

Advanced Networking

Developed by: Alberto Escudero Pascual, IT +46

Goals

- To understand “networking” aspects that can affect the overall performance of a wireless network
- To understand the interactions between IEEE 802.11 (Physical/Link) and TCP (Transport)
- To be able to improve the quality of service of a network

Table of Contents

- Methodology of the unit
- OSI versus Internet (TCP/IP)
- PHY/MAC
 - Media Access Layer, Error Control, MAC and Encryption
- Network
 - IP addressing, Error Control, Routing, NAT, IP Tunneling, IPsec
- Transport
 - TCP, UDP, Layer 3 Firewalls
- Application
 - Proxies, Firewalls++

Methodology

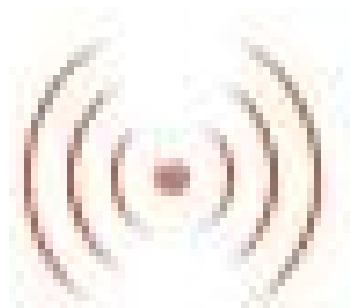
- Travelling through the protocol 'stack'
- Bottom-up
- Focus on 'concepts', not implementation specific
- Identify 'key' issues that need to be consider in your network design

Methodology

This unit is not:

- Magic
- A substitute for several weeks training in networking
- Training in how to implement each of the 'key' aspects that you need to consider

Wireless!



OSI versus TCP/IP

Layer	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Network	Network
2	Data link	Media Access
1	Physical	

Medium Access Control

- Physical layer
 - Modulation techniques, bit encoding, physical access to shared media
 - RS-232, V.35, 10BASET, ISDN
- Link Layer
 - Addressing/delivering packets on shared channel
 - Ethernet (IEEE 802.3), PPP, ATM

Media Access Layer



- IEEE 802.11 (WLAN)
 - Physical layer and link layer
- Physical layer protocols
 - IrDA
 - Spread Spectrum
 - FHSS, DSSS, OFDM

Error Control Protocols

- CSMA/CD
 - Aloha, Ethernet



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

MAC Addressing

- 48 bit unique address
- Hardware coded but can easily be modified



- MAC as authentication
 - Low security

Link Layer Encryption

- Secure data between hosts on same physical link
- Encryption algorithm and shared secret
- Requires trusted intermediate hosts



- WEP (low security)
- WPA, WPA-2
- Does not provide end-to-end security

OSI versus TCP/IP

Layer	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Network	Network
2	Data link	Media Access
1	Physical	

Network Layer (IP)

- IP Address
 - Routing, identify host, firewalling
- Subnetting
 - Netmask, classes



- Subnetting is crucial
- Troubleshooting
- Limit to 32-64 hosts per subnet

IP Error Control

- ICMP
 - Report problems that prevents delivery (destination unreachable)
 - Troubleshoot network (ping)



- Large amount of ICMP?
 - Viruses and trojans

Routing

- Source and Destination routing
- Policy Routing



- IP Source as routing decision
 - Load balancing

Network Address Translation

- Shortage of public IP addresses
- Firewall/DMZ
- Traffic load balance
- Computing load balance

Masquerading - SNAT

- Rewrites IP addresses
 - Let router act on others behalf
- Simple firewall security
- Limits access to outside services for internal hosts

Destination NAT

- Make internal services publicly available
 - Rewriting destination IP



- Availability of services
- Affect routing of packets
- Redirect web requests
- Login/registration processes

IP Tunneling

- Encapsulating IP packets inside of IP packets
- Requires fully routable end-points
- Provides no added security unless the encapsulated packet is encrypted

IP Tunneling

- Encapsulation inside of encrypted IP packets is known as:
 - Secure tunneling or VPN
- Secure tunneling is normally provided using IPSEC

IPSEC

- Ensures security on IP level
- Provides following protection:
 - Confidentiality
 - Authentication
 - Integrity
- Three main protocols:
 - AH, ESP, IKE

IPSEC



- Fully functional firewalls instead of NAT
- Use IPSec with compression
- Consider Application layer VPN's
 - Check www.openvpn.org

OSI versus TCP/IP

Layer	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Network	Network
2	Data link	Media Access
1	Physical	

Transport Layer

- Transfer of IP packets between processes using ports
- A port is a logical connection that associate a certain transfer with a running process

TCP

- Connection-oriented
- Reliable transport
 - acknowledgements
- Flow control
 - sliding window
 - window size
 - congestion avoidance

TCP versus UDP

Characteristics	UDP	TCP
QoS	Best effort	Reliable service
Connection establishment	No	Yes
Acknowledgements	No	Yes
Flow control	No	Sliding window, window size, congestion avoidance
Retransmission	No	Yes
Overhead	Low	Low but higher than UDP
Suitable for	Priority of speed, small packets, multicast/broadcast	Most application and protocols

TCP and IEEE 802.11 MAC



- TCP brings bad performance in IEEE 802.11
- Scenario 1: lots of low bit rate nodes
- Scenario 2: corrupted wireless packets

Layer 3 Firewalls

- Block outgoing traffic of type X
- Block incoming traffic of type Y
- Forward traffic of type Z
 - To provide an external service from an internal firewalled host
 - To provide multiple instances of a service from internal firewalled hosts for the purpose of load balancing

Firewall Design



- Crucial in wireless networks
- Traffic shaping and monitoring
- Detecting, blocking and removing malicious programs that exhaust bandwidth resources

OSI versus TCP/IP

Layer	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Network	Network
2	Data link	Media Access
1	Physical	

Application Layer

- Identify and make sure that the sender/receiver is ready for communication
- Authenticate (sender, receiver, message)
- Identify necessary communication resources
- Ensure agreements (error recovery, data integrity, privacy)
- Determine protocol and data syntax at application level

Application Firewalls

Prevents:

- SMTP, POP3 and DNS buffer overflow
- Webserver attacks based on information in http headers and requests
- Evil code hidden within SSL tunnels
- Block applications running at the top of HTTP (Messengering)
- Internal users to spread sensitive information

Application Firewalls

Disadvantages:

- Reduce performance in network
- Expensive
- Overrides personal integrity
- Missconfiguration

Application Firewalls



- Anti-virus and Anti-spam
 - Blocks or tags content
 - SPAM represents 30-50% of SMTP
- Web proxy server
 - Caches frequently requested data in RAM
 - Caches DNS lookups

Advanced Wireless Networking Implies



- Wise configuration of all protocol layers
 - Good network architecture
 - **The goal:**
 - Maximize the useful bits

Conclusions

- Building wireless networks that work is very “easy”
- Building wireless networks that perform **well** is not as “simple”
- Measure, measure, measure...
- Do not stop trying! Share your experiences with others.

Discussion Question:

How can we optimised a **VoIP wireless network**?

Layer	ISO	VoIP	
7	Application	Application	
6	Presentation		
5	Session	Transport	
4	Transport		
3	Network	Network	
2	Data link	Media Access	▼
1	Physical		