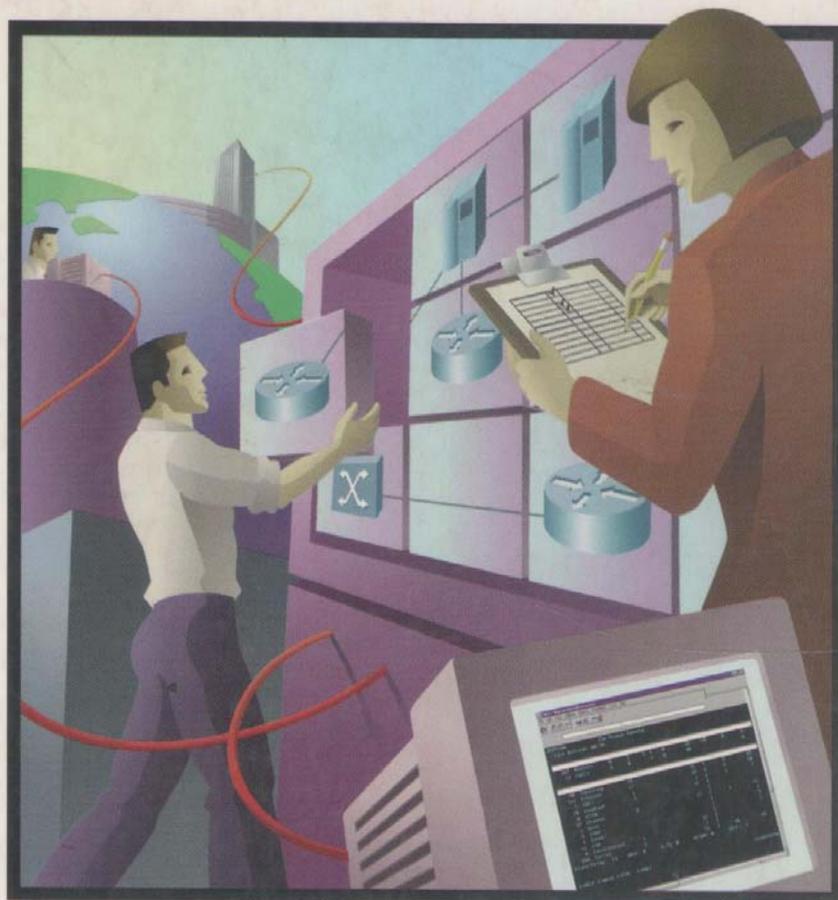


CISCO CERTIFIED INTERNETWORK EXPERT



Documentation agréée pour les candidats à l'examen CCIE

Notions essentielles pour la certification Cisco CCIE

ARCHITECTURE DE RÉSEAUX & ÉTUDES DE CAS

2^e ÉDITION

CISCO SYSTEMS

CISCO PRESS®
www.ciscopress.com

Table des matières

Partie I. Architecture de réseaux

Chapitre 1. Introduction	3
Conception d'un réseau de campus	4
Tendances de conception	5
Conception d'un réseau étendu (WAN)	7
Tendances de conception d'un WAN	8
Conception pour les connexions distantes	9
Tendances de conception des connexions distantes	10
Tendances de l'intégration LAN/WAN	10
Solutions intégrées	11
Définition des exigences de réseau	12
Problèmes de conception : optimisation de la disponibilité et des coûts	12
Résumé	17
Chapitre 2. Notions essentielles sur la conception de réseaux	19
Concepts de base de la mise en œuvre de réseaux	20
Equipements de réseau	20
Introduction à la commutation	21
Identification et choix des fonctionnalités de réseau	23
Identification et choix d'un modèle de conception de réseau	23
Modèle de conception hiérarchique	24
Services du réseau fédérateur	25
Services de distribution	37
Services d'accès locaux	44
Choix des options de fiabilité de réseau	50

