DISVE Licence	**ANNEE UNIVERSITAIRE 20011/2012** **SESSION 1** **ETAPE : MIAGE L3** **UE : J1IN6026** **Epreuve : Réseaux informatiques** **Date :** 10/05/2012 **Heure :** 11h00 **Durée :** 1h30 Documents : Tous documents de cours et de TP autorisés, sauf livres. Epreuve de Mr Esnard Aurélien	

Nota Bene : Le barème est donné à titre indicatif.

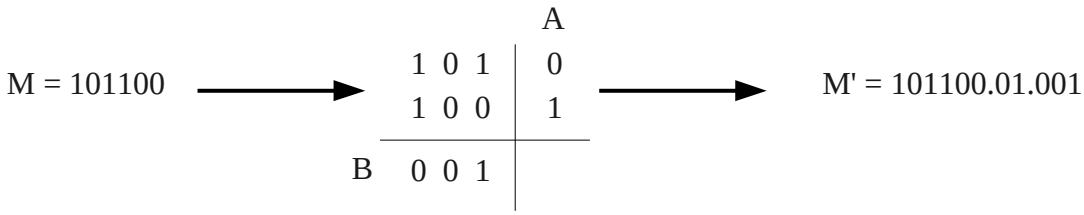
Exercice 1 – CRC (3 pt)

Un protocole de communication utilise la méthode CRC pour la détection d'erreurs avec le polynôme générateur : x + 1.

1. On souhaite transmettre le message binaire 0111110. Calculer la clé CRC en prenant soin de détailler les calculs.
2. Proposez une solution plus simple pour calculer la clé CRC dans ce cas précis.

Exercice 2 – Parité bi-dimensionnelle (4 pt)

On sait que l'ajout d'un bit de parité à une trame permet de détecter les erreurs simples (i.e. portant sur un seul bit) dans un message. Une généralisation de ce principe permet d'obtenir de meilleurs résultats. On organise le message M en plusieurs lignes blocs de *k* bits. On représente le résultat sous forme d'un tableau et on calcule un bit de parité par ligne et un par colonne, comme le montre l'exemple ci-dessous. On ajoute ensuite le résultat de ces deux chaînes de parité à la fin du message pour obtenir M'=M.A.B.



1. Déterminez la valeur d'un tel code M' pour le message M=1010111010111100 de longueur 16 bits. Vous utiliserez un code de parité bi-dimensionnelle avec 4 lignes de 4 bits.
2. Montrez que ce type de code permet de détecter et de corriger toute erreur simple dans un message, ainsi que de détecter toute erreur double.
3. Permet-il de corriger toute erreur double ? Si oui pourquoi, si non donnez un contre-exemple.

Exercice 3 – NAT dynamique (5 pt)

1. Rappeler brièvement le principe du NAT dynamique. A quoi cela-sert-il ?

Lorsqu'une trame est émise depuis une adresse interne vers l'extérieur, elle traverse le passerelle NAT qui remplace, dans l'en-tête du paquet TCP/IP, l'adresse de l'émetteur par l'adresse IP externe et le port source par un numéro de port libre sur le passerelle NAT choisi aléatoirement (parmi 65536 possibilités). Le remplacement inverse est fait lorsqu'une trame correspondant à cette connexion doit être routée vers

l'adresse interne, grâce à une table qui mémorise sur la passerelle NAT les différentes translation en cours.

