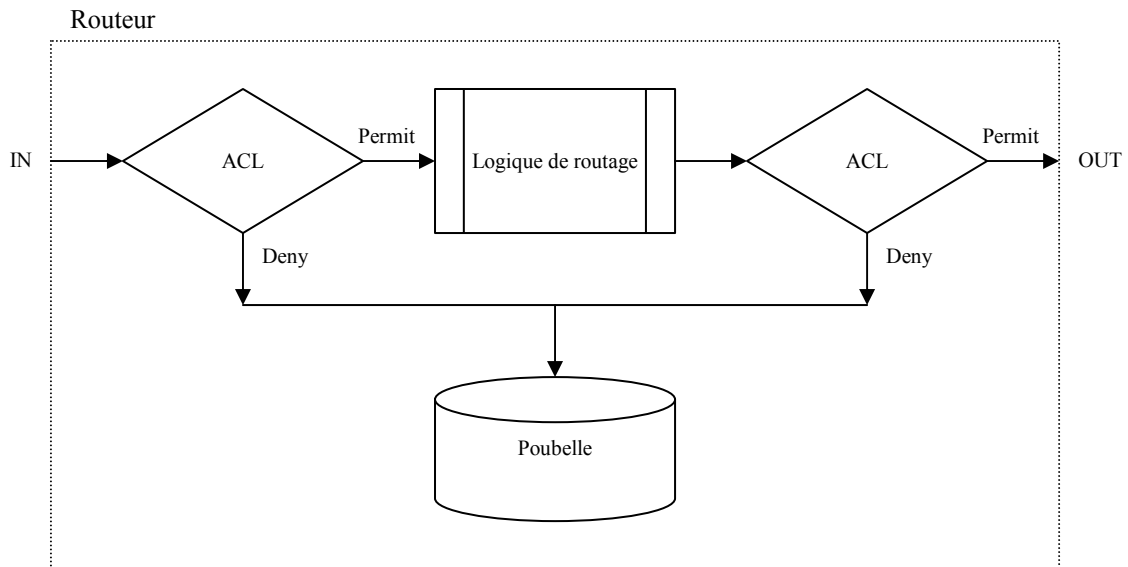
On parle de plus en plus de QoS, ou qualité de service en particulier si l'on utilise le réseau IP pour transporter la voix (VOIP : Voice over IP),

- la gestion de la numérotation sur RNIS par exemple,
 - la sécurité d'accès aux informations,
 - etc....
- ❑ Il existe deux familles d'Access-List :
 - les access-list classiques (faisant référence à un numéro d'Access-List),
 - l'access-list standard : uniquement l'adresse IP source.
 - l'access-list étendu : l'adresse IP source & destination, le protocole, le port source et destination
 - les access-list nommées.
 - ❑ Nous avons vu que les ACL sont numérotées, cette numérotation représente ce que peut faire la liste comme le montre la commande suivante :

```
Routeur(config)# access-list ?
  <1-99>          IP standard access list
  <100-199>       IP extended access list
  <1000-1099>     IPX SAP access list
  <1100-1199>     Extended 48-bit MAC address access list
  <1200-1299>     IPX summary address access list
  <1300-1999>     IP standard access list (expanded range)
  <200-299>       Protocol type-code access list
  <2000-2699>     IP extended access list (expanded range)
  <300-399>       DECnet access list
  <600-699>       Appletalk access list
  <700-799>       48-bit MAC address access list
  <800-899>       IPX standard access list
  <900-999>       IPX extended access list
```

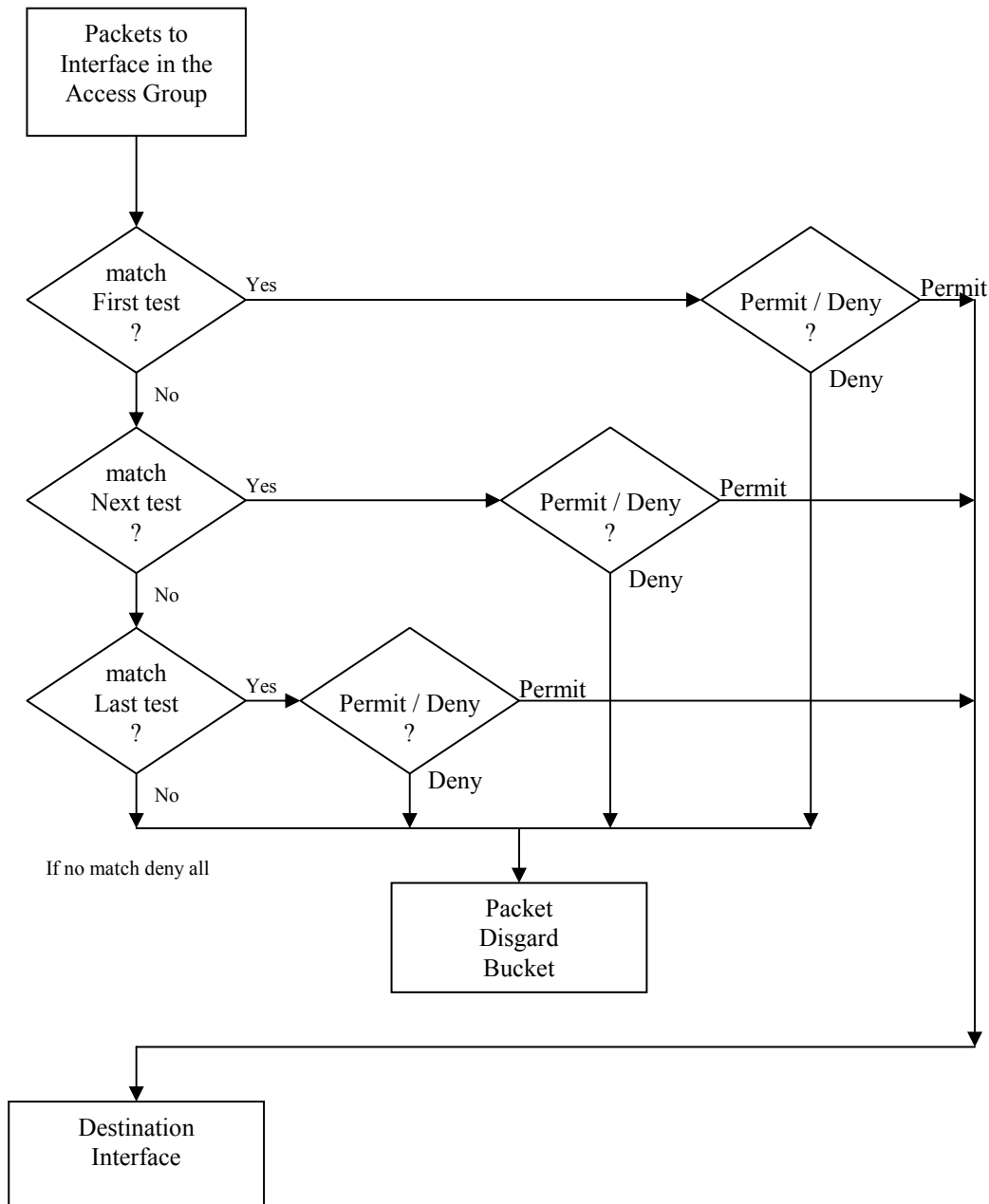
- ❑ L'IOS Cisco est riche au niveau de ses possibilités de filtrage.
- ❑ Nous allons revoir les :
 - ACL IP standard (1 à 99)
 - puis traiter les ACL IP étendues (100 à 199).

XV.B Fonctionnement



- ❑ Inbound access lists : L'ACL est appliquée **avant** la logique de routage.
- ❑ Outbound access lists : L'ACL est appliquée **après** la logique de routage

- Une ACL est une liste ordonnée d'ACE (*Access Control Entry*) décrivant des règles de filtrage à appliquer au trafic des datagrammes IP.
 - Ces règles sont utilisées pour rechercher une correspondance dans les datagrammes qui transitent dans le routeur.
 - La correspondance est recherchée en évaluant les ACE dans l'ordre de leurs saisies.
 - Dès qu'une correspondance est trouvée (match), on applique '*permit | deny*' et on sort de l'ACL.



XV.C Les commandes

Commandes	Commentaires
Routeur# configure terminal Router(config)# access-list <i>access-list-number</i> {permit deny} { <i>test conditions</i> }	Création de l'ACL
Router(config)# interface serial 1 Router(config-if)# {protocol} access-group <i>access-list-number</i> {in out}	Application de l'ACL à une interface
Routeur# show ip interface	Vérifie l'ACL
Routeur> show access-lists	Visualise toutes les ACL
Routeur# show access-lists log	Permet de connaître le taux d'utilisation d'une ACL

- ❑ Une même Access List peut-être appliquée sur plusieurs interfaces à la fois.

XV.D Types et Identification

Types d'Access List		<i>Access-list-number</i>
IP	Standards	De 1 à 99 et de 1300 à 1999
	Étendues nommées	De 100 à 199 et de 2000 à 2699 nom (à partir de l'IOS 11.2 et plus)
IPX	Standards	800 à 899
	Étendues	900 à 999
	SAP Filters	1000 à 1099
	nommées	nom (à partir de l'IOS 11.2 et plus)

- Les ACL IP standards testent uniquement l'adresse IP source dans le datagramme IP.
- Les ACL IP étendues teste : l'adresse IP source, l'adresse IP destination, le champ protocole et les ports TCP ou UDP, etc.
- Les ACL IP nommées fonctionnent comme les ACL numérotées, mais présentent plusieurs avantages :
 1. Un nom ou label est davantage significatif pour nous humains.
 2. Le nombre d'ACL n'est pas limité de 1 à 99 ou 100 à 199.
 3. Une simplification dans l'écriture des ACL en cas de modification, une instruction de l'ACL nommée peut-être supprimée séparément contrairement aux ACL numérotées où il faudra supprimer la liste entière.
 4. les commentaires sont possibles.

XV.E Les WILCARD MASK

XV.E.1 Présentation

- ❑ Il permet d'identifier une ou plusieurs adresses IP (Host).
- ❑ Il s'écrit comme une adresse IP.
 - ❖ 32 bits
 - ❖ représentés en notation décimale pointée
- ❑ C'est un masque de 32 bits.

- ❑ Quand le bit est à 0, il doit y avoir correspondance. (match)
- ❑ Quand le bit est à 1, on ignore la correspondance.

192 30 16	0	1100 0000.0001 1110.0001 0000.0000	0000
0 0 0	15	0000 0000.0000 0000.0000 0000.0000	1111
match	ignore	match 28 bits	Ignore 4 bits

XV.E.2 Exemples :

Adresse IP	Wildcard Mask	Signification
192.168.15.2	0.0.0.0	On vérifie la correspondance sur tous les bits.
192.168.15.0	0.0.0.255	Ici, on ignore les 8 bits de poids faible
192.168.15.4	0.0.0.3	Désigne les machines : 192.168.15.4 à 192.168.15.7
192.168.15.16	0.0.0.15	Désigne les machines : 192.168.15.16 à 192.168.15.31
192.168.15.2	0.0.0.0	Désigne la machine 192.168.15.2
0.0.0.0	255.255.255.255	Désigne toutes les machines
any		Désigne toutes les machines

- ❖ Le mot clé 'any' remplace '0.0.0.0 255.255.255.255'.

XV.F Les ACL Standards numérotées

- ❑ La logique implémentée par une liste d'accès peut être résumée par la séquence suivante :
- ❑ le paquet est comparé aux paramètres de la première instruction de la liste.
- ❑ Si une correspondance est trouvée, l'action définie dans l'instruction est exécutée (autoriser ou rejeter).
- ❑ Si aucune correspondance n'est trouvée, les deux premières étapes sont répétées avec l'instruction suivante de la liste.
- ❑ Si aucune correspondance n'est trouvée par l'ensemble des instructions de la liste, le paquet est rejeté par défaut.
- ❑ Chaque nouvelle instruction est inscrite à la fin de la liste.
- ❑ La logique de traitement décrite précédemment nous montre que l'ordre des instructions est très importante, pour ajouter une instruction « à sa place » dans la liste, il convient de supprimer la liste puis de la recréer. Pour cela l'on peut utiliser la technique du copier coller, ou encore se servir du service TFTP.(Remonter la configuration sur le serveur, la modifier, la redescendre sur le routeur).

XV.F.1 Les commandes :

```
access-list (1-99) {permit|deny} host (Adresse) [log]
access-list (1-99) {permit|deny} (Adresse) (Wildcard-mask) [log]
```

Commandes	Commentaires
Routeur# configure terminal Router(config)# access-list access-list-number {permit deny} source [mask] [log]	Création de l'ACL
Router(config)# interface serial 1 Router(config-if)# ip access-group access-list-number {in out}	Application de l'ACL à une interface

- ❑ Le wildcard mask par défaut = 0.0.0.0
- ❑ In | Out par défaut = Outbound
- ❑ Le terme 'any' est équivalent à '0.0.0.0 255.255.255.255' pour désigner 'source [mask]'

Commandes	Commentaires
Routeur# configure terminal Router(config)# no access-list access-list-number	Supprime l'ACL
Router(config)# interface serial 1 Router(config-if)# no ip access-group access-list-number	Supprime l'ACL de l'interface

Mot clé	Description
any	Spécifie tous les hôtes. Identique à '0.0.0.0 255.255.255.255'
host	Spécifie un hôte. Identique à un Subnet Mask de '0.0.0.0'
log	Active le log de tous paquets qui correspondent à l'état 'deny' ou 'permit'.

XV.F.2 Exemple :

```
Routeur(config)#no access-list 10
Routeur(config)#access-list 10 permit host 172.20.24.163
Routeur(config)#access-list 10 permit 172.20.24.140 0.0.0.0
Routeur(config)#access-list 10 deny 172.16.0.0 255.255.255.255 log
Routeur(config)#^Z
Routeur#sh access-lists 10
Standard IP access list 10
    permit 172.20.24.163
    permit 172.20.24.140
    deny any log
Routeur#
```

- ❑ Noter l'effet des wildcard mask **0.0.0.0** et **255.255.255.255**.
- ❑ L'option 'log' est apparue dans les access-lists simples avec la version 12.0 de l'IOS. Cette option permet de tracer le filtre au niveau du syslog.

Exemples d'utilisation :

- ❑ Contrôle du telnet sur un routeur

```
line vty 0 4
  access-class 10 in
```

- ❑ Contrôle au niveau de l'interface

```
interface ethernet 0
  ip access-group 10 out
```

- ❑ Sécurisation SNMP

```
snmp-server community private RW 10
snmp-server community public RO 11
```

XV.G Les ACL étendues numérotées

- ❑ Les Access-List IP étendues sont presque identiques aux listes d'accès standard, en ce qui concerne leur emploi et la logique de traitement des instructions. Cependant elles permettent de comparer un plus grand nombre de champs dans un paquet. La logique de filtrage est par conséquent beaucoup plus complexe. Néanmoins, ces deux types de liste peuvent filtrer des paquets en entrées comme en sortie.
- ❑ Rappel :
 - Les instructions de la liste sont traitées de façon séquentielle, c'est à dire que dès qu'une instruction fait l'objet d'une correspondance, la recherche prend fin et l'action définie par l'instruction est exécutée.
 - Une instruction est considérée comme correspondante seulement si une correspondance est trouvée pour chacun des ses paramètres ; sinon son exécution est interrompue et l'instruction suivante de la liste est examinée.
- ❑ Si aucune correspondance n'est trouvée par l'ensemble des instructions de la liste, le paquet est rejeté par défaut.

La commande :

```
access-list access-list-number {permit|deny} {protocol-number | protocol-
keyword} {source source-wilcard | any | host} operator {source-port}
{destination destion-wilcard| any | host} operator {destination-port}
[established] [log | log-input]
```

- ❑ Les access-lists étendues ne présente pas beaucoup plus de difficulté à mettre en œuvre que les Access-List simples, cependant elles nécessitent une préparation plus attentive.

Access-list Command	Description
<code>access-list 100-199 {permit deny} {ip tcp udp icmp} source source-mask dest dest-mask [lt gt eq neq dest-port]</code>	
101	Identifiant de l'ACL, ici une ACL étendue
deny	Le trafic, où la correspondance est réalisée, sera bloqué
tcp	Test sur le protocole encapsulé dans IP.
192.168.22.0 0.0.0.255	Adresses IP source : de 192.168.22.0 à 192.168.22.255
192.168.52.0 0.0.0.255	Adresses IP destination : de 192.168.52.0 à 192.168.52.255
eq 21	Spécifie le port pour les commandes FTP
eq 20	Spécifie le port pour les données FTP
range 20 21	Spécifie les ports de 20 à 21
Exemple:	
<code>access-list 101 deny tcp 192.168.22.0 0.0.0.255 192.168.52.0 0.0.0.255 range 20 21</code>	

Affectation de l'ACL :

Access-group Command :	Description
<code>interface ethernet 0</code>	Applique l'ACL 101 en sortie de l'interface Ethernet E0
<code>ip access-group 101 out</code>	Choix de l'interface
	Application de l'ACL étendue 101 en sortie

Remarque :

- ❑ A partir de la version 12 il est possible parfois suivant le routeur et l'IOS utilisé de commenter les Access-List.

XV.H Les ACL Standards nommées

- ❑ Vous pouvez identifier votre Access-List par un nom ceci peut permettre d'utiliser plus de 99 Access-Lists simples.
- ❑ Cette facilité est apparue avec la version 11.2 de l'IOS.
- ❑ Ce type de liste n'est utilisable que pour le filtrage des paquets ou des routes au niveau d'une interface.
- ❑ Une liste standard et une liste étendue ne peuvent pas avoir le même nom.
- ❑ Pour utiliser une Access-List Nommée, la méthode et la syntaxe des commandes sont légèrement différentes.

XV.H.1 Les commandes :

Création d'une ACL nommée standard	
<code>ip access-list standard name</code>	Définir le type et le nom
<code>{deny permit} {source [source-wildcard] any}</code>	Spécifier une ou plusieurs conditions pour lesquelles les paquets seront soit passés soit droppés.
<code>exit</code>	Sortir de l'Access-List nommée

XV.H.2 Exemple :

```

Routeur(config)#ip access-list standard ?
  <1-99> Standard IP access-list number
  WORD   Access-list name

Routeur(config)#ip access-list standard enter_filter
Routeur(config-std-nacl)#deny host 172.16.1.20
Routeur(config-std-nacl)#permit any
Routeur(config-std-nacl)#exit
Routeur(config)#^Z
Routeur#sh access-lists enter_filter
Standard IP access list enter_filter
  deny 172.16.1.20
  permit any

```

XV.I Les ACL Etendues nommées

- ❑ Vous pouvez identifier votre Access-List par un nom ceci peut permettre d'utiliser plus de 100 Access-List étendues.
- ❑ Cette facilité est apparue avec la version 11.2 de l'IOS.
- ❑ Ce type de liste n'est utilisable que pour le filtrage des paquets ou des routes au niveau d'une interface.
- ❑ Une liste standard et une liste étendue ne peuvent pas avoir le même nom.
- ❑ Pour utiliser une Access-List Nommée, la méthode et la syntaxe des commandes sont légèrement différentes.

XV.I.1 Les commandes :

```
ip access-list extended access-list-name {permit|deny} {protocol-number |
protocol-keyword} {source source-wilcard | any | host} operator {source-port}
{destination destion-wilcard| any | host} operator {destination-port}
[established] [log | log-input]
```

Création d'une ACL nommée étendue	
ip access-list extended name	Définir le type et le nom
{permit deny} {protocol-number protocol-keyword} {source source-wilcard any host} operator {source-port} {destination destion-wilcard any host} operator {destination-port} [established] [log log-input]	Spécifier une ou plusieurs conditions pour lesquelles les paquets seront soit passés soit droppés.
exit	Sortir de l'Access-List nommée

XV.I.2 Exemple :

```
Routeur(config)#ip access-list extended ?
  < > extended IP access-list number
  WORD Access-list name

Routeur(config)#ip access-list extended enter_filter
Routeur(config-std-nacl)#deny tcp any any
Routeur(config-std-nacl)#permit ip any any
Routeur(config-std-nacl)#exit
Routeur(config)#^Z
Routeur#sh access-lists enter_filter
```


XV.J Les ACL Dynamiques

- ❑ Ce sont des listes d'accès dont certaines lignes peuvent être validées par une commande de type « EXEC » sur le routeur (**access-enable**).
- ❑ L'option dynamique sera retenue pour les lignes activées par la commande EXEC : 'access-Enable'.

XV.J.1Exemple :

```
interface ethernet0
  ip address 172.18.23.9 255.255.255.0
  ip access-group 101 in

access-list 101 permit tcp any host 172.18.21.2 eq telnet
access-list 101 dynamic mytestlist timeout 120 permit ip any any

line vty 0
  login local
  autocommand access-enable timeout 5
```

- ❑ Il faudra dans un premier temps se connecter au routeur (`line VTY 0`), s'authentifier (`password`). L'auto command permettra de valider la ligne dynamique de l'ACL.
- ❑ On parle de 'lock & key', cette option est souvent implémentée avec une authentification locale ou un serveur AAA.

XV.K Les ACL basées sur le temps

- Ce type d'ACL permet d'autoriser un trafic donné en fonction de créneau horaire :

Commandes	Signification
<code>() configure terminal</code>	Entrez en mode configuration globale
<code>(global) interface fastethernet 0/0</code> ou <code>(global) interface range fastethernet 0/0 - 8</code>	Choix du port à configurer
<code>(config-if) ip access-group time in</code>	Application de l'ACL étendue nommée 'time'
<code>config-ifexit</code>	
<code>(global) ip access-list extended time</code>	Creation de l'ACL étendue nommée 'time'
<code>(global-ext-nacl) permit tcp any any eq www</code> <code>time-range webaccess</code>	
<code>(config-ext-nacl) exit</code>	
<code>(global) time-range webaccess</code>	
<code>(config-time-range) periodic weekdays 8:00 to 18:00</code>	Période : <ul style="list-style-type: none"> <input type="radio"/> Friday => Friday <input type="radio"/> Monday => Lundi <input type="radio"/> Saturday => <input type="radio"/> Sunday => <input type="radio"/> Thursday => <input type="radio"/> Tuesday => <input type="radio"/> Wednesday => <input type="radio"/> Daily => tous les jours de la semaine <input type="radio"/> Weekdays => du lundi au vendredi <input type="radio"/> Weekend => samedi et dimanche
<code>(config-time-range) end</code>	Retour en mode privileged EXEC
<code>() show access-list</code>	
<code>() show running-config</code>	Vérifiez votre configuration
<code>() copy running-config startup-config</code>	[optionnel] sauvegardez la configuration pour le prochain redémarrage.

XV.L Les ACL réfléchives

- ❑ **Note** : Les ACL réfléchives sont apparue après les listes d'accès dynamique, de part leur fonctionnement elles mériteraient de porter le nom de listes dynamiques.
- ❑ Les ACL réfléchives sont un moyen simple de filtrer le trafic IP. Elles permettent d'autoriser le trafic initialisé depuis une station de votre réseau et d'interdire le trafic initialisé par une station étrangère. Par exemple lorsqu'un premier paquet arrive sur le routeur et qu'il est autorisé par la liste, une nouvelle entrée temporaire est créée et ajouter à la « réfléchive liste ».
- ❑ Il existe deux restrictions relatives à l'utilisation des listes d'accès réfléchives :
 - Elles peuvent être définies uniquement avec des Access-Lists IP étendues nommées.
 - Elles ne fonctionnent pas avec certaines applications qui utilisent des numéros de ports changeant en cours de session, comme le protocole FTP.

XV.L.1 Les commandes :

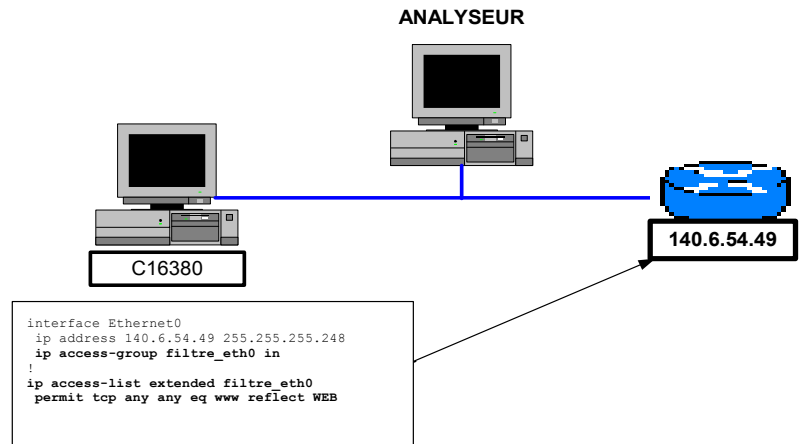
Création d'une ACL réfléchive	
<code>ip access-list extended name</code>	Définir le type et le nom
<code>{deny permit} protocol any any reflect reflection-name [timeout seconds]</code>	
<code>exit</code>	Sortir de l'Access-List nommée

XV.L.2 Exemple #1 :

- ❑ Refer page 147 Network Security Fundamentals CISCO

```
interface serial0/0
ip access-group incoming in
ip access-group outgoing out
!
ip access-list extended outgoing
 permit tcp any any reflect tcptraffic
!
ip access-list extended incoming
 permit eigrp any any
 deny icmp any any
 evaluate tcptraffic
```

XV.L.3 Exemple #2 :



- ❑ Le poste de travail va accéder au serveur HTTP du routeur.
- ❑ Ce que voit le routeur :

```

Router#sh access-lists WEB
Reflexive IP access list WEB
  permit tcp host 140.6.54.49 eq www host 140.6.54.51 eq 1210 (15 matches) (time left 54)
  permit tcp host 140.6.54.49 eq www host 140.6.54.51 eq 1209 (13 matches) (time left 52)
Router#
    
```

Ce que voit l'analyseur :

```

Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
16 [140.6.54.51] [140.6.54.49] 348 000:00:06.523 0.037.877 21/03/2000 16:14:05 HTTP: C Port=1209 GET / HTTP/1.0
17 [140.6.54.49] [140.6.54.51] 614 000:00:06.651 0.127.477 21/03/2000 16:14:05 HTTP: R Port=1209 HTML Data
18 [140.6.54.49] [140.6.54.51] 614 000:00:06.691 0.040.552 21/03/2000 16:14:06 HTTP: R Port=1209 HTML Data
19 [140.6.54.51] [140.6.54.49] 60 000:00:06.692 0.000.570 21/03/2000 16:14:06 TCP: D=80 S=1209 ACK=3421235876 WIN=7640
20 [140.6.54.49] [140.6.54.51] 614 000:00:06.985 0.292.870 21/03/2000 16:14:06 HTTP: R Port=1209 HTML Data
21 [140.6.54.49] [140.6.54.51] 505 000:00:07.016 0.031.892 21/03/2000 16:14:06 HTTP: R Port=1209 HTML Data
22 [140.6.54.51] [140.6.54.49] 60 000:00:07.017 0.000.734 21/03/2000 16:14:06 TCP: D=80 S=1209 ACK=3421236887 WIN=8760
23 [140.6.54.49] [140.6.54.51] 60 000:00:07.139 0.122.150 21/03/2000 16:14:06 TCP: D=1209 S=80 FIN ACK=19091757 SEQ=3421236887
LEN=0 WIN=3834
24 [140.6.54.51] [140.6.54.49] 60 000:00:07.140 0.000.618 21/03/2000 16:14:06 TCP: D=80 S=1209 ACK=3421236888 WIN=8760
25 [140.6.54.51] [140.6.54.49] 60 000:00:08.407 1.266.995 21/03/2000 16:14:07 TCP: D=80 S=1209 FIN ACK=3421236888 SEQ=19091757
LEN=0 WIN=8760
26 [140.6.54.49] [140.6.54.51] 60 000:00:08.409 0.002.411 21/03/2000 16:14:07 TCP: D=1209 S=80 ACK=19091758 WIN=3834
27 [140.6.54.51] [140.6.54.49] 60 000:00:10.186 1.776.971 21/03/2000 16:14:09 TCP: D=80 S=1210 SYN SEQ=19095167 LEN=0 WIN=8192
28 [140.6.54.49] [140.6.54.51] 60 000:00:10.190 0.003.369 21/03/2000 16:14:09 TCP: D=1210 S=80 SYN ACK=19095168 SEQ=3424940862
LEN=0 WIN=4128
29 [140.6.54.51] [140.6.54.49] 60 000:00:10.190 0.000.638 21/03/2000 16:14:09 TCP: D=80 S=1210 ACK=3424940863 WIN=8760
30 [140.6.54.51] [140.6.54.49] 401 000:00:10.223 0.032.541 21/03/2000 16:14:09 HTTP: C Port=1210 GET /exec/show/interfaces/CR
HTTP/1.0
31 [140.6.54.49] [140.6.54.51] 614 000:00:10.363 0.139.669 21/03/2000 16:14:09 HTTP: R Port=1210 HTML Data
32 [140.6.54.49] [140.6.54.51] 614 000:00:10.406 0.043.483 21/03/2000 16:14:09 HTTP: R Port=1210 HTML Data
33 [140.6.54.51] [140.6.54.49] 60 000:00:10.407 0.000.582 21/03/2000 16:14:09 TCP: D=80 S=1210 ACK=3424941983 WIN=7640
34 [140.6.54.49] [140.6.54.51] 614 000:00:10.450 0.042.977 21/03/2000 16:14:09 HTTP: R Port=1210 HTML Data
35 [140.6.54.49] [140.6.54.51] 614 000:00:10.491 0.041.204 21/03/2000 16:14:09 HTTP: R Port=1210 HTML Data
36 [140.6.54.51] [140.6.54.49] 60 000:00:10.491 0.000.565 21/03/2000 16:14:09 TCP: D=80 S=1210 ACK=3424943103 WIN=8760
37 [140.6.54.49] [140.6.54.51] 422 000:00:10.518 0.027.028 21/03/2000 16:14:09 HTTP: R Port=1210 HTML Data
38 [140.6.54.51] [140.6.54.49] 60 000:00:10.619 0.100.812 21/03/2000 16:14:09 TCP: D=80 S=1210 ACK=3424943471 WIN=8392
    
```

- ❑ Les ports sources 1209 et 1210 sont contrôlés comme le montre le détail d'une des trames (ici le port 1209 pour la trame 16):

```

----- Frame 16 -----
Frame Source Address   Dest. Address   Size Rel. Time   Delta Time   Abs. Time   Summary
16 [140.6.54.51]     [140.6.54.49]  348 000:00:06.523 0.037.877   21/03/2000 16:14:05 HTTP: C
Port=1209 GET / HTTP/1.0
DLC: ----- DLC Header -----
DLC:
DLC: Frame 16 arrived at 16:14:05.8685; frame size is 348 (015C hex) bytes.
DLC: Destination = Station Cisc147FD71A
DLC: Source       = Station 0010A4EC5886
DLC: Ethertype    = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: Total length = 334 bytes
IP: Identification = 5913
IP: Flags       = 4X
IP:   .1. . . . = don't fragment
IP:   ..0. . . . = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 5E20 (correct)
IP: Source address = [140.6.54.51]
IP: Destination address = [140.6.54.49]
IP: No options
IP:
TCP: ----- TCP header -----
TCP:
TCP: Source port = 1209
TCP: Destination port = 80 (WWW-HTTP)
TCP: Sequence number = 19091463
TCP: Next expected Seq number= 19091757
TCP: Acknowledgment number = 3421234756
TCP: Data offset = 20 bytes
TCP: Flags = 18
TCP:   ..0. . . . = (No urgent pointer)
TCP:   ...1 . . . = Acknowledgment
TCP:   .... 1... = Push
TCP:   .... .0.. = (No reset)
TCP:   .... ..0. = (No SYN)
TCP:   .... ...0 = (No FIN)
TCP: Window = 8760
TCP: Checksum = 20EB (correct)
TCP: No TCP options
TCP: [294 Bytes of data]
TCP:
HTTP: ----- Hypertext Transfer Protocol -----
HTTP:
HTTP: Line 1: GET / HTTP/1.0
HTTP: Line 2: Connection: Keep-Alive
HTTP: Line 3: User-Agent: Mozilla/4.7 [fr] (WinNT; I)
HTTP: Line 4: Host: 140.6.54.49
HTTP: Line 5: Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
HTTP:           image/png, */*
HTTP: Line 6: Accept-Encoding: gzip
HTTP: Line 7: Accept-Language: fr
HTTP: Line 8: Accept-Charset: iso-8859-1,*,utf-8
HTTP: Line 9: Authorization: Basic OkZ1bXBscHdk
HTTP: Line 10:
HTTP:

```

XVI. IOS Firewall

XVI.A Présentation

- ❑ Pour les réseaux hautement sécurisé ou pour sécuriser un réseau ouvert sur l'Internet, Cisco propose une version Firewall de l'IOS.

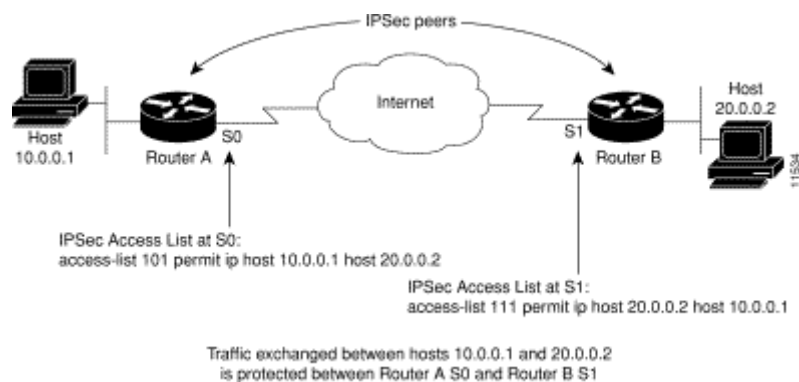
- ❑ Le pare feu est capable en plus du filtrage de fournir les fonctions suivantes :
 - Examen détaillé de chaque paquet,
 - Filtrage du contenu d'applications (CBAC),
 - Chiffrement, Authentification et Intégrité (IPSEC)
 - Translation d'adresses de réseau (NAT/PAT).

XVII. IPSec

IPSec : Internet Protocol Security

XVII.APrésentation

- ❑ IPSec permet une liaison sécurisée entre deux équipements par éventuellement de l'authentification des paquets (AH : *Authentication Header*) et chiffrement (ESP : *Encapsulating Security Payload*).
- ❑ IPSec va permettre de créer des tunnel sécurisé au travers de l'Internet pour assurer la liaison entre deux équipements, on appelle cela un VPN (*Virtual Private Network*).
- ❑ IPSec est un standard qui n'impose rien au niveau de l'authentification et du cryptage.



Config-isakmp Command Mode Keyword			
Keyword	Valeur Acceptée	Valeur par défaut	Description
des	56 bits DES-CBC	des	Algorithme de chiffrement des messages
sha	SHA-1 (HMAC variant)	sha	Algorithme d'intégrité des messages (hachage)
md5	MD-5 (HMAC variant)		
rsa-sig	RSA signatures	rsa-sig	Méthode d'authentification des stations (peer)
rsa-encr	RSA encrypted nonces		
pre-share	Preshared key		
1	Diffie-Hellman 768 bits	1	Identification du group D-H utilisé
2	Diffie-Hellman 1024 bits		
-		86.400 secondes (1 jour)	Durée de vie d'une SA ISAKMP
exit			Sortie du mode config-isakmp

Lecture conseillée :

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

```

C2621xm#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK8S-M), Version 12.2(11)T6,  RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
...
System image file is "flash:c2600-ik8s-mz.122-11.T6.bin"
...
Configuration register is 0x2102

C2621xm#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
C2621xm(config)#crypto isakmp policy 100
C2621xm(config-isakmp)#?
ISAKMP commands:
 authentication Set authentication method for protection suite
 default Set a command to its defaults
 encryption Set encryption algorithm for protection suite
 exit Exit from ISAKMP protection suite configuration mode
 group Set the Diffie-Hellman group
 hash Set hash algorithm for protection suite
 lifetime Set lifetime for ISAKMP security association
 no Negate a command or set its defaults

C2621xm(config-isakmp)#authentication ?
 pre-share Pre-Shared Key
 rsa-encr Rivest-Shamir-Adleman Encryption
 rsa-sig Rivest-Shamir-Adleman Signature

C2621xm(config-isakmp)#encryption ?
 des DES - Data Encryption Standard (56 bit keys).

C2621xm(config-isakmp)#hash ?
 md5 Message Digest 5
 sha Secure Hash Standard

C2621xm(config-isakmp)#group ?
 1 Diffie-Hellman group 1
 2 Diffie-Hellman group 2

C2621xm(config-isakmp)#^Z
C2621xm#

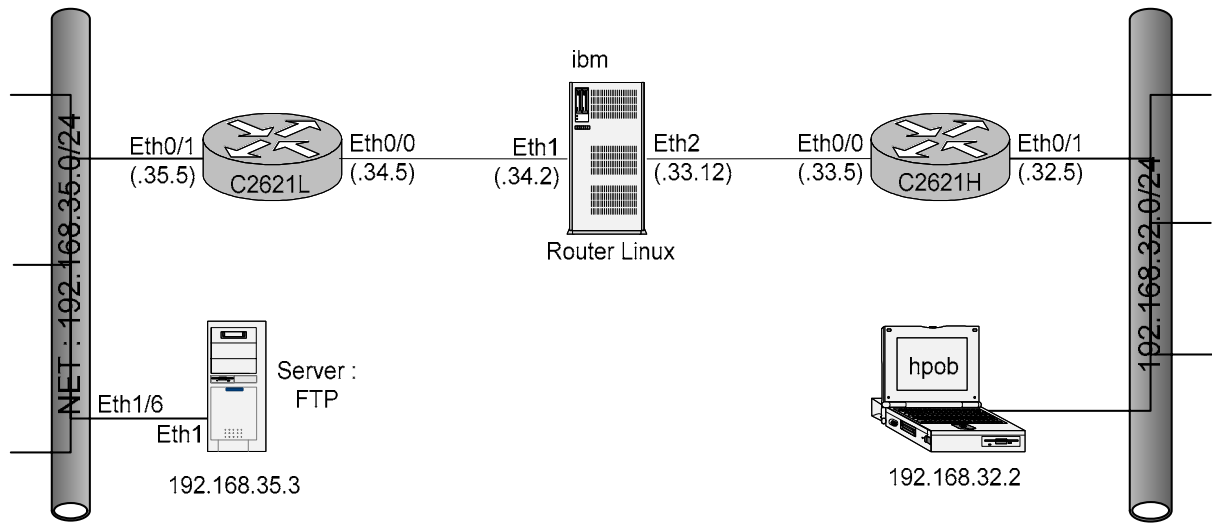
```

```

C2621xm#show crypto isakmp policy
Default protection suite
 encryption algorithm: DES - Data Encryption Standard (56 bit keys).
 hash algorithm: Secure Hash Standard
 authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #1 (768 bit)
 lifetime: 86400 seconds, no volume limit
C2621xm#

```


XVII.B Configuration en PSK Net-To-Net



XVII.B.1 Configuration IKE

Configuration IKE		
Step	Commande	Commentaire
1	R(config)#crypto isakmp enable	Activation d'IKE
2	R(config)#crypto isakmp policy priority	Identifie uniquement la police IKE et assigne une priorité à la police. La valeur '1' indique la plus haute priorité. Cette commande invoque le mode (config-isakmp)
	R(config-isakmp)#group 2	Déclaration du groupe Diffie-Hellman : <ul style="list-style-type: none"> o '1' par défaut sur 768 bits o '2' sur 1024 bits
	R(config-isakmp)#hash md5	Algorithme d'intégrité du message (hachage) <ul style="list-style-type: none"> o par défaut SHA, lequel est meilleur que o MD5
	R(config-isakmp)#lifetime 500	Par défaut 86.400 seconds (1 jour). Delay avant une nouvelle négociation.
	R(config-isakmp)#authentication pre-share	Méthode d'authentification <ul style="list-style-type: none"> o 'pre-share' o 'rsa-encr' o 'rsa-sig'
	R(config-isakmp)#exit	
3	R(config)#crypto isakmp key keystring address peer-address	Configuration de la PSK (PreShared Key) <ul style="list-style-type: none"> o 'keystring' combinaison jusqu'à 128 caractères alphanumériques. Et elle doit être identique sur les deux stations (peer). o 'peer-address' spécifie l'adresse IP de la station distante (remote peer)
4	R#show crypto isakmp policy	Vérification de la configuration IKE

XVII.B.2 Configuration IPSEC

- pour le step 1 de la procédure ci-dessous, l'authentification AH est rarement utilisée parce que l'authentification 'esp-sha-hmac' et 'esp-md5-hmac' est maintenant disponible. De plus AH n'est pas compatible avec NAT ou PAT.

Configuration IPSEC		
Step	Commande	Commentaire
1	R(config)#crypto ipsec transform-set trans-name esp-des esp-md5-hmac	Configuration de la phase 2 : <ul style="list-style-type: none"> ○ 'trans-name' appellation de la transform-set ○ 'esp-des' : chiffrement ○ 'esp-md5-hmac' : authentification
	R(cfg-crypto-trans)#default mode	
	R(cfg-crypto-trans)#mode tunnel	
2	R(config)#crypto ipsec security- association lifetime seconds 3600	Durée de vie
3	R(config)#access-list 100 permit ip 192.168.32.0 0.0.0.255 192.168.35.0 0.0.0.255	Création de l'ACL IPSEC, ACL qui sélectionne les paquets qui seront traités par ESP et/ou AH : <ul style="list-style-type: none"> ○ 'permit' implique chiffrement ○ 'deny' ne sélectionne pas le trafic pour le chiffrement
	R(config)#access-list 100 deny ip any any	
4	R(config)#crypto map map-name seq-num ipsec-isakmp	Création des mappes <ul style="list-style-type: none"> ○ 'map-name' ○ 'seq-num'
	R(config-crypto-map)#match address access- list	Déclaration de l'ACL qui identifie le trafic chiffré par IPSEC
	R(config-crypto-map)#set peer ip-address	Spécifie la station distante par son adresse IP
	R(config-crypto-map)#set transform-set trans-name(s)	Nom du step 1
	R(config-crypto-map)#set pfs group1	PFS <ul style="list-style-type: none"> ○ 'group1' par défaut
5	R(config)#interface serial 0	Application des mappages aux interfaces
	R(config-if)#crypto map map-name	
	R(config-if)#exit	

XVII.B.3 Application

```
c2621h#show running-config
Building configuration...

!
crypto isakmp policy 100
  hash md5
  authentication pre-share
crypto isakmp key cisco1234 address 192.168.34.5
!
!
crypto ipsec transform-set mine esp-des
!
crypto map mymap 100 ipsec-isakmp
  set peer 192.168.34.5
  set transform-set mine
  match address 102
!
!
!
interface FastEthernet0/0
  description Vers IBM
  ip address 192.168.33.5 255.255.255.0
  ip access-group 101 in
  speed 100
  full-duplex
  crypto map mymap
!
interface FastEthernet0/1
  description Le LAN
  ip address 192.168.32.5 255.255.255.0
  duplex auto
  speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.33.12
ip http server
ip pim bidir-enable
!
!
access-list 101 permit ahp host 192.168.34.5 host 192.168.33.5
access-list 101 permit esp host 192.168.34.5 host 192.168.33.5
access-list 101 permit udp host 192.168.34.5 host 192.168.33.5 eq isakmp
access-list 102 permit tcp 192.168.32.0 0.0.0.255 192.168.35.0 0.0.0.255
access-list 102 deny ip any any
!
!
end

c2621h#
```

```
c26211#show running-config
Building configuration...

!
!
crypto isakmp policy 100
  hash md5
  authentication pre-share
crypto isakmp key cisco1234 address 192.168.33.5
!
!
crypto ipsec transform-set mine esp-des
!
crypto map mymap 110 ipsec-isakmp
  set peer 192.168.33.5
  set transform-set mine
  match address 110
!
!
!
!
interface FastEthernet0/0
  ip address 192.168.34.5 255.255.255.0
  ip access-group 101 in
  duplex auto
  speed auto
  no cdp enable
  crypto map mymap
!
interface FastEthernet0/1
  ip address 192.168.35.5 255.255.255.0
  duplex auto
  speed auto
  no cdp enable
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.34.2
ip http server
!
!
access-list 101 permit ahp host 192.168.33.5 host 192.168.34.5
access-list 101 permit esp host 192.168.33.5 host 192.168.34.5
access-list 101 permit udp host 192.168.33.5 host 192.168.34.5 eq isakmp
access-list 110 permit tcp 192.168.35.0 0.0.0.255 192.168.32.0 0.0.0.255
access-list 110 deny ip any any
no cdp run
!
!
!
end
c26211#
```

XVII.B.4 Test et vérification

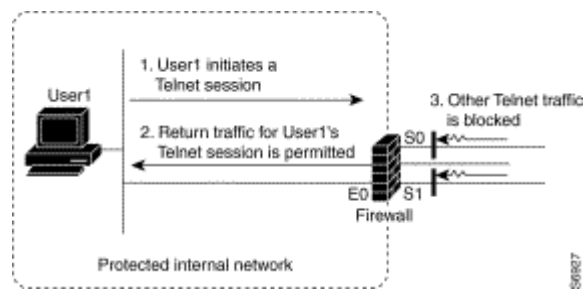
```
C2621xm#show running-config
!
interface Ethernet0/0
  ip address 192.168.16.5 255.255.255.0
  ip access-group 101 in
!
access-list 101 permit ahp permit 192.168.32.0 0.0.0.255 192.168.35.0 0.0.0.255
access-list 101 permit esp permit 192.168.32.0 0.0.0.255 192.168.35.0 0.0.0.255
access-list 101 permit udp permit 192.168.32.0 0.0.0.255 192.168.35.0 0.0.0.255 eq isakmp
!
C2621xm#
```

XVIII.CBAC : Contrôle d'accès basés contenu

CBAC : *Context-Based Access Control*

XVIII.A Présentation

- ❑ CBAC fournit un moteur d'inspection de paquets avec suivi de l'état des connexions (SPI) qui permet d'étendre les capacités de filtrage du routeur jusqu'au niveau application. Cette inspection repose sur l'emploi de liste d'accès CBAC.
- ❑ CBAC permet d'inspecter les paquets des applications qui utilisent TCP, ICMP (depuis la version 12.2.15T de IOS Cisco) et UDP des deux côtés du routeur, conférant à ce dernier des fonctions de pare-feu. CBAC n'est pas une implémentation pure de pare-feu et fait du routeur un équipement hybride, améliorant considérablement la sécurité du réseau.
- ❑ Le filtrage avancé de session au moyen du mécanisme CBAC permet un examen des informations des couches réseau et transport mais également celles des protocoles de la couche application (pour les connexions FTP par exemple), afin de connaître l'état des sessions TCP et UDP.



- ❑ De cette manière CBAC autorise le support de protocoles impliquant plusieurs canaux établis suite à des négociations sur le canal de contrôle.
- ❑ Pour définir un ensemble de règles la commande 'IP Inspect' est utilisée.
- ❑ CBAC permet de contrôler des protocoles de la couche application comme :
 - FTP
 - HTTP (association a un serveur de filtrage d'URL)
 - Java
 - RealAudio
 - RPC
 - SMTP
 - SQL NET
 - TFTP ...
- ❑ Lorsqu'une session se termine, les états associés et les règles créées dynamiquement dans les ACL sont détruits.

XVIII.B Configuration

```
C2503(config)#ip inspect ?
audit-trail      Enable the logging of session information (addresses and bytes)
dns-timeout      Specify timeout for DNS
max-incomplete   Specify maximum number of incomplete connections before clamping
name             Specify an inspection rule
one-minute       Specify one-minute-sample watermarks for clamping
tcp              Config timeout values for tcp connections
udp              Config timeout values for udp flows
<cr>
C2503(config)#ip inspect
```

Table 18 Timeout and Threshold Values		
Timeout or Threshold Value to Change	Command	Default
The length of time the software waits for a TCP session to reach the established state before dropping the session.	<code>ip inspect tcp synwait-time <i>seconds</i></code>	30 seconds
The length of time a TCP session will still be managed after the firewall detects a FIN-exchange.	<code>ip inspect tcp finwait-time <i>seconds</i></code>	5 seconds
The length of time a TCP session will still be managed after no activity (the TCP idle timeout). ¹	<code>ip inspect tcp idle-time <i>seconds</i></code>	3600 seconds (1 hour)
The length of time a UDP session will still be managed after no activity (the UDP idle timeout). ¹	<code>ip inspect udp idle-time <i>seconds</i></code>	30 seconds
The length of time a DNS name lookup session will still be managed after no activity.	<code>ip inspect dns-timeout <i>seconds</i></code>	5 seconds
The number of existing half-open sessions that will cause the software to start deleting half-open sessions. ²	<code>ip inspect max-incomplete high <i>number</i></code>	500 existing half-open sessions
The number of existing half-open sessions that will cause the software to stop deleting half-open sessions. ²	<code>ip inspect max-incomplete low <i>number</i></code>	400 existing half-open sessions
The rate of new sessions that will cause the software to start deleting half-open sessions. ²	<code>ip inspect one-minute high <i>number</i></code>	500 half-open sessions per minute
The rate of new sessions that will cause the software to stop deleting half-open sessions. ²	<code>ip inspect one-minute low <i>number</i></code>	400 half-open sessions per minute
The number of existing half-open TCP sessions with the same destination host address that will cause the software to start dropping half-open sessions to the same destination host address. ³	<code>ip inspect tcp max-incomplete host <i>number</i> block-time <i>minutes</i></code>	50 existing half-open TCP sessions; 0 minutes

¹The global TCP and UDP idle timeouts can be overridden for specified application-layer protocols' sessions as described in the `ip inspect` name (global configuration) command description, found in the "Context-Based Access Control Commands" chapter of the *Cisco IOS Security Command Reference*.

²See the following section, "Half-Open Sessions," for more information.

³Whenever the max-incomplete host threshold is exceeded, the software will drop half-open sessions differently depending on whether the block-time timeout is zero or a positive non-zero number. If the block-time timeout is zero, the software will delete the oldest existing half-open session for the host for every new connection request to the host and will let the SYN packet through. If the block-time timeout is greater than zero, the software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the block-time expires.

To reset any threshold or timeout to the default value, use the no form of the command in [Table 18](#).

```
C2503(config)#ip inspect audit-trail ?
<cr>

C2503(config)#ip inspect dns-timeout ?
<1-2147483647> Timeout in seconds

C2503(config)#ip inspect max-incomplete ?
high Specify high-watermark for clamping
low Specify low-watermark for clamping

C2503(config)#ip inspect one-minute ?
high Specify high-watermark for clamping
low Specify low-watermark for clamping

C2503(config)#ip inspect tcp ?
finwait-time Specify timeout for TCP connections after a FIN
idle-time Specify idle timeout for tcp connections
max-incomplete Specify max half-open connection per host
synwait-time Specify timeout for TCP connections after a SYN and no further data

C2503(config)#ip inspect udp ?
idle-time Specify idle timeout for udp

C2503(config)#ip inspect udp
```

```
C2503(config)#ip inspect name fw ?
cuseeme CUSeeMe Protocol
fragment IP fragment inspection
ftp File Transfer Protocol
```



```

h323      H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
http      HTTP Protocol
rcmd      R commands (r-exec, r-login, r-sh)
realaudio Real Audio Protocol
rpc       Remote Procedure Call Protocol
smtp      Simple Mail Transfer Protocol
sqlnet    SQL Net Protocol
streamworks StreamWorks Protocol
tcp       Transmission Control Protocol
tftp      TFTP Protocol
udp       User Datagram Protocol
vdolive   VDOLive Protocol
<cr>

```

```
C2503(config)#ip inspect name fw
```

XVIII.C Verifying CBAC

- ❑ You can view and verify CBAC configuration, status, statistics, and session information by using one or more of the following commands in EXEC mode:

Command	Purpose
Router# show ip access-lists	Displays the contents of all current IP access lists.
Router# show ip inspect name <i>inspection-name</i>	Shows a particular configured inspection rule.
Router# show ip inspect config	Shows the complete CBAC inspection configuration.
Router# show ip inspect interfaces	Shows interface configuration with regards to applied inspection rules and access lists.
Router# show ip inspect session [detail]	Shows existing sessions that are currently being tracked and inspected by CBAC.
Router# show ip inspect all	Shows all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.

- ❑ In most cases, you can tell whether CBAC is inspecting network traffic properly because network applications are working as expected. In some cases, however, you might want to verify CBAC operation. For example, to verify RTSP or H.323 inspection, initiate an RTSP- or H.323-based application through the firewall. Use the show ip inspect session and show ip access lists commands to verify CBAC operation. These commands display the dynamic ACL entries and the established connections for a multimedia session.

XVIII.D Ethernet Interface Configuration Example

- ❑ This example looks at each of these four components. For this example, CBAC is being configured to inspect RTSP and H.323 protocol traffic inbound from the protected network on a router with two Ethernet interfaces. Interface Ethernet1/0 is the protected network and interface Ethernet1/1 is the unprotected network. The security policy for the protected site uses access control lists (ACLs) to restrict inbound traffic on the unprotected interface to specific ICMP protocol traffic, denying inbound access for TCP and UDP protocol traffic. Inbound access for specific protocol traffic is provided through dynamic access lists, which are generated according to CBAC inspection rules.
- ❑ ACL 100 denies TCP and UDP traffic from any source or destination while permitting specific ICMP protocol traffic. The final deny statement is not required, but is included for explicitness—the final entry in any ACL is an implicit denial of all IP protocol traffic.

```
Router(config)# access-list 100 deny tcp any any
Router(config)# access-list 100 deny udp any any
Router(config)# access-list 100 permit icmp any any echo-reply
Router(config)# access-list 100 permit icmp any any time-exceeded
Router(config)# access-list 100 permit icmp any any packet-too-big
Router(config)# access-list 100 permit icmp any any traceroute
Router(config)# access-list 100 permit icmp any any unreachable
Router(config)# access-list 100 deny ip any any
```

- ❑ ACL 100 is applied inbound at interface Ethernet1/1 to block all access from the unprotected network to the protected network.

