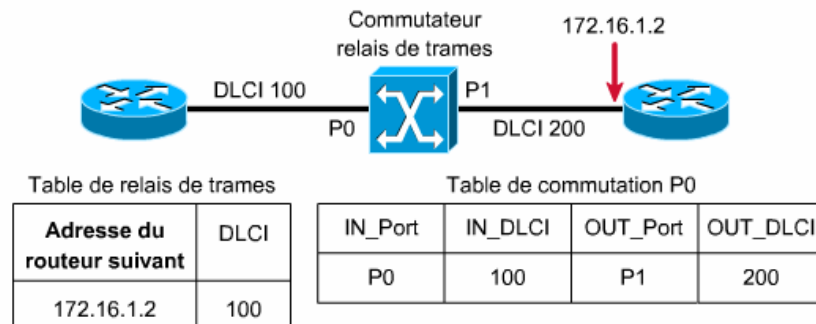


Les caractéristiques de l'interface LMI

Diffusion sélective et protocole de résolution d'adresses inversées

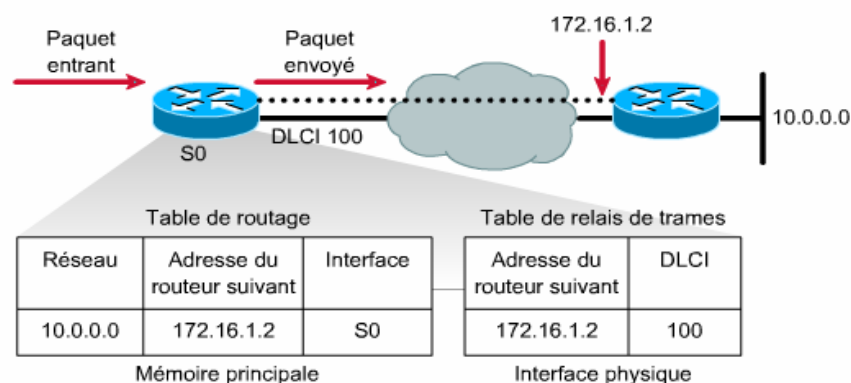
La diffusion sélective est une autre fonction facultative précieuse de l'interface LMI. Les groupes multipoints sont désignés par une série de quatre valeurs DLCI réservées (1019 à 1022). Les trames transmises par un dispositif utilisant un de ces DLCI réservés sont dupliquées par le réseau et envoyées à tous les points de sortie de l'ensemble désigné. L'extension de diffusion sélective définit également les messages LMI qui signalent l'ajout, la suppression et la présence de groupes multipoints aux unités utilisatrices. Dans les réseaux qui utilisent le routage dynamique, les données de routage doivent être échangées entre plusieurs routeurs. Les messages de routage peuvent être transmis efficacement au moyen de trames dotées d'un DLCI de diffusion multipoint. Cela permet d'envoyer des messages à des groupes spécifiques de routeurs.



Le mécanisme du protocole Inverse ARP permet au routeur de construire automatiquement la carte de relais de trames, comme l'illustre la figure. Le routeur prend connaissance des DLCI utilisés au moment de l'échange LMI initial avec le commutateur. Le routeur envoie alors une requête de protocole Inverse ARP à chaque DLCI pour chacun des protocoles configurés à l'interface, si le protocole est supporté. L'information retournée par la requête de protocole Inverse ARP est ensuite utilisée pour bâtir la carte de relais de trames.

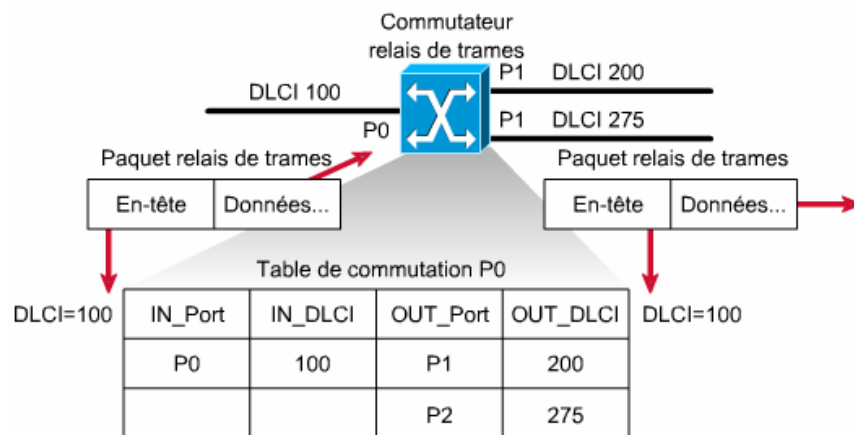
Mappage du relais de trames

L'adresse du saut suivant, déterminée à partir de la table de routage, doit être convertie en DLCI relais de trames, comme l'illustre la figure. Cette conversion est effectuée par le biais d'une structure de données appelée carte de relais de trames. La table de routage est alors utilisée pour générer l'adresse de protocole du saut suivant ou le DLCI du trafic sortant. Cette structure de données peut être statiquement configurée dans le routeur ou la carte peut être définie automatiquement par le protocole Inverse ARP.

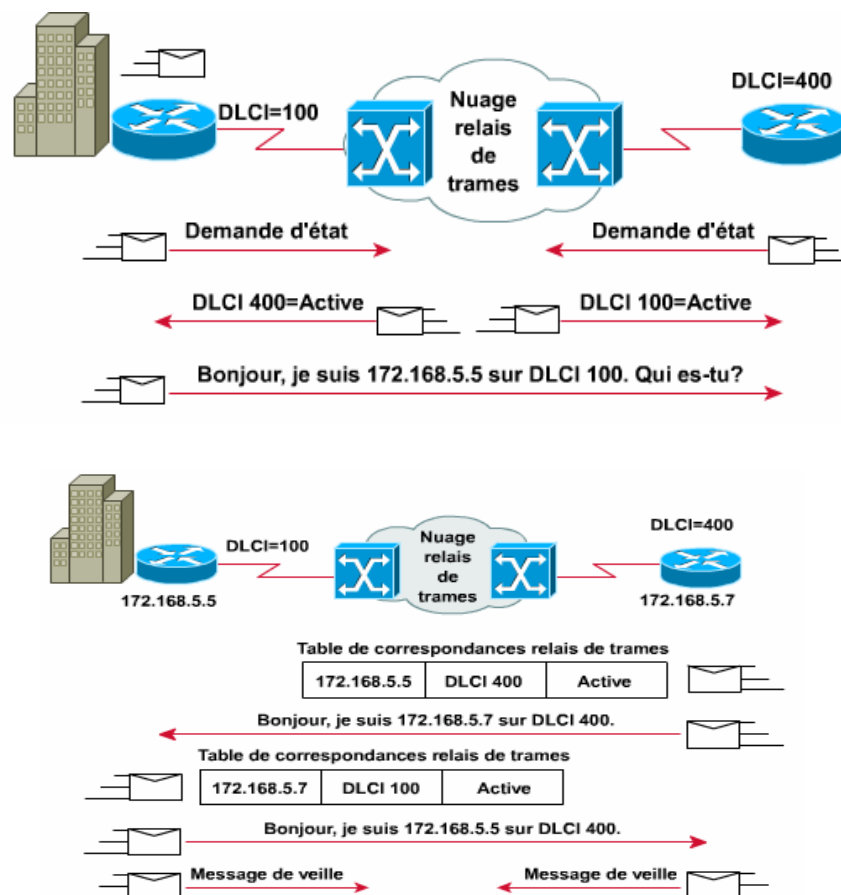


Tables de commutation de relais de trames

La table de commutation de relais de trames consiste en quatre entrées : deux pour le port et le DLCI d'entrée et deux pour le port et le DLCI de sortie, comme l'illustre la figure. La correspondance du DLCI peut donc être modifiée à chacun des commutateurs; le fait que la référence au port puisse être modifiée est la raison pour laquelle le DLCI reste inchangé.



Résumé



Les sous-interfaces relais de trames

Que sont les sous-interfaces relais de trames ?

Pour activer l'envoi de mises à jour de routage complètes au sein d'un réseau à relais de trames, il est possible de doter le routeur d'interfaces logiquement attribuées appelées sous-interfaces. Les sous-interfaces sont des subdivisions logiques d'une interface physique. Dans une configuration avec sous-interfaces, chaque circuit virtuel permanent peut être configuré comme une connexion point-à-point, ce qui permet à la sous-interface d'agir comme une ligne spécialisée.

Les premières mises en œuvre du relais de trames demandaient que le routeur (un dispositif ETTD) ait une interface série de réseau longue distance pour chaque circuit PVC, comme l'illustre la figure. En divisant de manière logique une seule interface physique série de réseau longue distance en plusieurs sous-interfaces virtuelles, il est possible de réduire le coût global de mise en œuvre d'un réseau à relais de trames. Comme l'illustre la figure, une seule interface de routeur peut desservir de nombreux emplacements éloignés par l'entremise de sous-interfaces uniques et distinctes.

