418351 Friday, September 5, 2008 ชื่อ นาย ชูเดช ศรีแดง รหัสนิสิต 4921002-4

12 ก.ย. 2551 บันทึกช่วยจำ

Icmp = Internet control message Protocol.

ใช้โดย Host กับ Router ที่ต้องการที่จะแจ้งข้อมูล

รายงาน error., Host ไม่ตอบ, protocol

ใช้ 8 byte of Ip datagram.

Type	code	
0	0	(ping) echo reply
3	0	dest, network unreach
3	1	" host unreach.
3	2	" protocol unreach
3	3	* " port unreach.
3	6	" network unknown
3	7	" host unknown
4	0	source quench
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery.
11	0	TTL expired
12	0	Bad IP Header.

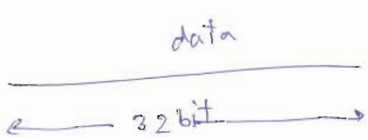
IPv6 fixed-length 40 byte header.
no fragmentation allowed. (32 bit)

ver	pri	flow label
payload len	next header	hop limit

source address
128 bit (16 byte)

dest add.
128 bit

data



Transition from IPv4 to IPv6.
~~flag day~~
no flag day.

Tunnelling IPv6 to IPV4

Dijsktra's Algorithm

```
1  initialization
2  N' = {u}
3  for all nodes v.
4  If v adjacent to u.
5     Then D(v) = c(u,v)
6     else D(v) = ∞
7
8  Loop
9  find w not in N' such that D(w) is minimum
10 add w to N'
11 update D(v) for all v adjacent to w and
     not in N'.
12    D(v) = min(D(v), D(w) + c(w,v))
13 /* new cost to v is either old cost to v
     or known shortest path cost to w plus
     cost from w to v */
14 until all node in N'
```

step	N'	D(v)	D(w)	D(x)	D(y)	D(z)
0	u	2, u	5, u	1, u	∞	∞
1	ux	2, u	4, x		2, x	∞
2	uxy	2, u	3, x			4, y
3	uxyv		3, y			4, y
4	uxyvw					4, y
5	uxyvwz					

ความดี ไม่มีล้วงหน้า = มารอรับ

418351 Friday, September 5, 2008 ชื่อนาย กฤษณ์ ทองสีอาด รหัสนิสิต 4921004 0

12 11.8. 2551 บันทึกช่วยจำ

IP Address

มีขนาด 32 bit เช่น 11111111.7.7.7

IP แบ่งออกเป็น 2 ส่วน { หน้า Network past / หลัง host Past

Class A / 8 1.0.0.0 → 127.255.255.255

B / 16 176.0.0.0 → 191.255.255.255

C / 24 192.0.0.0 → 223

d / 32 224.00.0 → 239

192.168.100.0 /27 → อยู่ในคลาส C /19 ยืมมาอีก 3 bit

Net work IP = 192.168.100.111 (31 = xxxxx)

subnet mash = 255-31 = 224 = 255.255.255.224

จำนวน subnet = $2^{n\text{-bit ยืม}} - 2 = 2^3 - 2 = 6$

host = $2^y - 2 = 2^5 - 2 = 30$ host

broad cast IP = 192.168.100.255

ขั้นตอนการต่อเชื่อมกับ DHCP

① ตัวอุปกรณ์เรียก DHCP โดยการขอ IP

② DHCP จะตอบ IP ที่ว่างอยู่ DHCP offer ให้ลูก

③ เมื่อลูกได้รับจะตอบกลับ

④ DHCP ส่งอีกครั้งเป็น DHCP Ack ให้ลูก

NAT (Network Address Translation)

- สามารถแปลง IP ในเครือข่ายให้เป็นอีกอย่างหนึ่งได้

ขั้นตอนการทำงาน

① จับเก็บ source IP add และ Port number

② แทนที่ IP

③ assign ค่า Port ในแต่ละ Packet

④ คำนวณใหม่ IP TCP checksum

CIDR (Classless Interfomain Routing)

- ต้องการอ้างถึงเครือข่าย IP โดยใช้ / ตามด้วยขนาด mash

- ใช้อธิบายเครือข่าย Prefix และแสดงด้วย = Suffix เช่น 128.10.0.0/16

DHCP (Dynamic Host configuration Protocol)

คือ โปรโตคอล ที่ใช้ในการกำหนด IP Address ให้กับอุปกรณ์ในระบบ ต้องใช้ TCP/IP

- DHCP Sever → เป็นเจ้าที่แจก IP ในเครือข่ายไม่ให้ซ้ำ

เป็นการลดความซ้ำซ้อน

NAT ป้องกัน virus ได้ด้วย

418351 Friday, September 5, 2008 ชื่อ [illegible] รหัสนิสิต [illegible]

12 ก.ย. 2551 บันทึกช่วยจำ

DHCP

ICMP [illegible]

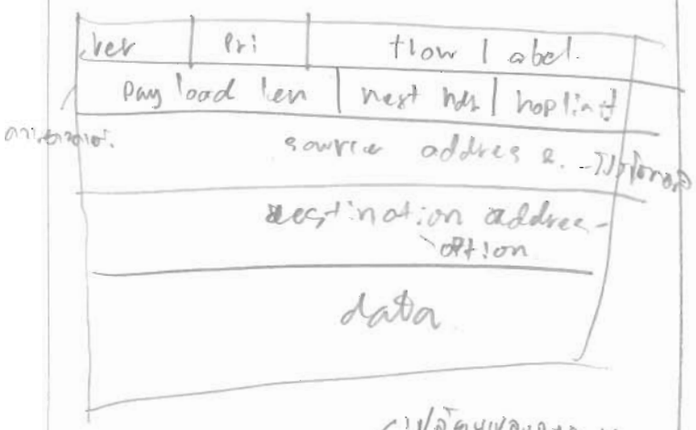
[illegible]

Type	code
0	0
3	0
5	1
7	2
8	3
9	6
10	17
11	0
12	0
9	0	router advertisement
10	0	router discovery
11	0	TTL expired.
12	0	bad IP head

IPv6

[illegible] check sum.

[illegible] IP header



[illegible]

Other Change IPv6

option [illegible] header [illegible] data

MTU Maximum Tranfer unit 1500

Tunneling.

[illegible]

Graph G = N E

N = set router = {u, v, w, x, y, z}

E = Set of link (uv) (ux) [illegible]

[illegible]

418351 Friday, September 5, 2008 ชื่อ นายกิตติพงศ์ รักษา รหัสนิสิต 4937000123

บันทึกช่วยจำ

Ping : ดูการตอบกลับของเครื่อง (Delay)

ICMPv4 เช่น Ping , จะใช้ร่วมกันเมื่อส่งงานใน Network layer ถูกใช้โดย host & Router

- ใช้ในการส่ง error report ต้อง host ไปไม่ถึง (ตรวจสอบว่าเครื่องปลายทางไม่เจอ) มีข้อมูลอยู่อย่างน้อย 2 อย่าง คือ ชนิด Type

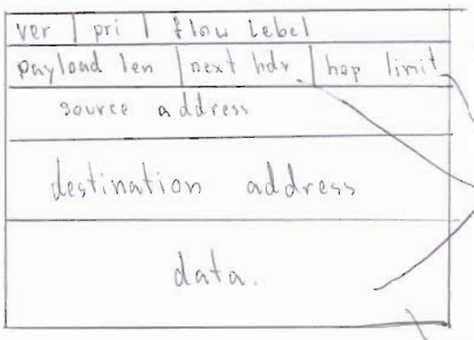
- ใช้ในการส่ง echo request : วัตถุประสงค์ว่าเครื่องปลายทางเปิดอยู่หรือไม่

Traceroute : จะทำ Ping 3 ครั้ง โดย TTL เริ่มต้นเป็น 1 ถ้าผ่านไปจนเจอแล้ว TTL จะเป็น 0 และถูกโยนทิ้งไป โดยจะส่งข้อความตอบกลับมาบอกว่าหาย , จะถูก hops ที่ Router ตัดไป , มี เครื่องหมาย * แสดงว่า บอก Router ยังไม่ตอบกลับมา จะครบ Router ถ้า TTL : n

เส้นทางที่เดินอาจไม่ใช่เส้นทางสั้นที่สุดขึ้นอยู่กับสถานการณ์ในขณะนั้น

IPv6 : ถูกนำมาแทนที่ IPv4 ที่ถูกกำหนดไว้ 32-bit ซึ่งไม่พอใช้

- Header : ยาว 40 byte จะยาวคงที่
- ไม่รับทำ fragment



ver : มี 4 bit เลข Version เพื่อให้ Router Process ได้

pri : ดูว่าจะได้รับการ Process เร็วกว่า

TTL

เช่น ถ้า เป็น TCP จะเป็นเลข 6

คือ Data ไดรับงานอื่น

Checksum ไม่ทำ

Option : มี แต่ไม่ต้องว่าเป็นส่วนหนึ่งของ Header แล้ว , ยกไปอยู่ใน Data. ไม่สามารถเปลี่ยน Router ทุก Router ได้ถามเป็นรายเส้นทาง

ใช้ Tunnel : สามารถใช้ IPv6 คุยกันโดยที่มี IPv4 อยู่ได้ โดยจะเก็บ Data ของ IPv6 ยัดใส่ใน IPv4.

