LES SAUVEGARDES LE WIFI ET ETHERNET

I) LES SAUVEGARDES

Sauvegardes normale : attribut d'archive réinitialisé
Sauvegardes incrementielle :sauvegarde que les fichiers modifiés, réinitialise attribut d'archive
Sauvegarde différentielle :sauvegarde les fichiers modifiés depuis la dernière sauvegarde normale

I.a) Les logiciels de sauvegarde

Logiciels : arcserve, backup.exe, ntbackup, autobackup

II) LE WIFI

II.a) Caracteristiques

- La communication s'effectue sur quelques dizaines de mètres
- Les antennes de gain autorise plusieurs centaines de mètres

II.b)Les normes de couche physique

- **802.11b** : vitesse 11 MBPS fréquence 2.4Ghz SSID (service set identifier)
- **802.11a** : 54 mbps , 5ghz
- **802.11g** : 54 MBPS , 2.4ghz
- **802.11n**: 200 mbps , 50 metres , 2.4 et 5ghz
- **802.11ac**: 5ghz, 6ghz , 7 gbps

II.C) Materiels pour mettre en place le wif

- **Carte réseau wifi**
- **Equipements d'infrastructure** : interconnexion du wifi au filaire (DS_distribution system)
- **Points d'acces** : AP
- **Pont** : permet d'interconnecter deux réseaux filaires entre eux

II.d) Architecture wifi

- **Egal à Egal** : reseal ad hoc **IBSS** : independent basic service set
- **Point d'acces** : BSS basic service set
- **Plusieurs points d'accès**: extended service set (ESS) déplacement au sein de l'entreprise en s'associant au point le plus proche (itinérance)

II.e) Sécurisation

- **WPA** : s'appuie sur le protocole TKIP (temporal key integrity) avec des clés plus longues que les clés wep. Permet l'échange dynamique de clé
- **WPA personnel** : pas de serveur d'authentification
- **WPA entreprise** : service RADIUS (remote authentification dial in user service) s'appuie sur un chiffrement AES (advanced encryption standart) (authentification, chiffrement, signature, comptage de trame)
- **WPA2** :chiffrement avec AES

II.f) Methode de communication : CSMA/CA

Avant d'émettre des données vers un point d'accès une station doit être connecté au basic service set (BSS) réseau de l'équipement maître. Un processus d'association est nécessaire, et une authentification de la station par le point d'accès.

II.g) L'en tête de trame wifi est plus complexe que son pendant internet.

Frame control	Duration /id	Address1	Address2	Address3	Sequence control	Address4	Qos control	Ht control	Frame body	FCS
2	2	6	6	6	2	6	2	4	0-7955	4

Les champs adresses :
La structure d'adressage 802.11 est plus riche que pour un réseau filaire. Car si on veut accéder à une station du même réseau (BSS), il faut passer par le point d'accès donc indiquer son adresse MAC pour qu'il relaie le paquet. De même pour accéder à une station d'un autre réseau (ESS), deux adresses intermédiaires peuvent être indiquées. Ces champs d'adresses sont définis en accord avec les indications des champs To DS et From DS.

les quatre types d'adresse sont :

-**DA (Destination Address)** : adresse, individuelle ou de groupe, identifie le(s) destinataire(s).

-SA (Source Address) : adresse individuelle ayant transmis la trame.

-RA (Receveir Address) : BSSID destination (point d'accès récepteur).

-TA (Transmitter Address) : BSSID source (point d'accès émetteur).

III) Structure ethernet II et correspondance avec les captures wireshark

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14 … 1513	1514	1515	1516	1517
Adresse MAC destination						Adresse MAC source						Type de protocole		Données	FCS/CRC			

Capture wireshark

```
Ethernet II, Src: Anovo_e9:5c:07 (40:5a:9b:e9:5c:07), Dst: LiteonTe_ec:c3:fe (70:1a:04:ec:c3:fe)
  Destination: LiteonTe_ec:c3:fe (70:1a:04:ec:c3:fe)
      Address: LiteonTe_ec:c3:fe (70:1a:04:ec:c3:fe)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Anovo_e9:5c:07 (40:5a:9b:e9:5c:07)
      Address: Anovo_e9:5c:07 (40:5a:9b:e9:5c:07)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    Padding: 203311472033
```

Structure Internet protocol version 4

En-tête IPv4

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version d'IP				Longueur de l'en-tête				Type de service								Longueur totale															
Identification																Indicateur			Fragment offset											
Durée de vie								Protocole								Somme de contrôle de l'en-tête															
Adresse source																															
Adresse destination																															
Option(s) + remplissage																															

Version (4 bits) :

Version d'IP utilisée. Ici, 4.

Longueur de l'en-tête ou *IHL* (pour *Internet Header Length*) (4 bits) :

Nombre de mots de 32 bits, soit 4 octets (ou nombre de lignes du schéma). La valeur est comprise entre 5 et 15, car il y a 20 octets minimum et on ne peut dépasser 40 octets d'option (soit en tout, 60 octets).

Type de service ou *ToS* (pour *Type of Service*) (8 bits) :

Ce champ permet de distinguer différentes qualités de service différenciant la manière dont les paquets sont traités. Composé de 3 bits de priorité (donc 8 niveaux) et trois indicateurs permettant de différencier le débit, le délai ou la fiabilité.

Longueur totale en octets ou *Total Length* (16 bits) : Nombre total d'octets du datagramme, en-tête IP comprise. Donc, la valeur maximale est $(2^{16})-1$ octets.

Identification (16 bits) :Numéro permettant d'identifier les fragments d'un même paquet.

Indicateurs ou *Flags* (3 bits) :

Fragment offset (13 bits) :Position du fragment par rapport au paquet de départ, en nombre de mots de 8 octets.

Durée de vie ou TTL (pour *Time To Live*) (8 bits) :

Initialisé par l'émetteur, ce champ est décrémenté d'une unité généralement à chaque saut de routeur. Quand TTL = 0, le paquet est abandonné et un message ICMP est envoyé à l'émetteur pour information.

Protocole (8 bits) :

Numéro du protocole au-dessus de la couche réseau : TCP = 6, UDP = 17, ICMP = 1.
Ce champ permet d'identifier le protocole utilisé par le niveau supérieur :

Somme de contrôle de l'en-tête ou *Header Checksum* (16 bits) :

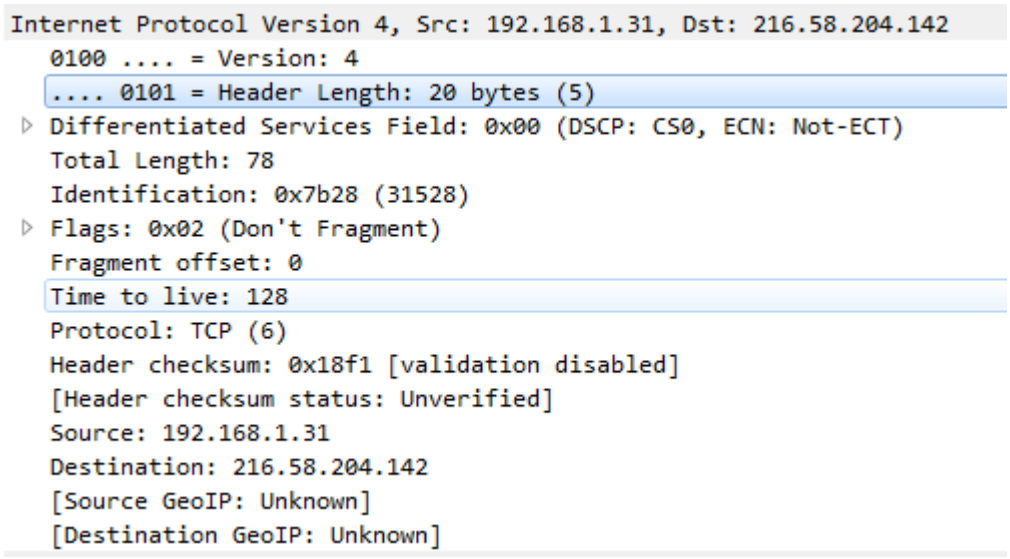
Adresse source (32 bits) :