Environnements de routage split horizon

Les mises à jour split horizon réduisent les boucles de routage en empêchant une mise à jour de routage reçu sur une interface physique d'être retransmise par la même interface. Par conséquent, si un routeur distant envoie une mise à jour au routeur central qui relie plusieurs circuits PVC sur une seule interface physique, le routeur central ne peut pas annoncer cette route aux autres routeurs distants par l'entremise de la même interface physique.

Résolution de questions d'accessibilité point à point et multipoint

Il est possible de configurer des sous-interfaces pour supporter les types de connexions qui suivent :

- Point à point -- Une seule sous-interface sert à établir une connexion PVC à une autre interface physique ou à une sous-interface d'un routeur éloigné. Dans ce cas, les interfaces feraient partie du même sous-réseau et chaque interface aurait un seul DLCI. Chaque connexion point à point est son propre sous-réseau. Dans cet environnement, la diffusion est facile à réaliser puisque les routeurs sont reliés point -à point et la connexion est comme une ligne louée.
- Multipoint -- Une seule sous-interface sert à établir de multiples connexions PVC à plusieurs interfaces physiques ou sous-interfaces de routeurs éloignés. Dans ce cas, toutes les interfaces feraient partie du même sous-réseau et chaque interface aurait son propre DLCI local. Dans cet environnement, puisque la sous-interface agit comme un réseau à relais de trames ordinaire, les mises à jour du routage sont sujets aux mises à jour split horizon.

Configuration de Base d'un routeur Cisco

Configuration de la sécurité

Exécutez les étapes suivantes pour munir le routeur de mesures de sécurité, comme le nom d'hôte du routeur et le mot de passe à entrer pour empêcher les accès non autorisés.

Étape 1

Attribuez un nom d'hôte au routeur. Ce nom est utilisé dans les invites et dans les noms de fichiers de configuration par défaut. Pour l'authentification du protocole point à point, le nom d'hôte entré avec cette commande doit correspondre au nom utilisateur du routeur au site central.

```
Router(config) # hostname 1600
```

Étape 2

Précisez un mot de passe pour empêcher l'accès non autorisé au routeur :

```
1600(config) # enable password 1600user
```

Séquence de commande IOS pour configurer entièrement le relais de trames

Une configuration de base du relais de trames suppose que le relais de trames sera configuré sur une ou sur plusieurs interfaces physiques et que l'interface LMI et le protocole de résolution d'adresses inversées (Inverse ARP) sont supportés par les routeurs éloignés. Dans ce type d'environnement, l'interface LMI signale les DLCI disponibles au routeur. Le protocole Inverse ARP est activé par défaut, il ne figure donc pas dans la sortie de la configuration. Marche à suivre pour la configuration du relais de trames de base

Configuration de la sécurité Ethernet

Exécutez les étapes suivantes pour configurer l'interface Ethernet (qui relie le routeur au réseau local) pour le routage IP et IPX et les adresses de réseau :

Étape 1 Entrez en mode configuration pour l'interface Ethernet :

```
1600(config)# interface ethernet 0
```

Étape 2 Dotez cette interface d'une adresse IP et d'un masque de sous-réseau :

```
1600(config-if)# ip address 172.16.25.1 255.255.255.0
```

Étape 3 Activez le routage IPX sur cette interface :

```
1600(config-if)# ipx network number
```

Étape 4 Activez l'interface et les modifications de configuration que vous venez d'effectuer sur l'interface :

```
1600(config-if)# no shutdown
```

Étape 5 Quittez le mode configuration pour cette interface :

```
1600(config-if)# exit
```

Configuration de l'accès au routeur par ligne de commande

Exécutez les étapes suivantes pour configurer certains paramètres qui contrôlent l'accès au routeur, notamment le type de ligne de terminal utilisée avec le routeur, le délai de temporisation du routeur lorsqu'il attend une entrée de l'utilisateur et le mot de passe à entrer pour lancer une session sur le routeur :

Étape 1 Précisez la ligne de terminal de la console :

```
1600(config)# line console 0
```

Étape 2 Réglez l'intervalle de sorte que l'interpréteur de commandes EXEC attende de détecter une entrée utilisateur :

```
1600(config-line)# exec-timeout 5
```

Étape 3 Précisez un terminal virtuel pour l'accès distant à la console :

```
1600(config-line)# line vty 0 4
```

Étape 4 Précisez un mot de passe :

```
1600(config-line)# password lineaccess
```

Étape 5 Activez la vérification du mot de passe à l'ouverture de la session :

```
1600(config-line)# login
```

Étape 6 - Quittez le mode de configuration :

```
1600(config-line)# end
```