

Copyright PRONETIS

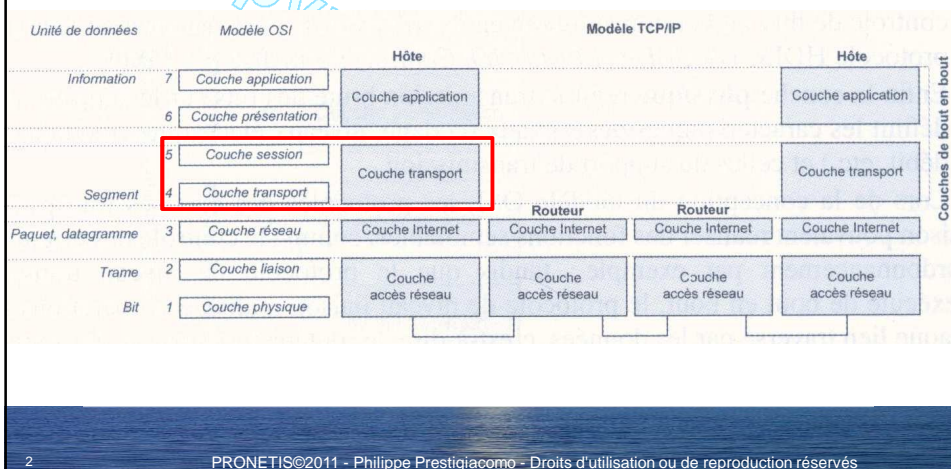
## Couche Transport

- Objectifs – Introduction
- Couche transport TCP et UDP
- TCP – Besoin d'un service fiable – caractéristiques
- Techniques d'acquittement et de fenêtrage
- UDP – Service non fiable – caractéristiques
- Résumé

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Objectifs

- Objectif de ce chapitre
  - Comprendre le rôle des protocoles de transport
  - Comprendre les fonctions et les caractéristiques de TCP et UDP

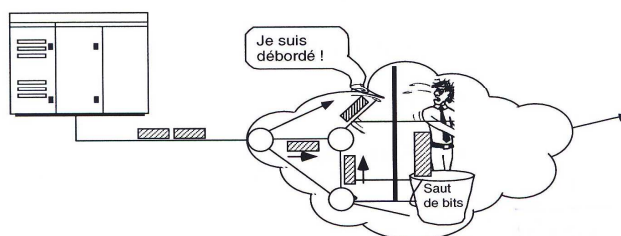


2

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Problématique

**Les services IP ne garantissent pas la remise des données**



Que se passerait-il si la couche réseau offrait un service avec connexion mais non fiable exploité par un opérateur et que la couche réseau perde des paquets IP lors du passage dans les routeurs de cet opérateur ?

C'est typiquement le cas, comme les utilisateurs de bout en bout ne peuvent pas corriger le tir en achetant un routeur plus robuste plus performant, la seule possibilité qu'il reste c'est de mettre une nouvelle couche au dessus de la couche réseau pour améliorer la qualité de service.

3

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

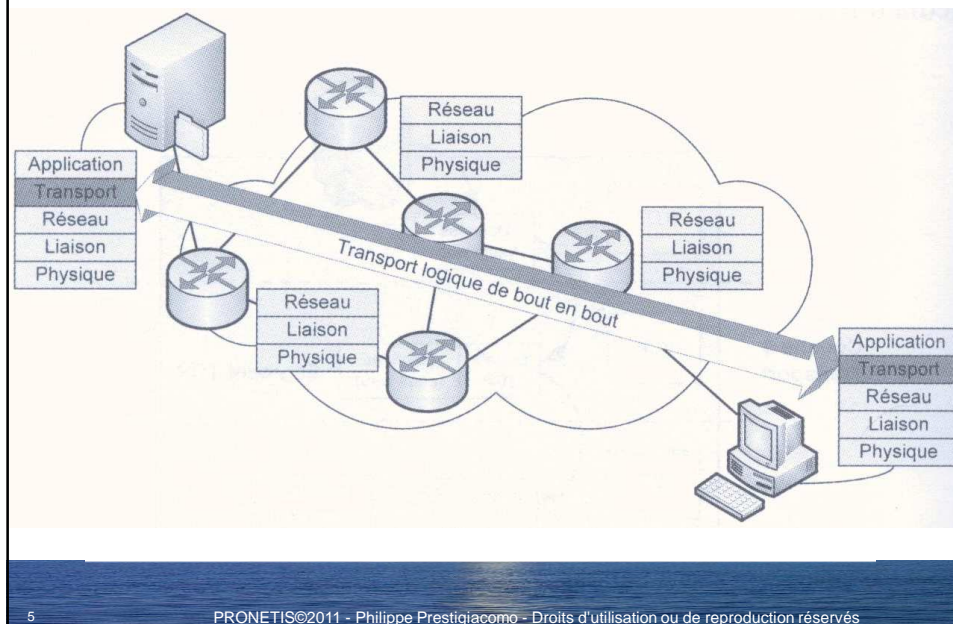
## Besoin d'un service de remise fiable des données

