

Configurazione dell'acquisizione pacchetti su un access point WAP125 o WAP581

Obiettivo

La funzione Packet Capture consente di catturare e memorizzare i pacchetti ricevuti e trasmessi dal punto di accesso wireless (WAP). I pacchetti acquisiti possono quindi essere analizzati da un analizzatore di protocolli di rete per la risoluzione dei problemi o l'ottimizzazione delle prestazioni. Esistono due metodi di acquisizione dei pacchetti:

- Salva file sul dispositivo - I pacchetti catturati vengono archiviati in un file sul WAP. Il protocollo WAP può inoltre inviare il file a un server TFTP (Trivial File Transport Protocol). Il file Administration Packet Capture è formattato in formato pcap e può essere esaminato utilizzando strumenti come Wireshark e OmniPeek.
- Stream to a Remote Host - I pacchetti acquisiti vengono reindirizzati in tempo reale a un computer esterno che esegue lo strumento Wireshark.

Questo articolo ha lo scopo di spiegare e guidare l'utente nella configurazione di Packet Capture su un WAP e ricevere queste acquisizioni di pacchetti in locale o in remoto.

Dispositivi interessati

- WAP125
- WAP581

Versione del software

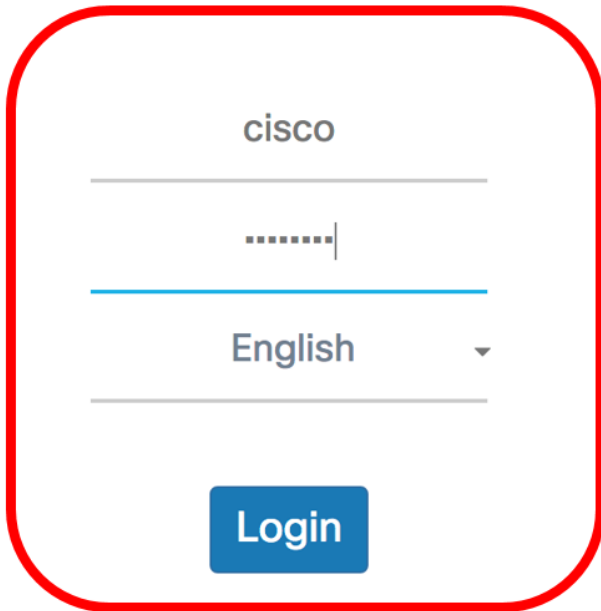
- 1.0.0.4 - WAP581
- 1.0.0.5 - WAP125

Configura impostazioni di acquisizione pacchetti

Passaggio 1. Accedere all'utilità basata sul Web di WAP. Il nome utente e la password predefiniti sono cisco/cisco.



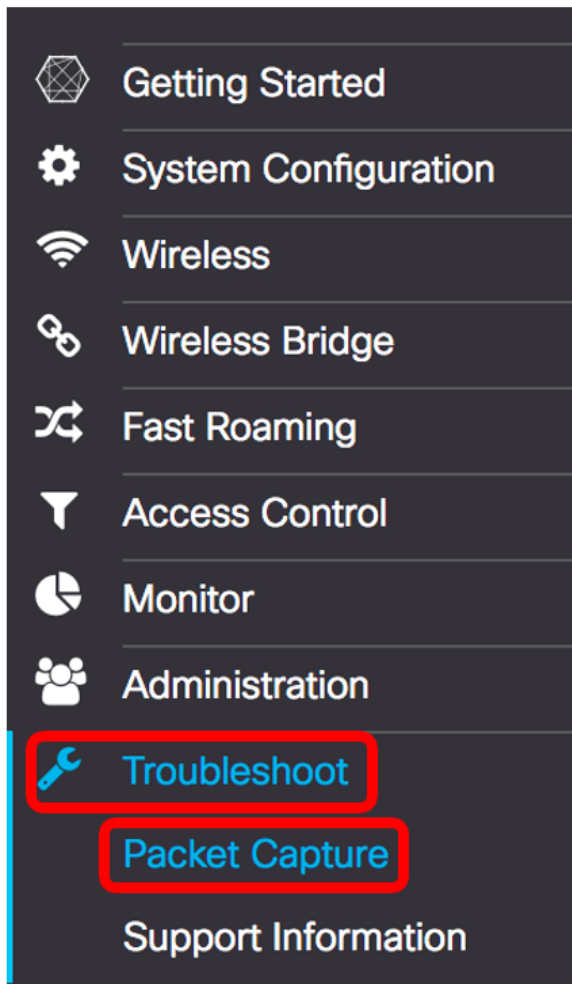
Wireless Access Point

A screenshot of the Cisco Wireless Access Point login interface, enclosed in a red rounded rectangular border. The interface features a text input field containing "cisco", a password field with masked characters ".....|", a language selection dropdown menu currently set to "English", and a blue "Login" button at the bottom.

