

TSR Bible

Novità:

22/06/2010 **Tecnologie e servizi di rete** (Prof. Luigi Ciminiera)

I partecipanti all'appello del 23 giugno sono pregati di distribuirsi nelle aule come segue:

- aula 6, da A a Durando
- aula 10, da Ferrara a Panico
- aula 3S, da Passannanti a ZZZZZ

Test online aggiornato: <http://magnetz.org/tsr/>

N.B. Per inserire un commento:

Inserisci -> Commento

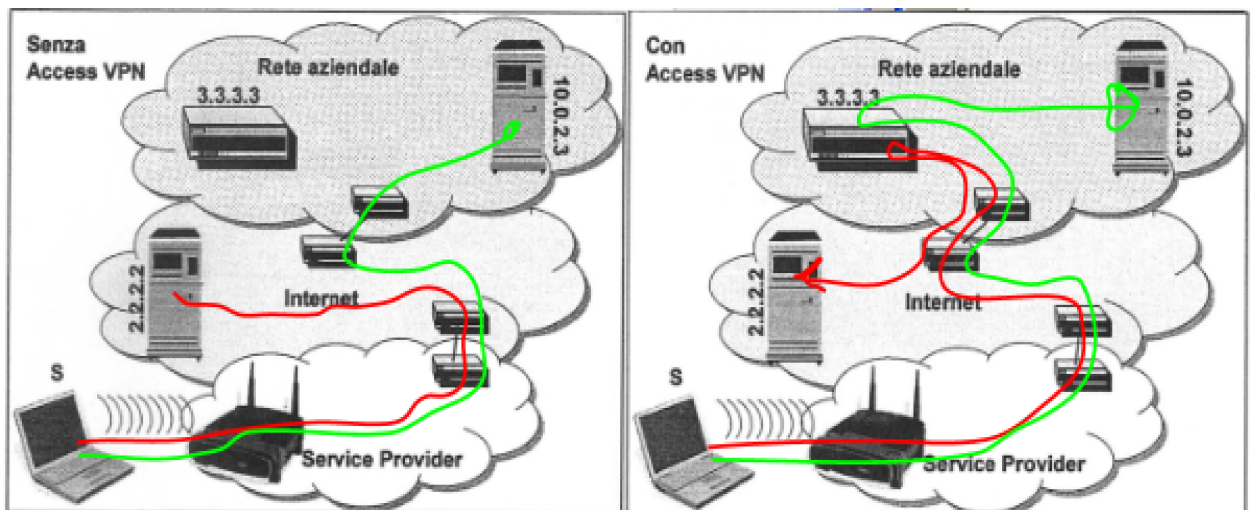
Indice:

- [Domande Aperte](#)
- [Domande Multiple](#)
- [IPv6](#)
- [VPN](#)
- [VoIP/SIP](#)
- [MPLS/ATM](#)
- [Domande multiple con risposte brevi](#)
- [Domande multiple 23 Giugno](#)

Domande Aperte con Risposte

(Compito 18 Luglio 2009)

(1) La stazione S mostrata nella figura si collega ad un hot-spot wireless. Una volta che abbia superato gli eventuali meccanismi di autenticazione, è autorizzata ad inviare traffico a qualsiasi destinazione IP. Indicare, direttamente sul disegno il percorso seguito dai pacchetti inviati alle destinazioni 2.2.2.2 e 10.0.2.3 mostrate in figura, prima e dopo che l'utente della stazione S abbia attivato una VPN di accesso basata su PPTP terminata sul gateway 3.3.3.3. Indicare brevemente eventuali assunzioni fatte se necessarie per giustificare la risposta data. (Nota. Si presti attenzione agli indirizzi IP indicati in figura)-----



clccare 2 volte per disegnare

(RISP)

Supposto l'accesso alla VPN di tipo **centralizzato** (come in figura), il traffico deve necessariamente passare prima dal VPN gateway (3.3.3.3), il quale reindirizza il traffico verso le due destinazioni.

Se l'accesso è di tipo distribuito, il traffico internet non passa necessariamente Domande multiple 23 Giugnodal gateway, ma viene indirizzato con le normali regole di routing.

N.B. Si può scegliere la modalità di accesso distribuita disabilitando l'opzione "Use Default Gateway on Remote Network" sulle opzioni di configurazioni della VPN.

con access VPN è giusto passare sempre per GW se l'accesso è centralizzato. Jonathan 21/06/10 14.01

(2) Descrivere la procedura di configurazione dell'indirizzo IPv6 su una stazione con la modalità stateless-----

(3) Si vuole mettere in funzione un servizio di proxy SIP che sia in grado di fornire il servizio SIP su SSL e UDP, utilizzando 2 server denominati sip1.mydomain.org e sip2.mydomain.org, che sono entrambi capaci di fornire entrambi i servizi. Si indichi cosa deve essere registrato nel DNS per riuscire ad attivare il servizio voluto-----

(RISP)

Nel DNS troveremo 3 tipologie di entry riguardanti il servizio SIP

- NAPTR: definisce quale protocollo di trasporto debba essere preferito per accedere al servizio (TCP,UDP,TLS/TCP,SCTP), non strettamente necessario ma se presente saranno 3 entry.

Record NAPTR:

domain-name|TTL|Class|NAPTR|order|preference|flags|service|regexp|target

- SRV: definisce i parametri per accedere a quel determinato servizio

Record SRV

_Service._Proto.name|TTL|Class|SRV|Priority|Weight|Port|Target

- A/AAAA: contengono gli indirizzi veri e propri A: IPV4, AAAA:IPV6

Record A/AAAA:

domain-name|TTL|Class|Type|address

Risultato:

```
sip1.mydomain.org 43200 IN A 10.0.0.30
```

```
sip2.mydomain.org 43200 IN A 10.0.0.40
```

```
;
```

```
_sips._tcp.mydomain.org 43200 IN SRV 0 0 5060 sip1.mydomain.org
```

```
_sips._tcp.mydomain.org 43200 IN SRV 0 0 5060 sip2.mydomain.org
```

```
_sip._udp.mydomain.org 43200 IN SRV 0 0 5060 sip1.mydomain.org
```

```
_sip._udp.mydomain.org 43200 IN SRV 0 0 5060 sip2.mydomain.org
```

```
;
```

```
mydomain.org 43200 IN NAPTR 0 0 "s" "SIPS+D2T" "" _sips._tcp.mydomain.org
```

```
mydomain.org 43200 IN NAPTR 1 0 "s" "SIP+D2U" "" _sip._udp.mydomain.org
```

```
mydomain.org 43200 IN NAPTR 2 0 "s" "SIP+D2U" "" _sip._udp.mydomain.org
```

```
;
```

NB: essendo necessari 3 entry per i NAPTR ma nn specificato il servizio su TCP (avrebbe avuto la sigla SIP+D2T), ho ridonato il record su UDP (quello con order =2).

dovrebbe essere cosi!? Jonathan 21/06/10 13.54

si, l'esempio che guardavo l'ha omesso Jonathan 22/06/10 17.01

(Compito Sconosciuto)

(1) Gli studenti del politecnico di Torino possono da un qualsiasi accesso internet, collegarsi alla rete di Ateneo tramite una VPN di accesso terminata sul VPN gateway avente indirizzo 130.192.18.253 e utilizzare tutti i servizi normalmente disponibili su tale rete. Si descriva schematicamente, fornendo le informazioni essenziali legate alla realizzazione e funzionamento delle VPN contenute nelle varie intestazioni, un pacchetto in transito sulla rete Internet verso la stazione di uno studente sulla quale un browser web stia scaricando una pagina da un server web di Ateneo, avente indirizzo ip 130.192.55.2 . Si indichino le assunzioni fatte riguardo alle informazioni non esplicitamente fornite nel testo della domanda.