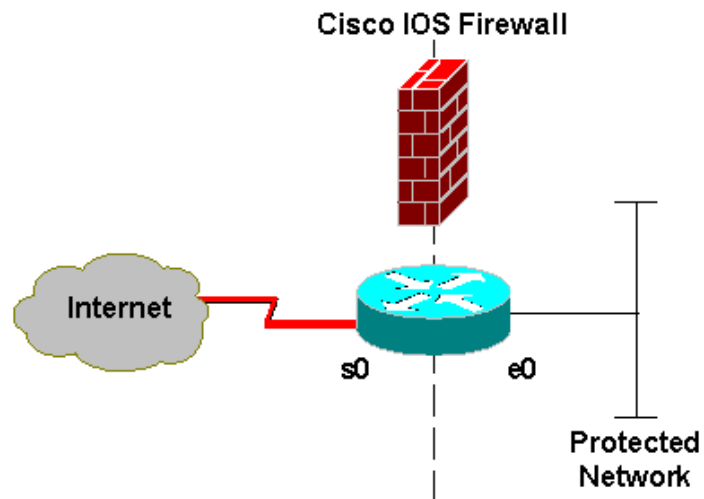
```
Router(config)# interface Ethernet1/1
Router(config-if)# ip access-group 100 in
```

- ❑ An inspection rule is created for "hqusers" that covers two protocols: RTSP and H.323.

```
Router(config)# ip inspect name hqusers rtsp
Router(config)# ip inspect name hqusers h323
```

- ❑ The inspection rule is applied inbound at interface Ethernet1/0 to inspect traffic from users on the protected network. When CBAC detects multimedia traffic from the protected network, CBAC creates dynamic entries in access list 100 to allow return traffic for multimedia sessions.

```
Router(config)# interface Ethernet1/0
Router(config-if)# ip inspect hqusers in
```

XVIII.E Application #1**XVIII.E.1 Example #1- Without CBAC**

- Without CBAC, a simplified partial configuration might look something like this:

```

!--- Ethernet 0 is the internal protected network.
interface ethernet 0
  ip address 10.0.0.1
!
!--- Network traffic from the Internet comes in Serial 0.
interface serial 0
  ip address 1.1.1.1
  ip access-group 101 in
!
!--- Lets in data associated with TCP connections we've made
!--- outgoing. This opens us to some fragmentation attacks. One
!--- Linux kernel security hack makes this a potential way
!--- to make a new connection to a Linux box from outside.
access-list 101 permit tcp any any established
!
!--- Our internal Domain Name System (DNS) Server (at 10.0.0.2) may send
!--- requests to other DNS servers using port 53. This entry
!--- also allows outside machines to query our DNS.
access-list 101 permit udp any host 10.0.0.2 eq 53
!
!--- We need this access list to give our users access to
!--- UDP-based services on the outside.
access-list 101 permit udp any any gt 1024
!
!--- We need this access list to allow users to access passive ftp.
access-list 101 permit tcp any any gt 1023
!
access-list 101 deny ip any any

```

With this configuration, users have to be selective about which clients they use for FTP, the UNIX rsh-based commands don't work, and there are still serious security risks. Any UDP service at a port above 1024 is available. This could be improved by blocking known dangerous ports, but that is a huge administrative burden, and not very reliable. If a proxy DNS server were used, we could block all UDP ports except the ports known to be used by safe programs, but again there would be a large administrative burden, and an unsafe service could choose the same port used by a safe one.

XVIII.E.2 Example #2 - Using CBAC

- ❑ Nécessite un IOS Firewall
- ❑ With CBAC, the simplified partial configuration looks something like this:

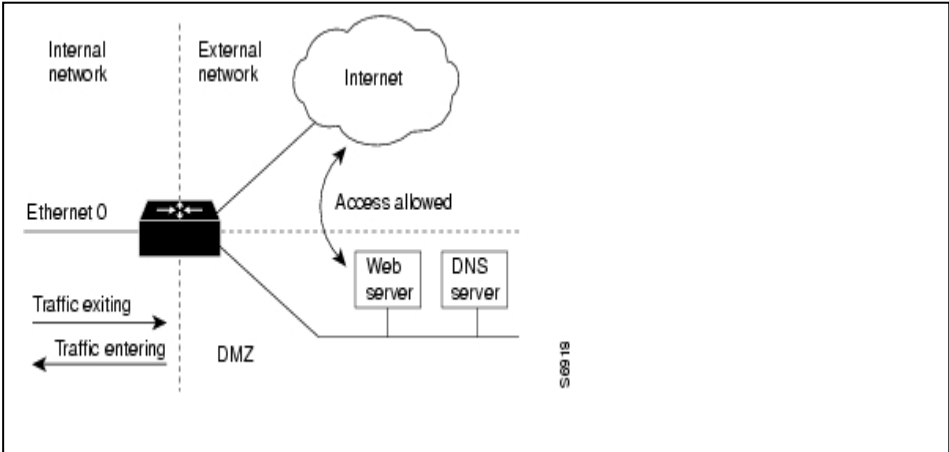
```

!--- Ethernet0 is the private internal network.
interface ethernet 0
  ip address 10.0.0.1
!
!--- Inspection is applied incoming, because connection initiation packets will be coming into this interface from the private
!--- network. Inspection always applies in the direction of conversation initiation, even though it may affect packets that are
!--- flowing in both directions. No conversations are allowed to be initiated from the Internet to the
!--- private network, so we have no inspection in that direction.
  ip inspect firewall in
!
!--- Network traffic from the Internet comes in Serial0.
interface serial 0
  ip address 1.1.1.1
  ip access-group 101 in
!
!--- The access list permits nothing onto the inside network (a real list would probably allow some ICMP traffic).
!--- CBAC opens holes in response to connections initiated from the
!--- private network, so return traffic will get through.
access-list 101 deny ip any any
!
!--- Here's the list of protocols we inspect. The assumption is that we want people on the private network to be able
!--- to create any kind of outgoing conversation.
ip inspect name firewall cuseeme
ip inspect name firewall ftp
ip inspect name firewall h323
!
!--- HTTP inspection is really a no-op here, equivalent to plain TCP inspection. You could turn on Java filtering here,
!--- but it's only really recommended if you have a specific threat to block.
ip inspect name firewall http
ip inspect name firewall netshow
ip inspect name firewall rcmd
ip inspect name firewall realaudio
!
!--- Note that Simple Mail Transfer Protocol (SMTP) inspection looks
!--- for bogus commands; no auxiliary channels are needed.
ip inspect name firewall smtp
ip inspect name firewall sqlnet
ip inspect name firewall streamworks
ip inspect name firewall tftp
!
!--- Generic TCP inspection lets almost any protocol work properly, as
!--- long as it uses only a single TCP connection.
ip inspect name firewall tcp
!
!--- Generic UDP is like generic TCP: as long as there is only one client
!--- host/port and one server host/port, it works for any UDP protocol.
ip inspect name firewall udp
ip inspect name firewall vdolive

```

This configuration is long, but not complicated; most of the lines simply turn on every possible kind of inspection (except SUN Remote Procedure Call protocol [RPC]). This configuration lets users use any TCP service that uses only one connection, any UDP service that uses only one server host/port and one client host/port, and several multimedia services. Users can use any FTP client or TFTP, and they can do r-commands. At the same time, the security exposure is much less than in Example #1. TCP packets can flow from the outside only in response to traffic sent from the inside. The limitations of the established keyword are avoided.

XVIII.F Application #2



XVIII.G Application #3

```

service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Cisco3620
!
enable secret CISCO
!
!
ip source-route
ip name-server 172.16.10.1
!
ip subnet-zero
ip domain-lookup
ip routing
!
! Context-Based Access Control
!
no ip inspect audit-trail
ip inspect tcp synwait-time 30
ip inspect tcp finwait-time 5
ip inspect tcp idle-time 3600
ip inspect udp idle-time 30
ip inspect dns-timeout 5
ip inspect one-minute low 900
ip inspect one-minute high 1100
ip inspect max-incomplete low 900
ip inspect max-incomplete high 1100
ip inspect tcp max-incomplete host 50 block-time 0
!
! IP inspect Ethernet_0_0
!
no ip inspect name Ethernet_0_0
ip inspect name Ethernet_0_0 tcp
ip inspect name Ethernet_0_0 udp
ip inspect name Ethernet_0_0 cuseeme
ip inspect name Ethernet_0_0 ftp
ip inspect name Ethernet_0_0 h323
ip inspect name Ethernet_0_0 rcmd
ip inspect name Ethernet_0_0 realaudio
ip inspect name Ethernet_0_0 smtp
ip inspect name Ethernet_0_0 streamworks
ip inspect name Ethernet_0_0 vdolive
ip inspect name Ethernet_0_0 sqlnet
ip inspect name Ethernet_0_0 tftp
!
interface Ethernet 0/0
no shutdown
description connected to EthernetLAN_1
ip address 172.16.16.1 255.255.248.0
ip helper-address 172.8.20.1
ip inspect Ethernet_0_0 in
ip access-group 100 in
!
!
interface Serial 1/0
no shutdown
description connected to Cisco1720
ip address 192.168.8.2 255.255.255.252
ip access-group 101 in
encapsulation hdlc
!
! Access Control List 100
!
no access-list 100
access-list 100 deny ip 192.168.8.0 0.0.0.3 any
access-list 100 deny ip 172.16.8.0 0.0.7.255 any
access-list 100 permit ip host 172.16.16.100 192.168.8.0 0.0.0.3
access-list 100 permit ip host 172.16.16.100 172.16.8.0 0.0.7.255
!
! Access Control List 101
!
no access-list 101
access-list 101 deny ip any any
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 1/0 1
ip http server
!
snmp-server community public RO
snmp-server community private RW
snmp-server location Paris
snmp-server contact NET_MANAGER,01.39.33.00.01,NETMANAGER@gefi.com
snmp-server host 172.16.1.10 public
!
ip forward-protocol udp 135
!
line console 0
exec-timeout 0 0
password cisco
login
!
line vty 0 4
password cisco
login
!
end

```

XIX. SNMP

SNMP : Simple Network Management Protocol

- ❑ En août 1988 apparaît la première référence au protocole SNMP dans la RFC 1067. La phrase d'introduction présente de manière explicite l'intérêt du protocole : *This memo defines a simple protocol by which management information for a network element may be inspected or altered by logically remote users.*
- ❑ Un administrateur de réseau a besoin de logiciels lui permettant par exemple de résoudre les différents problèmes qui surviennent sur le réseau, de contrôler le routage et d'effectuer des statistiques sur le trafic. SNMP permet d'administrer les équipements réseau de manière centralisée.
- ❑ Le protocole est ouvert, il gère les données d'équipements de constructeurs différents.
- ❑ Dans un environnement TCP/IP, le management de l'inter-réseau est situé au niveau applicatif. Il s'appuie sur TCP/IP pour transmettre les différents messages qu'il induit.
- ❑ SNMP est encapsulé par UDP dans les ports 161 et 162.
- ❑ Les outils d'administration réseau (**Sun Net Manager**, **HP Open View**, **SNMPC...**) se basent en règle générale sur le protocole SNMP.

XIX.A Architecture

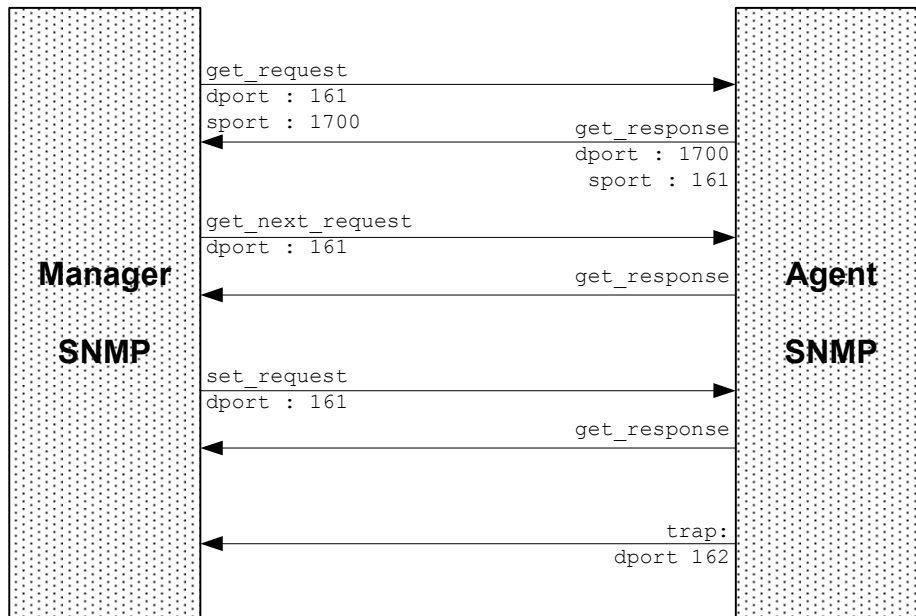
- ❑ Le groupe de protocoles TCP/IP n'a pas de protocole standard officiel pour la communication d'informations de management. Deux standards sont toutefois recommandés : SNMP et CMOT.
- ❑ SNMP (*Simple Network Management Protocol*) est de loin le plus largement utilisé. CMOT (*CMOP over TCP*) précise l'utilisation sur une connexion TCP du standard ISO CMIP (*Common Management Information Protocol*).
- ❑ Deux types de machines participent au processus de management :
 - Des agents ; programme et une base de données de gestion des objets et variables propres à la machine. Ils conservent des informations que le ou les managers ont la possibilité de consulter ou de modifier par des requêtes. Ces agents gardent, par exemple, des statistiques sur l'état des interfaces réseau, sur le trafic entrant et sortant, sur les messages d'erreurs générés. Ces agents peuvent être implémentés sur des HUB, Switchs, Routeurs, etc.
 - Un manager (NMS : *Network Management Station*), application à partir duquel est contrôlé et administré le réseau. Un programme de gestion centrale y réside ainsi qu'une base de données globale.
- ❑ Le manager SNMP (NMS) communique avec ses agents de deux manières :
 - Le '*polling*' : périodiquement le manager interroge les agents.
 - Les '*traps*' : un agent informe le manager d'événement.

XIX.B Les références

- ❑ SNMP : RFC 1157 et 1155
- ❑ SNMPv2 : RFC1441 et1452

XIX.C Le format d'un message SNMP

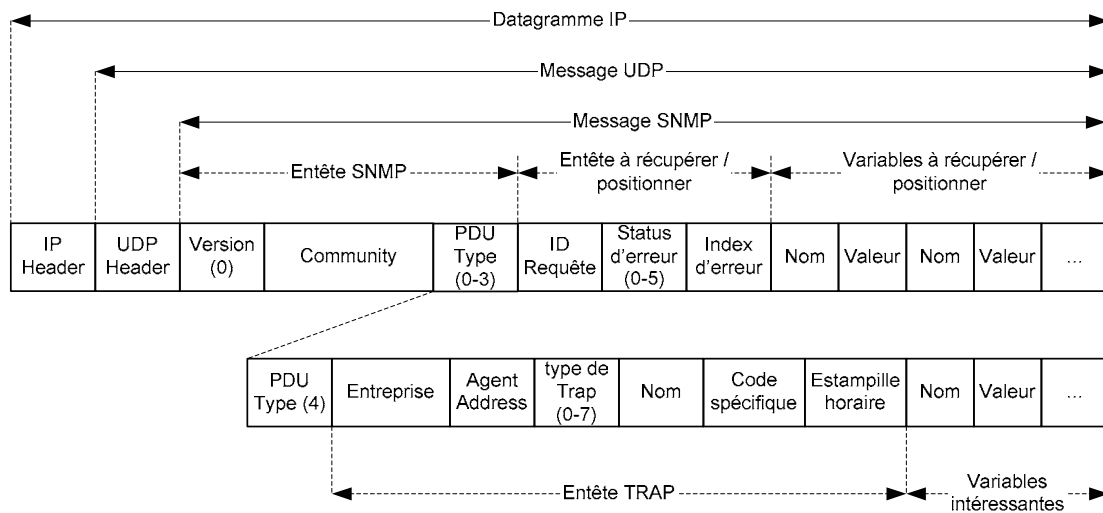
- ❑ Le protocole SNMP version 1 (SNMPv1) est décrit dans la RFC 1157.
- ❑ Les messages SNMP ou snmp-PDU sont encapsulés dans des messages UDP.
 - Les messages 'Get_Request', 'Get_Next', 'Set_Request' et 'Get_Response' utilisent le port 161.
 - Tandis que le message 'Trap' utilise le port 162.



- ❑ Les variables transmises par les messages SNMP sont décrites en ASN.1 (ou plutôt SMI).
- ❑ Le codage binaire du message ASN.1 repose ensuite sur la méthode BER (Basic Encoding Rules, CCITT X209). BER définit notamment que le huitième bit d'un octet est envoyé en premier et que les entiers signés sont codés en complément à deux.

- ❑ Il existe 5 types de messages :

get_request	Demande la lecture d'une variable.
get_next_request	Demande la lecture de la variable suivante, permet le parcours d'une table ou d'une liste.
set_request	Demande la modification d'une variable.
get_response	Réponse de l'agent à une requête (GET ou SET).
trap	Notification un événement par un agent à une station de management.



- ❑ Le champ 'Version' indique la version SNMP. La valeur '0' désigne SNMPv1.
- ❑ Le champ 'Community' désigne le nom qui permet d'authentifier le manager avant de lui donner l'accès à l'agent. La 'Community' réalise la fonction d'identification et d'authentification.
- ❑ Le champ type de PDU :
 - '0' -> 'get-request'
 - '1' -> 'get-next-request'
 - '2' -> 'set-request'
 - '3' -> 'get-response'
 - '4' -> 'trap'
- ❑ Le champ 'Statut d'erreur'

Statut d'erreur	Nom	Description
0	noError	Tout est OK.
1	tooBig	L'agent ne peut pas récupérer la réponse en seul message.
2	noSuchName	L'opération spécifiée une variable non existante.
3	badValue	Une opération d'écriture spécifiée une valeur ou une syntaxe invalide.
4	readOnly	Le manager a essayé de modifier une variable en lecture seule.
5	genErr	Une autre erreur.

- ❑ Le champ index d'erreur spécifie la variable en erreur.

- ❑ Type de Trap :

Type de trap	Nom	Description
0	coldStart	L'agent est lui-même initialisé.
1	warmStart	L'agent est lui-même réinitialisé.
2	linkDown	Une interface est passée de l'état actif à désactif. La première variable du message identifie l'interface.
3	linkUp	Une interface est passée de l'état désactif à actif. La première variable du message identifie l'interface.
4	authenticationFailure	Le manager SMP a émis un message avec un nom de 'Community' invalide.
5	egpNeighborLoss	Un homologue EGP a été désactivé. La première variable du message identifie l'homologue par son adresse IP.
6	enterpriseSpecific	Ce type de Trap permet à un constructeur d'implémenter un Trap spécifique à l'entreprise. Regardez le champ 'Specific Code' pour avoir une information sur le Trap.

- ❑ La commande *Get* permet d'obtenir des informations de l'agent, par exemple nom de l'équipement (« *SysName* »), localisation (« *SysLocation* »), paquets en in ou out ...
- ❑ La commande *Set* permet d'écrire une information, par exemple « *Sysname* », « *SysLocation* ». Cette commande est très puissante, elle permet par exemple de passer une interface dans l'état inactive (« *Shut Down* »), ou sur un équipement Cisco de télécharger une configuration.
- ❑ Trap permet à l'agent de remonter une information au manager, par exemple « *LinkDown* ».

XIX.D SNMPv1, v2 et v3

- ❑ Dans SNMPv1 aucune sécurité n'est implémentée. Les noms de 'Community' circulent en clair sur le réseau.
- ❑ Dans SNMPv2, l'IETF propose un modèle de sécurité permettant une authentification ainsi que le chiffrement des informations. Cependant, les dissensions parmi les éditeurs participant au projet ainsi que les problèmes d'interopérabilité avec l'existant ont imposé l'utilisation du modèle de sécurité de la v1. Cette réutilisation des 'Community' pour l'identification et l'authentification a donc donné un standard **SNMP v2c**.
- ❑ SNMPv3 implémente le modèle de sécurité définie dans la v2. Cependant, peu de systèmes supportant des agents SNMPv3 sont disponibles et la migration s'annonce longue.

XIX.E La MIB

MIB : Management Information Base

XIX.E.1 Présentation

- ❑ Les informations gérées par un agent sont organisées en MIB. On y trouve aussi bien des statistiques réseaux comme le nombre de trames émis ou reçus avec ou sans erreur que la configuration de l'équipement.

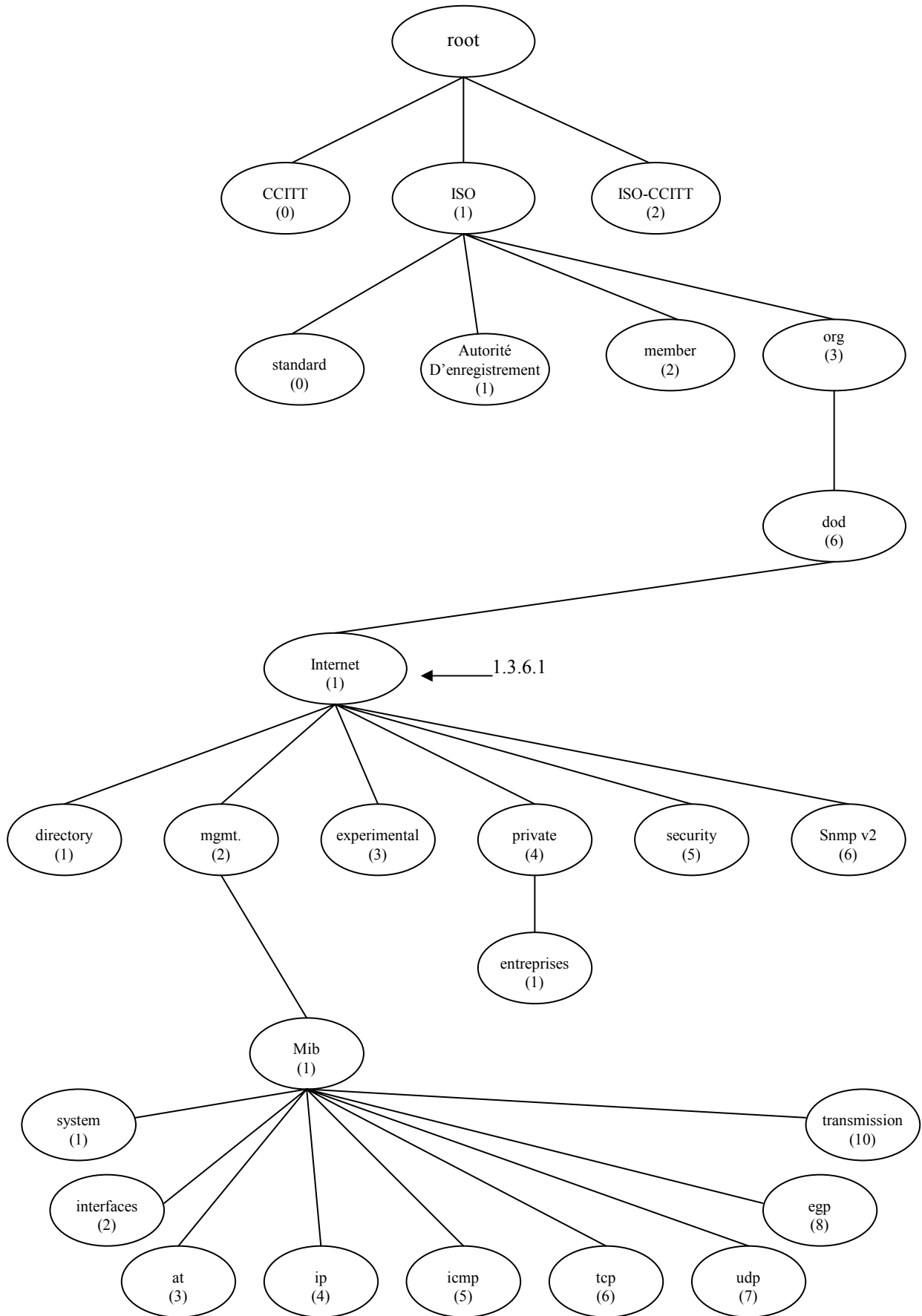
- ❑ Référence : RFC 1213 pour la MIB II

- ❑ Les deux groupes de travail qui ont proposé SNMP et CMOT ont coopéré initialement pour définir un standard concernant les données de management réseau. Ce standard est donc indépendant du protocole utilisé (SNMP ou CMIP).

- ❑ Connue sous le nom de la MIB (Management Information Base), le standard spécifie les types de données qu'un hôte ou un routeur IP doit conserver et les opérations permises sur ces types de données.

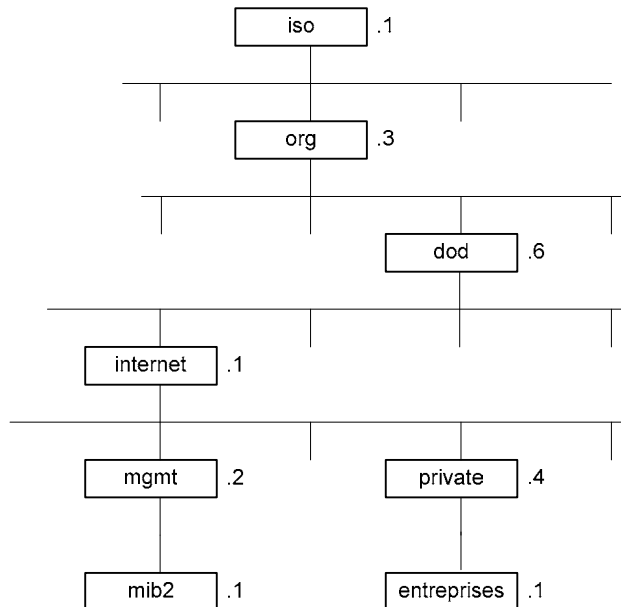
XIX.E.2 Identification des objets :

- ❑ Chaque variable définie dans une MIB est référencée de manière unique par son OID (Object Identifier). Cet OID indique l'emplacement de la variable dans un arbre comparable à celui constitué par les fichiers et les répertoires d'un système de fichiers d'un ordinateur.



XIX.E.3 MIB normalisées et propriétaires

- ❑ Il existe des MIB normalisées et des MIB propriétaires.
- ❑ Un agent SNMP doit supporter au moins la **MIB II**. Celle-ci, définie par la RFC 1213, contient les paramètres TCP/IP les plus courants. Elle commence par l'**OID 1.3.6.1.2.1**.



- ❑ Il existe des **MIB propriétaires** qui sont définies par les constructeurs et éditeurs eux-mêmes pour leurs équipements. Leur **OID** commence par **1.3.6.1.4.1** suivi de l'identification de l'entreprise :

OID des MIB propriétaires : 1.3.6.1.4.1.x

OID	Constructeur	OID	Constructeur
2	IBM	63	Apple
9	Cisco	71	NASA
11	HP	74	ATT
20	MIT	111	Oracle
23	Novell	193	Ericsson
42	Sun	232	Compaq
43	3Com	253	Xerox
59	SGI	311	Microsoft

OID des MIB propriétaires liées à Linux : 1.3.6.1.4.1.x

OID	Constructeur	OID	Constructeur
2312	RedHat	6893	TurboLinux
4682	Linux-HA Project	7057	Suse Linux
6500	VA Linux Systems	9586	Debian

XIX.E.4 MIB II

- La définition initiale de la MIB classe en huit catégories les informations de management (appelées variables MIB) :

Éléments du premier niveau de la MIB II :		
OID : 1.3.6.1.2.1. ou iso(1).org(3).dod(6).internet(1).mgmt(2).mib(1).		
1	system	The host or gateway operating system
2	interfaces	Individual network interfaces
3	at	Address Translation (ex : ARP)
4	ip	Internet Protocol Software
5	icmp	Internet Control Message Protocol software
6	tcp	Transmission Control Protocol software
7	udp	User Datagram Protocol software
8	egp	Exterior Gateway Protocol software
11	snmp	
14	ospf	
15	bgp	
16	rmon	
23	rip-2	
32	dns	

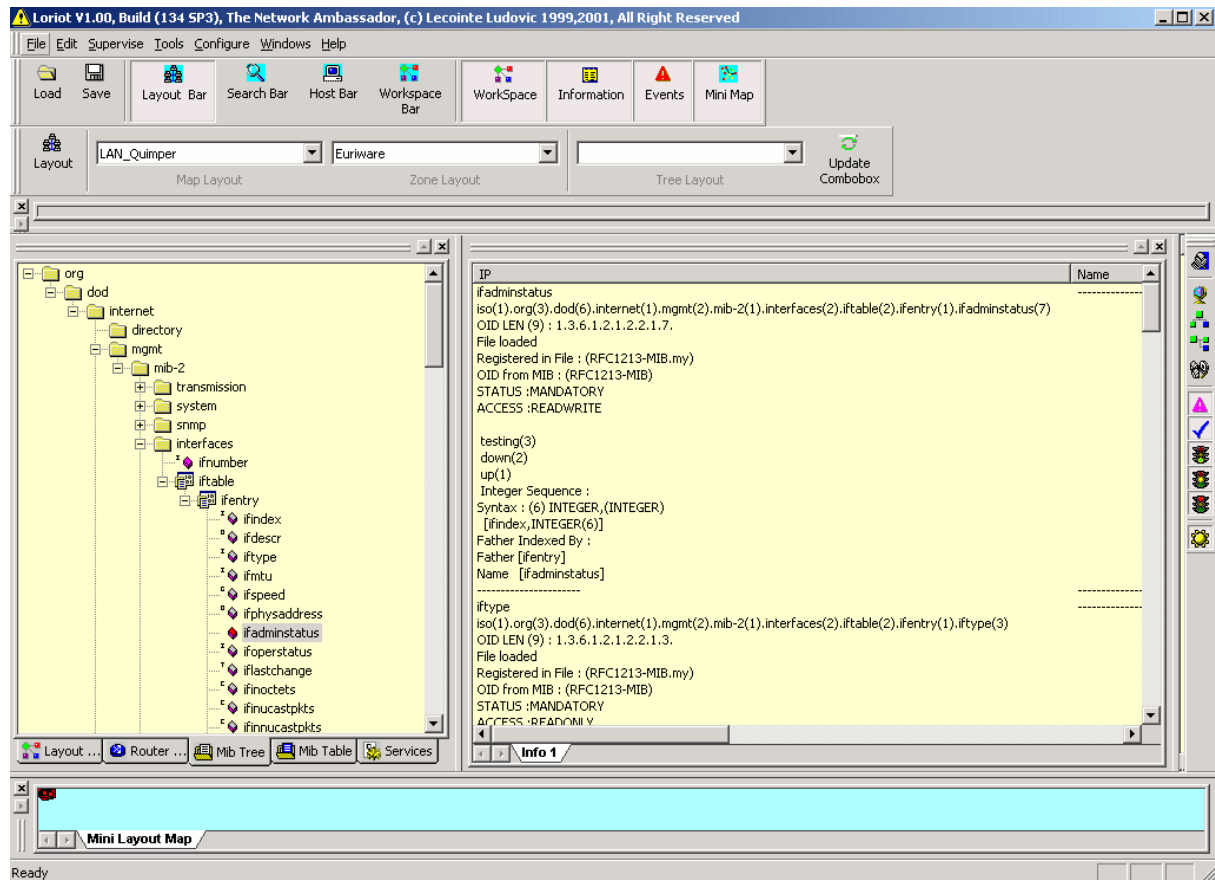
- Toute variable MIB est identifiée par une suite de chiffres séparés par des points. Toute identification d'une variable MIB a comme préfixe 1.3.6.1.2.1. Le chiffre suivant compris entre 1 et 8 indique la catégorie à laquelle appartient la variable MIB (system, ip, ...). Le chiffre suivant enfin identifie la variable dans la catégorie.
 - Par exemple, 1.3.6.1.2.1.4.3 correspondant à la variable ipInReceives

1.3.6.1.2.1.2.2.1.7

iso.org.dod.internet.mgmt.mib-2.interfaces.iftable.ifentry.ifadminstatus

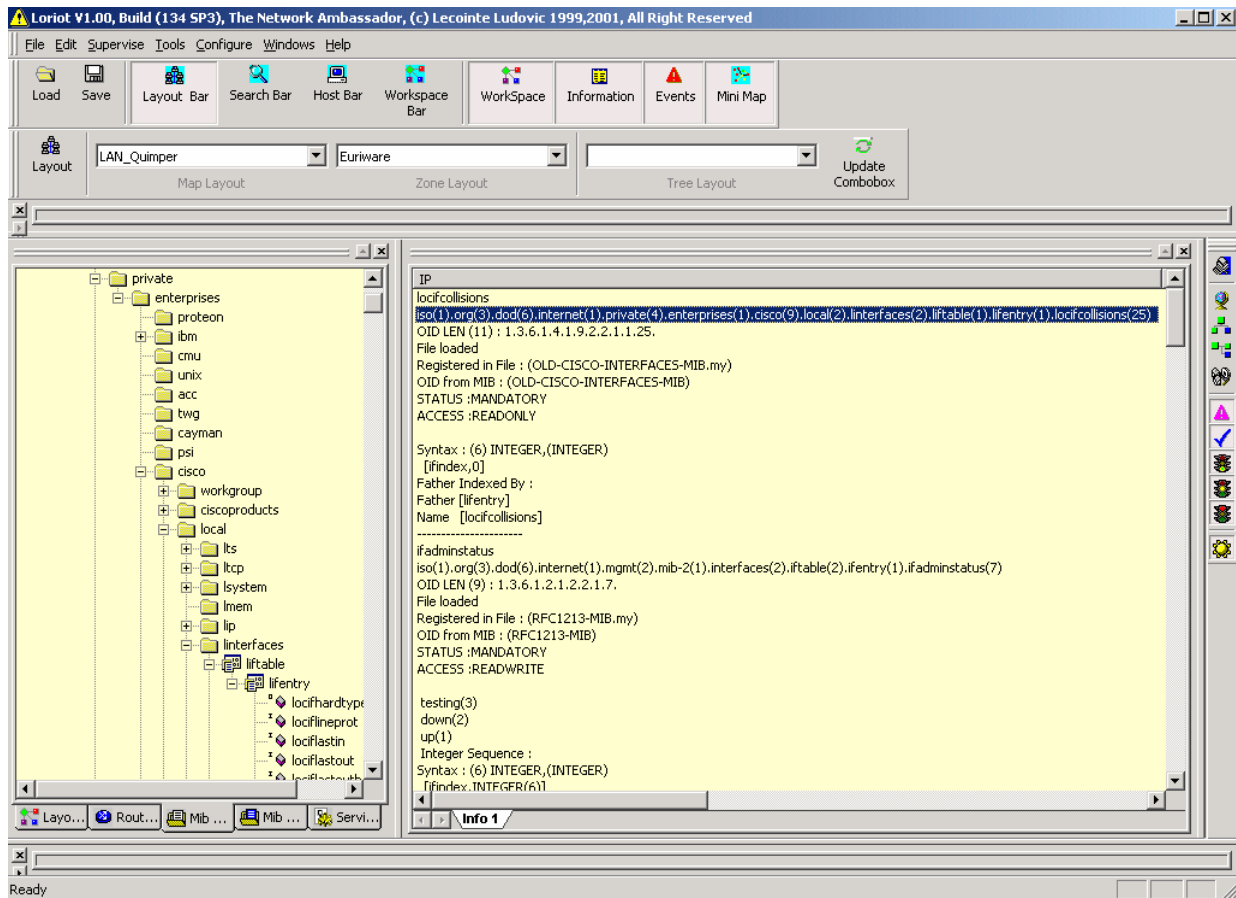
- Chaque objet correspond à une variable pouvant être lue ou modifiée. Les objets peuvent être atteints par un identifiant correspondant à une suite de chiffres séparés par des points, par exemple 1.3.6.1.2.1.2.2.1.7.
- Afin de permettre une compréhension plus facile on utilise une MIB (Management Information Base) qui va traduire ces chiffres en variables, par exemple iso.org.dod.internet.mgmt.mib-2.interfaces.iftable.ifentry.ifadminstatus.

Le groupe system :																										
OID : 1.3.6.1.2.1.1 ou																										
iso(1).org(3).dod(6).internet(1).mgmt(2).mib(1).system(1)																										
1	sysDescr	Décrit le noeud : nom du processeur et de l'OS.																								
2	sysObjectId	Spécifie l'OID de l'entreprise qui commercialise ce noeud.																								
3	sysUpTime	Le temps écoulé en centièmes de secondes depuis le démarrage de l'équipement.																								
4	sysContact	Le nom de la personne responsable du noeud, avec éventuellement son numéro de téléphone et son email.																								
5	sysName	Le nom du noeud.																								
6	sysLocator	Le lieu physique où se situe l'équipement (noeud).																								
7	sysServices	C'est un entier qui spécifie les services supportés par le noeud. Cet entier est créé par un OU logique à partir des constantes suivantes : <table border="1" data-bbox="703 725 1291 981"> <thead> <tr> <th>Bit</th> <th>Fonction</th> <th>Couche OSI</th> </tr> </thead> <tbody> <tr> <td>0x01</td> <td>Physical</td> <td>1</td> </tr> <tr> <td>0x02</td> <td>Data Link</td> <td>2</td> </tr> <tr> <td>0x04</td> <td></td> <td>3</td> </tr> <tr> <td>0x08</td> <td></td> <td>4</td> </tr> <tr> <td>0x10</td> <td></td> <td>5</td> </tr> <tr> <td>0x20</td> <td></td> <td>6</td> </tr> <tr> <td>0x40</td> <td></td> <td>7</td> </tr> </tbody> </table>	Bit	Fonction	Couche OSI	0x01	Physical	1	0x02	Data Link	2	0x04		3	0x08		4	0x10		5	0x20		6	0x40		7
Bit	Fonction	Couche OSI																								
0x01	Physical	1																								
0x02	Data Link	2																								
0x04		3																								
0x08		4																								
0x10		5																								
0x20		6																								
0x40		7																								

Exemple :

- ❑ Nous pouvons voir que l'objet 1.3.6.1.2.1.2.2.1.7. correspond à la variable Ifadminstatus(7) et peut prendre comme valeur un « integer » de 1 à 3 (1 pour UP, 2 pour down et 3 pour test).
 - Si l'on écrit 2 (« integer ») dans cet objet on passe l'interface en mode « administrativement down ».
- ❑ Le produit d'administration réseau utilisé pour cet exemple est un produit aujourd'hui libre, il est possible de le télécharger sous <http://lecointe.com>
- ❑ Le problème de l'administrateur réseau est d'intégrer les différentes MIB au niveau de sa station d'administration, on dit « compiler les MIBs », chaque objet doit se rattacher à un objet père, l'origine étant root.
- ❑ Vous comprendrez que l'ordre de compilation est essentiel.
- ❑ Chaque constructeur a développé ses propres objets et bien sur ses propres MIB.
- ❑ Chaque montée en version de l'IOS peut enrichir l'agent SNMP de l'équipement.
- ❑ Il faut parfois plusieurs mois à un administrateur pour configurer sa station, surtout dans un contexte multi constructeurs.

Exemple :



Nous voyons ici un objet permettant de remonter le nombre de collisions sur une interface.

Différentes branches et feuilles d'intérêt définies dans la MIB2					
OID	Nom	Description	Type		Exemple
.1.3.6.1.2.1.1	system				
.1.3.6.1.2.1.1.1	sysDescr	Description du système, fixée par l'éditeur.	String	R	Cisco Internetwork Operating System Software
.1.3.6.1.2.1.1.2	sysObjectID	Pointeur sur la branche 'entreprise' de la MIB	OID	R	.1.3.6.1.4.1.1.9.1.469
.1.3.6.1.2.1.1.5	sysName	Nom administratif du système, le FQDN par convention	String	R/W	www.gefi.com
.1.3.6.1.2.1.2.1	ifNumber	Nombre de NIC sur l'équipement	Entier	R	24
.1.3.6.1.2.1.2.2.1.2[ifIndex]	ifDescr	Description de l'interface	String	R	Intel(R) PRO/100 VE Network
.1.3.6.1.2.1.2.2.1.6[ifIndex]	ifPhysAddress	Adresse physique de l'interface	String	R	0:0:1:e6:49:60
.1.3.6.1.2.1.4.1	ipForwarding	Routage IP actif	Entier	R/W	1 -> Forwarding
.1.3.6.1.2.1.4.2	defaultTTL	TTL par défaut	Entier	R/W	
.1.3.6.1.2.1.4.22.1.2.1[ipAddress]	ipNetToMediaPhysAddress	Adresse physique correspondant à l'adresse IP dans l'OID	String	R/W	

XIX.E.5 RMON

- ❑ RMON (Remote Monitoring) est une MIB standard qui définit des statistiques associées à la couche liaison. Cette MIB permet à une station de management SNMP d'avoir une vue globale du trafic réseau traversant cet équipement (routeur et switch).

- ❑ Les RFC :
 - Rmon version 1 est spécifié dans les RFC 1271 et 2819.
 - Rmon version 2 est spécifié dans la RFC 2021.

XIX.F Configuration des agents

Définition des « Noms de community » :

- ❑ Les noms de 'community' par défaut pour la plus part des produits d'administration réseau sont :
 - 'public' pour la lecture et
 - 'private' pour l'écriture.
- ❑ Par défaut un équipement Cisco ne répond pas aux requêtes SNMP.
- ❑ La commande 'SNMP-Server Community' permet de configurer les « noms de community » et leurs droits.

Commandes	Description
# snmp-server community public ro	Active SNMP et permet un accès en lecture seule aux hôtes utilisant la chaîne 'public'.
# snmp-server community private rw	Active SNMP et permet un accès en lecture et écriture aux hôtes utilisant la chaîne 'private'.
# snmp-server host 192.168.0.1 public	Définit l'hôte 192.168.0.1 comme destinataire des messages trap SNMP avec la chaîne de communauté 'public'.

Champs de la commande	Description
snmp-server	
community	
WORD	'Word' représente le nom de community
droits	Droits : <ul style="list-style-type: none"> ○ 'RO' pour la lecture, ○ 'RW' pour la lecture et l'écriture
[ACL]	ACL : est une option permettant d'indiquer une access-list

Commandes	Commentaires
access-list 2 permit 192.168.3.32 0.0.0.1	ACL qui autorise les stations à l'accès SNMP 'Public'
snmp-server community private RW 2	Création de la community 'Private' en Read/Write aux stations correspondant à l'ACL 2.
snmp-server packetsize 4096	La taille par défaut est de 484 octets
snmp-server trap-authentication	Remonte des traps si des accès avec un nom de community incorrecte
snmp-server host 192.168.3.32 public	Identification du destinataire des TRAPs

Exemple :

Format de la commande :
snmp-server community <chaîne de caractères> {RO rw} [<access list>]
snmp-server community public RO 99
snmp-server community private RW 99

- ❑ Dans cet exemple le manager utilisera 'public' pour lire et 'private' pour écrire, cette station devra être autorisée au niveau de l'access liste 99.
- ❑ La commande 'snmp-server host' permet de définir la station recevant les traps.

Format de la commande :

```
snmp-server host @ip trap community
```

```
snmp-server host 10.6.48.100 trap public
```

Champs de la commande	Description
snmp-server	
host	
WORD	
10.6.48.100	Adresse IP de la station d'administration
trap	
public	le nom de community

Exemple :

```
snmp-server host 10.6.48.100 trap public
```

- ❑ L'équipement remontera ses traps à la station 10.6.48.100 avec le nom de community : « public ».
- ❑ Un routeur dispose de plusieurs interfaces donc de plusieurs adresses IP. Il est intéressant de recevoir les traps toujours de la même adresse, toutes les adresses ne sont pas forcément connues du DNS ou du fichier hosts. Ceci est possible grâce à la commande suivante :

```
snmp-server trap-source ethernet 0/0
```

- ❑ L'administrateur peut également définir les « traps » souhaités :

```
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps syslog
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
```

Lecture conseillée :

http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:SNMP

XIX.G NMS

NMS : Network Management Station

- Installation et utilisation des produits ;
 - SNMPc Network Manager : <http://www.castlerock.com>
 - SolarWinds : <http://www.solarwinds.net>

XX. La journalisation

XX.A Présentation

- ❑ Un équipement Cisco à la possibilité de journaliser les événements. Cette journalisation peut être soit locale (sur le routeur) ou distante (sur un serveur syslog).
- ❑ En comparaison avec les traps SNMP, la journalisation est plus simple à mettre en place, elle ne nécessite pas la compilation de MIBs.
- ❑ La journalisation distante se fait en UDP sur le port Syslog (UDP 514).
- ❑ Un trie des logs remontées par équipement est possible en utilisant une *'facility'* différente (local0 à local7).
- ❑ Le niveau de log remonté est également configurable de *'debug'* (le niveau le plus haut) au niveau *'warning'*.

XX.B Syslog

- ❑ Le système IOS génère des messages en réponse à différents événements et les envoie par défaut vers la console ; ces messages sont appelés *syslog*.
- ❑ Ces messages ne sont pas visibles lorsque vous vous connectez via Telnet, à moins d'émettre la commande *'terminal monitor'*.
- ❑ Un autre moyen d'obtenir ces messages est de faire en sorte que le système les mémorise dans un buffer mémoire RAM par la commande *'logging buffered'* en mode de configuration global, puis d'utiliser la commande *'show logging'* pour les afficher.

- ❑ Les messages syslog peuvent être envoyés vers un autre équipement. Deux possibilités existent :
 - Transmettre les messages à un serveur syslog ou bien les transmettre sous forme d'interceptions SNMP (SNMP trap) à une station d'administration (network management station). La commande *'logging host'*, où *host* représente l'adresse IP ou le nom DNS du serveur syslog, sert à activer l'envoi des messages vers le serveur externe.

 - La commande *'snmp-server enable traps'* indique au système IOS de transmettre les interceptions SNMP, notifications syslog incluses ; cela implique que SNMP ait été configuré auparavant.

XX.C Configuration Cisco

- ❑ Définition du 'buffer' local.

Loggin buffered 1024	On se réserve un « buffer » pour la log locale.
----------------------	---

- ❑ Configurer un ou plusieurs serveurs distants :

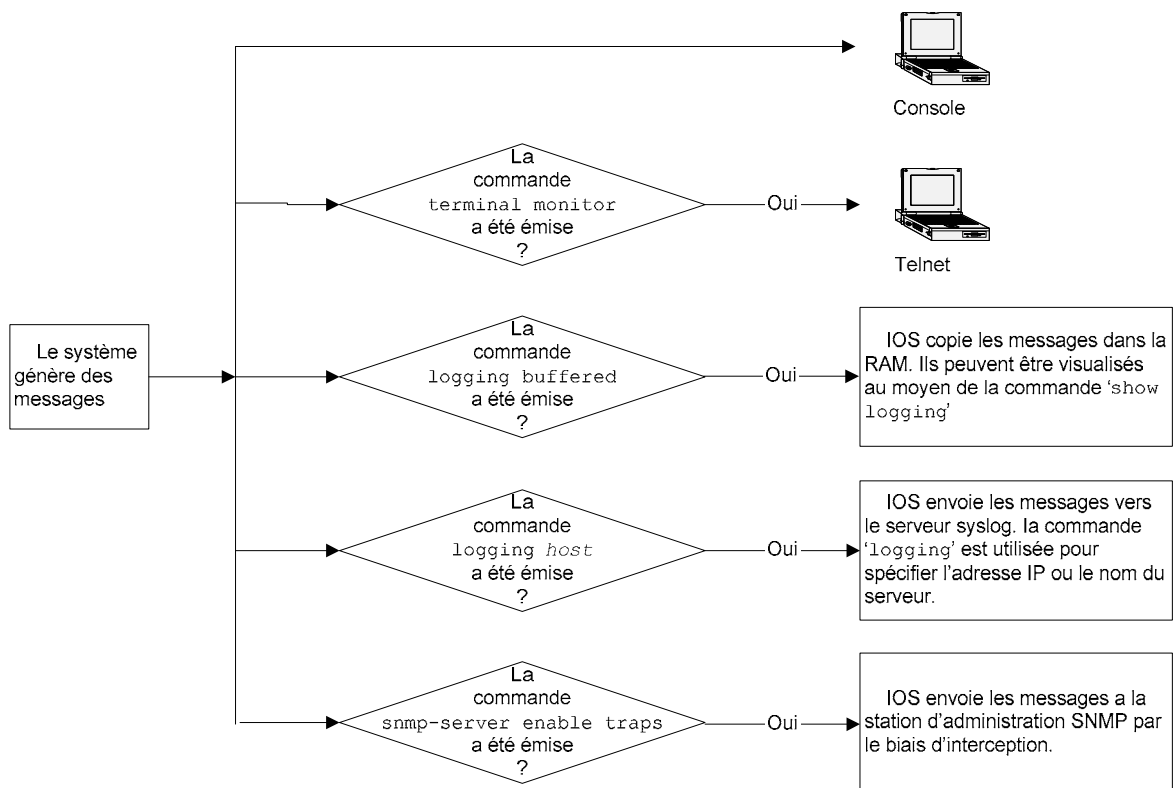
Loggin a.b.c.d	a.b.c.d adresse du serveur
----------------	----------------------------

- ❑ Configurer le niveau de journalisation

Loggin trap niveau	Niveau :
--------------------	----------

- ❑ Configurer la facility :

Logging facility localX	LocalX= local0 à local7
-------------------------	-------------------------



XX.D Configuration Syslog sous Linux

1. Configuration CISCO

```
# configure terminal
# logging @IP ; Adresse IP du syslog
# logging facility local0 ; précisez le nom de la Facility
# CTRL-Z
# wr
```

2. Configuration Linux

- ❑ Dans le fichier ‘/etc/syslog.conf’
- ❑ Il est nécessaire de définir dans ce fichier l’emplacement ou la log sera stocké en fonction de la « facility » choisie (local 0 – local7).

```
Local0.* -/var/log/cisco0 # mémorisation de la log dans le fichier '/var/log/cisco0'
Local0.* -/dev/tty12 # Visu de la log à l'écran
*. * -/dev/tty8 # tout afficher sur tty8
```

Localn : avec n compris entre 0 et 7, est réservé pour des usages propres au site

- ❑ Dans le fichier ‘/etc/rc.d/init.d/syslog’ : Il sera nécessaire de modifier ce fichier de démarrage (/etc/rc.d/init.d/syslog) afin de préciser au daemon d’écouter le réseau. L’option –r sera utilisée comme par exemple :

```
Start () {
    daemon syslogd -m 0 -r # option 'r' pour réseau
```

3. Lancement du serveur Syslog sur Linux

- ❑ Le démarrage du service se fait par le programme
 - # /etc/rc.d/init.d/syslog (start|stop|restart|status)

XXI. Le Policy-Based Routing

XXI.A Présentation

- ❑ Pour conclure sur le routage, une particularité montrant la puissance de l'IOS Cisco. Cette particularité est le routage sélectif, c'est-à-dire que le routage est effectué en fonction de l'adresse IP source.
- ❑ Le PBR (*Policy-Based Routing*), est une option propriétaire Cisco permettant de définir des règles de routage pour des datagrammes répondant à certaines conditions, pour ces paquets la règle est appliquée, la table de routage ne sera pas consultée.
- ❑ Le routage sélectif ne peut être que statique. S'il n'est pas planifié ni correctement implémenté, il peut avoir de très mauvaises conséquences sur le routage statique et dynamique existant.

XXI.B Application

```
access-list 1 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface ethernet 1
 ip policy route-map Mon-routage
!
route-map Mon-routage permit 10
 match ip address 1
 set ip next-hop 3.3.3.3
!
route-map Mon-routage permit 20
 match ip address 2
 set ip next-hop 3.3.3.5
!
route-map Mon-routage permit 30
 set default interface ethernet 1
```

- ❑ Les paquets arrivant sur l'interface Ethernet 1 et en provenance du réseau 1.1.1.1 seront routés vers la machine 3.3.3.3.
- ❑ Les paquets arrivant sur l'interface Ethernet 1 et en provenance du réseau 2.2.2.2 seront routés vers la machine 3.3.3.5.
- ❑ Nous pouvons donc 'router' en fonction de l'adresse source.
- ❑ Tous les autres paquets seront envoyés sur l'interface Ethernet 1.
- ❑ L'utilisation de listes d'accès étendues permet de définir des règles très puissantes, comme par exemple une route particulière pour un flux précis.
- ❑ Par exemple on pourrait en cas de panne d'un serveur, re-router le trafic vers un serveur de secours, voir re-router juste le trafic d'une application. Ceci ne nécessitant aucune modification de la configuration du DNS ou du poste client.

XXII. RNIS

RNIS : Réseau Numérique à Intégration de service

XXII.A Présentation

- ❑ RNIS est incontestablement le moyen d'obtenir rapidement une connexion opérationnelle « sécurisée » entre deux sites.
- ❑ RNIS permet également de relier des routeurs en solution de secours (panne de la ligne louée ou de l'accès Frame Relay) ou pour des connexions occasionnelles.
- ❑ RNIS est également une solution aux problèmes de surcharge d'une liaison WAN, l'on peut paramétrer un débordement de la ligne sur RNIS.
- ❑ Deux types d'interface sont disponibles :
 - BRI ou S0 ; pour un accès de base (soit deux canaux B à 64Kb/s),
 - PRI ; pour utiliser un accès primaire (23 ou 30 canaux B à 64Kb/s).
 - S1 ; au USA et Japon (23 canaux B à 56Kb/s).
 - S2 ; Europe (30 canaux B à 64Kb/s).
- ❑ Avec un accès RNIS de base on peut obtenir un débit de 128Kb/s.

- ❑ On peut également utiliser un boîtier d'adaptation connecté à une interface série du routeur.
- ❑ Ce type de boîtier ne permet pas toujours les appels entrants.

- ❑ Nous ne traiterons que l'accès Numéris de base.
- ❑ La configuration d'un accès primaire est sensiblement identique. Un exemple est donné en annexe.

- ❑ Cependant RNIS demande une configuration soignée afin d'éviter des surcoûts de consommation (consommations inutiles dues aux protocoles de routage, aux SAP IPX ...).

- ❑ Le principe de facturation d'une liaison RNIS est la suivante :
 - Abonnement correspondant au double d'un abonnement RTC (mais on dispose en fait de deux canaux RTC),
 - Consommation identique à celle d'une communication RTC par canal ouvert.

- ❑ Une liaison ouverte 24h/24 sur une longue distance va donc coûter cher, certainement plus qu'une ligne louée de même débit.

- ❑ Actuellement en France, le RNIS correspond à la norme EURO-ISDN depuis 1998.
- ❑ Avec un délai de livraison de dix jours contrairement aux six semaines pour une LS.

XXII.B Configuration de RNIS

- Il appartient dans un premier temps de définir le type de RNIS (ISDN en Anglais) utilisé :

isdn switch type	Définir le type d'ISDN
------------------	------------------------

Exemple :

```
Paris(config)#isdn switch-type ?
basic-ltr6      lTR6 switch type for Germany
basic-5ess     AT&T 5ESS switch type for the U.S.
basic-dms100   Northern DMS-100 switch type
basic-net3    NET3 switch type for UK and Europe
basic-ni       National ISDN switch type
basic-qsig     QSIG switch type
basic-ts013    TS013 switch type for Australia
ntt            NTT switch type for Japan
vn3            VN3 and VN4 switch types for France
<cr>
```

- On choisit de préférence BASIC NET 3 car nous sommes en France en EURO ISDN.
- On peut trouvera parfois vn3 qui correspond à l'ancienne norme RNIS, c'est souvent le cas sur d'anciennes configuration.
- Prévoir un Reboot en cas de changement de type ISDN.

- On devra ensuite définir la (les) numérotation(s) au niveau de l'interface.

dialer map	
------------	--

Exemple :

```
dialer map ip 172.16.14.125 broadcast name Lyon 0449485656
```

Ce qui signifie que pour atteindre 172.16.14.125 on numérotera 0449485656 et on utilisera le « login » Lyon (le username Lyon doit être défini sur le routeur distant), nous étudierons plus tard les modes d'authentification PAP et CHAP.

Attention au préfix de numérotation pour les liaisons passant par un PABX privé.

On définira également au niveau de l'interface un dialer group

```
dialer-group 2
```

Et enfin au niveau global un dialer list (correspondant au dialer group)

```
dialer-list 2 protocol ip permit
```

On peut éventuellement utiliser une liste d'accès au niveau du dialer list

```
dialer-list 2 protocole ip list 101
```

Les commandes dialer list et dialer group sont nécessaire pour limiter les ouvertures du lien RNIS.

Au niveau de l'interface, il est de plus « économique » de configurer le délai d'inactivité en secondes qui provoquera la coupure de la connexion.

```
dialer idle-timeout 300
```

XXII.C Protocoles PAP et CHAP

- ❑ Les protocoles PPP et HDLC peuvent être utilisés sur de réseaux commutés, on préférera cependant le protocole PPP qui bénéficie de l'authentification PAP (*Password Authentication Protocol*) ou CHAP (*Challenge Handshake Authentication Protocol*).
- ❑ Les deux protocoles PAP et CHAP requièrent l'échange de messages entre les équipements, le routeur appelé s'attend à recevoir des données d'Authentification. Avec PAP le nom de l'utilisateur et le mot de passe sont envoyés par le routeur appelant. Avec CHAP le routeur appelé envoie un message de défi (*challenge*) qui demande au routeur appelant d'envoyer le nom d'utilisateur et le mot de passe, et inclut aussi un numéro aléatoire. Le routeur appelant répond avec une valeur cryptée.
- ❑ On préférera une authentification CHAP plus sûre.

La commande :

<code>ppp authentication {chap pap}</code>	Définir le mode d'authentification (pap ou chap).
--	---

Exemple de configuration CHAP :

<pre>hostname Paris ! username Lyon password secretrnis ! Interface bri 0 encapsulation ppp ppp authentication chap</pre>	<pre>hostname Lyon ! username Paris password secretrnis ! Interface bri 0 encapsulation ppp ppp authentication chap</pre>
---	---

XXII.D Configurations

XXII.D.1 Multilink PPP

- ❑ Multilink PPP est une fonction qui autorise l'existence de plusieurs liens entre un routeur et un autre équipement, sur lesquels la charge d'un trafic est équilibrée.
- ❑ Les deux commandes sont ppp multilink et dialer load-threshold. La première active le protocole et la seconde indique au routeur d'établir une connexion sur un autre canal B si la moyenne d'utilisation des liens exploités dépasse le seuil , la valeur est exprimée en %, pour le trafic en entrée ou en sortie.

Commandes :

PPP multilink	Activation du multiligne
---------------	--------------------------

Load threshold 80	Fixe le seuil de charge à 80%
-------------------	-------------------------------

XXII.D.2 Secours et débordement

RNIS peut être utilisé en secours d'une interface série.
Il est également possible de paramétrer un débordement du trafic.

Commandes :

Backup interface	On va configurer une interface en secours, par exemple sur l'interface série, on précisera que le secours est l'interface RNIS.
Backup delay	On va définir un temps de coupure au bout duquel on ouvrira le secours, puis le temps de rétablissement pour la fermeture du secours.
Backup load	On précise le niveau de charge pour l'ouverture du débordement, le taux de charge pour sa fermeture.

Exemple :

<pre>Gefi#conf t Enter configuration commands, one per line. End with CNTL/Z. Gefi(config)#int s 1 Gefi(config-if)#backup ? delay Delays before backup line up or down transitions interface Configure an interface as a backup load Load thresholds for line up or down transitions Gefi(config-if)#backup interface bri 0 Gefi(config-if)#bac Gefi(config-if)#backup de Gefi(config-if)#backup delay ? <0-4294967294> Seconds never Never activate the backup line Gefi(config-if)#backup delay 15 ? <0-4294967294> Seconds never Never deactivate the backup line</pre>	<pre>Gefi(config-if)#backup delay 15 60? <0-4294967294> Gefi(config-if)#backup delay 15 60 Gefi(config-if)#backup load ? <0-100> Percentage never Never activate the backup line Gefi(config-if)#backup load 80 ? <0-100> Percentage never Never deactivate the backup line Gefi(config-if)#backup load 80 20 ? <cr> Gefi(config-if)#backup load 80 20 Gefi(config-if)#</pre>
---	---

A noter qu'il est possible de configurer un secours en utilisant le poids des routes. Cette solution permet une convergence plus rapide.

XXII.D.3 Contrôle du numéro appelant

La commande **isdn caller 01XXXXXX** permet de contrôler le numéro appelant (présenté par FT.)

isdn caller 01XXXXXX	Contrôle de l'appelant
----------------------	------------------------

On peut utiliser le debug dialer pour voir le numéro appelant.

XXII.D.4 Interface dialer

- ❑ L'utilisation d'une interface « dialer » permet de regrouper les commandes de configuration RNIS.
- ❑ On pourra par exemple utiliser une interface physique pour plusieurs connexions.

Exemple :

```
interface Dialer0
ip unnumbered Loopback0
encapsulation ppp
dialer remote-name Remote0
dialer pool 1
dialer string 5551212
dialer-group 1
!
interface Dialer1
ip unnumbered Loopback0
encapsulation ppp
dialer remote-name Remote1
dialer pool 1
dialer string 5551234
dialer-group 1
!
interface BRI0
encapsulation PPP
dialer pool-member 1
ppp authentication chap
!
interface Serial0
ip unnumbered Loopback0
backup interface Dialer0
backup delay 5 10
!
interface Serial
ip unnumbered Loopback0
backup interface Dialer1
backup delay 5 10
```

Lecture conseillée :

<http://www.cisco.com/warp/public/129/23.html>

XXII.D.5 Configuration d'un client Microsoft RAS

- ❑ Il est possible à un client Microsoft RAS disposant d'une carte RNIS, de se connecter au réseau via un routeur Numéris.
- ❑ Cette solution peut être utile pour des postes isolés se connectant de manière ponctuelle. (Consultation de la messagerie par exemple.)
- ❑ Dans ce cas il est possible au routeur d'affecter au poste client une adresse IP à la connexion. C'est ce type de configuration qu'utilisent les Provider Internet (ISP).
- ❑ On configurera un « pool » d'adresses (dans l'exemple suivant ce pool se nome RAS_Pool)
- ❑ Le contrôle PPP CHAP est possible il suffit de remplir les cases Login et Password du client, on ne remplit pas la case Domain.
- ❑ On prendra soin de configurer un username par poste, l'utilisation du même username pour plusieurs postes serait interprétée par le routeur comme l'ouverture de plusieurs canaux par un même poste (PPP Multilink), le fonctionnement serait aléatoire.

Mode de configuration :

Commande globale:

<code>ip local pool Nom A.A.A.A B.B.B.B</code>	ip local pool : la commande Nom : le nom du pool (un mot), A.A.A.A : la première adresse, B.B.B.B : la dernière adresse.
--	---

Sous commande d'interface :

<code>peer default ip address pool Nom</code>	peer default ip address pool : la commande, Nom : le nom du pool.
---	--

Exemple :

```

username pwh_sqj password 7 13524F4B5F595229
username pwh_mar password 7 115D4C534640580E
username pwh_paris password 7 145156155D507F
interface BRI0
description Access RAS pour postes Distants
bandwidth 64
ip address 192.168.101.1 255.255.255.0
ip access-group 105 in
no ip directed-broadcast
ip accounting output-packets
encapsulation ppp
dialer idle-timeout 300
dialer-group 2
isdn switch-type basic-net3
isdn caller 0466577777
isdn caller 0139322222
isdn caller 0130859999
isdn caller 0156895555
peer default ip address pool RAS_Pool
no cdp enable
ppp authentication chap
ip local pool RAS_Pool 192.168.101.11 192.168.101.12
ip classless
ip route 0.0.0.0 0.0.0.0 172.20.24.1

```

XXII.D.6 Exemple de configuration d'un routeur RNIS

```

service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname Lyon
!
enable secret 5 $1$0sfK$51cUae3vGfKf/gJvrx/6X/
!
username Paris password 7 00171605165E1F1401285F
ip subnet-zero
ip domain-name gefi.com
ip name-server 172.16.4.4
ipx routing 00d0.58af.d2e0
isdn switch-type basic-net3
!
interface Ethernet0/0
description LAN de Lyon

```

```

ip address 172.16.52.1 255.255.254.0
no ip directed-broadcast
ipx network 520
!
interface BRI0/0
description Lien RNIS vers Paris
bandwidth 64
ip address 195.1.10.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip mroute-cache
dialer idle-timeout 600
dialer map ip 195.1.10.1 name Paris broadcast 0130859164
dialer map ipx 31059702.0000.0000.0001 name Paris broadcast 0130859164
dialer map ipx 9069701.0000.0000.0001 name Paris broadcast 0130859164
dialer map ipx 824.0050.733f.0641 name Paris broadcast 0130859164
dialer-group 1
ipx network 824
isdn switch-type basic-net3
down-when-looped
compress stac
no cdp enable
ppp authentication chap
!
ip classless
ip route 0.0.0.0 0.0.0.0 195.1.10.1
!
access-list 12 permit any log
access-list 199 permit ip 172.16.48.0 0.0.0.127 any log
access-list 199 permit ip 172.20.0.0 0.0.1.255 any log
access-list 199 permit ip 172.16.8.0 0.0.7.255 any log
access-list 199 deny ip any any log
access-list 901 deny any 824.00d0.58af.d2e0 all 824.ffff.ffff.ffff all
access-list 901 deny rip any all any all
access-list 901 permit any any all any all
dialer-list 1 protocol ip list 12
dialer-list 1 protocol ipx list 901
no cdp run
!
ipx route default 824.0050.733f.0641
!
ipx sap 4 netware1 9069701.0000.0000.0001 451 2
ipx sap 4 netware2 31059702.0000.0000.0001 451 2
!
snmp-server community public RO 199
!
line con 0
transport input none
line aux 0
line vty 0 4
access-class 199 in
password 7 071F205F4A0C1B0A1B
login

```

Notez la configuration IP en violet et IPX en vert.

Lectures conseillées :

http://www.cisco.com/pcqi-bin/Support/PSP/psp_view.pl?p=Internetworking:ISDN

http://www.cisco.com/pcqi-bin/Support/PSP/psp_view.pl?p=Internetworking:DDR&s=Implementation and Configuration#Samples %26 Tips

XXIII. CDP

CDP : *Cisco Discovery Protocol*

XXIII.A *Présentation*

- ❑ CDP est un protocole propriétaire Cisco de niveau deux, permettant la découverte des équipements réseau.
- ❑ Les routeurs et commutateurs Cisco échangent les informations suivantes :
 - Nom et adresse de l'équipement,
 - Version logicielle,
 - Plate-forme matérielle,
 - Fonctionnalité de l'équipement,
 - VLAN natif...
- ❑ Il est recommandé de ne pas utiliser CDP, car ce protocole est un trou de sécurité en annonçant beaucoup trop de paramètres de configurations.

XXIII.B *Configuration*

Commande	Commentaire
no cdp run	Commande globale, pour arrêter les annonces CDP.
no cdp enable	Sous commande d'interface, pour arrêter les annonces CDP.

XXIV.Config Maker

XXIV.A Présentation

- ❑ L'outil Cisco Config Maker est disponible sous :
<http://www.cisco.com/warp/public/cc/pd/nemnsw/cm/index.shtml>
- ❑ Attention : L'outil ne semble plus maintenu, car la dernière version 2.6.006 du 13.03.2002 n'a pas été renouvelée depuis
- ❑ De plus, n'oubliez pas que le debugging ne peut être réalisée qu'en mode CLI.
- ❑ Nous allons utiliser l'outil Cisco Config Maker afin de réaliser la configuration d'un routeur permettant une connexion RNIS vers un ISP (*Internet service Provider*) et permettre ainsi l'accès à l'Internet.
- ❑ L'outil présente trois fenêtres :
 - '*Network Diagram*' : c'est là que nous allons construire notre réseau.
 - '*Devices*' : c'est l'ensemble des ressources disponibles pour notre réseau
 - '*Connections*' : c'est l'ensemble des connexions que nous allons réaliser.

XXIV.B Utilisation

Etape 1 :

- ❑ Faire glisser la fenêtre '*Devices*' vers la fenêtre '*Network Diagram*' le symbole Internet.
- ❑ Choisir dans '*Devices*' un routeur Cisco 2503 et le faire glisser dans '*Network Diagram*'.



L'outil nous demande le nom de cet équipement, routeur_Internet par exemple.

- Nous sommes maintenant invités à saisir les mots de passe.



The screenshot shows the 'Cisco 2503 Device Wizard - Assign Passwords' window. It features a blue title bar with a help icon and a close button. On the left, there is a graphic of a Cisco 2503 router with a key icon above it. The main area is divided into two sections: 'Login Password' and 'Enable Password'. Each section contains a description and two input fields for 'Enter Password' and 'Re-enter Password'. At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Annuler', and 'Aide'.

Cisco 2503 Device Wizard - Assign Passwords

Login Password
The Login Password allows you to log into the device through its console port or by telnet.

Enter Password:

Re-enter Password:

Enable Password
After you login, the Enable Password allows you to make changes to the device's configuration.

Enter Password:

Re-enter Password:

< Précédent Suivant > Annuler Aide

- Nous allons sélectionner les protocoles à configurer, pour notre cas IP.



The screenshot shows the 'Cisco 2503 Device Wizard - Select Network Protocols' window. It features a blue title bar with a help icon and a close button. On the left, there is a graphic of a Cisco 2503 router with a network diagram icon above it. The main area contains the text 'Select the network protocols you plan to use on this router.' followed by three checkboxes: 'TCP/IP' (checked), 'Novell IPX/SPX', and 'AppleTalk'. At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Annuler', and 'Aide'.

Cisco 2503 Device Wizard - Select Network Protocols

Select the network protocols you plan to use on this router.

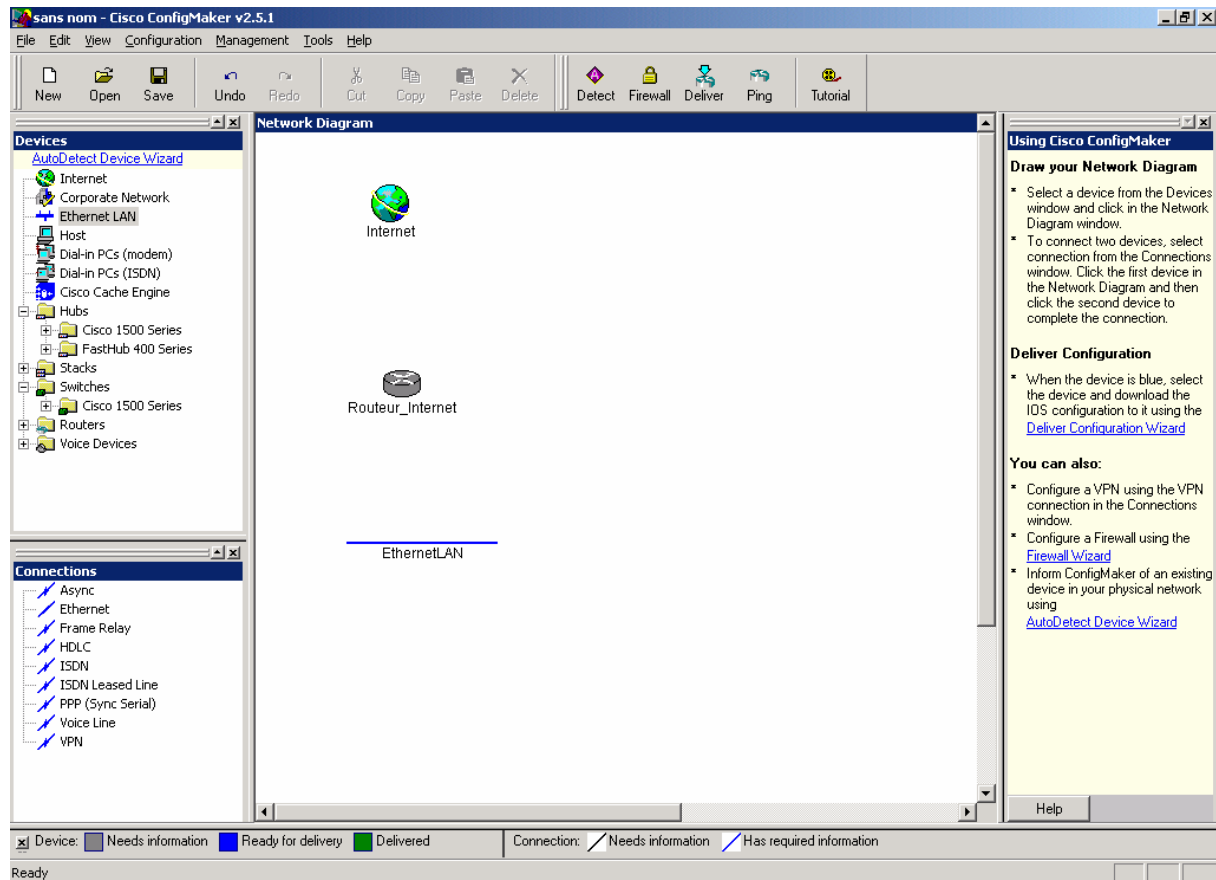
TCP/IP

Novell IPX/SPX

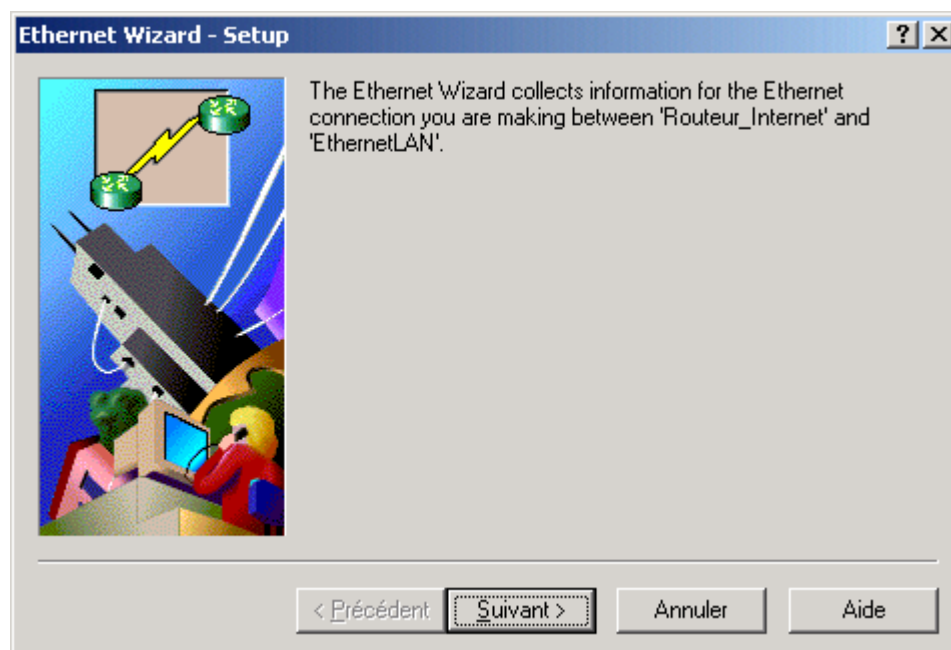
AppleTalk

< Précédent Suivant > Annuler Aide

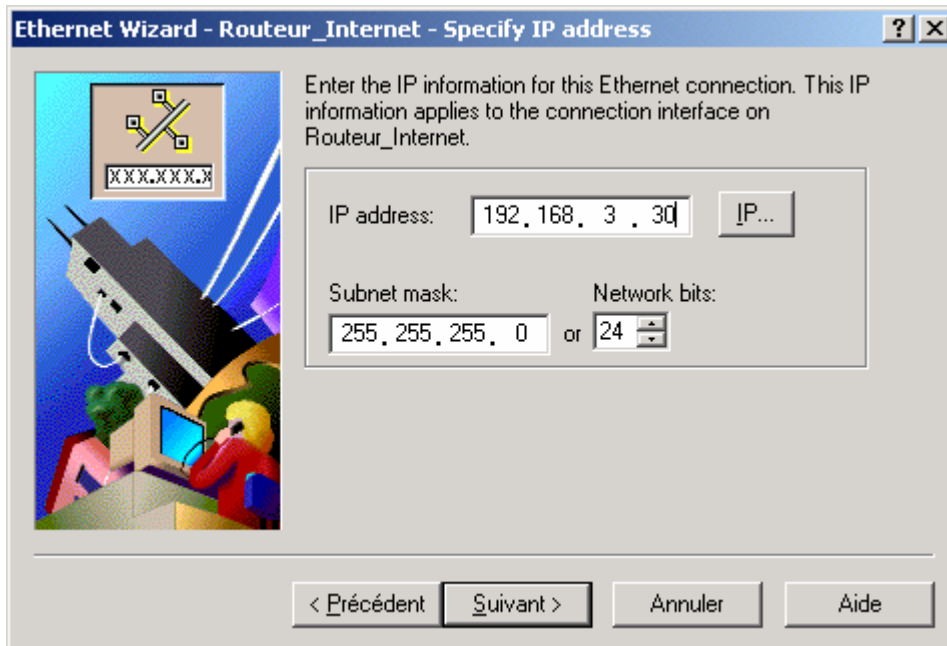
- ❑ Nous allons maintenant ajouter un LAN Ethernet.



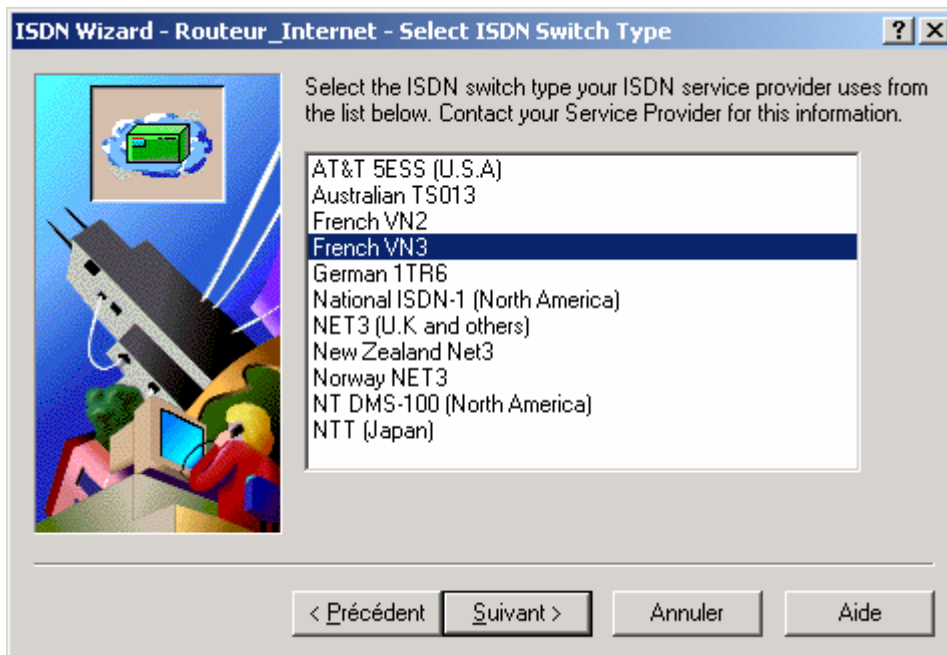
- ❑ Il nous reste maintenant à connecter le routeur au LAN et à l'Internet.
- ❑ Choisir dans connection l'objet Ethernet et plaçons le entre le LAN et le routeur.



- Nous allons maintenant entrer les informations de configuration de l'interface Ethernet.
 - Nous configurons l'adresse IP de l'interface.
 - Et son Subnet Mask.



- De même, nous allons connecter le routeur à l'Internet par une connexion ISDN.
- Nous choisissons ici le type d'ISDN.



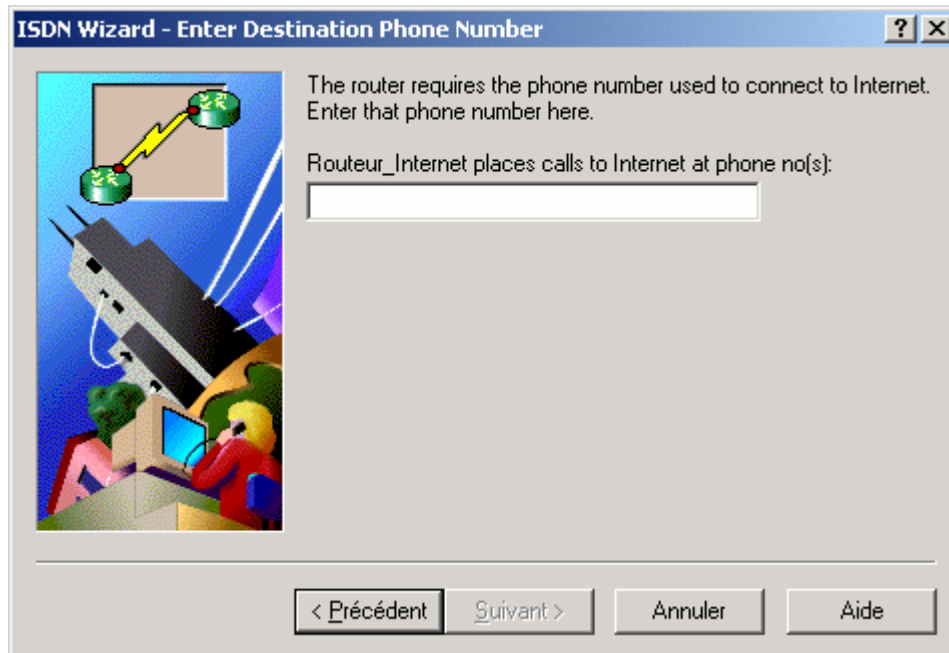
- Nous indiquons maintenant l'adresse IP, elle sera fournie par l'ISP.



