

نيوكتلا لوكوتورب عاڤخأ فاشكتسا لوحم ي ف احوالص او فيضم ل ل يكي ماني دل تاسس و م ل ا تاك ب ش و Catalyst Switch

تايوتحم ل ا

[عمدق م ل ا](#)

[عميساس ال ا تاب ل ط م ل ا](#)

[تاب ل ط م ل ا](#)

[عمدخت س م ل ا تانوك م ل ا](#)

[ت ا ح ال ط ص ال ا](#)

[عميساس ا تامول عم](#)

[عميسيس يئر ل ا ميهاف م ل ا](#)

[تاهو يران ي س ل ا ق ل ث م ا](#)

[DHCP لوكوتورب مهف](#)

[عمي ل ا ح ال ا DHCP RFC ع ح ا ر م](#)

[DHCP لئاسر ل و د ج](#)

[DHCPDISCOVER](#)

[ر ف و ك ذ](#)

[ت س ي و ك ش ت ا ي د](#)

[ك ا ه د](#)

[ك ا ن ك ذ](#)

[ش ت د ر ا ك د](#)

[م ر و ف ن ي ا ب ذ ذ](#)

[س ي ل ي ر ب ك د](#)

[ر ا ح ي ال ا د ق ع د ي د ج ت](#)

[DHCP مزح ل و د ج](#)

[DHCP م داخو ل ي م ع ل ا د ج و ي ث ي ح DHCP ناو ن ع ي ل ع ل ص ح ي ي ذ ل ا ل ي م ع ل ل م داخ ل ل ي م ع ل ا ع ث د ا ح م](#)

[اهس فن عمي عرف ل ا ك ب ش ل ا ي ل ع](#)

[DHCP/BootP ل ي ح ر ت ل ي ك و ر و د](#)

[Cisco IOS® ه ج و م ي ل ع DHCP/BootP ل ي ح ر ت ل ي ك و ق ز ي م ن ي و ك ت](#)

[عمي و د ي ط ا و ر ن ي ي ع ت](#)

[عمي و ن ا ث ل ا IP ع ط ا ق م ي ل ع ل م ع ي DHCP ل ع ج عمي ف ي ك](#)

[DHCP ل ي ح ر ت عمي ف ي ط و ع م DHCP Client-Server ع ث د ا ح م](#)

[IP ناو ن ع ي ل ع ل و ص ح ل ل DHCP ل ي م ع ل عمي ل م ع ل ا](#)

[DHCP ل \(PXE\) ذ ي ف ن ت ل ل ل ب ق ا م عمي ي ل ي غ ش ت ع د ب ت ا ر ا ب ت ع ا](#)

[sniffer ت ا ر ا س م م ا د خ ت س ا ب ا ح ا ل ص ا و ه ا ط خ ا ف ا ش ك ت س ا و DHCP مهف](#)

[\(LAN\) عمي ل ح م ل ا ك ب ش ل ا ع ط ق م س ف ن ي ل ع م داخ ل ل ا و DHCP ل ي م ع ع ب ت ر ي ف ش ت ك ف](#)

[\(LAN\) عمي ل ح م ل ا ك ب ش ل ا ع ط ق م س ف ن ي ل ع م داخ ل ل ا و DHCP ل ي م ع د ج ا و ت ي ث ي ح ك ب ش ل ا ط ا خ م](#)

[ل ي ح ر ت ل ي م ع ك ه ن ي و ك ت م ت ه ج و م ا م ه ل ص ف ي م داخ ل ل ا و DHCP ل ي م ع ع ب ت sniffer ر ي ف ش ت ك ف ي](#)

[DHCP](#)

[Sniffer-B ع ب ت ت](#)

[sniffer-A ع ب ت ت](#)

تاحالطصالا

[تاحالطصالا لوح تامولعملال ندم ديزم ىلع لوصحلل ةينقنل Cisco تاحيملت تاحالطصالا عجار تادنتسملال](#)

ةيلخادلل اعطخالل ريراقت ىل لوصولاب طقف نولجسملال Cisco ءالمع عتمت تي: ةظحال

ةيساسأ تامولعمل

في مكحتل لوكوتورب مدختست يتلار تويبمكلل ةزهجال اهلالخ ندم نكمي ةيل DHCP رفوي ندم ايئاقلت لوكوتوربال نيوكت تاملعمل ىلع لوصحلل (TCP/IP) تنرتنل لوكوتوربال لاسرلال [فيضملال نيوكت لمع ةعومجم](#) ةطساوب هرپوطت مت حوتفم رايعم وه DHCP. ةكبشلال لالخ (IETF) [تنرتنالل ةسدنه لمع ةقرفل](#) ةعباتل (DHC-WG) [يكيمنيدل](#).

لاثلل لابس ىلع DHCP ليمع لصتي شيح، مداخل-ليمع جذومن ىل DHCP دننسي، مداخل عقوم ديدحت متي ام ةداع. نيوكتل تاملعمل DHCP مداخل، يبتكم رتويبمك لوؤسم ةطساوب هلبيغشت متي مداخل نالو. ةكبشلال لوؤسم ةطساوب ايزكرم هلبيغشتو ةينبل ةبسانم تاملعمل مداخلتساب يكرحو قوتوم لكشب DHCP ءالمع نيوكت نكمي، ةكبشلال ةيلال ةكبشلال.

ةيعرف تاكبش ىل ةمسقم ةددعتم ةيعرف تاكبش ندم تاسسؤملا تاكبش مطعم فلأتت نيبي هيچوتلاب تاهجوملا موقت شيح، (VLANs) ةيرهالال LAN تاكبش مساب اهلا راشي ىلع DHCP مداخل مزليسي، يضارتفا لكشب ثبلار ررمت ال تاهجوملا نأ امب. ةيعرفل تاكبشلال ليلكو ةزيم مداخلتساب DHCP ثب هيچوت ةداعل تاهجوملا نيوكت متي مل ام ةيعرف ةكبشلال DHCP ليحرت.

ةيسيسيئرل ميهافل

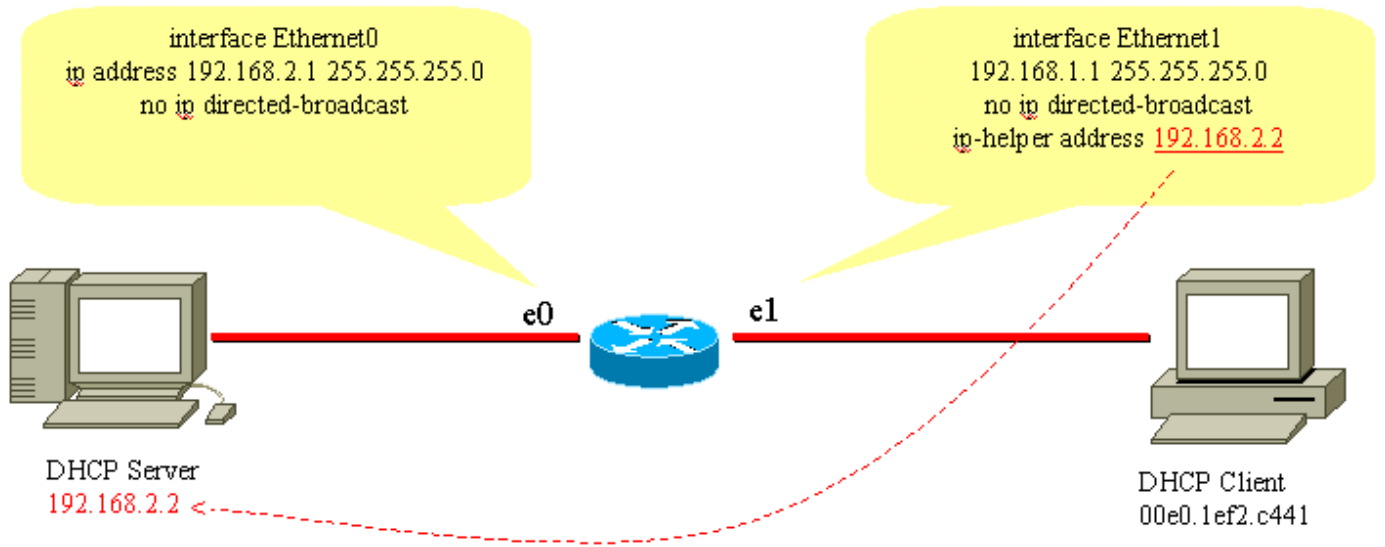
DHCP ل ةيسيسيئر ميهافل ةدع هذه

- ثب بلط لاسرا مهيلع بجي يلاتلابو نوكم IP ناووع ةيادلل في DHCP ءالمعل سيل
- DHCP مداخل ندم IP ناووع ىلع لوصحلل
- باعيتسا يرورضلال ندم. ثبلال تايلمع هيچوت ةداعب، يضارتفا لكشب، تاهجوملا موقت ال متي (L3) 3 ةقبتل (ل3) ىرخأ ثب ةكبش ىلع DHCP مداخل ناك اذا ليمعمل DHCP ثب تابلط DHCP ليحرت ليلكو مداخلتساب كلذ ذيفنت
- يوتسم ىلع IP دعاسم رماو لالخ ندم DHCP ليحرتل Cisco هجوم ذيفنت ريفوت متي ةهجال

