

Centre organisateur : Université Claude Bernard Lyon 1	Concours externe d'assistant ingénieur BAP E « gestionnaire de parc informatique et télécommunications »	durée	3 H
SESSION 2008	Epreuve : étude d'un dossier technique	Coefficient	4

Consignes Générales

Ce sujet comporte 25 pages. Assurez-vous que vous êtes en possession de la totalité du sujet avant de commencer l'épreuve (dans le cas contraire demandez en un autre aux surveillants).

Votre identité ne doit figurer que dans la partie supérieure de la copie double et votre nom et prénom sur chaque page du sujet mis à votre disposition.

Toute mention d'identité (nom, initiales, signature...) ou tout signe distinctif porté sur toute autre partie du sujet que vous remettrez en fin d'épreuve mènera à l'annulation pure et simple de votre épreuve.

Le candidat devra rendre l'intégralité du sujet non dégrafé dans la copie double.

Consignes du jury

L'usage de la calculatrice ou de tout autre document ou matériel est interdit.

Ne pas écrire au crayon de papier.

Les réponses doivent être obligatoirement faites sur les feuilles du sujet dans les cadres prévus.

Pour le QCM, cochez une case et une seule. Le barème du QCM s'établit comme suit :

- ✓ Une bonne réponse vaut un point ;
- ✓ L'absence de réponse ne rapporte aucun point ;
- ✓ Un point est retranché en cas de mauvaise réponse.

1. Dossier technique.....	3
2. QCM.....	10
3. Analyse algorithmique (explication de script).....	16

1. Dossier technique.

Contexte.

Vous allez étudier le réseau d'un département d'enseignement au sein d'une université dont le nom de domaine est **université.fr**.

Ce réseau est constitué de quatre sous-réseaux ou VLAN interconnectés par un pare-feu assumant les fonctions de routage, de *statefull firewall* et de translation d'adresses :

- ✓ Un VLAN des postes de travail des étudiants ;
- ✓ Un VLAN des postes de travail des personnels (enseignants, techniques et administratifs) ;
- ✓ Un VLAN des serveurs internes ;
- ✓ Un VLAN DMZ pour les serveurs joignables de l'extérieur.

Le routeur connecte également ces sous-réseaux du département d'enseignement à l'épine dorsale du réseau de l'université sur laquelle un routeur d'entrée connecte le réseau de l'université à Internet.

Le département d'enseignement gère les serveurs suivants :

- ✓ Un serveur DNS secondaire du domaine **université.fr**, dnsENS.universite.fr.
- ✓ Un serveur hébergeant le site Web institutionnel du département (<http://ENS.universite.fr>) destiné à la communication externe,
- ✓ Un serveur hébergeant le site Intranet (<http://intraENS.universite.fr>) réservé aux personnels du département,
- ✓ Un serveur d'impression (lpENS.universite.fr),
- ✓ Un serveur de fichiers (fichiersENS.universite.fr).

Le service informatique central de l'université gère les serveurs suivants connectés sur l'épine dorsale du réseau :

- ✓ Un annuaire LDAP de l'établissement, ldap.universite.fr
- ✓ Un serveur de messagerie mel.universite.fr (POP, IMAP et SMTP),
- ✓ Le serveur DNS primaire du domaine universite.fr, dns.universite.fr.

Découverte du réseau.

