

اهجالات و TCP عاطخأ فاشكتسأ

تايوت حمل

قم دقمل

قيس اسأل تابلطت مل

تابلطت مل

قم دختس مل تانوك مل

قيس اسأل تامول عم

TCP وه ام

قيس يئر دئ او ف ثالث

TCP/IP ني م صت يل ع قماع قرظن

(IEEE 802.3) ت نرثي اسأر

IP (IPv4) سأر

TCP سأر قينب

(10 ةكرت شمل) TCP تاراخي

(SYN/FIN كل ذي ف ام) همال عاو TCP لس لس ست كولس

(عيرس ل TCP حت ف) تاناي بل عم SYN: 1 لاثم

(لاص تال اعاهنا) تاناي بل عم FIN: 2 لاثم

MTU ب متق العو MSS

قيتال ل TCP ء ف اصم ي ف MSS ضوافت لمع قيفي

ي هات MSS: جات فمل ا قءاق

قم هول MSS نم رثكأ TCP ء لومح رقص مل لس ري نأ نكمي

اهلج و تالك شمل فاشكتس ال قيلم ع قير

(ق ف دتل ي ف مكحت ل) ء ذف ان ل ا م ح

Cisco Nexus 9000 (NX-OS) يل ع اهجال ص او TCP تاناي ب يوت سم عاطخأ فاشكتسأ

(لوص ول ا قين الكما) يل ول ا ق قحت ل

(تاو ج اول) رور مل ا ء كرح راس م في رعت

(Nexus 9300 ء باجس سا ي ق م) ELAM ني وكت

ع جمل

قم ج اول ا يوت سم ء حص نم ق قحت ل

ARP بارقت سا و هي و ت ل

قيزك رمل ا ء جلا عمل ا ء ج و ل ا اهم ا ق ت ن ا م تي مل رور مل ا ء كرح نم ق قحت ل

مزجل ا هي جوت ء داع ل لوص و نمز دي دحت

(تاناي بل ا يوت سم ل ء مزجل ا طاق ت ل) قي زك رمل ا ء جلا عمل ا ء ج و ل ا ني ت ماعد ني ب ء حس ف

مكحت ل ا يوت سم ل دعم دي دحت ء حص نم ق قحت ل

TCP ل ب ق ICMP ل ا ء دن ت س مل ا ء حص ل ا نم ق قحت ل

قمزجل ا طاق ت ل ا م ادخت سا ب Nexus لومح هي جوت ء داع ل لوص و نمز دي دحت

ع جمل

رخص مل ا في ض مل ا ء مزح طاق ت ل ا نم TCP رورم ء كرح ل ل لحت

قيتال ل TCP ء ف اصم ل ل لحت

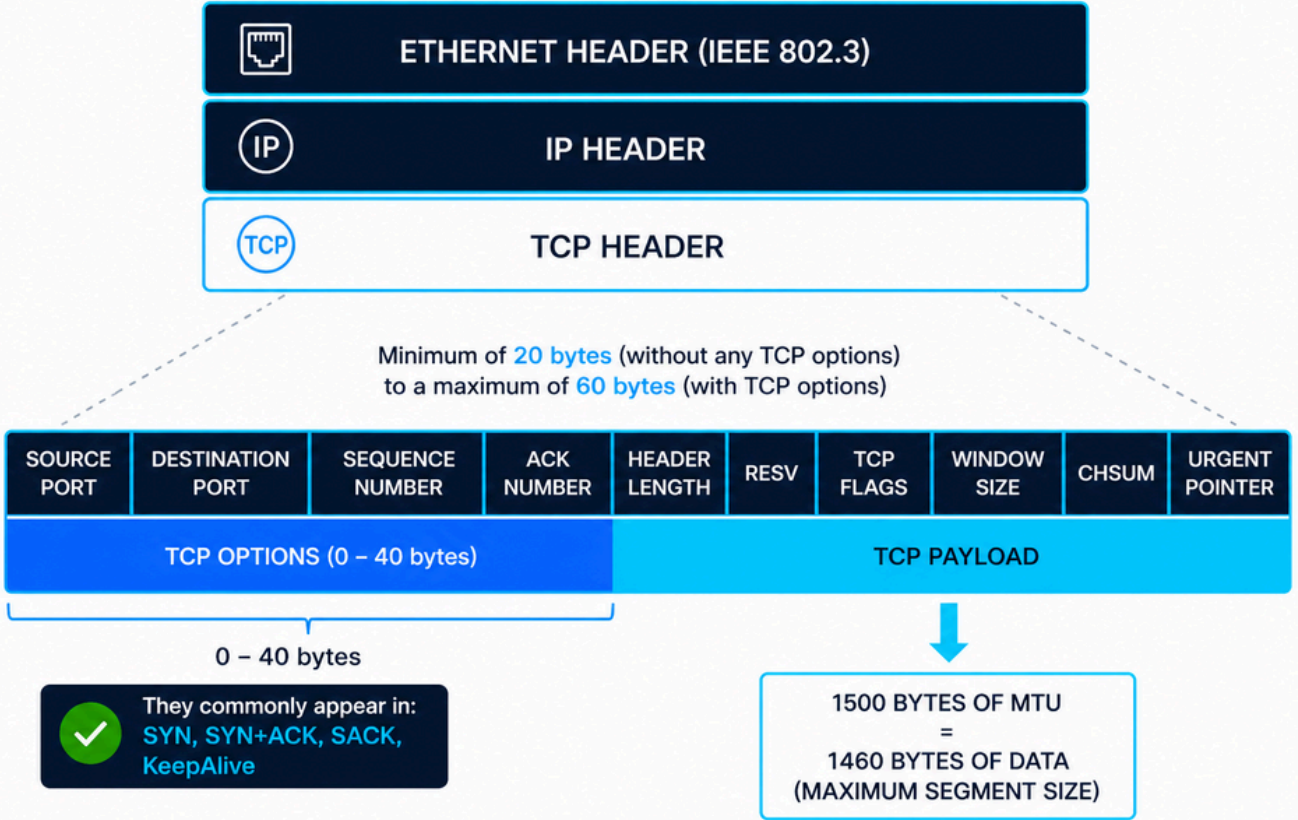
رور مل ا ء كرح دي دحت

(IRTT) اباي او اباه ذرف س ل ل يل ول ا ت ق ول ا ل ل لحت

TCP ذف نم يل ع فر ع ت ل

TCP ء ذف ان م ح ل ل لحت

TCP/IP PROTOCOL STACK



تنتري إيس آر (IEEE 802.3)

نم نوكتيو، تي اب 14 ءءال ي ف تنتري إيس آر نوكي:

- (تي اب 6) ناوع MAC ءي اء
- (تي اب 6) رءصم ال MAC ناوع
- (تي اب 2) لوط ال/EtherType

(FCS) تاراط ال نم ققءء ال لسلسءل ءروطقم تنتري إيس آر تاراط نمضءء، ءءذ ال ءفاض إيس آر ال ءوءءء يء ال تاراط ال IEEE 802.3 ءءءي 2. ءءبء ال ي ف ءاطء ال نع فءءءل ال تي اب 4 ءءس ال ءءابم لءءءب ءءءء ال ءءءء ال مءلءءء ال ءوئي قو مءءء ال ءصق ال/ءنء ال ءء ال TCP. لءم ال ءءبء ال ءالوكوءرب

ءءس آر IP (IPv4)

ءء اب 60 ءءء ءءءءءء نم ءءي، ءء اب 20 ءءبء مءءءل ءنءء ءء ال IPv4 ءءس آر ءوءءءي ءءل ءء ءءسءءءل لوءءء نمضءء. تاراط ال مءءءءء

- هه جولاو ردصم ال IP نيوانع
- (TTL) ءاقبلا ءدم
- (ءلومحك TCP ددحي) لوكوتوربلا

نمضت ال اهنكلو ، تاكبشلا ربع ءي قطنملا ءنونعل او هي جوتلا نع ءلوؤسم IP ءقبط دعت ءي قووثوملا

TCP سار ءينب

يلي ام ءيسيئرلا لوقحلا نمضتت . تاراخيلا بسح تياب 60 ىلا 20 نم TCP سارحوارتي

- هه جولاو/ردصملا ذفانم
- يلسلست مقرر
- رارقالا مقرر
- (كلذ ىلا امو RST و FIN و ACK و SYN) مالءالا
- ءذفانلا مچح
- يرابتخالا ءومجمل

قفذتلا ي ف م كحتلا و ا و ح ي ح ص ل س ل س ت و ء ق و و ت م م ي ل س ت ء ي ن ا ك م TCP لوكوتورب فيضي IP. تالاصتلا ىلا

(10 ءكرتشملا) TCP تاراخي

ام اعويش رومالا رثكأ نمو . يساسالا لوكوتوربلا ءيسوت ىلع TCP لوكوتورب تاراخي لمعت يلي:

1. اهلوبق فيضم لل نكمي TCP ءلومح ربكأ ددحي - (MSS) عطقملا مچحل ىصقألا دحلا
2. تياب 65535 زواجتي ام ىلا لابقتسالا ءذفان ددمي - ءذفانلا سايقم
3. يئاقتنالا رارقالا ءينانكم | ني كمت - (SACK ب حامسالا) يئاقتنالا راعشالاب حامسالا
4. ءءاعا تاي لمع بنجتل ءم لتسملا تانايبلا لتك ددحي - (SACK) يئاقتنالا رارقالا لمالكلا لاسرالا
5. ءفوفلملا لسالسا ماقرا نم ءي امحلاو RTT باسحل مدختست - ءينمزلا ءباوطلا (PAWS).
6. تاراخيلا ءءاحمل وشحلا - (NOP) ليغشتلا مدع
7. TCP تاراخي ءي اهن ددحي - (EOL) تاراخيلا ءمئاق ءي اهن
8. ءي لوالا ءحفاصملا ءانثا تانايبلا لءاب تب حمسي - (TFO) ءيرسلا TCP حتف
9. ءءءتم ءكبش تاراسم ني كمت ىلع لمعي - (MPTCP) تاراسملا دءتم TCP لوكوتورب ءءحاو TCP لمع ءسلجل
10. ءي لظت نا نكمي يتلا ءدملا ي ف م كحتي - (UTO) مدختسملا ءلهم ءاهتنا راخي ءفورعم ريغ ءل سرمل تانايبلا

SYN/FIN (بمب) هملعإو TCP لسلسلست كولس

لمعي .ةلومح دوجو مدع ةلاح يف ىتح ،دحاو لسلسلست مقر SYN و FIN ىتمالع نم لك كلهتست تامالعو - تياب لك لاسرا متي شيح ،تيابلل هجوم لسلسلست جذومن مادختساب TCP لوكوتورب يف قيقدل TCP ليلحتل ىرورض كولسلا اذه .لسلسلستلا ةحاسم ريوطتل - ةددحم مكحت رارقإل قسانت مدع تالاح وأ تالسلستلا صيخشتو مزحلا تاعومحم

$$ACK = SEQ + \text{ةلومحلا لوط} + (SYN \text{ ؟ } 1: 0) + (FIN \text{ ؟ } 1: 0)$$

شيح:

- يلوألا يلسلسلستلا مقرلا SEQ =
- تيابلل تانايبلا محح = ةلومحلا لوط
- 0 ال او ،SYN ةمالع نييعت مت اذا 1 ةفاضل = 1: 0 ؟ نيس
- 0 ال او ،ةنيعم FIN ةمالع تناك اذا 1 فيضي = 1: 0 ؟ ةفنعر
- يلاتلا عقوتملا تيابلل ACK =

(عيرسلا TCP حتف) تانايبلا عم SYN 1: لاثم

- ع م = 1000
- SYN = 1
- تياب 200 = ةلومحلا لوط

ACK باسح:

$$ACK = 1000 + 200 + 1 + 0 = 1201$$

نم لك كلهتست .TCP ةحفاصم ءانثأ تانايبلا لاسرا متي شيح ويرانيس اذه سكعيو لسلسلست ةحاسم SYN ةمالعو ةلومحلا

(لاصلالا ءاهن) تانايبلا عم FIN 2: لاثم

- ع م = 3000
- ةفنعر = 1
- تياب 150 = ةلومحلا لوط

ACK باسح:

$$ACK = 3000 + 150 + 0 + 1 = 3151 \quad \bullet$$

ةلومحلل نم لك نأو، لاصتالاضفخ ءانثأ تانايابل TCP نمضتي نأ نكمي هنأ حضوي اذهو
لسلسلالمقرر نم ديزت FIN ةمالعو

MTU ب هتقالعو MSS

اهلسرل TCP ل نكمي يتل ةلومحلل لىصقألدحل (MSS) عطقمالمحلل لىصقألدحل ددحي
عطقم ي ف

- تياب 1500 = ةيجذومنل تنرثي ةكبشل (MTU) لقنلل لىصقألدحل ةدحو
- $MSS = MTU - IP\ Header - TCP\ Header$
- (1500 - 20 - 20) تياب 1460 = لىصقألدحل MSS

ءانثأ MSS لىلع ضوافتل متي . كلذل اقفو MSS ضفخ متي ، ةدوجوم TCP تاراخي تناك اذا
IP ةقبط ي ف ةئزجتال عنمو ةيثالثل TCP ةحفاصم

ةيثالثل TCP ةحفاصم ي ف MSS ضوافت لمع ةي فيك

رايخ مادختساب ةيثالثل TCP ةحفاصم ءانثأ (MSS) عطقمالمحلل لىصقألدحل لدابت متي
syn مزح ي ف MSS

- (1460، لاثمالمليبس لىلع) هب صاخل MSS نعالعإل: B (SYN) فيضملا → A فيضملا
- (1380، لاثمالمليبس لىلع) هب صاخل MSS نعالعإل: B (SYN-ACK) فيضملا → A

ةيلاعفب لوقي فرط لكو

ةلوبقم TCP ةلومح ربكأ هذو

يهاجتأ MSS: حاتفملا ةدعاق

اهي لىلع قفتم ةدحاو ةمي قك ايئي ب ةميسللسلا ةرادإل ماظن لىلع ضوافتل متي ال

كلذل نم الدب

- رخأل بانجال لبق نم هنع نلعمل MSS فيضم لك مدختسي
- هاجتأ لك ي ف دحاو، نيلقتسم ني دودح قلخي نأ هنأش نم اذهو

كذلك:

- MSS B. ماديخ تساب تانايب ال A لسري
- MSS J A. ماديخ تساب تانايب ال B لسري

هوجلو MSS نم رثكأ TCP ةلومح رصم ال لسري نأ نكمي

م: جيحص لكشب لمعي TCP سدكم ي ف

- م. ملتسم ال لبق نم نلعم ال MSS مارتح لسرم ال يلع بجي
- ةرطاخم ال ال ربكأ تاعاطق لاسرا يدوي دق
 - (MTU زواجت ةلاح ي ف) IP ةئزجت
 - (مومدم ريغ وأ ةئزجت ال رطح م اذا) ةمزح ال طاقس ا تاي لمع
- ال يدوي اذهو
 - لاسر ال ةداع ا تاي لمع
 - ءادل ا ضافخ نا
 - (MTU فاشتك ا راسم) PMTUD ل ءادوس ال بوقث ال لثم تال كشم

اهلحو تال كشم ال فاشكتسال ةيلمع ةيؤر

- (SYN/SYN-ACK مزح) هاجت ال ةيثالث TCP ةحفاصم ي ف MSS ميق نم امئاد ققحت
- ن: ةجتان ال تاقباط ال مدع نم ققحت ال
 - (VXLAN، GRE، IPsec) قافنأ
 - (MSS ربع شيشو ال) MSS لدعت ي تل ةيامح ال نارح
- عنم ل MSS طبض ماديخ تساب م تي ام ابلاغ، Cisco، نم NX-OS لثم ةيساس ال ةمظن ال يلع ةجمدم ال تاراسم ال ربع ةئزجت ال

(ق فدل ي ف مكحت ال) ةذفان ال مجح

م. الع ا نود لبق تسم ال اهل بقي نأ نكمي ي تل تانايب ال مجح "ةذفان ال مجح" ددحي

وه ام:

- تقوؤم ال ني زخت ال ةعس زواجت عنم ل ق فدل ي ف مكحت ال ةيلأ

دصق ال:

- م. ملتسم ال كابر اب لسرم ال ماي ق مدع نمضي

اهيلع لصحت نيا نم

- (Wireshark، لاثملا لىبس ىلع) طاقتلال مزح ي في ئرم
- تقوؤملا نزخملا مجحو وليغشتلا ماظنل TCP سدكم نيوكت نم قتشم

ليغشتلا ماظن/دروملا ريغتم

- سايقلا مدختست (Cisco نم Linux، Windows، NX-OS) ةفلتخم ذي فننت تاي لمع
- ةذفانلل ةفلتخم ماجحأ ىلإ يدؤي امم، تقوؤملا طبضلاو يكي مانيدلا

ةيرفصلا ةذفانلا طرش

- ائلتمم لابققتسالا زاهج تقوؤملا نزخملا نوكي، $0 =$ ةذفانلا مجح نوكي ام دنع
- ةيرودلا تافشكتسملا لاسراو اتقوؤم لاسرالا فاقيا بسرملا موقيا

ةريغتملا Windows تايلا

- لدعمل ىلإ دنتسملا قفدتلا في مكحتلا
 - عيزوتلا كلذ تانايبلا زواجتت الأ نمضيو تباث تانايب لدعمل لسرملل نيغي وهو ادبأ
 - قفدتملا تاقيبطتلا ليغشتلا يلاثم
 - ددعتملا ثبلاو ثبلا ليصوت
- ةذفانلا ىلإ دنتسملا قفدتلا في مكحتلا
 - تقولا رورم عم ةذفانلا مجح فلتخي
 - حومسملا راطالا ىلإ ةراش لاسرالا لالخ نم قفدتلا في مكحتلا ملتسملا ققحي لسرمللا ةذفان تاتيدحتل هب

مادختسالا احوالصا واطخال فاشكتسا

- ةيزكرملا ةجلاعمل (دحو) Windows في مدع نم وأ ريغص لابققتسملا بناج → ةجاجز قنع (قيبطتلاو ةركاذلاو)
- لوصولا نمز) ةكبشلا تالكشم → ةضفخنم ةجلاعمل ةعس تاذ نكلو ةريكبكل ذفانلا (ماجدزلاو)
- TCP لمع تاسلج في ءادألا لكاشم صيخشتل ةيمهألا غلاب رمأ ةذفانلا كولس ليحت

Cisco ىلع احوالصا و TCP تانايب وتسم ااطخأ فاشكتسا
Nexus 9000 (NX-OS)

NX-OS ليغشي يذلا Cisco Nexus لوحم ناك اذا ام صيخشتل ةيلمع ةيجهنم مسقلا اذه فصلي

لإلخ نم جهنلا اذه ضرع متي و. عادألا يف لكاشم مدقي وأ TCP رورم ةكرح هيحوت ةداعإ يلع رثؤي
يفضارتفا ويرانيس

نأ يف هابتشالا ةيفادبلا يف عئاشلا نم، عادألا ضافخنا وأ TCP لوصو نمز ةظحالم دنع
لئلحتلا لإلخ نم ضارتفالا اذه ةحص نم ققحتلا بجي، كلذ عمو. كلذ يف ببستت ةكبشلا
طاقتلا يه اهحالصإو TCP اطاخأ فاشكتسال ةلوخمال ةقيرطلا. تانايبلا لإل دنس يذل
يفلاثم لكشب اهذيفنت متي و، مزحلا

- ةهجول او رصملا يف دحاو تقوي
- رورملا ةكرح ادب لبق

لوح ضوافتلا متي شح، ةيثالثلا TCP ةحفاصم ةيلمع يف ةيفورلا ةيناكمإ نمضي اذهو
نم قحال تقوي يف اهراركت متي ال و SAACK و Window Scale و MSS لثم ةيفويحلا تاملعمل
لإلخ نم لئلحتلا اارجإ نكمي، ةنمازتملا روصلا طاقنتلا نكمملا نم نكي مل اذإ. ةسلحلا
ةدودحم جئاتنلا نكلو، دحاو طاقنتلا

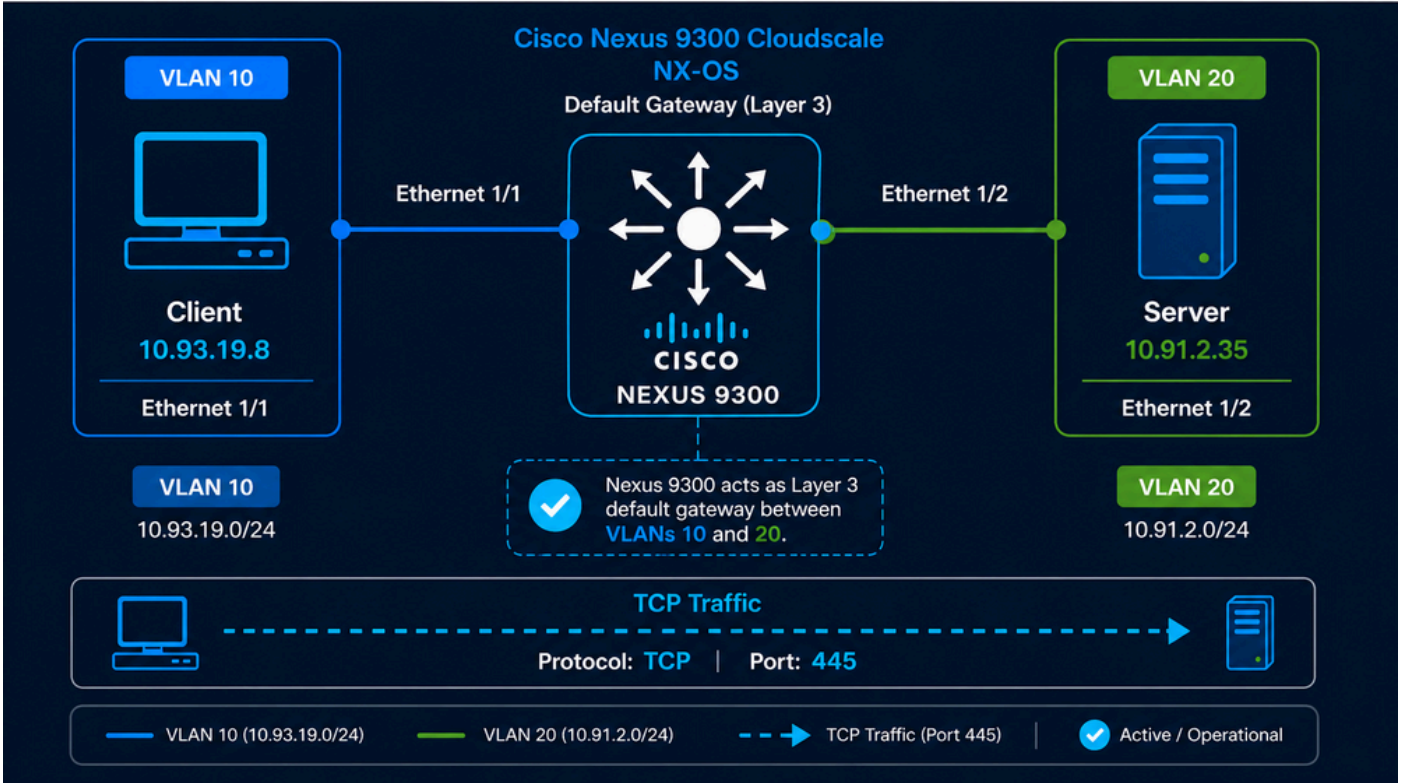
ويرانيسلا فيرعت

تاقيبطتلا تانايب ةومجمل يطايتحالا خسنلا ةيلمع نأ ديدحتب ني مدختسملا دحأ ماق
تاعاس 9 نوضغ يف اقباس اهلامكإ مت يتل او، ابيرقت تي اباريت 7.5 اهت عس غلبت يتل
لمع تاسلج عاشنإ متي لازي ال هنأ نم مغرلا يلع. ةعاس 21 يلاوح نألا قرغتست، ابيرقت
لإل ريشت يطايتحالا خسنلا ةدم يف ةريكبلا ةدايزلا نألا، حاجنب مداخل او لي عمل ني ب TCP
زاهج وه Nexus لوحم نأل ارظنو. يلامجإل TCP عادأ وأ ةجلعمل ةعس يف لمحتحم ضافخنا شودح
ةكبشلا لوؤسم كشي ف، 3 ةقبطلا ةرابع ةفيظو اضيأ رفوي و راسملا يف دحولا ةكبشلا
ةلكشملا ببس وه Nexus لوحم نأ يف

- 10.93.19.8 (VLAN 10) لي عمل
- 10.91.2.35 (VLAN ةكبش) مداخل
- ةيفضارتفا ةبوابك Nexus 9300 لمعي
- 445 مقرر TCP ذفنم

TCP Traffic Flow (Port 445)

Client to Server



(لوصول اةيناك م) ي ل و ا ل ا ق ق ح ت ل ا

- ن ع هة ج و ل و ا و ر د ص م ل ا ن ي ب (PMTU) م T U ر ا س م هة ح ص ن م ق ق ح ت ل ل ر م ا و ا ل ا ه ذ ه م ا د خ ت س ا م ت ي د ي د ح ت ي ف ل ك ل ذ د ع ا س ي . (DF) هة ئ ن ج ت م د ع ت ب هة و م ح م م ا د خ ت س ا ب I C M P م ز ح ل ا س ر ا ق ي ر ط ه ذ ه ذ ي ف ن ت ب ج ي . هة ئ ن ج ت ن و د ب هة ك ب ش ل ا ز ا ت ج ت ن ا ن ك م ي ي ت ل ا هة م ز ح ل ا م ج ح ل ي ص ق ا ل ا د ح ل ا هة ج و ل و ا و ر د ص م ل ا ن م ل ك ي ل ع هة ي ل م ع ل ا .
- ر د ص م ل ا ن م ل ك ي ل ع هة ي د ا م ل ا هة ج ا و ل ل (MTU) ل ق ن ل ل ي ص ق ا ل ا د ح ل ا هة و ن م ا م ا د ق ق ح ت هة ج و ل و ا .
- هة و د ي د ح ت م ت ش ي ح ، ر د ص م ل ا ف ي ض م ل ا ي ل ا ط ق ف ل و ص و ل ا ن ك م ي ، و ي ر ا ن ي س ل ا ا ذ ه ي ف 1500 غ ل ب ت (MTU) ل ق ن ل ل ي ص ق ا ل ا د ح ل ا .

Linux: ping -c 10 -I 10.93.19.8 -s 1472 -M do 10.91.2.35

- I C M P ي د ص ل ت ا ب ل ط 10 ل س ر ي → -c 10
- هة ج ا و ل / I P ل و ك و ت و ر ب ل د د ح م ل ا ر د ص م ل ا ا ذ ه م د خ ت س ي → 192.168.10.10 -I
- ت ي ا ب 1472 ي ل ا I C M P هة ل و م ح م ج ح ن ي ي ع ت ي ل ع 1472 ز ا ر ط ل ا → لم ع ي -
- (ؤ ن ج ت ا ل) D F ت ب هة و ط ب ض ي →
- هة ج و ل ل I P → 192.168.20.20

Windows: ping -n 10 -l 1472 -f 10.91.2.35

- ICMP يوصل تا بلط 10 لسري $-n 10$
- تياب 1472 لى ICMP ةلومح مچح نييعة لىع 1472 زارطلال \rightarrow لمعي-
- (DF) ةئزجتال مدع ةمالع طبضي $-f$
- ةهوجلل IP $\rightarrow 192.168.20.20$

تياب 1472 اذامل

- تياب 1472 ICMP ةلومح
- تياب 20 IP ناووع
- تياب 8 ICMP سار
- (MTU) لقنلل لىصقألا دحلا ةدحو) تياب 1500 = 1472 + 20 + 8 : ةمزحلال مچح لىلامچا (ةيسايقلال)
- نودب تياب 1500 تاذ (MTU) لقنلل لىصقألا دحلا ةدحو معدى راسملا ناك اذا ام رابتخا اذه نال لاصتال رابتخا لشف نكمي، ICMP ةلومح نم تياب 1500 لاسر تلوواح اذا. ةئزجت ICMP و IP سوؤرة فاضا دعب يسايقلال MTU زواجتي دق ةمزحلال مچح لىلامچا

هجاتنتسا نكمي ام

- لقنلل لىصقألا دحلا ةدحو راسملا معدى، (ةمزح نادقف نودب) لاصتال رابتخا حجن اذا. ةئزجت دوجو مزلي الولىقألا لىع تياب 1500 ةعسب (MTU)
 - TCP لىلحتل ةفيظنلل ICMP جئاتن ةعباتم \rightarrow
 - لدعمل ديح و رباع ماحدزا و مزحلال لمتم دقف \rightarrow عطقتم لاصتال رابتخا حاجن TCP لوكتورب نال ارظن، ةمزحلال نادقف لىلحت لىلقتنا؛ هيجوت ةداعا ةلكشم و ةءافكب لمعمل ةراسخالا نم اىلاخ اراسم بلطتي
- طابترا كانه، جورخال تاقوا و "ةبولطملا ةئزجتال" أطخ ثودح عم لاصتال رابتخا لشف اذا ةداعا نكمي ال، تياب 1500 نم لىقأ (MTU) لقنلل لىصقألا دحلا تادحو عم راسملا لىف لىصقألا دحلا ةدحو لىف ةلكشم دوجو لىل ريشي اذه و، DF تب ةدحو ببسب ةمزحلال هيجوت راسم لل (MTU) لقنلل

اهالصل وءاطخألا فاشكتسال رمالا اذه مادختسا لىفك

- ديححتل (1300 \rightarrow 1400 \rightarrow 1472، لالملا لىبس لىع) ايجيردت ةلومحلال مچح لىفختب مق حجني مچح ربكأ
- MTU = ةغىصلال مادختسا ب (MTU) لقنلل لىصقألا دحلا ةدحو باسحب مق، اهديححت درجمبو (IP + ICMP) سوؤر) تياب 28 + ةلومحلال

TCP ب ةيلمع ةلص

رابع عة جرم ل او م د ق م ل ا ت ا ن ا ي ب ل ا ر و ر م ة ك ر ح ل ن ك م ي ، ك ل ذ ل ة ج ي ت ن و . ة د د ع ت م ت ا ر ا س م ر ب ع ن م ل و ح م ل ك ي ل ع E L A M ذ ي ف ن ت ب ج ي ، ت ا ه و ي ر ا ن ي س ل ل ه ذ ه ي ف . ة ف ل ت خ م ت ا ه ج ا و ا ت ا ل و ح م . ة ل م ا ك ل ل ة ي ؤ ر ل ل ا ن ا م ص ل ل ة ل ص ل ل ا ت ا ذ N e x u s ت ا ل و ح م

ء ا ط خ أ ل ا ف ا ش ك ت س أ ق ا ط ن ل ي ل ق ت م ت ي ، ح ي ح ص ل ك ش ب ج و ر خ ل ل ا و ل و خ د ل ل ا ت ا ه ج ا و ا د ي د ح ت ل ل ا ل خ ن م ة م د خ ل ل ة د و ج ت ا س ا ي س و ة ه ج ا و ل ل ا ت ا د ا د ع ن م ز ك ر م ل ل ق ق ح ت ل ل ا ح ي ت ي ا م م ، ر ي ب ك ل ك ش ب ا ه ا ل ص ا و ه ي ج و ت ل ل ة د ا ع ا ر ا س م ي ل ع ة ل م ت ح م ل ل ا م ا ح د ز ا ل ل ط ا ق ن و (M T U) ل ق ن ل ل ي ص ق أ ل ل د ح ل ل ة د ح و ت ا د ا د ع ا و ق ي ق د ل ل

(Nexus 9300 ة ب ا ح س س ا ي ق م) E L A M ن ي و ك ت

، IP 10.91.2.35 ة ه ج و و ، IP 10.93.19.8 ر د ص م م ا د خ ت س ا ب ر و ر م ل ا ة ك ر ح ة ي ف ص ت ب ل ا ث م ل ا ا ذ ه م و ق ي TCP 445 ة ه ج و ذ ف ن م و

ELAM د ا د ع ا

<#root>

switch#

debug platform internal tah elam

switch(TAH-elam)#

trigger init

Slot 1: param values: start asic 0, start slice 0, lu-a2d 1, in-select 6, out-select 0
switch(TAH-elam-inse16)#

set outer ipv4 src_ip 10.93.19.8

switch(TAH-elam-inse16)#

set outer ipv4 dst_ip 10.91.2.35

switch(TAH-elam-inse16)#

set outer 14 14-type 0

switch(TAH-elam-inse16)#

set outer 14 dst-port 445

```
switch(TAH-elam-insel6)#
```

```
start
```

ةجيتننللا درتسا ،رورملا ةكرح ءاشنإ دعب

```
<#root>
```

```
switch(TAH-elam-insel6)#
```

```
report
```

(ةلماكلا ةيؤرلا ةينامال يمازلا) ةيسكعل رورملا ةكرح طاقتلا

ةهوجللا و ردصم لل IP نيوانع لي دبت قيرط نع نيوكتلا ررك ،عاجرالا راسم ةحص نم ققحتلل

```
<#root>
```

```
switch#
```

```
debug platform internal tah elam
```

```
switch(TAH-elam)# trigger init
```

```
Slot 1: param values: start asic 0, start slice 0, lu-a2d 1, in-select 6, out-select 0
```

```
switch(TAH-elam-insel6)#
```

```
set outer ipv4 dst_ip 10.93.19.8
```

```
switch(TAH-elam-insel6)#
```

```
set outer ipv4 src_ip 10.91.2.35
```

```
switch(TAH-elam-insel6)#
```

```
set outer 14 14-type 0
```

```
switch(TAH-elam-insel6)#
```

```
set outer 14 dst-port 445
```

switch(TAH-elam-inse16)#

start

ةيتاي لمع تاظحالم

- ادب دنع طشن لكشب رورملا ةكرح قفدت نم دكأت كلذل ،طقف ةدحاو ةمزح ELAM طقتلي رسأل
- .ةطبترملا ريغ رورملا ةكرح طاقتلا بنجتل ةقيد ةيفصتلا لماع نوكت نأ بجي
- نأ نكمي رورملا ةكرح نأل ارظن نيولوجملا الك ىلع ELAM ليغشتب مق ،vPC تائيب يف هاجتلا ل يف فلتخم لكشب كباشتت
- يف ةلوخم ةيؤر دوزي ،زاهج يف رارق هيحوت ةداعاو ،نراق جرخم ،لخدم نراق ضرع جاتنإلا .تانايبلل ىوتسم

عجرملا

[Cisco Nexus 9000 ةباحسلا سايقمب صاخلا ASIC ELAM ليلى](#)

ةهجالل ىوتسم ةحص نم ققحتلا

رثؤت ذودش وأ دويقي لأ لاخداب Nexus لوجم مايق مدع ةهجالل ىوتسم ةحص نم ققحتلا نمضي ةزهجالل تادادعو ليغشتلا ةلاحو نيوكتلا نأ ديكأت ىلع زيكرتلا متي و TCP رورم ةكرح ىلع .ءادلل يلاع تانايبلل ىوتسم هيحوت ةداعال عقوتملا كولسلا عم قفاوتت

نيوكتلا ةحص نم ققحتلا

- :تاهجالل ىلع ةيديقت (ACL) لوصولل يف مكحت مئوق ياً قيبطت مدع نم ققحت

<#root>

switch#

```
show running-config interface ethernet1/1-2 | include access-group
```

- رورم ةكرح ىلع ةدوصقملا ريغ ةمدخلال ةدوجل تاسايس ياً ريثأت مدع نم ققحتلا مئوق كلذ يف امب ،يملالال ىوتسملا ىلعو ةهجالل ىوتسم ىلع ةمدخلال ةدوج) تانايبلل

(لأشكال ليش وتأساس لعض وراظتنال):

<#root>

switch#

show running-config interface ethernet1/1-2 | include service-policy

switch#

show policy-map interface ethernet1/1-2

<#root>

switch#

show policy-map

<#root>

switch#

show class-map

<#root>

switch#

show class-map type network-qos

<#root>

switch#

show policy-map type network-qos

<#root>

switch#

show policy-map system type network-qos

<#root>

switch#

show queuing interface ethernet1/1-2

<#root>

switch#

show policy-map type queuing

- كل ذي فامب (ةهجوم لةهاول لباقم switchport) 3 ةقب طلال وأ 2 ةقب طلال نيوك تديكات
IP: ةنونعو (STP) ةعرفتم لةرشل لوكوتورب ةلأحو VLAN ةكبش ةيوضع

<#root>

switch#

show running-config interface ethernet1/1-2

<#root>

switch#

show interface ethernet1/1-2 switchport

<#root>

switch#

```
show spanning-tree interface ethernet1/1-2
```

<#root>

switch#

```
show ip interface ethernet1/1-2
```

ليغش التلا ة لاج نم ققحت ل

- نيوكت ل اهتق باطم نم دكأتو (MTU) لقن ل لصقأ ل دح ل ة دحو قسانت نم ققحت (تيا ب 9000 وأ 1500، لاثم ل ليبس يلع) ع قوتم ل

<#root>

switch#

```
show interface ethernet1/1-2 | include MTU
```

- هاجت إ ل يئانث ل اسر ل ا تاداع إ و ة هج اول ة عرس دي كأت

<#root>

switch#

```
show interface ethernet1/1-2 | include speed|duplex
```

- (ت اطا ب ترال ل ررك تم ل ا قتنا وأ حاش ترا دجوي ال) ة هج اول رارق تس ل نم ققحت ل

<#root>

switch#

```
show interface ethernet1/1-2 | include rate|flap
```

ءاطخألا دادع ةحص نم ققحتلا

- رابتخالال لبق تادادعالا حسم

<#root>

```
switch#
```

```
clear counters interface all
```

- (طاقف ةيرفص ريغ ميقي) ةبقارملا ءاطخأ تادادع

<#root>

```
switch#
```

```
show interface counters errors non-zero | include Port|Eth1/1|Eth1/2
```

رابتخالال دعب ام ةحص نم ققحتلا

- ىرخأ ةرم تادادعالا بقارو TCP رورم ةكرح رابتخال ليغشت دعأ

<#root>

```
switch#
```

```
show interface counters errors non-zero | include Port|Eth1/1|Eth1/2
```

- وأ 1 ةقبطلاب قلعتت ةلمتحم لكاشم ىلا ةدايزي ريشت؛ تادادعالا ةدايز مدع بجي
ننخمل طاقس/زواجت وأ CRC/FCS ءاطخأ وأ ةيلعفل تاطابت رالال ءاطخأ لثم ةزهجالا
تقؤملا.

ARP رارق تساو هيچوتلا

ةيلباق هيديل Nexus لوحم نأ نم دكأتلل ةيمهألا غلاب ارمأ ARP رارق تساو هيچوتلا نامض دعي
TCP. عادأ ىلع رثؤت نأ نكمي ةعطقتم ل لكاشم مدقي الو 3 ةقبطلال نم ةقسانتم لوصو
ةدايز وأ ةمزحل نادقف ىلا ARP ليلحت وأ هيچوتلا تالخالدا يف رارق تسالال مدع يدؤي نأ نكمي

رورملا ةكرح بّجح وأ لوصولا نمز

ةحصلال نم ققحتلال رييعام

- لكشب ريغتت الو ةرقتسم و ةدوجوم ةهجولاولاو ردملل هيحوتلال تالخدإ نوكت نأ بّجي رركتم
- رمتسم لكشب اهدقف وأ اهثيدحت مدعو ARP تالخدإ لّح بّجي

<#root>

switch#

show ip route 10.93.19.8

<#root>

switch#

show ip route 10.91.2.35

<#root>

switch#

show ip arp detail | include 10.93.19.8

<#root>

switch#

show ip arp detail | include 10.91.2.35

ةيزكرملا ةجلالعملال ةدحو ىلإ اهماقتنا متي مل رورملا ةكرح نم ققحتلال

ةدحو كراشت الو، (ASIC) ةزهجالا يف هيحوتلال ةداعإ ءارجإ متي، Cisco Nexus 9000 تالوحم يف TCP رورم ةكرح ةبقرم نإف، كلذل. ةيداعلال تانايبلا ىوتسم تايلمع يف ةيزكرملا ةجلالعملال مزحلال عيقوت متي هنا ىلإ ريشتو ةيداع ريغ مكحتلال ىوتسم يف فيضملا ىلإ فيضملا نم

ةدحو ةطس اوب رورم لة كرح ةجل اع م درجم ب .ةئطاخ ل اناي وكتل و اءا ان ثت س ال ا ب س ب نكم ي هنا ع قو ت م ل ا ن م و ، م ك ح ت ل ا ي و ت س م م ي ظ ن ت ل ة ع ض ا خ ح ب ص ت ، ة ي ز ك ر م ل ا ة ج ل ا ع م ل ا . ه ب ح و م س م ل ا م ك ح ت ل ا ي و ت س م ل د د م رورم ل ا ة ك ر ح ت ز و ا ج ت ا ذ ا ط و ق س ل ا ت ا ي ل م ع ة ظ ح ا ل م

ةحصل ال نم ققحت ال بولسأ

• رز ل ل ا ن ا ث ي ا ل ا م ا د خ ت س ا ب م ك ح ت ل ا ي و ت س م ي ل ا ل ص ت ي ت ل ا ت ا ن ا ي ب ل ا رورم ة ك ر ح ط ق ت ل ا

<#root>

switch#

```
ethalyzer local interface inband display-filter "ip.addr==10.93.19.8 and ip.addr==10.91.2.35" limit-ca
```

عقو ت م ل ا ك و ل س ل ا

• ي ف ي ف ي ض م ل ا ي ل ا ف ي ض م ل ا ن م TCP ت ا ن ا ي ب ي و ت س م ت ا ن ا ي ب رورم ة ك ر ح ة ظ ح ا ل م ن ك م ي ا ل . ة ي ز ك ر م ل ا ة ج ل ا ع م ل ا ة د ح و

