ITRAINONLINE MMTK
ADVANCED NETWORKING HANDOUT

Developed by: Alberto Escudero Pascual/ IT +46 <aep@it46.se>

Table of Contents

1. About this document

These materials are part of the ItrainOnline Multimedia Training Kit (MMTK). The MMTK provides an integrated set of multimedia training materials and resources to support community media, community multimedia centres, telecentres, and other initiatives using information and communications technologies (ICTs) to empower communities and support development work.

1.1 Copyright information

1.2 Requirements

To make best use of this unit you should have a basic understanding of Internet Protocols and the basic requirements for Internet connectivity, and be familiar with basic concepts such as Internet addressing and routing principles.

1.3 Degree of Difficulty

The degree of difficulty of this unit is Advanced.

2. Introduction

This unit is a review of the OSI/Internet protocol stack with focus on the issues that are critical in wireless network implementations. The unit outlines the effect of every layer in the overall performance of a wireless communication network.

The unit aims to give an understanding of how the different layers (components) of the OSI model affect each other and targets the key elements that need to be considered when performing network planning. The OSI model is used as a "reference" that help us to describe those interactions between components.

All through the document, the red icon below indicates that a section refers to **Wireless** networking in specific and not Internetworking in general.

3. The OSI model

The OSI *(Open Systems Interconnection)* Reference Model, created by ISO (International Standards Organization), is an abstract description for computer network (communication) protocol design. The model splits different communication functions in seven different layers that can work independent of each other.

A protocol design that follows the structure of the OSI model follows the principles of a '*stack*'. Having a *layered* or *stack* protocol model implies that each layer only uses the functionality of the layer below and only provides functionality to layers above. A protocol 'stack' can be implemented in either software, hardware of a combination of them both.

In many well known protocols the OSI model is not strictly followed in practise. For example, the Internet follows instead a four (4) level protocol suite consisting of media access control layer (link layer), network layer (IP), transport layer (TCP/UDP) and application layer.

Layer	***OSI***	***TCP/IP***
7	Application	Application
6	Presentation	
5	Session	Transport (TCP)
4	Transport	

Layer	***OSI***	***TCP/IP***
3	Network	Network (IP)
2	Data Link	Media Access Control
1	Physical	

Table 1: OSI model versus TCP/IP protocol suite.

Wireless standards normally refers to layer 1 and layer 2 of the OSI protocol *stack*, keeping the IP packet unaltered. The “IP packets” are transported over a **wireless specific** physical and data link protocols.

Wireless standards (IEEE 802.11, IEEE 802.16, Bluetooth, IrDA etc...) deal with physical and data link layers *only* and have been traditionally designed to carry all kind of types of data, IP is just one of the types. Wireless standards are designed outside of the Internet Engineering Task Force (IETF).

IEEE is *one* of the wireless standardization bodies http://standards.ieee.org/wireless

4. Media Access Control

The Media Access Control (MAC) layer in the TCP/IP model includes the OSI's *physical layer* that relates to the most physical aspects of the communication (modulation techniques, bit encoding, physical access to the share media etch) and the *link layer* protocol that is responsible for addressing and delivering packets from one computer (host) to another on a **common** shared channel.

In simple words, the physical layer is responsible of converting physical electromagnetic signals into **bits**, while the link layer is responsible of collecting those bits in a form of **data packet**.

Common physical layer protocols are RS-232, V.35, 10BASET, ISDN etc. ,
Common link layer protocols are Ethernet (IEEE 802.3), PPP, ATM etc.

Wireless networks protocols as IEEE 802.11 (WLAN) refer to both the *physical* and *link* level layers of the OSI model.

IEEE 802.11 family of protocols implements different physical (PHY) layer protocols based on spread spectrum (FHSS, DSSS, and OFDM).

