Esame di Reti di Calcolatori e Sicurezza

26 giugno 2006

1. In barba agli standard, si vuole realizzare una rete "pseudo fast Ethernet" a 100Mbps su un segmento unico (cioè senza ripetitori) di cavo coassiale lungo 2000 m.

   (a) Qual'è la lunghezza minima di un frame?

   (b) Qual'è l'efficienza di canale per questa rete, nel caso ottimale in cui la probabilità di acquisizione del canale in uno slot di contesa sia $A = 1/e$ e il payload dei frame sia di 1500 byte?

   (c) Si citino (almeno) un vantaggio e uno svantaggio rispetto alla soluzione standard 100Base-TX (100Mbps su doppino Cat.5).

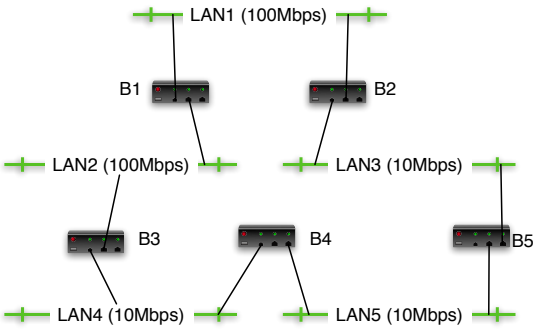
   Risposta:

   (a) (2pt) Si può fare (i cavi coassiali possono operare a frequenze ben maggiori), a patto che la lunghezza minima dei frame consenta il rilevamento delle collisioni. Il tempo di propagazione è $\tau = 2000/200 \cdot 10^6 = 10\mu$sec, quindi un frame non può durare meno di $2\tau = 20\mu$sec, ossia la lunghezza minima è $F_{min} = 2\tau B = 20 \cdot 100 = 2000$ bit = 250 byte.

   (b) (3pt) Usando la formula 4.7 del Tanenbaum, e ricordando che un frame contiene 18 byte oltre al payload, $R = \frac{1}{1+2BLe/cF} = \frac{1}{1+\frac{2 \cdot 100 \cdot 2000 \cdot 2,718}{200 \cdot 1518 \cdot 8}} = 69\%$

   (c) (3pt) Vantaggi: lunghezza molto superiore (2000 m invece di 100+100m); risparmio del costo dello switch centrale. Svantaggi: efficienza minore (c'è un solo dominio di collisione), delicatezza hardware, lunghezza frame minima superiore a quella di Fast Ethernet, comunicazione half duplex invece di full duplex.

2. Si consideri la seguente rete locale:



Bridge	Identifier	Priority
B1	08:00:2B:34:4A:21	32768
B2	08:00:2B:24:40:2F	32768
B3	08:00:2B:1A:85:20	32768
B4	08:00:2B:24:5A:21	32768
B5	08:00:2B:99:10:A1	32768

   (a) Si determini il root bridge

   (b) Si determini il root path cost di ogni LAN.

   (c) Si determini la root port di ogni bridge

   Risposta:

   (a) (2pt) Il root bridge è B3, perché ha l'ID minore e la priorità è uguale per tutti.

   (b) (2pt) LAN2=LAN4=0;
   LAN1=1000/100=10;
   LAN5=1000/10=100;
   LAN3=10+1000/100=20

   (c) (2pt) B1: su LAN2; B2: su LAN1; B4: su LAN4; B5: su LAN3. (Naturalmente B3 non ha root port perché è il root)

3. (a) Perché IPsec (a differenza di IP) è da ritenersi un protocollo orientato alla connessione?

   (b) Si potrebbe progettare una variante di IPsec senza connessione, e a che prezzo?

   Risposta:

   (a) (2pt) Perché all'inizio della connessione viene stabilita la *Security Association*, che è una informazione che viene mantenuta per più pacchetti (fino a 2^{32}, precisamente).

Inoltre ogni pacchetto ha un contatore progressivo (il Sequence Number) che lo distingue nella sequenza, per evitare attacchi replay.

(b) (3pt) Si potrebbe fare, a patto di omettere il numero di sequenza nei pacchetti e di negoziare una SA per ogni pacchetto da trasferire, oppure usare una cifratura a chiave asimmetrica (come PPTP). Questo però da un lato espone la trasmissione ad attacchi replay, e dall'altro comporta un notevole traffico di rete e un forte carico computazionale aggiuntivo, e quindi una inaccettabile perdita di performance.

4. (a) Si descriva il principio di funzionamento del cifrario 3DES.

   (b) Perché è stata adottata una struttura encrypt-decrypt-encrypt?

   (c) È possibile usare 3DES come cifrario a flusso (stream cypher)?

   Risposta:

   (a) (2pt) 3DES è un cifrario prodotto ottenuto componendo tre funzioni di DES: date due chiavi DES (K_1, K_2), si definisce $E^{3DES}_{K_1,K_2}(M) = E^{DES}_{K_1}(D^{DES}_{K_2}(E^{DES}_{K_1}(M)))$.

   (b) (3pt) Perché $56 * 2 = 112$ bit di chiave sono già sufficienti per un buon grado di sicurezza ($2^{112} = 5.19 * 10^{33}$ chiavi); perché se $K_1 = K_2$ il 3DES degenera nel DES; perché uno schema EE è vulnerabile ad un attaccho meet-in-the-middle.

   (c) (2pt) Sì. Si parte da un blocco di 64 bit (=8 byte) noto (l'IV), e lo si cifra con la chiave. Si ottengono i primi 8 byte dello keystream, da usare uno alla volta per lo XOR dei dati. Gli stessi 8 byte vengono cifrati nuovamente con la stessa chiave, ottenendo un secondo blocco di 8 byte del keystream, e via di seguito.

5. [Da sviluppare su un foglio a parte]

   (a) Si descriva la fase di Scanning della metodologia di attacco; in particolare, si descrivano le tecniche di port scanning "TCP Connect Scan", "Syn Scan", "Ack Scan".

   (b) Si spieghi in quali condizioni e con quali tecniche di scanning è possibile distinguere un firewall stateful da uno stateless.