

TLOC ءارجإو اهحالصإو OMP ءاطخأ فاشكتسأ

تايوتحمل

[عمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[\(OMP\) ءحوتفملا ءمظنألا ءرادا جمانرب ىلع ءماع ءرطن](#)

[EIGRP لشف ويرانيس](#)

[OMP لشف ويرانيس](#)

[رشابم لشف](#)

[رشابم ريغ لشف](#)

[نشكأ-كولت](#)

عمدقملا

فاشكتسال (OMP) تاكبشلا ءرادا لوكوتورب لشف تاهو ويرانيس دنتسملا اذه فصى Cisco نم SD-WAN ءكبش يف ءكبشلا ءنورم ريفوتل تاسرامملا لضفأو اهحالصإو ءاطخألا

ةيساسألا تابلطتملا

تابلطتملا

لج (SD-WAN) ءكبش ءقطنم فرعى ءيجمررب cisco ل نم ءفرعم تنأ ىقلتى نأ ىصوى cisco.

عمدختسملا تانوكملا

ةيلاتلا ءيداملا تانوكملا و جماربلا تارادصا ىل دنتسملا اذه يف ءدراولا تامولعمل دنتست

- vManage ابلاغ Cisco IOS Catalyst SD-WAN Manager جمانرب
- vBond مساب ءفورعمل Cisco IOS Catalyst SD-WAN Validator ءيوهلا نم ققحتلا ءادأ
- vSmart مساب ءفورعمل Cisco IOS Catalyst SD-WAN Controller مكحتلا ءدحو
- vEdge ءزهجأ

ءصاخ ءيلمعم ءئيب يف ءدوچوملا ءزهجألا نم دنتسملا اذه يف ءدراولا تامولعمل ءاشنإ مت تناك اذإ. (ىضارتفا) حوسمم نيوكتب دنتسملا اذه يف عمدختسملا ءزهجألا عيمج تأب رمأ يأل لمحتحمل ريثأتلل كمهف نم دكأتف ، ءرشابم كتكبش

(OMP) ءحوتفملا ءمظنألا ءرادا جمانرب ىلع ءماع ءرطن

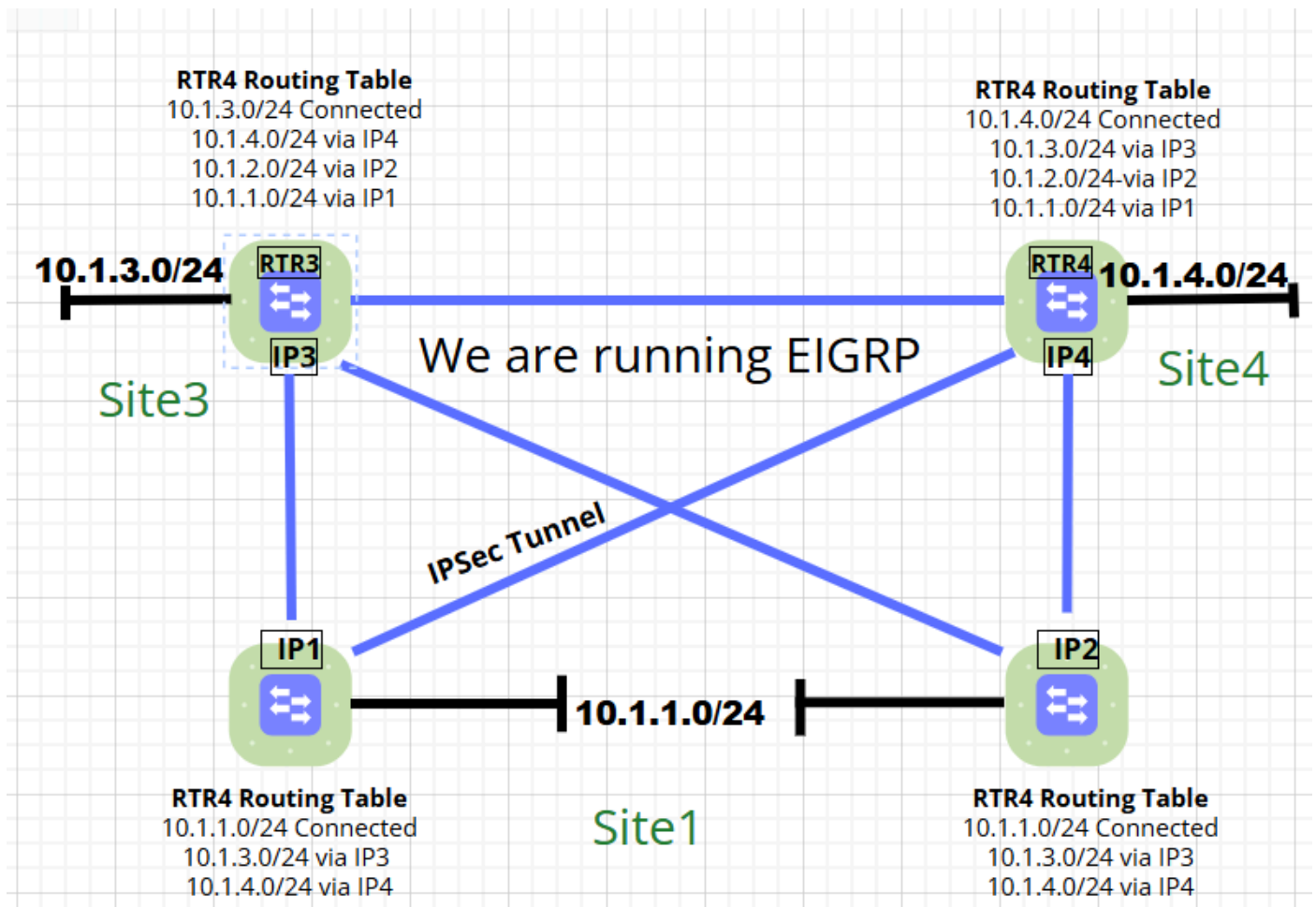
SD-WAN Catalyst مكحتلا ءدحو عم طقف تاراسملا كراشي Cisco SD-WAN Edge زاھج نإف ، فرعت امك مھ صاخلا هيجوتلا ءداعا لودج يف هتيبثت متي و اھل اص راسملا نوكتي كل WAN.