The original standard IEEE Std 802.11-1997 specifies a single Medium Access Control (MAC) layer and 3 Physical Layer Specifications. The standard provides 2 Physical layer specifications for radio, operating in the 2 400 - 2 483.5 MHz band (FHSS and DSSS) and one for infrared.

More info: http://grouper.ieee.org/groups/802/11/main.html

4.1 Access control protocols

4.1.1 Carrier Sense Multiple Access (CSMA) and Collision Detection (CD)

The most popular physical access control mechanism where a set of computers access a common shared media is *Ethernet.* Ethernet protocol or IEEE 802.3 uses an access control protocol known as *Carrier Sense Multiple Access* (CSMA), which is an improved version of a *contention technique* scheme known as ALOHA.

When a node has data to transmit, it first listens to the media to see if any other node on the network is sending (by listening to the shared channel). If no other transmission is detected, the data is sent. It is possible and not uncommon that two different nodes can send data simultaneously since they both can detect an idle medium. In the case that multiple senders send data at the same time, a collision will occur and the data will be corrupted. The collision will be detected by the **receiver** since the CRC field in the MAC header will not match the existing payload. Corrupted data is discarded by the receiver.

Collision Detection (CD) is a second element of the Ethernet access protocol and is used by the **sender** to detect collisions. Nodes that are transmitting data can simultaneously monitor the shared media (they can listen what is in the media while sending). If an collision is detected (the node listens to something different from what was sent) the node stops the transmission and sends out a *jam sequence* to ensure receiving nodes that a collision has taken place and any recently packet should be dropped.

After a detected collision, all nodes will retransmit the data. To prevent the retransmissions colliding one more time, Ethernet uses a random back-off period (based on a random coefficient and the number of earlier retransmission) in order to calculate the time to wait for next transmission. Ethernet tries to minimize the probability of “re-collisions” after a collision detection.

IEEE 802.11 (WLAN)

The MAC layer of IEEE 802.11 (WLAN) is called CSMA/CA. It has a lot similarities with Ethernet, it uses CSMA to share media other wireless nodes but lacks collision detection (CD). The sender **can not detect a collision,** as the data in the media can not be “listened” while sending. IEEE 802.11 operates in half duplex (send/receive) by using a TDD scheme. Collision detection, as is employed in Ethernet, cannot be used for the radio frequency transmissions of IEEE 802.11

Since nodes can detect idle media but can not detect collisions in wireless media, the access point needs to send an acknowledgement to ensure a successful transmission instead. This mechanism creates an overhead and reduces the useful data throughput.

Due to these limitations, a well known problem occurs in point to IEEE 802.11b multipoint configurations, the “hidden-node” problem. In a point to multipoint configuration, a set of nodes talk to a common node named “Access Point”. A “hidden node” is caused by the fact that all nodes can not hear each other in a wireless network and collisions are unavoidable using just “CSMA.” To solve (or ease) the problem the MAC layer of IEEE 802.11 includes a mechanism call Collision Avoidance (CA). When using CA, the transmitting node needs to send a RTS (request to send) packet to the access point and wait for a CTS (clear to send) before starting the transmission.

Even though all nodes might not be able to hear the RTS packet send by other nodes, they can always hear the CTS packet sent by the access point address to a given node. Hence, the nodes can avoid sending data during the time allocated by the access point to another node.

When the number of nodes in the network and the distance between the nodes and access point increases, RTS/CTS does not scale and other alternatives to IEEE 802.11b are needed.

IEEE 802.16 (WMAN)

IEEE 802.16 has taken some problems present in IEEE 802.11 into consideration and offers solutions to the “hidden node” problem for PtMP in radio links. After all, IEEE 802.11 was not intended/designed for outdoor environments. IEEE 802.16 is using a combination of TDMA and DAMA to deal with the problems that IEEE 802.11 still fighting with.

It is very important to mention that due to the native limitations in the MAC of IEEE 802.11, a good design of the network and transport architecture of wireless networks is required. Experience has shown the negative effects of adding many nodes to a wireless network when the network and transport issues have not been taken into account.