تاهويرانيسلال ةلثمأ

مداخل او DHCP ليمع تاكبش نيبي Cisco هجوم هيچوت: 1 وييرانيسلال

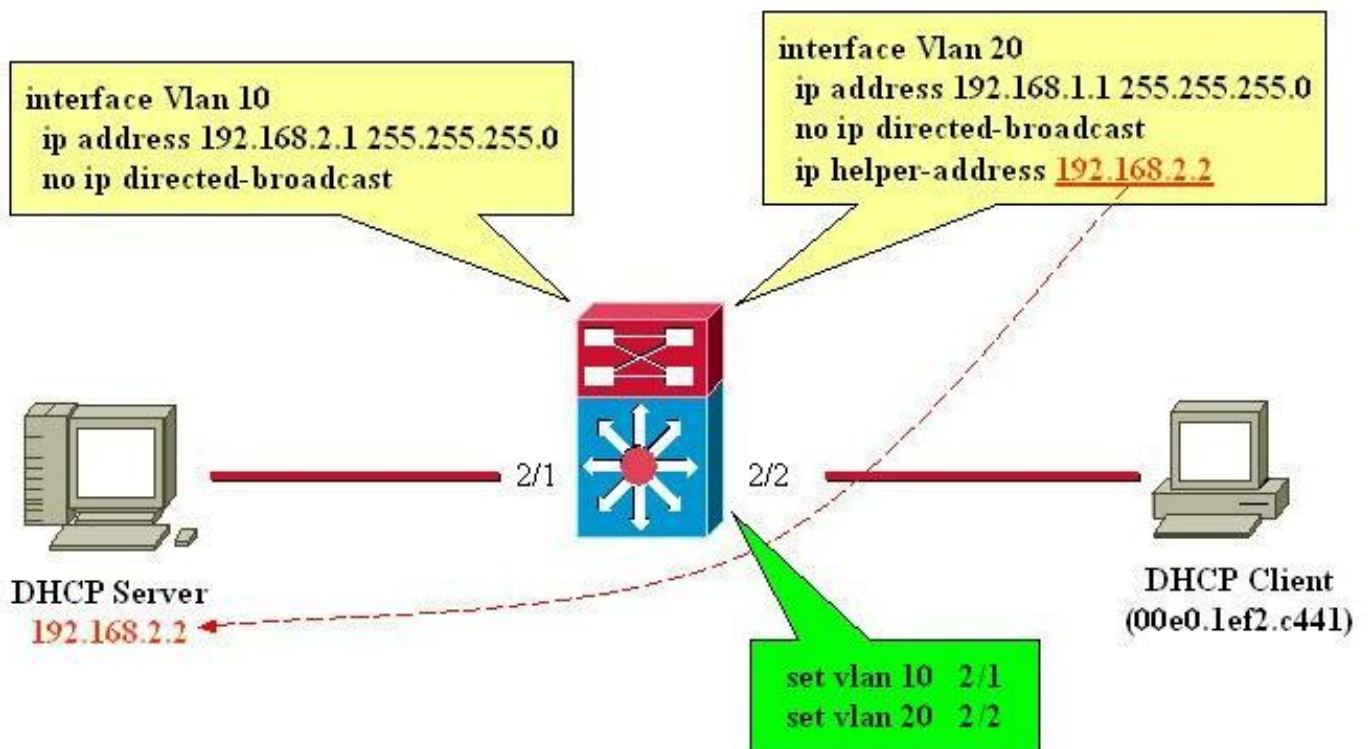
ليمعلل هيچوت ةداعب Ethernet1 ةهجال موقت، ططخملل اذه في هنيوكت مت امك ندم بلطلل DHCP مداخل في فوتسي. Ethernet1 ةهجال لالخ ندم 192.168.2.2 ىل DHCPDISCOVER لالخال. لالثلل اذه في هجوملل فياضا نيوكت مزلي ال. يدخالل ثبلال لالخال.



مداخل او DHCP ليمع تاكبش نيب هيچوتلا

كبش لدانو نوبز DHCP نيب هيچوت دحوو L3 عم حاتفم عزافح دام cisco: نيبثا ويرانيسلا

صاخلا Dhcpdiscover هيچوت دءاب VLAN20 هءاوا موقت ، ططخمالا يف اهنيوكت مت امكو
 ءصاخلا VLAN10 كبش لالخ نم 192.168.2.2 لىل هيل DHCPdiscover ثب مت يذلا ليمعلا ب
 ءوملل يفاضا نيوكت مزلي ال . يدخال ثبلا لالخ نم بلطال DHCP مداخ يفوتسي . هءاوا ب
 - رسجي ىقلى وءانيم فيضمك تلكش نوكي نأ ءانيم حاتحي حاتفملا . لاثملا اذه يف
 نجي ءانقو trunking و ، نكمي portFast (STP) لوكو تورب ءرئش .



مداخل او DHCP ليمع تاكبش نيب L3 ءيطم نلا دحوولا راسم

DHCP لوكو تورب مهف

هؤاغل مت نيحل كلذ ذنمو [1531 \(RFCs\) تاقيلعتلا تابلط](#) يف لصالا يف DHCP ديحت مت
 (BootP) رتويبمكلا ليغشت ديهمت ماظن لوكو تورب لىل DHCP دننسي . [RFC 2131](#) ءطساوب

[RFC 951](#) يه ه فيرعت مت يذلاو

تامولعم ىلع لوصحلل (ة فيضملا تائيبلا) لمعلا تاظم ةطساوب DHCP مادختسا متي ادب دنع ةيضارتفالا ةباوبلاو ةيعرفلا ةكبشلا عانقو IP ناووع لثم، ةيلوالا نيوكتلا اذا، كلذ ىلع ةوالع. ناووع عم فيضم لك ايودي لكشي نأ تنأ جاتحي ال، DHCP عم. ليغشتلا نع فللخم IP ناووع مدختسي نأ بجي ف، ةفللخم ةيعرف IP ةكبش ىلإ فيضم لقتنا فيضملا حمسي وهو. ايئاقلا رمألا اذهب DHCP ينعني. اقباس هم دختسا يذلا ناووعلا. ةححصلا ةيعرفلا IP ةكبش في IP ناووع رايختاب

ةيلال DHCP RFC عجارم

- (DHCP) فيضملا ل فيكيما نيديلا نيوكتلا لوكوتورب - RFC 2131 راي عملا
- تادادتم او (DHCP) فيضملا ل فيكيما نيديلا نيوكتلا لوكوتورب تاراخي - RFC 2132 راي عملا
- BootP لوكوتورب و DHCP لوكوتورب نيبي نيبيلا ليغشتلا - RFC 1534 راي عملا
- BootP لوكوتورب تادادتم او تاحيضوت - RFC 1542 راي عملا
- Novell ليلد تامدخ DHCP لوكوتورب تاراخي - RFC 2241 راي عملا
- NetWare/IP تامولعم و لاجم مسا - RFC 2242 راي عملا
- ةديدل DHCP تاراخي ديدحت عارج - RFC 2489 راي عملا

صيصختب (DHCP مداوخ) رثكأ وأ دحاو مداخ موقبي شيح مدخال-ليمعل جذومن DHCP مدختسي ادب دنع (ة فيضملا ةزهجالا) ءالمعل نيوكتلل ىرخالا ةيرايخالا تاملعمل او IP نيوانع تقولا ضعبل ليمعلل مداخلا ةطساوب هذه نيوكتلا تاملعمل ريحات متيو. ليمعل ليغشت (DHCPDISCOVER) ثب ةلاسر فيضملا في TCP/IP سدكم لسري، فيضم دهمي ام دنع. ددحمل ىلإ اذه يدوي. ىرخالا نيوكتلا تاملعمل نيبي نم، ةيعرف ةكبش عانقو IP ناووع ىلع لوصحلل تالال هذه ربع ليمعل رمي، لدابتلا اذه لالحو. فيضملا او DHCP مداخ نيبي لدابت ادب اديح ةدحمل:

1. ةئيهت
2. ديدحت
3. بلط
4. اوبصع
5. ديدحت
6. طبرلا ةداع

لودج في ةجرمدلا لئاسرلا عاونأ لدابت مدخال او ليمعل نكمي، تالال هذه نيبي لقتنتلل DHCP لئاسر.

DHCP لئاسر لودج

ةلاسر عجرملا	فصولا
0x01 DHCPDISCOVER	ةرفوتملا DHCP مداوخ نع ليمعلل شحي
0x02 رفوكد	ليمعل DHCPDISCOVER ل مداخلا ةباجتسا
0x03 شت يديتسيوك	م وه امك، اديحت دحاو مداخ نم ةمدقم تاملعمل بلطي و، مدخال ىلإ ليمعل عيدي ةمزلال في
0x04 شت دراك	مادختسالا ديق ةكبشلا ناووع نأ ىلإ مداخلا ىلإ ليمعل نم لاصتالا ريشي لعلاب
0x05 كاهد	بشلا ناووع ىلإ ةفاضلاب، نيوكتلا تاملعمل عم ليمعل ىلإ مداخ نم لاصتالا هب مزتلل

0x06	كانكذ	نيوكتلا ةملم بلط ليمعلا ىلإ مداخل نم لاصتالا ضفري
0x07	سيليربكذ	جاتلا ءاغلإو ةكبشلا ناووع ميلستب مداخل ىلإ ليمعلا نم لاصتالا موقى يقبتملا
0x08	مروفنيابذذ	الاطق ةيحلحملا نيوكتلا تاملم مداخل ىلإ ليمعلا نم لاصتالا بلطتي ناووعك لعفلاب ايجراخ ليمعلا لاهنيوكت

DHCPDISCOVER

الاسر لسريو، ةئيهتلا ةلاح يف هنإ لاقى، ةرم لوأل ديهمتلاب ليمعلا موقى ام دنع لوكوتورب ذفنم ربع هب ةصاخلا ةيحلحملا ةيداملا ةيعرفلا ةكبشلا ىلع DHCPDISCOVER ةقيرط هيدل سيل ليمعلا نأ امب. (BootP مداخل) 67 مقرر (UDP) مدختسملا تانايب ططخم عيمل ثب وه DHCPDISCOVER نإف، اهيا ليمتني يتلا ةيعرفلا ةكبشلا ةفرعمل 0.0.0.0 مقرر ردصم لل IP ناووعب، (255.255.255.255 مقرر ةهوجلل IP ناووع) ةيعرفلا تاكبشلا ةيعرفلا ةكبشلا هذه ىلع ادوجوم DHCP مداخل ناك اذا. نوكم IP ناووع هيدل سيل ليمعلا نأل عم بيحيتسيو ثبب لعمسي DHCP مداخل نإف، حيحص لكشب هليغشتو هنيوكت متو ةيحلحملا نأ بچيف، ةيحلحملا ةيعرفلا ةكبشلا ىلع ادوجوم DHCP مداخل نكي مل اذا DHCPoffer ةالاسر هيجوت ةداعل ةيحلحملا ةيعرفلا ةكبشلا هذه ىلع DHCP/BootP ليحرت ليكو كانه نوكي DHCP مداخل ىلع يوتحت ةيعرف ةكبش ىلإ DHCPdiscover ةالاسر.

