

تاهجوم ىل ع PXE ربع ةكبشلا ديهمت نيوكت ةلسلس RV34x

فدهلا

ةئيب راىخ ربع ةكبشلا ديهمت ةزيم نيوكتل ةبولطملا تاوطخلا لاقملا اذه ددحي
Cisco RV34x ةلسلس تاهجوم ىل ع ("PIXIE" و PXE) ديهمتلا لبق ام ذي فنن

اذا ام ةفرعم يف كتدعاسم لم ادختسالا تالاح ةعجارمب موقننس، تاوطخلا حىضوت لبق
كل ةبسانم ةزيملا هذه تنانك.

تابلطملا

IP ناوع ةمدخ/مداخ ةفاضتسا

- ليغشتلا ادب فلم
- ديهمتلا فلم يف ةفرعمل زاهجلا روص

([ليزنتلا ةحفص ىل طاابترا](#)) هاندا ةجردملا ةزهجالل ىل ع او 1.03.16 تباث جم انرب

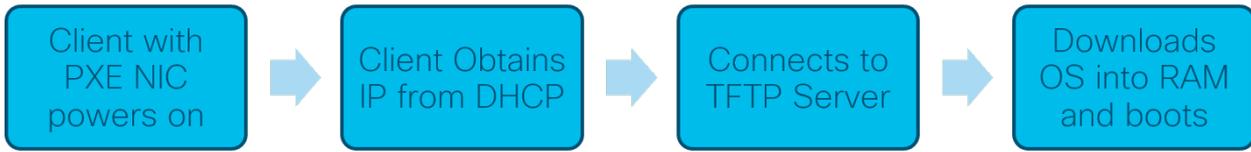
- RV340
- RV340W
- RV345
- RV345P زارطلا

هاندا ةجردملا ةزهجالل ىل ع ارادصا او 1.0.01.01 تباثلا جم انربلا

- RV160 ([ليزنتلا ةحفص ىل طاابترا](#))
- RV260 ([ليزنتلا ةحفص ىل طاابترا](#))

ةمدقملا

ةكبشلا ع قوم نم رتويبمك زاهج ديهمت ةيلمع يه يفاصللا ديهمتلا و ةكبشلا ديهمت
و ةفلغم ةروص ديهمتلا فلم نوكي، ناىحال مظعم يف. يلحم صارقا كرحم نم ال دب
قيسنت هنا، هباشم ةيواح عون وه "zip فلم" نا. نيوكتلا و (OS) ليغشتلا ماظنل ةطلق
فلم ةلومح نوكتس، ةلال هذه يف. ةريغتم تانايب ةلومح ىل ع يوتحي ددحم فلم
دن ع زاهجلا هيل جاتحي دق عيش ىل ع يلاتلاب يوتحي نيوكت و ليغشت ماظن ديهمتلا
نمضتت نا نكمي، ايرطن. (POST) ةقائلل يئاذلا رابتخالا يف ام دق يضمملا ديهمتلا
ةطساوب هذيفنت/هتجال عم و TFTP ربع هليزنت نكمي عيش ىل فلملا تاقيسنت
ديهمتلا ةيلمع حضوي يطيختت مسر هاندا. ةكبشلا ةقابطب صاخلا PXE سدكم
PXE زارطلل ةيلعلا



IP ناووع ل قح مادختس ال راىخ ال نآلا كىدل 1.03.16 تباثل اجم ان رپال رادصل نم اربا ت عا يذل - (DHCP) فيضملل يكي يمان ي دل نيوكتل لوكوتورب سار ي ف (*siaddr*) مداخلل وأ ديهمتل فل م وه ل قحلا اذه . فل مل مسا - **فل مل** ل قح و **ي لاتل** مداخلل ل قح يمسي (**RFC** [ضرع لطابترا](#)) RFC 2131 عجار ، قايسل نم ديزمل . كب ة صاخلا ةروصل

نم ديدعل ربع ةكبشلا ديهمت مادختس دن ع ؟ ةكبشلا ديهمت مادختس اذما ل اذ ا صارقالا ريوصت لولح ي ف ةيل معل ليهست نكمي ، لمعل اطاح

ةزيملا هذهل ةيفاضلا مادختس ال اناح نمضتتو

تاقاطب عيزوت ةزهجأ لثم) ةتمتؤملا ةيفرطلا اطاحملا وأ كاشكألا شي دحت يلع ظافحلا (مالفالا

