

ITRAINONLINE MMTK

RESEAUX TCP/IP: NOTIONS AVANCEES

Préparé par : Alberto Escudero Pascual/ IT +46 <aep@it46.se>

| | |
|---|--------------------|
| ITRAINONLINE MMTK..... | 1 |
| RESEAUX TCP/IP: NOTIONS AVANCEES..... | 1 |
| Au sujet de ce document..... | 1 |
| Renseignements sur le droit d'auteur..... | 1 |
| Exigences..... | 2 |
| Modèles OSI..... | 2 |
| Contrôle de l'accès au média « MAC »..... | 3 |
| Protocoles de contrôle d'accès..... | 3 |
| Adresses MAC..... | 5 |
| Le cryptage du niveau lien..... | 5 |
| Couche lien (IP)..... | 6 |
| Les adresses..... | 6 |
| Contrôle des erreurs..... | 7 |
| Routage..... | 8 |
| NAT « Traduction de l'adresse du réseau »..... | 8 |
| IP tunneling et « IPSEC »..... | 9 |
| Couche Transport (TCP)..... | 11 |
| TCP « Protocole de contrôle des transmission »..... | 11 |
| UDP « User Datagram Protocol »..... | 11 |
| Couche 3 pare-feu..... | 12 |
| Couche logiciel d'application..... | 14 |
| Logiciel pare-feu..... | 14 |

Au sujet de ce document

Ces documents font partie du ItrainOnline MMTK. Le MMTK est un ensemble intégré de documents et de ressources de formation multimédia destiné à aider les médias communautaires, les centres multimédia communautaires, les télécentres et autres initiatives qui utilisent les technologies de l'information et des communications (TIC) à renforcer les communautés et soutenir le travail de développement.

Renseignements sur le droit d'auteur

Cette unité est présentée sous licence Creative Commons. Pour savoir comment utiliser ces documents, veuillez lire la déclaration sur le droit d'auteur accompagnant cette unité ou consulter

<http://creativecommons.org/licenses/by-sa/2.5/deed.fr>

Exigences

Afin de mieux utiliser cette unité, vous devriez avoir déjà une connaissance élémentaire des protocoles Internet, des nécessités de base de la connectivité de même des principes du routage et de l'adressage Internet.

Modèles OSI

Le modèle de référence OSI « *Open Systems Interconnection* », créé par l'ISO « International Standards Organization » est une description abstraite pour le design des protocoles de communications entre ordinateurs « computer network protocol design ». Le modèle divise les différentes fonctions de la communication en sept différentes couches qui peuvent toutes fonctionner indépendamment les unes des autres.

Un protocole suivant le modèle OSI adoptera les principes d'une pile. Le modèle de protocole en pile « stack » ou en couches implique que chacune des couches utilise une fonction de la couche qui lui est inférieure et fournit des services aux couches supérieures. Le protocole en pile peut être mis en place autant au niveau logiciel, au niveau équipement que par une combinaison des deux.

Plusieurs protocoles bien connus ne respectent pas le modèle OSI en pratique. Par exemple, l'Internet suivra plutôt un modèle à quatre niveaux de protocoles qui sont : la couche de contrôle d'accès au média, la couche réseau, la couche transport et la couche logiciel d'application

| Couche | OSI | TCP/IP |
|--------|------------------------|---------------------------|
| 7 | Logiciel d'application | Logiciel d'application |
| 6 | Présentation | |
| 5 | Session | Transport (TCP) |
| 4 | Transport | |
| 3 | Réseau | Réseau (IP) |
| 2 | Lien de données | Contrôle d'accès au média |
| 1 | Physique | |

Image 1: le modèle OSI vs le protocole TCP/IP



Les normes sans fil réfèrent normalement aux couches 1 et 2 de la pile de protocoles OSI, laissant intact la couche IP. Les « paquets IP » sont transportés sur les protocoles **sans fil spécifiques** physiques et lien de données.

Les normes sans fil (IEEE 802.11, IEEE 802.16, Bluetooth, IrDA etc...) traite des couches physiques et lien de données seulement et ont été traditionnellement créées pour faire circuler toutes sortes de données; les données IP étant seulement une des sortes de données. Les normes sans fil sont créées à l'extérieur du *Internet Engineering Task Force (IETF)*.

IEEE est l'une des références sur la normalisation du sans fil <http://standards.ieee.org/wireless>

Contrôle de l'accès au média « MAC »

Le couche de contrôle de l'accès au Média « Media Access Control – MAC » du modèle TCP/IP inclut la couche physique du modèle OSI qui gère les aspects les plus physiques de la communication (techniques de modulation, cryptage, accès physique aux média partagés, etc.) et le protocole *couche de lien* qui est responsable d'adresser et livrer les paquets d'un ordinateur à l'autre sur un canal commun.

