Routage et acheminement

Pour transférer les données entre des systèmes hôtes d'un réseau, les messages suivent un chemin, souvent appelé circuit virtuel, dans le réseaux. Ils sont relayés, après un stockage temporaire de plus ou moins longue durée, dans les noeuds intermédiaires du réseau : routeurs ou commutateurs de paquets. Ceci met en oeuvre des fonctions complémentaires : routage et acheminement qui s'appuie sur des mécanismes d'adressage.

1.Définitions

ES (End system) Système terminal (synonyme ETTD) système qui émet et reçoit des "messages"

IS (Intermediate System) Système intermédiaire. Noeud de réseau possédant des fonctions de routage et de transmission des messages en provenance des systèmes terminaux.

Appellation : identificateur permanent d'une entité

Adresse réseau : Adresse logique d'un équipement connecté à un réseau. Ce terme peut servir à désigner différents éléments selon le contexte de l'étude. Il convient donc de le préciser.

Adresse de (sous-)réseau ou adresse de point d'attache de sous-réseau : terme qui désigne le point ou un système terminal réel, un réseau réel ou une unité d'interfonctionnement sont attachés à un (sous-)réseau réel.

Adresse NSAP : point d'accès au service réseau (NSAP) où le service réseau est offert à un utilisateur (interface niveau 3/4 de l'OSI). Cette valeur est un paramètre des primitives de connexion, de déconnexion ou de données unitaires (datagramme)

Information d'adresse de protocole de réseau (NPAI) Partie "adresse" de l'Information de commande de protocole (PCI) dans une NPDU.

Il existe une relation entre adresse NSAP et NPAI en ce sens que la sémantique de l'adresse NSAP est préservée par la NPAI

SNPA (Sub Network Point of Attachment) Point d'attachement au sous-réseau : Interface physique entre une machine et le sous-réseau (en quelque sorte la prise).

Routage : fonction traduisant l'appellation d'une entité ou l'adresse SAP(-N) à laquelle l'entité est reliée en un itinéraire permettant d'atteindre l'entité.

Relais(N) : Fonction (N) au moyen de laquelle une entité (N) retransmet des PDU(-N) d'une entité correspondante (N) à une autre entité correspondante (N)

Acheminement : Action de conduire un message à une destination prévue à l'avance.

2.Introduction

Les réseaux d'entreprise sont souvent réalisés par une interconnexion de réseaux locaux ou étendus privés ou publics. Dans ces réseaux la couche 3/OSI est décomposée en plusieurs sous-couches :

SNAP, Sub Network Access Protocol, qui traite de l'accès au réseau. Le protocole X25, supportant les réseaux de paquets en circuit virtuel commuté peut entrer dans cette catégorie.

SNDCP Sub Network Dependent Convergence Protocole qui traite les sous-réseaux de base. Ce peut être un réseau utilisant le protocole IP et géré, du point de vue routage, de manière homogène et connue de son administrateur (un seul protocole routé, dans un domaine de routage). Ce peut être aussi un réseau en commutation de paquets X25.

SNICP Sub Network Independent Convergence Protocol qui traite l'interconnexion de ces sous-réseaux de base, par exemple couche IP/ISO ou IP. Ce type de réseau est souvent multiprotocole (IP, IPX, etc.) et possède un grand nombre de domaine de routage.

Dans ce cas les mécanismes de routages et d'acheminement doivent être considérés au deux niveaux SNDCP et SNICP.

Ces mécanismes constituent un des facteurs fondamentaux pour obtenir les meilleures performances d'un réseau. Ils doivent être pris en compte dès la phase de conception, lorsque la topologie du réseau a été déterminée. On choisit alors un routage optimal pour lequel le réseau sera calculé. L'optimisation de ce routage consiste essentiellement a minimiser le nombre d'étapes moyen.

En phase d'exploitation, le réseau étant complètement déterminé, l'optimisation en fonction de la topologie, du trafic et des facteurs de coûts, permet d'obtenir les performances les meilleures.

Un grand nombre d'étude théoriques ont été menées sur ce problème et diverses techniques ont été proposées. seules les plus simples d'entre elles semblent jusqu'ici utilisées. cependant depuis quelques années, l'optimisation des performances (ou des coûts d'exploitation)

est devenue un objectif de l'administration de réseaux (on ne se contente plus d'un fonctionnement correct...). Des techniques adaptatives seront de plus en plus utilisées.

Depuis quelques années une normalisation se met en place.

ISO9542 (1988) pour l'échange d'information de routage entre ES et IS sur un réseau sans connexion (ISO8473 = IP)

ISO10030(12-1190) pour l'échange d'information de routage entre ES et IS sur un réseau en mode connecté (ISO8878 = X25)

ISO10589 (10-1990) pour l'échange d'information de routage entre IS sur un réseau en mode non connecté

Nous allons examiner successivement les problèmes à résoudre, les différentes méthodes de routage, la normalisation OSI et la mise en oeuvre du routage sur différents types de réseaux.

Par ailleurs sur Internet, un certain nombre de protocoles se sont imposés comme des standards de fait. Par exemple RIP (Routing Information Protocol) est installé sur tous les systèmes utilisant IP, en mode actif sur les routeurs et en mode passif sur les stations de travail (démon routed). Des protocoles "propriétaires" sont aussi très souvent utilisés.

3.Expression des besoins

Pour transférer un "message" à travers un réseau, il est nécessaire de déterminer quel itinéraire il va suivre (fonction routage), puis à chaque noeud du réseau d'aiguiller et de retransmettre ce message sur une liaison de données convenable (fonction acheminement).

Le calcul du routage nécessite de connaître la topologie du réseau et selon le niveau d'optimisation recherché, une estimation du trafic à acheminer et une expression des coûts respectifs des chemins possibles.

