MOBILITÀ: interessiamo la mobilità del terminale; al suo spostamento sposto comunque le comunicazioni [⇒ SONO SEMPRE CONNESSO]

NOMADICITÀ: utilizzare interfacce di rete in maniera discontinua per poter comunicare; ESEMPIO ⇒ ho un PC, sono a casa, e sono connesso alla rete; devo andare in ufficio ⇒ spengo la macchina [⇒ sono disconnesso dalla rete] e vado in ufficio; arrivo in ufficio, riaccendo il PC e mi collego alla rete aziendale

⇒ Durante lo spostamento non sposto le comunicazioni!

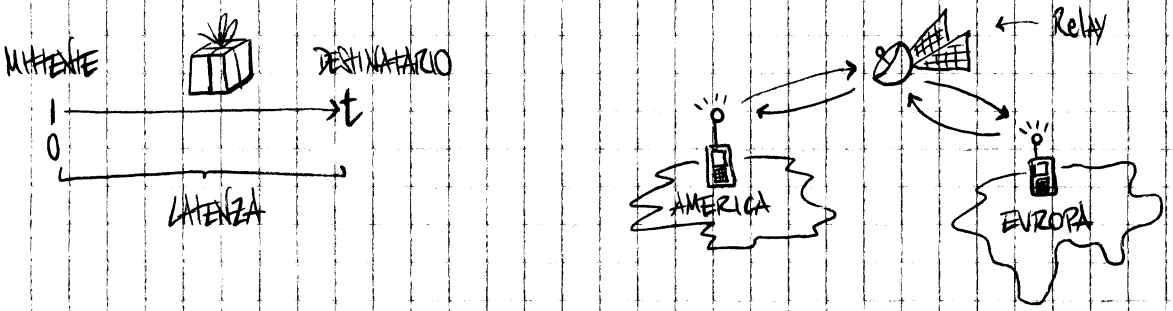
Applicazione non interattiva ⇒ per es: posta mail; se ricevo/trasmetto con ritardi comunque non succede niente

Applicazione interattiva ⇒ per es: VoIP [FORTEMENTE INTERATTIVA] non permette/tollera ritardi;

100 millisecondi = tolleranza MASSIMA [≃ tempo per dire una lettera/parola parlata];

Streaming Video = applicazione BLANDAMENTE interattiva grazie al BUFFERING

Più è necessaria/richiesta l'INTERATTIVITÀ e più è difficile garantire tale servizio



Architettura che introduce ritardi, pur garantendo la Mobilità: tempi di LATENZA enormi ≃ 300 millisecondi

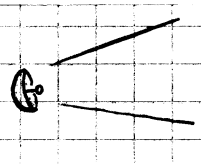
WIRELESS → Largo Raggio [2-3 Km]: GSM, GPRS, UMTS, WiMAX → permette le comunicazioni in zone in cui è difficile mettere celle con raggio d'azione di 2-3 Km [per es: deserto]; permette raggio fino 10/20 Km ... si riceve 1 Mb/sec vicino alla cella; a 20 Km di distanza molto molto meno!

→ Brave Raggio: Bluetooth, WiFi, ZigBee → 10/20 metri di raggio, con banda passante molto bassa in modo da non avere consumi alti; per es: centraline per il monitoraggio dell'ambiente

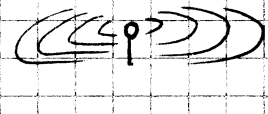
↓ BASA SULLA CONNETTIVITÀ RADIO

ACCESS POINT: permette all'utente mobile di collegarsi ad una rete wireless direttamente al suo terminale se dotato di scheda wireless; se un AP è collegato fisicamente ad una rete cablata può ricevere e inviare un segnale radio all'utente permettendo la comunicazione sotto forma di accesso radio.

Nelle tecnologie wireless a largo raggio e a breve è importante la potenza del segnale emesso; più aumento la potenza e più aumenta la distanza raggiungibile ... però più potenza ≡ più consumo l'energia ⇒ DIMINUZIONE BATTERIA!



concentro le comunicazioni verso un unico punto ⇒ meno dispersione segnale ;



il segnale viaggia verso ogni direzione ⇒ più dispersione

SIGNAL TO NOISE RATIO:

Rapporto Segnale-Rumore;

è un numero puro/adimensionale che esprime quanto il segnale sia più potente del rumore;

$$SNR = \frac{\text{POTENZA SEGNALE}}{\text{POTENZA RUMORE}}$$

[Potenza Segnale e Potenza Rumore vengono misurate in Watt o in dBm [DECIBEL]]

Ogni sistema che deve trasportare o trattare informazioni è affetto da rumore [per es: RUMORE TERMICO]; più è grande la potenza del rumore, minore è la qualità della comunicazione ⟹ necessario massimizzare o preservare il SNR; più basso è il SNR, più è difficoltosa la codifica del segnale trasmesso

MODULAZIONE:

insieme delle tecniche di trasmissione finalizzate ad imprimere un segnale elettrico o elettromagnetico, detto MODULANTE, su un altro segnale elettrico o elettromagnetico, detto PORTANTE, che ha invece lo scopo di trasmettere le informazioni del modulante ad "alta frequenza", ovvero converte il segnale modulante da BANDA BASE a BANDA TRASLATA; la PORTANTE, una volta "affetta" dalle informazioni del modulante viene chiamato segnale MODULATO.

Per ritornare da segnale MODULATO a segnale originario [⇒ BANDA BASE] si effettua l'operazione inversa: DEMODULAZIONE.

MODEM = MODULAZIONE - DEMODULAZIONE

NAT - Network Address Translation

tecnica di modifica degli indirizzi IP dei pacchetti che transitano su un router;

è implementato da router o firewall; effettuano modifiche a livello NETWORK e TRANSPORT

TIPI DI NAT:

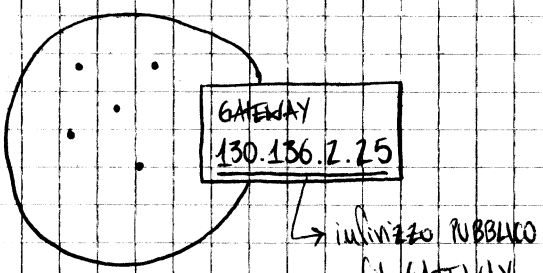
- se viene modificato l'indirizzo mittente ⇒ SOURCE NAT
- se viene modificato l'indirizzo destinazione ⇒ DESTINATION NAT

FIREWALL

Apparato di rete HARDWARE o SOFTWARE che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un host, applicando regole che contribuiscono alla sicurezza della comunicazione.

Può effettuare operazioni di READ e WRITE sugli header e sui Payload dei pacchetti.

Firewall e NAT



indirizzo PRIVATO

Consideriamo un HM all'interno della rete 192.168.1.X, avente come indirizzo IP 192.168.1.20, che vuole parlare con il CN; vuole inviare pacchetti sulla porta 80 del CN; i pacchetti uscenti dalla SUBNET passano per la porta 40'000 del Gateway

CN
1.1.1.1

⇓

TCP (192.168.1.20 40'000 ; 1.1.1.1 : 80)

⇐

il NAT cambia il 1° elemento del segmento TCP:

tcp (130.136.2.25 : 40'000 ; 1.1.1.1 : 80)

Se nella SUBNET vi è un altro HM che vuole comunicare con il CN passando per la porta 40'000 del Gateway e parlando per la porta 80 del CN ⇒ il NAT trasforma il segmento TCP in: TCP (130.136.2.25:40000; 1.1.1.1:80)

⇒ però la porta 40'000 è occupata ⇒ cambia la porta in 40'001, ma il HM non sa di questo cambiamento!

⇒ quando il CN risponde: TCP (1.1.1.1:80; 130.136.2.25:40'001) ⇒ il NAT capisce a chi è in realtà indirizzato, cambia nuovamente da 40'001 a 40'000, grazie alle tabelle di IP del NAT.

