Master SDRP
Réseau Avancé
Partie 2: TCP IP

Philippe Gros Session 2005-2006

Le modèle Arpanet

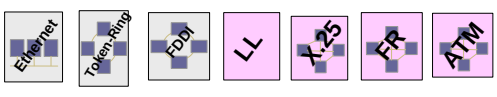
- **1969** Naissance D'ARPANET *(Advanced Research Projet Agency NETwork)*
- **1973** Démonstration d'ARPANET et création de l'IETF
- **1975** UNIX et TCP/IP: définition de TCP par l'IETF
- **1980** Berkeley fournit les versions 4.1 BSD contenant TCP
- **1983** TCP remplace définitivement NCP
- **1996** IPng devenu IPv6 voit le jour

2

Le modèle Arpanet
Comment IP se situe dans les réseaux ?

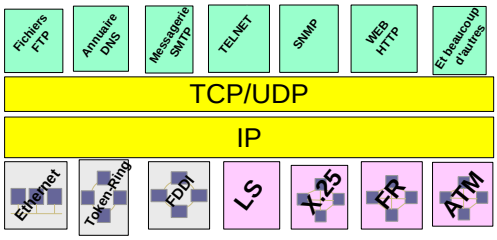
Le réseau Internet est constitué d'infrastructures de réseau de tous types :

- Des réseaux locaux
- Des liaisons point à point: RTC, RNIS, LS
- Des réseaux à commutation de paquet



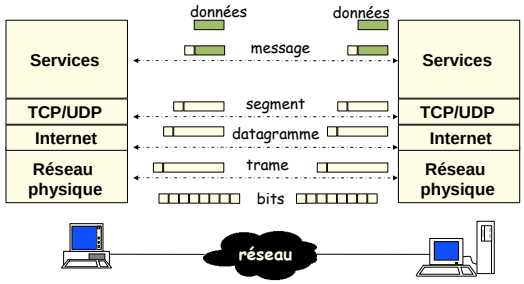
3

Le modèle Arpanet
IP offre des services



4

Le modèle Arpanet:Encapsulation IP



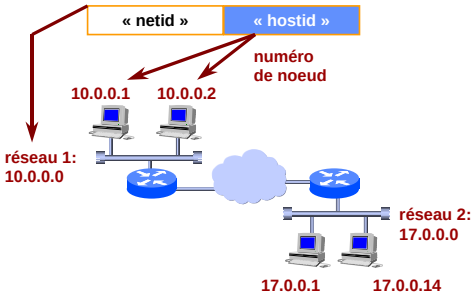
Adressage

Adressage public

- Dans le modèle IP
  - Norme RFC 1518
  - Adresses gérées par l'Internic
    - Pour IP v4 : 32 bits d'adresses, soit 4264967296 possibilités (arrive à saturation)
    - Pour IP v6 : 128 bits d'adresses, soit 3.40228237*10 exp 38 possibilités (10exp12 = 1 trillion)

6

Adressage: Netid Hostid



7

Adressage IP V4

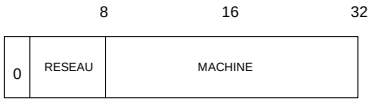
- Pour IP v4
  - 1 adresse = adresse de réseau (préfixe) + adresse de l'hôte (suffixe)
  - Adresse décimale pointée

124	.	10	.	45	.	126
01111100		00001010		00101101		01111110

8

Adressage Classe A

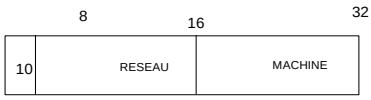
- 4 classes d'adresses en mode *pleine classe :*
  - Classe A : préfixe = 8bits, suffixe = 24 bits
    varie de 1.0.0.0 à 127.255.255.255 (0.0.0.0 est considéré comme réseau par défaut) : 127 réseaux et (16777216 -2) hôtes



9

Adressage Classe B

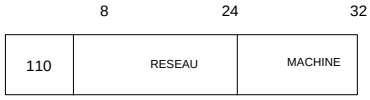
- Classe B : préfixe = 16 bits, suffixe = 16 bits
  varie de 128.0.0.0 à 191.255.255.255 : 16384 réseaux et (65535-2) hôtes



10

Adressage Classe C

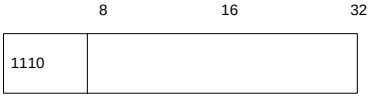
- Classe C : préfixe = 24 bits, suffixe = 8 bits
  varie de 192.0.0.0 à 223.255.255.255 : 2 097 152 réseaux et (256-2) hôtes



