

# RESEAUX TCP/IP: NOTIONS AVANCEES

Preparé par Alberto EscuderoPascual

# Objectifs... Répondre aux questions:

- Quelles aspects des réseaux IP peut affecter les performances d'un réseau Wi-Fi?
- Quelles sont les interactions entre l'IEEE 802.11 (physique/liaison) et TCP(transport)?
- Comment améliorer la qualité des services de notre réseau?

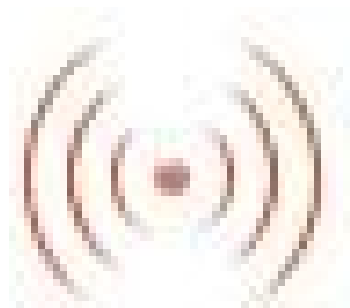
# Comment?... Methodologie

- Parcours de la pile des protocoles
- De Bas->Haut
- Se focaliser sur les concepts, non sur les implémentations
- Identifier les éléments essentiels à considérer dans le design d'un réseau

# Sommaire

- OSI VS Internet (TCP/IP)
- PHY/MAC
  - Accès au média & Contrôle d'erreurs
  - MAC Addresses & Cryptage Liaison
- Réseau
  - IP addresses & Contrôle d'erreurs
  - Routage & Network adresse Translation (NAT)
  - IP Tunneling & IPSec
- Transport
  - TCP, UDP, Firewalls
- Application
  - Proxies, Firewalls++

# Sans fil



# OSI VS TCP/IP

Layer	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Réseau	Réseau
2	Liaison	Accès au media
1	Physique	

# Contrôle d'accès au media

- Couche Physique
  - Techniques de modulation ,codage des bits, accès physique au média partagé.
  - RS-232, V.35, 10BASET, ISDN
- Couche liaison
  - S'occupe de la gestion de transfert des trames sur le au travers du média.
  - Ethernet (IEEE 802.3), PPP,...

# Controle d'accès au Media



- IEEE 802.11 (WLAN)
  - Couche Physique et Couche Liaison.
- Protocoles de la couche liaison
  - IrDA
  - Spread Spectrum (Etalement de Spectre)
    - FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum), OFDM (Orthogonal Frequency Division Multiplexing)



# Protocoles de contrôle d'erreur

- CSMA/CD
  - Ethernet



- CSMA/CD and CSMA/CA
- IEEE 802.11 (WLAN)
  - CSMA/CA (RTS,CTS)
- IEEE 802.16 (WMAN)
  - TDMA,...

# Addressage MAC

- 48 bits uniques



- Address MAC comme authentification
  - Faible sécurité

# Cryptage au niveau liaison

- Sécurise les données entre les équipements sur le même lien physique.
- Algorithme de cryptage et clés partagées.



- WEP (sécurité minimum)
- WPA, WPA-2
- Ne fournissent pas de sécurité de bout-en-bout

# OSI versus TCP/IP

Layer	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Réseau	Réseau
2	Liaison	Liaison
1	Physique	

# Couche réseau (IP)

- IP Addresses
  - Routage, identification des postes, firewall
- Sous-réseautage
  - Netmask, classes



- Le sous-réseautage est cruciale
- Maintenance
- Limiter à 32-64 postes par sous réseau

# Contrôle d'Erreurs IP

- ICMP
  - Reporte les problèmes qui pourraient rendre un poste injoignable.
  - Test de connectivité (ping)



- Présence d'un flux anormalement importants de ping?
  - Viruses ou trojans

# Routage

- Routage source ou destination
- Politique de routage



– Load balancing

# N.A.T

- Partage d'une address publique
- Firewall/DMZ



# Masquerading - SNAT

- Conversion des Adresses IP
  - laisser le routeur “se présenter” à la place des postes du réseau local sur l’extérieur.
- Simplification des politiques de firewall
- Maîtrise des accès vers l’extérieur.

# Destination NAT

- Rendre disponible des services internes à l'extérieur
  - transformer les IP destination



- Disponibilité de service
- Redirection des requêtes http
- Processus Login/registration

# IP Tunneling

- Encapsulation des packets à l'intérieur de packets IP
- Nécessite des équipements routables aux extrémités
- Ne fournit aucune sécurité sans cryptage supplémentaire.

# IP Tunneling

- Encapsulation + Cryptage= VPN
- Les tunnels IP sécurisés sont en général implémentés sur la base de IPSEC

# IPSEC

- Garantie de sécurité au niveau IP
- Fournit les protections suivantes:
  - Confidentialité
  - Authentification
  - Intégrité

# IPSEC



- Entièrement fonctionnel
- Considerer l'application VPN: OpenVPN  
([www.openvpn.org](http://www.openvpn.org))

# OSI versus TCP/IP

Layer	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Réseau	Réseau
2	Liaison	Media Access
1	Physique	

# Couche Transport

- Transfert les pkts IP entre les processus en utilisant les ports.
- Un port est une connexion logique qui associe un certain transfert avec un processus actif.



# TCP VS UDP

Caracteristiques	UDP	TCP
QoS	Non garantie	Service sûr
Établissement e la connexion	Non	oui
Acknowledgements	Non	Oui
Contrôle de flux	Non	Oui
Retransmission	Non	Oui
Surcharge	faible	>UDP
Optimale Pour	Transmission rapide de plusieurs petits paquets	La plupart des protocoles

# TCP et IEEE 802.11 MAC



- Performances mitigées sur l'IEEE 802.11  
→ IEEE 802.11e (QOS)

# Couche 3 Firewalls

- Bloque le trafic sortant de type X
- Bloque le trafic entrant de type Y
- Relais trafic de type Z

# design Firewall



- Très utile dans les réseaux sans fil.
- Détecter, bloquer and éliminer les programmes malicieux, dépassant leur bande passante.

# OSI versus TCP/IP

Layer	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Réseau	Réseau
2		Media Access
1	Physique	

# Couche application

- Identifie et s'assure que l'émetteur/le récepteur sont prêts à commmmuniquer.
- Authentification (émetteur,récepteur, message)
- Identifie les ressources nécessaires à la communication.
- Déterminine les protocoles et la syntaxe au niveau applicatif

# Application firewalls

Prévention contre:

- Les surcharges SMTP, POP3 , DNS
- Les attaques sur les serveurs WEB par injections d'informations suspectieuses à l'intérieur des entêtes HTML
- Les code malveillants caché sous des sessions SSL
- Bloque les applications tournant au dessus du http (messenger...)

# Application firewalls

## Inconvénients:

- Réduction des performances de réseau
- Coût
- Erreurs de configuration irréversibles



# Application Firewalls



- Anti-virus and Anti-spam
  - Bloque ou marque le paquets
  - Les SPAMs représentent 30-50% du trafic SMTP!
- Server proxy Web
  - Stockage en “Cache” les requêtes fréquentes
  - Cache des correspondences DNS

# Réseaux sans fil avancés



- Touche en profondeur à toutes les couches.
- **Le But Ultime:**
  - Maximiser le nombre de bits utiles qui traversent notre infrastructure de la couche physique à l'application.

# Conclusion

- Installer un réseau 802.11 qui marche est très est très “facile”
- Déployer un réseau sans fil performant est plus complexe.

# Retour vers le bas: Comment Optimiser les réseaux sans fils pour la VoIP? (VoWLAN)

Layer	ISO	VoIP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Réseau	Réseau
2	Liaison	Media Access
1	Physique	