EPREUVE DE TECHNOLOGIE E2

ANNEXES

Documents réponses :

ANNEXE 1 : Interlan FT

Inter LAN 2.0

1. **Une interconnexion de réseaux locaux à hauts débits**
2. **Un service sûr, disponible et garanti**
3. **Un service disponible sur les grandes agglomérations du territoire national**

Caractéristiques

Inter LAN 2.0 est un service de liaisons de 2 à 100 Mbit/s sous interfaces Ethernet, Fast Ethernet et ATM (G703 en option). L'offre est basée sur le réseau ATM de France Télécom et propose différents niveaux de service.

Les principales caractéristiques techniques d'Inter LAN sont :

- **Interconnexion à haut débit de 2 à plusieurs sites distants**

Inter LAN 2.0 permet de relier à haut débit de 2 à plusieurs sites distants situés dans la même agglomération. Les liaisons sont établies via le réseau sécurisé ATM de France Télécom.

- **Interfaces**

Inter LAN 2.0 est disponible sous interfaces **Ethernet, Fast Ethernet et ATM UNI 3.1.**

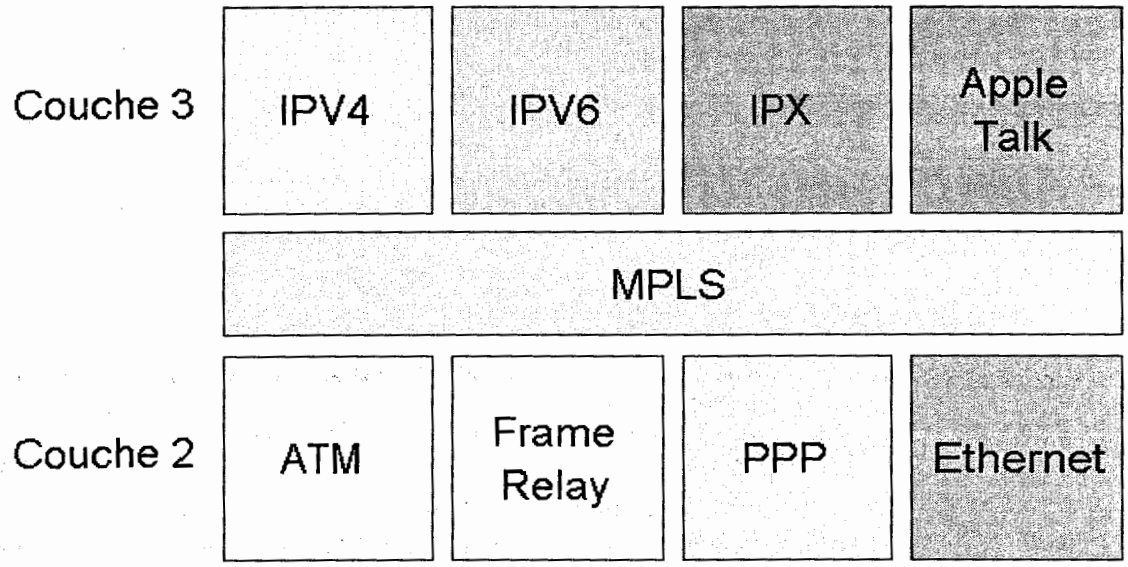
Les réseaux locaux connectés peuvent être **homogènes** (ex : Ethernet/Ethernet) ou **hétérogènes** (ex : Ethernet/Fast Ethernet). Inter LAN 2.0 est disponible en architectures **point à point et point à multipoint**. Pour les configurations point à multipoint, l'interface est habituellement mutualisée sur le site central. Si le client le souhaite, il est possible de livrer les liaisons arrivant sur le site central sur des interfaces distinctes (mais sur un même équipement d'accès) sans surcoût. Des **liaisons voix 2 Mbit/s** sont disponibles en option (interface G703).

- **Disponibilité et supervision du service**

Les liaisons bénéficient en standard d'une supervision pro-active 24h/24, 7j/7. Le service garantit une disponibilité sur l'année supérieur à 99 % et un rétablissement de la ligne dans les 4 heures suivant la défaillance en heures ouvrables. Cette garantie peut être étendue en option.

ANNEXE 2 : IP- MPLS

IP-MPLS : Le protocole MPLS ou "Multiprotocol Label Switching", est une technologie de transmission de données par paquet qui permet d'optimiser le routage des paquets
MPLS utilise un mécanisme de routage qui lui est propre, basé sur l'attribution d'un " label " à chaque paquet. Cela lui permet de router les paquets en optimisant les passages de la couche 2 à la couche 3 du modèle OSI et d'être indépendant du codage de celles-ci suivant les différentes technologies (ATM, Frame Relay, Ethernet etc...)
Le but est d'associer la puissance de la commutation de la couche 2 avec la flexibilité du routage de la couche 3. Schématiquement, on peut le représenter comme étant situé entre la couche 2 (liaison) et la couche 3 (réseau).



L'IP-MPLS permet d'apporter la vitesse de commutation de la couche 2 à la couche 3. L'utilisation de " label " permet de prendre des décisions de routage seulement basées sur la valeur du " label " et de ne pas effectuer des calculs complexes de routage portant sur l'adresse IP au niveau de la couche 3 du réseau. Cet aspect performant du protocole est aujourd'hui moins important du fait de l'apparition de composants hardware tels les commutateurs " switchs " de niveau 3.

-Le Principe :-1. Un routeur d'accès reçoit un paquet de données IP d'un autre réseau. Le routeur crée alors un court label, d'une largeur de 16 bits seulement, autour du paquet de données IP. Le chemin que suivra le paquet de données IP est prédéfini dans le label.

-2. Le routeur d'accès envoie le paquet de données IP à sa destination en utilisant le chemin prédéfini. Tous les routeurs rencontrés au cours de l'acheminement se contenteront de lire le label enveloppant le paquet de données IP et le feront suivre jusqu'au routeur suivant, ce qui accélère l'acheminement de chaque paquet de données IP.

-3. Lorsque le paquet de données IP arrive à destination, le routeur supprime le label et le transfère au réseau suivant

ANNEXE 3 : les technologies xDSL

Les technologies **xDSL** (*Digital Suscriber Line*) permettent la transmission à haut débit sur une ou plusieurs paires de cuivre en utilisant des signaux de très hautes fréquences. La condition est que la longueur des paires ne doit pas excéder une certaine limite, en raison de l'atténuation du signal.
On peut ainsi interconnecter à peu de frais et à haute vitesse plusieurs sites, pourvu qu'ils soient assez proches les uns des autres, ou assez proche du site d'un opérateur de télécommunications.
Grâce au **xDSL**, il est possible de bénéficier d'accès très rapide à *Internet*, et accéder à l'audio et à la vidéo en temps réel.

COMPARAISON DES TECHNOLOGIES XDSL

Technologie	Signification	Mode de transmission	Débit descendant	Débit remontant	Limite de distance à débit maximum
ADSL	Asymetric DSL	Asymétrique (DMT)	8 Mbit/s	640 kbit/s	2700 m
HDSL	High bit rate DSL	Symétrique (2B1Q/CAP)	2 Mbit/s	2 Mbit/s	3600 m
IDSL	ISDN over DSL	Symétrique (2B1Q)	144 kbit/s	144 kbit/s	5500 m
SDSL	Single-line DSL	Symétrique (2B1Q)	2 Mbit/s	2 Mbit/s	1500 m
VDSL	Very-High-Rate DSL	Asymétrique (CAP/DMT)	53 Mbit/s	2,3 Mbit/s	300 m

Les limites de distance peuvent varier suivant le diamètre des paires de cuivre utilisées. Il est également possible d'augmenter la distance de transmission au détriment de la vitesse car les plus hautes fréquences sont atténuées rapidement lorsque la longueur du support augmente. On peut ainsi transmettre en ADSL jusqu'à 5400 m, mais à 1544 kbit/s seulement en débit descendant.