Depuis la machine **pc1.universite.fr** connectée sur le VLAN des postes de travail des personnels, l'exécution de plusieurs commandes en ligne donne les résultats suivants :

```
admin@pc1:~$ /sbin/ifconfig
eth0  Lien encap:Ethernet  HWaddr 00:30:48:68:76:9C
      inet adr:192.168.2.24  Bcast:192.168.2.255  Masque:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:76424404  errors:0  dropped:0  overruns:0  frame:0
      TX packets:106436464  errors:0  dropped:0  overruns:0  carrier:0
      collisions:0 lg file transmission:1000
      RX bytes:4177535338 (3.8 GiB)  TX bytes:3290892447 (3.0 GiB)
      Adresse de base:0x2000 Mémoire:da300000-da320000

lo    Lien encap:Boucle locale
      inet adr:127.0.0.1  Masque:255.0.0.0
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:2104331  errors:0  dropped:0  overruns:0  frame:0
      TX packets:2104331  errors:0  dropped:0  overruns:0  carrier:0
      collisions:0 lg file transmission:0
      RX bytes:389408944 (371.3 MiB)  TX bytes:389408944 (371.3 MiB)
```

```
admin@pc1:~$ ping -c 2 dns.universite.fr
PING dns.universite.fr (193.48.100.6) 56(84) bytes of data:
64 bytes from dns.universite.fr(193.48.100.6): icmp_seq=1 ttl=63 time=1.49 ms
64 bytes from dns.universite.fr(193.48.100.6): icmp_seq=2 ttl=63 time=0.435 ms
--- dns.universite.fr ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.435/0.963/1.491/0.528 ms
```

```
admin@pcl:@pcl$ ping -c 1 -b 192.168.3.255
WARNING: pinging broadcast address
PING 192.168.3.255 (192.168.3.255) 56(84) bytes of data.
64 bytes from 192.168.3.12: icmp_seq=1 ttl=63 time=0.245 ms
64 bytes from 192.168.3.40: icmp_seq=1 ttl=63 time=0.212 ms
64 bytes from 192.168.3.22: icmp_seq=1 ttl=63 time=0.350 ms
--- 192.168.3.255 ping statistics ---
1 packets transmitted, 3 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.245/0.269/0.350/0.081 ms
```

```
admin@pcl:$ wget -S http://intraENS.universite.fr
--16:43:43-- http://intraENS.universite.fr/
=> 'index.html'
Résolution de intraENS.universite.fr... 192.168.3.22
Connexion vers intraENS.universite.fr[192.168.3.22]:80...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
HTTP/1.1 200 OK
Date: Tue, 10 Jun 2008 14:49:00 GMT
Server: Apache/2.0.54 (Debian GNU/Linux) PHP/4.3.10-22 mod_ssi/2.0.54
OpenSSL/0.9.7e
X-Powered-By: PHP/4.3.10-22
Content-Length: 6623
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
Longueur: 6 623 (6.5K) [text/html]
100%[=====>] 6 623 --.-K/s
16:43:43 (300.77 MB/s) - « index.html » sauvegardé [6623/6623]
```

```
admin@pcl:$ host dnsENS.universite.fr
dnsENS.universite.fr has address 193.48.100.136
admin@pcl:$ host ENS.universite.fr
ENS.universite.fr has address 193.48.100.131
```

```
admin@pc1:$ host lpENS.universite.fr
lpENS.universite.fr has address 192.168.3.12
admin@pc1:$ host pc2.universite.fr
pc2.universite.fr has address 192.168.1.57
```

Depuis la machine **pc2.universite.fr** connectée sur le VLAN des postes de travail des étudiants, l'exécution de plusieurs commandes en ligne donne les résultats suivants :

```
user@pc2$:netstat -rn
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic  MSS Fenêtre  irtt  Iface
192.168.1.0      0.0.0.0         255.255.255.0   U      0 0        0     eth0
0.0.0.0          192.168.1.1    0.0.0.0         UG     0 0        0     eth0
```

```
user@pc2:$ telnet mel.universite.fr smtp
Trying 193.48.100.17...
Connected to mel.universite.fr.
Escape character is '^]'.
220 mel.universite.fr ESMTP Postfix (Debian/GNU)
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

```
user@pc2:$ dig ldap.universite.fr a in +short
193.48.100.12
```

Depuis le routeur d'entrée du réseau de l'université connecté à l'épine dorsale du réseau de l'université, l'exécution d'une commande en ligne donne les résultats suivants :