418351 Friday, September 5, 2008 ชื่อ ... รหัสนิสิต ...

12 ก.ย. 2551

บันทึกช่วยจำ

IP datagram format

Ver	head len	type of service	length
16 bit identifier		flgs	fragment offset
time to live	upper layer	header checksum	
32 bit source IP addr.			
32 bit destination IP addr.			
options (if any)			
data (variable length)			

- ver. ปัจจุบัน 4 (ตัวแรกเป็น version ที่ต้องดูในการ version ถึงกัน ถ้าคนละ version ไม่รู้จักกัน ก็จะไม่ได้ผลลัพธ์)
- head len ของ header เป็น byte
- type of service ชนิดของการให้บริการ
- 16 bit identifier IP ของ packet ที่ถูก fragment (length 16 bit) ความยาวของ packet
- flgs ดูแลเรื่องปัญหา fragmentation แยกออกเป็นก้อนย่อย ถ้าเกิน link layer ในปัจจุบัน
- fragment offset ตำแหน่งของข้อมูลเดิม
- time to live packet ส่งไป router ต่างๆ เพื่อจะ lock ไม่ให้วนลูปกลับมาที่เดิม
- upper layer ชั้นที่ router นั้นของอ้างอิงถึง
- header checksum ตรวจสอบ header ตัวนี้ว่าถูกต้องหรือไม่ ในขณะที่
TCP รับแต่ข้อมูล data ในชั้นถัดไป
UDP ทำงานเหมือนกับ TCP

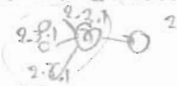
IP Fragmentation & reassembly

Network layer จะมีหน้าที่ (ในการดูแลเรื่อง) IP packet ที่ผ่านมาจาก router ต่างๆ ที่ link ออกมาจาก transport ได้ ไม่ใหญ่เกินกว่าที่ IP packet จะส่งต่อไปยังได้ ซึ่งจะมีข้อมูลที่ fragment แล้วส่วนต่างๆ ของ IP address ของแต่ละส่วน ถูกส่งไปยังปลายทางเดียวกัน ดูแลเรื่องการเรียงลำดับ

IP addressing

interface จะเชื่อมต่อระหว่าง host / router กับ link ของ router ในแต่ละ interface host มี interface เดียว IP address แบ่งเป็นส่วนย่อย กลุ่มละกี่ bit

subnet ในกลุ่มเครือข่ายที่มีส่วนของ subnet part เหมือนกัน อยู่ใน network เดียวกัน ถ้าต่างกันจะข้าม router เพราะว่าคนละ network



IP addressing: CIDR

อีกหน้าที่หลักๆ routing ดูจำนวน bit ใน network part แทนไม่ดูที่ class ดูตำแหน่งของ subnet ดูความยาวได้ไม่แน่นอนตัวดูที่ความยาวของตัวเอง

DHCP

host ส่ง "DHCP discover" ขอความ
DHCP server ตอบด้วย ข้อความ "DHCP offset"
host ขอ IP address ข้อความ "DHCP request"
DHCP server ส่งที่อยู่ ข้อความ "DHCP ack"

NAT

ตอนนี้ถามว่าจะไม่ได้ทำงานอย่างไร ไม่ได้ทำงานของที่ใช้ NAT ช่วย ส่งข้อมูลไปที่ web server ข้างนอก NAT จะเปลี่ยน IP address ในตารางและ port ไปเรื่อยๆ

NAT มีหน้าที่

1. เปลี่ยน IP address ทั้งในและนอก
2. หมายเลข port ที่ได้มาเปลี่ยนเครื่องมือก็ไม่ต้องไปยุ่งกับมัน
3. เครื่อง Internet จะ access เข้าในนี้ได้ยากเพราะมี IP address

NAT : Network address translation

- ของต้องเอาออกเพราะเมื่อใช้ข้อมูลเสร็จแล้วจะได้ส่งกลับ TCP จะได้ส่งถูกไปยังเครื่องที่ถูกต้อง
- Net ดูแลอยู่ใน Network layer ไม่ดูแล port ดูอยู่ใน header ของ TCP

Ex ไฟล์รหัสผ่านอยู่ในของเว็บ มีอะไรแล้วได้แต่ไม่ดู

- NAT ไม่เปลี่ยน IP address ตัวเองได้ แต่ NAT ของตัวเองเปลี่ยน port ได้
- NAT ทำให้ประหยัด IP address

418351 Friday, ~~September 5,~~ 2008 ชื่อ ช.ส. ลีลาพงษ์ ชื่อแล้ว รหัสนิสิต 49210181

12 ก.ย. 2551 บันทึกช่วยจำ

CSMA/CD efficiency กลาย Unslotted ALOH

$$\text{efficiency} = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

t_{prop} เวลาในสาย ส่ง เฟรมไปสุดสาย

t_{trans} เวลาที่ใช้ส่ง บุ๊ ๆ ไปสุด ๆ

- from ยิ่งไม่ยิ่งดี

- t_{prop} เข้าใกล้ 0 ดี - effi ที่จะเข้าใกล้ 1

802.3 - ลักษณะทางกายภาพ - ก. แบบแทงค์ต่าง

- media แทงค์ต่างชั้นล่าง

Manchester

ใช้ใน 10BaseT

HUB (repeater) เชื่อมต่อ ยิ่งไปยิ่งหาย - ส่ง bit ต่อ link copy ไปทุก link

- ไม่ buffer - ไม่ทำ frame buffing

- ไม่มี CSMA/CD ชิ้นส่วนหัวใจ

switch - ทำ frame ที่เข้ามา ทางปลาย MAC add ต้น-ปลาย

- เลือกช่องใส่ ช่องหนึ่ง หรือ หลายช่อง - พร้อม ต้นไม้

- switch table เหมือน hub ต่างกัน ตรง กลาย routing

- ข้อดีของ hub - ที่ เข้า ส่ง ไป host ใด

- ส่ง frame ได้หลาย MAC address ต้นทาง ส่งไปยังปลายทาง

ในพร้อมเข้าสู่ CSMA/CD

- user ไม่ต่อ - เรียนรู้เอง ไม่ต้องพึ่งพิง program

ทางาน switch เก็บ mac add. และ mac. add ไหนอยู่/Port ไหน

- time stamp ของว่าใช้ mac add เมื่อไร

- ปิด switch ไปแล้วเปิดใหม่ ๆ เขาจะเรียนรู้ใหม่ เก็บใน switch table

- TTL connection switch

A ต่อไป s_1 แต่ s_1 ไม่รู้ ว่าต่อ broadcast ออกไป

และ s_4 ได้ข้อ frame นี้ เข้าทางนี้ และ ปลายทาง และ s_4 ไม่มี ในทาง broad cast ออกไป ยิ่ง และ s_2, s_3 ก็ broadcast อีก ๆ เหมือน s_3 ก่อนหน้า ๆ และ ๆ ไม่รู้จัก frame

Chapter 4

network layer - layer ที่ทำงานเอง host ต่อ host

เท่านั้นเอง data หนึ่ง → data หนึ่ง

- ที่ router ในอากาศ จนถึง router ที่ต่อหนึ่งเครื่องจริงใช้งาน data

- Routing คำนวณเส้นทางเส้นทางของ data

A → B ที่ router ต่อ ส่ง frame ทาง mac ของ router ๆ รู้เส้นทางว่าส่งแต่ใช่รู้ mac add. จะหั่งล้อไป ห้องสายต่อ และจึงจะส่ง frame เป็นแบบนี้ทุกอย่าง เพื่อหน่

หน้าที่ Network layer

- Forwarding ส่ง Packet ภายใน Input ใน output

- routing หาเส้นทางไปยังปลายทาง

- routing ก่อน จึง forwarding ได้

- R ตัวนี้ routing algorithm ของเค้าส่งไปทางไหน

Network layer แบบ connectionless

- datagram network ไม่มีสาย connection ใช้ router ไม่เก็บสถานะ (ต้นปลาย ทาง)

มี โดยการส่งไป ไม่ยึดปลายทาง

เช่น Internet ccom ส่ง data ยิ่ง com) data network ง่าย (user ชุ่ยตาย)

dumb

- ATM (VC) - เชื่อมต่อได้

- ต่อได้ตามที่ปลายของ network user ใช้งาน)

มีการ check ก่อนส่ง ถ้าของมากยิ่งช้า

12 ก.ย. 2551

418351 Friday, September 12, 2008 ชื่อ น.ส.สุไรวัลย์ ฉิมไทย รหัสนิสิต 4921015 6

บันทึกช่วยจำ

IP datagram format

ขอคุณของ head

ขอบอกขนาดของการใช้งาน

ขอ version ของโปรแกรม

ความยาวของ Packet = 16 bit

32 bit

Ver	head len	type of service	length
16-bit identifier		flgs	fragment offset
time to live	upper layer	header check sum	
32 bit source IP address			
32 bit destination IP add			
options (if any)			
data (variable) lenght, typically a TCP or UDP segment			

ระยะทางกล่าว ๆ ว่าสิ่งที่ใช้สำหรับ Packet จนกลับออกที่เดิมเพื่อ Packet ว่ายผ่าน Router ตัวที่ 1 ทำการลดลงที่ละ 1 และส่งไปยัง Router ตัวต่อไป. ซึ่งเรื่องนี้จะหายไปที่ Set ตามเงื่อนไขก็จะทิ้ง Packet

check sum ของ header จะ check ทุกครั้งที่มีข้อมูลในส่วน.

- ☐ 20 byte of TCP
- ☐ 20 byte of IP
- ☐ = 40 + app layer overhead

IP Address

ที่อยู่ขนาด 32 bit แบ่ง

IIIIIIII . IIIIIIII . IIIIIIII . IIIIIIII

IP แบ่งเป็น 2 ส่วน

1) ส่วนแรก เรียก network part

2) ส่วนของ host part

Class A	/8	0.0.0.0 → 127.255.255.255
B	/16	128.0.0.0 → 191.255.255.255
C	/24	192.0.0.0 → 223.255.255.255
D	/32	224.0.0.0 → 239.255.255.255

192.168.100.0 /27 → อยู่ใน Class /191 เหลือว่าง

ยืม 3 bit

- Network IP = 192.168.100.111xxxxx (31)
- Subnet work = 255-31 = 224 = 255.255.255.224
- จน. Subnet = 2^n → bit ที่ยืม
- จน. host = $2^x - 2$ → จน. ที่เหลือให้ใช้

= $2^3 - 2 = 6$ Subnet

= $2^5 - 2 = 30$ host

- Broadcast IP = 192.168.100.255
- Rang host IP

subnet	zero	192.168.100.0 - 192.168.100.31
1	32 - n	n - 63
2	64 - n	n - 95
3	96 - n	n - 127
4	128 - n	n - 159
5	160 - n	n - 191
6	192 - n	n - 223

Subnet mask = ตัวเลข bit อันหน้าที่ติดกันเป็น 1 bit ที่ยืมมาเป็น 1 หมด.

IP Fragmentation and Reassembly

* MTU คือ ขนาดสูงสุดของแพ็กเกตที่สามารถผ่านไปได้

สมมติให้ข้อมูลเท่ากับ 4000 byte แบ่งเป็น Datagram ขนาดไม่เกิน MTU = 1500 bytes

1) ข้อมูลมี Header 20

∴ 4000 byte = 4000 - 20 = 3980

∴ เก็บข้อมูลได้จริง 3980 byte *

1500 - 20 = 1480/8

1480

1480

1020

ชุดข้อมูลใหม่ กลายเป็นชุดข้อมูลเล็ก

length	ID	fragflag	offset
4000	=X	=0	=0

ชนิดของข้อมูล

offset เริ่มต้นที่ 0

length	ID	fragflag	offset
1500	=X	=1	=0

1480/8

length	ID	fragflag	offset
1500	=X	=1	=185

(1480+1480)/8 = 370

length	ID	fragflag	offset
1040	=X	=0	=370

fragflag สุดท้ายจะเป็น 0

ขอขอบคุณ อ.ชื่อ

12 ก.ย. 2551

418351 Friday, September 5, 2008 ชื่อ นายชัยวัฒน์ สมบูรณ์ทิน รหัสนิสิต 49370158

บันทึกช่วยจำ

ATM(VC) virtual Circuit vs

- ต้นทางส่ง เวลาที่ ให้เริ่มส่งข้อมูลที่เหมาะสมไปยังปลายทาง
- ระบบไม่สามารถ - ผู้ใช้ งานง่าย แต่ผลไม่เหมาะสม ยาก

Routes Architecture Overview

ส่วนประกอบที่สำคัญ คือ Input Output switching fabric

switching fabric → เป็นแผงวงจรที่ใช้ในการส่ง ข้อมูล จาก ด้านหนึ่ง ไปยังอีกด้านหนึ่ง ซึ่งมีหลายรูปแบบ (ทำงานร่วมกับ Input port)

Input Port function

Decentrelized switching (ระบบกระจาย)

- ดูจาก forwarding table
- ส่งต่อหน้าที่ที่กำหนดไว้ เพื่อ forwarding table ที่เหมาะสม speed
- ถ้าหากมีไม่พอ จะเก็บไว้ใน queue

Input Port Queuing

- อยู่ที่หน่วยความจำของตัวเอง Input port
- มีผลต่อ delay ของข้อมูล ที่เราส่งออก ด้วยกันเอง
- แล้วขึ้นอยู่กับ switch fabric ที่ความเร็ว
- Input - output ไม่เท่ากันได้

Three type of switching fabrics

memory - ระบบเก่า ใช้ แอล ไม่ค่อยใช้

bus - Input port ใช้เพื่อที่ในการส่งต่อกันเอง

Crossbar - ในหนึ่งจุดนั้น จะมีจุดเชื่อมต่อ เสมอกัน ไม่ว่าจะมีกี่ port ก็ตาม เราสามารถ ส่งออก หรือรับกันได้

Output port - มีการ queue

The Internet Network layer

IP Protocol - ส่งแพ็คเกต ต่อ Address ไม่ชัดเจน ทางเดียวเสมอ แต่มีตัวกำหนด รูปแบบของ packet

IP header เปรียบได้กับ ซองจดหมาย ข้อมูลที่อยู่ข้างใน — จดหมาย

IP Addressing Introduction

Interface - คือ Connection ที่ router กับ physical link

IP Address 32 bit (IP ต่อ 1 interface)

Subnets แบ่ง 2 ส่วน

- ส่วน subnet ที่เหมือน high-low order
- Subnet เหมือนกัน เป็น network เดียวกัน

IP Addressing CIDR

- วิธีการในการทำ routing โดยดูที่ network part ถ้าอยู่ตรงกันไม่ได้ แต่ไม่เหมือน

IP Addresses : how to get one ?

- การ set IP แบบ - การ set IP แบบ อัตโนมัติ

DHCP Dynamic Host Config Port

- ทำให้เครื่อง ขอการ จอง IP ได้

NAT : Network Address Translation

- ขอการ เปลี่ยน IP Addr ของเครื่องใน network ไม่ให้ออกไปยัง ISP

NAT : Network Address Translation

16 bit port-number field 60,000 simultaneous

- ลดระดับ layer ชั้นได้ - ที่อยู่ภายในที่มี Addr ไม่ unique

ICMP : Internet Control Message Protocol

- ใช้โดย host และ routers
- ทำงานที่ Network level
- เพื่อรับ router ปลายทาง ให้ทำ request (ping) การตอบกลับ ของการทำ กับอยู่ที่ปลายทาง

- มี แรก Type code ที่บอกการทำงานของมัน

1. Traceroute and ICMP

- ใช้ UDP ไปยังปลายทาง และ ตั้ง drop router TTL ครั้งแรกเป็น 1 2 ครั้งต่อไปเรื่อยๆ
- ส่งการแจ้งกลับมา (ICMP)
- Traceroute does ทำได้ 3 ครั้ง

Stopping criterion
- ถึงปลายทาง drop
- ไม่ host ไม่ได้ error

12 ก.ย. 2551

418351 Friday, September 5, 2008 ชื่อ นายณัฐกรธัช แก้วสีขาว รหัสนิสิต 4921016U

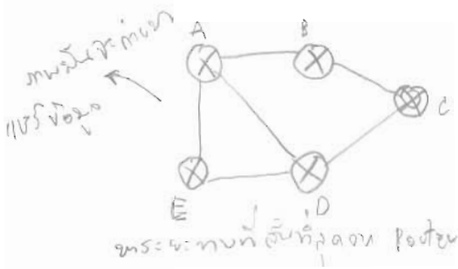
บันทึกช่วยจำ

TTL = time to live ค่าที่บ่งบอกว่า ping อันนี้จะมีอายุกี่วินาที

IPV6 = เลข IP รุ่นใหม่ ขยายเพิ่มขึ้นมาจากเดิม

Static = เป็นเส้นทางที่ให้กับ Router

Dynamic = เส้นทางเปลี่ยนไปเรื่อย



ขยายเพิ่มขึ้นจากเดิม

แบ่งข้อมูล

ขนาดของเส้นทางที่สั้นที่สุดของ Router to Router

โดยตัวมันเอง

12 ก.ย. 2551 12

418351 Friday, September 5, 2008 ชื่อ ธีระศักดิ์ แซ่ลิ้ม รหัสนิสิต 49340166

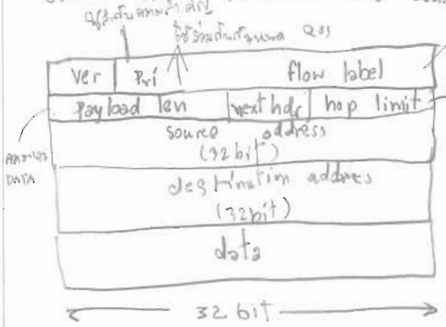
บันทึกช่วยจำ

ICMP Internet control Message Protocol

TTL ค่าลดลงไปเรื่อยๆ เมื่อ ค่าเท่ากับ hop ที่ Type 11 Code 0

IPV6 มีความยาวของ header 40 byte

ส่วน ของ header ที่ทำงานเพิ่ม QoS Quality of service



Next header ของ TCP เท่ากับ 6

options ใน V4 ตามใจ.

ใน V6 ค่าอยู่ในส่วนของ DATA Next header ค่าไม่เท่ากับ option.

ms ส่ง ผ่าน IPV4 โดย IPV6 ค่าเข้าชั้น ทดลองกัน

ตามแบบ Forcast Atgorithm ของ Rounting

gobal เหมือนกันทุก node	static คงไม่ใช่คน ตัวเอง
Decentralize ผลการทดลอง, ประสิทธิภาพการทำงาน.	Dynamic เปลี่ยนเส้นทางไปเรื่อยๆ

สรุปรวมได้

ชีวิตนี้ – ไฟ แม่ไม่ให้ใช้

ใส่ซับดูงพลาสติก โดนไม่ซักโน.

ไม่ชัด ตัวของสั้นเป็นสี่ๆ

ไม่ชัดเจนเรื่อง

12 ก.ย. 2551

418351 Friday, September 5, 2008 ชื่อ นาย บัณฑิตา รัตนวงศ์ไพบูลย์ รหัสนิสิต 4937016Z

12 บันทึกช่วยจำ

* ICMP : Internet Control Message Protocol

→ ถูกใช้งาน host comp / router เมื่อ datagram มีปัญหา error ระดับ port

→ ตามด้วย Type Code description.

∴ ถ้าเครื่องที่ไม่ใช่ปลายทาง ก็ จะถูกส่งกลับเป็นต้นทาง

* Traceroute and ICMP

→ เป็นการส่ง datagram ไปยัง host ปลายทาง ที่มีค่า TTL ในแต่ละครั้งที่ส่งมากขึ้น 256 เพื่อ ป้องกันไม่ให้ loop ไม่สิ้นสุด

ได้ผลลัพธ์ 3 รอบ (delay)

- ใช้ option ของ ip data - ส่งกลับได้หลายทาง

IPv.6 (v3) IPv.4

IPv.4 → เป็น 32bit ส่วน IPv.6 ที่เพิ่มขึ้น ที่เป็น 4 ออกเป็น header, no fragmentation

IPv.6 Header form. →

ver	pri	Flow label	
payload len		next hdr	hop limit
source address 16 byte			
destination addr. 16 byte			
data			

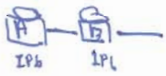
ไม่มี check sum

* ถูกใช้ IPv.4 option → ดูที่ last เสมอ

ผลลัพธ์ IP router ที่ไม่รู้จัก header ก็ส่งต่อไป

∴ last router → ตรวจสอบ option ที่ส่งมาด้วย ถ้าไม่ใช่ ก็ส่งต่อ ถ้าใช่ ก็ส่งกลับ

* วิธีการ Tunneling ที่ดูเหมือนว่าจะใช้งานได้ ถ้าเป็น IPv4 หรือ ถูกใช้ IPv6

Logical view 

Physical view

Graph abstraction : costs.

Routing Algorithm แบ่งได้ 2 แบบ.

1) Global : ทุกๆ router ทุกตัวในเครือข่าย ต้องรู้ topology ของ network ทั้งหมด ต้องรู้ว่า router นี้ cost เท่าไร

2) Decentralized : router แต่ละตัว ไม่รู้ topology ของ network ทั้งหมด ต้องรู้ cost ของ link ที่ตัวเองต่อกับ router ตัวอื่น

→ แบ่งได้ 2 แบบ Static / Dynamic

Static (เปลี่ยนไม่บ่อย) → router ทำงานน้อยลง

* ใช้ link - State Routing Algorithm.

Dijkstra's algorithm มีขั้นตอน 3 step

1) ต้องรู้ว่า node ต้องส่ง broadcast ไปที่ switch ไหนบ้าง

2) ต้องรู้ cost ของแต่ละ link

3) ป้องกัน loop ของ routing table

IP Addressing: introduction.

- IP address: 32 bit.

DHCP: Dynamic Host Configuration Protocol.

- host broadcasts "DHCP discover" msg. ค้นหา.
- DHCP sever responds with "DHCP offer" msg.
- host requests IP address: "DHCP request" msg.
- DHCP server send address: "DHCP ack" msg ตอบรับ

NAT: Network Address Translation.

* Motivation: local network use just one IP address as far as outside world is concerned:

- rage of address not needed from ISP: just one ~~ISP~~ IP address for all devices.
- can change address of devices in local network without notifying out side word.
- can change ISP with changing addresses of devices in local network.
- devices inside local net not explicitly addressable, invisible by outside world (a security plus).

ความคิดเห็น: ไม่มีข้อมูลเพิ่มเติม

418351 Friday, September 5, 2008 ชื่อ พรหนึ่ง [illegible] รหัสนิสิต 49370232

12 ก.ย. 2551 บันทึกช่วยจำ

IPV6 [illegible] (cost [illegible] (Jitter, ความล่าช้า)

type of service

100 mb cost น้อย

10 mb cost สูง

IPV6 Header

ver ความยาวของ header

pri n

flow label ระบุ

payload len ความยาวของ data เป็น byte

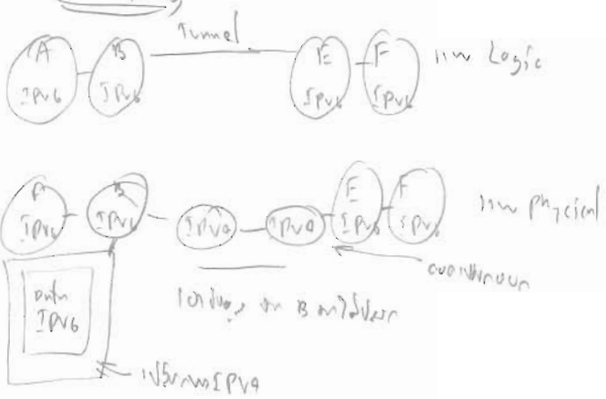
next hdr n ไปยังไหน

hoplimit n เหมือน TTL

Strategy [IPv4 / IPv6]

[illegible] Tunneling (อุโมงค์)

Tunneling



ความรู้ : การใช้งานร่วมกันอย่างน้อย 30 นาที

418351 Friday, September 5, 2008 ชื่อ นายสมรวมช วิศิษฐ์แยกษ์ รหัสนิสิต 4912025 5

12 ก.ย. 2551

บันทึกช่วยจำ

CIDR (classless Interfomain Routing)

- เป็นการอ้างอิงหมายเลข IP ตามขนาดของโดเมนไดเรียงหมาย / ตามด้วยขนาดของมาส์ก
- โดยเมื่อข้างจะเท่ากับ Prefix และเลขของ Suffix เช่น 128.10.0.0/16

DHCP (Dynamic Host configuration Protocol)

- คือโปรโตคอลที่ใช้แจกจ่ายหมาย IP Address อัตโนมัติของเครื่องลูกข่าย
ของระบบที่ติดตั้ง TCP/IP

