

Chapitre 4

PPP Point to Point Protocol

11-mars-20

1

1

Introduction 1/3

- Le protocole point à point a été conçu pour les liaisons simples qui transportent des paquets entre deux homologues : hôtes, ponts et routeurs connectés en point à point ;
- Ces liaisons permettent un fonctionnement bidirectionnel simultané et sont supposées livrer les paquets dans l'ordre ;
- PPP est capable de transporter sur une liaison série, sur une ligne téléphonique RTC par l'intermédiaire d'un modem, non seulement TCP/IP, mais tout protocole réseau comme IPX/SPX (Novell), AppleTalk, DECnet ou NetBEUI ;
- PPP est défini dans la RFC 1661.

2

2

Introduction 2/3

- Le protocole PPP fournit des connexions réseau local vers réseau étendu multi-protocoles gérant simultanément les protocoles TCP/IP, IPX et AppleTalk.
- Il peut être utilisé sur une paire torsadée, des lignes à fibre optique et des transmissions par satellite.
- PPP assure le transport sur des liaisons ATM, de relais de trames (Frame Relay), RNIS et optiques.
- PPP vous permet d'authentifier des connexions en utilisant le protocole d'authentification (PAP) ou le protocole d'authentification à échanges confirmés (CHAP).

3

3

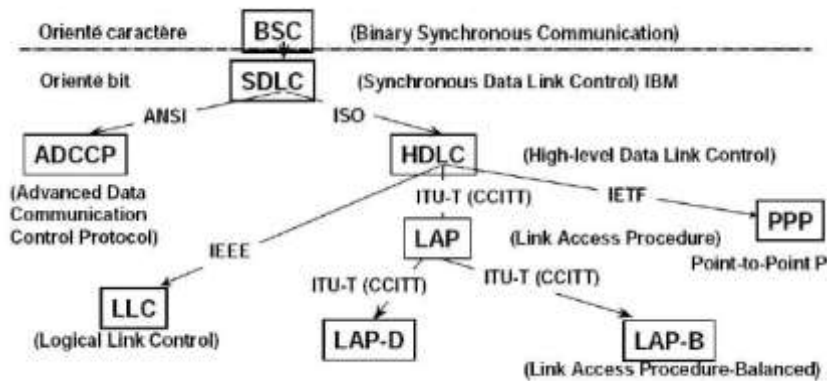
Introduction 3/3

- Sa principale caractéristique est, une fois la liaison établie et configurée, de permettre à plusieurs protocoles de transférer des données simultanément.
- L'adresse MAC, normalement, est inscrite en "dur" dans l'interface Ethernet. Dans le cas de PPP, il n'y a pas d'adresse MAC écrite en "dur" sur votre machine.
- Ethernet et PPP n'ont donc pas grand chose en commun, si ce n'est qu'ils peuvent supporter tous les deux IP.

4

4

Panorama des protocoles de la liaison de données



5

Caractéristiques PPP

Objectif :

- ❑ Faire transiter des paquets de données sur des liaisons point-à-point ;
- ❑ Accéder à Internet depuis un poste isolé (via un modem) ;
- ❑ dérivée d'HDLC ;
- ❑ Protocole WAN le plus utilisé.

Caractéristiques :

- ❑ Communication bidirectionnelle et garde l'ordre des paquets ;
- ❑ Supporte divers protocoles de niveau réseau (IP, IPX, NetBEUI...) ;
- ❑ Contrôle d'accès via des procédures d'authentications ;
- ❑ Contrôle d'erreurs ;
- ❑ Négociation des paramètres ;
- ❑ ...

6

6

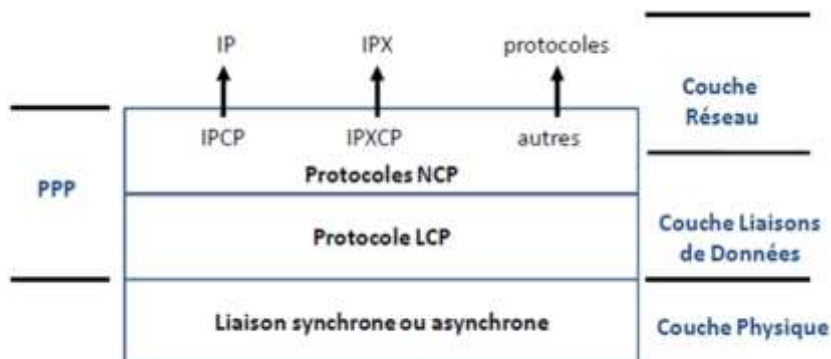
3 composants principaux

- Trame PPP = Trame HDLC générique modifiée. Un seul type de trame PPP quelque soit le protocole encapsulé.
- Protocole de contrôle de la liaison (LCP : Link Control Protocol) :
 - Établissement, maintien et libération de la connexion
 - Négociation d'options (taille des trames,...)
- Protocole de contrôle de la couche réseau (NCP : Network Control Protocol) :
 - Une famille de protocoles de contrôle réseau (IPCP,IPXCP,...) qui configure les protocoles de la couche réseau

7

7

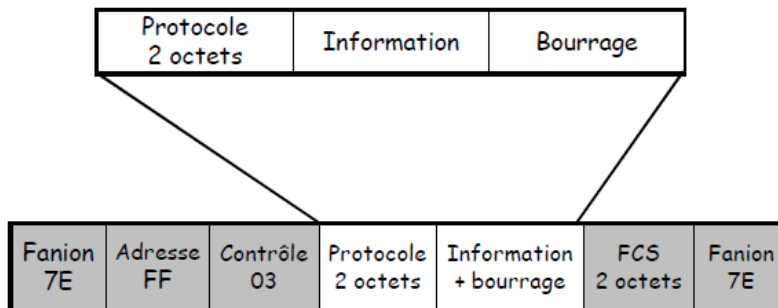
Encapsulation PPP



8

8

Format de la trame PPP



Adresse : Broadcast puisque PPP n'attribue pas d'adresse (liaison point à point...)

Le champ **Contrôle** est toujours positionné sur 00000011b pour indiquer que les trames sont de type non-numéroté.

9

9

Format de la trame PPP

- ❑ Fanion : indicateur du début / fin de trame "01111110" (0x7E).
- ❑ Adresse : inutile (0xFF, liaison point-à-point), laissée à Broadcast "11111111" (0xFF).
- ❑ Contrôle : Service non-orienté connexion (semblable au LLC) "00000011".
- ❑ Protocole (2 octets), identification du protocole encapsulé : IP, IPX,...
- ❑ Données : soit des données (1500 octets max), soit vide.
- ❑ FCS : Séquence de contrôle de trame pour une vérification des erreurs.

10

10

Le champ Protocole

Protocole 2 octets	Information	Bourrage
-----------------------	-------------	----------

Protocole : Identifie le datagramme encapsulé dans le champ Information de la trame.

0001	Protocole de bourrage		
0xxx à 3xxx	Protocole de niveau réseau spécifique	00 21	IP
8xxx à Bxxx	Paquets NCP		
Cxxx à Fxxx	Paquets LCP		
C021	Link Control Protocol		
C023	Password Aut		
C025	Link Quality Re		
C223	Challenge Han Protocol (CHA		

Protocole	Champ Type	Descriptif
IPCP	0x8021	Internet Protocol Control Protocol <ul style="list-style-type: none"> • Etablissement / config de l'IP • (Compression de l'en-tête TCP/IP)
IPXCP	0x802B	Internetwork Packet eXchange Control Protocol
CCP	0x80FD	Compression Control Protocol
ECP	0x8053	Encryption Control Protocol
IPv6CP	0x8057	IPv6 Control Protocol

11

11

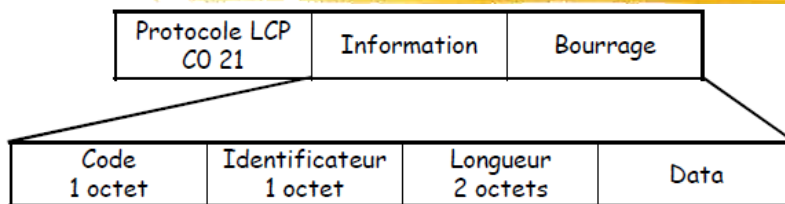
Link Control Protocol - LCP

- Afin d'être suffisamment adaptable pour être portable dans une grande variété d'environnements, PPP fournit un protocole de contrôle de liaison (LCP, *Link Control Protocol*).
- LCP est utilisé pour effectuer :
 - l'établissement et la terminaison de liaison
 - la négociation automatique des options de format d'encapsulation
 - la gestion de tailles variables de paquets
 - la rupture de liaison
 - la gestion des erreurs de configuration
 - ...

12

12

Format paquet LCP



- | | | | |
|---|------------------------------------|----|----------------------------|
| 1 | <i>Requête-Configuration</i> | 7 | <i>Code-Rejeté</i> |
| 2 | <i>Configuration-Acquittée</i> | 8 | <i>Protocole-Rejeté</i> |
| 3 | <i>Configuration-Non Acquittée</i> | 9 | <i>Requête-Echo</i> |
| 4 | <i>Configuration-Rejetée</i> | 10 | <i>Réponse-Echo</i> |
| 5 | <i>Requête-Fermeture</i> | 11 | <i>Requête-Elimination</i> |
| 6 | <i>Fermeture-Acquittée</i> | | |

- Chaque fois qu'une machine envoie un paquet, elle lui attribue un **numéro** différent ; la réponse à ce paquet devra porter le même numéro.
- Cette méthode aide à faire se correspondre les demandes et les réponses.

13

13

L'établissement de liaison LCP

- Le paquet *Configure-Request* contient en paramètre les options à négocier, les options non négociées étant prises à leurs valeurs par défaut.
- Les options négociées sont entièrement indépendantes de tout **protocole** de la couche réseau, les options de chacun de ces protocoles étant négociées par le NCP associé.
- Les options les plus courantes sont :
 - MRU (*Maximum Receive Unit*)
 - *Authentication Protocol*
 - *Quality Protocol* : L'éventuel protocole de contrôle de la qualité de la transmission
 - *Protocol Field Compression (PFC)*
 - *Adress and Control Field Compression (ACFC)*

14

14

Network Control Protocols - NCP

- **Famille de protocoles** de gestion réseau, chacun traitant des aspects particuliers à la gestion des différents protocoles de niveau réseau.
- Gestion des protocoles de la couche 3 :
 - IPCP (Internet Protocol Control Protocol)
 - IPXCP (Internetworking Packet eXchange Control Protocol)
 - BCP (Bridge Control Protocol)
- Beaucoup d'autres NCP existent, chacun étant prévu pour fonctionner avec un protocole de couche 3 spécifique.

15

15

Les différentes phases d'une transmission PPP 1/5

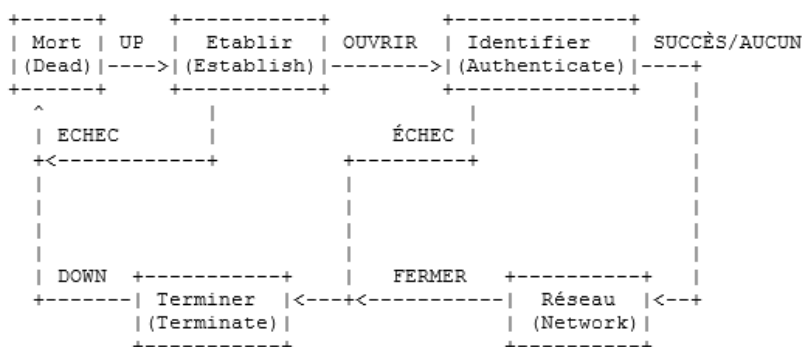
- **Phase I** : Chaque extrémité du lien PPP envoie des trames LCP pour configurer et tester la ligne : Négociation des options (MTU, Compression, QoS, ...).
- **Phase II** [option] : Authentification. Deux modes sont disponibles :
 - PAP : *Simple, mais le mot de passe transite en clair sur le réseau ;*
 - CHAP : *Fourni une protection contre les attaques.*
- **Phase III** : PPP envoie des trames NCP pour choisir et configurer un ou plusieurs protocoles réseau disponibles (IP, IPX) ;
- **Phase IV** : Transfert des datagrammes

16

16

Les différentes phases d'une transmission PPP 2/5

- Ces étapes sont représentées dans le schéma suivant :



17

17

Les différentes phases d'une transmission PPP 3/5

- *Phase liaison morte (Dead) :*
 - Cet état correspond à un moment où la liaison n'est pas prête à recevoir des données. Toute connexion commence par cette étape.
 - PPP passe à l'étape suivante (événement "UP") lorsqu'un événement extérieur se produit (détection d'une porteuse par exemple).
- *Phase d'établissement de la liaison (Establish) :*
 - C'est durant cette phase que le LCP (Link Control Protocol) est utilisé pour établir et configurer la liaison.
- *Phase d'identification (Authenticate) :*
 - Cette phase est facultative. Si l'utilisation d'un protocole d'authentification (PAP, CHAP, EAP) a été demandée pendant les négociations du LCP, on lance ce protocole avant tout autre échange de données.
 - Si cette phase échoue, la liaison est coupée (événement "DOWN").

18

18

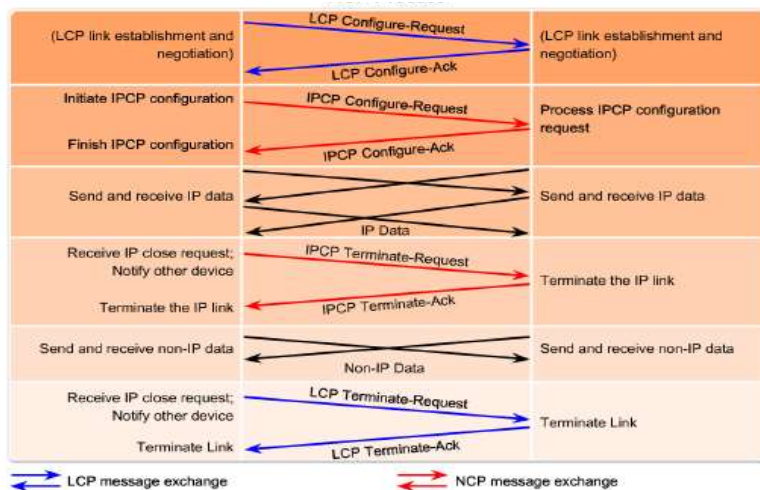
Les différentes phases d'une transmission PPP 4/5

- *Phase de configuration et d'utilisation des différents protocoles de la couche réseau (Network) :*
 - Une fois la liaison établie par le LCP, un ou plusieurs NCPs doivent être configurés pour permettre aux protocoles correspondants de transférer des données par encapsulage dans les trames de PPP.
 - Dès qu'un NCP a atteint l'état ouvert, le NP correspondant peut transporter des données jusqu'à la fermeture de son NCP.
- *Phase de terminaison (Terminate) :*
 - Pour fermer la liaison, on utilise à nouveau le LCP, en échangeant des paquets du type *Terminate*.
 - Le LCP informe alors les protocoles de la couche réseau (*Network Protocols, NPs*) que la liaison va être coupée.
 - Si la terminaison est provoquée de manière délibérée par envoi d'un paquet de type *Terminate-Request*, il faut attendre l'arrivée d'un paquet de type *Terminate-Ack* avant de fermer effectivement la liaison par l'événement « DOWN » .

19

19

Les différentes phases d'une transmission PPP 5/5



20

20

À propos de la phase de fermeture

- Trois cas :
 - Via des trames LCP ou NCP spécifiques ;
 - À cause d'un événement extérieur :
 - Expiration du délai d'inactivité
 - Perte de signaux
 - Par demande utilisateur.

21

21

Le protocole PAP



22

22

Le protocole PAP

- Échange en 2 étapes
 - envoie des informations d'authentification
 - acceptation ou refus du pair
- Méthode d'authentification simple.
- Emission du couple utilisateur/mot de passe de façon répétée jusqu'à :
 - confirmation de l'authentification
 - interruption de la connexion

23

23

Le protocole PAP

- Pas très efficace
 - Mots de passe envoyés en clair
 - Aucune protection
 - lecture répétée des informations
 - attaques répétées par essais et erreurs
- 2 méthodes d'authentification possibles :
 - Unidirectionnelle
 - Client authentifié par le serveur
 - Bidirectionnelle
 - Chaque pair authentifie l'autre

24

24

Protocole CHAP



25

25

Protocole CHAP

- Échange en 3 étapes (après demande)
 - Confirmation
 - Réponse (couple utilisateur/mot de passe)
 - Acceptation ou refus
- Méthode d'authentification plus évoluée :
 - Vérification régulière de l'identité du nœud distant
 - Authentification bidirectionnelle
 - Pas d'authentification sans confirmation préalable
 - Authentification cryptée via MD5

26

26

Protocole CHAP

- Chaque pair contrôle :
 - La fréquence des tentatives d'authentification
 - La durée de ces tentatives

- Efficacité contre le piratage :
 - valeur de confirmation variable unique et imprévisible
 - répétition des confirmations pour limiter la durée d'exposition aux attaques

27

27

Chapitre 5

Vérification de la connectivité

11-mars-20

28

28

Commande ipconfig

```
Invite de commandes
C:\Monye>ipconfig

Configuration IP de Windows

Carte réseau sans fil Connexion de red inalâhrica :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte Ethernet Connexion de área local :
    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::8553:ec4:92fc:e7b0c11
    Adresse IPv4. . . . . : 192.168.1.254
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.1
```

- **IPCONFIG** affiche un résumé des propriétés IP des cartes réseaux

11-mars-20

29

29

Commande ipconfig

- **Ipconfig /all** : Identique à la précédente mais plus complète

```
Invite de commandes

Carte réseau sans fil Connexion de red inalâhrica :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :
    Description. . . . . : Broadcom 43225 887.11b/g/n
    Adresse physique . . . . . : C4-17-FE-8C-81-32
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui

Carte Ethernet Connexion de área local :
    Suffixe DNS propre à la connexion. . . :
    Description. . . . . : Realtek PCIe FE Family Controller
    Adresse physique . . . . . : 88-26-9E-C5-65-1B
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::8553:ec4:92fc:e7b0c11 (préféré)
    Adresse IPv4. . . . . : 192.168.1.16 (préféré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail réseau. . . . . : 1001 23 août 2011 20:17:05
    Bail expiration. . . . . : 1001 30 août 2011 20:17:05
    Passerelle par défaut. . . . . : 192.168.1.1
    Serveur DHCP . . . . . : 192.168.1.1
    ID DnsPdu . . . . . : 33560734
    ID de client DHCPv6. . . . . : 88-81-80-81-13-F4-1E-24-00-26-9E-C5-65-1B
```

11-mars-20

30

30

Commande ping

- ❑ L'utilisation de la commande **ping** constitue un moyen efficace de tester la connectivité.
- ❑ Cette vérification est souvent appelée « test de la pile de protocoles » parce que la commande ping passe de la couche 3 du modèle OSI à la couche 2, puis à la couche 1.
- ❑ Elle emploie le protocole **ICMP** pour vérifier la connectivité.
- ❑ L'utilisation d'une série de commandes ping permet d'isoler les problèmes.

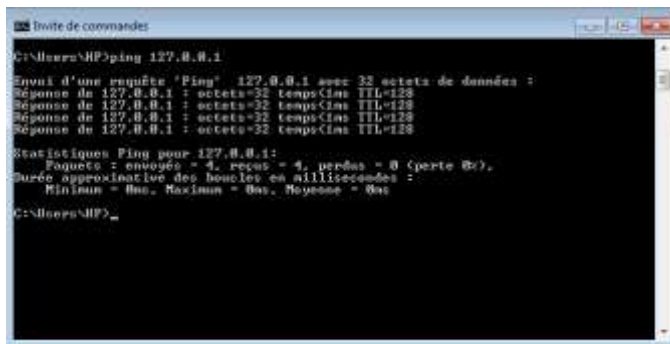
11-mars-20

31

31

Commande ping : localhost

- ❑ Test de la boucle pour vérifier la configuration IP interne sur l'hôte local : ping 127.0.0.1 (adresse de bouclage)



```
C:\Users\HP>ping 127.0.0.1
Envoi d'une requête 'Ping' 127.0.0.1 avec 32 octets de données :
Réponse de 127.0.0.1 : octets=32 temps<ms TTL=128
Réponse de 127.0.0.1 : octets=32 temps<ms TTL=128
Réponse de 127.0.0.1 : octets=32 temps<ms TTL=128
Réponse de 127.0.0.1 : octets=32 temps<ms TTL=128

Statistiques Ping pour 127.0.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 4ms, Maximum = 4ms, Moyenne = 4ms

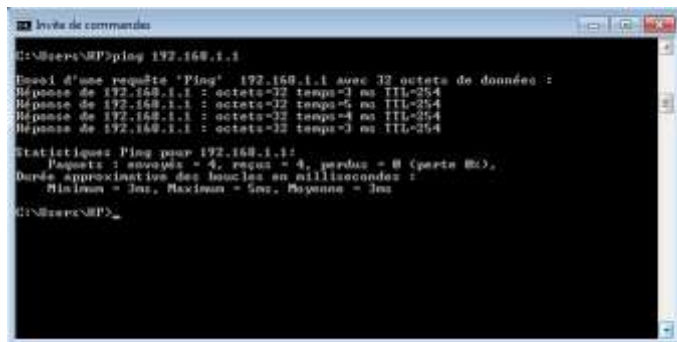
C:\Users\HP>
```

11-mars-20

32

32

Commande ping : LAN



```

C:\Users\NRP>ping 172.168.1.1

Envoi d'une requête 'Ping' 172.168.1.1 avec 32 octets de données :
Réponse de 172.168.1.1 : octets=32 temps=3 ms TTL=254
Réponse de 172.168.1.1 : octets=32 temps=6 ms TTL=254
Réponse de 172.168.1.1 : octets=32 temps=4 ms TTL=254
Réponse de 172.168.1.1 : octets=32 temps=3 ms TTL=254

Statistiques Ping pour 172.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 6ms, Moyenne = 4ms

C:\Users\NRP>

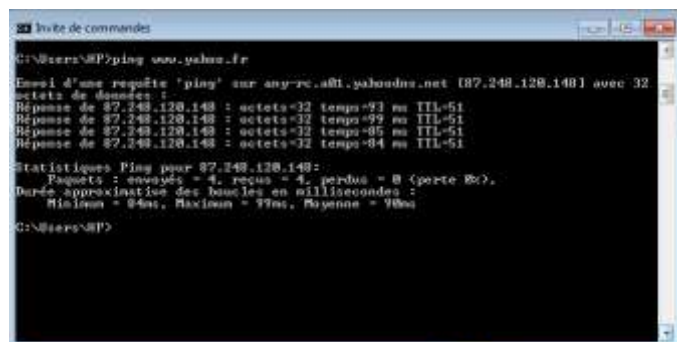
```

11-mars-20

33

33

Commande ping : WAN



```

C:\Users\NRP>ping www.yahoo.fr

Envoi d'une requête 'ping' sur any-rs.a81.yahoodns.net [87.248.128.148] avec 32
octets de données :
Réponse de 87.248.128.148 : octets=32 temps=93 ms TTL=51
Réponse de 87.248.128.148 : octets=32 temps=92 ms TTL=51
Réponse de 87.248.128.148 : octets=32 temps=85 ms TTL=51
Réponse de 87.248.128.148 : octets=32 temps=84 ms TTL=51

Statistiques Ping pour 87.248.128.148:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 84ms, Maximum = 93ms, Moyenne = 90ms

C:\Users\NRP>

```

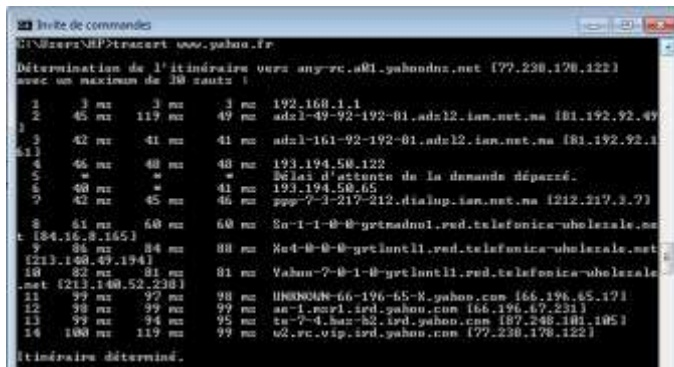
11-mars-20

34

34

Commande Tracert

- Tracert est un outil de diagnostic des réseaux



```

C:\Users\NFP>tracert www.yahoo.fr

Détermination de l'itinéraire vers any-cv.a01.yahoo.net [77.238.178.122]
avec un maximum de 30 sauts :

  0  0 ms  0 ms  0 ms  192.168.1.1
  1  45 ms 119 ms 49 ms  adsl-49-92-192-81.adsl2.lan.net.ma [81.192.92.49]
  2  42 ms 41 ms 41 ms  adsl-161-92-192-81.adsl2.lan.net.ma [81.192.92.161]
  3  46 ms 40 ms 48 ms  193.194.50.122
  4  46 ms 40 ms 48 ms  *
  5  46 ms 40 ms 41 ms  193.194.50.65
  6  42 ms 45 ms 46 ms  ppp-7-3-217-212.dialup.lan.net.ma [212.217.3.7]
  7  61 ms 60 ms 60 ms  Sn-1-1-0-0-gtlnadn01.red.telefonica-uhlesale.net
 [34.36.0.165]
  8  84 ms 84 ms 88 ms  Xed-0-0-0-gtlnatl1.red.telefonica-uhlesale.net
 [213.148.49.194]
  9  82 ms 81 ms 81 ms  Vahau-7-0-1-0-gtlnatl1.red.telefonica-uhlesale
 .net [213.140.52.230]
 10  99 ms 97 ms 99 ms  00000006-66-196-65-X.yahoo.com [66.196.65.17]
 11  98 ms 99 ms 99 ms  an-1-mcr1.red.yahoo.com [66.196.67.231]
 12  99 ms 94 ms 95 ms  tu-7-4-haz-b2.lrd.yahoo.com [87.248.101.105]
 13 100 ms 119 ms 99 ms  w2.vc.vip.lrd.yahoo.com [77.238.178.122]

Itinéraire déterminé.
```

11-mars-20

35

35

Chapitre 6

Planification et câblage des réseaux

11-mars-20

36

36

Introduction

- Identifier le support réseau nécessaire à l'établissement d'une connexion de réseau local.
- Identifier les types de connexion pour les connexions de périphériques intermédiaires ou de périphériques finaux dans un réseau local.
- Identifier les configurations de brochage pour les câbles droits et les câbles croisés.
- Identifier les différents types de câblage, les normes et les ports utilisés pour les connexions de réseau étendu.
- Définir le rôle des connexions de gestion des périphériques lors de l'utilisation d'un équipement.
- Concevoir un schéma d'adressage pour un interréseau et affecter des plages pour les hôtes, les périphériques réseau et l'interface du routeur.
- Comparer et distinguer l'importance des conceptions de réseau.

11-mars-20

37

37

Choix de périphérique de réseau local : routeur

- Périphériques **inter-réseau** :
 - Les routeurs sont les principaux périphériques utilisés pour interconnecter les réseaux.
 - Chaque port d'un routeur est connecté à un réseau différent et achemine les paquets entre les réseaux.
 - Les routeurs ont la possibilité de segmenter les domaines de diffusion et les domaines de collision.
 - Les routeurs sont également utilisés pour interconnecter des réseaux qui font appel à différentes technologies. Ils peuvent être dotés à la fois d'interfaces de réseau local et d'interfaces de réseau étendu.

11-mars-20

38

38

Choix de périphérique de réseau local : Concentrateur

□ Périphériques **intra-réseau** :

- Un concentrateur reçoit un **signal**, le régénère et l'envoie sur tous les ports. L'utilisation des concentrateurs crée un bus logique. Le réseau local utilise alors un support multi-accès.
- Les ports utilisent une approche de bande passante partagée et offrent souvent des performances réduites dans le réseau local en raison des collisions et des opérations de récupération.
- Les concentrateurs sont moins coûteux que les commutateurs.
- Un concentrateur est généralement sélectionné comme périphérique intermédiaire dans un très petit réseau local, dans un réseau local qui nécessite un débit faible ou lorsque les finances sont limitées.

11-mars-20

39

39

Choix de périphérique de réseau local : Commutateur

□ Périphériques **intra-réseau** :

- Un commutateur reçoit une **trame** et la régénère sur le port de destination approprié. Il est utilisé pour segmenter un réseau dans plusieurs domaines de collision.
- Chaque port du commutateur crée un domaine de collision distinct. Cela crée une topologie logique point à point sur le périphérique de chaque port.
- De plus, un commutateur fournit une bande passante dédiée sur chaque port, ce qui augmente les performances du réseau local. Un commutateur de réseau local peut également être utilisé pour interconnecter des segments de réseau à différentes vitesses.
- Même si un commutateur est plus coûteux qu'un concentrateur, ses performances améliorées et sa fiabilité accrue le rendent plus rentable

11-mars-20

40

40

Facteurs de sélection des périphériques

- Un réseau local doit faire l'objet d'une planification et d'une conception. La planification garantit que tous les besoins, les facteurs de coûts et les options de déploiement sont pris en compte.
- Lors du choix d'un périphérique différents facteurs doivent être pris en considération :
 - Coût
 - Vitesse et types de port/d'interface
 - Capacité d'extension
 - Facilité de gestion
 -

11-mars-20

41

41

Facteurs de sélection des périphériques : le coût

- Le coût d'un commutateur est déterminé par sa capacité et ses fonctions.
- La capacité du commutateur inclut le nombre de ports, les types de port disponibles et la vitesse de commutation.
- Les autres facteurs qui ont un impact sur le coût sont ses fonctions de gestion réseau, ses technologies de sécurité intégrées et ses technologies de commutation avancées facultatives.

11-mars-20

42

42

Facteurs de sélection des périphériques : vitesse et types

- La vitesse est toujours une nécessité dans un environnement de réseau local. Des ordinateurs récents avec des cartes réseau intégrées 10/100/1 000 Mbits/s sont disponibles.
- Lorsque vous choisissez un commutateur, le nombre et le type de ports est une décision très importante à prendre. Posez-vous les questions suivantes :
Achèteriez-vous un commutateur avec :
 - Juste assez de ports pour vos besoins actuels ?
 - Une combinaison de vitesses de câble UTP ?
 - Des ports UTP et à fibre optique ?

11-mars-20

43

43

Facteurs de sélection des périphériques : autres

- Pour un routeur, d'autres facteurs doivent être pris en considération :
 - Capacité d'extension : possibilité d'ajouter de nouveaux modules à mesure que les besoins évoluent ;
 - Support : un routeur peut avoir différentes interfaces pour différents supports ;
 - Fonctions du système d'exploitation : en fonction de la version, le routeur peut prendre en charge des fonctions et des services comme :
 - Sécurité
 - Qualité de service (QoS)
 - Voix sur IP (VoIP)
 - Protocoles de routage à plusieurs couches 3
 - Services spéciaux comme la traduction d'adresses de réseau (NAT) et le protocole DHCP (Dynamic Host Configuration Protocol)

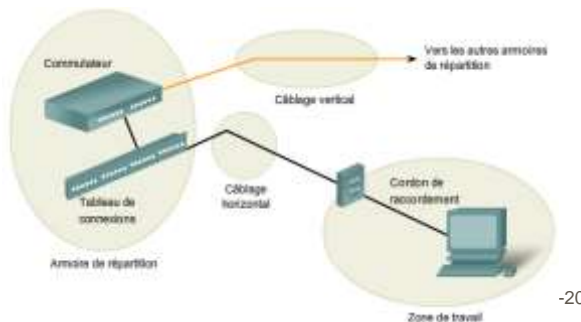
11-mars-20

44

44

Zone de câblage de réseau local : 1

- Lors de la planification de l'installation du câblage d'un réseau local, quatre domaines physiques doivent être pris en compte :
 - Zone de travail
 - Armoire de répartition également appelée point de distribution
 - Câblage du réseau fédérateur également appelé câblage vertical
 - Câblage de distribution également appelé câblage horizontal



45

Zone de câblage de réseau local : 2

- Longueur totale du câble est limitée.
- Zones de travail sont les emplacements dédiés aux périphériques finaux dont se sert chacun des utilisateurs. Le câble droit est le cordon de raccordement le plus couramment utilisé dans la zone de travail.
- Armoire de répartition est l'endroit où les connexions à des périphériques intermédiaires sont établies. Elle contient les périphériques intermédiaires (concentrateurs, commutateurs, routeurs et d'autres dispositifs de service d'accès aux données) qui forment le réseau. Ces périphériques fournissent des transitions entre le câblage du réseau fédérateur et le câblage horizontal.
- L'objectif de ces armoires est souvent double. Dans de nombreuses entreprises, l'armoire de répartition contient également les serveurs utilisés par le réseau.
- Câblage horizontal désigne les câbles qui connectent les armoires de répartition aux zones de travail.

11-mars-20

46

46

Zone de câblage de réseau local : 3

- Câblage du réseau fédérateur, ou câblage vertical, désigne le câblage utilisé pour connecter les armoires de répartition aux salles d'équipement, dans lesquelles se trouvent souvent les serveurs. Le câblage du réseau fédérateur interconnecte également plusieurs armoires de répartition dans l'ensemble du bâtiment.
- Ce câblage est utilisé pour le trafic agrégé comme le trafic en direction et en provenance d'Internet et l'accès aux ressources de l'entreprise sur un site distant.
- Une grande partie du trafic provenant des différentes zones de travail utilise le câblage du réseau fédérateur pour accéder aux ressources en dehors de la zone ou du bâtiment.
- Par conséquent, les câbles du réseau fédérateur nécessitent généralement un support de bande passante important comme un câblage à fibre optique.

11-mars-20

47

47

Type de support : 1

- La sélection des câbles nécessaires à l'établissement correct d'une connexion de réseau implique de prendre en compte les différents types de supports.
- Il existe différentes implémentations de couche physique qui prennent en charge plusieurs types de supports :
 - UTP (catégorie 5, 5e, 6 et 7)
 - Fibre optique
 - Sans fil
- Chaque type de support présente des avantages et des inconvénients.

11-mars-20

48

48

Type de support :

2

- Voici certains des facteurs à prendre en compte :
 - Longueur de câble - Le câble doit-il être tiré de part et d'autre d'une pièce ou d'un bâtiment à un autre ?
 - Coût - Le budget permet-il d'utiliser un type de support plus coûteux ?
 - Bande passante - La technologie utilisée avec le support fournit-elle une bande passante adéquate ?
 - Facilité d'installation - L'équipe en charge de l'implémentation est-elle en mesure d'installer le câble ou est-il nécessaire de faire appel à un tiers ?
 - Perturbations électromagnétiques ou radioélectriques potentielles - L'environnement local va-t-il interférer avec le signal ?

11-mars-20

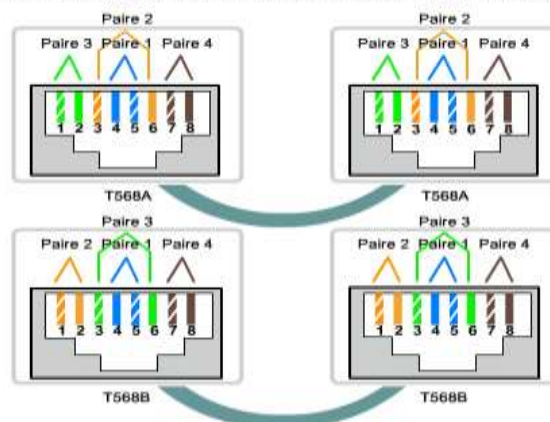
49

49

Exemple de support :

1

Câble droit
Les câbles droits comportent la même terminaison à chaque extrémité, T568A ou T568B.