11

Adressage Classe D

- Classe D : préfixe = 4 bits, suffixe = 28 bits
  Adresses de groupes (multicasts), il y a 28-2 hôtes possibles par sous-groupe; varie de 224.0.0.0 à 239.255.255.255



- Classe E: Expérimentale 240.0.0.0 à 254.255.255.255 non utilisée dans l 'internet

12

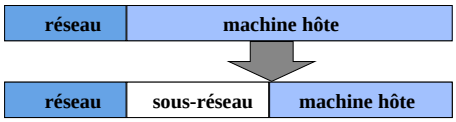
Adressage: Broadcast

- Adresse de réseau et de diffusion (broadcast)
  - Classe A
    - 123.0.0.0 est l'adresse de réseau du sous-réseau 123/8
    - 123.255.255.255 est l'adresse de diffusion du sous-réseau 123/8
  - Classe B
    - 172.123.0.0 est l'adresse de réseau du sous-réseau 172.123/16
    - 172.123.255.255 est l'adresse de diffusion du sous-réseau 172.123/16
  - Classe C
    - 201.233.65.0 est l'adresse de réseau du sous-réseau 201.233.65/24
    - 201.233.65.255 est l'adresse de diffusion du sous-réseau 201.233.65/24
      - REMARQUE : ces adresses (réseau et diffusion) ne sont pas disponibles pour les hôtes

13

Adressage: les masques

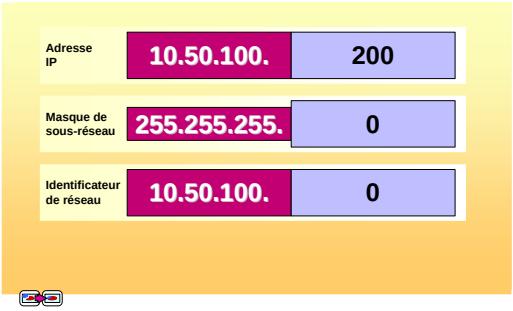
- Principe du sous-réseau



- C 'est le masque de sous réseau qui fait ce découpage

14

adressage: Exemple de sous réseaux



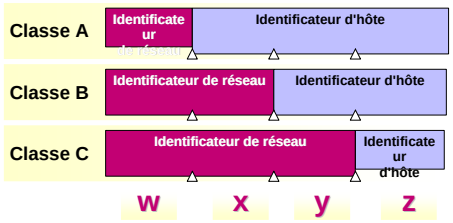
15

Adressage: double représentation des adresses

- Double représentation des adresses
- Préfixe CIDR (Classless Interdomain Routing)
  - Adresse IP / masque de sous-réseau :
    ex. 123.244.210.32 255.0.0.0
    123.244.210.32 : **01111011**.11110100.11010010.00100000
    255.0.0.0 :**11111111**.00000000.00000000.00000000
  - Préfixe : 123.244.210.32/8 indique que les 8 premiers bits sont significatifs pour le réseau
  - Classe A, masque : 255.0.0.0, préfixe /8
  - Classe B, masque : 255.255.0.0, préfixe /16
  - Classe C, masque : 255.255.255.0, préfixe /24
  - Classe D, masque : 255.255.255.n, préfixe /P

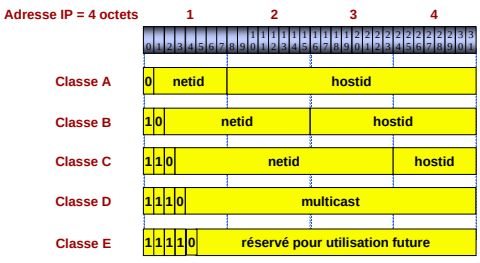
16

Adressage: Les classes d'adresses



17

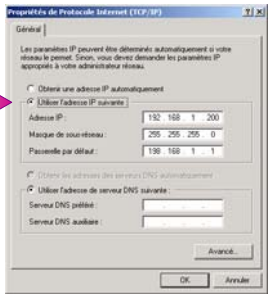
3 Adressage: Les classes d'adresses



18

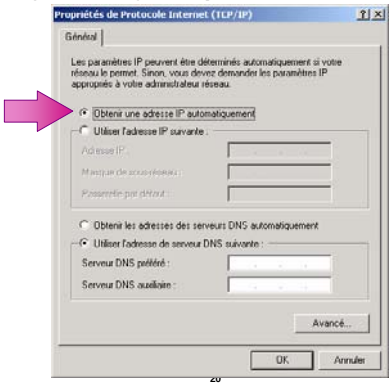
Configuration statique

- 1 Adresse IP
- 2 Subnet Mask
- 3 Default Gateway/passerelle par défaut -> désigne l'aiguilleur pour sortir du réseau



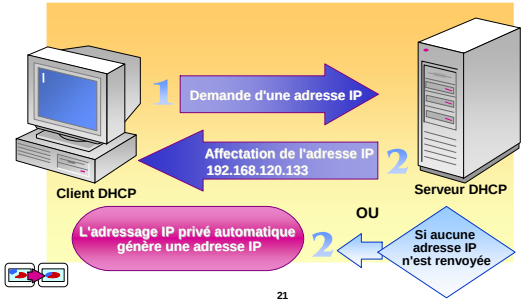
19

Configuration dynamique: DHCP



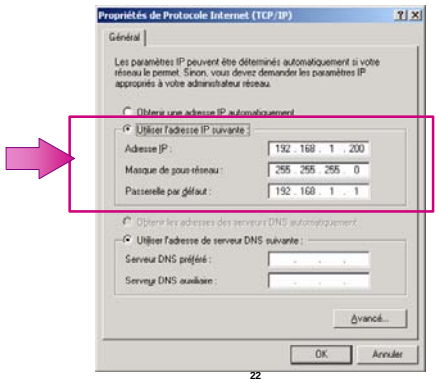
20

Configuration dynamique: DHCP



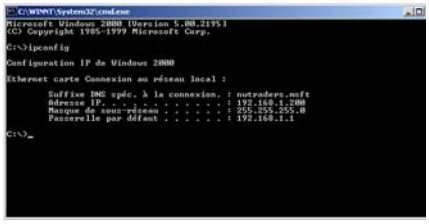
21

Affichage des élements réseaux



22

Affichage des élements réseaux



23

Adressage Exercices

- Exercice
  - Trouver les classes, préfixes, masque de sous-réseau et adresses de diffusion des adresses suivantes :
    - 12.5.124.32
    - 125.23.32.0
    - 173.33.134.15
    - 192.44.156.0
    - 255.233.23.0
    - 202.233.255.255

24

Adressage VLSM

- Classless et VLSM *(Variable-Length Subnet Masking)*
  - Il est possible de prendre des préfixes non standards afin d'optimiser la répartition des adresses. Cette méthode permet de segmenter les plages d'adresses des classes A, B et C.

25

Adressage VLSM

- Subnetting d 'une classe C en 8 réseaux de 32-2 hôtes possibles:
  - Réseau198.1.1.0
    - **1100 0110. 0000 0001.0000 0001. 000**0 0000
  - masque: 255.255.255.224
    - **1111 1111.1111 1111. 1111 1111. 111**0 0000
  - Subnet 1 198.1.1.0
  - Adresse de Broadcast du subnet1 198.1.1.31
  - Subnet 2 198.1.1.32
  - Adresse de Broadcast du subnet 2 198.1.1.63

26

Adressage CIDR

# Subnet Bits et CIDR	# Subnets	# Host Bits	# Hosts	Mask
1: /25	2	7	126	255.255.255.128
2:/26	4	6	62	255.255.255.192
3:/ 27	8	5	30	255.255.255.224
4: /28	16	4	14	255.255.255.240
5: /29	32	3	6	255.255.255.248
6: /30	64	2	2	255.255.255.252

27

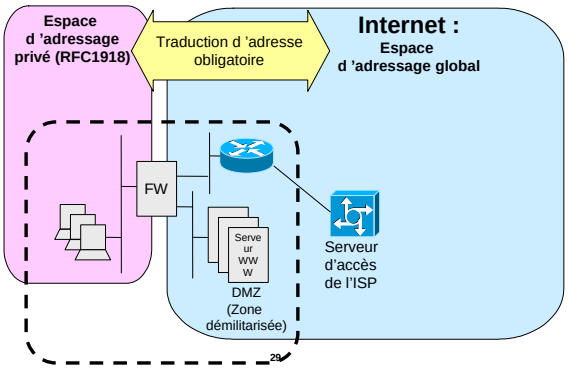
Adressage RFC 1918

Plan d'adressage privé

- Pour des raisons de peu de disponibilité des adresses IP et de sécurité, la RFC 1918 réserve les plages d'adresses suivantes aux réseaux privés :
  - Classe A : 10/8
  - Classe B : 172.16/16
  - Classe C : 192.168/16
- L'interconnexion entre les adresses publiques et un réseau privé exige une traduction d'adresses (NAT: Network Address Translation) faite par des routeurs ou des garde-barrières:
  - traduction une pour une
  - traduction par multiplexage des ports TCP (Port Adress Translation)

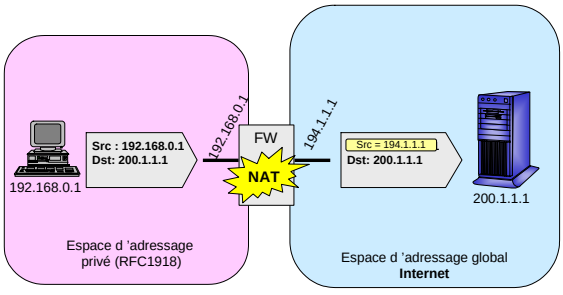
28

adressage: adresses privées



29

adressage: NAT



30

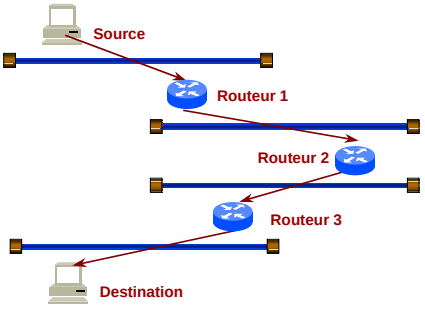
Routage

Cinématique

- Dans chaque hôte, il y a une table de routage avec l'adresse IP, le masque de sous-réseau et une passerelle par défaut
- Chaque routeur construit dynamiquement le plan du réseau avec toutes les adresses des sous-réseaux et le chemin pour les atteindre

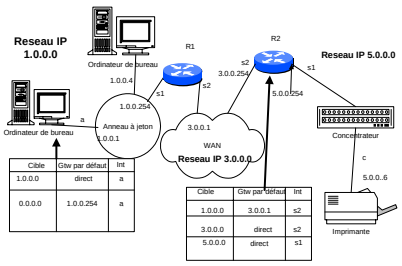
31

Routage



32

Routage



33

Routage Exercice

- Exercice
  - Trouver la table de routage du routeur R1 et de la carte réseau de l'imprimante

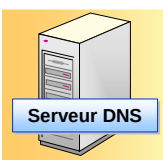
34

Routage: Un exemple de table de routage

- DHCP Server: Serveur dynamique d'adresses IP.(Dynamic Host Control Protocol)
- DNS (Domain Name Server): Serveur de nom de domaine (par exemple domaine.com) qui associe un nom de domaine a une adresse IP.

35

Routage: DNS et Wins

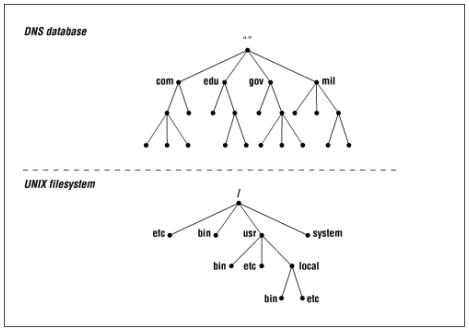


- Le système DNS est un système qui permet de nommer les ordinateurs et les services réseau
- Le système de dénomination DNS est organisé de façon hiérarchique
- Mappe les noms de domaine sur des adresses IP
- Les enregistrements de mappage sont stockés sur un serveur DNS

- Fournit une base de données distribuée pour l'inscription des mappages dynamiques de noms NetBIOS
- WINS mappe les noms NetBIOS sur des adresses IP

36

routage: arborescence DNS



37

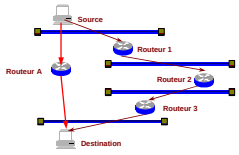
Protocole de routage versus protocole routé

- IP est un protocole routé, c'est-à-dire qu'il contient une adresse réseau permettant de connaître les points d'origine et de destination des trames
  - Les routeurs ou aiguilleurs doivent reconnaître ces adresses mais surtout avoir la topologie de l'ensemble des réseaux afin de trouver la meilleure route
- C'est le rôle des protocoles de routage tels que RIP, OSPF, IGRP, E -IGRP de le faire

38

Routage RIP

- Exemple de protocole de routage RIP V1 (Routing Information Protocol)
- 2 routes possibles
  - S->R1->R2->R3->D
  - S->A->D
- RIP choisira le nombre de sauts (hops) le plus courts avec un maximum de 15



39

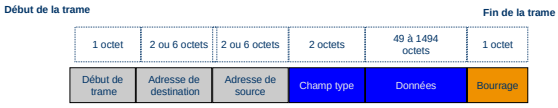
Protocoles ARP et RARP

- Problème
  - Les hôtes connaissent l'adresse de réseau de leur destination mais ignorent les adresses de couches 2 (MAC) pour les atteindre et construire les trames Ethernet. C'est à ARP et RARP de les aider à les découvrir.
    - Cette correspondance est alors mémorisée dans la table ARP des hôtes.