DHCP sever

- มีหน้าที่แจก IP ในเครือข่ายไม่ให้ซ้ำกัน เป็นการลดความผิดพลาด
ในการต่อเครื่องลูกกับ DHCP sever
- เครื่องลูกจะเครื่อง sever ในเครือข่ายโดยส่ง DHCP discover เพื่อร้องขอ IP address
- sever จะค้นหา IP ที่ว่างอยู่ในฐานข้อมูลแล้วส่ง DHCP offer กลับไปให้ลูก
- เมื่อเครื่องลูกได้รับ IP จะส่งข้อความตอบกลับ DHCP Request ไป sever ทราบ
- DHCP sever ส่งข้อความ DHCP Ack ไปให้ลูกเพื่อแจ้งว่าเริ่มใช้งานได้

NAT (Network Address Translation)

- ระบบลดปัญหา IP หายๆตัวที่ใช้งานในเครือข่ายไม่ติดต่อกับเครือข่ายอื่นโดยใช้ IP เดียวกันขึ้นตอนการทำงาน

เมื่อ NAT ทำงานจะมีตารางตารางไว้ ซึ่งมีไว้เพื่อเก็บข้อมูล IP Address ของเครื่องในเครือข่ายภายในที่ส่ง packet เข้าสู่ NAT devide ขาออกนั้นจะมีตารางไว้เก็บหมายเลข port ที่ลูกใช้ไปและ out side IP address และเมื่อมีการส่ง packet ขาเครือข่ายใน → นอก NAT จะ

- เปลี่ยนข้อมูล source IP address และ sever port number ไปตามที่เราต้องการ
- แทนที่ IP Packet ด้วย IP ขาออกของ NAT address
- assign เลข Port ในใหม่ใน packet และเปลี่ยนค่า Port ไว้ในตารางและจำแนก
ค่าที่ส่งใน sprvos packet นั้น

คำนวน IP/TCP check sum อีกครั้งเพื่อตรวจสอบความถูกต้อง

* ลดน้ำต้นไม้

12 ก.ย. 2551

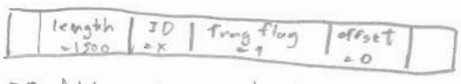
418351 Friday, September 5, 2008 ชื่อ น.ส.ดวงกมล แก้วศรี รหัสนิสิต 49210271

บันทึกช่วยจำ

IP Fragmentation & Reassembly

network layer มี MTU (maximum transmission unit) IP Packet สามารถที่จะใหญ่ได้มากกว่าค่านี้ แต่ปัญหาคือในกรณีที่ถูก router กั้น router ที่ link ของขาออกของ frame ที่ใหญ่กว่า MTU ก็จะต้องแบ่ง IP Packet ออกเป็นหลายๆส่วน หรือ fragment เรียก fragment ว่า IP header ของมันเอง เพื่อส่งไปที่ปลายทางแต่ละส่วนจะไม่รวมกันจนกว่าจะถึงปลายทาง (reassembly) เพื่อรวมกลับ

Ex datagram ขนาด 4000 byte ค่า MTU คือ 1500 byte ต้องแบ่งเป็น fragment แต่ละส่วนมี header อย่างน้อย 20 ตัวนั่นหมายถึงจะมี 1480 byte offset คือตำแหน่งของ frame นั้นอยู่ที่ตำแหน่งเท่าไร ส่วน flag = 1 คือยังมีอีกหลายตัว 0 คือ frame สุดท้าย



IP Addressing : introduction

interface : จุดเชื่อมต่อระหว่าง host/router กับ link

router's มีหลาย interface host มี interface เดียว

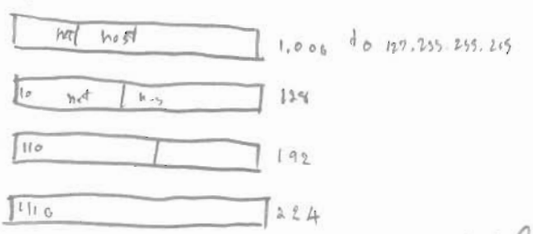
IP Address แบ่งเป็นกลุ่มละ 8 bit

233.1.1.1 = 11011111.00000001.00000001.00000001

IP address : subnet part, host part (network, subnet)

subnet คือ เครือข่ายที่มี subnet part เหมือนกันถือว่าอยู่ subnet เดียวกัน ถ้าต้องการออกต้องผ่าน router หมายถึงอยู่คนละ network

class



CIDR เป็นวิธีการในการทำ Router ลดจำนวน bit ใน network part ได้หลายๆ

DHCP protocal ที่ถูกพัฒนาขึ้นมา

address ที่ได้มาจาก server อาจจะแตกต่างกันได้ทุกครั้ง

คอมพิวเตอร์ที่มี DHCP อยู่ในนั้นจะส่งการ brand cast

DHCP ใจความสรุป host กระจาย "DHCP discover"

DHCP server ตอบ "DHCP offer"

host ขอ IP กลับ "DHCP request"

DHCP server ส่ง "DHCP ack"

NAT เป็นอุปกรณ์ที่แปลง IP หลายๆเครื่องที่ใช้ในเครือข่ายให้เหลือติดต่อกับเครือข่ายอื่นโดยใช้ IP เดียวกัน เช่น 192.168.1.1 เครื่องในนี้ 203.154.207.76 เครื่องนอกเมื่อจะติดต่อไปภายนอก NAT ภายนอกจะ IP ที่เข้าใน 203.154.207.76

NAT ความสามารถ

- ต้องแจกหมายเลข IP Add ได้
- ต้องทำ Packet ของข้อมูลที่มีการเปลี่ยนแปลง Add ได้
- เครื่อง Internet ที่ access ข้างในจาก NAT ต้องรู้จักแค่ IP add
- เปลี่ยน IP Add ภายในเครือข่าย เพื่อให้ติดต่อสื่อสารกับ Internet ได้

ขั้นตอนการทำงาน

1. NAT จับที่อยู่ source IP add และ source port number ไว้ในตาราง
2. NAT จะแทนที่ IP ของ packet ด้วย IP ของ NAT device เอง
3. NAT จะ assign เลข Port ใหม่ให้กับ packet และจับที่อยู่ Port ไว้ในตารางและกำหนดค่าใน source port number ของ packet
4. คำนวณหา IP, TCP checksum ขึ้นมาใหม่ เพื่อการตรวจสอบเมื่อ NAT ได้รับ packet ผ่านออกไปยัง external network อื่น Internet จะตรวจสอบ destination port num ของ packet ผ่านเข้ามาว่าตรงกับรายการที่มีอยู่ในตารางหรือไม่ ถ้าตรงจึงจะส่ง packet นั้นเข้าสู่ระบบ

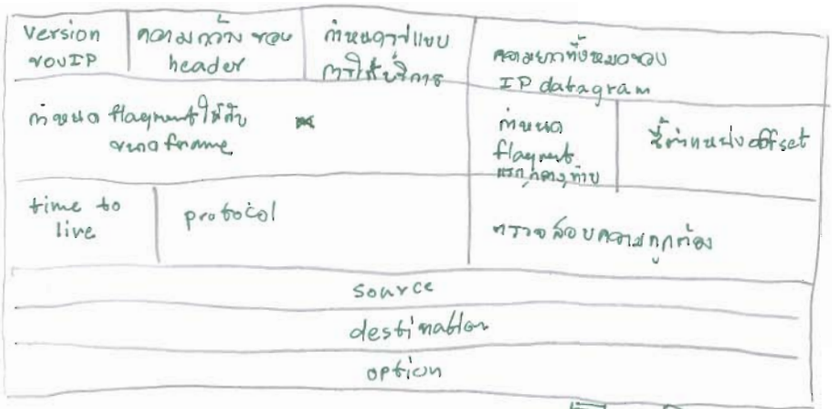
NAT ทำงานใน Network Layer ไม่ควรรู้จัก Port อยู่ใน header ของ TCP

12 ก.ย. 2551

418351 Friday, September 12, 2008 ชื่อ ศศกนิต ขวัญเมือง รหัสนิสิต 49210297

บันทึกช่วยจำ

Transport → TCP UDP Network → IP Link → PPP Ethernet

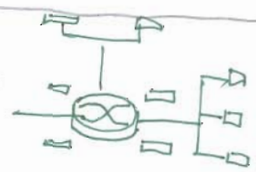


IP Fragmentation & Reassembly

MTU = maximum transfer Unix มีหมดของ ขนาดของ frame ที่ใหญ่ที่สุด

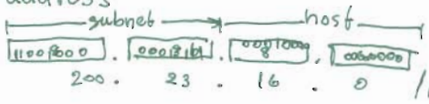
เช่น 1500

20 | 1480



- ชนิดของ router มีหลาย interfaces
- host มี 1 interface

IP address



- CIDR Classless Inter Domain Routing
  - มีวิธีการ Routing แบบ ค. เหมือนกันที่
  - address format : a.b.c.d/x x = จำนวน bit ของ subnet
- การได้มาซึ่ง IP address
  - hard-coded by system admin
  - DHCP - Dynamic Host configuration Protocol ใครคอมฯ ที่มี DHCP อยู่ในนี้บ้างไม่รู้ ?
    - DHCP discover, offer, request, ACK

broadcasts โดยการ

- NAT = Network Address Translation (ADSL)
  - ต้องการเปลี่ยน IP ของตัวเองข้างในโดยไม่บอก ISP ได้
  - ปัญหาการขาดแคลน address แก้ได้ด้วย IP v.6 (มี 128 bit)

① host 10.0.0.1 send datagram to 128.119.40.186,80

② NAT เปลี่ยนเป็น 10.0.0.1, 3345 — 138.76.29.7, 5001

③ ตอบกลับ Desti 138.76.29.7, 5001

④ NAT router เปลี่ยน datagram dest ถาก 138.76.29.7, 5001 to 10.0.0.1, 3345

NAT translation

WAN side	LAN side
② 138.76.29.7, 5001	10.0.0.1, 3345

1. ทำรายงานด้วยตัวเอง
2. ดูกันชัดๆ แต่ละขั้นตอนการเมล์

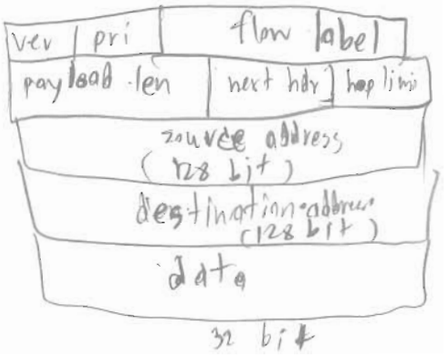
12 ก.ย. 2551

418351 Friday, September 5, 2008 ชื่อ นายชนะชัย ชำนองกย รหัสนิสิต 4911030S

บันทึกช่วยจำ

IPv6 : 32 bit ไม่เพียงพอในอนาคต

ข้อดีของ : header format ประมวลผลเร็วขึ้น forward ง่าย
header เปลี่ยนเป็น facilitate QoS



ข้อเสียเมื่อเทียบกับ IPv4 มี

checksum : ลบ entirely เพื่อ ลดการประมวลผลในแต่ละ hop

option : option ไม่เป็นส่วนหนึ่งของ header คือ การขยายของ
option ใช้วิธี point ถึง header

ICMPv6 : add "Packet Too Big"
multicast group management functions

Routing Algorithm

แบบ global : ทราบข้อมูลทั้งหมดของทั้ง Network
เป็นแบบ Dynamic : ปรับตลอดเวลา

: ทราบ ภาพรวม ของทั้ง Network และ cost ของลิงก์

- นำไปคำนวณ เส้นทางโดยใช้ link-state Algorithm

Link

Link state Algor

Dijkstra's algorithm

- ทราบภาพรวม topology เพื่อที่จะรู้ cost ของแต่ละ Nodes เรียกว่า link-state broadcast
- แล้วทุกโนดจะใช้ข้อมูลเดียวกัน
- แล้วมา คำนวณหา เส้นทางที่จะไปแต่ละโนดว่า เส้นทางที่ใกล้ที่สุด
- แล้วจะได้ forwarding table มา
- เลือกเส้นทางที่ใกล้ที่สุด

Algorithm complexity : n node

ข้อเสีย : ต้องคำนวณทุก node ที่ใช้ทราบภาพรวมทั้งหมด ใช้ $O(n^2)$

ถ้าหากทำให้ดีขึ้นได้ $O(n \log n)$

ยังมีเรื่องที่เรียนอีกหลายเรื่องที่ยังไม่ได้เขียนลงในกระดาษนี้

12 ก.ย. 2551 12

418351 Friday, September 5, 2008 ชื่อ นาย ภูดิวัฒน์ สัพเนตรโสม รหัสนิสิต 49370307

บันทึกช่วยจำ

Subnets

Ip address แบ่งเป็น 2 ส่วน
1 subnet part
2 host part

158.108.101.192 /30
.193 Getway
.194 ที่ใช้ได้
.195 → broadcast

วิธีการ routing

ยาว 16 bit
ดูตามยาวได้ไม่น่าน

- ตัวเครื่องลูกใช้ IP ที่ตั้งไว้
1 set เอง
2 ขอ address จาก server โดยอัตโนมัติ

DHCP
ขอรับ IP จาก server

- ตรวจสอบว่ามี DHCP server ในนี้
- รู้ว่า server อยู่ที่ไหน
- ขอ IP
- ได้รับ msg ที่ถูกใช้ IP ที่ขอได้

NAT Port-number เปรียบกับ นามสกุล น้องกันเอง

NAT ช่วยแก้ที่อยู่ซ้ำกัน
ช่วยลด information

ที่ไม่ต้องใช้ NAT ก็เพราะมีจำนวนที่อยู่ IPv6

NAT → หลักการคือการแปลง address

* by outside world (a security plus).

NAT : Network Address Translation

Motivation : local network uses just one IP address as far as outside world is concerned:

- range of address not needed from ISP : just one IP address for all devices
- can change address of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local net not explicitly addressable, visible*

12 ส.ค. 2551

418351 Friday, September 5, 2008 ชื่อ นายนิธิพล อุปรีคาติพงษ์ รหัสนิสิต 4932039G

บันทึกช่วยจำ

ICMP : Internet Control Message Protocol

ใช้ร่วมกับ IP, เนื่องจาก human ต้องการติดต่อกับ ... ใน ICMP

ICMP message: ขนาด 8 bytes

IPv6 : 32-bit address space

- header format helps speed processing / forwarding
- header changes to facilitate QoS

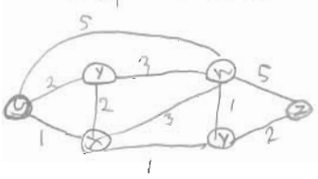
datagram format:

- fixed length 40 byte header
- no fragmentation allowed

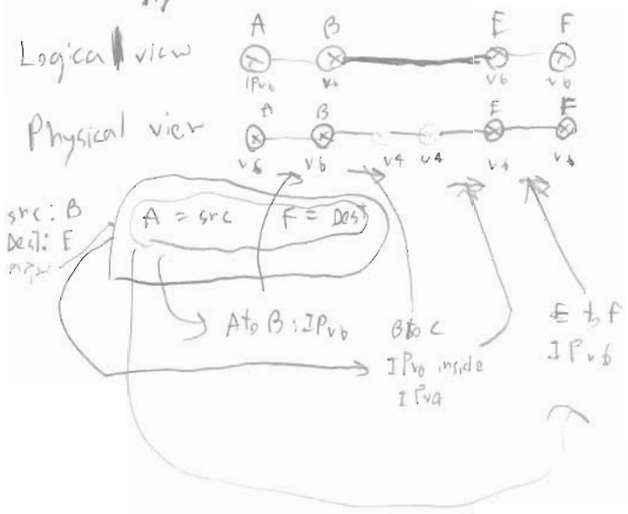
Other changes from IPv4

checksum, Options

Graph abstraction



Tunneling



12 ก.ย. 2551

418351 Friday, September 12, 2008 ชื่อ นาย ปรัชญา กนอมนาค รหัสนิสิต 49210438

บันทึกช่วยจำ

Input Port → Data ขาเข้ามา → ตรวจสอบ bit ผิดพลาด (line termination) → Landard → qveue → switching fabric → output

ทำงานใน Data link layer รับข้อมูลมาแล้ว เปลี่ยนรูปแบบ

ถ้าไม่เกิด error ส่งไปที่ qveueing

ความจำเป็น ที่ Input Port ต้องมี qveue

- เพื่อทำให้ไม่เกิด Head-of-Line blocking. (การที่ข้อมูล 2 ข้อมูล ออกทางเดียวกัน หรือมาพร้อมกัน ซึ่งจะออกไม่ได้ ต้องให้ข้อมูลหนึ่งออกก่อน ซึ่งส่วนใหญ่ Queue มาเพราะเหตุนี้)
- ถ้าข้อมูลเข้ามาเยอะ จะถูกจัดเก็บไว้ใน Queue ทำให้เกิด Queueing delay (ส่งช้า)

Output port: switch fabric → qveue → Landard → ออกสู่เส้นทางต่อไป

ทำไม Output จึงต้องมี Queue ด้วย

- หมุนทีรับ 3 พร้อมกัน จึงออก Output Port อันเดียวกัน ก็จะต้องไปเข้า Queue ก่อน

Transport layer

- TCP ข้อมูลถูกส่งถึงปลายทางแน่นอน แต่การทำงานของ TCP จะช้า เชื่องมาก
- UDP ข้อมูลถูกส่งถึงปลายทางแต่ข้อมูลอาจจะไม่ครบ แต่ทำงานได้เร็ว เช่น VDO, พวกไฟล์ภาพ

IP datagram format

ของ version ของ Program | ของความยาวของ head | ของชนิดของการให้บริการ | ความยาวของ packet = 16 bit

32 bit			
ver	head len	type of service	length
16-bit identifier		flgs	Fragment offset
time to live	upper layer	header checksum	
32 bit source IP add			
32 bit destination IP add			
options (if any)			
data (variable length, typically a TCP or UDP segment)			

จะมากกว่า 0 จะมีการใส่ค่าเพิ่มให้ Packet วนกลับมาที่เดิม เมื่อ Packet วิ่งผ่าน Router ตัวที่ 1 ทำจะลดลงที่จะ 1 และส่งไป ยัง Router ตัวถัดไป วนเรื่อยๆ จน จะทำให้ที่ set มาเป็น 0 ก็จะทิ้ง Packet

checksum ของ header จะ check ทุกครั้งที่มีข้อมูลใหม่มา

IP Fragmentation and Reassembly

MTU คือ ขนาดสูงสุดของ เฟรมที่สามารถผ่านไปได้

สมมุติ ให้ชุดข้อมูล เท่ากับ 4000 byte แบ่งเป็น Datagram ก่อนแล้วให้ MTU = 1500 byte

1) ชุดข้อมูลมี Header 20

∴ 4000 byte = 4000 - 20 = 3980 → 1480, 1480, 1020

∴ เต็มข้อมูลได้จริง 3980 byte แบ่งขนาดข้อมูลใหม่ เพื่อชุดข้อมูลใหม่

1500-20 = 1480 ∴ 8

length	ID	Frag flag	offset
4000	= x	= 0	= 0

offset แรกจะเป็น 0

1500	ID = x	= 1	= 0
1500	ID = x	= 1	= 185
1040	ID = x	= 0	= 370

(1480 + 1480)/8 = 370

ความดี อ่านหนังสือก่อนนอน

- ☐ 20 byte of TCP
- ☐ 20 byte of IP
- ☐ 40 + app layer over head

12 ก.ย. 2551 12

418351 Friday, September 5, 2008 ชื่อ พงศ์ธนพล ไชยรัตน์ รหัสนิสิต 4920461

บันทึกช่วยจำ

Ip addressing

ขนาด 32 bit

แบ่งเป็น < network / host

คลาส A /8 → 127.
- B /16 128
- C /24 192
- D /32 224.

มีกี่ subnet $2^n - 2$
host $2^{host} - 2$.

CIDR (classless Inter formain Routing)

- เป็นการอ้างอิงแบบรวม IP ตามขอบเขตของโครงข่าย ใช้สัญลักษณ์ / (slash) ตามด้วยจำนวนบิตที่

- ใช้งานแบ่งส่วน prefix หมายถึง suffix

เช่น 128.10.0.0/16.

DHCP (Dynamic Host configuration Protocol)

ตัวโปรแกรมที่ใช้การกำหนด IP address อัตโนมัติ

ทำหน้าที่ของเครื่องแม่ข่ายบนเครือข่าย TCP/IP

- DHCP sever → ปันหน้าที่ IP ให้ เครื่องลูกข่าย

ใน ช่วง เวลา ตาม ที่ ตั้ง ไว้

- เมื่อเครื่องลูกข่ายเชื่อมต่อกับ DHCP sever

① เครื่องลูกข่ายส่ง DHCP sever ในเครือข่าย โดย ใช้ DHCP discover เพื่อร้องขอ IP address

② DSCP sever ตอบกลับ IP ที่อยู่ว่างในระบบ ด้วย DHCP offer กลับไป

③ เมื่อได้รับ IP ก็จะส่งข้อความตอบกลับ DHCP Request ในลักษณะ

④ DHCP sverc ส่งข้อความ DHCP ACK ไปยัง เพื่อแจ้งว่าให้ใช้งานได้

NAT (network Address translation)

- สามารถแปลง IP แลงหนึ่งหรือหลายหมายในเครือข่ายภายในเดียวกันเครือข่ายอื่นโดยใช้ IP เครื่องเดียว

- ขั้นตอนการทำงาน

① เปลี่ยนค่าของ source IP address หรือ sver port number ให้เป็นตามที่กำหนดไว้

② แทนที่ IP ของ Packet ด้วย IP ของตัว NAT เอง

③ assign หมายเลข port ใหม่ ใน packet หรือหลักการ port เป็นต้น ตาม หมายเลขที่ตั้งไว้

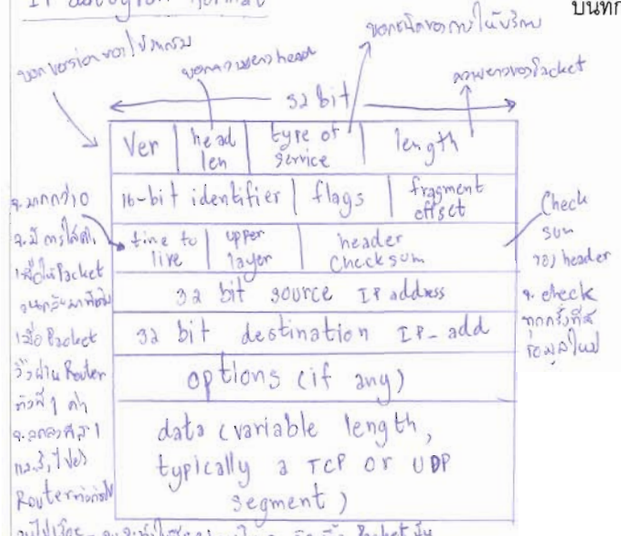
④ คำนวณ checksum ของ IP, TCP checksum ต่างๆ ใหม่ ตามข้อมูล ตาม กฎเกณฑ์

12 ก.ย. 2551

418351 Friday, September 12, 2008 ชื่อ น.ส.พัชรพรณ์ แหลือสอาดกุล รหัสนิสิต 4921051

บันทึกช่วยจำ

IP datagram format



- 20 byte of TCP
- 20 byte of IP
- = 40 + app layer over head

IP Fragmentation and Reassembly

MTU คือ ขนาดข้อมูลของเฟรม ที่ใหญ่ที่สุดที่ยอมให้ส่งผ่านได้

สมมติ ให้ข้อมูลของมูล เท่ากับ 4000 byte เพื่อแบ่ง Datagram

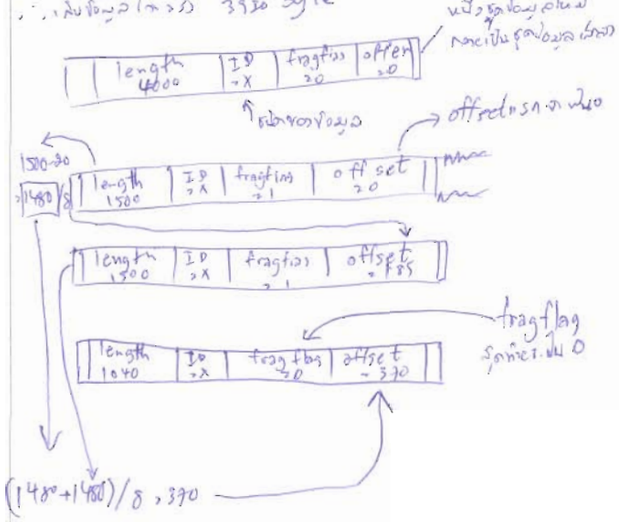
กำหนดให้ MTU = 1500 bytes

1 ข้อมูลมี Header 20

∴ 4000 byte → 4000 − 20 × 3980

∴ แบ่งข้อมูลได้ครั้งละ 3980 byte

1480
1480
1020



IP Addressing

มีขนาด 32 bit แบ่งเป็น 4 ส่วน

IP แบ่งออกเป็น 2 ส่วน < ส่วนที่ใช้ระบุ network part
ส่วนที่ใช้ระบุ host part

class A	/8	0.0.0.0 → 127.255.255.255
class B	/16	128.0.0.0 → 191.255.255.255
Class C	/24	192.0.0.0 → 223.255.255.255
Class D	/32	224.0.0.0 → 239.