Se un ulteriore CN manda pacchetti sulla porta 40'000 abbiamo 2 soluzioni:

1. BLOCCHIAMO il flusso, usando un FIREWALL SIMMETRICO;
2. non lo BLOCCHIAMO, ottenendo un "porto di mare".

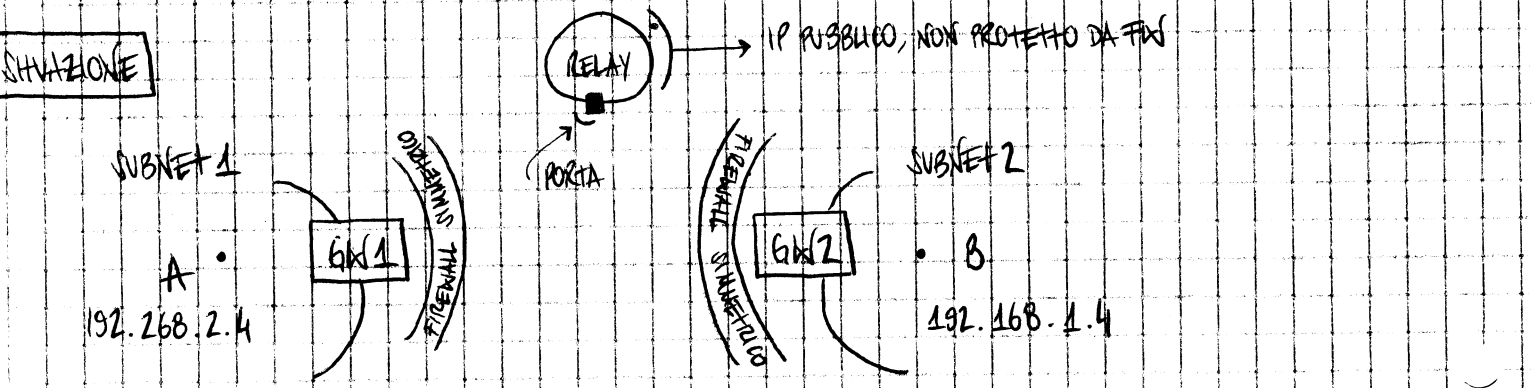
Se il mittente non invia più pacchetti sulla sua porta, dopo qualche minuto, la porta viene chiusa dal NAT.

N.B.

Se io NODO appartengo ad una rete schermata da NAT e FIREWALL, a meno che non sia io a contattare qualcuno all'esterno, nessuno da fuori può contattarmi!

Se io sono in una rete natted e voglio parlare con qualcuno dentro una rete natted: NON RIUSCIAMO!

SITUAZIONE



Se A ha intenzione di parlare con B, non invia neanche al GW2 ⇒ perdita pacchetti!

Supponiamo che la SUBNET 2 abbia indirizzi pubblici, con IP 130.136.4.200; se A prova a parlare con B, il GW2 blocca i pacchetti A → B, poiché deve essere B ad iniziare per prima la comunicazione.

Naturalmente, anche se A è in una rete con indirizzi pubblici, comunque B → A è impossibile!

⇓

1) CON I FW SIMMETRICI, O INIZIO LA COMUNICAZIONE, O NIENTE COMUNICAZIONE;
2) IMPOSSIBILE LE CONNESSIONI DIRETTE.

Introduciamo nello schema un RELAY:

↳ A e B sono indirizzi privati;

A manda un pacchetto, aprendo la comunicazione, alla porta del relay, dicendogli che vuole parlare con B;

B manda un pacchetto alla medesima porta del relay dicendogli che vuole parlare con A

⇓

viene utilizzato il Relay come tramite tra A e B ⇒ svolge da CORTOCIRCUITO!

Naturalmente uno tra A e B ogni tot di tempo deve inviare dei pacchetti sulla porta del relay per tenerla aperta alla comunicazione!

Poiché ogni dato passa per il relay ⇒ ⊙ aumenta la latenza;
⊙ se più comunicazioni passano per il relay ⇒ diminuzione banda passante

Inoltre, poiché il relay deve identificare gli estremi della comunicazione [A e B] ⇒ è necessario un PROTOCOLLO a LIVELLO APPLICAZIONE che dice al relay che A vuole parlare con B.

PROTOCOLLI ICE - TURN - STUN:

- tecniche utilizzate per il superamento dei FW SIMMETRICI tra 2 host;
  funzionano se 1 dei 2 non è coperto da FW SIMMETRICO;
  se entrambi sono coperti da FW SIMMETRICO ⟹ non funzionano!