40

Protocoles ARP et RARP (suite)

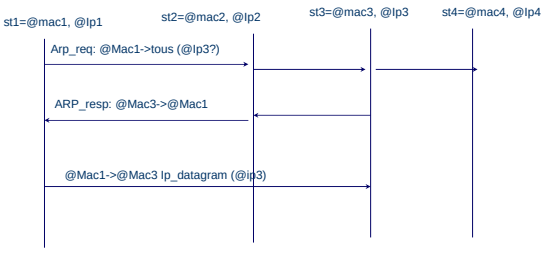
- La Trame Ethernet



41

Protocoles ARP et RARP (suite)

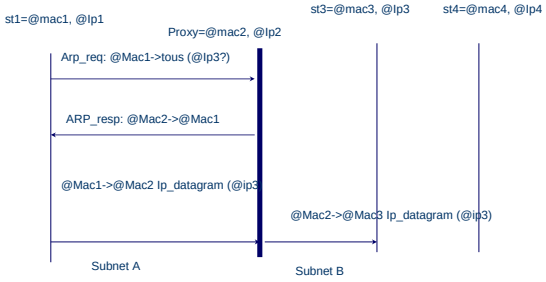
- Cinématique de ARP



42

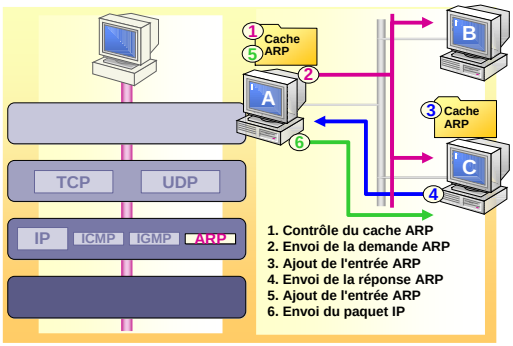
Protocoles ARP et RARP (suite)

- Réponse par Proxy ARP(ex. proxy)



43

Protocoles ARP et RARP



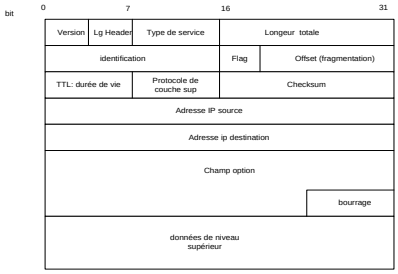
44

Protocoles IP et ICMP

- IP sert à interconnecter des réseaux indépendants
  - Caractéristiques
    - possibilité de segmentation et de réassemblage
    - mode datagramme sans garantie d'acheminement et de séquencement
    - Détection d'erreurs mais pas de correction
    - Contrôle de flux (limité), destruction des datagrammes en cas de manque de ressource dans les noeuds ou si durée de vie trop longue
    - Possibilité de connaître les chemins suivis et de choisir un chemin particulier
    - Possibilité de donner des niveaux de priorité aux datagrammes

45

Protocoles IP et ICMP (suite)



46

Protocoles IP et ICMP (suite)

- Quelques champs importants
  - Type de service donne la priorité
  - Longueur totale donne la longueur du datagramme courant
  - Champs identification et offset servent aux réassemblages en cas de fragmentation
  - TTL : de 0 à 255, incrémenté de 1 à chaque passage de routeur. Si TTL= 255, destruction du datagramme
  - Champ protocole : ex. 0x01 ICMP, 0x06 TCP, 0x11 UDP
  - Checksum uniquement sur l'en-tête IP
  - Champ option permet de donner des précisions aux routeurs ou hosts, ex. sécurité, chemin obligatoire, demande de trace, mesure et maintenance

47

Protocoles IP et ICMP (suite)

- Flags (3 bits)
  - Bit 0: réservé, doit être laissé à zéro
  - Bit 1: (AF) 0 = Fragmentation possible, 1 = Non fractionnable.
  - Bit 2: (DF) 0 = Dernier fragment, 1 = Fragment intermédiaire.

  0 1 2
  | | A | D |
  | 0 | F | F |
- Décalage fragment
  - Position de ce fragment relatif au début du datagramme original
- TTL
  - *Time To Live*. Compteur décrémenté par chaque aiguilleur traversé
- Protocole
  - Type de protocole dans le datagramme IP

48

Protocoles IP et ICMP (suite)

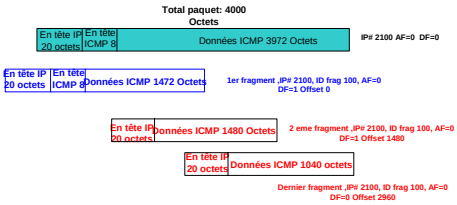
La fragmentation

- Selon la norme un paquet IP peut avoir une longueur de 65535 octets.
- En général les stack TCP/IP ne créent pas des paquets > 4000 octets.
- Le Maximum Transmit Unit (MTU) d 'un réseau décrit la longueur maximale admissible par un réseau IP sur un réseau donné.

49

Exemple defragmentation

- Exemple de Fragmentation: Soit un paquet ICMP de 4000 octets et un MTU de 1500 octets.



50

Protocoles IP et ICMP (suite)

- ICMP est encapsulé dans IP et sert à gérer le réseau
- Il est principalement utilisé par les aiguilleurs et certains hôtes
  - Gestion d'écho : Ping : ICMP_ECHO_REQ ---> ICMP_ECHO_RESP. (exemple ping 192.0.0.1)
  - Message d'erreur : ICMP_UNREACHABLE_DEST (réseau, hôte, protocole, port, fragmentation impossible, échec du source routing)
  - Contrôle de flux : ICMP_SOURCE_QUENCH
  - Redirection : ICMP_REDIRECT: signifie à un hôte qu'un chemin est plus approprié
  - Time-out : ICMP_TIME_OUT : ex. TTL atteint

51

Protocoles IP et ICMP (suite)

- ICMP (suite)
  - Erreur d'en-tête : ICMP_HEADER_ERROR
  - Gestion des horloges : ICMP_CLOCK_REQ et ICMP_CLOCK_RESP
  - Récupération de l'adresse de réseau par un hôte (comme RARP) : ICMP_INF_REQ, ICMP_INF_RESP
  - Récupération du masque de réseau : ICMP_MASK_REQ, ICMP_MASK_RESP

52

UDP *(User Datagram Protocol)*

- UDP met en relation des processus entre 2 hôtes (communication inter-processus)
  - Caractéristiques
    - mode non connecté
    - pas de segmentation et reséquencement
    - détection d'erreurs, pas de correction
    - full-duplex
    - pas de contrôle de flux
      - Un seul type de datagramme existe : UDP_DATA

53

UDP et TCP (suite)

- UDP (suite)
  - Certains services sont référencés par des numéros de ports réservés appelés «*Well Known Ports*»
    - echo 7/udp
    - time 37/udp
    - tftp 69/udp
    - sunrpc 111/udp
    - who 513/udp
    - syslog 514/udp
  - Pour les services non référencés, il y a une attribution dynamique d'un numéro de port
  - Sert pour des services non vitaux comme la gestion (SNMP), la journalisation, BOOTP, DHCP

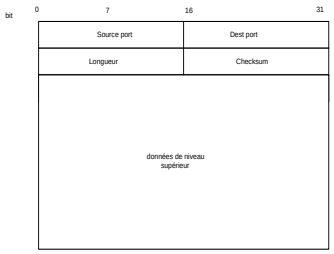
54

UDP et TCP (suite)

- N'offre aucune fiabilité
- Une connexion UDP/IP est caractérisée par le quadruplet adresses et numéros de port
  - Adresse IP source
  - Numéro de port de la source
  - Adresse IP destination
  - Numéro de port de la destination

55

UDP et TCP (suite)



56

UDP et TCP (suite)

- Port source
- Port destination
- Longueur
  - longueur de l'en-tête UDP + les données
- Somme de contrôle
  - effectuée sur l'en-tête UDP et les données

57

UDP et TCP (suite)

7.2 TCP *(Transmission Control Protocol)*

- Il permet d'assurer une transmission fiable des données et notamment de résoudre les problèmes non traités par les couches inférieures (erreurs, congestion)
  - Caractéristiques
    - Mode connecté
    - Transport orienté octet
    - Segmentation et reséquencement des données
    - Full-duplex
    - Détection d'erreurs
    - Contrôle de flux de bout en bout

58

UDP et TCP (suite)

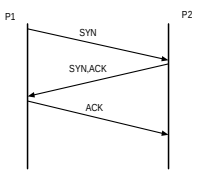
TCP (suite)

- Utilise également la notion de port de «Well Known Ports»
  - Exemples
    - echo 7/tcp
    - systat 11/tcp
    - ftp-data 20/tcp
    - ftp 21/tcp
    - telnet 23/tcp
    - smtp 25/tcp
    - x400 103/tcp
    - news 144/tcp
    - login 513/tcp

59

UDP et TCP (suite)