- Nous configurons l'équipement afin que nos adresses LAN soient traduites vers l'adresse fournie par l'ISP. Ici, la translation est NAT/PAT sur l'adresse IP de l'interface Internet.



- ❑ Nous indiquons le numéro d'appel du provider.



- ❑ Puis le nom et le mot de passe de notre compte chez l'ISP.



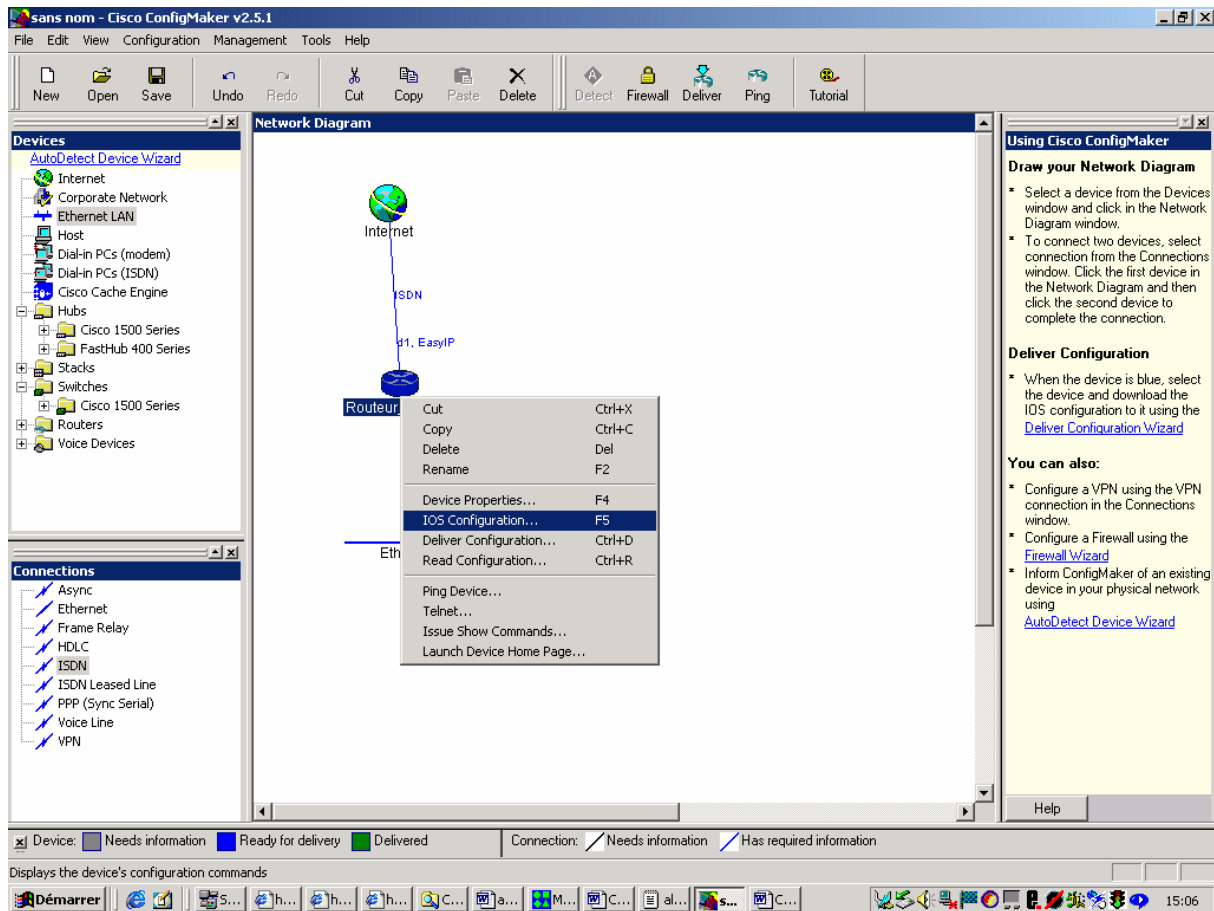
- ❑ Notre configuration est terminée.
- ❑ Nous obtenons le diagramme suivant :

The screenshot displays the Cisco ConfigMaker v2.5.1 application window. The main area shows a network diagram with the following components and connections:

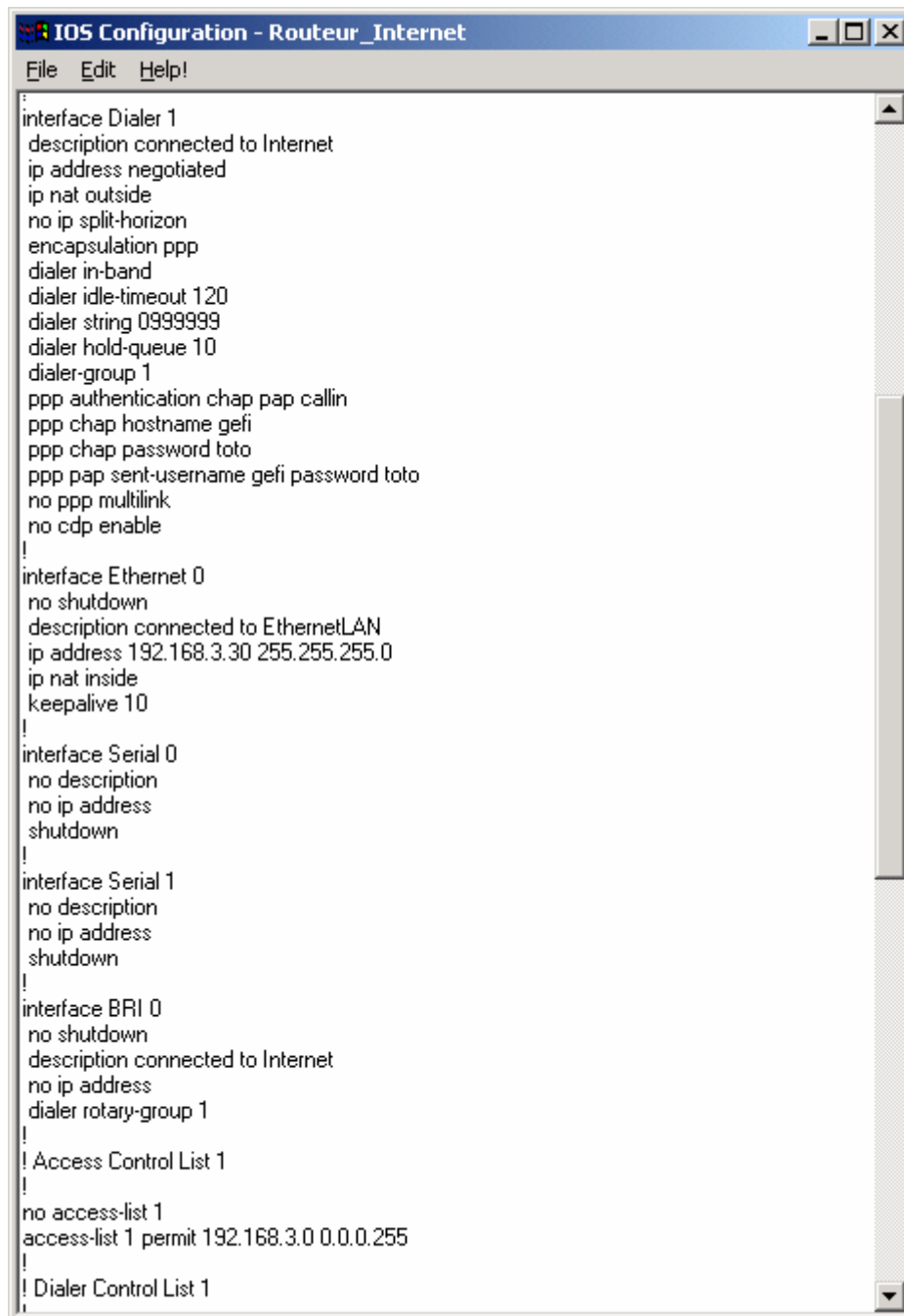
- Internet** (represented by a globe icon) connected to a **Routeur Internet** (represented by a router icon) via an **ISDN** connection labeled "d1, EasyIP".
- The **Routeur Internet** is connected to an **EthernetLAN** (represented by a horizontal line) via an **Eth** connection labeled "e0, 192.168.3.30/24".

The interface includes a menu bar (File, Edit, View, Configuration, Management, Tools, Help), a toolbar with icons for New, Open, Save, Undo, Redo, Cut, Copy, Paste, Delete, Detect, Firewall, Deliver, Ping, and Tutorial. On the left, there are two panes: **Devices** (listing various network components like Internet, Corporate Network, Ethernet LAN, Host, Dial-in PCs, Cisco Cache Engine, Hubs, Stacks, Switches, Routers, and Voice Devices) and **Connections** (listing connection types like Async, Ethernet, Frame Relay, HDLC, ISDN, ISDN Leased Line, PPP (Sync Serial), Voice Line, and VPN). On the right, a help pane titled "Using Cisco ConfigMaker" provides instructions on drawing the network diagram and delivering configuration. The status bar at the bottom shows "Ready" and a legend for device and connection states.

- En cliquant avec le bouton de droite sur le routeur nous pouvons choisir IOS Configuration.

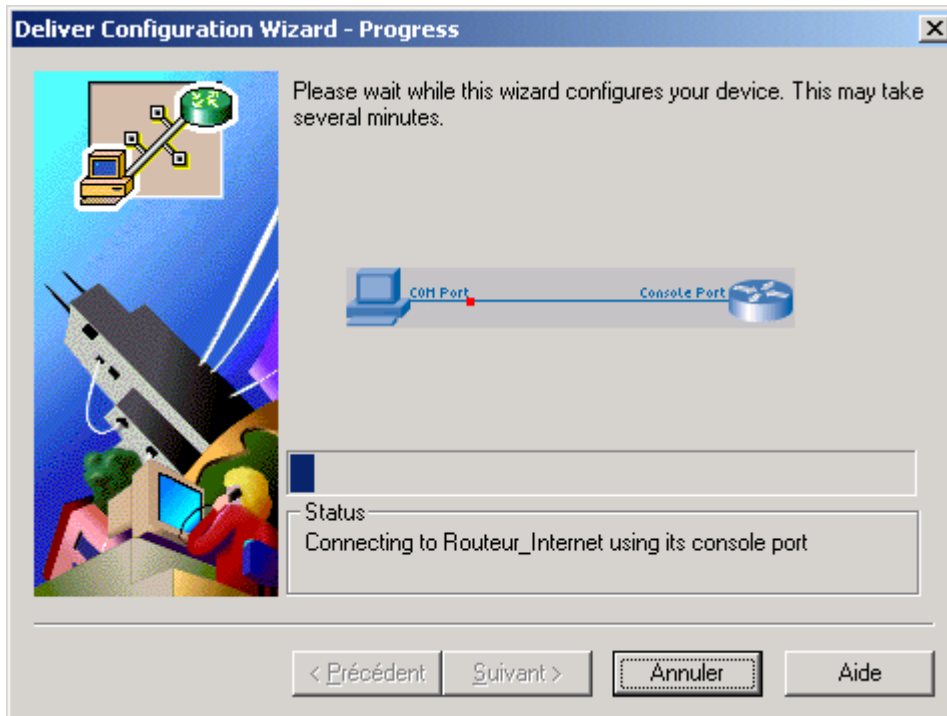


- ❑ Et visualiser la configuration obtenue :

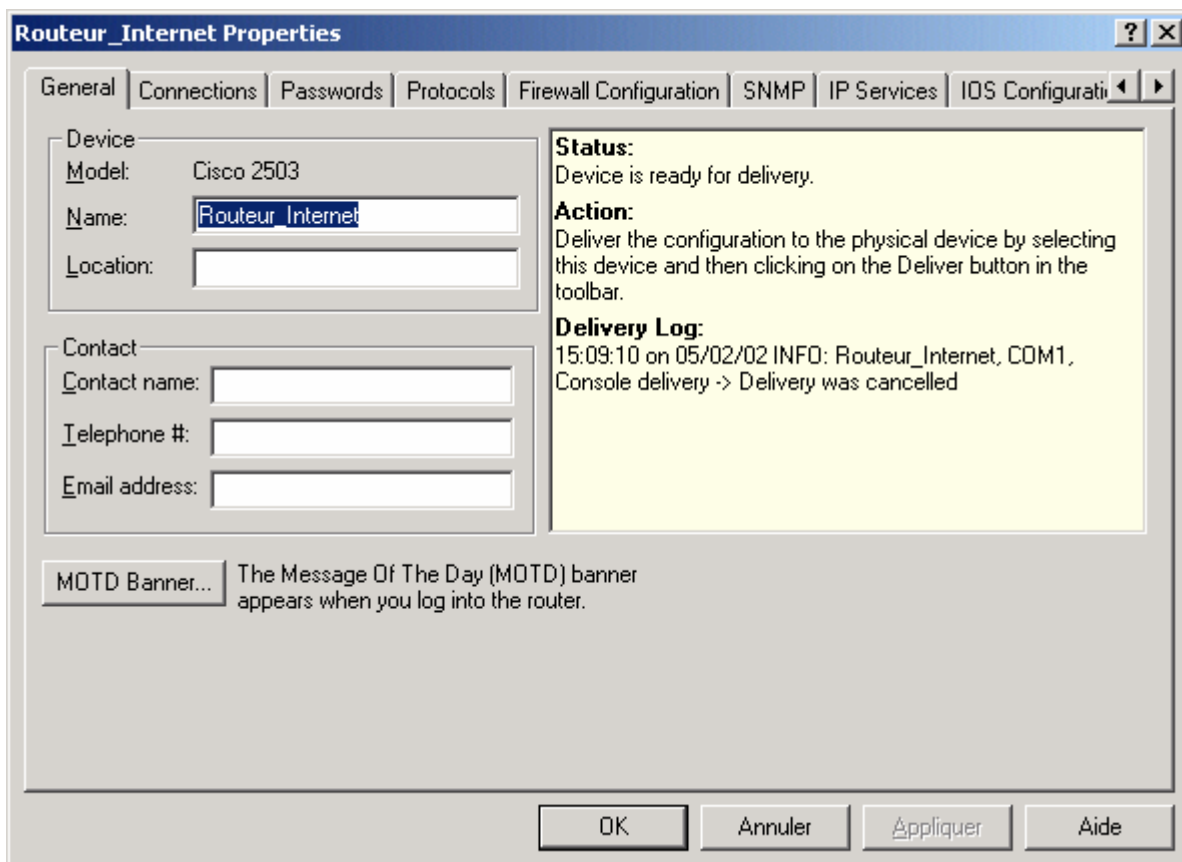


```
IOS Configuration - Routeur_Internet
File Edit Help!
:
interface Dialer 1
description connected to Internet
ip address negotiated
ip nat outside
no ip split-horizon
encapsulation ppp
dialer in-band
dialer idle-timeout 120
dialer string 0999999
dialer hold-queue 10
dialer-group 1
ppp authentication chap pap callin
ppp chap hostname gefi
ppp chap password toto
ppp pap sent-username gefi password toto
no ppp multilink
no cdp enable
!
interface Ethernet 0
no shutdown
description connected to EthernetLAN
ip address 192.168.3.30 255.255.255.0
ip nat inside
keepalive 10
!
interface Serial 0
no description
no ip address
shutdown
!
interface Serial 1
no description
no ip address
shutdown
!
interface BRI 0
no shutdown
description connected to Internet
no ip address
dialer rotary-group 1
!
! Access Control List 1
!
no access-list 1
access-list 1 permit 192.168.3.0 0.0.0.255
!
! Dialer Control List 1
!
```

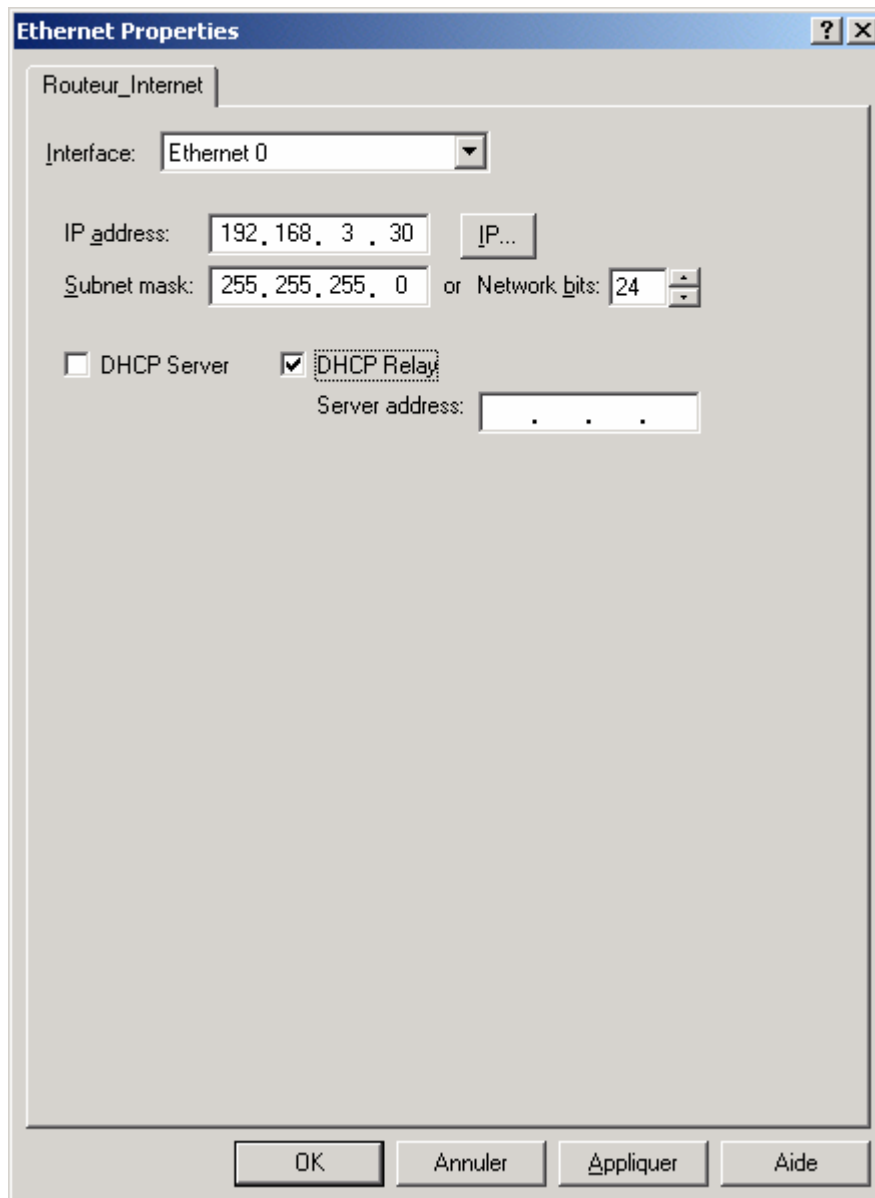
- ❑ Ou encore télécharger cette configuration par le port console :



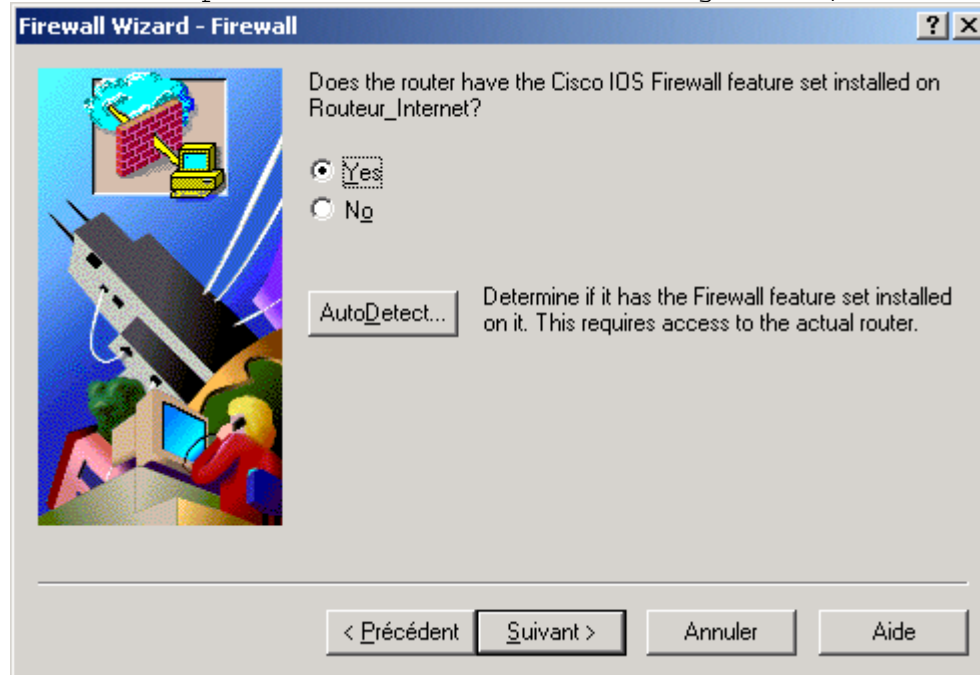
- ❑ Il est également possible de modifier ou de compléter cette configuration, choisir pour cela « device Property ».



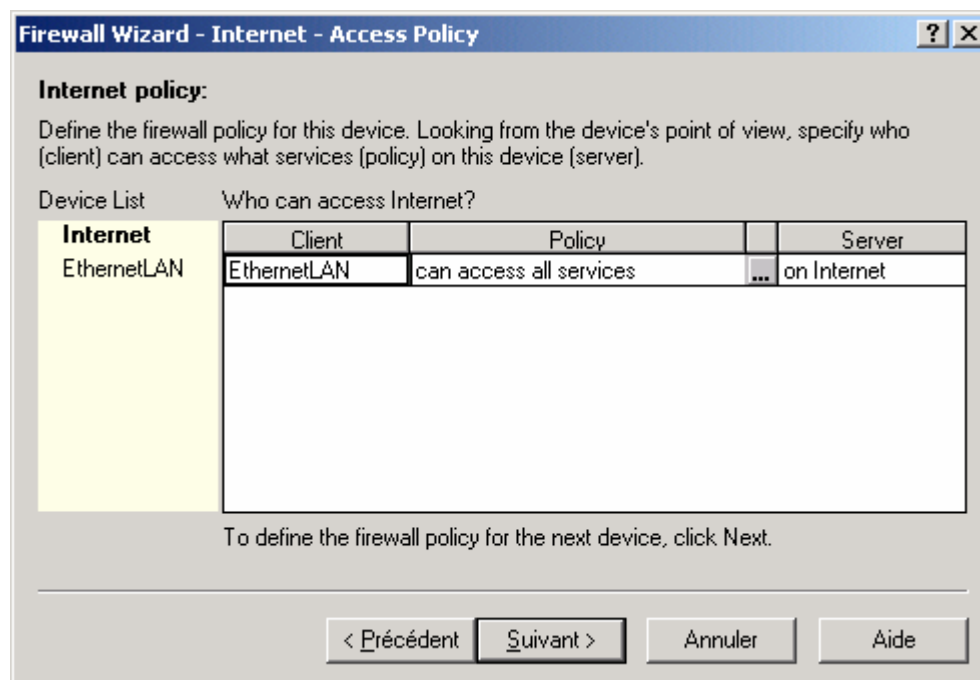
- On pourra par exemple configurer le relais DHCP en choisissant connection, interface Ethernet.



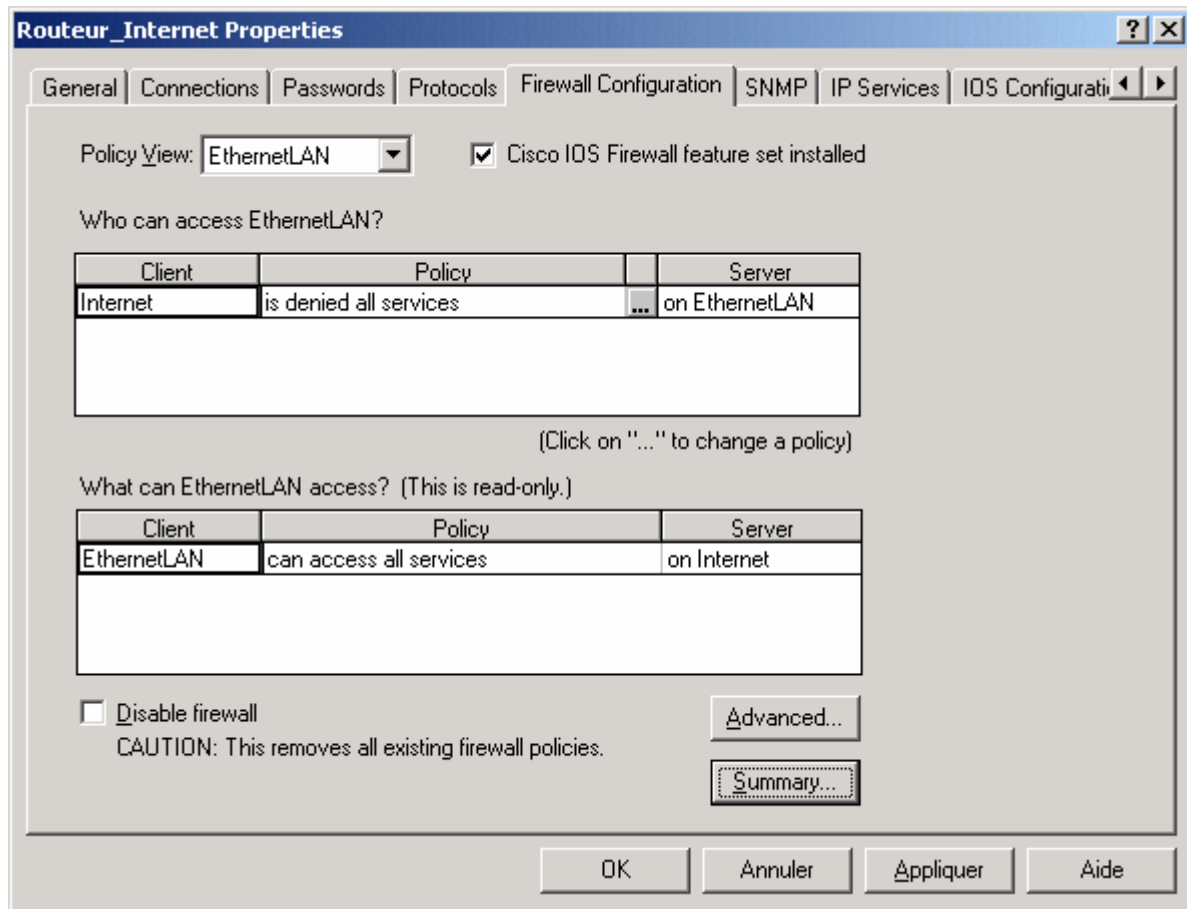
Si l'IOS installé sur le routeur est de type Firewall, la configuration des filtres est possible. Choisir le menu Configuration, firewall.



