

Configurazione dell'avvio di rete tramite PXE sui router serie RV34x

Obiettivo

In questo documento viene descritto come configurare la funzione Network Boot tramite l'opzione Pre-Boot eXecution Environment (PXE o "Pixie") sui router Cisco serie RV34x.

Prima di illustrare la procedura, verranno esaminati i casi di utilizzo per determinare se questa funzionalità è appropriata per l'utente.

Requisiti

Host server/servizio con indirizzo IP:

- un file di avvio
- Immagini dispositivo definite nel file di avvio

Firmware versione 1.03.16 o successiva per i dispositivi elencati di seguito ([collegamento alla pagina di download](#))

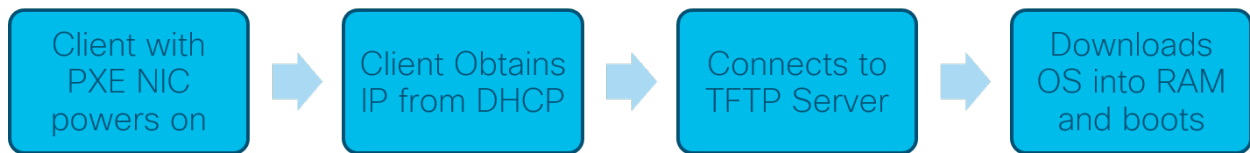
- RV340
- RV340W
- RV345
- RV345P

Firmware versione 1.0.01.01 o successiva per i dispositivi elencati di seguito

- RV160 ([collegamento alla pagina di download](#))
- RV260 ([collegamento alla pagina di download](#))

Introduzione

L'avvio di rete o l'avvio di rete è il processo di avvio di un computer da un percorso di rete anziché da un'unità locale. In genere, un file di avvio è un'immagine incapsulata o uno snapshot di un sistema operativo e di una configurazione. Un "file zip" è un tipo simile di contenitore; è un formato di file specifico che contiene un payload di dati variabile. In questo caso, il payload del file di avvio è un sistema operativo e la configurazione contiene tutto ciò di cui il dispositivo ha bisogno all'avvio per procedere oltre un POST (Power On Self-Test). In teoria, i formati di file possono includere qualsiasi cosa che possa essere scaricata via TFTP ed elaborata/eseguita dallo stack PXE della scheda di rete. Il diagramma seguente mostra il processo di avvio effettivo del PXE.



A partire dalla versione 1.03.16 del firmware è ora possibile utilizzare il campo indirizzo IP server (*siaddr*) nell'installazione DHCP (Dynamic Host Configuration Protocol), denominata campo *Server successivo* e nome file *del* file. Questo campo è il file di avvio o l'immagine. Per ulteriori informazioni, vedere la *RFC 2131* ([collegamento per la visualizzazione della RFC](#)).

Perché utilizzare l'avvio dalla rete? Se si utilizza l'avvio in rete su molte workstation, è possibile semplificare il processo nelle soluzioni di imaging dei dischi.

Ulteriori casi di utilizzo per questa funzione includono:

Aggiornamento continuo di chioschi o terminali automatici (come distributori di biglietti cinematografici)

Provisioning di più workstation tramite la rete

Dispositivi Cisco per PMI collegati a una rete aziendale che attualmente utilizzano l'avvio da rete

Perché usare Network Boot con l'opzione DHCP 66?

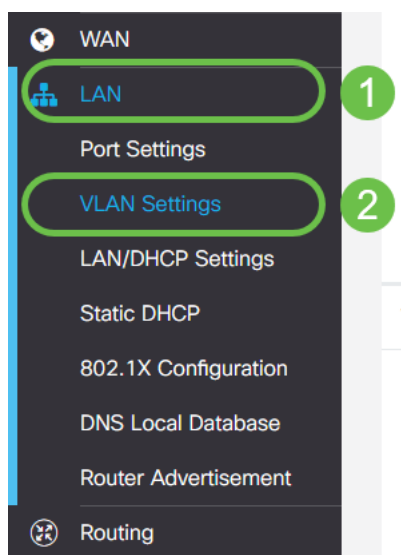
L'avvio da rete, analogamente all'opzione 66, consente di fornire un'immagine remota a un endpoint. Se è necessario fornire immagini diverse agli stessi dispositivi sulla stessa VLAN (Virtual Local Area Network), è possibile farlo sia con l'opzione Net Boot sia con l'opzione DHCP 6. In questo senso, le funzionalità sono complementari.

Inoltre, l'utilizzo di un server DHCP come percorso di avvio di rete non era la funzione di DHCP e ciò aggiunge complessità alla rete. Specialmente quando si cerca di servire l'avvio di rete su più piattaforme hardware.

Nota: Non tutti i client PXE interpreteranno correttamente l'opzione DHCP 150 come proprietà di Cisco; pertanto, se possibile, utilizzare l'opzione 66.

