

# Routeur d'accès modulaire Cisco 1720

*Accès Internet flexible pour petites et moyennes entreprises et petites succursales*

Internet est en train de révolutionner les méthodes commerciales des entreprises. L'avenir promet encore davantage de changements, en raison de l'évolution rapide des technologies et des applications d'administration de réseaux. Les entreprises qui se sont préparées aux technologies de pointe d'administration de réseaux possèdent un avantage considérable sur leurs concurrents.

Préparer une petite ou moyenne entreprise ou une petite succursale aux technologies du futur consiste à implémenter des équipements de réseau possédant les caractéristiques stratégiques suivantes :

- Souplesse d'adaptation à l'évolution des réseaux (croissance et besoins)
- Protection de l'investissement avec des caractéristiques et des performances pouvant supporter aujourd'hui comme demain de nouveaux services WAN, tels que les réseaux privés virtuels (VPN), l'accès à large bande xDSL (ligne d'abonné numérique ou câble) immédiatement ou en cas de nécessité
- Intégration de nombreuses fonctions de réseau, dont un pare-feu et une unité DSU (*data service unit*) en option, afin de simplifier le déploiement et l'administration

Le routeur d'accès Cisco 1720 combine toutes ces caractéristiques avec la puissance de la plate-forme logicielle Cisco IOS<sup>®</sup>, dans une solution intégrée modulaire permettant d'accéder à Internet, aux intranets et aux extranets. Le routeur Cisco 1720 propose une solution de routage d'accès sur mesure pour les petites et moyennes entreprises et les petites succursales.

**Figure 1** Le routeur Cisco 1720 propose une solution d'accès WAN polyvalente, alliant puissance de la plate-forme logicielle Cisco IOS, souplesse et intégration d'équipements.



Routeur d'accès modulaire Cisco 1720  
 Le routeur d'accès Cisco 1720 dispose des éléments suivants :

- Un port Fast Ethernet 10/100 à détection automatique
- Deux emplacements pour cartes d'interface WAN (WIC) supportant les mêmes cartes d'interfaces WAN de données que les routeurs des gammes Cisco 1600, 2600 et 3600
- Un port auxiliaire (AUX), pour connexion série asynchrone à 115,2 kbits/s maximum
- Un port de console
- Un processeur RISC supportant des fonctions de cryptage et de large bande hautes performances

- Un emplacement interne pour la carte de cryptage à accélération matérielle (MOD1700-VPN), avec des performances pouvant atteindre les débits T1/E1
- Connectivité à large bande par ligne d'abonné numérique (xDSL) ou par câble

Figure 2 Vue arrière du routeur Cisco 1720



Le routeur Cisco 1720 supporte jusqu'à deux cartes d'interface WAN répertoriées dans le tableau 1. Ces cartes prennent en charge un grand choix de technologies WAN : RNIS (*Réseau Numérique à Intégration de Services*), série asynchrone, série synchrone (lignes louées, par exemple), Frame Relay, Switched 56, X.25 et SMDS (*Switched Multimegabit Data Service*). D'autres cartes d'interface WAN sont également disponibles, pour l'intégration d'unités DSU/CSU (*Data Service Unit/*

*Channel Service Unit*) ; elles suppriment les coûts d'assistance, ainsi que le déploiement et l'administration complexes d'unités externes.

#### Caractéristiques et avantages

Le routeur Cisco 1720 offre une souplesse, une sécurité et une facilité de déploiement sans équivalent. Voir Tableau 2.

Tableau 1 Cartes d'interface WAN pour le routeur Cisco 1720

Référence Cisco	Description
WIC-1T	Carte d'interface un port série asynchrone (jusqu'à 115,2 kbps) et WAN synchrone (T1/E1)
WIC 2T	Carte d'interface deux ports série asynchrones (jusqu'à 115,2 kbps) et WAN synchrone (T1/E1)
WIC-2A/S	Carte d'interface deux ports faible débit asynchrones (jusqu'à 115,2 kbps) et WAN synchrone (jusqu'à 128 kbps)
WIC-1B-S/T	Carte d'interface WAN un port RNIS BRI S/T
WIC-1B-U	Carte d'interface un port RNIS BRI U avec WAN NT1 intégré
WIC-1DSU-56K4	Carte d'interface un port intégré 56/64 kbps, WAN DSU/CSU quatre fils
WIC-1DSU-T1	Carte d'interface monoport intégré T1/fraction de T1 WAN DSU/CSU
WIC-1ADSL	Carte WIC ADSL monoport
WIC-1ENET	Carte d'interface Ethernet 10BaseT monoport

Tableau 2 Caractéristiques et avantages

#### Caractéristiques

##### Souplesse

Prise en charge Cisco IOS intégrale (comprend le pontage et le routage [IP, IPX, AppleTalk, IBM/SNA] multiprotocoles)

##### Architecture modulaire (emplacements de carte WAN)

Cartes d'interface WAN partagées avec les routeurs Cisco 1600, 2600 et 3600

#### Avantages

Fournit le support logiciel de réseau le plus complet, robuste et évolutif du marché en utilisant la norme logicielle de fait pour les connexions Internet et les WAN privés  
Elément de la solution de réseau de bout en bout proposée par Cisco

Protège l'investissement en garantissant la souplesse de choix WAN sur le Cisco 1720

Réduction des coûts de gestion des inventaires  
Limitation des coûts de formation des techniciens d'assistance  
Protection des investissements grâce à une compatibilité avec différentes plates-formes



## Caractéristiques

## Avantages

<b>Fast Ethernet 10/100 à détection automatique</b>	Simplification de la mise en place dans des environnements Ethernet hétérogènes
<b>Emplacement d'extension sur la carte mère</b>	Permet l'évolutivité grâce au support de services tels que le cryptage assisté par matériel
<b>Options de connectivité à large bande</b> (La connectivité xDSL et par câble offre un accès professionnel à large bande)	Tire parti des technologies d'accès haut débit tels que le câble ou xDSL pour augmenter les débits de connexion au réseau étendu et réduire les coûts d'accès Apporte la connexion SDSL et ADSL au routeur Cisco 633 et à la carte d'interface WAN ADSL La connexion par câble au Cisco 1720 et le DSU câble intégré en option au routeur large bande universel Cisco uBR910 offrent un accès haut débit professionnel
<b>Intégration matérielle</b> (routeur, pare-feu, cryptage, serveur de tunnels VPN, unités DSU/CSU et NT1 intégrés à un seul équipement)	Réduit les coûts et simplifie l'administration considérablement, par rapport aux solutions à base de multiples équipements hétérogènes
<b>Sécurité et fonctionnalité de réseaux privés virtuels</b>	
<b>Pare-feu</b> (Cisco IOS Firewall comprend le contrôle d'accès par contexte pour le filtrage par pare-feu dynamique, la détection de refus de service, le blocage Java et les alarmes en temps réel.)	Possibilité pour les utilisateurs internes d'accéder à Internet avec contrôle d'accès dynamique sécurisé, par application, tout en protégeant le LAN interne contre les tentatives d'accès non autorisées via Internet
<b>Cryptage</b> (Module VPN IPSec ESP DES et Triple DES pour cryptage rapide à accélération matérielle)	Permet la création de réseaux VPN à la vitesse du médium en garantissant la confidentialité, l'intégrité et l'authenticité des données lors de leur transfert via un réseau public, conformément aux normes de l'industrie Option de mise en place de cryptage haut débit à accélération matérielle jusqu'au débit T1/E1
<b>Authentification d'équipement et administration centrale</b> IKE, certification numérique X.509v3, support du protocole CEP ( <i>Certificate Enrollment Protocol</i> ) avec organismes d'homologation (CA), tels que Verisign et Entrust	Identification et authentification des équipements et des données Évolutivité vers de très grands réseaux IPSec grâce à une administration centrale automatisée
<b>Fractionnement en canaux</b> IPSec, GRE, L2TP, L2F	Méthodes normalisées de mise en tunnel permettant de créer des réseaux privés virtuels pour trafic IP et non IP Possibilité pour tout client normalisé IPSec ou L2TP de fonctionner dynamiquement avec les technologies de tunnel de Cisco IOS
<b>Qualité de service (QoS)</b> (CAR, routage par politique, WFQ PQ/CBWFQ, GTS, FRTS, RSVP)	Optimisation des performances avec affectation de la bande passante WAN aux applications prioritaires
<b>Facilité de déploiement</b>	
<b>Administration</b> (administration via SNMP [CiscoView, CiscoWorks2000], Telnet et port de console)	Permet le contrôle, la configuration et le diagnostic centralisés pour toutes les fonctions intégrées du routeur Cisco 1720, réduisant ainsi les temps et les coûts d'administration
<b>Simplicité d'installation et d'utilisation</b> Programme Cisco ConfigMaker, utilitaire de configuration SETUP, AutoInstall, câbles et ports codés par couleurs et voyants LED indicateurs d'état	Réduction des coûts et du temps de déploiement, à l'aide d'un outil graphique de configuration de politiques LAN/VPN, d'un questionnaire de configuration orienté contexte en ligne de commande et d'un système de câblage simplifié Diagnostics et dépannage rapides à l'aide des voyants DEL
<b>Traduction NAT (<i>Network Address Translation</i>) et Easy IP</b>	Simplification du déploiement et réduction des coûts d'accès à Internet