Indirizzo mittente esterno 130.192.18.254

Indirizzo destinazione esterno : x.y.w.z (ISP)

Indirizzo mittente interno : 130.192.a.b (indirizzo aziendale client)

Indirizzo destinazione interno : 130.192.55.240 (2)

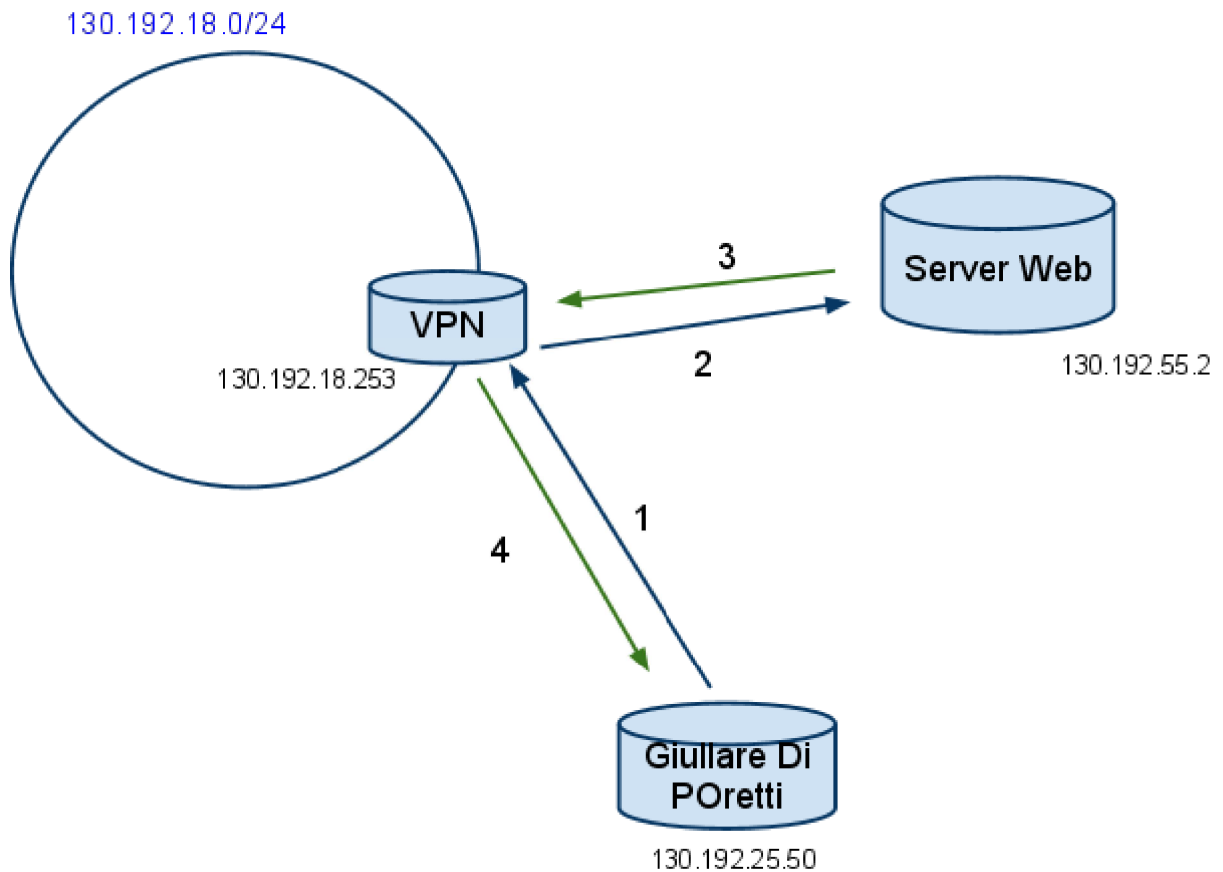
IP in IP con qualche tipo di imbustamento (GRE, PPP, ecc) – 1

(RISP)

Supponiamo:

- accesso centralizzato
- Giullare di Poretti 130.192.25.50
- indirizzo di Giullare nella VPN: 192.168.18.100
- la maschera di rete è /24
- i cerchi grandi indicano le sottoreti

Schema della Rete:



Nel caso che "Giuggiolò" spedisca una richiesta HTTP GET al server web, i pacchetti saranno:

1) L2 | IP | GRE | PPP | IP | TCP | HTTP (il get è un messaggio senza corpo)

- o IP src: 130.192.25.50 dst: 130.192.18.253
- o GRE: PPP
- o PPP: IP
- o IP src: 130.192.18.100 dst: 130.192.55.2

2) L2 | IP | TCP | HTTP (il get è un messaggio senza corpo)

- o IP src: 130.192.18.100 dst: 130.192.55.2

IL VPN GW ha tolto l'intestazione più esterna utile per attraversare il tunnel VPN

3) L2 | IP | TCP | HTTP | DATI

- o IP src: 130.192.55.2 dst: 192.130.18.100

4) L2 | IP | GRE | PPP | IP | TCP | HTTP | DATI

- IP src: 130.192.18.253 dst: 130.192.25.50
- GRE: PPP
- PPP: IP

- **IP** src: 130.192.55.2 dst: 192.130.18.100

Jonathan feat. ROBBERTO aka Batman e Robin hau ahuahauhauhauhauhaauh auah -Luca Landi 22/06/10 18.22 <http://www.youtube.com/watch?v=--mZhgmogPU&feature=related>
22/06/10 18.20 ...nn direi proprio semmai ci manca catzwoman e poison Ivy

(2) Descrivere la modalità con la quale una stazione Ipv6 è in grado di scoprire l'indirizzo MAC di un'altra stazione Ipv6.-----

(RISP) Supponiamo che la rete sia 2001:760:400:7::/64 e conosciamo l'IP, ma non il MAC dell'host da ricercare (supponiamo sia AA-BB-CC-DD-EE-FF). La stazione A, se vuole conoscere il MAC di B, fa partire una fase di Neighbor Discovery (l'equivalente all'ARP in IPv4), che consiste in un pacchetto Neighbor Solicitation che ha come

- MAC sorgente = MAC di A
- MAC destinazione = il MAC_solicited_node di B
- IPv6 src = IPv6 di A
- IPv6 dest. = solicited_node di B

Si ricavano gli indirizzi (inserendo alla fine, i 24 bit dell'indirizzo Ipv6 di B), quindi l'indirizzo multicast solicited_node di B è 33-33-FF-DD-EE-FF, mentre l'IPv6 multicast solicited_node di B è FF02::1:FF:DD:EE:FF.

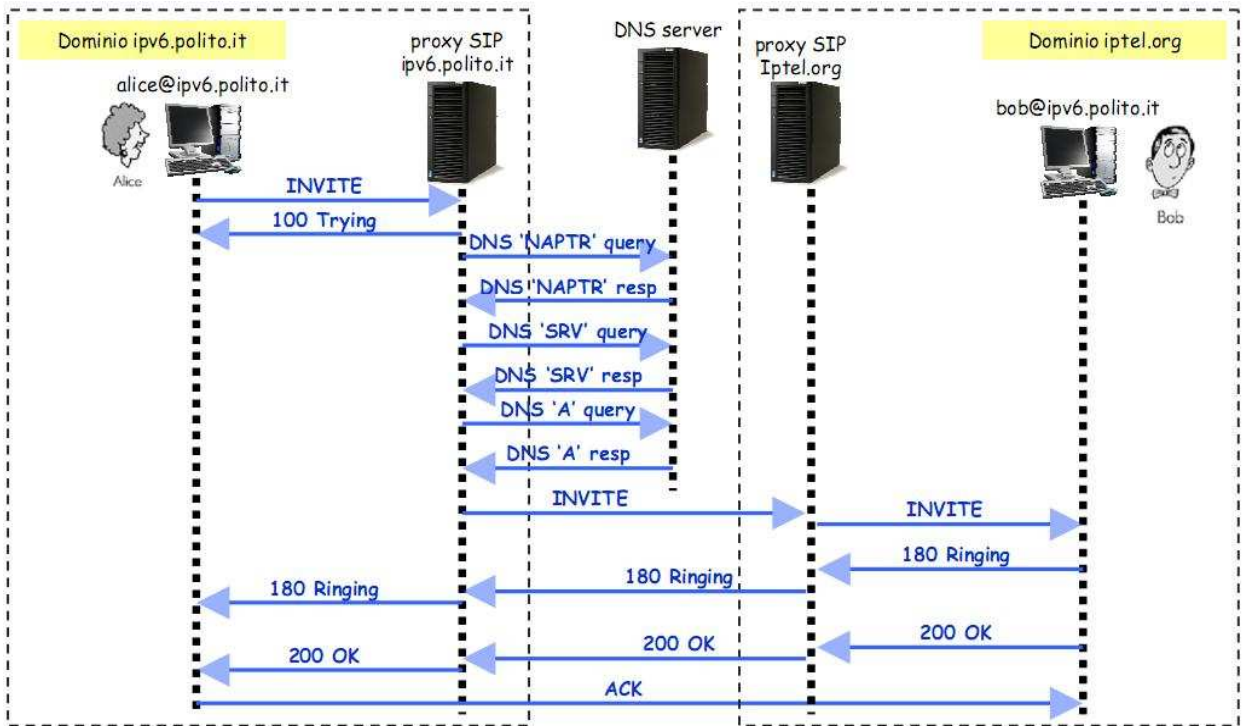
(Nota: la parte sottolineata si riferisce agli ultimi 24 bit dell'IPv6 relativo al MAC da cercare)

Alla fine, posso creare e inoltrare sulla rete il pacchetto di Neighbor Solicitation, così che, solo la stazione che ha quel MAC address lo riceverà rispondendo con un pacchetto unicast Neighbor Advertisement, con il suo MAC Address.

