# CommView® for WiFi

**Strumento di analisi e monitoraggio delle reti wireless per MS Windows**

# Documentazione della Guida

# Introduzione

## Informazioni su CommView for WiFi

**CommView for WiFi** rappresenta un'edizione speciale di CommView ed è stato progettato per la cattura e l'analisi dei pacchetti nelle reti 802.11a/b/g. CommView for WiFi raccoglie le informazioni dalla scheda di rete wireless e quindi decodifica i dati analizzati.

CommView for WiFi consente di visualizzare l'elenco delle connessioni di rete e delle statistiche IP più importanti ed esaminare i singoli pacchetti. È possibile decifrare i pacchetti mediante le chiavi WEP o WPA-PSK definite dall'utente e decodificarli fino al livello inferiore con l'analisi completa dei protocolli più diffusi. È supportato l'accesso completo ai dati non elaborati e il salvataggio dei pacchetti catturati nei file di registro per l'analisi successiva. Un sistema flessibile di filtri consente di eliminare i pacchetti non necessari oppure di catturare solo quelli indispensabili. È possibile configurare la visualizzazione dei messaggi di avviso al verificarsi di eventi importanti, ad esempio in caso di pacchetti sospetti, l'utilizzo di un elevata ampiezza di banda o di indirizzi sconosciuti.

CommView for WiFi supporta la decodifica dei protocolli seguenti: ARP, BCAST, BGP, BMP, CDP, DAYTIME, DDNS, DHCP, DIAG, DNS, EIGRP, FTP, G.723, GRE, H.225, H.261, H.263, H.323, HTTP, HTTPS, ICMP, ICQ, IGMP, IGRP, IMAP, IPsec, IPv4, IPv6, IPX, HSRP, LDAP, MS SQL, NCP, NDS, NetBIOS, NFS, NLSP, NNTP, NTP, OSPF, POP3, PPP, PPPoE, RARP, RADIUS, RDP, RIP, RIPX, RMCP, RPC, RSVP, RTP, RTCP, RTSP, SAP, SER, SIP, SMB, SMTP, SNA, SNMP, SNTP, SOCKS, SPX, SSH, TCP, TELNET, TFTP, TIME, TLS, UDP, VTP, WAP, WDOG, YMSG, 802.1Q, 802.1X.

CommView for WiFi è lo strumento ideale per gli amministratori WLAN, i professionisti della sicurezza, i programmatori di rete o tutti coloro che desiderano controllare il proprio traffico WLAN a 360 gradi. L'applicazione può essere eseguita in Windows 2000/XP/2003 mediante l'utilizzo di una scheda di rete wireless compatibile. Per l'elenco delle schede di rete supportate, visitare il nostro Sito Web.

# Novità

**Versione 5.1**

- Supporto di molte nuove schede: PC card wireless a/b/g 3Com OfficeConnect (3CRWE154A72), scheda cardbus wireless D-Link AirPlus G DWL-G630 (Rev. C), scheda PCI wireless D-Link AirPremier DWL-AG530, PC card wireless NETGEAR WG511U Double 108 Mbps.
- Driver aggiornato per garantire la compatibilità con le versioni più recenti di numerose schede D-Link.
- Correzione dei bug minori correlati all'acquisizione di file importati/esportati e alla decodifica dei protocolli.

**Versione 5.0**

- Scansione proattiva mediante i pacchetti PROBE REQUEST (è richiesta una scheda basata sul chipset Atheros).
- Packet Generator ora disponibile (è richiesta una scheda basata sul chipset Atheros).
- Nuove regole avanzate che consentono di filtrare i pacchetti in base ai tipi e ai sottotipi di frame, al numero di tentativi, alla durata e così via.
- Timestamp ad alta risoluzione (fino ai microsecondi).
- Nuovo formato di registro aperto e compatto.
- Matrici grafiche per la rappresentazione delle conversioni tra gli host.
- Aggiunta di nuovi moduli di decodifica, decodifica MS SQL, LDAP, YMSG. SMB e ICQ migliorata.
- Supporto di grafici nei report HTML.
- Nuovi tipi di avvisi.
- Minor utilizzo della CPU.

**Versione 4.2**

- Nuove schede Nodi e Canali con statistiche dettagliate in base al singolo nodo o canale: velocità di trasferimento dei dati, intensità del segnale, errori ICV e CRC e così via.
- Decifratura in fase di esecuzione dei pacchetti cifrati con la tecnologia WAP in modalità Pre-Shared Key (PSK): si tratta di una funzione esclusiva non disponibile negli altri strumenti di analisi di reti wireless.
- Notevoli miglioramenti alle prestazioni che consentono il monitoraggio delle risorse WLAN più utilizzate e la decifratura del traffico in fase di esecuzione senza occupare il 100% del tempo della CPU.
- Aggiunta di un avviso in caso di rilevamento di AP inaffidabili.
- Nuove versioni di driver per una migliore stabilità.

**Versione 4.1**

- Il programma supporta ora le schede wireless 802.11g e 802.11a.
- Funzionalità di scansione migliorata.
- Possibilità di registrare gli URL visitati.
- Nuovi moduli di decodifica dei protocolli: IMAP, NNTP, SSH, TLS.
- Interfaccia plug-in aperta per implementare la decodifica del proprio protocollo.
- Finestre di ricostruzione delle sessioni TCP che supportano ora la decompressione del contenuto Web GZIP'd e la visualizzazione delle immagini inviate con le sessioni HTTP.
- Finestre di ricostruzione delle sessioni TCP che consentono di passare alla sessione TCP successiva tra due host qualsiasi, nelle versioni precedenti era possibile passare alla sessione successiva solo tra i due host inizialmente selezionati.
- Supporto della generazione automatica di statistiche relative ai dati pre-acquisiti oltre alle statistiche in tempo reale.
- Funzioni di avviso migliorate che consentono di passare le variabili alle applicazioni avviate o ai messaggi di avviso.
- Numerosi altri miglioramenti minori.

# Contratto di licenza

Leggere attentamente i termini e le condizioni seguenti prima di utilizzare il software. L'utilizzo di questo software implica l'accettazione dei termini del presente Contratto di licenza. Se non si accettano le condizioni del presente Contratto di licenza, è necessario rimuovere il software dalle periferiche di memorizzazione e sospendere l'utilizzo del prodotto.

**Copyright**
Questo software è protetto da copyright 1999-2005 da TamoSoft. CommView è un marchio registrato di TamoSoft. L'utilizzo e il copyright di questo software sono governati dalle leggi internazionali sul copyright. TamoSoft detiene completamente i titoli di proprietà e i diritti su questo software e sulla relativa documentazione e la concessione di licenza non diminuisce in alcun modo i diritti di proprietà intellettuale di TamoSoft. È vietata la ridistribuzione dei codici di registrazione forniti nei formati cartaceo, elettronico o di qualsiasi altro tipo.

**Versione di valutazione**
Questo software non è gratuito. L'utente è autorizzato a utilizzare questo software a scopo di valutazione per un periodo di 30 giorni. L'utilizzo di questo software dopo la scadenza del periodo di valutazione rappresenta una violazione delle leggi sul copyright perseguibile penalmente e civilmente.

**Versione registrata (in licenza)**
Una copia registrata di questo software può essere utilizzata dalla singola persona che utilizza questo software personalmente su uno o più computer, oppure può essere installata su una singola workstation utilizzata non contemporaneamente da più di una persona ma non entrambe. È possibile installare questo software su un server di rete purché sia stata concessa da TamaSoft un'appropriata licenza distinta all'utilizzo del software per ciascun computer con accesso al software.

**Upgrade**
Il presente Contratto non concede alcun diritto a miglioramenti, aggiornamenti o upgrade per questo software (collettivamente "upgrade"). TamoSoft può o non può fornire, a propria discrezione, tali upgrade agli utenti con licenza. TamoSoft non garantisce la disponibilità di questi upgrade né garantisce che tali upgrade forniscano miglioramenti conformemente agli ultimi standard di settore, inclusi in via esemplificativa, le nuove periferiche hardware, i protocolli di rete o gli algoritmi di cifratura.

**Dichiarazione di non responsabilità**
TAMOSOFT NON GARANTISCE CHE IL PRODOTTO SIA PRIVO DI ERRORI. IL SOFTWARE VIENE FORNITO NEL FORMATO "ATTUALE" SENZA GARANZIE DI ALCUN TIPO, IMPLICITE O ESPLICITE, INCLUSI IN VIA ESEMPLIFICATIVA, GARANZIA DI COMMERCIABILITÀ O IDONEITÀ PER UNO SCOPO PARTICOLARE. TAMOSOFT NON SARÀ IN ALCUN CASO RESPONSABILE PER DANNI DI QUALSIASI TIPO, INCLUSI I DANNI INCIDENTALI O CONSEQUENZIALI, DERIVANTI DALL'UTILIZZO DI QUESTO SOFTWARE, ANCHE SE AVVISATI DELLA POSSIBLITÀ DI TALI DANNI. L'UTENTE DICHIARA DI AVER PRESO VISIONE DEL SEGUENTE CONTRATTO E DI ACCETTARNE I TERMINI.

**Legislazione di riferimento**
Questo Contratto è governato dalle leggi della Nuova Zelanda.

**Distribuzione**
Questo software può essere distribuito liberamente nel suo formato non modificato e non registrato. La distribuzione deve includere tutti i file della distribuzione originale senza che i distributori addebitino alcun importo. Tutti coloro che distribuiscono questo software per uno scopo renumerativo qualsiasi devono innanzitutto contattarci per ottenere l'autorizzazione.

**Altre restrizioni**
Non è possibile modificare, decodificare, decompilare o disassemblare questo software in alcun modo, inclusi la modifica o la rimozione di messaggi o finestre.

# Utilizzo del programma

## Installazione del driver

CommView for WiFi è uno strumento che consente di monitorare il traffico delle reti 802.11a/b/g wireless. Per utilizzare questo prodotto, è **necessario** disporre di una scheda wireless compatibile. Per abilitare le funzioni di monitoraggio della scheda wireless, è necessario il driver specifico fornito in dotazione. Qualora fosse già installata una scheda, sostituire il driver originale di tale scheda con quello nuovo. Se invece sul computer non è ancora installata alcuna scheda, installarla mediante il driver fornito in dotazione. Il presente manuale rappresenta una guida al processo di installazione.

Dopo aver sostituito il driver, è possibile che la scheda non sia più in grado di comunicare con gli altri punti di accesso oppure host wireless perché il driver utilizza una modalità di monitoraggio passivo. Per ripristinare le funzioni standard della scheda, è necessario eseguire il roll back o ripristinare il driver originale fornito con la scheda. Tuttavia, in base al modello della scheda e al sistema operativo in uso potrebbe essere possibile utilizzare il driver in modalità doppia (passiva quando CommView for WiFi è in esecuzione e attiva quando CommView for WiFi non è in esecuzione). Per scoprire se è possibile utilizzare la modalità doppia con il sistema in uso, vedere le note tecniche. In caso negativo, può essere opportuno mantenere la propria connessione wireless durante l'utilizzo del prodotto e prendere in considerazione l'alternativa di installare due schede wireless: una per il monitoraggio e l'altra per l'esecuzione delle funzioni di rete standard.

Prima di installare il nuovo driver per la scheda wireless, accertarsi che la scheda in uso sia compatibile con il prodotto. L'elenco delle schede compatibili è disponibile nell'URL seguente:

http://www.tamos.com/products/commwifi/

CommView for WiFi può supportare anche altre schede. Se la scheda in uso non è riportata nell'elenco, leggere le informazioni aggiornate nel capitolo Domande frequenti.

Per istruzioni dettagliate e con illustrazioni, avviare il programma, quindi fare clic su **? => Guida all'installazione del driver** nel menu del programma e scorrere fino alla parte inferiore della finestra.

# Panoramica

L'interfaccia del programma è costituita da 5 schede che consentono di visualizzare i dati e di elaborare i pacchetti acquisiti. Per iniziare ad acquisire i pacchetti, fare clic sul pulsante **Avvia acquisizione** oppure scegliere **File = > Avvia acquisizione** dal menu.

**Menu principale**

### File

**Avvia/Interrompi acquisizione:** avvia o sospende l'acquisizione dei pacchetti.
**Sospendi/Riprendi output pacchetti**: sospende o riprende l'output dei pacchetti in tempo reale sulla 4° scheda.
**Salva nodi come**: salva il contenuto della scheda Nodi.
**Salva canali come**: salva il contenuto della scheda Canali.
**Salva ultime connessioni IP come**: salva il contenuto della scheda Ultime connessioni IP.
**Salva registro pacchetti come**: salva il contenuto della scheda Pacchetti in diversi formati. Per opzioni di salvataggio avanzate, utilizzare la scheda Connessione.
**Visualizzatore registro:** apre una nuova finestra Visualizzatore registro.
**Cancella nodi:** cancella il contenuto della tabella Nodi (1° scheda).
**Cancella canali:** cancella il contenuto della tabella Canali (2° scheda).
**Cancella ultime connessioni IP:** cancella il contenuto della tabella Ultime connessioni IP (3° scheda).
**Cancella buffer pacchetti:** cancella il contenuto della memoria buffer del programma e l'elenco dei pacchetti (4° scheda).
**Dati prestazioni**: mostra le statistiche sulle prestazioni del programma, ad esempio il numero di pacchetti acquisiti e ignorati dal driver della periferica.
**Esci:** chiude il programma.

### Cerca

**Trova pacchetto:** mostra una finestra di dialogo che consente di trovare i pacchetti che corrispondono a un testo specifico.
**Vai a numero di pacchetto**: mostra una finestra di dialogo che consente di spostarsi sul pacchetto con il numero specificato.

### Visualizza

**Statistiche:** mostra una finestra contenente le statistiche sulla distribuzione dei protocolli e il trasferimento dei file.
**Riferimento porta:** mostra una finestra con le informazioni sul riferimento della porta.
**Directory registri:** apre la directory in cui vengono salvati i registri per impostazione predefinita.
**Colonne nodi:** mostra o nasconde le colonne nella scheda Nodi.
**Colonne canali:** mostra o nasconde le colonne nella scheda Canali.
**Colonne Ultime connessioni IP:** mostra o nasconde le colonne nella scheda Ultime connessioni IP.
**Colonne pacchetti:** mostra o nasconde le colonne nella scheda Pacchetti.

### Strumenti

**Packet Generator:** apre la finestra Packet Generator.
**Ricostruisci sessione TCP:** ricostruisce una sessione TCP a partire dal pacchetto selezionato. Verrà aperta una finestra che mostra l'intera conversazione tra i due host.
**Identificativo fornitore NIC:** apre una finestra che consente di identificare il fornitore della scheda di rete in base all'indirizzo MAC.
**Pianificatore:** aggiunge o rimuove le attività di acquisizione pianificate.

### Impostazioni

**Font:** mostra il sottomenu che consente di impostare i font per gli elementi di interfaccia.
**Chiavi WEP/WPA:** apre una finestra che consente di specificare le chiavi WEP/WPA.
**Alias MAC:** visualizza una finestra che consente di assegnare alias facili da ricordare agli indirizzi MAC.
**Alias IP:** visualizza una finestra che consente di assegnare alias facili da ricordare agli indirizzi IP.
**Opzioni:** visualizza la finestra Opzioni che consente di impostare ulteriori opzioni avanzate.
**Lingua:** consente di modificare la lingua di interfaccia. Accertarsi di riavviare il programma dopo aver modificato la lingua. Il pacchetto di installazione di CommView for WiFi può non contenere tutti i file di lingua disponibili per l'interfaccia. Fare clic sulla voce di menu **Altre lingue** per aprire la pagina di download delle altre lingue sul nostro sito Web e scaricare il file della lingua eventualmente disponibile per la versione corrente.

### Regole

**Acquisisci pacchetti di dati:** selezionare o deselezionare questa voce per abilitare o disabilitare rispettivamente l'acquisizione dei pacchetti del tipo "Dati".
**Acquisisci pacchetti di gestione:** selezionare o deselezionare questa voce per abilitare o disabilitare rispettivamente l'acquisizione dei pacchetti del tipo "Gestione".
**Acquisisci pacchetti di controllo:** selezionare o deselezionare questa voce per abilitare o disabilitare rispettivamente l'acquisizione dei pacchetti del tipo "Controllo".
**Ignora beacon:** selezionare o deselezionare questa voce per abilitare o disabilitare rispettivamente l'acquisizione dei pacchetti del tipo "Beacon."
**Salva regole correnti come:** consente di salvare la configurazione delle regole correnti in un file.
**Carica regole da:** consente di caricare da un file una configurazione di regole salvate in precedenza.
**Reimposta tutto:** cancella tutte le eventuali regole esistenti.

### ?

**Sommario:** avvia la Guida in linea di CommView.
**Cerca argomento ... :** mostra l'indice della Guida in linea di CommView.
**Guida all'installazione del driver... :** mostra le istruzioni dettagliate sull'installazione del driver.
**Informazioni su:** mostra le informazioni sul programma.

Quasi tutti gli elementi dell'interfaccia sono dotati di un menu sensibile al contesto richiamabile mediante il clic con il pulsante destro del mouse. Molti comandi sono disponibili solo mediante questi menu.

La prima scheda consente di visualizzare le stazioni e i punti di accesso attivi. Per ulteriori informazioni, vedere la sezione Nodi.

La seconda scheda consente di visualizzare le statistiche in base al canale. Per ulteriori informazioni, vedere la sezione Canali.

La terza scheda consente di visualizzare le informazioni dettagliate sulle connessioni della rete WLAN (solo protocollo IP). Per ulteriori informazioni, vedere la sezione Ultime connessioni IP.

La quarta scheda consente di visualizzare i pacchetti di rete acquisiti nonché le informazioni dettagliate sul pacchetto selezionato. Per ulteriori informazioni vedere la sezione Pacchetti.

La quinta scheda consente di salvare i pacchetti acquisiti nei file desiderati. Per ulteriori informazioni, vedere Connessione.

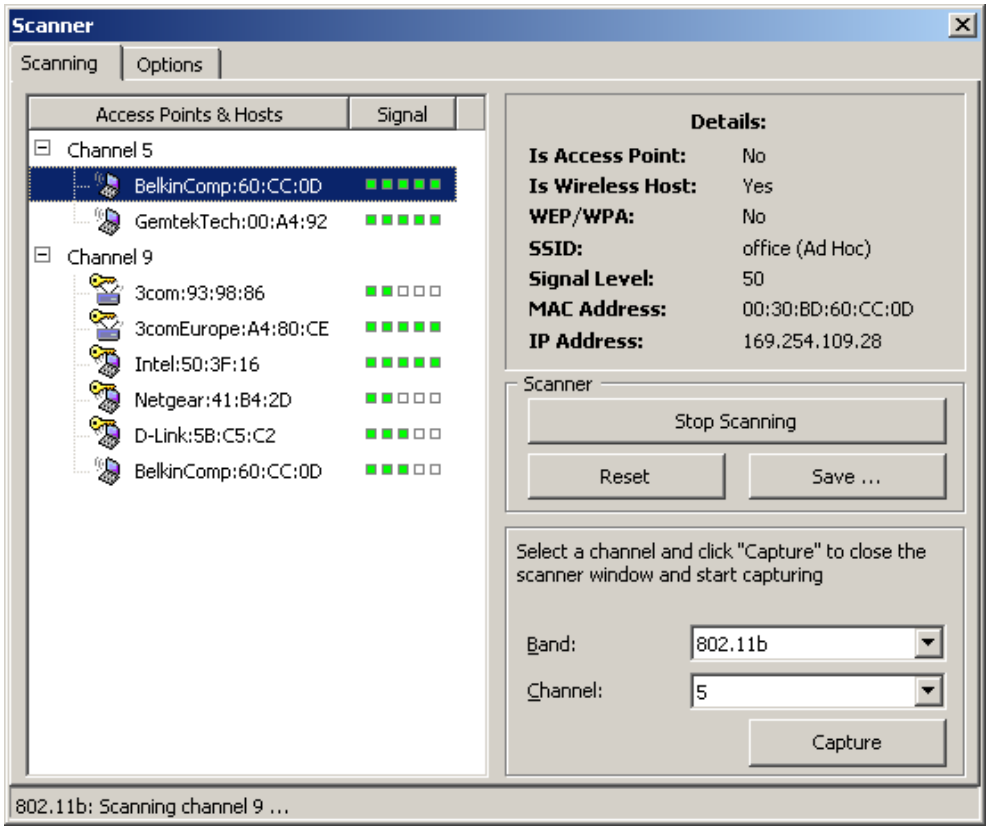
Le sesta scheda consente di configurare le regole per l'acquisizione o l'eliminazione dei pacchetti in base a vari criteri, ad esempio l'indirizzo IP o il numero di porta. Per ulteriori informazioni, vedere la sezione Regole.

La settima scheda consente di creare avvisi per la notifica di eventi importanti, ad esempio di pacchetti sospetti, dell'utilizzo di un elevata ampiezza di banda, di indirizzi sconosciuti e così via. Per ulteriori informazioni, vedere la sezione Avvisi.

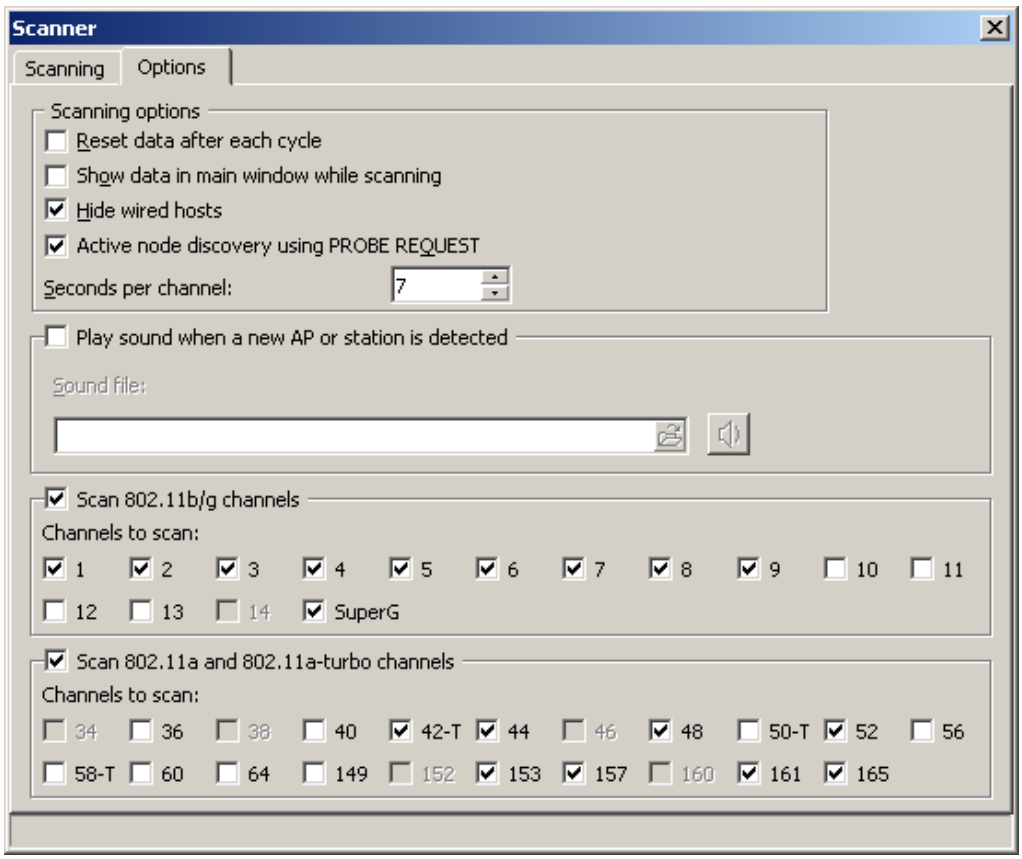
Per modificare alcune le impostazioni desiderate, ad esempio i font, i colori e la dimensione del buffer, scegliere Impostazioni dal menu. Per ulteriori informazioni, vedere la sezione Opzioni delle impostazioni.

# Scanner

La finestra Scanner consente di cercare i segnali WiFi e di selezionare un canale da monitorare. Per avviare il processo di scansione, è sufficiente fare clic sul pulsante **Avvia scansione**. Il processo di scansione è ciclico, ciò significa che il programma "ascolta" i segnali sul primo canale, quindi passa al canale successivo e così via fino all'ultimo canale per poi ripartire con un nuovo ciclo di scansione. Per interrompere il processo di scansione, è necessario fare clic su **Interrompi scansione**. Per cancellare i dati raccolti, selezionare **Reimposta**. Per salvare il report delle scansioni nel formato HTML, fare clic su **Salva**. Al termine del processo di scansione oppure se si conosce il canale sul quale si desidera vengano acquisiti i pacchetti, scegliere una banda dall'elenco a discesa **Banda** (802.11a, 802.11a-turbo e 802.11b/g in base alla scheda in uso), quindi selezionare un canale dall'elenco a discesa **Canale** e fare clic su **Acquisisci**.




La scheda **Opzioni** consente di configurare numerose opzioni di scansione. Le opzioni disponibili sono illustrate qui di seguito.




**Reimposta dati dopo ogni ciclo:** selezionare questa casella per fare in modo che tutti i dati raccolti dal programma vengano cancellati prima dell'avvio di un nuovo ciclo di scansione. Questa funzione ha i suoi pregi e suoi difetti. La reimpostazione dei dati consente di disporre di un'immagine sempre aggiornata delle comunicazioni via etere. Ad esempio, una stazione che non invia più dati non verrà più visualizzata nell'elenco. Tuttavia, anche se una determinata stazione rimane inattiva solo temporaneamente, vale a dire non invia dati per alcuni secondi in un minuto, non verrà comunque notata anche quando rileva un determinato canale e, inoltre, verrà rimossa dall'elenco.

**Mostra dati nella finestra principale durante scansione:** selezionare questa casella per fare in modo che i pacchetti in corso di scansione vengano visualizzati nella finestra principale del programma, in particolare nelle schede **Nodi, Canali, Pacchetti** e **Ultime connessioni IP**. Se la casella non è selezionata, i pacchetti acquisiti durante il processo di scansione non verranno visualizzati o registrati.

**Nascondi host cablati:** selezionare questa casella per fare in modo che vengano visualizzati solo i punti di accesso e gli host wireless. Se la casella non è selezionata, verranno visualizzati gli host con e senza fili nel segmento in corso di scansione. Si osservi che l'abilitazione di questa opzione può comportare a volte la mancata visualizzazione anche degli host wireless poiché per determinare se un host è di tipo cablato o wireless, è necessario acquisire numerosi pacchetti di dati.

**Rilevamento nodi attivi mediante PROBE REQUEST**: se questa casella è selezionata, verranno inviati periodicamente i pacchetti PROBE REQUEST i quali consentono di semplificare il rilevamento dei punti di accesso che non trasmettono i propri SSID. Si osservi che l'abilitazione di questa opzione può comportare la trasmissione di pacchetti da parte della scheda che quindi non risulterà più completamente nascosta. Questa impostazione non è disponibile per le schede precedenti alla 802.11b.

**Secondi per canale:** determina l'intervallo di ascolto dei dati su ciascun canale in corso di scansione.

**Riproduci suono al rilevamento di una nuova stazione o AP:s** selezionare questa casella e scegliere un file WAV per ricevere una notifica sui punti di accesso o le stazioni trovate. Per testare il file WAV selezionato, fare clic sul pulsante accanto al campo di selezione del file.

**Esegui scansione dei canali 802.11b/g** e **Esegui scansione dei canali 802.11a:** queste caselle di controllo consentono di selezionare i canali da analizzare. È necessario selezionare almeno un canale. Non tutti i canali visualizzati in questa finestra potrebbero essere supportati dalla scheda di rete wireless nel proprio paese. Se la scheda in uso non supporta un determinato canale, la casella corrispondente non sarà disponibile. Se la scheda in uso non supporta i canali 802.11a, anche la sezione **Esegui scansione dei canali 802.11a** non sarà disponibile. Se la scheda non supporta i canali 802.11g, la sezione **Esegui scansione dei canali 802.11b/g** assumerà il nome **Esegui scansione dei canali 802.11b**.

**Informazioni su SuperG e SuperAG**

SuperG/SuperAG è una tecnologia proprietaria di aumento della velocità effettiva introdotta da Atheros Communications e supportata da numerosi fornitori hardware (per ulteriori informazioni, visitare il sito: www.super-ag.com). SuperG/SuperAG utilizza i sistemi di bursting dei pacchetti, di "frame veloci", di compressione/decompressione dei dati in fase di esecuzione e di bonding a

doppio canale per offrire trasmissioni a una velocità fino a 108 Mbps. La scheda WLAN può funzionare correttamente o solo parzialmente in modalità SuperG/SuperAG in base all'hardware in uso. Generalmente, i dispositivi hardware abilitati alle tecnologie SuperG e SuperAG funzionano in diverse modalità: Super Mode senza Turbo, Super Mode con Static Turbo e Super Mode con Dynamic Turbo.

Quando si utilizza la banda 802.11g, la trasmissione dei dati in modalità Super con Static Turbo e modalità Super con Dynamic Turbo viene eseguita mediante il canale 6 802.11g. Tuttavia, se si seleziona il canale 6 802.11g per il monitoraggio, CommView for WiFi potrebbe non essere in grado di acquisire il traffico wireless. Questo perché per il monitoraggio è disponibile anche l'opzione SuperG che, se selezionata, consente di acquisire questo speciale tipo di frame. Il componente hardware può passare dinamicamente da una modalità all'altra in base al carico della rete e ad altri fattori, ostacolando il processo di monitoraggio.

Quando si utilizza la banda 802.11a,la trasmissione dei dati in modalità Super con Static Turbo e modalità Super con Dynamic Turbo viene eseguita mediante canali turbo speciali. Se la scheda utilizzata per il monitoraggio supporta la modalità turbo 802.11a, selezionare la banda e il canale appropriati negli elenchi a discesa. Questa modalità utilizza un gruppo distinto di canali, in particolare i canali 42, 50 e 58 corrispondono generalmente a canali turbo, mentre gli altri canali 802.11a sono di tipo non turbo. Esistono tuttavia eccezioni a questa regola, ad esempio in Giappone i canali 34, 38, 42 e 46 sono non turbo. Per poterli monitorare è quindi necessaria una build del driver specifica per questo paese. Per richiedere un driver per il Giappone o qualsiasi altro paese che utilizza gruppi di canali non standard, contattateci.

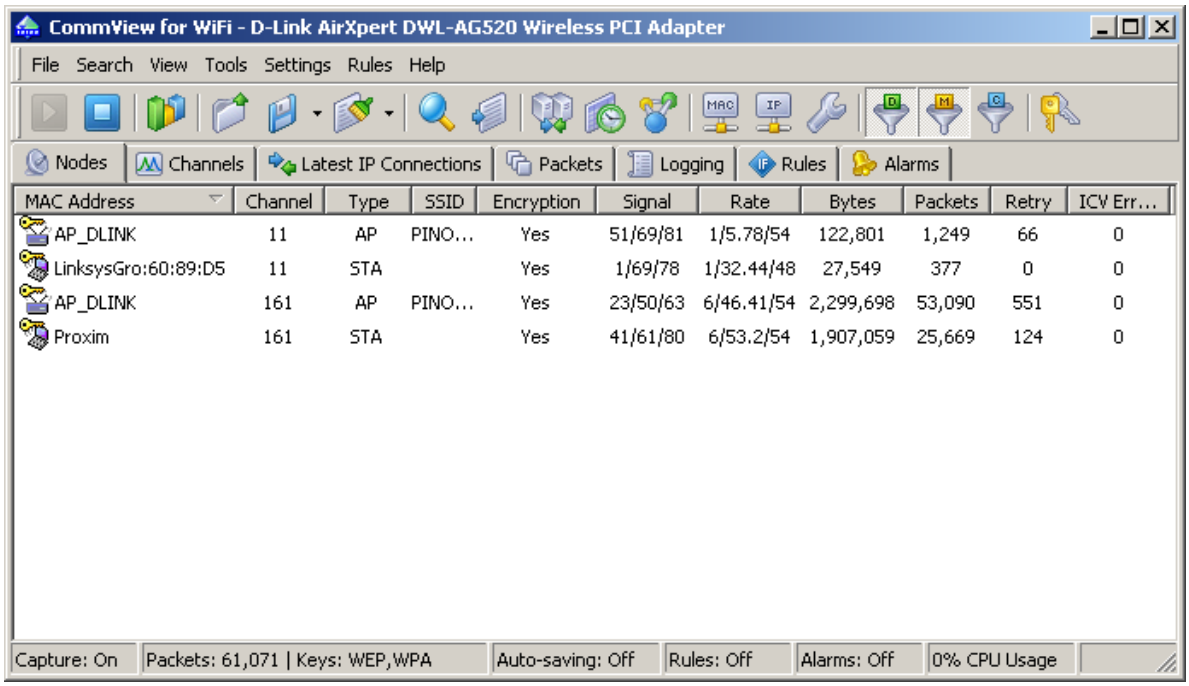
IMPORTANTE: SuperG/SuperAG è una tecnologia proprietaria non standard. Pertanto, è possibile che il nostro prodotto non riesca ad acquisire, decodificare e decifrare i dati trasmessi in modalità SuperG/SuperAG.

**Differenze tra la finestra Scanner e la scheda Nodi**

La finestra Scanner e la scheda **Nodi** della finestra principale dell'applicazione, benché apparentemente simili, presentano importanti differenze. Lo strumento Scanner è molto utile per un rapido esame dell'area e il rilevamento delle stazioni e dei punti di accesso. Non fornisce statistiche dettagliate su ciascun nodo e può includere anche host non wireless (purché la casella **Nascondi host cablati** non sia selezionata), per semplificare la comprensione della topologia della rete.

# Nodi

Questa scheda consente di visualizzare informazioni dettagliate sui nodi wireless attivi, ovvero sui punti di accesso e le stazioni associate che trasmettono dati sul canale o sui canali che vengono monitorati. Dopo aver selezionato un canale per il monitoraggio mediante la finestra Scanner, nella tabella verranno automaticamente inseriti i nodi wireless rilevati. Grazie al sistema di analisi dei pacchetti utilizzato dal programma, verranno visualizzati tutti i punti di accesso trovati sul canale specificato, le stazioni in modalità ad hoc e le stazioni associate in modalità infrastruttura. Verranno escluse le stazioni non associate e quelle che non inviano dati.




È importante ricordare che la radio utilizzata in una scheda wireless può ricevere dati solo su un canale alla volta. Pertanto, dopo che è stato selezionato un determinato canale per il monitoraggio, nella tabella verranno visualizzati i dati relativi ai punti di accesso e alle stazioni che trasmettono solo sul canale specificato. Tuttavia, è possibile selezionare un altro canale e riavviare il processo di acquisizione in qualsiasi momento senza reimpostare i dati nella tabella oppure lasciare che Scanner esegua una rapida scansione dei canali in modo da mostrare i nodi attivi. Accertarsi di avere selezionato la casella **Mostra dati nella finestra principale durante scansione** nelle opzioni della finestra Scanner per fare in modo che i dati vengano inseriti automaticamente nella scheda Nodi durante il processo di scansione.

Di seguito viene illustrato il significato delle colonne nella tabella:

**Indirizzo MAC:** indirizzi MAC e/o alias dei punti di accesso e delle stazioni. L'icona accanto all'indirizzo MAC rappresenta il tipo di nodo. Una casella con due antenne indica un punto di accesso mentre un notebook corrisponde a una stazione in modalità infrastruttura o ad hoc. La chiave dorata viene visualizzata quando i dati sono sottoposti a cifratura.
**Canale:** canale al quale trasmette la stazione o il punto di accesso specificato.
**Tipo**: tipo di nodo. I valori possibili sono AP (punti di accesso), STA (stazioni in modalità infrastruttura) e AD HOC (stazioni in modalità ad hoc).
**SSID:** Service Set Identifier. Stringa univoca che distingue una rete WLAN dall'altra.
**Cifratura:** mostra se il nodo utilizza la crittografia WEP o WPA.
**Segnale:** livello del segnale nel formato min/medio/max. Il valore medio viene calcolato dall'ultimo ripristino dei dati nella tabella.
**Frequenza:** frequenza di trasferimento dei dati nel formato min/medio/max. Il valore medio viene calcolato dall'ultimo ripristino dei dati nella tabella.
**Byte:** numero di byte inviati e ricevuti dal nodo.
**Pacchetti:** numero di pacchetti inviati e ricevuti dal nodo.
**Tentativo:** numero di pacchetti in cui è stato impostato il contrassegno Tentativo.
**Errori ICV:** numero di pacchetti con errori ICV. Per ulteriori informazioni, vedere Errori CRC e ICV.

Per mostrare o nascondere singole colonne, fare clic sulle voci corrispondenti nel menu **Visualizza** => **Colonne nodi**.

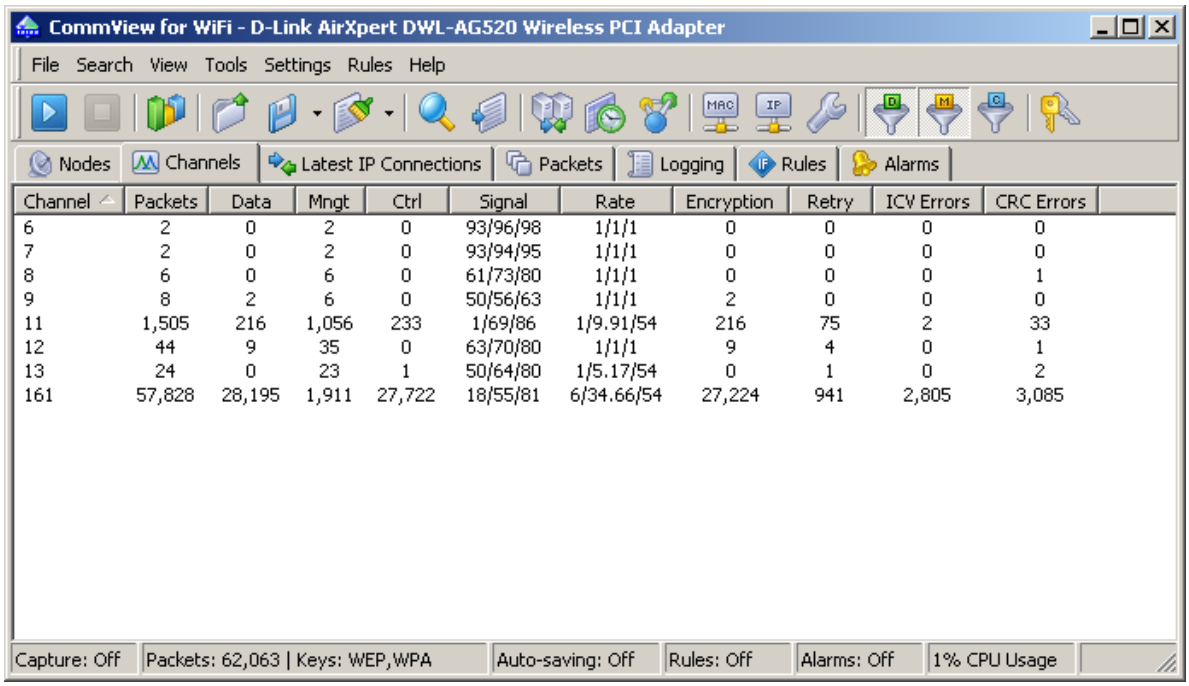
**Comandi del menu**

Fare clic con il pulsante destro del mouse sull'elenco Ultime connessioni IP per visualizzare un menu con i comandi seguenti:

**Copia indirizzo MAC:** copia l'indirizzo IP locale, l'indirizzo IP remoto o il nome host negli Appunti.
**Crea alias:** mostra un finestra che consente di assegnare un alias facile da ricordare all'indirizzo MAC selezionato.
**Salva nodo come:** consente di salvare il contenuto della scheda Nodi come report HTML.
**Cancella nodi:** cancella il contenuto della tabella.
**Ulteriori statistiche:** mostra una finestra con le statistiche sulla distribuzione dei protocolli e il trasferimento dei dati.

# Canali

Questa scheda mostra le statistiche di ciascuno dei canali già monitorati o in corso di monitoraggio. Il numero di canali disponibili nella tabella dipende dalla modalità di utilizzo di CommView for WiFi. Generalmente, quando si effettua il monitoraggio di un solo canale utilizzato dalla rete WLAN, nella tabella verranno visualizzati soltanto i dati del canale selezionato. Questo perché la radio utilizzata da una scheda wireless può ricevere i dati solo su un canale alla volta. Dopo che si seleziona un altro canale per il monitoraggio, questo verrà aggiunto alla tabella. In alternativa, se si utilizza la finestra Scanner per esplorare i canali e la casella **Mostra dati nella finestra principale durante scansione** è selezionata, nella tabella verranno visualizzati tutti i dati analizzati per i quali è stato acquisito almeno un pacchetto. Questo metodo è a volte utile per l'esplorazione di un'area.




Lo standard 802.11b/g utilizza le frequenze di canali sovrapposte. Pertanto, anche se la rete WLAN è configurata per l'utilizzo di un solo canale, ad esempio il canale 6, saranno ancora disponibili valori diversi da zero per i canali adiacenti. I canali 802.11a, a differenza di quelli 802.11b/g, non si sovrappongono.

Di seguito sono descritte le colonne della tabella:

**Canale:** numero del canale.
**Pacchetti:** numero totale di pacchetti trasmessi (Dati + Gestione + Controllo).
**Dati:** numero dei pacchetti di dati trasmessi.
**Gest.:** numero dei pacchetti di gestione trasmessi.
**Ctrl**: numero dei pacchetti di controllo trasmessi.
**Segnale:** livello del segnale nel formato min/medio/max. Il valore medio viene calcolato dall'ultimo ripristino della tabella.
**Frequenza:** velocità di trasferimento dei dati nel formato min/medio/max. Il valore medio viene calcolato dall'ultimo ripristino della tabella.
**Crittografia:** numero di pacchetti di dati per i quali è stato impostato il contrassegno di crittografia.
**Tentativo:** numero di pacchetti per i quali è stato impostato il contrassegno tentativo.
**Errori ICV:** numero di pacchetti con errori ICV. Per informazioni dettagliate, vedere la sezione Errori CRC e ICV.
**Errori CRC:** numero di pacchetti con errori CRC. Per informazioni dettagliate, vedere la sezione Errori CRC e ICV.

Per visualizzare o nascondere singole colonne, fare clic sulle voci corrispondenti nel menu **Visualizza** => **Colonne canali**.

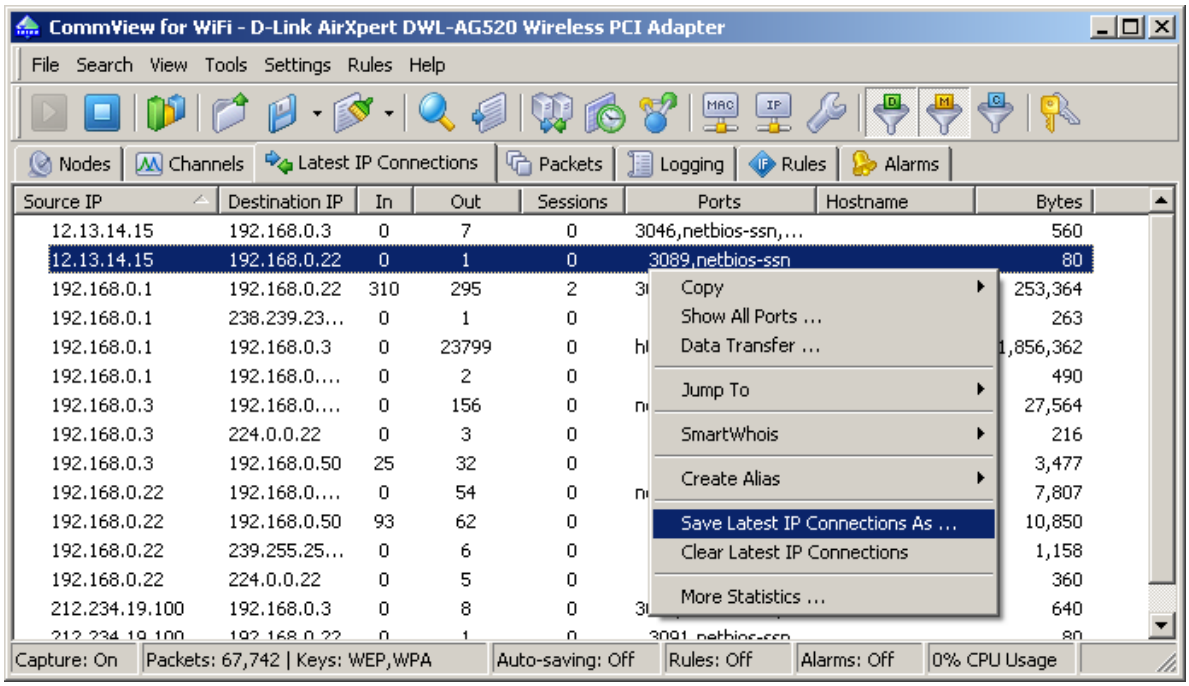
**Comandi del menu**

Fare clic con il pulsante destro del mouse sull'elenco Ultime connessioni IP per visualizzare un menu con i comandi seguenti:

**Salva canali come:** consente di salvare il contenuto della scheda canali come report HTML.
**Cancella canali:** cancella il contenuto della tabella.
**Ulteriori statistiche:** visualizza una finestra con le statistiche sulla distribuzione dei protocolli e il trasferimento dei dati.

# Ultime connessioni IP

Questa scheda consente di visualizzare informazioni dettagliate sulle connessioni WLAN (solo protocollo IP). Per avviare il processo di acquisizione dei pacchetti, selezionare **File = > Avvia acquisizione** nel menu oppure fare clic sul pulsante corrispondente nella barra degli strumenti. Questa scheda viene compilata solo se il programma è in grado di decifrare il traffico della rete WLAN cifrato con le chiavi WEP/WPA. Se la rete WLAN utilizza la cifratura WEP, tutti i pacchetti di dati in corso di invio verranno cifrati. Per ottenere le informazioni sul relativo indirizzo IP, è necessario immettere la chiave o le chiavi WEP o WPA corrette. A questo scopo, selezionare **Impostazioni => Chiavi WEP/WPA** nel menu.




Di seguito sono descritte le colonne della tabella:

**IP di origine, IP di destinazione:** mostra la coppia di indirizzi IP tra i pacchetti in corso di invio.
**In:** mostra il numero di pacchetti ricevuti.
**Out:** mostra il numero di pacchetti inviati.
**Sessioni:** mostra il numero di sessioni TCP/IP stabilite. Se non è stata stabilita alcuna connessione TCP (ad esempio perché la connessione non è riuscita o si utilizza il protocollo UDP/IP o ICMP/IP), verrà visualizzato il valore zero.
**Porte:** mostra le porte del computer remoto utilizzate durante il tentativo di connessione o la connessione TCP/IP. Se non si utilizza il protocollo TCP/IP, è possibile che l'elenco sia vuoto. Le porte possono venire visualizzate come valori numerici oppure come nomi dei servizi corrispondenti. Per ulteriori informazioni, vedere la sezione Opzioni impostazione.
**Nome host:** visualizza il nome host del computer remoto. Se non è possibile risolvere il nome host, la colonna sarà vuota.
**Byte:** mostra il numero di byte trasmessi durante la sessione.
**Ultimo pacchetto:** mostra l'ora dell'ultima operazione di invio/ricezione di pacchetti durante la sessione.

Per visualizzare o nascondere le singole colonne, fare clic sulle voci corrispondenti nel menu **Visualizza** => **Ultime connessioni IP**.

