Politecnico di Torino
Laurea Magistrale in Ingegneria Informatica

esercizi d'esame svolti di
Tecnologie e servizi di rete

Autori principali: Lorenzo Liotino, Federico Orta
Docenti: Mario Baldi, Guido Marchetto
Anno accademico: 2014/2015
Versione: 1.5
Data: 24 gennaio 2015

Informazioni su quest'opera

Scopo è stato quello di unificare un unico documento le innumerevoli informazioni in giro per il web, per quanto riguarda i temi d'esame. Si ringrazia il lavoro eseguito dai colleghi negli anni precedenti a quello corrente.
Le risposte che troverai in questa dispensa potrebbero facilitarti nello studio degli argomenti del corso, ma non c'è certezza assoluta circa la correttezza/completezza delle risposte: pertanto, in caso di errori o dubbi non esitate a correggere quanto presente, comunicandomi eventuali cambiamenti per poter offrire un documento più idoneo allo studio di questo interessante corso (mailto:deparrucca89@hotmail.it).
Sono contenute, se non la totalità delle domande degli anni precedenti, la maggior parte di esse (sia a scelta chiusa che a risposta aperta).
Per le prime, alcune potrebbero essere ambigue, per le seconde, sono ancora in fase di svolgimento → alcune già fatte.
Spero in un vostro contributo attivo.
Enjoy!

Sommario

VPN

1. Per realizzare una VPN usando MPLS, al livello 3 secondo il modello peer, è possibile:
A. Utilizzare una versione opportunamente modificata del BGP.
B. Utilizzare una versione opportunamente modificata del TCP.
C. Utilizzare una versione opportunamente modificata del RIP.
D. Utilizzare una versione opportunamente modificata del RTP.

3. Il protocollo GRE ha lo scopo di:
A. Proteggere i pacchetti contro le intercettazioni.
B. Gestire l'incapsulamento di pacchetti da trasportare attraverso un tunnel.
C. Autenticare il mittente dei pacchetti.
D. Verificare l'integrità dei pacchetti in arrivo.

4. Il protocollo GRE serve per:
A. Incapsulare i pacchetti in altre intestazioni IP, in modo da poterle inviare su un tunnel.
B. Garantire la riservatezza delle comunicazioni.
C. Garantire l'autenticità dei pacchetti.
D. Riservare della banda per la comunicazione.

5. Il protocollo PPTP viene utilizzato di solito per:
A. Permettere di creare un tunnel in una VPN di accesso.
B. Permettere di creare un tunnel in una VPN site-to-site di tipo overlay.
C. Permettere di creare un tunnel in una VPN site-to-site di tipo peer.
D. Permettere di creare un tunnel in una VPN di livello 4.

6. In un pacchetto che viaggia su un tunnel GRE, quante intestazioni possono essere presenti?
A. Una sola, altrimenti l'indirizzamento è ambiguo.
B. Due intestazioni, ma quella interna può solo contenere indirizzi privati.
C. Due intestazioni, senza particolari limitazioni.
D. Due intestazioni, ma quella esterna può solo contenere indirizzi privati.

7. Why is it useful to use GRE encapsulation protocol as opposed to IP
A. Because it provides encryption mechanism
B. Because it is possible to encapsulate lower levels protocols (e.g. data link layers) in IP datagrams. 错误
C. Because the resulting packet is shorter.
D. Because is possible to authenticate the sender.

8. In quale situazione è possibile che un pacchetto abbia due intestazioni IP?
A. Il pacchetto ha attraversato un firewall in ingresso.
B. Il pacchetto è nella rete pubblica, dopo aver attraversato in uscita un NAT.
C. Il pacchetto è nella rete pubblica, dopo aver attraversato in uscita un firewall.
D. Il pacchetto è nella rete pubblica in transito su un tunnel IP che collega due segmenti di una VPN basata su IP.

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

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

10. La caratteristica di una VPN di accesso centralizzata è che
A. Il traffico non diretto alla VPN viene fatto passare comunque attraverso il VPN gateway.
B. L'autenticazione dell'utente per l'accesso alla VPN viene delegato all'ISP.
C. Il traffico non diretto alla VPN non è costretto a passare attraverso il VPN gateway.
D. L'autenticazione dell'utente non viene fatta dal VPN gateway.

14. Le soluzioni di VPN (virtual private network) di livello 3 attraverso una dorsale MPLS sono caratterizzate da
A. Livelli particolarmente alti di sicurezza grazie all'utilizzo di tecniche crittografiche.
B. Buon livello di automatizzazione e integrazione tra la dorsale pubblica e le reti private.
C. Meccanismi di tunneling di livello 3, ovvero all'interno di pacchetti IP.
D. Gestione diretta da parte dell'utente, senza intervento dell'operatore.

15. What is a feature of a layer 3 VPN (virtual private network) implemented using an MPLS network?
A. High security standards.
B. High level of scalability.
C. It does require a NAT (network address translation) when private addresses are used.
D. QoS guaranteed for a flow travelling across the VPN

16. Le soluzioni per la realizzazione di VPN (virtual private network) di livello 3 attraverso una dorsale MPLS sono caratterizzate da
A. Livelli particolarmente alti di sicurezza
B. Elevata scalabilità
C. A differenza di tutte le altre soluzioni proposte, non richiedono l'utilizzo di funzionalità di NAT (network address translator) quando si abbia a che fare con indirizzi privati.
D. La fornitura di un servizio a qualità garantita al traffico che attraversa la VPN.

17. Why IPsec standard is used in some VPN (virtual private network)?
A. It is used only to verify the authentication credentials of remote users with a data exchange with an authentication server.
B. It is only used to allow remote user to send username and password to access the VPN
C. It is used to setup a secure tunnels between different sites of the same enterprise using a public network
D. It is used to overcome problems connected with the use of private networks

18. Lo standard IPsec viene utilizzato nelle VPN per
A. Verificare le informazioni di autenticazione fornite da utenti remoti tramite uno scambio di informazioni con un server di autenticazione
B. Consentire l'invio di informazioni di autenticazione (user e psw tramite challenge) da parte degli utenti di una VPN di accesso

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

19. Le così dette soluzioni VPN (virtual private network) di accesso o virtual dial-up VPN attualmente più diffuse sono basate su:
A. Connessioni dial-up.
B. Tunneling attraverso una rete IP.
C. Utilizzo di un'infrastruttura di cablaggio esistente per fornire servizi di accesso a larga banda
D. Nuovi protocolli di linea (livello data-link).

20. What is the distinctive feature of a VPN implementing a overlay model
A. The network provider does not know that we are implementing a vpn
B. The user devices at the edge of the vpn may ignore that we are using a VPN
C. It is not possible to have a secure connection
D. I cannot be implemented without the intervention network provider

21. What can be done with a VPN (virtual private network) based on SSL (secure socket layer)?
A. To distribute, in secure way, over several servers the workload related to a web based application
B. To implement clusters of private networks
C. To implement a backbone of an internet service provider for providing an interconnection service, in a simple and effective way
D. It is possible for an enterprise to make available in a secure way some applications aver the corporate network

22. What is the goal of PPTP
A. To implement site to site VPNs
B. To implement access VPN
C. To implement VPN with centralized access
D. To implement VPN with distributed access.

23. What is the role of GRE protocol?
A. It allows to increase the addressing space
B. It introduces an encryption mechanism for the packets
C. It allows to encapsulates a layer 2 frame into an IP packet
D. It allows the encapsulation but it is not possible to encapsulate units of lower layers into a layer 3 packet.

24. What is the typical role of IPSec in VPNs?
A. To distribute in a secure way the key required by other protocols to open a tunnel
B. To allow the transmission of authentication information (e.g. username and password) by users of access VPN
C. To open a managed secure tunnel across the public internet

D. To verify the user identity to allow other protocols to open tunnels only with authorized parties.

25. Why access virtual Private networks are used?
A. They are used to allow access to public internet using a private access network
B. They are used to allow an existing cabling infrastructure to provide wide-band services
C. They are used to build a private infrastructure by using a public one
D. They are used to connect two sites of an organization by using a dedicated line

26. The virtual private networks (VPN) are used for
A. Transporting private traffic over a shared infrastructure creating the same conditions that one would have by using a private infrastructure
B. Dividing a local area network of a company in a set of different subnetworks for different business activities (sales, purchases, engineering, marketing)
C. Partitioning a private network (for example the network of the main company with a number of secondary business units) in different network virtually divided

QoS

1. Gli algoritmi di scheduling vengono utilizzati:
A. 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.
B. 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
C. Nei router, per decidere quale sia l'ordine con cui debbano essere trasmessi i pacchetti in attesa ad una interfaccia
D. 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

2. How QoS is managed in SIP?
A. Is natively used managed by sip
B. the RTCP protocol is used to obtain QoS
C. It is optional
D. Sip does not provide any mechanism for QS

3. Nell'architettura DiffServ, il PHB permette di:
A. Trattare in modo differenziato le varie classi di servizio.
B. Tenere sotto controllo il tempo di attraversamento massimo di singolo router per ciascun flusso che lo attraversa
C. Fornire la garanzia end-to-end della QoS richiesta da ciascun flusso.
D. Garantire la QoS richiesta da ciascun flusso che attraversa un router.

4. What is a feature of the DiffServ (Differentiated Services) architecture?
A. Sophisticated signaling protocols for resource reservation.
B. Possibility to provide guaranteed QoS for packet flow explicitly requesting it.
C. A mechanism to provide different type of treatment to packets belonging to different service classes.
D. Sophisticated signaling protocols to make sure that each flow will receive a guaranteed QoS.

5. DiffServ si differenzia da IntServ perché:
A. DiffServ tende a fornire una garanzia su QoS che IntServ non dà.
B. DiffServ introduce nuovi protocolli per permettere la prenotazione di risorse allo scopo di ottenere una data QoS.
C. IntServ tende a fornire una garanzia su QoS che DiffServ non dà.
D. DiffServ tende a garantire un tempo massimo di attraversamento, mentre IntServ tende a fornire una banda minima garantita

6. Where queue scheduling policies are used?
A. In access routers to make sure that the traffic profile generated by a user is conforming with the agreed with the service provider.
B. In firewall, to delay packets entering the enterprise network from internet in order to prevent some kinds of attacks
C. In a router to decide the order of transmission of the packets waiting at each interfaces

D. In a router to schedule the list of the configuration commands issued by the user in order to minimize the impact on normal operations caused by the applications of configurations changes.

7. Where scheduling algorithms are used?
A. They are used in access routers to check that the traffic generated by the users is according what they negotiated with the provider.
B. They are used in firewalls to delay packets entering to an enterprise network in order to lessen risk of denial of services attacks.
C. They are used in routers to decide the order of transmission of the pending packets
D. They are used in routers to sequence correctly the configuration commands.

8. Qual è l'uso dei meccanismi di policing?
A. Servono all'utente per concordare con il fornitore il livello di QoS da ottenere.
B. Servono al fornitore di servizi per verificare che il traffico immesso dal cliente sia conforme agli accordi presi.
C. Servono all'utente per verificare che il traffico in arrivo dal fornitore sia conforme agli accordi presi.
D. Sono usati nei vari router per garantire un tempo massimo di attraversamento per ciascuno di essi

9. L'algoritmo RED (Random Early Deletion)
A. Gestisce le code interne dei router trasmettendo a rotazione pacchetti delle varie code.
B. Permette la marcatura in ingresso di traffici appartenenti a diverse classi.
C. Gestisce le code interne dei router, iniziando a scartare i pacchetti con probabilità crescente quando la coda raggiunge una lunghezza minima
D. Permette il controllo del massimo burst size.

IPV6

1. Lo schema di indirizzamento IPv6:
A. Prevede esclusivamente indirizzi assegnati in modo univoco da un ente preposto.
B. Prevede che ogni entità (es. azienda) si faccia assegnare globalmente un insieme di indirizzi, che diventano di sua proprietà a tempo illimitato.
C. Prevede che i primi 64 bit di un indirizzo siano normalmente identificati come il prefisso di rete, almeno sulle LAN.
D. Non prevede l'esistenza di indirizzi di multicast.

2. L'autoconfigurazione stateless in IPv6 richiede:
A. Un server DHCPv6 (Dinamic Host Configuration Protocol version 6).
B. Un server presente sulla rete locale.
C. Un server presente sulla rete aziendale (intranet).
D. È possibile anche se non si è in presenza di server o router

3. A differenza della versione 4 dell'IP, la versione 6:
A. Non ha una versione dell'ICMP associata
B. Non permette di scoprire l'indirizzo MAC di un'altra stazione, conoscendone l'indirizzo IP.
C. Non ha indirizzi broadcast
D. Non ha un equivalente del campo TTL (time-to-live).

4. In IPV6 protocol, IP packet header
A. Is always authenticated through the utilization of proper encryption algorithms in order to increase the security of transmissions.
B. Has a small size with respect to IPV4, in order to increase the bandwidth efficiency by reducing protocols overhead.
C. Includes only fixed size fields that carry the required information in each packet
D. Includes some fields available in IPV4 only as options to offer features that turn to be largely used along the time.

6. What are the differences between the transmission types in IPV4 and IPV6
A. No difference
B. IPV4 does not include anycast (included in IPV6) and it does include broadcast (not included in IPV6)
C. IPV4 does not include multicast included in IPV6
D. IPV4 does not include anycast and multicast both included in IPv6

7. Does exist a version of DHCP for IPV6?
A. It does not exist because stateless auto configuration alone solves the same problem.
B. It does not exist because stateless auto configuration and router advertisement solve the same problem.
C. It exists a DHCP IPV6
D. It Does not exist because it is more secure it the host is configured manually.

8. Is fragmentation allowed in IPV6?
A. Datagrams may only be fragmented by the sender and re-assembled at the final destination

B. The mechanism is similar to the one included in IPv4
C. It is not possible to fragment datagrams, both for routers and for the sender
D. Fragmentation is allowed only in routers whenever necessary.

9. A differenza della versione 4 dell'IP, la versione 6:
A. Non ha intestazione di lunghezza variabile.
B. Non permette di scoprire l'indirizzo MAC di un'altra stazione, conoscendone l'indirizzo IP.
C. Non ha un equivalente del TTL (time-to-live).
D. Non permette l'uso di IPsec.

10. Nel IPv6 cosa sparisce dalle intestazioni, rispetto a IPv4?
A. Il tempo di vita del pacchetto.
B. Gli indirizzi mittente e destinatario.
C. L'indicazione su quale sia l'intestazione successiva
D. Il checksum dell'intestazione.

11. Gli indirizzi link-local
A. Sono validi all'interno di una organizzazione che li può utilizzare per assegnare indirizzi alle macchine nelle varie sottoreti della propria intranet (sono gli omologhi degli indirizzi privati di IPv4).
B. Non possono essere assegnati ai router.
C. Sono normalmente costruiti automaticamente dalla stazione a partire dall'indirizzo MAC della propria scheda, a cui si pre-pende un prefisso predefinito.
D. Vengono utilizzati per identificare macchine che svolgono un certo servizio (ad esempio server DNS).

12. What is the role of link-local IPV6 address
A. It can be used to enable the communication between hosts in the same subnetwork when other type of IPV6 addresses are not available
B. It is used to physically connect 2 host over a local link
C. It is the only address that can be used to communicate over a LAN
D. It is the only address to communicate to routers

13. Un indirizzo link-local:
A. E' utilizzabile per permettere la comunicazione tra stazioni su link locali (es. una LAN) in mancanza di altri indirizzi IPv6.
B. Serve per collegare fisicamente due stazioni su un link locale.
C. E' l'indirizzo utilizzato dalle stazioni su una LAN per scambiarsi i dati.
D. E' utilizzato in tutte le comunicazioni tra stazioni locali.

13bis. Quale è la funzione dello "scope" associato agli indirizzi IPv6?
A. Serve a risolvere, in casi particolari, l'ambiguità riguardo il mittente.
B. Non esiste uno scope associato agli indirizzi IPv6.
C. Serve per poter utilizzare gli indirizzi globali.
D. Serve per poter utilizzare gli indirizzi anycast.

14. What is a feature of the IPv6 addressing scheme?
A. The whole address is assigned by a single authority.

B. Addresses are distributed in order to make it easy to aggregate them in the backbone router forwarding tables.

C. Multicast addresses are not used.

D. Variable length addresses are used.

15. Nel protocollo IPv6:
A. I protocolli di routing (ad esempio il formato dei pacchetti) non cambiano rispetto ad IPv4.
B. Il protocollo ARP viene inglobato in ICMPv6, ma mantiene esattamente lo schema di funzionamento (richiesta broadcast, risposta unicast) precedente.
C. Esiste la possibilità, per una stazione su un segmento di rete, di autoconfigurarsi attraverso l'ascolto di messaggi di Router Advertisement.
D. Come IPv4, IPv6 non prevede meccanismi di riconfigurazione dei router.

16. L'autoconfigurazione stateless di IPv6 presenta problemi di riservatezza?
A. Non vi sono particolari problemi.
B. Non permette la cifratura del carico.
C. E' possibile individuare la stessa interfaccia, se si collega a internet da vari provider.
D. Non permette l'uso delle intestazioni di sicurezza (tipo IPsec).

17. What is the feature of IPV6 address?
A. They allow communication between host with IPV4 and IPV6 addresses without additional mechanism
B. They keep the same flexible division between subnet and host fields.
C. They rigidly organized in network, subnetwork and host fields.
D. They include a unique broadcast address

18. Which mechanism is used to forward IPV6 packets over the LAN?
A. A neighbor discovery mechanism is not used because there is an algorithm to map any possible address onto a MAC address.
B. The neighbor discovery is not used for IPv6 multicast and broadcast packets because an algorithm exists to map those IPV6 address onto MAC address
C. The neighbor discovery mechanism is used for all the possible types of IPV6 address.
D. The neighbor discovery mechanism is not used for IPV6 multicast packets because an algorithm exist to map those IPV6 address onto MAC address

19. What is a feature of stateless auto-configuration in IPv6?

A. It is based on DHCPv6 (Dynamic Host Configuration Protocol version 6)

B. It uses a standard prefix followed by an host number 64 bit long, derived from the MAC address

C. It is mandatory to have a router in the sub-network to get the network prefix (the most significant 64 bits) with a message of router solicitation.

D. It is mandatory to have a router in the sub-network to get the network prefix (the most significant 64 bits) with a message of router advertisement.

20. Un host IPv6 al reboot, acquisirà il seguente indirizzo:

A. 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.
B. Un indirizzo FE80::/32
C. Per quanto riguarda l'indirizzo link-local, assumera' lo stesso indirizzo IPv6 che possedeva prima del reboot.
D. L'indirizzo dipende interamente dalla configurazione che acquisirà dal suo default router.

VOIP

1. What ENUM standard is used for?
A. It is used to call a sip user from a telephone set connected to the public telephone number
B. It is used to call a telephone in the public switched telephone network from a computer, using SIP
C. It is used to transmit the voice streams of a sip calls
D. It is used to implement e-presence in SIP

2. Il protocollo RTP è in grado di:
A. Limitare le variazioni di ritardo (jitter) subite dai pacchetti nei router.
B. Far conoscere ai router il profilo di traffico generato da una stazione.
C. Riservare risorse di calcolo nei server che condividono i loro processori.
D. Incapsulare i dati audio/video con intestazioni contenenti informazioni sulla loro codifica

3. Il protocollo RTP è in grado di:
A. Limitare le variazioni di ritardo (jitter) subite dai pacchetti nei router.
B. Raccogliere informazioni su come procede la trasmissione.
C. Riservare risorse nella rete per ottenere una certa QoS.
D. Incapsulare i dati audio video con intestazioni contenenti informazioni di codifica

4. What is one of the possible uses of RTP (Real-time Transport Protocol) ?
A. To carry a timestamp related to the block of samples transmitted in a packet
B. To implement real-time application for industrial plant control.
C. It can be used in multimedia applications to limit the packet transit time across the network
D. It is possible to distinguish different streams (e.g. audio + video) addressed to the same host, by means of the field PT (Payload Type).

5. Nel protocollo RTP, quando è possibile cambiare la codifica dei dati trasportati da un flusso?
A. Una volta iniziata la trasmissione del flusso audio/video, non è più possibile cambiare la codifica
B. E' possibile cambiare la codifica, quando si effettua una opportuna segnalazione di controllo utilizzando RTCP.
C. E' possibile cambiare la codifica ad ogni pacchetto inviato.
D. E' possibile cambiare la codifica, solo se si sta utilizzando un RTP mixer.

6. What is possible to do with the RTCP protocol?
A. It is possible to limit the jitter.
B. It is possible to communicate to other routers the profile of the traffic generated by a transmitter.
C. It is possible to reserve resources to obtain guaranteed QoS.
D. It is possible to monitor the number of losses of a specific flow of packets.

7. Which of the following statement applies to sip trapezoid?
A. It is mainly used to sends SUBSCRIBE-NOTIFY (e-presence) message
B. It is an obsolete mechanism of SIP, since manly current SIP implementations use a

more efficient mechanism
C. It is the standard mechanism to send REGISTER Messages
D. It is a standard mechanism to setup a call

8. Le funzioni di un voice gateway (o VoIP gateway) includono:
A. Inoltrare pacchetti IP tra una rete pubblica IP ed una rete aziendale IP (intranet).
B. Tradurre i flussi vocali generati su una rete a pacchetto (ad esempio tramite SIP o H.323) in telefonate su una rete telefonica tradizionale (plain old telephone system – POTS).
C. 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.
D. Tradurre la segnalazione telefonica SS #7 in segnalazione SIP.

9. La telefonia su IP prevede:
A. L'uso di voice gateway per consentire la comunicazione con utenti collegati a reti tradizionali (POTS).
B. L'aggiornamento del cablaggio della rete IP in modo da collegare ogni utente telefonico tramite fibra ottica
C. 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.
D. L'installazione di una rete in tecnologia IP parallela a quella dati, dedicata al trasporto di fonia

10. La telefonia su IP prevede:
A. L'uso di voice gateway per consentire la comunicazione con utenti collegati a reti tradizionali (POTS).
B. L'aggiornamento del cablaggio della rete IP in modo da collegare ogni utente telefonico tramite fibra ottica
C. 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.
D. Il protocollo SIP.

11. I messaggi SIP sono caratterizzati da:
A. Non avere un carico utile, vi sono solo i comandi/risposte e le intestazioni.
B. Avere, in alcuni casi, un carico utile composto da righe SDP (session description protocol).
C. Avere un codice di checksum che permette la rilevazione di errori.
D. Avere codifica numerica in base 2.

12. La principale motivazione per cui un operatore "telefonico" come Skype riesce a fornire un servizio telefonico a prezzi molto bassi:
A. E' dovuto al fatto che le telefonate viaggiano sulla rete IP (ad esempio ADSL), i cui costi sono già pagati dall'utente nel momento in cui stipula un contratto "flat" e quindi i pacchetti vocali viaggiano virtualmente "gratis" in gran parte del loro percorso
B. È 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
C. E' dovuto principalmente alla pubblicità che viene offerta insieme al servizio.

D. 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.

13. What is a feature of the Session Initialization Protocol (SIP)?
E. It is necessary that the media stream is established with the help of server called Media relay.
F. It is not scalable, because it does not specify how to find users in different domain than the caller.
G. It is necessary that User Agent is always associated to the same IP address
H. It is possible to use a server to register a User Agent, so that the server know the mapping between the username and its current IP address.

14. Dovendo trasportare traffico VoIP con garanzie "toll-quality":
A. È 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
Toll Quality *= Audio transmission at the quality level of a traditional landline, The standard of performance is generally a PCM line*. Quindi in teoria, pensandoci bene, la risposta corretta dovrebbe essere la prima, perché ad es. se la banda si satura, la qualità decresce.
B. E' possibile utilizzare Internet, Skype dimostra che questo approccio funziona decisamente bene.
C. E' necessario creare la propria rete IP e dare precedenza al traffico voce.
D. E' necessario creare una rete IP dedicata, in cui cioè non vi sia traffico dati.

15. Utilizzando l'algoritmo del secchiello a gettoni (o secchio bucato) di capacità **B** token e velocità di riempimento **r** token/s si riesce a controllare:
A. Che il tempo di attraversamento non superi **rB** secondi.
B. Il numero di pacchetti al secondo immessi non superi **r**, ed il massimo burst non superi **B.**
C. Il numero di pacchetti al secondo immessi non superi **B**, ed il massimo burst non superi **r**.
D. Il jitter non superi **B/r**.

16. Nel meccanismo del secchiello a gettoni si riesce a controllare:
A. Il tempo di attraversamento massimo di un router.
B. La gestione interna delle code con WFQ.
C. La velocità minima di immissione dei dati.
D. Il burst size massimo e la velocità media di immissione dei dati.

17. If we apply to a flow of packets the token bucket (or leaky bucket) algorithm with capacity K and inserting token every 1/W sec, what is the final effect?
A. The maximum burst size allowed is W.
B. All the packets of this flow will be routed on the same path (i.e. out of order arrival is eliminated).
C. It will be possible to implement traffic engineering mechanisms to this flow of packets.
D. The maximum burst size allowed is K

18. Nell'algoritmo del secchiello a gettoni:
A. La capacità del secchiello è legata alla velocità media sul lungo periodo.
B. La capacità del secchiello è legata al massimo burst size.
C. La capacità del secchiello ha relazione diretta con la banda

D. Serve per implementare il weighted fair queuing.

19. When it is necessary to design a new network for integrated data and voice traffic, which is the highest priority requirement to fulfill?
E. Mechanism to achieve deterministic characteristics for the voice calls
F. Mechanisms to reduce jitter as much as possible.
G. Mechanisms to obtain transit time for the voice packets as short as possible
H. Routing protocols to find alternative paths in order to avoid call interruption, in case of failure

20. What is a feature of the SIP protocol?
A. It is only implemented in "soft phones", that is software packages that are used for PC to PC calls.
B. It is based on ASN.1, it is extremely complex and it is used for implementing signaling operations in IP networks.
C. Often, It requires a server for each SIP domain.
D. It is used to implement the transmission of voice streams over an IP network.

21. La mobilità dell'utente viene trattata nel protocollo SIP?
A. Non viene trattata
B. Sì, all'utente non viene imposta nessuna limitazione sulla mobilità.
C. Sì, a patto però che l'utente si ricolleghi sempre con un indirizzo IP interno allo stesso provider.
D. Sì, a patto però che l'utente non cambi indirizzo IP durante una sessione SIP.

22. In un sistema VoIP basato su SIP, cosa può avvenire se effettuo una chiamata verso un destinatario non collegato a Internet?
A. Si può chiedere di essere avvertiti quando l'utente desiderato ritorna ad essere noto al sistema
B. Si può solo tornare a provare più tardi.
C. Si può essere avvertiti dell'apparizione dell'utente desiderato, solo se entrambi siano nello stesso dominio SIP (abbiamo lo stesso operatore).
D. Si può essere avvertiti dell'apparizione dell'utente desiderato, solo se lo stesso si ricollega da uno degli indirizzi IP noti al dominio SIP.
(**APPROFONDIMENTO**: attraverso il Media Server, contenente le caselle vocali che fungono da segreterie telefoniche, è possibile lasciare un messaggio anche se il client destinatario non è collegato a internet. Egli riceverà il messaggio non appena si riconnetterà)

23. L'utente SIP è caratterizzato dal fatto che
A. Ha uno specifico IP pubblico a cui deve essere collegato.
B. Ha un dominio di appartenenza
C. Ha un IP che può variare, ma che non può essere di tipo privato.
D. E' sempre collegato ad Internet.

24. What is the reason of diffusion of VoIP among domestic users?
A. The reduced cost associated to the possibility of VoIP technologies to compress voice channels, which require much less bandwidth the analog telephony, with a big reduction of bandwidth used in the backbone.

B. The reduced costs caused by higher costs in maintaining an high quality channel (the twisted pair) that is more expensive that physical lines used for data transmission.
C. Costs are often comparable with traditional telephony, but it is not necessary to pay an extra fee for each phone call, in addition to the flat rate tariff of the ADSL line.
D. Quality of the calls are higher in VoIP, because the providers adopt suitable QoS mechanisms to offer high standards of quality for the phone calls.

25. Which of the following mechanisms apply to SIP?
A. A voice gateway may be used to allow the communication between two IP phones connection to different physical networks
B. It is necessary to update the access network to fiber connection
C. Signaling protocols are used to setup a call and to negotiate its parameters
D. It's necessary to provide each user with a computer for sip cells and is normal phone set for calls from/to public switched network

26. Which of the following statement applies to sip protocol?
A. It is based on a distributed architecture where each domain should have a server to manage the domestic users
B. It is based on a centralized architecture with only one server to manage communications
C. It is based on a hierarchical organization where each level manages a particular area of the network
D. It is bases on a peer to peer architecture to enable a dynamic behavior for the users

27. Why the combination of a token bucket (or a leaky bucket) and weighted fair queuing (WFQ) is used?
A. It is used to have a maximum guarantee transversal time for a single router
B. It is used to have a maximum guarantee transversal time for a NAT
C. It is used to have a maximum guarantee transversal time for a flow of packets
D. It is used to obtain a guarantee jitter for packets

28. La combinazione di meccanismi di secchiello dei token (o secchio bucato) e Weighted Fair Queueing (WFQ) serve a garantire:
A. Un tempo di attraversamento massimo di un router.
B. Un tempo di attraversamento massimo di un NAT.
C. Una banda massima per ogni flusso di pacchetti.
D. Un burst massimo di pacchetti consecutivi, per ciascun flusso.

29. What is the role of NAPTR record in sip?
A. They are used which server are available in a domain with their relative priorities.
B. They are used which services are available in a domain with their relative priorities
C. They are used to verify the identity of the users during the registration phase.
D. They are used to possible change the voice encoding when two UAs do not have the same codec.

30. Il protocollo SIP:
A. E' basato su un'architettura distribuita, in cui ogni dominio deve dotarsi di un server che è responsabile dei propri utenti

B. E' basato su un'architettura rigidamente centralizzata, con un unico server per gestire le comunicazioni
C. E' basato su un'architettura gerarchica in cui ogni livello della gerarchia è responsabile d una particolare zona della rete
D. E' basato su un'architettura peer-to-peer per facilitare la dinamicità degli utenti

31. What is the role of Session Description Protocol?
A. It is used to negotiate the parameters to setup a call
B. It is used to select the use of sip or H.323 for the session being open
C. It is used to Exchange authentication information at the beginning of a session
D. It is used to select if a record routing should be selected or not, for the current SIP Session

32. Se si utilizza il protocollo SIP, quali tipi di informazioni possono essere memorizzate nel DNS?
A. Nessuna informazione differente dai soliti record RR del DNS.
B. La traduzione per tutti i nomi degli utenti in indirizzi IP.
C. Nuovi tipi di record che descrivono i servizi SIP disponibili in un dominio ed i relativi server.
D. Informazioni sui numeri di telefono da utilizzare per chiamare gli utenti SIP.

33. Which function is performed by a voice gateway (or VoIP gateway)?
A. It forwards packets between the public internet and a corporate network.
B. It translates packets carrying voice samples into signals understandable in a plain old telephone system (POTS)
C. It encrypts voice signals arriving from a classical telephone network, before they are forwarded to internet, so that the signal cannot be understood by an eavesdropper.
D. It translates SS #7 signaling into SIP signaling messages

34. Which of the following features are part of a voice gateway (or VoIP) Gateway?
A. It forwards packets from a public IP network to a private one
B. It translates voice streams generated over a packet network (e.g. using SIP or H232) into telephone calls over a traditional telephone network
C. It encrypts a voice signal arriving from a traditional telephone network before forwarding it over to the internet.
D. It synchronizes different RTP stream (lip synch)

35. What is the SDP role in SIP telephony?
A. It is used to carry the description of the main parameters of the conversation that is about to start.
B. It is used to reserve the required resources to obtain the quality of services needed to call
C. It is used to locate the IP address of the called user
D. It is used to encapsulate the audio/video sample during the phone call

36. What is the role of the NAPTR records in SIP?
A. They are used to discover the names of the sip servers of a given domain
B. They are used to discover the SIP services available in a given domain

C. They are used to translate the name into the IP addresses of the SIP server.
D. They include the IP address of the called SIP user

38. What is the role played by RTCP?
A. It provides control mechanism for RTP
B. It may be used to reserve the resources required to obtain a certain quality of services
C. It may be used to change the payload type of an RTP stream without restarting it
D. It may be used to distinguish between two streams (e.g. audio and video) with the same destination.

39. What is the role of Enum standard?
A. To Locate the sip server in all the inter domains calls
B. To translate a phone number into a Sip user name
C. To translate Sip user name into phone number
D. To register the users with the SIP servers

40. I codec specificatamente ingegnerizzati per la codifica della voce:
A. Tendono a creare pacchetti grossi per massimizzare l'efficienza della rete.
B. Tendono a creare pacchetti piccoli per minimizzare il ritardo end-to-end.
C. Aggiungono sempre dei bit di ridondanza per ridurre i danni in caso di perdita di pacchetti. *pag64 appunti*
D. Sono in grado di operare anche con sorgenti VoIP diverse (ad esempio modem o FAX).

MPLS

1. Gli LSP (label switched path) nell'architettura MPLS (multi-protocol label switching)
A. Rappresentano percorsi alternativi mantenuti nella tabella di un router per l'inoltro di pacchetti verso una destinazione.
B. Vengono scambiati dai router per costruire una mappa della rete.
C. Costituiscono il percorso più breve verso una destinazione.
D. Vengono creati (set up) per il trasporto di pacchetti appartenenti ad una classe di equivalenza di inoltro (forwarding equivalence class, FEC).

2. L'architettura MPLS (multi-protocol label switching) è caratterizzato da
A. Un supporto particolarmente evoluto per fornire servizi a qualità garantita
B. Un diverso meccanismo (rispetto all'IP puro) per decidere l'interfaccia di uscita verso cui un pacchetto debba essere inoltrato.
C. Protocolli di routing particolarmente veloci ad aggiornare le tabelle di routing in seguito a cambiamenti topologici in modo da recuperare velocemente i guasti.
D. Terminali di rete intelligenti in grado di personalizzare i servizi ricevuti dalla rete

3. Which operations can be performed on a label by a single MPLS router?
A. Add a label in any position (PUSH), drop one label in any position (POP), change the value of a label in any position (SWAP).
B. Add an external label (PUSH), drop the external label (POP), change the content of the external (SWAP)
C. Add a label if the router is the ingress one (only 1 label is allowed) (PUSH), drop the only label if the router is the egress one (POP), e change the content of the only label present (SWAP).
D. Labels cannot be manipulated by MPLS routers.

4. Gli LSP (label switched path) nell'architettura MPLS (multi-protocol label switching)
A. Sono ottenuti riservando risorse nei nodi di rete in modo da garantire opportuna qualità del servizio alle applicazioni che li hanno creati.
B. Costituiscono il percorso più breve verso una destinazione.
C. Vengono creati (set up) dalle applicazioni per il trasporto di pacchetti appartenenti ad una classe di equivalenza di inoltro (forwarding equivalence class, FEC).
D. 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 classe (FEC).

5. The importance of MPLS (multiprotocol label switching) today's networks derives from one of the following features.
A. It is possible to transport efficiently IP packet over ATM networks
B. It is possible to have a high speed connections between servers and their disk units
C. It is possible to implement efficient and effective traffic engineering operations
D. It is possible to implement devices that do not need complex configuration operation

6. In un pacchetto che viaggia su una rete MPLS, è possibile avere più label contemporaneamente?
A. No, non è previsto.
B. Sì, ma non più di 2.

C. Sì, ma non più di 20.
D. Sì, ma solo nei tunnel MPLS usati per le VPN.

7. In che modo MPLS può essere utilizzato per realizzare una VPN?
A. Per realizzare una VPN di accesso.
B. MPLS non può essere usato per realizzare VPN.
C. Può fornire tutto il meccanismo di instradamento in reti overlay o dei collegamenti punto-punto in reti peer.
D. Può fornire collegamenti punto-punto in reti overlay o tutto il meccanismo di instradamento in reti peer.

8. Why MPLS is important?
A. In such networks, it is possible to implement routers with a specific support to guarantee the required quality of services.
B. It is possible to have a single control plane for different switching technologies
C. It is possible to implement devices that should not be configured
D. It is possible to distribute the traffic among several equivalent servers

9. MPLS (Multiprotocol Label Switching) architecture is characterized by
A. End System that are able to negotiate with the network the label of packets generated
B. Intelligent terminals that can personalize service received from the network
C. Routing protocols that are extremely fast in updating routing tables when a topology changes occur in order to ensure fast fault recovery.
D. A different mechanism (with respect to pure IP) for selecting the output interface toward which packet should be forwarded.

WAN

1. In una rete frame relay la minima unità di trasmissione è:
A. La cella da 53 bytes.
B. L'unità di trasmissione del livello 2.
C. Il circuito virtuale.
D. Il pacchetto IP.

2. Le reti ATM vengono spesso utilizzate per:
A. Interconnettere diversi tronconi di LAN all'interno dello stesso campus.
B. Realizzare delle VLAN.
C. Interconnettere le terminazioni dei canali ADSL con la rete del fornitore di servizi prescelto dall'utente
D. Realizzare sistemi VoIP.

3. Il trasporto di pacchetti IP su reti ATM
A. E' attualmente utilizzato, sebbene in via di "estinzione", sulle dorsali geografiche degli operatori.
B. Non e' possibile
C. E' indispensabile per il trasporto di traffico real-time (per esempio video) su IP
D. E' considerato una soluzione ottimale il cui utilizzo è in rapida crescita.

3. What is a feature of ATM networks?
A. They do not allow fragmentation of long packets
B. They provide a datagram based packet forwarding.
C. They allow a unified control plane with IP networks.
D. They use a fixed size cell, as unit of transmission.

12. Where ATM networks are still used today?
A. In some LANS
B. In some connections between homes and the closest DSLAMs
C. In private networks
D. In some networks connecting DSLAMs with ISP networks (POP)

13. How popular is the transport of IP over ATM networks
A. It is possible and currently used, but this technique is going to disappear
B. It is not possible
C. It is only available solution for real time traffic (e.g. video = over IP)
D. It is considered a good solution and it will become more popular

6. La trasmissione in SONET/SDH è caratterizzata da:
A. Flessibilità nell'uso della banda
B. Meccanismi per il controllo della congestione.
C. Tempo uguale su tutti i tipi di canale per la trasmissione di un singolo byte, qualsiasi sia la velocità del collegamento.
D. Frame la cui durata è sempre di 125 microsecondi, qualsiasi sia la velocità del collegamenti

7. What is one of the problems with SONET/SDH networks?
A. Bandwidth management is rigid
B. They are not suitable for an implementation based on optical fibers.
C. They are not suitable to implement ATM or frame Relay networks.
D. They cannot achieve high transmission speed.

8. Una delle caratteristiche principali delle linee SONET/SDH è che:
A. L'allocazione degli slot di trasmissione avviene secondo le esigenze del momento delle varie stazioni.
B. Le varie frequenze di trasmissione sono una multipla dell'altra
C. La trasmissione avviene previa esecuzione di un meccanismo di contesa del canale che stabilisce chi ha diritto di trasmettere.
D. La trasmissione avviene a divisione di lunghezza d'onda

9. Per poter garantire qualità del servizio nelle reti a commutazione di pacchetto
A. I nodi di rete devono in atto opportuni meccanismi che regolano il servizio dei pacchetti (per esempio algoritmi di scheduling)
B. Le applicazioni devono essere in grado di codificare le informazioni da trasferire secondo livelli (layers) di importanza differente
C. Bisogna trasportare i pacchetti su un'infrastruttura a commutazione di cella (per esempio ATM)

11. In a Frame Relay network, what is the Committed Information Rate?
E. The maximum number of bits that can be sent to the network, in a specified time interval
F. The minimum bandwidth guaranteed.
G. The maximum length of a packet that can enter the network.
H. The maximum transit time.

SUMMARY OF TOPICS

VPN (Virtual Private Network): 2 tunnel end-points: macchina che si sta collegando, VPN Gateway. Instaurazione VPN: 3 fasi: configurazione canale di controllo (PPTP), configurazione di livello 2 (PPP - LCP), configurazione di livello 3 (PPP - IPCP). Autenticazione (CHAP) fra PPP-LCP e PPP-IPCP.
LCP (Link Control Protocol): VPN. Protocollo per fare operazioni di controllo iniziali. Fa parte del PPP.
CHAP (Challenge-Handshake Authentication Protocol): VPN. Protocollo per l'autenticazione.
IPCP (IP Control Protocol): VPN. Protocollo per ottenere dal VPN Gateway un indirizzo IP interno alla VPN. Fa parte del PPP.
Accesso Centralizzato: VPN. Il traffico passa prima dal VPN Gateway il quale lo reindirizza verso le destinazioni (opzione di configurazione "Use Default Gateway on Remote Networks" = true).
Accesso Distribuito: VPN. Il traffico non passa necessariamente dal VPN Gateway ma viene indirizzato con le normali regole di routing (opzione di configurazione "Use Default Gateway on Remot**e Networks" = false).**
PPTP (Point-to-Point Tunnelling Protocol): Access VPN. Effettua il tunneling a livello 2. Per costruire tunnel direttamente dalla macchina utente.
L2TP (Layer 2 Tunneling Protocol): Access VPN. Effettua il tunneling a livello 2. Per reti VPN dial-up nella quale gli host si possono connettere da postazioni diverse.
GRE (Generic Routing Encapsulation): Site-to-site VPN. Effettua il tunneling a livello IP.
IPsec: Site-to-site VPN. Effettua il tunneling a livello IP.
BGP (Border Gateway Protocol): Site-to-site VPN, MPLS. Protocollo di routing inter-AS utilizzato per connettere tra loro piu router gateway che appartengono a sistemi autonomi AS (Autonomous System) distinti fra loro. Protocollo a indicazione di percorso (Path Vector) che effettua il routing basandosi sulle regole determinate da ciascuna rete. Supporta il routing indipendente dalle classi (Classless InterDomain Routing) e aggrega gli instradamenti per diminuire la dimensione delle tabelle. Ideato per sostituire il protocollo EGP (legato alla filosofia dell'internet centralizzato dipendente dalla rete NSFNET) e rendere internet un sistema decentralizzato. Gli ISP sono obbligati a utilizzare BGP per stabilire i criteri di routing e lo rendono uno dei più importanti protocolli di internet.
MPLS Label Distribution Protocols: LDP, PIM, RSVP/CR-LDP, BGP.
MPLS Routing Protocols: OSPF, IS-IS, BGP-4, IGRP, RIP.
LSP (Label Switched Path): MPLS. Un LSP e un percorso virtuale basato su criteri FEC che parte da un Ingress Router verso un Egress Router attraverso una rete MPLS gestita da un protocollo di Label Distribution. Gli LSP sono dei tunnel MPLS poiche risultano opachi rispetto agli altri livelli. Sono unidirezionali pertanto per avere una comunicazione bidirezionale e necessario gestire un secondo LSP che va nella direzione opposta rispetto al primo. Funzionamento LSP: L'Ingress Router (LER) aggiunge una label (push) al pacchetto e determina l'LSP da seguire; uno o piu LSR intermedi cambiano la label del pacchetto con un'altra (swap) e inoltrano il pacchetto al router successivo; l'Egress Router (LER) rimuove la label piu esterna (pop) e inoltra il pacchetto basandosi sull'header del livello successivo (es. IPv4).
LER (Label Edge Router): LSP. Tramite le funzioni push/pop, aggiunge/toglie le label ai pacchetti IP entranti in base al FEC appropriato servendosi di una tabella.
LSR (Label Switching Router): LSP. Tramite la funzione swap cambia la label del pacchetto. Per ogni porta c'e una tabella che indica l'instradamento (data una label su una porta, viene indicata la porta ove smistare il pacchetto e la nuova label).
FEC (Forwarding Equivalence Class): LSP. E' la classe che distingue un LSP da un altro. Una FEC tende a corrispondere a un LSP e descrive un insieme di pacchetti con caratteristiche simili e/o identiche che possono essere spediti nella stessa maniera attraverso la stessa label. I criteri per attribuire una FEC possono essere: stessa destinazione (unicast/multicast); stesso tunnel VPN; ottimizzazione di alcune tipologie di pacchetti (traffic engineering); QoS o classe di servizio (VoIP/Web).
Skype: Protocollo VoIP proprietario che usa molti concetti delle reti P2P (Peer To Peer). Si basa su nodi client e supernodi. Vantaggi: non e necessario avere indirizzi IP pubblici (i NAT non sono piu un problema); come nelle reti P2P il traffico e distribuito fra i vari nodi e non e necessario disporre di infrastrutture

costose; la qualita del servizio (QoS) non e un prerequisito indispensabile in quanto la rete e abbastanza libera; la voce puo essere trasmessa anche su TCP; buca i firewall grazie a TCP perche la chiamata e spesso diretta e c'e una triangolazione attraverso relay (senza perdita della qualita); soppressione di pause ed eco; ottima gestione della voce; e free. Svantaggi: il codice e criptato; il debugging e impossibile; a livello aziendale si preferiscono soluzioni piu sicure, aperte e gestibili come SIP; il singolo nodo puo essere inaffidabile; problemi di intercettazione; overlay non influenzabile dall'utente (impossibile controllare chi sia il destinatario delle proprie informazioni).
Skype Overlay: Si basa su nodi client e supernodi (nodi client promossi che devono gestire circa 5Kbps di traffico aggiuntivo). I supernodi contengono l'indice dei nodi vicini e scambiano informazioni con loro. Il nodo client si collega ad uno o piu supernodi salvati in un file locale. In mancanza di essi o in caso di connessione fallita ci si collega a un insieme di nodi predefiniti detti Bootstrap Servers. Il protocollo preferito e UDP, anche se in caso di rete con firewall si usa TCP e si cambiano spesso le porte.
H.323: VoIP. Protocollo di derivazione telefonica (per sistemi di comunicazione multimediali a pacchetto). Nato per estendere le videoconferenze alle LAN. Il Gatekeeper fa segnalazione e gestisce la comunicazione fra due o piu client. La Multipoint Control Unit (MCU) gestisce i metodi di comunicazione e fa da mixer/switch dei flussi.
I dati viaggiano su RTP affiancati da RTCP. H.323 fornisce la maggior parte dei servizi (autenticazione, localizzazione) ed e molto diffuso ma complesso, in via di abbandono a favore di SIP.
SIP (Session Initiation Protocol): VoIP. Protocollo di derivazione dati definito in ambito internet. Si utilizza un server SIP per l'autenticazione. Molto piu semplice rispetto a H.323, nasce come protocollo di segnalazione (di tipo end-to-end, trasparente ai router) in grado di instaurare, modificare e terminare una sessione multimediale/dati. Il formato dei pacchetti e HTTP-like e la segnalazione puo avvenire tramite TCP (per aggirare i firewall), UDP (molto semplice) e TLS (consente la cifratura). Sfrutta in modo identico a H.323 i protocolli RTP e RTCP e aggiunge una parte di controllo nella quale e importante SDP. Componenti SIP: Registrar Server; AAA Server; Location Server; Proxy Server; Redirect Server; Media Server; Media Proxy; MCU; Gateway.
RTP (Real-Time Protocol): Pensato per trasportare pacchetti audio/video. Non gestisce frammentazione e riassemblaggio perche i pacchetti sono molto piccoli. Non gestisce errori di trasmissione perche la ritrasmissione non e necessaria. Non specifica il formato dei dati in modo da permettere un buon numero di codifiche. Completa il livello 4 insieme a UDP ed e usato solo dalle macchine alle estremita della comunicazione.
RTCP (Real-Time Control Protocol): Associato all'RTP per il monitoraggio e il controllo della comunicazione. Raccoglie informazioni sulla codifica.
SDP (Session Description Protocol): SIP. Definisce i parametri delle sessioni multimediali e in fase di INVITE trasporta diversi parametri utili (tipo media, codec, indirizzi, porte, ecc...).
Chiamata SIP (1 dominio): Struttura: Chiamante@dominio - Proxy SIP dominio - Ricevente@dominio. Messaggi: INVITE (Chiamante → Ricevente); 100 Trying (Proxy → Chiamante); 180 Ringing (Ricevente → Chiamante); 200 OK (Ricevente → Chiamante); ACK (Chiamante → Ricevente).
Chiamata SIP (2 domini): Struttura: Chiamante@dominio1 - Proxy SIP dominio1 - DNS Server - Proxy SIP dominio 2 - Ricevente@dominio2. Messaggi: INVITE (Chiamante → Proxy1); 100 Trying (Proxy1 → Chiamante);
DNS 'NAPTR' Query (Proxy1 → DNS); DNS 'NAPTR' Response (DNS → Proxy1); DNS 'SRV' Query + Response (Proxy1, DNS); DNS 'A'/'AAAA' Query + Response (Proxy1, DNS); INVITE (Proxy1 → Proxy2); INVITE (Proxy2 →
Ricevente); 180 Ringing (Ricevente → Chiamante); 200 OK (Ricevente → Chiamante); ACK (Chiamante → Ricevente).
SIP REGISTER: La registrazione permette di autenticare un utente che accede a un dominio SIP e permette di associare la URI SIP che identifica l'utente all'UA SIP (host) su cui si trova in quel momento. In questo modo l'utente puo essere raggiunto conoscendo solamente la URI SIP. Se l'utente si sposta dovra registrarsi nuovamente. Campi piu importanti dell'header di un messaggio SIP REGISTER: Command (riga di comando); Via (indica i sistemi SIP gia attraversati dal messaggio); Max-Forwards (numero massimo di sistemi SIP che possono essere attraversati dal messaggio); Contact (URI temporanea che identifica la posizione corrente dell'utente: IP+porta); To e From (contengono entrambi la URI che identifica l'utente SIP); Call-Id (identifica

univocamente la transazione); CSeq (permette di sapere a quale richiesta si riferisce questa risposta); Expires (periodo di validita della registrazione, in secondi); Allow (metodi utilizzabili dal chiamante nella sessione SIP); User-Agent (tipo di software usato dallo UA); Authorization (credenziali di autenticazione); Content-Lenght (lunghezza del corpo messaggio, 0).
NAPTR: SIP. Tipologia di entry nel DNS, non necessariamente presente, che definisce quale protocollo di trasporto debba essere preferito per accedere al servizio (TCP, UDP, TLS/TCP, SCTP). DNS 'NAPTR' Response = Nomi servizi
Formato: domain-name | TTL | class | NAPTR | order | preference | flags | service | regexp | target
Esempio: mydomain.org | 43200 | IN | NAPTR | 0 | 0 | "s" | "SIPS+D2T" | "" | _sips._tcp.mydomain.org
SRV: SIP. Tipologia di entry nel DNS che definisce i parametri per accedere a un determinato servizio. DNS 'SRV'
Response = Nomi server
Formato: _service._proto.name | TTL | class | SRV | priority | weight | port | target
Esempio: _sips._tcp.mydomain.org | 43200 | IN | SRV | 0 | 0 | 5060 | sip1.mydomain.org
A/AAAA: SIP. Tipologia di entry nel DNS che contiene un indirizzo (A: IPv4, AAAA: IPv6). DNS 'A'/'AAAA' Response = IP server
Formato: domain-name | TTL | class | type | address
Esempio: sip1.mydomain.org | 43200 | IN | A | 10.0.0.30
UA (User Agent): SIP. End-point della rete logica, utilizzato per creare o ricevere messaggi SIP e gestire una sessione SIP. Macchina a stati che evolve in dipendenza di messaggi SIP e registra informazioni rilevanti di un dialogo. Puç fungere da client o da server.
UAC (User Agent Client): SIP. UA che manda richieste SIP.
UAS (User Agent Server): SIP. UA che riceve richieste SIP e ritorna delle risposte SIP.
Dialogo SIP: ha inizio quando si risponde positivamente al messaggio di INVITE del chiamante e termina con un messaggio di BYE.
Messaggi SIP: REGISTER, INVITE, ACK, CANCEL, BYE, OPTIONS.
Frame Relay: Standard d'interfaccia DCE-DTE (Data Comunication Equipment - Data Terminal Equipment) che mette in comunicazione reti dati con reti LAN. Necessita alte velocita 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), e soggetto a jitter quindi non va bene per trasportare voce.
CIR (Committed Information Rate): valore entro il quale si possono trasmettere fino a Bc bit alla velocita del collegamento fisico in ogni intervallo di tempo di durata Tc (per non intasare la rete). Il traffico che eccede il valore CIR non e conforme alla rete e quindi non e garantito. Bc = numero di bit che si introducono in un lasso di tempo Tc (Committed Burst Time). Tc = Bc/CIR.
Link-Local: IPv6. Indirizzo privato valido solo su un segmento di rete locale (link fisico) oppure su una connessione point-to-point. Utile per l'autoconfigurazione stateless. Un pacchetto contenente un indirizzo Link-Local non viene mai inoltrato dai router. MAC_H = 24 bit alti del MAC + settimo bit da sinistra a 1, MAC_L = 24 bit bassi del MAC. Formato: fe80:MAC_HFF:FEMAC_L/10
Site/Global: IPv6. Indirizzo pubblico accessibile a tutta la rete internet. Formato: 2001:...
Site Local: IPv6. Indirizzo privato, utile solo nel Site scope. Formato: fec0::/10
Prefix: IPv6. Sostituisce il concetto di netmask di IPv4. E' un numero di bit posto dopo un indirizzo IPv6. Esempio: FEDC:0123:8700::/10. 10 e il prefix.
Neighbor Solicitation: IPv6. Significato: "Esiste qualcuno che abbia un certo indirizzo Link-Local all'interno della mia sottorete?" Un host puo fare una richiesta per vedere se il suo Link-Local e univoco. Se riceve una Neighbor Advertisement c'e gia qualcun altro con quell'indirizzo e deve generare un altro Link-Local (altri 64 bit bassi). Se non riceve risposte puo mandare un Group Membership Report. Puo usare il NS anche per chiedere chi ha un certo Link-Local per poi generare pacchetti ICMP verso quella destinazione. Formato:
[Eth]
MAC_Source → 3333FF-MAC_Searched_L | [IPv6] :: → FF02::1:FFMAC_Searched_L | [ICMP6] N.S.: Who has Link_Local_del_MAC_Searched?
Neighbor Advertisement: IPv6. Significato: "Si, ho questo Link-Local e questo MAC" Formato: [Eth]
MAC_Source → MAC_Dest | [IPv6] Link_Local_Source → Link_Local_Dest | [ICMP6] N.A.: I am Link_Local_Source at MAC_Source

Group Membership Report: IPv6. Significato: "Ho questo indirizzo IPv6 ed e mio" Formato: [Eth] MAC → 3333FF-MAC_L | [IPv6] Link_Local → FF02::1:FFMAC_L | [ICMP6] G.M.R. (Link_Local)
Router Solicitation: Ipv6. Significato: "Uno dei router che si affacciano sulla mia sottorete puo darmi un indirizzo IPv6 pubblico Aggregatable oppure un Site Local?" Se uno dei router ha abilitato il Router Advertisement risponde. Formato: [Eth] MAC → 3333FF-000002 | [IPv6] Link_Local → FF02::2 | [ICMP6] R.S.
Router Advertisement: IPv6. Se abilitato, permette al router di rispondere ai messaggi Router Solicitation mandati dagli host e di dare agli host degli indirizzi Site/Global o Site Local. Il pacchetto contiene informazioni come il prefix annunciato, il Valid Lifetime, il MAC del router (salvato dagli host nella cache). Formato: [Eth] MAC_Router → 3333FF-000001 | [IPv6] Link_Local_Router → FF02::1 | [ICMP6] R.A.
DAD (Duplicate Address Detection): IPv6. Consiste nell'inviare in multicast un pacchetto Neighbor Solicitation per verificare che il Link-Local appena generato sia univoco nella propria sottorete. Si attende almeno un secondo. Se qualcun'altro possiede quel Link-Local, arriverà una risposta tramite pacchetto Neighbor Advertisement e dovrà essere generato un altro Link-Local. In caso contrario si considera l'indirizzo Link-Local come valido ed e possibile iniziare la fase di Router Discovery.
Autoconfigurazione Stateless: IPv6. Al boot un nodo crea automaticamente un indirizzo Link-Local, esegue la procedura DAD. Se il Link-Local e valido il nodo può parlare con tutte le macchine della propria LAN anche senza router.
Router Discovery: IPv6. E' la fase successiva all'autoconfigurazione stateless. Se esiste un router il nodo rimane in ascolto dei messaggi Router Advertisement oppure manda un pacchetto Router Solicitation. Se un router risponde a quest'ultimo con un pacchetto Router Advertisement, il nodo ottiene anche un indirizzo globale.
Neighbor Discovery: IPv6. Serve a una stazione per scoprire l'indirizzo MAC di un'altra stazione conoscendone l'IPv6. Consiste in un pacchetto Neighbor Solicitation con [MAC destinazione] = 3333FF-ultime 6 cifre IPv6 e [IPv6 destinazione] = FF02::1:FF ultime 6 cifre IP.