L'on peut maintenant configurer les filtres :



Exemple de filtrage :



Exercice :

- ❑ Vous allez utiliser Cisco Config Maker pour réaliser la configuration de base de la maquette en utilisant le routage statique.
- ❑ Vous n'oubliez pas le routeur C2503 (192.168.3.30) pour permettre la connexion à l'internet.
- ❑ Vous pouvez télécharger les configurations réalisées.

XXV. QoS

QoS : Quality of Service

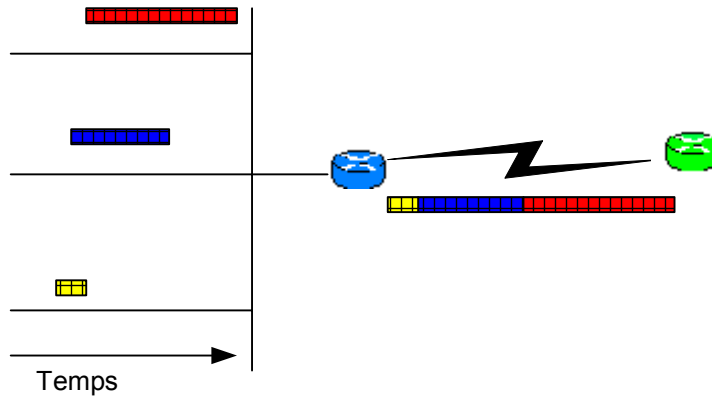
XXV.A *Présentation*

- ❑ La qualité de service est un domaine vaste, nous étudierons la façon de paramétrer les routeurs afin d'atténuer « les effets » de lignes chargées.
- ❑ L'algorithme classique de travail d'une interface est FIFO (First In, First Out), cependant l'IOS Cisco permet d'utiliser des méthodes de travail différentes :
 - Weighted Fair Queue (WFQ), la priorité est donnée au trafic interactif plutôt qu'au transfert de fichiers.
 - Priority Queue, la priorité est donnée à un ou des types de trafic par rapport aux autres.
 - Custom Queue permet de définir une bande passante pour chaque type de trafic.

XXV.B FIFO

FIFO : First In First Out

- ce principe élémentaire de gestion de queue est probablement le plus facile à implémenter.

Fonctionnement FIFO

Exemple :

```

Router#sh int s 0
Serial0 is down, line protocol is down
  Hardware is QUICC Serial
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
  1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer      Received 0
  broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  207 packets output, 43558 bytes, 0 underruns
    0 output errors, 0 collisions, 323 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  DCD=up DSR=up DTR=down RTS=down CTS=up
  
```

XXV.C Weighted Fair Queue

L'algorithme du Weighted Fair Queue se base sur les entêtes de paquets pour déterminer les « conversations ».

- ❑ Pour cela il utilise :
 - Les adresses réseau source et destination
 - Les adresses Mac source et destination
 - Les sockets et numéros de ports
 - Les identifiant Frame relay (DLCI)

Puis il place classe les paquets en fonction de la conversation, les petits paquets des conversations de faible volume seront prioritaires.

La commande :

<code>fair-queue [queue-limit queue-value]</code>	Queue limit : nombre maximum de paquets pour une queue. Queue value : le nombre maximum de paquets stockés par chaque queue.
---	---

Valeurs conseillées :

Moins de 64 kb/s	16
64 à 128 Kb/s	32
128 à 256 Kb/s	64
256 à 512 Kb/s	128
Plus de 512 Kb/s	256

Lecture conseillée :

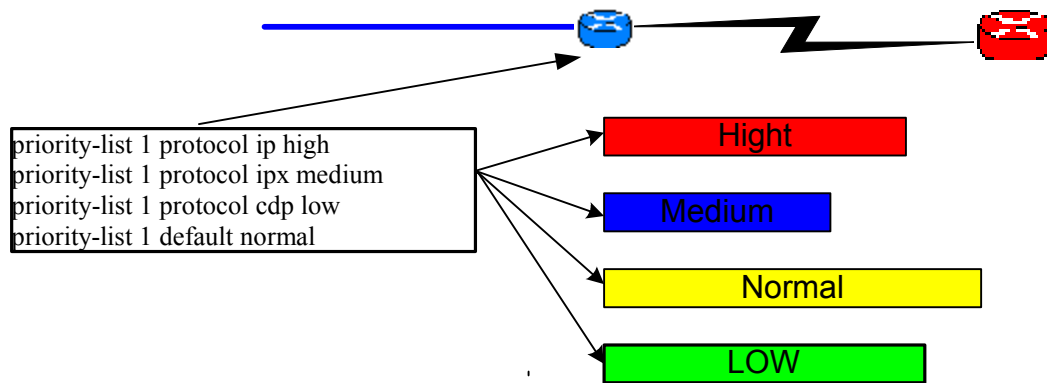
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_r/qrfcmd1.htm#20191

Exemple :

```
Router#sh int S0
Serial0 is down, line protocol is down
  Hardware is QICC Serial
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/128/0 (size/max total/threshold/drops)
    Conversations 0/0/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    207 packets output, 43558 bytes, 0 underruns
    0 output errors, 0 collisions, 319 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  DCD=up DSR=up DTR=down RTS=down CTS=up
```

XXV.D Priority Queuing

XXV.D.1 Principe de fonctionnement



Priority Queuing

XXV.D.2 Configuration

```
priority-list 2 interface Ethernet0 high
priority-list 2 interface Serial0 low
priority-list 2 protocol ip high
priority-list 2 default medium
```

La valeur défaut ne doit pas être omise.

Ce qui donne avec la liste 1 :

```
Router#sh int s 0
Serial0 is down, line protocol is down
  Hardware is QUICC Serial
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: priority-list 1
  Output queue (queue priority: size/max/drops):
    high: 0/20/0, medium: 0/40/0, normal: 0/60/0, low: 0/80/0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  207 packets output, 43558 bytes, 0 underruns
  0 output errors, 0 collisions, 386 interface resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
  DCD=up DSR=up DTR=down RTS=down CTS=up
```

Lecture conseillée :

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cqcr/qos_c/qcprt2/qcdpq.htm

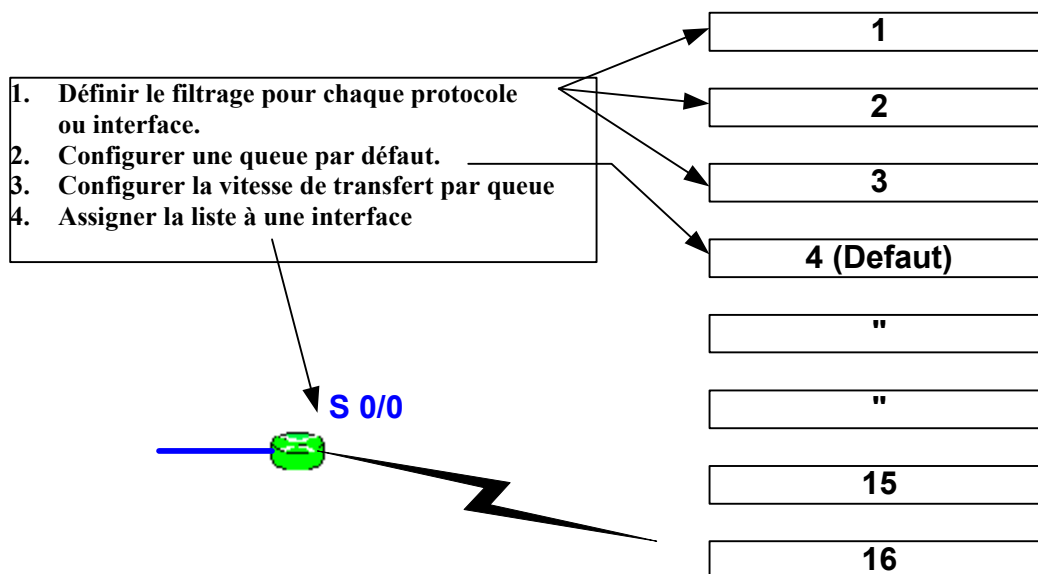
XXV.E Custom Queuing

XXV.E.1 Présentation

- ❑ Le Custom Queuing permet de garantir la bande passante pour un trafic en assignant une taille de queue pour chaque protocole.
- ❑ Avec le Priority Queuing , il est possible qu'un protocole ayant une priorité haute consomme toute la bande passante, interdisant ainsi le transfert pour les autres protocoles.
- ❑ Ce problème est réglé par l'utilisation du Custom Queuing.

XXV.E.2 Principe de fonctionnement

Principe de configuration du Custom Queuing



XXV.E.3 Configuration

```

!
interface Serial0
 ip address 192.168.1.1 255.255.255.252
 no ip directed-broadcast
 custom-queue-list 1
!

queue-list 1 protocol ip 1 tcp www
queue-list 1 protocol ip 2 tcp ftp-data
queue-list 1 protocol ip 2 tcp ftp
queue-list 1 default 5
queue-list 1 queue 1 byte-count 2000
queue-list 1 queue 2 byte-count 1000
queue-list 1 queue 5 byte-count 1000

```

Exemple :

```

Serial0 is administratively down, line protocol is down
Hardware is QUICC Serial
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: custom-list 1
Output queues: (queue #: size/max/drops)
  0: 0/20/0 1: 0/20/0 2: 0/20/0 3: 0/20/0 4: 0/20/0
  5: 0/20/0 6: 0/20/0 7: 0/20/0 8: 0/20/0 9: 0/20/0
 10: 0/20/0 11: 0/20/0 12: 0/20/0 13: 0/20/0 14: 0/20/0
 15: 0/20/0 16: 0/20/0
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 6 interface resets
 0 output buffer failures, 0 output buffers swapped out

```

Lecture conseillée :

<http://www.cisco.com/warp/public/614/15.html>

XXVI.Frame Relay

XXVI.A *Rappels*

- ❑ Frame relay est un réseau WAN dont les accès sont des lignes louées.
- ❑ Ce réseau présente l'avantage de mettre à disposition des CVP (Circuits Virtuels Permanents) entre les différents sites.
- ❑ Chaque CVP dispose débit moyen garanti (CIR, Committed Information Rate). La somme des CIR ne doit pas être supérieure à la bande passante de l'accès de ce site.
- ❑ Il est à la charge du fournisseur du service, Transpac en France de définir les différents CVP de ses clients.
- ❑ Le fournisseur dispose pour cela d'un réseau de liaisons entre différents commutateurs Frame Relay.
- ❑ Un équipement Cisco peut être soit un routeur Frame Relay soit un commutateur Frame Relay, parfois même les deux.
- ❑ A noter que la plus part des commutateurs Frame Relay sont, chez Transpac, des routeurs Cisco.
- ❑ Chaque CVP dispose à chaque extrémité d'un identifiant DLCI (Data Link Connection Identifier), cet identifiant est utilisé comme adresse Frame Relay.
- ❑ Un routeur connecté au réseau Frame Relay n'a besoin que d'une seule interface série pour pouvoir communiquer avec de nombreux sites distants.
- ❑ L'ajout de nouveaux CVP est une simple opération de paramétrage au niveau des routeurs et des commutateurs du réseau. (A condition bien sur que l'accès WAN existe et que sa bande passante soit suffisante).
- ❑ Il est possible de créer un réseau Frame Relay privé.

XXVI.B Configuration

- Une sous interface sera défini pour chaque CVP, chaque sous interface disposera d'une adresse Frame Relay (DLCI) et se configurera ensuite comme une simple liaison série.(adresse IP, adresse IPX)

frame-relay switching	Active la commutation Frame Relay
frame-relay intf-type [DTE DCE]	Configurer une interface DTE ou DCE
frame-relay route in-DLCI out-interface out-DLCI	Spécifier une route statique pour le switching PVC
frame-relay lmi-type {cisco ansi ccitt}	Spécifier le type de LMI
frame-relay keepalive number	Affecter la durée du Keepalive
interface interface-type subinterface-number [multipoint point-to-point]	Définir les sous interfaces
frame-relay interface-dlci DLCI	Associer un DLCI à une sous interface

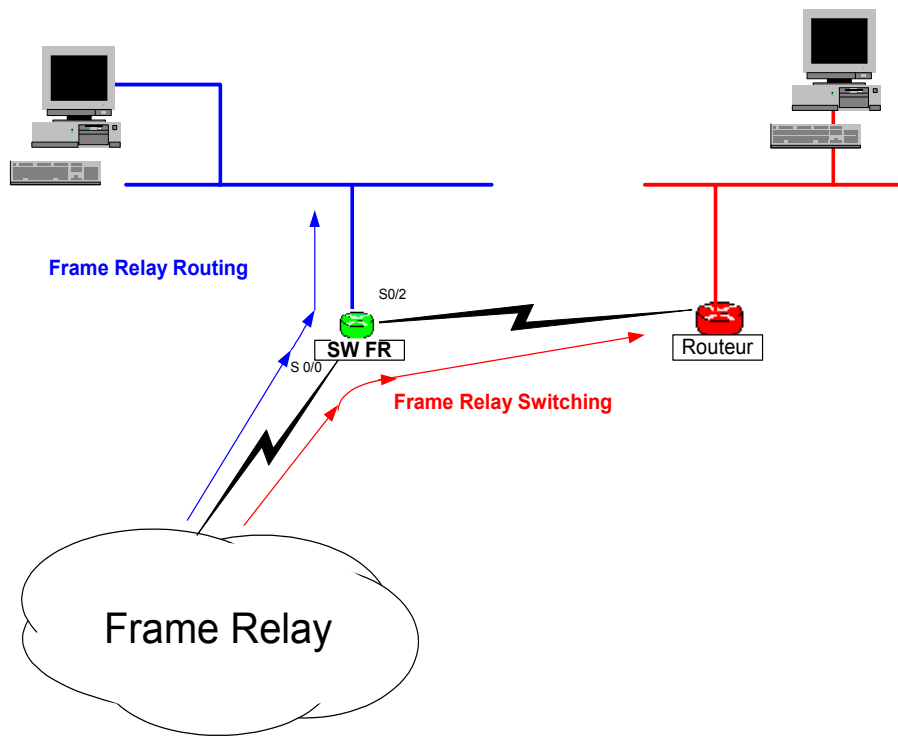
Les commandes de visualisation

show interfaces serial unit	Informations sur Frame Relay DLCI et LMI
show frame-relay lmi [interface]	Statistiques LMI
show frame-relay map	Map Frame Relay
show frame-relay pvc [interface [DLCI]]	Statistiques PVC
show frame-relay traffic	Trafic Frame relay

Exemple de configuration

```
!  
interface Serial1  
  description Frame Relay  
  no ip address  
  encapsulation frame-relay IETF  
  keepalive 12  
  frame-relay lmi-type ansi  
!  
interface Serial1.20 point-to-point  
  description Lien Frame Relay vers PARIS  
  ip address 192.168.200.34 255.255.255.252  
  bandwidth 64  
  ipx network F2032  
  snapshot client 5 120  
  frame-relay interface-dlci 20  
!  
interface Serial1.30 point-to-point  
  description Lien Frame Relay Vers Chambéry  
  ip address 192.168.200.54 255.255.255.252  
  bandwidth 64  
  ipx network F2052  
  snapshot client 5 120  
  frame-relay interface-dlci 30  
!  
router ospf 1  
  redistribute static  
  network 192.168.201.0 0.0.0.255 area 0.0.0.4  
  network 192.168.200.32 0.0.0.3 area 0.0.0.4  
  network 192.168.200.52 0.0.0.3 area 0.0.0.4  
!
```

Exemple de configuration d'un commutateur /routeur Frame Relay:



```
version 12.0
frame-relay switching
!
interface Serial0/0
description Lien 2 Mbits/s vers FT
no ip address
no ip directed-broadcast
encapsulation frame-relay IETF
no ip mroute-cache

FRAME-RELAY LMI-TYPE ANSI

frame-relay route 30 interface Serial0/2 30
!
interface Serial0/0.20 point-to-point
description CVP vers PARIS
bandwidth 64
ip address 192.168.200.26 255.255.255.252
no arp frame-relay
frame-relay interface-dlci 20
!
interface Serial0/0.30 point-to-point
description CVP vers Reseau prive client
no ip directed-broadcast
no arp frame-relay
!

INTERFACE SERIAL0/2
description Lien vers routeur Client
no ip address
no ip directed-broadcast
encapsulation frame-relay IETF
no ip mroute-cache
clockrate 2000000
frame-relay lmi-type ansi
frame-relay intf-type dce
frame-relay route 30 interface Serial0/0 30
!
interface Serial0/2.30 point-to-point
description CVP vers LAN Client
no ip directed-broadcast
```

XXVII. Le pontage

XXVII.A Fonctionnement du pontage

- ❑ Une table de pontage contenant l'association adresse destination et l'interface va permettre le pontage transparent des trames vers l'interface souhaitée.

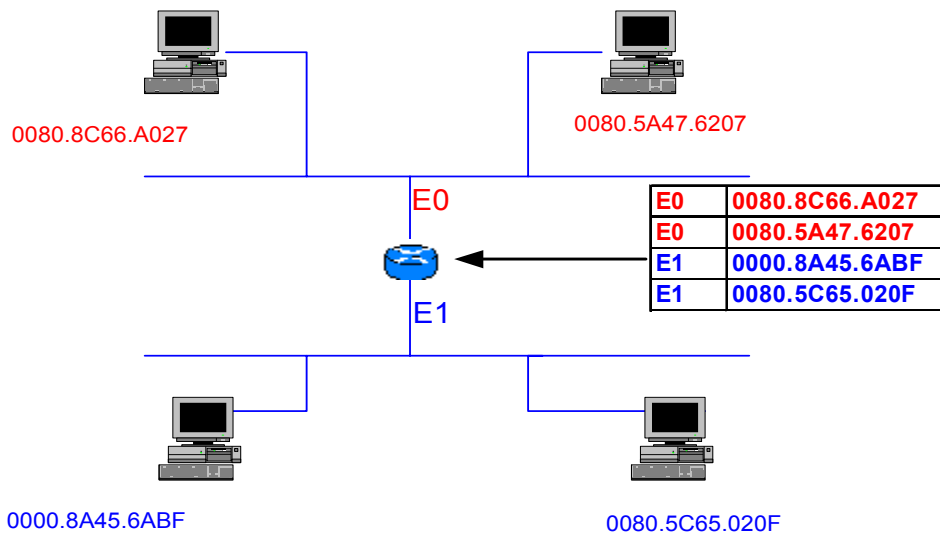


Figure 16

- ❑ Par exemple une trame venant de 0080.8C66.A027 passera de E0 vers E1 seulement si sa destination est 0080.8A45.6ABF ou 0080.5C65.020F (ou un broadcast).
- ❑ Les routeurs Cisco supportent différents types de pontage :

XXVII.B Transparent Bridging

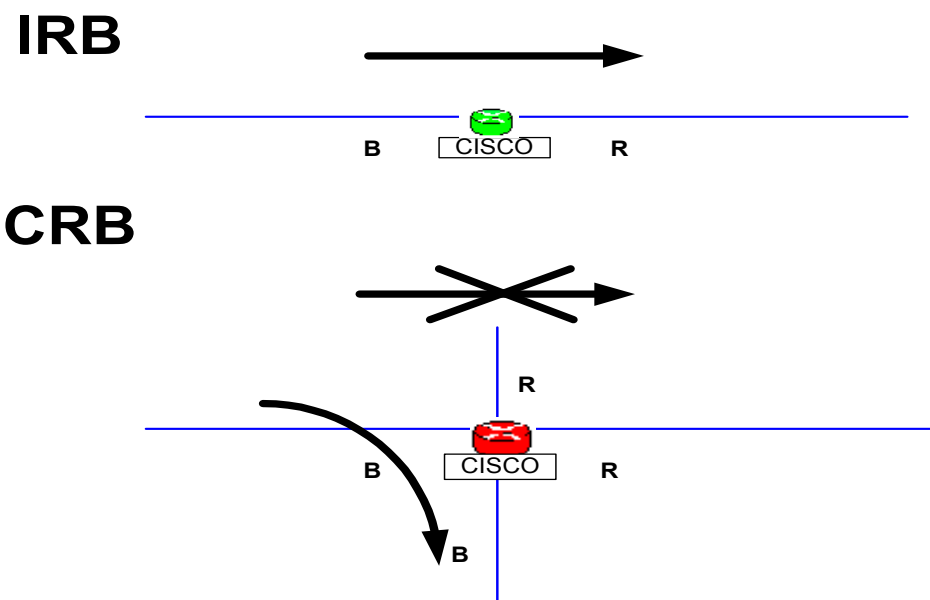
- ❑ Le transparent Bridging est utilisé pour connecter deux réseaux à un même LAN.
- ❑ Le transparent bridging fut développé par Digital (1980), sous le standard IEEE 802.1D.

XXVII.C IRB & CRB

Integrated / Concurrent Routing and bridging

XXVII.C.1 Présentation

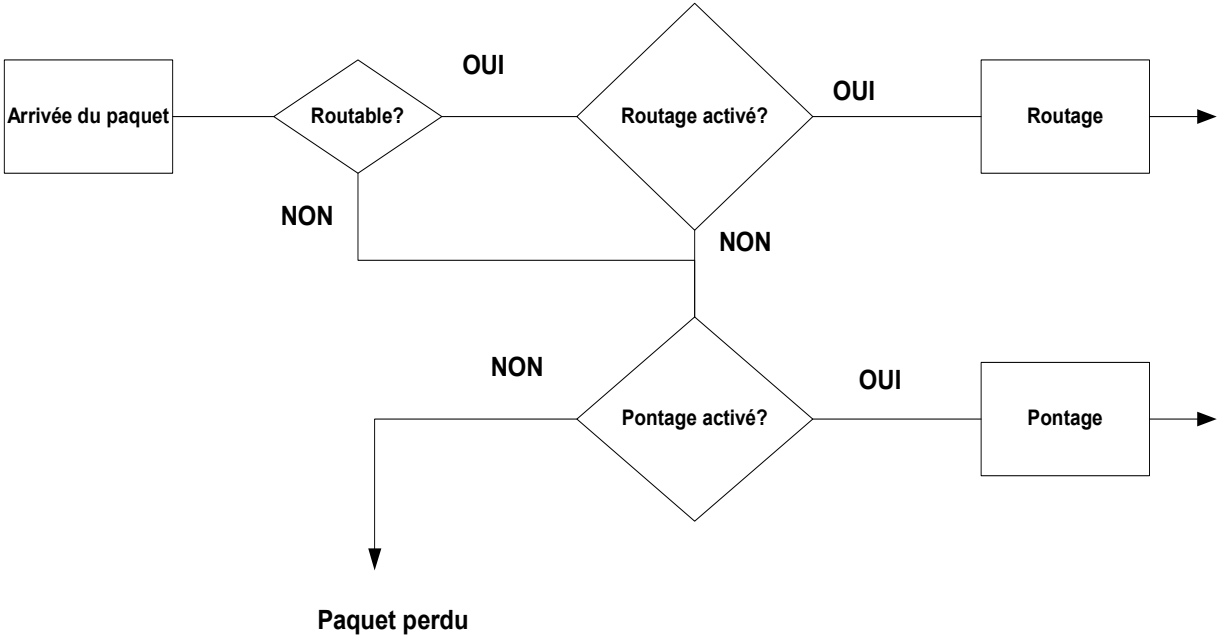
- ❑ IRB est une fonctionnalité apparue avec la version 11.2 de l'IOS Cisco, permettant le routage et le pontage d'un protocole donné. Vous pouvez pour un protocole donné router entre les interfaces routées et ponter entre les interfaces pontées d'un même routeur.
- ❑ Cependant il interdit le pontage et le routage du même protocole sur une interface.
- ❑ CRB (IOS Version 11.0) ne peut pas laisser passer un paquet entre une interface routée et une interface pontée.



- Source route Bridging (SRB),
- Source Route Transparent Bridging (SRT),
- Source route Translational Bridging (SR/TLB)

sont des pontages IBM utilisés pour Token Ring, ils ne seront pas traités.

XXVII.C.2 Le routeur se comporte de la façon suivante :



XXVII.D Configuration du transparent Bridging

bridge bridge-group protocol {ieee dec}	Assigner un bridge groupe et définir un protocole de spanning tree standard (IEEE 802.1D) ou DEC
Interface type number	
bridge-group bridge-group	Assigner un Bridge Group à une interface

Exemple :

```

Paris(config)#bridge 1 protocol ?
  dec  DEC protocol
  ibm  IBM protocol
  ieee IEEE 802.1 protocol

Paris(config)#bridge 1 protocol ieee
Paris(config)#int s 0
Paris(config-if)#bridge-group 1
Paris(config-if)#int eth 0
Paris(config-if)#bridge-group 1
Paris(config-if)#^Z

```

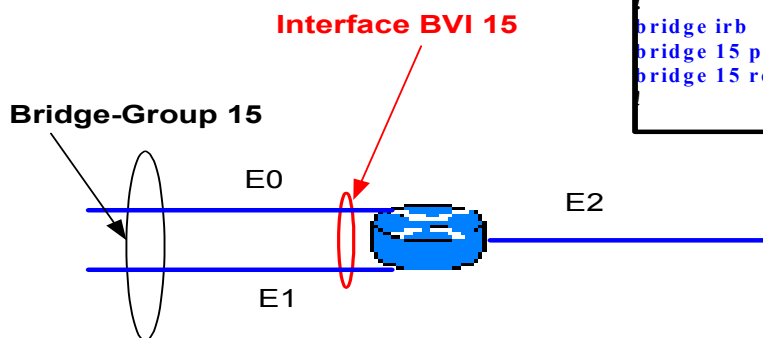
XXVII.D.1 Configuration

- IRB offre la possibilité de router entre une interface Physique et un Bridge-Group grâce à un concept appelle Bridge-Group Virtual Interface (BVI).
 - Le pontage est réalisé entre les interfaces du même Bridge-Group.
 - Les interfaces du Bridge-Group sont regroupées dans une interface BVI.
 - Le routage est réalisé entre l'interface BVI et les interfaces routées.

