



HOW TO

Configurazione delle funzioni iFeature

SIEMENS

Contents

Configurazione delle funzioni iFeature	3
iFeature. iPCF e iPCF-LF	3
iFeature. iPCF-HT	8
iFeature. iPCF-MC e iPCF-MC LF	9
iFeature. Come funziona iPCF?	14
iFeature. Come funziona iPCF-MC?	17
iFeature. Tip&Tricks iPCF-MC.	19

Configurazione delle funzioni iFeature

Il seguente tutorial vi permetterà di configurare le funzioni iFeature.

Condizione necessaria: dovete aver inserito la key-plug per l'attivazione della licenza.

In caso contrario, ad esclusione la serie W722, dovete acquistare:

- 6GKxxx-8PA (per access point)
- 6GKxxx-4PA (per client)

Prima di attivare e configurare le funzioni iFeature, dovete aver già letto e portato a termine le indicazioni del tutorial *how to wizard*.

Condizione necessaria prima di iniziare questo tutorial:

1. aver già attiva una comunicazione wireless tra AP e client.

Nota importante:

La lista delle funzioni iFeature è composta dalle seguenti opzioni:

1. iPCF e iPCF-LF
2. iPCF-HT
3. iPCF-MC e iPCF-MC LF
4. iPRP (argomento non trattato in questo tutorial)
5. iREF (argomento non trattato in questo tutorial)
6. AeroScout (argomento che non verrà trattato)

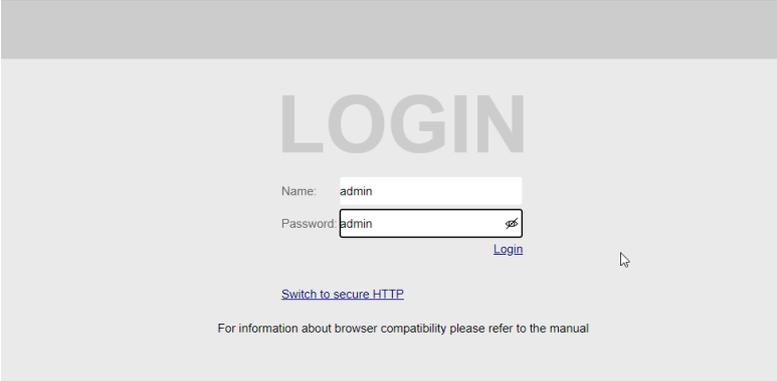
iFeature. iPCF e iPCF-LF

Partiamo dalla configurazione dell'access point.

Avviate il vostro browser (IE, Google Chrome, Firefox, MS Edge) e come URL digitate l'indirizzo IP del dispositivo.



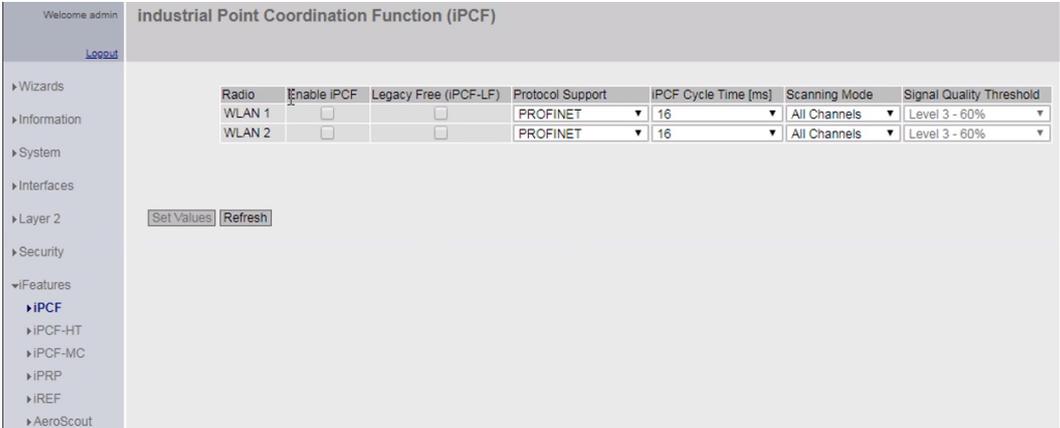
Dovrete successivamente inserire le credenziali di accesso.



Sul lato sinistro della pagina web, trovate una serie di link che sono il collettore dei vari parametri del dispositivo.
Dovete aprire il link iFeatures (l'ultimo della lista) e selezionare la voce iPCF.



La pagina web verrà aggiornata con le impostazioni specifiche della funzione iPCF.



Il primo passo è attivare la funzione iPCF o, eventualmente, la versione LF (Legacy Free).

Cosa differenzia le due opzioni?

La versione iPCF è utile nel caso in cui stiate inserendo i nuovi dispositivi scalance W in una rete wifi preesistente, costituita dalla versione precedente di questa gamma di prodotti.
La funzione iPCF impone che il protocollo attivo sul dispositivo sia la versione 802.11a.

La versione LF, Legacy Free, vi torna utile nei casi in cui la vostra rete wifi è costituita da client ed access point della nuova serie (la versione 'n').

La versione Legacy Free funziona sia con il protocollo 'a' che 'n'.
Una caratteristica del iPCF-LF è quella di ottimizzare le comunicazioni Profinet/safe con il protocollo 'n'.

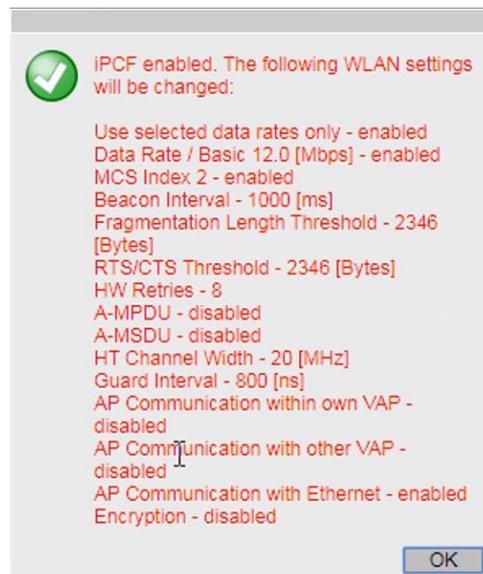
Nota importante:

Ricordatevi, tuttavia, di utilizzare questo protocollo (LF) solo nel caso in cui abbiate collegato ai dispositivi, più antenne.

Per esperienza vi posso dire che la condizione necessaria è che ci siano tre antenne (configurazione preclusa per alcuni modelli).

In caso contrario (1 o 2 antenne) vi consiglio di utilizzare la versione iPCF indipendentemente dalla tipologia di dispositivi presenti nella vostra rete.