## Caractéristiques

## Avantages

---

### Réduction des coûts d'exploitation

---

#### Fiabilité et évolutivité

(Plate forme logicielle Cisco IOS, routage à établissement de connexion à la demande, mémoire flash à double banc de composants, protocoles de routage modulable [OSPF, EIGRP, BGP et HSRP])

---

Accroît la fiabilité et permet la migration vers les grands réseaux

#### Souplesse

Le routeur Cisco 1720 propose une solution souple. Les cartes d'interface WAN interchangeable facilitent considérablement la mise à jour ou le changement de technologie WAN exigé par l'évolution de votre entreprise. L'utilisation de cartes identiques sur les routeurs des gammes Cisco 1600, 2600 et 3600 simplifie la gestion des pièces détachées et protège l'investissement déjà réalisé sur les autres routeurs. Au fur et à mesure de l'augmentation des besoins en performances du réseau local, le port Fast Ethernet 10/100 à détection automatique du Cisco 1720 permet un déploiement facile dans les réseaux Ethernet hétérogène. En outre, grâce à son architecture RISC, le Cisco 1720 possède la puissance nécessaire pour supporter les lignes xDSL et autres technologies d'accès large bande de plus en plus répandues.

#### Fonctions de Cisco IOS pour l'accès à Internet et aux intranets

Outre les caractéristiques décrites plus haut, le routeur Cisco 1720 se distingue de ses concurrents grâce aux nombreuses fonctions d'accès à Internet et aux intranets proposées par la plate-forme logicielle Cisco IOS :

- Routage multiprotocole (IP, IPX [*Internetwork Packet Exchange*] et AppleTalk), IBM SNA (*Systems Network Architecture*) et pontage transparent sur RNIS, série asynchrone ou synchrone par liaisons spécialisées, Frame Relay, SMDS, 56 commuté, X.25 et X.25 sur un canal D RNIS.
- La traduction d'adresses réseau NAT (*Network Address Translation*) réduit les coûts d'accès Internet : elle supprime le réadressage des hôtes disposant d'adresses de réseaux privés (traduction 1-1) ou permet à tous les hôtes internes de partager une même adresse IP enregistrée (traduction x-1, également désignée par « traduction d'adresses de ports », ou « PAT ») ;

la traduction d'adresses réseau améliore aussi la sécurité du réseau en masquant les adresses internes vis-à-vis du réseau public.