- نأ بجي هنأ يأ ،لوصول الالباق (TLOC) ةيالاتال ةوطخلال لقن عقوم ددحم نوكتي نأ بجي TLOC. ل حيص راسم ىلع Edge زاهج يوتحي
- نوكت يكل .طشن هيلإ ريشي يذلا (TLOC) لقنلال ىلإ لوصولال يف مكحتال رصنع ةطبترم ةطشن (BFD) هاجتالال ةيئانث هيجوت ةداعإ ةسلج نوكت نأ بجي ،ةطشن TLOC ةسلج عاشنإ ىلإ يدؤي امم زاهج لك ةطساوب BFD لمع تاسلج عاشنإ متي .اذه TLOC عم ةسلج تحبصأ اذا .دعب نع لوصولال يف مكحتال تادحو نم ةدحو لك عم ةلصفنم BFD لمع تاراسم عيمج ةلازاب موقت Cisco Catalyst SD-WAN مكحتال ةدحو نإف ،ةطشن ريغ BFD هيجوتال ةداعإ لودج نم TLOC كلذل ىلإ ريشت يتال OMP .راسم لصفأك OMP راسم باسح بجي

لوكتورب نيب ريبك فالتخأ دجوي ،ةرشابمو ةيقتنم تارابعال هذه عيمج نأ نم مغرلا ىلع هيجوت لوكتورب لثم ةيديلقتال هيجوتال تالوكتوربو (OMP) ةحوتفملا ةمظنألا ةرادا لشفال تاهويراني س ءانثأ (OSPF) الاو راسم رصقأ حتفو (EIGRP) نسحملال يلخادلا ةرابعال

EIGRP لشف ويراني س

تاهجوم ىلع يوتحت Site4 ، و Site3 ، و Site1 ، عقاوم ةثالث كانه ،ةيالاتال ةكبشلا يف لوكتورب ليغشت متي .دحاو WAN لاصتا عم يلاوتال ىلع RTR4 ، و RTR3 ، و RTR1/RTR2 ، ههجاو IP نيوانع يه IP4 ، و IP3 ، و IP2 ، و IP1 ، و IPsec ربع يديلقتال لوكتوربلل EIGRP .ةلباقملا عقاوملا يف WAN ةكبش



رمي RTR3 ، يف يلاحال تقولا يف RTR3 و RTR4 ىلع زيكرتال عم ،ةكبشلا ميسقت بجي ،الطعم قفنلا ناك اذا .RTR3-RTR4 نيب رشابم قفن ربع 10.1.4.0/24 ىلإ لوصولال قيرطال

EIGRP موقيس ،قننل رايهنا درجم ب ةلالحا هذه في EIGRP لعف در نو كيس في كف دودرلا ىل ا ادانتساو ،10.1.4.0/24 ةكبش ل ةرواجم ل ا هجوم ل ىل ا مالعسا لاسراو ليغشتب لصفأ رشن يذلا هيجوتل لودج في ةهوجلل ديدجل راسم ل تبثيو هصح في ،ةاقلتم ل راسم ل ل باسح .

نإف يلاتلابو .ةيديلقتل هيجوتل لوكوتورب براق ةيلمعل اء طيسب حرش اذه :ةكبش ل باسح ةءاع ىل ةرداق EIGRP لثم امومع ةيديلقتل هيجوتل لوكوتورب

- ةهوجلل ىل ا لالحا راسم ل راهني ام دنع
- ام ةهوجلل نولبقم ءافلخ كانه نكي مل اذا
- ططخم ل في ريغت ثودح دنع

OMP لشف ويرانيس

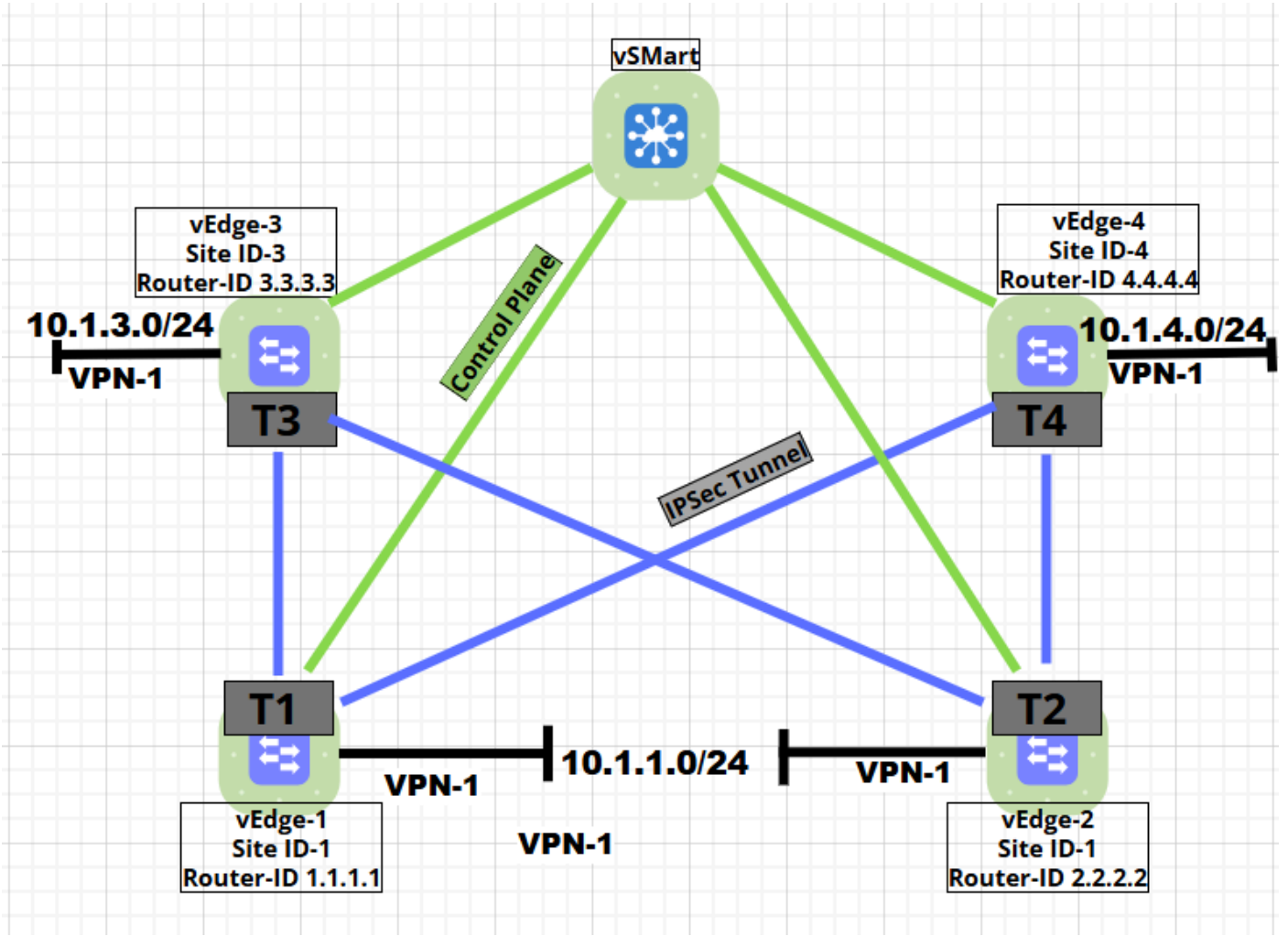
:عيراشم ل ةرادا جم انرب في لشفلل ناهو ويرانيس انه شقان يو

1. رشابم لشف
2. رشابم ريغ لشف

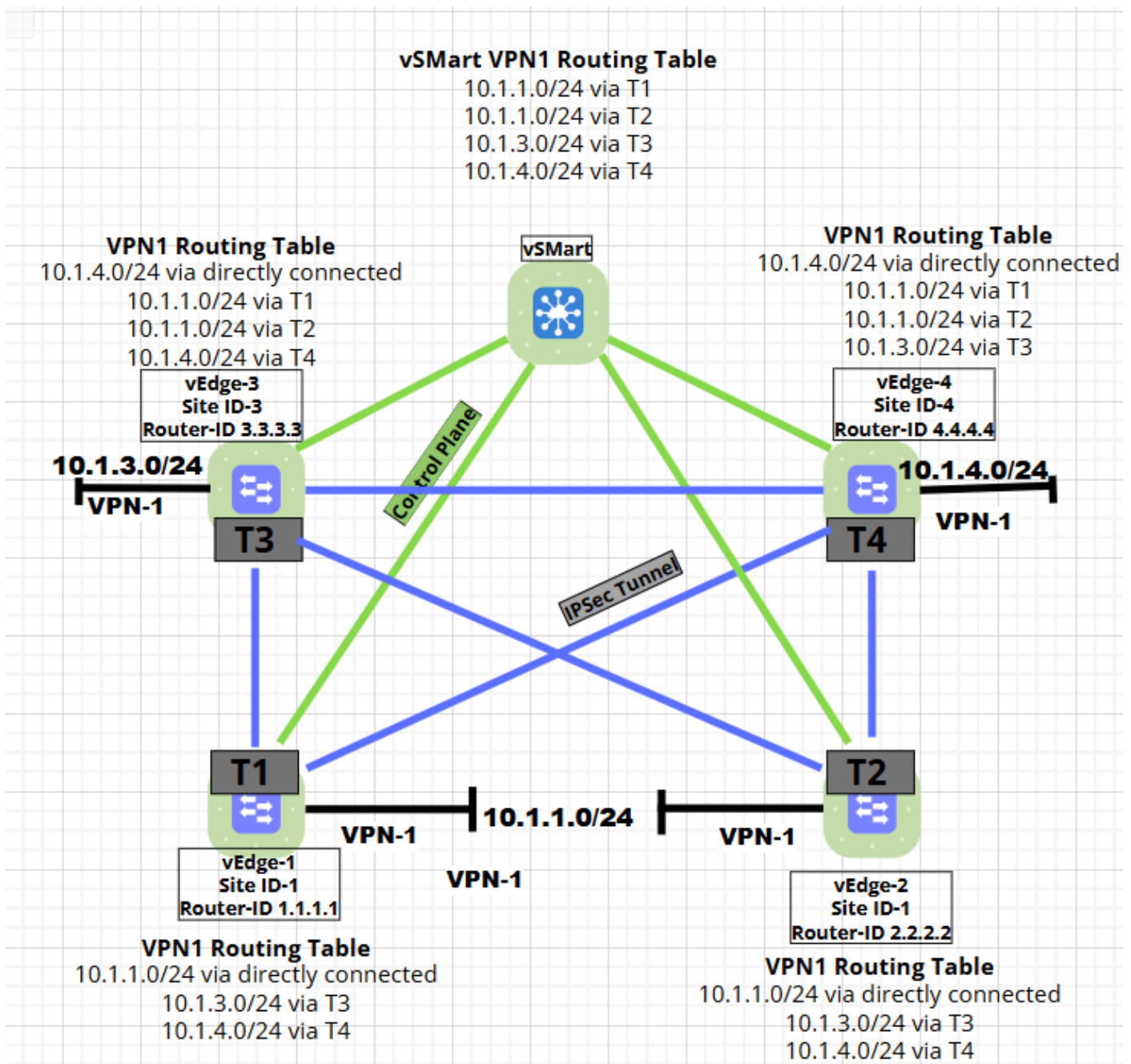
رشابم لشف

.دحاو لقن لاصتا عم عقاوم ةثالث كانه ،يلاتل ططخم ل في

ةكبش ةيعرف	IP ماطنلل	عقوم ددحم لقنل (TLOC)	هجوم ل	عقوم
10.1.1.0/24	1.1.1.1	T1	vEdge-1	Slte1
	2.2.2.2	T2	vEdge-2	
10.1.3.0/23	3.3.3.3	T3	vEdge-3	3-تياس
10.1.4.0/24	4.4.4.4	T4	vEdge-4	4-عقوم



هذه موقت. مكحت زاهج SD-WAN ةزافح ةداملا ىل ع ريصقت ىل نىعم ءيش لك نأ ضرثفإ ةدحو اهكراشتو، Catalyst SD-WAN مكحتلا ةدحو عم ةرشابم هيچوتلا تامولعم ةكراشمب vEdge تاهجوملا عيمجل هيچوتلا لودج يلاتلا ططخمل ضرعي. vEdge ههجا عيمج عم مكحتلا



قوف ةسلج BFD لك ،ايلاح

vEdge-DC1# show bfd sessions

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP
1.1.1.1	1	up	mpls	mpls	60.1.1.1
2.2.2.2	1	up	mpls	mpls	60.1.1.1
4.4.4.4	2	up	mpls	mpls	60.1.1.1

vEdge-DC1# show omp routes vpn 20 | t

Code:

C -> chosen

I -> installed

Red -> redistributed

Rej -> rejected

L -> looped
 R -> resolved
 S -> stale
 Ext -> extranet
 Inv -> invalid
 Stg -> staged
 IA -> On-demand inactive
 U -> TLOC unresolved

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
20	10.1.1.0/24	2.2.2.2	43	1005	C,I,R	installed	1.1.1.1	
			2.2.2.2	37	1006	C,I,R	installed	
20	10.1.3.0/24	0.0.0.0	66	1005	C,Red,R	installed	3.3.3.3	
20	10.1.4.0/24	2.2.2.2	45	1006	C,I,R	installed	4.4.4.4	

تاسلج ل طعتتس ف ، قف نلا عطقني ام دنع ف ، vEdge3 و vEdge4 ني ب لاصتالا لي طعتت مت اذا
 تاراسملا يلع "حل اص ريغ" عمال ع عضو ي ف ببست ي اذهو . اضيأ vEdge3 و vEdge4 نم لك لمع
 ي لالتل جارخلال ي ف كلذ ىرت نأ كنكمي . "لولحم ريغ TLOC" و قلابقملا

vEdge3# show bfd sessions

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP
1.1.1.1	1	up	mpls	mpls	60.1.1.1
2.2.2.2	1	up	mpls	mpls	60.1.1.1
4.4.4.4	4	down	mpls	mpls	60.1.1.1

vEdge3# show omp routes vpn 20 | t

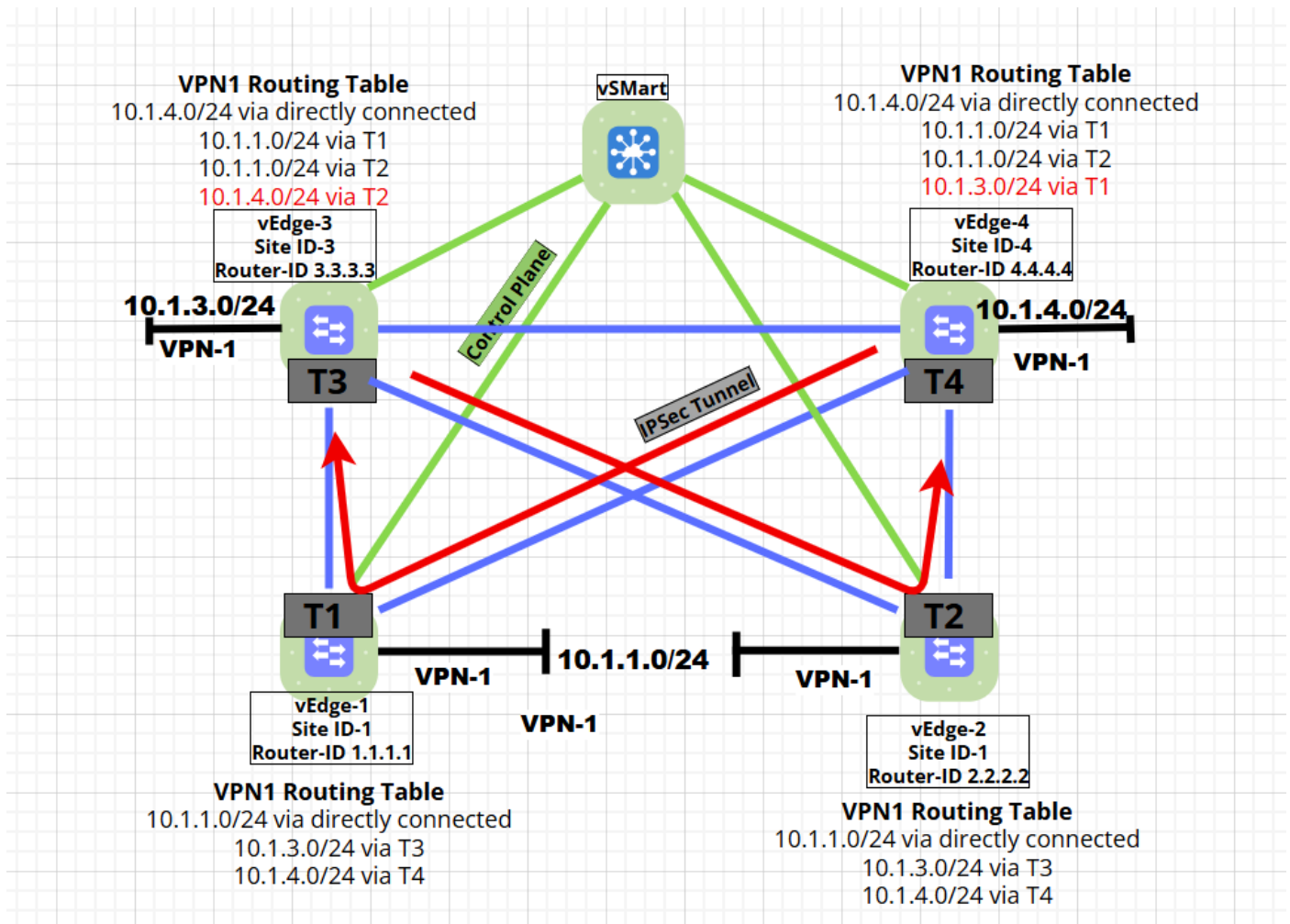
Code:

C -> chosen
 I -> installed
 Red -> redistributed
 Rej -> rejected
 L -> looped
 R -> resolved
 S -> stale
 Ext -> extranet
 Inv -> invalid
 Stg -> staged
 IA -> On-demand inactive
 U -> TLOC unresolved

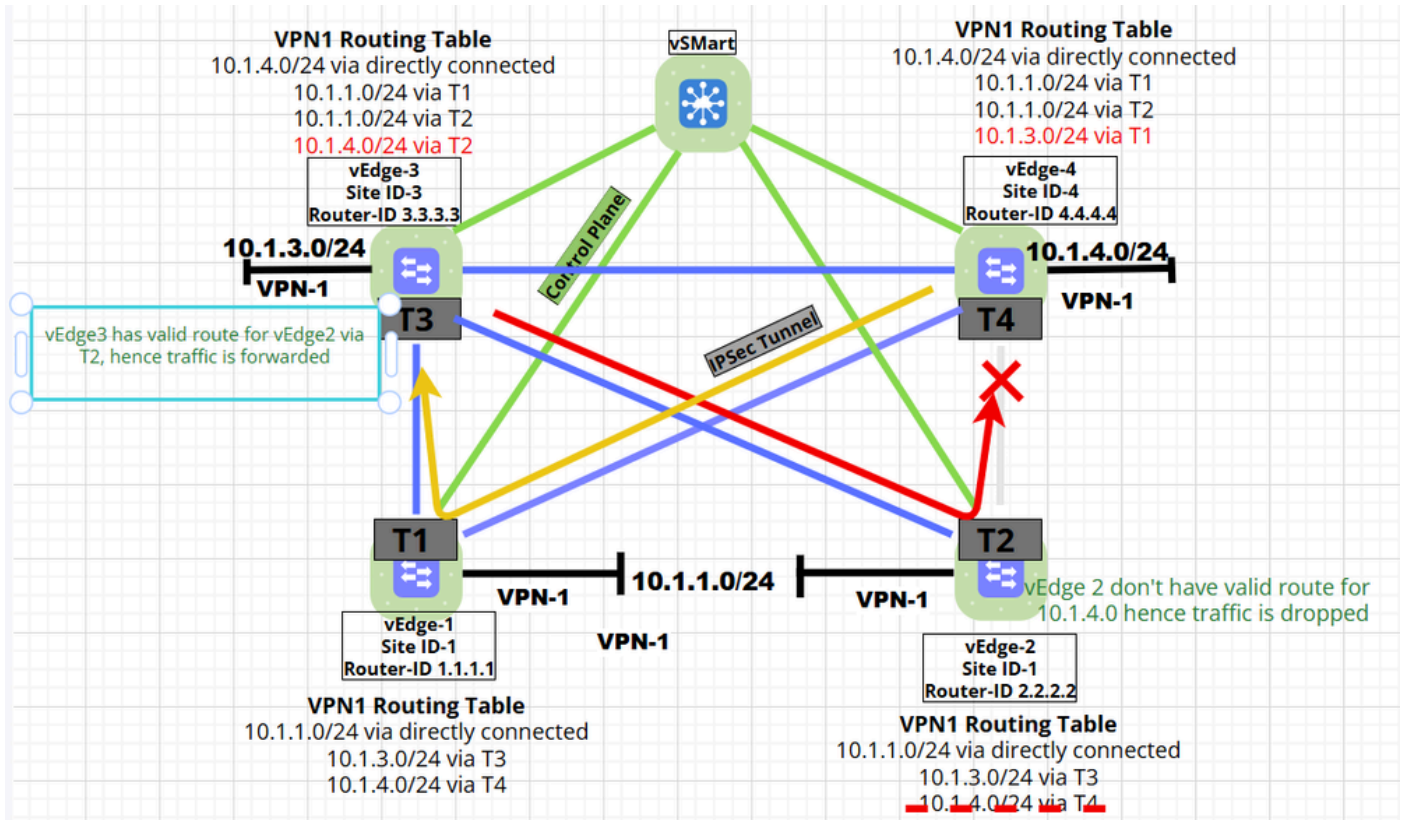
VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
1	10.1.1.0/24	2.2.2.2	43	1005	C,I,R	installed	1.1	
			2.2.2.2	37	1006	C,I,R	installe	
1	10.1.3.0/24	0.0.0.0	66	1005	C,Red,R	installed	3.3.3.	
1	10.1.4.0/24	2.2.2.2	45	1006	Inv,U	installed	4.4	

