DMIF, Università degli Studi di Udine — III appello A.A. 2017-18 — 18 giugno 2018

Esame di **Reti di Calcolatori**

Soluzione

1. Si supponga di progettare uno stack di rete a pacchetti simile a TCP/IP, ma in cui il controllo di flusso viene implementato a livello datalink in tutti i nodi. Quali servizi rimangono da implementare al livello del protocollo di trasporto affidabile (tipo TCP)?

   R: Non serve implementare il controllo di flusso e nemmeno la gestione della congestione. Però è necessario gestire il riordinamento, perché i pacchetti possono arrivare fuori ordine facendo strade diverse, e la consegna affidabile, perché i pacchetti possono andare perduti per guasti e malfunzionamenti. Oltre ovviamente alla connessione tra applicazioni anziché tra nodi o interfacce.

2. Nello standard IEEE 802.15.7, uno dei canali fisici wireless più semplici è realizzato modulando un segnale ottico (prodotto da un LED) con On-Off Keying (cioè l'intensità luminosa può essere in due stati, alto-basso), ad una velocità di 200.000 stati al secondo. I dati grezzi sono codificati con un codice Manchester. Determinare il baud rate del canale fisico descritto.

   R: Nel codice Manchester, il simbolo base è costituito da una coppia consecutiva di stati, dove il bit 0 viene indicato con il passaggio da alto a basso e il bit 1 dal passaggio da basso ad alto. Quindi ogni simbolo viene trasmesso in due cicli di clock ottico. Il baud rate è quindi 100 kBaud.

3. Con riferimento alla situazione della domanda precedente, determinare il bit rate effettivo del canale, sapendo che viene utilizzato un codice di correzione in avanti (FEC) in cui vengono usati pacchetti di 15 simboli, di cui 11 sono di dati e 4 di parità. Si ignori l'overhead dovuto alla struttura dei frame.

   R: Dato che un simbolo codifica un solo bit, il bit rate è di 100 kb/s, e viene ulteriormente ridotto di un fattore 11/15 dalla FEC, quando si passa a considerare la parte utile per il frame. Il bit rate netto è quindi di 11/15 * 100 kb/s =73.3 kb/s

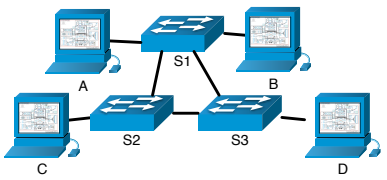
4. Una certa linea ha una probabilità di errore per bit $p = 10^{-6}$, con probabilità indipendenti. Ogni frame, lungo 1000 byte, contiene una FEC che permette al ricevitore di correggere fino a 2 bit errati. Qual è la probabilità Q che il frame debba essere scartato a causa di errori?

   R: La probabilità di eliminazione a causa di errori è $Q = P(n.errori > 2) = 1 - P(n.errori \leq 2) = 1 - (P(n.errori = 0) + P(n.errori = 1) + P(n.errori = 2)) = 1 - (q^n + n * p * q^{n-1} + n * (n-1) * p^2 * q^{n-2})$, ove $q = 1 - p$ e $n = 8000$ è il numero di bit in un frame. Sostituendo, viene $Q = 31,6 * 10^{-6}$.

5. In Bluetooth, il protocollo di accesso al mezzo è a *divisione di tempo*, dove il master può trasmettere negli slot pari, mentre gli slave negli slot dispari. Cosa garantisce questo metodo, rispetto al CSMA/CA del WiFi? E qual è un suo svantaggio?

   R: Pro: banda minima garantita, assenza di collisioni, semplicità (e quindi minore consumo) Cons: maggiore latenza, minore sfruttamento della banda (un nodo non può sfruttare mai più di metà canale, anche se gli altri non hanno niente da trasmettere).

6. La rete a lato è composta da switch ad autoapprendimento, S1 ha completato la fase di apprendimento mentre S2 e S3 sono appena stati resettati. L'host A invia un frame all'host D. Tale frame raggiunge D? Ci sono altri host che ricevono tale frame? In quante copie?



   R: S1 inoltra il frame a S3, correttamente, ma S3 non sa dove è collegato D, quindi lo inoltra su entrambe le porte. Da una di queste arriva a D, mentre dall'altra arriva a S2, il quale non conoscendo la posizione

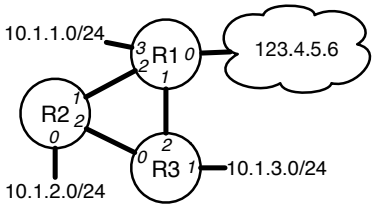
di D inoltra il frame sia a C sia a S1. A questo punto S1 aggiorna la sua tabella di inoltro, perché pensa che A abbia cambiato porta, e inoltra il frame allo switch S3, e così via. Quindi C e D ricevono molte copie dello stesso frame, finché S3 scopre dove è collegato D.

7. Nella rete 192.168.1.0/24 vengono ricavate due sottoreti, la 192.168.1.0/25 e la 192.168.1.128/27. Quali altre sottoreti e quanti indirizzi sono ancora disponibili?

   R: Rimangono disponibili tre reti $192.168.1.10100000_2/27 = 192.168.1.160/27$, $192.168.1.11000000_2/27 = 192.168.1.192/27$ e $192.168.1.11100000_2/27 = 192.168.1.224/27$. Ogni rete ha $2^5 = 32$ indirizzi, in totale 96 indirizzi—meno 6, se vogliamo togliere quelli non assegnabili.

   In realtà la seconda e terza rete possono essere unite nella $192.168.1.11000000_2/26 = 192.168.1.192/26$, che ha $2^6 = 64$. In totale sono sempre 96 indirizzi, ma quelli non assegnabili sono solo 4.

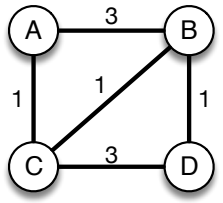
8. Nella rete a lato, si dia la tabella di inoltro del router R2, sapendo che l'indirizzo IP dell'interfaccia if2 di R1 è 192.168.1.2, e quello di if0 di R3 è 192.168.2.1.



   R:

Net/CIDR	if	next hop
10.1.2.0/24	if0	-
10.1.3.0/24	if2	192.168.2.1
/	if1	192.168.1.2

9. I router della figura a lato impiegano un algoritmo di instradamento basato sul vettore delle distanze. Si dia la tabella di instradamento di A (a) all'inizio, e (b) dopo che ha ricevuto il primo vettore da B (il quale non ha ancora ricevuto neussun vettore da nessun vicino).



   R: (a)

Dest.	dist	next hop
A	0	-
B	3	B
C	1	C

   (b)

Dest.	dist	next hop
A	0	-
B	3	B
C	1	C
D	4	B

10. Un'azienda usa gli indirizzi della rete 123.45.67.0/24 ed è un Autonomous System di tipo stub connesso ad un provider P. Ad un certo punto, decide di passare al provider Q. I provider utilizzano BGP per il routing interdominio. E' necessario che l'azienda cambi la numerazione della propria rete, o può continuare ad usare la rete già assegnata?

    R: Non è necessario cambiare la numerazione: lo speaker di P smette di annunciare la raggiungibilità della rete 123.45.67.0/24, e lo speaker di Q inizia ad annunciare la sua raggiungibilità. Le tabelle di instradamento si adeguano di corrispondenza.

11. Si vuole implementare una variante di UDP che garantisca la consegna in ordine dei datagrammi, ma non necessariamente affidabile: un datagramma viene consegnato solo se è successivo all'ultimo pacchetto consegnato, e datagrammi in ritardo vengono scartati. Quali informazione si deve aggiungere nell'intestazione, e come deve essere gestita dal ricevitore?

    R: Ci vuole un numero di sequenza in ogni datagramma, che viene incrementato ad ogni datagramma inviato. Il ricevitore mantiene il contatore dell'ultimo pacchetto consegnato, e consegna un datagramma solo se il suo numero di sequenza è strettamente maggiore di tale contatore.

12. A causa di un problema di trasmissione, il messaggio di ACK dal client al server alla fase di handshake di una connessione TCP va perduto. In che stato si trovano le due controparti? Il client deve ritrasmettere l'ACK prima di inviare un segmento con dati?

    R: Il client si trova nello stato ESTABLISHED, il server nello stato SYN_RCVD. Non è necessario reinviare l'ACK: praticamente il primo segmento dati dal client al server funge anche da ritrasmissione dell'ACK (avrà il bit opportuno attivo), e quindi fa transire il server nello stato ESTABLISHED.

13. Lo strato TCP di un host riceve un segmento con `SequenceNum=5000, Length=1500` e risponde con un segmento con `Acknowledge=4000`. Qual è il valore minimo di `AdvertisedWindow` riportato in tale segmento? (supponendo che l'applicazione non abbia consumato alcun dato nel frattempo)

R: Se il ricevitore dice di aspettare da 4000 in poi e il mittente ha inviato da 5000 a 6499, significa che ci sono dei dati in ritardo/perduti da 4000 a 4999. Quindi ci deve essere una finestra libera almeno da 4000 a 6499, altrimenti il mittente non avrebbe potuto inviare dati fino a quel punto. Quindi `AdvertisedWindow`=6500-4000=2500 (almeno).

14. Un router applica la politica RED ad una coda, con `Minthreshold`=10kB e `Maxthreshold`=20kB. La coda attualmente è piena a 9kB. Arrivano in rapida successione tre pacchetti, di rispettivamente 2kB, 3kB e 2kB. Qual è la probabilità che tutti e tre vengano accodati?

    R: Il primo pacchetto viene accodato sicuramente (quindi $P_1 = 1$, e la coda si allunga a 11kB. La probabilità che il secondo pacchetto sia scartato è $(11-10)/(20-10) = 1/10$, quindi $P_2 = 1-1/10 = 0,9$. Se il secondo pacchetto è stato accodato, la coda diventa 14kB. La probabilità che il terzo pacchetto sia scartato è $(14-10)/(20-10) = 4/10$, quindi $P_3 = 1-4/10 = 0,6$. La probabilità che tutti e tre i pacchetti vengano accodati è quindi $P = P_1P_2P_3 = 1*0,9*0,6 = 0,54 = 54\%$.

15. Si supponga che i voti degli esami vengano ancora registrati su registri cartacei, come si faceva fino ad una decina di anni fa. Si diano almeno due goal di sicurezza per tali registri, e si dica come si può implementare il relativi servizi di sicurezza.

    R: Confidenzialità: i voti devono essere leggibili solo da chi è autorizzato (docenti e amministrativi). Meccanismo: tenere il registro sotto chiave.

    Disponibilità: quando è necessario consultare il registro, deve essere disponibile. Meccanismo: la chiave deve essere accessibile a chi di dovere (docente e amministrativi). Deve essere disponibile anche per lo studente, per cui egli ha una copia dei suoi voti (libretto).

    Integrità e non ripudiabilità: non si può alterare i voti dopo averli scritti sul registro. Meccanismo: utilizzo di inchiostro non cancellabile e carta non alterabile (ad esempio si vede se una pagina è strappata), e firme di docente e studente su ogni statino.

16. Una serie di brevi messaggi $M_1, M_2, \ldots$ viene inviata al destinatario cifrati come segue: $C_i = M_i \oplus H(K, i)$ dove K è una chiave precondivisa e H è una funzione di hash (la cui lunghezza è superiore a quella di ogni singolo messaggio). Se il numero di sequenza i viene rappresentato con n bit, quale condizione bisogna porre sul numero massimo di messaggi trasmissibili?

    R: Non oltre 2^n, perché dopo l'indice torna a 0 e a quel punto il keystrem pseudorandom generato dalla hash si ripete, e quindi si può fare il solito attacco.

17. Si consideri la variante del Diffie-Hellman a lato, dove y_A, y_B sono le mezze chiavi pubbliche del protocollo, H è una funzione di hash e K_m è un segreto precondiviso (chiave master). Questo protocollo è vulnerabile all'attacco "man in the middle"? Perché?

    1. $A \to B : y_A$
    2. $B \to A : y_B, H(K_m, y_A, y_B)$

    R: Non si riesce a sferrare un vero attacco MITM, perché al passo 2 il messaggio di B è autenticato dalla hash con chiave. In effetti, B non ha nessuna garanzia di comunicare con A, ma dopo il passo 2 A ha la garanzia di comunicare con B. Quindi un attaccante potrebbe farsi passare per A presso B, ma non può farsi passare per B presso A.

18. Un certo sistema utilizza una variante semplificata di Kerberos in cui il service ticket contiene solo le seguenti informazioni: (C, S, K_{C-S}), dove C, S sono gli identificativi del client e del server e K_{C-S} è una chiave simmetrica di sessione. Che conseguenze ha questa semplificazione sull'utilizzo del ticket?

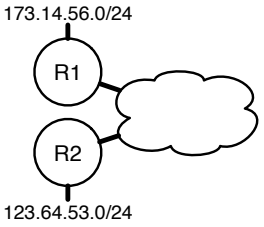
    R: Le informazioni che mancano sono il timestamp di inizio durata e lo span di vita del ticket. Questo significa che il ticket non ha scadenza: può essere usato finché si vuole. L'unico modo per limitarne l'utilizzo, quindi, è avere un modo per ritirare le chiavi di sessione (ma non è standard di Kerberos).

19. Nel protocollo a lato si completi il passo 3 in modo da garantire la non ripudiabilità e la puntualità di M, sapendo che A ha una chiave privata PR_A (la cui parte pubblica è nota a B), T è un timestamp generato da B, e si può usare una funzioni di hash.

    1. $A \to B : M$
    2. $B \to A : T$
    3. $A \to B$:?

    R: 3. $A \to B : E_{PR_A}(H(M,T))$. Oppure: 3. $A \to B : E_{PR_A}(H(M), T)$

20. Si vuole mettere in sicurezza le comunicazioni tra gli host di due reti connesse via Internet, come a lato. Ci sono due possibilità: a) gli host delle due reti comunicano direttamente con IPsec ESP in modalità trasporto; b) gli host usano normale IP, ma i due router R1, R2 comunicano con IPsec ESP in modalità tunnel. Quale di queste due possibilità garantisce una maggiore confidenzialità dei dati? e dei metadati? Quale è la più semplice da configurare e gestire da parte dell'amministratore di rete?



R: Con la modalità trasporto, i dati sono protetti end-to-end, quindi anche nei router e nelle reti locali, per cui la loro confidenzialità è maggiore. Però i metadati (ad esempio gli indirizzi IP mittente e destinatario) sono in chiaro lungo tutto il percorso, per cui non sono confidenziali.

Con la modalità tunnel, i dati e i metadati sono protetti da router a router, ma sono in chiaro nelle due reti locali e nei router. Perciò con questa modalità i dati sono meno sicuri ma i metadati sono più sicuri.

Per quanto riguarda la complessità di gestione, è più semplice la modalità tunnel, perché richiede la configurazione dei due soli router, e non di ogni nodo delle due reti.