(APPROFONDIMENTO): Quindi il neighbor solicitation viene usato per verificare che il proprio indirizzo IP sia unico, e in quel caso ci si aspetta che non ci sia nessuna risposta oppure per scoprire qual'è l'indirizzo MAC associato a un indirizzo IP che si trova nella stessa sottorete, compreso ad esempio l'indirizzo MAC del router)

(3) Uno UA SIP vuole effettuare la chiamata verso un altro UA di un differente dominio, mostrare la sequenza di operazioni necessaria ad aprire la connessione.-----

(RISP)



Supposto che il Record Routing sia disabilitato dai sip proxy. (Altrimenti l'ack sarebbe dovuto passare dai 2 sip proxy)

1. Una stazione ha 2 IP , perché?-----

(RISP) Rispetto all'IPv4, una stazione Ipv6 ha due indirizzi IP, l'indirizzo Link-Local e l'indirizzo Site/Global. L'indirizzo Link-Local, che comincia per FE80, è un indirizzo privato, mentre, l'indirizzo Global, che di solito inizia con 2001, e' accessibile a tutta la rete internet. Gli indirizzi sono strutturati a 128 bit, cioè 8 blocchi di 16 bit scritti in esadecimale. (es. 2001:BA98:0876:45FA:0562:CDAF:3DAF:BB01), con Ipv6 inoltre, scompare il concetto di Netmask, sostituito da quello di Prefix. Ad esempio FEDC:0123:8700::/N dove N è la lunghezza in bit del prefix. Inoltre, l'interfaccia può avere più indirizzi i quali possono essere usati per generare connessioni differenti, la modalità di generazione è default a partire dal MAC o privacy utilizzando numeri random e funzioni di hash come base per la generazione dell'indirizzo finale (RFC 4941). Jonathan 21/06/10 16.07

2. Protocolli su cui sono basate le reti VPN e MPLS

(RISP)

VPN

- Access VPN
 - o PPTP
 - o L2TP
- Site-to-site VPN

- o GRE
- o IPsec
- o **MPLS**
 - BGP (protocollo per le VPN)

MPLS

- Label distribution
 - o LDP
 - o PIM
 - o RSVP / CR-LDP
 - o BGP
- Routing
 - o OSPF
 - o IS-IS
 - o BGP-4
 - o IGRP
 - o RIP (non più utilizzato)

3. BGP

(RISP)

Il BGP (Border Gateway Protocol) è un protocollo di routing inter-AS utilizzato per connettere tra loro più router gateway che appartengono a sistemi autonomi AS (Autonomous System) distinti fra loro.

BGP, attraverso una tabella di reti IP, gestisce le informazioni sulla raggiungibilità delle diverse reti tra più AS.

E' un protocollo a indicazione di percorso (path vector) che effettua il routing basandosi sulle regole determinate da ciascuna rete.

BGP supporta il routing indipendente dalle classi (Classless InterDomain Routing) e aggrega gli instradamenti per diminuire la dimensione delle tabelle.

Il BGP è stato ideato per sostituire il protocollo EGP (ancora legato alla filosofia di "internet centralizzato" dipendente dalla rete NSFNET) e rendere internet un sistema decentralizzato.

Oggi gli ISP sono obbligati a utilizzare BGP per stabilire i criteri di routing e lo rendono uno dei più importanti protocolli di internet.

4. Perché Skype ha

successo?-----

(RISP)

Skype, nonostante i suoi numerosi problemi, derivanti principalmente dal fatto che il codice è chiuso, ed e' difficile capire il suo meccanismo (anche a Run-Time), riscuote un elevato successo per svariati motivi

Principalmente, con Skype, non è necessario avere indirizzi pubblici per fare VoIP. Quindi, i NAT non sono più un problema.

Inoltre, dato che Skype si basa su un modello P2P (come Kazaa), il traffico è distribuito tra i vari nodi, e non è necessario disporre di infrastrutture costose per fare VoIP.

Un ultimo fattore di successo deriva dal fatto che la qualità del servizio (QoS) è un prerequisito non indispensabile (anche se, a volte purtroppo potrebbe capitare di incappare in un SuperNodo lento)

Questo successo però, ha reso Skype un buon prodotto a livello consumer, ma in ambito aziendale si preferiscono soluzioni più "aperte", sicure, e gestibili, come SIP.

5. Come fare rete

Voip-----

(RISP)

(tipo linea, deve essere dedicata, con una percentuale di traffico)

6. Cos'è l' LSP ?

(RISP)

Un LSP (Label Switched Path) è un cammino attraverso una rete MPLS gestita da un protocollo di Label Distribution.

Il path è basato sui criteri FEC (Forwarding Equivalence Class):

- a. il LER (Label Edge Router) decide quale label attribuire ad un pacchetto in base al FEC appropriato
- b. il LSR (Label Switching Router) successivo sostituisce la label del pacchetto con un'altra più appropriata e inoltra il pacchetto al router che viene dopo
- c. il LSR (Label Switching Router) successivo sostituisce...
- d. l'ultimo router del path rimuove la label dal pacchetto e lo inoltra basandosi sull'header del livello successivo (ad esempio IPv4).

Gli LSP sono definiti come tunnel MPLS poichè sono opachi rispetto agli altri livelli.

Sono però unidirezionali e, poichè la comunicazione bidirezionale è spesso necessaria, viene gestito un secondo LSP che va nella direzione opposta rispetto al primo.

7. Cos'è una rete frame

relay?-----

E' uno standard d'interfaccia DCE-DTE (Data Communication Equipment, Data Terminal Equipment), mette in comunicazione reti dati con reti LAN. Necessita di alte velocità di lavoro. E' concepita su L2, dove effettua la commutazione di Frame. Prevede un meccanismo di correzione degli errori tramite ritrasmissione ma solo sull'edge (frontiera), è soggetto a jitter quindi non va bene per trasportare voce. Le dispense parlano anche di Committed Information Rate $CIR = Bc/Tc$ ma non so che è.

Jonathan 22/06/10 17.15

Il CIR sarebbe un valore entro il quale si possono trasmettere fino a Bc bit alla velocità del collegamento fisico in ogni intervallo di tempo di durata Tc (per non intasare la rete)

Bc = numero di bit che introduco in un lasso di tempo Tc (Committed Burst Time)

$Tc = Bc/CIR$ --> intervallo in cui il CIR è verificato

Bc e Tc sono numeri che impongono all'inizio dell'istanzaiozione. Il traffico che eccede la soglia di CIR è un potenziale candidato ad essere marcato come non conforme alla rete, e quindi non garantito

8. Commutazione di circuito-----

(RISP)

Configurazione di rete telefonica standard, pensata e progettata per il trasporto della voce. Prevede che gli switch interni alla rete commutino per creare un "circuito fisico" tra parte chiamante e parte chiamata. Ad ogni circuito viene garantita una banda di 64kbps bidirezionale .

Dato che ha una banda costante e un collegamento diretto, la qualità è garantita per tutta la durata della comunicazione, inoltre, utilizza il codec PCM64 (quindi non è possibile aumentare la qualità ad esempio, utilizzando compressione).

9. Differenza tra ipv4 e ipv6-----

Il cambiamento più rilevante nel passaggio dall' IPv4 all' IPv6 è la lunghezza dell'indirizzo di rete. L'indirizzo IPv6, è lungo 128 bit, cioè 32 cifre esadecimali, che sono normalmente utilizzate nella scrittura dell'indirizzo come descritto più avanti.

La seconda grossa differenza fra l'indirizzamento IPv4 e quello IPv6 è che le vecchie classi di indirizzo IPv4 erano basate sul concetto di rete e sottorete, mentre in IPv6 questa suddivisione è lasciata all'utente finale dell'indirizzo (si presume che diverrà prassi normale assegnare non un singolo indirizzo

agli utenti IPv6 ma intere sottoclassi). I primi 10 bit dell'indirizzo IPv6 descrivono genericamente il tipo di computer e l'uso che questo fa della connessione (telefono VoIP, PDA, data server, telefonia mobile ecc.)

Questa caratteristica svincola virtualmente il protocollo IPv6 dalla topologia della rete fisica, permettendo per esempio di avere lo stesso indirizzo IPv6 a prescindere dal particolare internet provider che si sta usando (il cosiddetto *IP personale*), rendendo l'indirizzo IPv6 simile a un numero di telefono. Queste nuove caratteristiche però complicano il routing IPv6, che deve tenere conto di mappe di instradamento più complesse rispetto all'IPv4; proprio le nuove proprietà dell'indirizzamento sono anche i potenziali talloni d'Achille del protocollo.

10. Come fa una stazione con autoconfigurazione stateless a connettersi-----

--

(RISP) Una stazione con autoconfigurazione STATELESS, si genera un indirizzo Link-Local. Successivamente effettua il probing, per verificare che esso sia l'unico presente nella rete, tramite protocollo Duplicate Address Detection.

Questo protocollo, consiste nell'inviare in MULTICAST un pacchetto ICMPv6 Neighbor Solicitation così costruito.

Source: viene messo :: (non sa ancora se il suo indirizzo è valido)

Dest.: Multicast solicited node, e infine nel campo

ICMPv6 Info -> Target Info : Indirizzo Link Local da verificare

L'host aspetta un po', e se nessuno risponde al suo Neighbor Solicitation, significa che il Link Local che si è generato è valido, quindi invia un pacchetto "ICMPv6 Multicast Listener Report" in MULTICAST per comunicare la sua configurazione di Link Local Address (Questa volta, come IPv6 source, metterà il suo indirizzo Link Local appena generato).

L'host può quindi parlare con TUTTE le macchine della propria LAN senza l'intervento di un ROUTER. Se esiste un router, esso manderà un messaggio di Router Advertisement.

In un pacchetto di Router Advertisement sono presenti:

- Source: Indirizzo LinkLocal del router
- Dest: FF02::1 (multicast che indica tutti gli host)
- Info: Contiene il Prefisso annunciato, il Valid Lifetime, e il MAC del Router (che i vari host salvano nella propria cache).

L'host rimane perennemente in ascolto dei messaggi dei router, in modo da poter configurare un host a runtime, e favorire il renumbering (ad es. per passare da indirizzo sitelocal a uno global)

(**APPROFONDIMENTO**: L'autoconf. STATEFUL(poco usata) invece, si basa su DHCPv6, ogni stazione viene munita di un ID in modo da ottenere sempre lo stesso indirizzo dal DHCP anche se si cambia scheda di rete)

11. 2 server voip (stesso dominio) equivalenti cosa scrive nel DNS ?----

12. 2 reti VPN senza e con accesso tunneled-----

13. telefonia su ip che protocolli prevede?-----

(RISP)

Prevede due protocolli:

- **H.323**: Protocollo di derivazione telefonica (per sistemi di comunicazione multimediali a pacchetto). E' nato come protocollo per estendere le videoconferenze alle LAN. Si ha un Gatekeeper principale, che e' l'entità predisposta alla segnalazione. Non è obbligatorio ma fornisce la maggior parte dei servizi (autenticazione, localizzazione). La codifica dei messaggi di H.323 e' basata su ASN.1.

E' un protocollo molto diffuso, tuttavia, data l'elevata complessità, si sta abbandonando questo protocollo a favore di SIP.

- **SIP**: Session Initiation Protocol, Protocollo di derivazione dati definito in ambito internet. Si utilizza un Server SIP per fornire l'autenticazione.

Molto più semplice rispetto a H.323. Nasce come un protocollo di segnalazione, che ha come scopo l'instaurazione, la modifica e la terminazione di una sessione multimediale/dati.

Il formato dei pacchetti è HTTP-like, e la segnalazione può avvenire tramite TCP, TLS e UDP (anche se TCP non è molto utilizzato).

L'architettura SIP, ha una parte MEDIA identica a H.323(quindi cio' che riguarda RTP, RTCP, e codec audio/video), e inoltre, aggiunge una parte di CONTROLLO, dove ogni componente è indipendente dagli altri.

Nella parte di controllo, importante è il ruolo dell'**SDP** (session description protocol), che, inviato in fase di "INVITE", trasporta diversi parametri utili (es. tipo di media, codec, indirizzi e porte,ecc)

14. Unità minima di trasmissione-----

15. ATM

Asynchronous Transfer Mode (è simile al TDM Time Division Multiplexing ad eccezione che è asincrono e con occupazione di banda statistica, in TDM se un canale nn trasmette, la sua porzione di banda rimane non disponibile ad altri).

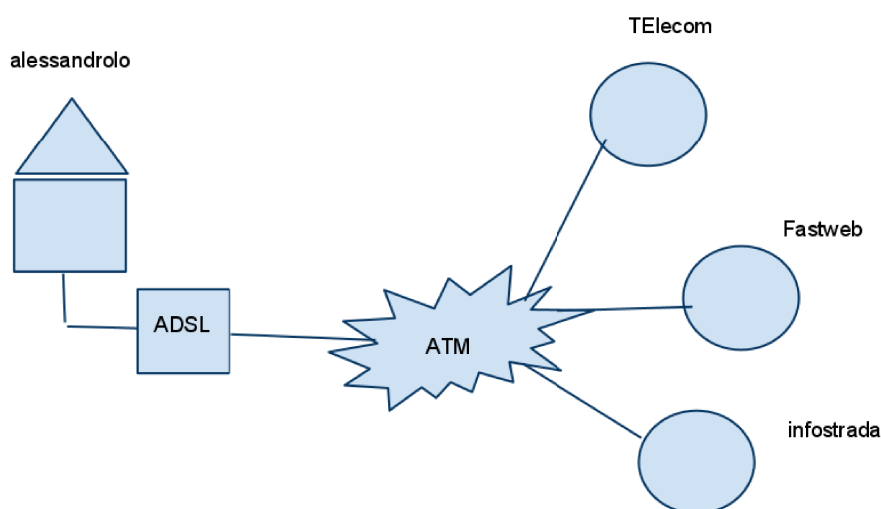
E' basato su circuito virtuale (a velocità costante), è un protocollo quasi morto, la sua banda $\leq 50\text{Mbps}$.

Caratterizzato da segnalazione sofisticata ma permette:

- gestione punto-punto e multipunto,
- l'allocazione della banda in modo dinamica,
- supporta anche bursty-traffic

La commutazione è su cella (pacchetto piccolo) dimensione $53\text{Byte} = 5\text{ header} + 48\text{ carico}$, la lunghezza fissa permette la gestione in hardware (\Rightarrow veloce), ideale per le sue ridotte dimensioni anche per il trasferimento audio/video.

Oggi è utilizzato per connettere l'utente di casa ai GW dei fornitori di internet:



16. MPLS perché ha successo-----

17. Info essenziali rilevate nell'intestazione di pacchetto in transito su una rete internet verso una stazione-----

18. Messaggi che genera un server proxy per instradare una connessione-----

Guarda il trapezoide sopra...

Domande a Risposta Multipla

(Test online disponibile su <http://magnetz.org/tsr/>)

Alcune domande non hanno risposte, se la si conosce, evidenziare la risposta in grassetto, Grazie!

..: IPv6 :..