Exemple :

Cette configuration permet :

- *Le pontage entre E0 et E1*
- *Le routage entre E0 et E2*
- *Le routage entre E1 et E2*



```
interface Ethernet 0
bridge-group 15

interface ethernet 1
bridge-group 15

interface ethernet 2
ip address 172.16.16.1 255.255.255.0

interface BVI 15
ip address 192.168.16.1 255.255.255.0

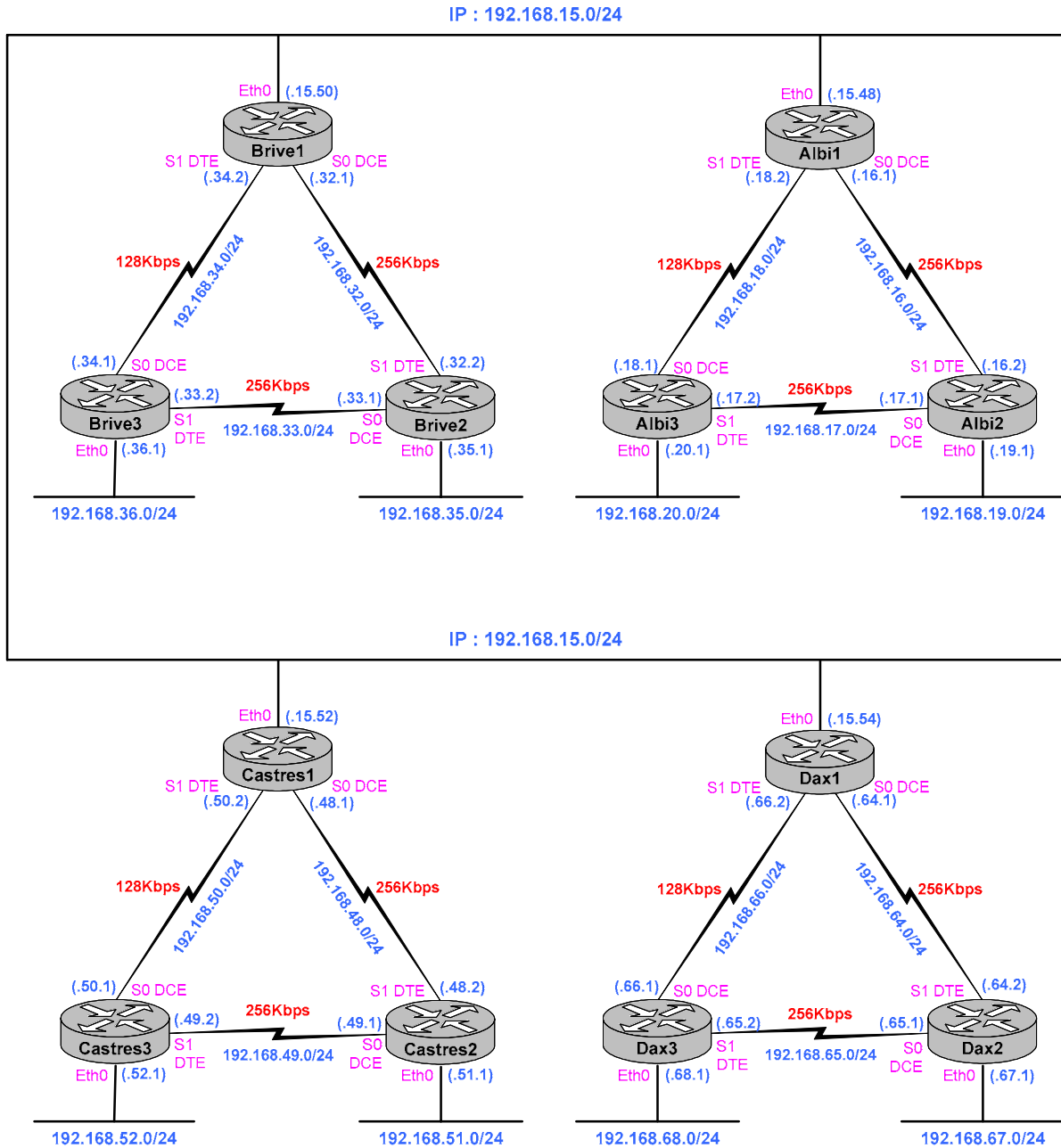
bridge irb
bridge 15 protocol ieee
bridge 15 route ip
```

XXVII.E Commandes

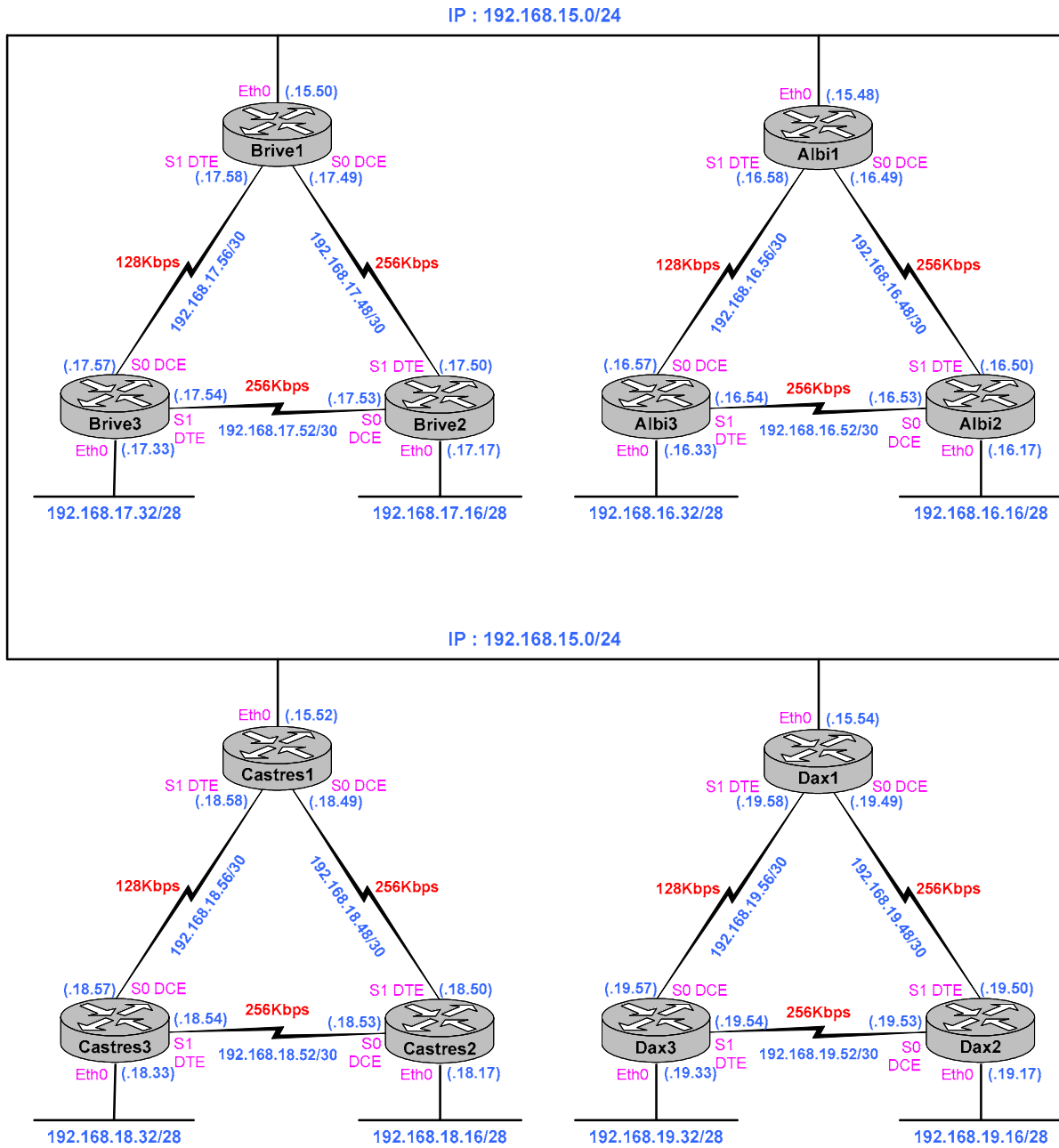
bridge bridge-group protocol {ieee dec}	Assigner un bridge groupe et définir un protocole de spanning tree standard (IEEE 802.1D) ou DEC
interface type number	
bridge-group bridge-group	Assigner un Bridge Group à une interface
BRIDGE IRB	Autoriser l'IRB
interface bvi bridge-group	Créer une interface BVI pour le Bridge-Group
bridge bridge-group route protocol	Spécifier un protocole à router dans un Bridge-Group
no bridge bridge-group route protocol	Spécifier un protocole à ne pas router dans un Bridge-Group
bridge bridge-group bridge protocol	Spécifier un protocole à ponter dans un Bridge-Group
no bridge bridge-group bridge protocol	Spécifier un protocole à ne pas ponter dans un Bridge-Group
exit	
show interface BVI (bridge-group)	Commande de visualisation d'une interface BVI

Annexe A. Maquette d'exercices

A.I Maquette sans VLSM



A.II Maquette avec VLSM



Annexe B. La commande PING

- ❑ La commande 'ping' peut être utilisée dans les modes 'user' et 'privileged EXEC'. Elle prend l'adresse IP de l'interface de sortie comme adresse IP source du paquet, sauf autrement spécifié avec la commande ping étendue.

```
Router > ping 192.168.3.1
```

Codes retour	Description
!	Réponse d'écho ICMP reçue
.	Aucune réponse
U	Message ICMP de destination inaccessible reçu : <i>unreachable</i> (code destination)
N	Message ICMP de réseau inaccessible reçu : <i>unreachable</i> (code réseau)
P	Message ICMP de port inaccessible reçu : <i>unreachable</i> (code port)
Q	Message ICMP de ralentissement de la source : <i>Source Quench</i>
M	Message ICMP de fragmentation impossible reçu : <i>Can't fragment message</i>
?	Paquet de type inconnu reçu.

- ❑ La commande 'ping' étendue est exécutable uniquement en mode 'privileged EXEC'

```
Albil#ping
Protocol [ip]:
Target IP address: 192.168.36.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.18.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.36.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/5/8 ms
Albil#
```

Annexe C. Le REGISTRE

Le REGISTRE															
												Boot field			
b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0
2				1				0				2			

Bits	Position par défaut	Signification
b0 à b3		Boot field
b4		
b5		
b6		Causes system software to ignore NVRAM contents
b7		OEM bit enabled
b8	Actif	BREAK command disabled
b9		Use secondary bootstrap
b10		IP broadcast with all zeros
b11 à b12		Console line speed (9600 bps par défaut)
b13	Actif	Boot default flash software if network boot fails
b14		IP broadcast do not have network numbers
b15		Enable diagnostic messages and ignore NVRAM contents

- Pour connaître la valeur du registre, tapez la commande '#show version'

C.I Rôles du 'Boot Field'

- Ce champ contient les bits : b0 à b3, servant à choisir l'IOS bootable.

Valeur du Boot Field	Commandes de boot system dans Startup-config	Résultat
0x0	Ignorée si présente	Mode contrôle ROM, ROM Monitor.
0x1	Ignorée si présente	Chargement du mini IOS de la ROM : RXBoot mode.
0x2 à 0xF	Aucune commande	Chargement du premier fichier (IOS) de la mémoire flash. Solution par défaut
0x2 à 0xF	#boot system rom	Chargement du mini IOS de la ROM : RXBoot mode.
0x2 à 0xF	#boot system flash	Chargement du premier fichier (IOS) de la mémoire flash.
0x2 à 0xF	#boot system flash <i>nomfichier</i>	Chargement du fichier IOS spécifié de la mémoire FLASH.
0x2 à 0xF	#boot system tftp 10.0.0.1 <i>nomfichier</i>	Chargement du fichier IOS spécifié du serveur TFTP.
0x2 à 0xF	Commandes multiples de <i>boot system</i>	Tentative de chargement du système à partir de la première commande d'amorçage dans la configuration. Si elle échoue, la deuxième commande est utilisée, et ainsi de suite jusqu'à l'exécution réussie d'une commande.

C.II Débit du port console

CISCO 2500		
B12	B11	Débit en bps
0	0	9600 bps par défaut
0	1	4800
1	0	1200
1	1	2400

CISCO 3600			
B5	B12	B11	Débit en bps
1	1	1	115200
1	1	0	57600
1	0	1	38400
1	0	0	19200
0	0	0	9600 bps par défaut
0	0	1	4800
0	1	1	2400
0	1	0	1200

C.III Adresse de broadcast

B14	B10	Adresse
0	0	<uns><uns>
0	1	<zéros><zéros>
1	0	<net><zéros>
1	1	<net><uns>

Le bit : b6, permet de shunter l'exécution du fichier de configuration (Startup-Config) au boot

Annexe E. comparaison des protocoles de routages

Fonctionnalités	RIP	IGRP	EIGRP	OSPF
Temporisateur de mise à jour	30 secondes	90 secondes		
Type	Vecteur de distance	Vecteur de distance		Etat de lien
Métrique	Compte de sauts	Métrique composée qui prend en compte la bande passante, le délai (par défaut), mais aussi la fiabilité, la charge et la valeur MTU.	Métrique composée qui prend en compte la bande passante, le délai (par défaut), mais aussi la fiabilité, la charge et la valeur MTU.	Coût
Valeur de métrique infinie	16	4.294.967.295		
Mécanisme de prévention des boucles	Temporisateur Holddown, Split-horizon	Temporisateur Holddown, Split-horizon	DUAL	Algorithme SPF et connaissance complète de la topologie
Temporisateur Holddown	180	280		
Mises à jour flash	Oui	Oui		
Masque de sous réseau envoyé dans la mise à jour	Non, pour RIP V1 Oui, pour RIP V2	non	Oui	oui

- ✓ En RIP, la métrique maximale est de 16 HOP (métrique infinie)
- ✓ Le coût **OSPF** : il est inversement proportionnel à la bande passante de l'interface. Une bande passante élevée signifie un coût faible. **Coût = 100.000.000 / Bande passante en bps.**
 - Une ligne Ethernet à 10Mbps coûtera $10^8 / 10^7 = 10$,
 - Une ligne T1 coûtera $10^8 / 154400 = 64$.

Protocole de routage	Synthèse automatique activée	Synthèse automatique désactivable	Supporte l'agrégation de routes
RIP v1	Oui, par défaut	Non	Non
RIP v2	Oui, par défaut	Oui	Oui
IGRP	Oui, par défaut	Non	Non
EIGRP	Oui, par défaut	Oui	Oui
OSPF	Non, mais l'agrégation peut remplir la même fonction	Non applicable	Oui

Protocole de routage	Type	Prévention des boucles	Masques envoyés
RIP v1	Vecteur distance	Temporisateur Hold-down et Split-horizon	Non
RIP v2	Vecteur distance	Temporisateur Hold-down et Split-horizon	Oui
IGRP	Vecteur distance	Temporisateur Hold-down et Split-horizon	Non
EIGRP	Hybride équilibré	DUAL et successeur possible	Oui
OSPF	Etat de lien	Algorithme SPF Dijkstra et carte topologique complète	Oui

DUAL : Diffusing Update Algorithm

Annexe F. Procédure de récupération d'un mot de passe perdu

Etape	Action	Modèles anciens : 2000, 2500, 3000, 4000, 7000	Modèles récents : 1600, 2600, 3600, 7200, 7500
1	Eteignez le routeur puis rallumez-le	Utilisez l'interrupteur	
2	Générez une séquence de Break pendant les soixante premières secondes	Appuyez sur la ou les touches qui génèrent la séquence de Break en fonction du terminal ou de l'émulateur de terminal. Sous HyperTerminal de Microsoft appuyez sur CTRL + PAUSE	
3	Visualisez et notez la valeur du registre de configuration : par défaut 0x2102	Exécuter la commande ROMMON > E/S 2000002	Néant
3	Activez le bit 6 du registre de configuration à 1	Exécuter la commande ROMMON > O/R 0x2142	Exécuter la commande ROMMON > confreg 0x2142
4	Bootez sur l'IOS	Exécuter la commande ROMMON > I	Exécuter la commande ROMMON > reset
5	N'acceptez pas le mode <i>Setup</i> qui vous sera proposé à la console	Répondez par NON	
6	Entrez dans le mode privilégié	Appuyez sur la touche Entrée et exécutez la commande : Router > enable (aucun mot de passe requis)	
7	Copiez la configuration de la NVRAM en RAM	Exécuter la commande : # copy startup-config running-config Ou Router# configure memory	
8	Visualisez la configuration pour obtenir les mots de passe non cryptés	Exécuter la commande exec : Router # show startup-config	
9	Changer les mots de passe cryptés	Exécuter les commandes : Routeur # configure terminal Router(Config) # enable secret XXXXXXX Router(Config) # line console 0 Router(Config-line) # login Router(Config-line) # password XXXXXXX Router(Config-line) # exit Router(Config) # line vty 0 4 Router(Config-line) # login Router(Config-line) # password XXXXXXX Router(Config-line) # <CTRL-Z>	
10	Rétablissez la valeur initiale du registre de configuration (voir l'étape 3)	Exécuter les commandes : Router # configure terminal Router(Config) # config-register 0x2102	
	Sauvegardez la configuration	Exécuter la commande : Router # copy running-config startup-config Ou Routeur # write	
11	Rebootez le routeur	Exécuter la commande : Router # reload	

- La commande ROMMON **confreg** sur le routeur 2621 par exemple permet de configurer le registre :
 - Le message « *Ignore system config info [y/n]?* », concerne en fait le bit 6 du registre de configuration. Le fait de répondre « y » place ce bit à 1.
 - La dernière question « *Change boot characteristics [y/n]?* », permet de déterminer si vous voulez modifier le champ d'amorçage du registre.

Séquence de BREAK	
Programme / Système d'exploitation	Caractère ou séquence
HyperTerminal Win9x	Ctrl-F6-Break
HyperTerminal Windows NT	Break-F5 ou Shift-F5
HyperTerminal Windows 2000	Ctrl-Break
Telnet	Ctrl-]
Kermit	Ctrl-b
VT100	F16

```
monitor: command "boot" aborted due to user interrupt
rommon 1 > confreg
```

```
Configuration Summary
(Virtual Configuration Register: 0x2102)
enabled are:
load rom after netboot fails
console baud: 9600
boot: image specified by the boot system commands
or default to: cisco2-C2600
```

```
do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]:
enable "use net in IP bcast address"? y/n [n]:
disable "load rom after netboot fails"? y/n [n]:
enable "use all zero broadcast"? y/n [n]:
enable "break/abort has effect"? y/n [n]:
enable "ignore system config info"? y/n [n]: y
change console baud rate? y/n [n]:
change the boot characteristics? y/n [n]:
```

```
Configuration Summary
(Virtual Configuration Register: 0x2142)
enabled are:
load rom after netboot fails
ignore system config info
console baud: 9600
boot: image specified by the boot system commands
or default to: cisco2-C2600
```

```
do you wish to change the configuration? y/n [n]:
```

```
You must reset or power cycle for new config to take effect
rommon 2 > reset
```

```
System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1)
Copyright (c) 2003 by cisco Systems, Inc.
C2600 platform with 131072 Kbytes of main memory
```

ou

```
System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1)
Copyright (c) 2003 by cisco Systems, Inc.
C2600 platform with 131072 Kbytes of main memory
```

```
monitor: command "boot" aborted due to user interrupt
rommon 1 > confreg 0x2142
```

```
You must reset or power cycle for new config to take effect
rommon 2 > reset
```

```
System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1)
Copyright (c) 2003 by cisco Systems, Inc.
```

Annexe G. Cisco 2600

- Sur les routeurs 2600, il n'y a pas de mini IOS en ROM.
- La mémoire FLASH mémorise une image d'IOS qui sera décompressée au BOOT et qui s'installera en RAM pour exécution.

```
Press RETURN to get started.
```

```
User Access Verification
```

```
Password:
```

```
C2621>enable
```

```
Password:
```

```
C2621#show flash:
```

```
System flash directory:
```

```
File Length Name/status
```

```
1 5248524 c2600-i-mz.122-5d.bin
```

```
[5248588 bytes used, 3140020 available, 8388608 total]
```

```
8192K bytes of processor board System flash (Read/Write)
```

```
C2621#
```

G.1 Sauvegarde IOS

```
C2621#copy flash:c2600-i-mz.122-5d.bin tftp
```

```
Address or name of remote host []? 192.168.3.254
```

```
Destination filename [c2600-i-mz.122-5d.bin]?
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
...
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
5248524 bytes copied in 50.284 secs (104970 bytes/sec)
```

```
C2621#
```

G.II Mise à jour de l'IOS

- ❑ Pour changer d'IOS sur les routeurs, il faut vérifier si celui-ci dispose de suffisamment d'espace mémoire en flash pour accueillir le nouveau IOS. Si la flash est insuffisante, il faut supprimer l'IOS existant.
- ❑ Lorsque vous indiquez le nom du fichier à télécharger, indiquez complètement le nom avec son extension.

```
C2621#erase flash:
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erasedee
Erase of flash: complete
C2621#copy ftp:192.168.3.254 flash:
Address or name of remote host [192.168.3.254]?
Source filename [192.168.3.254]? c2600-is-mz.120-7.T.bin
Destination filename [c2600-is-mz.120-7.T.bin]?
Loading c2600-is-mz.120-7.T.bin from 192.168.3.254 (via FastEthernet0/1): !!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7330920/14661632 bytes]

Verifying checksum... OK (0xE5BB)
7330920 bytes copied in 50.84 secs (146618 bytes/sec)
C2621#show flash:

System flash directory:
File Length Name/status
 1 7330920 c2600-is-mz.120-7.T.bin
[7330984 bytes used, 533336 available, 7864320 total]
8192K bytes of processor board System flash (Read/Write)

C2621#
```

Annexe H. LAN NAMAGER

OSI	LAN MANAGER		
7	Redirecteur		
6	SMB (Server Message Block)		
5	NetBIOS	NBT	NetBIOS
4	NetBEUI	TCP/IP	NWLINK
3			
2	NDIS		
1	Physique		

- ✓ Microsoft recommande NBT pour les réseaux de taille moyenne ou de grands réseaux, ou chaque fois qu'un réseau dispose d'une connexion WAN

Annexe I. Les Protocoles

Les numéros de Protocoles encapsulés dans IP		
Protocole	Numéro	
ICMP	1	
IGMP	2	
TCP	6	
UDP	17	
RSVP	103	
ESP	50	
AH	51	
EIGRP	88	
OSPF	89	
PIM	103	Protocol Independent Multicast
VRRP	112	Virtual Router Redundancy Protocol
L2TP	115	

Annexe J. Les numéros de port

Les numéros de ports utiles		
Port	Service	
20/tcp	ftp-data	FTP, données
21/tcp	ftp	FTP, contrôle
22/tcp	ssh	
23/tcp	telnet	
25/tcp	smtp	Format SMTP (Simple Mail Transfer Protocol)
49	tacacs	
53/tcp & udp	dns	
67/udp	bootps & dhcps	Serveur de protocole d'amorçage
68/udp	bootpc & dhcpc	Serveur de protocole d'amorçage
69/udp	tftp	Transfert de fichiers trivial
80/tcp	http	Serveur WEB (Apache, IIS)
110/tcp	pop-3	
123/udp	ntp : SNTP (MicroSoft)	Protocole date et heure du réseau ; 123 ↔ 123
135/tcp & udp		Microsoft RPC (pour les applications DCOM)
137/tcp & udp	netbios-ns	Service de nom NETBIOS
138/udp	netbios-dgm	Service de datagramme NETBIOS
139/tcp	netbios-ssn	Service de session NETBIOS
1512/tcp & udp	wins	Microsoft Windows Internet Name Service (WINS)
143	s-http ou imap2	
161/udp	snmp	SNMP
162/udp	snmptrap	snmp-trap
220	IMAP3	
514/udp	syslog	
389/tcp	ldap	
636/tcp	ldaps sldap	LDAP par TLS/SSL
443/tcp	https	
88/tcp & udp	kerberos	krb5 kerberos-sec
464/tcp & udp	kpasswd	Kerberos (v5)
500/udp	isakmp ike	Echange de clés Internet
520	rip	Routage dynamique : <ul style="list-style-type: none"> ○ RIP v1 : broadcast ○ RIP v2 : multicast
1812/udp	radius	Protocole d'authentification RADIUS
1813/udp	radacct	Protocole de gestion de comptes RADIUS
3306/tcp	mysql	

Annexe K. Console Port Signals and Pinouts

Use the console RJ-45 to DB-9 serial cable to connect the access point's console port to the COM port of your PC running a terminal emulation program.



Note Both the Ethernet and console ports use RJ-45 connectors. Be careful to avoid accidentally connecting the serial cable to the Ethernet port connector.



Note When your configuration changes are completed, you must remove the serial cable from the access point.

[Table E-1](#) lists the signals and pinouts for the console RJ-45 to DB-9 serial cable.

Console Port		PC COM Port	
RJ-45		DB-9	
Pins	Signals ^{1, 2, 3, 4}	Pins	Signals ^{1, 2, 3, 4}
1	NC	-	-
2	NC	-	-
3	TXD	2	RXD
4	GND	5	GND
5	GND	5	GND
6	RXD	3	TXD
7	NC	-	-
8	NC	-	-

¹NC indicates not connected.

²TXD indicates transmit data.

³GND indicates ground.

⁴RXD indicates receive data.

Annexe L. Les RFC

Protocole	RFC	Commentaire
OSPF	1583 (obsolète) 2328	

Annexe M. Glossaire

AS	Autonomous System Un système autonome désigne un groupement de réseaux, rassemblés dans un même domaine administratif. L'allocation de numéros de système autonome est régie par l'IANA (Internet Assigned Numbers Authority). Cette organisation coiffe plusieurs entités. Ainsi, plus précisément, l'ARIN (American Registry for Internet Numbers) a la responsabilité des numéros pour les Amériques, les Caraïbes et l'Afrique. Le RIPE-NIC (Réseaux IP Européens-Network Information Center) gère les numéros pour l'Europe et, enfin le AP-NIC (Asia Pacific-NIC) administre ceux de la zone Asie Pacifique. Ces numéros de système autonome sont des descripteurs 16 bits.
CIDR	Classless Internet Domain routing, RFC 1466
CSU/DSU	Channel Service Unit / Data Service Unit : équivalent à DCE
DUAL	Diffusing Update Algorithm Processus par l'intermédiaire duquel les routeurs EIGRP calculent collectivement les tables de routage.
FFS	Firewall Feature Set
NBMA	Non-Broadcast Multi-Access Les réseaux NBMA (Non-Broadcast Multi-Access / multiaccès sans diffusions) tels que X25, Frame Relay et ATM, permettent plusieurs connexions sur une seule interface.
OSPF	Open Shortest Path First
VLSM	Variable Length Subnet Mask
VRRP	Virtual Router Redundancy Protocol
WIC	WAN Interface Card

Annexe N. Bibliographie CISCO

Préparation à la certification CCNA	Wendell Odom	CISCO Press
Architecture de réseaux & études de cas		CISCO Press
Conception d'interréseaux CISCO	Matthew H. BIRKNER	CISCO Press
Sécurité des réseaux	Merike KAE0	CISCO Press
Installer et configurer un routeur CISCO	Chris LEWIS	EYROLLES
Configuration IP des routeurs CISCO	Innokenty RUDENKO	EYROLLES
Dépannage des réseaux	Jonathan FELDMAN	CampusPress