Capitolo 4

Tecnologia e metodi utilizzati

L'apparecchiatura utilizzata in questa tesi è basata sullo standard 802.11a, che simula il comportamento dello standard 802.16.

4.1 Introduzione

L'obiettivo di questa tesi, è stato quello di implementare un canale fisico di comunicazione basato sullo standard **IEEE 802.16** per reti WiMax.
È stato messo in opera il **link Point-To-Point**, al fine di valutare la robustezza del canale e le performance del dispositivo (qualità e velocità). Una prima fase è stata destinata alla raccolta di materiale sull'argomento, attraverso la consultazione di siti web, pubblicazioni e libri; il tutto per avere un approfondimento sulla tecnologia **WiMax**: basi teoriche, caratteristiche tecniche, punti di forza e gli eventuali possibili utilizzi.
Successivamente, si è dedicata una parte di tempo alla consulta di datasheet e di manuali sui dispositivi in dotazione, al fine di poter rendere possibile l'utilizzo degli stessi dispositivi. Si è proseguito, quindi, con dei test preliminari, necessari per comprendere meglio la gestione software dell'apparecchiatura. La fase successiva è stata quella della realizzazione di un collegamento punto-punto con connettività basata sulla tecnologia oggetto dei nostri interessi. Utilizzando diverse macchine collegate alle due stazioni, sono stati creati flussi d'informazione per valutare le prestazioni del link.
Le informazioni e i dati necessari per un'analisi del sistema, sono stati raccolti utilizzando software per lo *sniffing*; l'archiviazione è avvenuta utilizzando criteri propedeutici alla logica seguita durante le prove di carico.

Il traffico sul canale è stato opportunamente differenziato: *Real Time Packet* (**rtPS**) con lo streaming audio/video, *Extended Real Time* del VOIP (**Voice Over IP**), *Non-Real Time Packet* (**nrtPS**) per traffico basato su protocollo HTTP e FTP.
Per una maggiore qualità del lavoro effettuato, si è ritenuto opportuno aggiungere variabili quali "distanza" (tra BS e SS) e "potenza".

A tale scopo, ogni prova si è ripetuta per diverse distanze (0, 120, 500, 1200 metri) in modo da poter generare, durante l'analisi dei risultati, delle curve intuitive e leggibili per comprendere meglio il comportamento del sistema.

4.2 Dettagli del modello implementato

4.2.1 Hardware utilizzato

L'apparecchiatura utilizzata è stata fornita dalla **Proxim**, azienda leader nella realizzazione di componenti e antenne per la creazione di reti wireless a banda larga.
In particolare, per gli scopi della tesi, si è adoperato [28]:

- **Tsunami MP.11 5054-R Base Station Unit with Integrated 23 dBi Antenna** (Figura 4.1);
- **Tsunami MP.11 5054-R Subscriber Unit with Integrated 23 dBi Antenna** (Figura 4.2);

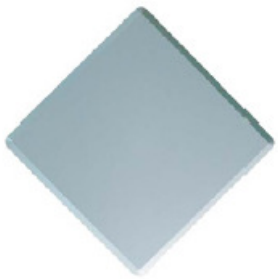

Figura 4.1. Tsunami MP.11 5054-R Base Station with Integrated 23 dBi Antenna.

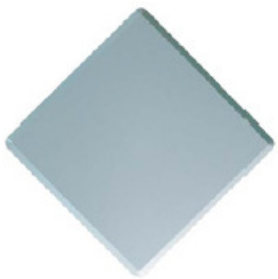

Figura 4.2. Tsunami MP.11 5054-R Subscriber Unit with Integrated 23 dBi Antenna.

Le frequenze utilizzate da queste componenti, sono frequenze senza licenza (5.47-5.725 GHz) utilizzabili per attività di ricerca.

Le caratteristiche dell'attrezzatura utilizzata, sono riportate nella Tabella 4.1.

PRODUCT MODEL	TSUNAMI MP.11 4954-R
RADIO & TRASMISSION	
MODULATION METHOD	OFDM (Orthogonal Frequency Division Multiplexing)
DATA RATE	54,48,36,24,18,12,9,6,4.5,3,2.25,1.5 Mbps
INTERFACES	
WIRED ETHERNET	10/100Base-TX Ethernet (RJ-45); SUR includes integrated 23 dBi antenna
WIRELESS PROTOCOL	WORP
ANTENNA CONNECTOR	Standard N-Female (BSUR & SUA)
PHYSICAL	
DIMENSIONS	
PACKAGED UNPACKAGED	14.6 x 13.7 x 8.2 in (370 x 348 x 208 mm) BSUR, SUA: 10.5 x 10.5 x 3.25 in (267 x 267 x 83 mm) SUR : 12.6 x 12.6 x 3.5 in (320 x 320 x 89 mm)
WEIGHT	
PACKAGED UNPACKAGED	BSUR, SUA: 10.2 lbs (4.6 kg) SUR: 11.1 lbs (5.02 kg) BSUR, SUA: 6.5 lbs (2.94 kg) SUR: 7 lbs (3.17 kg)
ENVIRONMENTAL	
TEMPERATURE	
OPERATING STORAGE	-33° to 60°C (-27.5° to 140°F) -55° to 80°C (-41° to 176°F)
HUMIDITY	Max 100% relative humidity (non-condensing)
ELECTRICAL	
INPUT	Voltage 110 to 250 VAC
OUTPUT	Current 420 mA at 48V
POWER CONSUMPTION	Maximum 20 Watt
POWER OVER ETHERNET	Via RJ-45 Ethernet interface port
MANAGEMENT	
LOCAL	RS-232 Serial Port (RJ11 and DB-9)
REMOTE	Telnet, Web GUI, TFTP
SNMP	SNMPv1/v2c; MIB-II; Ethernet-like MIB; 802.3MAU; 802.11MIB; Private MIB; ORiNOCO MIB; RFC 1157; RFC 1213; RFC 1643; RFC 1493; RFC 2668
MTBF AND WARRANTY	100,000 hours; 1-year on parts and labor
PACKAGE CONTENTS	• One (1) Tsunami MP.11 4954-BSUR with Type-N connector, or One (1) 4954-SUA Unit with Type-N connector, or One (1) 4954-SUR with 21 dBi integrated antenna • One (1) wall/pole mounting bracket • One (1) power injector and US/CAN power cord • One (1) Cable Termination Kit • One (1) CD-ROM with Software and Documentation
RELATED PRODUCTS	Quickbridge.11 4954-R, PoE Surge Arrestor (70251), Spare Power DC Injector for MP.11 or QB.11 (69823), MP.11 System Antennas, ORiNOCO Public Safety Mesh Access Points (AP-4900M and AP-4900MR-LR), ProximVision™ NMS, ServPak (US/CAN Only), Worldwide Extended Warranty

Tabella 4.1. Caratteristiche del modello Tusami MP.11 4954-R.

4.2.2 Software utilizzati

Il protocollo utilizzato dai dispositivi scelti (Tsunami MP.11 5054-BSUR per la *Base Station* e Tsunami MP.11 5054-SUR per la *Subscriber Station*) è denominato **WORP** ed è proprietario, ma comunque basato sugli standard dettati dal **WiMax Forum** [14] per il protocollo 802.16, sia per quanto riguarda le caratteristiche tecniche e tecnologiche per la connettività, sia per le restrizioni sulle classi di qualità del servizio che l'hardware deve offrire.

Si è reso necessario, inoltre, l'utilizzo di altri tipi di software, sia per generare il traffico testato sul canale sia per sniffare il traffico stesso:

- **WireShark:** software open source per sniffare il traffico e archiviare i dati;
- **VLC** (**multimedia framework, player and server**): software di streaming audio-video;
- **WAMP** (**Window, Apache, MySQL and PHP**): piattaforma in grado di simulare il comportamento di un server web e dei client FTP;
- **ASTERISK:** server con funzionalità di centralino VOIP per generare, appunto, traffico di tipo Voice Over IP.

4.2.2.1 Protocollo WORP (WIRELESS OUTDOOR ROUTER PROTOCOL)

È un nuovo protocollo designato ad ottimizzare la performance del sistema wireless esterno **point-to-point** e **point-to-multipoint**, che utilizza il link **802.11b**.

L'uso di questo link, rende possibile alla **Promix** di offrire una soluzione a basso costo,che è ideale per l' accesso alla rete esterna e interna.

WORP [25], si prende cura del degrado che ha la performance quando gli standard della tecnologia wireless basati sull'802.11b vengono usati per la connessione esterna "*da palazzo a palazzo*"; questo problema del degrado viene denominato "**hidden-node**".

Tutti i wireless **CSMA/CA** e **802.11**, danno per scontato che tutti i nodi sanno riconoscere i segnali (individuare il segnale). Ciò significa che tutte le radio presenti in un sistema, possono ascoltare i segnali radio l'uno dell'altro e, quindi, non trasmettono se altre stanno già trasmettendo.

Questo risultato è facilmente ottenibile in un'istallazione interna, mentre diventa non ottenibile in ambienti esterni point-to multipoint.

Il meccanismo di richiesta per "*mandare"* o per "*eliminare e mandare"* (**RTS** e **CTS**), è una soluzione che è stata inclusa nel modello 802.11 standard, ma non risolve il problema dell'*hidden-node*.

In una rete con pochi utenti, comunque, il modello 802.11b funzionerà anche all'esterno. Quando, invece, c'è il bisogno di aumentare ulteriormente la rete, una RTS mandata da una **Subscriber Unit** ad una **Base Station,** corromperà tutti i dati che altre unità stanno in quel momento mandando. Il risultato sarà una perdita di pacchetti che comporterà, a sua volta, ritrasmissioni multiple che causeranno la caduta drammatica delle performance della rete.

L'algoritmo WORP evita che queste collisioni possano accadere, il che aumenta in maniera significativa le prestazioni di tutta la rete.

Benefici del WORP in un ambiente esterno:

- **Più banda larga di rete**: risolvendo il problema dell'*hidden-node*, il WORP aumenta la rete a banda larga del sistema multipoint. La rete a banda larga del modello Wi-fi access point usata in un ambiente esterno può, quindi, essere aumentata fino a 6 Mb/s mediante l'utilizzo di WORP. È dunque, un protocollo più efficiente che protegge il sistema dalle collisioni, aumentandone la performance totale.
- **Più utenti simultaneamente**: una soluzione esterna *Point-To-Multipoint* basata sull'802.11b può connettere da 5 a 10 nodi remoti, ma può capitare che la prestazione inizi a soffrire di collisioni con soli 2 nodi remoti. Con l'utilizzo di WORP, invece, si possono connettere fino a 100 nodi remoti senza effetti contrari sulla banda larga, ciò permette l'attività a più utenti simultaneamente in un ambiente wireless multipoint.
- **Controllo banda larga**: permette al service provider di controllare la rete a banda larga, proteggendo la rete stessa dall'eccessivo uso della banda larga da qualsiasi stazione. Inoltre, permette ai service provider di differenziare le loro offerte di servizio.
- **Controllo della banda larga asimmetrica**: la banda larga asimmetrica da al gestore della rete la capacità di stabilire diversi indici massimi di banda larga per una varietà di gruppi di clienti. Questo permette al service provider di differenziare ulteriormente la loro offerta, massimizzando cosi gli introiti.

Il protocollo WORP è un protocollo più efficiente, in un retaggio all'esterno, del protocollo di un sistema router.

I benefici di WORP, dunque, su questa soluzione sono:

- **Rete a banda larga aumentata**;
- **Più utenti presenti sulla stessa stazione di base**;

- **Controllo a banda larga asimmetrico**;
- **Possibilità di fornire una statistica sui link**

Funzionalità del WORP:

- **Trasmissione e Registrazione**: in un sistema basato sul WORP, la **Base Station Unit** (**BSU**) agisce come un controllore del traffico. La BSU trasmette ogni 150 ms, in modo che una **Subscriber Unit** (**SU**) possa riconoscere il sistema. La BSU trasmette soltanto alle SU che hanno la stessa chiave di crittografia,il nome della rete e il nome della stazione di base. Una stazione che vuole entrare può farlo non appena vede trasmettere la BSU. Quando alla stazione base si registrano il numero massimo di SU, le trasmissioni si fermeranno fino a quando SU de-registrerà. Registrazione e autenticazione reciproca è basata sul **MD-5** usando una stringa segreta. La negoziazione di banda larga per la specifica Subscriber Unit, si verifica tra SU e SBU per eseguire la gestione della banda larga. Per ogni SU registrata è assegnato un numero di porta, fino ad un massimo di 100.
- **Polling (Interrogazione) Satelliti**, **Richiesta per Servizio e Programmazione Dinamica**: la BUS interrogherà regolarmente ogni satellite, mediamente ogni 4 secondi. Quando la SU ha nuovi dati, richiederà di essere interrogata immediatamente – se non è stata interrogata dopo l'ultima trasmissione – appena vede la trasmissione BSU. Il programma di interrogazione è dinamico, basato sulla quantità di dati che sono in attesa di ottimizzare l'uso della banda larga disponibile.
- **Windowing**, **Ritrasmissione e TimeOut**: i dati vengono inviati tra SU e BSU con un incremento della sequenza di numeri, e ogni **frame** viene riconosciuto. Un nuovo dato viene inviato immediatamente anche se "la finestra" della sequenza dei numeri non è ancora compilata. L'ultima sequenza di numeri riconosciuta è quella che sta al fondo della finestra. La ritrasmissione si verifica solo quando sono stati inviati diversi frame per i quali non è stato ricevuto nessun riconoscimento; ed avviene selettivamente solo su frame mancanti.

  Il TimeOut e lo *scarto* avviene quando il dato è troppo lungo in trasmissione coda (più di 1,5 secondi con una massima dimensione del buffer di 512 frame) è quando il dato è troppo lungo in ritrasmissione coda (16 ingressi) con il TimeOut dipendente dal tasso di dati radio e dal numero di Subscriber Unit registrate.

- **De-registrazione**: La de-registrazione accade quando BUS o BU non si "sono viste" tra loro per 30 secondi. La BSU considererà la BU de-registrata e, quest' ultima, deve ri-registrarsi non appena la BSU tornerà a trasmettere.
- **Throughput**, **Super-Packeting e frammentazione**: In un ambiente di rete, il massimo delle prestazioni avviene quando i frame hanno pacchetti di dati di dimensione di 2304 bytes. I pacchetti ethernet hanno dimensioni massime di 1514 bytes. Generalmente il 60% dei messaggi IP sono brevi (<100 bytes). Questi brevi frame hanno un impatto sull'efficacia del *throughput* (Figura 4.3).

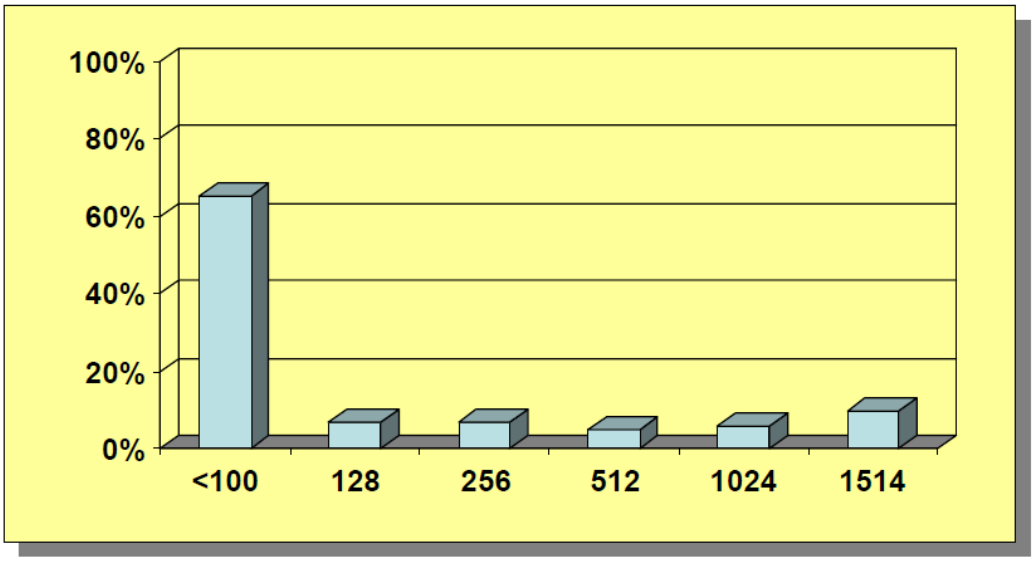

Figura 4.3. Throughput.

WORP usa super-packeting e la frammentazione per migliorare l'efficacia del throughput del sistema riducendo al minimo l'*overhead.* Con super-packeting , WORP mette pacchetti multipli in un unico frame. La frammentazione divide questi pacchetti in 2 frame.

- **Crittografia**: tutta la comunicazioni WORP viene inviata in frame di dati, cosi sono sempre al seguito dello stato di crittografia. Per la crittografia, la crittografia WEP a 64 e 128 bits è usata con una debole chiave di evasione (**WEP+**).

  Nella versione corrente, viene usata una chiave di crittografia statica. Con la crittografia a 128 bits attiva, il sistema raggiunge l'85% delle sue prestazioni normali.
- **Controllo Banda larga**: i service provider di rete possono limitare la banda larga che ogni cliente può utilizzare. Questa operazione viene eseguita nella Subscriber

Units. Il controllo della banda larga può essere configurato per il link SU-SBU. Esso è asimmetrico, può essere configurato in modo indipendente a monte e a valle; in questo modo i service provider possono fornire varie offerte di servizi ai clienti. Inoltre, questo controllo è un meccanismo di sicurezza per l'**ISP**. Garantisce un' equa ripartizione sui sistemi attivi della banda larga disponibile; in questo modo, un singolo abbonato non può consumare completamente tutta la banda larga del sistema. Il controllo della banda larga, infine, è in grado di impostare il **Maximun Information Rate** (**MIR**) ma non il **Committed Information Rate** (**CIR**). La configurazione del controllo della banda larga può essere: statico, in ogni interfaccia Subscriber Unit e Base Station Unit, o centralmente tramite un service radio.

- **Sicurezza**: WORP offre una varietà di elementi di sicurezza per proteggere i dati in rete. Il protocollo non viene pubblicato o standardizzato, il che lo rende meno vulnerabile agli hacker di un sistema basato sul Wi-Fi. WORP richiede la SU per registrare sulla base per fare un' autenticazione reciproca, con identificazione tramite una MD-5 con stringa segreta. Entrambi sanno che i loro pari appartengono alla rete (evitando entrambi fastidi su SU e SBU). In aggiunta, WORP usa una crittografia a 128 bit usando WEP+ con una chiave debole, per evitare di cifrare i dati inviati. Il controllo di accesso (autenticazione) si verifica a livello locale tramite un server radio. Infine, tutti i metodi di gestione remota sono protetti da password. Diverse password, possono essere impostate per **SNMP lettura**, **SNHP lettura/scrittura**, **Telnet** e **HTTP**.

4.3 Descrizione della tipologia di traffico

Come già accennato nella parte introduttiva, il traffico analizzato durante i test è stato traffico di tipo **VOIP**, **FTP** e **HTTP**.
Vediamo di seguito una descrizione di queste tipologie di traffico.

4.3.1 VOIP

Il **VoIP** [29], acronimo di ***Voice over IP***, utilizza la commutazione di pacchetti delle comunicazioni Internet per applicarla alla voce. Non è più presente il collegamento fisico di una linea (doppino telefonico e centrali), ma la voce, trasformata in un segnale digitale, viene divisa in pacchetti di dati e inviati in rete. Una volta giunti a destinazione questi

pacchetti vengono ricomposti per ricreare la situazione originale ed essere fruibili dall'apparecchio ricevente. L'utente ricevente deve utilizzare un dispositivo specifico, come un computer, un adattatore per il telefono utilizzato oppure un nuovo tipo di telefono (IP) per rendere possibile la conversione del segnale digitale in segnale sonoro. L'approccio utilizzato da internet nelle comunicazioni si basa sull'invio di pacchetti di dati attraverso la rete. Questo sistema permette ai dati di giungere a destinazione attraverso differenti percorsi, giunti poi a destinazione questi dati (informazioni) vengono poi ricomposti per essere utilizzati dall'utente (pagine web, video, mp3 e voce) con determinati programmi o accessori.

L'approccio di internet per la comunicazione è totalmente differente rispetto a quella tradizionale utilizzata con i telefoni di casa. I telefoni di casa utilizzano la classica comunicazione basata sulla commutazione in cui tutti i telefoni sono collegati fisicamente uno con l'altro e nel momento in cui un utente compone un numero, la linea che collega i due telefoni viene totalmente impegnata per l'intera durata della conversazione.

Utilizzare il proprio accesso a internet per telefonare permette di risparmiare sul costo della bolletta telefonica perché tutte le telefonate sarebbero locali, inoltre il costo della infrastruttura sarebbe inferiore e di molto.

Attualmente il VoIP è molto diffuso nelle aziende e si sta cercando di far convergere anche gli utenti domestici verso questa tecnologia anche perché le compagnie telefoniche hanno già cablato (o stanno provvedendo) le proprie dorsali per la trasmissione della voce su IP. Un problema serio di questa nuova tecnologia legato all'utilizzo della rete internet riguarda la sicurezza informatica perché i dati che scorrono sulla rete possono essere intercettati e i computer risultano sempre interessati da attacchi informatici e tentativi di intrusione. Non ultimo sono i problemi di sicurezza legati alle vulnerabilità presenti nei protocolli di comunicazione utilizzati dal VoIP che vengono puntualmente scoperti da aziende operanti nel campo della sicurezza informatica.

Al fine di migliorare la sicurezza delle comunicazioni mediante il VoIP è stata presentata in Texas, negli Stati Uniti, la prima alleanza per la sicurezza della telefonia VoIP (**VOIPSA**).

Le principali caratteristiche del VOIP sono [30]:

- **Minori costi**: il vantaggio, non trascurabile, che l'utente domestico può trarre dall'utilizzo del VoIP per le proprie telefonate riguarda il minor costo. Telefonare utilizzando il VoIP significa avere costo nullo tra utilizzatori dotati dello stesso fornitore di VoIP oppure una spesa molto ridotta per le chiamate verso altre

destinazioni geografiche (specialmente lunghe distanze). Per le aziende la convenienza è ancora maggiore perché, nel caso di multinazionali, possono utilizzare il VoIP per comunicare gratis tra le differenti filiali sparse nel mondo. I vantaggi non sono solo per gli utilizzatori ma anche per i gestori del servizio. Adottare il VoIP, dal lato del gestore, significa diminuire il costo di infrastruttura e cablaggio, perché è sufficiente un unico tipo di cavo per il funzionamento del PC e dei telefoni. Altri aspetti fondamentali che non possono essere trascurati riguardano la praticità e flessibilità. Il VoIP utilizza le stesse tecnologie di Internet e della comunicazione di rete tra PC, di conseguenza le risorse aziendali che si occupano della gestione e manutenzione della rete possono occuparsi anche della gestione del VoIP, con il vantaggio di non dover spendere denaro per l'utilizzo di tecnici esterni. Inoltre con l'utilizzo dei sistemi Wireless, nemmeno i cavi saranno più un problema.

- **Ampia flessibilità**: l'utilizzo del VoIP garantisce ampia flessibilità in quanto viene garantita la portabilità del numero a prefisso geografico poiché il numero non è più legato fisicamente a una linea telefonica (centrale relativa alla zona di residenza) e dal punto di vista dell'utilizzatore nulla cambia perché si userà sempre un normale telefono.
- **Sicurezza**: la tecnologia VoIP introduce nuovi aspetti, molto delicati, relativi alla sicurezza informatica. Nella spiegazione sul funzionamento del VoIP, è stato sottolineato come la voce viaggia in pacchetti IP e, di conseguenza, gli amministratori che curano la sicurezza potrebbero pensare che inserendo il traffico voce nella loro rete IP quest'ultima rimarrà sicura. In realtà non è così! Utilizzare il VoIP significa aggiungere nuovi e differenti elementi alla tecnologia di rete già presente, creando così anche nuovi problemi legati alla sicurezza informatica. Gestire la sicurezza con il VoIP significa dover considerare tutta una serie di accorgimenti che normalmente nella gestione della sicurezza aziendale non vengono considerati. Apparecchi come router, gateway e firewall sono presenti nelle Lan aziendali ma il problema legato alla sicurezza, nel caso del VoIP, riguarda il possibile deterioramento della QoS (qualità del servizio), per effetto dei ritardi o dei blocchi delle chiamate prodotti dai firewall, oppure della latenza e del jitter introdotto con l'utilizzo della crittografia. Il VoIp è sensibile alla velocità del trasferimento dei dati ed alla bassa tolleranza alla perdita di pacchetti, con la

conseguenza che diverse misure di sicurezza implementate nelle reti dati tradizionali potrebbero non essere applicabili alle reti VoIP.

- **Protocolli**: Per il funzionamento della tecnologia VoIP sono richiesti due tipologie di protocolli di comunicazione che funzionano in parallelo. Il primo protocollo è necessario per il trasporto dei dati (pacchetti voce su IP) e nella grande maggioranza delle implementazioni di VoIP viene impiegato il protocollo **RTP** (*Real-time Transport Protocol*). L'*Internet Engineering Task Force* (**IETF**) ha suddiviso in due parti il protocollo RTP strettamente legate:
  - **Real-time transport protocol** (RTP), per il trasferimento dei dati con proprietà di tempo reale (Real Time);
  - **RTP control protocol** (RTCP), per "monitorare" la qualità del servizio e fornire informazioni sui partecipanti di una sessione in atto

  Esistono altri protocolli per la codifica della segnalazione della conversazione che utilizzano altri tipi di protocolli alternativi:

  - **SIP** (Session Initiation Protocol) della IETF;
  - **H.323** della ITU;
  - **Skinny Client Control Protocol**, protocollo proprietario della Cisco;
  - **Megaco** (conosciuto anche come H.248) e MGCP;
  - **MiNET**, protocollo proprietario della Mitel;
  - **IAX**, usato dai server Asterisk open source PBX e dai relativi software client.

  Gli standard introdotti in precedenza possono essere usati per facilitare la trasmissione di messaggi tra i Gateway e, di conseguenza, possono essere utilizzati per implementare terminali senza alcuna intelligenza, in modo del tutto simile ai telefoni attuali collegati ad un centralino PBX.
- **Sicurezza anche "Fisica"**: i problemi di sicurezza legati all'utilizzo del VoIP non riguarda solo il lato informatico ma anche quello fisico ovvero qualunque persona potrebbe collegare alla rete aziendale un Tool di monitoraggio ed intercettare le conversazioni. Un modo per risolvere il problema è utilizzare la crittografia nell'utilizzo del VoIP, prestando sempre attenzione alla qualità del servizio e ai possibili ritardi nella comunicazione introdotti dalla cifratura. Altre misure di sicurezza fisica possono essere, guardie, lucchetti e sistema di controllo degli accessi.

4.3.2 Protocolli FTP e HTTP

4.3.2.1 Introduzione

Un protocollo è un insieme di regole che permettono di trovare uno standard di comunicazione tra diversi computer attraverso la rete, dove per rete si intende un insieme di due o più computer connessi tra di loro ed in grado di condividere informazioni. Quando due o più computer comunicano tra di loro si scambiano una serie di informazioni. Per potersi scambiare informazioni, i vari computer devono avere dei protocolli che permettano di attribuire ad un determinato comando un significato univoco per tutte le macchine.

Un protocollo descrive:

- il formato che il messaggio deve avere;
- il modo in cui i computers devono scambiarsi messaggi.

Ogni protocollo viene riferito ad una particolare attività, come ad esempio spedire messaggi attraverso la rete, stabilire connessioni remote, oppure trasferire files.

Pensiamo ad un messaggio di posta elettronica. Sia il formato del messaggio, sia il modo in cui viaggia attraverso la rete sono governati da un protocollo. Il protocollo assicura che il messaggio sia formattato e trasmesso correttamente dal mittente al destinatario (che in questo caso sono computer).

Esiste un protocollo diverso per ogni tipologia di servizio di rete.

Per esempio la connessione ad Internet è basata sulla famiglia di protocolli **TCP/IP**.

Altri protocolli utilizzati sono:

- **Simple Mail Transfer Protocol** (**SMTP**): permette la gestione dei messaggi di posta elettronica.
- **File Transfer Protocol** (**FTP**): permette il trasferimento di files tra macchine remote.
- **Hypertext Transfer Protocol** (**HTTP**): permette la trasmissione di informazioni attraverso il WEB.
- **Network News Transfer Protocol** (**NNTP**): permette la gestione dei gruppi di discussione.
- **Gopher**: permette un servizio di informazione distribuita ed organizzata ad albero, consistente in una serie di menu e files interconnessi tra loro.
- **Wide Area Information System** (**WAIS**): permette la ricerca ed il recupero in data base connessi in rete.