Si la topologie et les coûts ne subissent que de rares modifications, à des intervalles de temps de plusieurs mois, la prise en compte peut être faite en temps quasi réel. Cette prise en compte va conduire à des solutions très différentes.

Les modifications topologiques par suite de panne doivent aussi être prises en compte dans un délai très bref mais elles ont pu être prévues à l'avance et ne nécessitent, après que cette modification topologique a été signalée) qu'une modification de l'acheminement (routage alternatif).

Le résultat du calcul des routes est traduit dans des tables de routage qui sont transmises aux noeuds du réseau à partie d'une table globale (routage centralisé) ou élaborées

localement à chaque noeud (routage distribué). Dans chaque noeud relais, l'acheminement est traité à partir

- des adresses de réseau (NPAI)
- de la table de routage locale

En effet les normes OSI précisent qu'il n'est pas possible de déduire l'acheminement de la seule analyse des adresses, même si la structure de celles-ci peut faciliter le calcul des tables de routage.

Dans les systèmes transportant des NPDU unitaires (datagrammes), ceux-ci sont indépendants et chaque PDU de données porte l'adresse de destination et la route peut être différente pour chacune.

Dans les systèmes en mode connecté les NPDU d'une connexion suivent le même itinéraire, le circuit virtuel, qui est établit durant la phase d'appel. Les PDU de données portent une adresse temporaire plus courte (NVL : Numéro de voie logique) que l'adresse absolue de destination. Cette route reste fixe pendant toute la durée de connexion. Elle peut être différente d'une connexion à la suivante pour un même couple appelant-appelé.

L'examen de ces besoins montre que le problème essentiel réside dans l'élaboration des tables de routage de chaque noeud.

4.Algorithmes de routage

4.1.Types de routage

Fixe	-déterministe -avec alternative -aléatoire -par inondation
Adaptatif	- centralisé - distribué - à contrôle local - par domaine

Les routages fixes utilisent des algorithmes qui ne tiennent pas compte des fluctuations du trafic (sauf certains routages fixes avec alternative).

Un routage fixe peut être déterminé "manuellement" et chargé sur un routeur. On parle alors de "routes statiques". S'il peut être modifié automatiquement en fonction des modifications de l'état du réseau (liens ou noeuds en défaut par exemple) on parle de "routes dynamiques".

Un routage fixe déterministe est utilisé en phase de conception pour spécifier les caractéristiques des différentes liaisons. Il tient compte essentiellement de la topologie et minimise le nombre d'étapes moyen. En cas de chemin équivalents selon ce critère, un critère d'optimisation secondaire: concentration du trafic sur les noeuds les plus importants (critère de performance) ou équilibrage du trafic entre les noeuds (critère de sécurité) sera pris en compte. Ces critères étant fixés on peut calculer le réseau optimal correspondant. Toute modification du routage pour la même répartition de trafic ne peut qu'entraîner une dégradation des performances.

En cas de défaillance d'un noeud ou d'une liaison, il a modification de la topologie du réseau et une autre table de routage optimale peut être déterminée. On obtient ainsi des alternatives à la table de base.

Les routages aléatoires ou par inondation peuvent sembler une solution très mauvaise au vu des performances très médiocres qu'ils entraînent. Ils ont toutefois leur utilité

- soit pour les réseaux peu fiables
  réseaux militaires
  réseaux radio
- soit pour mettre à jour les tables de routage des réseaux classiques.

Le routage aléatoire consiste à acheminer un message reçu à un noeud K vers un des noeuds voisins (connecté) désigné au hasard. de proche en proche, le message atteint sa destination quelque soit la topologie actuelle du réseau (sauf si le noeud chargé de l'acheminement tombe en panne à cet instant ...)

Le routage par inondation consiste à acheminer un message reçu à un noeud K vers tous les noeuds voisins connectés (sauf éventuellement le noeud précédent). Dans chaque relais traversé, le passage d'un message est noté pour éviter de renvoyer un second fois ce message. On peut aussi dater les messages et les extraire après un certain délais.

4.1.1.Routage adaptatif centralisé

Dans ce type de routage, les itinéraires s'adaptent aux modifications topologiques du réseau et surtout aux fluctuations du trafic. Il nécessite donc de connaître à tout instant l'état du réseau. Ceci entraîne la transmission à travers le réseau, depuis chaque noeud, de messages indiquant la charge de ces noeuds, donc un accroissement du trafic (en particulier dans des périodes où il est déjà trop élevé). Ces messages sont collectés par un noeud central d'administration qui calcule les nouvelles routes et transmet à chaque noeud sa table de routage avec une heure de prise d'effet

4.1.2.Routage adaptatif distribué

Chaque noeud reçoit les messages indiquant l'état des autres noeuds et calcule sa tacle d'acheminement optimal. Le nombre de messages d'état peut être supérieur au cas précédent mais cette technique évite la transmission des tables de routage

4.1.3.Routage adaptatif local

Chaque noeud établit sa table d'acheminement en fonction de sa propre observation du trafic. Il n'y a plus de messages de routage à travers le réseau mais il n'y a aucune assurance que les décisions locales convergent vers une optimisation globale. On peut aussi observer des fluctuations (pompage) de fonctionnement.

Avec un routage non centralisé, les modifications d'acheminement ne sont pas synchronisée, et il est difficile d'assurer une optimisation globale du réseau. seules des simulations permettent de juger de la qualité des algorithmes utilisés.