En d'autres mots, la couche physique est responsable de convertir le signal électromagnétique en **bits** alors que la couche de lien est responsable de grouper ces bits en **paquets de données**.

Les couche de protocoles physique les plus communes sont RS-232, V.35, 10BASET, ISDN etc.
Les couches de protocoles de lien les plus communes sont Ethernet (IEEE 802.3), PPP, ATM etc.



Des protocoles de réseaux sans fils comme le IEEE 802.11 (WLAN) réfèrent autant aux couches de lien et physique du modèle OSI.

La famille de protocoles IEEE 802.11 gère différents protocoles physiques (PHY) basés sur le spectre FHSS, DSSS et OFDM

La norme original IEEE Std 802.11-1997 défini une seule couche de contrôle d'accès au Media « MAC » et 3 couches pour les spécificités physiques. La norme défini deux couches spécifiques pour la radio, opérant dans la bande 2400 – 2483,5 MHz (FHSS et DSSS) et une couche pour l'infrarouge

Pour information: <http://grouper.ieee.org/groups/802/11/main.html>

Protocoles de contrôle d'accès

CSMA « Carrier Sense Multiple Access » et détection des collisions « CD »

Le mécanisme le plus populaire de contrôle de l'accès physique,, où un ensemble d'ordinateurs accèdent à un média partagé, est l'Ethernet. Le protocole Ethernet ou IEEE 802.3 utilise un protocole d'accès à l'Internet appelé CSMA pour « Carrier Sense Multiple Access » qui est une version améliorée du schéma de contention technique appelé ALOHA.

Quand un node a des données à transmettre, il écoute d'abord le média pour savoir si un autre node sur le réseau est en train d'envoyer (en écoutant le canal partagé). Si aucune autre transmission n'est détectée, les données sont envoyées. Cela est possible bien que peu commun que deux nodes différents envoient simultanément des données car ils ont la capacité de détecter les temps morts sur le média. Lorsque que plusieurs envoyeurs font circuler en même temps des paquets de données, une collision se produira et les données seront corrompues. La collision sera détectée par le récepteur puisque le champ CRC et l'entête MAC ne sera pas associée correctement avec le contenu. Les données corrompus seront éliminés par le récepteur.

Le « CD » est un second élément du protocole d'accès Ethernet qui est utilisé par l'envoyeur pour détecter les collisions. Les nodes transmettant des données peuvent simultanément surveiller le média partagé et écouter ce que le média envoi. Si une collision est détectée (le node entend quelque chose de différent de ce qui fut envoyé), le node arrête la transmission et envoi une « jam sequence » pour informer le node récepteur de cette collision et que tout dce qui a pu être reçu doit être éliminé.

Dès qu'une collision est détectée, tous les nodes renvoient les données. Pour prévenir que les nouvelles retransmissions ne fassent de nouvelles collisions, Ethernet utilise un système aléatoire de priorités (basé sur un

coefficient aléatoire et le nombre de transmissions antérieures) de façon à calculer le temps d'attente jusqu'à la prochaine transmission. Ethernet vise à minimaliser la probabilité d'une nouvelle collision après une première détection.



IEEE 802.11 (WLAN)

La couche MAC de IEEE 802.11 (WLAN) est appelée CSMA/CA. Elle a beaucoup de similarités avec Ethernet. Elle utilise CSMA pour partager le média avec d'autres nodes sans fil, mais sans utiliser « CD ». L'envoyeur ne peut pas détecter une collision et lorsque les données sont envoyées, le média ne peut pas être écouté. IEEE 802.11 fonctionne en mode « *half duplex* » (envoi et réception) par un schéma TDD. La détection des collisions, telle qu'elle est utilisée par Ethernet, ne peut pas être utilisée par les transmissions sur fréquences radio sur IEEE 802.11.

Puisque les nodes peuvent détecter si le média est libre mais pas détecter les collisions sur ce même média, le point d'accès doit envoyer une confirmation pour assurer le succès d'une transmission. Ce mécanisme crée un surplus et diminue le débit.

À cause de ces limites, un problème très connu se produit dans les configurations IEEE 802.11b d'un point vers de multiples points : le problème du *node caché*. Dans ce type de configuration, un ensemble de nodes parlent à un node commun appelé le point d'accès. Le node caché est causé par le fait que chaque node ne peut pas écouter tous les autres dans un réseau sans fil et qu'ainsi, les collisions sont inévitable en utilisant seulement « CSMA ». Pour résoudre (ou diminuer) le problème, la couche MAC de IEEE 802.11 intègre un mécanisme appelé « CA » pour *Collision Avoidance* ou évitement des collisions. En utilisant CA, le node qui transmet doit envoyer d'abord un « paquet RTS » pour « *Request to Send* » ou requête pour l'envoi au point d'accès. Il attend par la suite le « CTS » pour « *Clear to send* » ou libre pour l'envoi avant de procéder avec la transmission.

Même si tous les nodes ne peuvent pas écouter les paquets RTS envoyés par les autres nodes, ils peuvent toujours entendre les paquets CTS envoyé par le point d'accès à un autre node sur le réseau. En conséquence, les nodes peuvent éviter d'envoyer des paquets de données pendant le temps alloué par le point d'accès à un autre node.

Quand le nombre de nodes dans le réseau ou la distance entre les nodes et le point d'accès augmente, RTS/CTS ne peut plus suffire et d'autres alternatives à IEEE 802.11b sont requises.



IEEE 802.16 (WMAN)

IEEE 802.16 a pris en considération quelques problèmes présents dans IEEE 802.11 et propose des solutions au problème du *node caché* pour le lien radio de un point à point multiple. Après tout, IEEE 802.11 n'a pas été prévu ou conçu pour fonctionner en extérieur. IEEE 802.16 utilise une combinaison de TDMA et DAMA pour régler les problèmes qui affectent encore IEEE 802.11.

Il est très important de mentionner, considérant les limites intrinsèques dans IEEE 802.11, qu'un bon design de l'architecture du transport et du réseau est nécessaire. L'expérience a démontrée les effets négatifs de l'ajout de plusieurs nodes sur un réseau sans fil quand les questions du transport et du réseau n'ont pas été prises en compte.

Adresses MAC

Une adresse MAC est utilisée dans la couche du lien comme un mécanisme pour identifier et donner des adresses au trafic de données qui circule sur le média partagé. Cela consiste en une séquence universellement unique de 48 bits (12 chiffres hex) associée avec chacune des interfaces du réseau (équipement).

Lorsqu'un paquet de données est envoyé sur le média partagé, la source et la destination des ordinateurs (hôtes) sont incluses dans l'entête du paquet. Quand un paquet doit être envoyé à tous les hôtes (diffusion), une adresse spéciale est utilisée. Sous Ethernet, une adresse MAC spéciale est utilisée pour la diffusion : ff:ff:ff:ff:ff:ff (tous les 48 bits à 1)

En circonstances normales, le NIC, « *network interface cards* » pour cartes d'interface de réseau, ne passe les paquets de données au Système d'Opération que lorsque l'adresse MAC correspond à celle de l'ordinateur.

L'adresse MAC est normalement intégrée à l'équipement physique lorsque envoyée par le vendeur.



Utiliser les adresses MAC pour l'identification

Il est devenu très fréquent dans pour plusieurs fournisseurs de services sans fil d'utiliser les adresses MAC de l'interface sans fil comme un mécanisme pour limiter ou fournir l'accès au réseau sans fil. On considère que les adresses MAC sont codées « en dur » et ne peuvent être modifiées par les usagers moyens. La réalité est différente car les adresses MAC **peuvent facilement être modifiées**.

Un mécanisme d'identification basé sur les adresses MAC est insécurité.

Le cryptage du niveau lien

Le cryptage du niveau lien est le processus permettant de sécuriser les données au niveau du lien quand les données sont transmises entre deux nodes attachées au même lien physique (ils peuvent aussi être dans deux liens physiques différents au moyen d'un répéteur, par exemple : satellitaire). Aucun autre protocole ou logiciel d'application fonctionnant au-dessus du lien physique n'est protégé de l'écoute illicite.

Le cryptage nécessite une certaine clef ou un secret partagé entre envoyeur et récepteur et un algorithme de cryptage. Quand l'envoyeur et le récepteur ne sont pas présents sur le même média, les données doivent être décryptées puis recryptées par tous les nodes sur la route vers le récepteur.

Le cryptage du niveau lien s'utilise normalement quand il n'y a aucun cryptage dans les protocoles de haut niveau.



Le cryptage du niveau lien dans IEEE 802.11

Le plus connu des algorithmes de cryptage pour IEEE 802.11 est aussi appelé WEP pour « *Wired Equivalent Privacy* ». L'insécurité de WEP a été démontrée et d'autres alternatives ont été proposées et normalisées telles que le WPA « *Wi-Fi Protected Access* ». LA nouvelle norme IEEE 802.11i inclura une amélioration de WPA appelé WPA-2.

Le cryptage du lien **ne fournit pas de sécurité** au-delà du lien physique et doit être considéré comme une mesure supplémentaire de sécurité dans le design de votre réseau.

Le cryptage du lien requiert plus de ressources en équipement dans les points d'accès de même qu'un design

sécuritaire de la gestion et de la distribution.

Couche lien (IP)

Le couche IP (Internet Protocole) est un protocole utilisé pour transmettre des données sur un réseau dirigeant des paquets. Les données envoyés sur le réseau IP sont connues sous le nom de datagrammes ou paquets. Le protocole IP fournit un service non fiable (bel effort) avec aucune garantie sur la livraison. Les paquets peuvent arriver endommagés, dupliqués, non fonctionnels ou encore être éliminé par tous nodes sur la route.

Les adresses des envoyeur et récepteur sont une part importante du protocole IP. Cette information (les adresses) n'est pas uniquement utilisée pour identifier les hôtes Internet et diriger les paquets, mais est aussi requise pour les applications de haut niveau comme les coupe-feu.

Les adresses

Le protocole IP le plus répandu est le IPv4 qui utilise un champs de 32 bit pour les adresses. La prochaine génération de protocoles IP utilise des adresses de 128 bits incluant la source et la destination pour contourner le fait que IPv4 n'a plus d'adresse **disponible**.

Création de sous-réseaux et masque de réseau « netmask »

On utilise principalement les sous-réseaux pour le contrôle et la division du trafic sur le réseau. Les sous-réseaux permettent des entrés simple de routage référant soit à un sous-réseau, soit à son hôte individuel. Cela implique qu'une entrée simple de routage peut être utilisée à l'échelle de l'Internet alors que les seulement des routes spécifiques sont requises pour les routeurs dans le bloc du sous-réseauté.

Le masque du réseau est un nombre à 32 bits qui indique le réseau d'une adresse IP. LE masque du réseau est divisé entre une partition de réseau et une partition de l'hôte au niveau des bits alors que le « 1 » symbolise le réseau et le « 0 » symbolise l'hôte.

| | |
|----------------------------|------------------------------|
| 10.0.0.0/255.0.0.0 | Classe A |
| 10.1.0.0/255.255.0.0 | Classes 255 B |
| 10.1.1.0/255.255.255.0 | Classes 255 C |
| 10.1.1.128/255.255.255.128 | Classe demi C (127 Adresses) |
| 10.1.1.64/255.255.255.192 | 63 adresses hôtes |
| 10.1.1.8/255.255.255.248 | 7 adresses hôtes |

Image 2: Les sous-réseaux dans un réseau de classe A

L'adresse du réseau est le résultat d'un opération logique **AND** entre l'adresse IP et le masque du sous-réseau.

Il existe des restrictions dans l'adresse du sous-réseau. Les adresses des hôtes consistant de « 0 » et de « 1 » seulement sont réservées pour préciser des réseaux locaux et des adresses de diffusion. Cela implique qu'un masque de sous-réseau à 1 bit n'est pas permis.

La formule suivante peut être utilisée pour calculer le nombre de sous-réseau et d'hôtes qu'un masque de sous-réseau permettra:

Nombre de sous-réseaux = $2^n - 2$, n étant le nombre de bits dans le sous-réseau

Nombre d'hôtes dans le sous-réseau = $2^m - 2$, m étant le nombre de bit dans le réseau hôte

Nombre total des hôtes = $(2^n - 2) (2^m - 2)$



Les sous-réseaux dans le sans fil

C'est devenue monnaie courante pour plusieurs fournisseurs de services sans fil de ne pas configurer les sous-réseaux de leurs réseaux correctement. Mettre en place un large sous-réseaux sans plusieurs décisions de routage est très facile à faire mais lors que le réseau s'agrandit, le dépannage est de loin plus complexe.

Un bon sous-réseautage et un bon design de routage dans le réseau sans fil limite la quantité de trafic diffusé inutilement et permet ainsi d'élargir le réseau.

Évitez autant que possible d'utiliser un seul grand sous-réseau. Nous recommandons de limiter les sous-réseaux à 32-64 hôtes.

Contrôle des erreurs

Le contrôle des erreurs s'effectue par un ensemble de messages de contrôle au niveau IP appelés ICMP pour « *Internet Control Message Protocol* ». Le protocole ne fournit pas un large système de contrôle des erreurs, mais se limite à peine à rapporter les erreurs aux hôtes opérants.

Deux des principales utilités de ICMP sont les suivantes :

- Rapporter les problèmes qui empêchent les livraisons (comme les **destinations non-jointes**)
- **Dépanner le réseau** à l'aide de messages de requêtes et de réponses (tels que « Echo Request » et « Echo Reply » utilisé par *ping*)

Un message d'erreur ICMP contient toujours l'entête complète IP (incluant les options) du *datagramme* (paquet) IP qui a échoué de même que les huit premiers bits du champ de données IP. L'erreur peut ainsi être associée à un certain protocole et processus spécifique (à partir du numéro de port dans les entêtes TCP ou UDP indiquant les huit premiers bits du champ de données IP)



Surveiller ICMP dans les réseaux sans fil

Surveiller le trafic ICMP dans vos réseaux sans fil vous permettra non seulement d'identifier les problèmes de connectivité au sein de vos réseaux mais aussi de confirmer la présence de certains virus ou chevaux de Troie. Certains de ceux-ci incluent le balayage automatique du réseau et donc la présence d'un nombre élevé de trafic ICMP avec des **destinations non-jointes** peut indiquer que des virus sont en activité.

Routage

Le processus permettant de transférer un paquet de données de la source à la destination est appelé *routage*. Une décision de routage est faite dans chaque ordinateur entre la source et la destination pour déterminer le

meilleur saut jusqu'à la prochaine machine. Les décisions de routage sont précisées dans les *tableaux de routage*.

Tous les algorithmes communs utilisent la *destination* ou la *source* de l'adresse IP. Dans le premier cas, la route est déterminée en regardant l'adresse de destination du paquet (utilisé plus souvent) alors que dans le deuxième cas, on peut utiliser l'adresse de la source pour déterminer le chemin du paquet. Une troisième option est appelée routage basé sur les politique et les décision de routage dépendent alors de d'autres sources d'information (adresses MAC, type de service, charge du réseau, etc.)



Utiliser la source IP pour les décisions de routage

Utiliser la source IP pour les décisions de routage est un mécanisme intéressant pour inclure un équilibre des charges dans le réseau sans fil. En insérant un routeur qui peut prendre des décisions basées sur l'adresse de la source du paquet, nous pouvons configurer différents nodes pour différents type de services et même router différents usagers d'un réseau sans fil vers différents routeurs frontières.

Par exemple, l'utilisation d'une politique de routage basée sur la source IP ne requiert pas de modifier le sous-réseau de votre réseau sans fil pour fournir à un certain hôte une passerelle extérieure différente qu'aux autres.

NAT « Traduction de l'adresse du réseau »

Le NAT est la capacité d'un routeur de ré-écrire la source ou la destination d'un datagramme IP. Il est devenu populaire puisqu'il permet à une machine unique avec une adresse publique IP unique de *représenter* un groupe d'ordinateur dans un réseau privé.

NAT n'est pas seulement utile lorsqu'il y a un manque d'adresses IP publiques, mais aussi comme un mécanisme à diverses fonctions telles que :

1. Coupe-feu / DMZ
2. Équilibre dans la charge du trafic (ex. : des serveurs Web identiques derrière un NAT pour équilibrer les requêtes)
3. Équilibre dans la charge des opération (ex. : des bases de données identiques pour équilibrer la charge des opération)

Cette section traitera de comment NAT peut-être utilisé pour améliorer la sécurité d'un réseau. Pour des raisons de clarté, NAT a été divisé selon ses deux principales fonctions : SNAT (manipulation de l'adresse de la source) et DNAT (Manipulation de la destination de l'adresse).

Mascarade - SNAT

La mascarade IP ou NAT de la source permet aux hôtes ayant des adresses IP privées de communiquer avec des hôtes à l'extérieur de leur propre réseau en laissant un machine agir pour eux. La mascarade IP demeure une forme simple mais limitée de pare-feu. La mascarade IP ne permet pas d'initier une connexion avec un autre hôte dans le réseau.

La mascarade réécrit l'adresse de la source des paquets au moment où ils traversent le routeur de façon à ce que la nouvelle machine cible voit toujours le routeur comme l'expéditeur. Lorsque le récepteur du trafic répond, le routeur réécrit l'adresse de la destination à l'expéditeur original.

La mascarade IP ajoute une certaine sécurité en agissant comme un pare-feu, mais aussi, il limite les usagers à l'intérieur du réseau pour fournir des services à l'extérieur.

NB au sens strict, la mascarade n'est pas identique au SNAT puis qu'elle jette les connexions précédentes quand l'interface s'arrête ou change les adresses IP.

NAT de la destination « DNAT »

Le DNAT – « Destination Network Address Translation » est régulièrement utilisé pour rendre disponible un service disponible publiquement d'un réseau interne (adresse IP privée) par la réécriture de la destination IP du paquet.

Le DNAT peut être utilisé pour router le trafic au sein d'une « DMZ » pour zone démilitarisée. Le DMZ est habituellement placé dans un autre segment du réseau, isolé du reste du trafic.

En utilisant DNAT, nous pouvons rediriger (organiser) le trafic entrant ayant une certaine adresse IP et un numéro de port vers les port et adresse IP du DMZ.



Manipuler le trafic dans un réseau sans fil

NAT (SNAT et DNAT) peuvent être utilisés pour manipuler le trafic au sein du réseau sans fil. Comme les usagers (hôtes) du réseau ont les mêmes configurations, nous pouvons influencer le routage du trafic et décider quels services seront rendus disponibles.

Par exemple:

Nous pouvons mettre en œuvre NAT pour rediriger les requêtes Web vers un serveur Proxy. Davantage, nous pouvons aussi rediriger différents segments du réseau vers différents serveurs Web liés à autant de fournisseurs Internet.

NAT peut aussi être utilisé pour rediriger les usagers vers un portail captif où ils devront souscrire au service ou s'identifier en entrant leur information de compte.

IP tunneling et « IPSEC »

Le **IP tunnelling** est la méthode qui permet de transporter des paquets IP à l'intérieur de d'autres paquets IP pour permettre aux premiers d'être redirigés d'abord vers un autre réseau. **Tunnelling** est le processus de capsulage des paquets IP. Lorsque le capsulage est fait à l'intérieur d'un paquet IP crypté, le tunnelling est connu sous le nom de tunnelling sécuritaire ou « VPN ».

Le IP tunnelling requiert que les extrémités du tunnel soient complètement routables donc non bloquées par un pare-feu ou encore NAT.

L'utilisation du tunnelling IP ne fournit pas de sécurité supplémentaire si le paquet capsulé (celui qui voyage à l'intérieur) n'est pas crypté. La façon habituelle de construire le IP Tunnelling secure est IPSEC.

IPSEC est un ensemble de protocoles qui assure la sécurité au niveau de la couche IP. IPSEC permet le capsulage IP sécuritaire et fourni certaines propriétés de sécurité à tous les logiciels fonctionnant au dessus de IPSEC.

Il existe 3 types de protection que IPSEC peut offrir au niveau IP:

1. **Confidentialité** (protection du contenu)
2. **Identification** (vérification de l'expéditeur)
3. **Intégrité** (contenu n'a pas été modifié)

Pour assurer ces propriétés sécuritaires, IPSEC utilise principalement trois protocoles :

« **AH - Authentication Header** » pour l'identification de l'entête: Une vérification en profondeur de « tout » le paquet IP chargé de confirmer que le paquet reçu origine bien de l'expéditeur et qu'il n'a pas été modifié durant le transfert.

« **ESP - Encapsulating Security Payload** » pour cryptage sécuritaire de la charge : Un cryptage dur de la charge – un paquet correctement décrypté assure la protection du contenu du paquet. Le paquet a été crypté en utilisant un secret partagé entre les expéditeurs et récepteur.

« **IKE - Internet Key Exchange** » pour échange de clef Internet : Fournit des moyens pour négocier les clés de sessions. **en anglais : to negotiate keys session keys.**



IPSEC dans les réseaux sans fil

IPSEC requiert une routabilité de bout en bout au sein du réseau sans fil. Si vous planifiez de mettre en œuvre IPSEC, évitez d'utiliser NAT et déployez toutes plutôt toutes les fonctions du pare-feu

Le encapsulage IP inclut aussi un **overhead** en supplément, utilisant IPSEC simultanément avec la compression est recommandé pour des résultats optimaux.

IPSEC requiert un bon design de la clef de gestion. Si un nombre très limité de parties communiqueront avec IPSEC, la méthode la plus simple et l'utilisation d'une clef symétrique. Malheureusement, la perfection dans le secret ne pourra pas être garantie.

Si vous devez construire des VPN à l'intérieur de votre réseau sans fil, vous pouvez aussi envisager d'utiliser la couche de logiciel d'application VPN, laquelle utilise normalement UDP **Tunnelling** et le protocole SSL pour le cryptage.

Plus d'information sur VPN:

<http://www.openvpn.org/>

Couche Transport (TCP)

La couche transport permet le transfert de paquets IP entre des processus (services) utilisant des ports (nombres). Le port TCP est une connexion logique associant un certain avec un processus en cours

TCP «Protocole de contrôle des transmission »

Le protocole de contrôle des transmission « *TCP* » est un protocole de transport orienté sur les connexions qui fournit un transport de données fiable entre les **pairs of process**. La fiabilité est assurée par la mise en place dans le protocole du *contrôle du débit* et de *connexion des erreurs*.

Le contrôle du débit entre l'expéditeur et le récepteur est géré trois mécanismes appelés : *sliding windows*, *window size adjustment heuristics* et *congestion avoidance algorithms*. Ces mécanismes doivent assurer que les ressources d'un média partagé sont distribuées équitablement entre les différentes sessions en cours.

La *confirmation* envoyée par chacun des paquets correctement reçus constitue le mécanisme de contrôle des erreurs dans TCP lequel contrôle la re-transmission des paquets.

TCP est compatible pour les applications qui requiert le transport de données (telles que http, ftp, smtp etc).

UDP « User Datagram Protocol »

Le UDP est un autre protocole de transport en couche qui fournit un bel effort pour le transport de datagrammes. Le service n'est pas fiable et n'intègre aucune protection quant aux pertes ou duplications de paquets. UNP ne gère pas non plus le contrôle du débit ni la correction d'erreur. Le seul mécanisme que UDP comporte lui permettant de vérifier si les données sont corrompues ou non, est une vérification du sommaire de la charge. Si le récepteur découvre des données non correctes par cette vérification, il rejette tout simplement le paquet sans même demander une nouvelle retransmission.

UDP fonctionne bien avec certaines applications en temps réel, là où la vitesse de transmission est plus importante que la fiabilité du service.

| Caractéristiques | UDP | TCP |
|-------------------------|---|--|
| Qualité du service | Bel effort, pas fiable | Service fiable |
| Protocole de Connexion | Moins de connexion | Orienté sur la connexion |
| Confirmation | Aucune | Tout est confirmé |
| Retransmissions | Aucune | Les données perdues sont totalement retransmises |
| Contrôle du débit | Aucune | <i>Sliding windows; window size adjustment, congestion avoidance</i> |
| overhead | Très bas | Bas, mais plus haut que UDP |
| Vitesse de Transmission | Très haut | Haute, mais moins haute que UDP |
| Valable pour : | 1. Quand la vitesse est une priorité plutôt que la fiabilité. 2. Transfère de petits paquets de données. 3. Lorsque la diffusion ou la distribution est utilisée. | La plupart des protocoles |



Anomalies entre TCP et la couche MAC dans IEEE 802.11

Il est important de mentionner que TCP ne performe pas bien dans les réseaux sans fil IEEE 802.11 et plusieurs recherches ont été faites visant à améliorer sa performance.

1. La couche d'accès au média, MAC, sous IEEE 802.11b est connue comme la méthode « *CSMA/CA channel access* » qui garantit les probabilités d'accès égales au canal à long terme à tous les hôtes.
2. TCP assume que les paquets perdus le sont à cause de la congestion du réseau. Cependant, TCP ne peut pas distinguer entre **congestion et corruption** et en conséquence, il réduit inutilement la fenêtre ce qui résulte de bas débits et longs délais de transit

Conséquence de l'overhead du protocole CSMA/CA, en pratique sur 802.11b, le débit maximum qu'une

application peut atteindre (sur un lien point à point) est d'environ 5.9 Mbit/s sur TCP et 7.1 Mbit/s sur UDP.

Il est très recommandé de créer les réseaux sans fil aussi « symétriques que possible ». Essayez de créer des réseaux sans fil aussi « symétriques que possible ». Essayez de permettre aux nodes de s'écouter les uns les autres et utilisez des taux de puissance effective similaire.

Incluez un mécanisme d'organisation du trafic au niveau du routeur frontière. L'organisation du trafic permet de contrôler les congestions TCP et peut aider à distribuer la ressource de la bande passante de façon équitable. Pour plus d'information: http://www.ieee-infocom.org/2003/papers/21_01.PDF

Couche 3 pare-feu

Dans la couche du transport, un pare-feu est mis en œuvre pour contrôler le trafic du réseau en bloquant les ports TCP ou UDP. Puisque plusieurs applications utilisent des ports « très connus » pour leurs communications, le filtrage des paquets peut être utilisé pour bloquer sur FTP (port 20) ,Telnet (port 23) ou SMTP (port 25).

Il y a deux stratégies différentes en termes de pare-feu au niveau TCP. Soit vous bloquez tous les ports et n'ouvrez que ceux dont vous avez réellement besoin, soit vous ouvrez tous les ports et ne bloquez que ceux que voyez comme des menaces. La mesure la plus restrictive étant celle où tous les ports sont bloqués à l'exception des seuls qui sont nécessaires.

Les pare-feu utilise une combinaison de 3 méthodes principales:

- Bloquer le trafic sortant du type X
- Bloquer le trafic entrant du type Y
- Rediriger le trafic de type Z

La redirection implique que le pare-feu renvoi toutes les connexions entrantes vers un certain port sur un autre hôte (et port) au sein du réseau. En redirigeant les ports, vous créez un trou dans votre pare-feu puisque vous permettez à des paquets d'entrer dans votre réseau. Les principaux objectifs de la redirection sont :

- Fournir un service externe à partir d'un hôte derrière un pare-feu
- Fournir plusieurs instances d'un service à partir d'hôtes derrière un pare-feu pour équilibrer la charge



Design du pare-feu

Le pare-feu est une partie fondamentale d'un réseau sans fil. Il peut bloquer l'entrée des codes malicieux dans le réseau et nous aider à décider quels services nous voulons rendre accessible à nos usagers. Un réseau sans fil devrait être considéré comme une ressource limitée et, par conséquent, a besoin de prioriser les services.

Un bon réseau sans fil devrait combiner le pare-feu, l'organisation du trafic et la surveillance. L'essentiel du dépannage dans les réseaux sans fil vient de (1) la détection, (2) le blocage (3) l'élimination des programmes malicieux qui consomment les ressources de bande passante.

Par exemple, si nous trouvons intéressant d'utiliser des programmes point à point, une part limitée de ressources de bande passante, devrait leur être alloué.

Couche logiciel d'application

La principale responsabilité de la couche logiciel est d'assurer qu'une communication effective avec les autres logiciels dans le réseau est possible. Il est important de comprendre que la couche logiciel n'est pas le logiciel elle-même. C'est simplement une couche de services qui fournit justement les services suivants:

- 1- Identifier et s'assurer que l'autre partie communicante est prête pour la communication
- 2- Identifier (message, expéditeur, destinataire)
- 3- Identifier les ressources de communication
- 4- Assurer le respect des conventions entre l'expéditeur et le destinataire au niveau des procédures de récupération des erreurs, de l'intégrité des données, de l'aspect privé.
- 5- Déterminer le protocole, et les réglages de syntaxe des données au niveau logiciel.

Les protocoles de la couche logiciel les plus utilisés aujourd'hui sont HTTPS, SMTP, IMAP/POP3, FTP, les protocoles de messagerie et RTP.

Logiciel pare-feu

Les pare-feu présentés jusqu'à maintenant fonctionnent sur les couches réseau et transport. Avec ces pare-feu, vous pouvez faire ce qui suit :

- Bloquer ou permettre le trafic entrant provenant d'une certaine adresse IP
- Bloquer ou permettre le trafic sortant vers une certaine adresse IP
- Bloquer ou permettre les trafics entrant ou sortant utilisant un certain port TCP ou UDP

Ce que ces pare-feu ne peuvent faire est d'examiner le contenu des données et ainsi bloquer les *paquets basés sur le contenu*. Si vous souhaitez faire cela, il faut filtrer les données au niveau logiciel: « *Application Layer Filter – ALF* ».

ALF peut identifier une information anormale dans l'entête d'un message et dans les données elles-mêmes. Il peut être configuré pour rechercher certaines lignes de code au sein des données pour bloquer le message basé sur cette information. Avec ces caractéristiques, ALF peut prévenir:

- SMTP, POP3 and DNS **buffer overflows**
- Les attaques sur le serveur Web basées sur l'information dans les entêtes et les requêtes HTTP
- Les attaques de code caché au sein du tunnel SSL
- Et bloquer les logiciels fonctionnant au-dessus de HTTP (Messenger)
- Des usagers interne de divulguer de l'information sensible

ALF peut aussi bloquer certaines commandes spécifiques au sein des protocoles des couches de logiciel. Par exemple, dans http, la commande GET peut être bloquée alors que POST reste permis.

Le désavantage primaire de ALF est son effet négatif sur les performances, conséquence de l'examen de toutes les données. Son utilisation soulève de plus des questions éthiques puisque la mise en place de ALF implique d'avoir la capacité d'analyser les données personnelles en temps réel.

Autre conséquence, son utilisation exige des équipements plus puissants que le filtrage traditionnel par les pare-feu et cela a donc un impact sur les coûts du service.

ALF amène aussi de la complexité au réseau ce qui cause des risques de mauvaise configuration du filtre et, donc, peut entraîner le blocage de bonnes données.



Filtre de la couche logiciel d'application

Variation fréquente des filtres de la couche logiciel d'application, les anti-virus ou anti-pourriels sont capables d'examiner le contenu des données et de bloquer ou étiqueter les pièces attachées suspectes de courriels.

En créant un réseau sans fil, vous devrez envisager d'installer un filtre pour la couche logiciel. Les pourriels représentent aujourd'hui de 30 à 50% du trafic total SMTP. En étiquetant les pourriels et en entraînant les usagers à utiliser IMAP dans leurs clients mails, vous pouvez empêcher le transfert de courriels non-sollicités par les liens sans fil.

Toujours au niveau de la couche logiciel, vous pouvez aussi envisager d'installer un serveur Web Proxy. Un serveur Proxy est utilisé pour conserver en cache des données fréquemment sollicitées dans le RAM et dans une cache DSN.



Conclusion finale:

Un des avantages des modèles OSI et Internet est qu'ils garantissent que chacune des couches de protocoles peuvent fonctionner indépendamment les uns des autres. Cela donne la flexibilité d'échanger notre couche physique et de bouger nos logiciels d'un réseau câblé à un réseau sans fil.

Mais la bonne qualité du service viendra de la bonne configuration de toutes les couches de protocoles ainsi que la bonne architecture réseau. En créant un réseau sans fil, ne sous-estimez pas les mécanismes disponibles dans le réseau, les couches logiciel et transport, pour améliorer la performance globale des réseaux sans fil.

Maximiser les **bits utiles** est une tâche qui requiert la compréhension des effets de chaque couches protocole sur la performance globale du réseau.