Ed. 00

SMT-R2000

Manuale d’utente

4. 2007

SAMSUNG ELECTRONICS

COPYRIGHT

TRADEMARKS

I nomi dei prodotti menzionati in questo documento possono essere marchi di fabbrica e/o marchi depositati delle rispettive aziende.

WEEE SYMBOL INFORMATION

Corretto smaltimento del prodotto
(rifiuti elettrici ed elettronici)

(Applicabile nei paesi dell'Unione Europea e in quelli con sistema di raccolta differenziata)

Il marchio riportato sul prodotto o sulla sua documentazione indica che il prodotto non deve essere smaltito con altri rifiuti domestici al termine del ciclo di vita. Per evitare eventuali danni all'ambiente o alla salute causati dall'inopportuno smaltimento dei rifiuti, si invita l'utente a separare questo prodotto da altri tipi di rifiuti e di riciclarlo in maniera responsabile per favorire il riutilizzo sostenibile delle risorse materiali.

Gli utenti domestici sono invitati a contattare il rivenditore presso il quale è stato acquistato il prodotto o l'ufficio locale preposto per tutte le informazioni relative alla raccolta differenziata e al riciclaggio per questo tipo di prodotto.

Gli utenti aziendali sono invitati a contattare il proprio fornitore e verificare i termini e le condizioni del contratto di acquisto. Questo prodotto non deve essere smaltito unitamente ad altri rifiuti commerciali.

L'utente è invitato al rispetto delle norme per la corretta raccolta del rifiuto. Tali norme prevedono delle sanzioni amministrative pecuniarie.

Prima di installare e mettere in funzione il sistema è necessario leggere attentamente il presente manuale, grazie al quale l'operatore dorebbe essere in grado di installare e far funzionare correttamente il prodotto.

Il presente manuale può essere soggetto, senza alcun preavviso, a modifiche volte al miglioramento del sistema, alla standardizzazione o determinate da altri motivi tecnici.

Per ulteriori informazioni sul manuale aggiornato o per qualsiasi quesito relativo al contenuto del manuale, contattate il Vostro Rivenditore Autorizzate Samsung.

http://www.tlc.samsung.it

Introduzione

Obiettivi del manuale

Questo manuale descrive i campi da compilare, le impostazioni delle funzioni ed i monitoraggi che possono essere fatte per il sistema SMT-R2000 con l'interfaccia di tipo Web Based.

Queste informazioni sono destinate al personale che installa e amministra il sistema SMT-R2000, per la formazione di una rete IT aziendale composta da piccoli e medi sistemi.

Indicazioni convenzionali

Le tipologie di paragrafo speciali, presentate di seguito, sono utilizzati in questo manuale per richiamare l'attenzione su informazioni importanti.

ATTENZIONE

Indica una situazione potenzialmente pericolosa che, se non evitata, può portare a gravi danni o addirittura alla morte.

CAUTELA

Indica una situazione potenzialmente pericolosa che, se non evitata, può comportare danni di entità lieve o moderata. Può anche essere usata per mettere in guardia contro operazioni potenzialmente rischiose.

VERIFICA

Provvede a dare all'operatore dei riferimenti di verifica per potere operare correttamente.

NOTA

Provvede a dare all'operatore dei riferimenti di verifica per potere operare correttamente.

Prestazioni, Browser supportati e restrizioni

La pagina di amministrazione del sistema SMT-R2000 fornisce le informazioni su tutte le funzioni e gli argomenti disponibili per l'interfaccia d'utente.
La guida presente nella parte destra della pagina fornisce le informazioni relative alla pagina stessa. Quando le informazioni visualizzate sono correlate ad altri argomenti, sono disponibili dei collegamenti che portano alla pagina in questione

- Premere un link (testo sottolineato di colore blu) per accedere all'argomento indicato

Impostazioni raccomandate, avvisi e attenzione

 Le informazioni indicate dalla "freccia" (vedi tabella) indicano impostazioni raccomandate per le opzioni relative all'Access Point (AP).

- Le **Note** indicano descrizioni e commenti relativi all'argomento.
- Gli **Avvisi** forniscono informazioni importanti sulle proprietà delle impostazioni di un AP, la combinazione delle varie impostazioni e le procedure che possono avere impatti negativi per eventi, connessioni di rete e sicurezza.

Annotazioni sul formato

Questo manuale adotta le annotazioni sul formato come presentate di seguito:

Corsivo	Terminologie, nuove terminologie e titoli
`Screen Font`	Testo, URL, indirizzi IP, indirizzi MAC, file Unix, comandi, nomi delle directory e comandi digitati dall'utente
`Screen Font Corsivo`	Variabili
Grassetto	Titoli dei menu, nomi finestre e nomi dei tasti

Cronologia delle revisioni

Edizione	Data di pubblicazione	Note
00	08. 2007.	Prima versione

Informazioni sulla sicurezza

Per un corretto e sicuro funzionamento del prodotto, è necessario che l'operatore e/o utente ricevano le informazioni riportate di seguito e le leggano attentamente prima di procedere all'installazione e alla sua messa in funzione.

Tali informazioni possono essere contenute o meno in una casella rettangolare, che le separa dal testo principale, ma sempre preceduta da un'icona e/o un titolo in grassetto.

Simbologia utilizzata nel manuale

Cautela

Indica cautela generica

Restrizione

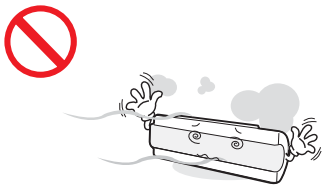
Indica il divieto di effettuare una determinata azione relativa ad un certo prodotto

Istruzione

Indica il comando di eseguire una determinata azione richiesta

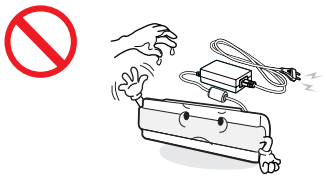
⚠ ATTENZIONE

Alimentazione



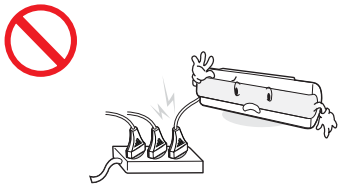
Non installare il prodotto in zone umide o polverose.

In tal modo si prevengono le possibilità di cortocircuito e incendio.



Non toccare con le mani bagnate i contatti elettrici.

In tal modo si prevengono le possibilità di cortocircuito e incendio..

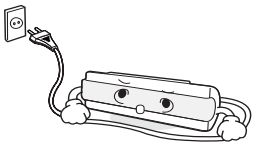


Inserire la presa di alimentazione della apparecchiatura in una presa di alimentazione dedicata.

Oltre il corretto funzionamento, questa misura aiuta a prevenire possibili incendi.

Inserire la spina del cavo di alimentazione correttamente nella presa di alimentazione.

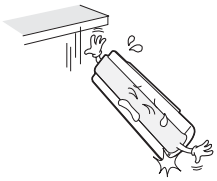
Se non è inserita correttamente si corre il pericolo di provocare cortocircuiti e incendi..



Sfilare il cavo di alimentazione dalla presa quando l'apparecchiatura non viene utilizzata per lungo periodo.

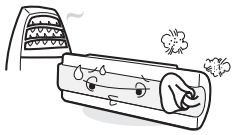
In tal modo si prevengono le possibilità di cortocircuito e incendio.

Installazione e immagazzinamento



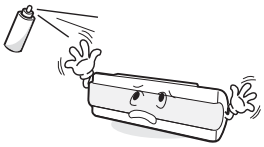
Attenzione a non fare cadere l'apparecchiatura.

In tal modo si prevengo i possibili danni causati da una sua caduta.



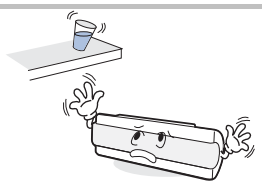
Non installare l'apparecchiatura vicino a fonti di calore o a delle fiamme libere (sigarette accese, stufe, ecc.)

Questa misura aiuta a prevenire la possibilità di cortocircuiti e incendi..



Non conservare e non utilizzare solventi o materiali infiammabili vicino alla apparecchiatura.

In tal modo si prevengono le possibilità di cortocircuito e incendio.

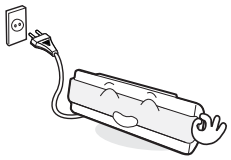


Evitare di posizionare vicino all'apparecchiatura oggetti contenenti acqua, ad esempio vasi, tazze, cosmetici o medicinali.

In tal modo si prevengono le possibilità di cortocircuito e incendio.

⚠ CAUTELA

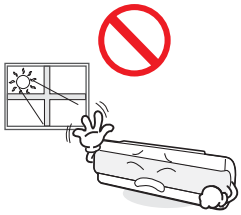
Alimentazione



L'apparecchiatura deve essere collegata all'alimentazione utilizzando l'adattatore fornito a corredo.

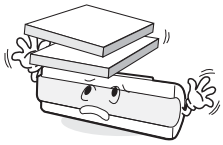
L'utilizzo di un altro adattatore può provocare gravi danni e causare incendi o pericolo di scosse elettriche.

Installazione e immagazzinamento



Non installare l'apparecchiatura in luoghi in cui possa essere esposto direttamente ai raggi solari.

Il prodotto potrebbe non funzionare correttamente poiché i componenti potrebbero deteriorarsi.

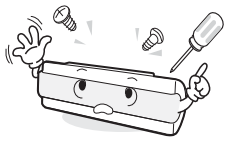


Non appoggiare oggetti pesanti sull'apparecchiatura.

In tal modo si prevengono danni al prodotto.

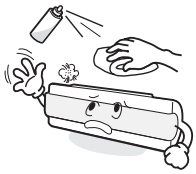
Non installare l'apparecchiatura su superfici instabili.

In tal modo si prevengono danni alla apparecchiatura causati da cadute.



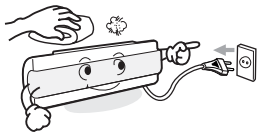
Per nessun motivo è permesso aprire, cercare di riparare o apportare modifiche all'apparecchiatura.

Per interventi o riparazioni contattare il proprio rivenditore o il Centro di assistenza Samsung



Per la pulizia non usare solventi chimici, benzene, alcool, aerosol, lubrificanti o detergenti.

L'uso di sostanze chimiche può far sbiadire, scolorire o danneggiarne i suoi componenti.



Per la sua pulizia utilizzare un panno morbido e asciutto.

Prima di iniziare l'operazione di pulizia sfilare la spina dalla presa di alimentazione.

In tal modo si prevengono danni al prodotto.

Contenuto della confezione e servizi

In funzione del fatto che la configurazione del dispositivo potrebbe variare in base al Paese nel quale e' distribuito alcune descrizioni fornite all'interno di questo manuale potrebbero non coincidere con le funzionalità effettivamente disponibili.

Le parti e gli accessori descritti all'interno di questo manuale potrebbero essere opzionali, anche se non espressamente indicato.

Pagina lasciata intenzionalmente bianca.

Indice

Pagina lasciata intenzionalmente bianca.

Capitolo 1. Impostazioni Base

1.1 Sommario delle impostazioni di base per gli AP

Parametro	Descrizione
Indirizzo IP	Mostra l'indirizzo IP di un AP, sia che venga assegnato dal DHCP oppure che venga assegnato con un valore fisso tramite il menu **Gestisci > Impostazioni Ethernet**. Questo valore non può essere modificato.
Indirizzo MAC	Mostra l'indirizzo MAC di un AP. Un indirizzo MAC è un indirizzo hardware univoco e prefissato per qualsiasi dispositivo che disponga di un'interfaccia alla rete. L'indirizzo MAC è assegnato dal produttore e non è modificabile. Questo indirizzo dovrà essere conosciuto dalle altre reti. Per verificare l'interfaccia Guest o Interna dell'AP, fare riferimento a **"Stato > Interfacce"**.
Versione Firmware	Mostra le informazioni relative al firmware attualmente installato in un AP. Ogni volta che una nuova versione del sistema SMT-R2000 viene rilasciata, il firmware viene aggiornato per abilitare l'AP ad utilizzare le nuove funzionalità. Per conoscere le modalità di aggiornamento del firmware, fare riferimento a "Aggiornamento del Firmware".
Codice Paese	Scegliere la nazionalità di utilizzo dell'AP. Quando viene modificato il codice del paese, fare attenzione alle impostazioni dei canali. NOTE Quando si modifica il codice del paese, dopo avere completato l'aggiornamento è necessario un riavvio del sistema.
Compensazione Tempo	Compensa l'orario (UTC) ricevuto via NTP (Network Time Protocol). Per esempio, dato che l'Italia ha una differenza di orario di 1 ora dall'UTC, va selezionato 1 (PR)
Posizione	Descrive dove è allocato l'AP.

1.2 Impostazioni della rete

Parametro	Descrizione
Password corrente	Inserire la password di amministrazione. Prima di cambiare la password, è necessario inserire la password corrente. Se la password è valida, viene visualizzato un segno di spunta ed i successivi elementi possono essere modificati.
Nuova password	Inserire una nuova password di amministrazione. Le lettere inserite sono mostrate come "*" in modo da non essere visualizzate ad alcuno. La password dell'amministratore dovrebbe essere una stringa alfabetica con lunghezza massima di 8 lettere. **Come primo passo per la sicurezza della LAN, si raccomanda di modificare la password di amministrazione.**
Conferma nuova password	Introdurre nuovamente la password di amministrazione per conferma.
802.11a, 802.11b/g (SSID)	Introdurre il nome della rete radio. Questo nome sarà applicato a tutti gli AP della rete. Ogni volta che vengono aggiunti degli AP, questi condivideranno questo SSID. L'SSID (*Service Set Identifier*) è una stringa alfanumerica con una lunghezza massima di 32 caratteri. NOTE Se viene reimpostato l'SSID mentre si sta accedendo all'AP tramite la rete radio del cliente, l'accesso all'AP può essere disconnesso. In questo caso si deve accedere nuovamente con un nuovo SSID dopo avere memorizzato i cambiamenti.

NOTE Il sistema SMT-R2000 non permette di effettuare cambiamenti multipli allo stesso tempo. Se si configura una rete con vari AP, o se vari amministratori accedono contemporaneamente tramite la pagina Web e cambiano le impostazioni, tutti gli AP nel gruppo entreranno nella modalità di "stand by" finché la sincronizzazione non viene completata. Comunque, questa azione non assicura l'aggiornamento delle variazioni effettuate dai vari utenti.

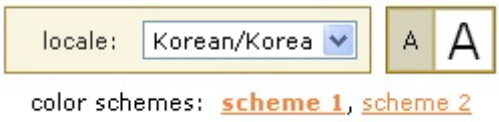
1.3 Aggiornamento delle impostazioni di base

Una volta completate le impostazioni, premere il tasto **Aggiorna** per attivare le variazioni.

1.4 Riepilogo dello stato delle impostazioni di base

Quando le impostazioni di base sono aggiornate, il riepilogo delle modifiche può essere visualizzato insieme alle informazioni relative al passo successivo. Le impostazioni di sicurezza per un AP non sono comprese tra le impostazioni iniziali.
Le impostazioni per la sicurezza sono un punto importante, fare riferimento a "Sicurezza".
Selezionando nuovamente **Impostazioni Di Base**, il riepilogo delle impostazioni di base viene ripresentato con i valori standard predefiniti.

1.5 Modifica del linguaggio della pagina Web e delle impostazioni



Il pannello posto nella parte superiore dell'impostazione dell'AP consente la personalizzazione di tutte le pagine Web. E' possibile modificare le dimensioni del carattere e selezionare il linguaggio tra i vari disponibili.

1.5.1 Impostazioni Internazionali

È possibile scegliere uno dei seguenti linguaggi:

- English/US
- Korean/Korea
- Danish/Dansk
- Dutch/Nederlands
- Finnish/Suomi
- German/Deutsch
- Italian/Italiano
- Portuguese/Portugues
- Russian/Russian
- Spanish/Espanol
- Swedish/Svenska

La scelta del linguaggio prevede la conversione del testo di tutte le pagine.

1.5.2 Dimensioni del carattere

Selezionare uno dei tasti che identifica il tipo di Font per cambiare le dimensioni del testo.

Configurazione	Descrizione
A	Caratteri Normali
A	Caratteri Grandi

1.5.3 Colore dello schermo

Per personalizzare il colore dello schermo, selezionare una delle seguenti tre opzioni:

Configurazione	Descrizione
Schema 1	Cambia i colori in Grigio e Blu.
Schema 2	Cambia i colori in Grigio e Bianco.

Pagina lasciata intenzionalmente bianca

Capitolo 2. Gestione degli Access Point e dei Cluster

Il sistema Samsung SMT-R2000 mostra le impostazioni di base per gruppi di AP (posizione, indirizzi IP, indirizzi MAC, stato e disponibilità) e fornisce un modo di navigare nella configurazione completa per specifici AP se fanno parte del gruppo.
AP che non fanno parte del gruppo o di tipo stand alone, non potranno essere visualizzati in questo elenco.
Per configurare un AP di tipo stand alone (singolo), è necessario scoprire (ad esempio tramite Kickstart) o conoscere l'indirizzo IP dell'AP e utilizzare tale indirizzo in un URL (http://IndirizzoIP).

Il sistema Samsung SMT-R2000 non è progettato per cambiamenti multipli o simultanei della configurazione. Se si dispone di una rete che include molteplici access point e più di un amministratore è connesso alla pagina Web di Amministrazione ed effettua cambiamenti alla configurazione, tutti gli access point nel gruppo (cluster) saranno sincronizzati, ma non è garantito che tutte le variazioni di configurazione verranno attivate.

2.1 Il concetto di Cluster

Una funzionalità importante del sistema Samsung SMT-R2000 è quella di avere l'abilità di formare dinamicamente un gruppo (chiamato cluster) con altri AP di riferimento Samsung su di una rete con la stessa subnet.
Gli access point possono partecipare in un cluster auto-organizzante, il quale vi facilita nella disposizione, l'amministrazione e la sicurezza della rete wireless.
Il cluster fornisce un unico punto d'accesso all'amministrazione e permette la visualizzazione della disposizione degli access point come una unica rete wireless integrata, piuttosto che come un insieme di dispositivi wireless.

2.1.1 Che cosa è un Cluster?

Un cluster è un gruppo di access point i quali sono coordinati come un singolo gruppo tramite l'amministrazione del sistema Samsung SMT-R2000.
Non è possibile creare cluster multipli in una rete singola wireless (SSID).
È supportato solo un cluster per una rete wireless.

2.1.2 Quanti Access Point sono supportati da un Cluster?

Fino a 12 access point possono essere supportati da un cluster allo stesso tempo. Se un nuovo AP viene aggiunto nella rete con un cluster che risulta già al limite della propria capacità, il nuovo AP verrà aggiunto nella modalità "Stand alone".
Si fa notare che quando un cluster è completo, AP extra verranno aggiunti in modalità stand alone a prescindere delle politiche di configurazione di nuovi AP impostate sul Cluster.

Per ulteriori informazioni fare riferimento a "Modalità Cluster", "Modalità Stand alone" e "Impostazioni delle politiche della configurazione per nuovi Access Point".

2.1.3 Quale tipo di AP possono essere inseriti in un Cluster?

Un singolo SMT-R2000 può formare un cluster con se stesso ("cluster a uno") oppure con altri AP dello stesso modello. Per essere membri dello stesso cluster, gli access point devono avere:

- La stessa configurazione di banda
- La stessa LAN

Avere un mix di AP nella rete non genera comunque problemi in un cluster del sistema Samsung SMT-R2000. Comunque, è utile capire il comportamento del cluster in funzione della configurazione:

- Gli access point dello stesso modello formano un cluster
- Gli access point di altre marche non faranno parte di un cluster. Questi AP dovrebbero essere amministrati con il relativo applicativo di gestione.

2.1.4 Impostazioni condivise nella configurazione di un cluster

La maggior parte delle configurazioni definite tramite le pagine Web di amministrazione del sistema Samsung SMT-R2000 saranno inviate ai membri del cluster come parte della configurazione del Cluster.

Impostazioni condivise nella configurazione di un Cluster

La configurazione di un cluster comprende:

- Il nome della rete (SSID)
- La password di amministrazione
- Le politiche di amministrazione
- Gli account utente e l'autenticazione
- Le impostazioni dell'interfaccia wireless
- Le impostazioni della visualizzazione iniziale per gli utenti "Guest"
- Le impostazione del Network Time Protocol (NTP)
- Le impostazioni radio
- Le impostazioni di sicurezza
- I parametri delle code QoS
- Gli indirizzi per il filtro MAC

Sono sincronizzati tramite il cluster solo le seguenti informazioni: "Modo", "Canale", "Soglia di Frammentazione", "Soglia RTS" e "Set Velocità", mentre non lo sono le seguenti: "Intervallo Beacon", "Periodo DTIM", "Max Postazioni" e "Potenza Trasmissione".


NOTE

Quando viene abilitata la gestione automatica dei canali, il canale radio non è sincronizzato tramite il cluster. Vedere "Stop/Start Assegnazione Automatica del Canale".

Impostazioni non condivise nella configurazione di un Cluster

Le poche eccezioni (impostazioni non condivise tra gli access point del cluster) sono le seguenti, la maggior parte delle quali hanno impostazioni per propria natura univoche:

- Indirizzo IP
- Indirizzo MAC
- Descrizione della posizione
- Impostazione del Bilanciamento Del Carico
- Bridge WDS
- Impostazioni Ethernet (rete cablata), comprese le abilitazioni o disabilitazioni dell'accesso
- Configurazione dell'interfaccia per gli utenti Guest

Le impostazioni che non sono condivise devono essere configurate individualmente nelle pagine di'amministrazione di ciascun access point. Per accedere alla pagina di amministrazione di un access point che è membro del cluster corrente, selezionare il link al suo indirizzo IP nella pagina **"Cluster > Punti di Accesso"** .

2.1.5 Modalità Cluster

Quando un access point è parte di un cluster, è considerato essere in modalità cluster. Potete definire se si vuole che i nuovi access point installati vengano compresi automaticamente nel cluster o meno tramite le politiche di configurazione definite nelle Impostazioni di Base. (Vedere "Politiche delle impostazioni di configurazione per un nuovo access point"). Potete impostare un access point da modalità cluster a modalità stand alone. (vedere "Rimozione di un Access Point dal Cluster")


NOTE

Quando un cluster è pieno (12 AP è il limite), ogni nuovo AP sarà aggiunto in modalità stand alone senza tener conto delle politiche di configurazione. Vedere "Quanti Access Point sono supportati da un Cluster?".

2.1.6 Modalità Stand alone

Il sistema Samsung SMT-R2000 può essere configurato in modalità stand alone. In questa modalità, l'access point non è un membro del cluster e non condivide la configurazione del cluster, ma richiede una configurazione manuale non condivisa con gli altri access point. (Vedere "Politiche delle impostazioni di configurazione per un nuovo access point" e "Rimozione di un Access Point dal Cluster").

Gli access point di tipo stand alone non sono visualizzati nel menu **"Cluster > Punti di Accesso"** dell'interfaccia d'utente per l'amministrazione del cluster. Per poter configurare e amministrare direttamente un access point stand alone è necessario conoscerne l'indirizzo IP (Vedere "Navigazione per un AP utilizzando il suo indirizzo IP nell'URL").

La tabella **"Cluster > Punti di accesso"** per gli AP stand alone, indica solamente che l'attuale modalità è di tipo "stand alone" e fornisce un tasto per aggiungere l'access point ad un cluster (gruppo). Se tenta di selezionare una delle tabelle del menu**"Cluster"** di un access point in modalità stand alone, si verrà indirizzati alla pagina **"Cluster > Punti di accesso"**, in quanto le impostazioni per il cluster non sono applicabili ad un AP stand alone.

Un access point in modalità stand alone può sempre essere reimpostato in modalità cluster (Vedere "Aggiungere un Access Point ad un Cluster").

Per facilitarne l'utilizzo, il cluster è progettato per permettere a nuovi dispositivi di partecipare ad esso senza autenticazioni restrittive. Comunque, le comunicazioni di tutti i dati tra gli access point in un cluster sono protette da eventuali intrusioni utilizzando SSL (Secure Sockets Layer). Si assume che la rete privata cablata, alla quale sono connessi i dispositivi, sia sicura. Sia il file della configurazione del cluster che il database sono trasmessi tra gli access point utilizzando SSL.

2.1.7 Sincronizzazione automatica della Configurazione del Cluster

Se si stanno effettuando modifiche alla configurazione dell'AP che richiedono relativamente molto tempo per il processo dei dati (come l'aggiunta di molti nuovi utenti), dopo avere premuto il tasto **"Aggiorna"** nelle pagine di amministrazione, è possibile vedere visualizzata sul video la barra che indica il progresso delle attività.
La barra progressiva indica che il sistema è occupato nell'esecuzione del sincronismo automatico per l'aggiornamento della configurazione di tutti gli AP nel cluster. Le pagine Web di amministrazione non sono editabili durante l'autosincronismo.

Notare che l'auto sincronizzazione è sempre attiva quando si effettua un aggiornamento della configurazione del cluster, ma il tempo di processo è generalmente trascurabile.
La barra relativa al progresso dell'auto sincronizzazione è visualizzata solamente in caso di un tempo di attesa elevato.

2.2 Conoscere le impostazioni dell'Access Point

La tabella **"Punti di Accesso"** fornisce le informazioni relative a tutti gli access point nel cluster. Da questa tabella, è possibile visualizzare la descrizione della posizione, gli indirizzi IP, abilitare/attivare o disabilitare/disattivare gli access point del cluster e rimuovere gli access point dal cluster.
E' possibile inoltre modificare la descrizione della posizione degli access point.
Il link dell'indirizzo dell'AP fornisce un modo per navigare alle impostazioni di configurazione e dati specifici di ciascun access point.
Gli access point stand alone (i quali non sono membri di un cluster) non sono visualizzati in questa pagina. La seguente tabella descrive le impostazioni degli access point e le informazioni visualizzate nel dettaglio.

Campo	Descrizione
Posizione	Descrive dove è fisicamente situato l'access point.
Indirizzo MAC	E' l'indirizzo MAC (Media Access Control) dell'access point. Un indirizzo MAC è un indirizzo hardware univoco e prefissato per qualsiasi dispositivo che disponga di un'interfaccia alla rete. L'indirizzo MAC è assegnato dal produttore e non è modificabile. Viene visualizzato per scopi informativi come identificatore univoco per un access point. L'indirizzo mostrato qui è l'indirizzo MAC per l'interfaccia BR0. Questo è l'indirizzo tramite il quale l'AP è conosciuto nelle altre reti. Per visualizzare gli indirizzi MAC degli utenti e delle interfacce interne nell'AP, vedere la tabella **"Stato > Interfacce"**.
Indirizzo IP	Specifica l'indirizzo IP per l'access point. Ogni indirizzo IP è un link nella pagina Web di amministrazione per quell'access point. E' possibile utilizzare i link per navigare nella pagina Web di amministrazione per uno specifico access point. Questo è utile per la visualizzazione dei dati per uno specifico access point e per modificare in sicurezza un membro di un cluster, per configurare in anticipo delle impostazioni per un particolare access point o commutare un access point da stand alone in un membro di cluster.

2.3 Modifiche della descrizione della localizzazione

Per modificare la descrizione della localizzazione:

1. Accedere alla tabella **"Cluster > Punti di Accesso"**
2. Aggiornare la descrizione della posizione nella sezione **"Opzioni di clustering …"**
3. Premere il tasto **"Aggiorna"** per confermare le modifiche.

2.4 Rimozione di un Access Point da un Cluster

Per rimuovere un access point dal cluster, seguire le seguenti istruzioni:

1. Selezionare la casella a lato dell'access point interessato
2. Premere il tasto **"Rimuovi"** per rimuovere l'access point dal cluster.

Il cambio verrà mostrato nello Stato di questo access point, che sarà ora indicato come *stand alone* invece che *cluster*.


NOTE

In alcune situazioni è possibile per un cluster andare fuori sincronismo. Se dopo la rimozione di un access point dal cluster, la lista degli AP indica ancora l'AP cancellato o mostra una visualizzazione incompleta, fare riferimento alle indicazioni in "Cluster Recovery" nell'Appendice B: "Ricerca guasti" della Guida per amministratore.

2.5 Aggiungere un Access Point in un cluster

Per aggiungere un access point attualmente nella modalità stand alone in un cluster, seguire le seguenti istruzioni:

1. Entrare nella pagina Web di amministrazione per l'access point stand alone (vedere Navigazione per un AP utilizzando il suo indirizzo IP nell'URL). Verranno visualizzate le pagine Web di amministrazione per l'access point.
2. Selezionare la tabella **"Cluster > Punti di accesso"** nella pagina di amministrazione dell'access point stand alone. La tabella indica che l'attuale modalità è stand alone e fornisce un tasto per aggiungere l'access point al cluster (gruppo).


NOTE

Se si tenta di selezionare uno dei menu **"Cluster"** nella pagina di amministrazione di un access point in modalità stand alone, si verrà indirizzati alla pagina **"Punti di accesso"**, in quanto le impostazioni per il cluster non sono applicabili ad un AP stand alone.

3 Premere il tasto **"Avvia Clustering"**.

L'access point è ora un membro del cluster. L'icona di stato del cluster nella tabella **"Cluster > Punti di Accesso"** indica ora "in cluster" invece che "non in cluster".


NOTE

In alcune situazioni è possibile per un cluster andare fuori sincronismo. Se dopo la rimozione di un access point dal cluster, la lista degli AP indica ancora l'AP cancellato o mostra una visualizzazione incompleta, fare riferimento alle indicazioni in "Cluster Recovery" nell'Appendice B: "Ricerca guasti" della Guida per amministratore.

2.6 Configurazione di uno specifico AP e gestione degli AP stand alone

In generale, il sistema Samsung SMT-R2000 è progettato per la gestione centralizzata degli access point appartenenti ad un gruppo cluster. In un cluster, tutti gli access point hanno la stessa configurazione. In questo caso, non è importante a quale access point si è attualmente connessi per l'amministrazione.

Ci possono essere comunque situazioni nelle quali si voglia visualizzare o gestire informazioni per uno specifico access point. Per esempio, si potrebbero voler verificare le informazioni sullo stato degli eventi per un access point e l'associazione dei client.

Oppure si potrebbe voler configurare e gestire le prestazioni di un access point che sta operando in modalità stand alone. In questo casi potete navigare tramite le pagine Web per l'amministrazione per singoli access point selezionando il link relativo all'indirizzo IP nella tabella **"Cluster > Punti di Accesso"**.

Tutti gli access point del cluster sono mostrati nella pagina **"Cluster > Punti di Accesso"**. Per accedere agli access point nel cluster è sufficiente selezionare l'indirizzo IP di uno specifico membro del cluster mostrato nella lista.

2.6.1 Accesso ad un AP utilizzando il suo indirizzo IP nell'URL

E' possibile anche attivare un collegamento alle pagine Web per l'amministrazione di uno specifico access point inserendo l'indirizzo IP dell'access point come URL direttamente nell'indirizzo Web del browser nel seguente formato:

http://*IindirizzoIPAccessPoint*

dove *IndirizzoIPAccessPoint* è l'indirizzo del particolare access point che si desidera monitorare o configurare.

Per un access point stand alone, questo è l'unico modo per accedere alle informazioni della configurazione.

Se non si conosce l'indirizzo IP di un access point stand alone, utilizzare un software quale Kickstart per individuarlo nella rete e tentare di identificarlo comparando i dati di Kickstart con i dati presenti nella tabella **"Cluster > Punti di Accesso"**.

Gli AP che Kickstart scopre e che non sono mostrati in questa tabella, sono probabilmente AP stand alone.

Pagina lasciata intenzionalmente bianca.

Capitolo 3. Impostazioni Ethernet

In questa pagina è possibile configurare la LAN (Local Area Network) Ethernet.


NOTE

In questa pagina è possibile impostare due Ethernet cablate, le reti virtuali (VLAN), NAT e server DHCP. Quando si configura una rete virtuale, il terminale dati che configura la rete deve supportare la VLAN.

3.1 Impostazioni del nome DNS

Parametro	Descrizione
Nome DNS	Inserire nella casella di testo il nome DNS dell"access point. Questo è un host name che può essere fornito dal vostro ISP, dall'amministratore della rete o da voi stessi. Le regole per il nome del sistema sono: • Il nome può essere lungo fino a 20 caratteri • Sono permessi solo lettere, numeri e trattini (dash) • Il nome deve iniziare con una lettera e terminare con una lettera o un numero

3.2 Utilizzare l'accesso per la rete Guest

Il sistema SMT-R2000 prevede la possibilità di configurare una rete LAN e una rete Guest..

3.2.1 Impostazione della rete LAN e Guest

La LAN (Local Area Network) è una rete di comunicazione utilizzata in un area limitata, come un piano di un edificio. Una LAN collega vari dispositivi di rete come un computer e stampanti.
Ethernet è la più diffusa tra le tecnologie che implementano la LAN.
Wi-Fi (IEEE) è un altro tipo di tecnologia LAN.
SMT-R2000 permette di configurare due differenti LAN nello stesso access point: una per una rete *interna* sicura ed un'altra per una rete pubblica *Guest (ospite)* senza sicurezza e poche o nessuna risorsa per accessi interni. Per configurare queste reti, avete necessità di prevedere le impostazioni sia della rete Ethernet (Wired) che Wireless.
Le informazioni su come configurare le impostazioni di Ethernet (Wired) sono presenti nella sezione seguente. (Per le informazioni su come configurare una rete Wireless, vedere "Impostazioni delle interfacce Wireless", Per una visione generale su come impostare l'interfaccia Guest, vedere "Impostazione dell'accesso Guest") -

3.2.2 Utilizzare l'accesso Guest

Il sistema SMT-R2000 come impostazioni di base ha le opzioni per l'accesso Guest disabilitate. Se si desidera fornire l'accesso guest al vostro AP, abilitare l'accesso Guest tramite la tabella **"Gestisci > Impostazioni Ethernet"**.

Parametro	Descrizione
Accesso Guest	Per default il sistema SMT-R2000 ha il servizio disabilitato. Per permettere l'accesso Guest, selezionare **Attivato** Per disabilitare l'accesso Guest, selezionare **Disattivato**

3.2.3 Specificare una Rete Guest Fisica o Virtuale

Se si abilita l'accesso guest, selezionare il metodo per la gestione nell'AP della "rete interna" e "rete Guest". Il primo metodo è un metodo fisico (1) che vede le due reti direttamente connesse via cavo alle due differenti porte LAN dell'AP.
Il secondo metodo è un metodo virtuale (2) che connette la porta WAN dell'AP alla porta VLAN dello switch e definisce due differenti LAN virtuali sullo switch. (Per maggiori informazioni, fare riferimento a "Impostare l'accesso Guest").
Scegliere il metodo fisico o virtuale per separare le LAN Interna e Guest come descritto di seguito.

Parametro	Descrizione
Accesso Guest	- Selezionare **Attivato** per autorizzare l'accesso Guest (se si sceglie questa opzione, nella prossima impostazione "Per Accesso Guest" bisogna indicare se utilizzare la separazione delle reti fisica o tramite VLAN e quindi fornire dettagli sulla VLAN o impostazioni della rete Wired per la rete Guest nel resto della pagina). - Selezionare **Disattivato** per disabilitare l'accesso Guest. - Se si connette questo access point a due separate reti per una soluzione di "sicurezza fisica", allora scegliere **"Porta LAN"** dal menù a discesa per impostare la vostra rete Guest sulla seconda porta Ethernet. - Se l'access point sta utilizzando una sola connessione fisica per la vostra LAN interna (non è in uso la porta LAN extra), scegliere **"Porta WAN VLAN"** dal menù a discesa. Questo abiliterà le impostazioni "VLAN", dove si deve fornire un VLAN ID. Vedere anche "Configurazione delle impostazioni dell'interfaccia Ethernet Guest".  NOTE Se le interfacce guest ed interna vengono riavviate tramite VLAN, la connessione con l'AP può fallire. Lo switch e il server DHCP devono supportare i servizi VLAN delle specifiche IEEE 802.1Q. Dopo l'attivazione della VLAN nella pagina delle impostazioni Ethernet dello switch connesso alla porta VLAN. Accedere alla pagina Web di amministrazione tramite un nuovo indirizzo IP.

3.3 Abilitare o disabilitare la rete wireless virtuale sull'AP

Se si desidera configurare la rete interna come VLAN (a prescindere dalla configurazione della rete Guest), dovete abilitare la rete Virtuale Wireless nell'AP.
Potete abilitare questa opzione se volete configurare una rete addizionale di una VLAN nella tabella **"Gestisci > VWN"** come descritto in "Configurazione della rete Virtuale Wireless".

Parametro	Descrizione
Virtual Wireless Networks	- Selezionare **Attivato** per abilitare la VLAN per la rete interna e per le reti addizionali. (Se si sceglie questa opzione, potete avviare una VLAN sulla rete interna a prescindere dalla configurazione dell'accesso Guest e potete impostare reti VLAN addizionali utilizzando la tabella **"Gestisci > VWN"** come descritto in "Configurazione della rete Virtuale Wireless"). - Selezionare **Disattivato** per disabilitare la VLAN per la rete interna e qualsiasi rete virtuale addizionale sull'access point. Quando l'utente disabilita le reti virtuali wireless (VWN) è comunque possibile aggiungere VWN nel menù **"Gestisci > VWN"**. In questo caso, l'SMT-R2000 non utilizza VLAN ma aggiunge VWN nella rete interna.

3.4 Configurazione della LAN o delle impostazioni dell'Interfaccia Interna Ethernet

Per configurare le Impostazioni Ethernet (cablata) per la LAN interna, compilare i campi come descritto di seguito:

Parametro	Descrizione
Indirizzo MAC	Indirizzo MAC dell''interfaccia interna della porta Ethernet dell'AP. Questo dato non può essere modificato ma è solo in visualizzazione.
ID VLAN	Se si sceglie di configurare le reti interna e Guest come "VLAN", il campo sarà abilitato alla modifica. Indicare un numero compreso tra 1 e 4094 per la VLAN interna. L'AP invierà una richiesta al DHCP includendo il VLAN tag. Lo switch e il server DHCP devono supportare il protocollo VLAN IEEE 802.1Q. L'AP deve essere connesso al server DHCP.
Tipo di Connessione	E' possibile selezione **"DHCP"** o **"IP Statico"**. - **DHCP** (Dynamic Host Configuration Protocol) è il protocollo che descrive come il server centrale fornisce le informazioni sulle impostazioni di rete al dispositivo. Il server DHCP assegna un indirizzo IP al sistema Client e fornisce le informazioni sul server DNS, sull'indirizzo IP del gateway e sulla subnet mask. - **IP Statico** indica che tutta le impostazioni di rete sono fornite manualmente. E' necessario fornire all'AP Samsung, un indirizzo IP e la relativa subnet mask, l'indirizzo IP del gateway di default e l'indirizzo IP di almeno un server DNS. -

(continua)

Parametro	Descrizione
Tipo di Connessione	Se si seleziona "DHCP" l'AP Samsung acquisirà il proprio indirizzo IP, subnet mask e le informazioni del DNS e gateway dal server DHCP. In caso contrario, se si seleziona "Static IP", compilare i campi descritti in "Impostazioni dell'indirizzo Statico". NOTE Se nella rete interna il server DHCP non esiste, il tipo di connessione per l'AP dovrebbe essere cambiata da DHCP in Static IP. Quindi, un nuovo indirizzo IP statico può essere assegnato all'AP o può essere utilizzato l'indirizzo IP di default. Se si prevede di aggiungere ulteriori AP Samsung, è consigliabile assegnare un nuovo indirizzo, in modo da prevenire una possibile collisione di due indirizzi tra di due AP. Se si ha la necessità di recuperare l'indirizzo IP statico di default, è possibile farlo reimpostando l'AP con i dati di fabbrica come descritto in "Reimpostare la configurazione di default". L'indirizzo IP di default dell'AP è **192.168.111.10**.
Indirizzo IP Statico	Se si sceglie "IP Statico" come tipo di connessione, questi campi saranno abilitati alla scrittura. Introdurre l'indirizzo IP statico nella casella di testo.
Subnet Mask	Introdurre la **Subnet Mask** nella casella di testo. Questa informazione deve essere data dal vostro ISP o dall'amministratore di rete.
Gateway predefinito	Introdurre il Default Gateway nella casella di testo.
Server nomi DNS	Il *DNS (Domain Name Service* (DNS) converte il nome di Dominio (es. www.Samsung.com) di una risorsa di rete in un indirizzo IP (es. 66.93.138.219). Il server DNS è chiamato *Name Server*. Ci sono di solito due Name Server, un server Primario ed un server Secondario. E' possibile scegliere la modalità **Dinamico** o **Manuale**. - Se si sceglie la modalità **Dinamico**, l'indirizzo IP del server DNS sarà assegnato automaticamente via DHCP. (Questa opzione è disponibile solamente se si specifica DHCP come tipo di connessione). - Se si sceglie la modalità **Manuale**, si deve assegnare l'indirizzo IP manualmente.

3.5 Configurazione dell'interfaccia Ethernet Guest (rete cablata)

Per configurare le impostazioni Ethernet (rete cablata) per l'interfaccia "Guest", compilare i seguenti campi:

Parametro	Descrizione
Indirizzo MAC	Indirizzo MAC dell'interfaccia guest della porta Ethernet dell'AP. Questo dato non può essere modificato ma è solo in visualizzazione.
ID VLAN	Se si abilita l'impostazione "VLAN" per l'impostazione delle reti interna e Guest, il campo sarà abilitato alla scrittura. Indicare un numero compreso tra 1 e 4094 per la VLAN interna.

3.6 Aggiornare le impostazioni

Per aggiornare le impostazioni Ethernet:

1. Accedere a **"Gestisci > Impostazioni Ethernet"**
2. Configurare le impostazioni Ethernet come richiesto
3. Premere il tasto **"Aggiorna"** per attivare le modifiche.

Pagina lasciata intenzionalmente
Bianca.

Capitolo 4. Impostazioni Wireless

Le impostazioni wireless descrivono gli aspetti della rete locale (LAN) relativi specificatamente ai dispositivi radio nell'access point ("Modo 802.11" e "Canale") e all'interfaccia di rete dell'access point (indirizzo MAC dell'access point e nome della rete wireless, conosciuto anche come SSID).

4.1 Supporto 802.11h

Parametro	Descrizione
Supporto 802.11h	L'interfaccia di amministrazione mostrerà se il supporto a IEEE 802.1h (Regulatory Domain Control) è attivo nell'AP. L' IEEE 802.11h non può essere disabilitato dall'utente. I seguenti dettagli hanno il solo scopo di fornire alcune informazioni. IEEE 802.11h è uno standard che fornisce due servizi richiesti per soddisfare alcune regole nazionali relative alla banda di 5 GHz. Questi due servizi sono il TPC (Transmit Power Control) e il DFS (Dynamic Frequency Selection). - TPC richiede che le Reti Radio Locali (RLAN) operanti nella banda di 5 GHz usino il "Transmitter power control". Questo è strettamente legato alla regolazione della potenza massima di trasmissione in uscita e dell'attenuazione richiesta per ciascun canale autorizzato, al fine di ridurre le interferenze con i servizi satellitari. - DFS richiede che le RLAN operanti nella banda di 5 GHz implementino un meccanismo che eviti l'interferenza con i sistemi radar ed assicuri un utilizzo uniforme dei canali disponibile. NOTE 1) 802.11h è automaticamente abilitato nelle nazioni dove è richiesto. Questo standard è necessario per quei paesi che utilizzano le normative ETSI. 802.11h viene abilitato quando vengono selezionate alcune nazioni, come la Corea (DFS) e l'Inghilterra. In questo caso, viene visualizzato il messaggio "Supporto IEEE802.11h Disponibile". 2) SMT-R2000 è un dispositivo wireless che imposta i canali dinamicamente secondo le specifiche della tecnologia standard di 5 GHz Dynamic Frequency Selection (DFS). SMT-R2000 può rilevare i segnale radar, così, quando i segnali radar vengono rilevati nelle comunicazioni tra SMT-R2000, dispositivi slave ed altri Access Point (AP), la comunicazione viene stabilita secondo i comandi di spostamento del canale.

4.2 Impostare la rete wireless

L'interfaccia radio permette di impostare il canale radio e la modalità 802.11h, come descritto di seguito:

Parametro	Descrizione
Indirizzo MAC	Indica l'indirizzo MAC (Media Access Control) relativo all'interfaccia. Un indirizzo MAC è un indirizzo hardware univoco e prefissato per qualsiasi dispositivo che disponga di un'interfaccia alla rete. L'indirizzo MAC è assegnato dal produttore e non è modificabile. Viene visualizzato a scopo informativo come identificatore univoco per ciascun access point.
Modo	Definisce lo standard del Physical Layer (PHY) usato per le interfacce radio. SMT-R2000 è un access point a doppia banda, con due interfacce radio. E' possibile selezionare una delle seguenti modalità, una per ogni interfaccia radio: • IEEE 802.11b • IEEE 802.11g • IEEE 802.11a
Canale	Selezionare il **Canale**. La scelta possibile ed il default è determinato dalla **Modalità (Mode)** dell'interfaccia radio. Il Canale definisce la porzione dello spettro delle trasmissioni radio che l'interfaccia utilizza per trasmettere e ricevere. Ogni modalità offre un certo numero di canali, dipendenti da come lo spettro è stato regolamentato dalle autorità nazionali, quali la Federal Communications Commission (FCC) o l'International Telecommunication Union (ITU-R). Quando si imposta con **"Auto"**, l'AP seleziona automaticamente il canale più appropriato. Se in modalità IEEE802.11a è supportato il DFS (quando viene visualizzato il messaggio "Supporto IEEE 802.11h disponibile"), il canale viene sempre impostato su AUTO.

4.3 Impostare la rete wireless "Interna"

Le "Impostazioni Interfaccia Interna" visualizzano l'indirizzo MAC (di sola lettura) e l'SSID per le rete interna Wireless LAN (WLAN), come descritto di seguito.

Parametro	Descrizione
Indirizzo MAC	Indica l'indirizzo MAC per l'interfaccia interna per questo access point. Questo campo è di sola lettura e non può essere modificato. Sebbene l'access point sia fisicamente un dispositivo singolo, può essere rappresentato nella rete come due o più nodi con un unico indirizzo MAC. Questo è consentito grazie all'utilizzo di Basic Service Set Identifier (BSSID) multipli su di un singolo access point. L'indirizzo MAC indicato in "Impostazioni Interfaccia Interna" è il BSSID per l'interfaccia "Interna" dell'access point. Sono mostrati due indirizzi MAC, uno per ciascuna radio sull'interfaccia interna.
SSID	Inserire l'**SSID** per la WLAN interna. L'SSID *(Service Set Identifier)* è una stringa alfanumerica fino a 32 caratteri che identifica in modo univoco una rete WLAN. Viene anche chiamato "*Network Name"*. Non ci sono restrizioni relative ai tipi di caratteri che possono esser utilizzati nell'SSID.

4.4 Impostare la rete wireless LAN "Guest"

"Impostazioni Guest" visualizza l'indirizzo MAC (di sola lettura) e l'SSID per la rete Guest, come descritto di seguito. Configurando un access point con due differenti nomi di rete (SSID), è possibile utilizzare le funzioni offerte dall'interfaccia Guest sull'AP Samsung. Per ulteriori informazioni, vedere la configurazione dell'accesso Guest.

Parametro	Descrizione
Indirizzo MAC	Indica l'indirizzo MAC per l'interfaccia Guest dell'access point. Questo è un campo di sola lettura e non può esser modificato. Sebbene questo access point è fisicamente un dispositivo singolo, può essere rappresentato sulla rete come due o più nodi ognuno con un unico indirizzo MAC. Questo è possibile utilizzando il *Basic Service Set Identifier* (BSSID) per un access point singolo. L'indirizzo MAC indicato in "Impostazioni Guest" è il BSSID per l'interfaccia "Guest" dell'access point. Sono mostrati due indirizzi MAC, uno per ciascuna radio sull'interfaccia interna.
SSID	Introdurre l'**SSID** relativo alla rete Guest. Il *Service Set Identifier* (SSID) è una stringa alfanumerica fino a 32 caratteri che identifica in modo univoco una rete WLAN. Viene anche chiamato "*Network Name"*. Non ci sono restrizioni relativi ai tipi di caratteri che possono esser utilizzati nell'SSID. Per la rete Guest, fornire un SSID differente dall'SSID interno e facilmente identificabile come rete "Guest".

4.5 Aggiornamento delle impostazioni

Per aggiornare le impostazioni Wireless:

1. Accedere a **"Gestisci > Impostazioni Wireless"**
2. Impostare la Configurazione desiderata
3. Premere il tasto **Aggiorna** per attivare le modifiche.

Capitolo 5. Impostazioni di sicurezza

Le impostazioni relative alla sicurezza delle due modalità radio sono gestite in modo indipendente. Nelle tabelle **"Impostazione di protezione 11a"** e **"Impostazione di protezione 11b/g"** devono essere configurate le rispettive impostazioni di sicurezza.

5.1 Blocco della rete tramite l' "Isolamento postazione"

Se l'opzione "Isolamento Postazione" è attivata, l'AP blocca le comunicazioni tra i client sulla relativa banda radio. Viene consentita unicamente la comunicazione tra i dispositivi client e la rete cablata.

Questo blocco del traffico, viene anche applicato ai client connessi alla rete tramite la connessione WDS. Se è attivato l' "Isolamento postazione", un client non può comunicare con gli altri client. Per le informazioni su WDS, fare riferimento a "Impostazioni del WDS".

Le seguenti informazioni relative alle impostazioni descrivono come configurare le impostazioni di sicurezza dell'AP. Per poter scambiare dati con l'AP, il client deve impostare le stesse modalità di sicurezza e la stessa chiave crittografica dell'AP.


NOTE

Le modalità di sicurezza ulteriori alla modalità "Testo normale" sono applicabili solamente per la rete interna. Sulla rete "Guest", è utilizzabile solamente la modalità "Testo normale" (per informazioni sulla rete Guest, fare riferimento a "Utilizzare l'accesso per la rete Guest".

5.2 Visualizzazione SSID, Isolamento postazione, Modalità di Sicurezza

Per impostare la sicurezza dell'AP, selezionare **"Protezione"**, ed impostare i campi decritti di seguito (come spiegato di seguito, la visualizzazione dell'SSID e l' "Isolamento postazione" possono essere attivati/disattivati come misure di difesa misure preliminari).

Parametro	Descrizione
Trasmissione SSID	Per attivare la **"Trasmissione SSID"**, selezionare la relativa casella. Nella configurazione di default, l'AP include il *Service Set Identifier* (SSID) nel frame "Beacon" per trasmetterlo. E' possibile prevenire l'identificazione automatica dell' AP evitando di trasmettere l'SSID. In questo caso, il nome della rete dell'AP (SSID) non viene visualizzato nella lista delle reti rilevate dal client. Per accedere all'AP il client deve conoscere a priori l'SSID corretto.

(Continua)

Parametro	Descrizione
Isolamento postazione	Selezionare la casella se si desidera attivare l' "Isolamento postazione". - Se l' "Isolamento postazione" **non è selezionato**, ciascun client può comunicare con gli altri client attraverso l' AP. - Se l' "Isolamento postazione" **è selezionato**, l'AP blocca le comunicazioni radio tra i client. Viene consentita unicamente la comunicazione tra i dispositivi client e la rete cablata. Questo blocco del traffico, viene anche applicato ai client connessi alla rete tramite la connessione WDS. Se è attivato l' "Isolamento postazione", un client non può comunicare con gli altri client. Per le informazioni su WDS, fare riferimento a "Impostazioni del WDS"..
Modo	Selezionare una delle seguenti **modalità di sicurezza**: - Nessuna (Testo normale) - WEP Statico - IEEE 802.1x - WPA Personale - WPA Aziendale Per la rete "Guest", può essere impostata solo la modalità "Nessuna (Testo normale)". (Per informazioni sulla rete Guest, fare riferimento a "Utilizzare l'accesso per la rete Guest").

5.2.1 Nessuna (Testo normale)

La modalità *Nessuna* (o Testo normale) significa che il client non effettua la crittografia dei dati quando comunica con l' SMT-R2000.
Se viene selezionato Nessuna (Testo normale), non sono necessarie altre impostazioni di parametri di sicurezza.

Rete Guest

Per la rete Guest è possibile impostare unicamente la modalità "Nessuna (Testo normale)".
Questa impostazione consente l'accesso dei client guest senza vincoli di sicurezza.
L'unico metodo di protezione della rete Guest è bloccare la trasmissione dell'SSID (Network name).
Per informazioni sulla rete Guest, fare riferimento a "Utilizzare l'accesso per la rete Guest".

5.2.2 WEP Statico

WEP (Wired Equivalent Privacy) è un protocollo di crittografia dei dati per le reti 802.11. Tutti client e gli AP dovrebbero avere la condivisione dei codici a 64 bit (40 bit di codice segreto più 24 bit del vettore di inizializzazione (IV)) per la crittografia dei dati.

Le chiavi WEP a 64 e a 128 bit non possono essere uste contemporaneamente.

Se si seleziona "WEP Statico" come modalità di sicurezza, devono essere configurati i seguenti parametri:

Parametro	Descrizione
Indice chiave di trasferimento	Selezionare l'indice della chiave nel menù a discesa (1-4). L'indice di default è 1. la selezione indica quale codice utilizzare per la crittografia nella trasmissione dei dati.
Lunghezza chiave	Definire la lunghezza del codice WEP selezionando uno dei seguenti: - 64 bit - 128 bit
Tipo di chiave	Definire modalità di digitazione del codice WEP selezionando uno dei seguenti: - ASCII - Hex
Chiavi WEP	Possono essere definiti fino a 4 codici WEP. Inserire in ogni casella di testo la stringa da utilizzare come codice WEP. Nel caso si selezioni "ASCII", l'inserimento può essere una combinazione di caratteri ASCII. Nel caso sia selezionato "HEX", l'inserimento può essere una combinazione di caratteri esadecimali, (una combinazione di 0-9 e a-f). Introdurre tanti caratteri quanti definiti nel parametro "Caratteri obbligatori". Il carattere inserito in questo parametro è il codice RC4WEP condiviso dal client e dall'AP. Il client dovrebbe impostare lo stesso codice WEP nello stesso indice come definito nell'AP. (Fare riferimento a "Regole d'impostazione del WEP statico") **"Caratteri obbligatori"**: indica il numero di caratteri necessari per il codice WEP. I parametri necessari sono automaticamente aggiornati in funzione della lunghezza dei codici e del tipo.
Autenticazione	L'algoritmo di autenticazione è la procedura che, nel caso si utilizzi la modalità di sicurezza "WEP Statico", verifica se il client è autorizzato ad accedere all'AP. Definire l'algoritmo di autenticazione usato selezionando uno dei seguenti: - Open System - Shared Key NOTE: E' necessario selezionare la voce "Sistema aperto" oppure "Chiave condivisa". Il metodo di autenticazione a **Sistema aperto** permette l'accesso a tutti i client. In questo caso, il fatto che il client utilizzi o meno il corretto WEP non è importante. Questo algoritmo di autenticazione è utilizzato nelle modalità di sicurezza "Nessuna (Testo normale) IEEE 802.1x e WPA. Se l'algoritmo di autenticazione è impostato come "Open System", tutti i client possono accedere all'AP.
Autenticazione	Va notato che il fatto che una stazione client sia autorizzata all'associazione, non implica la possibilità di scambiare traffico con l'access point. Una stazione, per avere la possibilità di cifrare/decrittare i dati scambiati con un access point, deve avere il codice WEP corretto. L'autenticazione a **"Chiave condivisa"** richiede che la stazione client, per avere la possibilità di associarsi all'access point, abbia il codice WEP corretto. Quando l'algoritmo di autenticazione è impostato come **"Chiave condivisa"**, una stazione con un codice WEP errato non sarà autorizzata ad associarsi con l'access point.

Regole d'impostazione del WEP Statico

- Tutti i client dovrebbero avere impostato la modalità di sicurezza Wireless LAN (WLAN) come WEP. In aggiunta, i client dovrebbero disporre di uno dei codici WEP impostati nell'AP per

decrittare i dati trasmessi dall'AP al client.

- Per decrittare i dati ricevuti dai client, l'AP dovrebbe disporre di tutti i codici che i client utilizzano.
- Sia l'AP che il client dovrebbero allocare gli stessi codici con lo stesso indice. Per esempio, se l'AP alloca il codice WEP "abe123" nell'indice N° 3, il client dovrebbe allocare lo stesso codice nell'indice N° 3.
- Alcuni software del client wireless (come ad esempio Funk Odyssey), possono crittografare i dati inviati con un altro codice, definendo codici WEP multipli. In questo caso l'AP non potrà discriminare questa trasmissione dati.
- Se WEP viene impostato per interfacciarsi ai terminali Samsung WIP 5000, va impostata l'autenticazione di tipo Open System, e il codice WEP dovrebbe essere impostato a 128 bit, di tipo ASCII, e comprendere solamente caratteri alfanumerici.

5.2.3 IEEE 802.1x

IEEE 802.1x è uno standard che definisce l'autenticazione "port-based" e un sistema di gestione delle chiavi (key management method). I messaggi EAP (Extensible Authentication Protocol) possono essere trasmessi sulla rete IEEE 802.11 utilizzando il protocollo "EAP Encapsulation Over LANs" (EAPOL). IEEE 802.1x genera periodicamente le chiavi. Il contenuto del frame 802.11 ed il CRC (Cycling Redundancy Checking) possono essere crittografati utilizzando lo "Stream Cipher" RC4.

Questa modalità necessita di un server RADIUS esterno per autenticare gli utenti. Gli account degli utenti possono essere gestito su tale server.

L'AP necessita di un server RADIUS che supporti l'EAP, come Microsoft Internet Authentication Server. Per consentire la connessione wireless di client windows, è necessario che il server di autenticazione supporti il protocollo EAP Protetto (PEAPO e MSCHAP V2).

Se si usa il server RADIUS esterno, si dovrebbero avere le opzioni per vari tipi di autenticazioni, come Kerberos, i certificati e le autenticazioni pubbliche, che sono supportati nella modalità IEEE 802.1x. La cosa più importante è che il client dovrebbe utilizzare la stessa modalità di autenticazione che utilizzata dagli AP.

Se si seleziona la modalità di sicurezza "IEEE 802.1x", devono essere configurati i seguenti parametri:

Parametro	Descrizione
IP Radius	Indicare l'indirizzo IP del server RADIUS nella casella di testo.
Chiave Radius	Introdurre la chiave codice RADIUS nella casella di testo. La chiave RADIUS è un codice condiviso che è utilizzato dal server RADIUS. Il testo che si introduce è visualizzato come caratteri "*", in modo che possano essere visualizzati. Questo valore non viene trasmesso sulla rete.

5.2.4 WPA Personale

Wi-Fi Protected Access Personal è uno standard Wi-Fi IEEE 802.11i che include i meccanismi CCMP-AES (*Counter mode/CBC-MAC Protocol-Advanced Encryption Algorithm)* e TKIP *(Temporal Key Integrity Protocol)*. WPA Personal usa la Pre-Shared Key (PSK) come autenticazione in luogo di IEEE 802.1x e l' EAP. PSK assume il ruolo del certificato.

Questa modalità di sicurezza è compatibile con i client wireless che supportano la vecchia modalità WPA ma non la WPA2.

Nel caso di utilizzo della modalità di sicurezza "WPA Personal", devono essere configurati i seguenti parametri:

Parametro	Descrizione
Versioni WPA	Selezionare le modalità di sicurezza del client che l'AP supporterà. - WPA - WPA2 **WPA**. Selezionare WPA se sulla rete sono presenti client che supportano il WPA **WPA2**. Selezionare WPA2, che supporta la sicurezza a livello dello standard IEEE 802.11i se sulla rete sono presenti client che supportano il WPA2.
Pacchetti di crittografia	Selezionare gli algoritmi di crittografia che si vuole utilizzare: - TKIP - CCMP(AES) **TKIP** (Temporal Key Integrity Protocol) è il valore di default. TKIP è un metodo di crittografia più sicuro del codice WEP. TKIP minimizza il riutilizzo dello stesso codice nella cifratura, il quale è una debolezza del WEP, cambiando il codice più frequentemente. TKIP utilizza una "Temporal Key" a 128 bit condivisa dall'AP e dal client. La "Temporal Key" può essere generata combinando l'indirizzo MAC del client ed i 16 ottetti del Vettori di Inizializzazione. TKIP esegue la crittografia utilizzando l'algoritmo RC4, lo stesso usato dal WEP, ma può aumentare la sicurezza della rete cambiando il Temporal Key ogni 10.000 pacchetti.
Pacchetti di crittografia	**CCMP** (Counter mode/CBC-MAC Protocol) è un metodo di crittografia per IEEE 802.11i che utilizza l' **AES** (Advanced Encryption Standard). CCMP usa il CCM in combinazione con la modalità CBC-CTR (Cipher Block Chaining) ed il CBC-MAC (Cipher Block Chaining Message Authentication Code) per la crittografia ed il controllo di integrità. Se si selezionano sia TKIP che CCMP(AES), la cifratura Pairwise sarà AES e la cifratura GroupWise sarà TKIP. Pairwise viene utilizzata per gli unicast, mentre GroupWise per i Broadcast/Multicast. Sia i client che supportano TKIP che quelli che supportano AES possono accedere all'AP. I client WPA dovranno avere uno dei seguenti parametri: - Un codice TKIP valido - Un codice CCMP(AES) valido I client che non sono impostati come WPA Personal non potranno accedere all'AP
Chiave	Il valore del codice corrispondente alla "Pre shared Key", il quale è un codice pubblico per la modalità WPA Personal. Possono essere introdotti da un minimo di 8 caratteri fino a 63.

5.2.5 WPA Aziendale

Il *Wi-Fi Protected Access* Aziendale, che utilizza RADIUS *(*Remote Authentication Dial-In User *Service*), ha portato alla definizione dello standard Wi-Fi IEEE 802.11i, che include i meccanismi CCMP-AES (*Counter mode/CBC-MAC Protocol-Advanced Encryption Algorithm)* e TKIP *(Temporal Key Integrity Protocol)*. Il WPA Aziendale necessita della presenza di un server RADIUS per l'autenticazione degli utenti

Questa modalità di sicurezza è compatibile con i client wireless che supportano la vecchia modalità WPA ma non la WPA2.

Nel caso di utilizzo della modalità di sicurezza "WPA Aziendale", devono essere configurati i seguenti parametri:

Parametro	Descrizione
Versioni WPA	Selezionare le modalità di sicurezza del client che l'AP supporterà. - WPA - WPA2 **WPA**. Selezionare WPA se sulla rete sono presenti client che supportano il WPA **WPA2**. Selezionare WPA2, che supporta la sicurezza a livello dello standard IEEE 802.11i se sulla rete sono presenti client che supportano il WPA2.
Pacchetti di crittografia	Selezionare gli algoritmi di crittografia che si vuole utilizzare: - TKIP - CCMP(AES) **TKIP (Temporal Key Integrity Protocol)** è il valore di default. TKIP è un metodo di crittografia più sicuro del codice WEP. TKIP minimizza il riutilizzo dello
Pacchetti di crittografia	stesso codice nella cifratura, il quale è una debolezza del WEP, cambiando il codice più frequentemente. TKIP utilizza una "Temporal Key" a 128 bit condivisa dall'AP e dal client. La "Temporal Key" può essere generata combinando l'indirizzo MAC del client ed i 16 ottetti del Vettori di Inizializzazione. TKIP esegue la crittografia utilizzando l'algoritmo RC4, lo stesso usato dal WEP, ma può aumentare la sicurezza della rete cambiando il Temporal Key ogni 10.000 pacchetti. **CCMP (Counter mode/CBC-MAC Protocol)** è un metodo di crittografia per IEEE 802.11i che utilizza l' **AES** (**Advanced Encryption Standard)**. CCMP usa il CCM in combinazione con la modalità CBC-CTR (Cipher Block Chaining) ed il CBC-MAC (Cipher Block Chaining Message Authentication Code) per la crittografia ed il controllo di integrità. Il client che non siano impostati come WPA Aziendali non potranno accedere all'AP. Le impostazioni predefinite prevedono sia l'utilizzo di TKIP che di CCMP. In questa condizione, i client dovranno avere uno dei seguenti parametri: - Un IP RADIUS TKIP valido e una chiave RADIUS - Un indirizzo IP CCMP(AES) valido e una chiave RADIUS
IP Radius	Indicare l'indirizzo IP del server RADIUS nella casella di testo.
Chiave Radius	Introdurre la chiave RADIUS nella casella di testo. La chiave RADIUS è un codice condiviso che è utilizzato dal server RADIUS. Il testo che si introduce è visualizzato come caratteri "*", in modo che possano essere visualizzati. Questo valore non viene trasmesso sulla rete.

5.3 Aggiornamento delle impostazioni

Le impostazioni di sicurezza possono essere aggiornate nel seguente modo:

1. Accedere al menù **Protezione**.
2. Impostare i parametri di sicurezza desiderati.
3. Premere il tasto **Aggiorna** per attivare le variazioni.

Pagina lasciata intenzionalmente bianca.

Capitolo 6. Impostazione delle reti Wireless virtuali

6.1 Impostazioni della VLAN

NOTE

- Per configurare reti o VLAN aggiuntive occorre prima abilitare le "Virtual Wireless Network" nella pagina delle "impostazioni Ethernet". Vedere "Abilitazione o Disabilitazione della rete virtuale Wireless nell'AP".
- Se è stata impostata l'opzione VLAN, la connessione all'AP può fallire. Per prima cosa verificare se lo switch e il server DHCP supportano la VLAN con IEEE 802.1Q. Dopo aver impostato l'opzione VLAN, collegare il cavo Ethernet della porta VLAN dello switch (porta WAN). Accedere nuovamente alla pagina WEB di amministrazione con un nuovo indirizzo IP. (Se necessario, contattare l'amministratore per l'impostazione della VLAN e del DHCP)

Parametro	Descrizione
Virtual Wireless Network	E' possibile configurare fino a 4 VWN.
Attivato	E' possibile abilitare o disabilitare una rete configurata. Per abilitare una rete specifica, marcare la casella **"Attivato"** corrispondente alla VWN appropriata. Per disabilitare una rete specifica, deselezionare la casella **"Attivato"** corrispondente alla VWN appropriata. Se si disabilita la rete, si perderà il VLAN ID inserito.
ID VLAN	Fornire un numero compreso 1 e 4094 per la VLAN Interna. Questo causerà da parte dell'access point l'invio di una richiesta DHCP con il tag VLAN. Lo switch e il server DHCP devono supportare i frame VLAN IEEE 802.1Q. L'access point deve poter raggiungere il server DHCP. Verificare con l'Amministratore di rete la configurazione della VLAN e del server DHCP.
SSID	Inserire un nome per la rete Wireless. Questo nome sarà applicato a tutti gli access point di questa rete. Aggiungendo nuovi access point, questi condivideranno questo stesso SSID. L' SSID *(Service Set Identified)* è una stringa alfanumerica lunga fino a 32 caratteri. NOTE Se siete connessi come client wireless allo stesso AP che state amministrando, la modifica dell'SSID causerà la perdita della connessione all'AP. Avrete bisogno di riconnettervi al nuovo SSID dopo avere salvato le impostazioni.

(Continua)

Parametro	Descrizione
Trasmissione SSID	Impostare la trasmissione dell'SSID tramite la casella **"Trasmissione SSID"**. Per default, sull'access point la trasmissione dell'SSID nei pacchetti è abilitata . E' possibile sopprimere (proibire) questa trasmissione per impedire alle postazioni di rilevare in modo automatico il vostro access point. Quando la "Trasmissione SSID" dell'AP è soppressa, il nome della rete non verrà visualizzato nella lista delle reti disponibili sulla postazione client. Al contrario il client deve conoscere nome esatto della rete configurata prima di essere autorizzato alla connessione. NOTE - L'opzione di "Trasmissione SSID" impostata è specifica per ciascuna Rete Virtuale. Le altre reti continuano ad utilizzare la modalità di sicurezza già configurata: - La vostra rete interna originale (configurata nella tabella "Impostazioni Ethernet") utilizza l'opzione di Broadcast impostata in "Protezione". - Se la rete Guest è configurata, su tale rete il Broadcast dell'SSID è sempre autorizzato.
Protezione	Impostare la **Protezione** per questa VLAN selezionandola tra i seguenti: - Nessuna (Testo normale) - WEP Statico - IEEE 802.1x - WPA Personale - WPA Aziendale NOTE - La modalità di sicurezza impostata è specifica per ciascuna Virtual Network. Le altre reti continuano ad utilizzare la modalità di sicurezza già configurata: - La rete interna originale (configurata nella pagina "Impostazioni Ethernet") utilizza la modalità di sicurezza impostata in "Protezione". - Se la rete Guest è configurata, su tale rete la modalità di sicurezza sarà sempre impostata su "Nessuna".

6.2 Aggiornamento delle impostazioni

Per aggiornare le impostazioni VLAN:

1. Accedere al menù "**Gestisci > VWN"**.
2. Configurare le impostazioni VLAN come richiesto.
3. Premere il tasto **Aggiorna** per attivare le variazioni.

.

Capitolo 7. Impostazioni Radio

La pagina delle impostazioni Radio permette all'utente di controllare le operazioni del sistema radio. Un utente può impostare come on/off la trasmissione radio, il canale RF, la potenza trasmissiva, la modalità IEEE 802.11, ecc.

SMT-R2000 può essere impostato come un AP dual band.
Prestazioni come l'area di copertura e la velocità di trasmissione saranno differente in funzione della modalità wireless considerata.
Anche nell'ambito della stessa modalità wireless, le prestazioni dell'SMT-R2000 possono variare in funzione delle caratteristiche ambientali.

L'AP opera nelle seguenti modalità:

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11a

Parametro	Descrizione
Radio	L' SMT-R2000 è un access point **Dual Band**. E' possibile selezionare la Radio 1 o la Radio 2.
Stato (Si/No)	Selezionare l'opzione **Sì** o **No** per attivare o disattivare l'interfaccia radio in esame (Radio 1 / Radio 2).
Modo	Il modo definisce lo standard a livello fisico (*Physical Layer* - PHY) usato per le operazioni radio.  NOTE Nell' SMT-R2000, la modalità IEEE802.11a può essere utilizzata solamente sull'interfaccia Radio 1, e le modalità IEEE802.11b o IEEE80211g possono essere utilizzate solamente sull'interfaccia Radio 2.
Canale	Il canale indica la porzione dello spettro radio utilizzato da una stazione per la trasmissione e ricezione dei dati. La portata di un canale e il canale base sono determinati dalla modalità d'interfaccia radio. Nella maggior parte delle modalità, l' impostazione di default è "Auto". Se l'impostazione del canale è Auto, l'AP seleziona il canale con il tasso di utilizzo più basso, basandosi sulle informazioni della potenza del segnale e del volume di traffico. Oltre a "Auto" è possibile selezionare manualmente un canale prefissato compreso fra 1 e 11.
Intervallo Beacon	Un AP trasferisce i frame di verifica in un intervallo regolare per notificare l'esistenza della rete wireless. Un AP di base trasferisce un frame di verifica ogni 100ms (10 volte per secondo). L'unità di misura dell'intervallo dei frame di verifica è in millisecondi e il valore che può essere inserito è compreso tra 20 e 2000.

(Continua)

Parametro	Descrizione
Periodo DTIM	Il DTIM *(Delivery Traffic Information Map)* è un messaggio utilizzato per i frame di controllo. DTIM contiene un segnale che indica ad un client che ha dati da trasmettere di uscire dalla modalità di "riposo". Il periodo DTIM indica con quale frequenza inviare i messaggi DTIM nei frame di verifica. Definire un valore compreso tra 1 e 255. Se il periodo DTIM è impostato a "1", il messaggio DTIM è incluso in tutti i frame di verifica. Se il periodo DTIM è impostato a "10", il messaggio DTIM è incluso ogni dieci frame di verifica.
Max Postazioni	Definire il numero massimo di client autorizzati ad accedere all'AP (0-2007).
Potenza Trasmissione	Introdurre la potenza di trasmissione dell'AP, espressa in percentuale. Il valore di default è 100%. **Raccomandazioni:** - E' possibile impostare come default il valore (100%) per massimizzare l'area di copertura dell'AP e ridurre il numero di AP nella rete. - Per incrementare la capacità della rete, impostare una bassa la potenza di trasmissione per l' AP e sistemare gli AP più vicini. Questo permette di ridurre la sovrapposizione e le interferenze tra gli AP. In aggiunta, abbassare la potenza di trasmissione rende una rete più sicura, in quanto un segnale di rete debole non viene trasmesso lontano.
Set Velocità	Imposta le velocità di trasmissione supportate dall' AP, il quale le comunicherà alla rete wireless. - L'unità di misura della velocità è Mbps (Megabit al secondo). - Le **Velocità supportate** indicano le velocità di trasmissione supportate da un AP. E' possibile impostare velocità di trasmissione multiple. Un AP seleziona la velocità di trasmissione ottimale considerando il tasso di errori e la distanza con il client. - Le **Velocità di base** vengono notificate sulla rete per comunicare con altri AP e client nella rete stessa.
Limite velocità di trasmissione / Multicast	E' possibile incrementare la prestazione qualsiasi rete limitando il numero di pacchetti trasferiti. Alcuni protocolli inviano pacchetti broadcast o multicast che la maggior parte dei nodi di rete non considera, come richieste ARP e messaggi DHCP o BOOTP. Per questi protocolli, è possibile limitare il numero di dei pacchetti ridondanti impostando il controllo limitazione del rate,. - Spuntare la casella per attivare l'opzione di limitazione di Multicast e Broadcast - Deselezionare la casella per disattivare l'opzione di limitazione di Multicast e Broadcast. Di default il **Limite velocità di trasmissione / Multicast** è disabilitato. Finché l'opzione non viene attivata, i successivi parametri rimangono in stato di disattivazione.
Limite di velocità	Introdurre il valore limite per il traffico Multicast/Broadcast. Il valore limite deve essere compreso tra 1 e 50 (in numero di pacchetti per secondo). Il valore di default del limite di traffico, che è anche il valore massimo, è di 50.
Burst limite di velocità	Il valore del "Limite di velocità Burst" è un valore indicante il numero di "raffiche" (burst) di traffico Broadcast/Multicast permesse prima di eccedere il limite. Il valore di default del limite,che è anche il valore massimo, è di 75.

7.1 Normative FCC

7.1.1 Dichiarazione di conformità FCC

Questo sistema è stato testato e verificato per soddisfare i limiti per la Classe B dei dispositivi digitali, secondo quanto riportato nella parte 15 della normativa FCC. Questi limiti sono stati imposti per fornire una ragionevole protezione contro interferenze accidentali nelle installazioni residenziali. Questo genera, utilizza e diffonde frequenze radio e se non installato ed utilizzato secondo quanto definito nelle istruzioni, può essere causa di interferenze accidentali nelle comunicazioni radio. Comunque, non vi è garanzia che le interferenze non possono verificarsi in particolare installazioni. Se questo dispositivo causa interferenze accidentali alle ricezioni radio o televisive, le quali possono essere determinate dall'accensione/spegnimento del dispositivo, l'utente è invitato a tentare di eliminare le interferenze applicando una o più delle seguenti misure:

1) Questo dispositivo richiede che l'utente o l'installatore orienti o riposizioni opportunamente l'antenna ricevente.
2) Aumentare la distanza tra il dispositivo e il ricevitore.
3) Connettere il dispositivo ad un circuito di alimentazione differente da quello dove è connesso il ricevitore.
4) Consultare il rivenditore o un tecnico esperto di radio/tv per un aiuto.

7.1.2 Dichiarazione di conformità FCC

L'antenna utilizzata per questo dispositivo deve essere installata in modo da garantire una distanza di almeno 20 cm da tutte le persone e non deve essere locata od operante in giunzione con altre antenne o ricevitori.

Esposizione alle radiofrequenze:

Questo dispositivo, nella la banda di 5.15 – 5.25 GHz, è dedicato al solo uso in interni per ridurre qualsiasi potenziale interferenza accidentale con l'attività di sistemi MSS

ATTENZIONE	Qualsiasi modifica al dispositivo non espressamente approvata dall'autorità responsabile per la conformità può far decadere li diritto dell'utente all'uso del dispositivo.

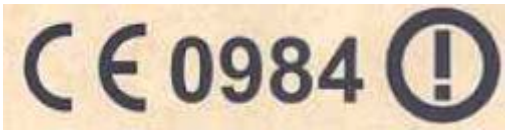

NOTE

La porta LAN, che consente di fornire l'alimentazione sulla rete LAN (PoE) in accordo all' IEEE 802-3af, dovrebbe essere considerata un dispositivo "UL Listed" e valutata come sorgente di alimentazione limitata, come definito in UL60950-1.


NOTE

Il sistema è inteso per un'installazione in una rete "Network Environment 0" come definito in IEC TR-62102 per cui, il cablaggio Ethernet associato deve essere limitato all'interno dell'edificio..

7.2 Informazioni per la Comunità Europea



Questo dispositivo è conforme alle direttive EMC 89/336/EEC, quelle di basso voltaggio 73/23/EEC e quelle R&TTE 1999/5/EC.
La conformità a queste direttive implica la conformità agli standard europei unificati (Normative Europee) che sono elencate nella Dichiarazione di Conformità EU che è stata emessa da Samsung per questo dispositivo.

7.2.1 Condizioni d'uso e operative per i paesi

Questo dispositivo può essere utilizzato nei seguenti paesi Comunità Europea e EFTA: Austria, Belgio, Cipro, Danimarca, Estonia, Finlandia, Francia, Germania, Gran Bretagna, Grecia, Islanda, Irlanda, Italia, Liechtenstein, Lituania, Lussemburgo, Malta, Norvegia, Olanda, Polonia, Portogallo, Repubblica Ceca, Repubblica Slovacca, Slovenia, Spagna, Svezia, Svizzera e Ungheria.

Le regolamentazioni per l'utilizzo interno piuttosto che esterno, la licenza e l'utilizzo dei canali utilizzati in alcuni paesi sono descritte di seguito:

L'utente deve utilizzare gli strumenti di configurazione forniti con questo dispositivo per garantire che i canali operativi siano conformi alle regole di utilizzo dello spettro per i paesi della Comunità Europea e EFTA come descritto di seguito.

7.2.2 Utilizzo delle frequenze GHz:

1. Questo dispositivo può essere utilizzato all'interno o all'esterno nei paesi della Comunità Europea e EFTA utilizzanti la banda 2.4 GHz (Canali 1-13), con eccezione di quelli indicati di seguito.
2. In Italia, è richiesta una licenza per l'utilizzo esterno. Verificare con il vostro venditore o direttamente con la Direzione Generale Pianificazione e Gestione Frequenze. E' necessaria una concessione ministeriale anche per l'uso del prodotto. Verifichi per favore con il proprio distributore o direttamente presso la Direzione Generale Pianificazione e Gestione Frequenze.
3. In Francia, questo dispositivo può essere utilizzato all'interno della banda 2400-2483 MHz (Canali da 1 a 13) per le applicazioni interne. Per l'utilizzo esterno, può essere utilizzata solo la banda 2454-2483 MHz (Canali da 10 a 13). Per le regolamentazioni più aggiornate consultare il sito http://www.art-telecom.fr.

7.2.3 Utilizzo delle frequenze GHz:

1. Questo dispositivo richiede che l'utente o l'installatore, prima di utilizzarlo, debba indicare la nazione in cui sta operando, nella pagina "Impostazioni di base", come descritto nella Guida di Gestione e Configurazione.
2. Questo dispositivo regolerà in modo automatico l'utilizzo dei canali definiti dal paese d'utilizzo. Inserire in modo errato il paese d'utilizzo, potrebbe non permettere una funzionalità corretta e

può causare interferenze accidentali con altri sistemi. L'utente è obbligato ad assicurarsi che il dispositivo stia operando in accordo con le limitazioni dei canali, restrizioni per interno/esterno e le licenze di ciascun paese della Comunità Europea, come descritto in questo documento.

3. Questo dispositivo impiega un sistema di rilevazione radar richiesto dalla Comunità Europea e dai paesi EFTA operanti nella banda da 5 GHz. Questa funzione viene automaticamente abilitata quando viene indicata come nazione un paese della Comunità Europea e EFTA. La presenza di segnali radar nelle vicinanze potrebbe causare una temporanea interruzione di questo dispositivo. Il sistema di rilevamento del radar effettuerà automaticamente un riavvio del sistema su canali liberi da segnali radar.
4. Questo dispositivo è limitato all'utilizzo interno quando opera nei paesi Comunità Europea e EFTA utilizzanti la banda 5.15 – 5.35 GHz (Canali 36, 40, 44, 48, 52, 56, 60 e 64). Vedere la tabella sottostante per i canali 5 GHz permessi.

7.2.4 Operatività nell'utilizzo dei canali 5 GHz nella Comunità Europea

L'utente/installatore deve utilizzare gli strumenti di configurazione forniti per verificare l'attuale canale operativo e fare le necessarie modifiche alla configurazione per assicurarsi una operatività conforme alle leggi relative allo spettro della Nazione Europea, come descritto di seguito e in altre parti di questo documento.

Banda di Frequenza (MHz)	Canali autorizzati	Utilizzo	Massimo EIRP (mW)
5150-5250	36, 40, 44, 48	Solo utilizzo interno	200
5250-5350	52, 56, 60, 64	Solo utilizzo interno	200
5470-5725	100, 104, 108, 112,116, 120, 124, 128, 132, 136, 140	Utilizzo interno o esterno	1000

7.2.5 Transmit Power Control (TPC) per l'operatività a 5 GHz

Questo dispositivo impiega il TPC (Transmit Power Control) per ridurre le potenziali interferenze con altri dispositivi di comunicazione operanti nella banda di frequenza da 5 GHz. La prestazione TPC implementata in questo dispositivo Wireless LAN deve essere configurata dall'utente finale quando sta operando in un qualsiasi paese della Comunità Europea o EFTA. L'utente finale deve seguire le procedure riportate nella Guida di Gestione e Configurazione per utilizzare questo dispositivo seguendo le regolamentazioni Europee per il controllo della potenza di trasmissione.


NOTE

La procedura TPC dovrebbe essere ripetuta quando si riposiziona questo dispositivo all'interno dell'attuale rete wireless o in una nuova rete wireless.

7.3 Aggiornamento delle impostazioni

Aggiornare le impostazioni wireless come indicato di seguito:

1. Accedere al menù **"Gestisci > Radio"**.
2. Configurare le impostazioni wireless come richiesto.
3. Premere il tasto "**Aggiorna"** per attivare le variazioni.


NOTE

Le impostazioni relative a "Radio 1" e "Radio 2" sono visualizzate sulla stessa pagina. In funzione del dispositivo selezionato, le impostazioni visualizzate verranno applicato a "Radio 1" o "Radio 2". Dopo aver configurato completamente una radio, premere il tasto **Aggiorna** per memorizzare le modifiche, dopo di che è possibile selezionare un altro dispositivo radio.

Capitolo 8. Impostazione del filtro degli Indirizzi MAC

Un indirizzo MAC (Media Access Control) è un indirizzo hardware che identifica univocamente ogni nodo di rete. Qualsiasi sistema di una rete IEEE 802 ha un indirizzo MAC di 48 bit che viene generalmente rappresentato come una sequenza di 12 caratteri esadecimali, come per esempio FE:DC:BA:09:87:65.

Anche le schede di rete wireless utilizzate dai clients hanno un proprio indirizzo MAC univoco.

Un utente può gestire i clients che tentano di accedere alla wireless impostando nella sezione "MAC Filtering" gli indirizzi MAC dei client autorizzarti/bloccati. Se la funzione di "MAC Filtering" è stata attivata, solo i client che hanno un indirizzo MAC autorizzato potranno accedere alla rete.

8.1 Utilizzo del filtro MAC

Utilizzare la funzione relativa al filtro MAC, permette all'utente di limitare l'accesso all'AP basandosi sugli indirizzi MAC *(Media Access Control)*. A seconda delle impostazioni del filtro, la lista può indicare gli indirizzi MAC che possono avere accesso alla rete o quelli che devono essere bloccati.

Se l'interfaccia guest è attiva, l'impostazione del filtro MAC è applicata ad entrambi le reti. In un AP che utilizza sia 802.11a che 802.11b/g, le impostazioni del filtro MAC saranno applicate ad entrambe le bande.

Parametro	Descrizione
Filtro	Selezionare una delle seguenti opzioni, per impostare il tipo di filtro MAC - Accesso autorizzato solo per i terminali presenti nella lista - Accesso bloccato per tutti i terminali nella lista - Filtro MAC non utilizzato
Stations List	Introdurre un indirizzo MAC da 48 bit e selezionare il tasto **Aggiungi** per aggiungere l'indirizzo MAC alla lista dei terminali. Selezionare un indirizzo MAC da 48 bit e premere il tasto **Rimuovi** per rimuovere l'indirizzo MAC presente nella lista

8.2 Aggiornamento delle impostazioni

Aggiornare le impostazioni di filtro MAC come indicato di seguito:

1. Accedere alla pagina **"Gestisci > Filtri MAC"**.
2. Configurare le impostazioni per il filtro MAC come richiesto.
3. Premere il tasto **Aggiorna** per attivare le variazioni.

Pagina lasciata intenzionalmente bianca

Capitolo 9. Impostazioni del Bilanciamento del Carico

SMT-R2000 permette ad un utente di distribuire le connessioni della rete wireless quando si configurano gli SMT-R2000 in un sistema con AP multipli. La funzione del Bilanciamento del Carico evita che le prestazioni di un specifico AP vengano ridotte eccessivamente a causa ad un traffico wireless non bilanciato.

9.1 Impostazioni del Bilanciamento del Carico

Attivare il Bilanciamento del carico prima di impostarne i parametri. Quindi impostare le restrizioni e il metodo di applicazione in funzione del carico di utilizzo dell'AP.