Microsoft Windows، لاثملا لىبس ىلع) اصصخم افيضم اذه ليحرتلا ليكو نوكي نأ نكمي IP دعاسم تارابع مادختساب هنيوكت مت يذلا Cisco هجوم، لاثملا لىبس ىلع) هجوم وأ (Server ةهجالو لىوتسم ىلع).

رفوكذ

الاسر مادختساب ةباجتسالا DHCPdiscover ةالاسر لبقتسي يذلا DHCP مداخل نكمي ىلإ لقتنيو DHCPoffer ل ليمعلا ملتسي. (BootP ليمع) 68 UDP ذفنم ىلع DHCPoffer ةالاسر يوتحت. ديحتلا ةلاح مدختسملا مسال لقلحلا يف DHCPoffer ةالاسر ةئبعتب DHCP مداخل موقى، لاثملا لىبس يف ةيضارتفالا ةباوبلاو ةيعرفلا ةكبشلا عانق ديحت متي. بولطملا IP ناووع مادختساب تارايل نمتت. يلاوتلا ىلع، هجوملا تارايلو ةيعرفلا ةكبشلا عانقو تارايل لقلح، لاجملا مسال مداخلو، ديحتلا تقوو، IP ناووع رجات تقو DHCPoffer ةالاسر يف يرخال ةعئاشلا، نمتت هنيوكت لولثلا ناووع ىلإ DHCPoffer DHCP مداخل لسري. NetBIOS (WINS) مسال مداخلو ةهوجل اهنا ليمعلا فرعي يتح، ضرعلا صاخلا chaddr لقلح يف ليمعلا زاغ ناووع DHCP مداخل لسري، ةيحلحملا ةيعرفلا ةكبشلا ىلع DHCP مداخل دوجو مدع ةلاح يف. ةدوصقملا مت يذلا DHCP/BootP ليحرت ليكو ىلإ يرخا ةرم، 67 UDP ذفنم ىلع، unicast ةمزحك، DHCP ل DHCPoffer ةعاذب امإ DHCP/BootP ليحرت ليمع موقى كلذ دعب. هنم DHCPdiscover فاشتك ةمالع ىلع دمتعي يذلاو، 68 UDP ذفنم ىلع ةيحلحملا ةيعرفلا ةكبشلا ىلع هطبر ةداعل وأ BOOTP ليمع ةطساوب هنيوكت مت يتلا ثبلا.

تسيوكتش يذ

همزع ىلإ ريشيو، DHCPprequest ةالاسر عم بيحيتسي، DHCPoffer ليمعلا ملتسي نأ دعب يقلت ليمعلا نكمي. بلطلا ةلاحلا ىلإ لقتنيو، DHCPoffer يف تاملم لوبق ىلع. ةيصلألا DHCPdiscover ةالاسر يقلتت DHCP مداخل لك نم ةدحاو، ةددعت DHCPoffer لئاسر لك اينيضم ضفريو، طقف لدان DHCP نأ ىلإ بيحيتسيو دحاو DHCPoffer ليمعلا راتخي فرعم رايخ لقلح علم دعب ددحملا مداخل فيرعتب ليمعلا موقى. يرخال DHCPoffer لئاسر

مداوخ عي مج نإف ك لذل ، ثب ن ع ةرابع DHCPprequest نأ امك . DHCP مداخل IP ناو نعب مداخل صاخال DHCPpoffer ناك اذا ام فرعي لكو ، DHCPprequest ىرت DHCPpoffer تلسرأ يتل DHCP لقح يف لي مغل اهلطي ةيفاضا نيوكت تاراخي يا ني مضم ت متي . هضفر وأ هلوبق مت اهبال ، لي مغل ال ع IP ناو ن ع ضرع مت دق هنأ نم مغل را لي ع . DHCPprequest ةلاسر يف تاراخي ال ملتسي مل ، تقولا اذه يف 0.0.0.0 رصم ال IP ناو نعب DHCPprequest ةلاسر لسري هنأ IP ناو ن ع مادختسا حضاولا نم هنأ نم ققحتلا دعب لي مغل

كاهد

كلذ دعبو ، DHCPACK ةلاسر عم بلطال رقي هنإف ، DHCP DHCPprequest مداخ ملتسي نأ دعب لثم يو ، DHCP مداخل رصم لل IP ناو ن ع لي ع DHCPACK ةلاسر يوتحت . ةئيه تال ةي لمع متي ةلاسر يف لي مغل اهلطي يتل تامل عمل عي مج لي ع يوتحي و ثب ىرخأ ةرم ةهجو ل ناو ن ع رح وه نأ لاو ، ةطبترم ةلودلا لخاد لخدي وه ، DHCPACK ل لي مغل ملتسي ام دن ع . DHCPprequest نيختب DHCP مداخ موقوي ، هسفن تقولا يفو . ةكبشلا لي ع لصتي نأ ناو ن ع ال لمعتسي نأ ناو ن ع و ناو ن ع ال وا لي مغل فرعمب ديرف لكش ب هفيري عتب موقوي وه تانايب ةدعاق يف رجاتل رجاتلا لي ةراشال تافرعمال نم ةومجمال هذه مداخل او لي مغل نم لك مدختسي . نرتقم ال IP طئاسولا عون لي ةفاضال اب زاهجلل MAC ناو ن ع وه لي مغل فرعم

تامل عم باسح DHCP لي مغل لي ع بجي ، دي دجل ناو ن ع ال مادختسا يف DHCP لي مغل أدبي نأ لب ق دادرتسا ال تقوو ، (T1) دي دجل تقوو ، (LT) راجي ال تقوي وه ، رجؤم ال ناو ن ع ال تقولا ظفحل رصقأ رجات تاقو مادختسا كنكمي . ةعاس 72 وه يضارتفال ياسايقلا مقررلا . (T2) رمال مزلا اذا ، نيوانع ال

كانكذ

ةلاسر رب بيختسي DHCP مداخ نإف ، DHCPprequest ةلاسر ةي بلبت ددحما مداخل لي ع رذعت اذا ةلاسرل ةباجتسا ملتسي ال وا DHCPnak ةلاسر لي مغل ملتسي ام دن ع . DHCP ةلاخل لي لقتنت ام دن ع نيوكتال ةي لمع لي غشت ةداعب لي مغل موقوي ، DHCPprequest لب ق ةيناث 60 نوضغ يف تارم عبرا لقال لي ع DHCPprequest ل لي مغل لسري . ةبولطم ال ةلاخ دي همتلا وه دي عي نأ

ش ت دراك د

موقوي . تامل عمل لي ع يئاهن صحف عارجاب ، ايرايتخا ، موقوي ، DHCPACK لي مغل لبقتسي IP ناو ن ع ال (ARP) لي لحت لوكوتورب تابلط لاسرا دن ع عارجالا اذه ذي فن تب لي مغل ام دن ع لع فل اب مادختسا ال دي ق ناو ن ع ال نأ لي مغل فشك اذا . DHCPACK يف رفوتم ال لي غشت دي عي و مداخل ال DHCPDECLINE ةلاسر لي مغل لسري ، ARP بلط لي ع ادر ملتسي بلطال ةلاخ يف نيوكتال ةي لمع

مروف ني اب ذذ

، ايودي نوكم IP ناو ن ع هي دل ناك وا ىرخأ لئاسو لال خ نم ةكبش ناو ن ع لي مغل لصح اذا ، نيوكت تامل عم لي ع لوصحلل DHCPinform بلط ةلاسر مادختسا لي مغل لمع ةطحمل نكمي ةلاسر DHCP مداوخ يقلتت ام دن ع . (DNS) لاجم ال مسا مداوخ و لاجم ال مسا لثم ، ىرخأ ةي لجم لي مغل ةبسانم ةي لجم نيوكت تامل عم يا عم DHCPACK ةلاسر عاشن اب موقت DHCPnForm لي مغل لي يداخل اال ثبلل اذه DHCPACK لاسرا متي . دي دج IP ناو ن ع نود

سي لي ربك د

DHCP ةلاسر لسري ام دن ع ةكبش ناو ن ع لي ع هراجي نع ي لختلا رايختا DHCP لي مغل نكمي


```
!--- IP helper-address pointing to DHCP server

no ip directed-broadcast
!
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

موقت DHCP ليحرت عالمك اهنويوكت مت يتي ل DHCP مداوخ لمح ةنزاوم Cisco تاهجوم معدت ال ةروكذمل ا ةدعاسم ل نيوانع عي مج ي ل DHCPDISCOVER ة لاسر هيجوت ةداع ب Cisco تاهجوم رورم ةكرح طقف ةيعرف ةكبش ةمدخل DHCP نم رثكأ وأ نيمداخ مادختس ا دي زي . ةهجاو ل كلتل جوز ل نيب DHCP / DHCPprequest و DHCPoffer و DHCP client لئاسر لدابت متي ثي DHCP مداوخ ل او DHCP عالمع نم

ةيودي طباور نييعت

Windows ريغ ي فيضمل رخال او ، Windows فيضمل امه دحأ ؛ ةيودي طباور دادع ل ناتقيرط كانه ريغ ل رخال او ، نوبز DHCP تفوسورك يام ل دحاو ؛ لكشي نأ لمعتسي فل تخم رمأ نانت ا كانه (نوبز DHCP تفوسورك يام - يودي طبر) DHCP-identifier نوبز : نوبز DHCP تفوسورك يام ني رمل ببس ل . (نوبز DHCP تفوسورك يام ريغ - يودي طبر) DHCPhardware-address و يه هذو . ناو نعل ةي ادب ي ف تفضا 01 و ، وه MACs ل دع ي Windows عم ضكري نأ pc نأ ني فل تخم تانويوكت ل نم ةني ع

- Microsoft DHCP عالمعل ليكشت اذه :

```
configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
client-identifier 01xxxxxxxxxxxx
```

!--- xxxxxx represents 48 bit MAC address prepended with 01

- تفوسورك يام ريغ نم DHCP عالمعل ليكشت اذه :

```
configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
hardware-address xxxxxxxxxxxx
```

!--- xxxxxx represents 48 bit MAC address

ةيونال IP عطاقم يلع لمعي DHCP ل ع ةي فيك

ي قلت مت اذا طقف اهل اسرا متي درلا مزح نأ ي ف دي دحت يلع DHCP يوتحي ، ي ضارت ف لكش ب رورم ةكرح مدختست . يساس ال IP ناو نعل مادختساب اهنويوكت مت يتي ل ةهجاو ل نم بل لال ههيجوت دي عي ه نإف ، هجوم ل ةهجاو ةطساوب DHCP بلط ي قلت متي ام دنع . ثب ل ناو نعل DHCP يساس ال IP لوكوتور بل ردصم ناو نعل مادختساب (IP دعاسم ناو نعل نيوكت دنع) DHCP مداوخ ي ل ه مادختس ا بجي ي ذل IP عمجت ةفرعم ب DHCP مداوخ ل ةهجاو ل يلع هنيوكت مت ي ذل DHCP در ةمزح ي ف (لي معلل)

IP ةكبش يلع دوجوم زاغ نم يتي أي DHCP ثب بلط ناك اذا ام ةفرعمل هجوم ل ل ةقيرط دجوت ال

لبق ام ةكبش ىلع مداخ نم ديهمتلاب لمعلال ةطحمل (PXE) ذي فننتلا لبق ام ةئيب حمست ةرايزى لىلا ةكبشلا لوؤسم جاتحي ال .ي لحملا ةبلصلال صارقألا كرحم ىلع ماظنلا ديهمت جماربلا وليغشنتلا ماظن ليمحت نكمي .ايودي اهليغشنت ديهمت و ايلع ف ةدحمل لمعلال ةطحمل PXE ةئيب مدختست .ةكبشلا ربع مداخ نم زاهجلا ىلع ،ةيصيغشنتلا جماربلا لثم ،ىرخألا هب صاخلا IP ناووع نيوكتل DHCP لوكتورب .

عطقم ىلع ادوجوم DHCP مداخ ناك اذا هجوملا ىلع DHCP/BootP ليحرت ليكو نيوكت عارجا بجي قزيم عجار .ةيلحملا هجوملا هجاو ىلع ip helper-address رمألا نيوكت بجي .ةكبشلا نم هجوم رخا لوصحلل دنتسمل اذه يف [Cisco IOS هجوم مسق ىلع Configure DHCP/BootP ليحرت ليكو](#) .نيوكتلا تامولعم ىلع

تاراسم مادختساب اهالصالو هئاطخا فاشكتساو DHCP مهف sniffer

ةيلحملا ةكبشلا عطقم س فن ىلع مداخالو DHCP ليمع عبتت ريفشت ك ف (LAN)

ةيلحملا ةكبشلا عطقم س فن ىلع مداخالو DHCP ليمع دجاوتي ثيح ةكبشلا ططخم

هيف دجاوتي ويراني س ةتسل تاراطالا هذه حضوت .تاراطا ةتس نم sniffer عبتت لاثم نوكتي يلاتلا زمرلا لاثم مدختسا .يقطنملا و ايداملا عطقملا س فن ىلع مداخالو DHCP ليمع راثالا ىلا ك صاخلا sniffer عبتت قباطت نا مهمل نم .اهالصالو DHCP هئاطخا فاشكتسال ةيلاتلا ةروصملا راثالا عم ةنراقم لبا تافالخال ضعب كانه نوكتي نا نكمي .لاثلما اذه يف تاشقانملا يلي ةمزحلا بقعت .س فن امامت نوكتي نا يغبني ماعلا ةمزحلا قفدت نا ريغ DHCP لمع ةيفيكي لوح ةقباصل

----- Frame 1 - DHCPDISCOVER -----

```
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1[0.0.0.0] [255.255.255.255] 618 0:01:26.810 0.575.244 05/07/2001 11:52:03 AM DHCP: Request,
  Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame larrived at 11:52:03.8106; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 9
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
```

```

IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B988 (correct)
IP: Source address = [0.0.0.0]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 68 (BootPc/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00000882
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCC9C640
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303030352E646363392E633634302D564C31
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

```

----- **Frame 2 - DHCP OFFER** -----

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2[192.168.1.1] [255.255.255.255] 331 0:01:26.825 0.015.172 05/07/2001 11:52:03 AM DHCP: Reply,
Message type: DHCP Offer
DLC: ----- DLC Header -----
DLC:
DLC: Frame 2 arrived at 11:52:03.8258; frame size is 331 (014B hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station 0005DCC42484
DLC: Ethertype = 0800 (IP)

```

DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 5
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F901 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = **67 (BootPs/DHCP)**
UDP: Destination port = **68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Address Renewal interval = 42767 (seconds)
DHCP: Address Rebinding interval = 74843 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- - - - - **Frame 3 - DHCPREQUEST** - - - - -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3[0.0.0.0] [255.255.255.255] 618 0:01:26.829 0.003.586 05/07/2001 11:52:03 AM DHCP: Request,
Message type: **DHCP Request**

DLC: ----- DLC Header -----

DLC:

DLC: Frame 56 arrived at 11:52:03.8294; frame size is 618 (026A hex) bytes.

DLC: **Destination = BROADCAST FFFFFFFF**, Broadcast

DLC: **Source = Station 0005DCC9C640**

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

IP:0. = ECT bit - transport protocol will ignore the CE bit

IP:0 = CE bit - no congestion

IP: Total length = 604 bytes

IP: Identification = 10

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = B987 (correct)

IP: **Source address = [0.0.0.0]**

IP: **Destination address = [255.255.255.255]**

IP: No options

IP:

UDP: ----- UDP Header -----

UDP:

UDP: **Source port = 68 (BootPc/DHCP)**

UDP: **Destination port = 67 (BootPs/DHCP)**

UDP: Length = 584

UDP: No checksum

UDP: [576 byte(s) of data]

UDP:

DHCP: ----- DHCP Header -----

DHCP:

DHCP: Boot record type = 1 (Request)

DHCP: Hardware address type = 1 (10Mb Ethernet)

DHCP: Hardware address length = 6 bytes

DHCP:

DHCP: Hops = 0

DHCP: **Transaction id = 00000882**

DHCP: Elapsed boot time = 0 seconds

DHCP: Flags = 8000

DHCP: 1... = Broadcast IP datagrams

DHCP: Client self-assigned IP address = [0.0.0.0]

DHCP: Client IP address = [0.0.0.0]

DHCP: Next Server to use in bootstrap = [0.0.0.0]

DHCP: Relay Agent = [0.0.0.0]

DHCP: **Client hardware address = 0005DCC9C640**

DHCP:

DHCP: Host name = ""

DHCP: Boot file name = ""

DHCP:

DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: **Server IP address = [192.168.1.1]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

- - - - - **Frame 4 - DHCPACK** - - - - -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4[192.168.1.1] [255.255.255.255] 331 0:01:26.844 0.014.658 05/07/2001 11:52:03 AM DHCP: Reply,
Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 57 arrived at 11:52:03.8440; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 6
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F900 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----

DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 0000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 86400 (seconds)
DHCP: Address Renewal interval = 43200 (seconds)
DHCP: Address Rebinding interval = 75600 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- - - - - **Frame 5 - ARP** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 0005DCC9C640 Broadcast 60 0:01:26.846 0.002.954 05/07/2001 11:52:03 AM ARP: R PA=[192.168.1.2]
HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 58 arrived at 11:52:03.8470; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- - - - - **Frame 6 - ARP** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
6 0005DCC9C640 Broadcast 60 0:01:27.355 0.508.778 05/07/2001 11:52:04 AM ARP: R PA=[192.168.1.2]
HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----

```

DLC:
DLC: Frame 59 arrived at 11:52:04.3557; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

```

هناك مت هجوم امهلص في مداخل او DHCP ليمع عبتت sniffer ريفشت كفي DHCP ليجرت ليمعك

عتتت Sniffer-B

```

- - - - - Frame 1 - DHCPDISCOVER - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1 [0.0.0.0] [255.255.255.255] 618 0:02:05.759 0.025.369 05/31/2001 06:53:04 AM DHCP: Request,
  Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 124 arrived at 06:53:04.2043; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station 0005DCF2C441
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 183
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8DA (correct)
IP: Source address = [0.0.0.0]
IP: Destination address = [255.255.255.255]
IP: No options

```

```

IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 68 (BootPc/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00001425
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

```

- - - - - **Frame 2 - DHCP OFFER** - - - - -

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summaryr
125 [192.168.1.1] [255.255.255.255] 347 0:02:05.772 0.012.764 05/31/2001 06:53:04 AM DHCP:
Reply,

```

Message type: **DHCP Offer**

```

DLC: ----- DLC Header -----
DLC:
DLC: Frame 125 arrived at 06:53:04.2171; frame size is 347 (015B hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station 003094248F71
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine

```

```

IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 45
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C9 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 68 (BootPc/DHCP)
UDP: Length = 313
UDP: Checksum = 8517 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00001425
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Address Renewal interval = 49735 (seconds)
DHCP: Address Rebinding interval = 87037 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:

```

```

- - - - - Frame 3 - DHCPREQUEST - - - - -
- - -

```

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary

```

3 [0.0.0.0] [255.255.255.255] 618 0:02:05.774 0.002.185 05/31/2001 06:53:04 AM DHCP: Request,
Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 126 arrived at 06:53:04.2193; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFF, Broadcast**
DLC: **Source = Station Cisc14F2C441**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 184
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8D9 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**

DHCP: **Server IP address = [192.168.2.2]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

- - - - - **Frame 4 - DHCPACK** - - - - -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.1.1] [255.255.255.255] 347 0:02:05.787 0.012.875 05/31/2001 06:53:04 AM DHCP: Reply,
Message type: **DHCP Ack**

DLC: ----- DLC Header -----
DLC:

DLC: Frame 127 arrived at 06:53:04.2321; frame size is 347 (015B hex) bytes.

DLC: **Destination = BROADCAST FFFFFFFF, Broadcast**

DLC: **Source = Station 003094248F71**

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

IP:0. = ECT bit - transport protocol will ignore the CE bit

IP:0 = CE bit - no congestion

IP: Total length = 333 bytes

IP: Identification = 47

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = F8C7 (correct)

IP: **Source address = [192.168.1.1]**

IP: **Destination address = [255.255.255.255]**

IP: No options

IP:

UDP: ----- UDP Header -----

UDP:

UDP: **Source port = 67 (BootPs/DHCP)**

UDP: **Destination port = 68 (BootPc/DHCP)**

UDP: Length = 313

UDP: Checksum = 326F (correct)

UDP: [305 byte(s) of data]

UDP:

DHCP: ----- DHCP Header -----

DHCP:

DHCP: Boot record type = 2 (Reply)

DHCP: Hardware address type = 1 (10Mb Ethernet)

DHCP: Hardware address length = 6 bytes

DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**
DHCP: **Domain name = "cisco.com"**
DHCP:

- - - - - **Frame 5 - ARP** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- - - - - **Frame 6 - ARP** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.

```

DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

```

sniffer-A عبتت

```

- - - - - Frame 1 - DHCPDISCOVER - - - - -
- - -

```

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
118 [192.168.1.1] [192.168.2.2] 618 0:00:51.212 0.489.912 05/31/2001 07:02:54 AM DHCP: Request,
  Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 118 arrived at 07:02:54.7463; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 52
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3509 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [192.168.2.2]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: Checksum = 0A19 (correct)

```

UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload = 3 (File and Sname fields hold options)
DHCP:

- - - - - **Frame 2 - DHCP OFFER** - - - - -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2 [192.168.2.2] [192.168.1.1] 347 0:00:51.214 0.002.133 05/31/2001 07:02:54 AM DHCP: Request,
Message type: **DHCP Offer**

DLC: ----- DLC Header -----
DLC:
DLC: Frame 119 arrived at 07:02:54.7485; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 41
IP: Flags = 0X

```

IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3623 (correct)
IP: Source address = [192.168.2.2]
IP: Destination address = [192.168.1.1]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 313
UDP: Checksum = A1F8 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Address Renewal interval = 86285 (seconds)
DHCP: Address Rebinding interval = 150999 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:

```

- - - - - **Frame 3 - DHCPREQUEST** - - - - -

```

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [192.168.1.1] [192.168.2.2] 618 0:00:51.240 0.025.974 05/31/2001 07:02:54 AM DHCP: Request,
  Message type: DHCP Request
DLC: ----- DLC Header -----
DLC:
DLC: Frame 120 arrived at 07:02:54.7745; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)

```

DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 54
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3507 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [192.168.2.2]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: Checksum = 4699 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: Server IP address = [192.168.2.2]
DHCP: Request specific IP address = [192.168.1.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server

DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- - - - - **Frame 4 - DHCPACK** - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.2.2] [192.168.1.1] 347 0:00:51.240 0.000.153 05/31/2001 07:02:54 AM DHCP: Request,
Message type: **DHCP Ack**

DLC: ----- DLC Header -----

DLC:

DLC: Frame 121 arrived at 07:02:54.7746; frame size is 347 (015B hex) bytes.

DLC: **Destination = Station 003094248F72**

DLC: **Source = Station 0005DC0BF2F4**

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

IP:0. = ECT bit - transport protocol will ignore the CE bit

IP:0 = CE bit - no congestion

IP: Total length = 333 bytes

IP: Identification = 42

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = 3622 (correct)

IP: **Source address = [192.168.2.2]**

IP: **Destination address = [192.168.1.1]**

IP: No options

IP:

UDP: ----- UDP Header -----

UDP:

UDP: **Source port = 67 (BootPs/DHCP)**

UDP: **Destination port = 67 (BootPs/DHCP)**

UDP: Length = 313

UDP: Checksum = 7DF6 (correct)

UDP: [305 byte(s) of data]

UDP:

DHCP: ----- DHCP Header -----

DHCP:

DHCP: Boot record type = 2 (Request)

DHCP: Hardware address type = 1 (10Mb Ethernet)

DHCP: Hardware address length = 6 bytes

DHCP:

DHCP: Hops = 0

DHCP: Transaction id = 000005F4

DHCP: Elapsed boot time = 0 seconds

DHCP: Flags = 8000

DHCP: 1... = Broadcast IP datagrams

DHCP: Client self-assigned IP address = [0.0.0.0]

DHCP: Client IP address = [192.168.1.2]

```
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:
```

لمع تاطحم نوكت امدنع احوال صا DHCP ءاطخأ فاشكتسا DHCP نيوانع يلع لوصحلا يلع ةرداق ريغ ليمعلا

نوبز DHCP ك VLAN وأ ةعطق lan هسفن لا يلع لدان DHCP: 1 مقرر ةلاح ةسارد

لوصحلا ليمعلا ل نكمي الو VLAN وأ LAN عطقم سفن يلع ليمعلا او DHCP مداخل دجاوتي امدنع ةلكشم يف يلحملا هجوملا ببستي نأ لم تحملا ريغ نم نكلو. DHCP مداخل نم IP ناوانع يلع نأ نكمي، كلكذ عمو. DHCP ليمعو DHCP مداخل لصوت يتلا ةزهجالاب ةلكشملا لصتت. DHCP يلع ةيطمنلا تادحولا هذه دعاست. هسفن ليمعلا وأ DHCP مداخل عم ةلكشملا نوكت ةلكشم ببسي يذلا زاهجلا دحوت و احوال صا زاهجلا ءاطخأ فاشكتسا.

تاعمجت دح، (VLAN) ةيرهاطة يلحم ةكبش لك ساسا يلع DHCP مداخل نيوكتل: ةظالم
كئالمع لا DHCP نيوانع مدخت (VLAN) ةيرهاطة يلحم ةكبش لك ةفلتخملا DHCP

م هجوم ةطساوب DHCP ليمعو DHCP مداخل لصف متي: 2 مقرر ةلاح ةسارد DHCP/BootP ليحرت ليكو ةفيظول هنيوكت

هجوملا لمعي، VLAN تاكبش وأ ةفلتخملا LAN عطاقم يلع ليمعلا او DHCP مداخل دجاوتي امدنع تاوطخ ذاختا مزلي. DHCP مداخل لا DHCP هيجوت ةداع| نع لوؤسم DHCP/BootP ليحرت ليمعك DHCP مداخل ةفاضلااب، احوال صا و DHCP/BootP ليحرت ليكو ءاطخأ فاشكتسال ةيفاضا ل. كاشملا ببسي يذلا زاهجلا دحوت ك نكمي، تادحولا هذه تعبت اذا. ليمعلا او

عمجتلا دافنتسا مت أطخ عم نيوانع نييعت يف هجوملا يلع DHCP مداخل لشفي

عمجتلا نم اهرادصا مت اذا يتح، ءالمعلا اهب ظفتحي لازي ال نيوانعلا ضعب نأ لم تحملا نم امدنع ناوانعلا يف ضراعت ثدحي. ip dhcp ضراعت جارخا لالخم نم ءارجالا اذه نم ققحتلا نكمي عم تاوضراعتلا نم DHCP ققحتي، ناوانعلا نييعت يف. IP ناوانع سفن نافيسي ضم مدختسي ي. يناجم ARP و لاصتالا رابتخا

موقبي يتح ناوانعلا نييعت متي. عمجتلا نم ناوانعلا ةلازا متت، ضراعت فاشكتكا ةلاح يف رادصا اذه لحل ليحست ضراعت ip dhcp لكشي. ضراعتلا لحب لوؤسملا

اهحال صإو DHCP ءاطخأ فاشكتسأ تادحو

DHCP لكاشم ثدحت نأ نكمي نيأ مهف

لكاشم يه اعويش بابسأل رثكأ. ةديدع بابسأ ببسب DHCP لكاشم أشنت نأ نكمي ؤمظنأل ي فجماربلل بوي ع ببسب DHCP لكاشم نم ديدعلل ثدحي دق، كلذ عمو. نيوكتلل يل ع لمعت يتل DHCP/BootP ليحرت لم اوع وأ (NIC) ةكبشلا ةهجاو ةقاطب ليغشت جمارب يجهنم جهن عابتا مزلي، لكاشم يل ع يوطننت دق يتل قاطنملا ددعل ارظنو. تاهجوملا اهحال صإو ءاطخأل فاشكتسال.

DHCP لكاشم ل ةلمتحملا بابسألل ةريصق ةمئاق:

- Catalyst لوحمل يضا رتفالال نيوكتلل
- DHCP/BootP ليحرت ليك و نيوكت
- DHCP ةزيم ةلكشم وأ NIC قفاوت ةلكشم
- حيصلا ريغ NIC وأ بي عملا NIC ليغشت جمانرب تيبتت
- ةرركتملا ةعرفتملا ةرجشلا باسح تاي لمع ببسب ةكبشلا ةعطقتم عاطقنا تالاح
- جمانربلل بي ع وأ ليغشتلا ماظن كولس
- جمانربلل بي ع وأ DHCP مداخ قاطن نيوكت
- لل ةيجمرب ليك و ليحرت DHCP/BootP cisco ios وأ حاتفم ةزافح ةدام cisco
- مالتسإ مت هنأل (uRPF) يداخالل ثبلل يسكعلا راسملا هي جوت ةداعإ نم ققحتلا لشف راسملا هي جوت ةداعإ ةزيم نيكمت متي ام دنع. ع قوتملا نع ةفلتخم ةهجاو يل ع DHCP ضرع نيوكتلل لوكوتورب مزح طاقسإ Cisco هجومل نكمي، ةهجاو يل ع (RPF) يسكعلا نيوانع يل ع يوتحت يتل (BOOTP) ديهتملا لوكوتوربو (DHCP) فيضملل يكي ماني دلا IP مزح عي مج طاقسإ اضيأ هجومل نكمي و. 255.255.255.255 نم ةهجو نيوانعو 0.0.0.0 ردصم id قب cisco ي رادصإ اذه تقثو. ةهجاو لا ي ف ددعتملا ثبلل IP ةهجو يل ع يوتحت يتل [CSCdw31925](#)

ن. لجل جسملا Cisco ءالمع ال ءاطخأل ريراقت يل لوصولا عيطتسي ال ةظحال

- DHCP ضراعت لي جست لي طعت متي نكلو، DHCP تانايب ةدعاق لي مع مادختسإ متي ال

ي داملا لاصتالا نم ققحتلا - فلأ

ة. لالحتا تاسارد عي مج يل ع ءارجلال اذه قبطني و

Catalyst لوحمل ال صتم تنك اذا. مداخالو DHCP لي معل يل عفلا لاصتالا نم ال و ققحت ةدنتسملا تالو حملل ةبسنلاب. ي دام لاصتالا هي دل مداخالو DHCP لي مع نم الك نأ نم ققحتف ةلالحلا ذفنم ضرعل ئفاكملا رمأل، Catalyst 2900XL/3500XL/2950/3550 لثم Cisco IOS يل ال ءاني مالا، قوف نوكي لوكوتورب طخ، قوف نوكي < > ريغ عيش يأ نراقلا ةلود نإ. <interface> رمال نم جاتنإلا. ببلط نوبز DHCP يتح الو، رورم ةكح رمي

```
Switch#show interface fastEthernet 0/1
```

```
FastEthernet0/1 is up, line protocol is up
```

```
Hardware is Fast Ethernet, address is 0030.94dc.ac1 (bia 0030.94dc.ac1)
```

Catalyst switch لوحمل ني ب طابتر ي أ لعفلاب دجوي الو يل عفلا لاصتالا نم ققحتلا مت اذا [عم Cisco Catalyst تالو حم قفاوت](#) لكاشم [ءاطخأ فاشكتسأ مسق](#) مدختسأ DHCP لي معو ةقبطلا لاصتالا ةلكشم ب ةقلعتملا لكاشملا نم اهحال صإو (NIC) [ةكبشلا ةهجاو ةقاطب](#) ةي داملا.

errdisable لخد بهذي نأ حاتفم ةزافح ةدام ضعب ىلع ءانيم أطخ ببسي ةوطخ طرفم تانايابل
فصي ي، [قصنم cisco ios لىلع ةداعتسا ءانيم لىل لىحي](#) ةمولعم ريثك ل . ةلود
ةلود اذه نم ةداعتسا نم لاثم دوزيو، وه نم درتسي نأ فيك رسفي، errdisable ةلودلا

ةكبشلا لاصتا رابتخال تباثلا IP و لىمعال لمع ةطحم نيوكت .ب

ةلجال تاسارد عيمج ىلع ءارجلا اذه قبطنيو

لمع ةطحم نوبز ىلع يكيتاتسا نكاس ناووع لكشي نأ مهم وه ، رادصا DHCP يا تيحت ام دنع
ةكبشلا دراوم ىلا لوصولا نم لمعلا ةطحم نكمتت مل اذا . ةيولوصوم ةكبش تققد in order to
يرذللا ببسلا نإف ، تباث لكش ببس هنيوكت مت IP ناووع اهل نأ ةقيقح نم مغرلا ىلع
ةكبشلا لاصتا ءاطخا فاشكتسا كمزلي ، ةطقنلا هذه دنع . DHCP سيلا ةلكشملا
ءاحالساو

ليغشت ءدب ةلكشم ةلكشملا نم ققحتلا .ج

ةلجال تاسارد عيمج ىلع ءارجلا اذه قبطنيو

كنكمي ف ، ليغشتلا ءدب دنع DHCP مداخ نم IP ناووع ىلع لوصولا DHCP لىمعال رذعت اذا
ىلع ايودي لوصولا ةيلالاتا ءاطخا رادصا مق . DHCP بلط لاسرا ىلع ايودي لىمعال رابجا
جردملا ليغشتلا ماظنل DHCP مداخ نم IP ناووع

Microsoft Windows 95/98/ME: ليغشتلا ماظن

1. WinIPCFG.exe جمانرب ليغشتب مقو Startbutton رزلا قوف رونا .
2. لكلا ديحت رزلا هعبتي مت ، لكلا ريحت رزلا قوف رونا .
3. IP؟ ناووع ىلع لوصولا ىلع نألا رداق DHCP لىمع له



IP نيوكت ءذفان

Microsoft Windows NT/2000: ليغشتلا ماظن

1. رماوالا ةبللاطم ءذفان حتفل Cmdin **Start/Run**field لخدأ .
2. **commandConfig/renin** رمالا هجوم ءذفان رادصا مق .
3. IP؟ ناووع ىلع لوصولا ىلع نألا رداق DHCP لىمع له

(NIC) ةكبشلا ةهجاو ةقاطب تامولعم ىلإ ةفاضلإاب DHCP ليمع ليغشت ماظن ةفرعم مزلي في لكاشم يا داعبتس لايغشت لاجم انرب رادصا و زارطلا و ةعنصملا ةكرشلا لثم ةدحملل احيحص لكشب قفاوتلا.

f. ةكبش و اءي عرفلا ةكبشلا سفن ىل ع IP ناو نع ىل ع نولصحي DHCP ءالمع ناك اذا ام زي م. VLAN مءا ك DHCP

ل يمع ل نوكي ام دن ع ال و احيحص لكشب لمعي DHCP لو كوتورب ناك اذا ام زي م ت م هم ل ن م لكشب DHCP لمعي مل اذا. DHCP مءا ك VLAN ةكبش و اءسفن ةي عرفلا ةكبشلا ىل ع ابلاغ DHCP رادصا ن ا ف، DHCP مءا ك اءسفن VLAN ةكبش و اءي عرفلا ةكبشلا ىل ع احيحص ىل ع DHCP راب ت ا دن ع ىل ع ةل كشم ل ا ترم ت سا اذا. DHCP/BootP ل يحر ت ل يكو ب بس ب نوكي ام ةل كشم ل نوك ت دق ف، DHCP مءا ك ةصا ا ل VLAN ةكبش و اءسفن ةي عرفلا ةكبشلا DHCP مءا ك عم ل ع ل ا ب.

g. DHCP/BootP هءوم ل ل يحر ت ن يوك ت ن م ق قح ت ل ل

ن يوك ت ل ل ن م ق قح ت ل ل:

1. ip helper-addresscommand رم ال ع قوم د يحر ت ن م ق قح ت، هءوم ىل ع DHCP ل يحر ت ن يوك ت ب موقت ام دن ع. DHCP مءا ك ىل ا هه يحر ت ب جي و DHCP ليمع لمع تاطحم ل ةءراول ا هءا و ل ا ىل ع اءوم احيحص ل ا.
2. ل يطر ع ت ب هءه ن يوك ت ل ا ةم ل عم موقت. service dhcp ماع ل ن يوك ت ل ا رم اءوم مءع ن م ق قح ت. ال و service dhcp، يضر ا ر ت ف ال ن يوك ت ل ا. هءوم ل ا ىل ع ل يحر ت ل ا ف اءظوو DHCP مءا ك ع ي م ج، DHCP راي ا ل ا اءه ن ي ك م ت م ت ي مل اذا. يضر ا ر ت ف ال ن يوك ت ل ا رم اءي هو، ن يوك ت ل ا ي ف ر ه ط ت ل غ ش ت ي ت ل ا ت ا هءوم ل ا ي ف: ةظا ل م. DHCP مءا ك ن م IP ن ي و ا ن ع اءالمع ل ا م ل ت س ي ن ل ف ال ا ب DHCP ل يحر ت ل يكو ة ف يظ و ip bootp server رم ال ا ج ل ا ع ي، مءق ال Cisco IOS ت ا ر ا د ص ا ت ا هءوم ل ا هءه ي ف ip bootp server رم ال ن ي ك م ت مز ل ي، ب بس ل ا اءه ل و service dhcp رم ال ن م لمع ل و DHCP UDP ث ب ت ا ي لمع ه يحر ت ةءاع ل ip helper-address رم ال ن يوك ت م ت اذا DHCP ل يحر ت ن ع ةب ا ي ن ل ا ب DHCP ل يحر ت ل يكو ك احيحص لكشب.
3. ناو نع ىل ا UDP ث ب ت ا ي لمع ه يحر ت ةءاع ل ip helper-addresscommand رم او اءا د خ ت سا دن ع. هءا و ا ي ا ىل ع ن يوك ت م ت ي مل no ip directed-broadcast كل ذ ن م ق قح ت، ةي عرف ةكبش ل ث ب ث ب ل ل ةم ج ر ت ي ا ع ن م no ip directed-broadcast رم ال ا ضر ع ي. UDP ث ب مز ح ا ه ز ا ت ج ت ن ا مز ل ي ةر د ا ص ىل ع او 12.0 ةغ ي ص ةي ج م ر ب ي ف ر ي ص ق ت ل ل ل ي ك ش ت ن ر ا ق اءه. ي ل ع ف ل ا ث ب ل ا ىل ا هءوم ل ا.
4. DHCP مءا ك ل ا ةي عرف ل ا ةكبش ل ا ث ب ناو نع ىل ا DHCP ث ب ت ا ي لمع ه يحر ت ةءاع ل م ت ام دن ع. لس ر ي ن ا ت ل و ا ح، DHCP لكاش م ت يحر ت ام دن ع. ج م ان ر ب ل ا ي ف ةل ك شم ا ش ن ت ن ا ن ك م ي ناو نع ل ا ن DHCP ل ا ىل ا ث ب DHCP udp:

(82) ك ر ت ش م ل ا ف ي ر ع ت ر ا ي خ ل ي غ ش ت م ت

ل ي م ع ن م DHCP ت ا ب ل ط ه يحر ت ةءاع ل دن ع ق ف ر م ل ل ي م ع ل ا و ه س ف ن ل و ح ت ا م و ل ع م ن ي م ص ت DHCP مءا ك ىل ا DHCP.

ل و ص و ل ا ي ف م ك ح ت ل ا ا ر ج ا و IP ن ي و ا ن ع ن ي ي ع ت ل ت ا م و ل ع م ل ا هءه م اءا د خ ت سا DHCP مءا ك ن ك م ي ل ك ل (ى ر خ ال ا ت ا م ل ع م ل ا ن ي ي ع ت ا س ا ي س و ا) ن ا م ال ا ت ا س ا ي س و (QoS) ةمءا ل ا ةءو ج ن ي ي ع ت و ىل ع DHCP لو كوتورب ىل ع ل ف ط ت ل ل ن ي ك م ت م ت ي ام دن ع. ةمءا ل ا ةءوم ةكبش ي ف ك ر ت ش م م اءا د خ ت س ا ب مز ح ل ا ةءال ع م ل DHCP مءا ك ن يوك ت م ت ي مل اذا. ا ي ا ق ل ل ت 82 راي خ ل ا ن ك م ي ه ن ا ف، ل و ح م ل ي ط ع ت ب م ق، ةل ك شم ل ا هءه ل ح ل. ب ل ط ل ا ل ك ل ذ ل ناو نع ل ا ص ي ص خ ت ن ع ف ق و ت ي ه ن ا ف، 82 راي خ ل ا

معالج نيوكتال رما م ادختساب (لجرتالءالكو) تالوحملا ف (82) كرتشملا فبرعت رايخ،
DHCP IP لجرت تامولعم رايخ نودب.

i. DHCP تاضراعت لججستو DHCP تانايب ةدعاق لماع

ننخي نألدان RCP أو TFTP أو FTP، لالملا لابس لعل-فبضم ي لكو تايطعم ةدعاق DHCP كنيومي، DHCP تانايب ةدعاق مالمع نم ديدعل نيوكت كنيومي. تايطعم ةدعاق طبر DHCP لمدختسا. ليمع لكل لقلنلا تايلمعو تانايبلا ةدعاق تاثيرحت نيبي نينمزللا لصال نيوكت تانايب ةدعاق لماع تاددحمو تانايب ةدعاق لماع نيوكتل `ip dhcp database` رمالا.

نيوانع تاضراعت لججست ليطعتب مق، DHCP تانايب ةدعاق لماع نيوكت مدع ترتخا اذا لججست ليطعتل `thenoip dhcp conflict logging` رمالا ذيفنتب مق. DHCP مداخل ل DHCP IP تاضراعت حسم نود اقبس م ةلجسمل تاضراعتال حسم. DHCP ناوانع تاضراعت

هذه أطلخال ةلسر رهظت، تاضراعتال لججست ليطعت ي ف اذه لش ف اذا:

```
%DHCPD-4-DECLINE_CONFLICT: DHCP address conflict: client
```

ز. تنرتنإلا لوكوتورب فاتاه تالاصتال CDP صحف

Cisco (CDP) فاشتكلا لوكوتورب هي دل Cisco IP فاتاهب لصتلملا Switchport نوكي ام دنع نييعت ل DHCP مداخل ليمي. فاتاهلل بسانم IP ناوانع نييعت DHCP مداخل نكمي ال، لطمع switchport. ل ةيعرفلا ةكبشلا / تانايبلل VLAN ةكبش ل يمتني يذلا IP ناوانع DHCP لوكوتورب بلطي Cisco IP فاتاه نأ فاشتكلا لوحملل نكمي، CDP لوكوتورب نيكممت نأ عيطتسي كلذ دعبلدان DHCP ل. ةححصلا ةيعرفلا ةكبشلا تامولعم رفوي نأ نكمي و ةمدخ طبرل ةبولطم ةحيرص تاوطخ دجوت ال. ةكرب VLAN / subnet توصلال نم ناوانع لسري ةيوتوصل VLAN ةكبش DHCP.

ك. DHCP لوكوتورب لعل لفطتلا ةي لمع لطي لفسأل SVI ةلازا ك.

نأ دعبل ايئاقلت (ةلود لمع فاقيل ي) SVI تقولخ، حاتفم 6500 sery ةزافح ةدام cisco ل لعل ةي لمعل لعل ةرشابم تاريثات هل SVI اذه دوجو نأ. صاخ VLAN ل لفطتي نأ DHCP ل لكشي DHCP لعل لفطتلل ةححصلا.

Cisco Catalyst 6500 Series Switches تالوحم لعل DHCP لوكوتورب لعل لفطتلا ذيفنت متي لعل سي لو، (MSFC أو RP) هي جوتال جلامع لعل ابلاغ لصلال Cisco IOS جمانرب لغشت يتل VACLs عم زاهج ي ف طبر 6500 sery ةزافح ةدام cisco ل ضرعتي. (فرشملا أو SP) لوحملا جلامع مه، RP ل تاراطال لخدني نأ ام. RP ل ب ل كرتشم (LTL) قطنم فده ي لعل طبرلا دوزي نأ ل ررمت تنك عيطتسي مه نأ ل بق IDB (SVI) نراق L3 عم تبحص نوكي نأ ال و نوجاتي ل RP ي ف مزحلل طاقسإ متي و، اذه IDB دجوي ال، SVI نودب. عجل لفطتلملا

دودحملا ثبل ناوانع - مال

لوكوتورب DHCP مداخل لسري، DHCP ةمزح ي ف ثبل تب ةدحو نييعت DHCP ليمع موق ي ام دنع اذا. (255.255.255.255) داخلال لكل ثبل ناوانع م ادختساب مالمعل ل DHCP لئاسر لجرتال داخلال لك ثب زواجت متي سف، ةكبشلا لعل ثب لاسرل `ip broadcast-address` رمالا نيوكت مت داخلال م ادختسا، ةلاجل هذه لعل DHCP. ةطساوب هلاسر مت يذلا ي ضارثال DHCP كولس هنيوكت مت يذلا ةكبشلا ثب زواجتي ال نامضل `address`.

مل ام DHCP ناوانع باس تكا مهنكمي الو طقف all-ones ثب لوبق DHCP مالمع ضعبل نكمي ليمعللاب ةلصتلملا هجوملا ةهجاو لعل رمالا اذه نيوكت متي.

هجوم ال عا طخ ا ححصت رما و ا عم debug dhcp

debug رما و ا مادختساب DHCP ب ل ط ي ق ل تي هجوم ال ن ا نم ق قحت

هجوم ال ن ا ك ا ذ ا امم ق قحت ال ك ن ك م ي ، DHCP مزح ج ل ا ع ت ي ت ل ا ج م ا ر ب ل ا م ع د ت ي ت ل ا ت ا ه ج و م ل ا ي ل ع ن م ت ا ب ل ط ه ج و م ل ا م ل ت س ي م ل ا ذ ا DHCP ة ي ل م ع ل ش ف ي . ل ي م ع ل ا ن م DHCP ب ل ط ي ق ل تي م ا د خ ت س ا م ت ي . ج ا ر خ ا ل ا ع ا ط خ ا ححصت ل ل و ص و ة م ا ق ن ي و ك ت ب م ق ، ة و ط خ ل ا ه ذ ه ي ف . ل ي م ع ل ا ه ج و م ل ا ي ل ع ة ل ي خ د ت س ي ل ي ه و ر م ا ع ا ط خ ا ححصت ل ط ق ف ه ذ ه ل و ص و ل ا ة م ا ق .

هذه ل و ص و ل ا ة م ا ق ل خ د ا ، م ا ع ل ا ن ي و ك ت ل ا ع ض و ي ف :

```
access-list 100 allowed ip host 0.0.0.0 255.255.255.255
```

اذ ه ا ع ا ط خ ا ل ا ححصت رما ل خ د ا ، EXEC ع ض و ي ف :