- Le rôle de la couche transport est de permettre le transfert de données de bout en bout de manière fiable et économique indépendamment de la nature du réseau mis en place de sa topologie.
- Le but de la couche transport permet **d'isoler les niveaux supérieurs des variations technologiques et des imperfections des couches inférieurs.**

4

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Besoin d'un service de remise fiable des données



## TCP : Transmission Control Protocol et ses caractéristiques

- TCP est un protocole orienté connexion, c'est-à-dire qu'il associe au transport des informations, la notion de qualité en offrant les services suivants :
  - Fiabilité
  - Division des messages sortant en segments - flux d'octets : pas de gestion de blocs de données pour le contrôle de flux
  - Réassemblage des messages au niveau du destinataire
  - Retransmission de toute donnée non reçue

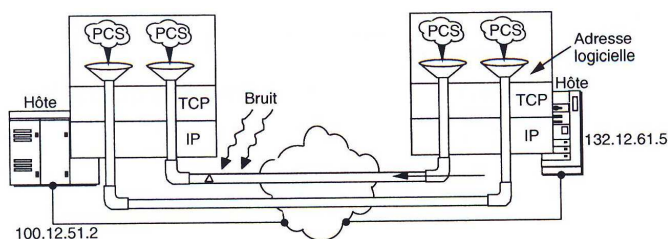
6

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Besoin d'un service de remise fiable des données

### Les protocoles de couches supérieures peuvent nécessiter

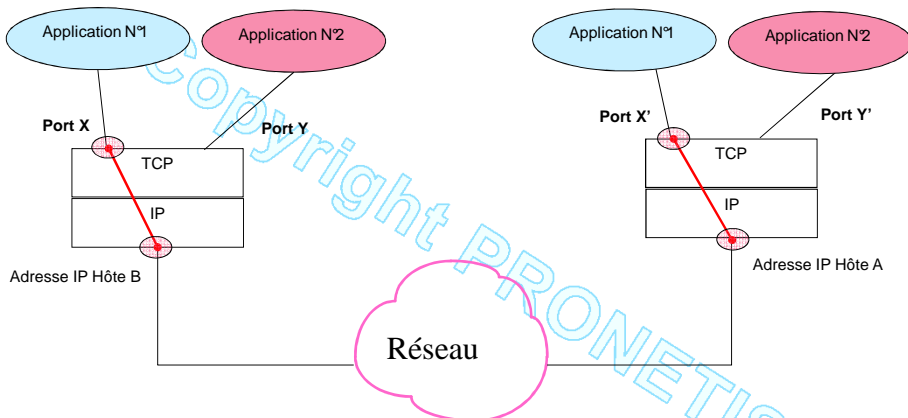
- Une remise fiable et garantie des données
  - Implémentée par des circuits virtuels
- L'utilisation d'une couche IP commune à plusieurs services d'application
  - Ce qui implique un **adressage supplémentaire** pour désigner les applications qui utilisent la même adresse IP



7

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Notion de connexion de transport & numérotations des ports



L'association des identifiants d'une connexion :

{ protocole, port destination, @IP destination, port source @IP source }

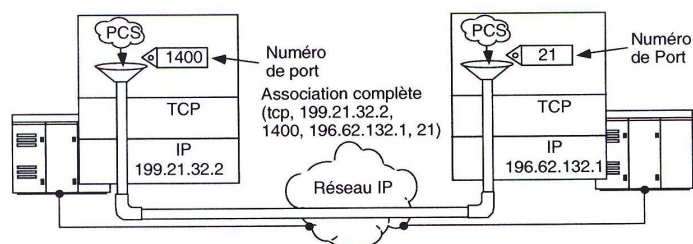
8

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Numérotation des ports - Illustration

**L'association** décrit une connexion en précisant

- Le protocole
- L'adresse locale
- Le numéro de port local
- L'adresse distante
- Le numéro de port distant
- Exemple : (tcp, 199.21.32.2, 1400, 196.62.132.1, 21)



9

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Numéros de ports TCP

- Afin que plusieurs communications puissent circuler en même temps, TCP et UDP utilisent des numéros de ports.
- Des conventions ont été établies

### Plage de ports

[ 0 à 1023 ]

[ 1024 à 65535 ]

### Utilisation

Réservés aux applications standardisées

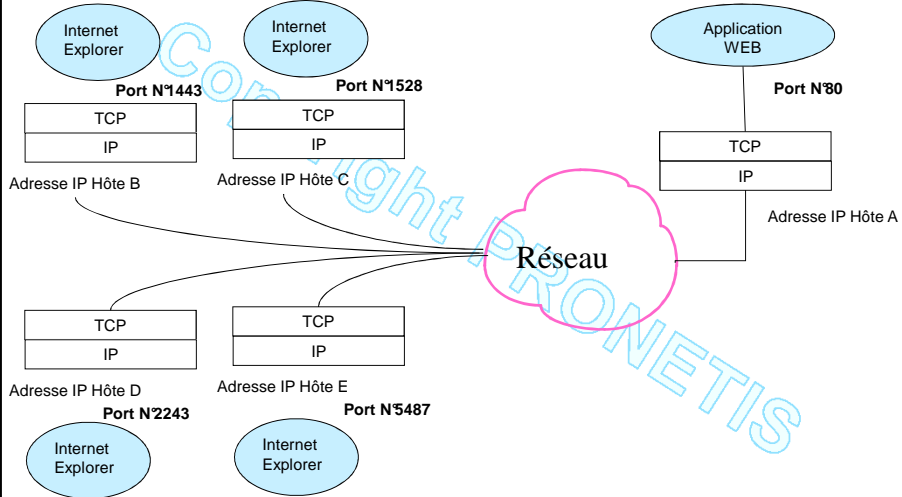
Attribués aux entreprises pour les applications et pour l'attribution dynamique des ports sources

10

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Notion de multiplexage de connexion de transport

N° de port compris entre [1024 – 65535]



11

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Numéros des ports TCP – RFC 1700

Numéro de port	Mot-clé	Description
20	FTP-DATA	File Transfer [Default Data]
21	FTP	File Transfer [Control]
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer
37	TIME	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
79	FINGER	Finger
80	HTTP	WWW
110	POP3	Post Office Protocol - Version 3
111	SUNRPC	SUN Remote Procedure Call
....		
443	HTTPS	WWW sécurisé

12

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Illustration avec le mémento « Common ports »

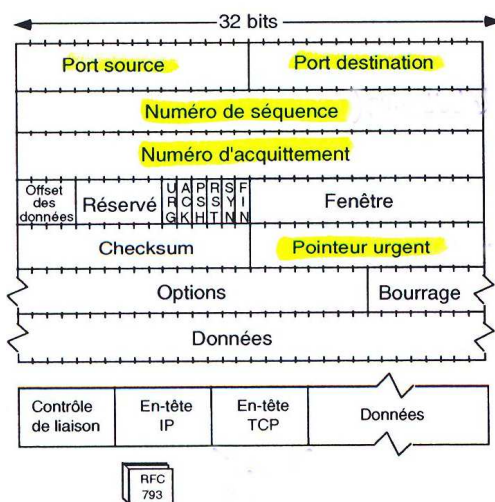
### COMMON PORTS

TCP/UDP Ports	
7 Echo	554 RTSP
19 Chargen	546-547 DHCPv6
20-21 FTP	560 rmonitor
22 SSH/SCP	563 NNTP over SSL
23 Telnet	587 SMTP
25 SMTP	591 FileMaker
42 WINS Replication	593 Microsoft DCOM
43 WHOIS	631 Internet Printing
49 TACACS	636 LDAP over SSL
53 DNS	639 MSDP (PIM)
67-68 DHCP/BOOTP	646 LDP (MPLS)
69 TFTP	691 MS Exchange
70 Gopher	860 iSCSI
79 Finger	873 rsync

13

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Format d'un paquet TCP



### Caractéristiques de TCP

- Circuits virtuels
- Full duplex
- Flux d'octets
- Numérotation de chaque octet
- Fermeture courtoise
- Contrôle de flux avec fenêtre

14

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Format d'un paquet TCP

Champs TCP	Signification
Port source et port destination	Identifient les processus source et destination
Numéro de séquence	Un numéro de 32 bits servant à identifier chaque octet qui est transmis
Numéro d'acquittement	Le nombre d'octets à l'intérieur du flux de données qui ont été correctement reçus
Offset des données	Taille de l'en-tête TCP en mots de 32 bits
URG, ACK, PSH, RST, SYN, FIN	Fanions gérant la connexion TCP
Fenêtre	Utilisé pour le contrôle de flux
Checksum	Vérification des données du paquet TCP
Pointeur urgent	Repère de message urgent
Options	Utile pour préciser la taille maximale des segments TCP

15

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Méthode de connexion TCP

- Un service orienté connexion :
  - Un chemin unique entre les unités d'origine et de destination est déterminé
  - Les données sont transmises de manière séquentielle et arrivent à destination dans l'ordre
  - La connexion est fermée lorsque cela n'est plus nécessaire

16

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Caractéristiques techniques de TCP

- Three-Way Handshake ( poignée de main en trois temps )
  - Ouverture de connexion en trois temps
- Segmentation, contrôle de flux
  - Les données transmises à TCP constituent un flot d'octets de longueur variable.
  - TCP divise ce flot de données en segments en utilisant un mécanisme de fenêtrage, puis il est émis dans un datagramme IP.
- Acquitement de messages
  - TCP garantit l'arrivée des messages, c'est à dire qu'en cas de perte, les deux extrémités sont prévenues.
  - Ce concept repose sur les techniques d'acquitement de message

17

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Méthode de connexion TCP

- Une connexion de type circuit virtuel est établie avant que les données ne soient échangées : Appel + Négociation + Transferts

Un **Circuit Virtuel** est un système de communication dans lequel les données d'un utilisateur source peuvent circuler sur différents circuits réels dans la même communication, afin d'atteindre l'utilisateur de destination.

- Une connexion = Une paire d'extrémités de connexion
- Une extrémité de connexion = Couple (adresse IP, port)
  - Exemple de connexion : [ (124.32.12.1,1034), (19.24.67.2,21) ] + Type de protocole TCP ou UDP

18

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Méthode de connexion TCP

- Une extrémité de connexion peut être partagée par plusieurs autres extrémités de connexions (multi-instanciations)
- La mise en œuvre de la connexion se fait de la manière suivante :
  - Soit, une autre application (extrémité) effectue une **ouverture active** pour demander l'établissement de la connexion.
  - Soit, une application (extrémité) effectue une **ouverture passive** en indiquant qu'elle accepte une connexion entrante,

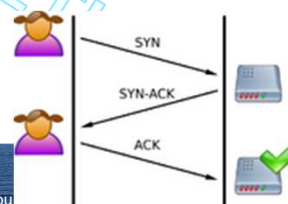
19

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Méthode de connexion TCP

- Les hôtes TCP établissent une connexion en 3 étapes, appelée aussi « **Three Way Handshake** » (voir illustration suivante)
  - Ouverture de connexion en 3 temps (**SYN, SYN-ACK, ACK**)
  - L'émetteur envoie un paquet avec un **numéro de séquence** initial (x) avec un bit dans l'en-tête pour indiquer une demande de connexion, et le bit **SYN à 1**
  - Le destinataire le reçoit, consigne le numéro de séquence initial, répond par un **accusé de réception** « x+1 » et inclut son propre n° de séquence (y). Il envoie également **les bits SYN et ACK à 1**
  - L'émetteur reçoit « x+1 ». Il renvoie « y+1 » pour dire au destinataire que la réception s'est bien passée et le bit **ACK à 1**