ADSL - UN ACCES RAPIDE POUR TOUS OU PRESQUE

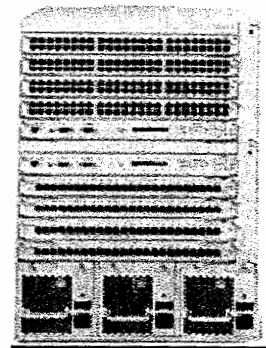
France Télécom a choisi de déployer en masse la technologie **ADSL** au travers de son offre **Netissimo**. En effet, cette technologie requiert peu d'équipements du côté abonné, privilégie l'accès descendant par rapport à l'accès remontant sur les distances moyennes, et les fréquences de l'**ADSL** sont distinctes des fréquences vocales. Au moyen d'un filtre, il est donc possible d'utiliser directement les lignes téléphoniques existantes pour l'accès haut débit à Internet. Vous pouvez donc surfer sur Internet sans que le fonctionnement de votre ligne téléphonique soit perturbé, ce qui signifie que vous continuez à recevoir vos fax et appels vocaux simultanément. Par ailleurs, votre accès à Internet ne passant plus par le réseau téléphonique commuté (**RTC**), vous ne payez qu'un forfait mensuel comprenant le modem **ADSL**.
Un accès de très haute qualité à prix avantageux
Les technologies **HDSL** et **SDSL** répondent aux exigences spécifiques d'un accès Internet professionnel. Le débit est symétrique (*full-duplex*) ce qui permet de transmettre dans les deux sens simultanément, sans dégradation des performances. Exploitées en *ATM* avec des équipements spécifiques, ces liaisons permettent entre autres de gérer plusieurs réseaux privés virtuels (*VPN*) sur le même lien physique, avec une garantie totale d'étanchéité des flux et de qualité de service.
Utilisant une infrastructure meilleur marché au niveau opérateur que les liaisons louées classiques, il est ainsi possible à une entreprise, grâce au liaisons **HDSL** et **SDSL**, de fournir des services Internet de haute qualité à prix très avantageux.

ANNEXE 4 : Passport 8600

Passport 8600 Ethernet Routing Switch for Enterprise

Converged applications which increase employee productivity and your bottom line require a resilient, secure, and intelligent network. The Passport 8600 Routing Switch combines high performance with reliability, intelligence and security. A chassis-based Ethernet switch, the Passport 8600 Routing Switch supports from 8 to 128 Gigabit Ethernet ports as well as connectivity for 10 Gigabit Ethernet, ATM, PoS, and Wave Division Multiplexing technologies.

- **View Chassis Images**
- **Request a Quote for this Product**



Product Resources

Request a Quote
- Product Literature
- Technical Documentation
- Downloads
- Training
- How to Buy

Key Features: This high-availability, high-performance Ethernet connectivity solution for enterprises offers:

- Classifies and filters traffic at wire speed with no impact on network performance for maximum scalability
- Highly redundant, low latency network solution designed for delay and jitter-sensitive applications
- Reliable, secure, and intelligent network capable of supporting unified communication applications which can increase revenues and employee productivity
- Flexibility in connectivity for the network core with support for 10/100 and 1000 Ethernet fiber and copper and fiber Ethernet, ATM, PoS provides smooth network technology transitions

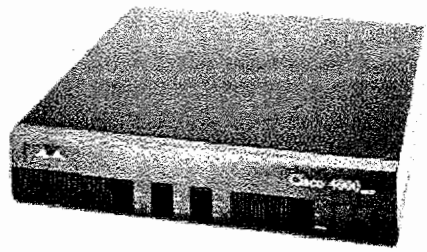
ANNEXE 5: CISCO série 4000

CISCO 4000 SERIES ROUTERS MID-RANGE ROUTING FOR REGIONAL OFFICE ETHERNET LAN AND TOKEN RING LAN CONNECTIVITY

The Cisco 4000 series routers are highly cost-effective, modular platforms that reduce network costs and complexity by aggregating multiple LANs into a single multiprotocol network. Cisco 4000 series routers offer increased security through packet filtering between LANs and provide the bandwidth reservation features and performance required for advanced applications such as LAN-to-Asynchronous Transfer Mode (ATM) access, IBM data-link switching (DLSw), Advanced Peer-to-Peer Networking (APPN), and videoconferencing.

This series of routers provides regional offices with a broad range of capabilities and features across its two models: Cisco 4500-M and Cisco 4700-M. Each model offers Flash memory that stores the powerful Cisco Internetwork Operating System (Cisco IOS®) software and slots for optional network processor modules (NPMs)—individual removable cards used for external network connections including Ethernet, Token Ring, Fast Ethernet, ATM, Fiber Distributed Data Interface (FDDI), High-Speed Serial Interface (HSSI), Integrated Services Digital Network (ISDN), Basic Rate Interface (BRI) and Primary Rate Interface (PRI), E1/T1 serial, and high-density, low-speed serial.

The Cisco 4500-M is a midrange router with a 100-MHz reduced instruction set (RISC) CPU for supporting high-density/low-speed or mid-density/high-speed LAN and WAN connectivity. The top-of-the-line Cisco 4700-M router, with its 133-MHz RISC CPU, delivers 30-50 percent more processing performance than the Cisco 4500-M. In addition to providing better support of high-speed media than the 4500-M, it has the reserve to excel in compute intensive tasks such as data compression, data encryption, tunneling, policy/security, protocol conversion applications, and IBM protocols.



These midrange routers are ideal for several regional office environments. For example, many multi-regional offices have a mixture of legacy and LAN traffic and want to connect to servers or mainframe hosts at larger sites. The Cisco 4500-M can convert legacy protocols to IP protocols, prioritize traffic, and provide ISDN BRI connectivity. These offices often act as central repositories for data and applications accessed by smaller remote sites and mobile users, and the Cisco 4500-M router gives them the multiple WAN ports necessary for this aggregation. Regional offices with multiple backbone networks such as FDDI and ATM often need to link them with a router for increased security and control, or they need to translate traffic between dissimilar LANs such as Token Ring and Ethernet. The Cisco 4700-M router gives them high performance for these processor-intensive applications with a processing power reserve for the future.

ANNEXE 6 : Principe du Netasq

Destinés à sécuriser des structures de toutes tailles, les Firewalls de la gamme Netasq sont des boîtiers pré-configurés : pas d'installation matérielle, ni d'installation logicielle, pas de compétences Unix nécessaires mais une configuration conviviale au moyen d'une interface graphique. Le Firewall Netasq permet de définir les règles de contrôle d'accès entrant ou sortant. **Son concept est simple : toute transmission entrante ou sortante transitant par le Firewall Netasq est contrôlée, autorisée ou refusée suivant les règles, paquet par paquet.**

Le Firewall Netasq est basé sur un mécanisme de filtrage de paquets évolué qui procure un haut niveau de sécurité. Tous les firewalls Netasq intégrent la technologie ASQ (Active security Qualification), développée par Netasq. Cette technologie permet la détection et le blocage, en temps réel, d'attaques informatiques : paquets illégaux, tentatives de deny de service, anomalies dans une connexion, scans de ports...

En cas de tentative d'intrusion, selon les consignes, le Firewall Netasq bloque la transmission, génère une alarme et mémorise les informations liées au paquet ayant provoqué l'alarme. Ainsi, il vous est possible d'analyser l'attaque et de rechercher son origine.

Le Firewall permet non seulement d'empêcher, ou de limiter à certains services, les connexions entrantes sur votre réseau mais aussi de contrôler l'utilisation de l'Internet faite par vos utilisateurs internes (HTTP, FTP, SMTP ...)

Le Firewall Netasq gère également les mécanismes de translations d'adresses et de ports. Ces mécanismes apportent sécurité (en masquant votre adressage interne), flexibilité (en permettant d'utiliser un plan d'adressage interne privé quelconque) et réduction de coût (en permettant la mise à disposition de plusieurs serveurs sur Internet avec une seule adresse IP publique).

Grâce à son interface utilisateur sous Windows, il offre la possibilité de définir rapidement et simplement les règles de sécurité pour votre réseau, à partir d'un poste local sous Windows . Vous pouvez aussi monitorer, en temps réel, l'activité de votre firewall.

