ใบงานที่5

การวิเคราะห์แพ็คเก็ตอย่างละเอียด

(แนะนำเทคนิคการเฝ้ามองแเพ็คเก็ตอย่างเป็นระบบ)

จุดประสงค์

1) เพื่อให้เข้าใจเกี่ยวกับการวิเคราะห์แพ็กเก็ตได้อย่างละเอียด

2) เพื่อให้รู้ขั้นตอนวิธีการวิเคราะห์แพ็คเก็ตอย่างละเอียด

3) เพื่อเฝ้าดูแพ็กเก็ตแบบต่อเนื่อง หรือเมื่อต้องการเฝ้ามองทีละ step ได้

Cisco Packet Tracer เป็น โปรแกรมสำหรับ จำลองระบบเครือข่าย (Networking Simulation Tool) ที่ พัฒนา โดย Cisco ช่วยให้นักเรียนสามารถจำลองการเชื่อมต่อของระบบเครือข่าย จำลองการทำงานของ อุปกรณ์จริงในระบบ Network ช่วยอำนวยความสะควกในการเรียนการสอนเกี่ยวกับเทค โน โลยีเครือข่ายที่ ซับซ้อน ช่วยให้นักเรียนสามารถสร้างเครือข่ายที่มีอุปกรณ์ได้ไม่จำกัดจำนวน กระตุ้นให้ฝึกฝน ค้นพบ และ แก้ไขปัญหาต่างๆ เกี่ยวกับระบบเน็ตเวิร์ค

การวิเคราะห์แพ็คเก็ตอย่างละเอียด

Scenario จะนำ lab จากบทความที่แล้วมาใช้ โดยจะเป็นการวิเคราะห์ packet ในโปรโตคอล ICMP และ ARP เริ่มจากนำ lab จากครั้งที่แล้วมาเตรียมไว้



ขั้นตอนแรกก็ใช้ inspect เช็ค device แต่ละเครื่องก่อนว่ามี ARP Table แล้วหรือป่าว ซึ่งตอนนี้ยังไม่การ เรียกใช้โปรโตคอล ARP แต่ละเครื่องก็จะยังไม่มี ARP Table (ARP เป็นโปรโตคอลที่ทำหน้าที่สอบถามว่า หมายเลข IP Address ที่ต้องการติดต่อมีหมายเลข MAC ใด และ Reverse ARP เป็นการถามกลับว่าหมายเลข MAC ที่ต้องการติดต่อตรงกับหมายเลข IP Address ใด)



จากนั้นก็ให้ใช้โหมด Simulation ในการ สังเกตพฤติกรรมการทำงานของแพ็กเก็ต

โดยจะให้ PC0 ping ไปหา Laptop0 (ping 192.168.0.12)

1000	Root	New Cluster Move Clisted	Set Tied Background		Vevport.		Environments	22:00:02
	No. 100		an neo ousgroure	Sinulation Famil Event Lat Via. Time(© 0.000 © 0.000	ec) LastDevice	AtDevice Type PCO ID99 PCO AttP	cashee	
PCD 3P 192,168.0.10 Subnet Mark 255,255,255,0 Subnet PCD 3P 192,168.0.10 Subnet Mark 255,255,0 Subnet PCD P1 192 Subnet P1 193 Subnet P1 192 Subnet P1 193 Subnet P1 193 Sub	PC1 Lay 2.163.0.11 IP 142 et Maek 255.355.255.0 Submit a	000-97 Itap0 I65.0.12 Mark 255.355.255.0		Play Controls Book Downt List Plan AQ, Hite, ARF, 5 HORR, HORP, 45	Auto C a - Vabla Eventa OP, COP, DHCP, DHCP THS, HTTPS, DORB, DO	ebure / Hay	Capture / Forward 95 ED0RPv6, PTR, H. 99 ING, LACP, LLOP,	323, NDF, TF,
Command Promat				SCCR SMTP, SHA	P, SSH, STP, SYSLÖG, At Filters	TACACS, TOI, TPT Sh	9, Tohel, UDP, VTP ox All/None	

จากนั้นโปรแกรมก็จะหยุดการส่ง packet รอจนกว่าเราจะกด Capture/Forward



จะเห็นว่ามีแพ็คเก็ต ICMP และ ARP วิ่งจากเครื่อง PC0 ที่เวลา 0.000 วินาที)

เนื่องจากกำสั่ง ping นั้นใช้หมายเลข IP Address ในการทคสอบ ณ สถานะการณ์ ปัจจุบันเครื่อง PC0 ไม่ ทราบว่าเครื่องเป้าหมาย (192.168.0.12) คือใคร เพราะในตาราง ARP Table ยังไม่มีข้อมูลใคๆ เลย ดังนั้น เครื่อง PC0 จึงส่งแพ็คเก็ต ARP กระจาย ออกไปยังทุกๆ พอร์ตยกเว้นตัวมันเอง (พอร์ต PC0)

แพ็คเก็ต ARP จะส่งต่อไปยัง HUB (เวลา 0.001 ใน Even List)



HUB จะส่งแพ็คเก็ต ARP ต่อไปยัง PC1 และ Labtop0 พร้อมกัน (เวลา 0.002 ใน Even List)



Labtop0 จะตอบกลับ ARP reply กลับมา เนื่องจากเป็นเครื่องที่มี IP Address เท่ากับ 192.168.0.12 แต่ เครื่อง PC1 จะไม่ตอบกลับเพราะไม่ใช่ IP ของตนเอง



HUB จะกระจายแพ็คเก็ตที่ส่งมาจาก Laptop0 ไปยังทุกๆ เครื่องเนื่องจากคุณสมบัติ ของ HUB จะกระจาย ข้อมูลไปยังทุกๆ พอร์ตเสมอ



ในเวลาที่ 0.004 เครื่อง PC0 ก็จะทราบแล้วว่า IP 192.168.0.12 คือใครจึงทำการส่ง ICMP ออกไปยังเครื่อง เป้าหมายทันที

			Viewport			Env	vironment: 21:00:0	00
•	Simulation	n Panel					8×	
	-Event Li	ist						
Ξ	Vis.	Time(sec)	Last Device	At Device	Туре	Info		_
		0.000		PC0	ICMP			
		0.000		PC0	ARP			
		0.001	PC0	Hub0	ARP			
		0.002	Hub0	PC1	ARP			
		0.002	Hub0	Laptop0	ARP			
		0.003	Laptop0	Hub0	ARP			
	۹	0.004	Hub0	PC0	ARP			
	()	0.004	Hub0	PC1	ARP		×	
	3	0.004		PC0	ICMP			
	Reset Sir	mulation 🔽	Constant Delay	/			Captured to: _* 0.004 s	

เมื่อถึงขั้นตอนนี้ ARP Table ของเครื่อง PC0 และ Labtop0 ก็จะถูก Update

ł





เวลาที่ 0.005 เครื่อง PC0 ส่ง ICMP อีกครั้งไปยัง HUB

เวลาที่ 0.006 HUB จะกระจายแพ็กเก็ต ICMP ไปยังทุกๆ พอร์ต (กุณสมบัติของ HUB)



Constraint	.ist					
10.	Time(sec)	Last Device	At Device	Туре	31152	
	0.002	Hubb	PC1	ARP		
	0.002	Hub0	Digotige.J	ARP		
	0.003	Lapitop0	Hub0	ARP		
	0.004	Hub0	PC0	ARP		
	0.004	Hub0	PCI	ARP		
	0.004	-	PC0	1CMP		1
	0.005	PC0	Hab0	ICMP		
া প্ৰচ	0.006	Hub0	PC1	ICMP		
192	0.006	Hub0	Laptop0	XMP		
least S	mulation 😨	Constant Dala	ŵ.		Ca	ptured to 0.006
Ray Cr	introls					
	Back	Auto	Capture / Play		Capture / Pr	France
			0			
lay Co	vritrols Back	Auto	Capture / Play		Capture / Pi	FAR

เวลาที่ 0.007 Labtop0 ส่งแพ็คเก็ต ICMP reply กลับไปยัง HUB



					st	Eventu
1	Info	Type	At Device	Last Device	Time(sec)	15.
		ARP	Laptop0	Hub0	0.002	
		ARP	Hub0	Laptop0	0.003	
		ARP	PC0	Hub0	0.004	
		ARP	PC1	Hub0	0.004	
		ICMP.	PCO	++ .	0.004	
1		ICMP.	Hubo	PC0	0.005	
		ICMP	PC1	Hub0	0.005	
		ICMP	Laptop0	Hubo	0.006	
		ICMP	Hub0	Laptopů	0.007	
Captured to: 0.007 s			r.	onstant Dela	mulation [2]	leset Si
					ntrola	Play Co
# / Parward	Centur		aptare / Play	Auto	Back	-
			15			-

เวลาที่ 0.008 HUB จะกระจายแพ็คเก็ต ICMP ไปยังทุกๆ พอร์ต (คุณสมบัติของ HUB)

		110	Event1	int.					
		1	Vir.	Tirse(sec)	Last Device	At Device	Type	Info	
1000			1	0.004	Hub0	PCD	ARP		
PHD _				0.004	Hubt	PCI	ARP		
Faich.or				0.004	+	PCD	10MP		
				0.005	PC0	Hub0	XHP		
//	N			0.006	Hubo	PC1	10P		
	1			0.006	Hub0	Laptop0	10HP		=
				0.007	Laptop0	Hub0	1046		
FeQ				0.008	Hubb	PCD	XMP		
4	FeO			0.008	Hub0	PC1	IONP		+
2			Reset Si	inulation 🔽	Constant Dela	y .			Ceptured to: . 0.008 s
PCI	Laptop0		Play Co	ntos					
192.168.0.11	IP 192.168.0.12		1.000	Dack	Auto	Capiture / Plan	1	Capiture	Porward
Mask 255.255.255.0	Subnet Mask 255,255,255,0		-			1			
			Event1 ACL Filte HSRR, HS NETFLOV SCCP, SM	Jat Filters - Vi r, ARP, BGP, C RIPv6, HTTP, V, NTP, CSPF, TTP, SNMP, SS	able Events DP, DHCP, DHC HTTPS, 10MP, 12 OSPFV6, PAgP, H, STP, SYSLOG	Pv6, ONS, DT CMPv6, IPSec POP3, PTP, I	P, EIGRE , ISAKM RADELIS, OP, TFTP	R, EIGRP R, Ioë, L REP, RJ	v6, FTP, H-323, ACP, LLOP, NDP, P, RJPhg, RTP, LLOP, VTP
				20 A 2 A 4				Contraction of the	

การเชื่อมต่อก็จะสำเร็จลง เมื่อทำการ ping ครั้งที่ 2 แพ็คเก็ตก็ยังคงเดินทางไปหาทุก เครื่อง เหมือนเดิม (ตอบกลับเฉพาะเครื่องที่เป็นเป้าหมายเท่านั้น) เพราะคุณสมบัติของ HUB นั้นจะส่งไปยังทุกๆ พอร์ต แต่จะไม่เกิดกระบวนการ ARP ครั้งที่ 2 จนกว่า จะถึง เวลาที่ ARP Cache expire ซึ่งจะใช้เวลา ประมาณ 10 นาที (600 วินาที)

IP 192-168-0-10 Subnet Neek 255-255-2



การวิเคราะห์แพ็คเก็ตใน Scenario 3 ได้ทำการวิเคราะห์ทิศทางการส่งข้อมูล สำหรับใน Scenario 4 นี้ จะพิจารณาแพ็คเก็ตใน ระดับที่ลึกซึ้งลงไปถึงระดับบิตข้อมูล Scenario ก็จะ ใช้ lab จาก Scenario 2 เช่นเดิมครัชช

แผนผังการเชื่อมต่อ :



เริ่มต้นที่เครื่อง PC0 โดยการใช้คำสั่ง ping จาก Command Prompt ไปยังเครื่อง Labtop0 อีกครั้ง



ในโหมด Simulation เมื่อออกกำสั่ง ping แล้ว ให้ใช้ Inspect ตรวจสอบแพ็กเก็ต ที่มี รูปเป็นซองจดหมาย



จากรูปข้างบนการสื่อสารข้อมูลในเน็ตเวิร์คจะแบ่งออกเป็นชั้นๆ ตามหลักการของ OSI Model จาก ในตัวอย่าง แพ็คเก็ตของ ICMP นั้นจะถูกซ่อนอยู่ ใน IP (encapsulation) เพื่อให้แพ็คเก็ต IP นั้นเป็นผู้ส่งแพ็ค เก็ต ICMP ไปให้ถึงปลายทาง ข้อมูลของ ICMP จะเป็นข้อมูลในส่วนของ DATA ใน IP แพ็คเก็ต โดย ICMP แพ็คเก็ตมี ขนาคเท่ากับ 32 บิต x 2 คือ 64 บิต ประกอบไปด้วย Type มีขนาค 8 บิต เอาไว้บอกว่าเป็น โพรโท กอล ICMP ชนิค Echo Request, CODE มีค่าเท่ากับ 0, CHECKSUM เป็นค่าที่ใช้ สำหรับตรวจสอบความ ผิดพลาดของข้อมูล, ID มีค่าเป็น 2, SEQ NUMBER คือลำดับของ แพ็คเก็ต ซึ่งจะเปลี่ยนไปเรื่อยๆ ในที่นี้คือ 1



จากรูปข้างบน แสดงข้อมูลของแพ็คเก็ต ARP ที่อาศัยโพร โทคอล Ethernet (ทำงานในเลเยอร์ที่ 2) ส่งไปยังปลายทาง ข้อมูลที่อยู่ใน DATA ของ Ethernet frame จะเป็นแพ็คเก็ตของ ARP มีข้อมูลคือ HARDWARE TYPE=1, PROTOCOL TYPE=0x800, HLEN=ความยาวของ Header, PLEN=ความยาวของ เนื้อข้อมูล, OPCODE=0x1, SOURCE MAC=48 บิต, SOURCE IP=32 บิต (192.168.0.10), TARGET MAC=48 บิต (เริ่มต้นจะต้องทำการกระจายข้อมูลไปทุกๆ เครื่อง โดยใช้ MAC=000.000.000), TARGET IP=32 บิต (192.168.0.12) สังเกตุว่าใน Ethernet frame จะ DEST MAC= FFF.FFF.FFF แสดง ว่าเป็นการ broadcast ข้อมูลไปทุกๆ เครื่อง

เมื่อเครื่องปลายทางได้รับแพ็คเก็ตแล้วจะส่ง ARP Reply กลับไปยังเครื่องที่ส่งข้อมูลมา โดยการ update ค่า SOURCE MAC, SOURCE IP, TARGET MAC, TARGET IP ในARP frame



ก่าของ SOURCE IP เป็น 192.168.0.10 และ TARGET IP เป็น 192.168.0.12 เมื่อ ตอบกลับ จะสลับก่าเป็น SOURCE IP เป็น 192.168.0.12 และ TARGET IP เป็น 192.168.0.10 เช่นเดียวกัน ก่าของ MAC ก็จะสลับ ตามหมายเลข IP สำหรับแพ็กเก็ตอื่นๆ ก็ จะสามารถสังเกตุได้ด้วยวิธีการเดียวกัน

เทคนิคการเฝ้ามองแเพ็คเก็ตอย่างเป็นระบบ

ขั้นตอนแรกให้เลือก End Device -> ลาก generic pc กับ generic server ไปวาง



ทีนี้ให้เลือก connection เป็น Copper Straight Through (เส้นสีดำไม่มีเส้นประ) ทำการเชื่อมต่อ เลือก port เป็น FastEthernet





แต่จะเห็นว่า link เป็น สีแดง ที่เป็นแบบนี้เพราะว่าเลือก สาย ผิด อิอิ ต้องเปลี่ยนใหม่เป็น Copper Cross Over แทน ลบสายเดิมได้โดยการ กดที่ ปุ่ม delete สีแดง



สถานะของถิ่งค์จะเป็นสีเขียว แสดงว่าใช้งานได้แล้ว





ทคลองเปิด-ปิด device ได้ โดนดับเบิลกลิกที่ pc ไปยังแท็บ physical แล้วกดที่ ปุ่ม power ตามรูป

จากนั้นทดลองตรวจสอบค่าของเครื่อง PC และ Server โดยใช้ Inspect คลิกที่เครื่อง ทั้งสอง ให้ทำการ ตรวจสอบ ARP Table, Port Status Summary Table และ DNS Cache Table







ตอนนี้ ARP Table, Port Status Summary Table และ DNS Cache Table จะยังไม่มีค่าใดๆ config อยู่ ต่อไปจะเป็นการกำหนด IP Address ให้กับ device ทำได้โดยการ ดับเบิลคลิก ที่ pc แล้วไปที่แท็บ config

PC-PT PC0	Physical Config Desktop Attributes Software/Services GLOBAL Settings Algorithm Settings INTERFACE FastEthernet0 Display Name PC0 Gateway/DNS IPv4 DHCP Static Gateway/DNS Server 0.0.0 Gateway/DNS IPv6 DHCP Auto Config Static IPv6 Gateway IPv6 DNS Server 	Global Settings
--------------	--	-----------------

กำหนด DNS Server เป็น 192.168.0.105

	control unaction control control control
GLOBAL Settings Algorithm Settings INTERFACE FastEthernet0	Global Settings Display Name PC0 Gateway/DNS IPv4 DHCP
	Static Gateway DNS Server 192.168.0.105
	Gateway/DNS IPv6 DHCP Auto Config Static IPv6 Gateway IPv6 DNS Server

เลือกอินเทอร์เฟสชนิด FastEthernet ให้กำหนด IP Address เป็น 192.168.0.110

0.084		FastEthernet0
Settions	Port Status	▼ 0
Abovithan Settinge	Bandwidth	(ii) 100 Mbps (iii) 10 Mbps V Aut
INTERFACE	Duplex	Half Duplex Full Duplex Aut
FastEthernet0	MAC Address	0001.6403.D550
	IP Configuration	
	© DWCP	
	Static	
	IP Address	192.168.0.110
	Subnet Mask	255.255.255.0
	IPv6 Configuration	
	C DHCP	
	Auto Config	
	Static	
	IPv6 Address	/
	Link Local Address: FE80::201:64EE:EE03:D59	0

แล้วทคสอบโดยใช้ Inspect (ยกเลิก Inspect ให้กดปุ่ม esc) อีกครั้ง ที่ Port Status จะปรากฎหมายเลข MAC Address และ IP Address



เมื่อต้องการกำหนดค่า Bandwidth,Duplex, DHCP, IPv6 ก็สามารถกำหนดได้ในเมนูนี้เช่นเดียวกัน การ กำหนดค่า IP Address, Subnet Mask, Default Gateway, DNS Server สามารถกำหนดได้ ใน แท็บ Desktop >> IP Configuration ได้เช่นเดียวกัน

ขั้นตอนต่อไป ให้แก้ไขคอพฟิกเครื่อง Server โดยการดับเบิ้ลคลิกที่ Server >> Config

P Server0		┦
Physical Config	Services Desktop Attributes Software/Services	
GLOBAL	Global Settings	
Algorithm Settings	Display Name Server0	
INTERFACE	Gateway/DNS IPv4	
FastEthernet0	O DHCP	
	Static	
	Gateway	
	TNIC Server	
	010 30 10	
	Gateway/DNS IPv6	
	O DHOP	
	C Auto Config	
	Static	
	IPv6 Gateway	
	IPv6 DNS Server	
	*	
🔄 Тор		

FastEthernet กำหนด IP Address เป็น 192.168.0.105 ตรวจสอบ Port Status เป็น On

hysical Config	Services	Desktop	Attributes	Software/Servi	ces			
GLOBAL	*				FastEt	hernet0		
Settings	Port S	tatus		-				Dn
Algorithm Settings	Bandy	ridth					🍥 100 Mbps 💮 10 Mbps 📝 Au	to
INTERFACE	Duples	¢					💿 Half Duplex 🛞 Full Duplex 📝 Au	ito
FastEthernet0	MAC A	ddress				0050.0F1D.8245		
	-IP (Configuration						
	0	DHOP						
	۲	Static						
	IP	Address			-	192.168.0.105		
	Sub	net Mask	-			255.255.255.0		
	IPv	6 Configuration						
	0	DHCP						
	ŏ	Auto Config						
	۲	Static						
	IPv	6 Address					X	
	Lini	Local Address	FE80::250:FI	FF:FE1D:8245				
	÷							

จากนั้นไปที่แท็บ Services เลือก DNS แท็บ กำหนดในช่อง Name เป็น <u>http://www.firstlab.com</u> type เป็น A Record และ ช่อง Address เป็น 192.168.0.105 คลิก Add สุดท้ายอย่าให้ตรวจสอบว่า DNS Service มีสถานะ เป็น On หรือไม