- Easy IP facilite le déploiement et réduit les coûts d'accès, en combinant les caractéristiques suivantes :
  - Traduction PAT pour la conservation des adresses IP,
  - Protocole PPP/PCP (*Point-to-Point Protocol/Internet Protocol Control Protocol*) pour permettre au routeur de négocier et de configurer dynamiquement ses propres adresses IP,
  - Serveur DHCP (*Dynamic Host Configuration Protocol*) pour l'attribution d'adresses IP réutilisables aux clients, de façon dynamique et transparente,
  - Client DHCP, pouvant accepter des adresses IP dynamiques.
- Réduction des coût du réseau étendu grâce aux fonctions d'optimisation telles que le routage à la demande (DDR), la bande passante à la demande (BOD) et l'ouverture de circuit OSPF (*Open Shortest Path First*) à la demande, le routage par cliché, la compression, le filtrage et le « spoofing ».
- Protocole PPPoE (*PPP over Ethernet*) sur le routeur Cisco 1720, permettant l'authentification en PPP du routeur sur le réseau d'un fournisseur de services ; en exigeant une procédure d'échange de mot de passe pour autoriser une configuration réseau, PPPoE fournit de façon transparente la procédure d'authentification nécessaire pour le suivi de l'utilisation et la facturation du service.

Sécurité et support de réseaux privés virtuels

**Puissance de la plate-forme logicielle Cisco IOS** – Norme de fait pour les WAN privés et Internet, la plate-forme logicielle Cisco IOS d'administration de réseaux propose l'ensemble le plus complet de fonctions VPN de sécurité, de qualité de service (QoS), d'administration, de fiabilité et d'évolutivité. Exploités conjointement, la plate-forme



logicielle Cisco IOS et le routeur Cisco 1720 permettent de déployer aujourd'hui et demain des VPN à grande échelle pour un coût très avantageux et des performances optimales.

**Sécurité** – La plate-forme logicielle Cisco IOS supporte un ensemble complet de fonctionnalités de sécurité, des plus simples aux plus perfectionnées : listes ACL de contrôle d'accès, authentification des utilisateurs, autorisation et statistiques (PAP/CHAP [ Password Authentication Protocol/Challenge Handshake Authentication Protocol ], TACACS+ et RADIUS[ Remote Access Dial-In User Service ]), ainsi que la prise en charge intégrale des VPN, y compris le cryptage. Pour accroître la sécurité, le pare-feu intégré protège les LAN internes contre les intrusions, grâce au contrôle CBAC (*Context-Based Access Control*).

En effet, ils permettent aux entreprises d'interconnecter leurs bureaux, leurs employés mobiles et leurs partenaires, grâce au partage des infrastructures de communication d'Internet ou du réseau fédérateur d'un fournisseur de service. Cette technologie évite les frais des appels longue distance des réseaux privés traditionnels et réduit donc considérablement les coûts inhérents aux réseaux WAN. En outre, elle renforce la sécurité des données et accroît les performances du réseau, tout en simplifiant les opérations de connexion. Le Cisco 1720 supporte non seulement tous les services et toutes les applications d'accès WAN actuellement répandues, mais également les réseaux privés virtuels. Il comporte tous les éléments nécessaires à la sécurisation des VPN aujourd'hui et demain : pare-feu intégré, fonctions et performances de cryptage, tunnels VPN et qualité de service.

Tunnels IPSec (*IP Security*) avec cryptage DES (*Data Encryption Standard*) et 3DES (*Triple DES*) pour assurer la confidentialité, l'intégrité et l'authenticité des données circulant sur un réseau public. Parallèlement, grâce aux protocoles L2F (*Layer 2 Forwarding*) et L2TP (*Layer 2 Tunneling Protocol*) intégrés, le cryptage IPSec constitue la solution multiprotocole (IP, IPX, AppleTalk et IBM SNA) sécurisée idéale pour les VPN d'accès distant. Les utilisateurs mobiles se connectent au point de présence local d'un fournisseur de services via une ligne

commutée, et les données sont renvoyées « par tunnel » (encapsulées par un second protocole, tel que L2TP) au routeur Cisco 1720, afin de sécuriser l'accès au réseau de l'entreprise via Internet.