Le Firewall Netasq est également doté de fonctions avancées de traçabilité. En cas de tentative d'intrusion, l'administrateur de réseau peut accéder à l'ensemble des données envoyées avant l'attaque et voir comment elle est préparée. Le Netasq REPORTER vous apportera une vision graphique et une analyse fine des logs générés sur le firewall.

Enfin, le Firewall NETASQ intègre les fonctionnalités de passerelle VPN vous permettant d'établir des tunnels chiffrés avec d'autres équipements VPN. Ainsi, vos communications inter-sites ou avec vos utilisateurs nomades ("Road Warriors") peuvent être sécurisées même en utilisant une infrastructure de communication non sûre comme l'est Internet.

Firewalls NETASQ

ASQ : Active Security Qualification

White Paper résumé

ASQ (résumé)

Real Time Intrusion Prevention (IPS) Technology

L'ASQ, moteur de détection et de prévention d'intrusion, est intégré dans toute la gamme des boîtiers firewalls NetASQ. Anticipant dès sa création l'évolution des technologies de sécurité Internet, les laboratoires de Recherche et Développement de NetASQ ont mis au point l'ASQ dès 1998. Ce moteur intelligent intègre un système de prévention d'intrusion (IPS : Intrusion Prevention System) qui détecte et élimine tout comportement malicieux en temps réel.

De nos jours, les contre-mesures sont très compliquées à mettre en place et très ciblées vis-à vis de type d'attaques visant le déni de service. En effet, d'un point de vue théorique, la plupart des attaques visant à créer des dénis de service sont basées sur des services ou protocoles standard sur Internet. S'en protéger reviendrait à couper les voies de communications normales avec Internet, alors que c'est bien là la raison principale des machines concernées (serveurs web, de messagerie, etc...)

Il reste tout de même la possibilité de se protéger mais cela implique beaucoup de démarches :

il faut monitorer le trafic (ce qui est loin d'être simple, du fait de la quantité de données qui transitent), établir des profils types de comportement et des écarts tolérables au-delà desquels on considérera que l'on fait l'objet d'une attaque; il faut également définir les types d'attaques contre lesquelles on souhaite se protéger (analyses de risques à l'appui) car il est impossible de toutes les prévoir. On est donc loin de la protection absolue; il s'agit de mettre en place une protection intelligente et flexible.

L'ASQ répond à ces contraintes et, grâce à son analyse du trafic, prévient les grandes familles d'attaques en temps réél.

La Solution NetASQ : une gamme complètement "Real Time Intrusion Prevention"

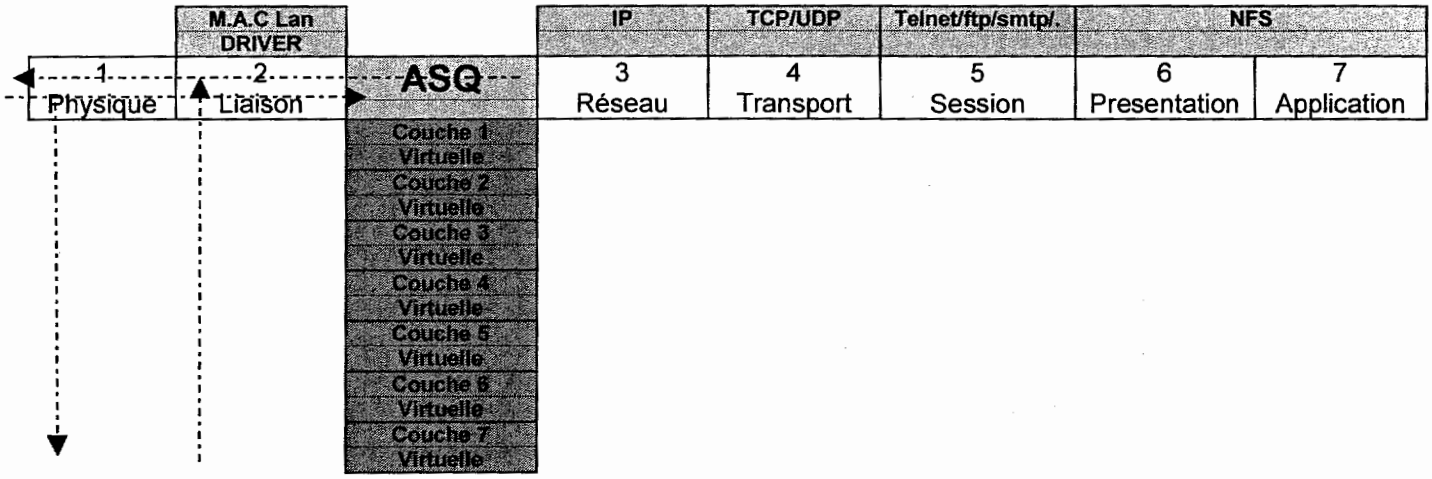
L'originalité de NetASQ est d'avoir intégré la technologie ASQ sur toute sa gamme. Ceci fait de chaque firewall NetASQ un outil puissant dans votre réseau capable de vous protéger contre les intrusions sans avoir à rajouter encore un autre élément. L'administration de votre politique de sécurité s'en trouve grandement simplifiée et donc plus performante.

L'intérêt d'avoir intégré cette technologie directement dans le firewall, est que celui ci se place en coupure sur le trajet des paquets. Contrairement à un IDS, qui se contente d'émettre des alarmes et d'envoyer des commandes RESET toujours trop tard (l'attaque est déjà passée). Le Firewall NetASQ coupe la connexion avant la transmission des derniers paquets. De ce fait l'attaque ne peut s'exécuter.

ASQ : Virtual OSI up to Layer 7

L'ASQ n'effectue aucune désencapsulation à proprement parlé. En effet on ne remonte pas la pile IP. Donc l'ASQ réalise ses analyses sur un paquet mis en tampon. Ceci signifie que toutes les fonctions de sécurité sont réalisées au niveau du noyau sans ajout de couche supplémentaire. Les performances sont grandement améliorées.

Une fois que toutes les analyses sont réalisées, le paquet est transmis à l'interface sortante. Le contexte de ce paquet est gardé en mémoire pour le paquet suivant. Lors du traitement du prochain paquet, l'ASQ réalisera une analyse du contexte, en plus de l'analyse du format du paquet en lui-même. Tout paquet mal formé est détruit, tout paquet participant à un contexte malicieux est détruit.



ANNEXE 7 : principe d'ASQ de netasq 2/2

ASQ : de multiples analyses pour une sécurité à toutes épreuves

Analyse IP
Analyse des fragments
Analyse globale
Filtrage
Analyse des protocoles applicatifs

Analyse IP
Le principe de cette analyse consiste à vérifier la conformité du format des paquets et datagrammes en fonction des RFC. Cette analyse permet de vérifier l'utilisation correcte et non frauduleuse des protocoles des couches 3 et 4 du modèle OSI (réseau et transport).
Les failles de sécurité de ces protocoles proviennent pour la plupart de l'implémentation de la pile TCP/IP. Les comportements que l'on analyse à ce niveau [Analyse IP] sont souvent liés à l'utilisation d'options peu ou rarement utilisées dans les communications Internet. Ces paquets « mal formés » provoquent des bugs et parfois le crash du système (Deny of Service).

Analyse des fragments
Le deuxième type de failles qui peut être exploité est le séquencement des fragments.
L'analyse n'est plus effectuée au niveau du paquet en lui-même mais à un niveau d'abstraction supérieur, le datagramme. On analyse désormais le fragment dans son environnement. C'est-àdire la cohérence qu'il y a entre celui-ci et ceux qui suivent, ou qui précèdent.
On cherche dans cette analyse à vérifier qu'en assemblant les fragments on obtient effectivement un paquet valide. C'est à dire qu'aucun fragment ne se chevauche (recouvrement de fragment), que le paquet soit entier et ne comporte pas d'ajout effectué frauduleusement (débordement sur un fragment, trou entre fragments).

Analyse globale Cette analyse se place à un degré d'abstraction supérieur à l'analyse des fragments mais cette fois-ci on s'intéresse au contexte des connexions. La technologie « Stateful Inspection » basée sur la mémorisation du contexte utilisateur permet une vérification du contenu des paquets transitant par le firewall.