L'inoltro di pacchetti Ipv6 su una LAN:

Non fa' uso di meccanismi di neighbor discovery in quanto esiste una regola per mappare un qualunque indirizzo Ipv6 in un indirizzo MAC

Non fa uso di meccanismo di neighbor discovery per quanto riguarda l'inoltro di pacchetti Ipv6 multicast e broadcast in quanto esiste una regola per mappare questi indirizzi Ipv6 in un indirizzo MAC

Fa uso di meccanismi di neighbor discovery per tutte le tipologie di indirizzi Ipv6

Non fa uso di meccanismi di neighbor discovery per quanto riguarda l'inoltro di pacchetti Ipv6 multicast in quanto esiste una regola per mappare questi indirizzi Ipv6 in un indirizzo MAC.

Un host IPv6 al reboot, acquisirà il seguente indirizzo:

- Non è possibile sapere con precisione l'indirizzo stesso, dal momento che l'indirizzo IPv6 viene ogni volta rigenerato con un numero casuale per quanto riguarda la parte riservata all'Interface ID
- Un indirizzo FE80::/32

- **Per quanto riguarda l'indirizzo link-local, assumerà lo stesso indirizzo IPv6 che possedeva prima del reboot**
- L'indirizzo dipende interamente dalla configurazione che acquisirà dal suo default router

A differenza della versione 4 dell'IP, la versione 6:

- Non ha una versione dell'ICMP associata.
- Non permette di scoprire l'indirizzo MAC di un'altra stazione, conoscendone l'indirizzo IP
- **Non ha indirizzi broadcast.** yeS Jonathan 20/06/10 18.19
- Non ha un equivalente del campo TTL (time to live)

L'autoconfigurazione stateless in IPv6 richiede:

- Un server DHCPv6 (Dynamic host configuration protocol version 6)
- Un server presente sulla rete locale
- Un server presente sulla rete aziendale (intranet)
- **E' possibile anche se non si è in presenza di server o router**

Un indirizzo link-local:

E' utilizzabile per permettere la comunicazione tra stazioni su link locali (es. Una LAN) in mancanza di altri indirizzi Ipv6

Serve per collegare fisicamente due stazioni su un link locale

E' l'indirizzo utilizzato dalle stazioni su una LAN per scambiarsi i dati

E' utilizzato in tutte le comunicazioni tra stazioni locali

Gli indirizzi Ipv6

Permettono la comunicazione di stazioni Ipv6 con stazioni Ipv4 senza nessun particolare meccanismo aggiuntivo

Mantengono la stessa suddivisione flessibile tra una parte network e una parte host già presente in Ipv4

Sono rigidamente partizionati in una parte network, subnet e host

Sono rigidamente partizionati in una parte network e una parte host.

Lo schema di indirizzamento IPv6:

- Prevede esclusivamente indirizzi assegnati in modo univoco da un ente preposto.
- **Prevede che ogni entità (es. azienda) si faccia assegnare globalmente un insieme di indirizzi, che diventano di sua proprietà a tempo illimitato.**
- Prevede che i primi 64 bit di un indirizzo siano normalmente identificati come il prefisso di rete, almeno sulle LAN. anche secondo me - Jonathan 20/06/10 18.10
- Non prevede l'esistenza di indirizzi di multicast.

...: VPN :...

Lo standard Ipsec viene utilizzato nelle VPN (virtual private network) per

Verificare le informazioni di autenticazione fornite da utenti remoti tramite uno scambio di informazione con un server di autenticazione.

Consentire l'invio di informazioni di autenticazione (per esempio username e password o tramite meccanismi di sfida) da parte degli utenti di una VPN di accesso.

La realizzazione di tunnel attraverso una rete IP pubblica tramite i quali sia possibile trasportare pacchetti verso una rete privata indipendentemente dal piano di indirizzamento utilizzato su tale rete privata.

La creazione automatica di collegamenti cifrati tra le sedi di un'azienda attraverso una rete pubblica, sulla quale la comunicazione è quindi intrinsecamente non sicura.

Cosa contraddistingue una VPN realizzata secondo uno schema Overlay?

Il gestore della rete non è al corrente che si sta realizzando una VPN

Le apparecchiature dell'utente sono le stesse che si userebbero nel caso i vari tronconi di rete aziendale fossero collegati direttamente.

Non è possibile avere comunicazioni riservate.

Non possono essere realizzate senza l'assenso dell'ISP prescelto.

Il protocollo GRE ha lo scopo di.

- Proteggere i pacchetti contro le intercettazioni.
- **Gestire l'incapsulamento di pacchetti da trasportare attraverso un tunnel** GRE è per il routing encapsulation delle vpn - Jonathan 20/06/10 18.10
- Autenticare il mittente dei pacchetti.
- Verificare l'integrità dei pacchetti in arrivo.

Le così dette soluzioni VPN (virtual private network) di accesso o virtual dial-up VPN attualmente più diffuse sono basate su

Connessioni dial-up

Tunneling attraverso una rete IP

Utilizzo di un'infrastruttura di cablaggio esistente per fornire servizi di accesso a larga banda

Nuovi protocolli di linea (livello data-link)

In quale situazione è possibile che un pacchetto abbia due intestazioni IP?

- Il pacchetto ha attraversato un firewall in ingresso.
- Il pacchetto è nella rete pubblica, dopo aver attraversato in uscita un NAT.

- Il pacchetto è nella rete pubblica, dopo aver attraversato in uscita un firewall.
- **Il pacchetto è nella rete pubblica in transito su un tunnel IP che collega due segmenti di una VPN basata su IP.** io confermo, uno per il vpn gateway e l'altro per la destinazione Jonathan 20/06/10 18.18

In una stazione utente collegata ad una VPN con accesso centralizzato, i messaggi diretti a stazioni esterne alla VPN passano attraverso:

- **Il sito della VPN a cui la macchina utente è collegata**
- Non è possibile raggiungere stazioni esterne alla VPN
- Un router specializzato per questi pacchetti.
- Vengono inviati direttamente dalla stazione utente al destinatario esterno.

...: **VoIP/SIP** :...

La telefonia su IP prevede:

- **L'uso di voice gateway per consentire la comunicazione con utenti collegati a reti tradizionali (POTS)**
- L'aggiornamento del cablaggio della rete IP in modo da collegare ogni utente telefonico tramite fibra ottica
- Di dotare il calcolatore di ogni utente di voce su IP di un software di telefonia per comunicare con altri utenti di telefonia su IP e di un telefono tradizionale per comunicare con utenti di telefonia tradizionale
- L'installazione di una rete in tecnologia IP parallela a quella dati, dedicata al trasporto di fonia

La telefonia su IP prevede: (**diverso dal precedente!**)

L'uso di voice gateway per consentire la comunicazione tra telefoni IP collegati in reti fisiche distinte

L'aggiornamento del cablaggio della rete IP in modo da collegare ogni utente telefonico tramite fibra ottica

Protocolli di segnalazione per l'instaurazione delle chiamate e la negoziazione dei loro parametri

Di dotare il calcolatore di ogni utente di voce su IP di un software di telefonia per comunicare con altri utenti di telefonia su IP e di un telefono tradizionale per comunicare con utenti di telefonia tradizionale

Il protocollo SIP:

E' basato su un'architettura distribuita, in cui ogni dominio deve dotarsi di un server che è responsabile dei propri utenti.

E' basato su un architettura rigidamente centralizzata, con un unico server per gestire le comunicazioni.

E' basato su un'architettura gerarchica in cui ogni livello della gerarchia è responsabile di una particolare zona della rete.

E' basato su un architettura peer-to-peer per facilitare la dinamicità degli utenti.

Il protocollo RTP è in grado di:

- Limitare le variazioni di ritardo (jitter) subite dai pacchetti nei router
- Far conoscere ai router il profilo di traffico generato da una stazione
- Riservare risorse di calcolo nei server che condividono i loro processori
- **Incapsulare i dati audio/video con intestazioni contenenti informazioni sulla codifica** Idem con kartofen - Jonathan 20/06/10 18.00

La gestione della qualita' del servizio (QoS) in una rete VoIP:

E' gestita nativamente da SIP:

E' gestita attraverso il protocollo RTCP

Fa parte di una specifica opzionale di SIP (generalmente non implementata)

Non e' gestita da SIP

Il trapezoide SIP:

E' utilizzato prevalentemente per l'invio di messaggi SUBSCRIBE-Notify (e-presence).

