DMIF, Università degli Studi di Udine  II appello A.A. 2017-18 — 19 febbraio 2018

Esame di **Reti di Calcolatori**

Soluzione

1. Perché una rete a commutazione di circuito permette di garantire una qualità di servizio (ad esempio una banda minima garantita), mentre ciò è più difficile in una rete a commutazione di pacchetto? Quale delle due strategie permette un migliore sfruttamento dei canali?

   R: Perché durante la creazione del circuito si possono allocare in ogni router le risorse richieste per garantire la qualità di servizio voluta. La commutazione di pacchetto permette un migliore sfruttamento, perché non c'è una allocazione statica delle risorse (che poi magari non vengono usate), ma c'è un migliore multiplexing delle risorse e si può scegliere il percorso migliore pacchetto per pacchetto.

2. Lo standard Ethernet 400GBASE-LR8 supporta 400Gbit/s su una singola fibra ottica, utilizzando segnali ottici generati ad 8 diverse lunghezze d'onda ciascuna realizzante un canale indipendente di trasmissione, separato al ricevitore da un demultiplexer. I dati sono modulati con un Pulse Amplitude Modulation 4 (PAM4), cioè ad ogni baud corrispondono 4 simboli possibili diversi. I dati trasmessi sono organizzati in frames, ognuno tipicamente di 1500 byte di dati, 30 byte di intestazione e 4 byte di controllo (CRC32).

   Determinare il baud rate per ogni canale (lunghezza d'onda) necessario a realizzare una trasmissione DATI di 400 Gbit/s complessivi.

   R: Il rapporto bitrate / bitrate dati è lo stesso che con i byte, quindi 1534/1500, per cui è necessario un bit rate complessivo di 400Gbit/s * 1534/1500 = 409.1 Gbit/s. Per ogni lunghezza d'onda si deve avere quindi un bit rate 409.1 Gbit/s / 8 = 51.13 Gbit/s. Poiché l'encoding è un PAM4, si hanno 2 bit per baud e quindi il baud rate per ogni canale è 25.56 GBaud.

3. Per la linea descritta nell'esercizio precedente, determinare il rapporto segnale/rumore minimo necessario per la trasmissione senza errori (rilevando un eventuale errore nel frame, ma trascurando il traffico causato dal reinvio).

   R: 25.56 GBaud corrispondono ad una larghezza di banda di 25.56/2=12.78 GHz. Dal teorema SH abbiamo per ciascun canale: $51.13 Gbit/s \leq 12.78 GHz \log_2(1+SNR)$. Risolvendo, si ottiene $SNR \geq 15$.

4. Lo standard Fast Ethernet (100BASE-TX) trasmette bit sul doppino a 100 Mb/s. Ricordando che ogni frame ha un preambolo di 8 byte, una intestazione di 14 byte e un FCS di 4 byte, e un interframe gap di 0,96μs, qual è la massima velocità netta (in Mb/s) ottenibile per dei payload di 1500 byte?

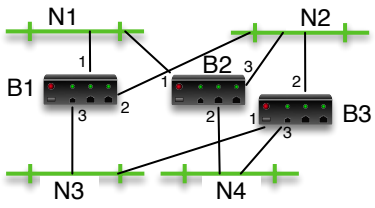
   R: Il gap di 0.96μs corrisponde quindi a $0.96 * 10^{-6} s * 100 * 10^6 b/s = 96b = 12$ byte. Quindi lo spazio occupato da un frame complessivamente è $8 + 14 + 1500 + 4 + 12 = 1538$ byte = 123,04 μs. La velocità massima è quindi $100 * 1500/1538 = 97,53 Mb/s$

5. Un certo protocollo utilizza l'algoritmo CRC con polinomio generatore $C(x) = x^3 + 1$. Si calcoli il CRC per la sequenza di bit 110011.

   R: Si fa la solita divisione tra polinomi, per cui viene CRC=101 (in binario).

```
110011 000 | 1001
-----------+-----
01011      |
 00101 0   |
   001 100 |
     0 101 |
```

6. Una rete è composta da quattro segmenti collegati da tre bridge, come in figura, i cui identificatori sono rispettivamente: B1: 8F7A; B2: 63D2; B3: A4C3. Le varie porte sono numerate come in figura. Si dica qual è il root bridge e quali bridge sono eventualmente inattivi, dopo l'esecuzione dell'algoritmo di spanning tree.

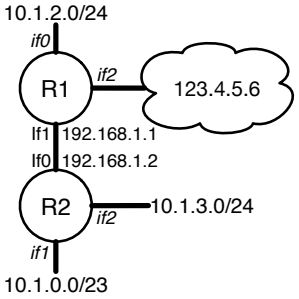


R: Il root bridge è quello con ID più basso, quindi B2, che quindi serve direttamente le reti N1, N2, N4. Per quanto riguarda N3, B1 e B3 sono alla stessa distanza dal root bridge, ma la porta designata per la rete N3 è la 3 di B1, perché B1 ha un id minore. Quindi B3 non è necessario e si disattiva.

7. Un provider offre la connessione a Internet a tre clienti che necessitano rispettivamente di 50, 100 e 300 indirizzi. Ad ogni cliente viene assegnata la minima sottorete sufficiente a coprire la sua necessità. Complessivamente, quant'è in percentuale l'utilizzo dello spazio di indirizzamento allocato ai tre clienti?

R: Al primo cliente basta una rete /26, che ha 64 indirizzi; al secondo viene assegnata una /25, che ha 128 indirizzi; al terzo viene assegnta una /23, che ha 512 indirizzi. Complessivamente sono impegnati 64+128+512=704 indirizzi, a fronte dei 50+100+300 = 450 richiesti, quindi l'utilizzo è 64%.

8. Si consideri la rete a lato, i cui router hanno le tabelle di inoltro qui sotto riportate. Cosa succede ad un pacchetto indirizzato a 10.1.1.10, inviato dall'esterno della rete?



R1:

Net/CIDR	if	next hop
10.1.2.0/24	if0	-
10.1.0.0/22	if1	192.168.1.2
/	if2	123.4.5.6

R2:

Net/CIDR	if	next hop
10.1.3.0/24	if2	-
10.1.0.0/24	if1	-
/	if0	192.168.1.1

R: Il pacchetto viene inoltrato da R1 a R2, che applica la regola default e quindi lo inoltra a R1, che lo inoltra di nuovo a R2, ecc., finché il TTL non scende a 0 e viene scartato.

9. Negli algoritmi di instradamento basati sullo stato dei collegamenti, come OSPF, come vengono diffusi i pacchetti LSP? Quando un router riceve un pacchetto LSP da un altro router, come fa a capire se è obsoleto e quindi da ignorare?

R: In flooding. Ogni pacchetto LSP porta l'identificativo del router che l'ha generato, e un numero progressivo di generazione. Ogni router tiene traccia del pacchetto più recente che ha visto fino a quel momento da ogni router, e quando arriva uno nuovo ne tiene conto solo se il suo numero progressivo è maggiore del numero che ha attualmente in memoria.

10. Una certa applicazione viene eseguita su una piattaforma le cui interfacce sono dotate di indirizzi IPv6 ma non IPv4. È possibile che tale applicazione stabilisca una connessione con un server in attesa di connessioni su una socket associata ad un indirizzo IPv4?

R: Sì, ma solo se c'è un router intermedio che traduce tra IPv4 e IPv6, tipo NAT ma sostituendo l'intere intestazioni. Le tecniche dual-stack e tunneling in questo caso non si applicano.

11. a) Quale protocollo di trasporto può essere usato per la comunicazione multicast su IP? b) In Java, prima di inviare o ricevere pacchetti multicast su una socket `s` per un certo gruppo `g`, è necessario chiamare il metodo `s.joinGroup(g)`. Che effetto ha tale chiamata, a livello di rete?

R: a) Solo UDP. b) Invia il pacchetti IGMP di join al gruppo indicato.

12. Un calcolatore sta ricevendo un flusso dati via TCP, a circa 10 kB/s, attraverso una interfaccia Ethernet, il cui cavo viene improvvisamente staccato e ricollegato dopo un secondo. La connessione TCP viene mantenuta o no? Se la controparte che sta inviando i dati adotta la ritrasmissione veloce, come reagisce quando viene ricollegato il cavo?

R: Sì, un secondo di scollegamento non è sufficiente per far cadere la connessione; rientra nei normali ritardi di consegna dei pacchetti. Però la controparte si accorge che un po' di pacchetti sono andati

perduti, perché quando il cavo viene ricollegato gli arriveranno un po' di ack duplicati, e riprenderà a spedire dai pacchetti che sono andati perduti.

13. Lo strato TCP di un host, appena entrato nello stato ESTABLISHED e con `NextByteExpected`=12000, riceve i seguenti segmenti, in questo ordine: `SequenceNum`=15600, `Length`=200; `SequenceNum`=12000, `Length`=1200. Se il buffer è di 4096 byte e l'applicazione non ha consumato ancora niente, quale valore di `Acknowledge` e `AdvertisedWindow` vengono inviati dopo il secondo segmento?

    R: `NextByteExpected`=13200 (perché c'è un buco), quindi `Acknowledge`=13200, `AdvertisedWindow`=4096-(13200-12000)=2896.

14. Un router sta servendo tre flussi di pacchetti, i cui payload pesano rispettivamente 500, 800 e 1500 byte. Ogni volta che deve inviare un pacchetto, il router sceglie a caso un pacchetto tra i tre flussi con probabilità 1/2, 1/4 e 1/4, rispettivamente. Quanto è l'indice di equità di Jain?

    R: $x_1 = 500 * 1/2 = 250$; $x_2 = 800 * 1/4 = 200$; $x_3 = 1500 * 1/4 = 375$. $f(x_1, x_2, x_3) = \frac{(x_1+x_2+x_3)^2}{3(x_1^2+x_2^2+x_3^2)} = \frac{(250+200+375)^2}{3(250^2+200^2+375^2)} = 0.93$.

15. Per ognuno dei seguenti protocolli di sicurezza si dica a quale strato dello stack OSI si colloca. a) WPA2; b) SSL Record; c) IKE.

    R: a) 2 (datalink); b) 4 (trasporto), ma meglio ancora 6 (presentazione); c) 7 (è un protocollo di scambio chiave che funzione a livello applicazione, anche se agisce sul SADB che si usa a livello 3).

16. Un certo sistema cifra i suoi dati con AES-128, la cui chiave è ottenuta calcolando la hash MD5 di una parola composta da 6 caratteri alfabetici (26 maiuscoli + 26 minuscoli) seguita da tre cifre. Si dica il numero medio di tentativi necessari per scoprire la password con un attacco brute force.

    R: La hash non aumenta la complessità del sistema: il vero spazio delle chiavi è quello delle possibili parole alfanumeriche. In questo caso sono $52^6 * 1000 = 1,977 * 10^{13}$, di cui in media si devono tentare circa la metà, ovvero $9,885 * 10^{12}$.

17. Nel protocollo a lato, K_S è una chiave simmetrica di sessione inventata da A, PU_B è la chiave pubblica di B e N una nonce. a) Si completi il messaggio al passo 3, in modo da garantire confidenzialità e puntualità di M. b) B è certo dell'origine del messaggio M (ovvero, è autentico)?

    1. $A \to B : E_{K_S}(M)$
    2. $B \to A : N$
    3. $A \to B : E_{PU_B}(??)$

    R: a) $A \to B : E_{PU_B}(N, K_S)$. b) No: B non può sapere da chi viene il messaggio: può essere stato inviato da chiunque.

18. Nel protocollo a lato, K_A e K_B sono chiavi master precondivise tra A e C, e B e C, rispettivamente; K è una chiave di sessione generata da C, e N una nonce generata da B. a) A è autenticato per B? b) B è autenticato per A?

    1. $A \to C : E_{K_A}(B)$
    2. $C \to B : E_{K_B}(A, K, E_{K_A}(K))$
    3. $B \to A : E_{K_A}(K), N$
    4. $A \to B : E_K(N)$

    R: a) A è autenticato perché risponde alla challenge di cifrare N con una chiave K decifrabile solo da chi conosce K_A. b) No, B non è autenticato, perché esiste un attacco: un attaccante E può usare una vecchia chiave K' che si è fatta dare da C durante una sessione precedente, per farsi passare per B:

    1. $A \to EE_{K_A}(B)$
    3. $E \to A : E_{K_A}(K'), N$
    4. $A \to E : E_{K'}(N)$

19. Come è noto, un *mailing list server* riceve mail su un certo indirizzo e le reinvia a tutti gli utenti iscritti alla lista, senza che gli utenti abbiano bisogno di conoscere le mail degli iscritti. Se un utente invia a tale indirizzo una mail PGP cifrata e firmata, la mail è a) confidenziale rispetto al server? b) autentico per ognuno dei destinatari?

    R: a) no, perché l'utente deve usare la chiave pubblica del server, il quale potrà (dovrà) decifrare il messaggio per reinviarlo a tutti gli utenti. b) sì, la firma può essere verificata da tutti gli utenti indipendentemente.

20. Un client apre una connessione TLS con un server, con scambio chiave RSA. Si dica per ognuna delle seguenti affermazioni se è vera o falsa. a) Il client è autenticato per il server; b) il server è autenticato per il client; c) il server possiede un certificato X.509 valido; d) la porta del server è cifrata.

    R: a) no; b) si; c) si; d) no.