Filtrage (ASQ Dynamic Filtering)
Le firewall NetASQ est de type « Stateful Inspection ». Cette technologie permet la conservation des contextes de connexions. L'intérêt est de pouvoir vérifier le trafic non plus au niveau paquet mais au niveau connexion. Ainsi une attaque se basant sur des paquets sains mais qui, réunis, se révèlent dangereux, sera détectée par un tel firewall. De plus cette technologie analyse le contenu des paquets à la volée et sans interruption de liaison ce qui lui assure de meilleures performances.
Pour optimiser le filtrage mis en place dans le cadre d'une politique de sécurité, NetASQ a développé un **algorithme nommé SKIP**. Lors de l'analyse des règles, celui-ci regroupe celles qui se suivent et qui ont un critère commun (à partir de trois règles). Le but est de sauter l'évaluation de plusieurs règles qui contiennent un critère éliminatoire. Etant donné le critère éliminatoire, l'évaluation de ces règles serait inutile (elle remontera forcément une réponse négative).

Exemple : principe de fonctionnement de SKIP

N°	Action	Protocole	Interface	Source	Destination	Port
...						
3	Autoriser	TCP	IN	Reseau_interne	Serveur_web	80
4	Bloquer	ICMP	OUT	Any	Reseau_interne	
5	Autoriser	TCP	OUT	Any	Serveur_web	80
6	Bloquer	TCP	OUT	Reseau_distant	Serveur_web	21
7	Autoriser	TCP	IN	Reseau_interne	Serveur_SMTP	25
...						

Par exemple : un paquet en provenance du réseau interne à destination de l'Internet testera la règle 3 et « sautera » directement à la règle 7.

ANNEXE 8 : liste des services du netasq 1/3

Dans cette annexe vous trouverez la liste de services TCP et UDP couramment utilisés tels que : FTP, Telnet, www, SMTP,...Cette annexe vous est présentée sous la forme d'une liste composée de quatre colonnes :

- Une colonne contenant le nom du service
- Une colonne contenant le numéro de port associé au service
- Une colonne indiquant le protocole utilisé (TCP et/ou UDP)
- Une colonne contenant une description du service

Cette grille vous permet de configurer les noms de services TCP et UDP utilisés dans vos fichiers de configuration de filtrage. Cette dénomination permet au Firewall Netasq de connaître la correspondance entre un nom de service, le protocole utilisé et le numéro de port TCP ou UDP associé.

Service	Port	Protocole	Description
echo	7	TCP / UDP	Echo
discard	9	TCP	Discard
systat	11	TCP / UDP	Systat
daytime	13	TCP / UDP	Daytime
qotd	17	TCP / UDP	Quote Of The Day
chargen	19	TCP / UDP	Character generator
ftp-data	20	TCP	File Transfer (Default Data)
ftp	21	TCP	File Transfer (Control)
telnet	23	TCP	Telnet
smtp	25	TCP	Simple Mail Transfer
time	37	TCP / UDP	
rlp	39	UDP	Resource Location Protocol
nameserver	42	TCP / UDP	Host Name Server
nicname	43	TCP	
Login	49	TCP / UDP	
domain	53	TCP / UDP	Domain Name Server (DNS)
sql-net	66	TCP / UDP	Oracle SQL Net
bootps	67	UDP	Bootstrap Protocol Server
bootpc	68	UDP	Bootstrap Protocol Client
tftp	69	TCP / UDP	Trivial File Transfert
gopher	70	TCP	Gopher
finger	79	TCP	Finger
www	80	TCP	World Wide Web

ANNEXE 8 : liste des services du netasq 2/3

Service	Port	Protocole	Description
kerberos	88	TCP / UDP	Kerberos
npp	92	TCP / UDP	Network Printing Protocol
hostname	101	TCP	NIC Host Name Server
iso-tsap	102	TCP	ISO-TSAP Class 0
rtelnet	107	TCP	Remote Telnet Service
pop2	109	TCP	Post Office Protocol version 2
pop3	110	TCP	Post Office Protocol version 3
sunrpc	111	TCP / UDP	Authentication Service
auth	113	TCP	SUN Remote Procedure Call
uucp-path	117	TCP	SQL Services
sqlserv	118	TCP / UDP	
nntp	119	TCP	Network News Transfer Protocol
ntp	123	UDP	Network Time Protocol
epmap	135	TCP / UDP	Netbios Net Service
netbios-ns	137	TCP / UDP	DCE endpoint resolution
netbios-dgm	138	UDP	Netbios Datagram Service
netbios-ssn	139	TCP	Netbios session service
imap2	143	TCP	Interim Mail Access Protocol version 2
sql-net	150	TCP / UDP	SQL-NET
snmp	161	UDP	Simple Network Management Protocol
snmptrap	162	UDP	SNMP trap
print-srv	170	TCP	
bgp	179	TCP	Border Gateway Protocol
irc	194	TCP	Internet Relay Chat Protocol
ipx	213	UDP	IPX over IP
imap3	220	TCP / UDP	Internet Message Access Protocol 3
ldap	389	TCP	Lightweight Directory Access Protocol

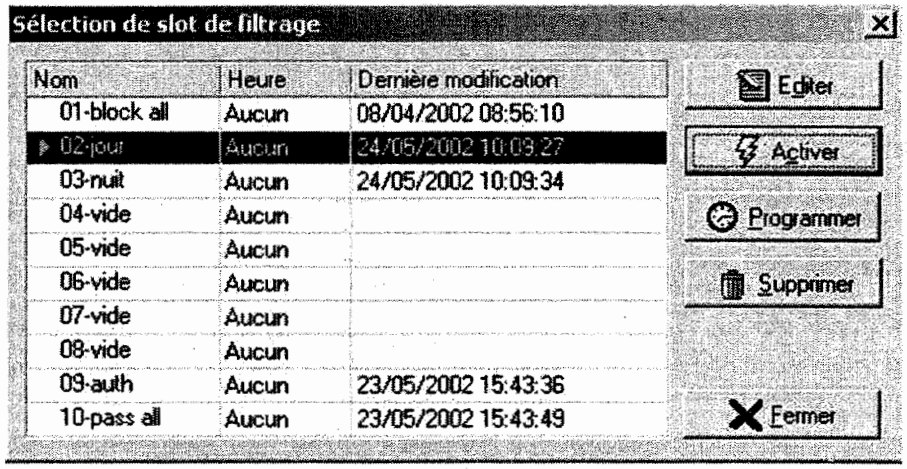
ANNEXE 8 : liste des services du netasq 3/3

Service	Port	Protocole	Description
netware-ip	396	TCP / UDP	Novell Netware over IP
ups	401	TCP / UDP	Uninterruptible Power Supply
smpte	420	TCP / UDP	SMPTE
https	443	TCP / UDP	Https Mcom
microsoft-ds	445	TCP / UDP	
kpasswd	464	TCP / UDP	Kerberos (v5)
isakmp	500	UDP	Internet Key Exchange
exec	512	TCP / UDP	Remote process execution
biff	512	TCP / UDP	Notify user of new mail received
login	513	TCP / UDP	Remote login
who	513	TCP / UDP	Who's logged in to machines
cmd	514	TCP / UDP	Remote exec
syslog	514	TCP / UDP	
printer	515	TCP	Spooler
talk	517	UDP	
ntalk	518	UDP	
router	520	TCP / UDP	Extended File Name Server
timed	525	UDP	Timeserver
tempo	526	TCP	
courier	530	TCP	
conference	531	TCP	
uucp	540	TCP	
klogin	543	TCP	Kerberos login
kshell	544	TCP	Kerberos remote shell
remotefs	556	TCP	Remote login using Kerberos
rmonitor	560	UDP	
rmonitor	561	UDP	
whoami	565	TCP / UDP	
ldaps	636	UDP	LDAP over TLS/SSL
kerberos-adm	749	TCP / UDP	Kerberos administration
kerberos-iv	750	UDP	Kerberos version IV

ANNEXE 9 : mise en œuvre des règles de filtrage 1/2

Les tables de filtrage sont stockées sur le Firewall NETASQ dans des slots (fichiers de configuration numérotés de 01 à 10).

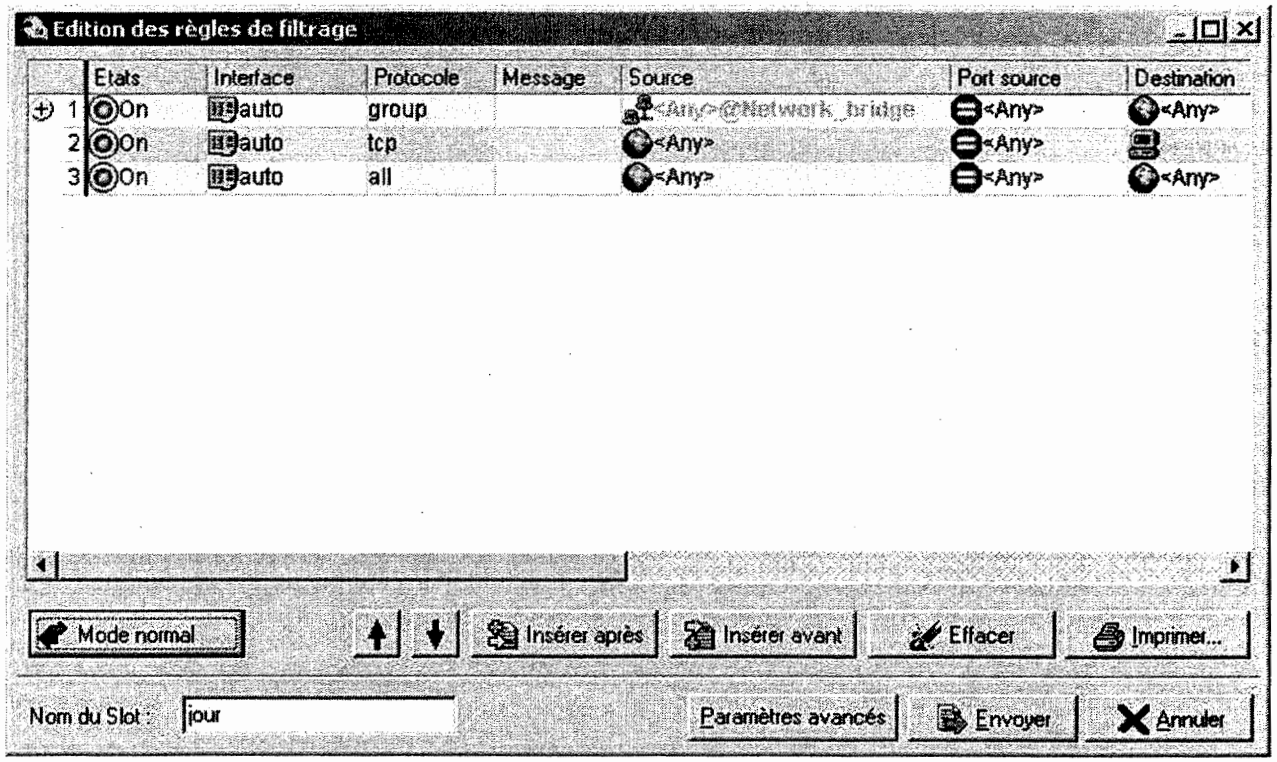
Chaque slot peut être programmé à une heure précise de la semaine, en écrasant la configuration du slot précédemment activé. A chaque slot est associé des règles de filtrage , qui doit être activé pour être appliqué .



Edition des règles de filtrage associées à un slot :

Mécanisme de filtrage:Le principe est simple : quand un paquet arrive au Firewall Netasq, celui-ci fait descendre le paquet dans la liste de règles de filtrage. Si le paquet correspond aux critères de sélection d'une règle, il applique l'action associée à cette règle sinon le paquet est automatiquement supprimé. Une fois qu'une règle peut être appliquée au paquet, ce dernier n'est plus comparé aux règles suivantes. **La façon dont vos règles de filtrage sont ordonnées est primordiale. La cohérence de cet ordre est la principale difficulté dans la configuration de votre Firewall.**

Cette grille vous permet de définir les règles de filtrage à appliquer. Faites attention à bien ordonner vos règles de filtrage afin d'avoir un résultat cohérent. Le Firewall exécute les règles dans l'ordre d'apparition à l'écran et s'arrête dès qu'une action s'applique au flux qui tente de le traverser. Il convient donc de définir les règles dans l'ordre du plus détaillé au plus général.



ANNEXE 9 : mise en œuvre des règles de filtrage 2/2

Interface :	La colonne interface permet de choisir l'interface sur laquelle doit s'appliquer la règle. Par défaut, le firewall la détecte automatiquement d'après l'adresse IP de la machine source (auto).
Message :	Vous pouvez choisir les messages ICMP que vous désirez filtrer. La liste des messages ICMP est présentée en annexe. Par défaut, lorsque vous sélectionnez le protocole ICMP, dans les règles de filtrage, seul le message "echo reply" (ping) est sélectionné.
Port Source:	La colonne Port source permet de préciser le port utilisé par la machine source, si c'est une valeur particulière. Par défaut, le module stateful mémorise le port source utilisé et seul celui-ci est autorisé pour les paquets retour.
Port Destination :	La colonne Port destination permet de préciser le port utilisé par la machine destination. Cela correspond au service que vous voulez autoriser ou interdire.

Etat :	Activation/désactivation d'une règle au sein d'un slot.
Protocole :	Protocole sur lequel s'applique la règle de filtrage.
Source :	Objet source utilisé comme critère de sélection pour cette règle. Un double clic sur cette zone permet de choisir la valeur associée.
Destination :	Objet destination utilisé comme critère de sélection pour cette règle. Un double clic sur cette zone permet de choisir la valeur associée.
Service :	Service ou groupe de service utilisé comme critère de sélection pour cette règle. Un double clic sur cette zone permet de choisir la valeur associée.
Action :	Action appliquée sur le paquet remplissant les critères de sélection de cette règle de filtrage.
Traces :	Type de trace générée
Commentaire :	Commentaires que vous voulez associer à cette règle.

Actions possibles :

Aucun :	Le Firewall Netasq n'effectue aucune action. Ceci est utile si vous voulez juste tracer certains flux sans appliquer d'action particulière.
Passer :	Le Firewall Netasq laisse passer le paquet correspondant à cette règle de filtrage. Le paquet ne descend plus dans la liste de règles.
Bloquer :	Le Firewall Netasq bloque silencieusement le paquet correspondant à cette règle de filtrage : le paquet est supprimé sans que l'émetteur ne le sache. Le paquet ne descend plus dans la liste des règles.
Réinitialiser :	Le Firewall Netasq bloque explicitement le paquet correspondant à cette règle de filtrage : une réponse TCP-IP est envoyée par le Firewall Netasq à l'émetteur du paquet. Le paquet ne descend plus dans la liste des règles.

Remarques : il existe des valeurs prédéfinies, par exemple :

- si interface = auto, le routeur recherche automatiquement d'après l'IP l'interface correspondant,
- si source/destination= any , signifie n'importe quelle adresse,
- source/destination peut être une adresse de machine ou une adresse de réseau,
- si port=any, signifie n'importe quel port,
- il existe aussi des ports préfinis :
  - mail incluant imap, pop3, smtp
  - web incluant domain_udp, http, https (domain_udp = dns)
  - full incluant domain_udp,http,https, imap,pop3,smtp,ftp,icq,telnet,...
- si protocole=all, n'importe quel protocole, sinon on précise TCP, UDP
- si protocole=group, on a utilisé un port prédéfini, par exemple web.

ANNEXE 10 : affectation des paires sur la RJ45

Applications	Nbre de paires	Affectation sur la RJ45
Téléphone analogique	1	4-5
Téléphone analogique+ extension	2	7-8 ;4-5
LS 2fils	2	7-8 ;3-6
Téléphone numérique	1	3-6
Accès Numéris S0	2	3-6 ;4-5
100 Base TX	2	1-2 ;3-6
ATM	2	1-2 ;7-8
Token ring	2	1-2 ;3-6
Vidéo analogique	4	1-2 ;3-6 ;4-5 ;7-8

ANNEXE 11 : câble rocade

Rocades non blindées

Les câbles multipaires de la gamme ACOME pour rocade se déclinent en versions 25 et 50 paires Cat 5 pour assurer l'interconnexion de sous-répartiteurs.