NOTE

- Selezionare **"Stato > Associazioni Client"** nella pagina web di amministrazione per visualizzare il tasso di utilizzo dell'AP. (Vedere la pagina "Monitoraggio della Sessione")
- Nonostante un client termini l'accesso ad un AP, se il client può accedere alla rete tramite un altro AP in servizio, la rete fornirà il servizio al client in modo continuativo. Il client tenterà di accedere ad un altro AP nella stessa subnet del precedente in modo automatico. Come risultato, il client può spostarsi su un altro AP della stessa subnet senza alcuna perdita.
- Le impostazioni del bilanciamento del carico sono applicate a tutto il carico di un AP. Se l'accesso guest è abilitato, il bilanciamento del carico è applicato a tutte le reti interne e reti guest.
- Le impostazioni del bilanciamento del carico sono applicate ad entrambi le interfacce radio. Comunque, il carico è valutato indipendentemente su ciascuna interfaccia. Se l'accesso guest è abilitato, le reti interne e guest sono tutte incluse.

Parametro	Descrizione
Bilanciamento del carico	Selezionare **Attivato** per abilitare la funzione di Bilanciamento del Carico. Selezionare **Disattivato** per disabilitare la funzione di Bilanciamento del Carico.
Utilizzo per nessuna nuova Associazione	Il limite impostato è relativo all'utilizzo della larghezza di banda wireless. Impostare il limite di utilizzo della larghezza di banda (%) superato il quale rifiutare l'accesso a nuovi client. Quando il tasso di utilizzo dell'AP eccede il limite impostato, l'AP rifiuta l'accesso a nuovi client. Se questo parametro è impostato a "0", l'AP permette tutti gli accessi, indipendentemente dal tasso di utilizzazione della banda.

(Continua)

Parametro	Descrizione
Utilizzazione per disconnessione	Il limite impostato è relativo all'utilizzo della larghezza di banda wireless. Impostare il limite di utilizzo della larghezza di banda (%) superato il quale rifiutare disconnettere i client. Quando il tasso di utilizzo dell'AP eccede il limite impostato, l'AP disconnetterà uno o più client. Se questo parametro è impostato a "0", l'AP non disconnetterà i client, indipendentemente dal tasso di utilizzazione della banda.
Soglia postazioni per Disconnessione	Impostare il numero di client desiderato nella "Soglia postazioni". Se il numero di client che stanno accedendo contemporaneamente all'AP è minore o uguale alla soglia indicata, i client non saranno disconnessi, indipendentemente dal valore di "Utilizzazione per disconnessione". Teoricamente, il numero massimo di accessi client simultanei consentiti è 2007.  Si raccomanda di impostare un valore compreso tra 30 e 50. In questo limite, un AP può fornire prestazioni ragionevoli.

9.2 Aggiornamento delle impostazioni

Aggiornare le impostazioni del Bilanciamento del Carico come indicato di seguito:

1) Accedere alla pagina **"Gestisci > Bilanciamento del carico"**.
2) Configurare le impostazioni per il bilanciamento del carico come richiesto.
3) Premere il tasto **Aggiorna** per attivare le variazioni.

Capitolo 10. Impostazioni di Inoltro Porte

La funzione NAT converte un indirizzo interno privato IP in un indirizzo IP pubblico valido su una rete esterna, per risolvere la scarsità degli indirizzi IP nella rete interna o per non rendere noti gli indirizzi interni sulla rete esterna.

La funzione di Inoltro porte permette ad un terminale con un indirizzo IP privato l'accesso ad una rete esterna tramite una specifica porta WAN IP.

10.1 Utilizzo della funzione di Inoltro Porte

Questa pagina permette di consentire l'accesso, da una rete esterna, ad un terminale avente un indirizzo IP privato tramite una specifica porta WAN IP.

Un utente può accedere a una porta TCP/IP di un client IP interno tramite una specifica porta TCP/IP di una WAN IP, utilizzando le impostazioni delle porte TCP/IP.

Parametro	Descrizione
Elenco inoltro porte UDP/TCP	L' "Elenco inoltro porte" mostra le attuali impostazioni della lista. Selezionare un elemento e premere il tasto **Rimuovi** per eliminarlo dalla lista. Selezionare un elemento e premere il tasto **Aggiungi** per aggiungerlo alla lista. - Elenco UDP inoltro porte - Elenco TCP inoltro porte
Indirizzo IP locale	Introdurre l'indirizzo IP interno a cui inoltrare i dati.
Porta locale	Introdurre la porta interna a cui inoltrare i dati.
Porta generale	Impostare un numero di una porta esterna da convertire in una porta locale esistente.
Rimuovi/Aggiungi	Le voci possono essere cancellate/aggiunte dalla lista utilizzando i tasto **Rimuovi** e **Aggiungi**

10.2 Aggiornamento delle impostazioni

Aggiornare le impostazioni l'Inoltro Porte come indicato di seguito:

1) Accedere a **"Gestisci > Inoltro Porte"**.
2) Configurare le impostazioni come richiesto.
3) Premere il tasto **Aggiorna** per attivare le variazioni.

Pagina lasciata intenzionalmente bianca

Capitolo 11. Impostazioni per il Controllo Porte

La funzione per il controllo delle porte consente o blocca ai servizi l'accesso ad una specifica porta per un IP WAN.

Se si inserisce una specifica porta che è utilizzata per un IP Locale, questa funzione permette o blocca l'accesso al servizio.

11.1 Utilizzo della funzione di Controllo Porte

La funzione per il controllo delle porte consente o blocca ai servizi l'accesso ad una specifica porta per un IP WAN.

Per un WAN IP, i servizi a cui può essere autorizzato o bloccato l'accesso sono i seguenti:

Telnet, HTTP, FTP, ICMP, ping.

L'utente può permettere o bloccare l'accesso ad uno specifica porta di servizio dalla WAN IP o da un terminale locale tramite la funzione di controllo delle porte.

Parametro	Descrizione
Filtri Porta Protocollo	I "Filtri Porta Protocollo" mostrano la lista dei servizi accessibili nell'attuale impostazione WAN IP. I servizi comprendono Telnet, HTTP, FTP, ICMP e ping. Un utente può permettere o bloccare l'accesso dalla WAN IP a tali servizi selezionando **"Senza Blocco"** o **"Blocco"**.
Elenco filtri porta UDP/TCP	L' "Elenco filtri porta" mostra l'impostazione corrente dei filtri. Selezionare l'elemento desiderato e premere il tasto **Rimuovi** per cancellarlo dalla lista. Digitare il valore desiderato e premere il tasto Aggiungi per aggiungerlo alla lista. - Elenco filtri porta UDP - Elenco filtri porta TCP
Numero Porta	Inserire una porta TCP/UDP specifica da bloccare per i terminali interni.
Rimuovi/Aggiungi	Le voci possono essere cancellate/aggiunte dalla lista utilizzando i tasti **Rimuovi** e **Aggiungi**.

11.2 Aggiornamento delle impostazioni

Aggiornare le impostazioni per il Controllo Porte come indicato di seguito:

1. Accedere alla pagina **"Gestisci > Controllo Porte"**.
2. Configurare le impostazioni come richiesto.
3. Premere il tasto **Aggiorna** per attivare le variazioni.

Pagina lasciata intenzionalmente bianca

Capitolo 12. Impostazione della qualità del servizio (QoS)

Nelle pagine della QoS (Quality of Service), si possono impostare i parametri relativi a differenti code al fine di garantire alte prestazioni al traffico radio di un tipo specifico, per esempio *Voice over IP* (VoIP), audio, video e streaming media.

12.1 Impostazione della Qualità del servizio

Impostare la qualità del servizio sull' SMT-R2000 significa impostare i parametri relativi alle varie categorie del traffico radio e ottimizzare l'efficienza del minimo/massimo tempo d'attesa della trasmissione tramite le "*Contention Windows"*. I parametri d'impostazione qui descritti hanno effetto sulla trasmissione dati dell'AP.


NOTE

- Nel caso dell'Interfaccia Guest, l'impostazione delle code QoS è applicata all'intero carico AP (entrambe le interfacce Radio).
- Le impostazioni sono applicate a tutte le frequenze (2.4 GHz e 5 GHz). Comunque, ogni banda radio utilizza code indipendenti. (Il traffico Guest è un'eccezione)
- Il traffico di una rete interna e di una rete Guest utilizzano sempre la stessa coda.

La QoS di un AP opera ispezionando il marcatore ToS (Type of Service) dell'intestazione di tutti i pacchetti IP in transito.
Le priorità dei pacchetti sono determinati dall'allocazione dei pacchetti in una delle code in funzione dei valori dell'area ToS. I parametri di configurazione determinano come ogni coda processa I pacchetti dei dati.
La pagina delle impostazioni della qualità del servizio comprende i seguenti menù.

- Impostazione del parametro EDCA dell'AP
- Wi Fi Multimedia
- Impostazione dei parametro EDCA delle postazioni
- Impostazione del Numero Tentativi
- Impostazione della priorità

12.1.1 Impostazione dei parametri EDCA dell'AP

I parametri *EDCA* (*Enhanced Distributed Channel Access*) dell'AP si applicano al traffico che è trasmesso dall'AP verso i client.

Parametro	Descrizione
Coda	Le code sono definite in funzione del tipo di dati che viene trasmesso dall'AP verso i client. Per ciascuna coda è possibile impostare parametri EDCA specifici **Dati 0 (Voce)** Questi dati necessitano di una alta priorità alta e del minimo ritardo possibile. I dati che sono sensibili al ritardo, come VoIP e streaming, sono inseriti in questa coda. **Dati 1 (Video)** I dati video hanno bisogno di alta priorità e del minimo ritardo possibile. I dati video vengono inseriti in questa coda. **Dati 2 (Maggior sforzo – Best Effort)** Questi dati necessitano di un medio livello di priorità, prestazioni e tempo di ritardo. La maggior parte dei dati IP sono trasmessi in questa coda. **Dati 3 (Sfondo – Background)** Questi dati necessitano di una priorità più bassa e di alte prestazioni. I flussi dati corposi, che necessitano di massimizzare le prestazioni complessive ma che sono poco influenzati dal tempo (come i dati FTP), saranno trasmessi in questa coda. Per maggiori informazioni, fare riferimento a "QoS Queues and Parameters to Coordinate Traffic Flow " nelle specifiche del protocollo IEE 802.11e.
AIFS (Inter-Frame Space)	L' AIFS *(Arbitration Inter-Frame Spacing)* corrisponde al tempo d'attesa (ms) per il *data frame*. Il valore dell' AIFS è compreso tra 1 e 255. Per maggiori informazioni, fare riferimento a "DCF Control of Data Frames and Interfame Spaces" nelle specifiche del protocollo IEEE802.11e.
CwMin (Minimum Contention Window)	Questo valore è il parametro fornito all'algoritmo che determina il valore del "random backoff wait time". Il valore definito dal parametro "*Minimum Contention Window"* rappresenta il massimo valore che l'algoritmo può assegnare all' "early random backoff wait time". Il valore casuale assegnato inizialmente dall'algoritmo a questo parametro sarà compreso tra 0 e il valore qui impostato. Se il "random backoff wait time" generato prima della trasmissione del data frame, viene superato, il contatore dei tentativi viene incrementato e il valore del "random backoff" viene raddoppiato. Questo processo viene ripetuto finché la misura del valore del "random backoff" raggiunge il valore definito nel parametro "*Maximum Contention Window"*. I valori validi "cwmin" sono 1, 3, 7, 15, 31, 63, 127, 255, 511 o 1024. Il valore di "cwmin" dovrebbe essere inferiore a quello di "cwmax". Per maggiori informazioni fare riferimento a "Random Backoff and Minimum/Maximum Contention Windows" nelle specifiche del protocollo IEEE 802.11e.

(Continua)

Parametro	Descrizione
CwMax (Maximum Contention Window)	Il valore definito nel parametro *Maximum Contention Window* è il massimo valore che il "random backoff" può raggiungere. Il valore di random backoff incrementa del doppio ad ogni tentativo, finché non raggiunge il valore di "*Maximum Contention Window"*. Una volta che il random backoff raggiunge tale valore, i tentativi verranno ripetuti finché non sarà raggiunto il valore del massimo numero di ripetizioni. I valori validi "cwmax" sono 1, 3, 7, 15, 31, 63, 127, 255, 511 o 1024. Il valore di "cwmax" dovrebbe essere maggiore di quello di "cwmin". Per maggiori informazioni fare riferimento a "Random Backoff and Minimum/Maximum Contention Windows" nelle specifiche del protocollo IEEE 802.11e.
Burst Max	**Parametro EDCA specifico per l'AP** (L'opzione Max. Burst Length è applicata solamente al traffico trasmesso dall'AP verso il client). Questo valore determina il massima durata (in millisecondi) che sarà consentita per l'invio di "raffiche" di pacchetti (packet burst) sulla la rete radio. Un "Packet Burst" è una serie di frame che vengono trasmessi senza le informazioni dell'header. Utilizzando il "packet burst", l'overhead può essere decrementato e come risultato potranno essere aumentate le prestazioni. Il "Max Burst Length" può essere compreso tra 0.0 e 999.9.

12.1.2 WMM (Wi-Fi Multimedia)

Nelle impostazioni di default, l'AP è impostato per utilizzare Wi Fi MultiMedia (WMM). Se l'opzione WMM è attivata, vengono attivate le funzioni di controllo della priorità del QoS e di'accesso al media radio. Utilizzando WMM, il servizio QoS dell' SMT-R2000 controlla sia il traffico *downstream* che viene trasmesso dall'AP verso i client (parametri EDCA dell'AP) che il traffico *upstream* che è trasmesso dai client verso l'AP (parametri EDCA dei client).
Se si indica di non usare WMM, le opzioni relative ai parametri EDCA dei client saranno rilasciate. Anche impostando WMM a "non used", è comunque ancora possibile impostare alcune opzioni dell'AP relative ai parametri EDCA dei client.

- Per disattivare il servizio WMM, premere "**Disattivato**"
- Per attivare il servizio WMM, premere "**Attivato**".

12.1.3 Impostazione dei parametri EDCA delle Postazioni

I parametri EDCA *(Enhanced Distributed Channel Access)* delle postazioni hanno effetto sul traffico trasmesso dal client all'AP.

Parametro	Descrizione
Coda	Le code sono definite in funzione del tipo di dati che viene trasmesso dall'AP verso i client. Per ciascuna coda è possibile impostare parametri EDCA specifici **Dati 0 (Voce)** Questi dati necessitano di una alta priorità alta e del minimo ritardo possibile. I dati che sono sensibili al ritardo, come VoIP e streaming, sono inseriti in questa coda. **Dati 1 (Video)** I dati video hanno bisogno di alta priorità e del minimo ritardo possibile. I dati video vengono inseriti in questa coda. **Dati 2 (Massimo sforzo – Best Effort)** Questi dati necessitano di un medio livello di priorità, prestazioni e tempo di ritardo. La maggior parte dei dati IP sono trasmessi in questa coda. **Dati 3 (Sfondo – Background)** Questi dati necessitano di una priorità più bassa e di alte prestazioni. I flussi dati corposi, che necessitano di massimizzare le prestazioni complessive ma che sono poco influenzati dal tempo (come i dati FTP), saranno trasmessi in questa coda. Per maggiori informazioni, fare riferimento a "QoS Queues and Parameters to Coordinate Traffic Flow " nelle specifiche del protocollo IEEE 802.11e.
AIFS (Inter-Frame Space)	L' AIFS *(Arbitration Inter-Frame Spacing)* corrisponde al tempo d'attesa (ms) per il *data frame*. Per maggiori informazioni, fare riferimento a "DCF Control of Data Frames and Interfame Spaces" nelle specifiche del protocollo IEEE 802.11e.
CwMin (Minimum Contention Window)	Questo valore è il parametro fornito all'algoritmo che determina il valore del "random backoff wait time". Il valore definito dal parametro "*Minimum Contention Window"* rappresenta il massimo valore che l'algoritmo può assegnare all' "early random backoff wait time". Il valore casuale assegnato inizialmente dall'algoritmo a questo parametro sarà compreso tra 0 e il valore qui impostato. Se il "random backoff wait time" generato prima della trasmissione del data frame, viene superato, il contatore dei tentativi viene incrementato e il valore del "random backoff" viene raddoppiato. Questo processo viene ripetuto finché la misura del valore del "random backoff" raggiunge il valore definito nel parametro "*Maximum Contention Window"*. I valori validi "cwmin" sono 1, 3, 7, 15, 31, 63, 127, 255, 511 o 1024. Il valore di "cwmin" dovrebbe essere inferiore a quello di "cwmax". Per maggiori informazioni fare riferimento a "Random Backoff and Minimum/Maximum Contention Windows" nelle specifiche del protocollo IEEE 802.11e.

(Continua)

Parametro	Descrizione
CwMax (Maximum Contention Window)	Il valore definito nel parametro *Maximum Contention Window* è il massimo valore che il "random backoff" può raggiungere. Il valore di random backoff incrementa del doppio ad ogni tentativo, finché non raggiunge il valore di "*Maximum Contention Window"*. Una volta che il random backoff raggiunge tale valore, i tentativi verranno ripetuti finché non sarà raggiunto il valore del massimo numero di ripetizioni. I valori validi "cwmax" sono 1, 3, 7, 15, 31, 63, 127, 255, 511 o 1024. Il valore di "cwmax" dovrebbe essere maggiore di quello di "cwmin". Per maggiori informazioni fare riferimento a "Random Backoff and Minimum/Maximum Contention Windows" nelle specifiche del protocollo IEEE 802.11e.
Limite TXOP	**Parametro EDCA Specifico per i Client** (L'opzione TXOP Limit è applicata solo al traffico trasmesso dal client all'AP). Il limite TXOP (Transmission Opportunity) indica l'intervallo di tempo entro il quali i client WME hanno il diritto di trasmettere i dati.

