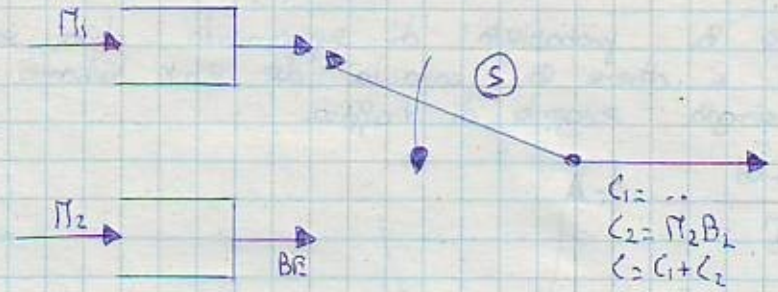
(112)

Abbiamo Π_1 sorgenti AF segmentate con $TB(\rho, \delta)$ con soglia di ritardo EDGE TO EDGE = d secondi. $Prob\{D > d\} = p$.
Poi:

Π_2 sorgenti BE con B_2 [bit/s] ciascuna (mediamente)

Core 1:



$$C_1 = \left(\Pi_1 \rho + \sqrt{\Pi_1^2 \rho^2 - h \frac{\Pi_2 \rho \delta \ln p}{2 d/h}} \right)^{1/2}$$

NB: Divido per h il budget di ritardo e la probabilità di ritardo complessiva.

Core 2: Ho più sorgenti

$$C_1 = (\Pi_1 + \Pi_3)\rho + \sqrt{\Pi_1^2 \Pi_3^2 \rho^2 - h \frac{\Pi_1 + \Pi_3 \rho \delta \ln p/h}{2 d/h}}^{1/2}$$

$$C_2 = \Pi_2 B_2$$

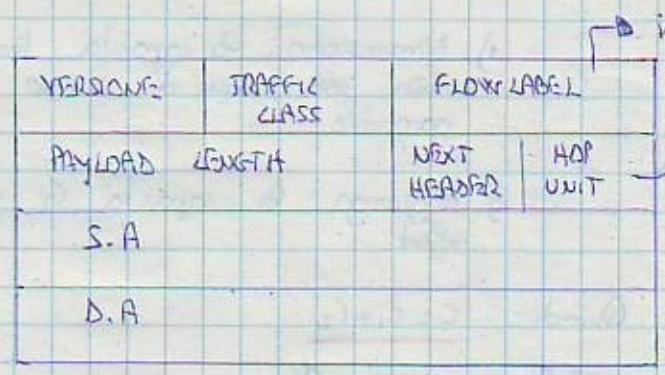
$$C = C_1 + C_2$$

Vediamo ora di parlare brevemente anche dell'indirizzo IPV6. IPV6 ha indirizzi di 128 bit e quindi si possono indirizzare 2^{128} indirizzi differenti. Poi gli indirizzi IPV6 hanno una loro struttura gerarchica già implicita e hanno un header flessibile.

HBASE	EXTENTION HEADER	. . .	PAYLOAD

NB: L'header viene impilato in maniera ricorsiva.

Vediamo ora l'header base di IPV6:



L'header base è lungo 40 byte, e non c'è nessuna frammentazione.

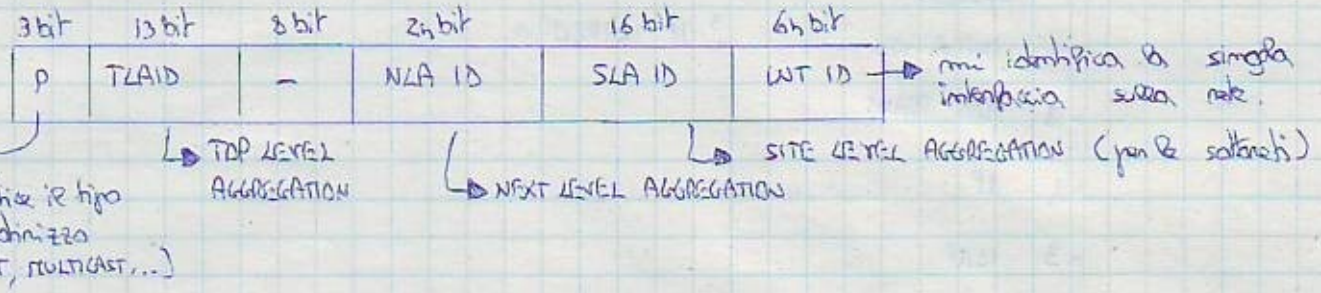
Per quanto riguarda il pacchetto TCP:

HEADER BASE NEXT: TCP	TCP SEGMENT

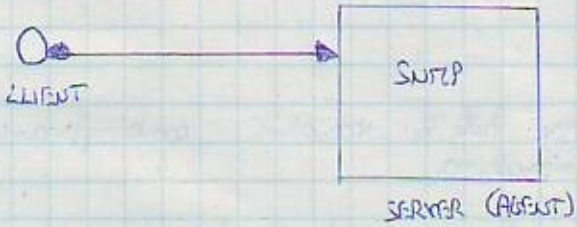
Per quanto riguarda le opzioni:

HEADER BASE NEXT: ROUTE	HEADER ROUTE NEXT: TCP	SEGMENT TCP

Qui i router non possono frammentare. Si frammenta le pacchetto all'origine della macchina. La gestione della dimensione dei pacchetti è in più complessa in una rete IPV6 e dovrebbe essere garantita da una MTU di 1280 byte. Purtroppo IPV6 ha dei punti negativi tra cui la notazione DOTTED DECIMAL che produce indirizzi molto maneggiabili. A rete si usa la notazione esadecimale. Noi ora vediamo indirizzi IPV6 unicast.



Per quanto riguarda ICMP versione 6, oltre a includere funzioni già viste mi contiene ARP, RARP, IGMP. Vediamo ora di introdurre SNMP (Simple Network Management Protocol). Ogni dispositivo di rete ha al suo interno un server SNMP.

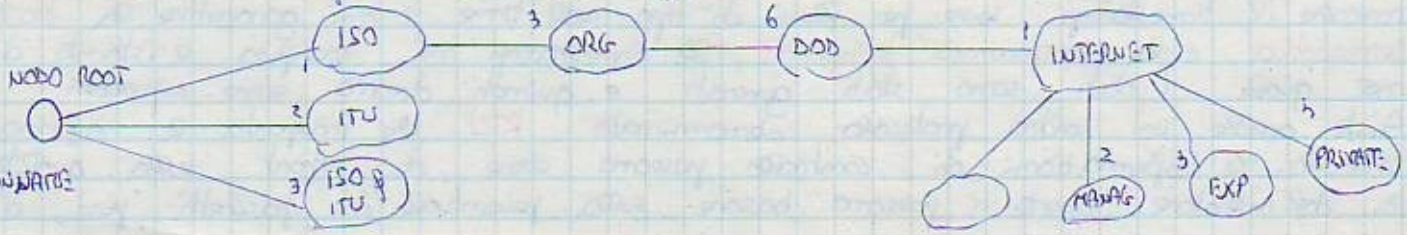


Si noti che il client è sostanzialmente un software che sta sul computer del Network Manager.

SNMP funziona su TCP. È sostanzialmente un'applicazione che mantiene sul server i dati di configurazione (READ, WRITE) e mantiene le statistiche di funzionamento. Per esempio per un router:

pacchetti ricevuti
pacchetti trasmessi
:

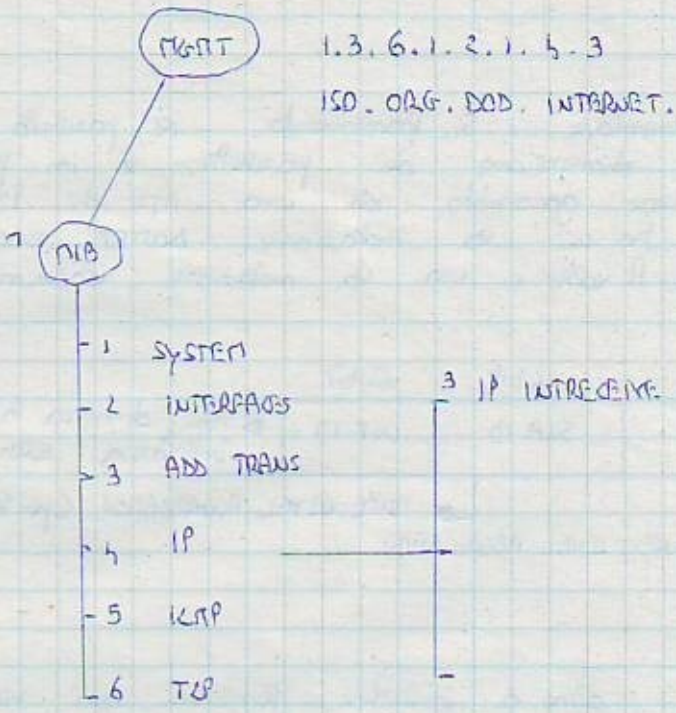
L'agent SNMP ha un database locale (MIB = Management Information Base), che elenca le variabili gestite dal dispositivo e specifica i permessi. La MIB è fornita dal costruttore, ma le Network Manager può customizzarla. Una questione piuttosto critica sono i nomi delle variabili. Esistono standard dei nomi delle variabili. Si hanno dei nomi definiti in modo gerarchico secondo un albero:



Tutti i nomi di qualsiasi variabile in Internet iniziano così:

1.3.6.1.2 ... nome di un qualsiasi dispositivo in Internet.

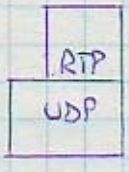
Esempio:



I comandi SNMP sono di tipo READ/WRITE. Sono comandi indiretti tramite variabili di decisione.

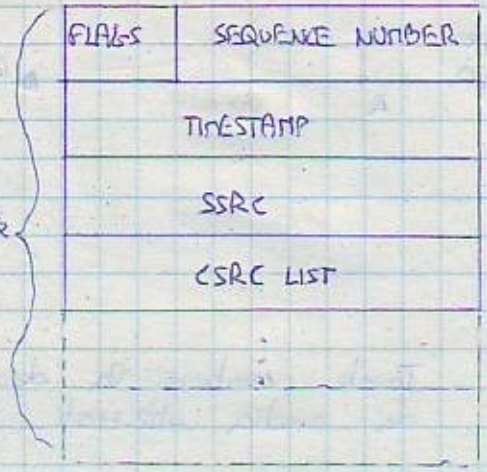
- GET - REQUEST
- SET - REQUEST
- GET - BULK - REQUEST → mi legge tutte le variabili contemporaneamente di una macchina.

Parliamo ora del protocollo RTP.
RTP è l'acronimo di Real-time-protocol ed è il protocollo di trasporto per applicazioni di tipo real time (voce, audio, video). RTP si appoggia su UDP.



In particolare il protocollo RTP non fa il multiplexing. L'interfaccia superiore di RTP non è standardizzata. RTP funziona sia in UNICAST che in MULTICAST. Gestisce quindi le comunicazioni multimediali tra gruppi. Esso è leggero e veloce. L'header delle RTP possiede due particolari campi denominati sequence number e timestamp. Il sequence number serve per segnare le perdite di pacchetti o i fuori sequenza, mentre il timestamp serve per flussi di tipo real-time e mi garantisce la trasparenza semantica e la trasparenza temporale. Il timestamp mi codifica l'istante di tempo nel quale i dati sono stati generati e quindi devono essere riprodotti.
Esiste anche un altro protocollo denominato RTCP che trasporta le informazioni di controllo. Le informazioni di controllo possono essere dei report sulla qualità ricevuta dal ricevitore. Queste si possono basare sulla percentuale di pacchetti persi, o sulla

variazione del ritardo. L'RTP ha delle funzioni di controllo anche per l'apertura, la chiusura, e la gestione delle connessioni. Analizziamo la struttura dei pacchetti RTP:



→ codice ID della sorgente che ha originato le TIMESTAMP.

RTCP invia periodicamente un rapporto di qualità a tutti i partecipanti. Se ho N partecipanti, il traffico di controllo è proporzionale a circa N^2. Quindi il periodo di invio dei rapporti RTCP è adattato in funzione del numero di partecipanti in modo da mantenere il traffico di controllo circa al 5% del traffico di informazione.

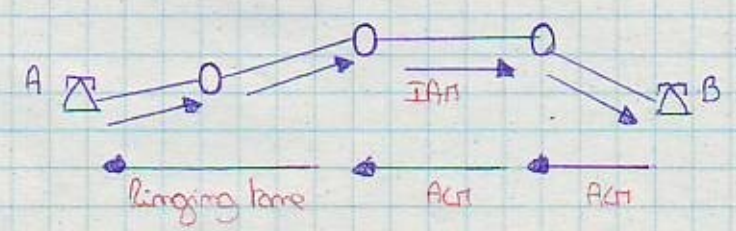
Parliamo ora della telefonia classica (PCM). Essa possiede:

1) piano utente
2) piano di controllo

La rete PCM viene campionata a 64 kbit/s a circuito costante. La qualità del servizio nella telefonia classica è molto ridotta. Essa non ha problemi perché la qualità nel PCM è molto elevata. Le varie centrali telefoniche si parlano tramite SIGNALING LINK a 64 kbit/s. Il piano di controllo della telefonia classica è un'intera architettura protocollare a pacchetto. Sia:

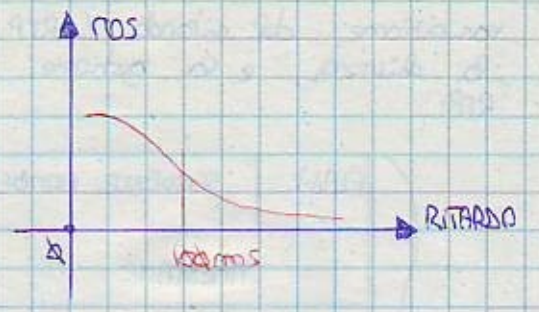
SS7 → SIGNALING SYSTEM 7

Quando effettuiamo una chiamata si ha:



IAM = Initial Address Message

La centrale invia tramite l'applicazione ISUP = Integrated Service User Part un messaggio IAM. Si instaura così una connessione END TO END. Quando B fa scattare il telefono, viene generato un messaggio ACM = Address Complete Message. Quando B alza la cornetta, viene generato un messaggio di risposta (ANS). Invece quando A chiude viene generato un messaggio REL (Release) e quando B a sua volta chiude spedisce un messaggio RELC (Release Complete).
RTCP va bene per il controllo della qualità, ma per la gestione delle connessioni bisogna usare altri protocolli. Se si ha come traffico il VoIP le centrali diventano dei router. La qualità del servizio sta nel piano utente come il MOS = Mean Opinion Score percepito dall'utente.

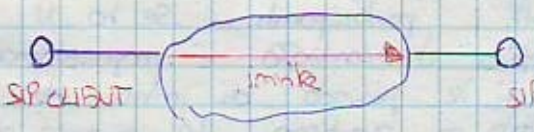


In VoIP il QOS cala all'aumentare del ritardo.

Parliamo ora di SIP (Session Initiation Protocol). Essa è un'applicazione di tipo client-server che serve per creare, gestire, terminare delle sessioni. SIP si occupa anche della segnalazione cioè del piano di controllo. La comunicazione può avvenire:

1) multicast
2) maglia di relazioni punto-punto

Graficamente:

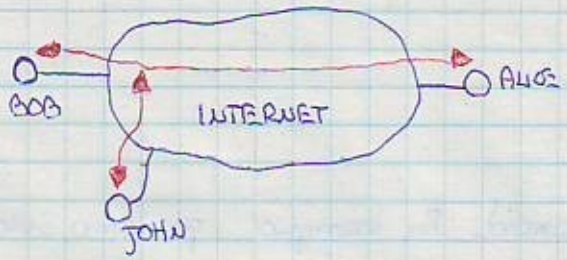


Invite contiene la descrizione dei media utilizzati.

Tipicamente si ha:

Una volta instaurata la connessione, il piano utente viaggia diretto tra i client. Gli indirizzi SIP vengono anche detti SIP URI (Universal Resource Identifier). Una SIP URI può essere richiamata anche mediante numero di telefono.

Concludiamo parlando di sicurezza. Consideriamo la seguente situazione:



John può intercettare la comunicazione tra Bob e Alice. Esistono fondamentalmente due tecniche per evitare ciò:

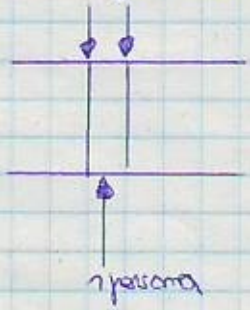
- end to end encryption
- tunnelling IP

Il tunnelling IP l'abbiamo già analizzato. Nelle aree più critiche cioè nelle aree dove ci sono i servizi più critici si ricorre alla sicurezza fisica (physical Security).

NB: Il perimetro più interno è un perimetro ad alta sicurezza.

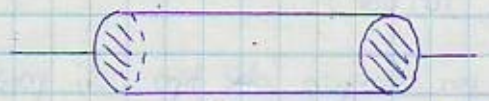
Il perimetro interno deve avere tutta una serie di caratteristiche tra cui:

1) numero limitato di accessi
2) Accessi controllati da porte comandate da Smart Card.
3) Porte doppie



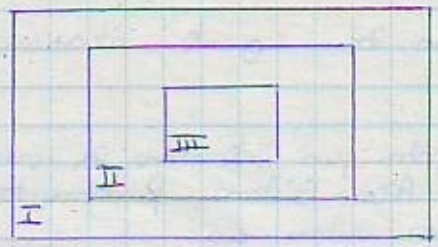
4) Il perimetro deve essere realizzato con muri contenenti una schermatura di piombo (gabbia di Faraday). I segnali radio non si devono propagare al di fuori del perimetro stesso.

5) I cavi che collegano il perimetro interno al perimetro esterno sono così fatti:

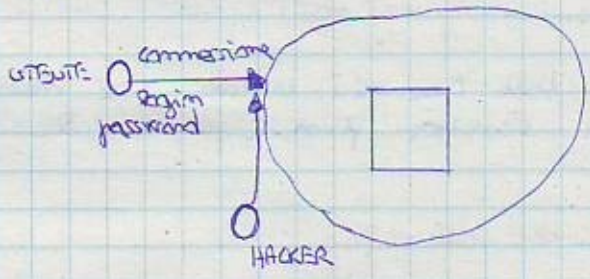


TUBO CON GAS INTERNO.

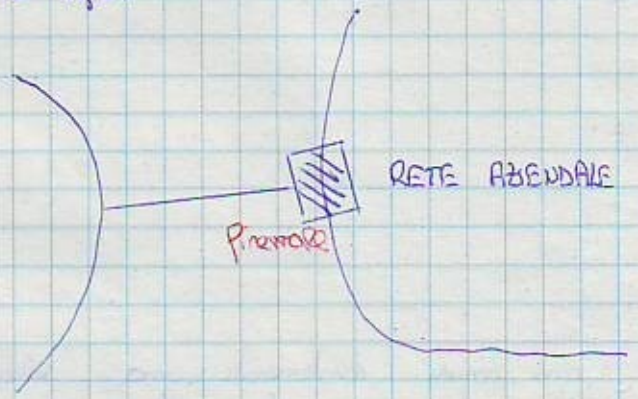
Un altro problema, non da poco, che bisogna gestire è l'accesso da parte di persone provenienti da altre aziende. In merito si divide gli edifici in zone di livello sempre più critiche.



Tale accesso può essere regolamentato da password. Per esempio possiamo usare una semplice password:



oppure possiamo usare password speciali come per esempio one-time-password che altro non è che una password che funziona una sola volta. Oggi si usano le password generate (con interfaccia USB). Comunque è il network manager che svolge la fase di configurazione in modo tale da avere la password disponibile per ogni accesso. Infine ci sono le password biometriche come per esempio password che sfruttano la scansione della retina o la scansione delle impronte digitali. Quest'ultime password sfruttano i così detti sistemi PR (Pattern Recognition). Questi sistemi sono sistemi di riconoscimento di pattern ossia sistemi di riconoscimento di oggetti che rappresentano determinati fenomeni fisici. Supponiamo ora di avere una situazione di questo tipo:



Un firewall è una "strumento" che controlla i pacchetti in ingresso ed esegue il filtraggio. Il filtraggio può essere di tre tipi:

1) filtraggio su base utente (filtraggio su S.A, login, password).
2) filtraggio su servizio (sfruttando porte TCP/UDP)
3) filtraggio a livello applicativo (verifica per esempio del tipo di payload).

Quindi un'azienda che ha una o più connessioni esterne deve installare un firewall su ciascuna di esse e poi coordinare tutti i firewall. Abbiamo visto che una azienda viene suddivisa in zone in base alla criticità dei servizi forniti dai vari livelli.