- TCP (suite)
  - Mécanismes de connexion
    - TCP_SEG_SYN
    - TCP_SEG_SYN_ACK
    - TCP_SEG_ACK
      - Le mode connecté entre 2 hôtes (a et b) se fait par l'échange des ports et de numéros de synchronisation unique et propre à chaque hôte :
        - (port source a, port dest b, sync a, sync b)



60

UDP et TCP (suite)

- Protocole avec connexion
- Un circuit doit être établi avant la transmission de données
- Une connexion TCP/IP est caractérisée par un quadruplet

61

UDP et TCP (suite)

- Numéro de séquence
  - Identifie un flux de données
  - Nombre aléatoire initialement et incrémentation à chaque transmission
- Numéro d'accusé (*acknowledgment*)
  - Utilisé lorsqu'une connexion est établie.

62

UDP et TCP (suite)

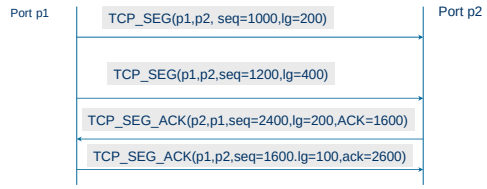
- Drapeaux
  - URG
    - champ pointeur urgent est valide
  - ACK
    - drapeau d'accusé de réception
  - PSH
    - pousse les données vers l'application en priorité
  - RST
    - ré-initialisation de la connexion
  - SYN
    - synchronise les numéros de séquence
  - FIN
    - termine la transmission

63

UDP et TCP (suite)

7.2 TCP (suite)

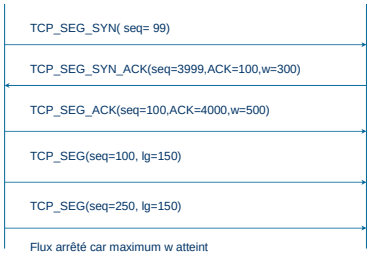
– À chaque échange, il y a en même temps que le transport des données un accusé de réception des données reçues



64

UDP et TCP (suite)

- TCP : le contrôle de flux *(Windowing)*



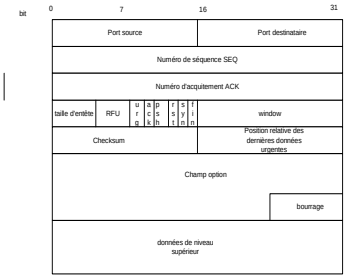
65

UDP et TCP (suite)

- TCP : le contrôle de flux
  - Le ralentissement peut être rapide par échange de w=0 qui oblige le distant à arrêter d'émettre
  - Il est possible de donner une notion d'urgence à la remise des données aux couches supérieures par les commandes suivantes :
    - TCP_SEG_PUSH (demande de remise sans utilisation de tampons (buffering))
    - TCP_SEG_URG (signifie que les échanges suivants sont à traiter en mode urgent)
  - Les déconnexions se font de 2 façons :
    - Mode normal : TCP_SEG_FIN -> TCP_SEG_ACK
    - Mode anormal : TCP_SEG_RST

66

UDP et TCP (suite)



SNMP *(Simple Network Management Protocol)*

- Protocole défini par la norme RFC 115 servant à administrer les réseaux et les éléments de réseaux (hôtes, concentrateurs, ponts, routeurs, etc.)
  - Chaque élément de réseau possède un agent qui détient des informations sur son état
  - Une station de gestion sur le réseau (HP OpenView, Sun NetManager) interroge, configure et reçoit des informations grâce à ce protocole

SNMP (*Simple Network Management Protocol,* suite)

- Il existe plusieurs versions de SNMP qui renforcent sa sécurité et ses capacités
  - SNMPv2
  - SNMPv3
  - Les informations de chaque élément de réseau sont maintenues dans une MIB (Management Information Base)
    - MIB I
    - MIB II
    - MIB propriétaires

SNMP (*Simple Network Management Protocol*, suite)

- SNMP fonctionne avec UDP (ports 160 et 161)
  - Les PDU sont :
    - GetRequest
    - GetNextRequest
    - GetResponse
    - SetRequest
    - Trap

70

Sécurité

- TCP/IP en tant que tel ne comporte que peu d'éléments de sécurité
  - C'est aux éléments de réseaux (routeurs, garde-barrières) à mettre en œuvre des éléments de sécurité tels que :
    - Filtrage sur adresses IP ou MAC
    - Filtrage sur les ports UDP/TCP
    - Sélection des applications de couches hautes

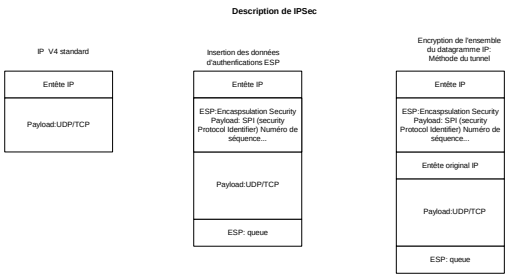
71

Sécurité

  - C'est aussi aux hôtes à intégrer des éléments de sécurité:
    - Réseau privé virtuel (Virtual Private Network ou VPN)
    - SSL (Secure Socket Layer)
    - IPsec

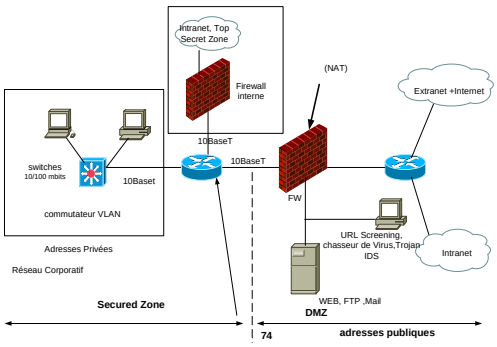
72

Sécurité (suite): IPsec



73

Sécurité: Exemple d 'architecture à coupe feu



74

Avenir de TCP / IP

- IP V6 pour
- SNMP v3 et basé sur Web :
  - MIB et méthodologie objet
  - Interface portée sur Web
  - Sécurité accrue
- IP et la téléphonie
- IP et la vidéo : RSVP, gestion des multicasts

75

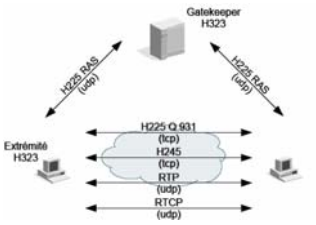
Avenir de TCP / IP : La téléphonie IP

- H225 Remote Access
  Serveur Enregistrement
  au Gatekeeper
- H225/Q931: Signalisation
- H245 Contrôle

H.225 RAS	Signalisation H.225/Q.931	Contrôle H.245
UDP	TCP	
Couche réseau		
Couche liaison		

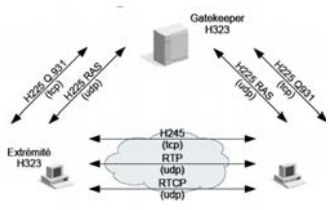
76

Voix sur IP Signalisation Directe



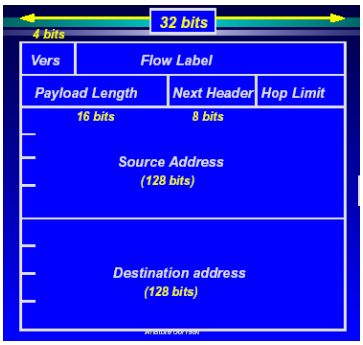
77

Voix sur Ip Signalisation routée vers le Gatekeeper



78

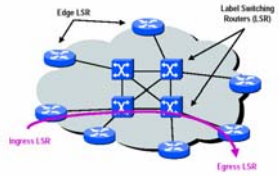
Le paquet IP V6



79

Avenir de TCP / IP: Mpls et QoS

- Gestion des priorités et de la qualité de service:
  - Diffserv: Differentiated Services RFC 2475
- Création de réseaux virtuels privés:
  - MPLS: Multiple Label Switching



80

Liste des RFC TCP / IP classée par couches

- Couche Réseau
  - IP (RFC 792) : Internet Protocol
  - ICMP (RFC 792) : Internet Control Message Protocol
- Couche Transport
  - UDP (RFC 768) : User Datagram Protocol
  - TCP (RFC 793) : Transmission Control Protocol
- Administration de routage
  - ARP : Address Resolution Protocol
  - RARP : Reverse ARP
  - IGP: Internal Gateway Protocol.
    - Ex: RIP (Routing Information Protocol), OSPF (Open Short Path First)
  - EGP: External Gateway Protocol.
    - Ex: BGP (Border Gateway Protocol)

81

Liste des RFC TCP / IP classée par couches

- Couches Sessions, Présentation et Application
  - TELNET: TELecommunication NETwork (couches 5, 6, 7)
  - XDR : eXternal Data Representation (couche 6)
  - SMTP : Simple Mail Transfer Protocol
  - DNS : Domain Name Service (couche 7)
  - FTP : File Transfer Procotol (couches 5, 6, 7)
  - SNMP : Simple Network Management Protocol (couches 5, 6, 7)
  - RPC : Remote Procedure Call (couches 5, 6, 7)
  - NFS : Network File System

82