12.1.4 Impostazione del numero di tentativi

Come impostazione di default l'AP consente l'eventuale ritrasmissione dei pacchetti IP per un determinato numero di volte (di default sei). Questo parametro si applica in generale a tutti i pacchetti IP.

L' "Elenco numero tentativi per porta" consente di specificare, in base al tipo di protocollo e alla porta di destinazione, un numero di ripetizioni specifico per un particolare flusso dati. La lista può comprendere sino a 16 elementi.

12.1.5 Impostazione dei livelli di Priorità

L' "Elenco livelli di priorità" consente di specificare, in base al tipo di protocollo e alla porta di destinazione, un livello di priorità specifico (da 0 a 7) nella trasmissione dei pacchetti. La lista delle priorità dei pacchetti IP può comprendere sino a 16 elementi.

12.2 Aggiornamento delle impostazioni

Aggiornare le impostazioni del QoS come indicato di seguito:

1. Accedere a **"Servizi > Qualità del Servizio"**.
2. Configurare le impostazioni come richiesto.
3. Premere il tasto **Aggiorna** per attivare le variazioni.

Pagina lasciata intenzionalmente bianca

Capitolo 13. Impostazioni WDS (sistema di distribuzione wireless)

L' SMT-R2000 permette di connettere tra loro più access points usando un sistema di distribuzione wireless (WDS - Wireless Distribution System). WDS permette agli access point di comunicare tra loro via wireless in modo standardizzato. Questa capacità consente di fornire in modo agevole servizi quali il "roaming" o la gestione di reti wireless multiple. Consente inoltre di semplificare l'infrastruttura della rete riducendo la necessità di connessioni cablate.

13.1 Impostazione del WDS

Le seguenti note riassumono alcuni aspetti critici della configurazione del WDS.
Leggere tutte le note prima di procedere con la configurazione dl WDS.


NOTE

- Quando si utilizza WDS, assicurarsi di configurare le impostazioni del WDS su entrambi gli access point partecipanti al link WDS.
- E' possibile avere un solo link WDS tra una qualsiasi coppia di access point. L'indirizzo MAC di un AP remoto può apparire una sola volta nella pagina WDS di ciascun access point.
- Entrambi gli access point partecipanti ad un link WDS devono essere sullo stesso canale radio e utilizzare la stessa modalità IEEE 802.11. (Per informazioni sulla configurazione di modalità Radio e canale vedere "Configurazione delle impostazioni Radio").
- Se il protocollo 802.11h è attivo, impostare i link WDS tra due AP può essere difficile, in quanto il canale attivo di ciascun AP può subire cambiamenti, in funzione della saturazione del canale e di eventuali interferenze radar.

Per configurare WDS su un access point, occorre elencare ciascun AP inteso a ricevere e trasmettere informazioni ad esso. Per ogni AP di destinazione vanno indicate le seguenti informazioni.

Parametro	Descrizione
Radio	Indica l'interfaccia radio su cui si configura il link WDS.
Indirizzo locale	Indica gli indirizzi MAC (Media Access Control) per questo access point. Un indirizzo MAC è un indirizzo hardware univoco e prefissato per qualsiasi dispositivo che disponga di un'interfaccia alla rete. L'indirizzo MAC è assegnato dal produttore e non è modificabile. Per ogni link WDS, l'indirizzo locale riflette l'indirizzo MAC dell'interfaccia radio selezionata (Radio uno su WLAN 0 o Radio due su WLAN 1).

(Continua)

Parametro	Descrizione
Indirizzo remoto	Specificare l'indirizzo MAC dell'access point destinatario, che è, l'access point al quale i dati saranno inviati ("hand-off") e dal quale i dati saranno ricevuti, in altre parole l'AP per il quale state creando il link WDS. Selezionando la freccia alla destra del campo **Remote Address** è possibile vedere una lista degli access point rilevati, il relativo indirizzo MAC, i loro SSID ed il Livello del segnale nella rete. Selezionare l'appropriato indirizzo MAC dalla lista. NOTE **L'**SSID visualizzato nella lista a discesa è un semplice aiuto per identificare il corretto indirizzo MAC per l'access point destinatario. Questo SSID è distinto dall' SSID per il quale si sta impostando il link WDS. I due AP non hanno (e non dovrebbero avere) lo stesso valore o nome.
Bridge con	Rete che sarà connessa al link WDS. Per default, è utilizzata la rete interna.
Crittografia	Se non è importante la sicurezza del link WDS, non è richiesto di decidere il tipo di crittografia, in caso contrario è possibile selezionare WEP statico oppure WPA(PSK). **Nessuna** Se si seleziona None, i dati inviati tra gli AP tramite WDS non saranno crittografati ma sanno inviati come testo. **WEP** Abilita sul link WDS la crittografia WEP (Wired Equivalent Privacy). WEP è un protocollo di crittografia dei dati per la rete wireless 802.11. Entrambi gli access point nel link WDS devono essere configurati con le stessa impostazione di sicurezza ovvero, per il WEP statico, un codice statico condiviso per la crittografia dei dati a 64 bit. Per maggiori informazioni sulla sicurezza WEP vedere "WEP Statico". **WPA(PSK)** Abilita sul link WDS la crittografia WPA(PSK) (Wi Fi Protected Access Pre Shared Key). WPA(PSK) è una forma di crittografia più sicura rispetto a WEP. Quando si usa la crittografia WPA (PSK), ogni AP nella rete dovrà essere impostato con lo stesso codice unico, in caso contrario gli AP non saranno abilitati a comunicare tra loro. Per maggiori informazioni sulla sicurezza WPA(PSK), vedere "WPA Personal".

13.1.1 Impostazione della modalità di sicurezza del link WDS a None

Se si seleziona **"Nessuna"** come opzione preferita di crittografia per WDS, non vi verrà chiesto di compilare altri campi della pagina WDS. Tutti i dati trasferiti tra i due AP sul link WDS, saranno non crittografati.

13.1.2 Impostazione della modalità di sicurezza del link WDS a WEP

Se si seleziona **"WEP"** come opzione di crittografia per WDS, nella tabella WDS appariranno dei campi aggiuntivi.

Parametro	Descrizione
Lunghezza chiave	Specificare la lunghezza del codice WEP: - 64 bit - 128 bit
Tipo di Chiave	Specificare il tipo di codice WEP: - ASCII - Hex
Caratteri obbligatori	Indica il numero di caratteri che sono richiesti nel codice WEP. Il numero di caratteri richiesto si aggiorna automaticamente in funzione dell'impostazione della lunghezza del codice e del tipo.
Chiave WEP	Inserire una stringa di caratteri. Se avete selezionato "ASCII", introdurre una combinazione di 0-9, a-z e A-Z. Se avete selezionato "HEX", introdurre cifre esadecimali (qualsiasi combinazione di 0-9 e a-f o A-F). Questa stringa è il codice crittografico condiviso con gli utenti che usano gli access point.

13.1.3 Impostazione della modalità di sicurezza del link WDS a WPA (PSK)

Se si seleziona **WPA(PSK)** come opzione di crittografia per WDS, nella tabella WDS appariranno dei campi aggiuntivi.

Parametro	Descrizione
SSID	Inserire un nome appropriato per il nuovo link WDS che avete creato. Questo SSID dovrebbe essere differente dagli altri SSID usati da questo AP. Comunque, è importante che lo stesso SSID è anche inserito nell'altro membro del link WDS. Se questo SSID non è lo stesso per entrambi gli AP sul link WDS, questi non potranno comunicare e scambiarsi dati. L'SSID può essere una combinazione alfanumerica.
chiave	Inserire un unico codice condiviso per il WDS. Questo codice condiviso deve anche essere inserito anche sull'altro AP del link WDS. Se questo codice non è lo stesso per entrambi gli AP, questi non potranno comunicare e scambiarsi dati.

13.2 Aggiornamento delle impostazioni

Aggiornare le impostazioni del QoS come indicato di seguito:

1. Accedere a **"Gestisci > WDS"**.
2. Configurare le impostazioni come richiesto.
3. Premere il tasto **Aggiorna** per attivare le variazioni.

Pagina lasciata intenzionalmente bianca

Capitolo 14. Impostazioni di SNMP (Simple Network Management Protocol)

14.1 Impostazioni di SNMP

Di seguito viene descritto come Avviare/Sospendere gli agenti SNMP, come configurare la "community password", l'accesso ai MIB e le destinazioni dei "Trap" SNMP Trap.

Parametro	Descrizione
SNMP Attivato / Disattivato	Consente di attivare il protocollo SNMP. Di default SNMP non è utilizzato. - Per abilitare SNMP, premere **Attivato**. - Per disabilitare SNMP, premere **Disattivato**. Premere **Aggiorna** per salvare le modifiche. NOTE: Se non si abilita SNMP, tutti campi rimanenti sulla pagina SNMP verranno disabilitati.
Nome community sola lettura (per richieste GET consentite)	Introdurre il nome della community di sola lettura. Il nome della community, come definito in SNMPv2c, attiva un semplice meccanismo di autenticazione per circoscrivere il numero di macchine nella rete che possono richiedere dati all'agente SNMP. Il nome indicato corrisponde ad una password e la richieste saranno autenticate se il mittente conosce la password. Il nome della community può essere in un qualsiasi formato alfanumerico.
Numero porta di ascolto agente SNMP	Per default un agente SNMP accetta richieste solo sulla porta 161. E' comunque possibile configurarlo in modo che possa accettare richieste su altre porte. Introdurre il numero della porta sulla quale volete che l'agente SNMP possa accettare richieste.
Limita origine richieste SNMP solo agli host o alle subnet designati	E' possibile limitare la sorgente per le richieste SNMP. - Per limitare le sorgenti autorizzate ad effettuare richieste SNMP, premere **Abilitato**. - Per abilitare qualsiasi sorgente ad effettuare richieste SNMP, premere **Disabilitato**.

(Continua)

Parametro	Descrizione
Nome host o subnet del sistema di gestione di rete	Impostare nome host DNS o la subnet del dispositivo che può effettuare le richieste GET/SET. Come per i nomi della community, questo fornisce un livello di sicurezza sulle impostazioni SNMP. L'agente SNMP accetterà solamente richieste dall'hostname o dalla subnet qui specificati. Per specificare una subnet, introdurre uno più indirizzi subnet nella schermata *AddressRange/MaskLength*, dove *AddressRange* è un indirizzo IP e *MaskLength* è il numero di bit della maschera. Sono supportati entrambi i formati NetAddress/NetMask e NetAddress/MaskLength. Per esempio, se si introduce una gamma di indirizzi 192.168.1.0/24, questi specificano una subnetwork con indirizzo 192.168.1.0 e una subnet mask 255.255.255.0. Solamente le macchine con gli indirizzi IP compresi in questa gamma sono autorizzati ad eseguire richieste GET e SET sul dispositivo. Nel caso dell'esempio sopra indicato, le macchine con indirizzi da 192.168.1.1 a 192.168.1.254 possono eseguire comandi SNMP sul dispositivo.

14.1.1 Impostazione di Trap SNMP

I "Trap SNMP" generano un scambio di messaggi asincrono da dispositivi SNMP come SMT-R2000, verso un host selezionato. Se i dispositivi monitorati hanno molti Network Management System (NMS), l'invio periodico di query a tutti i dispositivi non è efficace. Attivando il Trap SNMP dell'AP, ogni dispositivo può direttamente inviare un messaggio relativo agli eventi della rete ad un host selezionato sull'NMS o al Manager SNMP. Gli eventi della rete includono l'attivazione o disattivazione di un'interfaccia di rete, le connessioni all'AP o il fallimento di un'autenticazione, l'accensione o lo spegnimento di un sistema e i dati sulla tipologia della rete.

I Trap SNMP alleggeriscono la rete eliminando le richieste SNMP ridondanti. Permettono inoltre di rendere più facile al Manager SNMP la risoluzione di problemi sulla rete. Per esempio, se un Manager SNMP è responsabile di una grande rete che supporta molti dispositivi, e ciascuno di essi ha un grande numero di oggetti, è impraticabile richiedere informazioni da ogni singolo oggetto per ogni dispositivo. La soluzione ottimale è quella che ogni agente del dispositivo gestito notifichi al manager un evento inusuale. Questo viene fatto inviando un "Trap" dell'evento.

Dopo avere ricevuto l'informazione relativa all'evento, il manager può scegliere quale azione intraprendere, se necessario.

Parametro	Descrizione
Nome Community per trap	Inserire la stringa della community globale associata con i Trap SNMP. I trap inviati dal dispositivo forniranno questa stringa come nome della community.
Nome host	Inserire il nome host DNS del computer al quale si vuole inviare il Trap SNMP. Un esempio di nome host DNS è: snmptraps.SamsungElectronics.com. E possibile indicare un massimo di tre nomi host DNS. Assicurarsi marcare la casella **"Attivato"** relativa al nome host appropriato.

14.2 Aggiornamento delle impostazioni

Aggiornare le impostazioni dell'SNMP come indicato di seguito:

1. Accedere a **"Servizi > SNMP"**.
2. Configurare le impostazioni come richiesto.
3. Premere il tasto Aggiorna per attivare le variazioni.

Pagina lasciata intenzionalmente bianca

Capitolo 15. Impostazione del Server NTP (Network Time Protocol)

NTP (Network Time Protocol) è un protocollo standard di Internet per sincronizzare la temporizzazione tra i computer nella rete. Il server NTP invia al sistema client il *Coordinated Universal Time* (UTC o *Greenwich Mean Time*). NTP invia richieste periodiche al server e regola il clock tramite i segnatempo (timestamp) ricevuti.
I timestamp saranno utilizzati per indicare la data e l'ora di ogni evento nel log dei messaggi.
Per maggiori informazioni relative all'NTP, accedere al sito http://ww.ntp.org.

15.1 Utilizzo del server NTP

Se si desidera utilizzare un server NTP, attivare l'impostazione NTP e selezionare il server NTP di destinazione. Se si desidera disattivare il server NTP, disattivare l'impostazione del server NTP dell'AP.

Parametro	Descrizione
NTP (Network Time Protocol)	NTP fornisce all'access point un metodo per ottenere e mantenere data e ora corrette da un server alla rete. L'utilizzo di un server NTP fornisce all'AP la possibilità di mostrare il giorno corretto nel log dei messaggi e nelle informazioni relative alle sessioni. Per maggiori informazioni vedere http://www.ntp.org. Scegliere se abilitare o disabilitare l'utilizzo di un server NTP. - Per abilitare il server NTP, premere **Attivato** - Per disabilitare il server NTP, premere **Disattivato**
Server NTP	Se NTP è abilitato, selezionare il server NTP da utilizzare. Potete specificare il server NTP tramite il nome host o l'indirizzo IP, sebbene l'utilizzo dell'indirizzo IP non sia raccomandato, dato che questi possono cambiare frequentemente.

15.2 Aggiornamento delle impostazioni

Aggiornare le impostazioni della temporizzazione come indicato di seguito:

1. Accedere a **"Servizi > NTP"**.
2. Configurare le impostazioni come richiesto.
3. Premere il tasto **Aggiorna** per attivare le variazioni.

Pagina lasciata intenzionalmente bianca

Capitolo 16. Visualizzazione delle informazioni dell'Interfaccia

Per monitorare lo stato della LAN cablata e della wireless LAN (WLAN), Accedere a **"Stato > Interfacce"**.

La pagina mostra le attuali impostazioni di SMT-R2000, sia per l'interfaccia Ethernet (cablata) che per le interfacce Wireless.

16.1 Impostazioni rete cablata

Il parametro "LAN o Interna" mostra l'indirizzo MAC Ethernet, l'ID VLAN, l'indirizzo IP e la Subnet Mask.
Il parametro "Interfaccia Guest" mostra l'indirizzo MAC e l'ID VLAN.
Premere il link **Modifica** per modificare le impostazioni.

16.2 Impostazioni Wireless

I parametri "Radio 1" e "Radio 2" mostrano la modalità radio e il canale, in aggiunta all'indirizzo MAC ed al nome della rete dell'interfaccia interna e dell'interfaccia Guest. (Per maggiori informazioni , vedere Impostazioni Wireless e Impostazioni Radio).
Premere il link **Modifica** per modificare le impostazioni.

Pagina lasciata intenzionalmente bianca

Capitolo 17. Visualizzazione del log degli eventi

Un utente può, tramite questa pagina, verificare gli eventi generati dall' SMT-R2000.
Questa pagina fornisce un opzione per attivare il "Registro inoltri", per catturare gli errori mostrati nel log del kernel e tutti gli eventi di sistema. (Per queste impostazioni, è necessario configurare un host remoto di inoltro dei log. Vedere "Impostazione dell'host di inoltro dei log").


NOTE

SMT-R2000 ottiene informazioni sulla data e l'ora utilizzando Network Time Protocol (NTP). L'informazione relativa all'ora è memorizzata nel formato UTC (conosciuto come Greenwich Mean Time). Perciò, l'informazione relativa all'ora memorizzata dovrebbe essere modificata dall'utente per l'ora locale.

Per informazioni relative alle impostazioni NTP, fare riferimento ad "Impostazioni del server NTP".

17.1 Log remoto

Il log del kernel è una lista molto corposa, che include anche messaggi kernel come condizioni di errore ed eventi di sistema (vedere Log di Sistema).
I messaggi di log del Kernel sono direttamente verificabili tramite l'interfaccia web di amministrazione del relativo AP.
Per abilitare il log remoto, un server remoto dovrebbe essere configurato come "Host di inoltro dei Log": successivamente è possibile impostare il sistema SMT-R2000 per trasferire i messaggi syslog al server remoto.
La registrazione dei messaggi syslog degli AP su un server remoto, offre numerosi vantaggi, come indicato di seguito:

- Registrare ed accorpare i messaggi syslog di vari AP.
- Memorizzare i messaggi che vengono cancellati sull'AP.
- Gestire messaggi ed errori tramite script sul server.

17.2 Impostazione dell'host di inoltro dei Log

Per utilizzare la funzione di inoltro dei Log del Kernel, il server remoto deve essere impostato per poter ricevere i messaggi di syslog. Il metodo d'impostare il server remoto varia in funzione dell'host di inoltro dei Log utilizzato dall'utente. Il seguente è un esempio d'impostazione di un server remoto Linux che utilizza il syslog daemon.

Esempio di utilizzo della funzione Linux Syslog

E' possibile attivare il syslog daemon del server Linux attraverso le seguenti procedure. Per questo, sono richiesti i diritti amministrativi dell'account root.

1) Effettuare il Log in con l'account root del server che sarà usato come host di inoltro syslog. Le seguenti attività necessitano l'account di autorizzazione root. Se non si effettua il Log in con l'account root, digitare "su" (Super User) sulla riga di comando per acquisire le autorità dell'account `root`('super user').
2) Aggiungere '-r' dopo la variabile `SYSLOGD` all'inizio del file `etc/init.d/sysklogd`.
   `SYSLOGD='-r'`
   Le informazioni sulle opzioni del comando syslogd possono essere ottenute utilizzando il comando "man" (digitare "man syslogd"sulla riga di comando).
3) Per tutti i messaggi nel file, modificare il file `/etc/syslog.conf.`
   Come esempio, se memorizzate un file di log nominato '`AP_syslog`', aggiungere il seguente comando:
   `*.* -/tmp/AP_syslog`
   Per informazioni sulle opzioni del file `syslog.conf` è possibile utilizzare il comando "man" (digitare "man syslog.conf" sulla linea di comando).
4) Digitare il seguente comando per effettuare un riavvio del servizio syslog.
   `/etc/init.d/syslogd restart`


NOTE

Il processo syslog utilizza di norma la porta 514. Si raccomanda di mantenere le impostazioni di default.

Se si intende modificare la porta per il log, verificare prima che la porta che si intende allocare non sia utilizzata da altri processi.

17.3 Attivazione/Disattivazione del Registro Inoltri

Per impostare ed attivare la funzione inoltro dei Log, nella pagina "**Stato > Eventi"**, impostare l'opzione **"Registro Inoltri"** come descritto di seguito e premere il tasto **Aggiorna**.

Parametro	Descrizione
Registro Inoltri	Selezionare per attivare o disattivare l'inoltro dei Log all'host. Se si spunta la casella del **Registro Inoltri**, il servizio di inoltro dei log viene attivato ed è possibile modificare l'indirizzo IP e la porta del server di inoltro.
Host di inoltro	Impostare l'indirizzo IP o il DNS dell'host di inoltro.
Porta di inoltro	Impostare la porta utilizzata dal processo syslog del server di inoltro. La porta predefinita è 514.

17.4 Impostazioni per la Memorizzazione

Premere il tasto **Aggiorna** per attivare le modifiche.
Se si spunta l'opzione per il registro inoltri, il log remoto viene attivato da quando si preme il tasto **Aggiorna**. L'AP trasferirà in tempo reale i messaggi kernel al log del server remoto.
Se si deseleziona l'opzione per il registro inoltri, il log remoto viene disattivato da quando si preme il tasto **Aggiorna**.

17.5 Eventi

La pagina degli eventi mostra gli eventi di sistema dell'AP, come ad esempio la connessione e l'autenticazione degli utenti.

La visualizzazione in tempo reale degli eventi è disponibile nel menu di amministrazione alla pagina **"Stato > Eventi"**.

Pagina lasciata intenzionalmente bianca

Capitolo 18. Visualizzare le statistiche di Trasmissione/Ricezione

Per visualizzare le statistiche di ricezione/trasmissione di un access point, accedere alla pagina **"Stato > Trasmissione/Ricezione"**.
Questa pagina fornisce alcune informazioni sull'access point e visualizza in tempo reale le statistiche di trasmissione e ricezione come descritto nella seguente tabella. Tutte le statistiche di trasmissione e ricezione mostrate indicano i totali complessivi da quando l'access point è stato attivato. Se l'AP viene riavviato, questa pagina indica i totali della trasmissione/ricezione dal momento del riavvio.

18.1 Contenuto delle statistiche

Parametro	Descrizione
Indirizzo IP	E' l'indirizzo IP dell'access point.
Indirizzo MAC	L'indirizzo MAC (Media Access Control) per l'interfaccia specifica. L'indirizzo MAC è un indirizzo hardware permanente ed unico di un dispositivo, il quale indica l'interfaccia di rete. L'indirizzo MAC è assegnato dal produttore e l'utente non può modificarlo. SMT-R2000 ha uno specifico indirizzo MAC per ciascuna delle due interfacce radio disponibili.
ID VLAN	Virtual LAN (VLAN) ID Un VLAN è un raggruppamento logico, gestito via software, di dispositivi di rete, che in tal modo possono operare come se fossero fisicamente connessi ad un unica rete dedicata, anche se possono non esserlo. Le VLAN possono essere usate per realizzare una rete interna ed una rete "guest" sullo stesso access point.
Nome (SSID)	Nome della rete wireless. Anche conosciuto come SSID, questo codice alfanumerico identifica in modo univoco una rete locale (LAN).
Informazioni su Trasmissione e Ricezione	
Totale Pacchetti	Indica il totale dei pacchetti inviati (nella tabella della trasmissione) o ricevuti (nella tabella della ricezione) da questo access point.
Total Byte	Indica il totale dei bytes inviati (nella tabella della trasmissione) o ricevuti (nella tabella della ricezione) da questo access point.
Errori	Indica il totale degli errori relativi alla trasmissione e ricezione dei dati su questo access point.

Pagina lasciata intenzionalmente bianca

Capitolo 19. Visualizzazione della Lista delle Associazioni Client

Per visualizzare tutti i client che hanno avuto accesso ad uno specifico AP, utilizzare il menù **"Stato > Associazioni client"**.
Questa pagina mostra anche informazioni relative al traffico di pacchetti inviati/ricevuti da ogni client.

19.1 Monitoraggio dell'Integrità del Link

SMT-R2000 dispone della funzione di *Monitoraggio dell'Integrità del Link,* per verificare costantemente la connessione di client (compresa la situazione dello scambio di dati).
Per farlo, anche in assenza di traffico, l'AP invia pacchetti dati ai client ad intervalli di alcuni Tramite questo invio di dati, l'AP può rilevare se un client va fuori portata (anche in presenza di traffico anomalo). Se un client rimane fuori portata per più di 300 secondi, viene rimosso dalla lista dei client connessi.

19.2 Qual è la differenza tra Associazione e Sessione?

Associazione indica che un client accede ad uno specifico AP, mentre *Sessione* indica che un client accede alla rete. Nella stessa sessione, il punto di accesso del client alla rete (l'associazione), può passare da un AP del cluster ad un altro.

Pagina lasciata intenzionalmente bianca

Capitolo 20. Visualizzazione della lista degli AP adiacenti

Tramite la lista degli AP adiacenti potete ottenere in tempo reale le statistiche di tutti gli AP rilevati entro la portata di quello a cui si è connessi.

20.1 Lista AP Adiacenti

Parametro	Descrizione
MAC	Mostra l'indirizzo MAC dell'AP rilevato L'indirizzo MAC è un indirizzo hardware, univoco, specifico per ciascun nodo della rete.
Radio	Il parametro Radio indica quale interfaccia radio ha rilevato l'AP indicato. - Wlan0 (Interfaccia Radio 1) - Wlan1 (Interfaccia Radio 2)
Beacon Int.	Mostra l' "Intervallo Beacon" utilizzato dall'AP. Gli AP trasmettono un frame di controllo (Beacon) ad intervalli regolare di tempo per notificare la presenza della rete radio. Per default l'AP trasferisce un frame Beacon ogni 100 m/sec (o 10 frame per secondo). E' possibile modificare questo intervallo nel menu **"Gestisci > Radio"**. (Vedere "Configurazione delle impostazioni Radio").
Tipo	Mostra il tipo di dispositivo rilevato. - **AP** indica un dispositivo che supporta la modalità "Infrastruttura" (IEEE 802.11 Infrastructure Mode), ovvero opera come access point. - **Ad hoc** indica un terminale che sta operando in modalità "Ad hoc". I terminali possono essere impostati nella modalità Ad hoc per comunicare direttamente con altri terminali senza un AP (IEEE 802.11 peer-to-peer, o IBSS - Independent Basic Service Set).
SSID	*Service Set Identifier* di un AP. L' SSID è l'identificatore univoco di un'interfaccia radio LAN e consiste in una stringa alfanumerica fino a 32 lettere caratteri. L'SSID è in sostanza il nome della rete. L'SSID può essere impostato nel menù **"Impostazioni di Base"** (vedere Impostazioni della configurazione di base) o nel menù **"Gestisci > Impostazioni Wireless"** (vedere Impostazioni dell'interfaccia Wireless). La rete Guest e la rete Interna operanti sullo stesso AP dovrebbero avere due differenti SSID.
Privacy	Indica se il dispositivo utilizza le politiche di sicurezza. - **Off** indica che la modalità di sicurezza del dispositivo è impostata a None" (Nessuna sicurezza). - **On** indica che il dispositivo utilizza la politica di sicurezza. Gli utenti possono impostare la politica di sicurezza dell'AP nel menù **"Sicurezza"**. Per maggiori informazioni sull'impostazione della sicurezza, fare riferimento a Configurazione della Sicurezza.

(Continua)

Parametro	Descrizione
WPA	Indica se la modalità di sicurezza WPA dell'AP è impostata ad "On" o "Off".
Banda	Indica la modalità IEEE 802.11 utilizzata nell'AP (per esempio 802.11b e 802.11g) I valori che possono essere verificati da questo parametro sono i seguenti: - **2.4** indica la modalità IEEE 802.11b o IEEE 802.11g - **5** indica la modalità IEEE 802.11a - **5 Turbo** indica la modalità Atheros Turbo 5 GHz.
Canale	Mostra il canale usato dall'AP. Il canale corrisponde ad una parte dello spettro radio che l'interfaccia radio utilizza per lo scambio dei dati. Il canale può essere impostato nel menù **"Gestisci > Radio"** (vedere Impostazioni della configurazione dell'interfaccia Radio).
Velocità	Mostra l'attuale velocità (in Mbps) dell'AP. Questo valore è uno del transfer rate elencati nella lista del "Set Velocità".
Segnale	Indica l'intensità (in dB) del segnale emesso dall'AP.
Beacons	Mostra il numero complessivo di frame "Beacon" trasmessi dall'AP dopo l'ultimo riavvio.
Last Beacon	Mostra la data e ora di trasmissione dell'ultimo frame Beacon generato dall'AP.
Rates	Mostra le impostazioni delle velocità supportate e della velocità di base che l'AP supporta. L'unità di misura è megabit per secondo (Mbps). Sono elencate tutte le velocità supportate, e quella predefinita è visualizzata in grassetto. La velocità può essere impostata nel menù **"Gestisci > Radio"** (vedere "Impostazioni della configurazione dell'interfaccia Radio"). Le velocità riportate sono quelle elencate nella lista delle "Velocità supportate" dell'AP.

Capitolo 21. Gestione della configurazione dell'AP

21.1 Ripristino della configurazione di fabbrica

Se un problema generato dal sistema SMT-R2000 non è risolvibile tramite la ricerca guasti, utilizzare la funzione di **Riavvio**. Questa funzione ripristina tutte le configurazioni dell'AP con le impostazioni di fabbrica.

1. Selezionare il menù **"Manutenzione > Configurazione"**
2. Premere il tasto **"Reimp.Predef."**

Tutte le impostazioni verranno riportate ai valori predefiniti. I valori di predefiniti sono elencati nella seguente tabella.

Parametro	Valore Predefinito
Indirizzo IP Ethernet (rete cablata)	192.168.111.10
Codice Paese	NN
SSID 802.11a(5 Ghz)	SMT-R2000-WLAN0
SSID 802.11b/g (2.4 Ghz)	SMT-R2000-WLAN1
Nome AP (Nome DNS)	Samsung-AP
Impostazione Accesso Guest	Non impostato
Impostazione VWN	Non impostato
Server DHCP	Non impostato
Assegnazione IP	IP Statico

21.2 Memorizzare le impostazioni in un file di Back up

Per memorizzare le impostazioni correnti dell'AP in un file di back up (.cbk/code>format), procedere come indicato:

1. Premere il link "**Download configurazione**"
   Viene visualizzata una finestra di dialogo per download del file.
2. Selezionare l'opzione **Salva** dalla finestra di dialogo.
   Indicare il nome del file di destinazione
3. Selezionare la cartella di destinazione e premere il tasto **Salva** per memorizzare il file.

E' possibile usare il nome di file proposto (config.cbk) o rinominarlo. Comunque, il nome del file modificato deve avere la seguente forma '`Nome + config.cbk`'.

21.3 Ripristinare le impostazioni da un file memorizzato precedentemente

Ripristinare le precedenti impostazioni dal file di back up come indicato di seguito:

4. Selezionare il file di back up da ripristinare. Digitare il nome ed il percorso completo del file o premere il tasto Sfoglia… per selezionare il file.
5. (Il file deve chiamarsi config.cbk, oppure "nome + config.cbk", e deve essere stato creato utilizzando la funzione di back up vista al paragrafo precedente).
6. Premere il tasto Ripristina.

L' access point verrà riavviato.
Dopo il riavvio, introdurre l'indirizzo IP nella finestra degli indirizzi del browser per accedere alla pagina web di amministrazione. Quindi, l'utente può verificare che siano state ripristinate le configurazioni presenti nel file di back up.

21.4 Riavvio dell'AP

Un utente può effettuare un reboot dell'SMT-R2000 manualmente per la gestione o per risolvere un problema.

1. Selezionare il menù **"Manutenzione > Configurazione"**.
2. Premere il tasto **Riavvia**.

L'AP verrà riavviato.

Capitolo 22. Aggiornamento del Firmware

Se viene resa disponibile una nuova versione del firmware dell' SMT-R2000, potete effettuare un aggiornamento del firmware sul vostro dispositivo per sfruttare le nuove funzioni ed i miglioramenti apportati al sistema.

CAUTION

Non effettuare l'aggiornamento del firmware da un client wireless che è associato con l'access point che state aggiornando. Facendolo causerete il fallimento dell'aggiornamento. Successivamente, tutti i client wireless sarebbero dissociati e nessuna nuova associazione sarebbe permessa.

In queste condizioni, è necessario accedere all'access point bisogna da un cliente sulla rete cablata:
- Creare una connessione Ethernet da un PC all'access point.

- Accedere alla pagina di amministrazione

Ripetere il processo di aggiornamento utilizzando il client cablato.

NOTE

L' aggiornamento va effettuato separatamente su ciascun access point: non è possibile aggiornare il firmware in modo automatico tramite il cluster.

Tenere presente che al termine dell'aggiornamento l'access point viene inizializzato con le impostazioni predefinite di fabbrica.

Per aggiornare il firmware per un particolare access point:

1. Accedere a **"Manutenzione > Aggiorna"**

   Viene visualizzata l'informazione relativa all'attuale versione firmware e viene fornita l'opzione di aggiornare il firmware con una nuova immagine.
2. Se conoscete il percorso del file della **Nuova immagine Firmware**, immetterlo nella casella di testo. In caso contrario, premere il tasto **Sfoglia…** e localizzare il file con la nuova immagine del firmware.

NOTE

Il file di aggiornamento del firmware deve essere nel seguente formato: `<FileName>.upgrade.tar`. Non provare ad utilizzare il file `<FileName>.bin` o file di altro formato per l'aggiornamento, questi non funzioneranno.

22.1 Aggiornamento

1. Premere il tasto **Aggiorna** per caricare la nuova immagine del firmware.
2. Appena premuto il tasto **Aggiorna** per l'aggiornamento del firmware, verrà mostrata un messaggio di conferma, che descrive il processo di aggiornamento.
3. Premere il tasto **OK** per confermare l'avvio del processo di aggiornamento.

Il processo di aggiornamento può durare 7-9 minuti durante i quali l'access point non sarà disponibile. Durante il processo di aggiornamento non togliere l'alimentazione all'AP.
In caso contrario l'AP potrebbe danneggiarsi gravemente. Quando l'aggiornamento è completato, l'AP effettuerà un riavvio e inizierà a funzionare con le configurazioni precedenti all'aggiornamento.

22.2 Verifica dell'aggiornamento del firmware

Per verificare che l'aggiornamento del firmware sia andato a buon fine, , verificare la versione del firmware visualizzata nella tabella **"Manutenzione > Aggiorna"** (o nella tabella **"Impostazioni di Base"**).

Se l'aggiornamento ha avuto successo, verranno indicati il nome o il numero della nuova versione del firmware.

Pagina lasciata intenzionalmente bianca

Manuale Utente SMT-R2000

SAMSUNG ELECTRONICS