E' sostanzialmente obsoleto, dal momento che gran parte delle implementazioni è in grado di utilizzare un meccanismo più efficiente basato sulla triangolazione dei messaggi.

E' il meccanismo standard per l'invio di messaggi di REGISTER.

E' il meccanismo standard utilizzato per il setup di una nuova chiamata.

La principale motivazione per cui un operatore "telefonico" come Skype riesce a fornire un servizio telefonico a prezzi molto bassi:

- **E' dovuto al fatto che le telefonate viaggiano sulla rete IP (ad es. ADSL), i cui costi sono già pagati dall'utente nel momento in cui stipula un contratto "flat" e quindi i pacchetti vocali viaggiano su MySpace Music. Ascolta gratis MP3, guarda le foto e i video musicali virtualmente "gratis" in gran parte del loro percorso**
- E' dovuto al fatto che ha fatto accordi di interconnessione con i Telecom Provider che versano a Skype un compenso in base alla percentuale di traffico generata
- E' dovuto principalmente alla pubblicità che viene offerta insieme al servizio
- E' dovuto al fatto di possedere solamente un infrastruttura IP su lunga distanza lasciando l'infrastruttura d'accesso (molto più costosa a causa della elevata capillarità) a terze parti, con la conseguenza di comprimere di molto i costi

Dovendo trasportare traffico VoIP con garanzie "toll-quality"

- **E' necessario creare una propria rete IP e dare precedenza al traffico voce. Inoltre, è necessario assicurarsi che la percentuale di traffico voce non superi una data soglia**
- E' possibile utilizzare internet, Skype dimostra che questo approccio funziona decisamente bene.
- E' necessario creare la propria rete IP e dare precedenza al traffico voce
- E' necessario creare una rete IP dedicata, in cui cioè non vi sia traffico dati.

I codec specificatamente ingegnerizzati per la codifica della voce:

- Tendono a creare pacchetti grossi per massimizzare l'efficienza della rete
- **Tendono a creare pacchetti piccoli per minimizzare il ritardo end-to-end** confermate? Jonathan 20/06/10 18.10
- Aggiungono sempre dei bit di ridondanza per ridurre i danni in caso di perdita di pacchetti
- Sono in grado di operare anche con sorgenti VoIP diverse (ad es. modem o FAX)

Le funzioni di un voice gateway (o VoIP gateway) includono:

- Inoltare pacchetti IP tra una rete pubblica IP ed una rete aziendale IP (intranet)
- **Tradurre in flussi vocali generati su una rete a pacchetto (ad es tramite SIP o H.323) in telefonate su una rete telefonica tradizionale (plain old telephone system - POTS)**
- Cifrare un segnale vocale proveniente da una rete telefonica tradizionale prima dell'inoltro sulla rete Internet - Notoriamente poco sicura - In modo che tale segnale non possa essere compreso se intercettato
- Tradurre la segnalazione telefonica SS#7 in segnalazione SIP

Nel caso in cui un utente domestico voglia sottoscrivere un servizio telefonico VoIP basato su SIP:

Deve necessariamente sottoscrivere il servizio dallo stesso provider che gli fornisce la connettività di rete (es. Connessione ADSL)
Può sottoscrivere il servizio da un qualunque fornitore di telefonia VoIP, fatto salvo una comunicazione esplicita al provider che gli fornisce la connettività di rete.

Può sottoscrivere il servizio da un qualunque fornitore di telefonia VoIP

Può usufruire del servizio VoIP solamente all'interno della stessa rete del provider che gli fornisce la connettività di rete.

...: MPLS/ATM ...

Utilizzando l'algoritmo del secchiello a gettoni (o secchio bucato) di capacita' **B** token e velocità di riempimento **r** token/s, si riesce a controllare:

- Che il tempo di attraversamento non superi rB secondi
- **Il numero di pacchetti al secondo immessi non superi r , ed il massimo burst non superi B .** confermate? Jonathan 20/06/10 18.20
- Il numero di pacchetti al secondo immessi non superi **B** , ed il massimo burst non superi **r** .
- Il jitter non superi **B/r**

Le reti ATM vengono spesso utilizzate per:

- Interconnettere diversi tronconi di LAN all'interno dello stesso campus.
- Realizzare delle VLAN.
- **Interconnettere le terminazioni dei canali ADSL con la rete del fornitore di servizi prescelto dall'utente.**
- Realizzare sistemi VoIP.

Per realizzare una VPN usando MPLS, al livello 3 secondo il modello peer, è possibile:

- **Utilizzare una versione opportunamente modificata del BGP**
- Utilizzare una versione opportunamente modificata del TCP
- Utilizzare una versione opportunamente modificata del RIP
- Utilizzare una versione opportunamente modificata del RTP

Gli LSP (label switched path) nell'architettura MPLS (multi-protocol label switching)

Rappresentano percorsi alternativi mantenuti nella tabella di un router per l'inoltro di pacchetti verso una destinazione

Vengono scambiati dai router per costruire una mappa della rete

Costituiscono il percorso più breve verso una destinazione

Vengono creati (set up) per il trasporto di pacchetti appartenenti ad una classe di equivalenza di inoltro (forwarding equivalence class, FEC)

Nel meccanismo con secchiello di gettoni, quale è il significato dei parametri ?

La capacità del secchiello è legata al massimo burst e il ritmo di riempimento è legato alla velocità massima di introduzione dati sul lungo periodo

La capacita' del secchiello è legata alla massima velocità di introduzione dati sul lungo termine, mentre il ritmo di riempimento è legato al massimo burst

Il ritmo di riempimento è legato alla velocità massima di introduzione dati sul lungo periodo e la capacità limita il jitter
Il ritmo di riempimento serve a limitare il jitter, mentre la capacità serve per limitare il tempo di attraversamento

L'importanza di MPLS (multi protocol label switching) nelle reti odierne e future deriva dalla possibilità di:

Trasportare efficientemente pacchetti IP sulle reti ATM

Collegare ad alta velocità i server ai loro dischi

Realizzare facilmente ed efficacemente ingegnerizzazione del traffico (traffic engineering)

Realizzare apparati in grado di operare senza bisogno di configurazione

Nel MPLS, quale tipo di manipolazione del label può avvenire in un singolo router?

Non è possibile manipolare il contenuto del label

Si può solo aggiungere o togliere un label

Si può aggiungere un label, togliere un label o modificare il label, a seconda del tipo di router.

Si può solo modificare il contenuto del label.

La combinazione di meccanismi di secchiello dei token (o secchio bucato) e Weighted Fair Queueing (WFQ) serve a garantire:

Un tempo di attraversamento massimo di un router

Un tempo di attraversamento massimo di un NAT

Una banda massima per ogni flusso di pacchetti

Un burst massimo di pacchetti consecutivi, per ciascun flusso.

In una rete frame relay la minima unità di trasmissione è

- La cella da 53 bytes è quella di ATM
- **L'unità di trasmissione del livello 2** confermate? Jonathan 20/06/10 18.10
- Il circuito virtuale
- Il pacchetto IP

Il trasporto di pacchetti IP su reti ATM

E' attualmente utilizzato, sebbene in via di "estinzione", sulle dorsali geografiche degli operatori.

Non e' possibile

E' indispensabile per il trasporto di traffico real-time (per esempio video) su IP

E' considerato una soluzione ottimale il cui utilizzo è in rapida crescita.

Gli algoritmi di scheduling delle code vengono utilizzati:

Nei router di accesso, per assicurarsi che il traffico generato da un utente sia conforme al profilo di traffico contrattato con il proprio service provider.
Nei firewall, per ritardare i pacchetti che entrano in una rete aziendale provenendo dalla rete internet con lo scopo di impedire alcuni tipi di attacchi alla sicurezza

Nei router, per decidere quale sia l'ordine con cui debbano essere trasmessi i pacchetti in attesa ad una interfaccia.

Nei router per schedulare opportunamente l'elenco dei comandi di configurazione impartiti dall'utente in modo da minimizzare il disservizio causato dal tempo necessario per l'applicazione delle modifiche

Il sistema Differentiated Services si distingue dal sistema Integrated Services perchè:

Non dà garanzie assolute circa la qualità del servizio

Gestisce la trasmissione di dati audio/video, tenendo conto delle esigenze di real-time

Permette di raggiungere velocità di trasmissione più elevate.

