Étude d'un système informatisé – Session 2004

Le réseau mis en œuvre est à base d'une architecture Ethernet 100baseT. La communication entre le système temps réel et le système de supervision utilise un protocole propriétaire.

Compléter le tableau en donnant le numéro et le nom de la couche du modèle OSI concernée par les différentes entités ou protocoles présents sur le réseau utilisé. *Réponse: (*802.3 : Norme IEEE pour l'Ethernet CSMA-CD)*

Entité / protocole	Câble UTP	Routeur ADSL	802.3*	Connecteur RJ45	TCP	IP	hub	switch
Couche								
Nom de la couche								

Le réseau possède une adresse IP de classe C : 192.168.17.0

Proposer un plan d'adressage possible pour les différentes machines connectées.
Réponse:

	Routeur ADSL	PC de gestion	PC de commande	Système temps réel
Adresse IP				
Masque				

Pour des questions de maintenance, le technicien en charge du réseau souhaite effectuer une capture des trames émises par le système temps réel. Pour ce faire il dispose d'un ordinateur portable équipé d'un port 100BaseT / RJ45, et d'un logiciel de capture et d'analyse de trames. On connecte cet ordinateur sur le commutateur (switch - voir diagramme de déploiement et extrait de documentation en Annexe 8). Ce commutateur est équipé de 16 ports répartis comme suit :

- Port 1 : noté « UpLink »
- Port 2 et 3 : noté « Replication »
- Port 4 à 15 : ports standards 100 Mbits/sec
- Port 16 : port Gigabit

Le système temps réel est connecté sur le port 4 et le superviseur sur le port 5.

Sur quel port faut-il connecter l'ordinateur portable ?

Réponse: **Port du commutateur =**
Justification :

La question précédente a-t-elle une raison d'être si l'organe de liaison est un concentrateur et non un commutateur ? Justifier la réponse.

Réponse: Oui / Non (entourer la réponse exacte)
Justification :

Le câble UTP/RJ45 à utiliser est-il un câble croisé ou un câble droit ?

Réponse: Croisé / Droit (entourer la réponse exacte)
Justification :

 ©2008

La communication des informations capteur entre le système temps réel et le système de supervision utilise le réseau Ethernet 100baseT et le protocole IP .

On décide d'établir une communication en mode **connecté**. Le système temps réel joue le rôle de serveur ; le PC de supervision est un client de ce dernier. Le port d'écoute fixé par le service est le port **2467**.

Les lignes suivantes proposent des solutions en langage C pour l'ouverture de la socket de communication sur le PC de supervision et sur le système temps réel. Pour chaque ligne, préciser, sans justifier, si elle répond aux besoins de l'application.
Réponse: (Barrer les réponses inexactes)

```
int Sock = socket(AF_INET, SOCK_STREAM, 0) ;
int Sock = socket(AF_INET, SOCK_DGRAM, 0) ;
int Sock = socket(AF_INET, SOCK_RAW, IPPROTO_ICMP) ;
int Sock = socket(AF_UNIX, SOCK_STREAM, 0) ;
int Sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP) ;
int Sock = socket(AF_IPX, SOCK_STREAM, 0) ;
int Sock = socket(AF_INET, SOCK_STREAM, IPPROTO_UDP) ;
```

La socket de communication étant ouverte avec succès tant au niveau du PC de supervision que du système temps réel, l'application serveur attache maintenant cette socket à un point de communication. Cet attachement (binding) nécessite la fourniture d'une structure de type **sockaddr_in**.

Les questions qui suivent permettent de définir les valeurs des différents membres de la structure de type **sockaddr_in** à fournir à l'appel bind() lors de l'initialisation de la socket serveur.

Le type **u_int16_t** correspond à un entier non signé sur 16 bits. Quelle valeur doit être fournie pour le champ **sin_port** de la structure sur le système temps réel?

Réponse: **sin_port =**

A quoi correspond le champ **in_addr** de cette structure dans ce cas ? Ce champ est souvent initialisé avec la valeur symbolique **INADDR_ANY**. Que signifie cette valeur ?

Réponse: **in_addr :**
INADDR_ANY :

L'appel à **bind()** sera suivi d'un appel à la primitive **listen()** puis à la primitive **accept()**. Quels rôles jouent chacun de ces appels systèmes dans une communication en mode connecté ?

Réponse: **listen() :**
accept() :

Les deux trames reproduites ci-dessous sont extraites d'un relevé réalisé par l'analyseur de protocole lors de l'envoi de la séquence informant la supervision que le robot R1 est passé au-dessus de l'un des marqueurs d'un bain.

L'analyse présente, pour les trames 13 et 14, la description des différents protocoles utilisés : Ethernet, IP, TCP.
Pour chaque protocole, la première ligne donne les caractéristiques principales, les lignes suivantes les valeurs et la signification des différents champs.

La dernière partie donne pour chaque trame le contenu brut en hexadécimal suivi d'une représentation ASCII.

 ©2008

```
Trame   Heure       Adr MAC src     Adr MAC dst   Protocole   Description
13      5.643554    000BDB14E06B    LOCAL         TCP         .AP..., len:    3,

Frame: Total frame length: 60 bytes
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
    + ETHERNET: Destination address : 00E018B96B0B
    + ETHERNET: Source address : 000BDB14E06B
      ETHERNET: Frame Length : 60 (0x003C)
      ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
      ETHERNET: Ethernet Data: Number of data bytes remaining = 46 (0x002E)
  IP: ID = 0x6C12; Proto = TCP; Len: 43
      IP: Version = 4 (0x4)
      IP: Header Length = 20 (0x14)
      IP: Precedence = Routine
      IP: Type of Service = Normal Service
      IP: Total Length = 43 (0x2B)
      IP: Identification = 27666 (0x6C12)
      IP: Flags Summary = 2 (0x2)
          IP: .......0 = Last fragment in datagram
          IP: ......1. = Cannot fragment datagram
      IP: Fragment Offset = 0 (0x0) bytes
      IP: Time to Live = 128 (0x80)
      IP: Protocol = TCP - Transmission Control
      IP: Checksum = 0xEB49
      IP: Source Address = 192.168.17.22
      IP: Destination Address = 192.168.17.10
      IP: Data: Number of data bytes remaining = 23 (0x0017)
      IP: Padding: Number of data bytes remaining = 3 (0x0003)
  TCP: .AP..., len:    3, seq:2700201124-2700201127, ack:2053738035, src: 2467  dst: 4425
      TCP: Source Port = 0x09A3
      TCP: Destination Port = 0x1149
      TCP: Sequence Number = 2700201124 (0xA0F1CCA4)
      TCP: Acknowledgement Number = 2053738035 (0x7A698E33)
      TCP: Data Offset = 20 (0x14)
      TCP: Flags = 0x18 : .AP...
          TCP: ..0..... = No urgent data
          TCP: ...1.... = Acknowledgement field significant
          TCP: ....1... = Push function
          TCP: .....0.. = No Reset
          TCP: ......0. = No Synchronize
          TCP: .......0 = No Fin
      TCP: Checksum = 0x3D42
      TCP: Data: Number of data bytes remaining = 3 (0x0003)

00000:  00 E0 18 B9 6B 0B 00 0B DB 14 E0 6B 08 00 45 00   .à.¹k...Û.àk..E.
00010:  00 2B 6C 12 40 00 80 06 EB 49 C0 A8 11 16 C0 A8   .+l.@.€.ëIÀ¨..À¨
00020:  11 0A 09 A3 11 49 A0 F1 CC A4 7A 69 8E 33 50 18   ...£.I ñÌ¤ziŽ3P.
00030:  FA F0 3D 42 00 00 43 06 00 00 00 00               úð=B..C.....

*******************************************************************************

Trame   Heure       Adr MAC src     Adr MAC dst   Protocole   Description
14      5.846679    LOCAL           000BDB14E06B  TCP         .A...., len:    0

Frame: Total frame length: 54 bytes
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
    + ETHERNET: Destination address : 000BDB14E06B     + ETHERNET: Source address : 00E018B96B0B
      ETHERNET: Frame Length : 54 (0x0036)
      ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
      ETHERNET: Ethernet Data: Number of data bytes remaining = 40 (0x0028)
  IP: ID = 0xD73F; Proto = TCP; Len: 40
      IP: Version = 4 (0x4)
      IP: Header Length = 20 (0x14)
      IP: Type of Service = Normal Service
      IP: Total Length = 40 (0x28)
      IP: Identification = 55103 (0xD73F)
      IP: Flags Summary = 2 (0x2)
          IP: .......0 = Last fragment in datagram
          IP: ......1. = Cannot fragment datagram
      IP: Fragment Offset = 0 (0x0) bytes
      IP: Time to Live = 64 (0x40)
      IP: Protocol = TCP - Transmission Control
      IP: Checksum = 0xC01F
      IP: Source Address = 192.168.17.10      IP: Destination Address = 192.168.17.22
      IP: Data: Number of data bytes remaining = 20 (0x0014)
```