4.2 MAC Addressing

A MAC address is used in the *link layer* as the mechanism to identify and address data traffic to host in a shared media. It consists of a universally unique sequence of 48-bits (12 hex digit) associated with a particular wireless network interface (device).

When a data packet is sent over a shared media, the source and destination of the computers (hosts) are included in the header of the packet. When a packet needs to be send to all hosts (broadcast), a special MAC address is used, in Ethernet the broadcast MAC address is ff:ff:ff:ff:ff:ff (all 48 bits to 1)

In normal circumstances, the *network interface cards* (NIC) only pass to the Operative System the data packets that match the MAC address of the computer.

The MAC address is normally hardware coded when shipped from the vendor.

Using MAC addresses for authentication

It has become very common in many wireless ISPs (WISP) to use the MAC address of the wireless interface as a mechanism to limit/provide access to a wireless network. The assumption is that MAC addresses are “hard-coded” and can not be modified by normal users. The reality is different and MAC addresses in most (wireless) network interfaces **can easily be modified**.

An authentication mechanism based on MAC addresses is insecure.

4.3 Link level encryption

Link level encryption is the process to *secure data* at the link level when data is transmitted between two nodes attached to the same physical link (they can also be in two different physical links by means of a repeater e.g. Satellite). Any other protocols or application data running over the physical link are protected from eavesdroppers.

Encryption requires a certain key or secret shared between the communication parties and an agreed encryption algorithm. When the sender and the receiver are not present in the same media the data needs to be decrypted and re-encrypted in each of the node along the way to the receiver.

The link level encryption is normally used when higher level protocol encryption is not present.

Link level encryption in IEEE 802.11

The best known link level encryption algorithm for IEEE 802.11 is the so called Wired Equivalent Privacy (WEP). WEP has been proven to be insecure and other alternatives have been proposed and standardised as the Wi-Fi Protected Access (WPA). The new standard IEEE 802.11i will include an enhancement of WPA, named WPA-2.

Link encryption **does not provide end-to-end security** outside of the physical link and should always be consider as just an *extra security* measure in your network design.

Link encryption requires more hardware resources in the access points and the security design of key distribution and management.

5. Network layer (IP)

The IP (Internet Protocol) layer is a protocol used to transmit data across a *packet-switched network.* Data sent over an IP network is referred as packets (or datagrams). The IP protocol provides is an unreliable service (best effort) with no guaranty for delivery. Packets can arrive damaged, duplicated, out of order or be entirely discarded by any host along the path.

An important part of the IP protocol, is the source and destination address of the communicating parties. That information (the addresses) is not only used to route packets, identify Internet hosts but is also required by higher level applications as firewalls.

5.1 Addressing

The most commonly used IP protocol is IPv4 which uses a 32-bit field for addressing.
Ipv6. The next generation of IP protocol uses 128-bit source and destination addresses to avoid the fact that IPv4 are running out of ***available*** addresses.

5.1.1 Subnetting and netmask

The most common reason to use subnetting is to control/divide network traffic. Subnetting allows single routing entries to refer to either a subnet or its individual hosts. This implies that a single routing entry can be used throughout the Internet while more specific routes only is required for routers in the subnetted block.

A netmask is a 32-bit number that specifies the network of an given IP address. The netmask is split into a network partition and a host partition (bitwise) where the 1's symbolize the network and the 0's symbolise the host.

10.0.0.0/255.0.0.0	A Class
10.1.0.0/255.255.0.0	255 B Classes
10.1.1.0/255.255.255.0	255 C Classes
10.1.1.128/255.255.255.128	Half C Class (127 Address)
10.1.1.64/255.255.255.192	63 host addresses
10.1.1.8/255.255.255.248	7 host addresses

Table 2: Subnetting an A class network

A logical AND operation between the IP address and the subnet mask results in the network address.

There are some restrictions on the subnet address. Host addresses consisting of all "0"s or all "1"s are reserved for specifying the local network and the broadcast address. This rule also applies to subnets. This implies that a 1 bit subnet mask is not allowed.

To calculate the number of subnets and hosts that a certain subnetmask will allow the following formula can be used:

Number of subnets = 2^n-2 where n is the number of bits in the subnet
Number of host in subnet = 2^m-2 where m is the number of bits in the host network
Total number of hosts = $(2^n-2)\ (2^m-2)$

Subnetting in wireless networks

It is a common practise in many wireless ISPs not to subnet their networks properly. Having a big subnet without many routing decisions is very easy to deploy but on the contrary when the networks grow, troubleshooting is far more complex.

Having a good subnetting and routing design in the wireless network limits the amount of useless broadcast traffic and probes to scale better.

Avoid the use of one single big subnet as much as possible. Limiting the subnets to 32-64 hosts size is recommended.

5.2 Error control

Error control is handled by a set of control messages at the IP level, ICMP (Internet Control Message Protocol). The protocol does not provide extensive error control but merely reports error to the originating hosts.

Two of the main uses of ICMP are the following types of operations.

- Report problems that prevents delivery (such as "**Destination Unreachable**")
- **Troubleshooting the network** through use of request and reply messages (such as "Echo Request" and "Echo Reply" used by *ping*)

An ICMP error message always contains the full IP header (including options) of the IP datagram that failed and the first eight bytes of the IP data field. The error can therefore be associated with a certain protocol and a particular process (from the port number in the TCP or UDP header which are the first eight bytes in the IP data field).

Monitoring ICMP in wireless networks

Monitoring the ICMP traffic in your wireless network will allow you not only to identify connectivity problems inside of your network but the presence of some *viruses* and Trojans. Many viruses and Trojans include automatic network scanning, the presence of a high level of **Destination Unreachable ICMP** traffic can be indication of viruses activity.

5.3 Routing

The process of transfer a packet of data from source to destination is called *routing*. A *routing decision* is made in each computer between the source and destination to determine the most suitable next hop towards the target machine. The routing decision is specified in the *routing table***.**

All common routing algorithms use either the *destination* or *source* of the IP address. In the first case the route is determined by looking at the destination address of the packet (most commonly used) while the second one uses the source address to determine the path to the target. A third option is known as "policy-based routing", where routing decisions are dependent on other sources of information (MAC address, type of service, network load etc.).

Using IP Source as a routing decision

Using the IP Source address to make a routing decision is an interesting mechanism to include load balancing in wireless networks. By including a router that can make decisions based on the source address of the packets we can apply different Quality of Service to different nodes and even route different users of a wireless network to different border routers.

For example, the use of source-IP based policy-routing does not require changing the subnetting of your wireless network to provide a certain host a different upstream gateway than others.

5.4 NAT (Network Address Translation)

NAT translation as a general concept is the capability of a router to "rewrite" the source or destination address of a IP packet (datagram). NAT became popular because it allows single devices with a public IP address to *represent* a group of computers in a private network.

NAT is not only useful when there is a shortage of public IP addresses but also as a mechanism to implement other network functions:

1. Firewall / DMZ
2. Traffic load balance (e.g. identical web servers behind a NAT to balance requests)
3. Computing load balance (e.g. identical databases to balance computing load of queries)

This section will focus on how NAT can be used to enhance security in a network. For clarity, NAT have been divided into two main functions; SNAT (manipulation of source addresses) and DNAT (manipulation of destination addresses).

5.4.1 Masquerading - SNAT

IP masquerading or Source NAT allows hosts with private IP addresses to communicate with hosts outside their own network by letting one machine act on others behalf. IP masquerading is a *simple* and limited form of a firewall. Masquerading does not allow a host to **initiate** a connection to another host inside of the network.

Masquerading rewrites the source address of the packets as they pass through the router, so that the target machine always sees the router itself as the sender. When the recipient of the traffic answers back, the router rewrite the destination address to the original sender.

