

จัดสรรเส้นทางรับส่งข้อมูลแบบสแตติกเราติง

แก้ปัญหาบนเน็ตเวิร์กที่มีเส้นทางเพื่อสำรองด้วย Self-Tunnel

เวลาใช้สแตติกเราติงในเน็ตเวิร์กโทโพโลยีที่มีเส้นทางสำรอง (Redundant Path) หากสมมติว่าอินเทอร์เฟซแลนของเราเตอร์ฝั่งตรงข้ามขัดข้องก็อาจทำให้เครือข่ายแลนทั้งสองฝั่งถูกตัดขาดจากกันได้ แม้ในกรณีที่โพรโตคอล HSRP (Hot Standby Router Protocol) ได้รับการคอนฟิกไว้ที่เราเตอร์แล้วก็ตาม คุณสมบัติต่างๆ ของ Cisco IOS Software ฟีเจอร์ 12.3 ขึ้นไปอย่าง Object Tracking for Reliable Static Routing Backup หรือ Tunneling (การสร้างอุโมงค์รับส่งข้อมูล) ระหว่างไอเอสพี (ผู้ให้บริการอินเทอร์เน็ต) กับหน่วยงานที่อยู่ในระยะไกลอาจช่วยแก้ปัญหาได้ แต่หากคุณใช้ IOS รุ่นก่อนหน้าฟีเจอร์ 12.3 ซึ่งขาดคุณสมบัติดังกล่าวก็ยังมีทางเลือกในการใช้สแตติกเราติงส่วนๆ แก้ปัญหานี้ได้เช่นกัน

สิ่งที่เกิดขึ้นเมื่ออินเทอร์เฟซแลนขัดข้อง

จากภาพที่ 1 ISP1 และ ISP2 คือเราเตอร์ฝั่งไอเอสพี ซึ่ง ISP1 เป็นเราเตอร์ที่เปิดใช้ HSRP ซึ่งได้รับการคอนฟิกคำสั่ง track บนอินเทอร์เฟซแลน (Serial0/0) ด้วยนโยบายของไอเอสพีรายนี้จะอนุญาตให้ทำเฉพาะสแตติกเราติงไปยังไซต์ลูกค้าโดยห้ามทำ Tunneling เด็ดขาด ส่วน CUST1 และ CUST2 ก็คือเราเตอร์ฝั่งลูกค้าซึ่ง CUST1 ได้รับการคอนฟิกเป็นแอสท์พีเราเตอร์

ในภาวะปกติ ทราฟฟิกทั้งหมดซึ่งมีปลายทางอยู่ที่ 10.26.248.0/24 จะวิ่งผ่าน ISP1 (ซึ่งได้รับการคอนฟิกสแตติกเราติง: ip route 10.26.248.0 255.255.255.0 ser0/0) แต่เมื่ออินเทอร์เฟซแลนของ CUST1 ขัดข้อง ISP1

จะไม่รับรู้ และทำหน้าที่ส่งแพ็กเก็ตไปยัง CUST1 ผ่านแวนลิงก์ของมันต่อไป เนื่องจากว่าไม่มีกลไกใดที่คอยโอนหน้าที่ส่งทราฟฟิกอื่นนี้จาก ISP1 ไปยัง ISP2 ไซต์ทั้งฝั่งไอเอสพีกับลูกค้าจึงถูกตัดขาดจากกัน วิธีหนึ่งที่จะกอบกู้สถานการณ์โดยไม่ต้องรบกวนไอเอสพี คือให้ปิด CUST1 เสีย ซึ่งทำให้แวนลิงก์ที่เชื่อมต่อกับ ISP1 ดาวน์ และ ISP2 จะกลายเป็นแอสท์พีเราเตอร์แทน จากผลของคำสั่ง track

แก้ปัญหาด้วย Self-Tunnel

แต่เพื่อความสะดวกในการแก้ปัญหาข้างต้น เราขอแนะนำเทคนิคใหม่ที่เรียกว่า “Self-Tunnel” (ภาพที่ 2) ซึ่ง Self-Tunnel นี้หมายถึงอุโมงค์รับส่งข้อมูลที่มีต้นทางและปลายทางอยู่ในเราเตอร์เดียวกัน ขอให้เพิ่มบรรทัดคอนฟิกเรชันต่อไปนี้ที่ CUST1:

```
interface Loopback6000
ip address 10.26.247.1 255.255.255.252
! see note
!
interface Tunnel1000
ip address 10.26.247.9 255.255.255.252
backup interface ser0/0
tunnel source 10.26.247.2
tunnel destination 10.26.247.2
no keep-alive
!
interface Tunnel2000
```

```

ip address 10.26.247.13 255.255.255.252
backup interface Loopback6000
tunnel source 192.168.60.61
tunnel destination 192.168.60.61
no keep-alive
!
Interface FastEthernet0/0
Ip address 10.26.248.202 255.255.255.0
Standby 1 ip 10.26.248.201
Standby 1 preempt
Standby 1 priority 105
Standby 1 track Serial0/0

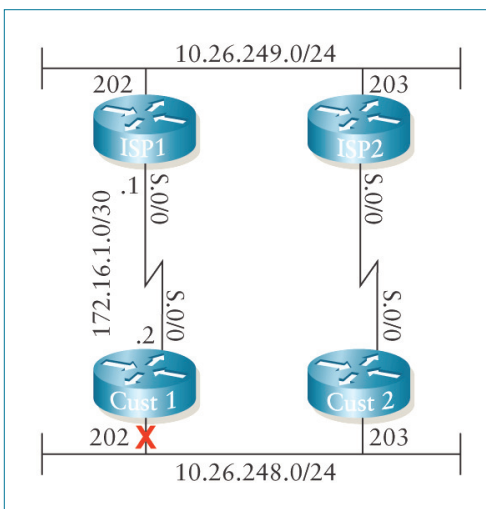
Interface Serial0/0
Ip address 172.16.1.2 255.255.255.252 (omitted)

ip route 192.168.60.60 255.255.255.252
FastEthernet0/0 ! This subnet is used only
to change Tunnel2000 interface status.

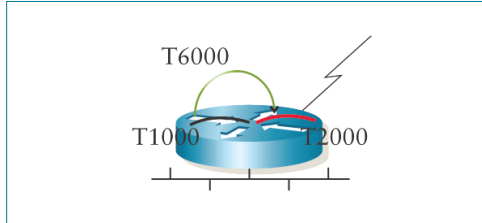
ip route 10.26.249.0 255.255.255.0 172.16.1.1

```

เพื่อให้กลไกนี้ทำงานอย่างถูกต้อง Loopback6000 จะต้องไม่เป็นสมาชิกของเมเจอร์เน็ตเวิร์กที่ CUST1 สามารถเราต์ได้ (นั่นคือไม่ควรมีดีฟอลต์เราต์หรือสแตตติกเราต์ที่ชี้ไป 10.26.247.0 ที่มีซัพเน็ตมาสก์ < 30 ปรากฏอยู่ ตัวอย่างเช่น หากเอ็นทรี 10.26.0.0/16 ปรากฏอยู่ในเราดิงเทเบิล Tunnel1000 ก็จะแอ็กทีฟตลอด ซึ่งขัดขวางกลไก Self-Tunnel ไม่ให้ทำงาน)



ภาพที่ 1: ไซตักทั้งสองฝั่งจะถูกตัดขาดจากกันทันที เมื่ออินเทอร์เฟซแวนของ CUST1 ชัดข้อง



ภาพที่ 2: Self-Tunnel จะมีต้นทางและปลายทางอยู่บนเราเตอร์เดียวกัน

ในภาวะปกติ Tunnel2000 จะแอ็กทีฟเมื่อสแตตติกเราต์ที่ชี้ไป 192.168.60.60/30 ปรากฏอยู่ในเราดิงเทเบิล (ซึ่งเป็นจริงตราบที่ Fa0/0 แอ็กทีฟ) อีกทั้งคำสั่ง backup interface ของ T2000 จะทำให้ Loopback6000 ยังคงดาวนอยู่ เพราะเหตุนี้ Tunnel1000 ก็จะดาวนไปด้วย (เพราะลูปแบ็กนี้เป็นทั้งต้นทางและปลายทางของอุโมงค์) และ Serial0/0 ก็จะแอ็กทีฟ (เพราะ Serial0/0 ทำหน้าที่เป็นแบ็กอัฟอินเทอร์เฟซของ Tunnel1000)

แต่ถ้าเมื่อใด FastEthernet0/0 เกิดขัดข้อง สแตตติกเราต์ข้างต้นจะถูกลบออกจากเราดิงเทเบิล และ T2000 ก็จะดาวน ส่งผลให้ Loopback6000 กลับมาแอ็กทีฟพร้อมกับ T1000 และในที่สุด Ser0/0 จะดาวนด้วยผลของคำสั่ง backup interface

นอกจากนี้ภายหลังกลไกทำงาน ซีเรียลอินเทอร์เฟซของ ISP1 ก็จะดาวนลงเช่นกัน ซึ่งกระตุ้นให้สถานะของ HSRP เปลี่ยนจาก active เป็น standby ด้วยผลของคำสั่ง track ที่คอนฟิกไว้บนซีเรียลอินเทอร์เฟซ เพราะฉะนั้น ทราฟฟิกขาเข้าจะเปลี่ยนไปวิ่งผ่าน ISP2 ซึ่งตอนนี้เป็นแอ็กทีฟเราเตอร์ตัวใหม่แทน

ตัวอย่างนี้เป็นเพียงสถานการณ์ง่าย ๆ ซึ่งในเน็ตเวิร์กโทโพโลยีที่ซับซ้อนขึ้น คุณอาจจำเป็นต้องประยุกต์ใช้เทคนิคอื่นด้วยนอกเหนือจาก Self-Tunnel เช่น การคอนฟิกไดนามิกโพรโตคอลใน CUST1-2 เพื่อทำ Recursive Lookup ในเน็ตเวิร์กโทโพโลยี เป็นต้น ■