SYN : Ouverture de connexion  
ACK : Accusé de réception

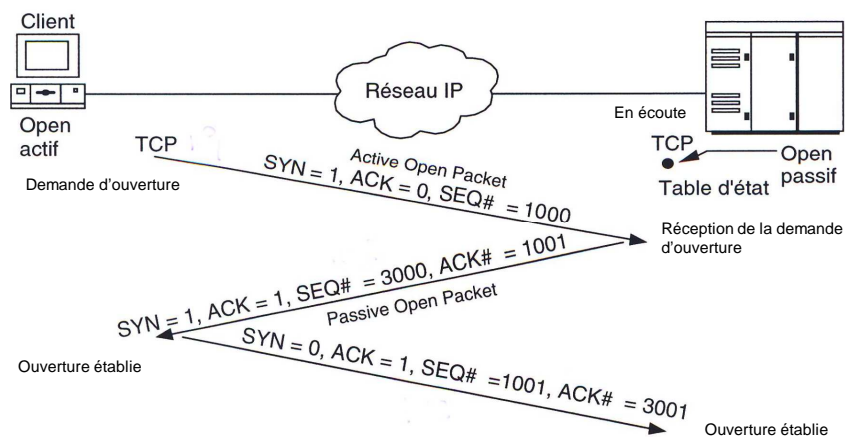


20

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou

## Méthode de connexion TCP : demande d'ouverture

- Ouverture de connexion –Three way Handshake



21

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

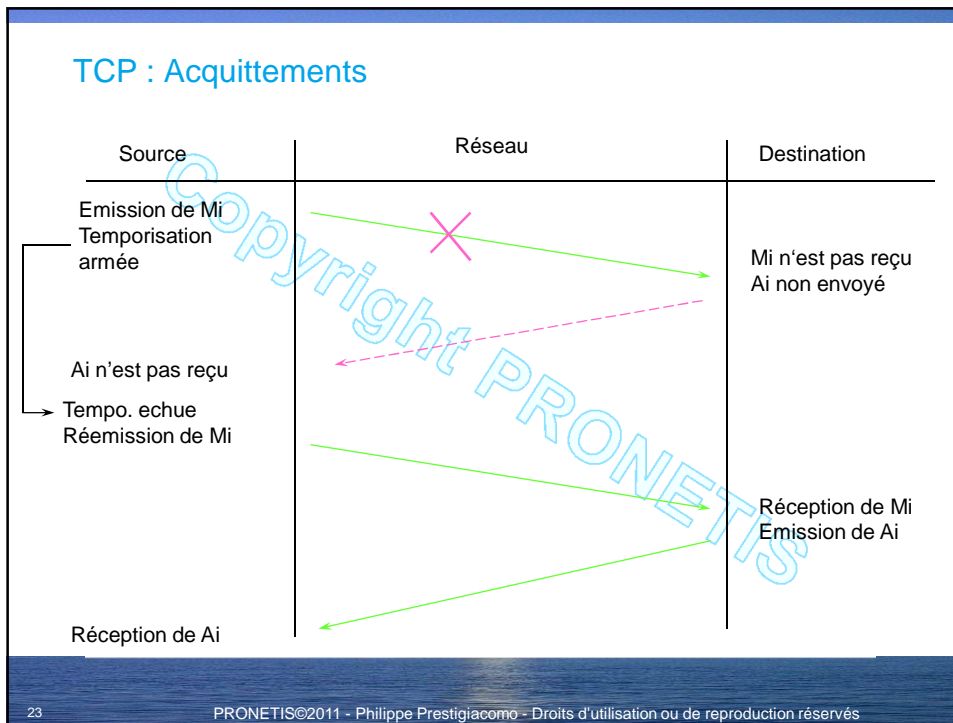
## TCP : Acquittement de messages

- Acquittement de messages
  - **Contrairement à UDP, TCP garantit l'arrivée des messages**, c'est à dire qu'en cas de perte, les deux extrémités sont prévenues.
  - Ce concept repose sur les techniques d'acquittement de message : lorsqu'une source S émet un message « Mi » vers une destination D, **S attend un acquittement « Ai » de D avant d'émettre le message suivant « Mi+1 »**.
  - **Si l'acquittement « Ai » ne parvient pas à S, S considère au bout d'un certain temps que le message est perdu et réémet « Mi »**.

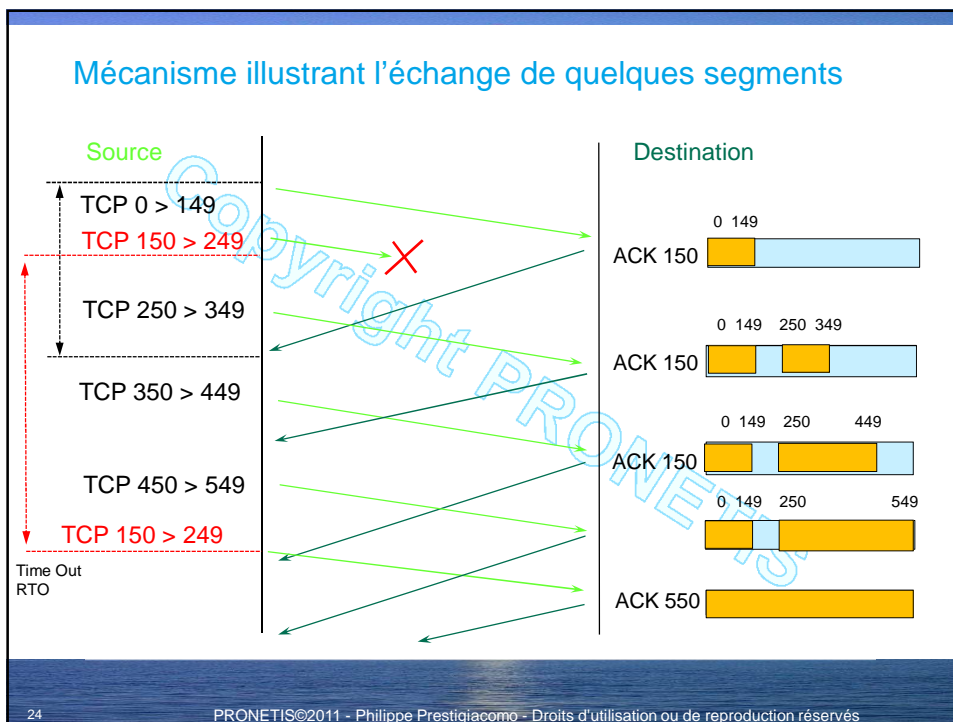
22

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## TCP : Acquittements



## Mécanisme illustrant l'échange de quelques segments



## Mécanisme illustrant l'échange de quelques segments

- La mise en œuvre de la **fiabilité passe par l'utilisation de paquets d'acquiescement (ACK) et de numéros de séquences**. Lorsqu'un destinataire reçoit un paquet, il émet un acquiescement en renseignant le numéro de séquence indiquant tous les octets reçus. **On parle d'acquiescement cumulatif.**
- Il est alors possible que l'on obtienne un second acquiescement pour un même numéro de séquence (**acquiescement dupliqué**), qui signifie qu'un paquet précédent a été détruit dans le réseau ou qu'il a été retardé.
- Cependant TCP décidera de réémettre le paquet en question qu'à l'expiration (TimeOut) d'un délai avant retransmission, le RTO (Retransmission Time Out), propre à chaque paquet qui court au moment de l'émission de celui-ci.

25

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Besoin de temporisation

- Les retransmissions du côté de l'émetteur comme le réordonnement du côté du récepteur imposent naturellement la **présence de tampon mémoire (ou buffer) des deux côtés de la connexion.**
- Il sera donc nécessaire **d'utiliser une fenêtre d'émission** donnant le nombre d'octets déjà envoyés et le nombre d'octets pouvant être encore envoyés en fonction de la place libre dans le tampon de réception.

26

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## TCP : Segmentation et le contrôle de flux

- Segmentation, contrôle de flux
  - Les données transmises à TCP constituent **un flot d'octets de longueur variable**.
  - TCP divise **ce flot de données en segments** en utilisant un **mécanisme de fenêtrage**.
  - **Un segment (ou message) est émis dans un datagramme IP**.

27

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

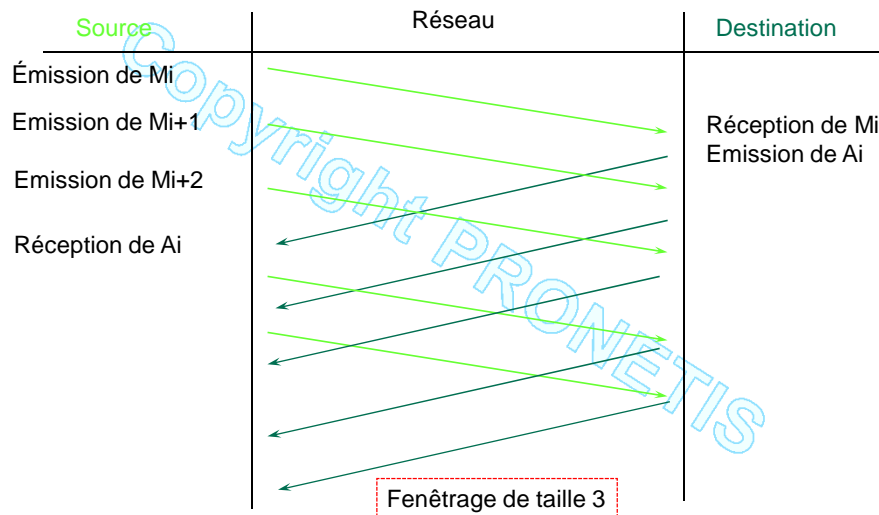
## TCP : Technique de fenêtrage conjuguée avec l'acquittement

- **La technique d'acquittement simple pénalise les performances** puisqu'il faut attendre un acquittement avant d'émettre un nouveau message. *Le fenêtrage améliore le rendement des réseaux.*
- **La technique du fenêtrage** : *une fenêtre de taille  $T$* , permet l'émission d'au plus  $T$  messages "non acquittés" avant de ne plus pouvoir émettre.
- **La taille de la fenêtre détermine la quantité de données** que l'on peut transmettre avant de recevoir un accusé de réception.

28

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## TCP : Technique de fenêtrage et le contrôle des échange



29

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## TCP : Technique de fenêtrage

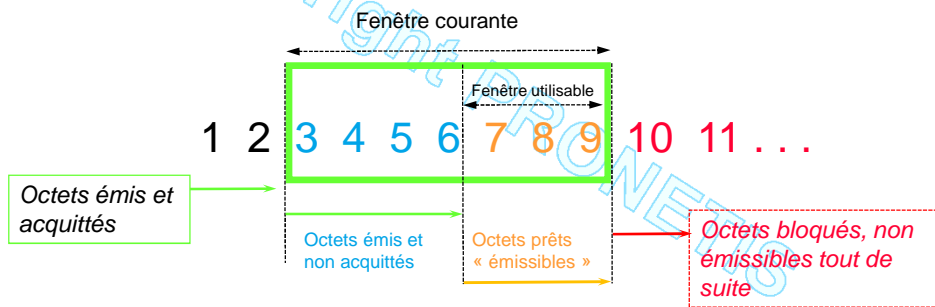
- La technique de fenêtrage permet de réguler le flux :
  - d'optimiser la bande passante
  - également au destinataire de faire diminuer le débit de l'émetteur donc de gérer le **contrôle de flux**.

30

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## TCP : Technique de fenêtrage

- Le mécanisme de fenêtrage repose sur :
  - la numérotation séquentielle des octets de données,
  - la gestion de pointeurs par fenêtrage



31

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

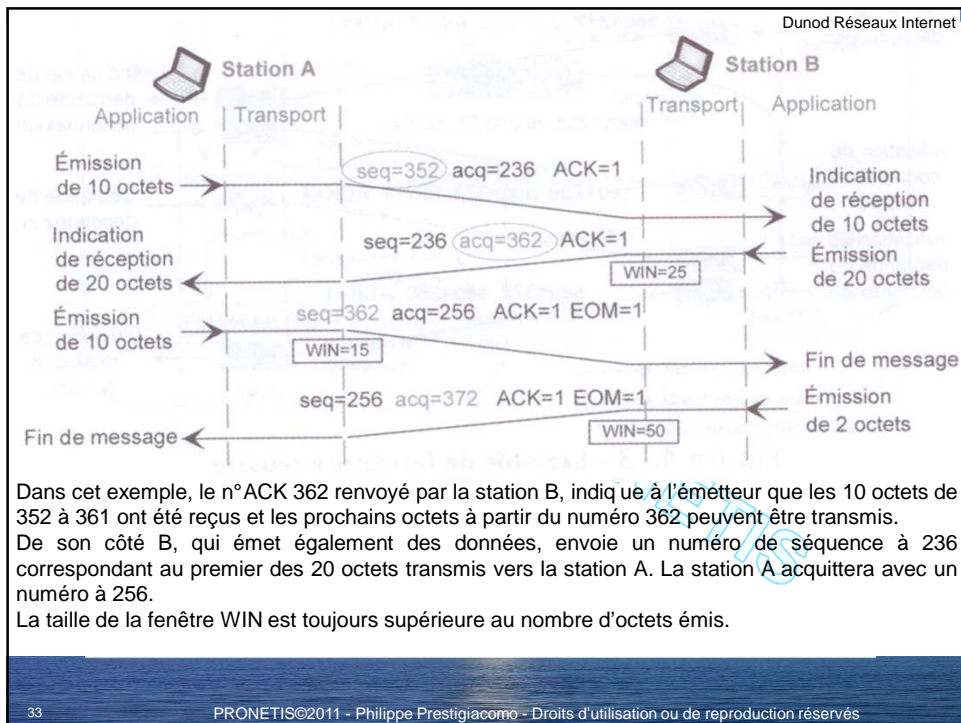
## TCP : Technique de fenêtrage

- Taille de la fenêtre
  - La taille de la fenêtre indique encore combien d'octets l'émetteur peut transmettre.
- Exemple :
  - Le champ fenêtre peut avoir une valeur nulle = indique que tous les octets reçus jusqu'au numéro d'accusé de réception (- 1) ont été reçus mais que le récepteur désire reprendre son souffle et ne désire plus recevoir de données pour l'instant.  
**Taille de la fenêtre à zéro = Saturation du récepteur**
  - L'autorisation d'émettre pourra être accordée un peu plus tard par l'envoi d'un segment avec le même numéro d'accusé de réception et un champ taille de fenêtre non nul.

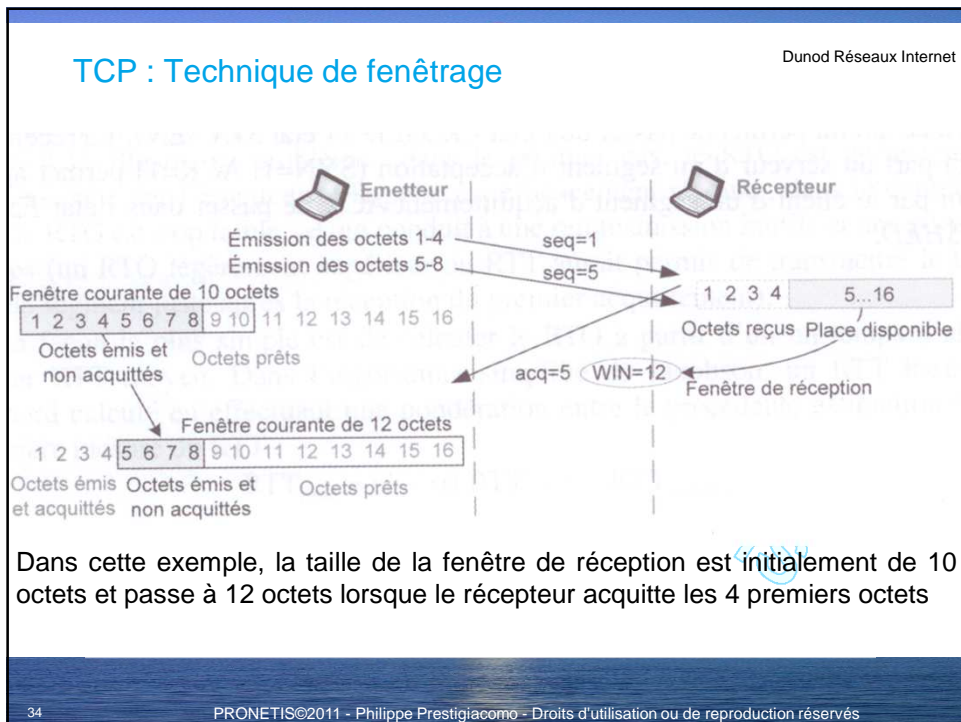
**Taille de la fenêtre = taille de la mémoire en octets du récepteur.**

32

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés



### TCP : Technique de fenêtrage





## UDP : User Datagram Protocol - Introduction

- Certaines applications et en particulier **les applications temps réel nécessitent des temps de traitement optimisés** (Visio conférence, Voix sur IP, Streaming Vidéo), d'autres n'ont que très peu de données à envoyer, comme par exemple le service de nom (DNS), d'autres encore n'ont nullement besoin d'un service fiable comme l'offre TCP, c'est par exemple le cas des informations de gestion de réseau (SNMP).
- Dans tous les cas cités ci-dessus, les mécanismes de TCP s'avèrent trop lourds et pénalisent les performances.
- Un mode de transport allégé a été défini, c'est UDP (User Datagram Protocol)

37

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## UDP : User Datagram Protocol

- **UDP est un protocole orienté sans connexion**, c'est-à-dire, qu'il n'offre pas de fonction de contrôle sur le bon acheminement des segments et leur ordonnancement.
  - Aucune vérification de la livraison des messages
  - Pas de réassemblage des messages entrant
  - Pas d'accusé de réception
  - Aucun contrôle de flux
- UDP offre l'**avantage de nécessiter moins de bande passante que TCP**. Il peut être **intéressant d'utiliser ce protocole** pour des **messages ne nécessitant pas de contrôle de transmission, ou bien, sur des réseaux « fiables »**.

38

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Caractéristiques de UDP

### User Datagram Protocol

- Protocole sans connexion (non fiable)
  - Pas d'overhead pour la gestion des connexions
  - Adapté pour les applications du type requête/réponse
- Protocole plus simple
  - Moins d'overhead
  - Fournit un service plus rapide (moins de traitement)
  - Possibilité de diffusion

### Construit sur les services de la couche IP et fournit

- Un adressage de niveau applicatif
- Des possibilités facultatives de détection d'erreur

39

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

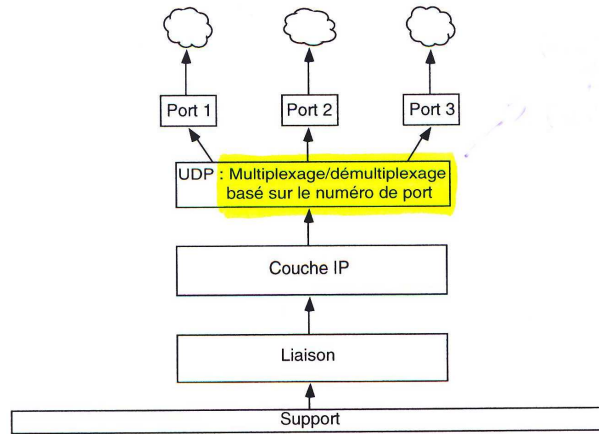
## Numéros des ports UDP

Numéro de port	Protocole
7	Echo
9	Discard
11	Utilisateurs actifs (sysstat)
13	Daytime (daytime)
15	netstat
19	Générateur de caractères (chargen)
37	Temps (time)
43	Qui est (whois)
53	Serveur de nom de domaine (nameserver)
67	Serveur de protocole de démarrage (bootps)
68	Client de protocole de démarrage (bootpc)
69	Protocole trivial de transfert de fichiers (tftp)
111	RPC de SUN Microsystems (sunrpc)
123	Protocole de temps réseau (ntp)
161	Gestionnaire de réseau SNMP (snmp)
162	Traps de SNMP (snmp-trap)

40

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Multiplexage et numéro de port UDP



Les numéros de port UDP sont indépendants des numéros de port TCP

41

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Pause-réflexion

Avez-vous des questions ?



42

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

## Résumé du module

**Protocole  
UDP**

**Protocole  
TCP**

**Numérotation  
des ports TCP /  
UDP  
– Multiplexage  
des connexions**

**Mécanisme de  
fenêtrage et  
contrôle de flux**

**Protocoles  
orientés  
connexion et  
sans connexion**

43

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

**FIN DU MODULE**

44

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés