

# ريظن ىلإ ريظن لاصتا نيكم تل NAT مهف IOS و IOS XE تاهجوم ىلع

## تايوتحمل

[مدمقمل](#)

[سياسا تامولعم](#)

[NAT زاي تاجا ىلإ ةجالحا](#)

[NAT لئاسل جلا لئاب ةدعاسم تاودا](#)

[NAT ذي فنت تاي لمع عاونأ](#)

[Symmetric NAT و NAT Traversal عم لكاشم](#)

[قلاسملا ج](#)

[صخلم](#)

## مدمقمل

ناونع ةكبش نم عونلا، (STUN) NAT لدانل ةعفنم لمع ةسلج ىلإ ةجالحا ةقيثو اذه فصبي  
لجلاو دادع اذه يف ةلكشم ببسي NAT فيك، STUN مداوخب قلعتي اميف (NAT) ةمجرت

## سياسا تامولعم

ةقطنم ةكبش يف ةصاخلا IP نيوانع تاذه ةجالحا حامسلا وه NAT ةزهجأ نم سياسي اساسا لضرغلا  
لكذ عمو. تنرتنإلا لثم، ةماعلا نيوانعلا تاخاسم يف ةزهجألاب لاصتالاب (LAN) ةيلحم  
لاصتالاب نييلخادلا نييفيضملا NAT ةزهجأ حمست نا ضرتملا نم هنا نم مغرلا ىلع  
رمألا قلعتي ام دنع هذه UDP تالاصت اءاشنإ يف ةبوعص رفوي NAT نا اءا، ةماعلا ةحاسملا ب  
ثيح تافلما ةكراشم و WebRTC و باءالاب VoIP لثم (P2P) ةطقن ىلإ ةطقن نم تاقبب طاب  
لاصتالا ىلع ظافحلل ءاوس دح ىلع مداو لي معك لمعلا ىلإ نويئاها نل نومدختسملا جاتحي  
تاي نقت نوكت. هذه UDP تالاصت اءاشنإ يف ةبوعص رفوي NAT نا اءا، ةطقن ىلإ ةطقن نم  
لمعت تاقبب طابلا هذه لجعل يجذومن لكشب ةبولطم NAT زاي تاجا

## NAT زاي تاجا ىلإ ةجالحا

مويلا دئاسلا هاجتالا وه تنرتنإلا ىلع ويديفلاو توصلاب يلعفلا تقولا يف لاصتالا نا  
يتلا ةريكبلا تابققلا يدح. VoIP تاملكم معدت يتلا (IM) ةيروفلا تالسا رمل نم ديدعلا عم  
ىرخالا ةزهجالا ورتوي بمكلا ةزهجأ مظعم نا اءا ئداب يف VoIP لوكوتورب يئبب تهجاو  
ناونع) صاخ ناونع ددعتي تنبي. ةصاخلا IP نيوانع مدختست و ةيماحلا نارنج فلخ عقت  
فرعي ال فرطال زاوجل نكلو. NAT عم ةيماح رادج ديحوماع ناونع ىلإ ةكبشلا يف (ذفنم و  
ناونعلا ىلع ديعبالا فرطال نم توصلال رورم ةكرح يقلت هنكمي ال يلاتلابو، ماعلا هانوع  
هب صاخلا VoIP لاصتالا يف هنع نلعا يذلا صاخلا

طاقن ضرب اهيف لواحت تاي لمع يه (UNSAF) يداحالا ناونعلا لئاب لئاب لئاب لئاب لئاب لئاب  
ىلع و اءا ةيماح ةطقن هب فرعي يذلا (ذفنم لئاب) ناونعلا لئاب لئاب لئاب لئاب لئاب لئاب

نع نالعالا وأ لوكوتوربالا لدابت في ناونعالا تانايب مادختسا إلى عةردقلا، لاثملا لىبس تالاصتالا هنم يقلتت ماع ناونع.

عاشنال عةئاشلالا قرطالا يدحا. UNSAF تايلمع يه عةشقانملا ديقي P2P تالاصتالا نإف، ماث نمو مدختست امدنع يه NAT ل عمئالم امنوك في رارمتسالاور يظن لمع تاسلجلا P2P تاقىببطت ريظنلا فاشتكوا وليجستلا ضارغأل ماع لكشبه هيحوتلل لباق خسن مداخ.

## NAT ل تاسلجلا لدابت عةدعاسم تاودأ

تاقاطب عم لماعتت عاأا (STUN) عةرفتملا عرجشلالا لوكوتورب رفوي، RFC 5389 راي عمل اقفو عاأا nat ب ني عي ذفنمو ناونعالا دحجي نأ عياهن عطقنل علسو رفوي وه. (NAT) عكبشلالا هعواو ايح NAT طبر عاقبال عياهن عطقنل عقي رط رفوي امك. صاخ ذفنمو ناونع وه لثامي نأ.

## NAT ذيفنت تايلمع عاونأ

ذيفنتلا تايلمع ني ب امي ففلتخت عمادتسملا عيمنتلا ططخمل NAT علماعم نأ طحولو يه ذيفنتلا تايلمع في تظحول يتلا عةبرألا تاجالعالا:

إلى تنيع ذفنمو ناونع يلىخاد هسفنلا نم بلط لك شيح دحاو لمك طورخم NAT: لمك طورخم إلى عمزح لاسرا يجرخا فيضم يأل نكمي، كلذىل عةوالع. يجرخا ذفنمو ناونع هسفنلا هني عت مت يذلا يجرخال ناونعالا إلى عمزح لسريو، يلىخادل فيضملا.

ذفنمو ناونع يلىخاد هسفنلا نم تابللطا لك شيح دحاو وه ديقم طورخم NAT: ديقم طورخم (x ناونع عم) يجرخا فيضم، لمك طورخم NAT فالخ ب. ذفنمو ناونع يجرخا هسفنلا إلى تنيع طبر تل سراً اقباس ناك يلىخاد فيضملا نإ طقف يلىخاد فيضملا إلى طبر تل سراً عي طتسي إلى x ناونع إلى.

ماقرأ نمضتي ديقل نأ ريغ، طورخم ديقملا طورخملا NAT هبشي: ذفنملا ديقملا طورخملا ردصم و X ناونع ردصم عم، عمزح لاسرا يجرخال فيضملا نكمي، صوصخال هجو إلى عو. ذفانملا إلى لباق نم عمزح لسراً دق يلىخادل فيضملا ناك إذا طقف يلىخادل فيضملا إلى، P ذفنم IP X ناونع P. ذفنم و X ناونع.

صاخ عياغ إلى ذفنمو ناونع يلىخاد هسفنلا نم بلط لك شيح دحاو لثامتم NAT: لثامتم عم طبر فيضم هسفنلا لسري نإ. ذفنمو ناونع يجرخا هسفنلا إلى تنيع، ذفنمو ناونع إلى عةوالع. تلمعستسا فلتخم ططخي، فلتخم عياغ إلى نأ ريغ، ذفنمو ناونع ردصم هسفنلا إلى رخأ عرم UDP عمزح لاسرا عمزح ملتسي يذلا يجرخال فيضملا طقف نكمي، كلذىل يلىخادل فيضملا.

ذفنملا وه PA و، IP ناونع وه A شيح) (A، PA) ردصملا لصتي شيح ططخم رابتعالا في عض nat. زاخ لالخنم (C، PC) و (B، Pb) عةجولاب (ردصملا).

NAT ذيفنت عون	مت امدنع ماع ردصم (B، Pb) إلى ههيجوت	متي امدنع ماع ردصم زاخ C، إلى اههيجوت (رتوي بمك)	(ب، ب): الثم) عياغ عي طتسي (أ، ب) إلى رورم عكرح لسري (ب، ب)؟
لمك طورخم	(x1، px1)	(x1، px1)	معم

ديقم طورخم	(x1,px1)	(x1,px1)	تلسرأ (A, Pa) اذا طقف ىل ةرم لوأل ةكرحلا
ديقم طورخم ذفنم لل	(x1,px1)	(x1,px1)	دق (A, PA) تناك اذا طقف ىل ةرم لوأل ةكرحلا تلسرأ (B, Pb)
يرطانت	(x1,px1)	(x2,px2)	دق (A, PA) تناك اذا طقف ىل ةرم لوأل ةكرحلا تلسرأ (B, Pb)

## NAT Traversal و Symmetric NAT عم لكاشملا

ذفنم رفوتو STUN ءالمع اهلسري يتلا STUN طبر تاب لطل STUN مداوخ بيحتست  
ف STUN ليمع لبق نم هذه ذفانملا/نيوانعلا ةعومجم مادختسا متي، نألا. ماعلا ليمعلا/IP  
هسفن لا لمعتسي EndHost نأ نألا، امهم. هب صاخلا ريظن ىل ريظن لاصتا تاراشا لاسرا  
ةباجتسالا يف دوزي ءانيم/ip ماعلا ىل طبترم نوكي نأ ضررتفن انوعد) صاخ ءانيم/ناونع  
لثامتم تلمعتسا نإ فلتخم ءانيم نأ ريغ ip هسفن لا ىل وه مجرتي nat لا (STUN  
ذفنملا ىل اذانتسا لاصتالا تاشنأ تاراشالا نأ UDP لاصتا عطق ىل اذه يدؤي. ذيفنت nat  
قباسلا.

نم، كذل. ايضارتفا لثامتم برض زجني وه امدنع ذيفنت nat ديخت جاحسم © cisco ios  
NAT. يدؤت يتلا تاهجوملا هذه عم UDP لاصتا لكاشم ىرت نأ عقوتملا

لسري امدنع. لثامتم سيل برض زجني امدنع ذيفنت nat ديخت جاحسم cisco IOS-XE لا، امهم  
ردصملا، فلتخم ةياغ ىل نأ ريغ ذفنم و IP ردصم هسفن لا عم فلتخم رايت نانثا ت نأ  
ذفنم و IP لماش لخاد هسفن لا ىل NATs لصحي.

## ةلأسملا ل

لقتسم تزجنا ت نأ نإ تللح تنك عيطتسي ةلكشملا نأ حضاولا نم نوكي، فصولا اذه نم  
نبيعت.

مادختسا ديعة NAT نإف، (EIM) ةياهن ةطقن نع لقتسم طبيطخت عم: RFC 4787 ل اقبط  
ناونع يا ىل (X:x) يلخاد ذفنم و IP ناونع سفن نم ةلسرمل ةيلاتلا مزحلل ذفنملا طبيطخت  
يجراخ ذفنم و IP.

نم EIM: ت نأ لمعتسي نإ nat تامجرت جئاتن انه، ةذفان فلتخم ةيفرط ةطحم نانثا ىلع، 5000  
nc -p 23456 10.0.0.4 4000 و nc -p 23456 10.0.0.5

```
Pro Inside global      Inside local           Outside local         Outside global
tcp 10.0.0.1:23456     192.168.0.2:23456    10.0.0.4:40000      10.0.0.4:40000
```

tcp 10.0.0.1:23456 192.168.0.2:23456 10.0.0.5:50000 10.0.0.5:50000

ناونع ردصم هسفن لاي قولي تي نأ قفدي رورم ةكرح فل تخم نأ تي أري عطتسي تنأ انه ناونع/ءانيم ةياغل regardless of ءانيم/ناونع هسفن لاي لاي تمجرت لصحي ذفنمو

مادختساب ةياهن لاي ةطقن لاي عمجمل لاي ذفنم لاي صي صخت ني كمت كنكمي Cisco IOS، تاهجوم لاي ع ip nat service enable-sym-port. رم لاي

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr\\_nat/configuration/15-mt/nat-15-mt-book/iadnat-fpg-port-alloc.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-fpg-port-alloc.html)

## صخلم

ناونع رسي تنأ لمعتسي ام دنع يضا رتفا لكشب لثامتم Cisco IOS NAT ذيفنت نوكي لدان بلطتي نأ رورم ةكرح p2p udp رمي وه ام دنع رادصا تبتسي عي عطتسي وهو (برض) ةمجرت لاي لاي اذه لاي NAT زاهج لاي عي رص لكشب EIM نيوكت لاي لاي جاتحت. nat رورم لاي STUN لثم

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت 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 ه ذ ه 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