Può essere realizzato senza cambiare i protocolli installati sui router

DOMANDE DEL 23 GIUGNO *jonathan filippini 5/7/10 11.10*

1)

Nel meccanismo del secchiello a gettoni si riesce a controllare:

- Il tempo di attraversamento massimo di un router.
- La gestione interna delle code con WFQ.
- La velocità minima di immissione dei dati._

IL burst size massimo e la velocità media di immissione dei dati.

2)

Nell'architettura DiffServ, il PHB permette di:

Trattare in modo differenziato le varie classi di servizio.

- Tenere sotto controllo il tempo di attraversamento massimo di singolo router per ciascun flusso che lo attraversa.

Fornire la garanzia end-to-end della QoS richiesta da ciascun flusso.

Garantire la QoS richiesta da ciascun flusso che lo attraversa un router.

3)

L'algoritmo RED (Random Early Access):

- Gestisce le code interne dei router trasmettendo a rotazione pacchetti delle varie code.
- Permette la marcatura in ingresso di traffici appartenenti a diverse classi_

Gestisce le code interne dei router, iniziando a scartare i pacchetti con probabilità crescente quando la coda raggiunge una lunghezza minima.

Permette il controllo del massimo burst size.

4)

La telefonia su IP prevede:

L'uso di voice gateway per consentire la comunicazione con utenti collegati a reti tradizionali (POTS).

- L'aggiornamento del cablaggio della rete IP in modo da collegare ogni utente telefonico tramite fibra ottica._

Di dotare il calcolatore di ogni utente di voce su IP di un software di telefonia per comunicare con altri utenti di telefonia su IP e di un telefono tradizionale per comunicare con utenti di telefonia tradizionale.

- il protocollo SIP.

5)

La telefonia su IP prevede:

- Una volta iniziata la trasmissione del flusso audio/video, non è più possibile cambiare la codifica_

é possibile cambiare la codifica, quando si effettua una opportuna segnalazione di controllo utilizzando RTCP.

- **é possibile cambiare la codifica ad ogni pacchetto inviato.**
- è possibile cambiare la codifica, solo se si sta utilizzando un RTP Mixer.

6)

La mobilità dell'utente viene trattata nel protocollo SIP?

- Non viene trattata_

Si, all'utente non viene imposta nessuna limitazione sulla mobilità.

- Si, a patto però che l'utente si ricollegi sempre con un indirizzo IP interno allo stesso provider.
- **Si, a patto però che l'utente non cambi indirizzo IP durante una sessione SIP.**

7)

In un sistema VOIP basato su SIP, cosa può avvenire se effettuo una chiamata verso un destinatario non collegato a internet

- **Si può chiedere di essere avvertiti quando l'utente desiderato ritorna ad essere noto al sistema.**
- Si può solo tornare a provare più tardi.

- Si può essere avvertiti dell'apparizione dell'utente desiderato, solo se entrambi siamo nello stesso dominio SIP (abbiamo lo stesso operatore).
- Si può essere avvertiti dell'apparizione dell'utente desiderato, solo se lo stesso si ricollega da uno degli indirizzi IP noti al dominio SIP

8)

L'architettura MPLS (Multi Protocol label Switching) è caratterizzata da

- Un supporto particolarmente evoluto per fornire servizi a qualità garantita
- **Un diverso meccanismo (rispetto all'IP puro) per decidere l'interfaccia di uscita verso cui un pacchetto debba essere inoltrato**
- Protocolli di routing particolarmente veloci ad aggiornare le tabelle di routing in seguito a cambiamenti topologici in modo da recuperare molto velocemente i guasti.
- Terminali di rete intelligenti in grado di personalizzare i servizi ricevuti dalla rete.

9)

Gli LSP (Label Switch Path) nell'architettura MPLS (multi protocol label switching)

- Sono ottenuti riservando risorse nei nodi di rete in modo da garantire opportuna qualità del servizio alle applicazioni che li hanno creati._

Costituiscono il percorso più breve verso una destinazione.

- Vengono creati (Set-Up) dalle applicazioni per il trasporto di pacchetti appartenenti ad una classe di equivalenza di inoltro (Forwarding Equivalence Class FEC)
- **Vengono creati dai nodi di rete che si accordano sulle etichette da utilizzare per i pacchetti appartenenti ad una classe di equivalenza di inoltro (Forwarding Equivalence Class FEC)**

10)

Le soluzioni di VPN (virtual private network) di livello 3 attraverso una dorsale MPLS sono caratterizzate da:

- Livelli particolarmente alti di sicurezza grazie all'utilizzo di tecniche crittografiche
- **Buon livello di automatizzazione e integrazione tra la dorsale pubblica e le reti private.**
- Meccanismi di tunnelling di livello 3, ovvero all'interno di pacchetti IP.

- Gestione diretta da parte dell'utente, senza intervento dell'operatore.

11)

Il protocollo GRE serve per:

- **Incapsulare i pacchetti in altre intestazioni IP, in modo da poterle inviare su un tunnel**
- Garantire la riservatezza delle comunicazioni.
- Garantire l'autenticità dei pacchetti.
- Riservare della banda per la comunicazione.

12)

La caratteristica di una VPN di accesso centralizzata è che:

- **Il traffico non diretto alla VPN viene fatto passare comunque attraverso il VPN Gateway.**
- L'autenticazione dell'utente per l'accesso alla VPN viene delegato all'ISP.
- Il traffico non diretto alla VPN non è costretto a passare attraverso il VPN Gateway
- L'autenticazione dell'utente non viene fatta dal VPN Gateway

13)

Una delle caratteristiche principali delle linee Sonet/SDH è che:

- L'allocazione degli slot di trasmissione avviene secondo le esigenze del momento delle varie stazioni.
- **Le varie frequenze di trasmissione sono una multipla dell'altra.**
- La trasmissione avviene previa esecuzione di un meccanismo di contesa del canale che stabilisce chi ha diritto di trasmettere
- La trasmissione avviene a divisione di lunghezza d'onda

14)

In una rete Frame Relay, la minima unità di trasmissione è:

- **La trama del livello 2.**
- Il circuito virtuale
- Il pacchetto IP
- La cella da 53 bytes

15)

Nel protocollo IPV6:

- I protocolli di routing (ad esempio il formato dei pacchetti) non cambiano rispetto ad IPV4_

Il protocollo ARP viene inglobato in ICMPv6, ma mantiene esattamente lo stesso schema di funzionamento (richiesta broadcast, risposta unicast) precedente.

- **Esiste la possibilità, per una stazione su un segmento di rete, di autoconfigurarsi attraverso l'ascolto di messaggi di Router Advertisement.**
- Come in IPv4, IPv6 non prevede meccanismi di riconfigurazione dei router.

16)

Nell'IPv6 cosa sparisce dalle intestazioni, rispetto a IPv4?

- Il tempo di del pacchetto_

Gli indirizzi mittente e destinatario

- l'indicazione su quale sia l'intestazione successiva
- **Il checksum dell'intestazione**

17)

Lo schema di indirizzamento IPV6:

- Prevede esclusivamente indirizzi assegnati in modo univoco da un ente preposto._

Prevede che ogni entità (es. azienda) si faccia assegnare globalmente un insieme di indirizzi, che diventano di sua proprietà a tempo illimitato.

- **Prevede che i primi 64 bit di un indirizzo siano normalmente identificati come il prefisso di rete, almeno sulle LAN.**
- Non prevede l'esistenza di indirizzi multicast.

18)

Gli indirizzi Link-local

- Sono validi all'interno di una organizzazione che li può utilizzare per assegnare indirizzi alle macchine nelle varie sottoreti della propria internet (sono gli omologhi degli indirizzi privati di IPv4)_

Non possono essere assegnati ai router

- **Ok**
- ...

Domande risposta multipla con risposte (brevi)

IPv6: L'inoltro di pacchetti Ipv6 su una LAN:	SIP/VOIP Il profitto di un operatore telefonico come Skype:
--	--

Non fa uso di meccanismi di neighbor discovery per quanto riguarda l'inoltro di pacchetti Ipv6 multicast in quanto esiste una regola per mappare questi indirizzi Ipv6 in un indirizzo MAC.

Gli indirizzi Ipv6

Mantengono la stessa suddivisione flessibile...

Il protocollo Ipv6 prevede che l'intestazione:

Sia costituita ...

L'autoconfigurazione STATELESS:

Utilizza ...

L'autoconfigurazione STATELESS:

(LINK LOCAL) ...

Gli indirizzi Link-Local:

Sono normalmente ...

Un indirizzo link-local

E' utilizzabile per permettere ...

Lo schema di indirizzamento Ipv6:

Prevede una ...

L'inoltro di pacchetti Ipv6 su una LAN:

Non fa' uso di meccanismi di neighbor discovery per quanto riguarda l'inoltro di pacchetti Ipv6 multicast in quanto..

Nel protocollo Ipv6:

esiste la possibilità...

VPN

..VPN secondo uno schema di overlay?

Gestore della rete non è al corrente...

Lo standard Ipsec viene utilizzato:

La creazione automatica...

Gli algoritmi di scheduling sono usati:

E' dovuto al fatto che le telefonate viaggiano su IP ...

Il trapezoide SIP:

E' il meccanismo standard utilizzato per il setup...

L'utilizzo di rete FR per il trasporto dei pacchetti IP è vantaggioso:

L'interfacciamento...

Nel momento in cui si progetta una nuova rete IP con capacità di fornire servizi integrati DATI e voce è fortemente consigliato privilegiare l'implementazione di:

meccanismi in grado di offrire un ritardo basso di pacchetti voce...

Le funzioni di un voice gateway includono:

Tradurre richieste di connessione generate tramite SIP H.323

La gestione della qualità del servizio in rete VoIP:

Non è gestita da SIP

Secondo la visione dello Standard SIP, la localizzazione di un utente di un pacchetto INVITE... secondo i seguenti Passi:

inoltro del pacchetto di INVITE al proxy server -> quindi inoltra il pacchetto al Proxy server ...

Le funzioni di un voice gateway includono:

tradurre i flussi vocali...

Le reti private virtuali vengono utilizzate per :

trasportare ...

Nel caso in cui un utente domestico voglia sottoscrivere un servizio ... Voip...:

Può sottoscrivere il servizio da un qualunque ...

MPLS

Gli LSP nell'architettura MPLS

<p>Nei router per decidere...</p> <p>Il protocollo SIP:</p> <p>E' un protocollo di segnalazione, controllo chiamate</p> <p>Il protocollo SIP:</p> <p>E' basato su un architettura distribuita.</p> <p>Il protocollo RTP:</p> <p>Per portare...</p> <p>Le cosiddette soluzioni di VPN di accesso o virtual VPN:</p> <p>...tunneling ...</p> <p>Il trasporto di pacchetti IP su reti ATM:</p> <p>E' attualmente utilizzato, sebbene in via di estinzione...</p> <p>L'architettura DIFFSERV è caratterizzata da:</p> <p>Un meccanismo per separare...</p> <p>L'architettura MPLS è caratterizzata da:</p> <p>Un diverso ..</p> <p>Le soluzioni di VPN basate su SSL consentono:</p> <p>ad un azienda ...</p>	<p>Vengono creati dai nodi...</p> <p>Il sistema differentiated services si distingue dal integrated service perchè</p> <p>Non dà garanzie assolute circa qualità servizio</p> <p>La combinazione di meccanismi secchiello dei token (o secchio bucato) e WFQ serve a garantire:</p> <p>Un tempo di attraversamento massimo di un router</p> <p>L'importanza di MPLS:</p> <p>..(traffic engineering) ...</p> <p>L'importanza associata alle reti ottiche deriva:</p> <p>Realizzare ...</p> <p>Le reti ottiche si basano sull'utilizzo di:</p> <p>apparati ...</p> <p>Nel caso sia necessario ingegnerizzare una rete con QoS:</p> <p>viene spesso ...</p> <p>Nel MPLS, quale tipo di manipolazione del label può avvenire in un singolo router?</p> <p>Si può aggiungere un label, togliere o modificare ...</p> <p>Nel meccanismo con secchiello di gettoni, quale è il significato dei parametri?</p> <p>La capacità del secchiello è legata al massimo burst...</p>
---	---

IPv6:

L'inoltro di pacchetti Ipv6 su una LAN:

Non fa uso di meccanismi di neighbor discovery per quanto riguarda l'inoltro di pacchetti Ipv6 multicast in quanto esiste una regola per mappare questi indirizzi Ipv6 in un indirizzo MAC.

Gli indirizzi Ipv6

Mantengono la stessa suddivisione flessibile...

Il protocollo Ipv6 prevede che l'intestazione:

Sia costituita ...

L'autoconfigurazione STATELESS:

Utilizza ...

L'autoconfigurazione STATELESS:

(LINK LOCAL) ...

Gli indirizzi Link-Local:

Sono normalmente ...

Un indirizzo link-local

E' utilizzabile per permettere ...

Lo schema di indirizzamento Ipv6:

Prevede una ...

L'inoltro di pacchetti Ipv6 su una LAN:

Non fa' uso di meccanismi di neighbor discovery per quanto riguarda l'inoltro di pacchetti Ipv6 multicast in quanto..

Nel protocollo Ipv6:

esiste la possibilità...

VPN

..VPN secondo uno schema di overlay?

Gestore della rete non è al corrente...

Lo standard Ipsec viene utilizzato:

La creazione automatica...

Gli algoritmi di scheduling sono usati:

Nei router per decidere...

Il protocollo SIP:

E' un protocollo di segnalazione, controllo chiamate

Il protocollo SIP:

E' basato su un architettura distribuita.

Il protocollo RTP:

Per portare...

Le cosiddette soluzioni di VPN di accesso o virtual VPN:

...tunneling ...

Il trasporto di pacchetti IP su reti ATM:

E' attualmente utilizzato, sebbene in via di estinzione...

L'architettura DIFFSERV è caratterizzata da:

Un meccanismo per separare...

L'architettura MPLS è caratterizzata da:

Un diverso ..

Le soluzioni di VPN basate su SSL consentono:

ad un azienda ...

SIP/VOIP

Il profitto di un operatore telefonico come Skype:

E' dovuto al fatto che le telefonate viaggiano su IP ...

Il trapezoide SIP:

E' il meccanismo standard utilizzato per il setup...

L'utilizzo di rete FR per il trasporto dei pacchetti IP è vantaggioso:

L'interfacciamento...

Nel momento in cui si progetta una nuova rete IP con capacità di fornire servizi integrati DATI e voce è fortemente consigliato privilegiare l'implementazione di:

meccanismi in grado di offrire un ritardo basso di pacchetti voce...

Le funzioni di un voice gateway includono:

Tradurre richieste di connessione generate tramite SIP H.323

La gestione della qualità del servizio in rete VoIP:

Non è gestita da SIP

Secondo la visione dello Standard SIP, la localizzazione di un utente di un pacchetto INVITE... secondo i seguenti Passi:

inoltra il pacchetto di INVITE al proxy server -> quindi inoltra il pacchetto al Proxy server ...

Le funzioni di un voice gateway includono:

tradurre i flussi vocali...

Le reti private virtuali vengono utilizzate per :

trasportare ...

Nel caso in cui un utente domestico voglia sottoscrivere un servizio ... Voip...:

Può sottoscrivere il servizio da un qualunque ...

MPLS

Gli LSP nell'architettura MPLS

Vengono creati dai nodi...

Il sistema differentiated services si distingue dal integrated service perchè

Non dà garanzie assolute circa qualità servizio

La combinazione di meccanismi scatchio dei token (o scatchio bucato) e WFQ serve a garantire:

Un tempo di attraversamento massimo di un router

L'importanza di MPLS:

..(traffic engineering) ...

L'importanza associata alle reti ottiche deriva:

Realizzare ...

Le reti ottiche si basano sull'utilizzo di:

apparati ...

Nel caso sia necessario ingegnerizzare una rete con QoS:

viene spesso ...

Nel MPLS, quale tipo di manipolazione del label può avvenire in un singolo router?

Si può aggiungere un label, togliere o modificare ...

Nel meccanismo con secchiello di gettoni, quale è il significato dei parametri?

La capacità del secchiello è legata al massimo burst...