4.1.4.Routage distribué par région (domaine)

Les grands réseaux peuvent être découpés hiérarchiquement en domaine (et sous-domaines)

Les noeuds de niveau 1 ne sont habilités à router les messages qu'au sein de leur domaine. Ils n'ont aucune connaissance topologique sur les autres régions (si ce n'est l'appartenance d'un noeud à une région et le ou les noeuds de sortie de son domaine vers les autres domaines).

Les noeuds de niveau 2 ont une vision plus globale du réseau. Ils ne connaissent pas la topologie exacte des autres domaines mais la topologie du réseau (partiel) constitué ,par les noeud frontières.

A chaque niveau (intra ou inter domaine) les noeuds s'envoient les informations de routage par un mécanisme d'inondation mais à un rythme bien plus faible pour le niveau 2 (interrégion).

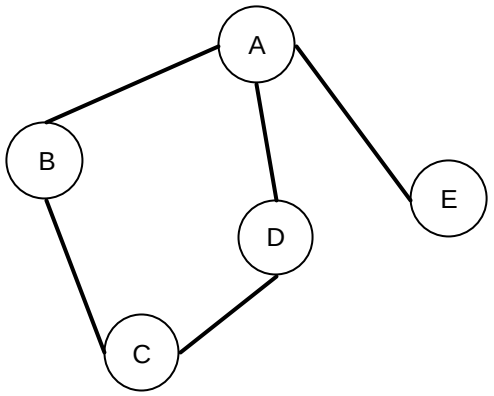
5.Tables de routage

Le résultat du calcul des routes est consigné dans les tables de routage. Pour un routage centralisé une table complète, décrivant l'ensemble des itinéraires, est créé au Centre de Gestion du réseau. Des parties de cette table sont transmises aux différents noeuds. Pour un routage distribué, les tables partielles sont élaborées dans chaque noeud.

Dans ces tables on indique pour chaque destination le **prochain noeud** à atteindre (noeud voisin).

5.1.Exemple :

On étudie le réseau suivant :



5.1.1.Table complète pour un routage fixe

Destination Source	A	B	C	D	E
A	A	B	B	D	E
B	A	B	C	C	A
C	B	B	C	D	D
D	A	C	C	D	A
E	A	A	A	A	E

5.1.2.Table complète pour routage avec alternatives

Destination Source	A	B	C	D	E
A	A	B	B,D	D	E
B	A	B	C,A	C	A
C	B,D	B	C	D,B	D
D	A	C,A	C	D	A
E	A	A	A	A	E

5.1.3.Tables pour le noeud C

Routage fixe

Destination	A	B	C	D	E
	B	B	C	D	D

Routage avec alternatives

Destination	A	B	C	D	E
	B,D	B	C	D,B	D

6.Comparaison des méthodes

La comparaison des méthodes de routage est difficile car les performances observées dépendent d'un grand nombre de facteurs souvent mal maîtrisés.

Kleinrock et son équipe, en particulier, ont montré , par simulation, quelques propriétés générales.

En phase de conception,

- il est souhaitable de minimiser le nombre moyen d'étapes.

- si pour aller d'un noeud j à un noeud k, il y a deux chemins possibles de même longueur l_{jk} , le temps de transit moyen sera toujours réduit si **on ne garde qu'un seul** de ces chemins.

- si le réseau a été optimisé pour un routage donné, ce routage fixe est préférable à tout système de routage avec alternative. Plus la table de routage présente d'alternatives, moins le routage est performant. (accroissement du nombre d'étapes moyen).

- si le réseau n'a pas été conçu de manière optimale, par exemple avec des liaisons toutes identiques ou proportionnelles au trafic circulant, des chemins avec des alternatives limitées améliorent les performances. trop d'alternatives peuvent les dégrader.

- si à un noeud j on dispose de M canaux C_i possibles pour atteindre un noeud k et si les capacités de ces canaux sont telles que $C_1 > C_2 > C_3 > \ldots > C_M$, on peut déterminer à quelle condition un message en position q_i dans la file d'attente doit emprunter le canal C_i ou attendre qu'un canal plus performant soit libéré. La règle suivante améliore le routage :

$$q_i < \frac{\sum_{j=i}^{i-1} C_j}{C_i} \leq q_i \quad \text{avec } q_1 = 1$$

Pour un réseau existant,

- L'introduction de chemins alternatifs peut compenser l'écart entre le réseau réel existant et sa version optimisée lors de sa conception, écart du à une variation du trafic par rapport au trafic prévu.

- L'introduction de chemins alternatifs utilisés uniquement en cas de panne sur les chemins de base assure la sécurité du réseau.

Routage aléatoire ou par inondation,

Ce type de routage peut multiplier par 10 ou plus le temps de transit moyen sur un réseau comme le montre le tableau ci-dessous (ρ est le facteur d'utilisation moyen du réseau). Les

valeurs sont obtenues par simulation sur un réseau à 13 noeuds où chaque noeud est connecté à 4 autres noeuds (réseau 4-connecté)

ρ	1/128	1/64	1/32	1/16	1/8	0.25	0.5
Fixe	87,5	88,4	93,7	102	120	170	580
Aléatoire	728	731	774	1803	∞	∞	∞

Nous observons que lorsque ρ reste inférieur à quelques % le temps de transit moyen reste stable quoique très élevé. La saturation commence pour un facteur d'utilisation de 5 % environ contre 50 % pour une procédure fixe. Le nombre d'étapes moyen est passé de 1,67 à 14 !

Ce type de procédure n'est donc utile que dans des applications particulières :

- réseaux peu fiables : réseaux radio, réseaux militaires

- **diffusion des informations de routage**. Dans ce cas les informations clientes du réseau sont transmises par un routage adaptatif.

7.Calcul du chemin le plus court

Les informations nécessaires au calcul du routage étant connues soit à un noeud central soit localement, il convient de calculer le chemin optimal.