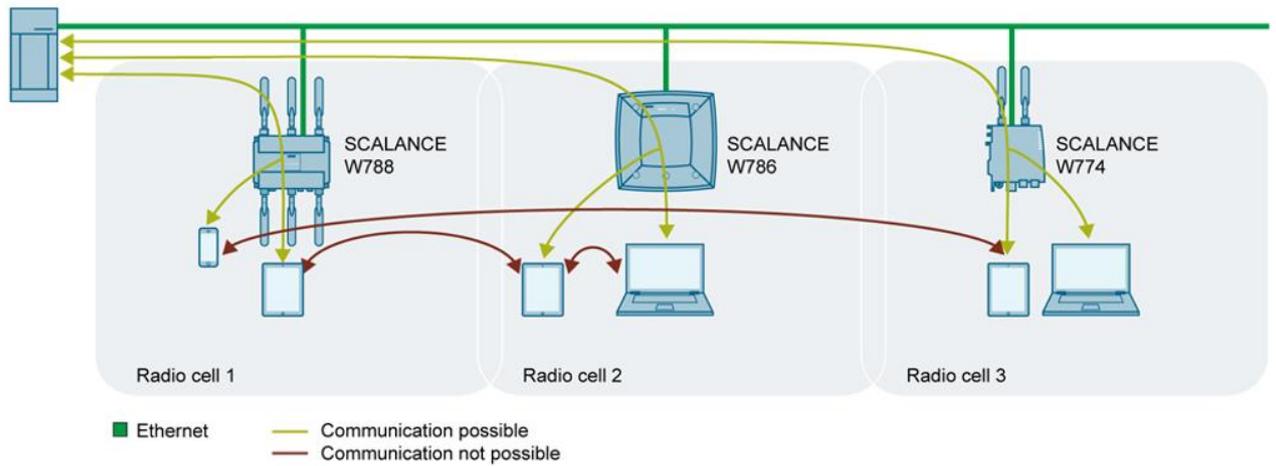
Quando abiliterete la funzione iPCF vi apparirà questo pop-up che riassume le limitazioni che verranno introdotte dopo l'attivazione iPCF.



Le limitazioni fondamentali sono:

1. La limitazione ad un baudrate di 12Mbps.
2. Le comunicazioni intracella

Il punto 2, in particolare, descrive il fatto che i nodi collegati a valle di un client non possono comunicare, direttamente, con altri dispositivi collegati ad altri client.



Questa limitazione, tuttavia, si può disabilitare (vedi tutorial relativo alla sicurezza della rete wifi).

Il passaggio successivo prevede di abilitare o meno, il supporto PNIO/Ethernet IP.

Wizard configuration interface showing the iPCF (IPsec Policy Control Function) settings for WLAN 1 and WLAN 2. The 'Protocol Support' dropdown menu is open, showing options: PROFINET, disabled, PROFINET, and EtherNet/IP.

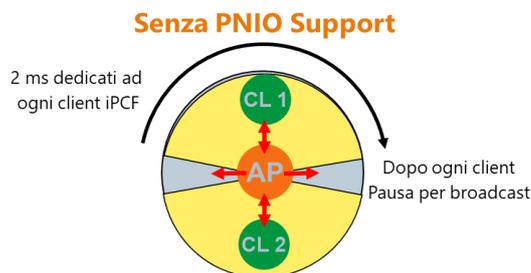
Radio	Enable iPCF	Legacy Free (iPCF-LF)	Protocol Support	iPCF Cycle Time [ms]	Scanning Mode	Signal Quality Threshold
WLAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	PROFINET	16	All Channels	Level 3 - 60%
WLAN 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disabled	16	All Channels	Level 3 - 60%

Buttons: Set Values, Refresh

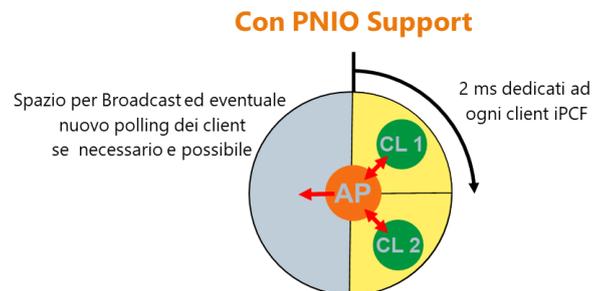
Cosa comporta l'abilitazione o meno del supporto PNIO?

iPCF PNIO Support

L'iPCF può essere implementato in due modalità di utilizzo:



Il **Ciclo iPCF** non è a lunghezza fissa ma è determinato dal numero di client: ogni nuovo client aumenta di 2 ms il ciclo complessivo. Non è possibile quindi stabilire a priori i tempi di risposta dei client a meno che non si abbia un perfetto controllo su di essi.



Il **Ciclo iPCF** è configurato a lunghezza fissa rigida (8, 16, ..., 256 ms):

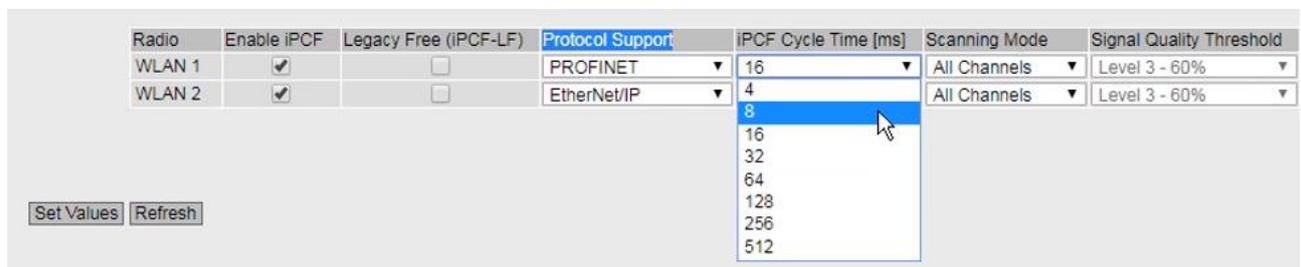
- se i client sono < (ciclo/2 ms), il tempo residuo è dedicato a quei client che ne fanno richiesta (oltre che al broadcast)
- Se i client sono superiori a ciclo/2ms gli ultimi arrivati non potranno comunicare finché uno slot non viene rilasciato da un altro client...

N.B.: i pacchetti di traffico Profinet (o alternativamente Ethernet/IP*) sono comunque trasmessi con priorità Superiore rispetto a tutti gli altri (per esempio TCP/IP).

* Solo dalla versione FW 6.0 in poi

Se siete interessati ad approfondire l'argomento vi rimando al capitolo dedicato alla descrizione del funzionamento della funzione iPCF (appendice A del presente tutorial).

Se avete optato per il supporto PNIO dovete definire il tempo di scansione della rete attraverso il parametro iPCF cycle time.



Rispettate le seguenti regole per definire la base dei tempi per lo iPCF Cycle Time:

1. Tra i 10 ed i 12 client in configurazione Rcoax, 32 ms.
2. Fino a 20 client, 64 ms.
3. Dai 20 ai 30 client, 128 ms (Info → stimate indicativamente il traffico di rete).
4. Dai 30 ai 50 client, 256 ms (Warning → valutate **bene** il traffico di rete).
5. Oltre, 512 ms (Alert → valutate **molto attentamente** il traffico di rete).

Perché dovete stare molto attenti al valore che assegnerete a questo parametro?

Il valore di questo parametro determina il tempo di aggiornamento Profinet dei nodi collegati a valle del client e nel caso di comunicazione Profisafe, il tempo di monitoraggio del protocollo di sicurezza (f_monitoring_time).

Formule:

tempo aggiornamento = iPCF cycle time x 2
watchdog = tempo aggiornamento x 4 o 5 tentativi

Esempio:

iPCF cycle time = 32 ms
 tempo aggiornamento dei nodi collegati al client = 64 ms
 watchdog = 192ms (per 3 tentativi) 256 ms (per 4 tentativi)

Se avrete anche la parte safety nel vostro progetto, dovrete calcolare il valore da assegnare al parametro `f_monitorin_time` in questo modo:

`f_monitoring_time` = watchdog x 3

Significherebbe impostare un `f_monitoring_time` pari a 576ms, nel caso in cui il watchdog è pari a 192ms, mentre aumenterà a 768ms, nel caso in cui il watchdog sarà pari a 256ms. Questo significa che, nel caso peggiore, l'evento di emergenza, per esempio la pressione di un fungo di emergenza, verrà segnalato al sistema di terra dopo 576 ms o 768ms.