**Qualité de service (gestion de trafic)** – Les fonctions de qualité de service de la plate-forme logicielle Cisco IOS contrôlent l'affectation de bande passante VPN aux applications stratégiques. Le Cisco 1720 propose des fonctions QoS de la pointe telles que le débit garanti (CAR = *Committed Access Rate*), le routage par politique, la file d'attente par priorité et la file d'attente par classe pondérée (PQ/CBWFQ), la détection avancée aléatoire pondérée (WRED), la mise en forme de trafic générique (GTS) et le protocole de réservation de ressources (RSVP).

**Administration et facilité d'installation** – Le routeur Cisco 1720 supporte différents outils d'administration de réseau et d'aide à l'installation.

- Cisco ConfigMaker est un utilitaire de type Assistant Windows qui permet de configurer un petit réseau de routeurs, commutateurs, concentrateurs et autres équipements Cisco, à partir d'un simple PC. Cet outil simplifie la configuration de fonctions de sécurité à valeur ajoutée, telles que la fonctionnalité Cisco IOS Firewall, le cryptage IPSec et la traduction d'adresses de réseau NAT. Il définit des politiques VPN (qualité de service et sécurité incluses) et configure le serveur DHCP (*Dynamic Host Configuration Protocol*).
- CiscoView est un programme d'administration d'équipements pour plates-formes UNIX, à interface graphique utilisateur. Il donne des informations complètes sur la configuration, fournit différentes statistiques et indique l'état dynamique du matériel.
- CiscoWorks2000, suite d'administration de réseaux via Internet de pointe proposée par Cisco, simplifie différentes tâches, telles que la gestion du parc du réseau, les changements d'équipements, le déploiement rapide d'images logicielles et le dépannage.
- Cisco Service Management (CSM) est destiné aux fournisseurs de services. Ce programme présente une suite complète de solutions d'administration de services permettant de planifier, d'approvisionner, de contrôler et de facturer les VPN, avec une grande rapidité.

**Fiabilité et évolutivité** – Grâce à sa fiabilité, la plate-forme logicielle Cisco IOS s’est imposée comme la norme de fait sur le marché de l’administration des réseaux. Ses technologies garantissent l’adaptation d’un VPN aux grands réseaux, en toute fiabilité : support d’IKE (*Internet Key Exchange*) et certifications numériques auprès des principaux organismes d’homologation, intégration des normes de routage évolutif, telles qu’OSPF (*Open Shortest Path First*) et EIGRP (*Enhanced Interior Gateway Routing Protocol*), BGP (*Border Gateway Protocol*) et services de fiabilité, tels que HSRP (*Hot Standby Router Protocol*).

**Performances de cryptage** – Grâce à la puissance de son processeur RISC, le Cisco 1720 supporte le cryptage logiciel IPSec à 512 kbits/s pour des paquets de 256 octets (taille de paquets la plus répandue). Les performances varient en fonction de l’algorithme de cryptage utilisé, de la taille des paquets sur le réseau, etc. Un emplacement d’extension sur la carte mère Cisco 1720 permet une accélération matérielle jusqu’au débit-T1/E1 (MOD1700-VPN).

#### Intégration matérielle

Le Cisco 1720 constitue une solution d’accès « tout en un » pouvant combiner un routeur, des unités DSU/CSU et un équipement NT1 (*Network Termination-1*) RNIS, ainsi qu’un pare-feu dynamique, un serveur de tunnel VPN (« home gateway ») et un utilitaire de cryptage. Le nombre d’équipements et de câbles à installer et à configurer étant considérablement réduit, cette intégration limite fortement les temps et les coûts de déploiement et d’administration. Un produit intégré permet également un gain d’encombrement et accroît la fiabilité de la solution, celle-ci nécessitant moins

d’équipements autonomes. Parallèlement, le routeur Cisco 1720 simplifie le support continu des petites succursales à partir d’un site central grâce à la configuration, au contrôle et au dépannage à distance de toutes les fonctions intégrées.