Il protocollo ICE viene utilizzato per determinare quale tra le 2 tecniche STUN e TURN sia la migliore per il superamento dei FW;

l'idea principale di queste tecniche è di non dover utilizzare il relay di supporto per avere la comunicazione. Queste tecniche provano a capire dei tra 2 host, A e B, è coperto da FW SIMMETRICO, invitandolo ad iniziare per primo la comunicazione

- TURN:

A deve inviare a B, e il protocollo TURN scopre che A è coperto da FW non SIMMETRICO
↳ A invia un pacchetto $[IP_A = 192.268.2.4 ; P_A = 40000]$ al relay;
il FW davanti ad A cambia l'indirizzo IP mittente, e [forse] la porta
↳ pacchetto $\equiv IP_{A(FW)} : 130.136.2.25 ; P_{A(FW)} : 40000$ [oppure 50000]

una volta ricevuto tale pacchetto il relay ritorna tali credenziali ad A ⟹ gli suggerisce come questo viene visto dall'esterno.

- Se il relay suggerisce queste informazioni a B ⟹ B può iniziare la comunicazione con A poiché ne conosce le credenziali criptate.

Nel caso di FW SIMMETRICI questo non può essere fatto poiché, se A è protetto da FW SIMMETRICO, deve essere lui stesso ad iniziare la conversazione.

CRITERI SCELTA AP

Di norma si utilizza la potenza del segnale - con relativi problemi; altri criteri:

- Banda passante disponibile ⟹ prova DOWNLOAD, però si perde tempo ⟹ non è utile per tempi di comunicazione;
- # pacchetti persi in un tot di tempo.

↳ MIX per la scelta delle tre!

HANDOVER:

procedura, composta da più fasi, durante la quale un terminale cambia la sua associazione da un AP ad un altro

↙

il NM è connesso ad un AP, si rende conto che l'interfaccia sta per "morire" ⟹ molla l'AP a cui è collegato, ne cerca un altro, e una volta trovato vi si collega!

FASI:

- ⊙ rilascio l'AP;
- ⊙ ricerco un nuovo AP;
- ⊙ scelgo un AP;
- ⊙ mi ci configuro

(PERDITA CONNESSIONE: dal rilascio dell'AP fino alla configurazione)

> [illegible] che legge i pacchetti PROBE inviati dagli altri AP

Questo è quello che avviene quando accendo il NM la prima volta!

∃ 2 tipologie di Handover:

① HANDOVER ORIZZONTALE ⟹ ho 1 interfaccia di rete disponibile sul mio NM, ed una volta che mi si scollega con un determinato ne cerca un altro per poi collegarvisi.

② HANDOVER VERTICALE ⟹ ho 2 interfacce di rete; sono collegato con la #1 che cade ⟹ lascio l'AP e ne trovo uno nuovo quale agganciarmi con l'interfaccia #2 [**GRAN CONSUMO DI ENERGIA**]

HANDOVER ORIZZONTALE:

Esistono delle tecniche per velocizzare l'Handover Orizzontale, per esempio GRATUITOUS ARP; queste tecniche funzionano così: appena l'interfaccia sta per cadere, l'AP a cui è collegata segnala a degli altri AP' che tale interfaccia è nei guai... questi AP' determinano quale tra loro è il migliore per l'interfaccia, la vecchia AP si sgancia e l'interfaccia si aggancia al miglior AP!

↓

Questa tecnica non può essere utilizzata nell'Handover Orizzontale, poiché generalmente, se ho 2 interfacce queste sfrutteranno protocolli differenti.

N.B.

momento 1: NM (INTERFACCIA #1: COLLEGATA ; INTERFACCIA #2: SCOLLEGATA) ; momento 2: mi cade la #1 e nel mentre la #2 si era collegata, ed è tutt'ora collegata... le 2 hanno IP diversi tra loro

⇓

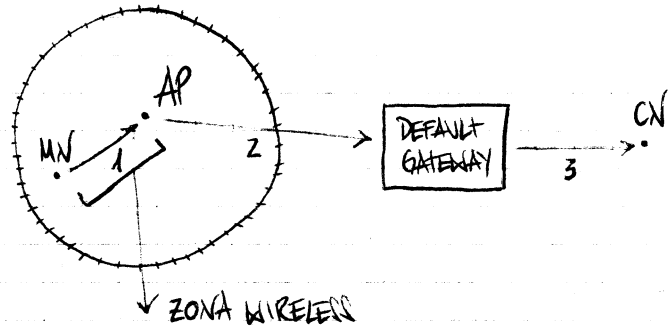
il CN con il quale comunicavamo con l'interfaccia #1 non riconosce l'IP della #2

CRITERI CAMBIO ACCESS POINT:

Un criterio potrebbe essere che ho una gran perdita di pacchetti ... in entrata o in uscita?

IN USCITA:

È necessario capire in quale punto avviene la perdita;



(1) Punto più critico, poiché wireless; ritrasmetto.

(3) Il CN deve trasmettere degli ACK;
lo MN deve attendere un tempo t per ricevere tali ACK;
tale t deve essere $\geq$ RTT [tempo per andare da MN a CN e tornare indietro] → Questa tecnica non può funzionare nelle comunicazioni INTERATTIVE

Poiché (1) è il punto più critico ⇒ posso usare la tecnica vista per il punto (3) dato che RTT è sicuramente minore in questo caso... ma l'AP è un'infrastruttura, ed è difficile modificarne le politiche burocratiche [non TECNICHE]; con i CN è più facile!

In generale a livello Datalink si sa se un pacchetto è stato perso o meno;
nel WiFi, quando MN $\xrightarrow{\text{📶}}$ AP, l'AP deve dare l'ACK al MN immediatamente [in teoria potrebbe essere perso anche l'ACK, ma è più raro che ciò si verifichi poiché le dimensioni dell'ACK sono <<< rispetto a quelle del pacchetto].
Il # di volte che deve essere ri-inviato un pacchetto perso nel WiFi è compreso tra 1 e 15, mediamente 7.
È il livello Datalink che si accorge se ho perso un pacchetto: i livelli APPLICATION, TRASPORT e NETWORK non se ne rendono!
In particolar modo il livello Data Link si rende conto:
- ⊙ se il pacchetto è stato perso;
- ⊙ quante volte è stato ritrasmesso.

Se queste informazioni riescono a farle giungere fino al livello APPLICAZIONE, ovvero fare all'applicazione se dei pacchetti sono stati persi o meno, l'applicazione stessa, una volta resasi conto che il # di ritrasmissioni è molto vicino a 7, potrebbe decidere se cambiare o meno l'interfaccia.

⟹

INDICI UTILI PER CAPIRE SE NECESSARIO CAMBIARE INTERFACCIA OPPURE NO

- # di pacchetti persi
- % di ritrasmissione pacchetti riuscita

Questi 2 indici cambiano a seconda della tecnologia, WiFi, UMTS, WiMAX, ecc..

- potenza segnale ricevuto dell' AP

↳ indice attualmente utilizzato, anche se come pecca ha che il segnale potrebbe essere ricevuto dal NM al 100%, ma quell' AP potrebbe gestire l'intero traffico, rendendo lente le comunicazioni.

⇓

nel momento in cui dovrei effettuare lo scambio di interfacce non sarei in grado di dire se WiMAX è migliore di UMTS, o WiFi migliore di WiMAX ecc...

MIH - Media Independent Handover

Protocollo che lavora a livello FISICO e DATALINK;

cerca di far avere ai livelli superiori delle informazioni riguardanti il buon o mal funzionamento delle differenti interfacce presenti sul NM.

Avvisa i livelli superiori quando:

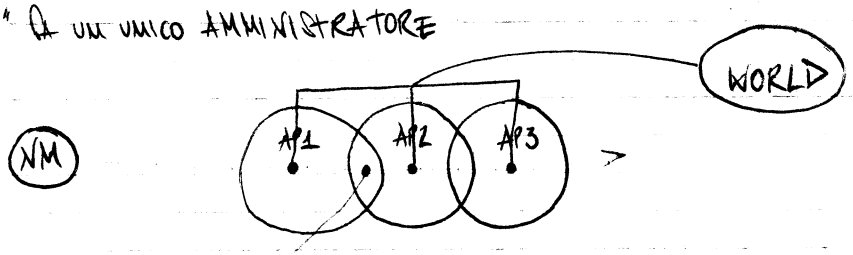
- una interfaccia NON è più attiva;
- una interfaccia è configurata correttamente e pronta per la trasmissione;
- [una interfaccia è sul punto di non funzionare.

↳ vuol dire che ci sono 2 possibilità: ① CADE; ② SI RIPRENDE.

GRATOITOUS ARP [Handover Orizzontale]

- posso fare controlli sulla potenza del segnale
- INTERFERENZA

Ci troviamo nella situazione in cui in una certa area ho vari AP, che lavorano sullo stesso canale e sono "sorvegliati" da un unico AMMINISTRATORE



↳ AP1 rompe a AP2, e viceversa, AP2 rompe a AP3 e viceversa; AP1 e AP3 non si danno fastidio

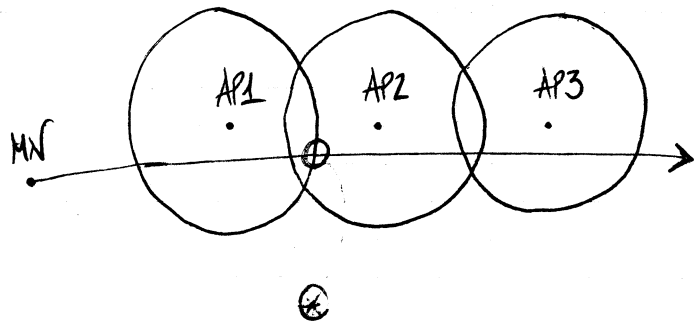
Attraverso BACKBONE i vari AP1, AP2 e AP3 si scambiano informazioni riguardanti le potenze dei segnali ricevute dai vari nodi mobili che si trovano nelle varie zone gestite da AP1, AP2, AP3.

Sia qui il NM passando dalla zona di AP1 a quella di AP2 [con NM agganciato a AP1] ⇒ AP1 avverte AP2 che NM riceve meglio da AP2 che da AP1

↳ AP1 invia al NM un GRATOITOUS ARP, facendo credere al NM che MAC1 sia in realtà MAC2 ⇒ in questo modo il NM pensa di essere collegato ancora a AP1 ma in realtà è attaccato a AP2

↳ ATTRAE IL NM DALL' HANDOVER

SITUAZIONE [PROBLEMA NON ANCORA RISOLTO]



N.B. AP1, AP2, AP3 potrebbero lavorare su canali differenti, essere gestiti da Provider differenti, ecc...

Quando il MN si trova nel punto ⊕ deve effettuare una scansione di frequenze e canali per capire a chi collegarsi poiché sta perdendo segnale da AP1.

Ogni 100 millisecondi un AP trasmette se è libero e a quali frequenze e canali è possibile agganciarsi

↳ 11 canali * 100 millisecondi ⇒ 1,1 secondi

↘ ≡ tempo impiegato da un MN per monitorare la presenza di Access Point;

- inoltre il MN deve anche connettersi all' Access Point, e per farlo ci impiega un pò di tempo

↳ ≃ 1,5 secondi per monitorare e connettersi!

⇒ nel mentre il MN effettua tali operazioni farà avvisare l' AP1 che per un tot di tempo resterà in standby per quanto riguarda la comunicazione ⇒ l' AP1 durante tale standby bufferizza [se ha memoria buffer sufficiente] i pacchetti diretti al MN, per poi riconsegnarglieli una volta che il MN ha terminato lo standby

⇓

- ⊙ 1,5 secondi sono tanti nelle comunicazioni VOIP e/o fortemente interattive;
- ⊙ dopo aver scansionato, riallacciatomi per poco ad AP1, e provare a collegarmi con un altro AP, la situazione potrebbe essere cambiata nel mentre ⇒ "VECCHIA VISIONE" della disponibilità degli AP, che potrebbero non essere più disponibili;
- ⊙ i buffer potrebbero essere pieni o comunque non sufficienti.

⇓

SOLUZIONE:

avere 2 interfacce omogenee sullo stesso nodo mobile [per es: 2 WiFi] dove #1 riceve/trasmette, e l'altra scansiona ⟶ con 2 interfacce però ho un gran consumo di energia;

le 2 antenne delle 2 interfacce inoltre potrebbero non avere la stessa visione del mondo esterno per esempio potrebbero creare interferenze tra di loro, avere una differente concezione del posizionamento del MN, ecc...]

⇒ SCANSIONE CANALI + configurazione Livello DATA LINK e Network: TEMPO TROPPO GRANDE PER INTERATTIVITÀ