عقو ت م ر ي غ ك و ل س

• ن ا ن ك م ي ي ذ ل و ، رورم ل ا ة ك ر ح ر ا ب ت خ ا م ت ي ه ن ا ف ، ة ي ئ ر م ق ف د ت ل ل ة ق ب ا ط م ل ا م ز ح ل ا ت ن ا ك ا ذ ا ن ع ج ت ن ي

- ل ي ج س ت و (TTL) ء ا ق ب ل ا ة د م ة ي ح ا ل ص ء ا ه ت ن ا) ي ئ ا ن ث ت س ا ل ك ش ب م ز ح ل ا ة ج ل ا ع م
- (ه ي ج و ت ل ا ة د ا ع ا و (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق
- ة م و ع د م ر ي غ ت ا ز ي م و ا ئ ط ا خ ن ي و ك ت
- ة ح ي ح ص ر ي غ ة ز ه ا ة ج م ر ب

م ز ح ل ا ه ي ج و ت ة د ا ع ا ل و ص و ن م ز د ي د ح ت

ة د ا ع ا ع ض و و ة م ز ح ل ا م ج ح ي ل ع Nexus 9000 ت ا ل و ح م ي ف م ز ح ل ا ه ي ج و ت ة د ا ع ا ل ا ق ت ن ا ن م ز د م ت ع ي م ز ح ل ل ل و ص و ل ا ن م ز ي ل ا ي ج ذ و م ن ل ك ش ب Cisco ت ا ف ص ا و م ر ي ش ت . ة ن ك م م ل ا ت ا ز ي م ل ا و ه ي ج و ت ل ا ر ش ا ب م ل ا ه ي ج و ت ل ا ة د ا ع ا ت ح ت ت ي ا ب 64 ت ا ذ

Switch Model	ASIC / Architecture	Ports (example config)	Typical Forwarding Latency (64B packet)
Nexus 93180YC-EX	Cloud Scale (EX)	48x25G + 6x100G	~1.0 - 1.2 microseconds
Nexus 93180YC-FX	Cloud Scale (FX)	48x25G + 6x100G	~0.9 - 1.0 microseconds
Nexus 93180YC-FX2	Cloud Scale (FX2)	48x25G + 6x100G	~0.8 - 0.9 microseconds

Nexus 9364C	Cloud Scale	64x100G	~1.0 microsecond
Nexus 9336C-FX2	Cloud Scale (FX2)	36x100G	~0.8 microseconds
Nexus 93240YC-FX2	Cloud Scale (FX2)	48x25G + 12x100G	~0.8 - 0.9 microseconds
Nexus 92300YC	Broadcom Trident II	48x10/25G + 6x40/100G	~2 - 3 microseconds
Nexus 92160YC-X	Broadcom Tomahawk	48x25G + 6x100G	~2 microseconds

- Nexus 9000 (في ضارثفالا) يلي صفتلا هي جوتلا ةداعإ
 - ةلمالكلا ةمزحلا مالتسا لبق هي جوتلا ةداعإ أدبي
 - ةيناثلا لىل ةيناثلا لىل ةيناثلا نم) ن دألا دل لىل لوصول نمز لىل لقت (ابيرقت)
 - هي جوتلا ةداعإ و نيزختلا
 - هي جوتلا ةداعإ لبق لمالكلا ةمزحلا يقلت بجي
 - ةمزحلا مخرج عم بسانتم لوصول نمز ةفاضإ
- في فاضإ لوصول نمز ةيفاضالا تازيما لرفوت نأ نكمي:

- VXLAN ةلسبك ك/ف/نيمضت
- (ACL) لوصول في مكحتلا ةمئاق في شحبلا تايلمع
- راطتالا مئاقو ةمدخل ةدوج في نصت
- Telemetry (NetFlow, ERSPAN, sFlow)
- ماحذالا ءانثأ تقوؤملا نيزختلا

كلذ عمو

- ةزهجالا بيبانأ طوطخ في تايلمعلا هذه ذيفنت متي

ماحذالا وه ظوالم لكشب لوصول نمز هي في ديزي يذلا ديحولاي عاقولا ويراني سالا نإ:

- جورخال راطتانا مئاق في اتقوؤم مزحلا نيزخت متي
- لىل ريخاتلا فقوتي
 - راطتالا ةمئاق قمع
 - ةهجالا مادختسا
 - ةمدخل ةدوج تاسايس

تالاحلا هذه في تحت

- ةضفخنم ةيناثوركيملا نم تائم لىل ةيناثوركيملا قاطن في ةداع نوكي لوصول نمز
- ةيناث لىل لملا يوتسم لىل رمتسملا ريخاتلا ينعى
 - ديدش ماحذالا
 - كارتشالا طرف
 - نوكملا ريغ تقوؤملا نيزختلا وأ (QoS) ةمدخل ةدوج

تانايايبل يوتسمل ةمزحلل طاقتلل) ةيزكرملا ةجلالعمل ةدحو ىلإ نيتماعد نيبة حسف

اهري دصتو ةمزحلل طاقتلل مكحتلل يوتسم في تانايايبل يوتسم رورم ةكرح خس نحتي اذهو
Wireshark في ليصفتلل ليحتلل اب حمسي امم، pcapng. فلم ىلإ

نيوكتللا

```
monitor session 1
source interface ethernet1/1 both
source interface ethernet1/2 both
destination interface sup-eth0
no shut
```

رسأ ذيفنت

<#root>

switch#

```
ethalyzer local interface inband mirror capture-filter "tcp port 445" limit-capture 0 write bootflash:
```

ةينقت تارابتعا

- ميظنتل (CPU) ةيزكرملا ةجلالعمل ةدحو ىلإ اهسكع متي يتل رورملا ةكرح عرضت (CoPP). مكحتلل يوتسم
- CoPP رورملا ةكرح تزواجت اذإ
 - مكحتلل يوتسم في طوقف مزحلل طاقسإ نكمي
 - ليحتلل اءانثأ ةئطاخ ةيباجي اءائتن روهظ ىلإ اذه يدؤي
- ةكرح تاهوييرانسي ل (CPU) ةيزكرملا ةجلالعمل ةدحو ىلإ نيتماعد نيبة حسف بصوي ةطسوتملا ىلإ ةضفخنملا تانايايبل رورم
- ةيلاعلا ةيجاتنإل تاذ تائيبلل
 - (يجراخ للحم) يلحم نيتماعد نيبة حسف تلمعتسا
 - دعب نع طاقتلل ERSPAN مادختسا

ةقيرط	ةزيملا	ديدحت
ربش	نيمضت نودب، قيقود	ايدام الاصتا بلطتي
ERSPAN	دعب نع طاقتلل اءائتن	ءكبشلا ماحدزال ةضرع

مكححتللا يوتسم لددم ديدحت ةحص نم ققحتللا

يرورضلا نم ، ةيزكرملا ةجلالعملا ةدحو لىل نيتماعد نيب ةحس ف طاقحتلا ةيقووثوم نامضل لدعمللا ديدحت ببسب ةقباطتملا مزحلا طاقسإب موقيا ال مكححتلا يوتسم نأ نم ققحتلا

ةحصلا نم ققحتلا رمأ

```
switch(config)# show hardware rate-limiter | i Allowed|span
Allowed, Dropped & Total: aggregated bytes since last clear counters
      R-L Class      Config Allowed Dropped Total
      span          50          0         0         0 <<<
      span-egress   disabled    0         0         0
```

ةحصلا نم ققحتلا ةيجهنم

- ناوٲ 3 نم اهلقأ ةينمز تارتف لىل رمألا ذيفنتب مق
- طاقسإ نراق لصتم نيتماعد نيب ةحس فل تبقار

لپوات

- نكمي طاقحتلا لىل فص نيتماعد نيب ةحس فل طاقسإلا تاداع ي ف ةدايزي أ ريشت ال هيلع دامتعالا
- لعي امم ، مكححتلا يوتسم ي ف ةمزحلا نادقف لىل طاقسإلا تاداع ي ف ةدايزلا ريشت هب قووثوم ريغ طاقحتلالا

ERSPAN وأ رسجي نأ تريغ تنك يغبني ةقيرط طاقحتلالا ، تارطق ظحول نإ

TCP لبق ICMP لىل ةدنتسملا ةحصلا نم ققحتلا

TCP ليلحت ءارجا لبق تانايبلا يوتسم ةمالس نم ياساسألا ققحتلا ICMP رابتخا روي نع عيرسلا فشك لاب حمسي هنإف ، طسبأو ةلاجال ميديع ICMP لوكو تورب نأل ارطن . دقعمللا راسملا قسانت مدع وأ راركنتلا وأ ةمزحلا نادقف

طاقحتلا نيتماعد نيب ةحس ف ي ف عقوقتم كولس

- نيترم ICMP ةم زح لك رهظت نأ نكمي
 - لوخدلا دنع ةرم
 - جورخلا دنع ةرم
- يسايق لاصتا رابتخا يلغ لوصحلل
 - طبر 2 يدص → بلط
 - مزح 2 → دادترالا در

تانايبلا يوتسم يف ةمزحلا نادقف بايغو ةحيجصللا هيجوتلا ةداعا دكؤي اذهو

ذاش كولس

- يلغ ةلمتحم دويق دوجو يلا ةلثامتملا ريغ مزحلا دادعا وأ ةدوقفملا تاراركتلا ريشت طاقتلالا وأ مزحلا نادقف
- عب بنملا لكاشم وأ امحذالا وأ 1، ةقبطلال لكاشم ةعطقتملا راطتالالا تارتف حرتقت

متي هئاب ريبك لامتحا كانهف، دقف نود قسانتم لكشب ICMP رورم ةكرح هيجوت ةداعا مت اذا 2/3 ةقبطلالا يف حيجصل لكشب TCP رورم ةكرح هيجوت ةداعا اضيا

ةمزحلا طاقتلالا مادختساب Nexus لوجم هيجوت ةداعا لوصو نمز ديدحت

نبي ةحس ف (أو CPU يلا نيتماماد نبي ةحس ف لمعتسي رورم ةكرح ضبق ام دنع ةدحاو ةرمو لخدملا يلغ ةدحاو ةرم: نيترم monitore تنك عيطتسي طبر لك، (ERSPAN/نيتماماد لوجملا هلخدأ يذلا هيجوتلا ةداعا لاقتنا نمز ريديقتل راركتلا اذه مادختسا نكمي. جرحملا يلغ ةمزحلا سفنل نيلايتملا الك نبي تقولا قرف باسح قيرط نع Nexus

اقباس اهطاقتلالا متي تل ICMP رورم ةكرح مادختساب ريخأتلالا اذه سايق نكمي، ايلمع ةدعاق رفوي اذهو. دادترالا يلغ درلا مزحو فعاضملا دادترالا بلط نبي تقولا اتلدة نراقمب نكمي، قمعأ ليلحت ابولطم ناك اذا. لوجملا هيجوت ةداعا اءادال ةلاعفو ةطيسب ةيساسأ تقولا قرف سايقو قفدتلا طاقتلالا لالخم TCP رورم ةكرح يلغ ةيجهنملا سفن قيبطت. ةرركملا TCP مزح نبي

ةيجهنم

- (يلسلسلستلا مقرلا سفن) اهل راركتو ةمزح فيرعت
- جرحملاو لخدملا خسن نبي تقولا اتلدة سايقم
- نأ نكمي هانأل ارظن، لوجملا هيجوت ةداعا لوصو نمزل يولعلال دحل ريديقت اتلدة هذه لثمت ي. نمزلا اهمتخو فيلاكتلا لسكع نمضتت

Wireshark ليكشت

• تقولا اتلدد ضرع نيكمت

View > Time Display Format > Seconds Since Previous Displayed Packet

• تقولا اتلدد صصخم دومع ةفاضإ

Right-click on "Time Delta from Previous Displayed Packet" → Apply as Column

• (لاثم) ةلصللا تاذ رورملا ةكرح ةيفصت

ip.addr==10.93.19.8 and ip.addr==10.91.2.35 and tcp

• TCP قفدت وأيلسلسلستلا مقرلا بسح مزحلا زرف

Right-click packet → Follow → TCP Stream

ليوات

- ةيناثوركيملا قاطن يف ةرركملا مزحلا نيب تقولا اتلدد نوكي نأ نكمي
 - هيجوت ةداعإ لىل لوصولا نمز مدقي ال Nexus لوحم نإف، ةلاحلا يه هذه تناك اذا مزحلا.
- ةزهجالا لىل عمئاقلا هيجوتلا ةداعإ ءادأ ةضفخنملاو ةقستملا تانايبلا دكؤت
- لىل ةقسانتملا ريغ وأ لىل ءالا تاواتلدلا ريشت نأ نكمي
 - تقؤملا نيزختلا وأ ماحذال

عجارملا

- [\(لوصولا نمز تافصاوم\) Cisco Nexus 9000 ةلسلس تانايب قاروأ](#)
- [Cisco Nexus 9000 ةينبلا يمسرلا ريرقتلا](#)
- [تقؤملا نيزختلاو Cisco NX-OS ةمدخ ةدوج كولس](#)

ردصملا فيضملا ةمزح طاقتلا نم TCP رورم ةكرح ليلحت

كلذ في فامب، Wireshark في TCP مزح طاقنتلا لي لحتل ةيلي صفت ةيجهنم مسقلا اذه رفوي روصلا تطقنتلا دقو. اقبس م ةحوضوملا ةيضارتفالا ةلاحلا لالخ نم، فيرعتلا فلم نيوكت وه ويراني سلا ناف، ريكذتلا لابس يلعو. Wireshark عقوم نم ةرشابم تضرع يتلا

تاقبب طنتلا تانايب ةعومجمل يطايتحال خسنلا ةيلمع نأ ديدحتب ني مدختس م لا دحأ ماق تاعاس 9 نوضغ في اقباس اهلامكإ مت يتلاو، ابيرقت تي ابيري 6.5 اهت عس غلبت يتلا وه هيل لوصولا نكمي يذلا ديحول ةكبشلا زاهج. ةعاس 21 يلاوح نألا قرغتست، ابيرقت دحلا ةدحو مجح غلبي. (10.93.19.8) ردصملا مداخب لصتم Cisco Nexus 9300 switch لوحم ةريكب تاراطال) تي اب 9000 لوحملا ةهجاو يلع اهنيوكت مت يتلا (MTU) لقنلل ي صقألا طاقنتلا رفوتي. مدخال يلع ةدوجوملا (MTU) لقنلل ي صقألا دحلا ةدحو فرعت ال امنيب، (مجال ةقباسلا Nexus ةحص نم ققحتلا تاوطخ عيجم لامكإ لعفلاب مت دقو، ردصملا مداخ نم ةمزح. ةذاش تالاح يا فاشتك نودب

ةيسيئرلا دويقلو تاظحالم - اثلاث

- Nexus لوحم داعبتسإ مت
 - مزح طاقسإ تايلمع دجوت ال
 - ةهجاو لا في ءاطخأ دجوت ال
 - (ACL) لوصولا في مكحتلا ةمئاق وأ ةمدخل ةدوج يلع ريثأت ال
 - ةزهجالا هيجوت ةداعإ ديكأت مت
- ليكشت نراق
 - لوصولا ذفنم
 - تي اب 9000: لقنلل ي صقألا دحلا ةدحو
- ةرفوملا تانايبلا
 - ردصملا في ةمزحلا طاقنتلا
 - (MTU) لقنلل ي صقألا دحلا ةدحول ةلماش ةفرعم
 - تي اب 1500 ةعس ةمزح مادختساب ةئزجت نودب حاجنب لاصتالا رابتخا لم تكا
 - تانايبلا نم تي اب 1472 عم
- ةدوقملا تانايبلا
 - ةهجولا ةيؤر
 - ةهجولا مدخال يلع ةمزح طاقنتلا رفوتي ال

نم ني عم عونل ةصصخم ةصصخم ةصصخم صي صخت تا فلم ءاشنإ كنكمي، Wireshark في هؤارجا ديرت يذلا لي لحتلا

دومعلا فصو

- ةحفاصم يلا اذانتسا باياو باهذ ةلحرلل يلاوأل تقولا ردقي: tcp.analysis.initial_rtt (iRTT) ةيثالثل TCP.
- هل لباقملا رارقإ او TCP عزج ني ب تقولا سيقوي: tcp.analysis.ack_rtt (ACK RTT)
- لباق لبقتسملا لباق نم نلعمل TCP ةذفان مجح يلا ةراشإلا: (ةذفان) tcp.window_size سايقلل قيبب طت
- باسحل مدختس م لا ةذفانلا سايق لماع لثمي: tcp.options.wscale.multiplier (ددعتم)

نوكي ام نيب ، (Client Server → ليمع) يمامألا راسملا يف (~94%) لوصولا نمز مظعم دجوي وأ (CPU) ةيزكرملا ةجلالعمل ةدحو دوجو مدع ىلا ريشي امم ، لقا رصملا نم ةباجتسال تقو ليمعلا ىلع قيبتللا رأت .

TCP ذفنم ىلع فرعتلا

• 445 :ءانيم TCP ةياغ

عئاش لكشب مدختسملا ، Microsoft Server Message Block (SMB) عم 445 ذفنملا قفاوتي لوكوتوربلا اذه دعي . Windows ةقداصم تامدخو ةكبشلا صارقا تاكرحم و تافللملا ةكراشملا TCP ةءافك ىلع ةريبك ةجردب ادمتعم هل عجي امم ، ةيجاتنإلا لوصولا نمز نم لكل اساسح ةكبشلا رارقتساو .

TCP ةذفان مجح ليلحت

• تياب 64,240 : (ساقم) رصملا ةذفانلا
• تياب 65,535 : ةهجولا ةذفان

نوكي ، ةلالا هذه يفو . رارقالا راطتنا لبق اهلاسرنا نكمي يتلا تانايبلا مجح TCP راطلا لثمي ، ةثيدحلا تائيبلل ةبسنلاب اي بسن ةريغص ميقللا هذهو . ةهجولا نم ادييقت رثكا رصملا لفظلا ىلا مالا نم ىودعلا لاقتنا لدعم ةدايز عم ةصاخو ، ةيجاتنإلا نم دحت دقو .

مادختساب يرظن جرخ ىصقا ري دقت نكمي :

RTT / TCP ةذفان مجح = جرخلا

اهتظالم تمت يتلا ميقللا لادبتسا :

• تياب 64,240 TCP ةذفان مجح
• ةيناث 0.000798 = ةيناثوركيم 798 RTT

ةيناثلا يف تباجم 644) ةيناثلا/تباجم 80.5 $\approx 64240 / 0.000798 \approx$ ةجلالعمل ةعس (ابيرقت

ضارفتاب تانايبلا لقن لدعمل ىلعألا دحلا اذه لثمي :

• ةمزحلا نادقف مدع
• لاسرلا ةداعلا
• ةيناثملا ةكبشلا فورظ

ةبولطملا طورشللاو لقنلا تقووجرخلا ليلحت

ةعسب فلم لقن قرغتسي، ةيناثلا يف تباجيم 644 غلبت يتلا ةيلالحلا ةجلالعمللا ةعرسبو راطا زاجنلا. طوولملا ضافخناللا ةزيم عم قفاوتي امم، ةعاس 23.5 نم برقي ام تيباريت 6.5 امم، ابيرقت ةيناثلا يف تباجيج 1.68 ىل ةجلالعمللا ةعس ةدايز بجي، تاعاس 9 ةدمل لقن (291μ يلاوح) طوولم لكشب لق RTT وأ ($2.7 \times$ يلاوح ةدايز) ربكأ TCP ةذفان ام بلطتي.

لوصوللا نكمي ال، (RTT نم 798μ يلاوحو ةذفانلا نم تيابوليكي 64) ةيلالحلا فورظلا لظ يف مجح ةدايز نودو. يددرتلا قاطنلا ريخأت جتنم ةطساوب ديقم TCP جرخ نأل، تاعاس 9 فده ىل امم، حاتم ربكأ يددرت قاطن مادختسا لوكوتوربلل نكمي ال، لوصوللا نمز ليلقت وأ ةذفانلا قيقحتلل لباق ريغ فدهلا لعجي.

RTT بولطملا	TCP راطا بولطملا	لقنلل ردقملا تقولا (تيباريت 6.5)	ةجلالعمللا ةعس	ويرانيسلا
798 μ s	تيابوليكي 64	ةعاس ~23.5	ةيناثلا يف تباجيم 644 (يف تياباجيم 80.5 ~)	ةيلالحلا
~291 μ	~172 تيابوليكي	تاعاس 9	ةيناثلا يف تباجيم 1683 ~ (ةيناثلا يف تياباجيم 210 ~)	9 فدهلا (تاعاس)

وأ ردصملا وأ قيبطتلا وأ ةكبشلا يف ريغت ثودح ىل ريشي امم، اقباس كلذمت دقو لعفلاب نكمي هدحو يلاوالا ليلحتلا اذه ىل اذانتسا هنا طحالن نأ ناكمب ةيمهاللا نمو. ةهوجللا قيقحت نكمي ال، ةيلالحلا RTT طورشو TCP ةذفان مجح لظ يف: ماه جاتنتسا ىل لصوتلا تاعاس 9 ل فده.

و RTT ةذفان مجح ناصقن وأ ةدايز بسح ةجلالعمللا ةعس نيابت ةيفيكل ةنراقم لواجللا ضرعت TCP.

(تياب 64,240 = تباثلا ةذفانلا مجح) ةجلالعمللا ةعس ىل RTT ريثأت

ةجلالعمللا ةعس (يف تباجيم) (ةيناثلا)	ةجلالعمللا ةعس (ةيناث/تياباجيم)	RTT
ةيناثلا يف تباجيم 2,568 ~	ةيناث/تياباجيم 321 ~	200 μ (0.0002 ةيناث)
ةيناثلا يف تباجيم 644 ~	ةيناث/تياباجيم 80.5 ~	798 μ (0.000798 s)
ةيناثلا يف تباجيم 257 ~	ةيناث/تياباجيم 32.1 ~	0.002 ةيناث يلل 2 (ةيناث)

RTT	عجلاعملال ةعس (ةيناث/تياياجيم)	يف تياجيم) ةجلاعملال ةعس (ةيناثال)
0.01 ةيناث يلم 10 (ةيناث)	ةيناث/تياياجيم ~6.4	ةيناثال يف تياجيم ~51

ةذفان مچح ريثأت TCP (RTT = 798 μ)

TCP ةذفان مچح	عجلاعملال ةعس (ةيناث/تياياجيم)	يف تياجيم) ةجلاعملال ةعس (ةيناثال)
16 تيابوليك (16 384 ايلم)	ةيناثال/تياياجيم ~20.5	ةيناثال يف تياجيم ~164
64 تيابوليك (64 240 ايلم)	ةيناثال/تياياجيم ~80.5	ةيناثال يف تياجيم ~644
256 تيابوليك (262 144 ايلم)	ةيناث/تياياجيم ~328	ةيناثال يف تياجيم ~2,624
1 تياياجيم (1,048,576 ايلم)	ةيناث/تياياجيم ~1,314	ةيناثال يف تياجيم ~10.5

ينفال ريسفتال

- ءادألال لوقي امام يلال \rightarrow RTT لوصول نم زم عم ايسكع تانايبال لقن لدعم بسانتي
- ةعس نم ديزت \rightarrow تي TCP ةذفان مچح عم رشابم لكشب تانايبال لقن لدعم بسانتي
ربكأال ذفاونال
- تائييبال يف يتح، ةجلاعملال ةعس نم ةدشب دجال يلع ةريغصلال تاراطال ماجألمعت
لوصول نم زاهيف لقي يتال
- نم ةلمالكال ةدافتسالل ةذفانال ريوطت (10G+) ةعرسالل ةقئاف تاكبشال بلطتت
ي ددرتال قاطنال

امهل يلحت بچي و TCP ءادأ يف نامساح نالماع امه TCP و RTT ةذفان مچح نم الك نأ حضوي اذهو
اهالصال و جخال ءاطخأ فاشكتسأ دنع اع

TCP و IP سألوط

- تياپ 20 IP سألوط
- تياپ 32 TCP سألوط

م تي هنأ تي اب 32 وذ TCP س أ ر د ك و ي . IP ت ا ر ا ي خ د و ج و م د ع ي ل ا تي اب 20 م ج ح ب IP س أ ر ر ي ش ي
ة د ا ع ت ا ر ا ي خ ل ه ذ ه ن م ض ت ت . ي س ا س أ ل س أ ر ل ا ج ر ا خ ت ي اب 12 ة ف ا ض ا ع م ، TCP ت ا ر ا ي خ م ا د خ ت س ا
ه ب ح و م س م ل SACK و ، ة ذ ف ا ن ل س ا ي ق ، MSS

TTL و TCP ت ا ر ا ي خ ل ي ل ح ت

ة ر و ص ل ا ي ف ي ئ ر م ر ي غ ا ذ ه . ة ي ا ه ن ل ا ي ت ط ق ن ي ل ع (SACK) ي ئ ا ق ت ن ا ل ا ر ا ر ق ا ل ا ن ي ك م ت م ت
غ ل ب ي ن ا و ، ت ا ن ا ي ب ل ا ن م ة ق ص ا ل ت م ل ا ر ي غ ل ت ك ل ا ب ف ر ت ع ي ن ا ي ق ل ت م ل ل SAACK ح ي ت ي و
ح ا ج ن ب ا ه م ا ل ت س ا م ت ي ت ل ا ع ا ز ج ا ل ا ب د ي د ح ت ل ا ه ج و ي ل ع ل س ر م ل ا

، 2000-3000 ن ا د ق ف م ت ن ك ل و 3000-4000 و 1000-2000 ع ا ز ج ا ل ا ي ق ل ت م ت ا ذ ا ، ل ا ث م ل ا ل ي ب س ي ل ع
ل س ر م ل ا ن ا ف SAACK م ا ط ن ب ا ي غ ي ف و . ح ي ر ص ل ك ش ب ك ل ذ ي ل ا ل ب ق ت س م ل ا ر ي ش ي ن ا ن ك م ي ف
ة د ا ع ا م ت ي د و ق ف م ل ا ع ز ج ا ل ط ق ف ، SAACK ع م ؛ ة و ج ف ل ا د ع ب ت ا ن ا ي ب ل ا ل ك ل ا س ر ا د ي ع ي ف و س
م ز ج ل ا ن ا د ق ف ن م ي ن ا ع ت ي ت ل ا ت ا ئ ي ب ل ا ي ف ة ر ي ب ك ة ج ر د ب ع ا د ا ل ا ن ي س ح ت ي ل ا ا ذ ه ي د و ي . ه ل ق ن

(SYN) 1 ة م ز ج ل ا ل ي ل ح ت

- (Wireshark ع ي ب ط ت م ت) 0 : # ق ي س
- ت ي اب 0 : ة ل و م ح ل ا
- ACK#: 0
- ت ي اب 1460 : س ا م ا
- ttl: 128

م غ ر ل ا ي ل ع ، ة ع ا ر ق ل ا ة ي ن ا ك م ا ل ج ا ن م ر ف ص ي ل ا ي ل س ل س ت ل ا م ق ر ل ا م ي م ع ت ب Wireshark م و ق ي
ع ا ش ن ا ع ا ن ث ا ة ل و م ح د و ج و م د ع ع ق و ت م ل ا ن م . ة ر ي ب ك ة ي ئ ا و ش ع ة م ي ق ل ث م ي ا ي ل م ع ه ن ا ن م
20 م ج ح ب IP س أ ر) ت ي اب 1500 ر ا د ق م ب MTU ي ل ا تي اب 1460 ة غ ل ا ب ل MSS ة م ي ق ر ي ش ت . ل ا ص ت ا ل ا
ي ل ا د ن ت س م ف ي ض م 128 ل (TTL) ع ا ق ب ل ا ة د م ن و ك ت ن ا ن ك م ي . (ت ي اب 20 م ج ح ب TCP س أ ر + ت ي اب
د ن ع ل م ت ح م ل ا ن م ن ا ك ط ا ق ت ل ا ل ا ن ا ي ل ا ر ي ش ت ط ا ق ت ل ا ل ا ي ف ة م ي ق ل ا ه ذ ه ة د ه ا ش م و ، Windows
2. ة ق ب ط ل ا ر ب ع ا د ج ه ن م ب ر ق ل ا ب ا و ا ر د ص م ل ا

(SYN-ACK) 2 ة م ز ج ل ا ل ي ل ح ت

- ACK#: 1

، ك ل ذ ل . ة ل و م ح د ج و ي ا ل ا م د ن ع ي ت ح ، د ح ا و ل س ل س ت م ق ر ك ل ه ت س ي SYN م ل ع ن ا ل 1 ي ه ACK ة م ي ق
ACK = SEQ + 1.

- ttl: 59

ي ت ل ا ة ي ل و ا ل ا (TTL) ع ا ق ب ل ا ة د م ي ل ا ا م د ق 59 ة غ ل ا ب ل ا ه د ص ر م ت ي ت ل ا (TTL) ع ا ق ب ل ا ة د م ر ي ش ت و

لك موقت. (5 = 64 - 59) هي جوت تال قن 5 نم برقي ام تازاتج| عمزحلا نأ ينعي امم، 64 غل بت دحاو رادقم ب (TTL) عاقبالا دم ضفخب ةهجوم ةوطخ

ةكبشلا رثاؤ ةئزجتلا رطخ

امي ف ةصاخ، عاأالا يل ع ةلمتحم رطاخم ضرف يل ابيرقت هي جوت تال قن سمخ دوجو يدؤي ةئزجتلاو (MTU) لقنلل يصقأالا دحلا ةدحو قباطت مدعب قلعتي

،ةيلصأالا عمزحلا مجح نم لقأ (MTU) لقنلل يصقأالا دحلا ةدحو طسوتم طابترأ يأل ناك اذا ةديدع بقاوع يل اذه اندوقيو. ةئزجتلا ثدحي نأ نكمي

- عيمجتلا ةداع| تاقفنو ةئزجتلا ببسب لوصولو نمز ةدايز
- لمالكاب عمزحلا لقن ةداع| بلطتي دحاو عزج نادقف نأل ارظن، عمزحلا نادقف ربكأ لامتحا
- للقيو ماحدزا انأ يل ع ةراسخلا رسفي TCP لوكوتورب نأل ارظن، ةجالعمل ةعس ليلقت اهب صاخلا لاسرالا لدعم نم
- ةئزجتلا جلاعت يتلا ةكبشلا ةزهجأ يل ع (CPU) ةيزكرملا ةجالعمل ةدحو مادختسا ةدايز
- (PMTUD) راسم لل (MTU) لقنلل يصقأالا دحلا ةدحو فاشتكاي ف لشف تالاح ثودح رطخ ةتاماص مزح طاقس| تايلمع يل ايدؤي امم، ICMP لوكوتورب رطح مت اذا

ربع لقنلل يصقأالا دحلا ةدحو قاستا نامض ناكمب ةيمهأالا نم، لماوعلا هذه يل رظنلابو عاضتقالا دنع ةيئاييميكل داوملا ةرادا| ماظن راطا| يف ددشتلا تاءارج| ذيفنت وأ راسملا

يلوالا RTT لباقم ACK RTT: TCP RTT ليلحت

طخالبا ةنراقم داز دق لوصولو نمز نأ يل اريشي هنإف، iRTT نم ربكأ ACK RTT نوكي ام دنع TCP ةحفاصم عانثأ هؤاشن| مت يذلا يساسأالا

ةداع كلذو، ةسلجال لالخر يخالأالا نم ديزم يف ببستت ةياهنلا طاقن وأ ةكبشلا نأ ينعي اذه ببسب:

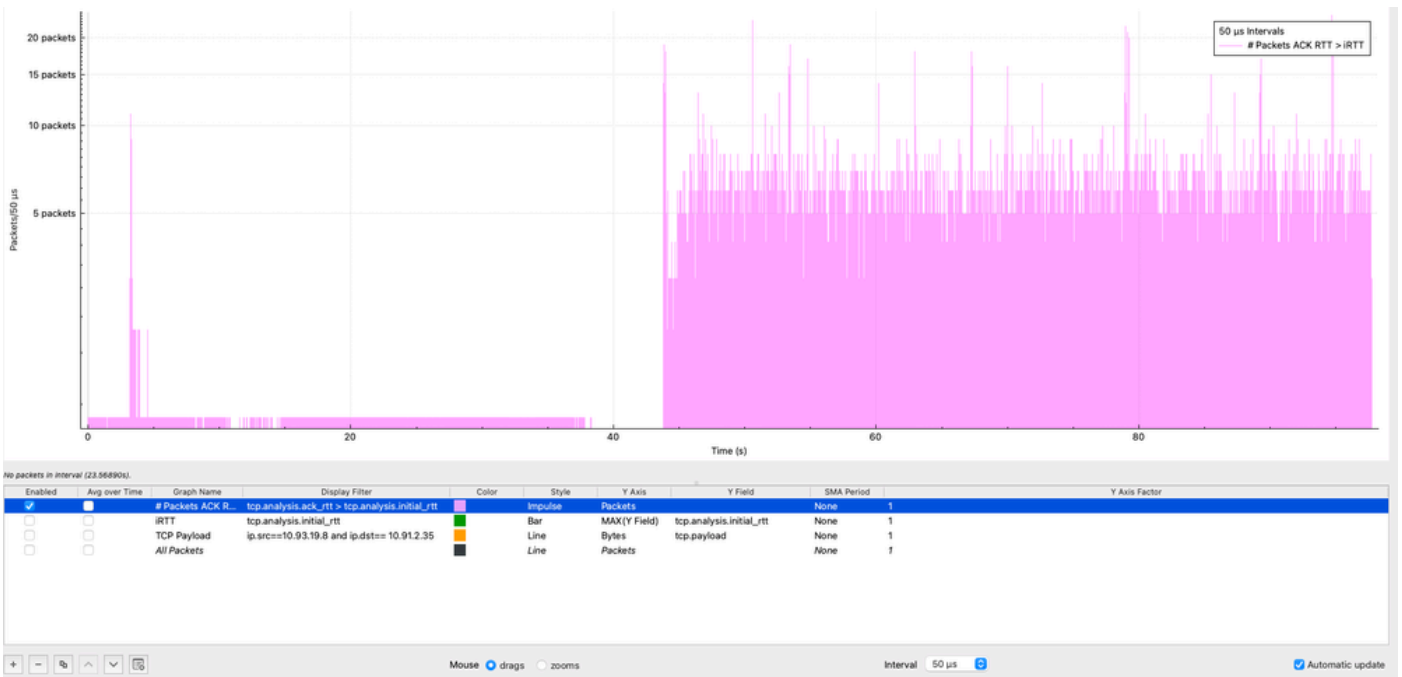
- راطتنا مئوق وأ ةكبشلا ماحدزا
- قيبطتلا وأ ليمعلا ةجالعمل يف تاريخأت
- (ليمحتلا نزاوم، ةيامحلا نارديج) ةطيسولا ةزهجأالا
- لاسرالا ةداع| تايلمع

يل ايدؤت هنإف، TCP ةسلج لاوط ةلالحلا هذه ترمتسا| اذا

- ضفخنم TCP جارخا لدعم
- ةذفانلل لاعف ريغ مادختسا|
- تاقيبطتلا لنسحم عاأالا

مسر ةزيم مادختساب ACK RTT > iRTT طرشلل ثودح تارم ددع ضرع نك مالم نم، Wireshark يف
I/O Graph، Statistics → I/O Graph، ضرعلا حشرم قيبطت، اندا ي نايبل I/O
لصاف مادختساو، مزحلا يلع Y روحملا دادع، تاضب نلا طمن ديدحت، (tcp.analysis.initial_rtt >
tcp.analysis.ack_rtt)، ةينات وركيم 50 هراقم.

ةلاحلا هذه يفوتست يتللا مزحلا ددع ةيجسفنبل تاضب نلا لثمت، ي نايبل م س رلا يف
ةمزحلا طاقتلا لاوط ةلاحلا هذه رمتست، طحول امكو. ةينات وركيم 50 لصاف لك نمض
طخللا نم قستم لكشب يلعا ةسلجلا ءانثا لوصولا نمزنا يل ريشي امم، لمكلا ب
ةلاح نم ال دب ءادالا يف رمتسم ضافخنا يل ءدشب كولسلا اذره ريشي و. يلوالا ياساسالا
نيزختلا واما دزالا لثم ةلمتحملا رداصملا يف قيقحتلا يل ءجالحا ززع ي امم، ةيلالقتنا
ةياهن يل ءياهن نم راسملا ربع ةياهنلا طاقن ءجالعم تاريخات و اتقو م.



ددع درجم س يلو، تانايبل ل قن لددعم زواجت اهيف متي يتلا ءدملا ديدحت اضيأ مهمللا نمو
ءارجا نكمي هنا ال، ءرشابم لوقحلا ني ب حرطالاب حمسي ال Wireshark نأ نم مغرلا يلع. تارملا
ةينايبل جارجال/الخال دال تاموسر مادختساب ةيئرم ءنراقم

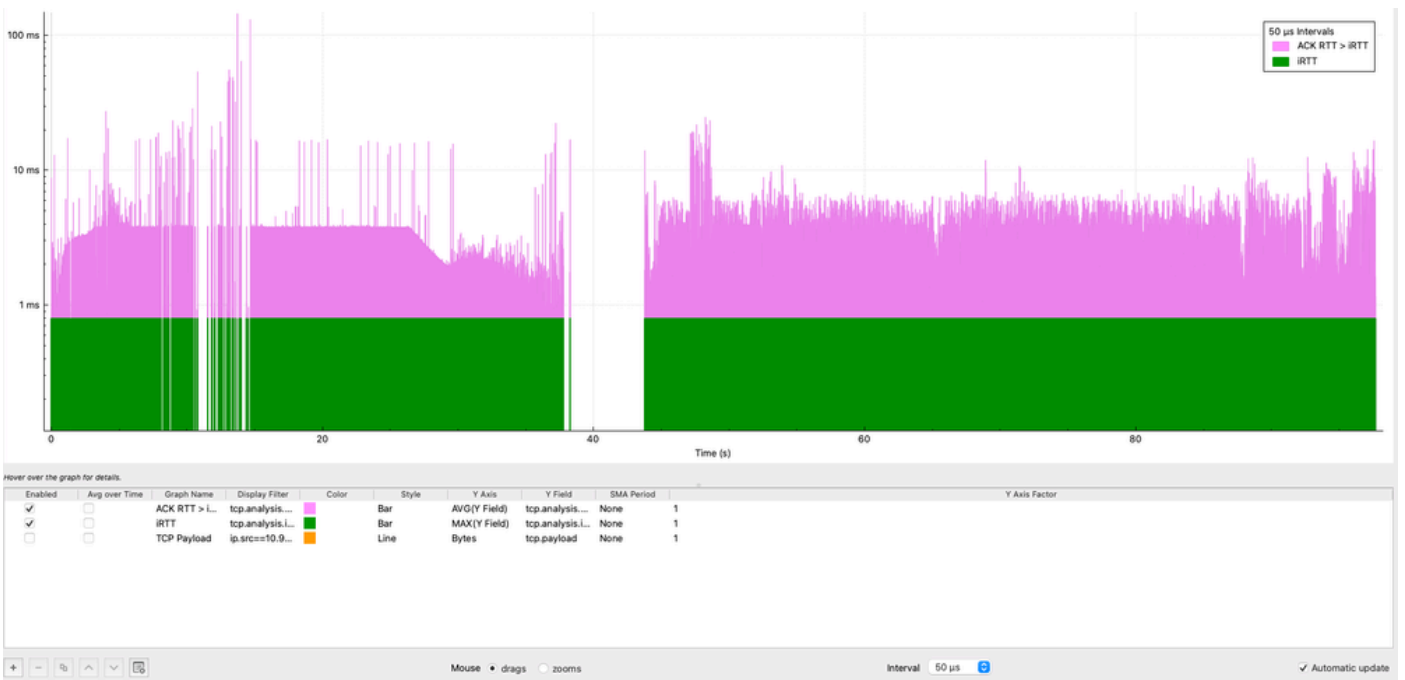
- ةيئاصح ال جارجال/الخال دال → تاموسر يل لقتنا
- 1: ي نايبل م س رلا
 - tcp.analysis.ack_rtt > tcp.analysis.initial_rtt: ضرعلا ةيفصت لماع
 - راب: طمنلا
 - طسوتم: ص روحم
 - tcp.analysis.ack_rtt: ص ل قح
 - ةينات وركيم 50: ي نمزلا لصافلا
- 2: ي نايبل م س رلا
 - tcp.analysis.initial_rtt: ضرعلا ةيفصت لماع
 - راب: طمنلا
 - ي صقألا دحلا: ص روحم

tcp.analysis.initial_rtt : ص ل ق ح

• ل ج س ل ا س ا ي ق ن ي ك م ت ب م ق و ي ن ا ي ب ل ا م س ر ل ا ي ل ع ن م ي ا ل ا س و ا م ل ا ر ز ب ر ق ن ا م ث

ي ذ ل ا و ، $ACK\ RTT > iRTT$ ط ر ش ل ا ي ج س ف ن ب ل ا ي ن ا ي ب ل ا م س ر ل ا ل ث م ي ، ي ئ ر م ل ا ض ر ع ل ا ا ذ ه ي ف ل ا ق ت ن ا ل ا ن م ز م خ ض ت ت ا ن ا ي ب ل ا ر ه ط ت و . ا ه ل م ك ا ب TCP ة س ل ج ل ا ل خ ت ب ا ث ل ك ش ب ا د و ج و م ن و ك ي ي ل ا ي ص ق ا ل ا د ح ل ا ع ف ت ر ت و ة ي ن ا ث ي ل ل م 11 ي ل ا د د ع ت م ة و ر ذ ت ا ر ت ف ل ص ت ث ي ح ، ر م ت س م ل ا $iRTT$ ل ي س ا س ا ل ا د ح ل ا ف ع ض 100 ي ل ا 11x ل ث م ي ا م م ، ة ي ن ا ث ي ل ل م 100 ن م ر ث ك ا

ة ل ا س م ي ل ا ر ي ش ي ا م م ، ة ر م ت س م ل ب ة ر ب ا ع ت س ي ل ل ا ق ت ن ا ل ا ن م ز ة د ا ي ز ن ا ك و ل س ل ا ا ذ ه د ك و ي و ل ث م ل م ا و ع ي ل ا ة د ش ب ر م ت س م ل ا ف ا ر ح ن a ل ا ا ذ ه ر ي ش ي و . ن م ز ل ا ر م ي ل ع ة ر و د ل ا ي ل ع ر ث و ت ة ي ه ن م ة ي ا ه ن ل ا ة ط ق ن ة ج ل ا ع م ت ا ر ي خ ا ت و ا (Bufferbloat) ت ق و م ل ا ن ي ز خ ت ل ا و ا ة ك ب ش ل ا م ا ح ذ ل ا



ة ف ئ ا ز ل ا ل ا س ر ا ل ا ة د ا ع ا ت ا ي ل م ع ل ي ل ح ت و TCP ل و ك و ت و ر ب ل ا س ر ا ة د ا ع ا ت ا ي ل م ع

، ت ق و ل ا ر ب ع ل ا س ر a ل ا ة د ا ع ا ت ا ي ل م ع ل ي ل ح ت ل ا ل خ ن م TCP ة ي ق و ث و م م ي ي ق ت ب م س ق ل a ا ذ ه م و ق ي ء ا د ا ل ا ض ا ف خ ن a ي ف م ه ا س ي ة م ز ح ل a ن ا د ق ف ن a ك ا ذ ا ا م م ق ق ح ت ل a ح ي ت ي ا م م

ت ق و ل a ر ب ع TCP ل و ك و ت و ر ب ل a س ر a ة د a ع a ت a ي ل م ع

ة د a ع a 42 ه ع و م ج م ا م ط ح و ل و . ت ق و ل a ر ب ع TCP ل a س R a ة د a ع a ت a ي ل م ع ع ي ز و ت ي ن a ي ب l a م س R l a ح ض و ي ر و ر م l a ة ك ر ح ع و م ج م ن م ط ق ف ة ئ a م l a ي ف 0.00125 ل ث م ت ، ل a س R a

a م ه a س م a l م a ع س ي l ة م ز ح l a ن a د ق ف ن a ي ل ا ح و ض و ب ر ي ش ي و ه ف a ت ل a S R a ل a ة د a ع a ن م ي و ت S M l a ا ذ ه

ويرانيسلا اذه يف

(TCP لاسرا ةداع| تايلمع) Wireshark نيوكت

Statistics → I/O Graphs

• ضرعلا ةيفصت لماع

tcp.analysis.retransmission and !tcp.analysis.spurious_retransmission

- طيرش وأ عفد: طمنلا
- مزحلا: ص روحم
- ةينات 1: ينمزلا لصافلا

ة في زملا TCP لاسرا ةداع| تايلمع

لصاوف يف TCP لوكوتوربل ة في زملا لاسرالا ةداع| تايلمع ددع ينبايبل م سرلا حضوي
10.93.19.8 رصملا ةطساوب اهؤاشن| مت ةينات 1 اهتدم ةينمز

متي مل عطقم لاسرا داعأ في ضملا نأ ىلى يلاي تحال TCP ثب ةداع| ريشي، Wireshark يف
ضرتفا لسرمل نكلو، حاجنب ملتسملا ىلى ةيلصألا ةمزحلا تلصو. لعفلا ب هنادق
ىلى كولسلا اذه ريشي ال. قيقدلا ريغ تي قوتلا ريدقت ببسب حيحص ريغ لكشب ةراسخ
لسرمل دنع لاعفلا ريغ لاسرالا ةداع| قطنم ىلى لب، ةمزحلل ةيقيقح ةراسخ

طاقتلالا اذه يف:

- طقف ةيناتوركيم 8 يلاوح دعب مزحلا 10.93.19.8 رصملا لسري
- ابيرقت ةينات يلم 200 دودح يف ةيجذومنلا لاسرالا ةداع| تاتقؤم نوكت امنيب

رصملا TCP سدكم ةطساوب لمالكلا ب هي ف مكحتلا متي لاسرالا ةداع| كولس نأ دكؤي اذهو،
ةكبشلا ةطساوب سيلاو

ام وهو، ةلاح 112 اهتظحالم تمت يتلا ةفئازلا لاسرالا ةداع| تايلمع ليامجالا ددعلا غلبوي
اهيلع ءاليتسال مت يتلا رورملا ةكرح يلامجالا نم %0.0332 لثمي

(ة في زملا TCP لاسرا ةداع| تايلمع) Wireshark نيوكت

• عرض الة ففصت لماع

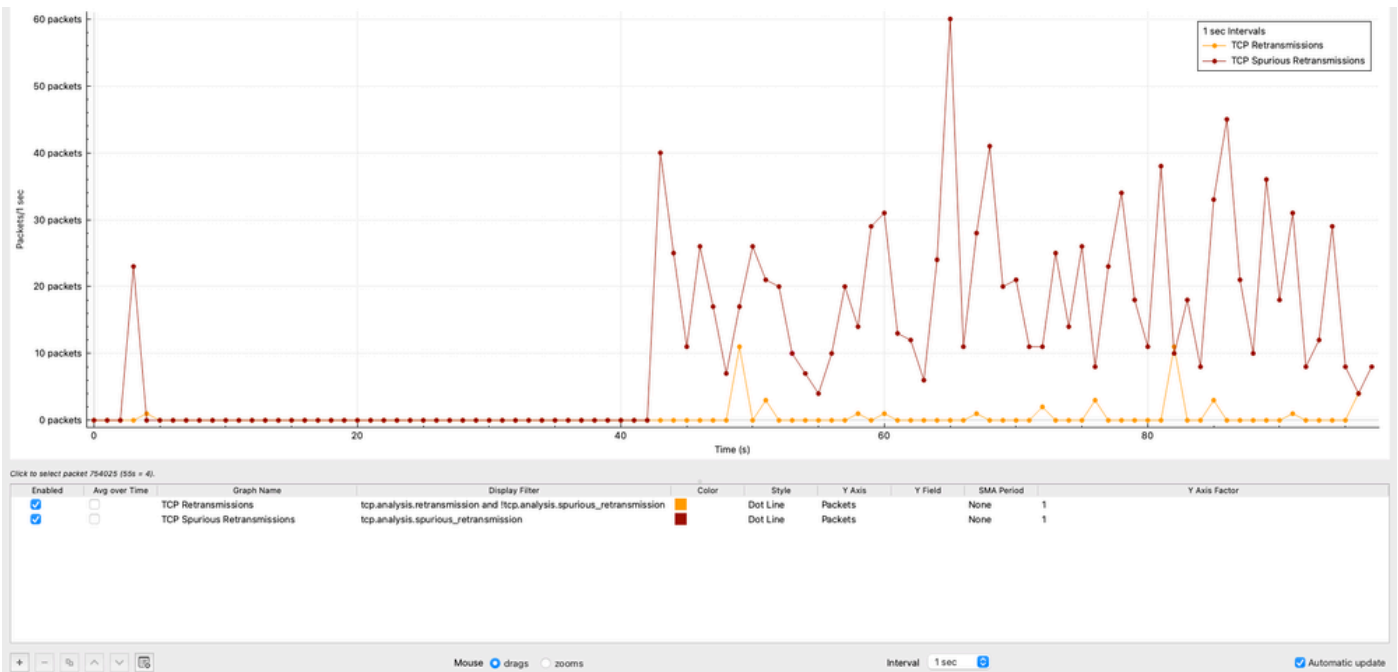
tcp.analysis.spurious_retransmission and ip.src==10.93.19.8

- طيرش وأ ع فد :طمنللا
- مزحلل :ص روحم
- ةي ناث 1 :ينمزللا لصلاللا

ينفلل ريسفلللا

- دوجو مدع ةيقي قحلال لاسرلال ةداعل تاي لمعل ةيغلل ةضفخنملا ةيويئملا ةبسنللا دكؤت ةكبشللا يف ةمزحلل نادقف
- نم اهانوال ةقوباسللا لاسرلال ةداعل تارارق لىل ةفئازللا لاسرلال ةداعل تاي لمعل دوجو ريشي ردمملا فيضم لبق
- ببسلل سيل هنكلو ،ةعافكللا لىل ع فيفط لكشب كولسللا اذه رثؤي نأ نكمي داحللا جاتنلال طاطحنال يساسأللا

نمز وأ TCP كولسب لب ،ةكبشللا ةي قووثوم ب قلعتت ال ةلكشملا نأ لىل حلال اذه ززع ي امك ةياهنلال طاقن عادأ وأ لوصوللا

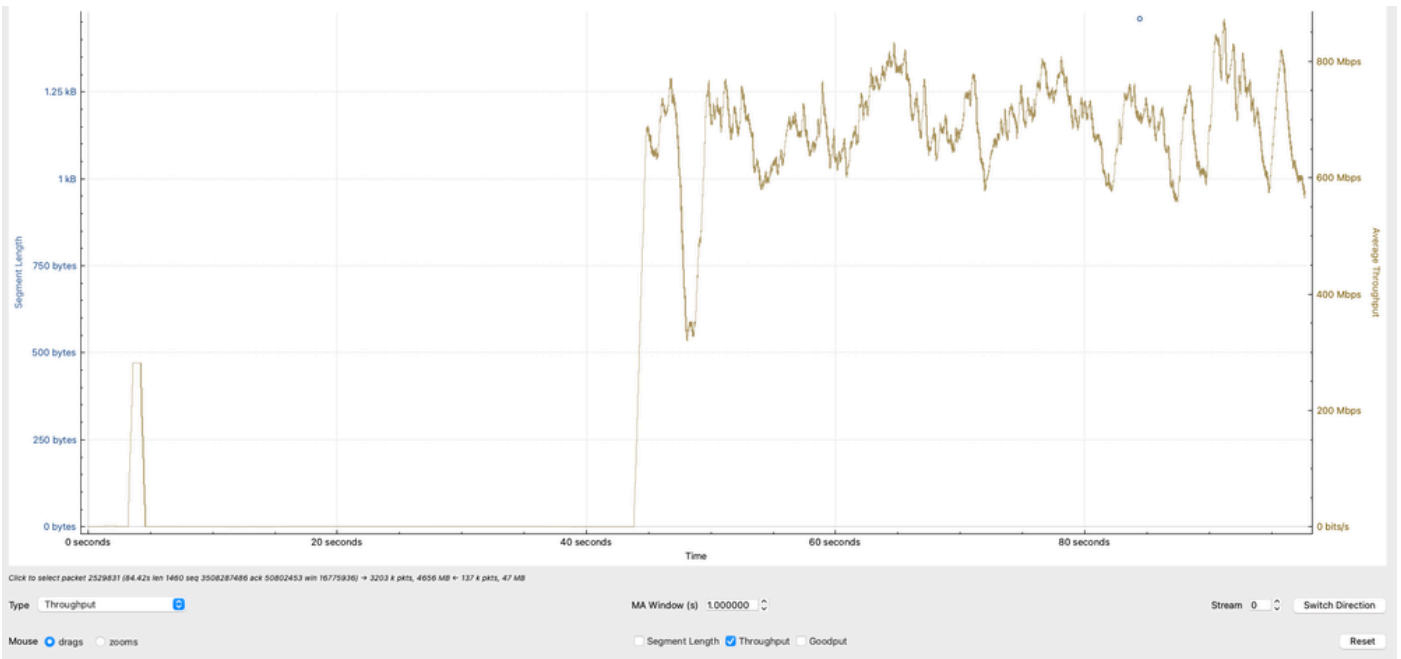


لاعفالات نإلال ليلحت

لوكونورب ةلومح إلال اءانسا اءاسح مءو، ةلاعفالات ةءلاعمل ةءس ةئنايبل ةمسرلا رهظء هءصر مء ءءلا ءرءلا بءبءءو. ةئناءلا ءفءا ءاوملاب (ةلوقنملا ةئلعفالات انايبل) TCP نء ءفءه نأ إلال رءشء امم، ةئناء/ءبءءم 800 و ةئناء/ءبءءم 600 نءب ءساسة لءشء قاطن ضرع ءاناءم إلال لصرء ال انه إء، طشن لءشء ءانايبل لقن إلع ةءبشلا لمعء ربكأ ءءرء.

(ةلاعفالات ءلاعمل ةءس) Wireshark نءوكت

Statistics → TCP Streams Graphs → Throughput



ئنفال رءسفتلا

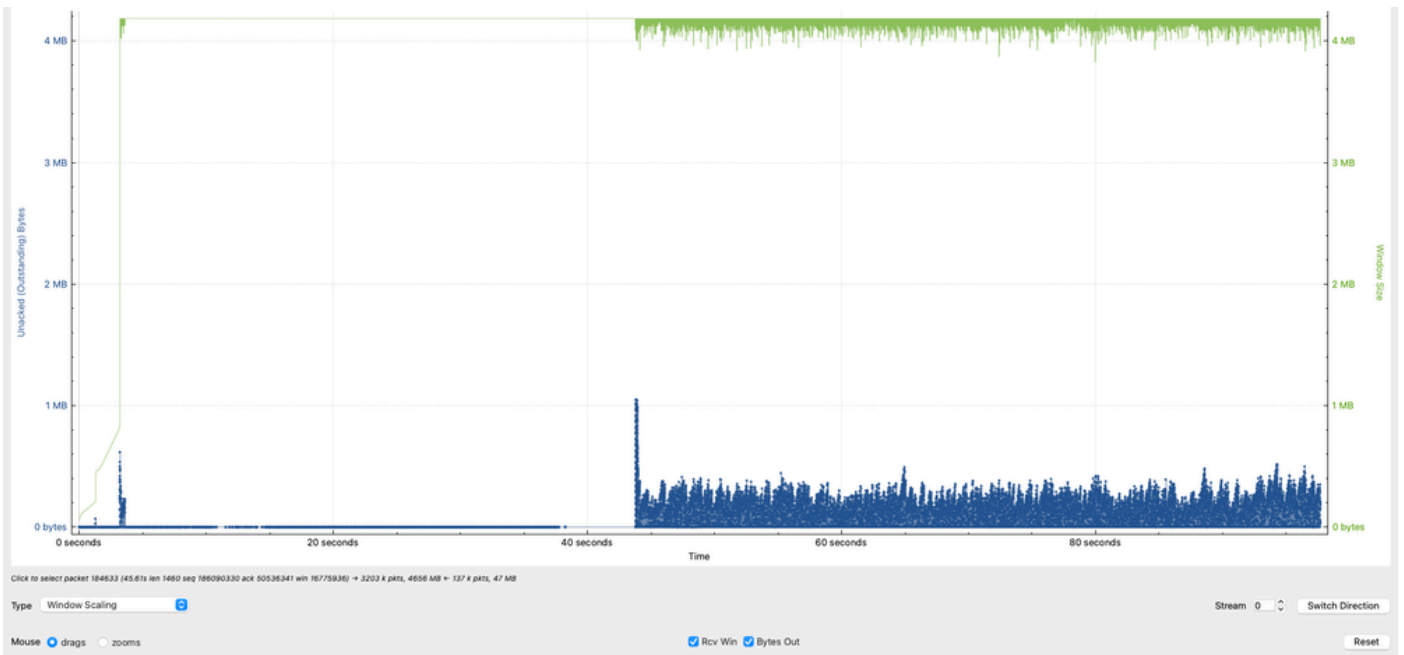
- عم ةئناءلا ءفءا ءبءءم 800 إلال 600 نم ءوارءو ءءلا ءلاعمل ةءس قاطن قءاوءو RTT و TCP ةءءان مءء إلال اءانسا ةقءاسلا ءاباسءلا
- ةئءاءانإال ءفءا ءالفالءءال سءعء
 - RTT ءاءرءء
 - TCP مءءءا ءفءا ءالءءعء
 - اءقوءم و اءقوءم ءاقءبءءلا نءءء
- نإء، (مء 10، لاءءملا لءبس إلع) طءءلا لءعم نم بءرءقء ال ءلاعمل ةءس نأل ارءن TCP لوكونورب ةءافك ءوئق لب ءءاملا ءءرءلا قاطنلا ضرع ءسءل ةئءوءءملا
- TCP لوكونورب ءوئق عم ءقءاوءم اهءظءالم مء ءفءا ءئناءانإال نأل لءلءءلا اءه ءكوءو ةءس و ءمءءلا ناءقء إلال ءءرء ال ءاقانءءال نأل ءكوءو امم، (لوصولا نمزو ءءءانلا مءء)

ة.ياهنلا ةطقن فورظو لقنلا ةقبط كولس ببسب نكلو، ةهجاولا

(TCP ةذفان) ناريطالا ليلحت يف تانايبلا

يقولتملا ةعس ةنراقم TCP لمع ةسلج يف جرح كولس ىلع ءوضلا ينايبلا مسرلا طلسي
(ناريطالا ءانثأ تيابل تادحو) لقنلا ءانثأ ةيلعفل تانايبلا لباقم

- اهلوبق (لبقتسملا) 10.91.2.35 ل نكمي يتلا TCP تانايب رادقم رضخألا طخلال لثمي
(ةلاعفل مالتسالا ةذفان)
- (لسرمل) 10.93.19.8 نم ايلاح ليغشلا ديقي TCP تانايب رادقم قرزألا طخلال لثمي



حوارتت ةيفاضا ممق عم، تياباغيم 1 وحن ةيوجل تالحرلا يف اهدصر مت يتلا تانايبلا ممقو
250 و تيابوليكي 1 نيبلوأل ةجردلابل زكرتت اهنكل، تيابوليكي 5 و تيابوليكي 8 نيبل
تيابوليكي.

إف، تانايبلا نم ربكأ تايملك ةجلاعم ىلع رداق يقولتملا نأ نم مغرلا ىلع هنأ ىلإ ريشي اذهو
رارمتساب ةحاتملا ةذفانلا مدختسي ال لسرمل

(ةذفانلا لباقم ناريطالا يف تانايب) Wireshark نيوكت

Statistics → TCP Streams Graphs → Throughput

ينفلا ريسفتلا

- يلع رداق هنا يلع لدي امم ،ريثك ب ربك أذفان نع (10.91.2.35) لابقتسالال زاغ نلعي تانايبال نم ديزم يقلت
- تانايبال نم حضورم وه امك ،ةحاتملا ةذفانلا مادختسا نم للقي (10.93.19.8) لسرملال ناريطال ميق يفة قسانتملا ريغو لقالا
 - ةيوجلال تالحرلا ميق يفة تانايبالاب ظافتحالال يلاثم لكشب لسرملال نكمي
 - ةيجاتنالال ةدايزل (تياغيم 1~) نيلبققتسملل نلعملال راطالال يلبرقأ لكشب يصقالال دلال
 - يلب ناريطالال اناثأ ةيلال تانايب تايوتسم يلع ظافحالال يلع ةردقلا مدع يدوي
- TCP لوكتورب ةءافك مدع يلع يوق رشؤم وهو ةيجاتنالال نم رشابم لكشب دلال ةكبشلال ةردق بقلعتت ةلكشم سيلول ،ردصملا نم

تقولال ربع MSS لباقم TCP ةلومح ليلحت

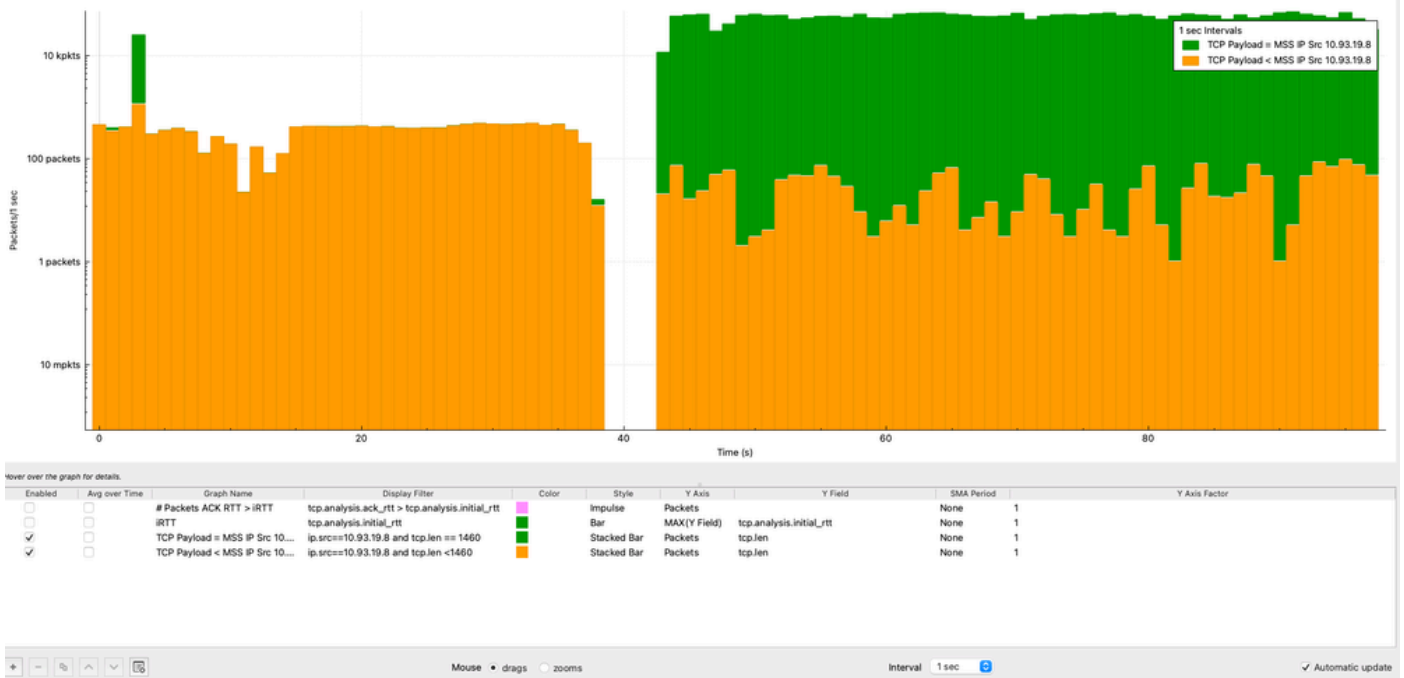
مدختسي لسرملال ناك اذا ام ديدحت يلع تقولال ربع MSS لباقم TCP ةلومح مجح ليلحت دعاسي (10.93.19.8) ردصملا IP ناوع روظنم نم ليلحتلال اذه ارجا متي .ال مأةءافكب TCP عطقم لك

يلي امك ةينايبال تاموسرلال نيوكت متي ،Wireshark يفة

- (MSS مجح مزحلا) 1 يينايبال مسرلا
 - ip.src==10.93.19.8 و tcp.len == 1460 :ضرعلا ةيفصت لماع
 - سدكم طيرش :طمنلا
 - مزحلا :ص روحم
 - ةدحاو ةيناث :ينمزلا لصافلا
- (MSS ≤ مزحلا ةفاك) 2 يينايبال مسرلا
 - ip.src==10.93.19.8 و tcp.len <= 1460 :ضرعلا ةيفصت لماع
 - سدكم طيرش :طمنلا
 - مزحلا :ص روحم
 - ةدحاو ةيناث :ينمزلا لصافلا
- لصفأ ةيؤر يلع لوصحلل يمتراغولل سايقلا قيبطت

ليلحتلال نم

- 1460 يهو MSS ةميقي يلبا تباث لكشب (ةيناثلال يفة ةمزح >10000) مزحلال مظعم لصت تيباب
- وأ ،ةئزجتلال وأ (ACKs) يداعلال TCP كولس ببسب لقا ةلومح مزحلال نم رغصأ عزج لمحي (قفدلا ةيانه تانايب)



TCP أداء ضايفخنا (RCA): يرنجلال ببسلا ليلحت

اجهن بلطتي TCP لوكتورب أداء لئاسمل يرنجلال ببسلا ديحت نأ ليلحتلا اذه حضوي روهدتلل يسيئرلا ردصملا يه ةكبشلال نأ ضارتفا نم الدب، الماكتمو الماش

كلذ ي ف امب، Cisco Nexus 9300 switch لوحملا ىلع فثكم لكشب ةحصلا نم ققحتلا عارجا مت ةجلاعمل ةدحو نم ققحتلاو ARP رارقتساو هيچوتلاو ةمدخلا ةدوج تاسايسو ةهجاوالاتاداع هيچوت ةداع نم ققحتلاو نيتماعد نيب ةحسف ىلع مئاقلا مزحلا طاقتلاو (CPU) ةيزكرمل نمض لمعي ناك لوحملا نأ تباث لكشب جئاتنلا عيجم تذكأ. ELAM مادختساب ASIC يوتسم ةعقوتملا تاملعمل:

- مزح طاقسإ تايلمع دجوت ال
- (ةيناثوركيم قاطن) يداع ريغ لوصو نمز دجوي ال
- مكحتلا يوتسم وأ ةمدخلا ةدوج ىلع ريثأت ال
- ةجحصلا ةزهجالا هيچوت ةداع

TCP لوكتورب ليلحت فشك، كلذ ىلى ةفاضلإاب

- ركذت ال تاليوحت (0.00125%)
- ةمزحلا نادقف ىلع ليلد دجوي ال
- ردصملا ي ف قسانتم MSS مادختسا
- RTT دويقو TCP ةذفان عم جرخلا ةاذحام تم
- (ةلجرلا ليلحت ي ف ةدوجوملا تانايبلا) لماك لكشب ةرفوتملا TCP ةذفان مادختسا مدع
- ةجازللا قنع تسيلا ةكبشلا
- ءادألا نم دحي ردصملا مداخل

رارقلا

1500 (MTU) لقنلل ىصقألا دحلا ةدحو عم روصملا مداخللا ليغشت ىلإ ءادألا ضافخنا عجري ةكبشلا ةعسل لاعفلا مادختسالا عنمي امم ، لاصتالا ىلع ةقئاف ةردق تاذ ةئيب يف ةحاتملا.

لحلا

تباب 9000 ىلإ 1500 نم روصملا مداخللا ىلع (MTU) لقنلل ىصقألا دحلا ةدحو ةدايزب مق :ءاوفلا . ةكبشلا ةيساسألا ةينبلاو ةهولا عم اهتاذاحمل

- ربكألا TCP حئارش نيكمتم
- تانايبلا مزح تافورصم ليلقت
- ةيلامجالا ةيجاتنالا نيسحت

ينف ساكعنا

تاجاتنتسالا بنجت ةيمهأ يهوليلحتلا اذه نم اهصالختسا نكمي ةيساسأ ةقئاف ةمثم يف عئاشلا نم هنأ نيح يف . اهجالصإو ةكبشلا ءادأ ءاطخأ فاشكتسأ دنع اهنأوال ةقباسلا لمعت تناك ةكبشلا نأ حوضوب حضوت ةلحال هذه نإف ، ةكبشلا ىلإ لكاشملا وزع ةيادبلا ىلع ةقدب فرعتلا نكمملا نم نكي مل . لمالكلا تانايبلا ىوتسم راسم ربع ححص لكشب ىلع ةهولاو روصملا يروظنم نم قيميعل TCP ليلحت ءارجا لالخ نم الإ ةيقيقحلا تاقانخال لاسرالا ءاعإو ءذفانلا مادختساو RTT كولسو ديلا ءفاصم تاملعم كلذ يف امب - ءاوس دح . ءلومحلا ءءافكو

، ئطاخل صيخشتللا عنمي لىصفتلاب TCP لوكوتورب كولس ليلحتل يفاكللا تقولا ذخأ نإ بابسلا وحن حالصإلا دوهج هيچوت نمضي و ، ةيرورضلا ريغ ةكبشلا تاريغت نم للقيو . يلعفلا يرذللا

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخلا مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحا وه
ىلإ أمئاد عوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يصلأل يزي لچنإل دن تسمل