Masquerading adds some level of security by acting as a type of firewall but also limits the users inside of the network to provide services to the outside.

NB In a pure sense, MASQUERADE is not identical to SNAT, since masquerading flushes previous connections when the interface goes down or changes IP address.

5.4.2 Destination NAT - DNAT

DNAT (Destination Network Address Translation) is commonly used to make a service publicly available from an internal network (private IP address) through rewriting the destination IP address of the packet.

DNAT can be used to route traffic inside of a DMZ. The DMZ or Demilitarized Zone is the area of a network that is dedicated to host public services. The DMZ is normally placed in another network segment isolated from other transit traffic.

By using DNAT we can redirect (*map)* incoming traffic to a certain public IP address and port number to one IP address and port number of the DMZ.

Manipulating traffic in a wireless network

NAT (SNAT/DNAT) can be used to manipulate traffic inside of a wireless network. While the users (hosts) of the network have the same settings, we can affect how their traffic is routed and which services are made available to them.

For example:

We can apply NAT to redirect web requests to a proxy server, furthermore we can also redirect different segments of the network to different web proxy servers attached to different Internet providers.

NAT can also be used to redirect users to a captive portal where they have to register or enter their wireless account information.

5.5 IP tunneling – IPSEC

IP tunnelling is a method to transport IP packets inside of other IP packets to allow packets destined for one IP address to be redirected to another network first. Tunnelling is the process of *encapsulating* IP packets. When the encapsulation is done inside of an encrypted IP packet, the IP tunnelling is known as secure tunnelling or VPN.

IP tunnelling requires that the end-points of the tunnel are *fully routable* and not blocked by firewalls or NATs.

Using IP tunnelling does not provide any added security if the encapsulated packet (the packet that travels inside) is not encrypted. The most common way to build secure IP tunnelling is to use IPSEC.

IPSEC is a set of protocols that ensures security on the IP level. IPSEC supports secure IP encapsulation and provide certain security properties to all applications running at the top of IPSEC.

When it comes to security on IP level, there are 3 kind of protection that IPSEC can ensure:

1. **Confidentiality** (protection of content)
2. **Authentication** (verification of message sender)
3. **Integrity** (content has not been forged)

To ensure those security properties, IPSEC uses three main protocols, in a nutshell:
Authentication Header (AH): Strong Crypto checksum on the "whole" IP packet. A correct checksum in a received packet ensures that the packet was originated by the intended sender and has not been modified during transfer.

Encapsulating Security Payload (ESP): Strong encryption on the payload. A correct decrypted packet ensures the protection of the content of the packet. The packet was encrypted using a *common shared secret* between the communicating parties.

Internet Key Exchange (IKE): Provide ways to negotiate keys session keys.

IPSEC in wireless networks

IPSEC requires end-to-end routability in a wireless networks. If you plan to deploy IPSEC, avoid the use of NATs and deploy full functional firewalls instead.

IP encapsulation also includes an extra overhead, using IPSEC in conjunction with compression is recommended for optimization.

IPSEC requires the design of a proper key management. If a very limited set of parties are going to communicate with IPSEC, the most simple *key distribution method* is the use of symmetric keys. Unfortunately, perfect forward secrecy will not be guaranteed.

If you need to build VPNs inside of you wireless network you can also consider using Application Layer VPNs. Application layer VPNs normally use UDP tunnelling and SSL protocol for encryption.

More information about application VPNs can be found in:
http://www.openvpn.org/

6. Transport Layer (TCP)

The Transport Layer supports transfer of IP packets between processes (services) using ports (numbers). A TCP port is a logical connection that associates a certain transfer with a running process.

6.1 TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) is a *connection-oriented* transport protocol that provides *reliable* transport of data between pairs of process. The reliability is ensured by the implementation of flow control and error correction in the protocol.