```
debug ip packet detail 100
```

ت ا ج ر خ م ل ل ج ذ و م ن

```
Router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
Router#
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
```

ل ي م ع ل ا ن م DHCP ت ا ب ل ط ط ش ن ل ك ش ب م ل ت س ي ه ج و م ل ا ن ا ح ص ا و ل ا ن م ، ا ذ ه ج ا ر خ ا ل ا ل ا ث م ن م ا ذ ا ا م د ي د ح ت ن ك م ي ا ل ، ك ل ذ ل . ا ه س ف ن ة م ز ح ل ا س ي ل و ة م ز ح ل ل ا ص خ ل م ط ق ف ج ا ر خ ا ل ا ا ذ ه ض ر ع ي ة ه ج و ل ا و ر د ص م ل a UDP و IP ذ ف ا ن م ع م ث ب ة م ز ح ه ج و م ل ا م ل ت س ا ، ك ل ذ ع م و . ة ححص ة م ز ح ل ا ت ن ا ك DHCP ل ة ححص ن و ك ت ي ت ل ا .

debug ip udp رما و ا مادختساب DHCP ب ل ط ل س ر ي و ل ب ق ت س ي ه ج و م ل ا ن ا نم ق قحت

ححصت ن ا ف ، ك ل ذ ع م و . ه ج و م ل ا ل ا خ ن م DHCP ب ل ط ر ا س م debug ip udp رما ل ا ع ب ت ت ي ن ا ن ك م ي ت م ت ي ت ل ا ة ل و ح م ل a UDP مزح ع ي م ج ض ر ع م ت ي ه ن ا ل ا ر ط ن ، ج ا ت ن ا ة ئ ي ب ي ف ل ي خ د ا ذ ه ا ع ا ط خ ا ل ا ج ا ت ن ا ل ي ف ا ذ ه ا ع ا ط خ ا ل ا ححصت رما و ا مادختساب مدع ب ج ي . م ك ح ت ل ا ة د ح و ي ل ا ه ت ج ل ا ع م

ة ج ل ا ع م ل ا ة د ح و م ا د خ ت س ا ي ف ب ب س ت ي ن ا ن ك م ي و ، ا ل ف ط ت م debug ip udp رما ل ا د ع ي : ر ي ذ ح ت ر ي ب ك ل ك ش ب (CPU) ة ي ز ك ر م ل

debug ip udp : ا ذ ه رما ل ا ل خ د ا ، EXEC ع ض و ي ف

ت ا ج ر خ م ل ل ج ذ و م ن

```
Router#debug ip udp
UDP packet debugging is on
Router#

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
```

```
!--- Router receiving DHCPDISCOVER from DHCP client.
00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source IP address.
00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313
!--- Router receiving DHCPOFFER from DHCP server directed to DHCP/BootP Relay Agent IP address.
00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333
!--- Router forwarding DHCPOFFER from DHCP server to DHCP client via DHCP/BootP Relay Agent.
00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
!--- Router receiving DHCPREQUEST from DHCP client.
00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source IP address.
00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313
!--- Router receiving DHCPACK (or DHCPNAK) from DHCP directed to DHCP/BootP Relay Agent IP address.
00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333
!--- Router forwarding DHCPACK (or DHCPNAK) to DHCP client via DHCP/BootP Relay Agent.
00:18:48: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32
!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.
00:18:50: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32
!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.
```

debug ip dhcp مداخل رمأ عم DHCP ب ل ط ل س ر ي و م ل ت س ي ه ج و م ل ن أ ن م ق ق ح ت

كنكم في Cisco IOS DHCP مداخله في ظل مودي 12.1 أو 12.0.x.T وه Cisco IOS هجوملنا ان اذا عم مداخلتس ال اذ ه ا ط خ ال ا ح ص ت م ي م ص ت م ت **debug ip dhcp server packet** رم ال ا م ا د خ ت س ا م ك . اض ي ا ه ا ل ص ا و DHCP/BootP ل ي ح ر ت ل ي ك و ة ز ي م ا ط خ ا ف ا ش ك ت س ا ل و IOS DHCP م د ا خ ة ز ي م ا ر ط ن ة ل ك ش م ل ل ا ق ي ق د ا د ي د ح ت ه ج و م ل ا ا ط خ ا ا ح ص ت ر ف و ت ال ، ة ق ب ا س ل ا ت ا و ط خ ل ا عم ل ا ح ل ا وه ا م ي ف ت ا ل ا ل د ت س ا ل ا ا ر ج ا ب ا ط خ ال ا ح م س ت ، ك ل ذ عم و . ة ي ل ع ف ل ا ة م ز ح ل ا ض ر ع ن ك م ي ال ه ن ال ا ذ ه ا ط خ ال ا ح ص ت ر م ا ل خ د ا ، EXEC ع ض و ي ف . DHCP ة ج ل ا ع م ب ق ل ع ت ي

debug ip dhcp مداخله عم

```
Router#debug ip dhcp server packet
```

```
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
```

```
!--- Router received DHCPDISCOVER/REQUEST/INFORM and setting Gateway IP address to 192.168.1.1 for forwarding.
```

```
00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..
!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.

!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.
00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.
!--- BOOTREPLY includes DHCPPOFFER and DHCPNAK.

!--- Client's MAC address is 00e0.1ef2.c441.
00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.
!--- Router is forwarding DHCPPOFFER or DHCPNAK broadcast on local LAN interface.
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- Router received DHCPDISCOVER/REQUEST/INFORM and set Gateway IP address to 192.168.1.1 for forwarding.
00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..
!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.

!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.
00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.
!--- BOOTREPLY includes DHCPPOFFER and DHCPNAK.

!--- Client's MAC address is 00e0.1ef2.c441.
00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.
!--- Router is forwarding DHCPPOFFER or DHCPNAK broadcast on local LAN interface.
```

تقولا سفن في اطاخ احي حصت دة ل غشت

لوق عم ردق فاشتك انكمي، دحاو تقو في اطاخ ال احي حصت نم دي دعال ل غشت ب موقت امدنع مدختست تنك اذا DHCP/BootP ل احي حصت م داخو ل و ل غشت ب قلعتي امي في تامول عمل نم ناكم لوح تال الدتسا اراج كنكمي في، احوال ص او اطاخ ال فاشك تسال ة ق باس ال اية ج راخ ال دودحل احي حصت لك ش ب DHCP/BootP ل احي حصت ل و ل غشت ب موقت امدنع.

```
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
```

```
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328.
```

DHCP ةلكش مل یرذجل ببس الل دیح و sniffer عبتت یلع لوصح الل

[ةیلح مل اةكبش لا عطقم سفن یلع مدخال او DHCP لیمل زیمرت لا كفل sniffer عبتت عجار یذلا هجوم لا عطقم اب نی لوصف مل ا مدخال او DHCP لیمل زیمرت لا كفل sniffer عبتت و \(LAN\) DHCP لیحرت لیك و ماسق أك هنیوكت مت](#)

DHCP. مزح تاراسم ریفش ت كفل

(نیتماعد نیب عحس ف) رسیأ للحم لوحی لا عم رثأ sniffer لصحی نأ فیک یلع ةمولعمل تلحأ (نیتماعد نیب عحس ف) رسیأ للحم لوحی ةزافح ةدام لا لكش ی، حاتفم ةزافح ةدام یلع ةمس [للا م لیكش ت](#).

هجوم لا یلع ااطخال اهیحصت عم ةمزح لا ریفش ت كفل لیذب لا بولس الل

ةمزح یلع لوصح الل نك ممل نم، Cisco هجوم یلع <acl> debug ip packet detail رم الل مادختساب [هجوم عجار](#) (CLI) رم الل رطس ةهجاو و امانن لا لچس یف ةضورعم ةیرشع ةیسادس ةلماك [ملتسی CommandVerify Router ااطخال اهیحصت عم DHCP بلط ملتسی عحص لا نم ققحت لا](#) عم، هالعأ ةدراولا [ااطخال اهیحصت رم او ا عم DHCP مدخال یل DHCP بلط لسری و DHCP بلط](#) سفن یلع لوصح الل، لوصول ةمئاق یل ا اهتفاضل تمت یل ا غیرفت ةیساس الل ةمك الل تايوتحم دیح تل. ةیرشع ةیسادس ةمزح لا لیصافت عم نكلو، ااطخال اهیحصت تامولعم ا قحلم لا یف لاثم كانه. ةمزح لا ةمچرت مزلی، ةمزح لا

Cisco IOS DHCP ةنیع نیوكت: ا قحلم لا

تاكبش لا نیوانع عمچت وه ةرچش لا رذج. ةرچش ك DHCP مدخال تانا یب ةدعاق میظنت متی ةیودی طباور یه قاروال او، ةیعرفل تاكبش لا نیوانع تاعمجت یه عرف الل او، ةیعیب الل ةیعرف الل تاكبش لا تامولعم ءالمعل ثری و ةكبش لا تامولعم ةیعرف الل تاكبش لا ثرت. ءالمعل و ءكبش لا) یوتسم یلع یلع، لاجم لا مسا لثم، ةعئاشل تامولعم نیوكت بچی، كذل ةرچشلل (ةیعرف الل ةكبش لا

[لیكش ت DHCP لا](#)، هب ةطبترم لا رم الل او DHCP لكش ی نأ فیک یلع ةمولعم ریثك ل تلحأ [ةمهم ةمئاق](#).

```
version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```



```
!  
hostname Router  
!  
enable password cisco  
ip subnet-zero  
no ip domain-lookup  
ip dhcp excluded-address 10.10.1.1 10.10.1.199  
  
!--- Address range excluded from DHCP pools.  
  
ip dhcp pool test_dhcp  
  
!--- DHCP pool (scope) name is test_dhcp.  
  
network 10.10.1.0 255.255.255.0  
  
!--- DHCP pool (address will be assigned in this range) for associated Gateway IP address.  
  
default-router 10.10.1.1  
  
!--- DHCP option for default gateway.  
  
dns-server 10.30.1.1  
  
!--- DHCP option for DNS server(s).  
  
netbios-name-server 10.40.1.1  
  
!--- DHCP option for NetBIOS name server(s) (WINS).  
  
lease 0 0 1  
  
!--- Lease time.  
  
interface Ethernet0  
description DHCP Client Network  
ip address 10.10.1.1 255.255.255.0  
no ip directed-broadcast  
!  
interface Ethernet1  
description Server Network  
ip address 10.10.2.1 255.255.255.0  
no ip directed-broadcast  
!  
line con 0  
transport input none  
line aux 0  
transport input all  
line vty 0 4  
login  
!  
end
```

قلم تاذ تامول عم

- [دراومل او ت او دال](#)
- [ښنفل مر عدل - Cisco Systems](#)

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 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 م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه 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