Nota: Se la password è già stata modificata o è stato creato un nuovo account, immettere le nuove credenziali.

Passaggio 2. Scegliere **Risoluzione dei problemi > Acquisizione pacchetto**.

Nota: Le opzioni disponibili possono variare a seconda del modello esatto del dispositivo. Nell'esempio viene utilizzato WAP125.



Passaggio 3. Scegliere uno dei seguenti pulsanti di opzione Metodo di acquisizione pacchetto:

- Save File on this Device (Salva file sul dispositivo) - Memorizza i pacchetti acquisiti come file sul WAP. Configurare l'interfaccia, la durata e le dimensioni massime dei file da salvare localmente.
- Stream to a Remote Host: reindirizza i pacchetti acquisiti in tempo reale a un computer esterno che esegue gli strumenti di Network Protocol Analyzer. Se si sceglie questa opzione, andare al passaggio 7.

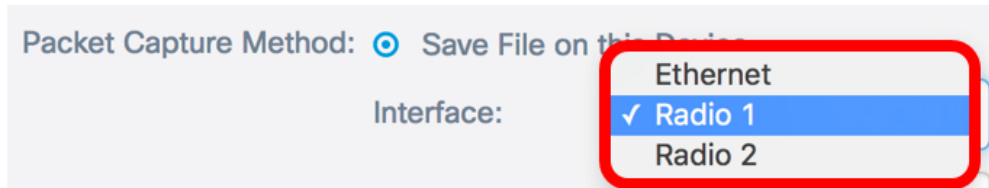
Nota: Nell'esempio, viene scelto Salva file sul dispositivo.

A configuration screen for 'Packet Capture Method'. At the top, 'Save File on this Device' is selected with a radio button. Below it are several fields: 'Interface:' with a dropdown menu showing 'Radio 1'; 'Duration:' with a text input '60' and 'Sec.' to its right; 'Max File Size:' with a text input '1024' and 'KB' to its right; 'Stream to a Remote Host' with an unselected radio button; and 'Remote Capture Port:' with a text input '2002'.

Passaggio 4. Dall'elenco a discesa Interfaccia, scegliere l'interfaccia per la quale i pacchetti devono essere acquisiti dall'elenco a discesa Interfaccia di acquisizione. Le opzioni sono:

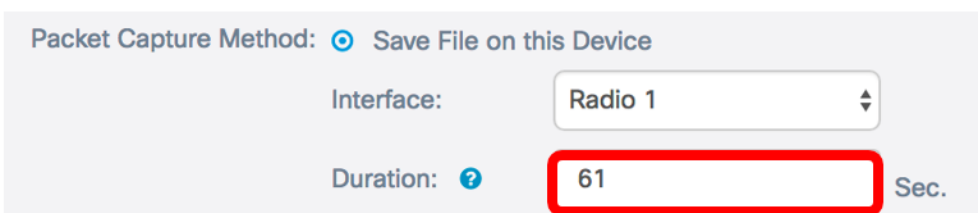
- Ethernet: traffico 802.3 sulla porta Ethernet.
- Radio 1 - traffico 802.11 sull'interfaccia radio 1.
- Radio 2 - traffico 802.11 sull'interfaccia radio 2.

Nota: Nell'esempio, viene scelto Radio 1.

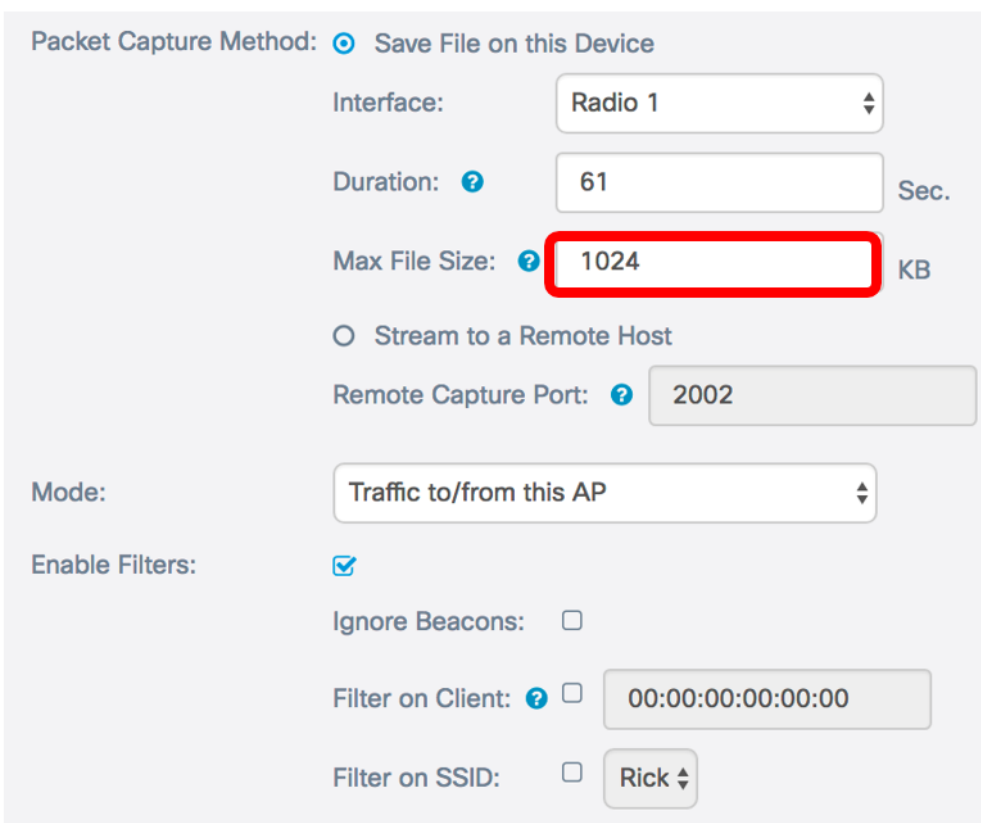


Passaggio 5. Inserire la durata dell'acquisizione nel campo *Durata* compresa tra 10 e 3600 secondi. L'impostazione predefinita è 60 secondi.

Nota: nell'esempio viene utilizzato 61.



Passaggio 6. Nel campo *Dimensioni massime file*, immettere le dimensioni massime del file di acquisizione, che vanno da 64 a 4096 KB, quindi andare al passaggio 8. Il valore predefinito è 1024 KB.



Nota: Nell'esempio viene utilizzato il valore predefinito.

Passaggio 7. Se si sceglie il metodo di acquisizione dei pacchetti in remoto, immettere un numero

di porta compreso tra 1 e 65530 nel campo *Porta di acquisizione remota*. Il valore predefinito è 2002.

Packet Capture Method: Save File on this Device

Interface: Radio 1

Duration: 61 Sec.

Max File Size: 1024 KB

Stream to a Remote Host

Remote Capture Port: 2002

Nota: Nell'esempio, viene usata la porta predefinita.

Passaggio 8. Dall'elenco a discesa Modalità, scegliere i pacchetti da acquisire. Le opzioni sono:

- Tutto il traffico wireless - Acquisisce tutti i pacchetti wireless, inclusi quelli inviati su altre reti.
- Traffico da/verso i pacchetti di acquisizione AP inviati tra il WAP e i client. In questo esempio viene scelta questa opzione.

Packet Capture Method: Save File on this Device

Interface: Radio 1

Duration: 61 Sec.

Max File Size: 1024 KB

Stream to a Remote Host

Remote Capture Port: 2002

Mode:
All Wireless Traffic
✓ Traffic to/from this AP

Passaggio 9. Selezionare la casella di controllo **Abilita filtri** per consentire filtri specifici nell'acquisizione dei pacchetti.