Se, per qualunque motivo, dovrete modificare un qualsiasi valore coinvolto nelle relazioni appena descritte dovrete, conseguentemente, aggiornare anche i tempi a valle di quello modificato.

I parametri SCANNING MODE e SIGNAL QUALITY TH intervengono sul roaming del client.

Il parametro SCANNING MODE ha due opzioni:

1. ALL CHANNELS
2. NEXT CHANNEL

All channels:

il client esegue, in backgorund, una scansione della rete wifi. Ad interrupt si attiva nella ricerca di tutti i possibili access point che riesce a captare. Questa ricerca avviene su tutti i canali. Se rileva un access point con un segnale migliore, attiva il roaming.

Next channel:

il client esegue, in backgorund, una scansione della rete wifi. In questo caso, tuttavia, il client esegue una scansione solo sui canali permessi. Se trova un nuovo access point (che rispetta le impostazioni del signal quality th.) effettua un roaming altrimenti rimane collegato alla rete preesistente.

Questa opzione abilita il parametro SIGNAL QUALITY TH. Questa soglia definisce il valore minimo di ricezione dell'access point da parte del client affinché, quest'ultimo, consideri l'access point come un nuovo dispositivo sul quale effettuare un roaming.

Qui di seguito i livelli selezionabili:

Level	Signal quality in RSSI	Signal quality in %
1	20	40
2	25	50
3	30	60
4	35	70
5	40	80

La configurazione del client si riduce solo all'attivazione della funzione attraverso una check box.

iFeature. iPCF-HT

La funzione iPCF-HT è stata sviluppata per sopperire alla limitazione di banda introdotta dalla funzione iPCF.

Vi ricordo che attivando le funzioni iPCF, il baudrate si riduce a soli 12 Mbps (19 Mbps con la versione LF).

Questo limite non rappresenta un problema nelle comunicazioni Profinet/safe in quanto, solitamente, il volume di dati scambiati tra i dispositivi di automazione (PLC, ET200sp, ect.) è molto contenuto.

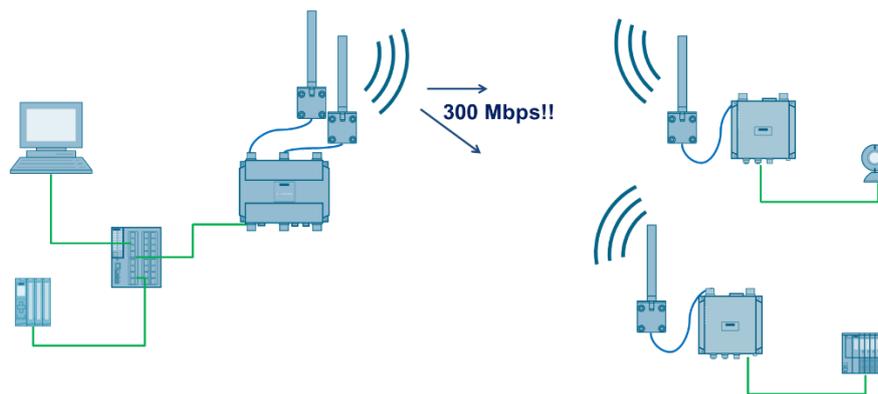
Ci sono, tuttavia, molte applicazioni dove i sistemi di automazione devono condividere la rete con dispositivi che necessitano ed occupano banda per trasmettere i loro dati.

Telecamere, VoIP sono solo alcuni esempi.

Tecnologie che sempre di più vengono integrate in una rete di automazione e che hanno un volume di scambio dati ben diverso.

Per venire incontro a queste richieste è stato sviluppato questo protocollo: iPCF-HT High Throughput.

Scalance W – Features utili iPCF-HT



La funzione iPCF-HT, incrementa il baudrate fino a 300Mbps

Dovete, tuttavia, considerare i seguenti vincoli:

1. si può usare solo nella banda 5GHz
2. si può usare solo in combinazione con il protocollo 802.11n
3. Si può attivare solo sulla scheda numero 1 (WLAN 1)
4. Devono essere presenti almeno due antenne (MIMO 2:2).

La configurazione del client si riduce solo all'attivazione della funzione attraverso una check box, nulla di più.

iFeature. iPCF-MC e iPCF-MC LF

In questo capitolo vedremo come attivare la funzione iPCF-MC.

Prerequisiti:

1. L'access point deve avere due schede radio Wlan1/Wlan2 (es. W788-2 M12).
2. I canali utilizzati per le schede DATA INTERFACE e MANAGEMENT INTERFACE devono operare nella medesima banda (2.4GHz o 5GHz)
3. La copertura WiFi delle due schede wlan deve essere la medesima.
È sconsigliato, per esempio, l'impiego di antenne direttive che rischiano di separare le due celle radio, (Wlan1 e Wlan2 devono condividere la stessa area wifi).
4. Il canale dedicato alla scheda wlan MANAGEMENT INTERFACE deve essere uguale su tutti gli AP
5. Il canale dedicato alla scheda wlan DATA INTERFACE deve essere diverso per ogni AP.
6. I canali ad uso outdoor soggetti alla funzione DFS non devono essere utilizzati come MANAGEMENT INTERFACE.
7. Il client non può operare in modalità USE ALLOWED CHANNELS ONLY.

Abilitate la funzione iPCF-MC o iPCF-MC LF.

industrial Point Coordination Function with Management Channel (iPCF-MC)

Enable iPCF-MC

Legacy Free (iPCF-MC-LF)

iPCF Cycle Time [ms]: 32

Protocol Support: PROFINET

Set Values Refresh

Cosa differenzia le due opzioni?

La versione iPCF-MC è utile nel caso in cui stiate inserendo i nuovi dispositivi scalance W in una rete wifi preesistente, costituita dalla versione precedente di questa gamma di prodotti.

La funzione iPCF-MC impone che il protocollo attivo sul dispositivo sia la versione 802.11a.

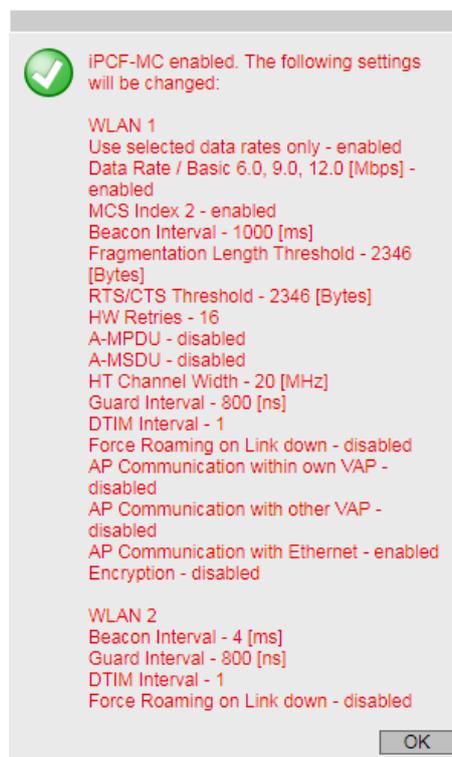
La versione LF, Legacy Free, vi torna utile nei casi in cui la vostra rete wifi è costituita da client e access point della nuova serie (versione 'n').

La versione Legacy Free funziona sia con il protocollo 'a' che 'n'.

La principale caratteristica del LF è quella di ottimizzare le comunicazioni Profinet/safe con il protocollo 'n'.

Ricordatevi, tuttavia, di utilizzare questo protocollo solo nel caso in cui avete collegato, ai dispositivi, più antenne.

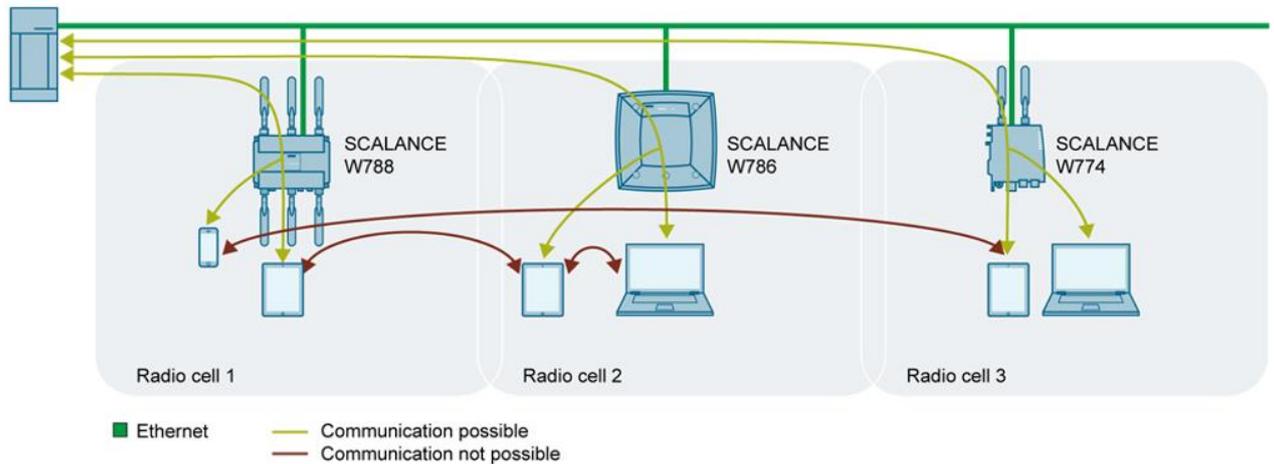
Quando abiliterete la funzione iPCF-MC vi apparirà questo pop-up che riassume le limitazioni che verranno introdotte dopo l'attivazione.



Le limitazioni fondamentali sono:

1. La limitazione ad un baud rate di 12Mbps.
2. Le comunicazioni intracella

Il punto 2, in particolare, descrive il fatto che i nodi collegati a valle di un client non possono comunicare, direttamente, con altri dispositivi collegati ad altri client.



Questa limitazione, tuttavia, si può disabilitare (vedi tutorial relativo alla sicurezza della rete wifi).

Impostate un tempo di scansione della vostra rete wifi.

SIEMENS

192.168.44.95/AP_Lab_7882M12

Welcome admin [Logout](#)

industrial Point Coordination Function with Management Channel (iPCF-MC)

Enable iPCF-MC
 Legacy Free (iPCF-MC-LF)

iPCF Cycle Time [ms]: 32

Protocol Support: 32 NET

iFeatures
 ▶ iPCF
 ▶ iPCF-HT
 ▶ **iPCF-MC**
 ▶ iPRP
 ▶ iREF
 ▶ AeroScout

Rispettate le seguenti regole per definire la base dei tempi per lo iPCF Cycle Time:

1. Fino a 10 client, 32 ms.
2. Dai 10 ai 20 client, 64 ms.
3. Dai 20 ai 30 client, 128 ms (Info→stimate indicativamente il traffico di rete).
4. Dai 30 ai 50 client, 256 ms (Warning→ valutate **bene** il traffico di rete).
5. Oltre, 512 ms (Alert→valutate **molto attentamente** il traffico di rete).

Il valore che assegnerete a questo parametro determinerà il tempo di aggiornamento hw dei nodi collegati a valle del client e, nel caso di comunicazione Profisafe, il tempo di monitoraggio del protocollo di sicurezza (f_monitoring_time).

Esempio:

tempo aggiornamento = iPCF cycle time x 2
 watchdog = tempo aggiornamento x 3 o 4 tentativi

iPCF cycle time = 32 ms
 tempo aggiornamento dei nodi collegati al client = 64 ms
 watchdog = 192ms (per 3 tentativi) 256 ms (per 4 tentativi)

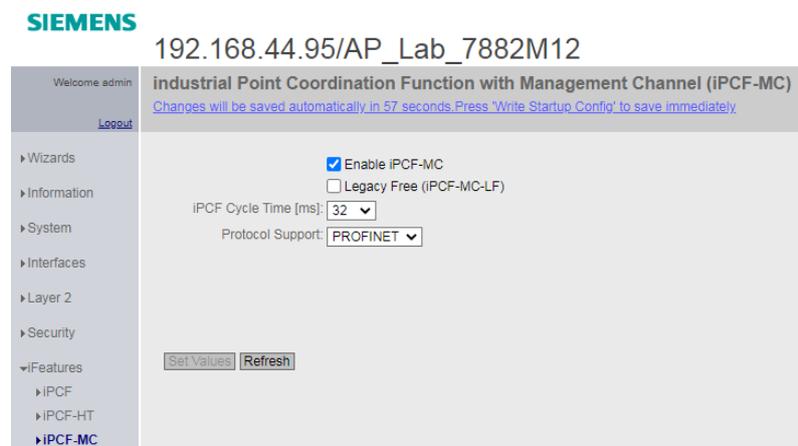
Se avrete anche la parte safety nel vostro progetto, dovrete calcolare il valore da assegnare al parametro f_monitorin_time in questo modo:

f_monitoring_time = watchdog x 3

Significherebbe impostare un f_monitoring_time pari a 576ms, nel caso in cui il watchdog è pari a 192ms, mentre aumenterà a 768ms, nel caso in cui il watchdog è pari a 256ms. Questo significa che, nel caso peggiore, l'evento di emergenza, per esempio la pressione di un fungo, verrebbe segnalato dopo 576 ms o 768ms.

Se, per qualunque motivo, dovrete modificare un qualsiasi valore coinvolto nelle relazioni appena descritte dovrete, conseguentemente, aggiornare anche i tempi a valle di quello modificato.

Premete il tasto SET VALUE.



Per velocizzare il salvataggio delle impostazioni cliccate sul link posto nella parte superiore della pagina. La pagina web verrà aggiornata e vi riporterà direttamente alla possibilità di salvare le nuove impostazioni, attraverso il pulsante WRITE STARTUP CONFIG



192.168.44.95/AP_Lab_7882M12

Welcome admin [Logout](#)

System Configuration
Changes will be saved automatically in 27 seconds. Press 'Write Startup Config' to save immediately.

- Telnet Server
Telnet Port: 23
- SSH Server
SSH Port: 22
- HTTP Server
HTTP Port: 80
- HTTPS Server
HTTPS Port: 443
- HTTP Services:
- Minimum TLS Version:
- DNS Client
- SMTP Client
- Syslog Client
- DCP Server:
- Time:
- SNMP:
 - SNMPv1/v2 Read-Only
 - SNMPv1 Traps
 - DHCP Client
 - DHCPv6 Client
 - SINEMA Configuration Interface
- Configuration Mode:

Noterete che, attivata la funzione iPCF-MC, molti parametri del dispositivo non sono più modificabili (es. SSID WLAN 2).
 Potete selezionare soltanto i canali delle due schede wlan.

Vi ricordo che la scheda Wlan1 dedicata ai dati dovrà essere diversa per ogni AP mentre la Wlan 2, dedicata al management channel dovrà essere uguale su tutti gli AP.



192.168.44.95/AP_Lab_7882M12

Welcome admin [Logout](#)

Access Point Settings

Basic | **Advanced** | Antennas | Allowed Channels | 802.11n | AP | AP WDS | AP 802.11a/b/g Rates | AP 802.11n Rates | Force Roaming | Spectrum Analyzer

Radio	Channel	Alternative DFS Channel	Channel Width [MHz]	Selected Channels	Selected Alternative DFS Channels
WLAN 1	44 (5220)	-	20	44 (5220 MHz)	-
WLAN 2	48 (5240)	-	20	48 (5240 MHz)	-

Radio Available Channels

Radio	Available Channels
WLAN 1	36,40,44,149,153,157,161,165
WLAN 2	36,40,48,149,153,157,161,165

Radio	Port	Enabled	SSID	Broadcast SSID	WDS only	WDS ID
WLAN 1	VAP 1.1	<input checked="" type="checkbox"/>	DATA NET	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 1	VAP 1.2	<input type="checkbox"/>	Siemens Wireless Network 1.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 1	VAP 1.3	<input type="checkbox"/>	Siemens Wireless Network 1.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 1	VAP 1.4	<input type="checkbox"/>	Siemens Wireless Network 1.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 1	VAP 1.5	<input type="checkbox"/>	Siemens Wireless Network 1.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 1	VAP 1.6	<input type="checkbox"/>	Siemens Wireless Network 1.6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 1	VAP 1.7	<input type="checkbox"/>	Siemens Wireless Network 1.7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 1	VAP 1.8	<input type="checkbox"/>	Siemens Wireless Network 1.8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 2	VAP 2.1	<input checked="" type="checkbox"/>	DATA NET	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 2	VAP 2.2	<input type="checkbox"/>	Siemens Wireless Network 2.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 2	VAP 2.3	<input type="checkbox"/>	Siemens Wireless Network 2.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 2	VAP 2.4	<input type="checkbox"/>	Siemens Wireless Network 2.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 2	VAP 2.5	<input type="checkbox"/>	Siemens Wireless Network 2.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 2	VAP 2.6	<input type="checkbox"/>	Siemens Wireless Network 2.6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 2	VAP 2.7	<input type="checkbox"/>	Siemens Wireless Network 2.7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
WLAN 2	VAP 2.8	<input type="checkbox"/>	Siemens Wireless Network 2.8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Warning: The approval process may not be finished in current country for channels denoted by a "*" character.
 Please check the following website for more detailed information:
<http://www.siemens.com/wireless-approvals>

Attivazione funzioni iPCF MC o iPCF MC LF sul client.
 Aprite il link: iFeature→iPCF MC

Management Scan Period

Questo parametro specifica il tempo tra due scansioni del management channel.
 Per esempio se si seleziona 2, il client esegue una scansione del management channel solo in ogni 2 cicli iPCF (iPCF cycle time).
 Un valore troppo basso per questo intervallo di scansione garantisce un roaming veloce ma, dall'altro lato, questo significa che non è possibile ottenere un elevato flusso di dati.
 Contrariamente un valore alto garantisce un flusso di dati maggiore.

Roaming Filter

Con questa impostazione si specifica il numero di campionamenti del valore RSSI utili a calcolare il valore della mediana.

Se il numero dei campioni è dispari, i valori campionati sono disposti in ordine ascendente.
 Il valore assegnato al RSSI è esattamente quello nel centro di campioni.

Es. 67-65-68-70-68

Mediana = 68

Se il numero dei campioni è pari, i valori campionati sono disposti in ordine ascendente.
 Il valore assegnato al RSSI è la media dei due numeri presenti nel centro della lista dei campioni.

Es. 67-65-68-70-68-66-67-64

Mediana = $(70 + 68) / 2$

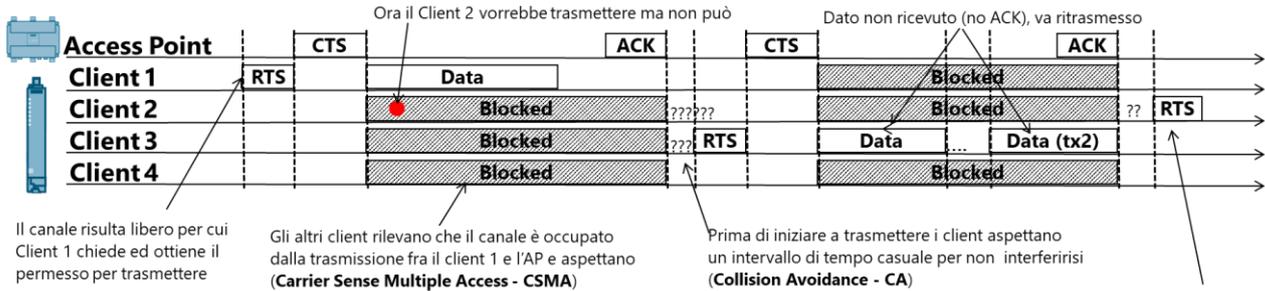
Questo metodo permette di filtrare eventuali forti fluttuazioni del segnale, migliorando l'intervento della fase di roaming da parte del client.

Eseguite il salvataggio delle impostazioni tramite il pulsante SET VALUE e seguite la medesima procedura descritta per l'access point per il salvataggio delle impostazioni.

iFeature. Come funziona iPCF?

Per comprendere l'utilità di questa funzione iniziamo a descrivere come una rete "standard" wifi gestisce il traffico ethernet tra access point e client.

WiFi Funzionamento classico con CSMA-CA e DCF



In questa situazione è impossibile stabilire a priori quando un client potrà trasmettere i propri dati
De facto **non è possibile avere una trasmissione deterministica** su più client

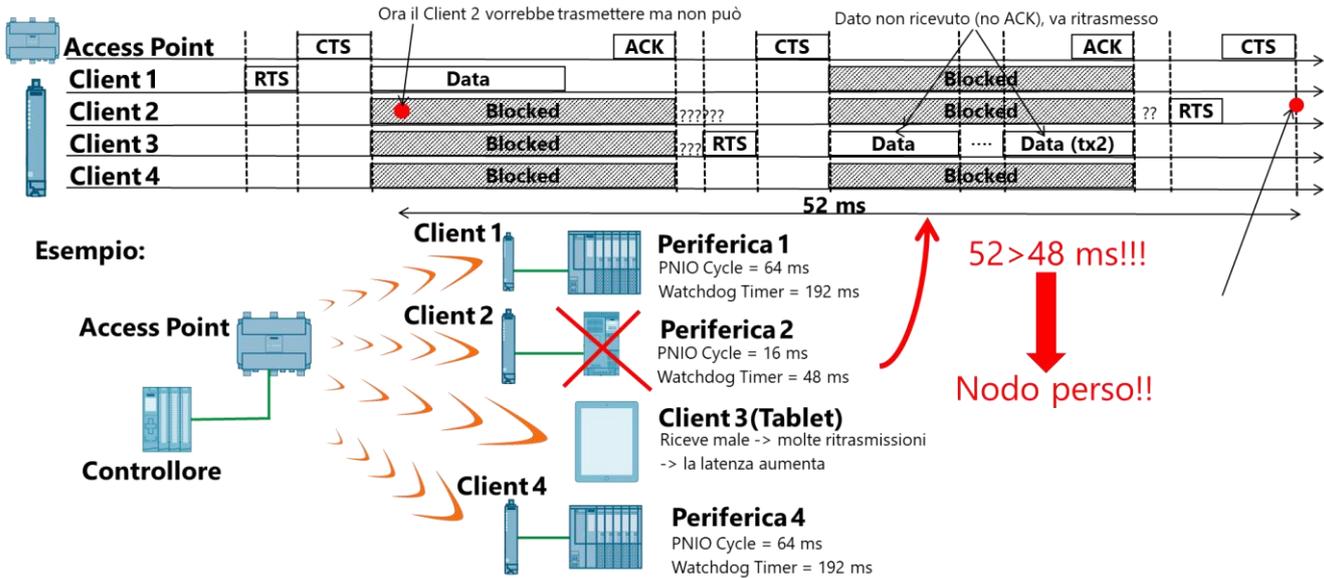
Questo sistema di gestione dei client è detto **DCF: Distributed Coordination Function**

↳ In pratica **sono i client stessi a coordinarsi e decidere quando parlare**

Legenda:
RTS=Request to Send
CTS=Clear To Send
ACK=Acknowledge

Ogni volta che un client comunica con il rispettivo access point, tutti i partecipanti della cella radio rimangono bloccati fin tanto che il client non terminerà la trasmissione dei dati all'access point.

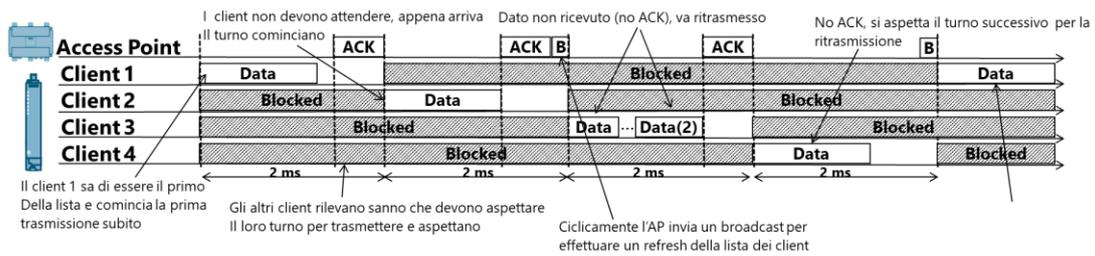
WiFi PNIO con DCF



Con una gestione simile il rischio di perdere dei nodi in una rete Profinet/safe, è molto elevata. Capite che le chiamate "random" dei vari client a contesa di banda, riduce notevolmente l'efficienza in una comunicazione Profinet/safe o Eth. IP.

La funzione iPCF (Industrial Point Coordination Function) nelle sue varie opzioni (HT, LF, ecc.) pone ordine nella gestione dei vari client collegati alla rete wifi.

iPCF Industrial Point Coordination Function



In questa situazione ogni client sa esattamente quando potrà trasmettere i propri dati. Per ciascuno di loro viene ciclicamente dedicato uno slot di tempo pari a 2 ms. In questo modo è possibile avere una trasmissione deterministica su più client

Questo sistema di gestione dei client è detto **iPCF: industrial Point Coordination Function**

In pratica è l'Access Point a stabilire quando i client possono parlare!

N.B.: iPCF è una feature proprietaria SIEMENS, client non-SIEMENS non possono comunicare con l'AP

L'access point registra e tiene costantemente aggiornato una propria MAC Table di tutti i client collegati alla propria cella radio.

Basandosi su questa lista di mac address effettua ciclicamente un polling di 2ms, affinché ogni client abbia il proprio slot temporale garantito per comunicare i dati Profinet/safe.

Oltretutto interviene anche in merito al roaming, la fase in cui un client si disconnette da una cella radio e si riconnette ad un altro access point.

Il roaming è un evento che avviene in qualsiasi rete wifi nella quale la topologia è costituita da più access point, utili a coprire un'area molto estesa.

DCF

Roaming standard: come avviene?



La criticità ricade nel fatto che i tempi di passaggio tra una rete e l'altra non sono certi e predeterminabili.

Questa incertezza non permette ad una rete wifi di poter coesistere con una comunicazione RT.

La funzione iPCF garantisce che l'evento di roaming si concluda indicativamente intorno a 50 ms.

Questa modalità, chiamata rapid roaming, permette di adeguare i tempi di disconnessione e riconnessione dei client tra le varie celle radio, in modo da poter gestire una comunicazione Profinet/safe e Eth. IP.

iPCF**Industrial Point Coordination Function: Rapid Roaming**

L'iPCF implementa una tecnica detta **"Rapid Roaming"** che necessita di un **massimo di 50 ms**.

Il client WLAN può rilevare errori di connessione molto rapidamente grazie a pacchetti specifici di polling. In questo modo riesce ad eseguire il roaming verso un altro AP in maniera molto più veloce.

"Rapid Roaming" basato su iPCF permette il funzionamento di applicazioni mobili senza interruzioni.

Riassumendo:

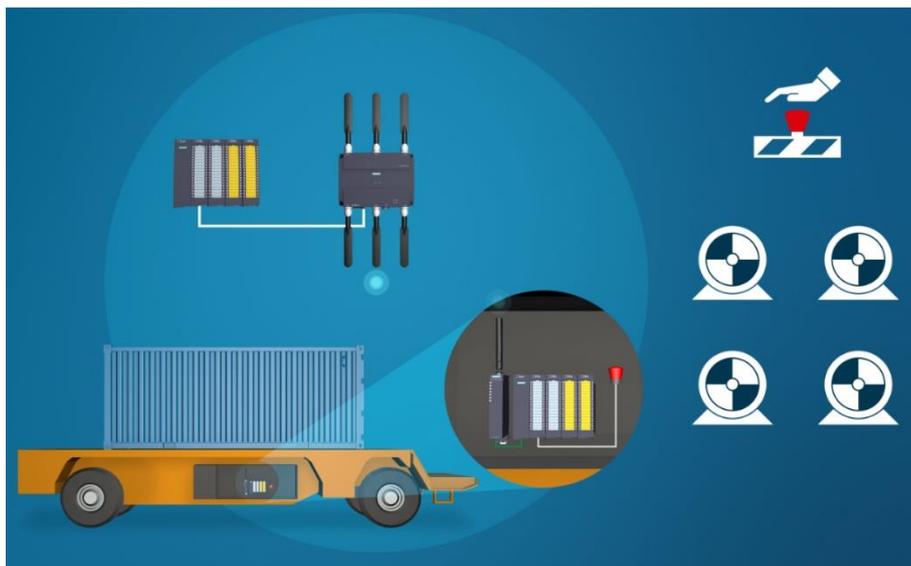
La funzione iPCF permette di garantire:

1. un polling predeterminato di tutti i client collegati alla rete wifi di uno specifico AP.
2. il rapid roaming. L'evento di disconnessione e riconnessione di un client entro i 50 ms

iFeature. Come funziona iPCF-MC?

Questa ulteriore evoluzione della funzione iPCF permette di ottimizzare ulteriormente la fase di roaming del client.

Vediamo nel dettaglio come funziona la versione MC (Management channel).



Per poter usufruire di questa funzione, dovrete acquistare un access point con doppia scheda radio. Una scheda wifi (WLAN 1) la dedicherete alla comunicazione dei dati (data channel, vedi immagine precedente) mentre la seconda (WLAN 2) sarà dedicata alla funzione di roaming (management channel).

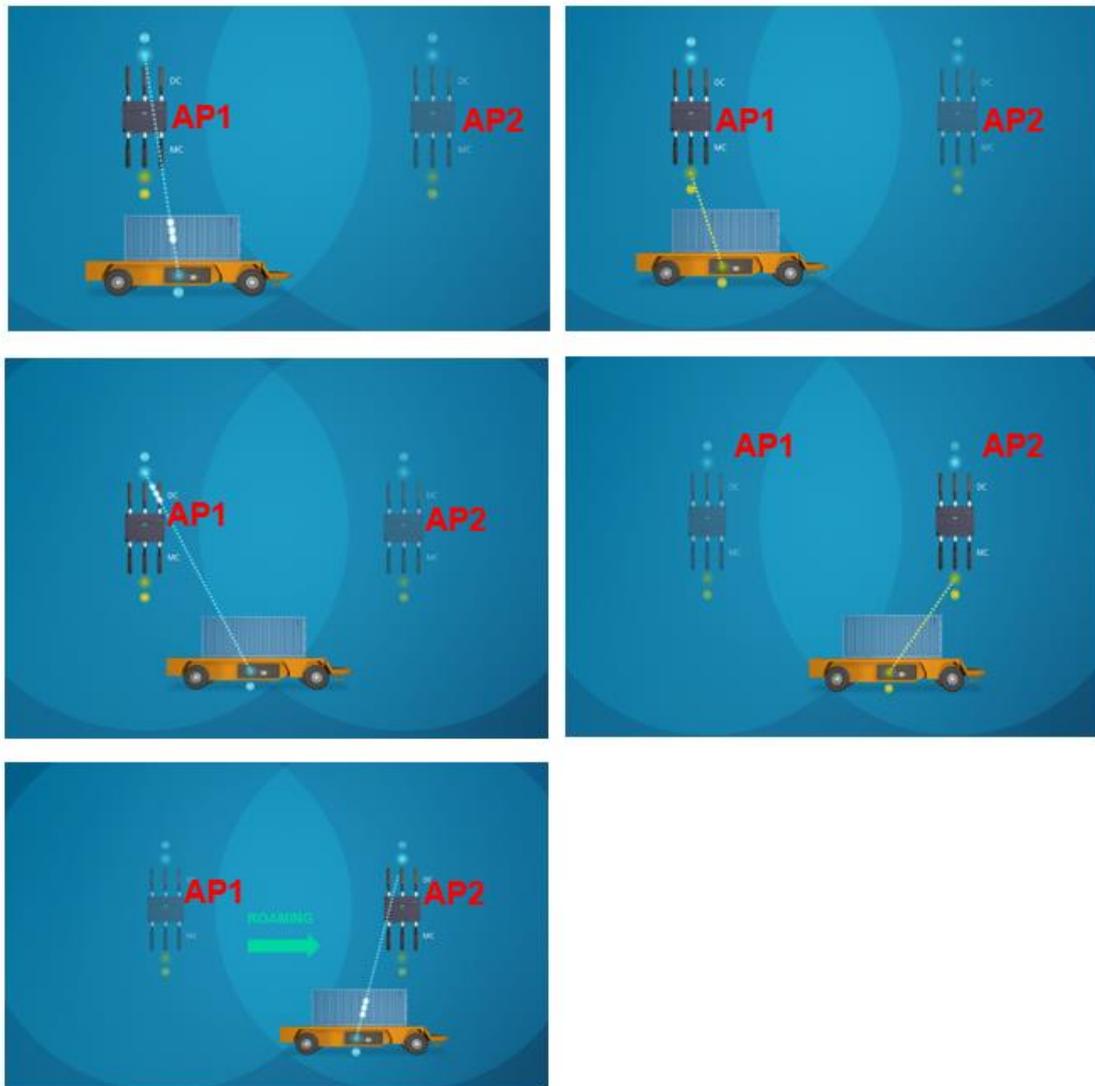
L'access point, attraverso il management channel, invia costantemente dei dati ai client che sono sintonizzati, in quel momento, su questo canale.

In questi messaggi i client possono determinare la qualità del servizio WiFi. Il client ovviamente ha una sola scheda di rete, tuttavia si sintonizzerà su questo canale a seconda del carico di dati che dovrà trasmettere sul data channel. Ovviamente, il client non sarà sempre e costantemente impegnato in questa attività.

Ad interrupt si metterà in ricezione sul management channel ed in funzione delle varie informazioni che riceverà dai vari access point che riuscirà a ricevere in quel punto, determinerà se attivare o meno il roaming.

In poche parole, il client effettua il roaming basandosi sulla qualità del servizio WiFi offerto dai vari access point che è in grado di captare in quello specifico e momento ed area.

Qui di seguito la sequenza appena descritta (DC data channel, MC management channel).



Riassumendo:

La funzione iPCF-MC ottimizza la fase di roaming, finalizzando l'attivazione della disconnessione del client da un AP verso un altro, solo nel caso in cui quest'ultimo è in grado di fornire un servizio migliore.

La modalità iPCF, per farvi capire, basa l'attivazione o meno del roaming utilizzando il fattore tempo. Viene monitorato costantemente un tempo di interrogazione tra client e AP.

Se questo tempo eccede il timeout, il client è autorizzato a ricercare e a collegarsi verso un altro AP.

iFeature. Tip&Tricks iPCF-MC.

Come devo installare le antenne?

Bisogna garantire che le antenne collegate alla scheda Wlan 1 e 2 dedicate rispettivamente al canale Management e Data, siano in vista tra loro in modo da garantire che le due celle radio condividano la medesima area WiFi.

Non orientate le antenne in modo differente.

Per esempio, il fissaggio essere identico per entrambe le antenne della Wlan 1 e 2.

In caso contrario il funzionamento del protocollo iPCF-MC potrebbe risentire di un deterioramento delle performance.

Qui sotto alcuni esempi di come installare le antenne:





Roaming Threshold

È importante capire che il roaming threshold funziona in modo diverso quando le funzioni iFeature sono abilitate. Le impostazioni che trovate nel menù a tendina, LOW/MEDIUM/HIGH, attivano il roaming quando la differenza tra il signal strenght tra due Management channel, eccede un certo valore come indicato nell'immagine qui sotto:

Client Settings					
Basic Advanced Antennas Allowed Channels 802.11n Client Signal Recorder Force Roaming					
Radio	MAC Mode	MAC Address	Any SSID	DHCP Renew After Roaming	min. AP Signal Strength [dBm]
WLAN 1	Automatic	00-00-00-00-00-00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
Radio	Roaming Threshold	Background Scan Mode	Background Scan Interval [ms]	Background Scan Threshold [dBm]	
WLAN 1	medium	idle	5000	0	
Radio	Scan Channels				
WLAN 1	1,2,3,4,5,6,7,8,9,10,11,12,13				

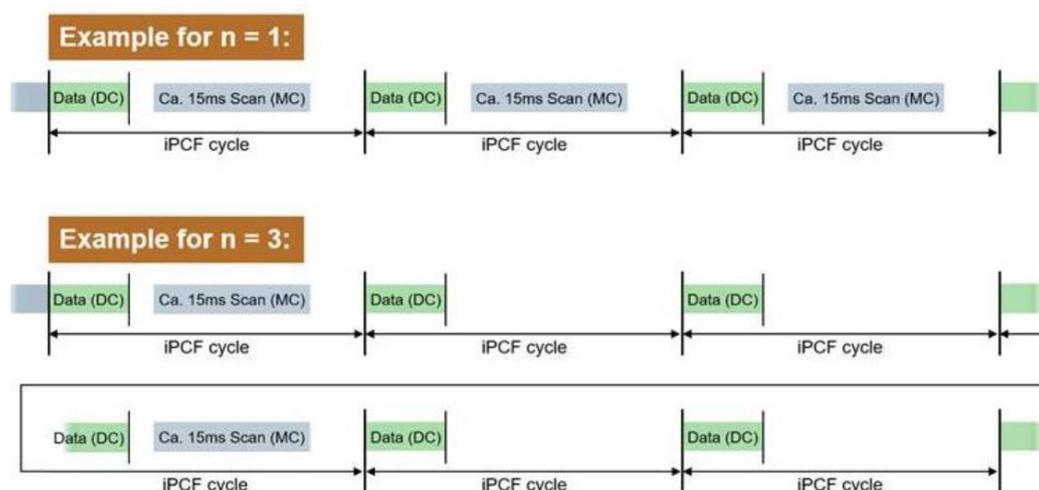
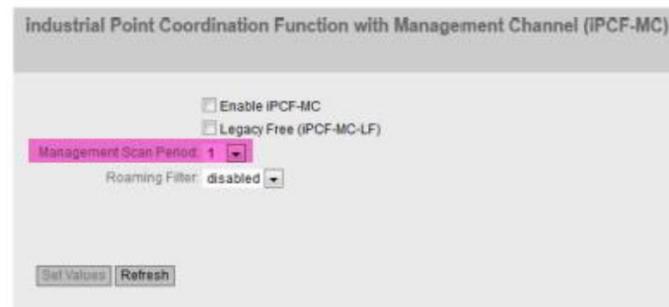
Roaming threshold	Own RSSI	RSSI difference	Notes
Low	35	13	If the MC of its own AP drops below RSSI 35, the new AP must be at least 13 dB better → The client will roam earlier
Medium	30	10	If the MC of its own AP drops below RSSI 30, the new AP must be at least 10 dB better
High	25	7	If the MC of its own AP drops below RSSI 25, the new AP must be at least 7 dB better → The client will roam later

Il valore di default è MEDIUM. Se si desidera che il client permanga il più possibile collegato all'access point, impostare questa soglia al valore HIGH.

Se, contrariamente, si preferisce che nel momento in cui un access point possa fornire un servizio wireless, per quanto leggermente migliore, rispetto a quello ai cui il client è collegato, allora selezionate LOW. Noterete che il client cambierà più velocemente e più frequentemente la connessione verso altri access point.

Management Scan Period.

Questo parametro vi permette di definire con quale frequenza il client deve interrogare il canale MANAGEMENT per attuare, nel caso, il roaming. Se l'efficienza del roaming è maggiore del data throughput allora dovrete impostare un valore basso.



Noterete che con il valore impostato ad uno, la scansione del MANAGEMENT channel avviene ad ogni invio di dati all'interno del IPCF cycle time.

Con un valore leggermente più alto, favorite il data throughput evitando una continua interrogazione del MANAGEMENT channel.

Roaming Filter.

Il filtro roaming è un ottimo strumento per sopprimere i disturbi o il roaming prematuro causati da un valore anomalo del signal strength rilevato sul MANAGEMENT channel.

Se il segnale è soggetto a pesanti fenomeni di riflessioni, attenuazione o altri fattori causati dall'ambiente in cui opera la cella radio, l'intensità ricevuta può subire dei forti sbalzi o disuniformità nel tempo.

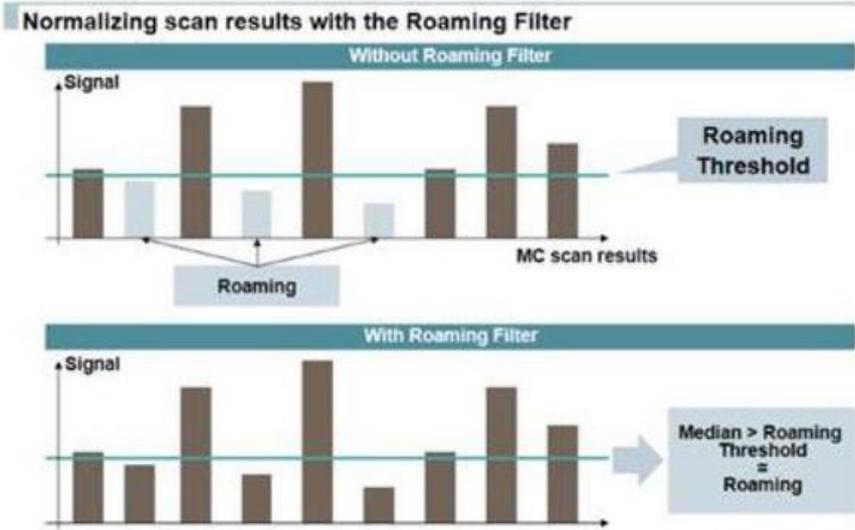
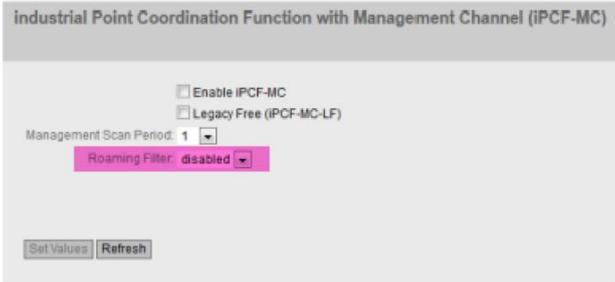
Senza questa funzione, una volta rilevata l'intensità del segnale di un canale MGT, il client decide immediatamente se effettuare il roaming o meno secondo il procedimento appena descritto nelle pagine precedenti.

Se questo valore rilevato è un valore estremo, determinato da fenomeni fisici legati alla propagazione delle onde radio nell'ambiente (es. riflessioni, rifrazione, ect.) allora l'attivazione del roaming potrebbe essere inutile e poco efficace.

Ad esempio.

Se impostiamo un valore pari a 5, il client camperà 5 valori del segnale e calcolerà la mediana di questi 5 valori per valutare se attivare o meno il roaming.

La mediana viene calcolata ogni 5 campionamenti dopo di che questo insieme numerico, viene cancellato a favore di altri nuovi 5 campioni e via di seguito.



Si tenga presente, tuttavia, che il filtro di roaming (quando abilitato), è correlato al periodo di scansione MGT (Management Scan Period.).

Ad esempio, se si esegue la scansione dei canali MGT ogni 5 cicli IPCF-MC con il filtro di roaming impostato a 5, allora sarà $5 \times 5 = 25$ IPCF-MC cicli prima che il client prenda la decisione di effettuare un roaming.

Con riserva di modifiche e salvo errori.

Il presente documento contiene solo descrizioni generali o informazioni su caratteristiche non sempre applicabili, nella forma descritta, al caso concreto o che possono cambiare a seguito di un ulteriore sviluppo dei prodotti. Le caratteristiche desiderate sono vincolanti solo se espressamente concordate all'atto di stipula del contratto.

Tutte le denominazioni dei prodotti possono essere marchi oppure denominazioni di prodotti della Siemens AG o di altre ditte fornitrici, il cui utilizzo da parte di terzi per propri scopi può violare il diritto dei proprietari.