Identification et choix des équipements de réseau	57
Avantages des commutateurs (services de niveau 2)	58
Avantages des routeurs (services de niveau 3)	58
Types de commutateurs	60
Comparaison entre commutateurs et routeurs	62
Résumé	66
Chapitre 3. Conception de réseaux IP étendus avec protocoles de routage interne	67
Implémentation des protocoles de routage	67
Topologie de réseau	68
Adressage et synthèse de routage	68
Sélection d'itinéraire	70
Convergence	71
Evolutivité du réseau	72
Sécurité	74
Directives de conception d'un réseau EIGRP	75
Topologie de réseau EIGRP	75
Adressage EIGRP	75
Synthèse de routes EIGRP	76
Sélection de route EIGRP	76
Convergence EIGRP	77
Evolutivité d'un réseau EIGRP	81
Sécurité avec EIGRP	81
Directives de conception d'un réseau OSPF	81
Topologie de réseau OSPF	82
Adressage et synthèse de routes OSPF	84
Sélection de route OSPF	90
Convergence OSPF	91
Evolutivité d'un réseau OSPF	91
Sécurité avec OSPF	92
Fonctionnalités de la zone NSSA de OSPF	92
OSPF On-Demand Circuit	95
OSPF sur les réseaux non broadcast	98
Routage à la demande (ODR, On-Demand Routing)	101
Avantages de ODR	101
Remarques sur l'utilisation de ODR	102
Résumé	102

Elaboration de solutions RNIS	348
Connectivité RNIS	348
Encapsulation de datagrammes	349
Routage DDR	349
Problèmes de sécurité	349
Limitation des coûts	349
Problèmes de connectivité avec RNIS	350
Implémentation d'une interface d'accès de base BRI	350
Implémentation d'une interface d'accès primaire PRI	355
RNIS de bout en bout	358
Problèmes d'encapsulation de datagrammes	360
Sécurité RNIS	363
Evolutivité des réseaux RNIS	365
Nœuds distants virtuels	365
Profils virtuels	367
MultiLink PPP multichâssis (MMP)	367
Limitation des frais d'utilisation de RNIS	370
Analyse de trafic	370
Structure de tarification	371
Formation des utilisateurs	371
Exploitation de SNMP	371
Emploi de l'application CEA (Cisco Enterprise Accounting) pour RNIS	373
Comptabilité AAA	373
Dépannage de RNIS	373
Dépannage de la couche physique	374
Dépannage de la couche liaison de données	376
Dépannage de la couche réseau	378
Résumé	384
Chapitre 12. Conception de réseaux LAN commutés	385
Evolution des réseaux partagés vers des réseaux commutés	385
Technologies de conception de réseaux LAN commutés	387
Rôle de la commutation LAN sur les réseaux de campus	388
Solutions de réseaux commutés	389
Composants du modèle de réseau commuté	390
Plates-formes de commutation évolutives	390
Infrastructure logicielle commune	394
Outils et applications d'administration de réseau	396

Chapitre 4. Conception de réseaux IP étendus avec BGP	103
Fonctionnement de BGP	103
BGP interne (IBGP)	105
BGP externe (EBGP)	107
BGP et cartes de routage	108
Annonces de réseaux	110
Attributs de BGP	113
Attribut de cheminement (AS_path)	113
Attribut d'origine (Origin)	114
Attribut de prochain saut (Next Hop)	114
Attribut de poids (Weight)	117
Attribut de préférence locale (Local Preference)	119
Attribut de préférence d'accès AS (Multi-Exit Discriminator)	121
Attribut de communauté (Community)	123
Critères de sélection de chemin BGP	124
Compréhension et définition des stratégies de routage BGP	125
Distances administratives	125
Filtrage BGP	125
Groupes d'homologues BGP	131
CIDR et agrégats d'adresses	133
Confédérations	134
Réflecteurs de route	136
Contrôle d'instabilité de route (Route Flap Dampening)	138
Résumé	138
Chapitre 5. Conception de réseaux ATM	139
Présentation d'ATM	139
Rôle d'ATM sur les réseaux	140
Couches fonctionnelles ATM	141
Adressage ATM	146
Médias ATM	147
Réseaux multiservices	148
Solutions intégrées	148
Types de commutateurs ATM	149
Commutateurs ATM de groupe de travail et de campus	150
Commutateurs et routeurs ATM d'entreprise	151
Commutateurs d'opérateur	152
Structure d'un réseau ATM	152
Fonctionnement d'un réseau ATM	153