 ©2008

```
TCP: .A...., len:    0, seq:2053738035-2053738035, ack:2700201127, src: 4425  dst: 2467
    TCP: Source Port = 0x1149
    TCP: Destination Port = 0x09A3
    TCP: Sequence Number = 2053738035 (0x7A698E33)
    TCP: Acknowledgement Number = 2700201127 (0xA0F1CCA7)
    TCP: Data Offset = 20 (0x14)
    TCP: Flags = 0x10 : .A....
        TCP: ..0..... = No urgent data
        TCP: ...1.... = Acknowledgement field significant
        TCP: ....0... = No Push function
        TCP: .....0.. = No Reset
        TCP: ......0. = No Synchronize
        TCP: .......0 = No Fin
    TCP: Checksum = 0x8053

00000:  00 0B DB 14 E0 6B 00 E0 18 B9 6B 0B 08 00 45 00   ..Û.àk.à.¹k...E.
00010:  00 28 D7 3F 40 00 40 06 C0 1F C0 A8 11 0A C0 A8   .(×?@.@.À.À¨..À¨
00020:  11 16 11 49 09 A3 7A 69 8E 33 A0 F1 CC A7 50 10   ...I.£ziŽ3 ñÌ§P.
00030:  FA ED 80 53 00 00                                 úí€S..
```

Indiquez les adresses Ethernet et les adresses IP du système de supervision et du système temps réel. *Réponse:*

	PC de supervision	Système temps réel
Adresse Ethernet		
Adresse IP		

En identifiant dans la trame 13 le numéro de port source, préciser si cette trame a été émise par le serveur ou par le client.

Réponse: **Port source =** **Emise par :**

Les paquets IP sont-ils fragmentés ? Justifier la réponse.

Réponse: Paquets fragmentés : Oui / Non (entourer la réponse exacte)
Justification :

Les données spécifiques au service de l'application commence à l'octet 36 hexadécimal de la trame 13. Quel est l'identifiant du capteur concerné par cette capture ?

Réponse: **Capteur concerné =**

Quel est le rôle de la trame 14 ?

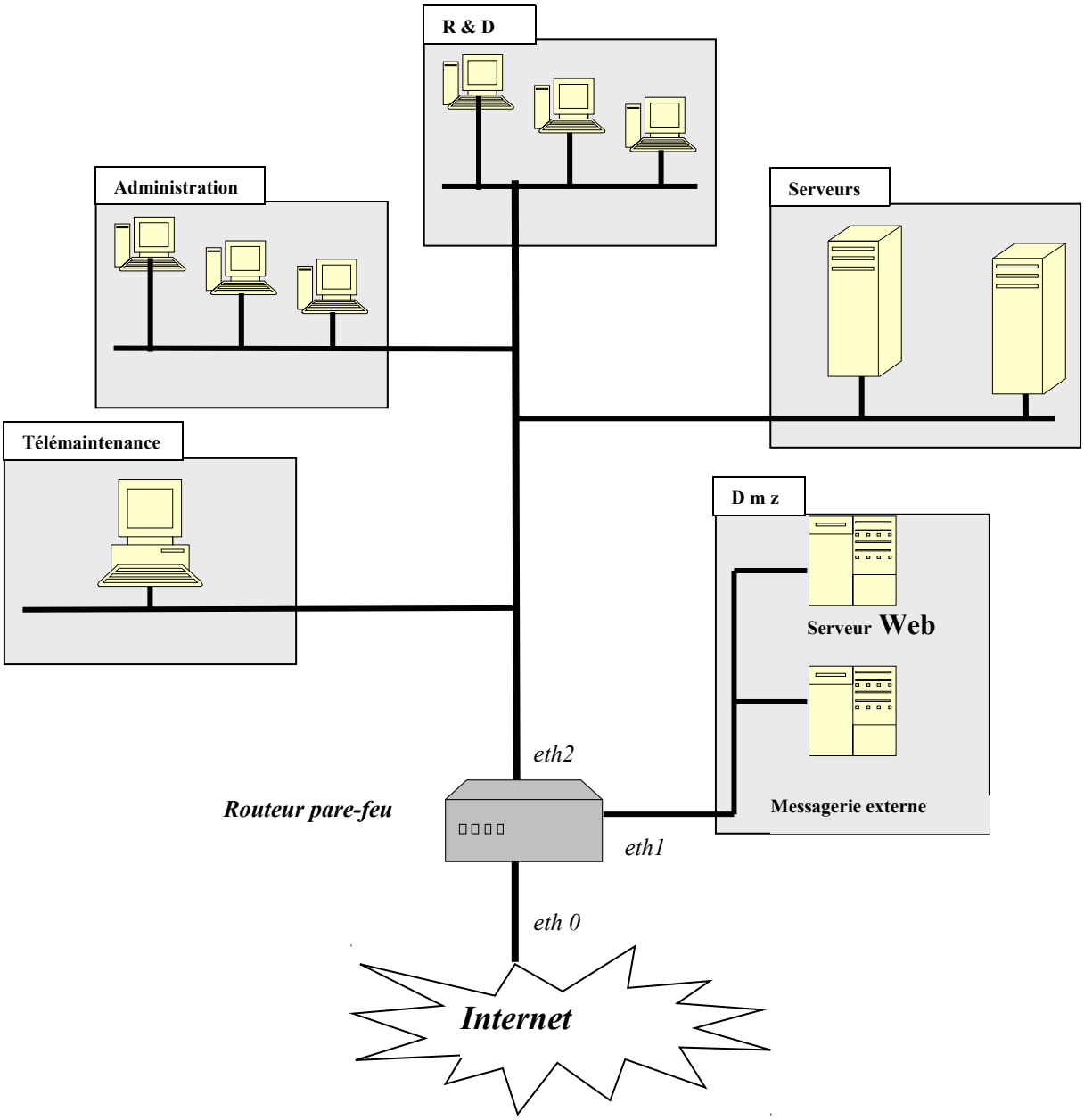
Réponse: **Trame 14 :**

 ©2008

Étude d'un système informatisé – Session 2005

Architecture du réseau du site fournisseur

On dénombre 4 sous-réseaux dont la télémaintenance reliés au routeur WAN.
Une zone DMZ gérée par le pare-feu intègre le serveur Web de la société.