Adresse destination (32 bits) :

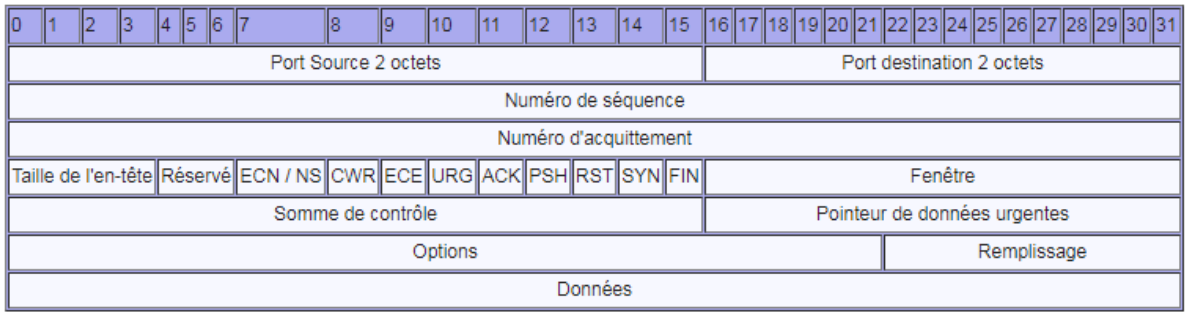
Options (0 à 40 octets par mots de 4 octets) :

Remplissage ou *Padding* :

Capture wireshark

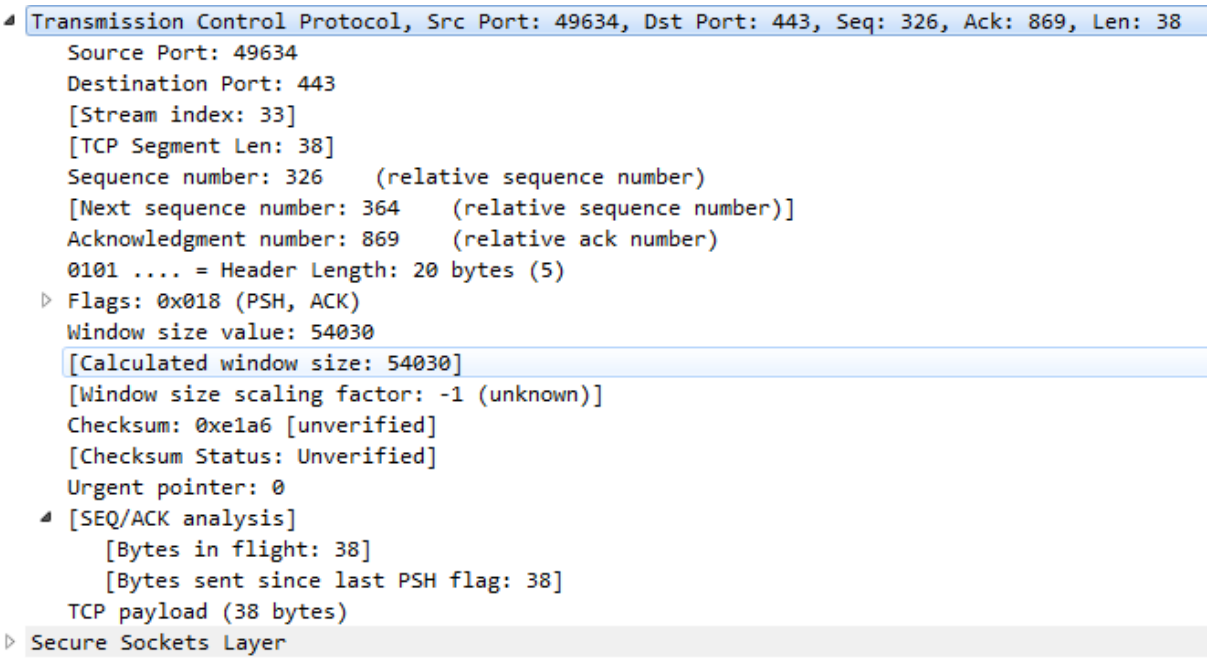


Structure d'un segment TCP



- Port source : numéro du port source
- Port destination : numéro du port destination
- Numéro de séquence : numéro de séquence du premier octet de ce segment
- Numéro d'acquittement : numéro de séquence du prochain octet attendu
- Taille de l'en-tête : longueur de l'en-tête en mots de 32 bits (les options font partie de l'en-tête)
- Indicateurs ou *Flags* :
  - Réservé : réservé pour un usage futur
  - ECN/NS : signale la présence de congestion, voir RFC 3168[3] ; ou Nonce Signaling, voir RFC 3540[4]
  - CWR : Congestion Window Reduced : indique qu'un paquet avec ECE a été reçu et que la congestion a été traitée
  - ECE : ECN-Echo : si SYN=1 indique la capacité de gestion ECN, si SYN=0 indique une congestion signalée par IP (voir RFC 3168)
  - URG : Signale la présence de données **urg**entes
  - ACK : signale que le paquet est un accusé de réception (**ack**nowledgement)
  - PSH : données à envoyer tout de suite (**push**)
  - RST : rupture anormale de la connexion (**reset**)
  - SYN : demande de **syn**chronisation ou établissement de connexion
  - FIN : demande la **fin** de la connexion
- Fenêtre : taille de fenêtre demandée, c'est-à-dire le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception
- Somme de contrôle : somme de contrôle calculée sur l'ensemble de l'en-tête TCP et des données, mais aussi sur un pseudo en-tête (extrait de l'en-tête IP)
- Pointeur de données urgentes : position relative des dernières données urgentes
- Options : facultatives
- Remplissage : zéros ajoutés pour aligner les champs suivants du paquet sur 32 bits, si nécessaire
- Données : séquences d'octets transmis par l'application (par exemple : +OK POP3 server ready...)

Capture wireshark



IV)La Communication sur ethernet

Dans un réseau local Ethernet en bus, maillé ou plus généralement filaire où plusieurs hôtes se trouvent sur un même segment de réseau, la méthode d'accès utilisée par les machines est le **CSMA/CD (Carrier Sense Multiple Access with Collision Detection**), pour lequel chaque machine est libre de communiquer lorsque le réseau est libre (aucun signal en cours). Chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine. Si c'est le cas, les deux machines patientent pendant un temps aléatoire avant de recommencer à émettre.

Dans un environnement sans fil ce procédé n'est pas toujours utilisable dans la mesure où deux stations voulant communiquer avec un récepteur commun peuvent être situées à l'opposé l'une de l'autre et ne s'entendent pas forcément mutuellement en raison du rayon de portée du signal radio1. Ainsi la norme **802.11** propose un protocole similaire appelé **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance**).

Le protocole **CSMA/CA** utilise un mécanisme d'esquive de collision basé sur un principe de négociation préalable et d'accusés de réception réciproques entre l'émetteur et le récepteur :

La station voulant émettre écoute le réseau. Si le réseau est occupé, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé **DIFS pour Distributed Inter Frame Space**), alors la station peut émettre. La station transmet un message appelé **Ready To Send** (ou **Request To Send**, noté RTS signifiant prêt à émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un **Clear To Send** (**CTS**, signifiant Le champ est libre pour émettre), puis la station commence l'émission des données. Toutes les stations avoisinantes patientent pendant un temps calculé à partir du CTS (ou du RTS, mais tous les voisins ne reçoivent pas forcément le RTS de la station émettrice en raison des rayons de portée radio).

À réception de toutes les données émises par la station, le récepteur envoie un accusé de réception **(ACK).**