```
Routeur-entree>show ip route
S    192.168.1.0/24 [1/0] via 193.48.100.105
S    192.168.2.0/24 [1/0] via 193.48.100.105
S    192.168.3.0/24 [1/0] via 193.48.100.105
     193.48.100.0/24 is variably subnetted, 2 subnets, 2 masks
C    193.48.100.0/25 is directly connected
S    193.48.100.128/28 [1/0] via 193.48.100.105
```

Q1 : Quelle est l'adresse MAC (Ethernet) de pc1.universite.fr ?

Q2 : Quel logiciel de serveur de messagerie tourne sur mel.universite.fr ?

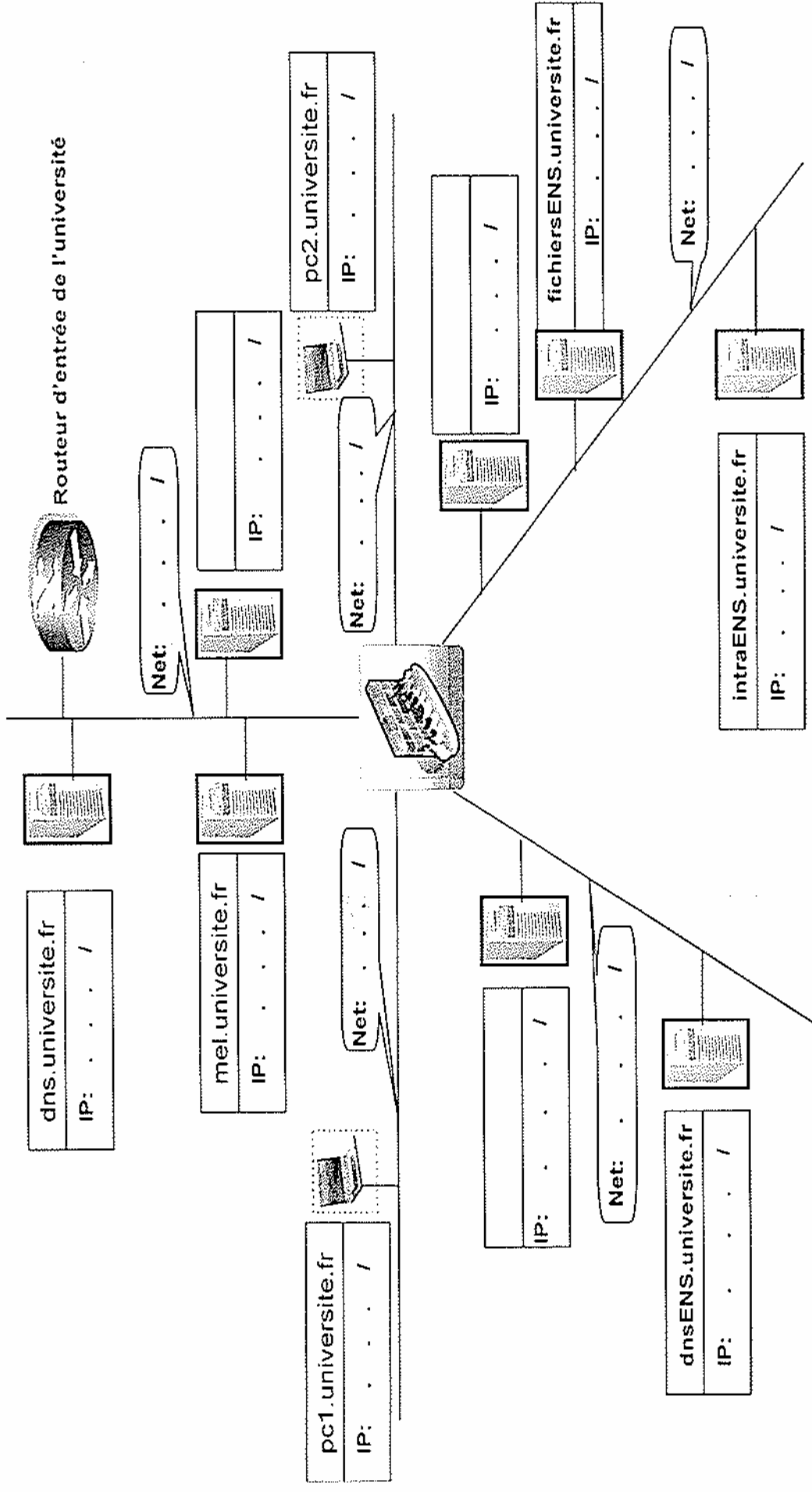
Q3 : Quel système d'exploitation tourne sur intraENS.universite.fr ?

Q4 : Quel est le *round trip time* maximal mesuré entre pc1.universite.fr et dns.universite.fr (temps aller du paquet ICMP echo plus temps retour du paquet ICMP reply) ?

Q5 : Quelle est l'adresse IP de l'interface du pare-feu connectant l'épine dorsale du réseau de l'université ?

Q6 : combien reste-t-il d'adresses IP disponibles pour numéroté les futurs serveurs sur le VLAN de la DMZ du département ?

Q7 : complétez les noms Internet, les adresses IP et les préfixes de réseau manquant dans le schéma du réseau ci-dessous. Les noms Internet doivent être au format FQDN (par exemple, intraENS.universite.fr). Les adresses IP des machines et des préfixes de réseau doivent être accompagnées du masque au format CIDR (par exemple 192.168.1.1/24).



Attention : pour Q8 et Q9 vous pouvez citer **au choix** les versions non sécurisées des protocoles **ou** les versions sécurisées.

Q8 : Quels sont les ports TCP ou les protocoles que le pare-feu doit laisser passer entre le VLAN des personnels et l'épine dorsale pour que les personnels puissent relever leur courrier et envoyer des messages à l'aide d'un client de messagerie (c'est-à-dire **pas** en WebMail) ?

Q9 : Quels sont les ports TCP ou les protocoles que le pare-feu doit laisser passer entre l'épine dorsale du réseau de l'université et intraENS.universite.fr pour que ce serveur puisse authentifier les personnels en interrogeant l'annuaire de l'établissement ?

Q10: A l'aide du manuel de l'outil *ldapsearch* donné en annexe, décrivez les informations qui seront récupérées à l'aide de la commande suivante :

```
ldapsearch -x -LLL -h ldap.universite.fr  
-b "ou=People,dc=universite,dc=fr" -s sub  
'(&(employeeType=etudiant)(mail=*))' givenName name mail
```

Q11: Quelle est la différence entre une configuration statique d'un serveur DHCP et une configuration dynamique ? Quels sont les avantages de la configuration statique ?

Q12: Comment maîtriseriez-vous la place disque qu'occupe un utilisateur sur le serveur de fichiers ?

2. QCM.

Cochez une case et une seule. Le barème du QCM s'établit comme suit :

- ✓ Une bonne réponse vaut un point ;
- ✓ L'absence de réponse ne rapporte aucun point ;
- ✓ Un point est retranché en cas de mauvaise réponse.

1. Lequel de ces standards ne désigne pas un support de sauvegarde sur bande magnétique.

- LTO
- DLT
- SATA
- DAT

2. Quelle est la notation décimale du nombre binaire 01001100 ?

- 64
- 72
- 76
- 84

3. La norme ISO 8859-15 :

- Est un mode de codage des caractères sur 8 bits créé par IBM à l'époque des cartes perforées.
- Est une norme donnant un code numérique tenant sur 8 bits aux caractères de l'alphabet latin utilisés en français et pour d'autres langues européennes.
- définit 128 caractères numérotés de 0 à 127
- est un jeu de caractères disponible sur le système d'exploitation Microsoft Windows aux USA et en Europe aussi appelé CP1252.

4. Le Peripheral Component Interconnect (abrégié en PCI) est :

- un standard définissant un bus informatique permettant de relier un ordinateur à des périphériques ou bien même à un autre ordinateur.
- un standard de bus local (interne) permettant de connecter des cartes d'extension sur la carte mère d'un ordinateur.
- un bus informatique *plug-and-play* à transmission série servant à brancher des périphériques informatiques à un ordinateur.
- un bus rapide Plug and Play utilisé pour brancher toutes sortes de périphériques gourmands en bande passante comme un disque dur ou un caméscope.

5. Lequel de ces standards n'est pas relatif à une technologie de réseau sans fil ?
- IEEE802.3
 - IEEE802.11g
 - Bluetooth
 - WIMAX
6. IMAP est un:
- Protocole de gestion de boîte aux lettres électroniques.
 - Système d'information géographique
 - Système de gestion de fichier
 - Langage de programmation orienté objet
7. Lequel de ces acronymes ne désigne ni un protocole ni un standard utilisé en téléphonie sur IP ?
- SIP
 - SPIP
 - H.323
 - UIT-T G.761
8. Lequel de ces standards désigne une liaison Ethernet 1 Gbit/s sur fibres optiques ?
- IEEE 10/100BaseTX
 - IEEE 10/100/1000BaseT
 - IEEE 1000BaseSX
 - IEEE 100BaseFX
9. Laquelle de ces méthodes de configuration d'un VLAN sur un commutateur Ethernet nécessite-t-elle l'usage du protocole IEEE802.1x ?
- Par port
 - Par protocole
 - Par adresse MAC
 - Par utilisateur authentifié
10. Quel est le débit nominal maximal d'un point d'accès au réseau sans fil à la norme IEEE802.11b ?
- 2 Mbit/s
 - 11 Mbit/s
 - 54 Mbits/s
 - 108 Mbit/s
11. Lequel de ces protocoles ne désigne pas une méthode d'authentification utilisable en IEEE802.11x ?
- TLS
 - TTLS
 - PEAP
 - AES
12. Lequel de ces noms ne désigne pas une distribution du système Linux ?
- Mandriva
 - Debian
 - Redhat
 - Solaris

13. Lequel de ces systèmes de gestion de fichier ne permet pas la gestion des droits d'accès par utilisateur ?
- FAT
 - NTFS
 - EXT3
 - XFS
14. Quelle technique permet de sauvegarder le contenu d'une page de mémoire vive inutilisée sur disque afin de libérer de la place en mémoire pour un autre processus ?
- Phishing
 - Mapping
 - Dampening
 - Swapping
15. Quelle commande unix permet de connaître l'activité et la charge des différents composants du système d'exploitation ?
- vmstat
 - netstat
 - Ifconfig
 - mem
16. Quel logiciel permet la prise de contrôle à distance d'un ordinateur ?
- PVC
 - SVC
 - VLC
 - VNC
17. Quel logiciel permet la réplication d'une image disque simultanément sur plusieurs ordinateurs de configuration matérielle identique ?
- Ghost
 - Wpkg
 - OCS Inventory
 - PC Anywhere
18. Laquelle de ces actions n'est pas réalisée par un logiciel antivirus ?
- Mise à jour du système d'exploitation
 - Analyse temps-réel des fichiers ouverts
 - Mise à jour des signatures virales
 - Analyse différée des fichiers présents sur un support fixe ou amovible.
19. Lequel de ces outils permet la gestion et l'inventaire d'un parc d'ordinateurs ?
- XEN
 - NFS
 - OCS Inventory
 - VMWARE

20. Lequel de ces langages de programmation est orienté objet ?
- Bash
 - C++
 - C
 - Basic
21. Laquelle de cette technique ne désigne pas une méthode de passage de paramètres à un sous-programme ?
- Par nom
 - Par adresse
 - Par valeur
 - Par dichotomie
22. Laquelle de ces structures de contrôle d'algorithme ne correspond pas à une boucle itérative ?
- Si ($i > n$) alors {instruction1 ; instruction 2 ; ... ; instruction n}
 - Pour ($i = \text{de } 1 \text{ à } n$) faire {instruction1 ; instruction 2 ; ... ; instruction n}
 - Tant que ($i < n$) faire {instruction1 ; instruction 2 ; ... ; instruction n}
 - A moins que ($i = n$) faire {instruction1 ; instruction 2 ; ... ; instruction n}
23. Lequel de ces langages de programmation est interprété ?
- PHP
 - C
 - C++
 - Pascal
24. Lequel de ces logiciels ne désigne pas un système de gestion de base de données ?
- Oracle
 - PostgreSQL
 - Business Object
 - MySQL
25. Que fait la commande SQL suivante : `DELETE FROM etudiants ;`
- Supprime la table *etudiants*
 - Vide la table *etudiants* de ses enregistrements
 - Supprime les cinquante derniers enregistrements de la table *etudiants*
 - Supprime le dernier champ de la table *etudiants*
26. Quelle commande SQL permet de rendre effectives les dernières mises à jour des données ?
- COMMIT
 - ROLLBACK
 - UPDATE
 - INSERT

27. Laquelle de ces adresses IP est privée ?
- 132.25.210.11
 - 195.93.63.60
 - 172.16.100.2
 - 224.2.2.25
28. A quelle classe appartient l'adresse 138.12.25.101 ?
- Classe A
 - Classe B
 - Classe C
 - Classe D
29. Lequel de ces protocoles est un protocole de routage inter-domaine ?
- EIGRP
 - OSPF
 - ISIS
 - BGP
30. Quel protocole est utilisé pour le dialogue entre deux serveurs de messagerie ?
- SNTF
 - SNMP
 - NNTP
 - SMTP
31. Quelle application/protocole n'utilise pas des ports TCP ou UDP dont les numéros sont négociés dynamiquement lors de la session ?
- H.323
 - SQLnet
 - FTP
 - http
32. A quelle couche du modèle OSI correspondent les tâches principales d'un routeur ?
- Physique
 - Liaison
 - Réseau
 - Transport
33. Quel dispositif permet à un pare-feu de remplacer dans l'en-tête IP d'un paquet une adresse privée par une adresse publique ?
- FAT
 - NAT
 - VPN
 - SSL
34. Lequel de ces logiciels n'est pas un client de messagerie ?
- Thunderbird
 - Eudora
 - Outlook
 - Windows Media Player

35. Lequel de ces éditeurs ne produit pas de logiciel antivirus ?
- Symantec
 - MacAfee
 - Autodesk
 - Trend Micro
36. Qu'est-ce que le format ODT ?
- Un protocole réseau
 - Une norme de schéma d'annuaire
 - Un protocole de routage en téléphonie
 - Un format ouvert de données pour traitement de texte
37. Lequel de ces logiciels désigne un traitement de texte ?
- Open Office Writer
 - Adobe Acrobat Reader
 - Quark Xpress
 - Quicktime
38. A quel organisme doit-on déclarer des fichiers informatiques comportant des informations nominatives ?
- La Préfecture de département
 - Le CSA
 - L'ARCEP (ex ART)
 - La CNIL
39. Pendant combien de temps, un fournisseur d'accès à Internet, doit-il conserver les données techniques de connexion en vue d'une réquisition judiciaire ?
- Quinze jours
 - Deux mois
 - Un an
 - Cinq ans
40. Quel organisme est chargé d'alerter et de sensibiliser les responsables de la sécurité des systèmes d'information sur les problèmes actuels de sécurité sur Internet ?
- RIPE
 - CERT
 - IETF
 - AFNIC

3. Analyse algorithmique (explication de script).

Dans le cadre prévu à cet effet, expliquez en quelques lignes ce que font les deux scripts ci-dessous. Les deux scripts effectuent les mêmes tâches. Le premier est un script DOS, le second un script BASH. Vous êtes donc libre de choisir l'un des deux pour répondre en fonction de votre pratique.

```
echo off
echo Bonjour %USERNAME%
cd /d %USERPROFILE%
dir c:\serveur\devoir\*.txt 1>resdir 2>resdirerr
if %ERRORLEVEL% EQU 0 (GOTO DevoirAFaire) ELSE (GOTO PasDeDevoir)
:DevoirAFaire
echo Les enonces des devoirs a rendre se trouvent
echo dans le fichier ListeDevoir.txt du sous repertoire
echo devoir de votre repertoire personnel
cd devoir
if %ERRORLEVEL% EQU 0 GOTO Endif ELSE GOTO CreerDevoir
:CreerDevoir
mkdir devoir
cd devoir
:Endif
echo "Liste des devoirs a rendre" > ListeDevoir.txt
FOR %%f in (c:\serveur\devoir\*.txt) do type %%f >> ListeDevoir.txt
cd ..
goto end
:PasDeDevoir
echo Vous n'avez pas de devoir a rendre
:end
del resdir
del resdirerr
```


Annexe 1. Manuel de l'utilitaire ldapsearch.

LDAPSEARCH(1)

NAME

ldapsearch - LDAP search tool

SYNOPSIS

```
ldapsearch [-n] [-u] [-v] [-t{t}] [-T path] [-F prefix] [-A] [-L[L[L]]] [-M[M]] [-S attribute] [-d debuglevel] [-f file] [-x] [-D binddn] [-W] [-w passwd] [-y passwdfile] [-H ldapuri] [-h ldaphost] [-p ldapport] [-b searchbase] [-s base|one|sub|children] [-a never|always|search|find] [-P 2|3] [-c [!]ext[=extparam]] [-E [!]ext[=extparam]] [-l timelimit] [-z sizelimit] [-O security-properties] [-I] [-Q] [-U authcid] [-R realm] [-X authzid] [-Y mech] [-Z[Z]] filter [attrs...]
```

DESCRIPTION

ldapsearch is a shell-accessible interface to the ldap_search_ext(3) library call.

ldapsearch opens a connection to an LDAP server, binds, and performs asearch using specified parameters. **The filter should conform to the string representation for search filters as defined in RFC 4515.** If not provided, the default filter, (objectClass=*), is used.

If ldapsearch finds one or more entries, the attributes specified by attrs are returned. If * is listed, all user attributes are returned.

If + is listed, all operational attributes are returned. If no attrs are listed, all user attributes are returned. If only 1.1 is listed, no attributes will be returned.

OPTIONS

-n Show what would be done, but don't actually perform the search. Useful for debugging in conjunction with -v.

-u Include the User Friendly Name form of the Distinguished Name DN) in the output.

-v Run in verbose mode, with many diagnostics written to standard output.

-t{t} A single -t writes retrieved non-printable values to a set of temporary files. This is useful for dealing with values containing non-character data such as jpeg Photo or audio. A second -t writes all retrieved values to files.

-T path Write temporary files to directory specified by path (default: /var/tmp/)

-F prefix URL prefix for temporary files. Default is file://path/ where path is /var/tmp/ or specified with -T.

-A Retrieve attributes only (no values). This is useful when you just want to see if an attribute is present in an entry and are not interested in the specific values.

-L Search results are display in LDAP Data Interchange Format detailed in ldif(5). A single -L restricts the output to LDIFv1. A second -L disables comments. A third -L disables printing of the LDIF version. The default is to use an extended version of LDIF.

-M[M] Enable manage DSA IT control. -MM makes control critical.

-S attribute Sort the entries returned based on attribute. The default is not to sort entries returned. If attribute is a zero-length string (""), the entries are sorted by the components of their Distinguished Name. See ldap_sort(3) for more details. Note that ldapsearch normally prints out entries as it receives them. The use of the -S option defeats this behavior, causing all entries to be retrieved, then sorted, then printed.

-d debuglevel Set the LDAP debugging level to debuglevel. ldapsearch must be compiled with LDAP_DEBUG defined for this option to have any effect.

-f file Read a series of lines from file, performing one LDAP search for each line. In this case, the filter given on the command line is treated as a pattern where the first and only occurrence of %s is replaced with a line from file. Any other occurrence of the the % character in the pattern will be regarded as an error. Where it is desired that the search filter include a % character, the character should be encoded as \% (see RFC 4515). If file is a single - character, then the lines are read from standard input.

-x Usesimple authentication instead of SASL.

-D binddn Use the Distinguished Name binddn to bind to the LDAP directory.

-W Prompt for simple authentication. This is used instead of specifying the password on the command line.

-w passwd Use passwd as the password for simple authentication.

-y passwdfile Use complete contents of passwdfile as the password for simple authentication.

-H ldapuri Specify URI(s) referring to the ldap server(s); only the protocol/host/port fields are allowed; a list of URI, separated by whitespace or commas is expected.

-h ldaphost Specify an alternate host on which the ldap server is running. Deprecate in favor of -H.

-p ldappport Specify an alternate TCP port where the ldap server is listening. Deprecated in favor of **-H**.

-b searchbase Use searchbase as the starting point for the search instead of the default.

-s base|one|sub|children Specify the scope of the search to be one of base, one, sub, or children to specify a base object, one-level, subtree, or children search. The default is sub. Note: children scope requires LDAPv3 subordinate feature extension.

-a never|always|search|find Specify how aliases dereferencing is done. Should be one of never, always, search, or find to specify that aliases are never dereferenced, always dereferenced, dereferenced when searching, or dereferenced only when locating the base object for the search. The default is to never dereference aliases.

-P 2|3 Specify the LDAP protocol version to use.

-l timelimit wait at most timelimit seconds for a search to complete. A timelimit of 0 (zero) or none means no limit. A timelimit of max means the maximum integer allowable by the protocol. A server may impose a maximal timelimit which only the root user may override.

-z sizelimit retrieve at most sizelimit entries for a search. A sizelimit of 0 (zero) or none means no limit. A sizelimit of max means the maximum integer allowable by the protocol. A server may impose a maximal sizelimit which only the root user may override.

-O security-properties Specify SASL security properties.

-I Enable SASL Interactive mode. Always prompt. Default is to prompt only as needed.

-Q Enable SASL Quiet mode. Never prompt.

-U authcid Specify the authentication ID for SASL bind. The form of the ID depends on the actual SASL mechanism used.

-R realm Specify the realm of authentication ID for SASL bind. The form of the realm depends on the actual SASL mechanism used.

OUTPUT FORMAT

If one or more entries are found, each entry is written to standard output in LDAP Data Interchange Format or ldif(5):

```
version: 1
# bjensen, example, net
dn: uid=bjensen,dc=example,dc=net
objectClass: person
objectClass: dcObject
```

```
uid: bjensen
cn: Barbara Jensen
sn: Jensen
...
```

If the `-t` option is used, the URI of a temporary file is used in place of the actual value. If the `-A` option is given, only the "attributename" part is written.

EXAMPLE

The following command:

```
ldapsearch -LLL "(sn=smith)" cn sn telephoneNumber
```

will perform a subtree search (using the default search base and other parameters defined in `ldap.conf(5)`) for entries with a surname (`sn`) of `smith`. The common name (`cn`), surname (`sn`) and `telephoneNumber` values will be retrieved and printed to standard output. The output might look something like this if two entries are found:

```
dn: uid=jts,dc=example,dc=com
cn: John Smith
cn: John T. Smith
sn: Smith
sn;lang-en: Smith
sn;lang-de: Schmidt
telephoneNumber: 1 555 123-4567

dn: uid=sss,dc=example,dc=com
cn: Steve Smith
cn: Steve S. Smith
sn: Smith
sn;lang-en: Smith
sn;lang-de: Schmidt
telephoneNumber: 1 555 765-4321
```

The command:

```
ldapsearch -LLL -u -t "(uid=xyz)" jpegPhoto audio
```

will perform a subtree search using the default search base for entries with user id of "xyz". The user friendly form of the entry's DN will be output after the line that contains the DN itself, and the jpeg Photo and audio values will be retrieved and written to temporary files. The output might look like this if one entry with one value for each of the requested attributes is found:

```
dn: uid=xyz,dc=example,dc=com
ufn: xyz, example, com
audio:< file:///tmp/ldapsearch-audio-a19924
jpegPhoto:< file:///tmp/ldapsearch-jpegPhoto-a19924
```

This command:

```
ldapsearch -LLL -s one -b "c=US" "(o=University*)" o description
```

will perform a one-level search at the c=US level for all entries whose organization name (o) begins begins with University. The organization name and description attribute values will be retrieved and printed to standard output, resulting in output similar to this:

```
dn: o=University of Alaska Fairbanks,c=US
o: University of Alaska Fairbanks
description: Preparing Alaska for a brave new yesterday
description: leaf node only
```

```
dn: o=University of Colorado at Boulder,c=US
o: University of Colorado at Boulder
description: No personnel information
description: Institution of education and research
```

```
dn: o=University of Colorado at Denver,c=US
o: University of Colorado at Denver
o: UCD
o: CU/Denver
o: CU-Denver
description: Institute for Higher Learning and Research
```

```
dn: o=University of Florida,c=US
o: University of Florida
o: UF1
description: Warper of young minds
...
```

DIAGNOSTICS

Exit status is zero if no errors occur. Errors result in a non-zero exit status and a diagnostic message being written to standard error.

SEE ALSO

ldapadd(1), ldapdelete(1), ldapmodify(1), ldapmodrdn(1),
ldap.conf(5), ldif(5), ldap(3), ldap_search_ext(3), ldap_sort(3)

AUTHOR

The OpenLDAP Project <<http://www.openldap.org/>>

ACKNOWLEDGEMENTS

OpenLDAP is developed and maintained by The OpenLDAP Project (<http://www.openldap.org/>). OpenLDAP is derived from University of Michigan LDAP 3.3 Release.

OpenLDAP 2.3.30
LDAPSEARCH(1)

2006/11/14

Annexe 2. Extrait du RFC 4515: Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters

3. String Search Filter Definition

The string representation of an LDAP search filter is a string of UTF-8 [RFC3629] encoded Unicode characters [Unicode] that is defined by the following grammar, following the ABNF notation defined in [RFC4234]. The productions used that are not defined here are defined in Section 1.4 (Common ABNF Productions) of [RFC4512] unless otherwise noted. The filter format uses a prefix notation.

```
filter           = LPAREN filtercomp RPAREN
filtercomp      = and / or / not / item
and             = AMPERSAND filterlist
or             = VERTBAR filterlist
not            = EXCLAMATION filter
filterlist     = 1*filter
item           = simple / present / substring / extensible
simple          = attr filtertype assertionvalue
filtertype     = equal / approx / greaterorequal / lessorequal
```

RFC 4515 LDAP: String Representation of Search Filters June 2006

```
equal           = EQUALS
approx          = TILDE EQUALS
greaterorequal = RANGLE EQUALS
lessorequal    = LANGLE EQUALS
extensible     = ( attr [dnattrs]
                  [matchingrule] COLON EQUALS assertionvalue )
                  / ( [dnattrs]
                  matchingrule COLON EQUALS assertionvalue )

present        = attr EQUALS ASTERISK
substring     = attr EQUALS [initial] any [final]
initial       = assertionvalue
any           = ASTERISK *(assertionvalue ASTERISK)
final        = assertionvalue
attr         = attributedescription
               ; The attributedescription rule is defined in
               ; Section 2.5 of [RFC4512].

dnattrs       = COLON "dn"
matchingrule  = COLON oid
assertionvalue = valueencoding
               ; The <valueencoding> rule is used to encode an <AssertionValue>
               ; from Section 4.1.6 of [RFC4511].
valueencoding = 0*(normal / escaped)
normal       = UTF1SUBSET / UTFMB
escaped      = ESC HEX HEX
UTF1SUBSET   = %x01-27 / %x2B-5B / %x5D-7F
               ; UTF1SUBSET excludes 0x00 (NUL), LPAREN,
               ; RPAREN, ASTERISK, and ESC.

EXCLAMATION   = %x21 ; exclamation mark ("!")
AMPERSAND     = %x26 ; ampersand (or AND symbol) ("&")
ASTERISK     = %x2A ; asterisk ("*")
COLON        = %x3A ; colon (":")
VERTBAR      = %x7C ; vertical bar (or pipe) ("|")
TILDE       = %x7E ; tilde ("-")
```