Dynamic Buffer Limiting

ครั้งแรกของวงการ! ด้วยเทคโนโลยีป้องกันภาวะจราจรติดขัดแบบ Flow-based บนฮาร์ดแวร์ความเร็วสูง ซึ่งใช้ในผลิตภัณฑ์ของซิสโก้เป็นเจ้าแรก

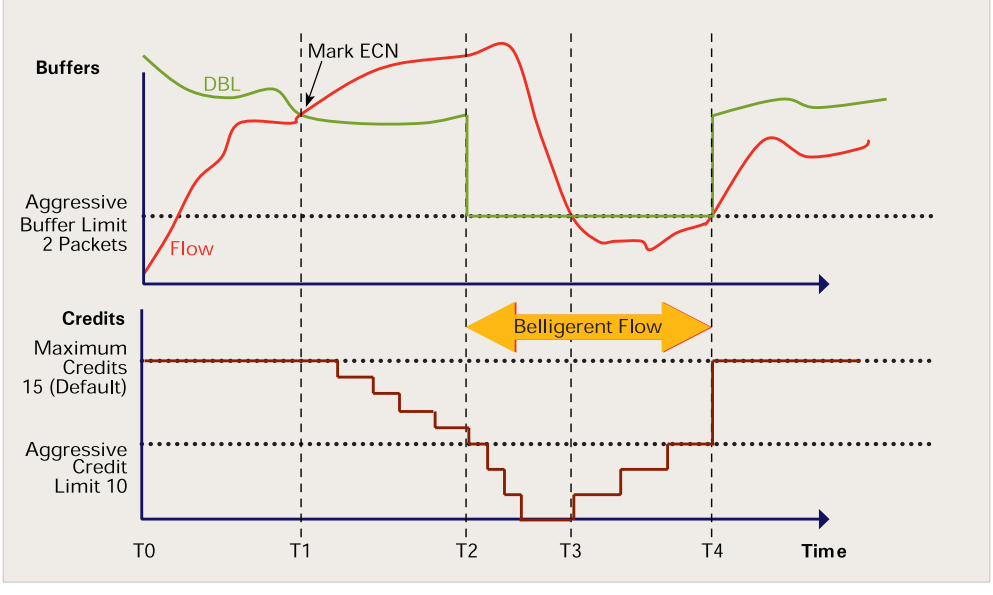
นวัตกรรม ใหม่ของซิสโก้ที่มีชื่อว่า Dynamic Buffer Limiting หรือ DBL คือเทคโนโลยีลดภาวะจราจรติดขัดแบบ Flow-based ตัวแรกของโลกที่ออกแบบมาเพื่อฝังในฮาร์ดแวร์ โดยการทำงานบนทุกพอร์ตของสวิตช์ Cisco Catalyst 4500 Series เทคโนโลยี DBL จะสามารถรู้จัก และจำกัดปริมาณการไหลเวียนของทราฟฟิกที่มีความประพฤติผิดปกติได้ โดยเฉพาะอย่างยิ่งทราฟฟิกที่ไม่ตอบสนองกับการติดขัดเมื่อถูกดร็อปแพ็กเก็ตทิ้งไป (ส่วนมากเป็นโฟลว์ของแพ็กเก็ต UDP) ทั้งนี้ DBL จัดเป็นเทคนิคมัลติโพรโตคอลที่สามารถตรวจสอบเนื้อหาของฟิลด์ในเลเยอร์ 2, 3 และ 4 ได้

DBL ให้คุณสมบัติ Active Queue Management แบบ On-demand ได้โดยวิธีตรวจวัดความยาวคิวของแต่ละทราฟฟิกโฟลว์ (Traffic Flow) ในสวิตช์ เมื่อความยาวคิวของโฟลว์ใดโฟลว์หนึ่งนั้นมีค่าเกินขีดจำกัด DBL ก็จะดร็อปแพ็กเก็ต หรือทำเครื่องหมายพิเศษที่ฟิลด์ ECN (Explicit Congestion Notification) ในเฮดเดอร์ของแพ็กเก็ต เพื่อเซิร์ฟเวอร์จะสามารถจัดการโฟลว์ดังกล่าวได้ถูกต้องในสภาวะที่เกิดภาวะจราจรติดขัดขึ้น โดยปกติโฟลว์ที่ไม่ได้รับการทำเครื่องหมายพิเศษ ซึ่งนิยมเรียกว่า Non-adaptive Flows นั้นบริโภคแบนด์วิดธ์มหาศาล และการใช้พื้นที่บัฟเฟอร์ของสวิตช์มากขนาดนี้ ทำให้แอพพลิเคชันของเอนด์ยูสเซอร์ทำงานช้าลง ส่งผลถึง QoS ที่ย่ำแย่ลงด้วย

เนื่องจาก DBL ได้รับการบรรจุลงในวงจร ASIC แยกเฉพาะ การส่งต่อแพ็กเก็ตที่ความเร็ว Wire-speed จึงสามารถเป็นไปได้ โดยที่สมรรถนะของตัวสวิตช์ไม่ได้ลดลง

ภาพที่ 1: ต่อไปนี้ คือกุญแจไขปริศนาวิธีทำงานของ DBL สำหรับโฟลว์ทั่งๆ โดยสวิตช์จะคอยจัดการเรื่องจำนวนเครดิตคงเหลือ และบัฟเฟอร์ไปพร้อมกัน

HOW DBL WORKS



แม้แต่น้อย ทั้งนี้ Cisco Catalyst 4500 Series หนึ่งตัวให้อัตราเร็วการสวิตช์ข้อมูลที่ 136 กิกะบิตต่อวินาที และอัตราการส่งต่อแพ็กเก็ตที่ 102 ล้านแพ็กเก็ตต่อวินาที ซึ่งเทคโนโลยี DBL ถือว่าสำคัญอย่างยิ่งต่อเครือข่ายทั้งในส่วน Edge Network, Core Network และ Distribution Network

ยิ่งเร็วยิ่งต้องระวัง

ทุกวันนี้ระบบเครือข่ายในองค์กรขนาดใหญ่ได้รับการประกอบขึ้นโดยใช้อุปกรณ์ที่มีแบนด์วิดธ์สูงมากๆ (กิกะบิตต่อวินาที) และมีสมรรถนะในการส่งต่อแพ็กเก็ตที่เยี่ยมมากๆ (เมกะแพ็กเก็ตต่อวินาที) เป็นหลัก แต่ยิ่งระบบเครือข่ายมีแบนด์วิดธ์มากเท่าใด กลไก QoS ที่มีประสิทธิภาพก็ยิ่งเป็นเรื่องที่จำเป็นมากขึ้นเท่านั้น โดยเฉพาะกับเครือข่ายกิกะบิตอีเธอร์เน็ตซึ่งสามารถถ่ายโอนข้อมูลที่อัตราเร็วถึง 1,000 เมกะบิตต่อวินาที ขณะที่เครือข่าย WAN T1/T3 ดั้งเดิมมีอัตราเร็วเพียง 1.55 หรือ 45 เมกะบิตต่อวินาที หากปราศจากระบบป้องกันที่ดีพอ ปริมาณผู้ใช้แบนด์วิดธ์ที่ยิ่งมากจะยิ่งเป็นตัวถ่วง QoS ให้ทำงานแย่ลง เช่น สัญญาณเสียงของ VoIP จะด้อยคุณภาพอย่างเห็นได้ชัด เมื่อมีการระดมยิงทราฟฟิกโฟลว์เข้าสู่เครือข่ายอย่างไม่ขาดสาย และ QoS จะเริ่มเสียศูนย์ เมื่อโฟลว์ที่ยิงเข้ามานั้นก่อให้เกิดการปฏิเสธการให้บริการ (Denial-of-Service- DoS) กับทราฟฟิกที่ประพฤติตัวปกติ

ทราฟฟิกโฟลว์ประเภทรุกราน (Belligerent Flow) จะวิ่งด้วยความเร็วสูงมาก และไม่ยอมลดอัตราการไหลใดๆ ทั้งสิ้น เมื่อเครือข่ายส่งให้ดร็อปแพ็กเก็ต ตัวอย่างเช่น

- Thick UDP flows: การดาวน์โหลดภาพยนตร์จากอินเทอร์เน็ตคือตัวอย่างของโฟลว์ที่มีความหนาแน่นสูง ซึ่งต้องการไดนามิกบัฟเฟอร์มากๆ (อัตราส่งบิตสูง) เปรียบเทียบกับกรณีที่ผู้ใช้ล็อกอินเข้าเราเตอร์ผ่าน Secure Shell ซึ่งไม่ต้องการอัตราส่งบิตสูงนัก (โฟลว์ความหนาแน่นต่ำ) หรือสัญญาณเสียงพูดก็เป็นอีกตัวอย่างของโฟลว์ความหนาแน่นต่ำ ซึ่งต้องจัดลำดับการส่งอยู่ในลำดับแรกๆ เป็นต้น

- Spanning Tree, IP Multicast loops: ลูป Spanning Tree มักกินเวลาประมาณ 30 วินาที ขึ้นอยู่กับปริมาณแบนด์วิดธ์ที่ใช้บนเครือข่าย (ของอัพลิงก์ เป็นต้น)

- Streaming Multimedia: นิยมใช้บนแอพพลิเคชันอินเทอร์เน็ตทั่วไป

หลักการพื้นฐานของ DBL

หากจะเอ่ยถึงสถานการณ์ที่ใช้อธิบายการทำงานของ DBL ได้นั้น คงหนีไม่พ้นการสอบใบอนุญาตขับขี่ของพลเมืองสหรัฐฯ ที่เมื่ออายุเข้าตามเกณฑ์และผ่านการสอบข้อเขียนแล้ว ผู้สมัครจะต้องเข้าสอบภาคปฏิบัติเพื่อให้ได้ใบอนุญาตขับขี่ยานพาหนะ Class C ทั้งนี้ ผู้สมัครจะมีคะแนนเริ่มต้น 100 แต้ม แล้วค่อยๆ ถูกหักตามจำนวนความผิดที่ก่อ (เช่น จอดรถไม่เข้าซอง ขับรถเร็วเกินข้อกำหนด ฯลฯ) ถ้าคะแนนที่ถูกหักไม่เกิน 30 แต้ม ถือว่าผู้นั้นสอบผ่าน

เทคนิค DBL สำหรับลดภาวะจราจรติดขัดก็มีหลักการคล้ายกัน แต่แทนที่จะหักแต้ม DBL จะหักเครดิต (Credit) ของทราฟฟิกโฟลว์ที่ประพฤติตัวรุกราน โดยในภาวะจราจรติดขัดระยะแรกจะไม่มีการดร็อปแพ็กเก็ตใดๆ และฟิลด์ ECN ในแพ็กเก็ตตัวใดตัวหนึ่งจะถูกทำเครื่องหมายไว้ เพื่อเปิดโอกาส (หรือเตือน) ให้ทราฟฟิกโฟลว์นั้นปรับปรุงพฤติกรรม หรือล่าถอยโดยไม่สูญเสียแพ็กเก็ตไปมากกว่าที่เป็นอยู่

ระบบปฏิบัติการลีนุกซ์ และโซลารีส 9 สนับสนุนการทำงานของฟิลด์ ECN โดยแต่ละโฟลว์จะมีเครดิตเริ่มต้นที่ 15 เครดิต (ผู้บริหารระบบสามารถปรับเพิ่มลดได้) และค่อยๆ ถูกหักลดลงไป ทั้งนี้ DBL จะคำนวณค่าขีดจำกัดต่างๆ แบบไดนามิกโดยพิจารณาจากโฟลว์ ไม่ใช่จากแพ็กเก็ตทั้งหมดที่อยู่ในคิว ซึ่งนั่นคือข้อแตกต่างที่ชัดเจนระหว่าง DBL กับเทคนิค WRED (Weighted Random Early Detection)

ดังแสดงในภาพที่ 1 สวิตช์จะสังเกตพารามิเตอร์สองค่าควบคู่กันสำหรับทุกๆ โฟลว์ที่วิ่ง ได้แก่ จำนวนเครดิตและปริมาณบัฟเฟอร์ เมื่อโฟลว์ใช้ปริมาณบัฟเฟอร์เกินค่าขีดจำกัดที่คำนวณไว้ DBL (เริ่มทำงาน ณ T1) DBL จะทำเครื่องหมายในฟิลด์ ECN หรือดร็อปแพ็กเก็ตหนึ่งตัวทิ้ง หากโฟลว์ไม่สนใจและยังคงส่งแพ็กเก็ตในอัตราเท่าเดิมอยู่ โฟลว์นั้นก็จะถูกหักเครดิตทีละหนึ่งจนหมด

โฟลว์ใดโฟลว์หนึ่งจะได้รับการจัดเข้าหมวด "**รุกราน**" ต่อเมื่อเครดิตมีค่าน้อยกว่าขีดจำกัดที่คำนวณไว้ และจังหวะนี้ ปริมาณการใช้บัฟเฟอร์จะถูกบีบให้เหลืออยู่ที่ค่าขีดจำกัดที่จัดไว้สำหรับทราฟฟิกรุกรานโดยเฉพาะ ส่วนในทางกลับกัน ณ เวลา T3 เมื่อโฟลว์ปรับพฤติกรรม และใช้บัฟเฟอร์น้อยกว่าขีดจำกัดที่คำนวณไว้ จำนวนเครดิตจะค่อยๆ เพิ่มขึ้นจนครบ 15 เครดิตเหมือนเดิม

การเซตคอนฟิกูเรชัน DBL

การเซตคอนฟิกูเรชันของ DBL ใน Cisco IOS นับว่าง่ายมาก (ดูภาพที่ 2) โดยสวิตช์ของซิสโก้จะใช้อินเทอร์เฟซ MQC (Modular QoS Command-Line Interface) ร่วมกับคีย์เวิร์ด "dbl" สำหรับการแมพโพลิซี นอกจากนี้

คอนฟิกูเรชันของ ECN ยังสามารถใช้ได้ทุกที่ กล่าวคือมีความเป็น Global ส่วนพารามิเตอร์ของบัฟเฟอร์ และเครดิต ทั้งหมดที่กล่าวไปข้างต้นจะแสดงได้โดยใช้คำสั่ง show qos dbl

กระบวนการ DBL จะทำงานร่วมกับคิวการส่งโฟลว์สี่คิวบนแต่ละพอร์ต (รวมแล้วเท่ากับ 1500 กว่าคิว ในกรณีของสวิตช์ Cisco Catalyst 4510R) และที่สำคัญคือ DBL สามารถจัดการโฟลว์บนพอร์ตประเภทอะไรก็ได้ เช่น Switched, Routed, Trunk, Access หรือ EtherChannel เป็นต้น

DBL ลดผลการเกิดลูป Spanning Tree

ภาพที่ 3 แสดงให้เห็นสมรรถนะของเครือข่ายที่ดีขึ้น ในยามที่จำลองการเกิดลูป STP (Spanning Tree Protocol) ในห้องทดลอง ซึ่งหากปราศจาก DBL แล้วโฟลว์ TCP จะมีอัตราไหลช้าลง และโฟลว์ความเร็ว 70 เมกะบิตต่อวินาทีที่ไม่เกิดลูปจะเหลือทรูพุตเพียง 26.5 เมกะบิตต่อวินาทีหรือคิดเป็นร้อยละ 37 จากเดิมเท่านั้น แต่เมื่อใช้ระบบ DBL โฟลว์ที่ไม่เกิดลูปจะมีทรูพุตสูงขึ้นเป็น 69 เมกะบิตต่อวินาที (ร้อยละ 99) เลยทีเดียว

DBL, AutoQoS, และ WRED

ด้วยพอร์ตกว่า 50 ล้านพอร์ตที่ใช้กันทั่วโลกขณะนี้ ย่อมเป็นเครื่องยืนยันความสำเร็จของสวิตช์ Cisco Catalyst 4500 Series ซึ่งเป็นผลจากสถาปัตยกรรมแบบรวมศูนย์และการปรับคอนฟิกูเรชันด้วยชุดมาโครที่ใช้ง่ายได้อย่างดี ตัวอย่างของมาโครประเภทนี้ ได้แก่ AutoQoS ที่สามารถปรับคอนฟิกูเรชัน DBL กับ QoS บนแต่ละพอร์ตได้โดยอัตโนมัติ และองค์กรนับพันๆ แห่งยังใช้ AutoQoS ร่วมกับ DBL ในระบบ VoIP ของตนด้วย

สำหรับ WRED ซึ่งเป็นเทคนิคการจัดการคิวแบบแอ็กทีฟ (Active Queue Management) ยอดนิยมอีกหนึ่งตัวนั้นก็สามารถทำงานร่วมกับ DBL บนเครือข่ายได้ทุกสภาวะแวดล้อม ข้อแตกต่างที่สำคัญระหว่าง DBL และ WRED คือ DBL นั้นเป็น Flow-based ถ้าเกิดจราจรติดขัดขึ้นลอจิกในฮาร์ดแวร์จะดร็อปแพ็กเก็ตทิ้งโดยคิดคำนวณตามโฟลว์ที่ผ่านเข้ามา

นอกจากนี้ ระดับการมีส่วนร่วมให้เกิดจราจรติดขัดของแต่ละโฟลว์ยังจะได้รับการพิจารณาร่วมกันด้วย ยกตัวอย่างเช่น ถ้าจราจรติดขัดเกิดขึ้นที่พอร์ตอัพลิงก์อีเทอร์เน็ตความเร็ว 10 กิกะบิตต่อวินาที แพ็กเก็ตเสียงที่เป็น UDP ก็จะเป็นเป้าหมายที่ DBL สนใจมากกว่าแพ็กเก็ตเสียงพูดหรือเทลเน็ต เนื่องจากเสียงใช้ปริมาณบัฟเฟอร์มากกว่า แต่อย่างไรก็ตาม DBL จะทำงานต่อเมื่อท่อส่งข้อมูลเต็มเท่านั้น เช่น กรณีที่มีข้อมูลไหลเกินกว่า 20 กิกะบิตต่อวินาทีบนพอร์ตอีเทอร์เน็ตแชนแนลคู่ความเร็ว 10 กิกะบิตต่อวินาที เป็นต้น

DBL คือเทคนิคหลีกเลี่ยงภาวะจราจรติดขัด ซึ่งรองรับหลายโพรโตคอล และทำงานในเลเยอร์ 2-4 ที่ช่วยเสริมแกร่งความปลอดภัยของเครือข่าย โดยจำกัดปริมาณการไหลของโฟลว์ประเภทรุกราน และป้องกันการโจมตีแบบ DoS ได้อย่างมีประสิทธิภาพ ทั้งนี้ โฟลว์ประเภทรุกรานมักจะเกิดขึ้นที่บริเวณขอบเครือข่าย ที่ซึ่งสตรีมมิงมีเดีย และแอพพลิเคชันผู้หิวกระหายแบนด์วิดธ์อื่นๆ สามารถก่อปัญหาให้เครือข่ายได้

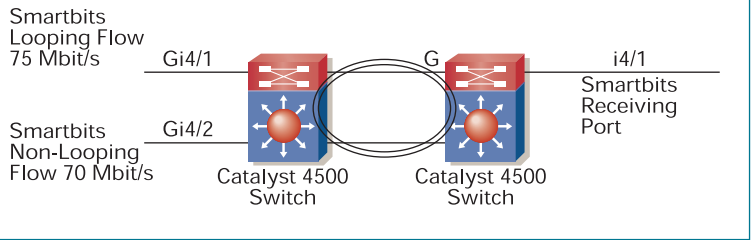
เพราะฉะนั้น สวิตช์ Cisco Catalyst 4500 Series จึงควรถูกจัดวางไว้ที่ขอบเครือข่าย เพื่อให้การปกป้องเครือข่ายจากภาวะจราจรคับคั่งที่ดีพอ สวิตช์ตระกูลนี้จะมี DBL ฝังในตัวฮาร์ดแวร์บน Supervisor ทั้งหมด (ตั้งแต่ Sup2+ ขึ้นไป) พร้อมความสามารถในการส่งต่อข้อมูลที่อัตราตั้งแต่ 64 Gbps/48 Mpps ถึง 136 Gbps/102 Mpps นอกจากนี้ Cisco Catalyst 4948 แบบ Fixed-switch ขนาดเคส 1U ก็มีการสนับสนุน DBL ที่ระดับฮาร์ดแวร์ด้วยเช่นกัน ■

CISCO IOS DBL CONFIGURATION

```
4xxx(cong)#qos dbl
4xxx(cong)#qos dbl exceed-action ecn
4xxx# show qos dbl // Truncated
DBL ow includes layer4-ports
DBL uses ecn to indicate congestion
DBL max credits: 15
DBL aggressive credit limit: 10
```

ภาพที่ 2: พารามิเตอร์ของบัฟเฟอร์ และเครดิตได้รับการแสดงขึ้น

DBL AND SPANNING TREE LOOP



ภาพที่ 3: DBL ช่วยเพิ่มบรรเทาความคับคั่งของจราจรได้มาก ในสถานการณ์ที่เกิดลูป STP

อ่านเพิ่มเติม

- IETF RFC 3168, "The Addition of ECN to IP"
  ietf.org/rfc/rfc3168.txt
- Cisco Catalyst 4500 Series Switches
  cisco.com/packet/181_5b1