Mode: Traffic to/from this AP

Enable Filters:

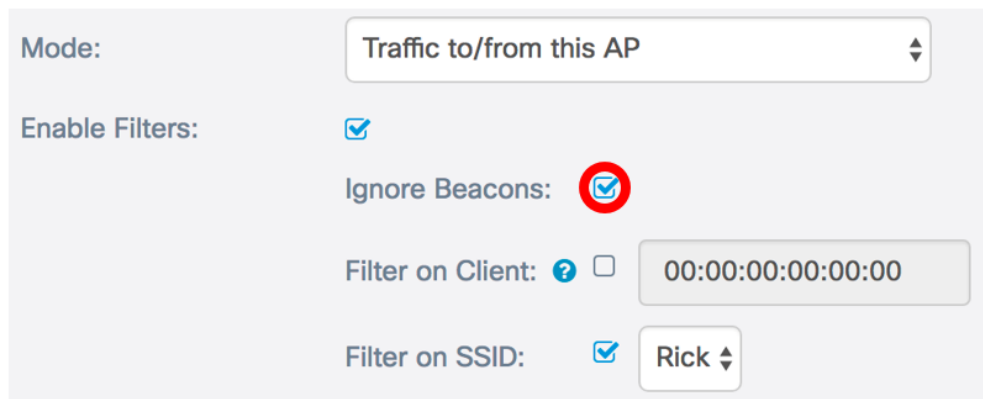
Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

Passaggio 10. (Facoltativo) Selezionare la casella di controllo **Ignora beacon** per disabilitare la cattura dei beacon 802.11 rilevati o trasmessi dalla radio. I frame dei beacon vengono trasmessi periodicamente per annunciare la presenza di una rete WLAN (Wireless Local Area Network).

Nota: Nell'esempio, l'opzione Ignora beacon è abilitata.



Mode: Traffic to/from this AP

Enable Filters:

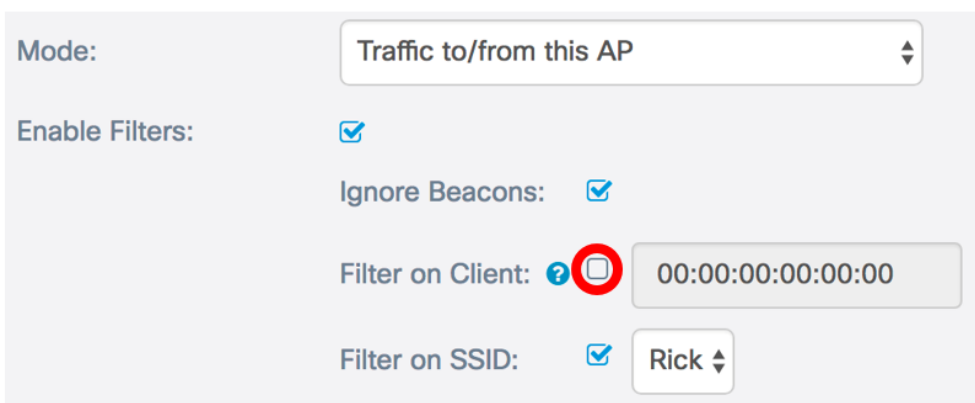
Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

Passaggio 11. (Facoltativo) Selezionare la casella di controllo **Filtra sul client** per specificare un indirizzo MAC di un client wireless.

Nota: In questo esempio, l'opzione Filtra su client è deselezionata.



Mode: Traffic to/from this AP

Enable Filters:

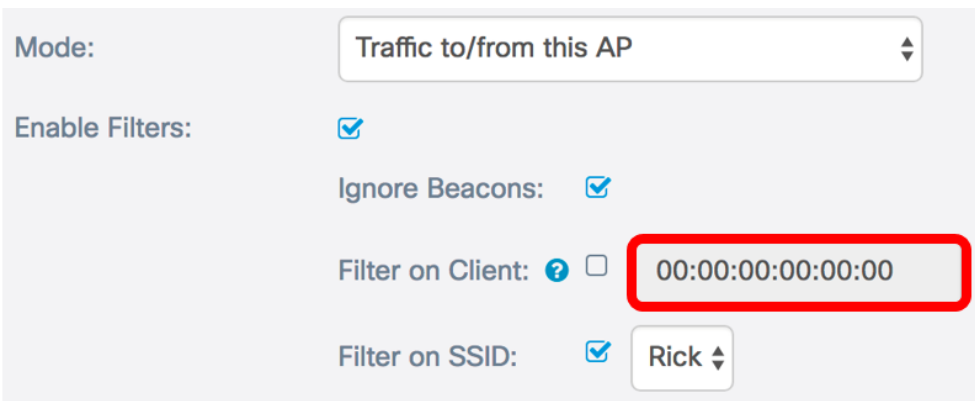
Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

Passaggio 12. (Facoltativo) Immettere l'indirizzo MAC del client nel campo *Filtra su client*. Questa funzione è attiva solo se l'acquisizione del pacchetto viene eseguita su un'interfaccia radio.

Nota: In questo esempio, l'opzione Filtra su client è disattivata.



Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

Passaggio 13. Selezionare la casella di controllo **Filtra su SSID** per acquisire i pacchetti su un SSID specifico.

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

Passaggio 14. Dall'elenco a discesa SSID, scegliere un SSID per acquisire i pacchetti.

Nota: Gli SSID visualizzati nell'elenco a discesa dipendono dall'interfaccia scelta e dal numero di SSID configurati. Nell'esempio viene scelto Rick.

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

Passaggio 15. Fare clic sul pulsante **Save** per salvare le impostazioni configurate.

Packet Capture

Save

Packet Capture Method: Save File on this Device

Interface: Radio 1

Duration: 61 Sec.

Max File Size: 1024 KB

Stream to a Remote Host

Remote Capture Port: 2002

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

Le impostazioni di acquisizione pacchetti sono state configurate correttamente.

Acquisizione pacchetti

Passaggio 16. L'area Stato acquisizione pacchetto contiene le seguenti informazioni. Fare clic su **Aggiorna** per visualizzare lo stato corrente.





Packet Capture Status

Current Capture Status: Stopped due to administrative action

Packet Capture Time: 00:00:17

Packet Capture File Size: 1024 KB

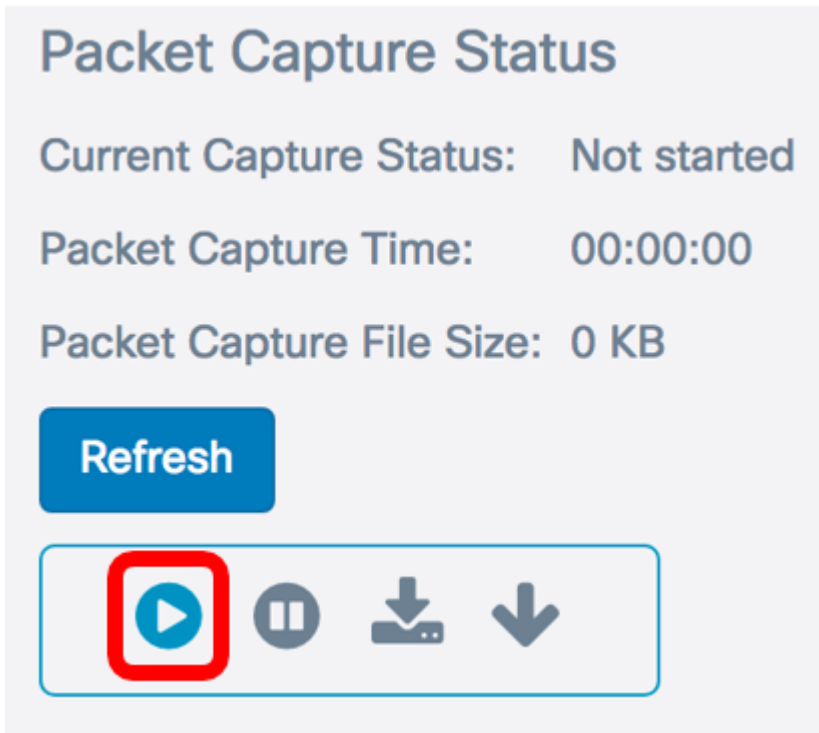
Refresh

- Current Capture Status (Stato acquisizione corrente) - Visualizza lo stato di acquisizione del pacchetto corrente. **In questo esempio**, lo stato corrente è - Arrestato a causa di un'azione amministrativa -.
- Ora di acquisizione pacchetto: visualizza la durata per la quale i pacchetti vengono acquisiti. Nell'esempio, sono stati registrati 00:00:17 secondi.

- Packet Capture File Size (Dimensioni file di acquisizione pacchetto) - Visualizza le dimensioni del file di acquisizione del pacchetto. Nell'esempio, le dimensioni della cattura sono 1024 kb.

Passaggio 17. Fare clic sul pulsante **Avvia acquisizione** per avviare il processo di acquisizione dei pacchetti.



Packet Capture Status

Current Capture Status: Not started

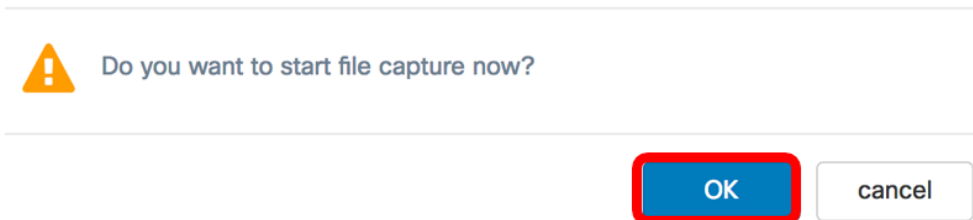
Packet Capture Time: 00:00:00

Packet Capture File Size: 0 KB

Refresh

⏪ ⏸ ⬇️ ↻

Passaggio 18. Viene visualizzata una finestra che informa dell'avvio dell'acquisizione del pacchetto. Fare clic su **OK** per continuare.



⚠️ Do you want to start file capture now?

OK cancel

Passaggio 19. Fare clic sul pulsante **Interrompi acquisizione** per interrompere il processo di acquisizione dei pacchetti.

Packet Capture Status

Current Capture Status: Not started

Packet Capture Time: 00:00:00

Packet Capture File Size: 0 KB

Refresh



Passaggio 20. Viene visualizzata una finestra che indica di confermare l'interruzione dell'acquisizione del pacchetto. Fare clic su **OK** per continuare.

Alert

x



Stop packet capture.

OK

A questo punto, i pacchetti sul punto di accesso dovrebbero essere stati acquisiti correttamente.

Download file di acquisizione pacchetti

Scarica su questo dispositivo

Passaggio 1. Fare clic sul pulsante **Scarica su questo dispositivo**.





Packet Capture Status

Current Capture Status: Not started

Packet Capture Time: 00:00:00


Packet Capture File Size: 0 KB

Refresh

Passaggio 2. Verrà visualizzata una finestra per avviare il download. Fare clic su **OK** per continuare.



Confirm ✕

 The file is downloading now.

OK

Al termine del download, il file scaricato verrà visualizzato nella cronologia dei download del browser. Il file viene scaricato con HTTP/HTTPS e il relativo formato è .pcap.

Nota: In questo esempio, apcapture.pcap è il file scaricato.

 apcapture.pcap 

Il file di acquisizione dei pacchetti di WAP è stato scaricato nel computer.

Scarica su server TFTP

Passaggio 1. (Facoltativo) Se il file catturato deve essere scaricato tramite un server TFTP, fare clic sul pulsante **Scarica su server TFTP**.

Packet Capture Status

Current Capture Status: Not started

Packet Capture Time: 00:00:00

Packet Capture File Size: 0 KB

Refresh



Dopo aver fatto clic su di esso, viene visualizzata una finestra con i campi Indirizzo IPv4 server e Nome file di destinazione.

Download File Using TFTP

Server IPv4 Address 

Destination File Name 

Download

cancel

Passaggio 2. Immettere l'indirizzo IPv4 del server TFTP nel campo Indirizzo IPv4 server. Il numero di porta immesso nel campo *Remote Capture Port* al punto 6 viene quindi collegato all'indirizzo del server TFTP.

Nota: nell'esempio viene usato 128.12.8.128.

Download File Using TFTP

Server IPv4 Address 

Destination File Name 


Download


cancel

Passaggio 3. Inserire il nome del file in formato pcap nel campo *Nome file di destinazione*.

Nota: Nell'esempio viene utilizzato apcapture.pcap.


Download File Using TFTP


Server IPv4 Address 

Destination File Name 

Passaggio 4. Fare clic su **Download**.


Download File Using TFTP


Server IPv4 Address 


Destination File Name 

Sotto il campo *Nome file di destinazione* viene visualizzata una barra di avanzamento.

Download File Using TFTP

Server IPv4 Address 

Destination File Name 



A questo punto, è necessario scaricare il file Packet Capture tramite un server TFTP.