رشابم ريغ لشف

ةيلاتال ةوطخلال ريغيغل مكحتال جهن فيرعت مت هنا ضررتفا، "رشابملا ريغ لشفل" مهفل ل ةيلاتال ةوطخلال ريغيغل متي vEdge4 ىلعو، vEdge2 ربع 10.1.4.0/24 راسملا ل vEdge3 ىلع vEdge 3 و 4 و vEdge 3 و 4 نيب تانايبال رورم ةكرج جارد مت، ىرخأ تاملكبو. 10.1.3.0/24 ىل vEdge1. ةيلاتال يطي طختال مسرلا في كلذ ىرت نأ كنكمي. ةطيسو تالقنك 1 و 2



امنيب، vEdge2 و vEdge4 نيب لاصتال نادقف ىللا يديوي ةكبشلا في لشف كانه ناك اذا ربع 10.1.4.0 ل حلاص راسم هيذل vEdge3 لازي الف، اطعم T2-T4 نيب يعرفال قفنلا نوكي حلاص قفن ىلع vEdge2 يوتحي ال. vEdge2 ىل تانايبال رورم ةكرج لسري هناف مت نمو. T2 رورملا ةكرج طقس تيلاتالابو هيلع ةطشن تاراسملا نوكت نل كلذل، vEdge4 عم



يولي امب جات ننتس الال نكمي ، ةقباس الال تارابتخال الال و تالجل الال ال ادانتس

- ةيل الال طاقن الال و هي جوت الال عارظن ل يئاقلت فاشتكا دجوي ال OMP م ادختس اب
- قفن رايهن دن ع اي جول و بوط الال باسح ةداع دجوي ال
- ث دحي يذال دي حولا ريغيغ الال . قفن ل طعت دن ع ادبأ ةه جولا ةئداب الال OMP قرط ريغت الال TLOC ، يأ ، ةيل الال ةوطخل الال ل وصولا ةيناكم او
- ةه جولا الال ددعت م قفن راركت ريغوت بجي ، ةرشابم الال ةيشغت الال لشف ةلاح ي ف اهسفن
- زواج الال راسم ي ف ةطس و تم الال تا و طخل الال / م يدقت عانثا رذحل نم ديزم الال ي غوت بجي رورم ةكرح دوجو مدع بنجتل قفن الال راركت ريغوت بجي و

يلع هي جوت الال ةداع او باسح الال ةداع اب OMP موقوي ال ، يضا رتفا لكشب هنأ نال فرعت تنأ نذا نم 'TLOC-Action' يمست ةزيم ني كمت كنكمي ، ةلكشم الال هذه يلع بلغلل . ةيشغت الال لشف م كحت الال جهن لال

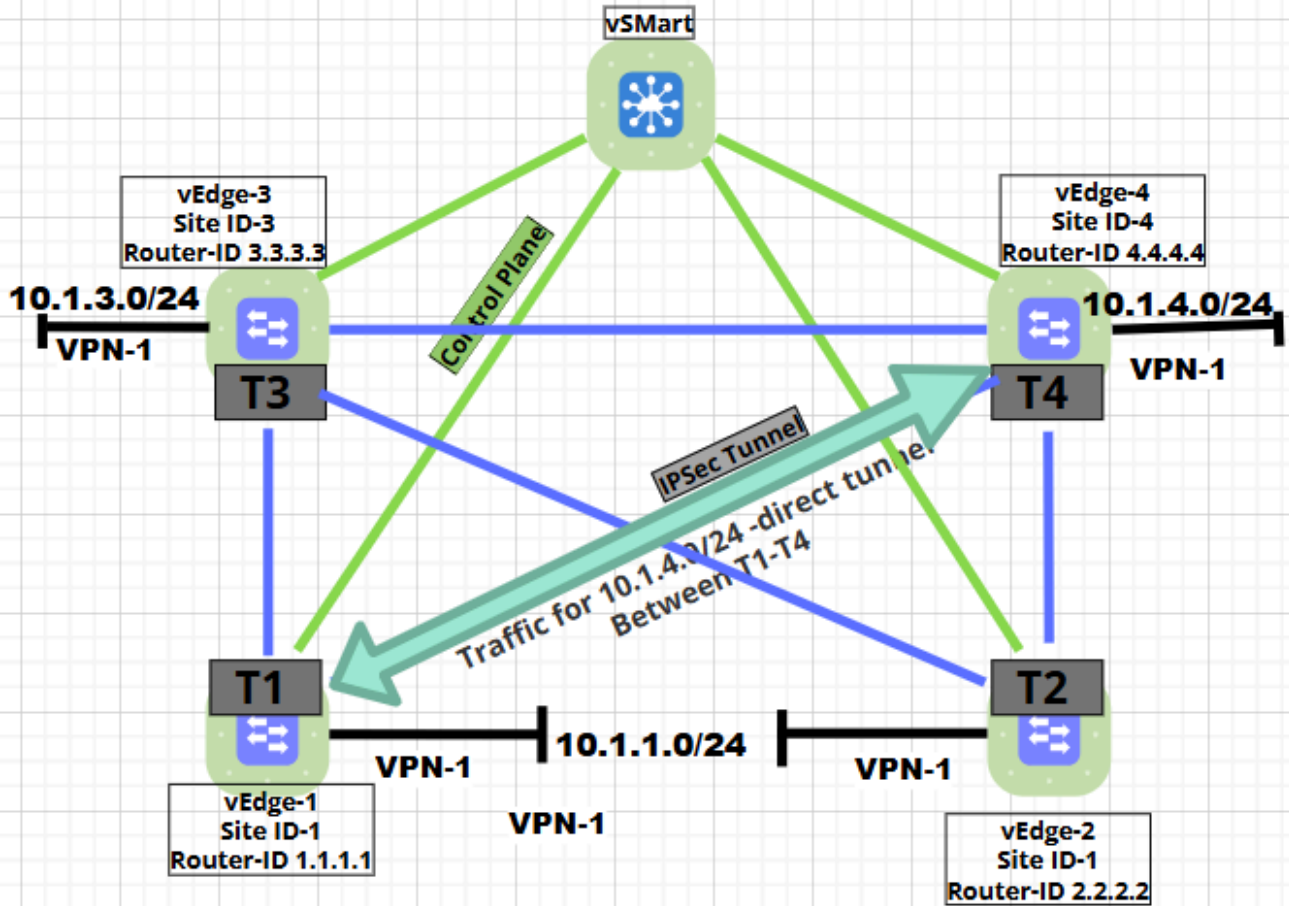
نشك-كولت

- ةطس و تم ةوطخ لاداب م كحت الال ةسايس نمض 'TLOC' عارجل حمسي Cisco SD-WAN ي ف ةيؤرل ةيناكم يلع طا فحل عم رورم الال ةكرح هي جوت ةداع الال م ادختس م تي يكل (TLOC) ني كمت TLOC عارجل رايخ ني يعيت ينع ي اذه . ةه جولا الال ردصم الال نم لم اك الال راسم الال ي ف الال راسم الال ةي هن الال ةي هن نم عبتت الال عارجل نم Cisco Catalyst SD-WAN م كحت الال ةدحو WAN ةفاح تاهجوم مالع اب م كحت الال ةدحو موقت ، راسم الال اذه راهن اذا . ةيئاهن الال ةه جولا زاهج اذه OMP راسم تقلت ي الت
- يلع لم عي امم ، يساس الال طابترالال لشف ةلاح ي ف يطايتح ا خسن راسم رفوي وهو SD-WAN . ةكبشل ةي عرف الال ةكبشل ل ل خاد لاطع الال ةه جومو ةكبشل الال ةنورم ني سحت لال نم ةكبشل الال نم تاناي بل رورم ةكرح هي جوت ةي ف ي ف م كحت الال ةقيرط

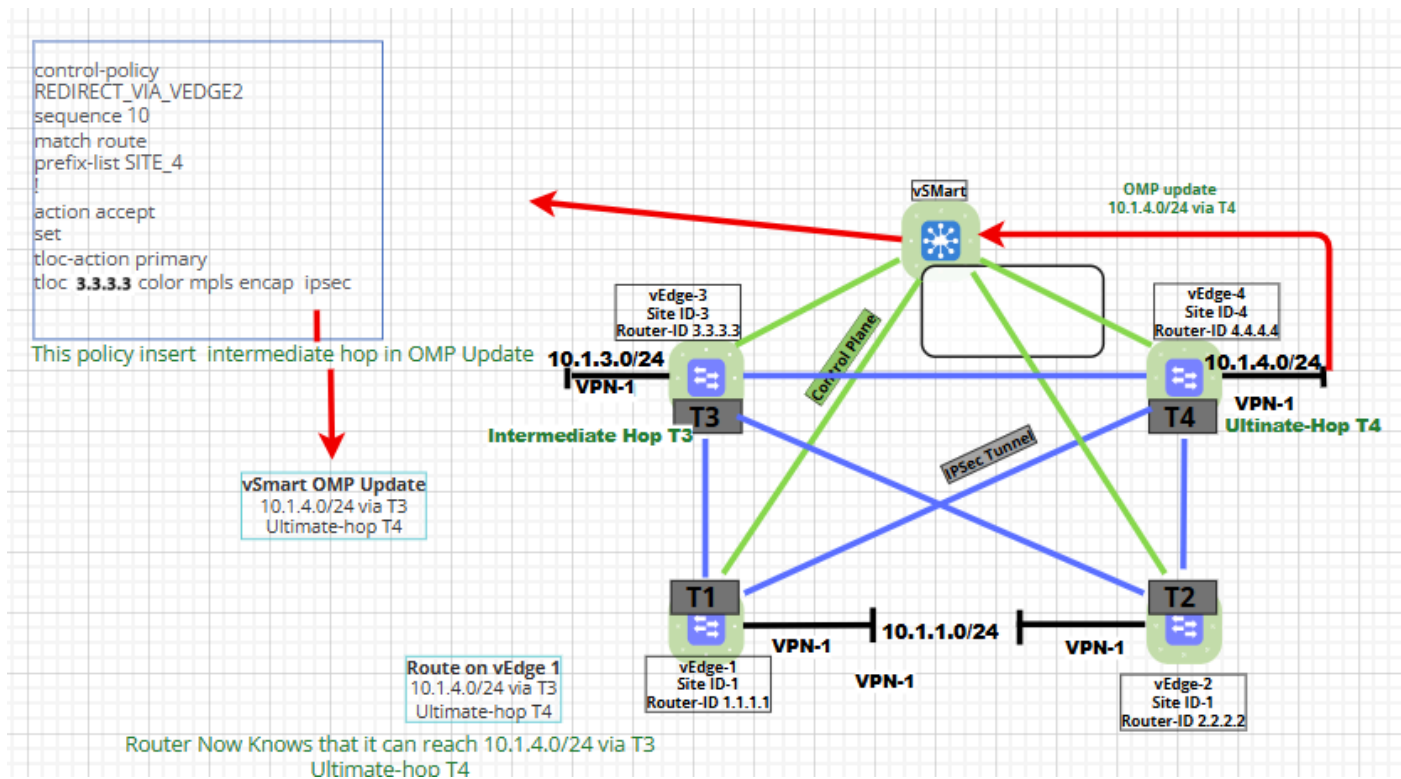
ىلإ لوصول ل ةمدختسم ل (TLOCs) لقنلإ ىلإ لوصولأ ف مكحتلأ مئوق ةجلأعم ةهوجلأ.

- TLOC جاردل SD-WAN مكحت ةدحو دشرى هنإف، ةسايس ف TLOC ءارجا ديدحت دن ع قوم ىلإ الوأ لقتنت فوس رورملا ءكر نأ ينعي امم، راسملا باسح ف طسوتم رملأ مزل اذا ةيئاهنلا ةهوجلأ ىلإ لوصولأ لبق ددحملأ "يطايتحالأ خسنلأ" راهنأ اذا ىتح لاصتالأ نامض اهف ديرت يتلأ تاهوي رانيسلل صاخ لكشب ديفم اذهو فلتخم راسم ربع ايئاقلت تانايبلا رورم ءكر هيجوت ةداعل لالخنم، يساسأ طابترا (ةدحملأ (TLOC) لقنلأ ىلإ لوصولأ ف مكحتلأ ةدحو ربع).

vEdge2 و vEdge3 و vEdge4 مداوخ ىلع زيكرتلأ كنكمي، ةيلاتلأ ايجولوبطلاب قلعتي امي ل تانايبلا رورم ءكر رمت امك، ةسايس يأ ديدحت ايلاح متي ال. لصفأ لكشب اهمهفل T3 و T4 نيبرشابم قفن ربع vEdge3 ىلع 10.1.4.0/24.



ةداعل مكحتلأ ةسايس نيوكت مت، ءكبشلأ ءنورمولاطعألأ ةهجاوم ىلع ءردقلأ ري فوتل (TLOC) لقنلأ ىلإ لوصولأ ف مكحتلأ ةدحو ربع) فلتخم راسم لالخنم رورملا ءكر هيجوت (ةدحملأ).



- عوطخل عم 10.1.4.0/24 ةرشابم ةلصتلم هتكبش ل OMP ثي دحت vEdge4 لسري 'T4 ربع 10.1.4.0/24' ةئيه يلع Catalyst نم SD-WAN مكحتل ةدحو يلى T4 ةئيه لالتل.
- SD-WAN مكحتل ةدحو يلع اهنيوكت مت يلى مكحتل ةسايس عم راسم اذه قباطتي جري هنأ، هيلع ددحمال جهنلل اقبط نيديديج TLOC-ACTIONS و TLOC نيغي و SD-WAN "TLOC" ديجل.
- نيئيلات نيئطقن مادختساب vEdge1 لى OMP هجوم نع نالعالاب مكحتل ةدحو موقت نم T4-ةئيه لالتل ةلحرمال) ةئيه لالتل TLOC ةدحو (3.3.3.3 و T3) ةطيسول TLOC ةدحو - نالال لوصول نكمي 10.1.4.0/24 ةئيه لالتل نأ vEdge1 ل ءاكذ يطي اذهو. (يلصلال راسم) T4 ربع و T2 ربع اهليل.

10.1.4.0/24 ل تانايبال رورم ةكره هيجوت ةداع vEdge1 ددحمال TLOC-Action يلع ءانب نالال مكحتل يوتسم ةسايس في TLOC-ACTIONS نم ةعبرالال ءاونالال هذه ديديجت كنكمي كلذل:

1. بجي vEdge1 و vEdge4 نيئ رورم ةكره نأ "TLOC-Action Strict" ددحي - (يضارتفا) دي قم قفنل راهنأ اذا طقس ت نأ بجي رورم ةكره نأ و (ةطسولم ةلحرمال) T3 ربع نوكت نأ بجي vEdge1 و vEdge4.
2. ربع رمت vEdge1 و vEdge4 نيئ رورم ةكره نأ "TLOC-Action primary" ددحي - يساسأ في مكحتل ةدحو موقت، يعرفال قفنل اذه فاقاي مت اذو T3 (3.3.3.3) ةطسولم ةوطخل T4 لى رشابم قفنل ربع تانايبال رورم ةكره هيجوت و vEdge1 مالعاب SD-WAN رورم ةكره نأ "TLOC-Action" ةيلمعل يطايتحالال خسنالال" ددحي - يطايتحالال خسنالال ةئيه لالتل LOC ةطقن لى ةرشابم لقننت vEdge1 و vEdge4 رادصلال نيئ تانايبال نيئ رشابم يعرفال قفنل فاقاي مت اذو (يلصلال راسم ل T4-ةئيه لالتل ةوطخل) vEdge1 رادصلال غلبت SD-WAN ةكبش في مكحتل ةدحو ناف، vEdge1 و vEdge4 رادصلال T3 ةطيسول ةوطخل ربع تانايبال رورم ةكره رمت و
4. هنأ "TLOC ءارجالاب صاخال ECMP" ددحي - (ECMP) ةفلكتل ةيواسم تاراسم الددعتم لالال نم لمحال نزاوتم vEdge1 و vEdge4 نيئ لالصالال نوكتي، ةيداعال فورظال في T4 ةئيه لالتل ةوطخلال و T3 ةطسولم ةلحرمال.

ةمچرتل هذه ل و ح

ةيلآل تاي نقتل ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج 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 ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط 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 م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا