

**Consorzio Residenti San Michele di Pagana e zone
limitrofe
16035 – RAPALLO (GE)**

**Progetto Tecnico
Impianto di Videosorveglianza**



**Sicurproject S.r.l.
Via Privata O.T.O 47/49 19136 La Spezia**



1	CARATTERISTICHE GENERALI DEL PROGETTO	3
2	STUDIO DELL'AREA DI INTERESSE	4
2.1	RILEVAZIONE DELLE AREE GEOGRAFICHE	4
2.2	CONSIDERAZIONI PRELIMINARI	5
3	DETERMINAZIONE DELLA TECNOLOGIA DEGLI IMPIANTI DA UTILIZZARE	6
3.1	SISTEMI DI VIDEOSORVEGLIANZA DIGITALI	6
3.2	LA SCELTA DIGITALE E IP	6
3.3	LA TECNOLOGIA IP (INTERNET PROTOCOL)	7
3.4	LA RETE IP E LE SUE CARATTERISTICHE	8
3.4.1	<i>Livello fisico</i>	9
3.4.2	<i>Ethernet</i>	9
3.4.3	<i>10 Mbit/s (10 Mbps) Ethernet</i>	9
3.4.4	<i>Fast Ethernet (100 Mbit/s)</i>	9
3.4.5	<i>Gigabit Ethernet (1000 Mbit/s)</i>	10
3.4.6	<i>Power Over Ethernet (PoE)</i>	10
3.4.7	<i>Uso di Power over Ethernet</i>	11
3.5	WIRELESS.....	11
3.5.1	<i>Wireless LAN (chiamata anche WLAN):</i>	11
3.5.2	<i>Bridge wireless</i>	11
3.5.3	<i>Standard LAN wireless</i>	11
3.5.4	<i>802.11a</i>	11
3.5.5	<i>802.11b</i>	12
3.5.6	<i>802.11g</i>	12
3.5.7	<i>802.11n</i>	12
3.5.8	<i>802.16 - WiMAX</i>	12
3.5.9	<i>Protezione Wireless</i>	12
3.5.10	<i>Bridge wireless</i>	12
3.5.11	<i>Livello trasmissivo</i>	13
3.5.12	<i>Protocolli per il trasporto dei dati</i>	13
3.5.13	<i>Metodi di trasmissione usati dai sistemi video di rete: Unicasting, Multicasting e Broadcasting</i>	14
3.5.14	<i>Livello logico</i>	14

3.5.15	<i>Indirizzi IP</i>	14
3.5.16	<i>Ip version 6 (IPv6)</i>	15
3.6	UTILIZZO DI UNA RETE IP COME INFRASTRUTTURA DI COMUNICAZIONE	16
3.7	TECNOLOGIE DA IMPIEGARE NELLA COSTITUZIONE DELLE TRATTE DI COMUNICAZIONE	16
3.8	TRATTE DI INTERCONNESSIONE	16
3.8.1	<i>Fibra Ottica</i>	16
3.8.2	<i>Cablaggio in rame UTP/STP</i>	17
3.8.3	<i>Wireless</i>	18
3.8.4	<i>802.11b</i>	18
3.8.5	<i>Canali e compatibilità internazionale</i>	18
3.8.6	<i>802.11g</i>	18
3.8.7	<i>Certificazione</i>	19
3.8.8	<i>Sicurezza</i>	19
3.8.9	<i>Nodi di comunicazione</i>	19
3.8.10	<i>Nodi di interconnessione</i>	20
3.8.11	<i>Switch PoE</i>	20
3.9	TELECAMERA IP AD ALTE PRESTAZIONI.....	20
4	DIMENSIONAMENTO DELL'INFRASTRUTTURA SUL TERRITORIO	22
4.1	SCHEMA GENERIC LOGICO	22
4.2	COSTITUZIONE DI UNA DORSALE IN TECNOLOGIA HYPERLAN	23
4.3	POSIZIONAMENTO DELLE TELECAMERE IN PROSSIMITÀ DEI NODI DI INTERCONNESSIONE	23
5	ELENCO PRODOTTI	24
6	IMPIANTI PER LA RIPRESA DELLE IMMAGINI	24
6.1	VIDEOCAMERA IP DIREZIONALE E DI LETTURA TARGHE	25
7	ANTENNA HYPERLAN PER IL COLLEGAMENTO	27
7.1	ANTENNA EPMP 1000.....	27
8	SOFTWARE DI LETTURA TARGHE	28
8.1	IVMS 4200.....	28
8.1.1	<i>IVMS-4200, sistema intelligente di gestione video</i>	28
8.1.2	<i>NVR Server, software per la registrazione</i>	28
8.1.3	<i>IVMS-4500, client software per dispositivi mobile</i>	29

1 CARATTERISTICHE GENERALI DEL PROGETTO

Il progetto consiste nella realizzazione di un ampliamento al **Sistema di Videosorveglianza del Comune di Rapallo** nel comprensorio cittadino di Rapallo in particolare Frazione San Michele di Pagana in modo da coprire in maniera maggiormente efficiente alcune aree della città e zone ancora non servite dal sistema precedente.

Le finalità riguardano:

- Copertura della zona pubblica di Via Floria bassa;
- Copertura della zona pubblica di Via Floria incrocio Via Meucci
- Copertura della zona pubblica di Via Floria Alta
- Copertura della zona pubblica di Via del Mandraccio

Il progetto si configura come un ampliamento strutturale del sistema primario ed il controllo viene assegnato alla Centrale Operativa del Comune di Rapallo.

L'impianto è strutturato in modo da soddisfare gli stessi criteri di affidabilità, sicurezza e utilizzabilità ottimali che contraddistinguono il sistema principale del Comune di Rapallo, ma tiene anche conto delle evoluzioni tecnologiche intercorse durante il periodo di sviluppo.

Tale sistema deve essere in grado di essere semplicemente ampliato ed integrabile con le attrezzature in continua evoluzione e capace di fornire tipologie di servizi differenti e complementari quali registrazione degli eventi, protezione delle apparecchiature, programmabilità degli eventi, allarme in caso di necessità, controllo remoto delle apparecchiature, presenza di una rete dati sfruttabile in maniera modulare. Oltre ovviamente ai servizi di sorveglianza.

In pratica un sistema di sorveglianza dotato delle migliori tecnologie presenti sul mercato, interamente scalabile, ampliabile e gestibile in maniera interamente automatica.

Il progetto è suddiviso come segue:

Studio dell'area di interesse

Analisi del comprensorio urbano e periferico finalizzato alla collocazione ottima degli impianti costitutivi, in particolare degli strumenti di ripresa, degli apparecchi di comunicazione, dei sistemi di gestione e archiviazione dati;

Determinazione della tecnologia degli impianti da utilizzare

Selezione di apparecchiature dotate di specifiche tecniche in grado di soddisfare i requisiti qualitativi dell'impianto in modo da integrare naturalmente nel sistema esistente;

Dimensionamento di una infrastruttura sul territorio

Costituzione di una infrastruttura in grado di ospitare le tecnologie e gli impianti adottati per l'impianto e che soddisfi tutti i criteri di espandibilità, scalabilità e usabilità richiesti;

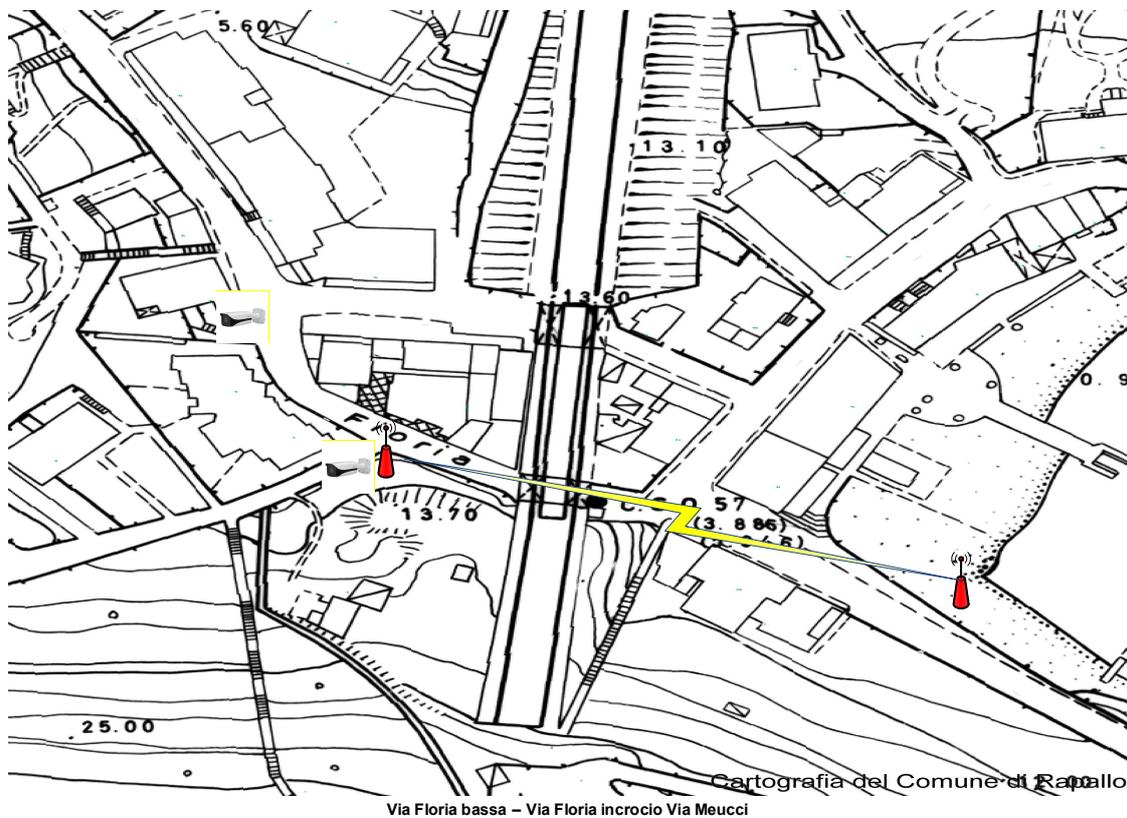
Istruzione, messa a punto e collaudo del sistema

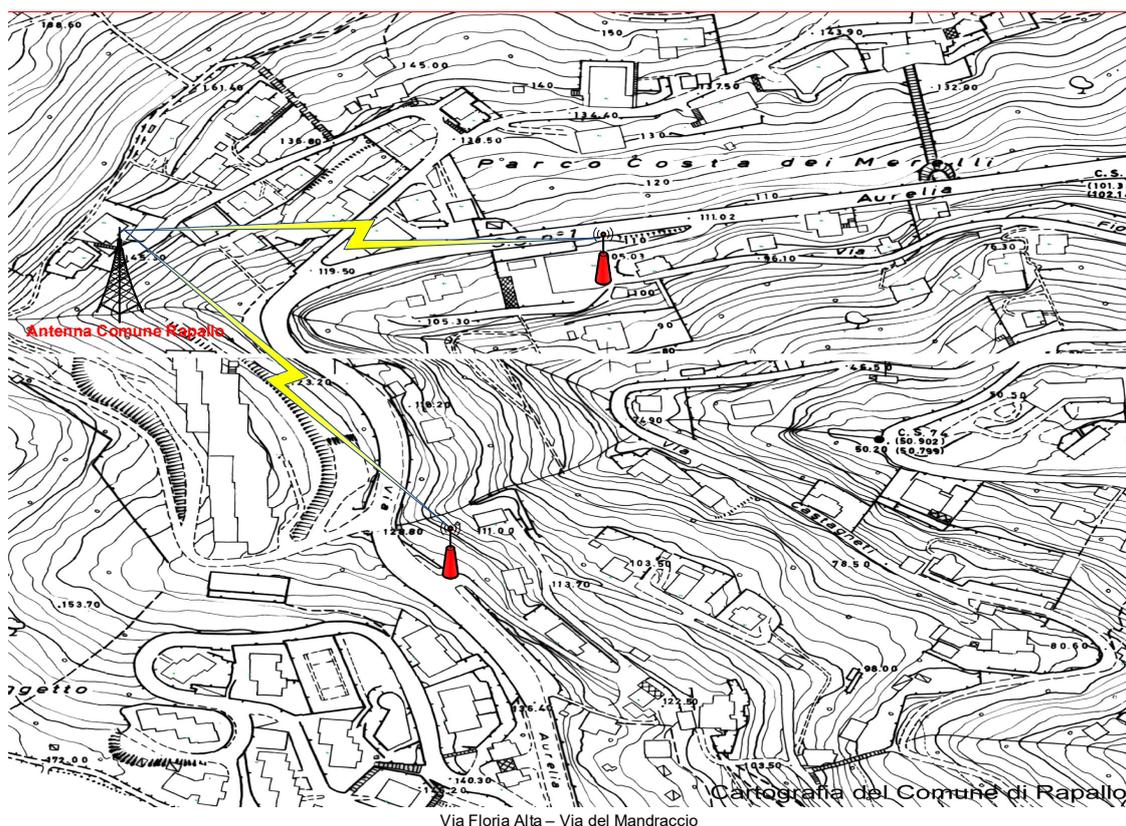
Una volta interconnessi gli impianti si può procedere con la programmazione degli stessi, ai dovuti test di funzionalità propedeutici alla messa in opera definitiva.

2 STUDIO DELL'AREA DI INTERESSE

2.1 RILEVAZIONE DELLE AREE GEOGRAFICHE

L'area di interesse viene studiata in base alla configurazione geografica delle zone indicate al precedente punto 1.





Le finalità specifiche sono:

- Copertura più ampia e capillare possibile della zona di interesse;
- Finalità specifiche di sicurezza per il cittadino e i beni di proprietà del Comune.

L'impianto è stato progettato per sopportare gli ampliamenti in oggetto e per la stragrande maggioranza delle zone si presta ad essere servita da prolungamenti delle dorsali in HiperLan ed eventualmente in fibra ottica

2.2 CONSIDERAZIONI PRELIMINARI

Lo scenario delineato descrive una realtà urbana moderna intersecando zone con prevalente traffico pedonale con via Floria a traffico misto pedonale e veicolare.

Per raggiungere lo scopo di ottenere una videosorveglianza affidabile, capace di adattarsi adeguatamente alle condizioni geografiche dell'area di interesse è necessario valutare attentamente le tecnologie disponibili sul mercato tenendo bene presente quelle che contraddistinguono l'attuale impianto in uso al Comune di Rapallo.

In ogni caso risulta evidente la necessità dell'impiego di telecamere per esterni con funzionalità di movimento, ripresa notturna, in grado di resistere ad intemperie e ad atti vandalici. E primariamente di una struttura tecnologica in grado di interconnettere tutte le telecamere presenti nell'area di interesse e di far convergere le loro acquisizioni in uno o più punti di raccolta presenti sul territorio.

3 DETERMINAZIONE DELLA TECNOLOGIA DEGLI IMPIANTI DA UTILIZZARE

I sistemi di videosorveglianza esistono ormai da più di 25 anni e, come ogni altra applicazione tecnologica dello scorso secolo, ha vissuto nel tempo numerosi cambiamenti e miglioramenti.

Un'evoluzione che ha visto un principio in campo analogico che ha raggiunto la sua espressione massima da pochi anni e, più di recente intorno al 1999, l'avvento della tecnologia digitale.

Le due metodologie, **analogico** e **digitale**, seppur condividendo i sistemi ottici si differenziano nella tecnica di trasmissione dell'immagine e, più in generale nella tecnologia adottata per acquisire l'immagine stessa.

3.1 SISTEMI DI VIDEOSORVEGLIANZA DIGITALI

Per sistema di videosorveglianza digitale si intende un sistema che si avvale di segnali digitali per propagare le informazioni. In pratica l'acquisizione dell'immagine avviene in maniera analogica dall'ottica della videocamera, successivamente avviene la digitalizzazione (ovvero il campionamento dell'immagine) direttamente mediante il sensore CCD o CMOS presente sulla telecamera.

A parte alcune eccezioni presenti in sistemi proprietari, i sistemi di videosorveglianza digitali sono detti di rete in quanto utilizzano metodi di interconnessione e di trasporto dati propri della rete IP ethernet.

Le telecamere di rete sono dispositivi costituiti da una telecamera, un computer che digitalizza e comprime le immagini e un connettore di rete. Il video viene trasmesso tramite una rete IP utilizzando gli switch di rete e salvato su un PC standard munito di software di gestione video. Questo sistema è un vero sistema video di rete poiché è completamente digitale e non prevede l'utilizzo di componenti analogici.

I sistemi video di rete con telecamere di rete offrono i seguenti vantaggi:

- Consentono l'utilizzo di telecamere ad alta risoluzione (megapixel);
- Garantiscono immagini di qualità uniforme;
- Offrono le funzionalità Power over Ethernet e wireless;
- Consentono di trasmettere dati di tipo PTZ, audio o di ingressi e uscite digitali;
- Sono totalmente flessibili e scalabili.

3.2 LA SCELTA DIGITALE E IP

L'impianto esistente del Comune di Rapallo, essendo il sistema da ampliare, viene preso in considerazione sul piano tecnologico per definire le soluzioni di integrazione dei nuovi impianti.

Il sistema del Comune di Rapallo è composto dai seguenti sistemi logico/funzionali:

- Dorsale di comunicazione in fibra ottica con protocollo di comunicazione IP;
- Sistema di ripresa IP ad alta definizione mediante telecamere di rete;
- Utilizzo di sistemi IP Wireless per la gestione di aree difficilmente raggiungibili;
- Sala di controllo digitale multi monitor con sistema IP di gestione.

Risulta evidente che la tecnologia IP sia la scelta più opportuna per integrare un impianto interamente digitale le cui informazioni e trasmissioni utilizzano TCP/IP.

Inoltre, in virtù dei pregi di un sistema di sorveglianza digitale, occorre scegliere un'applicazione digitale in grado di costituire un'infrastruttura solida ed affidabile in ambito cittadino ed IP, forte della sua implementazione su scala mondiale per sistemi di comunicazione di ogni genere, è sicuramente la scelta più corretta.

3.3 LA TECNOLOGIA IP (INTERNET PROTOCOL)

IP (Internet Protocol) è il protocollo di comunicazione attualmente più usato, poiché costituisce il protocollo di base usato per le comunicazioni tramite Internet, compresi la posta elettronica, il Web e le applicazioni multimediali. Una delle ragioni della sua popolarità risiede nella sua scalabilità. Ciò significa, in altre parole, che questo protocollo può essere usato sia per le piccole installazioni che per quelle di dimensioni maggiori, perché è in grado di garantire prestazioni elevate, costi ridotti e un'ampia compatibilità con attrezzature e tecnologie consolidate.

La tecnologia IP rappresenta il cuore delle telecomunicazioni digitali con modello client-server. Una qualsiasi rete privata contenuta in un piccolo ufficio, il computer di casa, i computer della rete di una grande azienda, i server che ospitano i siti di tutto il mondo, si avvalgono della tecnologia IP in una delle sue molteplici configurazioni.

IP infatti è un protocollo di comunicazione progettato per gestire le interazioni e lo scambio di informazioni a livello di pacchetti (pacchetti IP), e per sua natura è in grado di interconnettere migliaia di utenze senza subire le conseguenze della mole di carico.

Utilizzare IP significa avvalersi di uno strumento potente, ampiamente collaudato e in continua evoluzione, ma soprattutto in grado di sopportare le esigenze di un sistema di sorveglianza geograficamente esteso in quanto:

- Comprende sistemi avanzati di crittografia;
- Utilizza sistemi di mantenimento della qualità del servizio (QoS);
- E' possibile disegnare la rete seguendo le direttive dell'EIA/TIA 568, approvato standard di configurazione della rete;
- Una rete IP è compatibile con molteplici sistemi di comunicazione differenti, sia uniti, che intersecati ma anche logicamente disgiunti;

- L'indirizzamento dei pacchetti è trasparente al mezzo di trasmissione. Questo significa che le tratte sono sostituibili (magari da cavo a wireless) senza che il sistema debba essere riprogrammato.

Il nome Internet Protocol può fuorviare, una rete IP non fa necessariamente parte di Internet così come la si conosce popolarmente (siti web, email, virus), ma semplicemente Internet usa IP esattamente come farebbe un piccolo ufficio isolato dal resto del mondo. Solo lo fa su scala mondiale.

In pratica una qualsiasi rete IP può o meno disporre di una connessione alla rete globale; nel caso della videosorveglianza è da considerarsi solamente nel caso in cui l'osservatore disti dalla telecamera più di quanto sia estesa la rete locale privata.

IP però è solo il metodo di comunicazione e lo standard che definisce la forma della trasmissione del messaggio unitamente ai criteri di scambio che vengono adottati in una rete capace IP.

3.4 LA RETE IP E LE SUE CARATTERISTICHE

L'informazione contenuta nei pacchetti IP è un segnale digitale opportunamente modulato e dimensionato. I pacchetti IP sono costituiti di Byte (otto bit) e vengono riversati nel mezzo trasmissivo muniti di tutte le informazioni accessorie per la corretta ricezione del messaggio. Ad esempio, un pacchetto IP che contiene un'immagine proveniente da una telecamera conterrà una consistente porzione di dati dedicato all'informazione stessa dell'immagine, ma conterrà anche gli identificativi del mittente e del destinatario.

Più precisamente un pacchetto IP contiene:

- Porzione dati (l'informazione da spedire);
- Indirizzo IP del destinatario;
- Indirizzo IP del mittente;
- Codici di controllo trasmissione;
- Bit di parità;
- Codici che regolamentano le priorità del flusso dati;
- Codici che permettono di ricostruire la segmentazione del flusso dati;
- Codici di sincronizzazione.

A questo punto, specificata la natura dell'informazione, è possibile definire a più livelli la struttura di un'architettura IP:

- Livello fisico: interconnessione fisica della rete mediante cablaggio o tecnologie alternative;
- Livello trasmissivo: metodologia per la generazione del segnale portatore dell'informazione IP;

- Livello logico: una volta interconnesse fisicamente le identità, metodologia di identificazione dei soggetti facenti parte della rete congiuntamente alla tecnica di gestione dei flussi dati e del loro instradamento.

3.4.1 Livello fisico

L'interconnessione fisica di una rete IP richiede l'applicazione di standard rigidi e ben definiti in ambito internazionale e si avvale delle più recenti ed evolute tecniche di linking.

L'interconnessione può avvenire mediante cavo in rame, onde radio, onde ottiche, fibre ottiche, guide d'onda. Solo alcune di queste tecnologie presentano i requisiti di utilizzo e di costo ideali per l'implementazione del sistema di San Michele di Pagana.

3.4.2 Ethernet

La maggior parte dei computer attualmente installati negli uffici utilizza generalmente il protocollo TCP/IP ed è collegato ad altri sistemi tramite una rete Ethernet. Ethernet consente di disporre di una rete veloce a un costo ridotto. La maggior parte dei computer attualmente in commercio ha un'interfaccia Ethernet integrata o è predisposta per l'installazione di una scheda di interfaccia di rete (NIC).

Tipi di protocolli Ethernet più diffusi:

3.4.3 10 Mbit/s (10 Mbps) Ethernet

Questo standard, raramente utilizzato per le reti a causa della sua ridotta capacità, è stato sostituito alla metà degli anni '90 con lo standard 100 Mbit/s Ethernet. La topologia più comunemente utilizzata con il protocollo 10 Mbit/s Ethernet era nota con il nome di 10BASE-T. Questa tipologia prevede l'uso di 8 fili (4 fili a doppino incrociato) alloggiati all'interno di un cavo Cat. 3 o Cat. 5. Al centro viene installato un hub o switch, che dispone di una porta per ciascun nodo. La stessa configurazione viene usata anche per Fast Ethernet e Gigabit Ethernet.

3.4.4 Fast Ethernet (100 Mbit/s)

Fast Ethernet, che supporta velocità di trasmissione dati fino a 100 Mbit/s, è il tipo di protocollo Ethernet più comunemente usato nelle reti di oggi. Lo standard principale prende il nome di 100BASE-T. Pur essendo più recente e più veloce rispetto allo standard 10 Mbit Ethernet, questo protocollo ne condivide tutte le caratteristiche di base. Lo standard 1000 Mbit/s può essere diviso in:

- • 100BASE-TX: che prevede l'uso di cavi in rame a doppino incrociato (Cat. 5, Cat. 5E, Cat. 6).
- • 100BASE-FX: che assicura velocità di trasmissione 100 Mbit/s Ethernet su cavi in fibre ottiche.

Nota: la maggior parte degli switch di rete 100 Mbit supporta sia lo standard 10 che 100 Mbit per garantire la compatibilità con i sistemi esistenti (generalmente chiamati switch di rete 10/100).

3.4.5 Gigabit Ethernet (1000 Mbit/s)

È lo standard corrente utilizzato dai produttori di computer desktop collegati in rete. Tuttavia, questo standard viene soprattutto utilizzato per le dorsali che collegano i server agli switch di rete. 1000BASE-T è ampiamente utilizzato e può essere suddiviso in:

- 1000BASE-T: velocità di trasmissione pari a 1 Gbit/s su cavi in rame Cat. 5 o Cat. 6.
- 1000BASE-SX: velocità di trasmissione pari a 1 Gbit/s su cavi in fibre Multi-mode (fino a distanze massime di 550 m).
- 1000BASE-LX: velocità di trasmissione pari a 1 Gbit/s su cavi in fibre Multi-mode (fino a distanze massime di 550 m); se utilizzato con cavi in fibre Single-mode, può essere ottimizzato anche per distanze più lunghe (fino a 10 km).
- 1000BASE-LH: velocità di trasmissione pari a 1 Gbit/s su cavi in fibre Single-mode (fino a distanze massime di 100 km); questa è la soluzione più idonea per le grandi distanze.
- 10 Gigabit Ethernet (10 000 Mbit/s).

Questo nuovo standard viene sempre più diffusamente utilizzato per le dorsali di reti aziendali. Lo standard 10 Gigabit Ethernet utilizza sette diversi tipi di supporti per le reti LAN, WAN e MAN (Metropolitan Area Network). I suoi requisiti sono attualmente stati raggruppati in uno standard supplementare, IEEE 802.3ae, che verrà integrato nella nuova versione dello standard IEEE 802.3.5.2.

3.4.6 Power Over Ethernet (PoE)

Power over Ethernet (PoE) è una tecnologia che permette di fornire alimentazione tramite l'infrastruttura della rete LAN. In altre parole, permette di alimentare altre periferiche di rete, come i telefoni IP o le telecamere di rete, utilizzando lo stesso cavo utilizzato per la connessione di rete. Questa soluzione elimina la necessità di usare prese di alimentazione nei punti di installazione delle telecamere e semplifica l'installazione di gruppi di continuità (UPS) capaci di garantire un funzionamento continuativo, 24 ore al giorno e 7 giorni alla settimana.

La tecnologia PoE è disciplinata da uno standard denominato IEEE 802.3af ed è appositamente progettata per non interferire con la trasmissione dei dati o ridurre la portata della rete.

L'alimentazione viene trasmessa tramite l'infrastruttura LAN appena viene rilevato un terminale compatibile e bloccata se vengono rilevate periferiche più vecchie non compatibili con questa tecnologia. Questa funzione permette dunque agli utenti di utilizzare contemporaneamente in rete periferiche compatibili o meno con la tecnologia PoE, con la massima flessibilità e in tutta sicurezza.

Lo standard assicura una potenza massima di 15,4 W sul lato dello switch o del midspan, che equivale a un consumo massimo di 12,9 W sul lato della periferica/telecamera. Pertanto, è la soluzione ideale per le telecamere di rete. Le telecamere per esterni, PTZ e Dome richiedono generalmente una maggiore potenza e non sono pertanto indicate per l'uso con la tecnologia PoE. Alcuni produttori offrono anche prodotti personalizzati proprietari capaci di garantire la potenza sufficiente ad alimentare queste applicazioni, tuttavia trattandosi di prodotti personalizzati non è

sempre possibile assicurare l'interoperabilità tra le varie marche. Lo standard 802.3af supporta anche la cosiddetta classificazione dell'alimentazione che permette all'unità PoE e alle altre periferiche di "negoziare" la quantità di alimentazione necessaria. Ciò significa, ad esempio, che uno switch intelligente può riservare una quantità di alimentazione sufficiente e idonea per la periferica (telecamera), con il conseguente vantaggio che lo switch può essere utilizzato con un maggior numero di uscite PoE.

3.4.7 Uso di Power over Ethernet

PoE utilizza i cavi di rete standard (ad esempio i cavi Cat. 5) per fornire l'alimentazione alle periferiche connesse in rete tramite le porte dati. La maggior parte dei produttori di switch di rete di oggi fornisce il supporto per PoE integrato. Gli utenti che già dispongono di un'infrastruttura di rete basata su switch possono usufruire della stessa funzionalità aggiungendo semplicemente un cosiddetto midspan allo switch, che aggiunge potenza al cavo di rete. Tutte le telecamere di rete senza tecnologia PoE incorporata possono essere integrate in un sistema PoE mediante uno splitter attivo.

3.5 WIRELESS

Sebbene le reti cablate siano ampiamente diffuse, l'uso di una rete wireless può talvolta offrire maggiori vantaggi funzionali ed economici. Questa tipologia di rete può essere utile, ad esempio, negli edifici protetti dove l'installazione di cavi rischierebbe di danneggiare gli interni o nelle strutture in cui è necessario spostare regolarmente le telecamere in punti diversi senza dover reinstallare i cavi, come nel caso specifico dei punti vendita al dettaglio. La tecnologia wireless viene anche comunemente usata per collegare edifici o siti senza ricorrere a complessi e costosi lavori di scavo. La tecnologia wireless può essere utilizzata al di là dei limiti fisici delle reti, poiché può essere impiegata con sistemi video sia analogici che di rete. Le due categorie principali di comunicazioni wireless sono le seguenti:

3.5.1 Wireless LAN (chiamata anche WLAN):

Una LAN è per definizione una rete locale, cioè una rete che copre distanze limitate, generalmente installata all'interno di edifici. Gli standard per le reti wireless sono oggi ampiamente consolidati, tanto che è possibile usare insieme periferiche di più produttori.

3.5.2 Bridge wireless

Per poter collegare edifici o siti con collegamenti ad alta velocità, è necessario usare un collegamento dati point-to-point capace di coprire lunghe distanze e garantire velocità elevate. Le due tecnologie più comunemente usate sono i raggi a microonde e laser.

3.5.3 Standard LAN wireless

3.5.4 802.11a

Standard che utilizza una larghezza di banda pari a 5 GHz e garantisce una velocità effettiva pari a ~24 Mbps, in ambienti esterni e fino a distanze di 30 m (100 piedi). Questo standard è supportato solo da un numero limitato di prodotti. La larghezza di banda teorica è 54 Mbps.

3.5.5 802.11b

Standard che garantisce una velocità effettiva di ~5 Mbps in ambienti esterni, fino a distanze massime di 100 m (300 piedi). Questo standard usa la banda 2,4 GHz. La larghezza di banda teorica è 11 Mbps.

3.5.6 802.11g

Rappresenta lo standard più comunemente utilizzato che offre prestazioni migliori rispetto allo standard 802.11b, con velocità di trasmissione effettive massime di ~24 Mbps in ambienti esterni, fino a distanze massime di 100 m (300 piedi). Questo standard usa la banda 2,4 GHz e ha una larghezza di banda teorica di 54 Mbps.

3.5.7 802.11n

Versione successiva dello standard 802.11 Wireless LAN. La velocità effettiva sarà superiore a 100Mbps.

Accesso wireless a banda larga

3.5.8 802.16 - WiMAX

Lo standard IEEE 802.16, noto anche con il nome di WiMAX, definisce le specifiche per le reti metropolitane wireless fisse a banda larga (MAN) basate su un'architettura punto-multipunto. Lo standard disciplina l'uso della larghezza di banda entro gli intervalli di frequenza compresi tra 10GHz e 66GHz, e inferiori a 11GHz. 802.16 supporta velocità di caricamento/download in bit estremamente elevate su stazioni base situate a una distanza massima di 50km/30 miglia, utile per la gestione di servizi di tipo VoIP.

3.5.9 Protezione Wireless

La natura stessa delle comunicazioni wireless fa sì che qualsiasi utente in possesso di un dispositivo wireless, che si trovi nell'area di copertura della rete, possa collegarsi alla rete e condividerne i servizi. Ciò spiega perché è così importante proteggere le reti.

3.5.10 Bridge wireless

Alcune soluzioni utilizzano standard diversi, rispetto all'ultra-diffuso standard 802.11, che garantiscono prestazioni di gran lunga superiori e la possibilità di usare cavi di maggiore lunghezza con un livello di protezione molto elevato. Questi standard prevedono l'uso di altri sistemi a radiofrequenza come i collegamenti a microonde. Un'altra tecnologia molto diffusa è quella basata su sistemi ottici quali i collegamenti

laser. I collegamenti a microonde offrono velocità fino a 1000 Mbps fino a distanze massime di 80 km (130 miglia). Per collegare distanze non coperte dalla portata di questi sistemi, è possibile anche usare i sistemi di comunicazione satellitare. Tuttavia, la modalità di trasmissione di questi sistemi, che prevede l'invio/la ricezione dei dati al/dal satellite, può incrementare significativamente la latenza (nell'ordine di molti secondi) e li rende pertanto inadeguati per funzioni come il controllo manuale delle telecamere Dome e le applicazioni per le video conferenze, in cui è generalmente richiesta una bassa latenza. Inoltre, se la larghezza di banda richiesta è molto alta, i sistemi satellitari possono rivelarsi molto costosi.

3.5.11 Livello trasmissivo

Una volta instaurata l'interconnessione fisica tra gli utenti della rete (per utenti della rete si intendono sia soggetti fruitori della rete come computer e postazioni di lavoro, sia soggetti passivi come telecamere e altri sistemi di acquisizione) è necessario stabilire in che modo i segnali debbano essere trasmessi e soprattutto in che modo disciplinare il flusso dati.

In pratica, realizzata una rete interconnessa coerente, tutti gli utenti possono liberamente immettere nel sistema i propri messaggi. Essendo il mezzo condiviso fra tutti, e potendo essere gli utenti anche svariate migliaia, risulta evidente la problematica del flusso dati: ogni utente inserisce nel mezzo il suo pacchetto IP.

Analogamente a quanto accade in un corso d'acqua, gli utenti inseriscono nel sistema i propri pacchetti come fossero gocce d'acqua. Un osservatore è in grado di vedere lo scorrere del fiume ma non può distinguere una goccia da un'altra ma soprattutto non è in grado di capire a priori dove ogni singola goccia è diretta.

Una rete IP è in grado di risolvere questa non banale problematica.

3.5.12 Protocolli per il trasporto dei dati

Il protocollo più comunemente usato per la trasmissione di dati in rete è la suite di protocolli TCP/IP. Il protocollo TCP/IP funge da "portante" per molti altri protocolli; ad esempio per il protocollo HTTP (Hyper Text Transfer Protocol) utilizzato per visualizzare le pagine Web su server collegati a Internet.

I protocolli e le porte più comunemente utilizzati per il trasferimento di video in rete comprendono:

- FTP (File Transfer Protocol), per immagini e files da un server o applicativo compatibile;
- SMTP (Send Mail Transfer Protocol), unicamente utilizzato per inviare email;
- HTTP (Hyper Text Transfer Protocol), utilizzato per l'invio di ipertesti elettronici come pagine web e le interfacce di controllo delle telecamere di rete;
- HTTPS (Hyper Text Transfer Protocol Secure), come HTTP ma con crittografia dei dati mediante certificati digitali;
- RTP (Real Time Protocol), usato per video streaming e audio;
- RTSP (Real Time Streaming Protocol): livello superiore di RTP.

IP utilizza due protocolli: TCP (Transmission Control Protocol) e UDP (User Datagram Protocol). Il protocollo TCP offre un canale di trasmissione affidabile e basato su connessione in grado di suddividere grandi volumi in dati in pacchetti più piccoli che possano essere trasmessi sulla rete fisica. Questo protocollo verifica inoltre che i dati trasmessi da un lato della rete vengano ricevuti sull'altro lato. Il protocollo UDP è invece un protocollo non basato su alcuna connessione che non garantisce l'effettiva consegna dei dati e lascia quindi all'applicazione il compito di effettuare il controllo delle trasmissioni e la verifica degli errori.

Il protocollo TCP viene generalmente usato quando la sicurezza delle comunicazioni ha la priorità sulla latenza di trasmissione. Tuttavia, le ripetute trasmissioni che si verificano con il protocollo

TCP possono provocare ritardi significativi. Il protocollo UDP non prevede la possibilità di ritrasmettere i dati persi, quindi non esiste il rischio di ritardi.

3.5.13 Metodi di trasmissione usati dai sistemi video di rete: Unicasting, Multicasting e Broadcasting

I dati possono essere trasmessi in rete in tre modi diversi:

- • Unicast - il mittente e il destinatario comunicano utilizzando uno schema point-to-point. I pacchetti dati vengono inviati solo a un destinatario, quindi gli altri computer della rete non hanno la necessità di elaborare le informazioni.
- • Multicast - comunicazione tra un unico mittente e più destinatari collegati in rete. Le tecnologie multicast vengono utilizzate per ridurre il traffico di rete nel caso in cui più destinatari abbiano l'esigenza di visualizzare simultaneamente la stessa fonte, poiché consentono di trasmettere contemporaneamente un unico flusso di dati a centinaia di destinatari. La principale differenza rispetto al metodo unicasting risiede nel fatto che il flusso video deve essere inviato una sola volta. Il multicasting (o IP-Multicasting) viene comunemente usato per le trasmissioni RTP.
- • Broadcast - trasmissione di tipo da "uno-a-tutti". Sulle reti LAN, questi tipi di trasmissioni vengono generalmente usati solo su alcuni segmenti specifici della rete e non sono generalmente idonei per la trasmissione di video in rete.

3.5.14 Livello logico

Connessi tutti gli utenti ed adottato un sistema trasmissivo in grado di trasferire i messaggi, è necessario individuare un sistema per identificare gli utenti in modo univoco.

A questo punto per distinguere tutti gli utenti logicamente connessi alla rete si applica loro un indirizzo IP univoco.

3.5.15 Indirizzi IP

L'indirizzo IP (Internet Protocol address) è un numero univoco utilizzato dalle periferiche per identificarsi e comunicare in reti che utilizzano il protocollo IP. Ciascun indirizzo IP è costituito da quattro numeri separati da un punto ("."). Ciascun numero deve essere compreso tra 0 e 255. Un esempio tipico di indirizzo potrebbe essere "192.36.253.80".

L'indirizzo IP è ulteriormente diviso in due sezioni che identificano rispettivamente la rete e l'host. Il limite tra queste due sezioni è la cosiddetta netmask o lunghezza del prefisso. Una netmask con il numero 255.255.255.0 indica che i primi 3 byte sono riservati all'indirizzo di rete e che l'ultimo byte è riservato all'indirizzo dell'host. L'indirizzo può anche essere delimitato tramite la lunghezza del prefisso. Nel caso dell'esempio precedente, la lunghezza del prefisso sarebbe equivalente a 24 bit (ad esempio 192.36.253.80/24)

Alcuni blocchi di indirizzi sono riservati per l'uso su reti private:

- • 10.0.0.0/8 (netmask 255.0.0.0);

- • 172.16.0.0/12 (netmask 255.240.0.0);
- • 192.168.0.0/16 (netmask 255.255.0.0);

Questi indirizzi vengono usati su reti Internet private, e non possono essere usati sulla rete Internet pubblica.

Tutti gli indirizzi IP non privati sono pubblici e sono assegnati univocamente ad apparati di rete raggiungibili liberamente (o meno) su internet o nelle comunicazioni facenti parte di servizi su scala mondiale come telefonia e reti VPN.

Nel caso di SVC verranno unicamente utilizzati indirizzi IP privati utilizzati nella rete privata Comunale, e verrà considerato l'utilizzo di IP pubblici sole nel caso in cui si necessiti di accessi al servizio remoti veicolati tramite internet.

3.5.16 Ip version 6 (IPv6)

IPv6, ovvero la versione 6 del protocollo IP, è stato progettato come aggiornamento avanzato della versione precedente e verrà utilizzato insieme alla versione 4 per un periodo limitato di tempo. Il protocollo IPv6 è stato progettato per consentire una crescita graduale di Internet, sia in termini di numero di host che di volume complessivo di traffico trasmesso.

Il vantaggio più evidente del protocollo IPv6 rispetto al protocollo IPv4 deriva dalla maggiore lunghezza

degli indirizzi, incrementata da 32 a 128 bit. Questo ampliamento è stato introdotto in vista della crescita di Internet, ovvero per permettere un uso illimitato (per scopi diversi) di reti e sistemi. Il protocollo IPv6, ad esempio, prevede l'assegnazione di un indirizzo univoco a cellulari e periferiche portatili elettroniche.

La versione del protocollo utilizzata in SVC è IPv4, motivata anche dal fatto che funzionando ad hoc per una rete locale, la versione 4, garantisce di per sé migliaia di utenze (assolutamente adeguate per un sistema come SVC).

Gli indirizzi IP vengono applicati a tutte le identità di rete indipendentemente dal luogo geografico in cui sono connessi alla rete. In fatti, mediante switching di livello 2 o mediante algoritmi di routing o semplicemente mediante interrogazione sistematica della rete, il protocollo IP fa in modo di assegnare al pacchetto interessato l'IP del destinatario, la rete interroga i suoi utenti per conoscere la posizione del destinatario, a quel punto il pacchetto viene instradato fino a destinazione.

Questo procedimento avviene con assoluta trasparenza del mezzo trasmissivo e della morfologia della rete stessa; ovviamente, nel caso in cui un utente si trovi in una zona remota rispetto all'identità di partenza, il pacchetto potrà impiegare maggior tempo per conoscere e percorrere correttamente il percorso per giungere a destinazione, considerando anche che può essere soggetto a restringimenti di banda dovuti a congestione di traffico nel mezzo trasmissivo (dovuta per esempio a occupazione di banda dovuta a utenza massiva).

Questo genere di problemi si risolve durante la progettazione della rete dati tenendo bene presente i principi dell'ingegneria delle comunicazioni di rete che impongono canoni precisi per la conformazione della rete.

3.6 UTILIZZO DI UNA RETE IP COME INFRASTRUTTURA DI COMUNICAZIONE

Alla luce delle considerazioni emerse dall'analisi dell'architettura di una rete IP è possibile delineare le caratteristiche di una struttura di comunicazione integrabile nel comprensorio cittadino in grado di ospitare un quantitativo adeguato di utenze private IP.

Valutati i vantaggi e la semplicità di installazione ed ampliamento di una rete IP cittadina e della possibilità di reperire telecamere IP (e di utenze Internet) di alta qualità configurabili in tutti come utenze IP, occorre delineare le caratteristiche delle tecnologie da utilizzare:

- Per interconnettere in modo coerente le utenze IP cittadine derivanti dalle telecamere IP dislocati nel comprensorio
- Sistemi di riprese IP evoluti e programmabili;
- Sistemi di registrazione, monitoraggio e programmazione del sistema del Comune di Rapallo;
- Sistemi di sorveglianza da adottare nei luoghi di difficile raggiungibilità;
- Sistemi di distribuzione della banda di accesso ad internet.

3.7 TECNOLOGIE DA IMPIEGARE NELLA COSTITUZIONE DELLE TRATTE DI COMUNICAZIONE

Per la costituzione della rete IP vengono impiegati impianti di networking avanzati che permettono l'interconnessione di utenze a seconda delle loro caratteristiche primarie.

In previsione anche dell'utilizzo di un'architettura stellare di rete (precisata opportunamente nel capitolo successivo) viene adottato il modello di interconnessione a nodi che prevede la notazione di 2 tipologie di oggetti:

- NODO: apparato di interconnessione tra 2 o più tratte, è in grado di commutare le informazioni tra una tipologia di mezzo ad un'altra (ad es.: rame – fibra ottica);
- TRATTA: interconnette fisicamente 2 nodi utilizzando una sola tipologia di mezzo trasmissivo.

3.8 TRATTE DI INTERCONNESSIONE

3.8.1 Fibra Ottica

Le tratte di interconnessione costituiscono fisicamente il canale trasmissivo capace di convogliare tutti i pacchetti i IP da un punto ad un altro della rete stessa. Sostanzialmente sono di tre tipi:

- Tratte in fibra ottica;
- Tratte in rame;
- Tratte irradiate (wireless).

Il sistema di cablaggio in fibra ottica consente la trasmissione di dati, voce e video su un unico cavo alla velocità di GigaBit Ethernet (1000Base-x) e 10-GigaBit Ethernet (10GBase-x).

Il cavo in fibra ottica è generalmente sempre presente in coppia: una per ognuno dei due sensi di trasmissione.

I vantaggi peculiari della fibra ottica sono:

- Elevata capacità in termini di ampiezza di banda (fino a 10Gb/s);
- Elevata estensibilità: 550m a 10Gb/s e fino a 2Km con le opportune ottimizzazioni;
- Completa immunità ai disturbi elettromagnetici tipici della rete elettrica (quali alimentazione di lampioni o tratte di competenza telefonica);
- Mini-invasività del cavo.

Le sue caratteristiche, giustificate anche da un costo relativamente elevato, la rendono ideale per costituire una dorsale per il grande traffico della rete.

3.8.2 Cablaggio in rame UTP/STP

Il sistema di cablaggio in rame di tipo UTP è in assoluto il più diffuso nell'implementazione delle tecnologie di rete.

UTP (Unshielded Twisted Pairs) è un cavo formato da 4 doppi in rame attorcigliati in modo da ridurre le interferenze tra i medesimi 8 cavi.

STP (Shielded Twisted Pairs) è il medesimo cavo dell'UTP ma dotato di doppia schermatura gomma/metallo per ridurre le eventuali interferenze elettromagnetiche con l'esterno. STP è particolarmente adatto per il cablaggio di esterni.

UTP ed STP sono l'anima dell'ultimo miglio dei cablaggi tipici dello standard EIA/TIA 568.

Attualmente ha raggiunto la versione CAT7 adatta per le trasmissioni Gigabit multilivello, tuttavia lo standard precedente, CAT6, si presta maggiormente per la videosorveglianza in quanto certificato sì per trasmissioni a 1Gbps ma con una maggiore estensione: fino a 100 m.

Le sue caratteristiche sono:

- Basso costo e facile installazione;
- Interfacciabilità con tutte le telecamere, nodi e periferiche di rete;
- Facilità di gestione;
- Possibilità di estendere la tratta mediante ripetitori economici.

Solitamente si utilizzano terminali di tipo RJ45 per la connessione con gli apparati di rete per via della loro semplicità d'uso e per la loro solidità.

Queste caratteristiche rendono UTP/FTP ideale per connettere tutte le estremità della rete (videocamere, terminali, unità di registrazione e in generale nodi terminali) alla dorsale.

3.8.3 Wireless

Per tratta di comunicazione wireless si intende una tipologia di comunicazione ad onde elettromagnetiche regolamentata dallo standard IEEE 802.11.

IEEE 802.11 o Wi-Fi definisce uno standard per le reti WLAN sviluppato dal gruppo 11 dell'IEEE 802, in particolare in livello fisico e MAC del modello ISO/OSI, specificando sia l'interfaccia tra client e base station (o access point) sia tra client wireless.

Questa famiglia di protocolli include tre protocolli dedicati alla trasmissione delle informazioni (a,b,g), la sicurezza è stata inclusa in uno standard a parte, 802.11i. Gli altri standard della famiglia (c, d, e, f, h, ...) riguardano estensioni dei servizi base e miglioramenti di servizi già disponibili. Il primo protocollo largamente diffuso è stato il b; in seguito si sono diffusi il protocollo a e soprattutto il protocollo g.

3.8.4 802.11b

802.11b ha la capacità di trasmettere al massimo 11Mbit/s e utilizza il Carrier Sense Multiple Access con Collision Avoidance (CSMA/CA) come metodo di trasmissione delle informazioni. Una buona parte della banda disponibile viene utilizzata dal CSMA/CA. In pratica il massimo trasferimento ottenibile è di 5.9 Mbit/s in TCP e di 7.1 Mbit/s in UDP. Metallo, acqua e in generale ostacoli solidi riducono drasticamente la portata del segnale. Il protocollo utilizza le frequenze nell'intorno dei 2.4GHz. Utilizzando antenne direzionali esterne dotate di alto guadagno si è in grado di stabilire delle connessioni punto a punto del raggio di molti chilometri. Utilizzando ricevitori con guadagno di 80 decibel si può arrivare a 8 chilometri o se le condizioni del tempo sono favorevoli anche a distanze maggiori ma sono situazioni temporanee che non consentono una copertura affidabile. Quando il segnale è troppo disturbato o debole lo standard prevede di ridurre la velocità massima a 5.5, 2 o 1 Mbit/s per consentire al segnale di essere decodificato correttamente.

3.8.5 Canali e compatibilità internazionale

802.11b e 802.11g dividono lo spettro in 14 sottocanali da 22MHz l'uno. I canali sono parzialmente sovrapposti tra loro in frequenza, quindi tra due canali consecutivi esiste una forte interferenza. I 2 gruppi di canali 1, 6, 11 e 2, 7 e 12 non si sovrappongono fra loro e vengono utilizzati negli ambienti con altre reti wireless. Gli unici canali utilizzabili in tutto il mondo sono il 10 e 11 dato che la Spagna non ha concesso i canali dall'1 al 9 e molte nazioni si limitano ai primi 11 sottocanali.

3.8.6 802.11g

Questo standard venne ratificato nel giugno del 2003 . Utilizza le stesse frequenze del b cioè la banda di 2.4 GHz e fornisce una banda teorica di 54 Mbit/s che nella realtà si traduce in una banda netta di 24.7 Mbit/s, simile a quella dello standard 802.11a. È totalmente compatibile con lo standard b ma quando si trova a operare con periferiche b deve ovviamente ridurre la sua velocità a quella dello standard b.

3.8.7 Certificazione

Dato che l'IEEE rilascia solo un insieme di specifiche, ma non prevede nessun test né certificazione per riconoscere che un prodotto rispetti dette specifiche, un gruppo di fabbricanti ha creato la Wi-Fi Alliance, un'associazione nata per certificare l'interoperabilità dei prodotti e per diffondere le reti Wi-Fi. In questa associazione vi sono praticamente tutti i costruttori di componenti per schede Wi-Fi. Attualmente l'Alliance si occupa solo degli standard a, b e g, oltre che degli standard di sicurezza come il WEP, il WPA e il nuovo 802.11i, conosciuto anche come WPA2.

3.8.8 Sicurezza

Le versioni originali dei protocolli 802.11 erano basati sulla crittografia WEP.

Nel 2001 un gruppo dell'università di Berkeley presentò un lavoro dove descriveva le falle di sicurezza del protocollo 802.11. Questo gruppo si concentrò sull'algoritmo di cifratura utilizzato dal WEP (RC4), che nell'implementazione scelta per lo standard 802.11 era molto debole e facilmente forzabile.

L'IEEE mise al lavoro un gruppo di lavoro per progettare un'evoluzione dello standard di sicurezza WEP. Anche la Wi-Fi Alliance creò un gruppo di lavoro per risolvere il problema e la Wi-Fi Alliance annunciò la nascita del WPA durante il 2003. Il WPA era un'evoluzione del WEP che rimuoveva la maggior parte dei problemi di sicurezza rendendo le reti wireless discretamente sicure. Intanto il gruppo dell'IEEE era al lavoro e nel giugno del 2004 rilasciò le specifiche dell'IEEE 802.11i. Questo standard rendeva le reti wireless molto sicure e la Wi-Fi Alliance lo adottò subito sotto il nome di WPA2. Il WPA2 abbandona l'RC4 come algoritmo di codifica per passare al più sicuro Advanced Encryption Standard.

Le varie opzioni di sicurezza disponibili comportano però livelli di complessità crescente per la configurazione e l'adeguamento del firmware e di drive di sistema operativo di Access Point e schede di rete wireless.

L'intercettazione costituisce un rischio per la privacy degli utenti (potrebbero ad esempio essere sottratti segreti industriali o dati bancari). L'accesso abusivo alla rete è rischioso anche perché non è possibile rintracciare a posteriori gli autori di comportamenti pericolosi o illegali.

3.8.9 Nodi di comunicazione

I nodi di interconnessione rappresentano il cuore del livello trasmissivo della rete. Vengono interconnessi dalle tratte opportune e generano/ricevono i segnali attraverso il mezzo concesso dalla tratta.

Ne esistono di due tipi:

- Nodo di interconnessione (switch, router, Access Point). Utilizzato per prolungare la rete, generalmente può operare un cambio di tipologia di tratta interconnettendo di fatto tratte di diverso tipo, genera o rigenera il segnale contenente i pacchetti IP;
- Nodo terminale (telecamera IP, server, registratore IP). Definiti anche come utenze della rete, banalmente sono di tipo o ricevente o trasmettente.

3.8.10 Nodi di interconnessione

I nodi di interconnessione sono apparecchi ad alta efficienza e ad alto carico di rete in grado di trasferire qualsiasi richiesta dati da un punto ad un altro della rete.

Generalmente vanno configurati e posizionati sul territorio in modo protetto, poi vengono gestiti tramite i terminali di amministrazione della rete.

Una volta posizionati e nascosti, lavorano costantemente e sostengono la rete. Effettivamente sono il cuore della rete. Per questo la loro scelta va eseguita in modo oculato e consapevole.

Questi nodi interconnettono sia segmenti di fibra ottica o wireless sia avviano un centro di accesso alla rete UTP/STP. Per via della loro neuralgicità vengono installati all'interno di opportuni box su standard RACK poi collocati sul territorio.

3.8.11 Switch PoE

Lo Switch ethernet è un elemento chiave nella realizzazione della rete LAN. Esso è in grado di trasmettere i pacchetti IP in maniera trasparente alla comunicazione istradando direttamente verso la porzione di rete indicata nell'indirizzo IP di destinazione. E' in grado di interconnettere tratte in fibra ottica (mediante opportuno adattatore miniGBIC) con tratte in rame. E' un impianto attivo, quindi necessita di alimentazione 220V con sistema di messa a terra a norma (per esterni). E' dotato di almeno 8 porte per UTP/STP.

Capace interconnettere da 8 utenze in UTP/STP tra cui telecamere ed altri switch, tutte garantendo le specifiche necessarie a mantenere il Power over Ethernet (PoE) delle telecamere.

Le sue caratteristiche:

- Carico interno: 4Gb/s;
- Rack 1 1U;
- Almeno 8 connessioni UTP/STP;
- PoE (Power over Ethernet);
- Compatibile con tutti gli standard di trasmissione.

Ideale come centro stella per diffondere il collegamento adatto alla collocazione delle telecamere PoE e bridging in fibra ottica. Intrinsecamente utilizzabile come ripetitore.

3.9 TELECAMERA IP AD ALTE PRESTAZIONI

Si tratta di un particolare tipo di telecamera IP dalle caratteristiche tecniche molto particolari. Sfruttando riprese ad ampio raggio della grandezza di oltre 2 Megapixels è in grado di registrare su risorsa di rete (nas o server) immagini su cui è possibile effettuare ingrandimenti a posteriori direttamente sul registrato.

E' interamente programmabile e dispone di modulo di montaggio rinforzato per esterni.

Le sue caratteristiche sono peculiari:

- Sensore CMOS ad alte prestazioni: 2Mp a colori con illuminatori a infrarossi;

- Sistema di connessione di rete con ausilio di alimentazione PoE;
- Operatività 0° - 45°C;
- Consumo 7,5W.

Relativamente all'impianto di San Michel di Pagana sono presenti 2 tipologie di telecamere ad alte prestazioni:

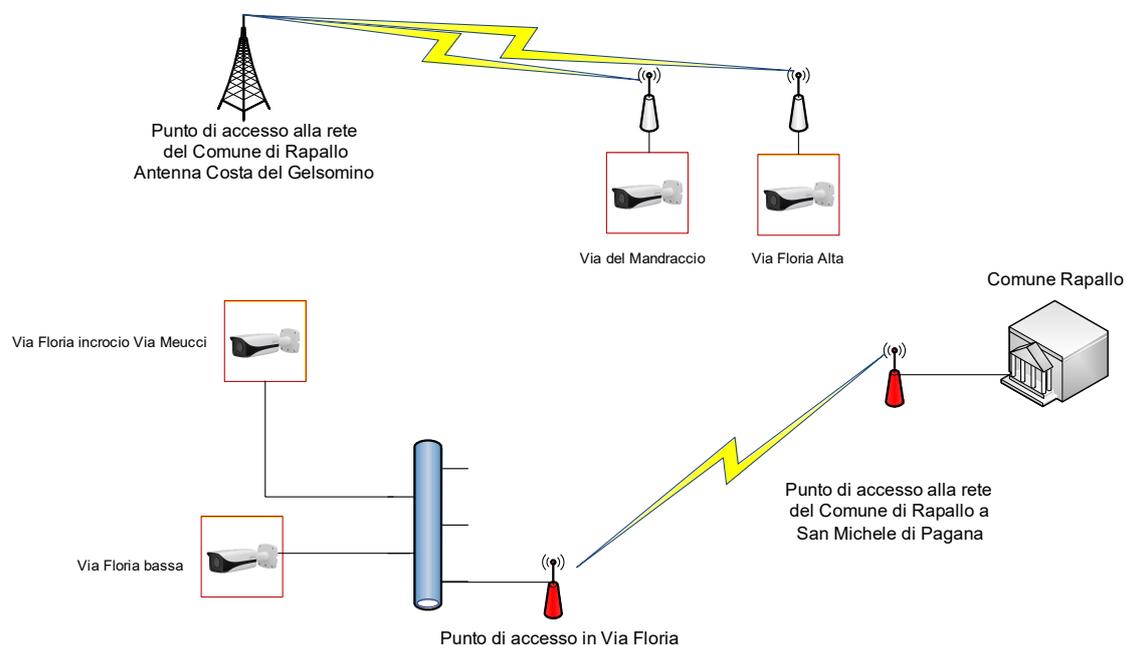
- a) Direzionale: si tratta di una telecamera IP dotata di 1 ottica direzionale con raggio visivo di 83° e illuminatore a 30m.
- b) Direzionale per lettura targhe: si tratta di una telecamera IP dotata di 1 ottica variabile e direzionale con software a bordo per la lettura delle targhe.

4 DIMENSIONAMENTO DELL'INFRASTRUTTURA SUL TERRITORIO

Valutate le tecnologie degli impianti utilizzabili nel progetto è possibile delineare uno schema generico dell'infrastruttura di rete prima di modellarla direttamente sul territorio.

4.1 SCHEMA GENERICO LOGICO

Come specificato in precedenza, viene utilizzato un modello di tipo BUS a Stella multipla o ad albero.



Sostanzialmente consiste nel delineare un segmento multi direzionale a cui sono connessi tutti gli utenti in maniera locale; ogni utente attinge o inserisce dati nel BUS ed è il BUS stesso che gestisce le collisioni e lo scambio dati vero e proprio. Il fatto che si tratta di un albero permette che ogni nodo *padre* sia responsabile solo delle proprie telecamere *figlie* in modo da ridurre al minimo la possibilità di guasti gravi.

Questo tipo di soluzione si adatta bene a configurazioni geografiche longitudinali quale quella del comprensorio cittadino di Rapallo in particolare della Frazione di San Michele di Pagana

Dalla morfologia si evince un dato sostanziale: il BUS rappresenta il cuore dello scambio dati della rete, per tanto va dimensionato con la tecnologia più stabile e dotata della maggiore capacità possibile in virtù anche di una possibile futura espansione del sistema.

Per questo proposito il collegamento in HyperLan e la cablatura con cavi UTP è la scelta più corretta, anche in virtù della vicinanza del primo punto fibra del Comune di Rapallo.

4.2 COSTITUZIONE DI UNA DORSALE IN TECNOLOGIA HYPERLAN

La tecnologia utilizzata per il collegamento dei vari punti alla fibra ottica del Comune di Rapallo è quella a 5,4 Ghz attraverso backhaul PTP (point to point) ed access point (point multi point).

Il Backhaul sarà realizzato tra Via Floria Bassa ed il punto fibra del Comune di Rapallo ubicato in San Michele di Pagana presso il palo utilizzato per le telecamere in prossimità della fermata dell'autobus. Il collegamento dell'antenna avverrà tramite cavo UTP in switch esistente o attraverso la fornitura di uno switch dedicato.

Il collegamento tra subscriber ed access point è previsto tra il sito di Via Floria Bassa, il sito di Via del Mandraccio e la torre di Costa del Gelsomino dove è ubicato il collegamento con la fibra ottica del Comune di Rapallo.

4.3 POSIZIONAMENTO DELLE TELECAMERE IN PROSSIMITÀ DEI NODI DI INTERCONNESSIONE

Individuati i nodi (armadi tecnici forniti ed installati dal Comune di Rapallo) e dotati di corrente elettrica, è possibile installare le telecamere IP nella zona di competenza del nodo adottando le seguenti direttive:

- Entro 90m dal nodo se si intende utilizzare una telecamera IP dotata di PoE.

A questo punto tutte le telecamere connesse alla dorsale (BUS) tramite il nodo fanno parte di un'unica rete globale IP, basta collegare alla dorsale la centrale di controllo e si ottiene il completo controllo di tutte le funzionalità degli apparecchi facenti parte della rete.

Inoltre:

- Sarà possibile in futuro connettere altre centrali di controllo in qualsiasi punto della dorsale;
- Sarà possibile quindi anche spostare in qualsiasi punto della dorsale la centrale di controllo.

Le postazioni di ripresa sono le seguenti:

- N° 4 Telecamere di visione generale e lettura delle targhe
 - Via Floria Bassa
 - Via Floria incrocio Via Meucci
 - Via Floria Alta
 - Via del Mandraccio

5 ELENCO PRODOTTI

Il presente elenco contiene le descrizioni tecniche di ogni singolo elemento contenuto nell'impianto di San Michele di Pagana, le specifiche tecniche incluse sono da considerarsi vincolanti per la produzione degli impianti stessi.

Tutti gli elaborati facenti parte del progetto fanno riferimento direttamente alle direttive incluse nell'elenco prodotti.

6 IMPIANTI PER LA RIPRESA DELLE IMMAGINI

Di seguito sono elencati gli impianti necessari per le riprese delle immagini e dei video congiuntamente alle caratteristiche tecniche vincolanti.

Viene considerata la telecamera un unico oggetto accorpato con la sua custodia singola e il kit di montaggio a muro/palo poiché esistono sul mercato telecamere che hanno la possibilità di essere separate dalla propria custodia per effettuare installazioni interne e altre che sono inscindibili dal proprio involucro per esterni. Altre invece offrono l'involucro esterno separato dai braccetti per aggancio palo per scegliere la tipologia di braccio mentre altri offrono l'involucro già munito di braccio e agganci.

Quindi, come Telecamera IP si intende:

- Telecamera IP (postazione di ripresa);
- Custodia per esterni (se non già compresa);
- Kit di braccetti per installazione palo (braccetti, placche, viteria);
- Adattatore per alimentazione esterna (se non già presente linea PoE).
- Armadio stagno base palo

Data la natura unicamente esterna dell'impianto è corretto considerare la telecamera mutuamente con la propria custodia e tutti gli accessori che la rendono installabile all'esterno.

6.1 VIDEOCAMERA IP DIREZIONALE E DI LETTURA TARGHE

Videocamera di rete IP dotata delle seguenti caratteristiche:

Un progetto di security all'avanguardia può aggiungere ulteriore valore alla clientela finale scegliendo sistemi di videosorveglianza, videocontrollo e controllo accessi veicolare capaci di riconoscere in automatico le targhe.

Forte di queste considerazioni, Hikvision ha progettato e realizzato una propria tecnologia di rilevamento ed identificazione targhe basata sui dispositivi di ripresa IP già presenti a catalogo ed ha sviluppato una linea di prodotti che non si differenziano nell'aspetto esteriore e nelle peculiarità installative, ma che sono basati su una specifica famiglia di sensori CMOS Ultra Low-Light con WDR a 120dB (capace di gestire fortissimi livelli di contrasto) e processori di elaborazione video tra i più avanzati. E' la famiglia Darkfighter.



Alla base di tutte le soluzioni di riconoscimento targhe Hikvision troviamo l'hardware Darkfighter, derivato dalla famiglia di prodotti più performanti del catalogo Hikvision e caratterizzato da un sensore dotato di estrema sensibilità (Ultra Low-Light), in grado di fornire immagini sino a 60 fotogrammi al secondo sia in riprese diurne che notturne, ed in grado di mantenere il giusto equilibrio cromatico e dei contrasti dell'immagine anche con riprese in controluce. Il tutto ad una risoluzione Full HD.

La famiglia di prodotti ANPR – AUTOMATIC NUMBER PLATE RECOGNITION, caratterizzata da un hardware allo stato dell'arte dotato di elevatissima capacità di calcolo, oltre ai noti algoritmi di Video Content Analysis di Hikvision (presenti di default in questa classe di prodotti), ospita anche lo specifico algoritmo di Licence Plate Recognition sviluppato dalla Divisione Ricerca e Sviluppo di Hikvision.

L'impiego di una libreria di riconoscimento delle targhe contenente oltre 35 paesi dell'area europea e 15 paesi dell'ex area sovietica, oltre ad altre librerie per Medio Oriente, Africa, area

Asia-Pacifico ed America, permette il riconoscimento automatico del profilo della targa e la relativa nazionalità, oltre alla lettura automatica dei caratteri. L'elevata qualità delle immagini generate dal sensore delle telecamere Darkfighter permette di rilevare le targhe anche in condizioni di illuminazione estremamente ridotte, sia con immagini a colori (luce diurna), sia in bianco e nero (notturna).

L'elevata qualità ed efficacia dell'algoritmo di lettura targhe, in grado di riconoscere una targa che occupa anche solo 1/8 in orizzontale della scena ripresa su una risoluzione Full HD, permette di adottare anche una sola telecamera di lettura targhe per rilevare le targhe sino a 4 corsie contemporanee (installazione sulla verticale e velocità inferiore ai 50 Km/h). Le elevate performance dell'algoritmo garantiscono ottimi risultati di rilevamento a basse velocità anche in condizioni limite, ad esempio in caso di disallineamento tra targa e telecamera di quasi 40 gradi. E' quindi possibile impiegare questi prodotti per il controllo accessi veicolare anche nelle situazioni più complesse in termini di geometrie di ripresa.

Relativamente alle capacità di riconoscimento delle targhe, nelle corrette condizioni operative l'evoluzione dell'algoritmo ANPR Hikvision consente oggi una "capture rate" (percentuale di targhe lette rispetto alle vetture transitate) del 99% ed una "recognition rate" (percentuale di corretto riconoscimento delle targhe lette) del 98%. In funzione del modello, differenziato per tipologia di involucro, queste prestazioni sono ottenibili sino a velocità di 120 Km/h e 160 Km/h. Nei prodotti di lettura targhe Hikvision sono disponibili ben quattro modelli (bullet, box, ecc): è quindi assicurata la massima flessibilità sia nella fase di progettazione sia in quella installativa. Conseguenza: massimo risultato con il minimo sforzo, sia in termini di posa in opera che di manutenzione.

Le telecamere di lettura targhe Hikvision sono infatti disponibili sia con un form factor di tipo bullet (con obiettivo varifocale motorizzato, autofocus ed illuminatore IR integrato), sia come box camera (telecamera "nuda" da inserire in una custodia esistente con obiettivo varifocale manuale e back focus motorizzato), sia come box camera in custodia (con obiettivo varifocale manuale, back focus motorizzato ed illuminatore integrato nella custodia). Quest'ultima soluzione supporta l'impiego di obiettivi dotati di lunghezze focali più spinte, tali da garantire un funzionamento impeccabile anche in condizioni installative solitamente proibitive.

7 ANTENNA HYPERLAN PER IL COLLEGAMENTO

Di seguito le caratteristiche delle antenne in tecnologia HyperLan che permettono il collegamento degli apparati di visione al server di registrazione del Comune di Rapallo.

Viene considerata l'antenna un unico oggetto accorpato con la sua custodia singola e il kit di montaggio a palo.

Quindi, come Antenna HyperLan si intende:

- Antenna a 5,4 Ghz (Backhaul, Access Point, Subscriber);
- Staffa a snood per installazione a palo/muro
- Alimentatore PoE

7.1 ANTENNA EPMP 1000

EPMP 1000: sono soluzioni punto-punto e punto-multipunto HiperLAN in banda libera 5.x GHz low-cost ma ad alte prestazioni che si vanno ad affiancare alla linea ad altissime prestazioni. Permettono l'accesso a banda larga con una soluzione di accesso fisso, in grado di erogare oltre 200 Mbps utilizzando tecnologia MIMO 2x2 con modulazioni OFDM. Utilizzando la sincronizzazione GPS, permette un uso scalabile delle frequenze radio disponibili in grado di far crescere la rete senza problemi di mutua interferenza.

Un algoritmo proprietario permette di allocare la banda disponibile dei link wireless in maniera adattativa, garantendo una Quality-of-Service definita utente per utente. La soluzione è estremamente versatile e permette installazioni anche di tipo punto-punto, per backhaul ad alta capacità.

Principali caratteristiche ePMP 1000

- Numero di utenze (subscriber) per settore (AP): fino a 120
- Range di frequenza: 5150 – 5970 MHz
- Potenza trasmissiva al connettore: +30dBm
- Ampiezza canale radio: 5, 10, 20 o 40 MHz
- Sincronizzazione possibile con: Ricevitore GPS integrato, CMM3/CMM4
- Massima distanza raggiungibile con canale @20 MHz: 21km/13 miglia

8 SOFTWARE DI LETTURA TARGHE

Di seguito il software che permette l'analisi dei flussi derivanti da telecamere OCR di lettura delle targhe.

Il software compatibile con i principali sistemi operativi permette la configurazione e l'analisi dei transiti, delle white list e delle black list.

Come software si intende:

- Chiave USB contenente software e manuali operativi
- Installazione su server

8.1 IVMS 4200

8.1.1 IVMS-4200, sistema intelligente di gestione video

iVMS-4200 è un software di recente sviluppo che include non solo la gestione delle funzioni di NVR, HVR, DVR, telecamere IP, schede di compressione video e decoder, ma anche funzioni di programmazione, centralizzazione e gestione del sistema video. Le sue potenti funzionalità lo rendono di uso comune in molteplici applicazioni di sorveglianza - anche complesse, locali e remote - di grandi sistemi, supermarket, negozi, monitoraggio urbano, applicazioni residenziali e industriali. iVMS4200 gestisce fino a 256 dispositivi e fino a 1024 telecamere, provenienti da siti differenti, ed è in grado di visualizzare su un monitor dedicato le immagini live di 64 telecamere contemporaneamente nella stessa schermata. Grazie alla presenza di diverse icone che si sovrappongono all'immagine live, si può accedere al controllo PTZ di Speed Dome, e si può accedere rapidamente al playback della telecamera selezionata.

Inoltre, la videata principale riporta tutte le applicazioni eseguite dal software sotto forma di icone, riprendendo la disposizione e la gestione delle App degli smartphones. Tra le applicazioni attuabili, la singola postazione iVMS-4000, che può gestire fino a 4 monitor con funzioni dedicate e personalizzabili, può essere impostata per ricevere le segnalazioni di allarme provenienti dal DVR, HVR e NVR o dalle telecamere IP, richiamando l'attenzione dell'operatore attraverso un segnale acustico, oppure generando un pop-up video della telecamera allarmata. Dalla postazione stessa sarà possibile generare l'invio di una e-mail a fronte di un allarme per assenza di segnale video oppure per lo scollegamento dalla rete ethernet di un dispositivo. iVMS permette inoltre di utilizzare l'Applicazione Decoder e di aggiungere una tastiera con Joystick sulla porta USB del computer.

8.1.2 NVR Server, software per la registrazione

Alla già completa piattaforma iVMS4200, è possibile aggiungere il servizio di registrazione locale NVR Server, il quale permette di unire le prestazioni del software a quelle di un registratore di immagini su computer o NAS: iVMS4200 diventerà così una vera e propria postazione di registrazione ridondata, utile sia per le immagini provenienti dalle singole telecamere IP, sia per

quelle collegate ad un registratore. Il playback delle immagini registrate su HDD o su Hard Disk del PC viene eseguito dalla stessa postazione iVMS-4200.

8.1.3 iVMS-4500, client software per dispositivi mobile

iVMS-4500 è un software nato per applicazioni smartphone e tablet che può essere utilizzato per il controllo delle immagini live da remoto di DVR analogici, HVR (Hybrid), NVR, Telecamere IP, Speed Dome IP o Encoder. Permette di visualizzare fino a 4 telecamere contemporaneamente provenienti da siti differenti. Il controllo remoto consente, oltre alla visualizzazione delle immagini live, anche il controllo PTZ delle Speed Dome, permette di scattare delle foto (Snapshot) e di registrare dei piccoli filmati. Su iPhone, iPad e Android è possibile anche la visualizzazione delle immagini registrate. Tramite l'utilizzo della Piattaforma Software di programmazione e gestione iVMS4200, si dispone della funzione di Movimentazione e Posizionamento Intelligente per tutte le telecamere zoom e PTZ analogiche (tramite connessione seriale) ed IP (tramite connessione ethernet) della gamma Hikvision. Grazie a questa funzionalità integrata del Software iVMS4000, interagendo semplicemente con il mouse sarà possibile ingrandire, allargare, centrare, dislocare le immagini provenienti dalle telecamere zoom e PTZ con grande semplicità, intuitività ed immediatezza. Il Posizionamento 3D Intelligente, oltre a velocizzare e migliorare sensibilmente le operazioni di gestione delle Telecamere PTZ, semplifica anche la fase progettuale e installativa, rendendo spesso superfluo l'uso di tastiere di controllo multifunzione.