LEZIONE 1

Con la commutazione di pacchetto
a) Ciascun flusso di dati è suddiviso in pacchetti gestiti dai nodi della rete con la tecnica nota come "Store and Forward"
b) Ciascun flusso e' suddiviso in pacchetti recanti tutti il medesimo identificativo di circuito virtuale
c) Ciascun flusso di dati e' suddiviso in pacchetti aventi tutti la medesima dimensione
d) Ciascun flusso di dati è sempre instradato lungo il medesimo percorso all'interno della rete
e) Nessuna delle precedenti risposte è esatta

R: a (RC1_L01 pag. 7 slide 14)

Quante delle seguenti affermazioni sono false, con riferimento alle reti "a datagrammi"?
Affermazione 1: Ogni pacchetto e' sempre costituito da un'intestazione (header) e dal payload
Affermazione 2: La sorgente decide quale strada i pacchetti dovranno percorrere
Affermazione 3: I nodi intermedi si occupano dell'instradamento di ogni singolo pacchetto
Affermazione 4: Ogni nodo memorizza i pacchetti in ingresso, per poi instradarli verso il nodo successivo (store & forward)

affermazione 2

La commutazione di pacchetto
a) Adotta tecniche di multiplexing statistico per rendere efficiente la trasmissione
b) è una tecnica appropriata per trasmissioni di tipo real-time
c) adotta circuiti fisici o virtuali
d) nessuna delle precedenti affermazioni è vera

R: a (RC1_L01 pag. 8 slide 15)

Nelle reti a commutazione di pacchetto, il tempo di trasmissione di un pacchetto su un link
a) è proporzionale alla lunghezza della linea
b) è il tempo necessario per effettuare il controllo degli errori dovuti alla trasmissione
c) è il rapporto tra la lunghezza del pacchetto e la velocità del link
d) è il tempo necessario per far transitare il pacchetto dal livello rete al livello data-link
e) E' la somma di tutti i contributi citati nelle precedenti risposte

R: c (RC1_L01 pag. 9 slide 17)

Quante delle seguenti affermazioni sono vere, con riferimento ad una rete a circuiti virtuali?
Affermazione 1: comporta un overhead per la creazione del circuito virtuale, ma, rispetto ad una rete a datagrammi, risulta meno sensibile agli effetti dovuti a guasti ai nodi
Affermazione 2: comporta un overhead per la creazione del circuito virtuale e, rispetto ad una rete a datagrammi, aumenta la quantità di informazioni di stato da mantenere
Affermazione 3: comporta un overhead per la creazione del circuito virtuale, ma, rispetto ad una rete a datagrammi, semplifica le operazioni di instradamento dei dati
Affermazione 4: è necessariamente realizzata in tecnologia ATM
a) Nessuna affermazione è vera
b) Due affermazioni sono vere
c) Tre affermazioni sono vere
d) Una sola affermazione è vera

R: b (Aff. 2 e Aff. 3) (RC1_L01 pag. 10 slide 20)

LEZIONE 2

Con riferimento ad un un modello protocollare a livelli, quale delle seguenti affermazioni è falsa?
a) Ciascun livello offre servizi ai livelli inferiori
b) Ciascun livello è responsabile di un sottoinsieme definito e limitato di compiti
c) Una entità di livello n comunica secondo un protocollo con una entità di pari livello
d) Ciascuno livello fa affidamento sui servizi forniti dal livello immediatamente inferiore
e) La organizzazione a livelli (stratificazione) è una tecnica utilizzata per gestire la complessità e la eterogeneità delle reti

R: a (RC1_L02 pag. 2 slide 4)

Nelle reti di calcolatori, un'interfaccia
a) definisce i servizi offerti dal livello (n-1) al livello n
b) regola la comunicazione tra entità di pari livello esistenti in due dispositivi della rete tra loro comunicanti
c) definisce i servizi offerti dal livello n al livello (n-1)
d) definisce i servizi offerti dallo strato rete allo strato applicazione

R: a (RC1_L02 pag. 2 slide 4)

In un modello a strati
a) Lo strato n-esimo di un dispositivo comunica con lo strato n-esimo di un'altra entità secondo un protocollo assegnato
b) Lo strato n-esimo di un dispositivo comunica con lo strato n-esimo di un'altra entità secondo un'interfaccia ben precisa
c) Lo strato n-esimo di un dispositivo comunica con lo strato (n-1)-esimo di un'altra entità-dispositivo secondo un'interfaccia ben precisa
d) Lo strato n-esimo di un dispositivo comunica con lo strato (n-1)-esimo del medesimo dispositivo secondo un protocollo assegnato
e) Nessuna delle precedenti risposte è esatta

R: a (RC1_L02.pdf pag. 3 slide 6)

Il livello sessione
a) è il livello 6 dello stack ISO/OSI
b) si occupa di sincronizzare lo scambio di dati tra due programmi applicativi che utilizzano il protocollo di trasporto TCP
c) regola gli aspetti sintattici delle informazioni da trasferire
d) nessuna delle precedenti risposte

-risposta D

LEZIONE 4-5

Il protocollo HTTP
a) è un protocollo stateful, in quanto sia il server che il client mantengono informazioni relative ai messaggi precedentemente scambiati
b) nella versione persistente è un protocollo stateful, in quanto memorizza, dal lato del server, informazioni relative ai client
c) è un protocollo stateless, in quanto né il server né il client mantengono informazioni relative ai messaggi precedentemente scambiati
d) è un protocollo stateless, a patto che non si adoperino tecniche di caching delle risorse

R: c (RC1_L04_L05 pag. 6 slide 12)

Il protocollo HTTP è stateless (senza stato)
a) mai, lo diventa quando si utilizzano i cookie
b) sempre
c) mai
d) solo nella modalità persistente
e) in funzione della versione del server utilizzato

R: b (RC1_L04_L05 pag. 6 slide 12)

Come fa un Client a conoscere la fine di una frame HTTP
a) Col messaggio <\HTML>
b) Perché la connessione TCP viene interrotta
c) Con una riga vuota
d) Dal campo contenent lenght

R: c (RC1_L04_L05 pag. 11 slide 21)

Quante connessioni TCP vengono aperte, con HTTP in versione non persistente, nel caso di trasferimento di un contenuto web costituito da una pagina base HTML, 6 immagini gif e 5 immagini jpeg ?
NB: Si supponga che nella pagina base sia presente un "link" ad un'altra pagina HTML, memorizzata in un server differente...
a) 12
b) 11
c) 11 non persistenti (per le immagini) ed una persistente (per la pagina base)
d) 13, così suddivise: 12 per la pagina base più le immagini; un'ulteriore connessione per il riferimento ipertestuale alla risorsa esterna
e) 10
f) Nessuna delle precedenti risposte è esatta

R: a (RC1_L04_L05 pag. 13 slide 25)

Quante connessioni TCP vengono aperte, con HTTP in versione persistente, nel caso di trasferimento di un contenuto web costituito da una pagina base HTML, 6 immagini gif e 5 immagini jpeg?
NB: Si supponga che nella pagina base sia presente un "link" ad un'altra pagina HTML, memorizzata in un server differente...
a) 13, così suddivise: 12 per la pagina base più le immagini; un'ulteriore connessione per il riferimento ipertestuale alla risorsa esterna
b) 10
c) 11
d) 11 non persistenti (per le immagini) ed una persistente (per la pagina base)
e) 12
f) Nessuna delle precedenti risposte è esatta

R: f (RC1_L04_L05 pag. 13 slide 25)

Come si realizza il cosiddetto GET condizionato (Conditional GET)?
a) Tramite il metodo POST di HTTP
b) Utilizzando un apposito messaggio GET-IF messo a disposizione dal protocollo HTTP

c) Tramite il messaggio GET standard, facendo uso di un’apposita linea di intestazione opzionale (If-modified-since)
d) Eseguendo la richiesta solo nel caso siano passati più di dieci minuti dall’ultimo aggiornamento

R: c (RC1_L04_L05 pag.14 slide 27)

Quante delle seguenti affermazioni sono vere, con riferimento al metodo HTTP HEAD?
Affermazione 1: E' simile al metodo GET, ma prevede, da parte del server, solo l'invio degli header relativi alla risposta, senza alcun payload
Affermazione 2: Può essere usato per verificare l'accessibilità di una risorsa web
Affermazione 3: Serve per inviare al server dati contenuti all'interno di una form HTML
Affermazione 4: Può essere utilizzato per verificare se l'header (HEAD) della richiesta è privo di errori
a) Una affermazione e' vera
b) Nessuna affermazione e' vera
c) Due affermazioni sono vere
d) Tre affermazioni sono vere
e) Tutte le affermazioni sono vere

R: c (Aff. 1 & Aff. 2) (RC1_L04_L05 pag. 15 slide 29)

In un messaggio HTTP l'header "Date" rappresenta
a) data ed ora dell'ultima modifica dell'oggetto trasmesso
b) data ed ora della trasmissione del messaggio
c) data ed ora della creazione dell'oggetto trasmesso
d) data ed ora dell'ultimo riavvio del server web
e) nessuna delle precedenti

R: b (RC1_L04_L05 pag. 17 slide 34)

Con riferimento al protocollo HTTP, indicare quale delle seguenti affermazioni è VERA.
a) è un protocollo testuale adoperato per descrivere la collocazione di una particolare risorsa nella rete, al fine di nascondere il corrispondente indirizzo numerico
b) è un protocollo del livello rete
c) I comandi del protocollo sono identificati da un codice numerico di tre cifre (ad es. 200) in cui la prima cifra indica il tipo di comando e le rimanenti due le opzioni associate a quest'ultimo
d) è un protocollo testuale nel quale i messaggi di risposta contengono un codice numerico di tre cifre detto status code

R: d (RC1_L04_L05 pag. 18 slide 36)

Dove si inseriscono le informazioni relative ai cookie scambiati tra client e server HTTP?
a) Nell’header della richiesta
b) Nell’header della risposta
c) Sia nell’header della risposta (inserito dal server), che in quello della richiesta (inserito dal client)
d) In un file nascosto, automaticamente generato dal browser del client

R: c

LEZIONE 6

Perché si dice che nel protocollo FTP le informazioni di controllo sono "out-of-band"?
a) Perché, a differenza del protocollo HTTP, con FTP è necessario che il client sia autenticato ("controllato") dal server, prima di iniziare il trasferimento. Tale autenticazione avviene con ulteriori protocolli, che richiedono la codifica di nome utente e password.
b) Perché prima di inviare i dati bisogna stabilire una connessione tra client e server, che viene chiusa non appena terminata la fase di autenticazione; dopodiché si procede al trasferimento dei dati su un'altra connessione TCP (che usa tipicamente la porta 20)
c) Perché tra client e server si aprono due connessioni TCP parallele: una (sulla porta 21) per lo scambio di informazioni di controllo; l'altra (sulla porta 20) per lo scambio dei dati
d) Perché tra client e server si aprono due connessioni, una TCP e l'altra UDP: la prima (sulla porta 21) per lo scambio di informazioni di controllo; la seconda (sulla porta 20) per lo scambio dei dati
e) Nessuna delle altre risposte è vera

R: c (RC1_L06 pag. 3 slide 6)

Quante delle seguenti affermazioni sono vere, in relazione al tipo di informazioni di controllo gestite dal protocollo FTP?
Affermazione 1: Informazioni dette out-of-band, perché spedite su di un canale UDP, piuttosto che sul canale TCP associato ai dati
Affermazione 2: Informazioni dette in-band, perché spedite sul medesimo canale utilizzato per la trasmissione dei dati
Affermazione 3: Informazioni out-of-band nel caso di connessioni persistenti, in-band nel caso di connessioni non persistenti
Affermazione 4: Informazioni crittografate, appositamente concepite per salvaguardare la privacy degli utenti della rete
a) Tre affermazioni sono vere
b) Due affermazioni sono vere
c) Una affermazione è vera
d) Nessuna affermazione è vera
e) Tutte le affermazioni sono vere

R: d (RC1_L06 pag. 3 slide 6)

Si supponga di voler scaricare 4 files da un server FTP (nel corso di una stessa sessione): quante connessioni TCP saranno complessivamente instaurate tra client e server?
a) 2
b) 5
c) 4
d) 3
e) 1

R: b

SMTP
a)È un protocollo di tipo pull (il server di posta del mittente “preleva” il messaggio dal server di posta del destinatario)
b)È un protocollo sia di tipo push che di tipo pull, a seconda dello scenario di funzionamento
c)È un protocollo di tipo push (il server di posta del mittente “spinge” il messaggio verso il server di posta del destinatario)
d)Usa lo stesso paradigma di interazione di http

R: c (RC1_L06 pag. 9 slide 17)

A cosa servono le estensioni MIME (Multipurpose Internet Mail Extensions)?
a) Ad utilizzare la posta elettronica anche per altri fini ("multipurpose"), quali l'Instant Messaging ed il Peer-To-Peer
b) A definire nuovi campi dell'header di protocolli quali HTTP e SMTP, volti a descrivere in maniera appropriata il contenuto (ad esempio, tipo e codifica impiegata) di un messaggio
c) Ad inviare tramite posta elettronica informazioni aggiuntive riguardanti l'agente della posta posseduto dal client SMTP

d) A definire nuovi campi dell'header del protocollo SMTP, volti esclusivamente a gestire i cosiddetti messaggi "multiparte" (contenenti, ad esempio, testo ed immagini)
e) Nessuna delle precedenti

R: d (RC1_L06 pag. 13 slide 25)

Il protocollo POP3
a) Usato in combinazione con il protocollo IMAP, consente di gestire cartelle di posta elettronica
b) Permette il collegamento al server di posta del mittente di un'email, per prelevare i messaggi inviati da quest'ultimo
c) Permette il collegamento al proprio server di posta per accedere alla posta in arrivo
d) Serve per gestire il servizio delle news

R: c

LEZIONE 7

Quale delle seguenti operazioni può essere svolta agendo sul servizio di risoluzione dei nomi di dominio (DNS).
a) Redirezione del numero di porto utilizzato da un client all'atto dell'accesso ad un servizio attestato su una porta ben nota (well-known port).
b) Redirezione di un web client verso una nuova URL, nel caso in cui una richiesta HTTP fornisca il codice di errore 301 (Moved Permanently).
c) Bilanciamento su più server differenti del carico prodotto dalla fruizione di un servizio.
d) Modifica delle tabelle di instradamento conseguentemente alla migrazione di un servizio tra 2 differenti server.
e) Nessuna delle precedenti

R: c (RC1_L07 pag. 3 slide 6)

Cosa si intende per "alias" del nome di un host di Internet?
a) Si usa per assegnare lo stesso nome a più host di Internet, così da bilanciare, tramite DNS, il carico nell'accesso ad una particolare risorsa(che risulterà replicata su tutti gli host in oggetto)
b) Ad un'interfaccia di rete di un host si possono assegnare più indirizzi IP virtuali
c) Ad una macchina con un nome complicato può essere associato un "soprannome" più piccolo e semplice da ricordare. Tale servizio è a carico del DNS
d) Ad un server di posta si può associare il nome di un dominio, per facilitare la memorizzazione dell'indirizzo di posta elettronica degli utenti di quel dominio. Di ciò se ne occupa il DNS
e) Nessuna delle precedenti

R: c (RC1_L07 pag. 3 slide 6)

Quale tipo di DNS server viene contattato da un host per la risoluzione di un indirizzo simbolico? (si suppongano tutte le cache vuote)
a) un local name server
b) l'authoritative (assoluto) name server del dominio di cui si vuole risolvere l'indirizzo
c) un root name server
d) Nessuno. Un host non inoltra in nessun caso richieste dirette di risoluzione degli indirizzi

R: a (RC1_L07 pag. 5 slide 10)

Quale delle seguenti affermazioni è vera?
a) Il server dei nomi locale tipicamente è "vicino" (ad esempio situato sulla stessa LAN) all'host client
b) Il server dei nomi locale si comporta da server per la risoluzione degli indirizzi nei confronti di un server dei nomi radice
c) Un server dei nomi assoluto si trova ad un livello gerarchico superiore rispetto ad un server dei nomi radice
d) Un host deve essere registrato presso tutti i server dei nomi assoluti

R: a

Riferendosi al formato dei messaggi di query e risposta di tipo DNS, scegliere l'affermazione corretta:
a) A differenza dei messaggi di risposta, nei messaggi di query non e' presente il campo "numero di RR di risposta"
b) A differenza dei messaggi di query, nei messaggi di risposta non e' presente il campo "numero di RR addizionali"
c) A differenza dei messaggi di risposta, nei messaggi di query non e' presente il campo "Competenza"
d) A differenza dei messaggi di risposta, nei messaggi di query non e' presente il campo "numero di RR autorevoli"
e) Il formato dei messaggi e' lo stesso

R: e (RC1_L07 pag. 10 slide 20)

LEZIONE 8

Qual è il vantaggio che si ottiene in seguito alla messa in opera di una rete per la distribuzione dei contenuti (Content Distribution Network - CDN)?
a) l'accesso da parte dei client a contenuti sempre estremamente aggiornati
b) la disponibilità di una maggiore varietà di contenuti
c) una maggiore velocità di accesso ai contenuti da parte dei client
d) una minor costo di produzione dei contenuti da parte dei loro fornitori

R: c (RC1_L08 pag. 2)

Una Content Delivery Network (CDN) ha l'obiettivo di
a) minimizzare lo spazio per la memorizzazione dei contenuti
b) facilitare l'aggiornamento dei contenuti da parte del provider
c) minimizzare il tempo di accesso alle risorse per l'utente finale
d) minimizzare la probabilità di accedere ad un contenuto non aggiornato
e) Nessuna delle precedenti risposte è esatta
R: c

R: c

Cosa si intende per Content Distribution Network (CDN)?
a) una rete costituita da un banco di server che offrono servizi l'uno all'altro
b) una rete costituita da un banco di server, tutti in possesso degli stessi contenuti e dislocati in Internet in modo tale da aumentare l'efficienza nell'accesso da parte dei client
c) una rete costituita da entità pari che si scambiano tra loro contenuti
d) una rete di server che inviano contenuti ai client in modalità push

R: b (RC1_L08 pag. 2)

In un sistema peer-to-peer con directory centralizzata
a) Ogni peer si registra presso un server centralizzato e lo informa riguardo i contenuti che intende mettere in condivisione. Le richieste di contenuti vengono, poi, indirizzate a tutti gli altri peer disponibili (la lista di tali peer è reperibile presso il server centrale).
b) Ogni peer si registra presso un server centralizzato e lo informa riguardo i contenuti che intende mettere in condivisione. Anche le richieste di contenuti vengono indirizzate a tale server, il quale risponde con la lista dei potenziali nodi da contattare per il trasferimento di file in modalità peer-to-peer.
c) Ogni peer informa tutti gli altri nodi della sua presenza. Le richieste di contenuti vengono, invece, indirizzate ad un server centrale presso cui sono state preventivamente pubblicate le informazioni relative a tutti i contenuti disponibili.
d) Esiste un server centrale, che si occupa di gestire la rete overlay mediante la tecnica dell'allagamento (ogni peer invia le proprie richieste al server centrale, il quale le inoltra a tutti gli altri nodi presenti nella rete).

R: b (RC1_L08_parte2 pag. 5 slide 9)

Quante delle seguenti affermazioni sono vere?
Affermazione 1: In una rete peer-to-peer non esiste in nessun caso una directory centralizzata f
Affermazione 2: In una rete peer-to-peer si costruisce sempre un'overlay network di tipo gerarchico f
Affermazione 3: In una rete peer-to-peer non esistono né client, né server f
Affermazione 4: In una rete peer-to-peer è possibile realizzare un'overlay network di tipo paritetico, in cui v l'instradamento delle richieste può avvenire tramite flooding
a) una sola affermazione è vera
b) due affermazioni sono vere
c) tutte le affermazioni sono vere
d) tre affermazioni sono vere
e) Tutte le affermazioni sono vere

R: a (Aff. 4) (RC1_L08_parte2 pag. 6)

LEZIONE 9

Quante delle seguenti affermazioni sono vere
Affermazione 1: Nelle reti a circuiti virtuali ogni pacchetto contiene il numero del circuito virtuale v
Affermazione 2: Nelle reti a circuiti virtuali il circuito virtuale è sempre stabilito prima della trasmissione dei dati v
Affermazione 3: Nelle reti a circuiti virtuali i nodi devono conservare informazioni relative ai circuiti che li attraversano v
Affermazione 4: Nelle reti a circuiti virtuali pacchetti tra la stessa coppia sorgente-destinazione possono seguire percorsi differenti f
a) Nessuna affermazione è vera
b) Due affermazioni sono vere
c) Tutte le affermazioni sono vere
d) Tre affermazioni sono vere
e) Una sola affermazione è vera

R: d

Il campo checksum nella intestazione del pacchetto IP
a) è calcolato sul payload del pacchetto IP
b) è controllato da ogni router che inoltra il pacchetto
c) è calcolato dall'host destinatario del pacchetto IP che ne controlla l'uguaglianza con il valore inserito nel pacchetto dall'host mittente
d) è calcolato su una combinazione di payload ed intestazione del pacchetto IP
e) è utilizzato dal protocollo TCP per garantire l'integrità dei dati non sono sicuro

R: b

Con riferimento alla frammentazione IP, quante delle seguenti affermazioni sono false:
1) Il campo fragment-offset dell'header IP ha una dimensione pari a 15 bit, per cui un datagramma IP puo' al massimo essere scomposto in 32767 frammenti f
2) Il campo fragment-offset esprime lo spiazzamento in multipli di parole di 8 byte v
3) Se si considera un pacchetto di dimensione pari a 6420 byte (20 byte header, 6400 byte payload) che debba attraversare un link con MTU pari a 1500 byte, il Fragment-offset dell'ultimo frammento è 740 v
4) Se si considera un pacchetto di dimensione pari a 2941 byte che debba attraversare un link con MTU pari a 1500 byte, il pacchetto viene scomposto in 2 frammenti v
5) Solo in alcuni casi tutti i frammenti ottenuti dal medesimo pacchetto IP presentano lo stesso identificativo f
a) Tre affermazioni sono false
b) Due affermazioni sono false
c) Solo un'affermazione e' falsa
d) Quattro affermazioni sono false
e) Nessuna affermazione e' falsa

R: b (Aff. 1 e Aff. 5) (RC1_L09 pag. 9, pag. 10 slide 20)

Come si riconoscono frammenti di uno stesso pacchetto IP?
a) dal campo identification uguale per tutti i pacchetti
b) dal campo source address uguale per tutti i pacchetti
c) dal campo source port uguale per tutti i pacchetti
d) dal campo destination address uguale per tutti i pacchetti
e) dal campo fragment offset uguale per tutti i pacchetti
f) dal campo destination port uguale per tutti i pacchetti
g) da una specifica opzione contenuta nell'intestazione dei pacchetti IP costituenti i frammenti

R: a (RC1_L09 pag. 9 slide 17)

Quale delle seguenti affermazioni è vera, in merito al campo Offset dell'header IP
a) Il campo Offset è ignorato se il bit Reserved è settato ad 1
b) Il campo Offset indica blocchi di 8 byte
c) Il campo Offset è ignorato se il bit More Fragments è settato ad 0
d) Il campo Offset è sempre diverso da zero quando usato nella frammentazione
e) Nessuna affermazione è vera

R: b

Quante delle seguenti affermazioni sono false, in relazione alla frammentazione di un datagramma IP?
Affermazione 1: Tutti i frammenti riportano l'identificativo del pacchetto originario all'interno del proprio header
Affermazione 2: Un frammento non può essere ulteriormente frammentato
Affermazione 3: Tutti i frammenti, tranne l'ultimo, contengono il valore 1 nel flag M (More Fragments)
Affermazione 4: Si possono avere al massimo 8192 frammenti di 8 byte ciascuno
Affermazione 5: Il riassemblaggio dei frammenti è compito del livello di trasporto presso il nodo destinazione
a) Nessuna affermazione è falsa
b) una sola affermazione è falsa
c) due affermazioni sono false
d) Tre affermazioni sono false
e) Quattro affermazioni sono false
f) Tutte le affermazioni sono false

R: c (Aff. 2 e Aff. 5) (RC1_L09 pag. 9 slide 17)

A proposito della frammentazione di pacchetti IP, quale delle seguenti affermazioni NON e' vera ?
a) Un host non può evitare che i pacchetti inviati siano frammentati lungo il percorso
b) La frammentazione dei pacchetti IP compiuta dai router
c) Il riassemblaggio dei pacchetti IP compiuto esclusivamente dall'host destinatario anche il protocollo IP svolge questa funzione
d) Un pacchetto frammentato può essere ulteriormente frammentato lungo il percorso
e) La frammentazione si verifica tipicamente quando un router collega reti basate su differenti tecnologie (es. Token Ring ed Ethernet)

R: a

LEZIONE 11

Il protocollo ARP viene utilizzato per conoscere l'indirizzo fisico dell'host con cui si vuole comunicare solo se:
a) Tale host si trova in un'altra sottorete
b) La AND bit a bit tra l'indirizzo di tale host e la nostra netmask fornisce un risultato con almeno 16 bit pari ad 1
c) Si è verificato un guasto nella rete
d) Per comunicare con tale host abbiamo bisogno di un router
e) Tale host si trova nella nostra stessa sottorete ed il suo indirizzo fisico non è presente in cache
f) Nessuna delle precedenti

R: e (RC1_L11 pag. 3)

Una richiesta ARP
a) Viene spedita da un host mittente ad un host destinatario per ottenere la corrispondenza "indirizzo IP del destinatatio --> indirizzo MAC del destinatario"
b) Viaggia sempre all'interno di una frame Ethernet
c) Viaggia sempre in broadcast su di una rete locale e serve per risolvere l'indirizzo IP del router di default
d) Si usa per risolvere l'indirizzo IP del router di default nel caso in cui il destinatario appartenga alla medesima rete logica del mittente
e) Nessuna delle risposte precedenti è esatta

R: e (RC1_L11 pag. 3 slide 5)

Per poter effettuare una trasmissione dati, come fa un ipotetico host situato in Italia a conoscere l'indirizzo MAC della sua entità paritaria situata a Cuba?
a) attraverso invocazioni iterate del protocollo ARP tra i vari hop che separano i due host
b) attraverso un'unica invocazione del protocollo ARP
c) ai fini di una trasmissione dati, non c'è alcun motivo per cui l'host in Italia debba conoscere l'indirizzo MAC dell'host a Cuba
d) lo chiede direttamente all'host situato a Cuba attraverso un pacchetto di livello applicazione

R: c (RC1_L11 pag. 3 slide 5)

Secondo il protocollo ARP, affinche' un host (A) possa conoscere il mac address di un altro host (B), appartenente ad una diversa sottorete e di cui conosce l'indirizzo IP (supposto che la cache di A sia vuota)
a) A invia in broadcast una richiesta ARP (ARP-request), B invia la risposta (ARP-reply) in broadcast contenente il proprio MAC.
b) A invia in broadcast una richiesta ARP (ARP-request), B invia la risposta (ARP-reply) in unicast all'indirizzo MAC sorgente, contenente il proprio MAC. slide 360
c) A invia in unicast una richiesta ARP (ARP-request), B invia la risposta (ARP-reply) in broadcast contenente il proprio MAC.
d) A invia in unicast una richiesta ARP (ARP-request), B invia la risposta (ARP-reply) in unicast all'indirizzo MAC sorgente, contenente il proprio MAC.
e) Nessuna delle precedenti

R: e

Su una LAN Ethernet l'host con indirizzo IP1 deve inviare un file all'host con indirizzo IP2. Suddiviso in pacchetti (pacchetti dati), il file lungo 300 pacchetti e i pacchetti vengono inviati alla velocità di 1 pacchetto ogni 3ms. L'ARP cache ha un tempo di refresh di 20s e all'invio del primo pacchetto l'ARP cache di IP1 vuota mentre quella di IP2 contiene l'associazione IP1-MAC1. Per quanto attiene l'invio di pacchetti dati (il file) e pacchetti di controllo (ARP) da IP1 verso IP2 si ha che:
a) vengono inviati 300 pacchetti dati e 1 ARP request
b) vengono inviati 300 pacchetti dati e 100 ARP request
c) vengono inviati 300 pacchetti dati e 20 ARP request
d) vengono inviati 300 pacchetti dati e 300 ARP request
e) vengono inviati 300 pacchetti dati e 1 ARP request ogni 20 secondi

R: a (RC1_L11 pag. 8 slide 16)

La cache ARP viene popolata
a) Con le informazioni relative al destinatario di una richiesta ARP, all'interno di tutti gli elementi della rete che ricevono la richiesta stessa
b) Con le informazioni relative al mittente di una richiesta ARP, all'interno di tutti gli elementi della rete che ricevono la richiesta stessa
c) Con le informazioni relative al destinatario di una richiesta ARP, all'interno di tutti gli elementi della rete che ricevono la richiesta stessa, all'atto della ricezione del messaggio di risposta inviato in broadcast sulla rete locale
d) Con le informazioni relative al router di default della rete, quando quest'ultimo risponde ad una richiesta ARP
inoltrata verso l'esterno
e) nessuna delle precedenti

R: b (RC1_L11 pag. 9 slide 17)

Con il messaggio "discovery" del protocollo DHCP - Dynamic Host Configuration Protocol
a) il client DHCP annuncia, alla rete in cui entra, di essere alla ricerca di un server DHCP che possa offrirgli un indirizzo IP
b) il server DHCP fa una richiesta broadcast per scoprire se, nella rete da esso gestita, vi sono host che necessitano di ottenere un indirizzo IP
c) il server DHCP interroga i nodi della rete gestita per scoprire quali indirizzi del pool a sua disposizione sono già stati assegnati e quali sono ancora liberi
d) il client DHCP interroga il server DHCP per scoprire quali sono gli indirizzi tra cui può scegliere
e) il client DHCP interroga i nodi della sua stessa subnet per scoprire di che tipo sono i loro indirizzi

R: a (RC1_L11 pag. 13 slide 25)

Nel protocollo DHCP
a) il pacchetto DHCP discover è inviato all'indirizzo IP del server DHCP, il quale fornirà all'host i dati per la corretta configurazione dei parametri di rete, assegnandoglieli per un periodo di tempo denominato lease time
b) il pacchetto DHCP discover è incapsulato direttamente in un datagramma IP, con il campo Protocol opportuamente configurato pari al numero standard del protocollo DHCP
c) il pacchetto DHCP discover è inviato utilizzando, al livello trasporto, il protocollo UDP
d) il pacchetto DHCP discover è inviato utilizzando, al livello trasporto, il protocollo TCP, al fine di instaurare una connessione permanente al server che garantisca una configurazione automatica degli host con i parametri corretti
e) Nessuna delle precedenti

R: c (Wikipedia)

LEZIONE 12 RIPETI LEZIONE 11 E 12

Il protocollo ICMP (Internet Control Message Protocol) permette
a) lo scambio di messaggi di errore tra router o tra router ed host
b) lo scambio di messaggi di errore tra un DNS primario e un DNS secondario
c) lo scambio di messaggi di errore tra ricevente e mittente legati al controllo di flusso TCP
d) di concordare e gestire la frammentazione tra l'host ricevente e l'host mittente

R: a (RC1_L12 pag. 2)

I pacchetti del protocollo ICMP slide 383
a) contengono un identificatore di sessione
b) sono incapsulati in datagrammi IP
c) sono trasmessi in datagrammi UDP
d) contengono numeri di porto sorgente e destinazione
e) nessuna delle precedenti

R: b (RC1_L12 pag. 2 slide 3)

Con riferimento alla rete schematizzata di seguito: a) slide 387
(A)-------(R1)-------(R2)-------(B)
se l'host A esegue il comando traceroute verso l'host B, indicare quale delle seguenti affermazioni è FALSA.
a) L'host A riceve messaggi ICMP da B di tipo "time exceeded", causati da pacchetti il cui TTL è diventato pari a zero
b) L'host A trasmette sequenze di pacchetti IP con valori crescenti di TTL e tutti aventi come destinazione B
c) L'host A riceve messaggi ICMP da R1 ed R2 di tipo "time exceeded", causati da pacchetti il cui TTL è diventato pari a zero
d) L'host A riceve messaggi ICMP da B di tipo "port unreachable" (se traceroute invia pacchetti UDP) o "echo reply" (se traceroute invia pacchetti ICMP di tipo "echo request")
e) Può restituire valori di Round Trip Time diversi se eseguito in momenti differenti

R: d

Il messaggio "Echo Request"
a) Appartiene al protocollo HTTP
b) Appartiene al protocollo UDP
c) Appartiene al protocollo ICMP
d) Viene generato da un host in risposta ad un messaggio "Echo Reply"
e) Viene generato in caso di host non dotato di interfaccia Ethernet
f) Nessuna delle precedenti

R: c (RC1_L12 pag. 2 slide 3)

Quante delle seguenti affermazioni sono vere?
Affermazione 1: Il programma traceroute utilizza, tra l'altro, il messaggio di errore "Time-To-Live Exceeded" del protocollo ICMP v
Affermazione 2: Il programma traceroute è una versione avanzata del programma ping, in cui il messaggio "echo request" è inviato tre volte di seguito f
non sono sicuro Affermazione 3: Il programma traceroute manda un messaggio "echo request" indirizzato ad ogni router lungo il percorso tra sorgente e destinazione v
Affermazione 4: Il programma traceroute sfrutta opportunamente il campo TTL dell'header del protocollo ICMP per scoprire iterativamente i router presenti sul percorso tra sorgente e destinazione v
a) Due affermazioni sono vere
b) Una sola affermazione è vera
c) Tre affermazioni sono vere
d) Nessuna affermazione è vera
e) Tutte le affermazioni sono vere

R: c (RC1_L12 pag. 3 slide 5 in poi)

Quante delle seguenti affermazioni relative all'applicazione "Ping" sono vere:

1. E' utilizzata per verificare la connettivita' a livello rete tra due host; V
2. E' utilizzata per determinare il percorso per raggiungere una certa destinazione; F
3. Invia una serie di pacchetti con campo TTL via via crescente, a partire da 1; F
4. Invia un pacchetto ICMP di tipo "echo request" ed attende la ricezione di un pacchetto di tipo "echo reply"; V
5. Invia pacchetti TCP. F

a) 3
b) 1
c) 2
d) 4
e) 5

R: c (Aff. 1 e Aff. 4) (RC1_L12 pag. 3 slide 5)

Il programma traceroute

a) E' tipicamente usato anche per analizzare le caratteristiche del collegamento tra due endpoint della rete Internet
b) Utilizza il messaggio di errore “Time To Live Exceeded” del protocollo ICMP per scoprire iterativamente i router presenti sul percorso tra sorgente e destinazione
c) Si arresta alla ricezione del messaggio ICMP "Echo Reply" da parte della destinazione
d) Tutte le precedenti risposte sono esatte

R: b (RC1_L12 pag. 7 slide 14)

LEZIONE 13

Si consideri l'interfaccia di programmazione (API) delle socket di Berkeley. Qual è la primitiva che un server non orientato alla connessione certamente non invocherà?
a) socket()
b) bind()
c) writeto()
d) accept()
e) readfrom()
f) read()
g) Tutte le precedenti chiamate posso essere potenzialmente utilizzate.

R: d (RC1_L13 pag. 12 slide 24)

Quante delle seguenti affermazioni sono valide, in relazione ad un client connection oriented (che utilizza, cioè, il protocollo TCP) che invochi la funzione CONNECT( )?
a) viene concordata tutta una serie di parametri che caratterizzano la connessione tra client e Server
b) Il client si blocca; il controllo gli viene restituito solo dopo che sia stata instaurata la connessione (o in seguito ad una notifica di errore)
c) Il client se realizzato in modalità concorrente, prosegue le sue elaborazioni demandando ad un nuovo processo la gestione delle successive richieste di connessione provenienti dal server.
d) Si scatena una fase di segnalazione tra il client ed il server intesa a stabilire un circuito virtuale tra tali entità

R: due (Aff. A e Aff. B) (RC1_L13 pag. 19 slide 38)

La system call recvfrom() serve per
a) Prelevare una richiesta dalla coda associata ad una socket passiva (sulla quale, cioè, sia stata eseguita la chiamata di sistema listen())
b) Ricevere dati da un altro terminale, restituendo, tra le altre informazioni, l'indirizzo del mittente
c) Specificare qual è il client da cui si intende ricevere i datagrammi
d) Prelevare un segmento TCP memorizzato nel buffer di ricezione del destinatario
e) Nessuna delle precedenti

R: b (RC1_L13 pag. 24 slide 47)

LEZIONE 14

Quale di queste affermazioni relative al NAT è VERA
a) Identifica il destinatario di un pacchetto in ingresso alla LAN in funzione del IP destinazione
b) Identifica il destinatario di un pacchetto in ingresso alla LAN in funzione della porta di destinazione
c) Consente di identificare il destinatario di un pacchetto in uscita da una LAN in funzione del campo TTL dell'header IP
d) Consente di tradurre l'indirizzo MAC contenuto in un pacchetto per individuare la casa produttrice della scheda di rete utilizzata dal mittente
e) Nessuna delle precedenti

R: b (RC1_L14 pag. 3 slide 5)

Come fa un server ad identificare le richieste provenienti da due diversi client in esecuzione su macchine diverse?
a) Si basa sull'indirizzo IP, che sarà diverso per i due client (a differenza del numero di porta sorgente, che potrebbe anche coincidere)
b) Utilizza due porte di ricezione diversi, una per il primo client ed una per il secondo
c) Si basa sul numero di porta sorgente, che sara' sicuramente diversa per i due client
d) Si basa sia sul numero di porta sorgente, sia sul numero di porta destinazione, come richiesto dal demultiplexing delle connessioni
e) Nessuna delle precedenti

R: a (RC1_L14 pag. 3 slide 5)

Come fa un server ad identificare le richieste provenienti da due diversi client in esecuzione sulla stessa macchina?
a) si basa sul numero di porto sorgente, che sarà sicuramente diverso per i due client
b) si basa sul numero di porto sorgente, sia sul numero di porto destinazione, come richiesto dal demultiplexing delle connessioni
c) si basa sull'inidirizzo IP, che sarà diverso per i due client(a differenza del numero di porto sorgente, che potrebbe anche coincidere)
d) utilizza due porti di ricezione diversi, uno per il primo client ed uno per il secondo client
e) nessuna delle precedenti.

R: a (RC1_L14 pag. 3 slide 5)

Si supponga che due istanze di un Web Browser (per esempio Firefox oppure Internet Explorer) siano contemporaneamente attive su un host, e abbiano richiesto entrambe una certa risorsa sul web. Alla ricezione delle risposte, in che modo è possibile distinguere i pacchetti che appartengono ad un'istanza dai pacchetti che appartengono all'altra, al fine di consentirne il corretto smistamento?
a) Da un'analisi del payload applicativo dei pacchetti (conforme al protocollo HTTP)
b) Dall'indirizzo IP destinazione dei pacchetti
c) Dall'indirizzo IP sorgente dei pacchetti
d) Dal numero di porta di destinazione dei pacchetti
e) Nessuna delle precedenti

R: d

Con riferimento al protocollo IPv6, quale delle seguenti affermazioni è falsa?
a) In IPv6 non è consentita la frammentazione dei pacchetti nei router
b) Gli indirizzi di rete IPv6 sono da 128 bit
c) Il campo "Protocol Type" di IPv4 è stato sostituito dal campo "Next Header" (Intestazione Successiva)
d) La checksum dell'header è calcolata più rapidamente rispetto a IPv4, grazie ad una riduzione della lunghezza dell'apposito campo
e) E' possibile associare un pacchetto ad un flusso attraverso una "Etichetta di flusso"

R: d (RC1_L14_parte2 pag. 7 slide 13)

Cosa si intende per "approccio dual stack" in IPv6?

a) Si fa riferimento alla scelta, all'interno dei router della rete, di supportare o il protocollo IPv4 o il protocollo IPv6
b) Si fa riferimento alla possibilità di configurare un'interfaccia di un router con un indirizzo IPv6 ed un'altra interfaccia con un indirizzo IPv4
c) Si fa riferimento alla possibilità di far accedere un host ad un'isola IPv6, tramite un tunnel IPv4
d) Si fa riferimento alla possibilità di far accedere un host ad un'isola IPv4, tramite un tunnel IPv6
e) Nessuna delle precedenti risposte è esatta

R: e (RC1_L14_parte2 pag. 10 slide 20)

Come viene gestita la frammentazione in IPv6?
a) Nel caso in cui un router abbia una MTU più piccola della dimensione del pacchetto da inoltrare, esso si limita ad eliminare il pacchetto. Sarà poi il protocollo TCP soprastante a determinare l'avvenuta perdita di dati ed a gestire la ritrasmissione.
b) Nel caso in cui un router abbia una MTU più piccola della dimensione del pacchetto da inoltrare, esso si limita ad eliminare il pacchetto. Sarà poi compito del livello IP nell'host sorgente accorgersi della perdita e ritrasmetterlo opportunamente frammentato.
c) Nel caso in cui un router abbia una MTU più piccola della dimensione del pacchetto da inoltrare, esso:
1) elimina il pacchetto
2) invia un messaggio ICMP di errore verso l'host sorgente, il quale si occuperà di frammentare opportunamente il pacchetto
d) Nel caso in cui un router abbia una MTU più piccola della dimensione del pacchetto da inoltrare, esso lo frammenterà utilizzando un apposito Extension Header

R: c

LEZIONE 15

Con un algoritmo di instradamento di tipo link state
a) ogni router invia in broadcast le informazioni presenti nella propria tabella di instradamento
b) ogni router invia ai propri vicini le informazioni relative ai percorsi inter-dominio ad esso noti
c) ogni router contatta il proprio area border gateway per ricevere informazioni relative all'instradamento al di fuori del proprio sistema autonomo
d) ogni router invia ai propri vicini le informazioni relative a tutti gli altri elementi della rete
e) Nessuna delle precedenti risposte è esatta

R: e (RC1_L15 pag. 11 slide 22)

In riferimento all'algoritmo Link State, quale delle seguenti affermazioni è vera?
a) Ogni router manda a tutti informazioni su tutti
b) Ogni router manda solo ai suoi vicini informazioni solo su se stesso (numero di interfacce di rete e relativa configurazione)
c) Ogni router manda ai suoi vicini informazioni su tutti
d) Ogni router manda a tutti informazioni sui suoi vicini
e) Ogni router manda a tutti informazioni solo su se stesso (numero di interfacce di rete e relativa configurazione)

R: e (RC1_L15 pag. 11 slide 22)

Nel funzionamento a regime di un algoritmo di routing di tipo Link State, un router è esclusivamente a conoscenza dei costi per raggiungere
a) i suoi vicini
b) tutti i router del dominio autonomo io penso sia questa pagina 62 riassunto
c) i router di frontiera (edge-routers) del dominio autonomo
d) i router interni (core-routers) al dominio autonomo

R: b (RC1_L15 pag. 16 slide 31)

Un protocollo di routing link state
a) Richiede che la topologia della rete sia nota a tutti i router di un dominio
b) Non richiede alcuno scambio di informazioni di raggiungibilità tra i router della rete
c) Soffre del problema del conteggio all'infinito
d) Non è mai soggetto ad oscillazioni
e) Può subire oscillazioni nel caso in cui la funzione di costo adottata dipenda dal numero di passi

R: a (RC1_L15 pag. 16 slide 31)

LEZIONE 16

Quante delle seguenti informazioni contenute nel pacchetto dello stato delle linee (LSP) sono necessarie per il calcolo dei percorsi minimi mediante l'algoritmo di Dijkstra?

a) identificativo del nodo che ha generato il pacchetto	F
b) Numero di sequenza del pacchetto	V
c) Costo della linea che collega il nodo che ha generato il pacchetto ai suoi vicini	V
d) elenco dei vicini direttamente connessi al nodo che ha generato il pacchetto	V
e) Tempo di vita del pacchetto	V

R: Tutte Tranne la A (RC1_L16 pag.2 slide 4)

LEZIONE 18

Quale delle seguenti affermazioni è vera, in merito ad un algoritmo di routing di tipo Distance Vector slide 502
a) ogni router manda periodicamente a tutti gli altri router le informazioni sui suoi vicini
b) ogni router calcola la sua tabella di routing usando l'algoritmo di Dijkstra
c) ogni router calcola la sua tabella di routing usando l'algoritmo Shortest Path First
d) ogni router manda periodicamente ai suoi vicini l'intero contenuto della sua tabella di routing
e) nessuna affermazione è vera

R: d (RC1_L18 pag. 2)

L'algoritmo di instradamento "distance-vector":
a) Se prevede la tecnica "poisoned reverse", garantisce che non si verifichi mai la formazione di percorsi ciclici.
b) Si differenzia da quello "link-state" poiché', mentre quest'ultimo e' di tipo centralizzato, il "distance-vector" e' di tipo distribuito.
c) E' quello usato dal protocollo di routine intradominio OSPF (Open Shortest Path First).
d) E' cosi' chiamato poiche' si basa sullo scambio tra nodi adiacenti di informazioni sotto forma di "vettori di distanze" del formato (destinazione, costo), tramite cui un nodo comunica la propria capacita' di instradare verso la "destinazione" ad un certo "costo".
e) Risulta piu' scalabile e robusto rispetto ai guasti del "link-state".

R: b (RC1_L18 pag. 5 slide 10) la b è sicuramente sbagliata idiota!

Quante delle seguenti affermazioni sono false, in relazione all'algoritmo distance vector?
Affermazione 1: Non è possibile che si creino cicli di instradamento F
Affermazione 2: E' un algoritmo di tipo iterativo, asincrono e distribuito V
Affermazione 3: Non esiste il concetto di convergenza: lo scambio dei messaggi tra i router della rete continua ad avvenire con scadenza periodica F
Affermazione 4: È sempre possibile incorrere in situazioni di routing ciclico, anche se si adottano tecniche quali il poisoned reverse V
a) tutte le affermazioni sono false
b) una sola affermazione è falsa
c) tre affermazioni sono false
d) due affermazioni sono false

R: D (RC1_L18 pag. 5 slide 10, pag. 8, pag. 11 slide 22)

La tecnica poison reverse per Distance vector:
a) Diminuisce la complessità
b) Aumenta la robustezza
c) Risolve il problema dei cicli di instradamento
d) Risolve il problema del conteggio all'infinito Falso! l'ho verificato sul libro
e) Nessuna delle precedenti

R: a (RC1_L18 pag. 8)

Con la tecnica del poisoned reverse
a) Se un router A raggiunge un router B tramite un router C, allora A mente a B riguardo la sua distanza da C (in pratica A comunica a B che la sua distanza da C è "infinita"). Ciò ha lo scopo di evitare che si creino cicli di instradamento
b) Se un router A raggiunge un router B tramite un router C, allora A comunica a B che la sua distanza da C è pari alla distanza di C da B, più uno.
c) Se un router A raggiunge un router B tramite un router C, allora A invierà in broadcast sulla rete un messaggio di aggiornamento dello stato dei link contenente il percorso A->C->B
d) Se un router A raggiunge un router B tramite un router C, allora A mente a C riguardo la sua distanza da B (in pratica A comunica a C che la sua distanza da B è "infinita")
e) Nessuna delle precedenti risposte è esatta

R: d (RC1_L15 pag. 10 slide 20)

LEZIONE 19

A cosa serve il campo Max Response Time dell'header del protocollo IGMP? slide 571
a) E' usato per configurare in maniera esplicita il valore del timeout nelle trasmissioni multicast
b) E' usato dagli host della rete locale per "diluire", in maniera random, le risposte ad una query IGMP (proveniente dal router del primo hop) su di un opportuno intervallo temporale, così da migliorare la scalabilità del protocollo
c) E' usato per indicare un limite superiore al ritardo di trasmissione relativo ad una sessione multicast su Internet
d) Nessuna delle precedenti risposte è esatta

R: b (RC1_L19 pag. 15 slide 29)

Il protocollo IGMP
a) Si occupa di gestire l'associazione ai gruppi multicast, qualora nella rete eista un tunnel multicast verso Internet
b) Si occupa di inoltrare in Internet le informazioni locali relative ai gruppi multicast presenti
c) Funziona tra gli host ed il router di una rete locale per gestire l'iscrizione (JOIN) a gruppi mulitcast, nonché il loro abbandono (LEAVE)
d) Nel caso dell'approccio core-based, consente agli host di una rete locale di comunicare con il router del "primo hop" per creare l'albero di instradamento multicast
e) Nessuna delle precedenti risposte è esatta

R: c (RC1_L19 pag. 11 slide 22)

Con la trasmissione multicast in Internet
a) Chiunque può inviare dati ad un gruppo, a patto di rispettare il vincolo dell'impiego del protocollo TCP
b) Chiunque può inviare dati ad un gruppo, a patto che utilizzi un indirizzo sorgente di classe D
c) Per inviare dati ad un gruppo, è necessario iscriversi ad esso tramite IGMP
d) Per inviare dati ad un gruppo è necessario supportare il routing multicast
e) Nessuna delle risposte precedenti è esatta

R: e (RC1_L19 pag. 9 slide 17)

LEZIONE 20

Il protocollo DVMRP (Distance Vector Multicast Routing Protocol)
a) Usa l'approccio "Truncated Reverse Path Forwarding" per realizzare l'instradamento di tipo multicast
b) E' il più utilizzato protocollo per il routing multicast con approccio group-shared
c) In modalita' "densa" effettua allagamento totale della rete
d) E' un protocollo indipendente dal protocollo di instradamento unicast sottostante

R: c (RC1_L20 pag. 7 slide 13)

Il protocollo PIM
a) In modalita' "sparsa" utilizza la tecnica del tunneling
b) E' indipendente da qualsiasi altro protocollo multicast utilizzato nella rete
c) In modalita' "densa" utilizza un approccio simile al Truncated Reverse Path Forwarding
d) E' basato sul protocollo unicast Distance Vector
e) Nessuna delle precedenti affermazioni e' vera

R: c (RC1_L20 pag. 9 slide 17)

Il protocollo PIM
a)E' indipedente dal protocollo di instradamento unicast sottostante
b)E' basato sul protocollo unicast Distance Vector
c)In modalita' "densa" utilizza utilizza un approccio center-based, tipo il protocollo Core Based Tree (CBT)
d)E' indipendente da qualsiasi altro protocollo multicast utilizzato nella rete
e)In modalita' "sparsa" utilizza un approccio simile al Truncated Reverse Path Forwarding
f)Nessuna delle precedenti affermazioni e' vera

R: c (RC1_L20 pag. 9 slide 17)

La rete MBone
a) è una rete in cui pacchetti unicast vengono incapsulati in pacchetti multicast per attraversare "isole" che supportano l'IP multicasting
b) è una rete dotata del supporto del protocollo IGMP in tutti i suoi router
c) è una rete overlay, realizzata con la tecnica del tunneling, per il supporto di trasmissioni multicast in Internet
d) Nessuna delle precedenti affermazioni è vera

R: c (RC1_L20 pag. 10 slide 19)

LEZIONE 21

In relazione al protocollo UDP, quale delle seguenti affermazioni è falsa?
a) La trasmissione non è affidabile, ma esiste un controllo di errore (checksum) effettuato su tutto il datagramma
b) Non è garantita l'affidabilità della trasmissione, e l'ordine di arrivo dei datagrammi non necessariamente coincide con l'ordine con cui sono stati inviati
c) La tramissione è affidabile, ma i datagrammi vanno riordinati alla destinazione
d) Lo spazio dei numeri di porto UDP è logicamente distinto dallo spazio dei numeri di porto TCP
e) L'eventuale riordino dei datagrammi UDP deve essere trattato dai protocolli di livello superiore

R: c (RC1_L21_parte2 pag. 8 slide 15)

L'header UDP
a) include un campo Extension Header per campi aggiuntivi
b) include un campo Checksum per controllare eventuali errori nell'header e nel payload
c) include un campo Fragment Offset per gestire l'eventuale frammentazione
d) include un campo Sequence Number per l'ordinamento dei pacchetti, essendo un protocollo inaffidabile
e) include esclusivamente i campi porto ed indirizzo sorgente, porto ed indirizzo destinazione

R: b (RC1_L21_parte2 pag. 9 slide 17)

quale delle seguenti affermazioni su udp è falsa
a) il suo header è inferiore a quello di tcp
b) non fa controllo di congestione
c) non ha nessun tipo di controllo di errore
d) tutte le precedenti sono vere

R: c (RC1_L21_parte2 pag. 9 slide 18)

L'header del protocollo UDP e' composto esclusivamente da:
a) porto sorgente, porto destinazione, numero di sequenza
b) porto sorgente, porto destinazione, lunghezza e checksum
c) porto sorgente, porto destinazione, IP sorgente, IP destinazione
d) porto sorgente, porto destinazione, IP sorgente, IP destinazione, lunghezza e checksum
e) porto sorgente, porto destinazione, IP sorgente, IP destinazione, numero di sequenza

R: b (RC1_L21_parte2 pag. 9 slide 17)

LEZIONE 22

Con la tecnica del "pipelining"
a) E' necessario "bufferizzare" alcuni dati nel mittente e/o nel destinatario
b) Non è necessario aumentare l'intervallo dei numeri di sequenza
c) Si può' utilizzare solo l'approccio "Go Back N"
d) Tutte le precedenti affermazioni sono vere

R: a (RC1_L22 pag. 6 slide 12) ?

Quale delle seguenti affermazioni sul protocollo Go-Back-N e' falsa:
a) Al verificarsi di un timeout, il mittente invia nuovamente tutti i pacchetti spediti che non sono stati ancora riscontrati io penso sia questa
b) Prevede che il mittente possa trasmettere più pacchetti senza dover attendere il riscontro
c) Un errore su un solo pacchetto può causare la ritrasmissione di un elevato numero di pacchetti
d) Prevede che il destinatario salvi in un buffer i pacchetti che giungono fuori sequenza
e) Nessuna delle precedenti

a (forse E)

Quale tra i seguenti protocolli a finestra scorrevole (sliding-window) è più conveniente utilizzare su un canale di trasmissione avente una latenza molto bassa e capacità ed affidabilità molto elevate?
a) Stop and wait
b) Selective repeat
c) Go Back-N
d) Indifferentemente uno dei tre

R: c

LEZIONE 23-24

Il controllo di flusso nel protocollo TCP slide 603
a) si basa sulla segnalazione da parte del ricevitore della finestra di ricezione disponibile
b) si basa su una decisione da parte del trasmettitore sulla base dei segmenti persi a causa della congestione
c) è ottenuto con il controllo di errore sul campo checksum
d) non è disponibile
e) nessuna delle precedenti

R: a (RC1_L23_L24 pag. 2 slide 4)

Il campo "Acknowledgement Number" dell'header del TCP
a) Ha senso solo se il flag ACK e' posto ad zero
b) Contiene il numero di sequenza del ricevitore di una porzione di dati trasmessa su di una connessione TCP
c) Se si utilizza la tecnica del piggybacking, consente di inviare un riscontro insieme al "carico utile" (dati) di un segmento
d) Tutte le precedenti affermazioni sono vere

R: c (RC1_L23_L24 pag. 3 slide 6)

Qual è lo svantaggio ad impostare un time-out troppo corto per l'attesa dei riscontri in TCP?
a) che si rischia di inviare pacchetti duplicati inutili sulla rete
b) che il destinatario rischia di essere sommerso di dati che non ha la capacità di elaborare
c) che la rete verrà utilizzata in maniera particolarmente efficiente rischiando la congestione
d) che su una rete non particolarmente affidabile la trasmissione è inefficiente a causa di lunghe ed inutili pause
e) Tutte le precedenti affermazioni sono vere

R: a (RC1_L23_L24 pag. 8 slide 16)

Il timeout di ritrasmissione utilizzato in TCP:
a) è calcolato in base ai valori misurati di RTT
b) è calcolato in base ai valori della finestra di congestione
c) ad ogni evento di perdita viene posto pari alla metà del valore precedente
d) viene concordato tra mittente e destinatario all'inizio della connessione
e) è un valore costante dipendente dall'implementazione (Reno, Tahoe, Vegas) di TCP

R: a (RC1_L23_L24 pag. 9 slide 18)

Come viene utilizzata la stima del Round Trip Time (RTT) effettuata dal protocollo TCP durante il suo funzionamento?
a) Per il corretto dimensionamento del timeout legato alla ricezione dei riscontri.
b) Per incrementare o decrementare il rate di trasmissione secondo un legame di diretta proporzionalità.
c) Per incrementare o decrementare il rate di trasmissione secondo un legame basato su media esponenziale pesata.
d) TCP non effettua alcuna stima del RTT durante il suo funzionamento.

R: a (RC1_L23_L24 pag. 9 slide 18)

Cosa si deduce quando si riceve un pacchetto TCP in cui i flag SYN e ACK sono entrambi pari ad uno?
a) Che l'entità da cui si riceve il pacchetto ha intenzione di instaurare una connessione
b) Che l'entità da cui si riceve il pacchetto è disposta ad accettare la connessione che era stata precedentemente richiesta
c) Che l'ultimo pacchetto è stato perso ma la connessione non è stata abbattuta
d) Che l'entità da cui si riceve il pacchetto effettua una richiesta di risincronizzazione a causa della perdita di uno o più pacchetti nel flusso
e) Che l'entità da cui si riceve il pacchetto vuole chiudere la connessione

R: b (RC1_L23_L24 pag. 10 slide 19)

A cosa serve il three way handshacking in TCP ?
a) A concordare la RcvWindow e la… (non mi ricordo) rcv win e num sea
b) ad essere completamente sicuri che entrambi siano disponibili alla connessione
c) perché per iniziare una connessione sono necessari 3 ACK duplicati
d) perché per chiudere una connessione sono necessari 3 ACK duplicati

R: a (RC1_L23_L24 pag. 10 slide 19)

Nell'implementazione del TCP, in quale caso si raddoppia l'intervallo di timeout?
a) In seguito ad un timeout, in occasione della ritrasmissione del segmento non ancora riscontrato ed avente il più piccolo numero di sequenza
b) Quando il valore di EstimatedRTT diventa il doppio di DevRTT
c) Quando la finestra di congestione raggiunge il valore corrente della soglia
d) Quando si perdono tre segmenti consecutivi

R: a (RC1_L23_L24 pag. 18 slide 35)

Con riferimento alla ritrasmissione di segmenti TCP, quale delle seguenti affermazioni è falsa ?
a) La ricezione di tre ack duplicati determina una ritrasmissione immediata
b) Se il ricevitore rileva un "buco" nella sequenza dei segmenti ricevuti, aumenta il valore corrente del timeout
c) Se il timeout è settato ad un valore troppo piccolo, si determina un utilizzo della rete poco efficiente (ritrasmissioni inutili)
d) Il timeout di ritrasmissione è aggiustato dinamicamente in funzione del valore stimato di RTT
e) Se il timeout è settato ad un valore troppo elevato, si limita il throughput della comunicazione

R: b (RC1_L23_L24 pag. 18 slide 36)

LEZIONE 25

In una trasmissione TCP tra due end-point, cosa si intende con il termine finestra di ricezione? slide 695
a) Il tempo di andata e ritorno (round trip time) entro il quale il sender, dopo l'invio di dati verso un receiver, attende la conferma(acknowledge) prima di considerare perso il pacchetto inviato
b) La dimensione in byte che il sender sa di non poter eccedere nell'invio di dati verso un receiver
c) La dimensione in byte alla quale viene troncato un pacchetto troppo grande inviato da un sender verso un receiver.
d) Il numero di pacchetti massimo che il sender invia prima di iniziare ad attendere i pacchetti di conferma da parte del receiver.

R: b (RC1_L25 pag. 3 slide 25)

Nel controllo di flusso del protocollo TCP:
a) il receiver calcola la propria finestra di ricezione come: RcvWindow = RcvBuffer - [LastByteSent - LastByteAcked]
b) la quantita' di dai inviati e' vincolata anche alla gestione del controllo di congestione, ossia: LastByteSent - LastByteAcked < = min(CongWin,RcvWindow)
c) il mittente riceve un'informazione sulla RcvWindow del destinatario e da quel momento gestisce la dinamica della finestra senza alcun feedback da parte di quest'ultimo.
d) se il receiver ha la RcvWindow a zero e non ha nulla da rispedire al mittente, dopo lo svuotamento del buffer in ricezione, la trasmissione verra' ripristinata con l'instaurazione di una nuova connessione.
e) e' necessario che il mittente calcoli il RcvBuffer del destinatario, a partire dalla RcvWindow.

R: b (RC1_L25 pag. 5 slide 9)

Per "slow start" (partenza lenta) si intende:
a) La fase del meccanismo di controllo di congestione di TCP in cui il mittente incrementa la propria frequenza di invio in modo esponenziale
b) La fase del meccanismo di controllo di congestione di TCP in cui il mittente incrementa la propria frequenza di invio in modo lineare
c) La fase del meccanismo di controllo di congestione di TCP che segue alla ricezione di tre ACK duplicati
d) Nessuna delle precedenti

R: a (RC1_L25_parte2 pag. 6 slide 12)

LEZIONE 27

Quante delle seguenti affermazioni sono vere, con riferimento alle funzioni svolte dal livello Data Link? slide 52

Affermazione 1: Ha come scopo la trasmissione affidabile di frame di dati
Affermazione 2: Accetta come input frame di dati e li trasmette sequenzialmente
Affermazione 3: Verifica la presenza di eventuali errori di trasmissione, aggiungendo delle informazioni aggiuntive di controllo
Affermazione 4: Può gestire meccanismi di correzione di errori tramite ritrasmissione F
a) Tre affermazioni sono vere
b) Una affermazione e' vera
c) Nessuna affermazione e' vera
d) Due affermazioni sono vere
e) Tutte le affermazioni sono vere

R: e

Con il controllo di parita' a tre bit e' possibile
a) Rilevare errori su tre bit e correggere errori su due bit
b) Rilevare e correggere errori su tre bit
c) Rilevare errori su tre bit, e correggere errori su un solo bit
d) Nessuna delle precedenti risposte è esatta

R: d (RC1_L27 pag. 5 slide 10)

Con un codice a ridondanza ciclica che impieghi un "generatore" di 6 bit e' possibile
a) Correggere tutti gli errori che coinvolgono al massimo 5 bit
b) Rilevare tutti gli errori che coinvolgono al massimo 6 bit
c) Rilevare tutti gli errori che coinvolgono al massimo 5 bit
d) Rilevare e correggere tutti gli errori che coinvolgono al piu' 6 bit

R: c (RC1_L27 pag. 6 slide 12)

La tecnica CSMA/CD ...
a) è utilizzata nel livello MAC delle reti wireless
b) consente una maggiore efficienza nell'utilizzo del mezzo trasmissivo rispetto alla sola tecnica CSMA (senza Collision Detection)
c) si basa sull'utilizzo di opportune sequenze di codifica (Chipping sequence) per codificare i dati
d) elimina le collisioni in reti LAN nelle quali il mezzo trasmissivo è condiviso
e) presuppone la sincronizzazione delle stazioni trasmittenti

R: b (RC1_L27 pag. 16 slide 31)

LEZIONE 28

Con il Binary Exponential Backoff
a) Dopo ogni collisione si incrementa di uno l'intervallo di slot tra cui scegliere per la ritrasmissione
b) Dopo la terza collisione consecutiva si aspetta, prima di ritrasmettere, un numero di slot scelto in maniera casuale tra 0 e 7
c) Dopo ogni collisione si incrementa di due l'intervallo di slot tra cui scegliere per la ritrasmissione
d) Dopo l'undicesima collisione consecutiva si aspetta, prima di ritrasmettere, un numero di slot scelto in maniera casuale tra 0 e 2047

R: b (RC1_L28 pag. 7 slide 14)

In CSMA/CD con algoritmo del Backoff Esponenziale, partendo dall'istante zero in assenza di collisioni, se si verificano 16 collisioni consecutive per il tempo di attesa casuale (k) si avrà: ok
a) k scelto tra {0,1,2,3,4,...,65535}
b) k scelto tra {0,1,2,3,4,...,1023}
c) k scelto tra {0,1,2,3,4,...,65536}
d) k scelto tra {0,1,2,3,4,...,16}
e) nessuna delle precedenti

R: b (RC1_L28 pag. 7 slide 14)

Con il Binary Exponential Backoff ?
a) Dopo ogni collisione si raddoppia l'intervallo di slot tra cui scegliere per la ritrasmissione, fino alla decima collisione consecutiva
b) Dopo la prima collisione si aspetta, prima di ritrasmettere, un numero di slot scelto in maniera casuale tra 0 e 1
c) Dopo la dodicesima collisione consecutiva si aspetta, prima di ritrasmettere, un numero di slot scelto in maniera casuale tra 0 e 1023
d) Tutte le risposte precedenti sono esatte

R: d

Un bridge che fa auto-apprendimento
a) Per ogni frame ricevuta, memorizza l'interfaccia di ingresso della frame, il MAC address sorgente in essa contenuto ed il tempo attuale
b) Per ogni frame ricevuta, memorizza l'interfaccia di ingresso della frame ed il MAC address destinazione in essa contenuto
c) Per ogni frame ricevuta, memorizza l'interfaccia di ingresso della frame ed il MAC address sorgente in essa contenuto
d) Per ogni frame ricevuta, memorizza l'interfaccia di uscita selezionata per la frame ed il MAC address destinazione in essa contenuto

R: a (RC1_L28_parte2 pag. 7 slide 14)

Un bridge che fa auto-apprendimento
a) Per ogni frame ricevuta, memorizza l'interfaccia di ingresso della frame, il MAC address destinazione in essa contenuto ed il tempo attuale
b) Per ogni frame ricevuta, memorizza l'interfaccia di ingresso della frame ed il MAC address destinazione in essa contenuto
c) Per ogni frame ricevuta, memorizza l'interfaccia di uscita selezionata ed il MAC address sorgente in essa contenuto
d) All'accensione non possiede alcuna informazione utile per ottimizzare le trasmissioni

R: d (RC1_L28_parte2 pag. 8 slide 16)

LEZIONE 29

Con riferimento alle WLAN, quante delle seguenti affermazioni sono vere:
1) Con la tecnica del frequency hopping, il ricevitore e' in grado di saltare le frequenze in maniera sincronizzata con il mittente per ricevere correttamente le frame V
2) L'operazione di associazione ad un Access Point prevede sempre una fase di autenticazione F
3) La frame contiene un campo duration che da' un'indicazione relativa alla durata della trasmissione dati V
4) La tecnica per selezionare un Access Point e' detta "scanning" e prevede tre passi: probe, risposta al probe, conferma di associazione F
a) Due affermazioni sono vere
b) Solo un'affermazione vera
c) Tre affermazioni sono vere
d) Quattro affermazioni sono vere
e) Nessuna affermazione e' vera

R: a (RC1_L29 pag. 8 slide 15, pag. 9 slide 18, pag. 14 slide 27, pag. 19 slide 38)

A cosa serve la tecnica dello scanning adottata nelle reti 802.11?
a) A selezionare un particolare Access Point cui associarsi mediante invio di una speciale frame di richiesta di associazione
b) A determinare la presenza di altre stazioni nella stessa cella del nodo trasmittente
c) A determinare il range di frequenza ottimale per la trasmissione con la tecnica DSSS (Direct Sequence Spread Spectrum)
d) A verificare se ci sono stazioni già impegnate a trasmettere verso una specifica destinazione

R: a (RC1_L29 pag. 10 slide 19)

Quando si utilizza il protocollo 802.11
a)Non si possono mai verificare collisioni, grazie all'impiego della tecnica CSMA/CA
b)E' impossibile che vi siano collisioni perché nella frame c'è un campo Duration che indica la durata della trasmissione
c)Le collisioni possono essere sempre rilevate dal mittente
d)Le stazioni mittenti non sempre sono in grado di rilevare le collisioni a causa di fenomeni quali il fading

R: a (RC1_L29 pag. 14 slide 28)

Con la tecnica CSMA/CA
a) Si introduce un messaggio di richiesta di trasmissione (Request To Send) per regolare la fase di accesso al canale
b) Si introduce un messaggio di richiesta di trasmissione (Request To Send) per regolare la fase di accesso al canale dopo una prima collisione
c) Non e' piu' necessario attendere un tempo pari allo Short Inter Frame Spacing (SIFS) prima di rispondere ad un messaggio proveniente dalla controparte
d) Si introduce un messaggio di richiesta di trasmissione (Request To Send), eliminando la necessita' di utilizzare il Network Allocation Vector

R: a (RC1_L29 pag. 14 slide 28)

Quante delle seguenti affermazioni sono vere?
Affermazione 1: Il problema della "stazione nascosta" si risolve facendo in modo che una stazione che ascolta il messaggio CTS (Clear To Send) non interferisca con l'imminente trasmissione V
Affermazione 2: Il problema della "stazione nascosta" si risolve facendo in modo che una stazione che ascolta il messaggio RTS (Request To Send) non interferisca con l'imminente trasmissione F
Affermazione 3: Il problema della "stazione nascosta" si risolve facendo in modo che una stazione che ha atteso un tempo pari al Distributed Inter Frame Space (DIFS) sia l'unica a trasmettere F
Affermazione 4: Il problema della "stazione nascosta" si risolve introducendo un meccanismo esplicito di riscontro anche per le frame RTS e CTS V
a)Tutte le affermazioni sono vere
b)Due affermazioni sono vere
c)Una sola affermazione è vera
d)Nessuna affermazione è vera
e)Tre affermazioni sono vere

R: b

DOMANDE NON CATALOGATE

Quanti, tra i seguenti protocolli, non possono prescindere dall'invio in broadcast di pacchetti per poter funzionare correttamente?
* DHCP
* DNS
* ARP
* IGMP
* HTTP
* SMTP
a) 0
b) 1
c) 2
d) 3
e) 4
f) 5
g) 6

D (dhcp arp igmp)

La commutazione di messaggio (commutazione di pacchetto senza frammentazione)
a) È meno efficiente della commutazione di pacchetto (con i messaggi frammentati), perché sfrutta tecniche di trasmissione meno avanzate (tipo time division multiplexing)
b) È in generale più efficiente della commutazione di pacchetto (con i messaggi frammentati), perché sfrutta l'effetto del pipelining per la trasmissione dei messaggi
c) È sempre più efficiente della commutazione di pacchetto (con i messaggi frammentati), anche in caso di messaggi di grandi dimensioni, perché aggiunge meno overhead dovuto all'header
d) Nessuna delle precedenti risposte è esatta

d)

Quante delle seguenti affermazioni sono vere, con riferimento ad una rete di accesso?
Affermazione 1: fornisce la connettività agli end-system e può essere realizzata sia in tecnologia wired che wireless
Affermazione 2: fa da collante tra due reti backbone e può essere realizzata sia in tecnologia wired che wireless
Affermazione3: fornisce la connettività agli end-system e deve essere necessariamente realizzata in tecnologia wired
Affermazione 4: è una rete locale che si collega ad Internet tramite un bridge
a) Una sola affermazione è vera
b) Tre affermazioni sono vere
c) Due affermazioni sono vere
d) Tutte le affermazioni sono vere

c)

In una rete di calcolatori, i programmi applicativi
a) sono eseguiti nei router della rete e rispettano il paradigma client-server
b) sono eseguiti negli end-system della rete e rispettano sempre il paradigma client-server
c) sono eseguiti negli end-system della rete ed usano sempre il protocollo di trasporto TCP
d) sono eseguiti sia negli end-system della rete che nei router e rispettano il paradigma client-server
e) Nessuna delle precedenti affermazioni è vera

e)

Si supponga che un bridge ad 8 porte riceva su una delle sue porte una frame destinata ad un indirizzo MACx. Indicare come tale frame verrà trattata dal bridge supponendo che MACx non sia presente nella sua tabella.
a) il bridge inoltra copie della frame sulle tutte le sue 8 porte
b) il bridge invoca il protocollo ARP per individuare la localizzazione del destinatario
c) il bridge inoltra copie della frame sulle sue restanti 7 porte
d) il bridge scarta la frame
e) il bridge segnala un errore al mittente della frame
f) il bridge invia la frame esclusivamente sulla porta sulla quale è connessa la scheda di rete avente indirizzo MACx

c)

Quale delle seguenti affermazioni è falsa?
a) I ripetitori operano soltanto al livello fisico
b) I bridge e gli switch di rete locale operano fino al livello Data Link
c) I router operano fino al livello rete
d) Nessuna affermazione è falsa
e) I bridge e gli switch di rete locale possono effettuare instradamento tra reti distribuite eterogenee
f) Tutte le affermazioni sono false

e)

Come si divide la banda tra due grossi flussi, uno TCP ed uno UDP, che competono sullo stesso canale?
a) Il flusso TCP acquisirà maggiori risorse grazie all'algoritmo di controllo di congestione che provocherà delle perdite nei pacchetti del flusso UDP non affidabile.
b) Non è possibile fare alcuna previsione sulla ripartizione della banda tra i due flussi, a causa dell'eterogeneità dei protocolli in gioco
c) Due flussi aventi protocolli di trasporto differenti non possono coesistere su uno stesso canale.
d) La banda si equi ripartisce (approssimativamente) tra i due flussi.
e) Nessuna delle precedenti affermazioni è vera

e)

In TCP, come si garantisce che connessioni multiple su uno stesso canale condividano in maniera equa la banda totale?
a) Non vi è alcuna garanzia. Come ottenere la condivisione equa della banda è ancora oggetto di studio.
b) L'equità è garantita implicitamente dal meccanismo di controllo di congestione.
c) Si fa in modo che il mittente che per primo inizia la trasmissione si accorga della entrata di un'altra connessione e riduca immediatamente il suo rate di trasmissione (meccanismo passivo).
d) Si fa in modo che un mittente che inizia a trasmettere i suoi dati chieda agli altri mittenti che occupano il canale di ridurre il loro rate di trasmissione (meccanismo attivo).

b)

Quante delle seguenti affermazioni sono false, in relazione alla frammentazione di un datagramma IP?
Affermazione 1: Tutti i frammenti riportano l'identificativo del pacchetto originario all'interno del proprio header v
Affermazione 2: Un frammento non può essere ulteriormente frammentato f
Affermazione 3: Tutti i frammenti, tranne l'ultimo, contengono il valore 1 nel flag M (More Fragments) f
Affermazione 4: Si possono avere al massimo 8192 frammenti di 8 byte ciascuno v
Affermazione 5: Il riassemblaggio dei frammenti è compito del livello di trasporto presso il nodo destinazione v
a) Nessuna affermazione è falsa
b) Quattro afermazioni sono false
c) Tre affermazioni sono false
d) una sola affermazione è falsa
e) due affermazioni sono false
f) tutte le affermazioni sono false

Con riferimento alla trasmissione IP multicast, quale delle seguenti affermazioni è falsa?
a) Un host che vuole inviare un pacchetto multicast al di fuori della propria rete fisica, incapsula il pacchetto in un pacchetto con indirizzo destinazione unicast
b) Il livello IP non fornisce meccanismi per consentire ad un membro di un gruppo multicast di conoscere quanti host hanno fatto il join al gruppo
c) La trasmissione di pacchetti multicast su rete Ethernet avviene utilizzando speciali indirizzi MAC come indirizzo destinazione
d) I messaggi IGMP sono sempre trasmessi con un indirizzo multicast come destinazione
e) Un host può trasmettere pacchetti ad un gruppo multicast anche senza aver fatto il join al gruppo

c)

Il protocollo Reverse Path Forwarding
a) E' una tecnica di "broadcast selettivo", che può essere applicata alla trasmissione multicast con opportuni accorgimenti atti ad evitare l'allagamento di zone non interessate alla trasmissione multicast
b) Serve per evitare che copie inutili di un pacchetto multicast circolino sull'albero groupshared calcolato
c) In modalità "densa" effettua allagamento totale della rete
d) E' un protocollo indipendente dal protocollo di instradamento unicast sottostante

a)

Quale delle seguenti affermazioni è esatta:
1) Un Frammento Ip è un datagramma privo di un header IP e di un playload contenente dati di livello 4 della pila ISO/OSI
2) Un Frammento Ip è un datagramma formato da un header IP ed un playload contenente dati di livello 4 della pila ISO/OSI
3) Un Frammento Ip è un datagramma privo di un header IP e di un playload contenente dati di livello 2 della pila ISO/OSI
4) Un Frammento IP è un datagramma formato da un header IP ed un playload contenente dati di livello 2 della pila ISO/OSI

2

Il tempo di trasmissione è dato da
a) Tempo necessario per effettuare il controllo degli errori + tempo necessario per determinare l'instradamento dei pacchetti
b) Tempo di attesa nelle code dei router + tempo di elaborazione nei singoli nodi
c) Lunghezza del canale di comunicazione/velocità del segnale
d) Lunghezza del pacchetto/velocità del segnale
e) Nessuna delle precedenti

d)

Quante delle seguenti affermazioni sono false?
Affermazione 1: In un canale con errori, ma senza perdita di pacchetti è necessario introdurre un meccanismo di "timeout" per fare in modo che il ricevitore possa distinguere eventuali duplicati di pacchetti F
Affermazione 2: In un canale con errori, ma senza perdita di pacchetti è sufficiente intordurre un meccanismo di riscontro (ACK) F
Affermazione 3: In un canale con errori, ma senza perdita di pacchetti è necessario introdurre un meccanismo di riscontro (ACK) ed un "numero di sequenza" per consentire al ricevitore di distinguere le ritramissioni da segmenti contenenti nuovi dati V
Affermazione 4: In un canale con errori, ma senza perdita di pacchetti è necessario introdurre un meccanismo di riscontro (ACK), insieme ad un meccanismo di timeout F
a)Tutte le affermazioni sono false
b)Due affermazioni sono false
c)Nessuna affermazione è falsa
d)Tre affermazioni sono false
e)Una sola affermazione è falsa

d)

Il numero di porta serve per
a) Gestire più connessioni UDP in parallelo
b) Gestire il demultiplexing dei segmenti a livello TCP
c) Gestire il demultiplexing dei datagrammi al livello IP
d) Realizzare server web che utilizzino connessioni persistenti per lo scambio degli oggetti

b)

Quanti dei i seguenti protocolli di livello applicativo fanno uso di un servizio di trasporto inaffidabile?
- HTTP
- FTP
- DHCP
- POP3
- SMTP
- DNS
-
a) 2

b) 1
c) 3
d) 4
e)5
f)6

a)DHCP E DNS

Quante delle seguenti affermazioni sono vere, con riferimento ai protocolli di comunicazione?
Affermazione 1: Per protocollo di comunicazione si intende un insieme di regole che permette la corretta instaurazione, mantenimento e terminazione della comunicazione tra due o più entità F
Affermazione 2: All'interno di un singolo dispositivo di rete, un protocollo di comunicazione consente lo scambio di informazioni tra due strati adiacenti della pila protocollare F
Affermazione 3: Un protocollo di comunicazione definisce il formato e l'ordine dello scambio di messaggi tra le entità comunicanti V
Affermazione 4: In una rete di calcolatori, un protocollo regola la comunicazione tra entità di pari livello presenti in due dispositivi della rete tra loro comunicanti V
a) Tre affermazioni sono vere
b) Due affermazioni sono vere
c) Nessuna affermazione è vera
d) Una affermazione è vera
e) Tutte le affermazioni sono vere

Con riferimento al seguente percorso di rete:
(SRC)----mtu=1500----(R1)----mtu=500----(R2)----mtu=1500----(DST)
se la sorgente (SRC) invia un pacchetto (con ID=5 e DF=0) di 1400 byte verso la destinazione (DST), nella ipotesi che non vi siano perdite di pacchetti, indicare quale delle seguenti affermazioni è FALSA.
a) A DST sono consegnati tre pacchetti, ciascuno di dimensione totale 500 byte
b) R2 inoltra un pacchetto con ID=5 ed offset=120
c) Il router R2 trasmette a DST 3 pacchetti IP
d) Il router R1 produce 3 frammenti a partire dal pacchetto

a

Un buon protocollo di routing deve
a) ridurre al minimo il traffico generato per controllare la topologia della rete sulla quale esso opera
b) ridurre al minimo il numero di nodi che controlla
c) essere sia di tipo IGP che di tipo BGP
d) aumentare al massimo il tempo per accorgersi di cambiamenti sulla topologia della rete sulla quale esso opera, per evitare oscillazioni
e) basarsi su algoritmi di routing di tipo Link State

a)

In un router il processo di instradamento (routing)
a) si occupa di inviare i pacchetti al router di next hop
b) si occupa di inviare i pacchetti al gateway di default
c) si occupa di determinare le best route mentre il processo di inoltro (forwarding) invia i pacchetti al router di next hop
d) si occupa di inviare i pacchetti al router di next hop mentre il processo di inoltro (forwarding) di determinare le best route
e) è sempre e solo dinamico

c

Un'attività di monitoraggio di una rete locale rivela che il throughput risulta limitato a causa del forte impatto del traffico di broadcast dovuto all'elevato numero di host presenti. In seguito a ciò, l'amministratore di rete decide di sostituire a tutti i dispositivi di tipo hub (di livello 1), dei bridge (anche detti switch, di livello 2). Qual è l'effetto di questo cambiamento.
a) Le prestazioni complessive migliorano, ma l'impatto del broadcast resta il medesimo
b) Le prestazioni complessive migliorano e l'impatto del broadcast diminuisce fino quasi ad annullarsi
c) Le prestazioni peggiorano

d) Le prestazioni restano esattamente inalterate
e) Non è possibile prevedere come cambino le prestazioni senza conoscere la particolare topologia della rete

b

Cosa si intende con il termine "demultiplexing" al livello trasporto?
a) Raccogliere i dati provenienti dal livello rete, esaminare l'header di livello trasporto per effettuare controlli ed eventualmente smistare i dati al livello applicazione
b) Raccogliere i dati dal livello applicazione ed "imbustarli" aggiungendo un header appropriato che consenta al ricevitore di distinguerli da dati appartenenti ad un processo distinto
c) Raccogliere i dati dal livello applicazione ed inviarli al ricevitore in maniera affidabile
d) Raccogliere i dati dal livello rete e controllare che la checksum sia corretta

a)

Con un hub
a) Si realizza un unico dominio di collisione
b) si puo' collegare un troncone di LAN Ethernet 100BaseT con un troncone 10Base2
c) si puo' collegare un troncone di LAN Ethernet 10BaseT con un troncone 100BaseT
d) Si realizzano tanti domini di collisione quanti sono i tronconi di rete collegati tra di loro

a

Un host H vuole contattare l'indirizzo unina.it. Quante richieste verranno inviate sapendo che H è completamente indipendente dai server autoritative .it e unina.it e che la cache sia vuota. Nel caso di richiesta iterativa e ricorsiva.
a)6-8
b)7-8
c)6-6
d)8-8
e)8-7
f)8-6

d)

Il protocollo BGP
a) Consente di estendere l'approccio link state al caso inter-dominio
b) Consente di far funzionare il protocollo distance vector anche tra sistemi autonomi differenti
c) Consente lo scambio di informazioni di tipo burocratico-amministrativo tra sistemi autonomi differenti
d) Può essere utilizzato per realizzare un instradamento multicast del tipo source-based tree
e) Nessuna delle precedenti ripsoste è esatta

e)

Un messaggio BGP di tipo UPDATE, serve a:
a) inviare ad un peer BGP una risposta ad un messaggio errato
b) aggiornare la tabella di instradamento di un peer BGP, inviandogli un nuovo vettore delledistanze
c) verificare che un peer BGP sia ancora attivo
d) inizializzare la connessione TCP tra due peer BGP
e) aggiornare un peer in relazione alla raggiungibilità di alcune destinazioni (aggiunta/eliminazione di cammini)
f) Tutte le precedenti risposte sono esatte

e)

Quante delle segenti affermazioni sono valide, in relazione ad un client connectionless (che utilizza, cioè, il protocollo UDP) che invochi la funzione connect()?
Affermazione 1: Il server non viene realmente contattato, ma si produce semplicemente la memorizzazione locale dell'indirizzo del suo indirizzo V
Affermazione 2: ogni successivo messaggio scritto sulla socket sarà diretto al server indicato nella chiamata alla connect() F
Affermazione 3: ogni successivo messaggio ricevuto sulla socket verrà accettato solo se proveniente dal server indicato nella chiamata alla connect() F
Affermazione 4: Si scatena una fase di segnalazione tra il client ed il server intesa a stabilire un circuito virtuale tra tali entità F
a) Tre affermazioni sono vere
b) Due affermazioni sono vere
c) Una affermazione è vera

d) Tutte le affermazioni sono vere
e) Nessuna affermazione è vera

Un PC ha un link di rete con bandwidth di 100 kbit/s. Il link viene adoperato esclusivamente per inviare dati da tre differenti processi in esecuzione sul PC, ciascuno dei quali richiede il massimo della bandwidth disponibile.
Supponendo che il primo processo adoperi il protocollo UDP e che i rimanenti adoperino TCP, la bandwidth del link di rete sara':
a) suddivisa in parti uguali fra le connessioni TCP, mentre il processo che adopera UDP non riuscirà' ad inviare dati. Infatti, UDP non ha nessun meccanismo di controllo che gli consente di segnalare la sua richiesta di bandwidth e viene quindi scavalcato dalle connessioni TCP che invece 'prenotano' la bandwidth sul link.
b) occupata in prevalenza dai dati inviati con UDP, poiché' le connessioni TCP si auto-limitano nell'invio dei dati se rilevano congestione sulla rete.
c) suddivisa in modo totalmente casuale e dipendente esclusivamente dal sistema operativo del PC.
d) suddivisa in parti uguali in misura di 1/3 della bandwidth totale. La suddivisione della bandwidth di rete e' infatti indipendente dai protocolli di rete che si occupano soltanto di trasferire i dati da un punto ad un altro della rete.
e) suddivisa con una politica di tipo FCFS (First Come First Served). La bandwidth viene monopolizzata dal primo processo che richiede l'invio dei dati.

b)