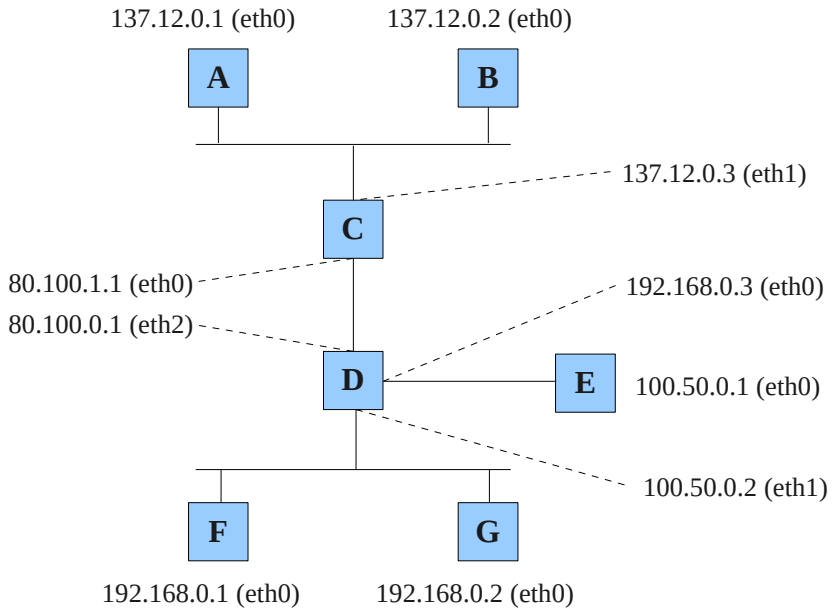
2. Une entreprise pratique la translation d'adresse dynamique avec une passerelle NAT d'adresse publique 193.49.96.60. Quatre stations du réseau (A, B, C et D) souhaitent accéder au site Web dont l'adresse IP est 128.178.50.93. Les adresses internes des stations A, B, C et D sont respectivement 192.168.10.1, 192.168.10.2, 192.168.10.3 et 192.168.10.4. Les quatre machines utilisent le même port source 3001. Compléter la table de translation de la passerelle NAT pendant la connexion.

interne				externe			
source	port	dest	port	source	port	dest	port
192.168.10.1							
192.168.10.2							
192.168.10.3							
192.168.10.4							

3. D'après vous, pourquoi la translation d'adresse IP s'accompagne-t-elle d'une translation de port au niveau de la passerelle NAT ?
4. Combien de connexion TCP/IP les 4 stations peuvent-elles ouvrir simultanément à destination du serveur Web (128.178.50.93) ?

Exercice 4 – Réparer un réseau (8 pt)

Un étudiant en MIAGE a configuré le réseau ci-dessous. Hélas, il a commis quelques erreurs :-(



Voici les tables de routage des différentes machines, configurées par notre étudiant.

	Destination	**Gateway**	**Genmask**	**Flags**	**Iface**
A	137.12.0.0 default	0.0.0.0 137.12.0.3	255.255.255.0 0.0.0.0	U UG	eth0 eth0
B	137.12.0.0 default	0.0.0.0 137.12.0.3	255.255.255.255 0.0.0.0	UH UG	eth0 eth0
C	80.100.0.0 137.12.0.0	0.0.0.0 0.0.0.0	255.255.255.0 255.255.255.0	U U	eth0 eth1
D	192.168.0.0 100.50.0.0 80.100.0.0 default	0.0.0.0 0.0.0.0 0.0.0.0 80.100.0.2	255.255.255.0 255.255.255.0 255.255.0.0 0.0.0.0	U U U UG	eth0 eth1 eth2 eth0
E	100.50.0.0 default	0.0.0.0 100.50.0.2	255.255.255.0 0.0.0.0	U UG	eth0 eth0
F	192.168.0.0 default	0.0.0.0 192.168.0.3	255.255.255.0 0.0.0.0	U UG	eth0 eth0
G	168.192.0.0 default	0.0.0.0 192.168.0.3	255.255.255.0 0.0.0.0	U UG	eth0 eth0

1. Pour chaque machine, indiquez si vous observez une erreur et proposez une ou plusieurs commandes pour la corriger (commandes *route* et/ou *ifconfig* uniquement). Attention, il ne s'agit pas de tout reconfigurer mais de corriger au plus simple.

On se propose maintenant de sécuriser notre réseau avec un firewall. On fixe la politique par défaut de toutes les machines à DROP. Donnez les commandes *iptables* les plus précises pour répondre aux questions suivantes. Attention, il est nécessaire de modifier le firewall de plusieurs machines en INPUT, OUTPUT ou FORWARD pour répondre à chaque question.