#### Fonctionnalités de la plate-forme logicielle Cisco IOS

Le routeur Cisco 1720 supporte toute une gamme de fonctionnalités de la plate-forme logicielle Cisco IOS, Chacune d’entre elles exige une quantité de mémoire RAM et de mémoire flash donnée. (Remarque : À partir de la version 12.0, les programmes et fonctions du routeur Cisco 1720 sont les mêmes que ceux des routeurs Cisco 1600. Ils intègrent en outre les solutions IPSec 3DES et ADSL (*asymmetric digital subscriber line*).

À partir de la version 12.0 de la plate-forme logicielle Cisco IOS, les solutions de base intègrent des fonctionnalités auparavant comprises dans les solutions Plus : NAT, OSPF, RADIUS et protocole NHRP (*Next Hop Resolution Protocol*). Les fonctions supplémentaires sont en particulier L2TP, L2F, BGP, la multidiffusion IP, les circuits virtuels commutés sur relais de trame (SVC), RSVP, le protocole NLSP (*Netware Link Services Protocol*), le protocole de routage SMRP AppleTalk, le protocole de contrôle de cache web (WCCP) et le protocole de synchronisation réseau (NTP = *Network Timing Protocol*). Le cryptage est proposé dans les fonctionnalités Plus IPSec 56 et Plus IPSec 3DES uniquement.

Pour élaborer un réseau privé virtuel IP, les fonctionnalités suivantes sont recommandées : IP/Firewall Plus IPSec 56 ou IP/Firewall Plus IPSec 3DES.

**Tableau 3** Fonctionnalités logicielles et mémoire requises pour le routeur Cisco 1720, avec les versions 12.1 Mainline de la plate-forme logicielle Cisco IOS

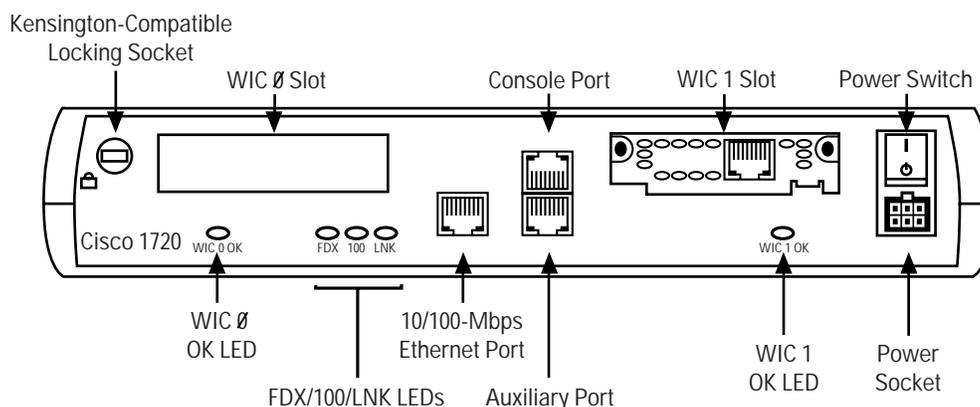
Fonctionnalité logicielle	Mémoire Flash requise (Mo)	Mémoire RAM requise (Mo)
IP	4	16
IP/Firewall	4	20
IP Plus	4	20
IP Plus IPSec 56	8	20
IP Plus IPSec 3DES	8	24
IP/Firewall Plus IPSec 56	8	24



Fonctionnalité logicielle	Mémoire Flash requise (Mo)	Mémoire RAM requise (Mo)
IP/Firewall Plus IPSec 3DES	8	32
IP/IPX	4	20
IP/IPX/Firewall Plus	8	20
IP/IPX/AppleTalk/IBM	8	24
IP/IPX/AppleTalk/IBM Plus	8	32
IP/IPX/AppleTalk/IBM/Firewall Plus IPSec 56	8	32
IP/IPX/AppleTalk/IBM/Firewall Plus IPSec 3DES	8	32

Remarque : Pour plus de détails sur cette version, consultez notre site à l'adresse suivante : <http://www.cisco.com/public/sw-center/sw-ios.shtml>

Figure 3 Panneau arrière du routeur d'accès Cisco 1720



### Caractéristiques techniques

#### Interfaces physiques/ports

- Un port Fast Ethernet 10/100BaseTX (RJ-45)
  - Détection automatique du débit
  - Négociation automatique du mode bidirectionnel
- Deux emplacements pour carte d'interface WAN
  - Supporte toute combinaison de cartes d'interfaces WAN (deux maximum), comme illustré dans le tableau 1. WIC-1T, WIC-2T, WIC-1DSU-56K4, WIC-1DSU-T1, WIC-1B-S/T, WIC-1B-U, WIC-2A/S, WIC-1ADSL, WIC-1ENET
- Interfaces série synchrones sur cartes d'interface WAN série
  - Débit d'interface : jusqu'à 2 Mbits/s (T1/E1)
  - Protocoles série synchrones : PPP, HDLC (*High-Level Data Link Control*), LAPB (*Link Access Procedure, Balanced*), IBM SNA
  - Services WAN série synchrones : Frame Relay, X.25 et SMDS
- Interfaces série synchrones supportées sur les cartes WIC-1T, WIC-2T et WIC-2A/S : V.35, EIA/TIA-232, EIA/TIA-449, X.21 et EIA-530
- Interfaces série asynchrones sur cartes d'interface WAN série
  - Débit d'interface : jusqu'à 115,2 kbits/s
  - Protocoles série asynchrones : Protocoles PPP, SLIP (*Serial Line Internet Protocol*)
  - Interface asynchrone : EIA/TIA-232
- Carte d'interface WAN ADSL
  - Compatible avec les services et application d'adaptation ATM de couche 5 (AAL5)
  - Interopérable avec le multiplexeur d'accès DSL Alcatel (DSLAM) avec jeu de composants Alcatel et le DSLAM Cisco 6130/6260 avec jeu de composants Globespan
  - Compatible avec la norme ANSI T1.413 révision 2 et ITU 992.1 (G.DMT)

- Carte d'interface WAN RNIS
  - Connexions commutées RNIS et IDSL (*ISDN DSL*) à 64 et 128 kbits/s
  - Encapsulation sur relais de trame IDSL et PPP
- Un port auxiliaire (AUX)
  - Jack RJ-45 avec interface EIA/TIA-232 (compatible avec le port auxiliaire de la gamme Cisco 2500)
  - DTE (*Data Terminal Equipment*) série asynchrone avec contrôle complet du modem par CD (*Carrier Detect*), DSR (*Data Set Ready*), RTS (*Request To Send*) et CTS (*Clear To Send*)
  - Débits série asynchrones jusqu'à 115,2 kbits/s
- Un port de console
  - Jack RJ-45 avec interface EIA/TIA-232 (compatible avec les ports de console des gammes Cisco 1000, 1600, 2500 et 2600)
  - DTE série asynchrone
  - Débit d'émission/réception jusqu'à 115,2 kbits/s (par défaut : 9600 bits/s) – À ne pas confondre avec un port de données
  - Pas d'échange bidirectionnel matériel tel que RTS/CTS
- Un emplacement d'extension interne pour le support de services assistés par matériel, tels que le cryptage (jusqu'à T1/E1)

#### Processeur

- Motorola MPC860T PowerQUICC à 48 MHz

#### Mémoires DRAM et flash

- Exécution à partir de la RAM
- DRAM
  - Embarquée (fixe/par défaut) : 32 Mo
  - Un emplacement DIMM
  - DRAM maximum : 48 Mo
- Flash
  - Type : carte miniflash embarquée (sur emplacement)
  - Par défaut : 8 Mo
  - Formats disponibles : 16 Mo
  - Flash maximum : 16 Mo
  - Support de double banc de flash

#### Dimensions

- Largeur : 28,4 cm
- Hauteur : 7,85 cm
- Profondeur : 22,1 cm

- Poids (minimum) : 1,18 kg
- Poids (maximum) : 1,32 kg

#### Alimentation

- Connecteur de verrouillage sur prise d'alimentation
- Tension d'alimentation alternative : 100 à 240 V
- Fréquence : 47 à 64 Hz
- Courant CA en entrée : 0,5 A
- Dissipation électrique : 20 W (maximum)

#### Environnement

- Température de fonctionnement : 0 à 40 C
- Température de stockage : -20 à +65 C
- Humidité relative : de 10 à 85 % sans condensation (fonctionnement) ; de 5 à 95 % sans condensation (stockage)

#### Sécurité

- UL 1950
- CSA 22.2 – N° 950
- EN60950
- EN 41003
- AUSTEL TS001
- AS/NZS 3260
- ETSI 300-047
- BS 6301 (alimentation)

#### Interférences électromagnétiques

- AS/NRZ 3548 Class A
- Class B
- FCC Part 15 Class B
- EN 60555-2 Class B
- EN 55022 Class B
- VCCI Class II
- CISPR-22 Class B

#### Immunité

- 55082-1 Generic Immunity Specification Part 1 : Zones résidentielles et petites industries
- IEC 1000-4-2 (EN61000-4-2)
- IEC 1000-4-3 (ENV50140)
- IEC 1000-4-4 (EN61000-4-4)
- IEC 1000-4-5 (EN61000-4-5)
- IEC 1000-4-6 (ENV50141)
- IEC 1000-4-11
- IEC 1000-3-2

## Homologation réseaux

- Europe : CTR2, CTR3
- Canada : CS-03
- États-Unis : FCC Part 68
- Japon : Jate NTT
- Australie/Nouvelle Zélande : TS013/TS-031
- Hong-Kong : CR22



### Siège social

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
États-Unis  
www.cisco.com  
Tél. : 408 526-4000  
800 553-NETS (6387)  
Fax : 408 526-4100

### Siège Europe

Cisco Systems Europe  
11, rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9  
France  
www.cisco.com  
Tél. : 33 1 58 04 60 00  
Fax : 33 1 58 04 61 00

### Siège Amérique

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
États-Unis  
www.cisco.com  
Tél. : 408 526-7660  
Fax : 408 527-883

### Siège Asie/Pacifique

Cisco Systems Australia, Pty., Ltd  
Level 17, 99 Walker Street  
North Sydney  
NSW 2059, Australie  
www.cisco.com  
Tél : +61 2 8448 7100  
Fax : +61 2 9957 4350

**Cisco Systems compte plus de 200 bureaux dans les pays suivants. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site Web [www.cisco.com](http://www.cisco.com) à l'adresse [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Afrique du sud • Allemagne • Arabie Saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie  
Corée • Costa-Rica • Croatie • Danemark • Dubaï • Écosse • Espagne • États-Unis • Finlande • France • Grèce • Hong-Kong • Hongrie  
Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle-Zélande • Norvège • Pays-Bas • Pérou  
Philippines • Pologne • Portugal • Porto Rico • République populaire de Chine • République-tchèque • Roumanie • Royaume-Uni • Russie  
Singapour • Slovaquie • Slovénie • Suède • Suisse • Taïwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. Tous droits réservés. Imprimé aux États-Unis. Cisco, Cisco IOS, Cisco Systems et le logo Cisco Systems sont des marques déposées de Cisco Systems, Inc. ou de ses filiales aux États-Unis ou dans d'autres pays. Tous les autres noms ou marques de fabrique mentionnés dans ce document ou site Web appartiennent à leurs propriétaires respectifs. L'emploi du mot partenaire n'implique pas nécessairement une relation de partenariat entre Cisco et une autre société. (0010R)