ةكبشلا ربع ةددعتم لمع اطاحم دادم

يفاصللا ليغشتل اناح مدختست يتلاو ةسسؤم ةكبش ةلصت مل Cisco ةزهجأ

66 DHCP راىخ اني دل نو كي ام دن ع ةكبشلا ديهمت مدختسن اذما ل

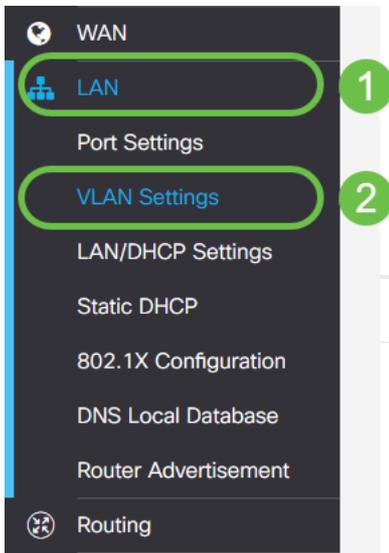
ةياهن ةطقنل دعب نع ةروص ري فوتب 66 راىخلا لثم اب يرق ت ي فاصللا ديهمتل حمسي . قطنملا ةكبش يلع ةزهجال س فن يلى ةفلتخم روص ري فوت يلى ةج ا ح ت نك اذ ا Net Boot نم لك مادختساب كلذب ما ي قلل كنكم ي ف ، اهس فن (VLAN) ةيره ا طلا ةي ل حملا . صعبلا اهضعب لمكت تامسلا ن ا ف ينعمل ا اذبو . 66 DHCP راىخو

وه ام ةكبشلا ديهمت ع قومك DHCP مداخل مادختس انكي مل ، كلذ يلى ةفاضلا ابو ديهمت ةمدخ ةلواحم دن ع ةصاخ . كتكبش يلى ادي قعت فيضي اذهو DHCP پ دوصقملا . ةددعتم ةزهجأ ةمظنأل ةكبشلا

Cisco وه نأ امب حيحص لكشب DHCP 150 راىخ نورس فيس PXE ءالمع لك سيل : **ةظحالم** 66 راىخ تلمعتسا نكمأ ن ا ، كلذل ؛ صاخ

ةكبشلا ديهمت نيوكت تاوطخ

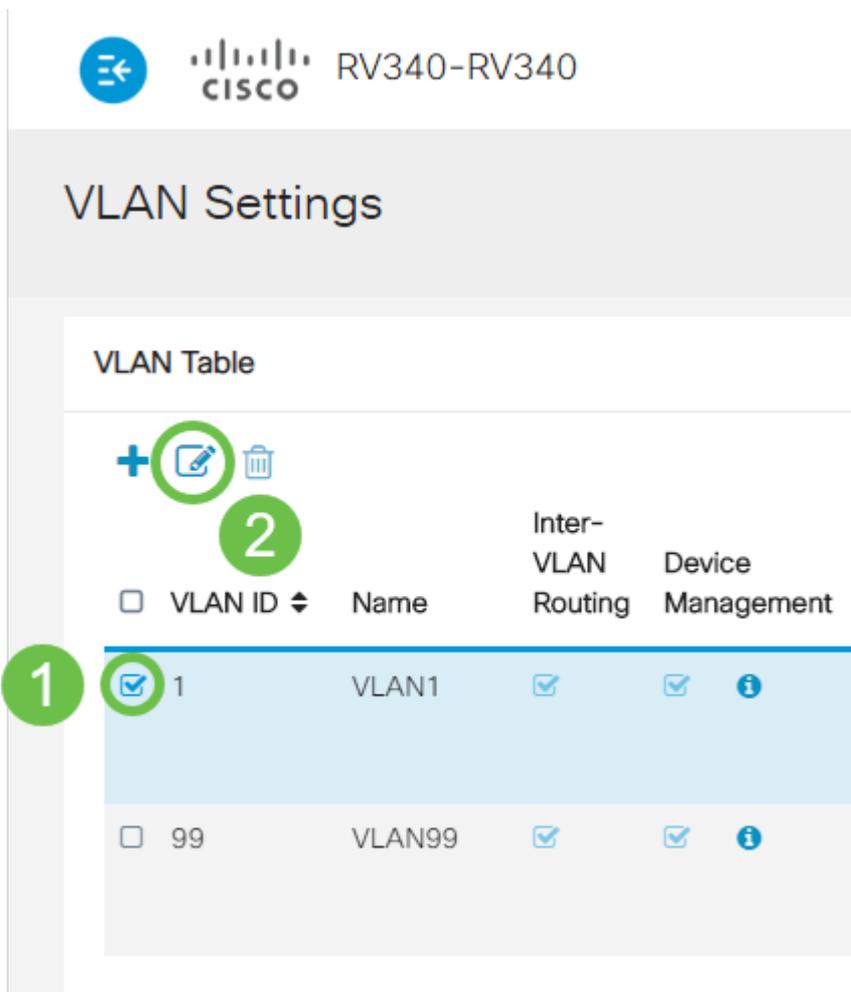
VLAN تاداعل رصانع > LAN ةكبش قوف رقنا ، كزاهج يلى لوخدلا ليحست دعب 1. ةوطخللا ةمئاقلل يبن اناحلا طيرشلا نم



ةيواهتم ةلأح يف يبناج-ةمئاق نوك ت دق ؟ةمئاق لل يبناج ال طيرشللا ىرت ال: **ةطخال**م
 لىلاتلا لاثم ل. ىرسىلا ةيولعلا ةيوازلا يف دوجوملا رزلا قوف رقنلا لواح:



ديرت يتلا VLAN ةكبش راسى ىلإ رايخالا ةناخ رقنا، VLAN لودج يف 2. ةوطخال
 VLAN 1 رىصقتلا انقتنا، انتلأح يف . رىرحت رز رقنا م ث، PXE ديهمت ىلإ اههيجوت



رايخالا اذه نىكمتل ةكبشلا ديهمت راوجب ةدوجوملا رايخالا ةناخ قوف رقنا 3. ةوطخال
 لىلاتلا مداخلل IP ناوعو ديهمتلا فلم مسال لخدأ م ث

طوق IP ناونع: ڤلالتل مداخل

تافل م تاقيسنت نمضتت. قوطملا و اڤيسننلا فلملا راسم لوبق مت: ڤهمتلا فلم
ةقفاوتملا ڤهمتلا:

- لڤشنتلا ماظن تڤتت تاي لمعل Windows رشن تامدخ - *.efi و *.cmd
- *.BIN ڤهمت Citrix vDisk
- ڤي بابضلا صارقالا ريوصت - *.KPXE
- ڤي زي متي هئا امك، ؤني عم (BIOS) ياساسالا جارخال او لاخلال ماظن تاراخي/ةتبات
ةصاخلا ؤزهجالاب بلال

هئا نم مغرلا لعل، ؤشاشلا ؤقول ي ف حضوم وه امك، note:.com تافل م لوبق متي امك
اعويش لقا نوكت دق.



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

قڤبطت رزلا قوف رقنا 4. ؤوطخلا



VLAN Settings

VLAN Table

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	IPv6 Address/Prefix Length
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 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: bootx86\wdsnbp.com	Prefix: fec0:1: Prefix Length: 64 Preview: [fec0:1:0:0:0:0:1] Interface Identifier: <input checked="" type="radio"/> EUI-64 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server Lease Time: 1440 Range Start: fec0:1:: + 1 Range End: fec0:1:: + fe DNS Server: Use DNS Proxy

قوف رقنل نم دكأتف ،ةيذحلأل ني ب نيوكتل اذه ظفح يف بغرت تنك اذا :ةظحال م ةشاشلل نم يولعل اعزلال يف ضماولا ظفح ةنوقيا .

Wireshark ربع نيوكتل نم ققحتلا

نييلاتلا ديهمتلاو مداخل فل م يلقح ىل ع روثعل ناكم ةيلاتلا ةشاشللا ةطول ضرعت في Wireshark نم DHCP ضرع في

Dynamic Host Configuration Protocol (Offer)

```

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 (00:15:5d:47:1d:04)
Client hardware address padding: 0000000000000000
Server host name not given
Boot file name: bootx86\wdsnbp.com
Magic cookie: DHCP
Option: (53) DHCP Message Type (Offer)
Option: (54) DHCP Server Identifier (192.168.1.1)
Option: (51) IP Address Lease Time
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value
    
```

اهحال صإو PXE ءاطخأ فاشكتسأ

نل ف، PXE مءاخ نم *DHCP* لئك وبلط رارق| لئمعلل ملتسئ نأ ءعب ءاطخأ تهءاو اءا رابءءا لولء اءعاصف ءطقنلل هءه نم و. لكاشملا هءه ف ءرشابم ءءعاسملا نم نكمءن ءكبش ىل ع PXE مءاخ ناك اءا. هسفن PXE لئمع وأ ىساسألل IP لاصءا كلءك و PXE مءاخ ءصاألل (ARP) ناونعلل لئلءل لوءوربءاب لط ءارءاب PXE لئمع موقئ، اهسفن VLAN ءبوابل ىل VLAN ءكبش ءراخ ءءوءومل PXE مءاوآ هئءوء مءئس الل و. PXE مءاأل هب ءئصاءءف الل.

انعمءءم عم لصاصءل نإف، ءلكشم هءاوءءل لزامو رصانعلل هءه نم ءققءء ءقءءنك اءا [هرفون ىءللا ءرئغصلل ءاكءشلل هءوم عمءءم ءرئزل انه رقنل](#). اراءئ نوئس

رارقلل

نم ءنئعم VLAN ءكبش ىل ع لمعلل ءاطءم ءئهمءل ءاءءلل ءئق نألل ءنأف، رمألل هءءنل و RV34x ءلسلسلل نم هءوم مءءءءسابل PXE رعب ءكبشلل عءوم

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا