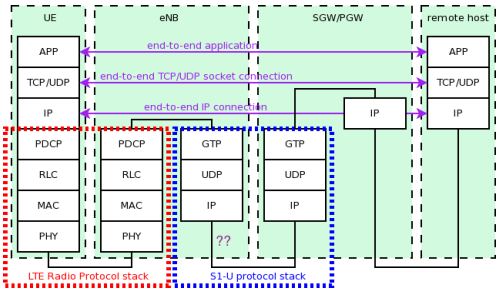
DMIF, Università degli Studi di Udine I appello A.A. 2017-18 — 29 gennaio 2018

Esame di **Reti di Calcolatori**

Soluzione

1. Nella figura a fianco è mostrata l'architettura di rete di LTE. Si mostri la forma (ossia, sequenza di intestazioni e payload) dei messaggi scambiati tra gli strati IP di eNB e SGW/PGW (ossia, nel punto indicato da "??").
(Sugg.: non è necessario conoscere LTE per rispondere).
R: IP-UDP-GTP-IP-(TCP o UDP)-payload applicativo



2. Lo standard WiFi 802.11n può usare uno o due canali nella regione dei 5 GHz, di bandwith di 20 MHz. In condizioni normali, permette di avere un bit rate di (circa) 80 Mbps di dati senza errori. Determinare il rapporto SNR nominale minimo per uno dei canali.

   R: Dal teorema Shannon-Hartley abbiamo la seguente relazione per la capacità del canale: $C \leq B\log_2(1+SNR)$; quindi $80Mbps \leq 20MHz\log_2(1+SNR)$ da cui $SNR = 15 \approx 12dB$ (ricordiamo che la conversione in dB è $SNR_{dB} = 10\log_{10}(SNR)$.

3. Nella situazione dell'esercizio precedente, determinare la dimensione minima dell'alfabeto per i simboli trasmessi in un baud, supponendo di usare un FEC Hamming (7,4) (4 bit di dati con 3 di parità).

   R: Su un canale di larghezza 20MHz si possono trasmettere al massimo 40Mbaud. Dai conti precedenti, il bit rate "netto" è $80/40 = 2$ bit per Baud, ma, tenendo conto del code ratio di 4/7, per poter ottenere 2 bit di dati utili da ogni Baud bisogna avere 3.5 bit trasmessi per Baud (ovvero, 7 bit ogni 2 baud). Per cui la dimensione minima dell'alfabeto è di $2^{3.5} = 11.3 \approx 12$.

4. Una certa linea ha una probabilità di errore per bit $p = 10^{-6}$. Se gli errori sono indipendenti, si calcoli la probabilità di ricevere un frame da 1000 bit con esattamente 1 bit errato.

   R: Dato $n = 1000$, è $P(1err) = \binom{n}{1} * p * (1-p)^{n-1} = 9,99 * 10^{-4} \approx 10^{-3}$.

5. Nel protocollo 802.3 (Ethernet, 10Mbps), se la distanza massima tra le stazioni fosse di 5000m invece di 2500m (ma sempre con massimo 4 repeater con un ritardo di $5\mu s$ ciascuno), quanto sarebbe la dimensione minima del frame?

   R: Il tempo di propagazione massimo sarebbe di $25 + 4 * 5 = 45\mu s$ invece di 22,5 μs, di conseguenza il RTT sarebbe di 90 μs, che a 10 Mbps corrisponde ad un frame minimo di 900 bit.

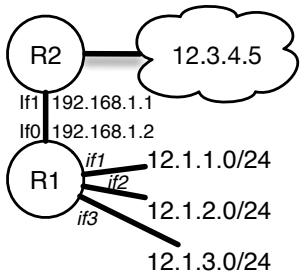
6. La rete 153.84.26.0/23 viene suddivisa in 4 sottoreti uguali. Si diano gli indirizzi di tali sottoreti, e il range di indirizzi assegnabili agli host della prima di queste sottoreti.

   R: Le reti sono 153.84.26.0/25, 153.84.26.128/25, 153.84.27.0/25, 153.84.27.128/25. Il range della prima sottorete è 153.84.26.1—153.84.26.126.

7. Ad un host arriva un pacchetto IP con Length=1200, Offset=150, MoreFragments=0; poi un pacchetto IP con Length=400, Offset=100, MoreFragments=1. Cosa deve fare l'host per ricostruire il pacchetto?

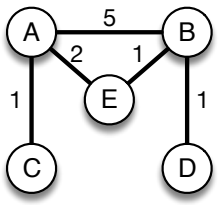
   R: I due frammenti sono rispettivamente l'ultimo e il secondo di un pacchetto. Mancano i dati dalla posizione 0 alla 799, perché il secondo frammento inizia da 100*8=800. Quindi il datagramma IP non può essere ricostruito e consegnato, se prima non arrivano il frammento mancante. Alla scadenza del timeout (tipicamente 30 secondi) tutti i frammenti vengono scartati; eventualmente (ma non è obbligatorio) viene inviato un ICMP di notifica al mittente.

8. Si dia la tabella di inoltro del router R2.
R:



Net/CIDR	if	next hop
12.1.0.0/24	if0	12.3.4.5
12.1.0.0/22	if1	192.168.1.2
192.168.0.0/16	if1	-
/	if0	12.3.4.5

9. I router a lato impiegano un algoritmo basato sul vettore delle distanze. Si dia il vettore iniziale di E (a) all'inizio; (b) dopo che ha ricevuto quello iniziale di A.
R:



Dest	d	next hop
A	2	A
B	1	B
E	0	-

Dest	d	next hop
A	2	A
B	1	B
C	3	A
E	0	-

10. I protocolli di routing basati sul vettore di percorso, come BGP, non tengono conto di eventuali costi degli "hop" tra AS, ma solo dei percorsi. Ma allora perché non si potrebbe usare un protocollo basato sul vettore delle distanze, come RIP, ove ogni hop ha costo 1?

    R: Perché nel routing interdominio l'instradamento non segue necessariamente il percorso più breve, ma si decide in base ad altre politiche (ad esempio tipo di AS), per cui bisogna conoscere l'intero path per ogni destinazione e non solo la distanza. Inoltre RIP e simili non scalano abbastanza alla dimensione necessaria per il routing interdominio (la stabilità si raggiungerebbe troppo lentamente). Infine c'è il problema dell'instabilità causata dai loop (quella che in RIP si risolve con l'"infinito finito").

11. Un utente sta ascoltando musica in formato MP3 a 128kbps; i dati sono trasmessi via UDP in datagrammi da 1kB di payload. In media, un datagramma ogni 100 non arriva; in tal caso, il client ne richiede la ritrasmissione con un altro datagramma UDP di payload 100 byte. Quanta banda (n kB/s)viene impiegata complessivamente (download + upload), comprendendo anche le intestazioni UDP e IPv4?

    R: 128kpbs corrispondono a 16kB/s, quindi in un secondo vengono ricevuti 16 datagrammi da 1kB e spediti 0,16 datagrammi da 100byte (per richiedere le ritrasmissioni). L'intestazione UDP è di 8 byte, quella IP è di 20 byte, quindi l'overhead per ogni datagramma è di 28 byte. Complessivamente il traffico è $16 * (1024 + 28) + 0,16 * (100 + 28) = 16852,48$ B/s $= 16.46$ kB/s.

12. In assenza di ritrasmissione veloce, quando viene ritrasmesso un segmento TCP? Come viene inizializzato il timeout nel momento in cui la connessione si porta nello stato ESTABLISHED?

    R: Viene ritrasmesso se non viene riconosciuto (ossia, non arriva un ACK che lo comprenda) entro un intervallo di tempo, il timeout. Questo viene inizializzato durante la fase di handshake, osservando il tempo che intercorre tra l'invio di un segmento e la ricezione della sua risposta.

13. Durante una connessione TCP, A ha inviato a B un segmento con `SequenceNum`=1000, Length=1000, poi uno con `SequenceNum`=2000, Length=1000, e poi uno con `SequenceNum`=500, Length=500. A questo punto riceve da B un segmento con `AdvertisedWindow`=1000, `Acknowledge`=2000. Quanti byte può ancora spedire A?

    R: B ha sicuramente ricevuto fino a 1999; del resto non sappiamo niente, ma evidentemente il segmento con SequenceNum=2000 non è arrivato; siccome potrebbe essere solo in ritardo, A deve ritenere che sia ancora in viaggio, come il suo successore. Quindi se il segmento da 1000 byte con SequenceNum=2000 arriva a destinazione, riempie completamente i 1000 byte liberi nel buffer di B, quindi A non può mandare ancora niente finché la finestra non si riapre.

14. Si consideri una comunicazione TCP con recupero veloce con MSS=2kB e CongestionWindow=10kB. Vengono eseguiti 5 cicli di incremento additivo senza problemi, ma durante il sesto ciclo due segmenti inviati non vengono riconosciuti. Quanto diventa CongestionWindow alla fine del sesto ciclo?

R: Durante i 5 cicli senza problemi si incrementa di 1 MSS per ciclo, quindi all'inizio del sesto ciclo CongestionWindow=10+2*5=20kB. Nel sesto ciclo vengono inviati 20/2=10 segmenti, ma solo 8 vengono riconosciuti, quindi l'incremento è MSS*8/10 = 1,6kB. La nuova CongestionWindow è 21,6kB.

15. Dopo che gli ha fatto riparare tutti i bagni del castello, la principessa Peach paga l'idraulico Mario con un assegno bancario. Si dica che tipo di attacco è ognuna delle seguenti azioni che Mario potrebbe tentare: a) Alterare l'importo dell'assegno; b) Alterare l'intestazione dell'assegno (ossia il conto corrente da cui prelevare i soldi); c) Fotocopiare l'assegno e provare ad incassarlo più volte.

    R: a) attacco all'integrità. b) attacco masquerade; c) attacco replay.

16. Alice vuole mandare a Bob un messaggio M garantendo integrità e confidenzialità. A questo scopo, il messaggio viene suddiviso in blocchi $M = M_1 M_2 \dots M_n$ ognuno dei quali è cifrato con AES in modalità CTR; quindi ciò che viene inviato è $C = C_1 C_2 \dots C_n$ dove $C_i = M_i \oplus E_K(i)$, dove K è una chiave precondivisa. Se Alice successivamente manda a Bob un nuovo messaggio M', usando lo stesso meccanismo (e quindi ripartendo con il contatore da 1), Bob può essere sicuro dell'autenticità di M'?

    R: No, perché un attaccante potrebbe sostituire il blocco i-esimo di M' con il blocco i-esimo di M, e la decifratura avrebbe successo.

17. Cosa significa se due utenti scoprono di avere nei propri certificati X.509, regolarmente rilasciati da due CA, lo stesso modulo n e lo stesso esponente e (che solitamente è 65537)? In tal caso cosa si deve fare?

    R: In tal caso significa che i numeri primi generatori sono gli stessi, e quindi anche le due chiavi private coincidono. Questo è grave, quindi i certificati vanno immediatamente ritirati. Comunque la probabilità che succeda è molto bassa.

18. Nel protocollo a lato PU_A è la chiave pubblica di A, nota a B, e H è una funzione di hash. Il messaggio M è (a) autentico per B? (b) puntuale (ossia non soggetto ad attacchi replay)? (c) ripudiabile da A?

    1. $A \to B : A, M$
    2. $B \to A : E_{PU_A}(N)$
    3. $A \to B : N, E_{PR_A}(H(M))$

    R: (a) sì, perché c'è la hash di M firmata con la chiave privata di A (b) no, perché la hash non è autenticata al passo 3, quindi un attaccante potrebbe riproporre un messaggio vecchio al passo 1 e la corrispondente vecchia hash al passo 3, assieme ad una nuova nonce. (c) no, è firmato al passo 3.

19. Alice riceve una mail S/MIME cifrata con una chiave pubblica PU_A intestata a lei, di cui possiede la chiave privata PR_A, ma il certificato X.509 è scaduto da qualche ora. (a) Alice può dire che il messaggio è confidenziale? (b) Può Alice rispondere firmando con la chiave privata PR_A?

    R: (a) se la chiave è scaduta al termine della sua durata naturale, sì. (b) no, non può, rischia che la firma non venga riconosciuta.

20. Perché in IPsec le intestazioni AH e ESP contengono un numero di sequenza? Cosa fa un host quando riceve un pacchetto il cui numero di sequenza è più grande del massimo numero osservato fino a quel momento?

    R: Per applicare la misura anti-replay: pacchetti che arrivano doppi o troppo tardi vengono scartati. Lo accetta (se è corretto), e sposta la finestra anti-reply puntandone l'inizio sul nuovo pacchetto appena arrivato.