Procedura per configurare l'avvio dalla rete

Passaggio 1. Dopo aver effettuato l'accesso al dispositivo, fare clic su **LAN > Impostazioni VLAN** dalle voci della barra laterale dei menu.



Nota: Non viene visualizzata la barra laterale del menu? La barra laterale dei menu potrebbe essere compressa. Fare clic sul pulsante nell'angolo superiore sinistro. Esempio:



Passaggio 2. Nella *tabella VLAN*, fare clic sulla **casella di controllo** a sinistra della VLAN che si desidera indirizzare all'avvio PXE, quindi fare clic sul pulsante **Edit**. Nel nostro caso, è stata selezionata la **VLAN 1** predefinita.



VLAN Settings

VLAN Table



2

1

<input type="checkbox"/>	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management
<input checked="" type="checkbox"/>	1	VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 
<input type="checkbox"/>	99	VLAN99	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 

Passaggio 3. Selezionare la **casella di controllo** accanto a *Avvio in rete* per attivarla. Quindi immettere l'indirizzo IP **del server successivo** e il nome del **file di avvio**.

Server successivo: Solo indirizzo IP

File di avvio: *Percorso file relativo o assoluto accettato. I formati compatibili per i file di avvio includono:*

- *.CMD e *.EFI - Installazione di Servizi di distribuzione Windows per il sistema operativo
- *.BIN - Avvio Citrix vDisk
- *.KPXE - Imaging disco FOG
- *.XML - L'avvio remoto dell'hypervisor richiede in genere specifiche opzioni firmware/bios e viene principalmente utilizzato nei dispositivi proprietari

Nota: anche i file .com sono accettati, come rappresentato nello screenshot, anche se possono essere meno comuni.

VLAN Settings

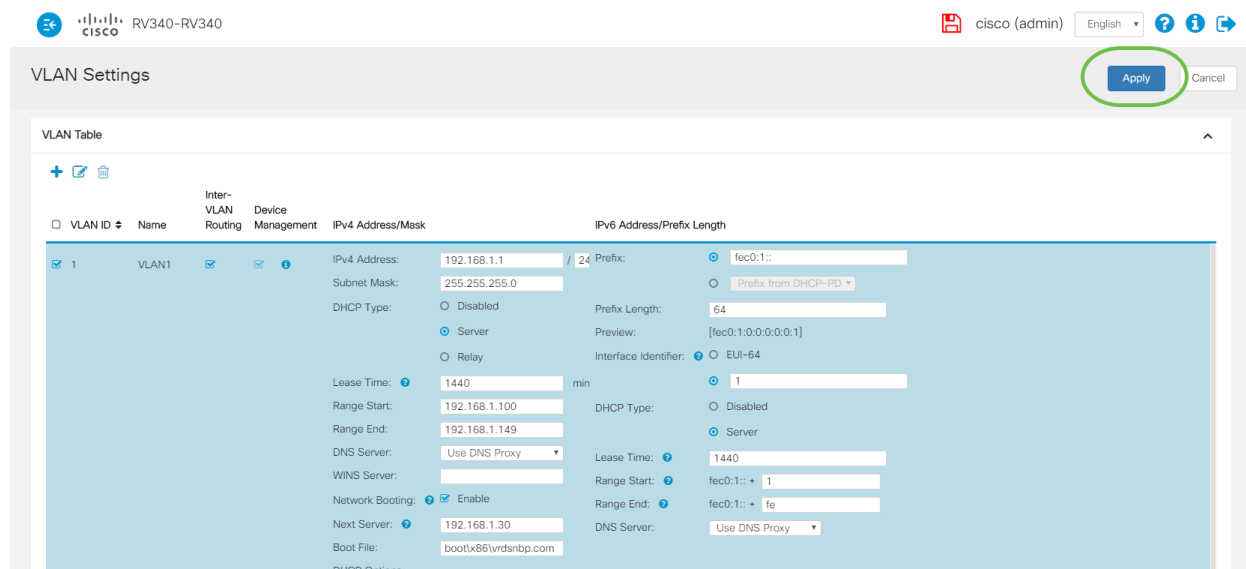
VLAN Table



<input type="checkbox"/> VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input checked="" type="checkbox"/> 1	VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 Address: 192.168.1.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min Range Start: 192.168.1.100 Range End: 192.168.1.149 DNS Server: Use DNS Proxy WINS Server: Network Booting: <input checked="" type="checkbox"/> Enable Next Server: 192.168.1.30 Boot File: boot\x86\vrdsnbp.com DHCP Options

- 1
- 2
- 3

Passaggio 4. Fare clic sul pulsante **Applica**.



Nota: Per salvare la configurazione tra un avvio e l'altro, fare clic sull'icona di salvataggio lampeggiante nella parte superiore della schermata.

Verifica della configurazione tramite Wireshark

Nello screenshot seguente viene mostrato dove trovare i campi Server successivo e File di avvio nell'offerta DHCP di Wireshark.

The screenshot shows a network traffic capture in Wireshark. The main packet list table includes the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.146	171.70.192.11	ESP	142	ESP (SPI=0x1f017198)
2	1.460489	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x5e471d04
3	1.462061	192.168.1.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x5e471d04
4	1.477532	192.168.1.30	255.255.255.255	DHCP	322	DHCP Offer - Transaction ID 0x5e471d04
5	2.517183	192.168.1.155	52.242.211.89	TLSv1	126	Application Data
6	2.582088	52.242.211.89	192.168.1.155	TLSv1	178	Application Data
7	2.622486	192.168.1.155	52.242.211.89	TCP	54	55375 → 443 [ACK] Seq=73 Ack=125 Win=258 Len=0
8	3.605412	13.59.223.155	192.168.1.101	TLSv1	85	Application Data
9	3.605977	192.168.1.101	13.59.223.155	TLSv1	89	Application Data
10	3.666082	13.59.223.155	192.168.1.101	TCP	60	443 → 54693 [ACK] Seq=32 Ack=36 Win=18 Len=0
11	3.834826	Cisco_44:5a:0a	WistronI_4b:03:36	ARP	60	Who has 192.168.1.101? Tell 192.168.1.1
12	3.835073	WistronI_4b:03:36	Cisco_44:5a:0a	ARP	60	192.168.1.101 is at 48:2a:e3:4b:03:36
13	5.455768	0.0.0.0	255.255.255.255	DHCP	590	DHCP Request - Transaction ID 0x5e471d04
14	5.457980	192.168.1.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x5e471d04
15	5.458752	Microsof_47:1d:04	Broadcast	ARP	60	Who has 192.168.1.30? Tell 192.168.1.194
16	5.460433	IntelCor_67:4d:5a	Microsof_47:1d:04	ARP	60	192.168.1.30 is at 84:fd:d1:67:4d:5a
17	5.461188	192.168.1.194	192.168.1.30	DHCP	590	proxyDHCP Request - Transaction ID 0x5e471d04
18	5.469974	192.168.1.30	192.168.1.194	DHCP	387	proxyDHCP ACK - Transaction ID 0x5e471d04
19	5.470073	192.168.1.101	192.168.1.30	ICMP	70	Destination unreachable (Port unreachable)
20	5.498500	192.168.1.194	192.168.1.30	TFTP	78	Read Request, File: boot\x86\wdsnbp.com, Transfer
21	5.500389	192.168.1.30	192.168.1.194	TFTP	60	Option Acknowledgement, tsize=30832
22	5.501690	192.168.1.194	192.168.1.30	TFTP	60	Error Code, Code: Not defined, Message: TFTP Abort
23	5.511789	192.168.1.194	192.168.1.30	TFTP	83	Read Request, File: boot\x86\wdsnbp.com, Transfer
24	5.513640	192.168.1.30	192.168.1.194	TFTP	60	Option Acknowledgement, blksize=1456
25	5.514710	192.168.1.194	192.168.1.30	TFTP	60	Acknowledgement, Block: 0

The detailed view of the DHCP Offer (packet 4) shows the following fields:

- Message type: Boot Reply (2)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x5e471d04
- Seconds elapsed: 4
- Bootp flags: 0x8000, Broadcast flag (Broadcast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 192.168.1.194
- Next server IP address: 192.168.1.30
- Relay agent IP address: 0.0.0.0
- Client MAC address: Microsof_47:1d:04 (08:15:5d:47:1d:04)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name: boot\x86\wdsnbp.com
- Magic cookie: DHCP
- Options: (53) DHCP Message Type (Offer), (54) DHCP Server Identifier (192.168.1.1), (51) IP Address Lease Time, (58) Renewal Time Value, (59) Rebinding Time Value

Risoluzione dei problemi PXE

Se si verificano degli errori dopo che il client riceve la *conferma della richiesta del proxy DHCP* dal server PXE, non sarà possibile fornire assistenza diretta in merito a tali problemi. Da quel momento in poi provare il server PXE e la connettività IP di base o lo stesso client PXE. Se il server PXE si trova sulla stessa VLAN, il client PXE invia le richieste ARP (Address Resolution Protocol) per il server PXE. In caso contrario, i server PXE esterni alla VLAN verranno indirizzati al gateway predefinito.

Se hai controllato questi elementi e riscontri ancora un problema, accedere alla nostra Community sarebbe un'opzione. [Fare clic qui per visitare la community dei router per piccole imprese.](#)

Conclusioni

A questo punto, è possibile configurare le workstation per l'avvio su una determinata VLAN da un percorso di rete tramite PXE utilizzando il router serie RV34x.