🥙 Server0					X
Physical Config	Services Deskto	Attributes Software/	Services		
SERVICES HTTP	A		DNS		_
DHCP	DNS Service	•	On	Off	
DHCPv6 TFTP DNS	Resource Records			Type A Record	•
SYSLOG	Address				
NTP		Add	Save	Remove	
EMAIL	No.	Name	Туре	Detai	5
InF	0	www.frstlab.com	ARecord	192, 168, 0, 105	
VM Management					
Top	v DNS Cache	Ν			

ตรวจสอบเครื่อง Server อีกครั้ง โดยใช้ Inspect



ทคลองสร้างข้อมูล (Add Simple PDU) เพื่อทคสอบการเชื่อมต่อในโหมด Realtime

คลิกเลือก Add Simple PDU



Add Simple PDU หมายถึงโพรโทคอลชนิดหนึ่งที่ใช้สำหรับทดสอบเครื่องปลายทางว่าทำงานอยู่หรือไม่ (เรียกว่า ping message หรือเรียกว่า echo request)

กลิกที่เครื่อง PC 1 ครั้ง และคลิกที่เครื่อง Server อีก 1 ครั้ง เมื่อ ping สำเร็จจะมี message ที่เรียกว่า echo reply ตอบกลับมาจาก Server ให้ดูผลลัพธ์การทำงานได้ในส่วน User Created Packet Window อยู่ ด้านขวา ล่าง



สำหรับข้อมูลที่ แสดงใน Scenario จะแสดง Last Status ว่า Successful แปลว่าการทำงานสำเร็จ (จากตัวอย่าง Source=Pacman, Destination=Web Server, Type=ICMP เป็นต้น) ลองทดสอบ ping กลับทิศทางอีกครั้งว่า เป็นอย่างไร เป็นอันสิ้นสุดการทดสอบด้วยการ ใช้ Simple PDU (ping request/reply)



ทคสอบการทำงานของเว็บเซิร์ฟเวอร์ โดยใช้ โปรแกรม Browser ที่ฝั่งใคล์แอนท์ โดยคลิกที่เครื่อง PC เลือก แท็บ Desktop เลือก Web Browser ในช่อง URL ใส่ข้อมูลเป็น <u>http://www.firstlab.com</u> เสร็จแล้วกคปุ่ม go โปรแกรมจะแสดงข้อมูลใน Web Browser



ทดลองเปลี่ยนโหมดการทำงานเป็น Simulation ซึ่งในโหมดนี้ผู้ใช้สามารถควบคุม เวลาการทำงานได้ ส่งผล ให้เวลาในการทำงานของโปรแกรมจะช้ากว่าปกติ และผู้ใช้ ก็สามารถสังเกตพฤติกรรมของข้อมูลได้ชัดเจน

โดย คลิก ที่ Desktop >> Web Browser >> ใส่ในช่อง URL เป็น <u>http://www.firstlab.com</u> กดปุ่ม go กลับไป ยัง workspace แล้ว สังเกตุที่ Even List จะ ปรากฏ โพรโทคอล DNS อยู่และมีซองจดหมายปรากฏบนเครื่อง PC ด้วย ให้ เลือก Auto Capture/Play เมื่อต้องการเฝ้าดูแพ็กเก็ตแบบต่อเนื่อง หรือเมื่อต้องการเฝ้ามองที ละ step ให้เลือก Capture/Forward



สังเกตุว่า ในการทดสอบครั้งนี้จะมีโพรโทคอลปรากฎใน Even List 2 ชนิคคือ DNS และ TCP (Web Server) เนื่องจากเครื่อง PC จะต้องสอบถามชื่อผ่าน Domain Name Server ก่อนเสมอ เพื่อแปลง URL (www.firstlab.com) เป็นหมายเลข IP Address จากนั้น PC จึงใช้หมายเลขไอพีดังกล่าวเข้าใช้บริการเว็บ เซิร์ฟเวอร์ต่อไป

สมาชิกภายในกลุ่ม

นาย	พิชญุตม์	ห้วยห้อง	161404710050
นาย	ศุภวัฒน์	ศรีสุขใส	161404710056
นาย	เลิศชัย	<u>ລ</u> ືก ข ุวาโย	161404710059
นาย	วรรษพจน์	จาระวรรณ	161404710061
นาย	ทิวัตถ์	จันทรานุสรณ์	161404710040