Chapitre 4. Conception de réseaux IP étendus avec BGP	103
Fonctionnement de BGP	103
BGP interne (IBGP)	105
BGP externe (EBGP)	107
BGP et cartes de routage	108
Annonces de réseaux	110
Attributs de BGP	113
Attribut de cheminement (AS_path)	113
Attribut d'origine (Origin)	114
Attribut de prochain saut (Next Hop)	114
Attribut de poids (Weight)	117
Attribut de préférence locale (Local Preference)	119
Attribut de préférence d'accès AS (Multi-Exit Discriminator)	121
Attribut de communauté (Community)	123
Critères de sélection de chemin BGP	124
Compréhension et définition des stratégies de routage BGP	125
Distances administratives	125
Filtrage BGP	125
Groupes d'homologues BGP	131
CIDR et agrégats d'adresses	133
Confédérations	134
Réflecteurs de route	136
Contrôle d'instabilité de route (Route Flap Dampening)	138
Résumé	138
Chapitre 5. Conception de réseaux ATM	139
Présentation d'ATM	139
Rôle d'ATM sur les réseaux	140
Couches fonctionnelles ATM	141
Adressage ATM	146
Médias ATM	147
Réseaux multiservices	148
Solutions intégrées	148
Types de commutateurs ATM	149
Commutateurs ATM de groupe de travail et de campus	150
Commutateurs et routeurs ATM d'entreprise	151
Commutateurs d'opérateur	152
Structure d'un réseau ATM	152
Fonctionnement d'un réseau ATM	153

APPN ou autres méthodes de transport SNA	205
Présentation d'APPN	206
Définition de nœuds	206
Etablissement de sessions APPN	207
Routage intermédiaire de session	208
Utilisation des DLUR/DLUS	209
Implémentation Cisco d'APPN	210
Problèmes d'évolutivité	210
Réduction des mises à jour de bases de données topologiques	211
Réduction des recherches LOCATE	217
Techniques de secours sur un réseau APPN	220
Ligne de secours	220
Redondance totale	221
Prise en charge SSCP	223
APPN dans un environnement multiprotocole	224
Gestion de bande passante et de file d'attente	225
Autres considérations relatives aux environnements multiprotocoles	228
Gestion de réseau	228
Exemples de configuration	230
Configuration d'un réseau APPN simple	230
Configuration d'un réseau APPN avec des stations terminales	233
Configuration d'APPN sur DLSw+	236
Migration d'une sous-zone vers APPN	239
APPN/CIP dans un environnement Sysplex	244
APPN avec FRAS BNN	252
Résumé	256
Chapitre 8. Interréseaux DLSw+	257
Introduction à DLSw+	257
Définition de DLSw+	257
Standard DLSw	258
Fonctionnalités DLSw+	261
Comment procéder	265
Débuter avec DLSw+	266
Configuration minimale requise	266
Token Ring	267
Ethernet	268
SDLC	268
QLLC	270

Fonctionnalités avancées de DLSw+	272
Etablissement de connexion par des homologues DLSw+	273
Equilibrage de charge et redondance	273
Contrôle de la sélection d'homologue	276
Homologues de secours	276
Homologues de secours versus homologues actifs multiples	278
Options d'encapsulation	278
Listes de ports	282
Groupes d'homologues, homologues interzones, homologues à la demande	283
Homologues dynamiques	284
Résumé	288
Chapitre 9. Conception et configuration avec CIP	289
Critères de conception	290
Concentration des fonctions sur un routeur CIP	291
Combinaison du CIP et de SNA	292
CIP en solo	292
Configurations de conception	293
Configurations avec PCA, ESCON et MPC	294
Chargement du microcode du CIP	298
Définition du support CSNA	300
Assignation de CSNA à une adresse de dispositif d'entrée/sortie	300
Définition du LAN virtuel interne	301
Définition du nœud principal VTAM XCA	302
Définition pour le support du serveur TN3270	303
Support de TN3270 Server avec DLUR/DLUS	306
Définition de la fonction CIP CMPC	307
Nœud principal VTAM TRL (Transport Resource List)	307
Définition du nœud principal SNA local	308
Définition des sous-canaux CMPC	308
Définition du groupe de transmission CMPC	309
Exemples de configuration CIP	309
Haute disponibilité en utilisant RSRB et deux routeurs CIP	309
Haute disponibilité et équilibrage de charge au moyen de DLSw+ et de deux routeurs CIP	310
Connectivité CMPC entre deux VTAM sur un seul routeur CIP	311
Commutation de sessions TN3270 avec DLUR/DLUS et la redondance d'hôte VTAM ..	312
VTAM vers nœud de réseau (NN) APPN avec HPR sur CMPC	313

Chapitre 10. Conception de réseaux DDR	315
Introduction au routage DDR	315
Pile de conception DDR	316
Nuage de numérotation	316
Trafic et topologie DDR	317
Topologies	317
Analyse du trafic	319
Interfaces de numérotation	320
Interfaces physiques supportées	320
Groupes de rotation de numérotation	322
Profils de numérotation	322
Méthodes d'encapsulation	323
Adressage de nuage de numérotation	323
Correspondances de numérotation	323
Stratégies de routage	326
Routage statique	326
Routage dynamique	327
Routage Snapshot	329
Secours commuté pour liaisons louées	331
Filtrage d'appel	334
Filtrage par listes ACL	335
Paquets IPX	337
Filtrage AppleTalk	338
Paquets Banyan VINES, DECnet et OSI	340
Routage à la demande et PPP	340
Authentification	341
Authentification PPP	341
Protocole CHAP	341
Protocole PAP	342
Sécurité RNIS	343
Fonction de rappel DDR	343
Listes d'accès IPX	343
Résumé	343
Chapitre 11. Conception de réseaux RNIS	345
Applications de RNIS	346
Routage DDR	346
Liaison de secours par ligne commutée	347
Connectivité SOHO	347
Agrégation de modems	348

Conception de réseaux LAN commutés	396
Modèle hub et routeur	397
Modèle de VLAN de campus	398
MPOA (Mutliprotocol over ATM)	400
Modèle multicouche	401
Augmentation de la bande passante	408
Organisation de la couche centrale	409
Positionnement des serveurs	410
Epine dorsale LANE ATM	411
Multicast IP	413
Problèmes d'évolutivité	415
Stratégies de migration	417
Sécurité dans le modèle multicouche	418
Pontage dans le modèle multicouche	418
Avantages du modèle multicouche	419
Résumé	420
Chapitre 13. Protocole PIM Sparse Mode	421
Modèle d'adhésion explicite	422
Arbres partagés PIM-SM	422
Adhésion à un arbre partagé	423
Elagage d'un arbre partagé	426
Arbres de plus court chemin PIM-SM	428
Adhésion à un arbre SPT	429
Elagage d'un arbre SPT	430
Messages Join/Prune PIM	433
Actualisation d'état PIM-SM (State-Refresh)	434
Enregistrement de source multicast	434
Messages Register PIM	435
Messages Register-Stop PIM	436
Exemple d'enregistrement de source	436
Basculement SPT	439
Exemple de basculement SPT	439
Elagage de source sur l'arbre partagé	441
Routeur DR PIM-SM	443
Rôle du routeur DR	443
Reprise de fonction du routeur DR	443
Découverte de RP	444
Evolutivité de PIM-SM	444
Résumé	445

Etude de cas 2 : conception d'une architecture pare-feu	763
Contrôle du flux de trafic	764
Configuration du routeur pare-feu	765
Définition de listes d'accès de pare-feu	765
Application de listes d'accès sur des interfaces	768
Configuration du serveur de communication pare-feu	769
Définition de listes d'accès sur le serveur de communication	769
Listes d'accès en entrée et usurpation d'adresse (spoofing)	770
Assignation de numéros de ports	771
Suggestions de lectures	774
Livres et périodiques	774
RFC (Requests For Comments)	774
Sites Internet	775
Résumé	775
Chapitre 23. HSRP pour un routage IP avec tolérance aux pannes	777
Fonctionnement de HSRP	780
Configuration de HSRP	781
Configuration de groupes de secours Hot Standby	783
Suivi d'interface	785
Equilibrage de charge	787
Interaction de HSRP avec des protocoles routés	789
AppleTalk, Banyan VINES et Novell IPX	789
DECnet et XNS	789
Résumé	790
Partie III. Annexes	
Annexe A. Segmentation d'un espace d'adresse IP	793
Annexe B. Implémentation de liaisons série IBM	807
Semi-duplex versus duplex	807
Liaisons asynchrones	807
SNA d'IBM	808
ETCD	808
Connexions multipoints	809
Annexe C. Configuration d'hôte SNA pour des réseaux SRB	811
Configuration FEP	811
Définitions de nœud principal commuté par VTAM	815
Exemple de configuration d'un contrôleur de cluster 3174	816

Partie II. Etudes de cas

Chapitre 14. Gestion de réseau commuté	449
Présentation	450
Lectorat de ce chapitre	450
Termes et acronymes employés dans ce chapitre	450
Introduction à l'administration de réseau	452
Présentation technique des équipements Cisco	453
Introduction aux commutateurs	453
Introduction aux routeurs	457
Introduction aux commutateurs de niveau 3	457
Technologies communes aux commutateurs et aux routeurs	457
Protocole d'administration de réseau	459
Protocoles de base	459
Présentation du modèle d'événements	460
Directives d'administration de réseau	464
Conception efficace et armoires de câblage sécurisées	464
Identification des ports jugés "critiques"	465
Mise en place du suivi d'erreurs	466
Collecte de données de référence	467
Valeurs de seuils	469
Recommandations sur les commutateurs Cisco Catalyst	471
Recommandations de conception et de configuration	471
Etat des ressources de commutateur	482
Etat de châssis et d'environnement	486
Etat de modules de commutateur	489
Topologie STP	490
Informations de base de données de transmission de pont	492
Erreurs de port	493
Taux d'utilisation des ports, broadcast, multicast, et unicast	495
Utilisation client	496
Reporting de temps de réponse	497
Variables MIB pour les environnements commutés	497
Autres objets à surveiller	500
Recommandations sur les routeur Cisco	511
Gestion des erreurs	511
Gestion des performances	517

Scénarios de corrélation d'événements de réseau	524
Test d'accessibilité périodique	524
Base de données de topologie logique	525
Base de données de topologie physique	525
Elaboration de la base de référence	525
Personnalisation	525
Scénarios de situations à problèmes	525
Résumé	535
Chapitre 15. Architecture de commutation de paquets	537
Commutation par processus	538
Equilibrage de charge avec la commutation par processus	540
Inconvénients de la commutation par processus	541
Mise en cache avec la commutation rapide	543
Structure du cache rapide	545
Maintenance du cache rapide	548
Equilibrage de charge avec la commutation rapide	550
Commutation optimale	551
Transmission expresse Cisco (CEF)	553
Fonctionnement de la commutation CEF	553
Equilibrage de charge avec la commutation CEF	556
Révision de CEF	558
Résumé	559
Chapitre 16. Redistribution EIGRP et OSPF	561
Configuration de la redistribution mutuelle entre EIGRP et OSPF	561
Exemples de fichiers de configuration	563
Vérification de la redistribution de routes	565
Ajout d'une route dans une liste de redistribution	568
Résumé	569
Chapitre 17. Configuration de EIGRP sur des réseaux Novell et AppleTalk	571
Réseau Novell IPX	571
Configuration d'un réseau Novell IPX	572
Intégration de EIGRP sur un réseau Novell IPX	572
Réseau AppleTalk	582
Configuration d'un réseau AppleTalk	582
Intégration de EIGRP sur un réseau AppleTalk	583
Résumé	585