Caractéristiques :

- Impédance 100
- assemblage en paires
- Câbles UTP Cat5
- Conducteurs cuivre monobrin AWG 24
- Existent en 50 et 100 paires
- Gaine PVC (gris) ou LSOH (ivoire)

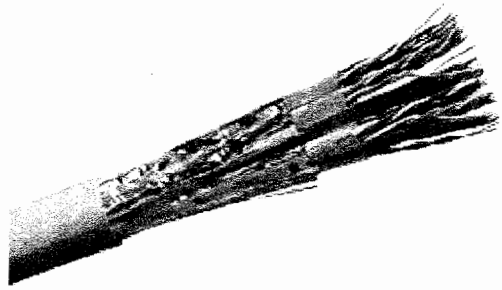
Référence	Désignation	Prix pour	Prix H.T. (€)
ACO M4662ST	Câble rocade 25 paires Cat 5 UTP LSOH	1000	**3 417,50**
ACO M3926ST	Câble rocade 25 paires Cat 5 UTP PVC	1000	**3 110,00**
ACO M4811AST	Câble rocade 50 paires Cat 5 UTP PVC	1000	**5 057,50**
ACO M4814AST	Câble rocade 50 paires Cat 5 UTP LSOH	1000	**5 550,00**

Rocades blindées

Les câbles multipaires de la gamme ACOME pour rocade se déclinent en versions 32, 64 et 128 paires Cat 5 pour assurer l'interconnexion de sous-répartiteurs.

Caractéristiques :

- Impédance 100
- Assemblage en paires
- Conducteurs cuivre monobrin AWG 24
- Câbles FTP Cat 5
- Existent en versions 32, 64 et 128 paires
- Gaine LSOH (ivoire) ou PVC (gris)



Référence	Désignation	Prix pour	Prix H.T. (€)
ACO M4980ST	Câble rocade 32 paires Cat 5 FTP LSOH	1000	**4 930,00**
ACO M5014ST	Câble rocade 64 paires Cat 5 FTP LSOH	1000	**9 945,00**
ACO M5016ST	Câble Rocade 128 paires Cat 5 FTP LSOH	1000	**19 787,50**
ACO M5013ST	Câble rocade 64 paires Cat 5 FTP PVC	1000	**4500,00**
ACO M5015ST	Câble rocade 128 paires Cat 5 FTP PVC	1000	**15760,00**
ACO M4979AST	Câble rocade 32 paires Cat 5 FTP PVC	1000	**4 540,00**

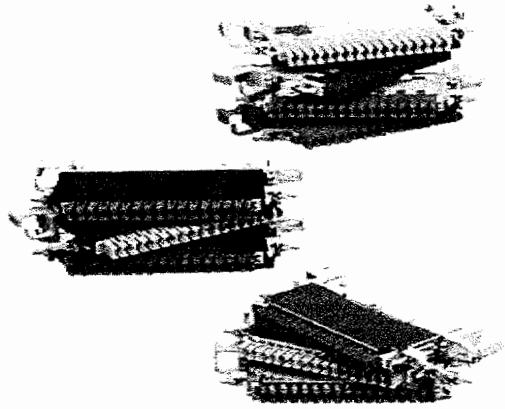
ANNEXE 12 :

Modules (SCP) de raccordement gamme Europe

Une gamme spécifiquement conçue pour les applications haut débit, offrant un large choix de modules blindés à câblage arrière ou latéral, pour tous types d'utilisations. Principalement de performance Cat 5, il sont d'utilisation polyvalente pour des applications telles que l'informatique, la téléphonie, la distribution vidéo, gestion technique et signalisation.

Caractéristiques :

- Utilisation aisée
- Sécurisation totale grâce au système de rétention à cliquet
- Détrompage vertical automatique des cordons
- Gestion des câbles et liaisons facilitée par porte étiquette et code couleur
- Diamétre de conducteurs acceptés : entre 0,4mm et 0,7mm
- Montage selon le type de module sur châssis de type RIBE, fermes FAE
- Pour le câblage arrière, utiliser impérativement les châssis et profilés Europe E8
- Pour le cablâge latéral, possibilité de choisir le profilé HPUL ou Europe E8



Référence	Désignation	Prix pour	Prix H.T. (€)
POU P45920DH	Module à coupure bleu 8 paires, à câblage arrière blindé	1	**12,64**
POU P45840DH	Module à coupure jaune 8 paires, à câblage arrière blindé	1	**12,64**
POU P45839DH	Module à coupure vert 8 paires, à câblage arrière blindé	1	**12,64**
POU P45809DH	Module à coupure rouge 8 paires, à câblage arrière blindé	1	**12,64**
POU P45734DH	Module à coupure ivoire (numéris) à coupure 8 paires, à câblage arrière blindé	1	**12,64**
POU P45920DK	Module à coupure bleu à coupure 16 paires	1	**13,63**

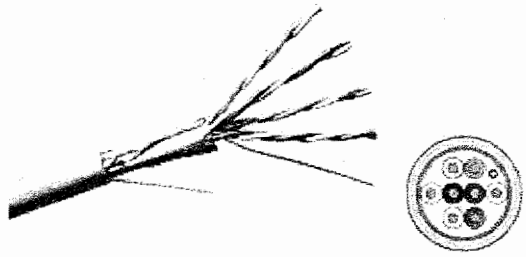
ANNEXE 13 : Câble de distribution

Câbles Cat 5E FTP

La gamme FLEX200 en cuivre Catégorie 5E rigide et souple est développée depuis 2000 . Cette gamme de produits UTP/FTP/SFTP répond largement aux exigences de la norme ANSI/TIA/EIA 568-A . Ces câbles de transmission de données existent en version de gaine extérieure en PVC ou Zéro Halogène (LSOH). Ils sont fournis sur touret en conditionnement de 500 et 1000 métres et en box de 305 m pour les câbles UTP/FTP catégorie 5E en version 4et 2x4 paires.

Caractéristiques :

- Impédance 100 +/- 15%.
- Paires torsadées, conducteur en cuivre monobrin 24 AWG.
- Gaine extérieure PVC, LSOH.
- Testé contre la propagation du feu selon : IEC 60332-1 en IEC 60332-3C.
- Capacitance UTP : 47pF/m.
- Capacitance FTP : 52pF/m.
- Capacitance S-FTP : 50pF/m. NVP : 70 %.
- Couleur de la gaine extérieure : gris RAL 7035/7032.
- Atténuation 19 dB 100 m @100 Mhz
- NEXT 41 dB@100 Mhz
- ACR 21 dB@100 Mhz

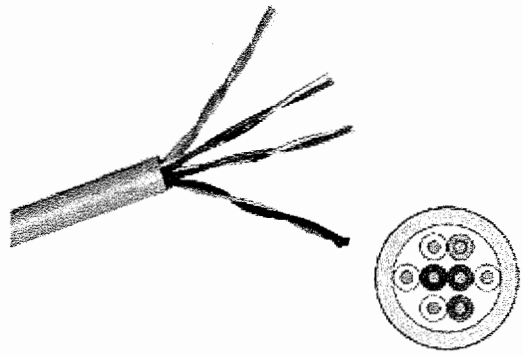


Référence	Désignation	Prix pour	Prix H.T. (€)
DK4 C5EFST	Câble 4 paires Cat 5E FTP PVC	1000	**389,15**
DK4 C5EFT5	Câble 4 paires Cat 5E FTP PVC - 500m	1000	**389,15**
DK4 C5EFU3	Câble 4 paires Cat 5E FTP PVC - 305m	1	**118,70**
DK4 C5EFC1	Câble 4 paires Cat 5E FTP PVC - 100m	1000	**389,15**
DK4 C5EDFST	Câble 2x4 paires Cat 5E FTP PVC	1000	**800,80**
DK4 C5EFZHST	Câble 4 paires Cat 5E FTP LSOH	1000	**406,65**
DK4 C5EDFZHST	Câble 2x4 paires Cat 5E FTP LSOH	1000	**840,80**
DK4 C5EF12PZHST	Câble 3x4 paires Cat 5E FTP LSOH	1000	**1200,00**
DK4 C5EDFT5	Câble 2x4 paires Cat 5E FTP PVC - 500m	1000	**800,80**

Câbles Cat 5E UTP

Caractéristiques :

- Impédance 100 +/- 15%.
- Paires torsadées, conducteurs en cuivre monobrin 24 AWG.
- Gaine extérieure PVC, LSOH.
- Testés contre la propagation du feu selon : IEC 60332-1 en IEC 60332-3C.
- Capacitance UTP : 47pF/m.
- Capacitance FTP : 52pF/m.
- Capacitance S-FTP : 50pF/m.
- NVP : 70 %.
- Couleur de la gaine extérieure : gris RAL 7035/7032.
- Atténuation 19 dB 100 m @100 Mhz
- NEXT 41 dB@100 Mhz
- ACR 21 dB@100 Mhz



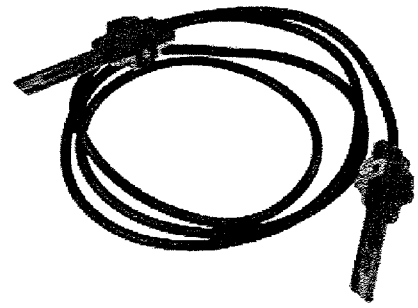
Référence	Désignation	Prix pour	Prix H.T. (€)
DK4 C5EUST	Câble 4 paires Cat 5E UTP PVC	1000	**301,53**
DK4 C5EUT5	Câble 4 paires Cat 5E UTP PVC - 500m	1000	**301,52**
DK4 C5EUU3	Câble 4 paires Cat 5E UTP PVC - 305m	1	**91,95**
DK4 C5EUC1	Câble 4 paires Cat 5E UTP PVC - 100m	1000	**301,53**
DK4 C5EDUST	Câble 2x4 paires Cat 5E UTP PVC	1000	**665,55**
DK4 C5EDUZHST	Câble 2x4 paires Cat 5E UTP LSOH	1000	**738,05**
DK4 C5EUZHST	Câble 4 paires Cat 5E UTP LSOH	1000	**364,00**

ANNEXE 14 : Câble de brassage

Cordons pour modules de raccordement

Caractéristiques :

- Cordons de brassage en version simple face ou double face recommandés pour les liaisons analogiques
- Cordons de brassage SCP (à verrouillage)/ SCP (à verrouillage) recommandés pour les liaisons numériques
- Câblage croisé ou droit (nous consulter)
- Version de cordons pour test de dérivation
- Cordons d'adaptation pour adaptation SCP (à verrouillage)/RJ45



Référence	Désignation	Prix pour	Prix H.T. (€)
POU P24751DA	Cordon simple face droit 1 paire 0,90m	1	**10,02**
POU P24752DA	Cordon simple face droit 1 paire 1,80m	1	**10,51**
POU P34612DA	Cordon simple face droit 2 paires 0,45m	1	**13,51**
POU P34864DA	Cordon simple face droit 2 paires 0,90m	1	**13,70**
POU P34865DA	Cordon double face droit 2 paires 1,80m	1	**15,01**
POU P24868DA	Cordon double face droit 4 paires 0,90m	1	**23,24**
POU P24869DA	Cordon double face droit 4 paires 1,80m	1	**25,74**
POU P34866DA	Cordon croisé simple face 2 paires 0,90m	1	**13,70**
POU P34867DA	Cordon croisé simple face 2 paires 1,80m	1	**15,01**
POU P24746AA	Cordon SCP/SCP 1 paire 0,90m	1	**10,76**
POU P24784AA	Cordon SCP/SCP 1 paire 1,80m	1	**11,70**
POU P24788AA	Cordon SCP/SCP 2 paires 1,80 m	1	**16,22**
POU P24789AA	Cordon SCP/SCP 4 paires 1,80m	1	**18,19**
POU P24747AA	Cordon SCP/RJ45 1 paire 1,80m	1	**11,58**
POU P2917703	Cordon SCP /RJ45 2 paires 1,80m	1	**22,21**
POU P2906203	Cordon SCP /RJ45 4 paires 1,80m	1	**25,74**

ANNEXE 15: SWITCH

Switchs 10/100Mbps non manageables

Les switchs GIGAMEDIA sont conçus pour les utilisateurs recherchant une solution simple et efficace pour interconnecter leurs postes de travail. Le switch 16 ports GGM NE816X s'intègre dans le coffret 123 CONNECT. Proposant une souplesse et une facilité d'installation considérables, la série des commutateurs GIGAMEDIA se conforme entièrement à la norme IEEE802.3x. Chacun d'entre eux offre des solutions de commutation 10/100 puissantes, nécessaires aux environnements de bureau et réseau de petite taille. Chacun des ports prend automatiquement en charge la détection des modes full-duplex. Ce qui permet d'obtenir une performance maximale sur l'ensemble du trafic réseaux.

Caractéristiques :
- Switchs 10/100Mbps autosensing
- 5, 8 et 16 ports 10/100BaseTX
- Installation simple et rapide
- Format desktop
- Port de cascade MDI/MDIX
- LEDS de fonctionnement en façade
- Contrôle de flux Half/Full Duplex
- Alimentation externe
- Authentification par contrôle de flux

Référence	Désignation	Prix pour	Prix H.T. (€)
GGM NE805XR	switch 5 ports 10/100 Mbps RJ45	1	**32,00**
GGM NE808XR	switch 8 ports 10/100 Mbps RJ45	1	**38,40**
GGM NE816X	switch 16 ports 10/100 Mbps RJ45	1	**91,26**

Switchs Fast Ethernet 10/100Mbps manageables

La nouvelle génération de commutateurs Fast Ethernet justifie une liaison très performante en Backbone grâce à l'intégration des ports Gigabit Ethernet. Elle permet de fédérer plusieurs réseaux locaux à l'intérieur d'un même site et en garantissant un haut débit entre les serveurs de fichiers et les postes de travail.

Caractéristiques :
- 24 ou 48 ports RJ45 10BaseT/100BaseTX
- Management : SNMP, RMON, VLAN, IGMP, Web
- Half/Full duplex sur les ports 10/100MBps
- Protocoles : Spanning Tree, Flow control, Trunking
- Aggrégation des liens
- Bande passante jusqu'à 13,6Gbps (Série SMC6948L2EU)

Référence	Désignation	Prix pour	Prix H.T. (€)
SYY 6724L2EU	Switch 24 Ports 10/100Mbps avec 2 slots GBIC	1	**760,00**
SYY 6724L2GSSC	Module 1000SX (SC multimode)	1	**360,00**
SYY 6948L2EU	Switch 48 ports 10/100MBps avec 2 slots GBIC	1	**1400,00**
SYY 6900FSC	Module 2 ports 100BaseFX (SC multimode)	1	**540,00**
SYY 6900FST	Module 2 ports 100BaseFX (ST multimode)	NC	**NC**

SYY 6900GLSC	Module 1 port 1000BaseLX (SC monomode)	1	**1 300,00**
SYY RPU150W	Alimentation redondante	NC	**NC**
SYY 6724L2GLSC	Module 1000LX (SC monomode)	NC	**NC**
SYY 6724L2GT	Module 10/100/1000BaseT	1	**480,00**
SYY 6900GT	Module 1 port 10/100/1000BaseT	1	**600,00**
SYY 6725L2FMSC	Module 100FX (SC multimode)	1	**270,00**
SYY 6725L2FSSC	Module 100FX (SC monomode)	1	**650,00**
SYY EliteView	Logiciel gratuit d'administration réseau	NC	**NC**
SYY RPU160W	Alimentation redondante pour 6724L2	1	**700,00**
SYY 6900G	Module 1000BaseSX (SC multimode)	NC	**NC**
SYY 6900FSSC	Module 100FX (SC monomode)	NC	**NC**
SYY 6750L2	Switch 48 ports 10/100BaseT avec 2 emplacements d'extension GBIC	1	**1 180,00**

Switchs 10/100Mbps & 1000Mbps manageables & empilables

L'AT-8326GB offre deux ports cuivre Gigabit Ethernet et deux emplacements d'extension GBIC. Les emplacements GBIC peuvent être équipés de cartes d'extension fibre à courte ou longue portée. Les utilisateurs peuvent ainsi configurer le commutateur pour exploiter simultanément les deux ports cuivre Gigabit Ethernet existants, ou bien les deux emplacements GBIC, voire une combinaison constituée d'un port cuivre Gigabit Ethernet et d'un port GBIC. Il supporte le protocole GVRP, 256 sous-réseaux VLAN et s'adapte parfaitement aux administrateurs de réseau qui souhaitent déployer un commutateur empilable dans leur réseau de collecte. Le protocole GVRP permet au 8326GB de créer dynamiquement des sous-réseaux VLAN compatibles 802.1Q et relier ainsi le commutateur d'Allied Telesyn à tout autre équipement utilisant GVRP, quel que soit son fabricant. Ce protocole réduit les risques d'erreur dans la configuration des VLAN en fournissant automatiquement une identité de sous-réseau. Il assure aussi la propagation automatique des VLAN à d'autres équipements supportant GVRP, ou manuellement et équipement par équipement pour les autres. Si la configuration des sous-réseaux vient à changer, GVRP exclut automatiquement de la configuration de sous-réseaux les équipements affectés par l'incident.

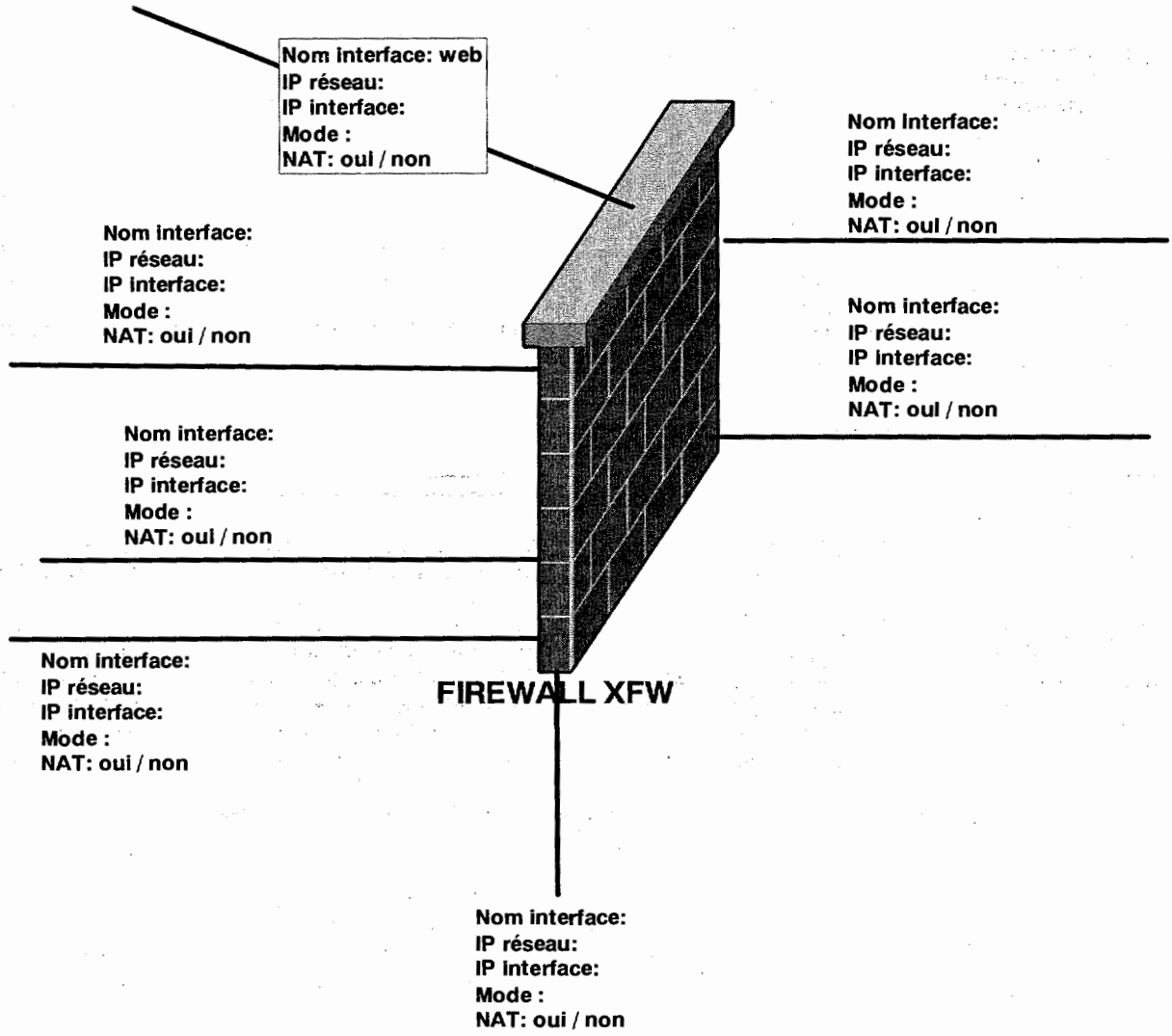
Caractéristiques :

- 24 ports 10/100TX + 2 ports 10/100/1000T
- 2 Modules GBIC "slots"
- Manageables via SNMP, RMON et TELNET
- Module de stack intégré
- 144 ports maxi (mixables)
- Netcover Basic + 3 ans
- Protocoles : Flow control, Trunking
- 00 800 287 877 678 Hot line Internationale (N° gratuit)

Référence	Désignation	Prix pour	Prix H.T. (€)
ATI AT8326GB	Switch 24 ports 10/100 + 2 Giga cuivre + 2 GBIC	1	**750,72**
ATI AT8350GB	Switch 48 p 10/100 + 2 1000T ou 2 GBIC + 1slot	1	**1 370,80**
ATI ATA48	2 ports 100FX pour 8350	NC	**NC**
ATI ATA49	2 ports 10/100/1000BaseT pour 8350	1	**517,04**

Document réponse DR1 :

Question B-2-1 : *complétez le schéma ci-dessous en précisant toutes les paramètres.*



Mode : bridge ou avancé

Nat : entourez la bonne réponse

Document réponse DR2 :

Question B-1-8 : *Complétez les cellules vides du tableau ci-dessous* :

N° d'action	Etat	interface	Protocole	Source	Destination	Port source	Port destination	Action	N° de contrainte
1	on	web	group	128.156.0.0	Any	any	web	passer	
2		agences							C5
3		agences							C5
4	on	res_interne	tcp /udp	195.151.64.0	128.156.0.0	Any	telnet	bloquer	
5	on	res_interne	tcp /udp	195.151.64.0	128.156.0.0	Any	login	bloquer	
6	on	res_interne	tcp /udp	195.151.64.0	128.156.0.0	Any	echo	bloquer	
7	on	res_interne	tcp /udp	195.151.64.0	128.156.0.0	Any	http	bloquer	
8	on	res_interne	tcp /udp	195.151.64.0	128.156.0.0	Any	netbios-ns	Bloquer	
9	on	res_interne	tcp /udp	195.151.64.0	128.156.0.0	Any	netbios-dgm	Bloquer	

Document réponse DR3 :

Répartiteur PAT

Modules jaunes téléphonie numérique							
200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215
216							

Modules jaunes téléphonie analogique							
400	401	402	403	404	405	406	407
408	409	410	411	412	413	414	415
416							

SWITCH							
Eth1	Eth2	Eth3	Eth4	Eth5	Eth6	Eth7	Eth8
Eth9	Eth10	Eth11	Eth12	Eth13	Eth14	Eth15	Eth16

Réf :

Rocade Modules verts							
400							

Poste2

Poste de travail 1

tél. num.

télécopieur

station de travail

Répartiteur MAR16

Bandeau RJ45							
400							

Réf. câble :

Rocade Modules verts							
400							