11-mars-20

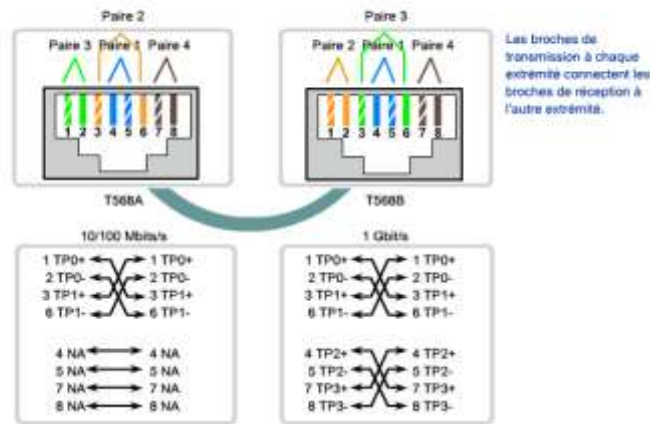
50

50

Exemple de support : 2

Câble croisé

Les câbles croisés possèdent une terminaison T568A à une extrémité et une terminaison T568B à l'autre extrémité.



51

Etablissement d'un schéma d'adressage 1

- Les périphériques finaux qui nécessitent une adresse IP sont les suivants :
 - Ordinateurs des utilisateurs
 - Ordinateurs des administrateurs
 - Serveurs
 - Autres périphériques finaux tels que les imprimantes, les téléphones IP et les appareils photo IP
- Les périphériques réseau qui nécessitent une adresse IP sont les suivants :
 - Interfaces de réseau local du routeur
 - Interfaces (série) de réseau étendu du routeur
- Les périphériques réseau qui nécessitent une adresse IP pour la gestion sont les suivants :
 - Commutateurs
 - Points d'accès sans fil

52

52

Etablissement d'un schéma d'adressage 2

- Ensuite, déterminez si tous les hôtes font partie du même réseau ou si le réseau entier est divisé en sous-réseaux distincts.
- De nombreuses raisons incitent à diviser un réseau en sous-réseaux :
 - Gestion du trafic de diffusion - Les diffusions peuvent être contrôlées car un grand domaine de diffusion est divisé en domaines plus petits. Tous les hôtes du système ne reçoivent pas toutes les diffusions.
 - Différents besoins en matière de réseau - Si différents groupes d'utilisateurs nécessitent des équipements réseau ou informatiques spécifiques, il est plus facile de gérer ces besoins si ces utilisateurs sont tous rassemblés sur un seul sous-réseau.
 - Sécurité - Différents niveaux de sécurité réseau peuvent être implémentés en fonction des adresses réseau. Cela permet de gérer l'accès à différents services réseau et de données.
- Après, il faut procéder au comptage des sous-réseaux :
 - Chaque sous-réseau, en tant que segment de réseau physique, nécessite une interface de routeur faisant office de passerelle pour ce sous-réseau. De plus, chaque connexion entre routeurs est un sous-réseau distinct.
- Une fois déterminé le nombre requis d'hôtes et de sous-réseaux, la suite consiste à calculer les valeurs suivantes :
 - Un sous-réseau et un masque de sous-réseau uniques pour chaque segment physique
 - Une plage d'adresses d'hôte utilisables pour chaque sous-réseau

53

53

Etablissement d'un schéma d'adressage 3

Calcul des adresses sans plages d'adresses VLSM pour les sous-réseaux

Cas n° 1

Réseau	Adresse de sous-réseau	Plage d'adresses d'hôte	Adresse de diffusion
Participat	172.16.0.0/23	172.16.0.1	172.16.1.254
Formateur	172.16.2.0/23	172.16.2.1	172.16.3.254
Administration	172.16.4.0/23	172.16.4.1	172.16.5.254
Réseau client (WAN)	172.16.6.0/23	172.16.6.1	172.16.7.254



54

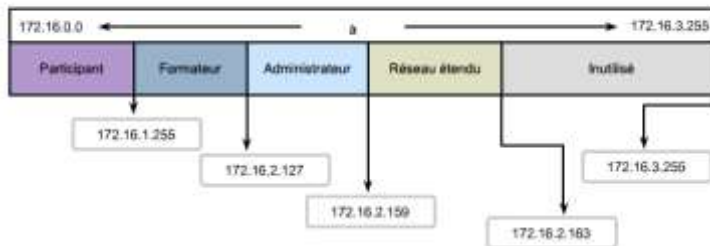
54

Etablissement d'un schéma d'adressage

4

Calcul des adresses avec plages d'adresses VLSM pour les sous-réseaux Cas n°2

Reseau	Adresse de sous-reseau	Plage d'adresses d'ôte		Adresse de diffusion
Participant	172.16.0.0/23	172.16.0.1	172.16.1.254	172.16.1.255
Formateur	172.16.2.0/25	172.16.2.1	172.16.2.126	172.16.2.127
Administration	172.16.2.128/27	172.16.2.129	172.16.2.158	172.16.2.159
Réseau étendu	172.16.2.160/30	172.16.2.161	172.16.2.162	172.16.2.163
Inutilisé	nd	172.16.2.184	172.16.2.254	nd



55

55