 ©2008

Décrire la méthode d'accès utilisé par le réseau Ethernet. Peut-on qualifier ce réseau de probabiliste ou déterministe ?
Réponse:
La méthode d'accès utilisée sur les réseaux Ethernet est **CSMA/CD (Carrier Sense Multiple Access / Collision Detection)** . Sur ce type de réseau, il est possible que 2 ou plusieurs stations détectent le support libre, décident de transmettre en même temps et ce qui provoque une collision : cette situation pose problème. Le réseau Ethernet a décidé de s'en accommoder en mettant en place un mécanisme de détection et reprise de collision (arrêt de la transmission des stations impliquées, attente d'un temps aléatoire et reprise de la procédure normale). Évidemment, on ne peut prévoir la présence et le nombre de collisions qui vont exister sur ce type de réseau. Remarque: on n'aura pas plus de collisions sur un réseau à 100Mbps que sur un réseau à 10Mbps puisque les collisions ne sont qu'une probabilité !

Donc on qualifie ce type de réseau de **probabiliste**. Un réseau déterministe serait un réseau de type Token Ring ou bus CAN par exemple.

Expliquer le terme 100BASET.
Réponse:
100 -> **100 Mbps -** BASE -> transmission en **bande de base** (sans modulation) - T -> Twisted Pairs (**Paires Torsadées**)

Donner le nom du codage utilisé par Ethernet pour la transmission du signal. Expliquer le principe général de ce type de codage et son rôle.
Réponse: (question ambiguë car les codages utilisés sont différents suivants suivant les normes Ethernet, donc de manière générale :)
10BASET : codage manchester (ou exclusif entre les DATA et l'Horloge) -> réponse donnée dans le corrigé officiel
100BASET : codage 4B/5B MLT3 (le NRZI est utilisé pour du 100BASEFX sur fibre optique)
GigaBit : codage 8B/10B qui consiste à coder, à l'aide d'une table de correspondance une série de 8 bits en un symbole de transmission de 10 bits (appelé Transmission Character). Sur les 1024 valeurs possibles (210 combinaisons), on ne retient pour coder les données que les 256 valeurs qui comprennent moins de quatre transitions et qui ont au plus six zéros consécutifs, même entre les symboles. Ce codage 8B/10B garantit ainsi une bonne récupération d'horloge en réception à très haut débit. Le codage 8B/10B nécessite une vitesse de transmission de 1,25 Gbit/s du fait qu'il faut transmettre 10 bits pour 8 bits d'information. Pour l'instant, une telle vitesse de transmission ne peut être atteint que sur la fibre optique ou sur de courtes distances en cuivre.

Le réseau, présenté dans le sujet, étant **100BASET**, la bonne réponse est : **codage 4B/5B MLT3**
Dans ce codage MLT3, seuls les 1 font changer le signal d'état en prenant successivement sur trois états : +V, 0 et -V (le codage NRZ (Non Retour à Zéro) I (Inversé) n'utilise que 2 états). Les 0 sont codés en conservant la valeur précédemment transmise.
Le principal avantage du codage MLT3 est de diminuer fortement la fréquence nécessaire pour un débit donné grâce à l'utilisation de 3 états. Par contre, les longues séquences de 0 peuvent entraîner une perte ou un déphasage de l'horloge du récepteur. Pour éviter cela, on met en place un codage 4B/5B. Ce codage 4B/5B consiste à coder, à l'aide d'une table de correspondance, une série de 4 bits en 5 bits (par exemple, la séquence 0000 sera codé 01010, il faudra toujours au minimum 2 transitions pour 5 bits et on n'aura jamais plus de 2 zéros consécutifs)

La transmission en bande de base est une transmission sans transposition de fréquence par modulation.
Les codages numériques sont utilisés pour plusieurs raisons :
- la récupération du signal d'horloge facilitée par des variations du signal pour chaque bit d'information transmis
- le spectre d'un signal binaire est concentré sur les fréquences basses qui sont les plus affaiblies sur la ligne.
- les perturbations subies par un signal sont proportionnelles à la largeur de sa bande de fréquence.

Les codages en bande de base vont donc essentiellement avoir pour rôle de diminuer la largeur de bande du signal binaire, de transposer celle-ci vers des fréquences plus élevées et d'utiliser les transitions du signal afin d'assurer une transmission synchrone (qui permettront au récepteur de synchroniser son horloge)**..**

Donner la classe d'adresse du réseau 128.128.0.0. Justifier votre réponse.
Réponse:
128 -> **10**00 0000 (10 indique la **classe B** pour cette adresse)

 ©2008

Donner le masque de sous-réseaux. Justifier votre réponse.
Réponse:

Donner les adresses des sous-réseaux etc...
Réponse:

Nom	Adresse Réseau	Masque	Broadcast	Adresse mini	Adresse maxi

Qu'est-ce qu'une adresse « *broadcast* » ?
Réponse:

Quelle doit être l'adresse de passerelle à préciser dans les paramètres réseau de stations souhaitant accèder à Internet ?
(question ambiguë et piège: cette question aurait dû être placée avant de parler de sous-réseaux)

 ©2008

Expliquer la fonction de cette zone DMZ ?
Réponse:
Il existe plusieurs **zones de sécurité** commune aux réseaux. Ces zones déterminent un niveau de sécurité en fonction des accès réseaux et donnent les bases de l'architecture.

On considère en général trois zones ou réseaux :

Réseaux externes : c'est le réseau généralement le plus ouvert. L'entreprise n'a pas ou très peu de contrôle sur les informations, les systèmes et les équipements qui se trouvent dans ce domaine.

Réseaux internes : les éléments de ce réseau doivent être sérieusement protégés. C'est souvent dans cette zone que l'on trouve les mesures de sécurité les plus restrictives et c'est donc le réseau le moins ouvert.

Réseaux intermédiaires : cette zone est un compromis entre les deux précédentes. Ce réseau est composé de services fournis aux réseaux internes et externes. Les services publiquement accessibles (serveurs de messagerie, Web, FTP et DNS le plus souvent) sont destinés aux utilisateurs internes et aux utilisateurs par Internet. Cette zone est couramment appelée réseau de service ou de zone démilitarisée (DMZ *De-Militarized Zone*).

Donc, la DMZ est considérée comme la zone moins protégée de tout le réseau et qui permet un accès aux services publics de l'entreprise pour les utilisateurs extérieurs.

Cette décomposition (et la présence d'une DMZ) est important pour définir les règles de filtrage du firewall (parefeu).

Quelles seraient les fonctionnalités apportées par l'installation d'un serveur proxy HTTP ?
Réponse:
Un *proxy* procure :
- de nouveaux mécanismes de sécurité (filtrage d'URL, authentification des utilisateurs, ...)
- améliorer les performances en offrant une fonction de cache de pages Web.

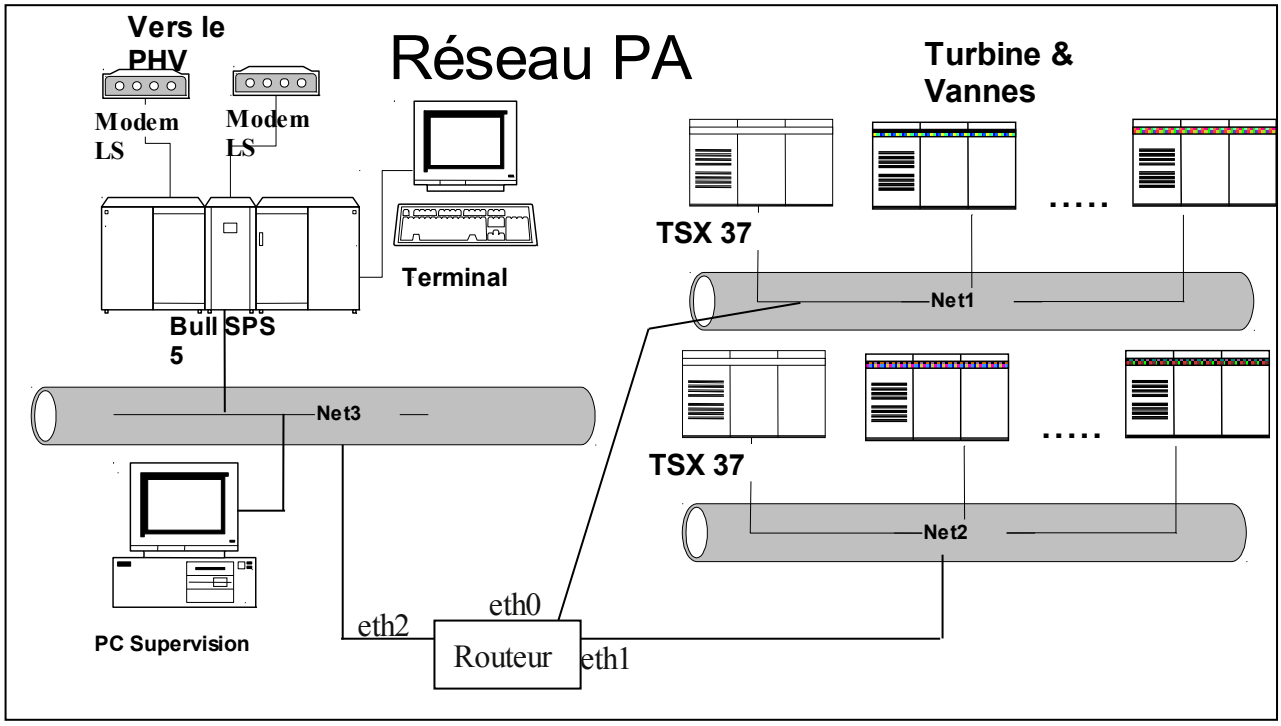
Techniquement parlant, le *proxy* est un relais entre le client et le serveur de destination. Dans l'exemple du Web, le navigateur va se connecter au *proxy* et le *proxy* se connecte ensuite au serveur. Ainsi les utilisateurs du réseau interne ne sont pas reliés directement à Internet, seul le *proxy* y est connecté. Le *proxy* sera donc placé dans la DMZ.

 ©2008

Étude d'un système informatisé – Session 2006

Réseaux du P.A.

On désire remplacer le réseau Modbus par un réseau TCP/IP et la console de supervision par un ordinateur de type PC sur lequel se fera la supervision du système. L'architecture voulue du futur réseau est représentée sur la figure suivante.



Pour des raisons de sécurité, les automates sont dédoublés, ainsi chaque groupe est contrôlé par 2 automates, soit un total de 12 automates nommés API-1 à API-12. Le réseau est lui aussi dédoublé, les automates dont le numéro est impair sont connectés au réseau nommé "net1" et les automates dont le numéro est pair sont connectés au réseau nommé "net2". Le réseau "net3" relie le calculateur BULL et le PC de supervision. Les trois réseaux sont connectés entre eux par un routeur disposant de 3 interfaces réseaux (eth0, eth1 et eth2).

L' "adresse réseau" est **192.168.1.0**.

Quelle est la classe de cette adresse ? Justifiez votre réponse.
Pour cette adresse réseau, quelle est le "masque réseau" par défaut ?
Quelle est l'adresse de diffusion (*broadcast*) de ce réseau ?
Réponse:

 ©2008

Pour réaliser l'architecture réseau présentée ci-dessus, on crée 3 sous réseaux.

D'après le schéma réseau sur la page précédente, quel est le nombre de machines présentes sur le sous-réseau "net1" ?
En tenant compte de l'adresse réseau et de l'adresse *broadcast*, combien de bits d'adresse seront nécessaires pour la partie "adresse machine" de l'adresse IP ?
Combien de bits d'adresse restent-ils pour la partie "adresse sous-réseau" de l'adresse IP ? Justifiez vos réponses.
Réponse:
Nombre d'équipements :
Nombre de bits pour l'adresse équipements :
Nombre de bits pour l'adresse sous-réseau :
Justification :

On choisira finalement d'utiliser 3 bits pour l' "adresse sous réseau" et 5 bits pour l' "adresse machine".

Remplir le tableau du document réponse :
Réponse: Il y a 8 possibilités d'adresse sous-réseau, on peut choisir n'importe lesquelles.
Voici un exemple :

Nom	**Adresse Réseau**	**Masque**	**Broadcast**	**Adresse mini**	**Adresse maxi**
net1					
net2					
net3					

Proposer un plan d'adressage pour l'ensemble du réseau PA.

Équipement	Adresse IP	Équipement	Adresse IP
Routeur: eth0			
eth1			
eth2			
PC supervision			
BULL SPS 5			
API-1		API-2	
API-3		API-4	
API-5		API-6	
API-7		API-8	
API-9		API-10	
API-11		API-12	

L'étude porte sur un échanges entre un maître MODBUS (BULL) et un esclave MODBUS (API) (Trames ÉTHERNET TCP/IP MODBUS) : Les trames Ethernet en annexe 6 ont été relevées à l'aide d'un logiciel de capture de trames.

 ©2008

Remplir les champs contenus dans le tableau du document réponse en vous aidant de l'échange « Réponse API ☐ PC »

CHAMP (IP)	VALEUR	CHAMP (TCP)	VALEUR
Version :	04	Port Source :	502
Type de service :	00	Port Destination :	1062
Identification :	40	Numéro d'ordre :	7EBC69D5
Durée de vie :	64	Numéro d'accusé de réception :	3E544F58
Protocole :	06	URG :	0
Somme de contrôle de l'en-tête :	1CCA	ACK :	1
Adresse source:	192.168.1.1	PSH :	1
Adresse destination :	192.168.1.129	FIN :	0
Nombre d'octets que comporte le datagramme IP	33	Somme de contrôle :	C9A2
		Nombre d'octets que comporte le datagramme TCP	20

Remplir les champs contenus dans le tableau du document réponse en vous aidant des échanges PC☐ API et du protocole Modbus sur TCP/IP de l'annexe 6.

CHAMP (MODBUS)	VALEUR	CHAMP (MODBUS)	VALEUR	CHAMP (MODBUS)	VALEUR
Identificateur de transaction	0000	Unit Identifier	00	Nombre de mots lus	01
Identificateur de protocole	0000	Code requête	03	Numéro du mot lu	0019
Longueur	06				

 ©2008

Étude d'un système informatisé – Session 2007

Quelle information des protocoles TCP et UDP identifie sans équivoque le processus destinataire du message ?
Réponse:

Citer les trois informations définies par /etc/services pour chacun des services.
Réponse:

1)
2)
3)

Un même numéro de port peut-il être utilisé simultanément en TCP et en UDP par deux processus distincts ? Justifier votre réponse.
Réponse:

Particularités des protocoles TCP et UDP ?
Réponses:

	TCP	**UDP**
numéro et nom de couche OSI		
protocole sous-jacent		
fiabilité du transport		
séquencement des données		
mode de connexion		
taille maximale des données		
possibilité de diffusion		

Protocole ARP ?
Réponse:

Vrai / Faux	**Propositions**
	ARP est un protocole de couche 6.
	ARP signifie protocole de résolution d'adresses.
	Une requête ARP est forcément en diffusion.
	ARP est utilisé par un ordinateur lorsqu'il souhaite émettre une trame Ethernet à une autre machine dont il ne connaît que l'adresse MAC.
	Si l'adresse IP est présente dans le cache de l'émetteur, il suffit de lire l'adresse MAC correspondante pour envoyer la trame Ethernet.

 ©2008