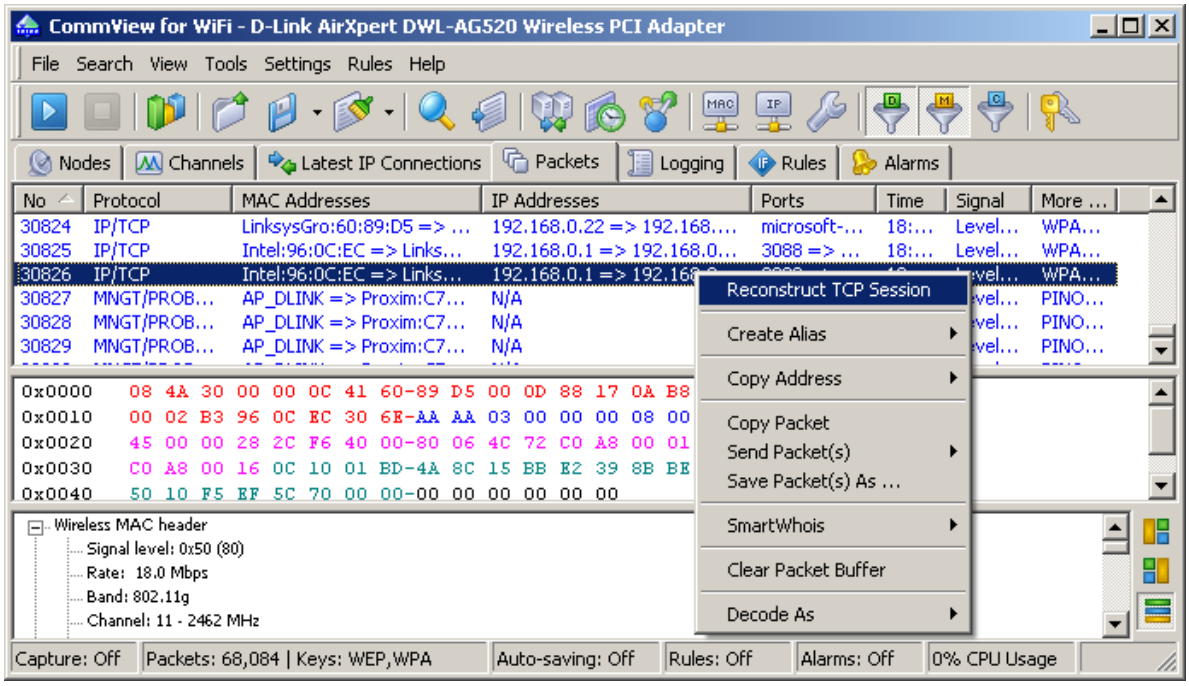
### Comandi del menu

Fare clic con il pulsante destro del mouse sull'elenco Ultime connessioni IP per visualizzare un menu con i comandi seguenti:

**Copia:** copia l'indirizzo IP locale, l'indirizzo IP remoto o il nome host negli Appunti.
**Mostra tutte le porte:** visualizza una finestra con l'elenco completo delle porte utilizzate durante la comunicazione tra la coppia di indirizzi IP selezionata. Questa opzione è utile quando si utilizzano molte porte non incluse nella colonna corrispondente.
**Trasferimento dati:** visualizza una finestra che contiene le informazioni sulla quantità di dati trasmessi tra la coppia di indirizzi IP selezionata e l'ora dell'ultima operazione di trasmissione.
**Passa a:** consente di passare velocemente al primo e/o ultimo pacchetto con l'indirizzo IP di origine o destinazione selezionato. Verrà visualizzata la scheda Pacchetti e il cursore del mouse verrà posizionato sul pacchetto che soddisfa i criteri specificati.
**SmartWhois:** invia l'indirizzo IP di origine o destinazione selezionato a SmartWhois, purché installato sul computer in uso. SmartWhois è un'applicazione autonoma sviluppata da TamaSoft che consente di ottenere informazioni su qualsiasi indirizzo IP o nome host. Fornisce automaticamente le informazioni associate a un indirizzo IP, ad esempio il dominio, il nome della rete, il paese, lo stato, la provincia o la città. Il programma può essere scaricato dal nostro sito Web.
**Crea alias:** visualizza una finestra che consente di assegnare un alias facile da ricordare all'indirizzo IP selezionato.
**Salva ultime connessioni IP come:** consente di salvare il contenuto della scheda Ultime connessioni IP come report HTML.
**Cancella ultime connessioni IP:** cancella la tabella.
**Ulteriori statistiche:** mostra una finestra con le statistiche sulla distribuzione dei protocolli e il trasferimento dei dati.

# Pacchetti

Questa scheda consente di visualizzare tutti i pacchetti di rete acquisiti e le informazioni dettagliate su un pacchetto selezionato.




Nella **tabella superiore** viene visualizzato l'elenco dei pacchetti acquisiti. Utilizzare questo elenco per selezionare un pacchetto che si desidera venga visualizzato e analizzato. Quando si fa clic su un pacchetto, negli altri riquadri verranno visualizzate le informazioni su di esso.

Di seguito sono descritte le colonne della tabella.

**N.**: numero di pacchetto univoco.
**Protocollo:** visualizza il protocollo del pacchetto.
**Indirizzi MAC:** visualizza gli indirizzi MAC di origine e destinazione.
**Indirizzi IP:** visualizza gli indirizzi IP di origine e di destinazione, dove applicabile.
**Porte:** visualizza le porte di origine e di destinazione, dove applicabile. Le porte possono venire visualizzate come valori numerici o come nome di servizi corrispondenti. Per ulteriori informazioni, vedere Opzioni di configurazione.
**Ora/Delta:** visualizza l'ora delta o assoluta del pacchetto. L'ora delta corrisponde alla differenza tra le ore assolute degli ultimi due pacchetti. Per passare dall'ora assoluta all'ora delta, scegliere **Visualizza** =>**Colonne pacchetti** =>**Mostra tempo come**.
**Dimensione:** visualizza la dimensione di un pacchetto in byte. Questa colonna è nascosta per impostazione predefinita.
**Segnale:** visualizzata l'intensità del segnale e la velocità di trasferimento dei dati.
**Ulteriori dettagli:** visualizza ulteriori informazioni per alcuni tipi di pacchetti.
**Errori:** visualizza le informazioni sugli errori. Per una descrizione dettagliata, vedere Errori CRC e ICV. Questa colonna è nascosta per impostazione predefinita.

Per visualizzare o nascondere le singole colonne, fare clic sulle voci corrispondenti nel menu **Visualizza** =>**Colonne pacchetti**. Per sospendere l'emissione di pacchetti, scegliere **File** =>**Sospendi output pacchetti**. In modalità sospensione i pacchetti vengono catturati, ma non visualizzati nella scheda **Pacchetti**. Questa opzione è utile quando si desidera esaminare solo le statistiche anziché i singoli pacchetti. Per visualizzare di nuovo i pacchetti in tempo reale, scegliere **File** =>**Riprendi output pacchetti**.

Nel **riquadro centrale** viene visualizzato il contenuto non elaborato del pacchetto, nei formati esadecimali e testo normale. In quest'ultimo caso, i caratteri non stampabili vengono sostituiti da punti. Se nella **tabella superiore** sono stati selezionati più pacchetti, nel **riquadro inferiore** viene visualizzato il numero totale dei pacchetti selezionati, le relative dimensioni e l'intervallo tra il primo e l'ultimo pacchetto.

Nel **riquadro inferiore** vengono visualizzate le informazioni sul pacchetto codificato per il pacchetto selezionato. Queste informazioni includono dati molto importanti che possono essere utilizzati dai professionisti della rete. Fare clic con il pulsante destro del mouse sul riquadro per richiamare il menu contestuale che consente di comprimere o espandere tutti i nodi, oppure di copiare solo il nodo selezionati o tutti i nodi. Per cambiare la posizione della finestra del decoder, fare clic su uno dei tre pulsanti sul bordo del riquadro. È possibile allineare la finestra del decoder in basso, a sinistra o a destra.

### Comandi di menu

Fare clic con il pulsante destro del mouse sull'elenco dei pacchetti per visualizzare un menu con i seguenti comandi:

**Ricostruisci sessione TCP:** consente di ricostruire una sessione TCP a partire dal pacchetto selezionato. Verrà visualizzata una finestra che mostra l'intera conversazione tra due host.
**Crea alias:** visualizza una finestra che consente di assegnare un alias facile da ricordare all'indirizzo IP o MAC selezionato.
**Copia indirizzo:** copia L'indirizzo MAC di origine, l'indirizzo MAC di destinazione, l'indirizzo IP di origine o l'indirizzo IP di destinazione negli Appunti.
**Copia pacchetto:** copia i dati non elaborati dei pacchetti selezionati negli Appunti.
**Salva pacchetto/i come:** salva il contenuto del pacchetto o dei pacchetti selezionati in un file. La finestra di dialogo Salva con nome consente di scegliere dall'elenco a discesa il formato da utilizzare per il salvataggio dei dati.
**SmartWhois**: invia l'indirizzo IP di origine o di destinazione dal pacchetto selezionato a SmartWhois, se installato sul computer. SmartWhois è un'applicazione sviluppata da TamaSoft in grado di ottenere le informazioni su tutti i nomi host e gli indirizzi IP del mondo. Fornisce automaticamente le informazioni associate a un indirizzo IP, ad esempio il dominio, il nome della rete, il paese, lo stato o la provincia e la città. È possibile scaricare il programma dal nostro sito. Questa opzione è disabilitata per i pacchetti non di tipo IP.
**Cancella buffer pacchetti:** cancella il contenuto del buffer del programma. L'elenco dei pacchetti verrà cancellato e non sarà più possibile visualizzare i pacchetti precedentemente catturati dal programma.
**Decodifica come:** consente di decodificare i protocolli supportati che utilizzano porte non standard per i pacchetti TCP e UDP. Se ad esempio il server SOCKS viene eseguito sulla porta 333 anziché 1080, è possibile selezionare un pacchetto appartenente alla sessione SOCKS e utilizzare questo comando per fare in modo che tutti i pacchetti ricevuti sulla porta 333 vengano decodificati come pacchetti SOCKS. Queste riassegnazioni porta-protocollo non sono permanenti e restano valide fino alla chiusura del programma. Non è possibile ignorare le coppie porta-protocollo standard, ovvero non è possibile fare in modo che i pacchetti sulla porta 80 vengano decodificati come pacchetti TELNET.

Il pacchetto o i pacchetti selezionati possono anche essere trascinati sul desktop.

# Connessione

Questa scheda viene utilizzata per salvare i pacchetti acquisiti in un file sul disco, nel formato di origine con l'estensione .NCF. Il vecchio formato .CCF è supportato per la compatibilità con le versioni precedenti. Tuttavia, non è più possibile salvare i pacchetti catturati. È possibile aprire e visualizzare questi file in qualsiasi momento con Visualizzatore registro, oppure è possibile fare doppio clic su un file NCF o CCF per fare in modo che vengano caricati e decodificati.

NCF è un formato aperto. Per informazioni dettagliate sul formato NFC, vedere Formato dei file di registro di CommView.

**Salva e gestisci**

Utilizzare questo frame per salvare manualmente i pacchetti acquisiti in un file e per concatenare/dividere i file acquisiti.

È possibile salvare tutti i pacchetti correntemente archiviati nel buffer oppure salvarne solo una parte inclusa in un determinato intervallo. Nei campi **A** e **Da** è possibile impostare l'intervallo necessario in base ai numeri di pacchetti come illustrato nella scheda Pacchetti. Fare clic su **Salva con nome ...** per scegliere un nome di file.

Per unire manualmente più file NCF in un unico file più grande, fare clic sul pulsante **Concatena registri**. Per dividere i file NCF troppo grandi in porzioni più piccole, fare clic sul pulsante **Dividi registri**. Verrà visualizzata dettagliatamene la procedura da eseguire e sarà possibile specificare le dimensioni desiderate dei file di output.

**Salvataggio automatico**

Selezionare questa casella per fare in modo che i pacchetti catturati vengano salvati automaticamente al momento dell'arrivo. Utilizzare il campo **Dimensioni massime directory** per limitare le dimensioni totali dei file catturati archiviati nella **Directory registri**. Se le dimensioni totali dei file catturati superano il limite massimo, verranno automaticamente eliminati i file più vecchi contenuti nella directory. Il campo **Dimensioni medie file di registro** consente di specificare le dimensioni desiderate per ciascun file di registro. Quando il file di registro raggiunge le dimensioni limite specificate, viene automaticamente creato un nuovo file. Per cambiare la **Directory registri** predefinita, fare clic sulla casella **Salva file in**, quindi scegliere un'altra cartella.

IMPORTANTE: se si desidera lasciare memorizzato per lungo tempo un importante file acquisito, spostarlo dalla Directory registri predefinita in un'altra cartella, per evitare che venga automaticamente eliminato per il salvataggio di nuovi file.

Si noti che ciascun pacchetto non viene salvato singolarmente al momento dell'arrivo. Pertanto, se si sceglie di visualizzare il file di registro in tempo reale, gli ultimi pacchetti potrebbero non essere inclusi. Per eseguire subito il dump nel file di registro, fare clic su **Interrompi acquisizione** o deselezionare la casella **Salvataggio automatico**.

**Registrazione accesso WWW**

Selezionare questa casella di controllo per abilitare la registrazione delle sessioni HTTP. Utilizzare il campo **Dimensioni max file** per limitare le dimensioni del file di registro. Se quest'ultimo supera il limite massimo, verranno automaticamente eliminati i record più vecchi nel file. Per modificare il nome e il percorso predefiniti del file, fare clic sulla casella **Salva file in** e specificare un altro nome. I file di registro possono essere generati nei formati **HTML** o **TXT**. Scegliere **Configura** per modificare le opzioni di connessione predefinite, ad esempio il numero di porta utilizzato per l'accesso HTTP (il valore predefinito 80 potrebbe impedire le connessioni quando si utilizza un server proxy) ed escludere alcuni tipi di dati (la registrazione di pagine non HTML è generalmente poco utilizzata, pertanto si consiglia si escludere gli URL di immagini dai file di registro).

# Visualizzazione di registri

Visualizzatore registro è uno strumento per la visualizzazione e l'esplorazione dei file acquisiti creati da CommView e da molti altri analizzatori di pacchetti. Offre le stesse funzioni della scheda **Pacchetti** disponibile nella finestra principale del programma, tuttavia visualizza i pacchetti caricati dai file sul disco anziché quelli acquisiti in tempo reale.

Per aprire Visualizzatore registro, scegliere **File => Visualizzatore registro** nel menu principale del programma oppure fare doppio clic su un file qualsiasi di CommView salvato in precedenza. È possibile aprire il numero di finestre desiderato, ciascuna della quali può essere utilizzata per l'esplorazione di uno o più file acquisiti.

È possibile utilizzare Visualizzatore registro per esplorare file acquisiti creati da altri analizzatori di pacchetti e firewall personali. La versione corrente supporta l'importazione dei file nei formati Network Instruments Observer®, Network General Sniffer® for DOS/Windows, Microsoft® NetMon, WildPackets EtherPeek™ e AiroPeek™ e Tcpdump (libcap). Questi formati sono utilizzati anche da numerose applicazioni di terze parti. Visualizzatore registro consente di esportare i dati dei pacchetti, mediante la creazione dei file nei formati Network Instruments Observer®, Network General Sniffer® for DOS/Windows, Microsoft® NetMon, WildPackets EtherPeek™ e AiroPeek™ e Tcpdump (libcap) oppure nel formato CommView nativo.

Le funzioni di Visualizzatore registro sono molto simili a quelle della scheda **Pacchetti** nella finestra principale. Per ulteriori informazioni, vedere il capitolo Pacchetti.

**Menu Visualizzatore registro**

### File

**Carica registri di CommView:** consente di aprire e caricare uno o più file acquisiti con CommView.
**Importa registri:** consente di importare i file acquisiti creati con altri analizzatori di pacchetti.
**Esporta registri:** consente di esportare i pacchetti visualizzati nei file di acquisizione in numerosi formati.
**Cancella finestra:** consente di cancellare l'elenco di pacchetti.
**Genera statistiche:** consente di generare le statistiche sui pacchetti caricati in Visualizzatore pacchetti. È anche possibile ripristinare le statistiche raccolte in precedenza, visualizzate nella finestra **Statistiche.** Si noti che questa opzione non supporta la visualizzazione della distribuzione dei pacchetti sulla timeline, ma solo la visualizzazione dei titoli, dei grafici dei protocolli e delle tabelle degli host LAN.
**Chiudi finestra:** chiude la finestra.

### Cerca

**Trova pacchetto:** consente di visualizzare una finestra di dialogo che consente di trovare i pacchetti che corrispondono a un testo specifico.
**Vai a Numero di pacchetto:** consente di visualizzare una finestra di dialogo che consente di passare direttamente al pacchetto con il numero specificato.

### Regole

**Applica:** applica il gruppo di regole correnti ai pacchetti visualizzati nel Visualizzatore registro. Pertanto, questa funzione può comportare l'eliminazione dei pacchetti che non corrispondono al gruppo di regole applicate. Si noti che il file sul disco non verrà eliminato.
**Da file ...**: equivale al commando **Applica**, tuttavia consente di utilizzare un gruppo di regole di un file .RLS già salvato al posto del gruppo di regole correnti.

# Regole

CommView consente di impostare due tipi di regole.

Il primo tipo (**regole wireless**) consente di applicare un filtro ai pacchetti in base al tipo di pacchetto wireless: **Dati**, **Gestione** e **Controllo**. Per attivare o disattivare la cattura di questi tipi di pacchetti, utilizzare il comando **Regole** del menu del programma oppure il pulsante della barra degli strumenti corrispondente. Il comando **Ignora beacon** consente di attivare o disattivare la cattura dei pacchetti beacon.

Il secondo tipo (**regole convenzionali**) consente di applicare un filtro ai pacchetti in base a molti criteri, tra cui il numero di porta o l'indirizzo MAC. Per utilizzare questo tipo di regola, selezionare la scheda **Regole** della finestra principale del programma. Se si impostano una o più regole, i pacchetti verranno filtrati in base a queste regole impostate e verranno visualizzato solo quelli compatibili con queste regole. Se si imposta una regola, il nome della pagina corrispondente verrà visualizzato in grassetto.

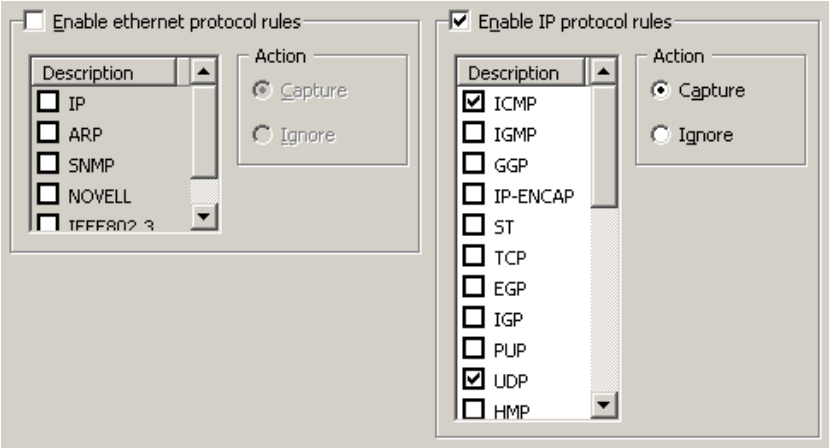
Nella barra di stato del programma è visualizzato il numero di regole convenzionali correntemente attive. Si noti che **non** è disponibile il numero di regole attive wireless. Infatti, i pulsanti della barra degli strumenti (su o giù) indicano chiaramente solo lo stato attivo o disattivo di tali regole. Inoltre, le regole wireless sono prioritarie rispetto a quelle convenzionali. Qualsiasi pacchetto acquisito deve prima soddisfare i requisiti delle regole wireless prima che abbia luogo qualsiasi altra operazione. Se ad esempio non si seleziona alcun pulsante sulla barra degli strumenti delle regole wireless, non verrà visualizzato alcun pacchetto.

Il comando **Regole** nel menu del programma consente di salvare la regola o le regole di configurazione in un file e quindi di caricarle.

Poiché durante una comunicazione WLAN vengono spesso generati numerosi pacchetti, si consiglia di utilizzare le regole per l'esclusione dei pacchetti non necessari. Ciò consente di ridurre significativamente le risorse consumate dal programma. Per abilitare o disabilitare una regola, scegliere il gruppo appropriato sul lato sinistro della finestra, vale a dire **Indirizzi IP** o **Porte**, quindi selezionare o deselezionare la casella che descrive la regola, vale a dire **Abilita regole indirizzi IP** o **Abilita regole porta**. Esistono sette tipi di regole che è possibile utilizzare:

**Protocolli**

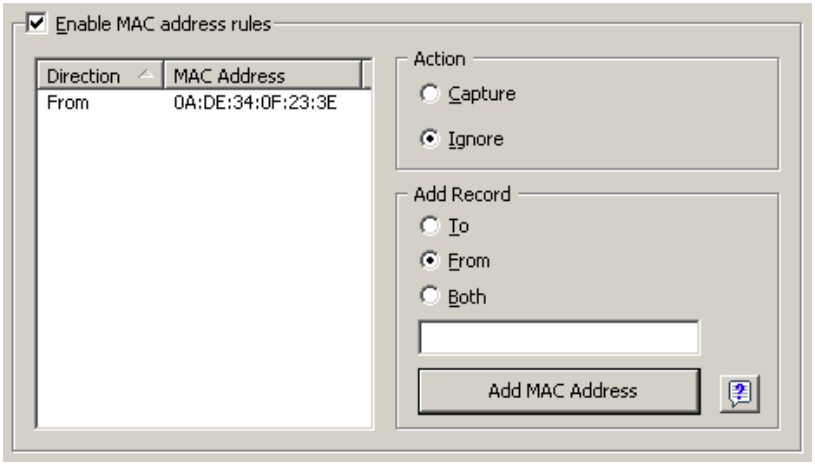
Consentono di ignorare o acquisire i pacchetti in base ai protocolli Ethernet (Layer 2) e IP (Layer 3).




Nell'esempio è illustrata la configurazione per l'acquisizione solo dei pacchetti ICMP e UDP. Tutti gli altri pacchetti della famiglia IP verranno ignorati.

**Indirizzi MAC**

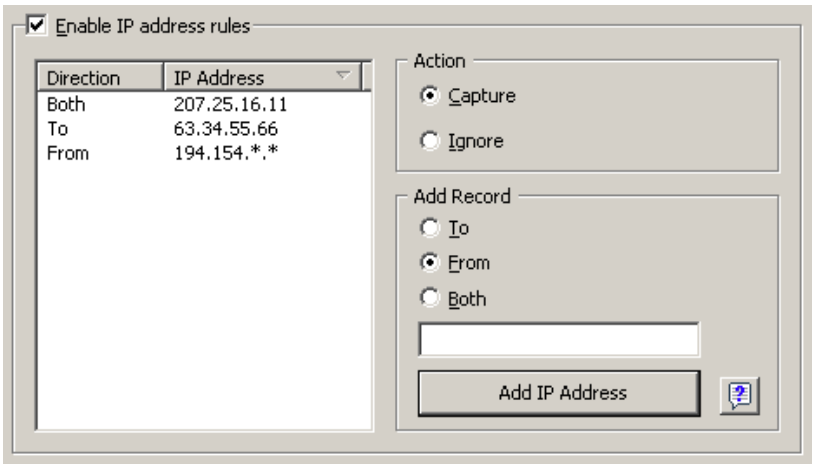
Consente di ignorare o acquisire i pacchetti in base agli indirizzi MAC (hardware). Immettere un indirizzo MAC nel frame **Aggiungi record**, scegliere la direzione (**Da, A** o **Entrambi**), quindi fare click **Aggiungi indirizzo MAC**. Verrà visualizzata la nuova regola. È ora possibile selezionare l'azione da eseguire quando viene elaborato un nuovo pacchetto: quest'ultimo può essere acquisito o ignorato. È anche possibile fare clic sul pulsante Alias MAC per ottenere un elenco degli alias. È sufficiente fare doppio clic sull'alias che si desidera aggiungere per visualizzare l'indirizzo MAC corrispondente nella casella di input.




Nell'esempio viene illustrata la configurazione che consente di ignorare i pacchetti provenienti da 0A:DE:34:0F:23:3E. Verranno acquisiti tutti i pacchetti che provengono dagli altri indirizzi MAC.

**Indirizzi IP**

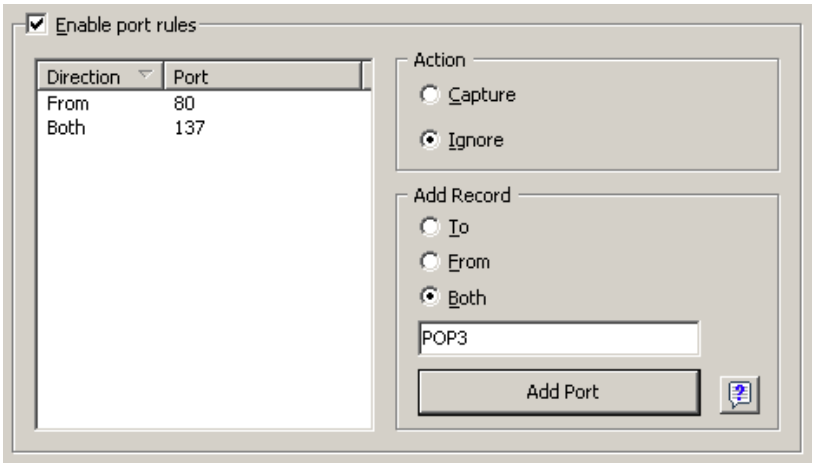
Consente di acquisire o ignorare i pacchetti in base agli indirizzi IP. Immettere un indirizzo IP nel frame **Aggiungi record**, selezionare la direzione (**Da, A** o **Entrambi**), quindi fare clic su **Aggiungi indirizzo IP**. È anche possibile specificare blocchi di indirizzi IP mediante l'utilizzo di caratteri jolly. Verrà quindi visualizzata la nuova regola. È ora possibile selezionare l'azione da eseguire quando viene elaborato un nuovo pacchetto: ignorare o acquisire il pacchetto. È anche possibile fare clic sul pulsante Alias IP per ottenere un elenco degli alias. È sufficiente fare doppio clic sull'alias che si desidera aggiungere per visualizzare l'indirizzo IP corrispondente nella casella di input.




Nell'esempio viene illustrata la configurazione per acquisire i pacchetti verso 63.34.55.66, da e verso 207.25.16.11 e da tutti gli indirizzi compresi tra 194.154.0.0 e 194.154.255.255. Tutti i pacchetti da e verso altri indirizzi verranno ignorati. Poiché gli indirizzi IIP vengono utilizzati nel protocollo IP, questa configurazione consente di ignorare automaticamente tutti pacchetti non IP.

**Porte**

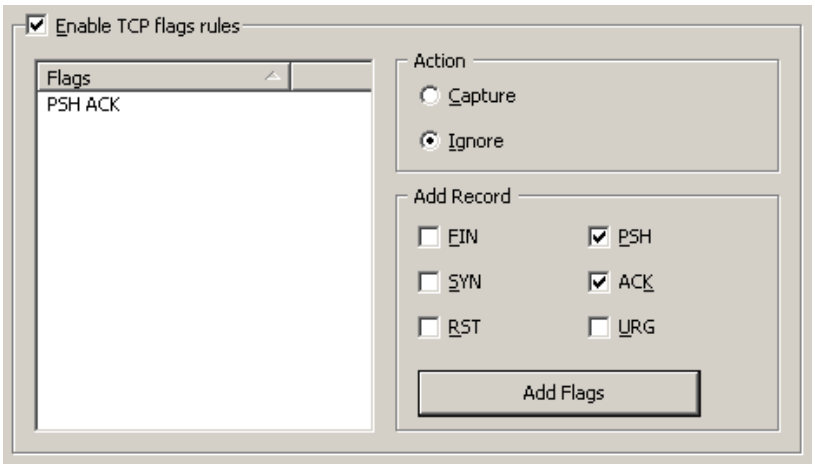
Consente di ignorare o acquisire i pacchetti in base alle porte. Immettere un numero di porta nel frame **Aggiungi record**, selezionare la direzione (**Da, A** o **Entrambi**), quindi fare clic su **Aggiungi porta**. Verrà visualizzata la nuova regola. È ora possibile selezionare l'azione da eseguire quando viene elaborato un nuovo pacchetto: ignorare o acquisire il pacchetto. È anche possibile scegliere Riferimento porta per ottenere un elenco di tutte le porte conosciute. È sufficiente fare doppio clic sulla porta che si desidera aggiungere per visualizzare il numero di porta corrispondente nella casella di input. Le porte possono essere specificate anche come testo, ad esempio è possibile digitare *http* o *pop3* per fare in modo che il programma converta il numero di porta in un valore numerico.




Nell'esempio viene illustrata la configurazione per ignorare i pacchetti indirizzati alla porta 80 e provenienti dalla porta 137. Questa regola impedisce la visualizzazione del traffico HTTP in entrata e del traffico dei Servizio dei nomi NetBIOS in uscita. Verranno acquisiti tutti i pacchetti da e verso altre porte.

**Flag TCP**

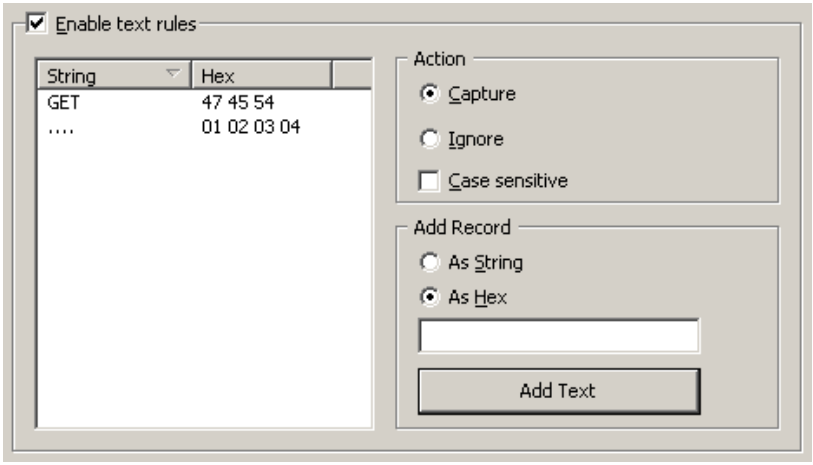
Consente di ignorare o acquisire i pacchetti in base ai flag TCP. Selezionare un flag o una combinazione di flag nel frame **Aggiungi record,** quindi fare clic su **Aggiungi flag.** Verrà visualizzata la nuove regola. È ora possibile selezionare l'azione da eseguire quando viene elaborato un nuovo pacchetto con i flag TCP specificati: ignorare o acquisire il pacchetto.




Nell'esempio viene illustrata la configurazione che consente di ignorare i pacchetti TCP con il flag PSH ACK. Verranno acquisiti tutti i pacchetti con altri flag TCP.

**Testo**

Consente di acquisire i pacchetti che contengono un determinato testo. Immettere una stringa di testo nel frame **Aggiungi record,** selezionare il tipo di informazioni immesse (**Stringa** o **Hex**), quindi fare clic su **Aggiungi testo**. Verrà visualizzata la nuova regola. È possibile immettere il testo come stringa (intuitiva) oppure come valore esadecimale. Si consiglia di utilizzare i valori esadecimali quando si desidera immettere caratteri non stampabili, in questo caso è sufficiente digitare i valori separati da uno spazio, come illustrato di seguito. È ora possibile selezionare l'azione da eseguire quando viene elaborato un nuovo pacchetto: ignorare o acquisire il pacchetto.



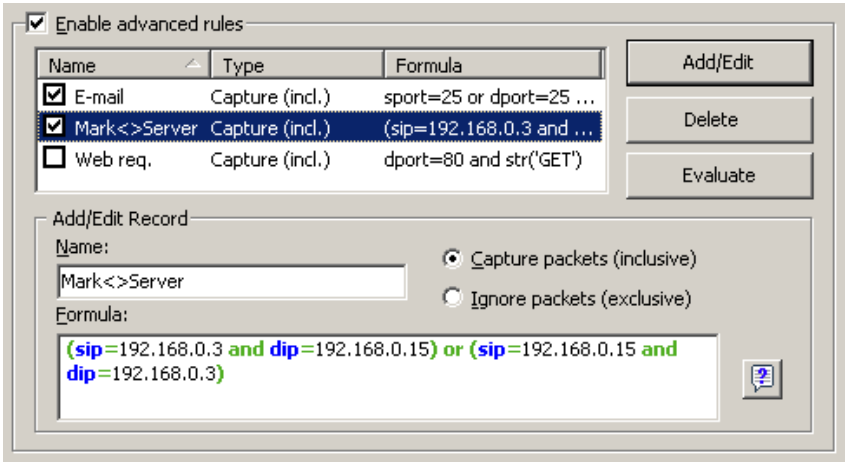

Nell'esempio viene illustrata la configurazione per acquisire solo i pacchetti che contengono "GET" o i dati esadecimali 01 02 03 04. Selezionare la casella **Maiuscole / minuscole** se si desidera applicare la distinzione tra maiuscole e minuscole nelle regole. Tutti gli altri pacchetti che non contengono il testo sopra menzionato verranno ignorati.

**Avanzate**

Le regole avanzate sono le più efficiente e flessibili per la creazione di filtri complessi mediante l'utilizzo di operatori logici booleani. Per ulteriori informazioni sull'utilizzo delle regole avanzate, vedere il capitolo Regole avanzate.

# Regole avanzate

Le regole avanzate sono le più efficiente e flessibili per la creazione di filtri complessi mediante l'utilizzo di operatori logici booleani. L'utilizzo di queste regole richiede una conoscenza di base di matematica e logica, tuttavia la sintassi delle regole è piuttosto semplice.




**Introduzione**

Per aggiungere una nuova regola, immettere un nome arbitrario nel campo **Nome**, selezionare l'azione (**Acquisisci / Ignora**), immettere una **Formula** utilizzando la sintassi seguente, quindi scegliere **Aggiungi / Modifica**. La nuova regola verrà aggiunta all'elenco e diventerà subito attiva. È possibile aggiungere tutte le regole desiderate, tuttavia solo le regole con un segno di spunta accanto al loro nome sono correntemente attive. Per attivare o disattivare le regole, selezionare o deselezionare le caselle corrispondenti oppure eliminare le regole selezionate mediante il pulsante **Elimina**. Se sono attive più regole, è possibile stimare la regola risultante selezionando **Valuta**. Si noti che per combinare più regole attive è necessario utilizzare l'operatore logico OR. Se ad esempio sono attive tre regole: REGOLA1, REGOLA2 e REGOLA3, la regola risultante sarà REGOLA1 OR REGOLA2 OR REGOLA3.

È possibile utilizzare le regole avanzate insieme alle regole di base descritte nel capitolo precedente. Tuttavia, se si ha una certa dimestichezza con gli operatori logici Booleani, si consiglia di utilizzare solo le regole avanzate in quanto più flessibili. Per combinare le regole avanzate con quelle di base, è necessario utilizzare l'operatore logico AND.

**Descrizione della sintassi**

**dir**: direzione dei pacchetti. I valori possibili sono *in* (in entrata), *out* (in uscita) e *pass* (in entrata e in uscita "pass-through"). Questa parola chiave viene utilizzata solo per compatibilità con l'edizione standard non wireless di CommView. CommView for WiFi non include pacchetti in entrata o in uscita perché la scheda non partecipa allo scambio dei dati e monitora il passaggio dei pacchetti solo in modalità passiva.

**etherproto**: protocollo Ethernet, il 13° e 14° byte del pacchetto. I valori accettabili sono numeri (ad esempio *etherproto=0x0800* per il protocollo IP) o alias comuni (ad esempio *etherproto=ARP*, equivalente a 0x0806).

**ipproto**: protocollo IP. I valori accettabili sono numeri (ad esempio *ipproto!=0x06* per il protocollo TCP) o gli alias più spesso utilizzati (ad esempio *ipproto=UDP*, equivalente a 0x11).

**smac**: indirizzo MAC di origine. I valori accettabili sono gli indirizzi MAC nel formato esadecimale (ad esempio *smac=00:00:21:0A:13:0F*) o gli alias definiti dall'utente.

**dmac**: indirizzo MAC di destinazione.

**sip**: indirizzo IP di destinazione. I valori accettabili sono gli indirizzi IP con punti (ad esempio *sip=192.168.0.1*), gli indirizzi IP con caratteri jolly (ad esempio *sip!=*.*.*.255*), indirizzi di rete con maschere di sottorete (ad esempio *sip=192.168.0.4/255.255.255.240* o *sip=192.168.0.5/28*), gli intervalli IP (ad esempio *sip from 192.168.0.15 to 192.168.0.18* or *sip in 192.168.0.15 .. 192.168.0.18* ), oppure gli alias definiti dall'utente.

**dip**: indirizzo IP di destinazione.

**sport**: porta di origine per i pacchetti TCP e UDP. I valori accettabili sono numeri (ad esempio *sport=80* per HTTP), intervalli (ad esempio *sport from 20 to 50* or *sport in 20..50* per tutti i numeri di porta compresi tra 20 e 50) o gli alias definiti dal sistema operativo in uso (ad esempio *sport=ftp*, equivalente a 21). Per l'elenco di indirizzi supportati dal sistema operativo in uso, scegliere **Visualizza => Riferimento porta**.

**dport**: porta di destinazione per i pacchetti TCP e UDP.

**flag**: flag TCP. I valori accettabili sono numeri (ad esempio *0x18* per PSH ACK) oppure o più dei caratteri seguenti: *F* (FIN), *S* (SYN), *R* (RST), *P* (PSH), *A* (ACK), e *U* (URG) oppure la parola chiave *has*, che indica che il flag contiene un determinato valore. Esempi di utilizzo: *flag=0x18*, *flag=SA*, *flag has F*.

**size**: dimensioni dei pacchetti. I valori possibili sono numeri (ad esempio *size=1514*) oppure intervalli (ad esempio *size from 64 to 84* or *size in 64..84* per tutte le dimensioni comprese tra 64 e 84).

**str**: contenuto dei pacchetti. Utilizzare questa funzione per indicare che il pacchetto deve contenere una determinata stringa. Questa funzione include tre argomenti: stringa, posizione, maiuscole/minuscole. Il primo argomento è una stringa, ad esempio *'GET'*. Il secondo argomento è un numero che indica la posizione della stringa (offset) nel pacchetto. L'offset è basato su zero. Se ad esempio si sta cercando il primo valore nel pacchetto, il valore offset deve essere pari *0*. Se il valore offset non è importante, utilizzare *–1*. Il terzo argomento indica la distinzione tra maiuscole e minuscole e può corrispondere a *false* (nessuna distinzione tra maiuscole e minuscole) o *true* (distinzione tra maiuscole e minuscole). Il secondo e il terzo argomento sono facoltativi. Se non specificati, i valori offset verranno impostati su *–1* e il valore di maiuscole e minuscole sarà impostato su *false*. Esempi di utilizzo: *str('GET',-1,false)*, *str('GET',-1)*, *str ('GET')*.

**hex**: contenuto dei pacchetti. Utilizzare questa funzione per indicare che il pacchetto deve contenere un determinato modello di byte esadecimali. Questa funzione include due argomenti: modello esadecimale e posizione. Il primo argomento corrisponde a un valore esadecimale, ad esempio *0x4500*. Il secondo argomento è un numero che indica la posizione del modello (offset) nel pacchetto. L'offset è basato su zero. Ciò significa che se si cerca il primo byte nel pacchetto, il valore offset deve essere uguale a *0*. Se il valore offset non è importante, utilizzare *–1*. Il secondo argomento è facoltativo. Se non specificato, i valori offset verranno impostati su *–1*. Esempi di utilizzo: *hex(0x04500, 14)* , *hex(0x4500, 0x0E)*, *hex (0x010101)*.

**bit**: contenuto dei pacchetti. Utilizzare questa funzione per stabilire se il bit specificato per l'offset immesso è impostato su 1. In caso affermativo, la funzione restituisce *true*. Se il bit specificato è impostato su 0 oppure il byte specificato supera il limite del pacchetto, la funzione restituisce *false*. Il primo argomento corrisponde all'indice di bit nel byte. I valori possibile sono 0-7. Il valore 0x01 indica che l'indice di bit 0 è impostato su 1, tutti gli altri bit vengono impostati su 0. Il secondo argomento è un numero che indica la posizione del byte (offset) nel pacchetto. L'offset è basato su zero, quindi se si cerca il primo byte nel pacchetto, il valore offset deve essere pari a *0*. Entrambi gli argomenti sono obbligatori. Esempi di utilizzo: *bit(0, 14)* , *bit(0, 0x0E)*.

**ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP, Order, Ftype, FsubType, Duration, FragNum, SeqNum**: consente di utilizzare campi di intestazione del pacchetto 802.11 nelle regole avanzate. I nomi degli operatori corrispondono completamente ai campi di intestazione del pacchetto come descritto nella specifica standard 802.11. I valori possibili per ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP e Order sono 0 o 1. Per gli operatori Ftype, FsubType, Duration, FragNum e SeqNum sono accettabili altri valori numerici.

Per informazioni dettagliate sui campi delle intestazioni del pacchetto 802.11 e i valori possibili, vedere la specifica standard 802.1.

È possibile utilizzare le parole chiave descritte sopra con gli operatori seguenti:

**and**: operatore Booleano di congiunzione.
**or:** operatore Booleano di separazione.
**not:** operatore Booleano di negazione.
**=** : valore aritmetico di uguaglianza.
**!=**: valore aritmetico di disuguaglianza.
**<>**: come sopra.
**>**: valore aritmetico di maggioranza.
**<** : valore aritmetico di minoranza.
**( )**: parentesi, controllano le regole di precedenza degli operatori.

Tutti i numeri possono essere nel formato decimale o esadecimale. Per utilizzare il formato esadecimale, è necessario aggiungere *0x* prima del numero, ovvero è possibile utilizzare *15* o *0x0F*.

**Esempi**

Di seguito sono riportati alcuni esempi che illustrano la sintassi delle regole. Ciascuna regola è seguita dalla relativa descrizione. Le regole sono visualizzate in rosso. Per separare i commenti dalle regole, vengono utilizzati due slash.

- **(smac=00:00:21:0A:13:0E or smac=00:00:21:0A:13:0F) and etherproto=arp** // Acquisisce i pacchetti ARP inviati dai due computer 00:00:21:0A:13:0E e 00:00:21:0A:13:0F.
- **ipproto=udp and dport=137** // Acquisisce i pacchetti UDP/IP inviati alla porta numero 137.
- **dport=25 and str('RCPT TO:', -1, true)** // Acquisisce i pacchetti TCP/IP o UDP/IP che contengono "'RCPT TO:" e la porta di destinazione 25.
- **not (sport>110)** // Acquisisce tutti i pacchetti eccetto quelli in cui la porta di origine è maggiore di 110.
- **(sip=192.168.0.3 and dip=192.168.0.15) or (sip=192.168.0.15 and dip=192.168.0.3)** // Acquisisce solo i pacchetti IP inviati tra due computer: 192.168.0.3 e 192.168.0.15. Tutti gli altri pacchetti verranno ignorati.
- **((sip from 192.168.0.3 to 192.168.0.7) and (dip = 192.168.1.0/28)) and (flag=PA) and (size in 200..600)** // Acquisisce i pacchetti TCP con dimensioni comprese tra 200 e 600 byte provenienti dagli indirizzi IP inclusi nell'intervallo

192.168.0.3 - 192.168.0.7 in cui l'indirizzo IP di destinazione è compreso nel segmento 192.168.1.0/255.255.255.240 e in cui il flag TCP equivale a PSH ACK.

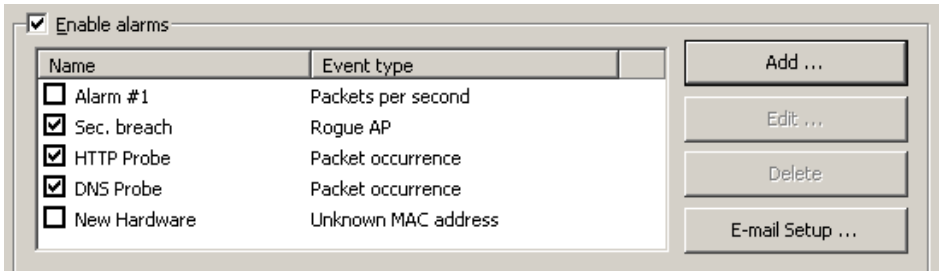
- **Hex(0x0203, 89) and (dir<>in)** // Acquisisce i pacchetti che contengono 0x0203 nell'offset 89, in cui la direzione dei pacchetti non è in entrata.
- **not(ftype=0 and fsubtype=8)** // Ignora i pacchetti di gestione di tipo beacon
- **ftype=2 and wep=1** // Acquisisce i pacchetti di dai cifrati
- **MoreFrag=0 and FragNum=0** // Acquisisce i pacchetti non frammentati

# Avvisi

Questa scheda consente di creare gli avvisi per la notifica di eventi importanti, ad esempio pacchetti sospetti, utilizzo di un'elevata ampiezza di banda, indirizzi sconosciuti ecc. Gli avvisi sono utili nelle situazioni in cui è necessario monitorare la rete alla ricerca di eventi sospetti, quali modelli di byte caratteristici nei pacchetti acquisiti, scansioni di porte o connessioni impreviste di dispositivi hardware.

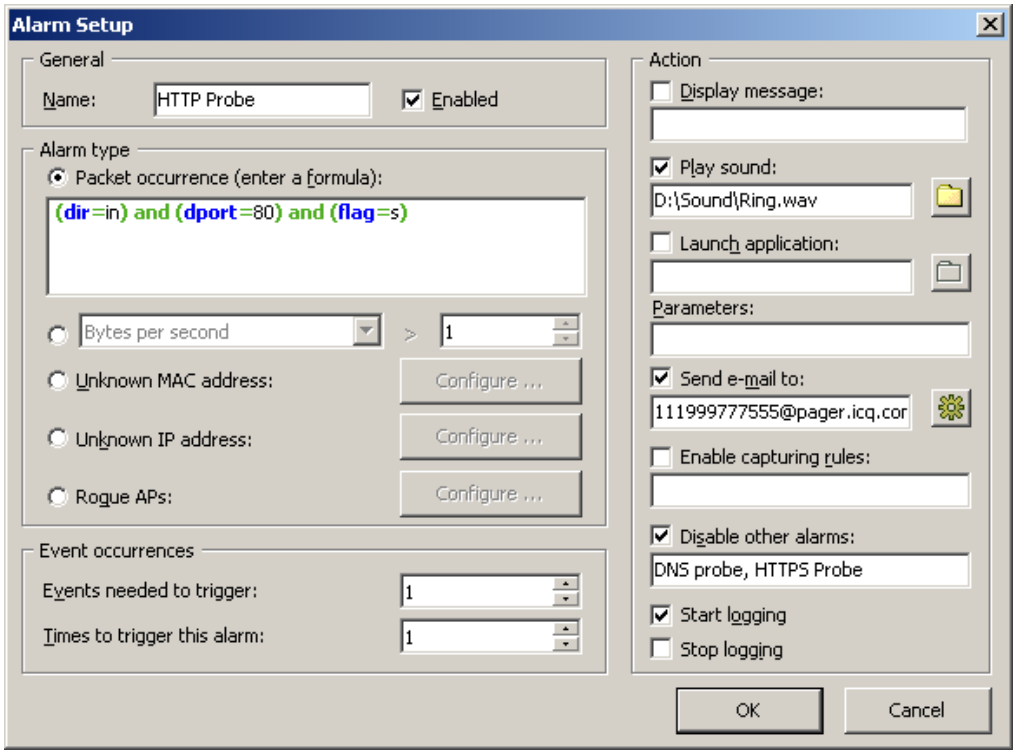
Importante: gli avvisi possono essere attivati solo dai pacchetti cha hanno attraversato i filtri del programma. Se ad esempio il programma è stato configurato per escludere i pacchetti UDP mediante la creazione della regola corrispondente e si presume che un avviso sia stato attivato da un pacchetto UDP, tale avviso non verrà mai attivato.

Gli avvisi vengono gestiti mediante l'elenco illustrato di seguito:




Ogni riga rappresenta un avviso separato e la casella di controllo accanto all'avviso indica se questo è correntemente attivo. Quando si attiva un avviso, il segno di spunta scompare. Per riattivare un avviso disattivato, selezionare la casella di controllo accanto al relativo nome. Per disabilitare tutti gli avvisi, deselezionare la casella di controllo **Abilita avvisi**. Per aggiungere un nuovo avviso, oppure per modificare o eliminare un avviso esistente, utilizzare i pulsanti a destra dell'elenco degli avvisi. Utilizzare il pulsante **Impostazione e-mail** per immettere le informazioni sul server SMTP se desidera utilizzare opzioni di notifica e-mail (vedere sotto).

Di seguito è illustrata la finestra per la configurazione degli avvisi:




Nel campo **Nome** è possibile descrivere la funzione dell'avviso. Selezionare la casella **Abilitato** per attivare l'avviso aggiunto o modificato al termine del processo di configurazione. Questa casella di controllo equivale a quella visualizzata nell'elenco degli avvisi. Il frame **Tipo di avviso** consente di selezionare uno dei dieci tipi di avviso seguenti:

- **Occorrenza pacchetti:** l'allarme verrà attivato dopo l'acquisizione di un pacchetto che corrisponde alla formula specificata. La sintassi della formula equivale a quella utilizzata in Regole avanzate ed è descritta dettagliatamente nel capitolo Regole avanzate.

- **Byte al secondo:** l'avviso viene attivato dopo che il numero di byte al secondo supera il valore specificato. Si noti che è necessario specificare i valori in byte. Se ad esempio si desidera che l'avviso venga attivato quando il trasferimento dei dati supera la velocità di 1Mbyte al secondo, immettere 1000000.

- **Pacchetti al secondo**: l'avviso verrà attivato dopo che il numero di byte al secondo dei pacchetti supera il valore specificato.

- **Trasmissioni al secondo**: l'allarme verrà attivato dopo che il numero di pacchetti trasmessi al secondo supera il valore specificato.

- **Multicast al secondo**: l'avviso verrà attivato dopo che il numero di pacchetti multicast supera il valore specificato.

- **Errori CCRC al secondo**: l'avviso verrà attivato dopo che il numero di errori CRC al secondo supera il valore specificato.

- **Tentativi al secondo:** l'avviso verrà attivato dopo che il numero di tentativi al secondo supera il valore specificato.

- **Indirizzo MAC sconosciuto:** l'avviso verrà attivato dopo che viene acquisito un pacchetto con un indirizzo MAC di origine o destinazione sconosciuto. Utilizzare il pulsante **Configura** per immettere gli indirizzi MAC sconosciuti. Questo avviso è importante per il rilevamento di nuovi dispositivi hardware non autorizzati collegati alla rete WLAN.

- **Indirizzo IP sconosciuto:** l'avviso verrà attivato dopo che viene acquisito un pacchetto con un indirizzo IP di destinazione o di origine sconosciuto. Utilizzare il pulsante **Configura** per immettere gli indirizzi IP sconosciuti. Questo avviso è utile per il rilevamento di connessioni IP non autorizzate dietro il firewall aziendale.

- **AP sconosciuti:** l'avviso verrà attivato dopo che viene rilevato un pacchetto beacon da un punto di accesso sconosciuto. Utilizzare il pulsante **Configura** per immettere gli indirizzi MAC dei punti di accesso conosciuti. Questo avviso è utile per il rilevamento dei punti di accesso non autorizzati.

Il campo **Eventi necessari per l'attivazione** consente di specificare il numero di volte in cui deve verificarsi l'evento previsto prima che venga attivato l'avviso. Se ad esempio si specifica il valore 3, l'avviso verrà attivato solo dopo che l'evento si è verificato tre volte. Se si modifica un avviso esistente, verrà ripristinato il contatore degli eventi interni.

Il campo **Numero di attivazioni dell'avviso** consente di specificare il numero di volte in cui è necessario attivare l'avviso prima che venga disattivato. Il valore predefinito equivale a 1, quindi l'avviso verrà disabilitato dopo la prima occorrenza dell'evento. Se si sceglie di aumentare questo valore, l'avviso verrà attivato più volte. Se si modifica un avviso esistente, verrà ripristinato il contatore delle attivazioni interne.

Il frame **Azione** consente di selezionare le azioni da eseguire quando si verifica l'avviso. Sono disponibili le opzioni seguenti:

- **Messaggio visualizzato**: mostra una finestra di messaggio non modale con il testo specificato. Questa azione consente di utilizzare le variabili che devono essere sostituite dai parametri corrispondenti del pacchetto che ha attivato l'allarme. Le variabili disponibili sono le seguenti:
  %SMAC% -- indirizzo MAC di origine.
  %DMAC% -- indirizzo MAC di destinazione.
  %SIP% -- indirizzo IP di origine.
  %DIP% -- indirizzo IP di destinazione.
  %SPORT% -- porta di origine.
  %DPORT% -- porta di destinazione.
  %ETHERPROTO% -- protocollo Ethernet.
  %IPPROTO% -- protocollo IP.
  %SIZE% -- dimensioni pacchetto.
  %FILE% -- percorso di un file temporaneo che contiene un pacchetto acquisito.

  Se ad esempio il messaggio è "pacchetto SYN ricevuto da %SIP%", il testo effettivo della finestra a comparsa %SIP% verrà sostituito con l'indirizzo IP di origine del pacchetto che ha attivato l'avviso. Se si utilizza la variabile %FILE%, verrà creato un file .NCF nella cartella temporanea. È responsabilità dell'utente eliminare il file dopo che è stato elaborato, poiché non viene rimosso automaticamente. Se l'avviso viene attivato dai valori **Byte al secondo** o **Pacchetti al secondo,** non utilizzare le variabili poiché questi tipi di avvisi non vengono avviati da singoli pacchetti.

- **Riproduci suono:** riproduce il file WAV specificato.

- **Avvia applicazione:** esegue il file EXE o COM specificato. Utilizzare il campo opzionale **Parametri** per attivare i parametri a riga di comando. Come parametri a riga di comando è anche possibile utilizzare le variabili descritte nella precedente sezione **Messaggio visualizzato,** se si desidera che l'applicazione riceva ed elabori le informazioni sul pacchetto che ha attivato l'avviso.

- **Invia e-mail a:** invia un messaggio di posta elettronica all'indirizzo e-mail specificato. È necessario configurare CommView in modo che il server SMTP in uso venga utilizzato prima dell'invio del messaggio e-mail. Selezionare **Impostazione e-mail** accanto all'elenco degli avvisi per specificare le impostazioni del server SMTP e inviare un messaggio di prova. In genere, un messaggio e-mail consente anche di inviare gli avvisi all'applicazione di messaggistica immediata, al telefono cellulare o al cercapersone. Ad esempio, per inviare un messaggio a un utente ICQ, è necessario immettere l'indirizzo e-mail nel formato ICQ_USER_UIN@pager.icq.com, dove ICQ_USER_UIN corrisponde al numero di identificazione ICQ univoco dell'utente, e attivare i messaggi EmailExpress nelle opzioni ICQ. Per ulteriori informazioni vedere la documentazione dell'applicazione di messaggistica immediata in uso o contattare l'operatore del telefono cellulare.

- **Abilita regole di acquisizione:** abilita le Regole avanzate; è necessario immettere il nome o i nomi delle regole. Se è necessario abilitare più regole, separarle con una virgola o un punto e virgola.
- **Disabilita altri avvisi:** disabilita gli altri avvisi; è necessario immettere il nome e i nomi degli avvisi. Se è necessario disabilitare più avvisi, separarli con una virgola o un punto e virgola.
- **Inizia connessione:** attiva il salvataggio automatico (vedere il capitolo Connessione). Verrà avviato il dump dei pacchetti CommView sull'unità disco rigido.
- **Interrompi connessione:** disattiva il salvataggio automatico.

Scegliere **OK** per salvare le impostazioni e chiudere la finestra di configurazione degli avvisi.

Tutti gli eventi e le azioni relative agli avvisi verranno elencate nella finestra **Registro eventi** sotto all'elenco degli avvisi.

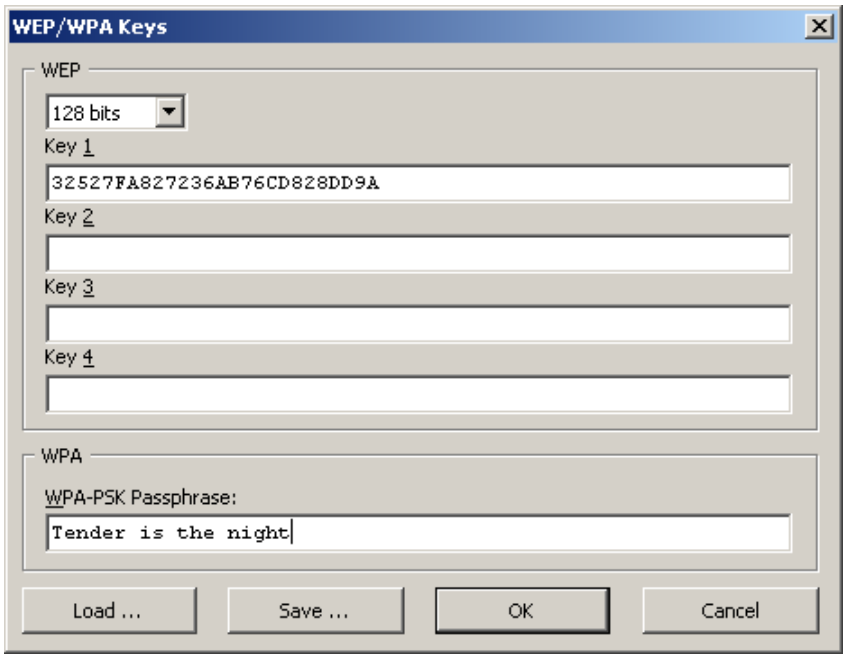
# Chiavi WEP/WPA

La finestra **Chiavi WEP/WPA** consente di immettere chiavi WEP o WPA per descrivere i pacchetti acquisiti. Senza queste chiavi, il programma non è in grado di decifrare i pacchetti di dati che vengono trasmessi sulla rete WLAN. Poiché alcune reti WLAN utilizzano la cifratura in modalità mista in cui entrambi i client WEP e WPA supportano l'autenticazione, è possibile utilizzare contemporaneamente una chiave WEP e una passphrase WPA.

**WEP**
Lo standard WEP consente di utilizzare fino a quattro chiavi WEP. È quindi possibile specificare una, due, tre o quattro chiavi. Nell'elenco a discesa delle lunghezze delle chiavi è possibile selezionare la lunghezza di chiave desiderata tra quelle supportate: 64, 128, 152 e 256 bit. È anche possibile immettere una stringa esadecimali di 10, 26, 32 o 58 caratteri.

**WPA**
Lo standard WPA (Wi-Fi Protected Access) definisce numerose modalità di autenticazione e cifratura. Non tutte queste modalità sono supportate da CommView for WiFi a causa delle limitazioni del modello di sicurezza sottostante. CommView for WiFi supporta la decifratura WPA in modalità PSK (Pre-Shared Key) mediante il protocollo TKIP (Temporal Key Integrity Protocol) o AES/CCMP (Advanced Encryption Standard/Counter CBC-MAC Protocol). È possibile immettere una passphrase o una chiave esadecimale di 64 caratteri.

Importante: per informazioni dettagliate su come CommView for WiFi elabora il traffico in modalità WPA, vedere il capitolo Decifratura WPA.

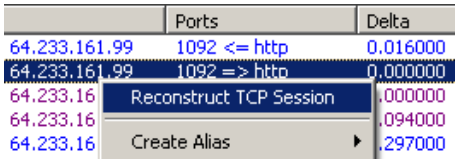



Per salvare il set di chiavi corrente, scegliere **Salva** .... Per caricare un set di chiavi salvato in precedenza, scegliere **Carica ...**.

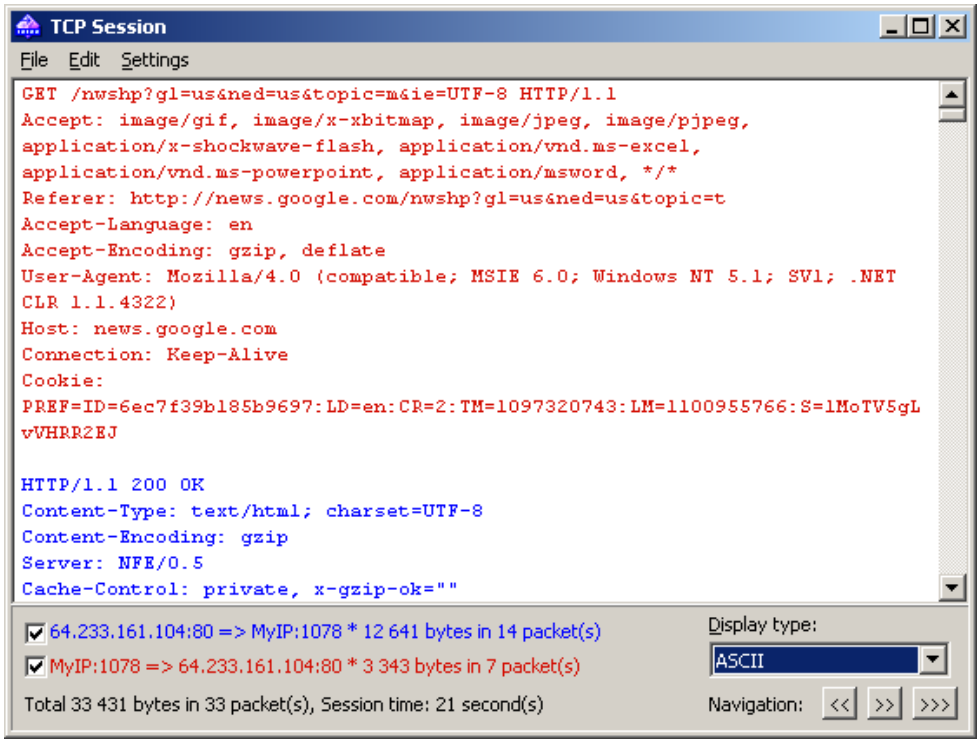
Il set di chiavi che è possibile immettere o caricare mediante questa finestra di dialogo verrà applicato ai pacchetti acquisiti in tempo reale nonché a tutti gli altri file NCF acquisiti e salvati in precedenza. Se si sceglie di salvare i pacchetti acquisiti in un file NCF, tutti quelli decifrati correttamente verranno salvati nel formato decifrato mentre gli altri verranno salvati nel formato originale non modificato.

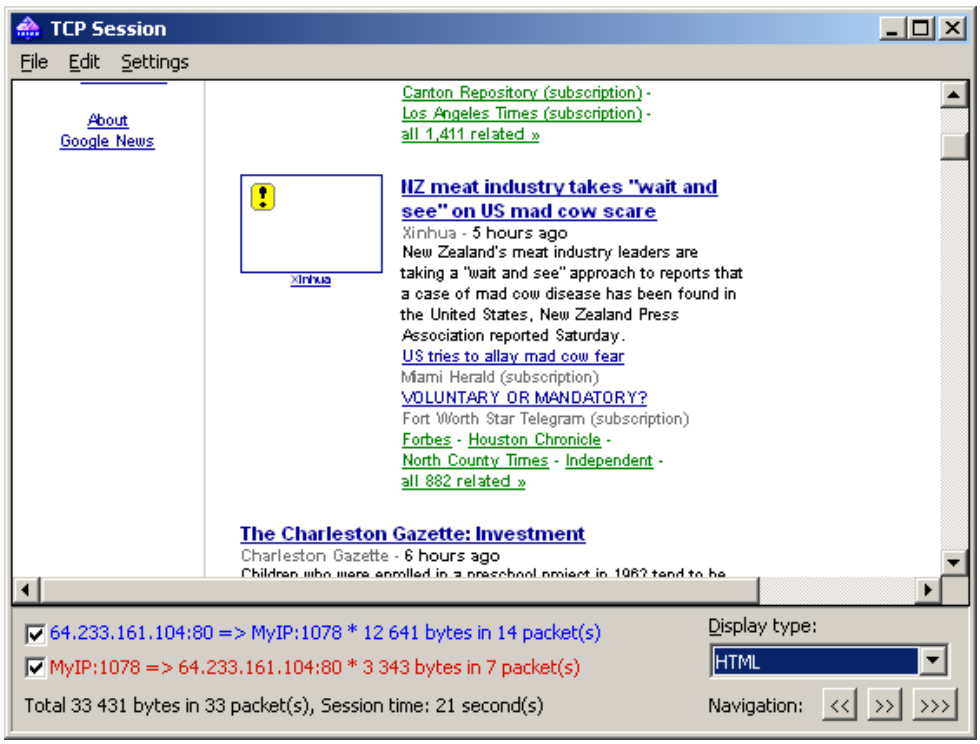
# Ricostruzione di sessioni TCP

Questo strumento consente di visualizzare la conversazione TCP tra due host. Per ricostruire una sessione TCP, è innanzitutto necessario selezionare un pacchetto TCP nella scheda **Pacchetti**. Per ricostruire l'intera sessione, si consiglia di selezionare il primo pacchetto nella sessione per evitare che il processo di ricostruzione inizi da metà conversazione. Dopo aver individuato e selezionato il pacchetto, fare clic con il pulsante destro del mouse su di esso, quindi scegliere **Ricostruisci sessione TCP** dal menu a discesa come illustrato di seguito:

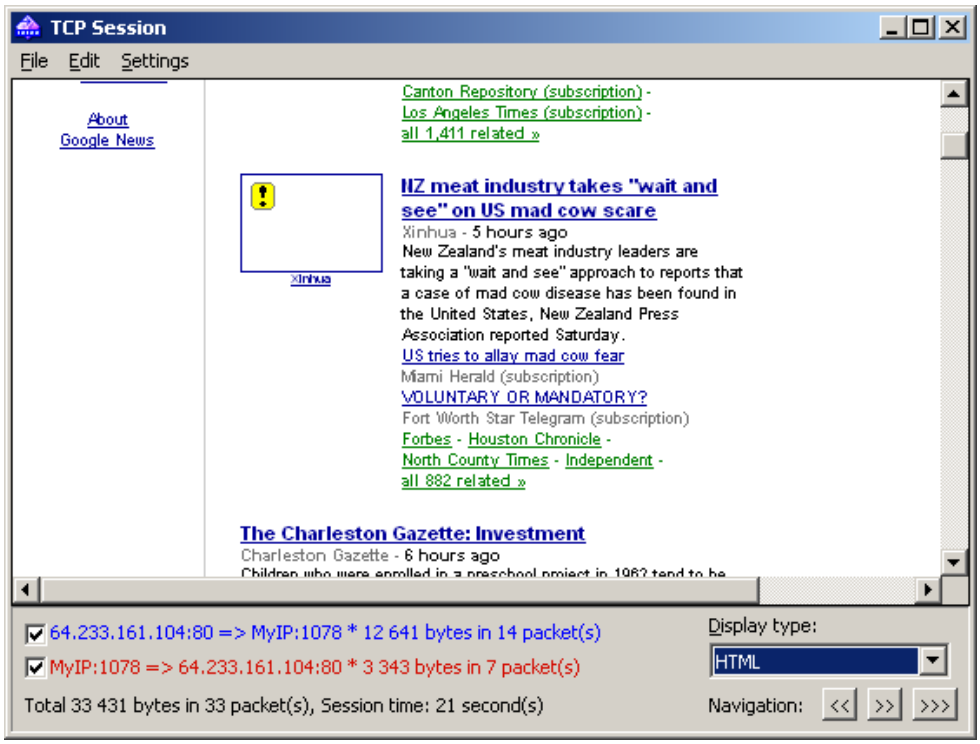



Per ricostruire le sessioni è preferibile utilizzare i protocolli basati sul testo, ad esempio POP3, Telnet o HTTP. Naturalmente, è anche possibile ricostruire un download di un grande file zippato, benché in CommView la ricostruzione di numerosi megabyte di dati sia un processo piuttosto lento e le informazioni ottenute restano inutilizzate nella maggior parte dei casi. Di seguito è illustrata una sessione http che contiene dati HTML visualizzati nelle modalità ASCII e HTML.






In modalità di visualizzazione HTML, le pagine HTML non includono mai grafica inline perché il protocollo HTTP le trasferisce separatamente dai dati HTML. Per visualizzare le immagini, in genere è necessario passare alla sessione TCP successiva. Di seguito è illustrata una sessione http di esempio contenente i dati immagine.




Per impostazione predefinita, in CommView viene effettuato il tentativo di decomprimere il contenuto Web GZIP'd e di ricostruire le immagini dai flussi binari. Per disattivare questa funzionalità, utilizzare la scheda **Decodifica** della finestra di dialogo **Opzioni**.

Per escludere i dati provenienti da una determinata direzione, deselezionare la casella di controllo corrispondente nel riquadro inferiore. I dati in ingresso e in uscita sono contrassegnati in diversi colori per maggiore praticità. Per cambiare colore, scegliere **Impostazioni** =>**Colori**, quindi selezionare il colore desiderato. È anche possibile abilitare o disabilitare il ritorno a capo automatico mediante la voce **A capo automatico** nel menu **Impostazioni**.

L'elenco a discesa **Tipo di visualizzazione** consente di visualizzare i dati in modalità **ASCII** (testo normale), **HEX** (esadecimale), **HTML** (pagine Web e immagini) e **EBCDIC** (codifica dati del mainframe IBM). La visualizzazione dei dati nel formato HTML non sempre consente di ottenere gli stessi risultati di quelli visualizzati nel browser Web, ad esempio non è supportata la grafica inline. Tuttavia, fornisce un'idea dell'aspetto della pagina originale.

È anche possibile scegliere il tipo di visualizzazione predefinito per la finestra Ricostruisci sessione TCP nella scheda **Decodifica** della finestra di dialogo **Opzioni**.

I pulsanti di **Esplorazione** consentono di cercare nella memoria buffer la sessione TCP precedente o successiva. Il primo pulsante di avanzamento (>>) consente di cercare la sessione tra due host coinvolti nella prima sessione ricostruita. Il secondo pulsante di avanzamento (>>>) consente di cercare la sessione successiva tra due host qualsiasi. Se tra due host nel buffer sono comprese più sessioni TCP e si desidera visualizzarle una alla volta, si consiglia di avviare la ricostruzione a partire dalla prima sessione poiché il pulsante indietro (**<<**) non consente di passare alle sessioni TCP precedenti alla prima ricostruita.

I dati ottenuti possono essere salvati nel formato binario, di testo o RTF mediante **File** =>**Salva con nome**... . Per cercare una stringa nella sessione, scegliere **Modifica => Trova**... .

# Statistiche e Report

Scegliere **Visualizza => Statistiche** per visualizzare la finestra delle statistiche che contiene informazioni importanti sul segmento di rete WLAN in uso, ad esempio il grafico relativo alla distribuzione della velocità di pacchetti al secondo, della velocità di byte al secondo e dei protocolli Ethernet, IP e dei protocolli secondari. Per copiare una parte del grafico negli Appunti, fare doppio clic sul grafico. È possibile ruotare i grafici a torta relativi ai protocolli Ethernet, IP e secondari utilizzando i piccoli pulsanti nell'angolo inferiore destro per una migliore visualizzazione delle sezioni.

I dati visualizzati in ogni pagina verranno salvati come file bitmap o di testo delimitati da virgole mediante il menu contestuale o trascinamento. La pagina **Report** consente di generare automaticamente report personalizzabili nei formati HTML o testo delimitato da virgole.

È possibile raccogliere le statistiche di rete sulla base dei pacchetti che attraversano la scheda di rete oppure delle regole correntemente impostate. Se si desidera che i contatori delle statistiche elaborino solo i dati (pacchetti) che corrispondono al set di regole impostato ignorando tutti gli altri, selezionare la casella **Applica regole correnti**.

**Generale**
Consente di visualizzare gli istogrammi relativi ai pacchetti al secondo e ai byte/bit al secondo, il grafico relativo alla larghezza di banda utilizzata (traffico al secondo diviso per la velocità di connessione modem o NIC) nonché il numero di pacchetti e byte complessivi.

**Protocolli**
Consente di visualizzare la distribuzione dei protocolli Ethernet, ad esempio ARP, IP, SNAP, SPX ecc.... Utilizzare l'elenco a discesa **Grafico per** per selezionare uno dei due metodi di calcolo disponibili: per numero di pacchetti o per numero di byte. Se la rete WLAN utilizza un sistema di cifratura WEP o WPA, è necessario configurare le chiavi WEP o WPA correttamente per poter decifrare il traffico in rete, altrimenti il grafico sarà vuoto.

**Protocolli IP**
Consente di visualizzare la distribuzione dei protocolli IP, TCP, UD e ICMP. Utilizzare l'elenco a discesa **Grafico per** per selezionare uno dei due metodi di calcolo disponibili: per numero di pacchetti o per numero di byte. Se la rete WLAN utilizza un sistema di cifratura WEP o WPA, è necessario configurare le chiavi WEP o WPA correttamente per poter decifrare il traffico in rete, altrimenti il grafico sarà vuoto.

**Protocolli IP secondari**
Consente di visualizzare la distribuzione dei protocolli secondari a livello di applicazione IP principale: HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS e DNS. Per aggiungere altri protocolli, fare clic sul pulsante **Personalizza**. Questa finestra di dialogo consente dei definire fino a otto protocolli personalizzati. È necessario immettere il nome del protocollo, scegliere il tipo di protocollo IP (TCP/UDP) e il numero di porta. Utilizzare l'elenco a discesa **Grafico per** per selezionare uno dei due metodi di calcolo disponibili: per numero di pacchetti o per numero di byte. Se la rete WLAN utilizza un sistema di cifratura WEP o WPA, è necessario configurare le chiavi WEP o WPA correttamente per poter decifrare il traffico in rete, altrimenti il grafico sarà vuoto.

**Dimensioni**
Consente di visualizzare il grafico relativo alla distribuzione delle dimensioni dei pacchetti.

**Host per MAC**
Consente di visualizzare l'elenco degli host WLAN in base all'indirizzo MAC nonché le statistiche sul trasferimento dei dati. Agli indirizzi MAC è anche possibile assegnare alias. Se sulla rete sono presenti troppi pacchetti multicast e la tabella Host MAC è sovraccarica, può essere opportuno raggruppare gli indirizzi multicast in una riga di nome GroupedMulticast. Per abilitare questa funzione, selezionare la casella **Raggruppa indirizzi multicast**. Si noti che solo i pacchetti arrivati dopo la selezione di questa opzione verranno raggruppati di conseguenza mentre quelli ricevuti precedentemente verranno ignorati.

**Host per IP**
Visualizza un elenco degli host WLAN attivi in base all'indirizzo IP nonché le statistiche sul trasferimento dati. Poiché i pacchetti IP acquisiti dal programma possono essere originati da un numero illimitato di indirizzi IP, interni ed esterni alla rete WLAN, per impostazione predefinita in questa scheda non vengono visualizzate statistiche. Per visualizzarle, è innanzitutto necessario impostare l'intervallo di indirizzi IP da monitorare, scegliendo **Aggiungi/Imposta intervalli**. Generalmente, questi intervalli devono appartenere alla rete WLAN. La configurazione del programma per il monitoraggio di un determinato intervallo di indirizzi IP consente di utilizzare le statistiche. È possibile immettere un numero qualsiasi di indirizzi, tuttavia non è possibile monitorare oltre 1000 indirizzi IP. Per eliminare un intervallo, fare clic con il pulsante destro sull'elenco degli intervalli, quindi scegliere il comando di menu appropriato. Agli indirizzi IP è anche possibile assegnare alias. Se la rete WLAN utilizza un sistema di cifratura WEP o WPA, è necessario configurare le chiavi WEP o WPA correttamente per poter decifrare il traffico in rete, altrimenti il grafico sarà vuoto.

**Matrice per MAC**
Consente di visualizzare la matrice di conversione grafica tra due host in base ai relativi indirizzi MAC. Gli host rappresentati dai relativi indirizzi MAC sono visualizzati su un cerchio e le sessioni tra questi due host vengono visualizzate come linee che li collegano. Spostare il mouse su un host per evidenziare tutte le connessioni da questo create con gli altri host. È anche possibile modificare il numero di coppie host più attive visualizzate nella matrice modificando il valore nel campo **Coppie host più attive**. Per modificare il numero delle ultime coppie di indirizzi IP esaminate dal programma, modificare il valore nel campo **Ultime coppie da contare**. Se il segmento di rete in uso presenta molti pacchetti broadcast o multicast che sovraccaricano la matrice, è possibile ignorare tali pacchetti selezionando le caselle **Ignora broadcast** e **Ignora multicast**.

**Matrice per IP**

Consente di visualizzare la matrice di conversione grafica tra gli host in base ai relativi indirizzi IP. Gli host rappresentati dai relativi indirizzi IP sono visualizzati su un cerchio e le sessioni tra questi due host vengono visualizzate come linee che li collegano. Spostare il mouse su un host per evidenziare tutte le connessioni da questo create con gli altri host. È anche possibile modificare il numero di coppie host più attive visualizzate nella matrice modificando il valore nel campo **Coppie host più attive**. Per modificare il numero delle ultime coppie di indirizzi IP esaminate dal programma, modificare il valore nel campo **Ultime coppie da contare**. Se il segmento di rete in uso presenta molti pacchetti broadcast o multicast che sovraccaricano la matrice, è possibile ignorare tali pacchetti selezionando le caselle **Ignora broadcast** e **Ignora multicast**. Se la rete WLAN utilizza un sistema di cifratura WEP o WPA, è necessario configurare le chiavi WEP o WPA correttamente per poter decifrare il traffico in rete, altrimenti il grafico sarà vuoto.

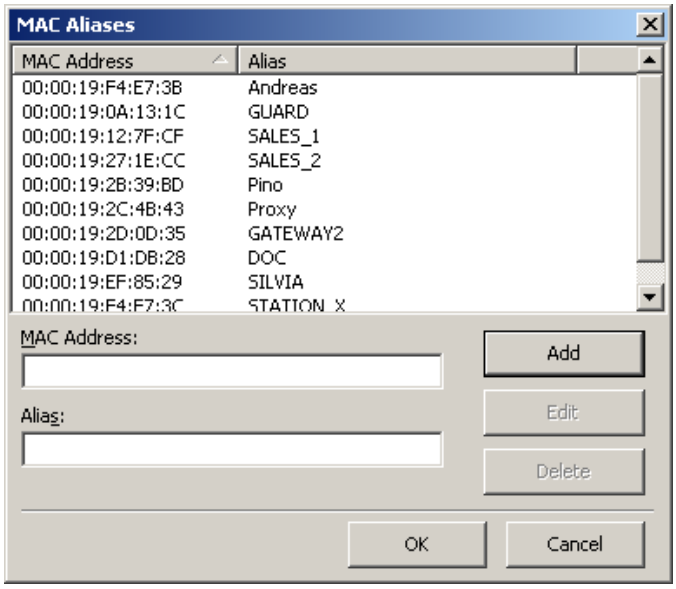
**Report**
Consente di generare automaticamente i report personalizzabili nei formati HTML (inclusi immagine e grafici) oppure testo delimitato da virgole.

È possibile scegliere di generare statistiche sui dati pre-acquisiti oltre a quelle in tempo reale. A questo scopo, caricare un file acquisito in Visualizzatore registro, quindi scegliere **File => Genera statistica**. È anche possibile reimpostare facoltativamente le statistiche raccolte in precedenza visualizzate nella finestra **Statistiche**. Si noti che questa funzione non supporta la distribuzione dei pacchetti sulla timeline, bensì solo la visualizzazione di totali, grafici di protocolli e tabelle host LAN.

# Uso di alias

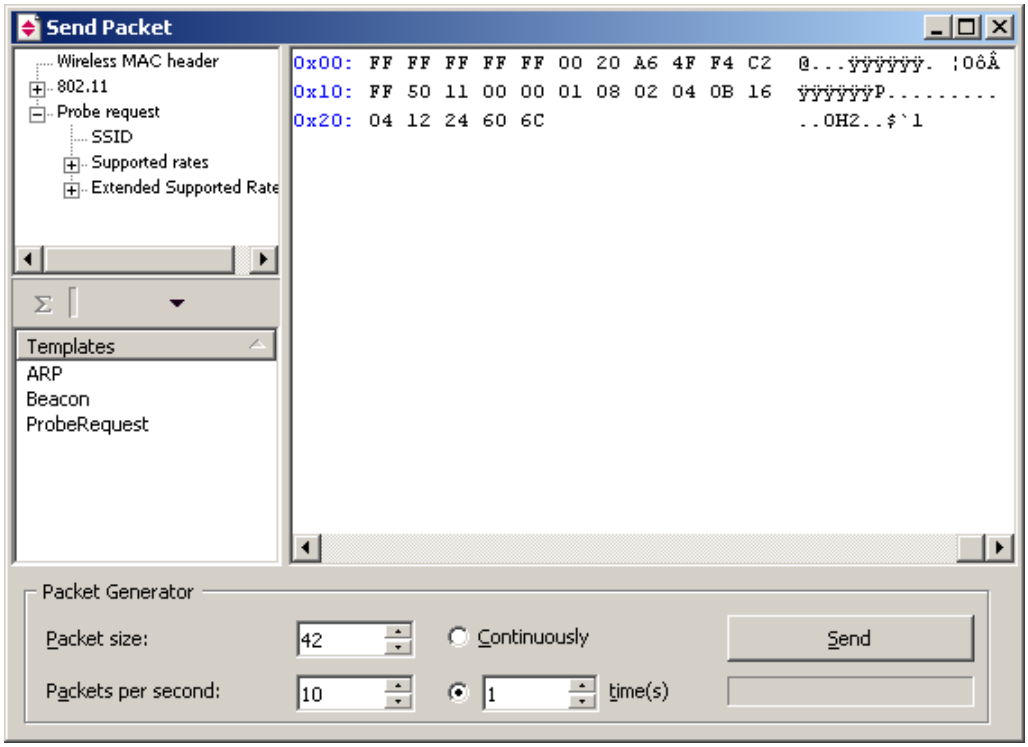
Gli alias sono nomi intuitivi e facili da ricordare utilizzati in CommView al posto di un indirizzo MAC o IP durante la visualizzazione dei pacchetti nelle schede **Pacchetti** e **Statistiche**. Ciò semplifica il riconoscimento e l'analisi dei pacchetti. Ad esempio 00:00:19:2D:0D:35 diventa GATEWAY2 e ns1.earthlink.com diventa MyDNS.

Per aggiungere un alias MAC, fare clic con il pulsante destro del mouse su un pacchetto, quindi scegliere **Crea alias usando MAC di origine** o **Usando MAC di destinazione** dal menu a tendina. Verrà visualizzata una finestra a comparsa con il campo dell'indirizzo MAC già compilato e che richiede solo l'inserimento di un alias. In alternativa, è possibile selezionare **Impostazioni** => **Alias MAC** ... e compilare l'indirizzo MAC e i campi Alias manualmente. Per eliminare un alias o cancellare l'intero elenco di alias, fare clic con il pulsante destro del mouse sulla finestra Alias w scegliere **Elimina record** o **Cancella tutto**. Eseguire la stessa procedura per la creazione degli alias IP. Quando viene creato un nuovo alias IP facendo clic con il pulsante destro del mouse su un pacchetto, il campo alias viene pre-compilato con il nome host corrispondente, se disponibile, che può quindi esser modificato dall'utente.



# Packet Generator

Questo strumento consente di modificare e inviare pacchetti mediante la scheda di rete wireless. Per aprire Packet Generator, scegliere **Strumenti => Packet Generator**, oppure selezionare un pacchetto nella scheda **Pacchetti** o infine fare clic con il pulsante destro del mouse sul pacchetto desiderato e scegliere **Invia pacchetto**.




Leggere le importanti informazioni seguenti sui limiti e le peculiarità relativi all'utilizzo di Packet Generator con le schede di rete:

- Non utilizzare Packet Generator se non si conosce esattamente l'effetto che si desidera ottenere. L'invio di pacchetti può infatti provocare risultati imprevedibili per questo si consiglia di evitare l'utilizzo di questo strumento se non si è un amministratore di rete esperto.
- Packet Generator non supporta le schede di rete precedenti ai modelli 802.11b.
- Alcuni campi nell'intestazione di un pacchetto possono venire modificati dal firmware della scheda prima dell'invio del pacchetto. Ad esempio, i valori Durata e Numero sequenza vengono ignorati dal firmware della scheda e il valore di Altri frammenti è impostato sempre su 0.
- Il firmware della scheda può non riuscire a inviare alcuni pacchetti oppure può inviare gli stessi pacchetti più volte. Ciò è controllato completamente dal firmware e non dall'utente.
- Il firmware della scheda può impedire l'invio dei pacchetti a una frequenza arbitraria. Ad esempio, se si seleziona la velocità di 1000 pacchetti al secondo, è possibile che il firmware invii i pacchetti a una velocità molto inferiore.

Si noti che Packet Generator non può e non deve essere utilizzato per l'invio di flussi TCP a livello di applicazione, ovvero non può occuparsi dell'aumento automatico dei valori SEQ o ACK, della modifica delle checksum e delle dimensioni dei pacchetti e così via. Per inviare un flusso TCP, è necessario utilizzare un'applicazione Winsock creata appositamente per questo scopo. Packet Generator consente di riprodurre i dati pre-acquisiti, di testare i firewall e i sistemi di rilevamento delle intrusioni e di eseguire altre attività specifiche che richiedono un'elaborazione manuale dei pacchetti.

Packet Generator consente di modificare il contenuto dei pacchetti e di visualizzare in una finestra a sinistra il pacchetto decodificato durante l'operazione di modifica. È possibile creare pacchetti di qualsiasi tipo e controllarne completamente il contenuto. Per i pacchetti IP, TCP, UDP e ICMP è possibile correggere automaticamente le checksum con il pulsante **Sigma**.

È anche possibile fare clic sul pulsante con una freccia per visualizzare l'elenco dei modelli di pacchetti disponibili. Il programma include i modelli di pacchetti **TCP**, **UDP** e **ICMP**, più veloci rispetto all'immissione di codici esadecimali nella finestra dell'editor. Questi modelli contengono pacchetti TCP, UDP e ICMP tradizionali, tuttavia può essere opportuno modificare alcuni campi e utilizzare valori in base alle proprie esigenze, come ad esempio indirizzi MAC e IP reali, numeri di porta, numeri SEQ e ACK e così via. È anche possibile utilizzare modelli personalizzati anziché quelli incorporati. È anche possibile trascinare un pacchetto dalla scheda Pacchetti CommView nella sezione Modelli della finestra Packet Generator. Se si trascinano più pacchetti nella sezione Modelli, solo il primo pacchetto verrà utilizzato come modello. Nell'elenco dei modelli viene visualizzata la voce Nuovo modello. Per rinominare un modello, fare clic con il pulsante destro del mouse su di esso nell'elenco, quindi scegliere **Rinomina.** Per eliminare

un modello, fare clic con il pulsante destro del mouse su di esso, quindi scegliere **Elimina** dal menu a comparsa. Se si seleziona un modello nell'elenco, il pacchetto in esso contenuto verrà caricato nella finestra dell'editor per essere modificato prima dell'invio.

È anche possibile inserire i file NCF con i modelli desiderati nella sottocartella TEMPLATES inclusa nella cartella dell'applicazione. Gli eventuali file presenti nella sottocartella TEMPLATES verranno visualizzati nell'elenco a discesa dei modelli disponibili. I file NCF devono contenere un solo pacchetto per file. Tuttavia se si utilizza un file che contiene molti pacchetti, verrà caricato solo il primo pacchetto.

Dopo aver modificato un pacchetto, utilizzare i controlli seguenti per inviarlo:

**Dimensione pacchetto:** consente di modificare la dimensione del pacchetto.
**Pacchetti al secondo:** consente di controllare la velocità con cui vengono inviati i pacchetti.
**Continuamente:** consente di inviare i pacchetti continuamente finché non si seleziona Interrompi.
**Volta/e:** consente di inviare un pacchetto il numero di volte specificato.
**Invia/Interrompi:** consente di inviare i pacchetti o interrompere l'invio.

**Utilizzo di più pacchetti**

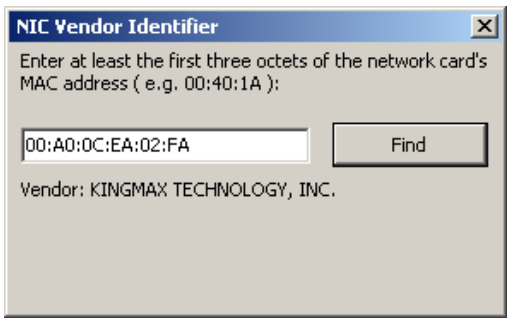
È possibile utilizzare Packet Generator per inviare più pacchetti contemporaneamente. A questo scopo, selezionare i pacchetti che si desidera inviare nell'elenco, quindi richiamare Packet Generator facendo clic con il pulsante destro sul menu, oppure trascinare i pacchetti selezionare nella finestra Packet Generator. In alternativa, è possibile trascinare i file catturati in tutti i formati supportati direttamente nella finestra Packet Generator. Durante l'invio di più pacchetti, la struttura relativa all'editor e al decoder dei pacchetti diventa invisibile.

**Salvataggio di pacchetti modificati**

Per salvare un pacchetto modificato, trascinare la struttura del decoder sul desktop o su una cartella per creare un nuovo file in formato NFC contenente il pacchetto. Il nome del file è sempre PACKET.NCF. È anche possibile trascinare il pacchetto nella finestra dei modelli. Per modificare e inviare più pacchetti, modificare un pacchetto alla volta, trascinarlo sul desktop e rinominarlo. Quindi, aprire una nuova finestra in Visualizzatore registro, trascinare i pacchetti modificati dal desktop sul Visualizzatore registro, selezionarli utilizzando il tasto Maiusc, quindi richiamare Packet Generator con il menu contestuale.

# Identificativo fornitore NIC

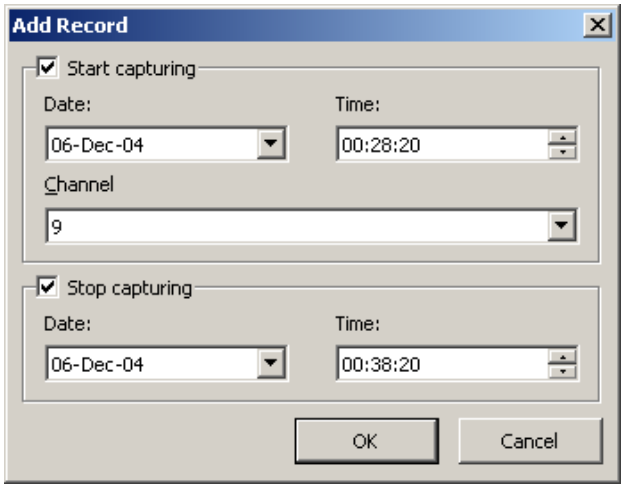
I primi 24 bit dell'indirizzo MAC di una scheda di rete servono a identificare univocamente il fornitore della scheda. Questo numero a 24 bit è denominato OUI ("Organizationally Unique Identifier"). L'identificativo del fornitore NIC è una funzionalità che consente di individuare il nome di un fornitore in base all'indirizzo MAC. A questo scopo, scegliere **Strumenti** =>**Identificativo fornitore NIC**, immettere un indirizzo MAC quindi fare clic su **Trova**. Verrà visualizzato il nome del fornitore. Per impostazione predefinita, in CommView i primi tre ottetti dell'indirizzo MAC vengono sostituiti dal nome del fornitore della scheda di rete nella scheda **Pacchetti**. Per modificare questo comportamento, deselezionare la casella di controllo **Visualizza nome fornitore in indirizzi MAC** nella scheda **Generale** della finestra di dialogo **Opzioni**.




L'elenco dei fornitore è incluso nel file MACS.TXT disponibile nella cartella dell'applicazione CommView. È possibile modificare manualmente questo elenco aggiungendo o modificando le informazioni.

# Pianificatore

È possibile utilizzare questo strumento per creare e modificare attività di acquisizione pianificate. Ciò è utile quando si desidera avviare o interrompere l'acquisizione in CommView nei periodi di inattività, ad esempio di notte o durante il weekend. Per aggiungere una nuova attività, scegliere **Strumenti** => **Pianificatore**, quindi fare clic su **Aggiungi**.




Nel riquadro **Avvia acquisizione** specificare la data e l'ora di inizio acquisizione in CommView. Nell'elenco a discesa **Canale** specificare il canale WLAN da monitorare. In **Interrompi acquisizione** specificare la data e l'ora di fine acquisizione in CommView. Le caselle di controllo **Avvia acquisizione** e **Interrompi acquisizione** non sono obbligatorie. Se si seleziona solo la prima casella di controllo, il processo di acquisizione continuerà finché non viene intercotto manualmente. Se si seleziona solo la seconda casella di controllo, è necessario avviare manualmente il processo di acquisizione che verrà interrotto all'ora specificata.

Se CommView è impostato per acquisire i pacchetti all'ora in cui avverrà l'attività pianificata e la scheda di rete specificata è diversa da quella effettivamente monitorata, il processo di acquisizione verrà interrotto per passare alla scheda di rete specificata. Quindi verrà ripristinato.

Le attività pianificate possono essere eseguite solo quando CommView è in esecuzione.

# Opzioni di configurazione

È possibile configurare alcune opzioni del programma con le voci del menu **Impostazioni**.

### Font

Questo menu consente di impostare il font dell'interfaccia, del testo dei pacchetti e del decodificatore. Per modificare i colori del testo dei pacchetti, utilizzare il menu **Opzioni** (illustrato di seguito).

### Opzioni

#### Generale

**Avvio automatico acquisizione:** selezionare questa casella di controllo per fare in modo che in CommView venga automaticamente avviata l'acquisizione dei pacchetti subito dopo l'avvio del programma. Selezionare nell'elenco a discesa il canale da monitorare.

**Disabilita risoluzione DNS:** selezionare questa casella per impedire le ricerche DNS al contrario degli indirizzi IP in CommView. Se si sceglie di selezionarla, la colonna **Nome host** della scheda **Ultime connessioni IP** sarà vuota.

**Converti valori numerici porte in nomi di servizi:** selezionare questa casella di controllo per visualizzare i nomi dei servizi anziché i numeri. Se si seleziona questa casella, la porta **21** verrà visualizzata come **ftp** e la porta **23** come **telnet**. La conversione dei valori numerici in nomi di servizi viene effettuata mediante il file SERVICES installato da Windows e disponibile nella cartella \Winnt\system32\drivers\etc. Per aggiungere altri nomi di porte e/o servizi, modificare questo file manualmente.

**Converti indirizzi MAC in alias:** selezionare questa casella per sostituire gli indirizzi MAC negli alias della scheda **Pacchetti**. Per assegnare gli alias a un indirizzo MAC, scegliere **Impostazioni => Alias MAC**.

**Converti indirizzi IP in alias:** selezionare questa casella per sostituire gli indirizzi IP negli alias delle schede **Pacchetti** e **Statistiche**. Per assegnare gli alias a un indirizzo IP, scegliere **Impostazioni => Alias IP**.

**Converti indirizzi IP in nomi host nella scheda "Pacchetti":** selezionare questa casella per visualizzare i nomi host risolti anziché gli indirizzi IP nella scheda **Pacchetti**. Se si seleziona questa casella, in CommView verrà innanzitutto cercato un alias per l'indirizzo IP specificato. Se non viene trovato alcun alias oppure se la casella precedente (**Converti indirizzi IP in alias**) non è selezionata, il nome host verrà richiesto dalla cache interna. Se non è possibile trovare alcun nome host, l'indirizzo IP verrà visualizzato come valore numerico.

**Visualizza nomi fornitori negli indirizzi MAC:** per impostazione predefinita in CommView i primi tre ottetti dell'indirizzo MAC vengono sostituiti dal nome del fornitore della scheda di rete nella scheda **Pacchetti**. Per modificare questo comportamento, deselezionare questa casella di controllo.

**Decifratura WEP imposta:** selezionare questa casella se la scheda di rete wireless riporta che per errore sono stati acquisiti pacchetti non cifrati (il flag WEP nell'intestazione 802.11 è impostato su 0). Ciò può capitare con alcune schede di rete in particolare, ad esempio Belkin. Per decifrare questi pacchetti in CommView, è necessario abilitare questa opzione.

**Acquisisci pacchetti danneggiati:** selezionare questa casella per consentire l'acquisizione e la visualizzazione dei pacchetti danneggiati (ovvero contenenti dati completamente o parzialmente non validi) per vari motivi, quali la distanza, le interferenza radio e altri fenomeni fisici. Questa opzione presenta vantaggi e svantaggi. Il vantaggio è che se ci si trova molto distanti dai punti di accesso e/o dalle stazioni WLAN, può danneggiarsi un'alta percentuale di pacchetti. Pertanto, l'abilitazione di questa opzione consente la visualizzazione di un maggior numero di dati, anche se parzialmente danneggiati. Lo svantaggio è che con la visualizzazione dei pacchetti con dati non validi possono venire visualizzati anche pacchetti IP inviati a indirizzi IP inesistenti. Inoltre, quando si seleziona questa casella, il programma tenta di decifrare i pacchetti WEP o WPA in cui il valore di verifica dell'intergità non è corretto ma le intestazioni sembrano essere valide.

**Ignora pacchetti danneggiati nello scanner**: selezionare questa casella per ignorare i pacchetti danneggiati durante la scansione dei canali e tenere in considerazione solo i nodi che trasmettono pacchetti validi.

**Rilevamento nodi attivi mediante PROBE REQUEST:** selezionare questa casella per consentire l'invio periodico dei pacchetti PROBE REQUEST, i quali semplificano il rilevamento dei punti di accesso che non trasmettono il proprio SSID. Si noti che l'utilizzo di questa opzione consente la trasmissione dei pacchetti mediante la scheda di rete che non risulteranno quindi completamente nascosti. Questa opzione non è disponibile per le schede precedenti ai modelli 802.11b.

#### Utilizzo della memoria

#### Visualizzazione

**Numero max pacchetti nel buffer:** consente di impostare il numero massimo di pacchetti che è possibile archiviare nella memoria e visualizzare nell'elenco dei pacchetti (2° scheda). Se ad esempio si imposta questo valore su 3000, solo gli ultimi 3000 pacchetti verranno archiviati nella memoria e quindi visualizzati nell'elenco dei pacchetti. Quanto più alto è il valore impostato tanto maggiori saranno le risorse consumate.

Per accedere a un numero più elevato di pacchetti, si consiglia di utilizzare le funzioni di salvataggio automatico (per ulteriori informazioni, vedere Connessione): ciò consente il dump di tutti i pacchetti in un file di registro sul disco rigido.

**Numero max ultime righe connessioni IP:** consente di impostare il numero di righe che è possibile visualizzare nella scheda Ultime connessioni IP. Se il numero di connessioni supera il limite specificato, le connessioni rimaste attive più a lungo verranno rimosse dall'elenco.

**Buffer driver:** consente di impostare le dimensioni della memoria buffer del driver. Questa impostazione influisce sulle prestazione del programma: quanto maggiore è la memoria allocata per il buffer del driver e tanto minore sarà il numero di pacchetti eliminati. In caso di un traffico LAN non elevato e di connessioni remote, le dimensioni della memoria buffer non sono importanti. Nelle reti WLAN a traffico elevato, invece, può essere opportuno aumentare le dimensioni della memoria buffer se i pacchetti vengono ignorati. Per controllare il numero di pacchetti eliminati, scegliere **File => Dati prestazioni** quando l'acquisizione è attiva.

### Ultime connessioni IP

**Logica di visualizzazione:** consente di selezionare il layout delle ultime connessioni IP più adatto alle proprie esigenze. Scegliere una voce dall'elenco a discesa per visualizzare la descrizione della logica selezionata. In genere si consiglia di utilizzare la logica **Smart** predefinita.

**Definisci indirizzi IP locali:** utilizzare questa funzionalità per monitorare il traffico WLAN contenente molti pacchetti pass-through e una combinazione di indirizzi IP interni ed esterni. In questo caso, CommView for WiFi non "conosce" quali indirizzi IP considerare come locali con il rischio che gli indirizzi IP nelle colonne IP di origine e IP di destinazione vengano invertiti. Questa funzionalità consente di definire gli indirizzi della rete locale e le maschere di sottorete per garantire che la finestra Ultime connessioni IP funzioni correttamente. A questo scopo, è necessario utilizzare la logica **Smart** predefinita.

### Colori

**Colore pacchetto:** consente di impostare i colori per la visualizzazione di diversi tipi di pacchetti (Normali, CRC danneggiati, ICV danneggiati) nella scheda **Pacchetti**.

**Colora intestazioni pacchetti:** consente di colorare il contenuto dei pacchetti. Se si seleziona questa casella di controllo verranno visualizzati i primi otto livelli di pacchetti in diversi colori. Per cambiare un colore, selezionare il tipo di intestazione di cui si desidera cambiare il colore, quindi fare clic nel rettangolo dei colori.

**Evidenzia sintassi formula:** consente di impostare i colori di evidenziazione delle parole chiave nelle formule della finestra Regole avanzate.

**Colore sequenza di byte selezionata:** consente di impostare il colore del font e dello sfondo per la visualizzazione della sequenza di byte selezionata nella struttura del decoder. Se ad esempio si seleziona il nodo della struttura "TCP", la parte corrispondente dei pacchetti verrà evidenziata con questi colori.

### Decodifica

**Espandi sempre tutti i nodi nella finestra decoder:** consente di espandere automaticamente tutti i nodi nelle finestre decoder quando si seleziona un nuovo pacchetto nell'elenco dei pacchetti.

**Decodifica fino al primo livello solo nell'esportazione ASCII:** consente di salvare solo i nodi di primo livello. Questa opzione influenza il formato di decodifica utilizzato quando si esporta un registro di pacchetti o un singolo pacchetto nel formato ASCII per la decodifica. Se ad esempio si salva un pacchetto TCP/IP quando questa opzione è disabitata, verranno salvati tutti i sottonodi di *Tipo di servizio*. Quando questa opzione è abilitata, questi sottonodi non vengono salvati. Selezionare questa casella per rendere il file ASCII di output meno dettagliato e più compatto.

**Ignora checksum errate durante la ricostruzione delle sessioni TCP:** consente di specificare in che modo i pacchetti TCP/IP errati devono essere considerati durante la ricostruzione delle sessioni TCP. Per impostazione predefinita questa opzione è abilitata e i pacchetti con checksum non corrette non vengono ignorati durante il processo di ricostruzione. Se si disattiva questa opzione, i pacchetti con checksum errate verranno ignorati e non visualizzati nella finestra di ricostruzione delle sessioni TCP.

**Decomprimi contenuto GZIP:** consente di convertire il contenuto HTTP compresso con GZIP in formato testo leggibile nelle finestre Ricostruzione sessioni TCP. Il contenuto GZIP viene decompresso solo quando il tipo di visualizzazione nella finestra è impostato su "ASCII."

**Ricostruisci immagini:** consente di convertire i flussi HTTP binari che rappresentano le immagini nei formati JPG, BMP, PNG e GIF nella finestra Ricostruzione sessioni TCP. Le immagini vengono visualizzate solo quando il tipo di visualizzazione nella finestra è impostato su "HTML". Le immagini non vengono mai visualizzate nelle pagine HTML a cui appartengono poiché vengono trasferite dal server in una sessione HTTP separata.

**Tipo di visualizzazione predefinito:** consente di selezionare dall'elenco a discesa il valore per il tipo che si desidera impostare come predefinito per la funzione Ricostruzione sessioni TCP. I valori disponibili sono ASCII, HEX, HTML e EBCDIC.

### Varie

**Nascondi riduzione a icona sulla barra delle applicazioni:** consente di non visualizzare il pulsante del programma sulla barra delle applicazioni di Windows quando si riduce il programma a icona. Se si seleziona questa casella, utilizzare l'icona della barra delle applicazioni del programma per il ripristino dopo la riduzione a icona.

**Chiedi conferma all'uscita dall'applicazione:** consente di visualizzare una richiesta di conferma per la chiusura del programma.

**Scorri automatic. finestra dati pacchetti:** consente di scorrere automaticamente il testo nella finestra dei dati dei pacchetti quando si seleziona un nuovo pacchetto nell'elenco dei pacchetti (solo se il testo non si adatta alla finestra). Questa funzione è utile per visualizzare il contenuto di un pacchetto lungo senza scorrere la finestra manualmente.

**Scorri automatic. elenco pacchetti fino a ultimo pacchetto:** consente di scorrere automaticamente l'elenco dei pacchetti nella scheda **Pacchetti** fino all'ultimo pacchetto ricevuto.

**Ordina automatic nuovi record nelle ultime connessioni IP:** consente di ordinare automaticamente i nuovi record nella scheda Ultime connessioni IP in base ai criteri di ordinamento definiti dall'utente, ad esempio ordine crescente degli indirizzi IP remoti.

**Controllo utilizzo CPU intelligente:** consente di provare a diminuire l'utilizzo della CPU durante l'acquisizione di numerosi dati, a discapito della qualità e della frequenza di aggiornamento delle finestre.

**Esegui all'avvio di Windows:** consente di avviare automaticamente il programma ogni volta che si avvia Windows.

**Esegui ridotto a icona:** consente di avviare il programma con riduzione a icona. Per visualizzare la finestra principale è necessario fare clic sul pulsante della barra delle applicazioni.

### Plug-in

Questa scheda viene utilizzata dai plug-in di terze parti per l'esecuzione di attività di configurazione. Per ulteriori informazioni, vedere Decodifica personalizzata.

# Trova pacchetto

Questa finestra di dialogo (**Cerca => Trova pacchetto**) consente di trovare i pacchetti che corrispondono a un testo specifico. Immettere una stringa di ricerca, selezionare il tipo di informazioni immesse (**Stringa** o **Hex**), quindi fare clic su **Trova successivo** Verranno cercati i pacchetti che soddisfano i criteri di ricerca specificati e quindi visualizzati nella scheda **Pacchetti**.

È possibile immettere il testo come stringa, valore esadecimale oppure indirizzo IP. Se si immettono caratteri non stampabili, è necessario utilizzare una stringa esadecimale, ovvero caratteri esadecimali separati da spazi come AD 0A 02 78 04.

Selezionare **Maiuscole/Minuscole** per includere la distinzione tra maiuscole e minuscole nella ricerca. Selezionare **All'offset** per cercare una stringa che inizia in un determinato offset. Si noti che l'indicatore di offset è un valore esadecimale o basato su zero, quindi se si cerca il primo byte nel pacchetto il valore di offset è pari a 0.

# Riferimento porta

In questa finestra vengono visualizzati i numeri di porta e i nomi dei servizi corrispondenti. Il riferimento è disponibile nel file SERVICES installato da Windows nella cartella **\system32\drivers\etc**. Per aggiungere altri nomi di servizi e/o porte, è possibile modificare manualmente questo file. CommView for WiFi legge questo file all'avvio di modo che le modifiche apportate vengano visualizzate dopo il riavvio del programma.

# Domande frequenti

Questo capitolo include le risposte ad alcune delle domande più frequenti. Le ultime risposte alle domande frequenti sono disponibili in http://www.tamos.com/products/commwifi/faq.php

**D. Quale prodotto è più adatto per una rete wireless in cui è necessario monitorare i pacchetti in ingresso e in uscita: CommView standard non wireless o CommView for WiFi?**
R. È sufficiente l'edizione CommView standard non wireless che consente di monitorare il traffico sul proprio computer ma non sulle altre stazioni WLAN. CommView for WiFi, invece, consente di monitorare anche gli altri computer wireless.

**D. Sono necessari componenti hardware speciali per l'utilizzo di CommView for WiFi?**
R. È necessaria una scheda di rete wireless compatibile. Per un elenco delle schede di rete compatibili, visitare la pagina Web http://www.tamos.com/products/commwifi/. È necessario installare un driver speciale per la scheda di rete fornito in dotazione con CommView for WiFi. Dopo avere installato il driver, la scheda di rete verrà impostata sulla modalità di monitoraggio passivo e non potrà più comunicare con gli altri punti di accesso oppure host wireless. Per ripristinare le funzioni standard della scheda di rete, è necessario effettuare il roll back e/o ripristinare il driver della scheda di rete fornito dal produttore. Tuttavia, questa operazione non è sempre obbligatoria. In base al modello della scheda e al sistema operativo in uso, è possibile utilizzare il driver in doppia modalità: passiva durante l'esecuzione di CommView for WiFi e attiva quando CommView non è in esecuzione. Per ulteriori informazioni sui casi specifici, consultare le note tecniche. Se non è possibile utilizzare la modalità doppia e si desidera preservare la connessione wireless durante l'utilizzo di questo prodotto, può essere opportuno installare due schede di rete: una per il monitoraggio e l'altra per l'esecuzione delle funzioni di rete standard.

Se si sceglie di utilizzare due schede di rete e una è basata sul chipset Atheros, si consiglia di basare la seconda scheda su un altro chipset, perché se entrambe utilizzano Atheros una delle due non funzionerà. Occorre inoltre considerare le dimensioni delle schede di rete: se ad esempio si desidera utilizzare due schede di rete su un notebook non dotato di una scheda di rete wireless incorporata, è possibile provare a utilizzare entrambi gli slot PCMCIA del computer notebook. Ciò potrebbe tuttavia non riuscire soprattutto se le schede di rete sono troppo spesse e quindi non entrare negli slot. Per evitare problemi, può essere opportuno ricorrere a una scheda Proxim ORiNOCO 802.11ag ComboCard, la quale è molto sottile e, una volta inserita nello slot inferiore consente di inserire qualsiasi altra scheda in quello superiore.

**D. Se la scheda in uso non è inclusa nell'elenco dei componenti hardware supportati, cosa bisogna fare?**
R. Innanzitutto, i tipi di schede di rete non supportate sono le seguenti:

- Schede di rete USB.
- Schede di rete 802.11b, eccetto quelle già supportate. Un numero sempre inferiore di produttori crea nuovi modelli di schede di rete 802.11b, le quali sono state quasi completamente sostituite dalle schede 802.11g, 802.11a e 802.11a/b/g combinate.
- Schede di rete basate sui chipset Broadcom finché Broadcom non collabori al supporto.

In secondo luogo, nell'elenco dei componenti hardware compatibili sono incluse solo le schede testate nei nostri laboratori. Sono disponibili numerosi fornitori hardware che utilizzano chipset Atheros, ovvero il chipset supportato principalmente dal nostro prodotto. Naturalmente non possiamo collaudare tutti questi tipi di schede. Se la scheda PCMCIA o PCI 802.11g o 802.11a/b/g in uso è basata sul chipset Atheros, è probabile che la scheda funzioni con il driver esistente. Scaricare l'Utilità di verifica della scheda di rete ed eseguirla sul computer. Se è installata una scheda di rete compatibile, verrà visualizzato il nome dell'utilità. La scheda di rete compatibile può venire visualizzata sotto il nome generico "Scheda di rete wireless Atheros". Questo è normale. Se è stata rilevata una scheda i rete compatibile, è possibile installare CommView for WiFi. Se CommView for WiFi funziona con una scheda di rete non inclusa nell'elenco, comunicarcelo.

Se la scheda in uso NON è basata sul chipset Atheros, può essere opportuno attendere finché non vengono supportati altri chipset anche se non possiamo garantire per alcuna scheda o per i tempi previsti. Inoltre, può essere opportuno acquistare una scheda compatibile dal momento che ormai i costi sono ridotti.

**D. Quale scheda è consigliabile utilizzare con l'applicazione?**
R. Se si dispone già di una scheda di rete inclusa nell'elenco dei componenti hardware compatibili, è molto probabile che non sia necessario sostituirla. Alcune schede sono migliori in termini di sensibilità e possibilità di ignorare frame danneggiati, tuttavia queste differenze non sono critiche. Se si desidera acquistare una nuova scheda di rete, consigliamo il modello 802.11b, poiché gli standard 802.11g e 802.11a sono sempre più diffusi. Le schede di rete più idonee includono la scheda di rete PCMCIA a doppia banda e tre modalità, ad esempio Proxim ORiNOCO ComboCard 8480, Proxim ORiNOCO ComboCard 8481 o D-Link AirXpert DWL-AG650. In genere, le schede di rete PCMCIA offrono prestazioni migliori rispetto alle PCI.

**D. Durante il processo di installazione del driver CommView for WiFi per la scheda di rete in uso, nella finestra di installazione viene visualizzato il seguente messaggio di errore: "Il nome è già utilizzato come nome di servizio o come nome di visualizzazione di servizio". Cosa bisogna fare?**
R. Questo messaggio viene visualizzato quando si tenta di installare il driver CommView for WiFi per più schede di rete o quando si sostituisce la scheda di rete precedente con una nuova, ad esempio la scheda 802.11b, e si desidera utilizzare CommView for WiFi con la nuova scheda 802.11g. Accertarsi che il driver venga utilizzato solo con una scheda per il motivo illustrato nella risposta seguente.

**D. Dopo avere utilizzato una scheda di rete con CommView for WiFi per un determinato periodo, com'è possibile sostituirla con una nuova?**
R. Accertarsi che il driver venga utilizzato solo per una scheda di rete. A questo scopo, eseguire le operazioni seguenti:

- Aprire il Registro di sistema con REGEDIT.
- Individuare la seguente cartella di Registro di sistema: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.
- Cercare le chiavi seguenti: COMMCS, COMMPR e COMMSYM e quindi eliminarle (generalmente è disponibile solo una di queste chiavi).
- Riavviare il computer.

È ora possibile procedere all'installazione del driver di CommView for WiFi seguendo le istruzioni riportate nella Guida all'installazione del driver.

**D. Il programma supporta la modalità 802.11a Turbo?**
R. Sì, purché sia supportato anche dalla scheda di rete in uso. Alcune schede di rete che supportano la modalità 802.11a Turbo sono Linksys WPC55AG e NETGEAR WAG511.

**D. Alcuni canali nella finestra delle opzioni di scansione non sono disponibili. È normale? Com'è possibile monitorare questi canali?**
R. In base al paese, è possibile che la scheda di rete wireless non supporti tutti i canali visualizzati nella finestra delle opzioni di scansione. I canali disponibili in un determinato paese dipendono alle normative in vigore. Negli Stati Uniti, ad esempio, le normative FCC consentono solo l'utilizzo dei canali da 1 a 11 nella banda 802.11b/g. Il firmware delle schede di rete wireless venduto negli Stati Uniti è generalmente configurato con i canali 12 e 13 disabilitati. Ciò non è pratico per gli utenti che devono viaggiare in altre parti del mondo e non possono monitorare localmente i canali disponibili con CommView for WiFi. Può essere opportuno acquistare una scheda di rete in loco oppure utilizzare un'applicazione che consenta di modificare il dominio e l'indicativo di paese in alcune schede di rete. Per scaricare e utilizzare questa applicazione, occorre tenere presente che:

- La sovrascrittura delle impostazioni di paese e di dominio può danneggiare il dispositivo in modo permanente. Eseguire questa operazione a proprio rischio.
- La modifica delle impostazioni di dominio e paese può non essere legale nel proprio paese. Chiedere informazioni al legale della società.
- Per questa applicazione non è disponibile alcun supporto tecnico.
- Questa applicazione funziona SOLO con le schede di rete 802.11 b/g e 802.11 a/b/g basate sui chipset Atheros.

Per scaricare questa applicazione, fare clic qui.

**D. Durante il monitoraggio di una rete WLAN è sicuro che il programma acquisisce tutti i pacchetti inviati e ricevuti?**
R. No. Quando una stazione wireless è connessa e autenticata, tale stazione e i punti di accesso utilizzano un sistema che consente loro di rinviare i pacchetti non ricevuti dall'altra parte o danneggiati durante il tragitto per un determinato motivo, ad esempio per interferenze radio. Nel caso di CommView for WiFi la scheda di rete viene impostata sulla modalità di monitoraggio passivo. Pertanto, la scheda di rete non può inviare "richieste" di rinvio di pacchetti né sapere se i pacchetti sono stati ricevuti. Ciò comporta la perdita dei pacchetti. La percentuale di pacchetti perduti può variare. In genere, quanto più vicine sono le altre stazioni e i punti di accesso e tanto minori saranno i pacchetti non ricevuti.

**D. Il programma supporta la decifratura dei pacchetti WPA**?
R. Sì, in modalità WPA-PSK (sono supportati entrambi i sistemi: TKIP e AES). CommView for WiFi rappresenta il primo e finora l'unico programma di analisi delle reti wireless a supportare la decifratura WPA. Gli altri prodotti supportano solo la cifratura WEP.

**D. Durante la connessione a una rete WLAN con traffico elevato CommView for WiFi aumenta il carico della CPU e/o diventa più lento. Com'è possibile risolvere questo problema?**
Durante la cattura di dati da una porzione della rete molto grande e sovraccarica, l'elaborazione di migliaia di pacchetti al secondo può aumentare significativamente l'utilizzo della CPU e rallentare l'applicazione. Per migliorare le prestazioni del programma, è possibile escludere i pacchetti che non è necessario monitorare. Ad esempio, l'invio di un file di 50 MB tra due computer collegati a una rete WLAN genera circa 40.000 pacchetti NetBIOS a una velocità di 5 MB al secondo che può rallentare l'applicazione. Poiché generalmente non è necessario visualizzare ogni pacchetto NetBIOS inviato, è possibile configurare CommView for WiFi in modo che acquisisca solo i pacchetti IP. CommView for WiFi dispone di un sistema flessibile di filtri che consente di personalizzare l'applicazione in modo da visualizzare solo i pacchetti effettivamente necessari. Per visualizzare solo le statistiche, ovvero gli istogrammi verdi, i grafici a torta e le tabelle host, selezionare **Sospendi output pacchetti** che consente di mostrare i dati sulle statistiche senza visualizzare il traffico dei pacchetti in tempo reale. Per ulteriori informazioni, vedere anche il capitolo Acquisizione di un volume elevato di dati.

**D. Dopo avere avviato il programma, selezionato il canale e iniziato il processo di acquisizione non viene visualizzato alcun pacchetto. Cosa bisogna fare?**
R. Aprire la scheda **Pacchetti**. È possibile che la scheda **Ultime connessioni IP** sia vuota se non sono state immesse le chiavi WEP corrette e la rete WLAN utilizza la cifratura WEP. Se anche la scheda **Pacchetti** è vuota, controllare la barra di stato del programma. Se il numero di pacchetti è in aumento, sono state impostate delle regole che impediscono la visualizzazione dei pacchetti. Scegliere **Regole => Reimposta tutto**, quindi selezionare i tre pulsanti della barra degli strumenti: **Acquisisci pacchetti di dati**, **Acquisisci pacchetti di gestione** e **Acquisisci pacchetti di controllo.** Se il numero di pacchetti sulla barra di stato non è in aumento, è possibile che non ci siano punti di accesso o stazioni wireless attive disponibili e/o rilevate. Se si è assolutamente certi che sono disponibili punti di accesso o stazioni wireless, inviarci una notifica su questo problema.

**D. CommView for WiFi supporta la lettura dei file di registro NCF generati dalla versione standard CommonView non wireless e viceversa??**
R. Sì, CommView for WiFi può leggere i file di registro NFC generati dalla versione CommnView standard non wireless. Inoltre, la versione standard non-wireless può leggere i file di registro NCF generati da CommView for WiFi, tuttavia (a) è necessario installare CommView 4.0 Build 321 o versione successiva e (b) non è possibile visualizzare le colonne specifiche delle connessioni wireless, come ad esempio l'intensità del segnale o il numero di chiave WEP.

**D. È possibile eseguire CommView for WiFi sui computer multiprocessore?**
R. Sì.

**D. Nell'applicazione firewall viene visualizzato un messaggio di avviso che CommView for WiFi sta "tentando di accedere a Internet". Poiché esistono alcuni siti in grado di monitorare gli utenti raccogliendo le informazioni inviate dai loro programmi via Internet perché anche CommonView "tenta di accedere a Internet"?**
R. Gli avvisi visualizzati dal firewall in uso indicano il tentativo di risolvere gli indirizzi IP in nomi host. Poiché CommView deve contattare i server DNS per inviare una query DNS, la visualizzazione di questo avviso è inevitabile. Benché sia possibile disabilitare questa funzione scegliendo Impostazioni => Opzioni => Disabilita risoluzione DNS, occorre tenere presente che in questo caso nella scheda Ultime connessioni IP non potranno venire visualizzati i nomi host. Le query DNS rappresentano l'unico tipo di connessione supportata da CommView. Non esistono altre attività nascoste. Non vendiamo spyware.

**D. Se ci si collega a Windows 2000/XP come utente senza privilegi amministrativi, è necessario scollegarsi e ricollegarsi come amministratore per poter eseguire CommView?**
R. No, è possibile aprire la cartella CommView, fare clic con il pulsante destro del mouse sul file CV.exe tenendo premuto Maiusc, quindi scegliere "Esegui come" dal menu a comparsa. Immettere l'account utente e la password di amministratore nella finestra che viene visualizzata, quindi fare clic su OK per eseguire il programma.

**D. Sono disponibili valide risorse online sulle reti wireless con informazioni sulla relativa protezione e configurazione?**
R. Di seguito è riportato un elenco di alcuni siti validi. Alcuni sono più indicati per i principianti, altri forniscono informazioni dettagliate per i professionisti:

LAN Ethernet wireless: domande generiche sugli standard 802.11/802.11b
http://support.intel.com/support/network/wireless/sb/CS-008409.htm
Esercitazione su Wi-Fi Planet
http://www.wi-fiplanet.com/tutorials/
Zone degli standard wireless IEEE
http://standards.ieee.org/wireless/
Sicurezza wireless WPA per le reti domestiche
http://www.microsoft.com/WindowsXP/expertzone/columns/bowman/03july28.asp
Configurazione delle reti wireless IEEE 802.11b Windows XP per abitazioni e piccoli uffici
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx
Evoluzione della sicurezza wireless nelle reti 802.11: standard WEP, WPA e 802.11
http://www.sans.org/rr/papers/68/1109.pdf
SICUREZZA: protezione delle reti LAN wireless nel dettaglio
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

# Argomenti avanzati

## Errori CRC e ICV

**Errori CRC**

Ciascun componente wireless è costituito dai seguenti componenti di base:

- Un'intestazione MAC che include le informazioni sul controllo delle sequenze, l'indirizzo, la durata e controllo dei frame.
- Un corpo frame di lunghezza variabile con le informazioni specifiche sul tipo di frame.
- Un frame FCS (frame check sequence) con CRC (cyclic redundancy code) di 4 byte.

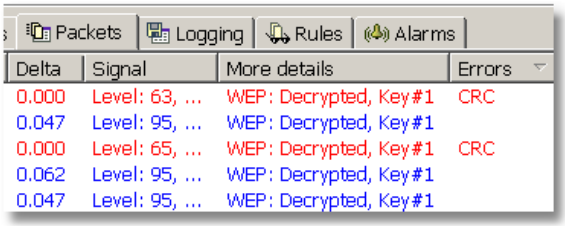
L'ultimo componente FCS è utilizzato per controllare l'integrità del pacchetto sulla parte ricevente, la quale elabora il valore CRC sul frame ricevuto e lo confronta con i quattro byte alla fine del pacchetto. Se i valori non corrispondono, il pacchetto viene considerato danneggiato.

Il modo in cui CommView for WiFi gestisce i frame danneggiati dipende dalle impostazione definite dall'utente. Per impostazione predefinita, questi frame vengono ignorati dall'applicazione con le eccezioni seguenti:

- Incrementano il numero complessivo di byte e pacchetti.
- Incrementano il numero di errori CRC nella scheda **Canali.**
- Sono inclusi nel grafico Dimensioni pacchetti della finestra **Statistiche**.

I frame danneggiati non vengono considerati negli altri grafici e tabelle per ovvie ragioni: nessuna parte di un frame con valore CRC errato è credibile. Può includere un indirizzo IP danneggiato, carico utile di dati e così via anche se nella vita reale questi frame sono simili all'originale. Per lo stesso motivo, non è possibile attribuire gli errori CRC a un particolare punto di accesso o a una stazione wireless e, inoltre, non è possibile determinare l'indirizzo MAC reale del mittente.

Tuttavia, l'utente può scegliere di selezionare la casella **Acquisisci frame danneggiati** nelle opzioni per fare in modo che i frame danneggiati vengano visualizzati nell'elenco dei pacchetti. Per impostazione predefinita questi frame sono contrassegnati in rosso e presentano l'identificativo "CRC" nella colonna **Errori** della scheda **Pacchetti**:




Si noti che un frame ricevuto con un errore in CommView for WiFi può essere stato ricevuto dal nodo di destinazione senza tale errore. A parte il fatto che i frame danneggiati dovrebbero venire ignorati dal nodo di destinazione senza ulteriori elaborazioni, in CommView for WiFi verrà eseguito il tentativo di decodificare e persino decifrare questi frame.

Non tutte le schede di rete wireless riescono a passare i frame danneggiati a livello di applicazione. Questa funzionalità è garantita solo per le nuove schede di rete 802.11g e 802.11a/b/g supportate da CommView for WiFi.

**Errori ICV**

Il valore ICV (Integrity Check Value) rappresenta una checksum a 4 byte utilizzata nei frame WEP e WPA per verificare il risultato della decifratura. La parte ricevente elabora il valore ICV sulla porzione di dati del frame ricevuto e confronta il valore calcolato con i quattro byte alla fine della porzione di dati del pacchetto. Se i valori non corrispondono, l'operazione di decifratura viene considerata come non riuscita.

CommView for WiFi supporta la decifratura WEP e WPA in fase di esecuzione, purché vengano immesse dall'utente le chiavi WEP/WPA corrette. Le informazioni ICV vengono visualizzate in tre diverse posizioni: nelle schede **Nodi** e **Canali** e nella colonna **Errori** della scheda **Pacchetti**. Il modo in cui gli errori ICV vengono visualizzati e calcolati dal programma dipende dall'immissione della chiave e dalla relativa correttezza. Sono disponibili tre diverse alternative:

1. L'utente ha immesso una chiave corretta per la rete WLAN specificata.
2. L'utente ha immesso una chiave non corretta per la rete WLAN specificata.
3. Non è stata immessa alcuna chiave.

Nel primo caso, verranno riportati pochi errori ICV. Nel secondo caso, tutti i frame di dati acquisiti verranno contrassegnati con il flag Errore ICV perché quando per la cifratura viene utilizzata una chiave errata, i valori calcolati e quelli ICV reali non corrispondono. Nel terzo caso, nessun frame includerà errori ICV perché non viene effettuato alcun tentativo di decifratura.

Come già illustrato, gli errori CRC sono di tipo hardware mentre quelli ICV sono di tipo software poiché dipendono dalla chiave di decifratura. Se in CommView for WiFi si immette la chiave WEP errata, verranno segnalati molti errori ICV anche se la rete WLAN è perfettamente funzionante. Poiché gli errori ICV sono di tipo software, i pacchetti con questo tipo di errori vengono visualizzati per

impostazione predefinita nello stesso colore degli altri pacchetti. Per modificare questo comportamento, utilizzare la finestra di dialogo Opzioni del programma.

Se un frame presenta un errore CRC, il rilevamento di un errore ICV non ha alcuna importanza. Per questo motivo, in CommView for WiFi il flag degli errori ICV non viene mai impostato per i frame con errori CRC.

# Decifratura WPA

Come già menzionato nella presente documentazione, CommView for WiFi supporta la decifratura del traffico di rete WEP e WPA in fase di esecuzione. Per utilizzare questa funzionalità, è necessario conoscere i principi di crittografia.

**WEP** (**Wired Equivalent Privacy**) è un sistema per la sicurezza dei dati nelle reti wireless. La tecnologia WEP consente agli amministratori di definire un gruppo di chiavi, o solo una chiave, per la rete WLAN. Queste chiavi vengono condivise tra i client e i punti di accesso e utilizzate per cifrare i dati prima che vengano trasmessi. Se un client non dispone di una chiave WEP corretta, non è possibile decifrare i pacchetti ricevuti o inviare dati ad altri client per impedire accessi e ascolti non autorizzati. La decifratura WEP è semplice finché si immette la chiave corretta, rappresenta un sistema di cifratura statico e indipendente. Ciò significa che è sufficiente immettere la chiave corretta nella finestra di dialogo Chiavi WEP/WPA, per consentire la decifratura immediata dei pacchetti in CommView for WiFi.

**WPA (Wi-Fi Protected Access)** sostituisce lo standard WEP meno sicuro. WPA risolve molti dei problemi di privacy e sicurezza WEP, aumentando significativamente il livello di protezione dei dati e di controllo degli accessi nelle reti WLAN. A differenza della tecnologia WEP, WPA rappresenta un sistema di cifratura dinamico basato sulla ridigitazione, su chiavi pre-stazione univoche e su molte altre misure che migliorano la sicurezza. La tecnologia WPA supporta due modalità: PSK (Pre-Shared Key) ed Enterprise diverse in molti aspetti. CommView for WiFi supporta la decifratura WPA in modalità PSK.

Considerata la natura dinamica della cifratura WPA, la sola immissione della passphrase WPA non è sufficiente per la decifratura del traffico. A questo scopo, è necessario che durante lo scambio delle chiavi mediante il protocollo EAPOL, CommView for WiFi sia in esecuzione in modalità di acquisizione dei pacchetti. Inoltre, è importante che tutti i pacchetti di scambio delle chiavi EAPOL vengano acquisiti correttamente. Un pacchetto EAPOL mancante o danneggiato, infatti, può impedire in CommView for WiFi la decifratura dei pacchetti che verranno quindi inviati verso e dalla stazione specificata e potrebbe essere necessario acquisire la successiva conversazione EAPOL tra la stazione e il punto di accesso. Ciò rappresenta una significativa differenza tra le modalità di cifratura WEP e WPA.

In base ai principi sopra descritti, dopo aver immesso la passphrase WPA, avere chiuso la finestra di dialogo Chiavi WEP/WPA e avere avviato l'acquisizione dei pacchetti, è necessario attendere l'autenticazione successiva e l'evento di scambio dei dati prima che i pacchetti relativi alla stazione in oggetto possano essere autenticati. Naturalmente, può capitare che vengono decifrati i pacchetti in viaggio verso e da un determinato client piuttosto che un altro perché non sono ancora stati acquisiti i pacchetti EAPOL di tutti i client.

Per attivare la ri-autenticazione, riavviare i punti di accesso di tutte le stazioni autenticate o riconnettere alla rete il client in questione. Nelle successive versioni di CommView for WiFi è probabile che venga aggiunta una tecnologia per forzare il processo di ri-autenticazione.

# Acquisizione di un volume elevato di dati

Durante l'acquisizione di dati da una porzione di rete molto grande e sovraccarica, occorre ricordare che l'elaborazione di migliaia di pacchetti al secondo può aumentare significativamente l'utilizzo della CPU e rallentare l'applicazione. Per ottimizzare le prestazioni del programma, utilizzare le regole per escludere i pacchetti che non devono essere monitorati. Ad esempio, l'invio di un file di 50 MB tra due computer collegati a una rete WLAN genera circa 40.000 pacchetti NetBIOS a una velocità di 5 MB al secondo che può rallentare l'applicazione. Poiché generalmente non è necessario visualizzare ogni pacchetto NetBIOS inviato, è possibile configurare CommView for WiFi in modo che acquisisca solo i pacchetti IP. CommView for WiFi dispone di un sistema flessibile di filtri che consente di personalizzare l'applicazione in modo da visualizzare solo i pacchetti effettivamente necessari. Per visualizzare solo le statistiche, ovvero gli istogrammi verdi, i grafici a torta e le tabelle host, selezionare "Sospendi output pacchetti" che consente di mostrare i dati sulle statistiche senza la visualizzazione dei pacchetti in tempo reale.

I seguenti fattori aiutano a migliorare le prestazioni del programma:

- CPU veloce (Pentium IV consigliato)
- RAM (128 e superiore consigliata)
- Utilizzo delle regole per l'esclusione del traffico non necessario

# Esecuzione di CommView for WiFi in modalità invisibile

Sono disponibili due metodi per eseguire CommView in modalità nascosta:

1. Avviare CommView con l'opzione "hidden", vale a dire:

   CV.EXE hidden

2. Se CommView è già in esecuzione, è possibile nasconderlo e/o mostrarlo mediante il "tasto di scelta". Per nascondere l'applicazione, premere la combinazione di tasti ALT+MAIUSC+h. Per mostrare l'applicazione, premere la combinazione di tasti ALT+MAISC+u.

Non è possibile nascondere completamente un'applicazione Windows. Durante l'esecuzione in modalità invisibile, CommView può comunque essere mostrata mediante un'apposita utilità di elenco dei processi in esecuzione. In Windows NT/2000/XP/2003 questa utilità è parte di Task Manager.

# Parametri della riga di comando

È possibile utilizzare i parametri della riga di comando per eseguire le operazioni seguenti all'avvio del programma:

- Caricare e attivare un gruppo di regole da un file. Utilizzare l'opzione "/ruleset" seguita dal nome del file e dal percorso completo, ad esempio:

  CV.EXE /ruleset "C:\Programmmi\CommViewWiFi\Rules\POP3Rules.rls"

  Se il nome di un file o il relativo percorso contiene degli spazi, è necessario racchiuderlo tra virgolette (" ").

- Caricare e attivare un gruppo di chiavi WEP/WPA da un file. Utilizzare l'opzione "/keyset" seguita dal nome del file e dal percorso completo, ad esempio:

  CV.EXE /keyset "C:\Programmi\CommViewWiFi\WLAN3Keys.wep"

  Se il nome di un file o il relativo percorso contiene degli spazi, è necessario racchiuderlo tra virgolette (" ").

- Utilizzare la cartella specificata per l'archiviazione dei file di registro. Utilizzare l'opzione /logdir seguita dal percorso completo della cartella, ad esempio:

  CV.EXE /logdir "C:\Programmi\CommView\Logs"

È possibile utilizzare tutti questi parametri contemporaneamente.

# Scambio di dati con l'applicazione in uso

CommView fornisce un'interfaccia TCP/IP intuitiva che consente di elaborare i pacchetti acquisiti da CommView con l'applicazione in uso in tempo reale. A partire dalla versione 5.0 è anche possibile utilizzare questa interfaccia per inviare i pacchetti (in modo simile alla funzione Packet Generator di CommView).

**Funzionamento**
CommView può essere avviato con uno speciale argomento della riga di commando "MIRROR" che indica al programma di eseguire il mirroring dei pacchetti acquisiti sull'indirizzo IP o sulla porta TCP desiderata.

Esempi:
CV.EXE mirror:127.0.0.1:5555 // esegue il mirroring dei pacchetti sull'indirizzo di loopback, porta TCP 5555
CV.EXE mirror:192.169.0.2:10200 // esegue il mirroring dei pacchetti su 192.169.0.2, porta TCP 10200

Quando si avvia CommView con un'opzione simile a questa, il programma prova a stabilire una sessione TCP collegandosi all'indirizzo IP e al numero di porta specificati. Pertanto, è necessario che l'applicazione in uso sia già in esecuzione e in ascolto della porta specificata. Se CommView non riesce a stabilire una connessione, eseguirà un nuovo tentativo ogni 15 secondi. Lo stesso vale se la connessione si interrompe: CommView proverà a ristabilire la connessione ogni 15 secondi. Se la connessione viene stabilita, i pacchetti acquisiti vengono inviati all'indirizzo IP specificato non appena arrivano, in tempo reale.

**Formato dei dati**

I dati vengono trasmessi nel formato NCF. Per una descrizione di questo formato, fare riferimento alla sezione Formato dei file di registro CommView.

**Invio di pacchetti**

CommView supporta la ricezione e anche l'invio dei pacchetti come se si stesse utilizzando Packet Generator. È possibile inviare i dati a CommView con la stessa connessione TCP utilizzata per la ricezione dei dati. Il formato dei dati è semplice: è necessario inviare la lunghezza del pacchetto (un valore intero di due byte senza segno nell'ordine standard little-endian) seguito dal pacchetto stesso. Se la scheda di rete non è aperta o non supporta l'introduzione di pacchetti, il pacchetto viene ignorato in modalità invisibile.

**Progetti di esempio**
Sono disponibili due applicazioni dimostrative di esempio che ascoltano le connessioni in ingresso, estraggono i pacchetti dal flusso e visualizzano i dati non elaborati (raw).

- http://www.tamos.com/products/commview/samp_mirr_c5.zip. Progetto Visual Studio con il codice sorgente C++.
- http://www.tamos.com/products/commview/samp_mirr_d5.zip. Progetto Delphi con il codice sorgente Pascal. Per compilare il progetto, è necessaria la popolare suite di componenti ICS di Francois Piette, disponibile all'indirizzo http://www.overbyte.be.

**Larghezza di banda**
Durante il mirroring dei dati su un computer remoto, verificare che il collegamento tra CommView e il computer sul quale viene effettuato il mirroring sia sufficientemente veloce da trasferire tutti i dati in corso di acquisizione. Se ad esempio in CommView la velocità di acquisizione è pari a 500 Kbyte al secondo e la connessione può gestire solo 50 Kbyte al secondo, si verificherà un intasamento del traffico che potrebbe comportare vari problemi, ad esempio Winsock potrebbe interrompere l'invio dei dati in alcune versione di Windows.

# Decodfica personalizzata

CommView for WiFi consente di utilizzare due tipi di decoder personalizzati.

**Decoder semplice**

Se si implementa questo tipo di decoder, l'output corrispondente verrà visualizzato nella colonna aggiuntiva della scheda **Pacchetti**. Il decoder deve corrispondere a un file DLL a 32 bit di nome "Custom.dll" che esporti l'unica routine denominata "Decode." Il prototipo di questa routine è visualizzato in C e Pascal:

```
extern "C" {
  void __stdcall Decode(unsigned char *PacketData, int PacketLen, char *Buffer, int BufferLen);
}

procedure Decode (PacketData: PChar; PacketLen: integer; Buffer: PChar; BufferLen: integer); stdcall;
```

Il file DLL deve essere incluso nella cartella dell'applicazione CommView. All'avvio di CommView, il file "Custom.dll" viene cercato nella cartella dell'applicazione e quindi caricato nella memoria. Se viene individuata la voce "Decode", viene aggiunta la nuova colonna "Personalizzato" nell'elenco dei pacchetti.

Quando viene acquisito un nuovo pacchetto, prima che venga visualizzato in CommView viene chiamata la routine "Decode" e il contenuto del pacchetto viene passato al file DLL. La routine "Decode" deve elaborare i dati dei pacchetti e copiare il risultato nella memoria buffer fornita. Il primo argomento corrisponde al puntatore ai dati del pacchetto, il secondo argomento è la lunghezza dei dati, il terzo argomento è il puntatore alla memoria buffer in cui devono essere copiati i risultati della decodifica e il quarto argomento corrisponde alle dimensioni del buffer (attualmente sempre 1024). La memoria buffer viene allocata e liberata da CommView, pertanto non provare a riallocarla o liberarla. Il risultato copiato nella memoria buffer verrà visualizzato come stringa nella colonna "Personalizzata".

La routine deve essere sufficientemente veloce da gestire migliaia di pacchetti al secondo per non rallentare l'applicazione. Non dimenticare di utilizzare la convenzione di chiamata STDCALL.

Sono disponibili due DLL che dimostrano un'operazione molto semplice: l'output della funzione "Decode" corrisponde al codice esadecimale dell'ultimo byte del pacchetto. Il decoder personalizzato può essere complesso fino al livello desiderato.

- http://www.tamos.com/products/commview/cust_decoder_c.zip. Progetto Visual Studio con codice sorgente C++.
- http://www.tamos.com/products/commview/cust_decoder_d.zip. Progetto Delphi con codice sorgente Pascal.

**Decoder complesso**

Se si implementa questo tipo di decoder, l'output corrispondente verrà visualizzato come elemento aggiuntivo nella struttura dei decoder dei pacchetti. Per ulteriori informazioni sull'implementazione di questo tipo di decoder, scaricare il file seguente:

http://www.tamos.com/products/commview/complex_decoder_c5.zip

Questo tipo di decoder può essere scritto solo in Microsoft Visual C++ poiché è incorporato mediante le classi C++.

**Supporto tecnico**

Il nostro team del Supporto tecnico mette a disposizione la propria esperienza per i decoder personalizzati, tuttavia non può rispondere ai problemi di programmazione.

# Formato dei file di registro di CommView

CommView e CommView for WiFi utilizzano il formato di dati riportato di seguito per la scrittura dei pacchetti nei file .NCFs. Rappresenta un formato aperto che consente di elaborare i file di registro generati da CommView nelle applicazioni in uso e per lo scambio dei dati direttamente con l'applicazione (sistema descritto in questo file della Guida).

I pacchetti vengono registrati consecutivamente. A ciascun corpo del pacchetto viene aggiunta un'intestazione di 24 byte, la cui struttura è illustrata di seguito. Tutti i campi di intestazione con lunghezza superiore a 1 byte utilizzano l'ordine di byte little-endian.

| Nome campo | Lunghezza (byte) | Descrizione |
|---|---|---|
| Lunghezza dati | 2 | Lunghezza del corpo del pacchetto che segue l'intestazione |
| Lunghezza dati di origine | 2 | Lunghezza originale del corpo del pacchetto che segue l'intestazione, senza compressione. Se non viene utilizzata alcuna compressione, il valore di questo campo è uguale al valore del campo precedente. |
| Versione | 1 | Versione del formato del pacchetto (0 per l'implementazione corrente) |
| Anno | 2 | Data del pacchetto (anno) |
| Mese | 1 | Data del pacchetto (mese) |
| Giorno | 1 | Data del pacchetto (giorno) |
| Ore | 1 | Ora del pacchetto (ore) |
| Minuti | 1 | Ora del pacchetto (minuti) |
| Secondi | 1 | Ora del pacchetto (secondi) |
| Microsecondi | 4 | Ora del pacchetto (microsecondi) |
| Flag | 1 | Flag bit:<br>Medio — 0…3 — Tipo medio per il pacchetto (0 - Ethernet, 1 - WiFi, 2 - Token Ring )<br>Decifrato — 4 — Il pacchetto è stato decifrato (applicabile solo ai pacchetti WiFi)<br>Interrotto — 5 — Il pacchetto è stato danneggiato, ovvero presenta un valore CRC errato (applicabile solo ai pacchetti WiFi)<br>Compresso — 6 — Il pacchetto è archiviato in formato compresso<br>Riservato — 7 — Riservato |
| Livello segnale | 1 | Livello del segnale in percentuale (applicabile solo ai pacchetti WiFi) |
| Velocità | 1 | Velocità di trasmissione dei dati in Mbps moltiplicata per 2 (applicabile solo i pacchetti WiFi) |
| Banda | 1 | Banda di trasmissione. 0x01 per 802.11a, 0x02 per 802.11b, 0x04 per 802.11g, 0x08 per 802.11a-turbo, 0x10 per 802.11 SuperG. (applicabile solo ai pacchetti WiFi) |
| Canale | 1 | Numero di canale (applicabile solo ai pacchetti WiFi) |
| Direzione | 1 | Direzione di un pacchetto. 0x00 per pass-through, 0x01 per in ingresso, 0x02 per in uscita (non applicabile ai pacchetti WiFi) |
| Riservato | 2 | Riservato |
| Dati | ... | Corpo del pacchetto (non modificato, come trasmesso sul supporto). Se è impostato il flag di compressione, i dati verranno compressi mediante la libreria Zlib 1.1.4 pubblicamente disponibile. La lunghezza di questo campo è registrata in Lunghezza dati. |

La lunghezza totale del titolo è pari a 24 byte.
Se i pacchetti vengono archiviati in formato compresso, nel campo Lunghezza dati sarà disponibile la lunghezza dei dati dopo la compressione mentre il campo Lunghezza origine conterrà la lunghezza originale dei dati. Se un pacchetto non è compresso, entrambi i campi presenteranno lo stesso valore.

# Informazioni

## Per acquistare CommView for WiFi

Questo programma è una versione di valutazione valida per 30 giorni.

Il prezzo della versione completa e senza limitazioni del programma è di 499 dollari.

I clienti che hanno già acquistato l'edizione CommView standard non wireless possono usufruire di un notevole sconto. Per ulteriori dettagli, visitare il nostro sito Web.

Una copia in licenza di CommView può essere utilizzata da una sola persona su uno o più computer oppure installata su una singola workstation utilizzata non contemporaneamente da più persone, ma non entrambe. Se è necessario acquistare il prodotto per più utenti, visitare il nostro sito Web per i prezzi delle licenze multiutente.

Gli utenti registrati riceveranno:

- Una copia completa senza limitazioni del programma
- Aggiornamenti gratuiti che verranno rilasciati entro 1 anno dalla data di acquisto
- Informazioni sugli aggiornamenti e i nuovi prodotti
- Supporto tecnico gratuito

Accettiamo pagamenti con carte di credito, per telefono o fax, assegni, ordini di acquisto e bonifici bancari. I prezzi, i termini e le condizioni sono soggetti a modifiche senza preavviso. Per le ultime offerte sui prodotti e i prezzi aggiornati, visitate il nostro sito Web.

http://www.tamos.com/order/

# Informazioni sui contatti

## Web

http://www.tamos.com

## E-mail

sales@tamos.com (per informazioni sulle vendite)
support@tamos.com (per tutte le altre richieste)

## Indirizzo di posta numero di fax

Indirizzo di posta:

PO Box 1385
Christchurch 8015
Nuova Zelanda

Fax: +64 3 359 0392 (Nuova Zelanda)
Fax: +1 917 591-6567 (USA)

# Altri prodotti TamoSoft

**CommView**

CommView è un programma per il monitoraggio di Internet e delle reti LAN (Local Area Network) in grado di acquisire e analizzare i pacchetti in rete. Raccoglie le informazioni sui dati che attraversano la connessione remota o la scheda e quindi decodifica i dati analizzati. Con CommView è possibile visualizzare l'elenco delle connessioni di rete e le statistiche IP importanti a livello di singolo pacchetto. I pacchetti vengono decodificati fino al livello inferiore con l'analisi completa dei più diffusi protocolli. È anche disponibili il totale accesso ai dati non elaborati in tempo reale. CommView è uno strumento molto utile per gli amministratori delle reti LAN, i professionisti della sicurezza, i programmatori di reti o tutti colori che desiderano avere una panoramica completa del traffico che attraversa il computer o la porzione di rete LAN in uso.

Ulteriori informazioni

**CommTraffic**

CommTraffic rappresenta una utilità per la rete che consente di raccogliere, elaborare e visualizzare le statistiche sull'utilizzo della rete e il traffico relative alle connessioni di rete, incluse quelle remote e LAN, per ciascun computer collegato. Questa applicazione offre un'interfaccia molto accattivante e personalizzabile con un menu icona opzionale nella barra delle applicazioni che mostra le statistiche generiche sulla rete. È anche possibile generare report che riflettono il volume del traffico in rete e gli eventuali costi di connessione Internet. CommTraffic supporta virtualmente qualsiasi piano tariffario ISP, ad esempio quelli basati sul tempo di connessione, sul volume dei dati, sull'orario e così via. È anche possibile impostare la visualizzazione di avvisi quando vengono raggiunti determinati criteri, ad esempio il volume del traffico, i costi e così via. La configurazione guidata semplifica notevolmente il processo di configurazione e rileva automaticamente le impostazioni della connessione e della rete.

Ulteriori informazioni

**SmartWhois**

SmartWhois è un utile strumento che consente di ottenere informazioni su qualsiasi dominio, nome host e indirizzo IP del mondo. A differenza delle altre utilità whois, distribuisce automaticamente le informazioni associate a un dominio o indirizzo IP, indipendentemente dalla regione geografica in cui è stato registrato. In pochi istanti è possibile ottenere tutte le informazioni desiderate su un utente: dominio, nome della rete, paese, stato o provincia e città. Anche se non è possibile risolvere un indirizzo su un nome host, SmartWhois non fallirà.

Ulteriori informazioni

**Essential NetTools**

Essential NetTools è un gruppo di strumenti per la rete utile per la diagnosi delle reti e il monitoraggio delle connessioni di rete di un computer. È una soluzione molto efficiente per tutti coloro che desiderano utilizzare quotidianamente strumenti di rete molto affidabili. Questa soluzione include l'utilità NetStat che visualizza le connessioni di rete e le porte aperte del computer mappandole con l'applicazione in uso. Supporta inoltre lo scanner NetBIOS, uno strumento di auditing NetBIOS per il controllo della sicurezza LAN e un controllore delle connessioni esterne sulle risorse condivise del computer nonché un monitor di processi che visualizza le informazioni su tutti i programmi e i servizi in esecuzione sul computer. Sono integrati altri strumenti utili, quali Ping, TraceRoute e NSLookup. Le altre funzioni disponibili includono la generazione di report nei formati HTML, testo e CSV e un'interfaccia personalizzabile. Questo programma rappresenta una soluzione efficiente e intuitiva che può essere utilizzata al posto di applicazioni Windows, quali nbtstat, netta e NetWatcher. Incorpora molte funzioni avanzate non supportate dagli strumenti Windows standard.

Ulteriori informazioni

**DigiSecret**

DigiSecret rappresenta un'applicazione efficiente, sicura e facile da utilizzare per la cifratura e la condivisione dei file. Si basa su algoritmi di cifratura avanzati e comprovati per la creazione di archivi cifrati, di file EXE a estrazione automatica e la condivisione dei file con colleghi e amici. DigiSecret include inoltre un'efficace sistema di compressione dei file. Non sono più necessari file nel formato ZIP quando è possibile creare file DigiSecret cifrati e compressi. Questo programma è integrato nella shell di Windows. Per elaborare i file, è sufficiente fare clic con il pulsante destro del mouse su di essi. Sono supportate anche le operazioni di trascinamento.

Ulteriori informazioni