- A chaque lien est affectée une métrique (un coût). La distance d'un noeud à la destination finale est la somme des "longueurs" des liens constituant le chemin.

- Plusieurs types d'algorithmes permettent d'effectuer ce calcul (Dijkstra, Pape, Déviation de flux (Gerla), etc.)

Nous devons donc choisir une métrique puis un algorithme d'optimisation.

7.1.Métriques

Une métrique de coût prend en compte le coût de fonctionnement d'une liaison pour le calcul du chemin optimal.

Une métrique de performance minimise seulement de délai de transmission moyen d'un paquet sur un intervalle de temps donné grâce à la mesure directe de la disponibilité des ressources indispensables à la transmission: nombre de circuits disponibles, débits, nombre de buffers, temps de calcul...

Les deux métriques peuvent être utilisées conjointement : chemin de coût minima parmi les plus performants ou chemin le plus performant parmi les moins coûteux.

Ce système founit un **"vecteur distance"** donnant, pour chaque routeur, la "distance" à tous les autres. Ces distances peuvent indiquer simplement le nombre d'étapes (distance 1 entre noeuds voisin) ou tenir compte des caractéristiques les liens.

7.2.Algorithme

L'algorithme décrit ci-dessous est l'un des plus simples utilisables. Il est donné à titre indicatif pour illustrer le problème à traiter.

7.2.1.Algorithme du plus court chemin

Nota : Cet algorithme n'est pas adapté à déterminer rapidement le plus court chemin si le critère de distance est le nombre de noeuds traversés. Un algorithme utilisant les élévations à la puissance k (k allant de 1 à k_{max}) de la matrice de connexion pour trouver les chemins de k étapes est plus efficace.

Initialisation :

N_i = noeud courant
N_a = noeud de départ

L'algorithme s'applique en prenant successivement les noeuds du réseau comme noeuds de départ.

A chaque noeud on assigne un couple de valeurs (noeud, distance)

Le noeud indiqué est le prochain noeud sur le chemin le plus court. S'il n'est pas encore connu il est noté : ✹. La distance notée d_i est la distance au noeud origine par le plus court chemin connu. Si elle n'est pas déterminée est vaut l'infini : ∞ pour tous les noeuds sauf le noeud de départ pour lequel elle vaut 0.

l(i,j) désigne la distance entre les noeuds N_i et N_j.

à l'état initial $d_a = 0$, $d_i = \infty$ si $a \neq i$ couple = (✹, d_i)

Plus courte distance :

Méthode par balayage

On recherche pour tout couple i,j une branche i,j telle que

$$d_i + l(i,j) < d_j$$

On associe au noeud N_j le couple (N_i, $d_i + l(i,j)$)

On dispose alors pour chaque noeud de la plus courte distance au noeud source N_a et le noeud voisin le plus proche.

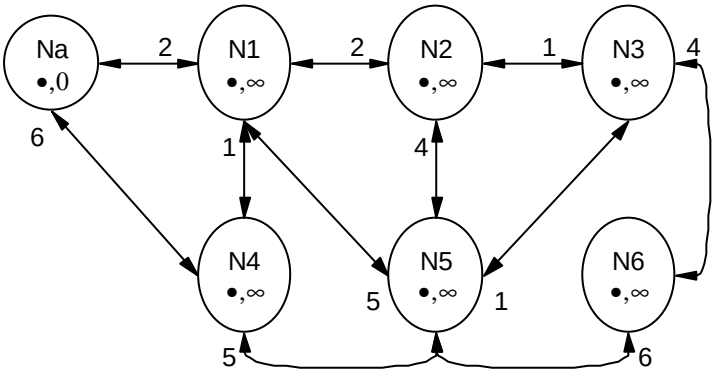
Chemin le plus court pour le noeud N_b :

1) faire i = b
2) identifier N_k par le couple (N_k , d_b) associé à N_b
Si N_k n'existe pas, il n'y a pas de chemin liant N_a à N_b.
3) faire = = k si i = a Fin
sinon retourner à 2)

Cet algorithme donne tous les noeuds intermédiaires entre N_a et N_b par le chemin le plus court.

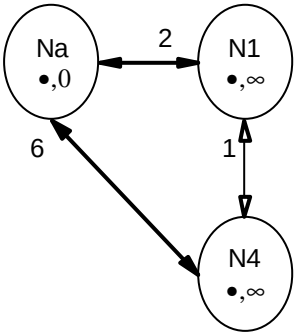
7.2.2.Exemple :

On considère le réseau ci-dessous vu du noeud initial Na à partir duquel on calcule les chemins les plus coûts vers 6 autre noeuds Ni.



Les "distances" entre noeuds sont indiquées sur le graphe initial ci-contre. Par exemple la distance l(3,6) entre les noeuds N3 et N6 vaut 4.

On détermine successivement le chemin le plus court depuis les différents noeuds.



Pour le noeud N4 :

$d(4) = \infty > d(a) + l(a,4) = 0 + 6 = 6$
N4 ($\bullet$, ∞) $\rightarrow$ N4(a,6)

Pour le noeud N1 :

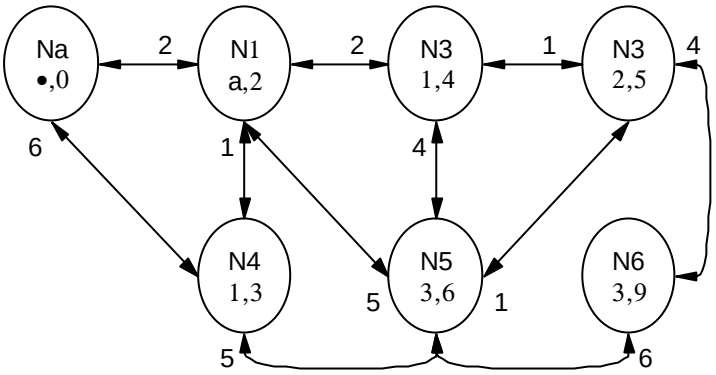
$d(1) = \infty > d(a) + l(a,1) = 0 + 2 = 2$
N1 ($\bullet$, ∞) $\rightarrow$ N1(a,2)

On revient au noeud N4

$d(4) = 6 > d(1) + l(1,4) = 2 + 1 = 3$

N4 (a,6) $\rightarrow$ N4(1,3)

On poursuit l'algorithme pour tous les noeuds et on obtient le graphe ci- dessous :



Le chemin de N5 à Na passe par N3 . Il a une distance 6.

{N5 (3,6) }

Il est établi par

N5(3,6) → N3(2,5) → N2(1,4)
→ N1(a,2) → Na(•,0)

Soit b = 5 → 3 → 2 → 1 → a. Sa distance est 6.

8.Normalisation

8.1.ISO9542

Echange d'information de routage entre ES et IS ou IS et ES sur un réseau sans connexion.

- pour permettre aux ES de trouver les IS permettant de relayer les NPDU vers d'autres sous-réseaux

- pour permettre aux ES de trouver d'autres ES sur le même sous-réseau si l'adresse du NSAP destinataire est insuffisante.

-pour permettre aux IS de connaître l'existence des ES situés sur chaque sous-réseau auquel ils sont connectés

-pour permettre aux ES quel IS utiliser quand plusieurs IS sont possibles.

Le protocole garantit que le routage à un Point d'attachement de sous-réseau (SNPA) du sous-réseau est supporté par le sous-réseau lui-même mais celui-ci n'est pas capable de le faire sur la seule base des adresses NSAP. Il fournit aussi des fonctions de diffusion totale (Broadcast) ou partielle (Multicast).

Ce protocole doit aussi minimiser

-l'échange d'informations à entrer dans chaque ES avant qu'il puisse commencer à communiquer

- la taille mémoire nécessaire au routage
- la complexité de calcul de l'algorithme de routage.

Il spécifie

- les procédures de transmission d'information de configuration et de routage entre ES et IS

- Le codage des PDU- les procédures nécessaires à l'interprétation correcte des PCI

Le protocole 9542 fournit deux types d'information

- informations de configuration

Elles permettent

- aux ES et IS de découvrir dynamiquement leurs existences réciproques et leur disponibilité (signalisation de présence et de disponibilité)

- aux ES d'obtenir des informations sur d'autres ES en l'absence d'IS disponible

- Informations de redirection (reroutage)

qui permettent aux IS d'indiquer aux ES des routes potentiellement meilleures pour expédier une NPDU à une destination particulière.

Les adresses utilisées sont les adresses de NSAP données dans le protocole OSI 8348/add2 : service sans connexion IP/ISO

8.2.ISO10030

Protocole d'échange d'information pour le routage pour les systèmes d'extrémité utilisant un service réseau connecté en commutation de paquet ISO8878 (X25)

Ce protocole apporte des solutions aux problèmes suivants :

Comment les ES découvrent les IS pouvant router des NPDU à des destinations situées sur d'autres sous-réseaux

Comment les ES découvrent d'autres ES sur le même sous-réseau (quand la connaissance de l'adresse de NSAP ne donne pas d'information sur l'adresse de sous-réseau du système destinataire

Comment une entité de résolution des adresse de sous-réseau : SNARE (Subnetwork adress resolution entity) découvre les ES de son sous-réseau.

Ce protocole garantit que le routage à un SNPA du sous-réseau est supporté par le sous-réseau lui-même

Mais le sous-réseau n'est pas capable de router sur la seule base des adresses de NSAP. Les ES utilisant ce protocole doivent connaître l'adresse d'au moins un SNPA permettant d'atteindre un SNARE.

Ce protocole doit minimiser

- l'information à entrer à priori dans chaque ES avant qu'il puisse commencer à communiquer

- dans les ES la mémoire nécessaire au routage et la complexité de calcul des algorithmes de routage

Ce protocole est un complément du protocole ISO9542 pour les environnements sans diffusion (pour la partie configuration) et pour les environnements avec diffusion totale pour lesquels le sous-ensemble redirection n'est pas valable (pour la partie redirection)

8.2.1.Vue générale

Ce protocole comporte deux sous-ensembles :

- Information de Configuration
- Information de Redirection

Il s'articule autour de la fonction **SNARE**

Un SNARE est un fournisseur d'information de routage pour un seul sous-réseau. Il doit aussi communiquer avec des IS mais ceci n'est pas pris en compte par le protocole ISO 10030. La fonction SNARE est supportée par un ou plusieurs Es ou IS du sous-réseau. Dans un sous-réseau X25, il est possible que les opérations de SNARE soient supportées par le sous-réseau lui-même.

Information de configuration

Ce sont des informations sur les ES et les IS attachés à un sous-réseau en termes de types de système, Adresses Réseau présentes, Nom d'Entités Réseau (NET) présents, correspondances entre systèmes, adresse SNPA et routes potentielles.

Les ES communiquent leur adresse réseau (NA) à un SNARE

Les ES découvrent (pour certaines NA éloignées) les adresses SNPA du système du sous-réseau (IS) par lesquelles la communication pourrait être acheminée.

Pour réaliser ceci une ES établit une connexion X25 vers un SNARE par une demande d'appel. Dans ce paquet d'appel, le premier octet des données utilisateur contient un

identificateur de protocole spécifique. Si le SNARE accepte l'appel, l'ES peut alors lui transmettre des détails sur ses Adresses Réseau puis lui envoyer une PDU "information complète". L'ES peut aussi demander une information sur les NA éloignées. La SNARE envoie alors l'information correspondante, les SNPA par lesquelles celles-ci peuvent être atteintes et la qualité de service (QoS) associée. L'ES libère alors la connexion

Ainsi les ES présents se signalent dynamiquement les unes aux autres (et aux SNARE) : on obtient ainsi la configuration du sous-réseau sans intervention manuelle d'un opérateur dans chaque entité du réseau

Informations de redirection

Cette fonction comporte deux parties

La première est utilisée lorsqu'un ES veut établir une connexion de réseau (X25) mais ne dispose pas des informations nécessaires pour déterminer l'adresse appropriée de sous-réseau. Dans ce cas, l'ES s'adresse au SNARE par une demande d'appel (X25) à celui-ci.

Si le SNARE est un ES ou un IS attaché au sous-réseau il peut

- utiliser la facilité de réacheminement d'appel pour rerouter l'appel vers un ES ou IS approprié

- libérer l'appel en indiquant le SNPA approprié qui doit être utilisé dans l'avenir

- s'il contient une fonction relais, accepter l'appel et acheminer celui-ci.

Si la fonction SNARE est intégrée au sous-réseau elle peut utiliser des moyens spécifiques pour appeler le SNPA approprié.

L'établissement de connexion de l'ES d'origine peut alors se poursuivre normalement si une libération n'a pas été émise.

La Réception d'une indication de libération provoque la mise en oeuvre de la seconde partie. Les champs cause et diagnostic du paquet de libération montre quel celle-ci n'a pas été initié par l'Utilisateur du service Réseau. L'ES appelante recherche dans les données utilisateurs un PDU d'information du protocol 10030 indiquant une adresse de sous-réseau appropriée par laquelle une connexion équivalente à celle qui vient d'être rejetée peut établie (mêmes NSAP avec même qualité de service). l'ES peut alors utiliser ces informations pour ses futurs appels.

En résumé cette fonction permet d'établir un appel vers un équipement d'un sous-réseau dont on ne connaît pas l'adresse complète directement par l'intermédiaire d'un SNARE ou grâce aux informations fournies par celui-ci.

Un ES peut supporter soit la fonction "information de configuration", soit la fonction "information de redirection" soit les deux fonctions.

8.2.2.Adresse sous-réseau d'un SNARE

Chaque Es doit connaître au moins une adresse de réseau à laquelle un SNARE peut être joint. Certaines méthodes spécifiques pour cela peuvent être utilisées si les ES sont connectés à un réseau local utilisant un protocole ISO 8802.2 de type LLC1 à l'aide de mécanismes de diffusion totale (Broadcast).

8.2.3.PDU utilisés

Structure

Ils sont composés d'une en-tête sur 3 octets et éventuellement d'un champ de données portant des paramètres.

L'en-tête a la composition suivante

identificateur de protocole
numéro de version
type du PDU

Les paramètres d'adresse comportent
un champ longueur
un champ valeur
(l'adresse SNPA a aussi un champ type sur 2 bits)

Les autres paramètres ont une structure TLV : type-longueur-valeur

Types de PDU

Emis pas les ES

ECQ :End System Configuration Query	code : 1	hexa
ENC : End System Notification Complete	: 2	
ESC : End System Connect		: 3
ESH : Ens System Hello	: 4	
SRH : SNARE Request Hello	: 11	

Emis par les SNARE

RD : Redirect	: 8
SCC : SNARE Configuration Complete	: 9

SCR : SNARE Configuration Response : A
SNC : SNARE Notification Complete : B
SRN : SNARE Received Notification : C
SHL : SNARE Hello : 10

Paramètres :

Adresse réseau

Sa longueur est codée sur un octet. Elle suit les règles définies dans OSI8348/add2

Adresse SNPA

Elle spécifie une adresse qui peut être utilisée pour atteindre l'adresse réseau requise.

Dans le premier octet 2 bits de type indiquent le type de codage (normalisé ou local). Les 6 autres bis donnent la longueur de l'adresse qui peut être codée sous d'une suite d'octets (adresse MAC de réseau local ou adresse codée en AI5) ou sous forme de demi-octets pour une adresse codée en décimal. dans ce cas le dernier octets est éventuellement complété par 1111.

Masque d'adresse (champ optionnel)

Ce champ indique que les informations d'expédition fournies par la PDU s'applique à une plus large population d'adresses réseau que celle associée à la SCR PDU ou la RD PDU. Ce paramètre crée une classe d'équivalence d'adresses réseau pour laquelle d'applique les mêmes règles d'expédition.

Masque SNPA (Paramètre optionnel)

Si ce paramètre est présent, la classe d'équivalence définie par le masque d'adresse a aussi une structure commune dans la partie du masque d'adresse à 0. Le masque SNPA fournit des indications sue ce champ, en particulier la position de l'adresse SNPA dans l'adresse réseau.

Qualité de service
- Débit (maximal et minimal)
- Délai de transit (maximal et minimal)
- Priorités (maximale et minimale)
  - pour obtenir une connexion
  - garder une connexion
  - transmettre des données
- Protection (niveaux maximal et minimal)

Temps de maintien (durée de validité des données émises)

Temps de rétention (durée de validité des données dans une SRH PDU)

Limite de recherche (permission pour un ES de demander de nouvelles informations de configuration)

Temps d'appel (intervalle de temps permis entre 2 requêtes à un SNARE)

Notification demandée (intervalle de temps suggéré pour envoyer la notification)

8.2.4.Eléments de procédure

Etablissement de connexion

Un ES établit une connexion vers un SNARE par une demande d'appel X25 contenant une ESC PDU dans les données utilisateurs. Le champ de facilité "Sélection rapide sans restriction" (unrestricted Fast Select) doit être utilisé et pas de bit Q.

Si le SNARE peut accepter l'appel, il envoie un Appel accepté contenant une SNC PDU dans les données utilisateur (avec paramètre "temps d'appel").

La communication est alors établie. Les informations nécessaires sont alors échangées dans une séquence complète de paquets de données X25.

Notification de configuration

l'ES transmet au SNARE une ESH PDU pour chaque adresse réseau accessible à travers son SNPA (paramètres adresse réseau et qualité de service). Il termine cette séquence par une ENC PDU.

Le SNARE acquitte ces informations par une SRN PDU (paramètre "Notification demandée")

La connexion peut alors être libérée.

Collecte de configuration

L'ES demande des informations à un SNARE par l'envoi d'une ESC PDU (paramètre "Adresse réseau").

Le SNARE répond par des SCR PDU (pour chaque SNPA pouvant être utilisée) contenant les paramètres suivants : temps de maintien, adresse réseau, adresse SNPA (qui permet d'atteindre l'adresse demandée), masque d'adresse, masque SNPA, qualité de service.

Le SNARE termine la collecte par le transfert d'une SCC PDU (paramètres : adresse réseau, limite demandée)

La communication peut alors être libérée.

Invocation de redirection

Un ES qui ne connaît pas l'adresse réseau d'un système appelé peut utiliser le mécanisme de redirection.

Pour cela il établit une connexion X25 vers un SNARE avec le champ de facilité "Extension d'adresse" contenant l'adresse NSAP du système à atteindre.

Si le SNARE peut relayer l'appel (par son relais local) il achemine celui-ci et la connexion est établie par son intermédiaire.

Il peut aussi rerouter l'appel vers un autre SNARE susceptible d'établir la communication.

Il peut enfin libérer l'appel (code 0 diagnostic 230) en plaçant une RD PDU dans le champ de données utilisateur du paquet de libération.

Cette RD PDU contient en paramètre un temps de maintien, une adresse SNPA permettant d'atteindre la destination souhaitée, un masque d'adresse et un masque SNPA.

Utilisation d'un réseau local
avec service de liaison de données de type LLC1

Sur un réseau local fournissant des fonctions de diffusion partielle et totale, les ES peuvent découvrir un SNARE permettant de découvrir des adresses SNPA de SNARE.

Pour cela un SNARE peut envoyer dans une trame en diffusion une SHL PDU contenant une "notification demandée" et un "temps de rétention" lui permettant de connaître d'adresse SNPA du SNARE.

Un ES qui n'a pas reçu de SHL PDU peut en solliciter un en envoyant une trame contenant une SRH PDU en diffusion partielle avec comme adresse "tous les SNARE x25".

8.3.ISO10589

Protocole intra-domaine de routage d'un système intermédiaire à un système intermédiaire utilisable avec un protocole de réseau en mode non connecté (IP/ISO 8473)

Ce protocole est utilisé dans les réseaux très étendus ayant une organisation hiérarchique. Les domaines sont divisés en régions gérées par un centre de gestion de routage. A l'intérieur d'une région le routage est de niveau 1. Entre deux régions il est de niveau 2. Les IS de niveau 1 relayent les messages des ES de leur région soit dans la région soit vers un IS de niveau 2 pour les ES d'une autre région.

9.Routage sur le réseau Transpac

Le routage de Transpac est adaptatif. Il s'adapte dynamiquement aux modifications éventuelles de l'état du réseau : panne ou surcharge très importante sur une artère ou sur un commutateur. Pour cela les commutateurs surveillent leur environnement local et le compare à des seuils préenrégistrés. Lors d'un dépassement de seuil un nouvel itinéraire est choisi. Le retour au dessous d'un seuil inférieur (hystérésis) ramène au chemin initial.

Dans une première version l'algorithme de routage était centralisé : des messages étaient créés à la suite des dépassements de seuils et transmis à un Centre de Gestion du Réseau qui analysait l'état global du réseau et calculait éventuellement de nouvelles routes. Les nouvelles tables de routage étaient transmises à tous les noeuds concernés et pris en compte pour les nouveaux appels. En cas de panne du Centre de Gestion et du Centre de Secours, les décisions étaient purement locales.

Ce système présente des limitations, en particulier avec l'extension du réseau et la mise en place de nouveaux commutateurs. En 1984, il a été remplacé par un algorithme distribué sur l'ensemble des commutateurs.

Chaque commutateur est autonome et détermine son routage en fonction de l'état de son environnement local et de l'état de l'ensemble du réseau dont il est informé par ses voisins et un mécanisme de propagation de proche en proche de l'état de chaque commutateur.

Lorsque les itinéraires doivent emprunter des "liaisons périphériques" (réseaux extérieures, par exemple partie du réseau téléphonique) particulières, un algorithme particulier est mis en oeuvre pour tenir compte du coût de ces liaisons (par exemple en fonction de la distance). En cas de panne ou de surcharge de ces liaisons leur "coût" est augmenter pour les pénaliser et éviter qu'elles continuent à être (trop) utilisées.

Ce routage est hiérarchisable : lorsque le nombre de commutateur croît seuls les commutateurs qui ont vocation de transit entre régions connaissent finement l'état des autres commutateurs. Les commutateurs qui ont un rôle de concentrateur n'ont qu'une connaissance partielle (locale) de l'état du réseau. Pour un transfert assez proche, un commutateur peut avoir une connaissance fine des routes possibles. Pour un transfert éloigné, il peut se contenter de calculer globalement le "coût" d'accès à un "point visé" proche de la destination finale.

10.Routage sur le Réseau Internet

Sur les (sous-) réseaux de l'Internet le routage utilise le plus souvent un protocole RIP : Routing Internet Protocol qui suit la RFC 1088 (C.Hedrick 1988). Toutefois le protocole OSI 10589 (IS-IS) peut être utilisé en suivant la RFC 1195 (R. Callon 1990) : Use of OSI IS-IS for Routing in TCP/IP and Dual environments. Une nouvelle proposition : OSPF Open Shortest Path First (RFC 1247 J.Moy 1991) peut aussi être utilisé pour transporter les messages RIP.

Dans IS-IS et OSPF, les routeurs sont responsables de l'identification de leurs voisins et de la création de "paquets d'état des liens" (LSP Link State Packet). Les deux protocoles supportent un routage hiérarchique.

Ces informations, plus riches qu'un "vecteur distance" permettent d'établir les tables de routages en tenant compte d'autres facteurs sur le fonctionnement du réseau et **d'éviter des problèmes de bouclage de routes ou de convergence lente dans les réseaux maillés** (problèmes qui autrement doivent être réglès par des mécanismes annexes, par exemple des temporisations pour certaines demandes de mises à jour).

Une différence essentielle réside dans l'architecture logicielle. OSPF est situé au dessus de la couche IP et utilise des paquets IP pour transférer ses informations. IS-IS (OSI) est de niveau IP et utilise directement la couche Liaison de données.

10.1.RIP : Routing Information Protocol

Ce protocole est un standard de fait pour échanger des informations de routage entre des routeurs et des hôtes dans l'architecture Inet (TCP/IP). Il utilise un algorithme de type "vecteur distance" (Bellman-Ford). La mise à jour des routes est limitée à un minimum de 30 secondes. Le chemin le plus long est limité à 15 étapes (ce qui permet d'éviter les boucles infinies mais limite la taille "gérable" du (sous-)réseau. Il utilise des métriques fixes pour comparer les routes et n'est pas approprié pour un routage adaptatif tenant compte de paramètres temps réels comme les temps de transit, la fiabilité de l'information ou la charge du réseau.

La métrique la plus simple consiste à utiliser le nombre de routeurs traversé (**nombre d'étapes ou sauts**). On peut aussi ajouter un "coût" à chaque étape.

Le coût D(i,j) d'une liaison entre i et j passant par le voisin k de j est

$D(i,j) = \min_k d(i,k) + D(k,j)$

La meilleure route est celle qui passe par le noeud k qui rend d(i,k) + D(k,j) minimal.

Sur cet algorithme on établit pour chaque noeud une table de routage donnant la distance vers chaque destination et le prochain noeud à emprunter.

Périodiquement cette table est envoyée pour mise à jour à chaque voisin.

A partir de cette mise à jour il est possible de calculer une nouvelle version de la table de routage locale tenant compte des modifications données par les voisins ou observées localement.

Ceci suppose que la topologie reste fixe. Si elle change la liste des voisins est modifiée et la modification sera répercutée graduellement dans tout le réseau.

Les messages RIP sont transportés par le protocole de transport sans connexion UDP.

10.2.EGP: Exterior Gateway Protocol

Le protocole RIP est adapté aux réseaux "convergents" de taille limitée, appelés "systèmes autonomes". Les grands réseaux sont constitués de plusieurs systèmes autonomes. EGP est utilisé par un routeur d'un système autonome pour faire connaître ses routes à un routeur d'un **autre** système autonome.

EGP comporte un mécanisme d'acquisition de voisinage pour demander à un voisin (externe) d'échanger des informations de routage: il acquiert ainsi un "voisin EGP" ou "pair EGP". (il n'y a aucune notion de distance géographique dans ce concept…). Un routeur EGP vérifie en permanence que ses "pairs EGP" sont toujours accessibles (donc que les réseaux autonomes externes auquels il est relié sont joignables). Enfin il échange régulièrement des informations de mise à jour du routage.

Pour cela, il supporte 9 types de messages: Demande d'acquisition, Confirmation d'acquisition, Refus d'acquisition, Demande de cessation, Confirmation de cessation, Hello (Signe de vie), Je t'ai entendu (réponse Hello), Demande de mise à jour, Mise à jour de routage, Erreur.

EGP n'interprète aucune des indications de distance qu'il transmet. En fait il ne propage que des indications sur l'accessibilié et limite la topologie des réseaux internet qui l'utilisent à un structure d'arbre entre les systèmes autonomes reliés.

Il est donc généralement abandonné au profit de OSPF ou de protocoles propriétaires comme EIGRP de Cisco.

10.3.OSPF

OSPF comporte le routage par type de service: les aministrateurs peuvent définir plusieurs routes vers une destination donnée en fonction de qulité de service requise (haut débit, faible délai, sécurité par exemple). Il assure l'équilibrage de charge en plusieurs routes de même coût (voir avantages et inconvénients dans "Conception Optimale des Réseaux…).

Pour les grands réseaux, il travaille à deux niveaux dans des "zones" (systèmes autonomes) interconnectées.

Il assure une certaine sécurité des messages de routage en les authentifiant.

Il permet aux routeurs d'échanger des informations de routage acquises de sites extérieurs.

10.4.EIGRP

Ce protocole permet d'utiliser un routage hybride, s'appuyant sur des vecteurs distances et l'état des liens (bande passante, mémoire, surcharge des processeurs) comme le fait le protocole ISO 10589 (IS-IS). Ce type de routage assure un convergence plus rapide.

Il est utilisable sur des réseaux maillés en définissant des routes avec des distances différentes pour atteindre le même réseau externe. La route la plus courte est choisie tant qu'elle reste opérationnelle.

Il supporte différentes procoles: IP, IPX, AppleTalk.