The flow control between sender and receiver is managed by using *sliding windows, window size adjustment heuristics and congestion avoidance algorithms*. These three mechanisms should ensure that the resources of a share media are distributed equally among the different **sessions** in progress.

The *acknowledgement* sent for each packet that was correctly received constitutes the error correction (control) mechanism in TCP that controls the re-transmission of packets.

TCP is suitable for applications that require reliable transport of data (such as http, ftp, smtp etc).

6.2 UDP (User Data Protocol)

UDP (User Datagram Protocol) is a another transport layer protocol that provides *best-effort* service for transport of datagrams. The service is unreliable and implies no protection from duplicates of packets or packet loss. No flow control or error correction is implemented in UDP. The only mechanism that UDP supports to verify if data is corrupted or nor, is a checksum of the payload. If the receiver discovers a corrupted frame by its non-correct checksum, it simply drops the packet without any attempt to ask for re-transmission.

UDP is suitable for some types of RTA (Real Time Applications) where the speed of the transfer is of greater importance than the reliability of the service.

Characteristics	**UDP**	**TCP**
QoS	Best effort, not reliable	Reliable service
Protocol Connection	Connection-less	Connection oriented
Acknowledgements	No acknowledgements	All data is acknowledged
Retransmissions	Not implemented	Lost data is automatically retransmitted.
Flow Control	None	Sliding windows; window size adjustment, congestion avoidance
Overhead	Very low	Low, but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Suitable for:	1. When speed is a priority more than reliability. 2. Transfer of small data packets 3. Where multicast/broadcast are used	Most protocols

Table 3: A comparison between the characteristics of UDP and TCP.

Anomalies between TCP and IEEE 802.11 MAC

It is important to mention that TCP does not perform well in IEEE 802.11 wireless networks and multiple research has been done to enhance its performance.

1. IEEE 802.11b MAC known as *CSMA/CA channel access* method guarantees an equal long term channel access probability to all hosts. The implication is that when one host captures the channel for a long time because its bit rate is low, it penalizes other hosts that use the higher rate.
2. TCP assumes that packet lost is due to congestions. TCP cannot distinguish between **corruption and congestion,** so it unnecessarily reduces window, resulting in low throughput and high latency.

Due to the CSMA/CA protocol overhead, in practice the maximum 802.11b throughput that an application can achieve (in a PtP link) is about 5.9 Mbit/s over TCP and 7.1 Mbit/s over UDP.

It is highly recommended to design to wireless networks as “symmetric as possible”. Try to get nodes to listen to each other and use similar effective power rates.

Include some *traffic shaping* mechanism in the border router. Traffic shaping allows to control TCP congestion and can help to distribute the bandwidth resources evenly.
Further reading: http://www.ieee-infocom.org/2003/papers/21_01.PDF

6.3 Layer 3 Firewalls

In the transport layer, a firewall is implemented to control the network traffic by blocking TCP or UDP ports. Since many applications use “well known” ports for their communications, packet filtering can be used to block for example FTP (port 20) or Telnet (port 23) or SMTP (port 25).

There are two different strategies when it comes to firewalls on TCP level. Either you block all ports and only opens the ones that you truly need, or you open all ports and then block only the ones that you see as a threat. The more restrictive alternative that blocks all ports that you don’t want to keep open is of course the safest one.

Firewalls use a combination of three main methods:

- block outgoing traffic of type X
- block incoming traffic of type Y
- forwarding traffic of type Z

Forwarding implies that the firewall passes all incoming connection for a certain port to another host and port within the network. By forwarding ports you are creating a hole in your firewall since you allow incoming packets to enter your network. The main purposes of port forwarding are

- 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

The firewall is a fundamental part of a wireless network. It can block malicious code entering the wireless network and help us to allow us to decide which services we want to make available to our users. A wireless network should be considered as a “limited” resource and hence needs service prioritization.

A good wireless design should combine a **firewall, traffic shaping and monitoring**. Most of the troubleshooting in wireless networks comes from (1) detecting, (2) blocking and (3) removing malicious programs that exhaust the bandwidth resources.

For example, if we find interesting the use of peer-to-peer programs, a set of limited bandwidth resources should be allocated to them.

7. Application layer

The main responsibility for the application layer is to ensure that effective communication with other application programs in a network is possible. It is important to understand that the application layer is NOT the application itself. It is purely a service layer that provides the following services:

1. Identify and make sure that the other part is ready for communication
2. Authenticate (message, sender, receiver)
3. Identify necessary communication resources
4. Ensure agreement between sender and receiver regarding error recovery procedures, data integrity, privacy
5. Determine protocol and data syntax rules at application level.

The most widely used application layer protocols today are HTTPS, SMTP, IMAP/POP3, FTP, Messengering Protocols and RTP.

7.1 Application firewalls

The firewalls that has been discussed so far has been operating on network and transport layer. With such firewalls, you are able to do the following:

- block or allow incoming traffic from a particular IP address
- block or allow outgoing traffic to a particular IP address
- block or allow incoming/outgoing traffic using a particular TCP or UDP port

What these firewalls can't to is to examine the actual content of that data and *block packets based on its contents*. For achieve that, you need to filter the data on application layer: Application Layer Filter (ALF).

ALF can identify abnormal information in the header of the message and in the data itself.
It can be configured to search for certain strings in the data to block the message based on that information. With those characteristics, ALF can prevent the following:

- SMTP, POP3 and DNS buffer overflows
- Web server attacks based on information in HTTP headers and requests
- Attack code hidden within SSL tunnels
- Block applications running at the top of HTTP (Messengering)
- Internal users to spread "sensitive: information

ALF can also block specific commands within the application layer protocols. For example, in HTTP the command GET can be blocked while POST is still allowed.

The primary disadvantage of ALF is its negative effect on performance due to the examination of all data. It also raises some ethical questions as building ALF implies having the capabilities of analysing personal data in real time.

An implication of that is that more powerful hardware is needed than for traditional packet filtering firewalls which has a direct impact in the price of the service.

A disadvantage that occurs due to the complexity that ALF brings to the network, is the risk of misconfiguration of the filter with may result in incorrect blocking of data.

Application Layer Filter

A common variation of application layer filters are *anti-virus* and *anti-spam* systems. Anti-virus/spam system are able to examine the contents of the application and block or tag suspicious e-mail attachments.

When designing a wireless network you will have to consider implementing such application layer filter. SPAM represents today between 30-50% of the total SMTP traffic. By tagging SPAM and training users to run IMAP in their mail clients, you can avoid the transfer of unsolicited mail over wireless links.

Another application layer filter that you might consider implementing is a web proxy server. A web proxy server is used to cache frequently requested data in RAM and cache DNS-lookups.

8. Conclusions

One of the advantages of the OSI and the Internet model is that they guarantee that each of the protocol layers can work independently of each other. It gives the flexibility of exchanging our physical layer and move our applications from the wire to the wireless network. The model also allows us to describe better the interactions between layers (components) of a communication network.

But it is the wise configuration of **all protocol layers** and a good network architecture what will give to wireless users a good and optimal quality of service. When designing a wireless network do not underestimate the mechanisms that are available in the network, transport and application layer to enhance the performance of your overall wireless networks.

Maximizing the **useful bits** is a task that requires understanding the effect of each protocol layer in the overall network performance.

The five main issues you should remember from this unit can be summarized as:

1. Building wireless networks that work is very “easy” but building wireless networks that perform **well** is not as simple
2. The key issue in any networking is to maximize the useful bits in each protocol layer, i.e. minimize overheads.
3. Only by measuring the performance of your network, you can find out what can be improved
4. Building good wireless networks in complex scenarios requires experience but that should not stop you trying. Join discussion forums and share your experience with others.