Chapitre 18. Conception, configuration et dépannage de MPOA	587
Introduction	587
MPOA avec AAL5 (RFC 1483)	588
Circuits virtuels permanents (PVC)	588
Circuits virtuels commutés (SVC)	594
Classical IP sur ATM (RFC 1577)	603
Considérations de conception	604
Topologie	604
Configuration	604
Dépannage	605
Introduction à LANE	609
Considérations de conception	610
Topologie	611
Configuration	611
Dépannage	614
Protocole MPOA (Multiprotocols Over ATM)	623
Considérations de conception	623
Topologie	624
Configuration MPOA	624
Dépannage	626
Résumé	631
Chapitre 19. Routage DDR	633
Configuration du site central pour les appels sortants	634
Configuration d'une interface pour chaque site distant	635
Configuration d'une seule interface pour plusieurs sites distants	638
Configuration de plusieurs interfaces pour plusieurs sites distants	640
Configuration du site central et des sites distants pour les appels entrants et sortants	643
Configuration d'une interface pour chaque site distant	643
Configuration d'une seule interface pour plusieurs sites distants	645
Configuration de plusieurs interfaces pour plusieurs sites distants	648
Configuration des sites distants pour les appels sortants	650
Configuration de plusieurs interfaces pour plusieurs sites distants	651
DDR : la solution de secours pour des liaisons louées	653
Routes statiques flottantes	654
Routes statiques flottantes sur interfaces partagées	656
Liaisons louées et secours commuté	657
Numérotation DTR	657
Numérotation V.25 bis	658

Scripts de dialogue (chat script)	660
Création et implémentation de scripts de dialogue	660
Scripts de dialogue et correspondances de numérotation	660
Résumé	661
Chapitre 20. Evolutivité du routage DDR	663
Conception du réseau	663
Modèles de trafic	664
Choix du média	664
Protocoles requis	664
Solution matérielle	665
Solution logicielle	666
Authentification	666
Adressage de la couche réseau	666
Stratégie de routage	668
Configuration des routeurs d'accès de site central	670
Configuration du nom d'utilisateur pour les sites distants	671
Configuration de la numérotation pour les sites distants	671
Configuration des interfaces de bouclage	672
Configuration des interfaces asynchrones	672
Configuration de l'interface de numérotation	673
Configuration du routage OSPF	674
Configuration du routage RIP	675
Configuration du routage statique	675
Problèmes de sécurité	676
Taille du fichier de configuration	676
Configuration des routeurs de site distant	676
Configuration de scripts de dialogue pour appeler le site central	677
Configuration des interfaces asynchrones	677
Commande site	677
Configuration du routage statique	678
Configuration complète	679
Configuration du routeur CENTRAL-1	679
Configuration de Router 2	681
Réseaux d'entreprise commutés	681
Réseaux de FAI commutés	683
Résumé	684

Chapitre 21. Emploi efficace de RNIS en milieu multiprotocole	685
Configuration de DDR sur RNIS	685
Interface pour RNIS natif	687
Configuration d'une interface RNIS	687
Configuration des numéros d'identification de lignes appelantes	691
Configuration du service de rappel (callback)	692
Configuration du routage Snapshot sur RNIS	694
Evolution du réseau de télétravail	696
Réseau Novell IPX avec routage Snapshot	698
Configuration d'AppleTalk sur RNIS	701
Configuration du routeur A	702
Configuration du routeur B	704
Configuration de IPX sur RNIS	705
Exemple de réseau pour la configuration de IPX sur RNIS	705
Configuration du routeur C2503	706
Explication de la configuration du routeur C2503	707
Configuration du routeur C4000	713
Résumé	714
Chapitre 22. Amélioration de la sécurité sur les réseaux IP	715
Services de sécurité Cisco	717
Evaluation de l'état de la sécurité	717
Contrôle et rétablissement après incident	719
La guerre de l'information a-t-elle lieu ?	720
Menaces de la guerre de l'information	720
Motivations des cyber-pirates	721
Vulnérabilité des réseaux	721
Vulnérabilité de l'authentification CHAP de Cisco	722
Attaques par déni de service avec boucle TCP (land.c)	722
Attaques par déni de service "smurf"	722
Attaques par déni de service vers port de diagnostic UDP	722
Cryptage des mots de passe Cisco IOS	722
Evaluation des besoins en sécurité	723
Stratégies de sécurité	723
Création d'une stratégie de sécurité	725
Documenter et analyser une stratégie de sécurité	726

Approche Cisco de la sécurité	726
Connaître son ennemi	726
Evaluer les coûts	726
Identifier les dangers potentiels	727
Contrôler les informations confidentielles	727
Considérer le facteur humain	727
Connaître les faiblesses du système de sécurité	728
Limiter l'étendue de l'accès	728
Comprendre son environnement	728
Limiter sa confiance	729
Penser à la sécurité physique	729
La sécurité est envahissante	729
Contrôle de l'accès aux routeurs Cisco	729
Accès par console	730
Accès Telnet	731
Accès SNMP	731
Techniques additionnelles de sécurisation d'un routeur	733
Listes de contrôle d'accès	736
Fonctionnement	736
Application de listes d'accès sur un routeur	738
Masque générique	739
Listes de contrôle d'accès standards	740
Listes de contrôle d'accès étendues	741
Listes de contrôle d'accès réflexives	743
Listes de contrôle d'accès dynamiques (sécurité Lock-and-Key)	749
Autres mesures de sécurité Cisco	756
Contrôle de l'accès aux serveurs de réseau hébergeant des fichiers de configuration ..	756
Messages de notification d'utilisations non autorisées	757
Sécurisation de services non standards	757
Sécurité avec niveaux de privilèges	757
Cryptage des données de réseau	758
Etude de cas 1 : authentification de protocole de routage	759
Authentification de routeur voisin OSPF	760
Avantages de l'authentification de voisin OSPF	760
Conditions de déploiement de l'authentification de voisin OSPF	761
Fonctionnement de l'authentification de voisin	761
Authentification en texte clair	761
Authentification MD5	762
Dépannage de OSPF et authentification	762

Annexe D. Configuration d'hôte SNA pour des réseaux SDLC	821
Configuration FEP pour liaisons SDLC	822
Tableau de configuration SDLC pour 3174	824
Annexe E. Diffusions broadcast sur des réseaux commutés	827
Multicast IP	827
Réseaux IP	828
Réseaux Novell	831
Réseaux AppleTalk	832
Réseaux multiprotocoles	834
Annexe F. Réduction du trafic SAP sur les réseaux Novell IPX	835
Listes d'accès de filtrage des mises à jour SAP	837
Site central	837
Sites distants	838
Mises à jour SAP incrémentielles	838
Site central	838
Sites distants	839
Résumé	840
Annexe G. Introduction au transport de la voix en paquets	841
Introduction	842
Codage de la voix	843
Standards de codage de la voix	844
Qualité de compression	846
Délai	846
Options et problèmes du transport de la voix par paquets	848
Réseaux synchrones à circuits commutés	849
Réseaux de trames/cellules	849
Réseaux de données en mode non connecté	850
Réseaux de paquets X.25	850
Réseaux de données privés	851
Signalisation : établissement de la connexion pour la voix	852
Signalisation externe	853
Signalisation interne	854
Applications de la voix par paquets	856
Résumé	857
Annexe H. Références et suggestions de lectures	859
Ouvrages et publications périodiques	859
Publications techniques et standards	862

Annexe I. Présentation de la technologie multicast IP	865
Avantages du multicast	865
Notions élémentaires sur le multicast	867
Adressage	867
Enregistrement dynamique	868
Livraison multicast	868
Routage multicast	868
Processus multicast	869
Exigences du multicast IP sur un réseau d'entreprise	870
Microsoft NetShow et réseau multicast Microsoft	872
Index	875