2. A communique avec le serveur Web de F.
3. E communique avec le serveur SSH de B.

Corrigé Partiel

Exo 1 (3pt)

1) On pose la division $(X^5+X^4+X^3+X^2+X).X$ / $(X+1)$ et on trouve $Q(X) = X^5+X^3+X+1$ et $C(X) = 1$ comme reste et donc la clé binaire (de longueur 1) est 1 ! **(2pt)**

2) Il s'agit en fait d'un simple calcul de bit de parité. On ne demande pas de preuve... **(1pt)**

Exo 2 (4pt)

1) On pose le calcul sur 4 lignes et 4 colonnes...

1010 => 0
1110 => 1
1011 => 1
1100 => 0

0011

Donc M' = 1010111010111100.A.B avec A=0110 et B=0011. **(2pt)**

2) Pour simplifier notre réponse, nous allons considérer que l'erreur se produit parmi les bits du mot initial (M). Une erreur simple en (i,j) va entraîner que les bits de parité de la ligne i et de la colonne j sont faux ; réciproquement, on peut donc détecter et corriger ce bit faux ! Si deux erreurs se produisent, on pourra la détecter car il y aura au moins 1 bit de parité de faux (et au plus 4 bits faux), mais on ne pourra pas corriger ces erreurs doubles. **(1 pt)**

3) Non. Il suffit de donner un contre exemple bien choisi... **(1pt)**

Exo 3 (5pt)

1) cf. cours **(1pt)**

2) On complète le tableau ci-dessous avec un scénario possible. **(2pt)**

interne (avant translation)				externe (après translation)			
source	port	dest.	port	source	port	dest.	port
192.168.10.1	1000 (a)	128.178.50.93	80	193.49.96.60	2001 (b)	128.178.50.93	80
192.168.10.2	1000 (a)	128.178.50.93	80	193.49.96.60	2002 (b)	128.178.50.93	80
192.168.10.3	1000 (a)	128.178.50.93	80	193.49.96.60	2003 (b)	128.178.50.93	80
192.168.10.4	1000 (a)	128.178.50.93	80	193.49.96.60	2004 (b)	128.178.50.93	80

(a) Le port source est quelconque :en général, choisi aléatoirement parmi les ports libre de chaque machine.
(b) Le port source après translation est choisi aléatoirement sur la passerelle NAT, mais différent des autres !

3) Cela permet de distinguer au niveau de la passerelle NAT plusieurs connexions, provenant de machines internes différentes mais utilisant le même port source. Dans ce cas, la translation inverse serait ambiguë ! **(1pt)**

4) Le facteur limitant est le nombre maximum de translation possibles au niveau de la passerelle NAT, soit 65 536 au total (peu importe le nombre de stations). **(1pt)**

Exo 4 (8pt)

1) Voici la liste des erreurs...
- D : inversion eth1 et eth0
- C : manque la route par défaut
- B : problème du masque pour la route local
- C : le masque de la route local est en /24 au lieu de /16
- G : mauvaise route locale

2) A communique avec le serveur Web de F.

A : iptables -A OUTPUT -d 192.168.0.1 -p tcp –dport 80 -j ACCEPT
A : iptables -A INPUT -s 192.168.0.1 -p tcp –sport 80 -m state –state ESTABLISHED -j ACCEPT
F : iptables -A INPUT -s 137.12.0.1 -p tcp –dport 80 -j ACCEPT
F : iptables -A OUTPUT -d 137.12.0.1 -p tcp –sport 80 -m state –state ESTABLISHED -j ACCEPT
C/D : iptables -A FORWARD -s 137.12.0.1 -d 192.168.0.1 -p tcp –dport 80 -j ACCEPT
C/D : iptables -A FORWARD -d 137.12.0.1 -s 192.168.0.1 -p tcp –sport 80 -m state –state ESTABLISHED -j ACCEPT

3) E communique avec le serveur SSH de B. => idem avec le port 22 pour SSH et @E=100.50.0.1 à la place @F !