192.168.100.0 / 27 → อยู่ในคลาส C/19 เหลือ 3 bit

Network IP = 192.168.100.111 XXXXX (31)

Subnet mask = 255 − 31 = 224 = 255.255.255.224

จำนวน subnet = $2^n - 2$ (n = จำนวน bit ที่ยืมมา) $= 2^3 - 2 = 6$ subnet

จำนวน host = $2^x - 2$ $= 2^5 - 2 = 30$ host

Broadcast IP = 192.168.100.255

Range host IP

subnet zero	192.168.100.0 ~	192.168.100.31
1	32 ~	63
2	64 ~	95
3	96 ~	127
4	128 ~	159
5	160 ~	191
6	192 ~	223
Broad cast	224 ~	255

Subnet mask ที่เอา bit ด้านซ้ายของสุดมา 3 bit ที่ยืมมาเป็น 1 หมด

CIDR (Classless InterDomain Routing)

- เป็นการอ้างถึงหมายเลข IP ตามมาตรฐาน โดยใช้เครื่องหมาย / (slash) ตามด้วยตัวเลขจำนวนบิต
- โดยจะแบ่งออกเป็น Prefix และใช้ร่วมกับ Suffix

เช่น 128.10.0.0 /16

* DHCP (Dynamic Host Configuration Protocol)

คือ โปรโตคอลที่ใช้ในการกำหนด IP address อัตโนมัติ แต่เครื่องลูกข่ายจะต้องรองรับโปรโตคอล TCP/IP

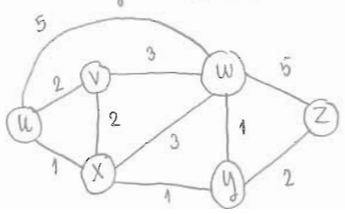
- DHCP server → มีหน้าที่แจก IP ในเครือข่ายให้กับเครื่องลูกข่ายที่ร้องขอ

ความหมาย ในเพื่อน ฝึก ปากกา

418351 Friday, September 5, 2008 ชื่อ พงศิษฐ์ เกิดเจริญ รหัสนิสิต 4921053537

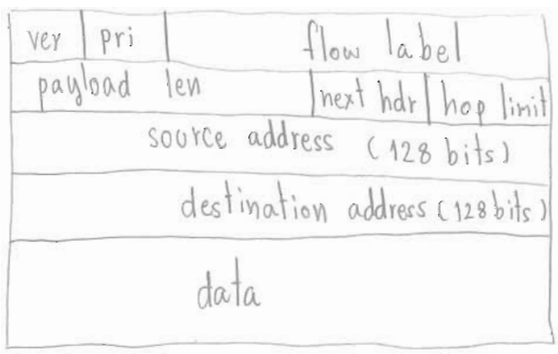
12 ก.ย. 2551 บันทึกช่วยจำ

Step	N'	D(v), p(v)	D(w), p(w)	D(x), p(x)	D(y), p(y)	D(z), p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	
2	uxy	2,u	3,y			4,y
3	uxyv					
4	uxyvw					4,y
5	uxyvwz					4,y

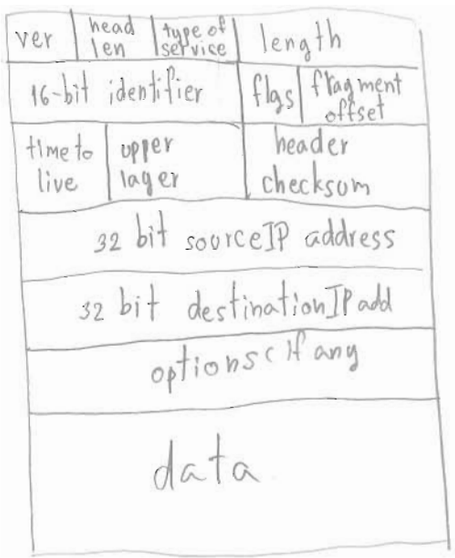


DST	PRE	COST
x	u	1
y	x	2
v	u	2
w	y	3
z	y	4

IPv6 Header



IPv4



IPV6 other Changes from IPv4

- Checksum ไม่มี checksum.
- Options ยังมีอยู่แต่แยกส่วนอยู่นอกของ header แล้ว
- ICMPV6 newVersion ตามใหม่

ความดี ไม่ได้ลอกมาจาก ซี ลอด ครับ.

418351 Friday, September 5, 2008 ชื่อ นายพิสิฐพงษ์ สินธารา รหัสนิสิต 49210545

12 ก.ย. 2551

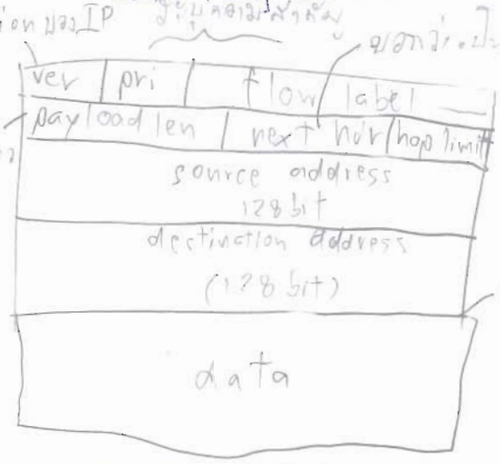
บันทึกช่วยจำ

ICMP - Type =0 Code =0 คือ echo reply อันๆ คือ ไม่เปิดหรือไม่ได้ใช้งาน

TTL - Time to Live

IPv6 - ใช้แทน IPv4 ในที่สุดจะใช้แทนหมด

- มีการกำหนดขนาดของ header ตายตัวที่ 40 byte
- ไม่มีการ Fragmentation



- Checksum - ไม่ทำ
- Option ไม่ถือเป็น header

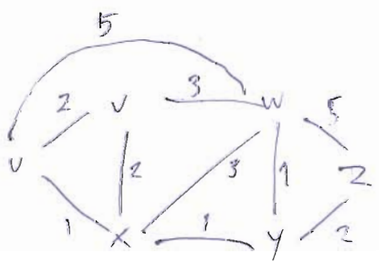
การเปลี่ยนจาก 4 → 6 ทำได้ยาก ต้องค่อยๆ เปลี่ยน โดยใช้ Tunneling มาใช้ (อุโมงค์)

การหา Routing - Global มีศูนย์กลาง - ใช้ link state (Dinamic)

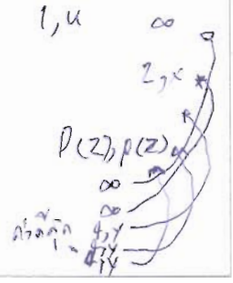
- Decentralized ไม่มีศูนย์กลาง - ใช้ distance vector

Link-State - 1) รู้ข้อมูลของทุก Node (สังเกตภาพกราฟมา) ← ขาดตรงนี้

2) หาเส้นทางที่สั้นที่สุด



step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)
0	u	2,u	5,u	1,u	∞
1	ux	2,u	4,x		2,x
2	uxy	2,u	3,y		
3	uxyv		3,y		
4	uxyvw				
5	uxyvwz				



418351 Friday, September 5, 2008 ชื่อ ภูษณาภรณ์ สังข์ช้อน รหัสนิสิต 4924956

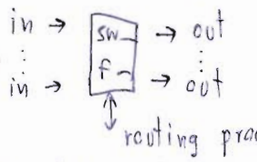
12 ก.ย. 2551 บันทึกช่วยจำ

Forwarding table
ถ้า IP ข้างหน้าเหมือนกันก็จับทิ้งไว้ แล้วจะ 0, 1 ก็จะไปที่ link นั้น เรียกว่า Prefix match

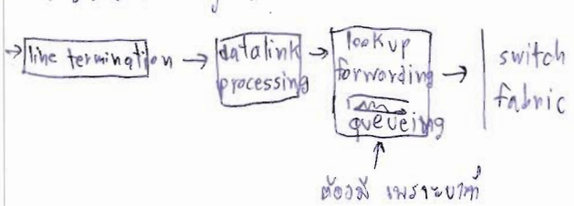
- Longest matching
  -forward packet โดยเปรียบ add ปลาย กับ add ที่เก็บอยู่ใน routing table โดยดูจาก จน. bit ที่ยาวที่สุดก่อน

- Data or vc network
  -Internet (datagrame) ยืดหยุ่น
  -ยุ่งยากในการใช้งาน
  -ภายใน network มีหลายทิศทาง
  -เครื่องปลายทางต้องจัดลำดับ
  - ATM (VC)
  -reliability (ให้เวลาที่แน่นอนได้)
  -เครื่องปลายใส่ต้องจัดลำดับ
  เช่น Tel. = ใช้ง่าย
  ภายใน = ยุ่งยาก

*what's inside a router
- การทำงานภายใน Router แบ่ง 3 ส่วน Input, output, Router ทำงาน
-switching fabric เป็นตัว forward data
ขาดล้าน 1→1 ในลักษณะที่มีทางเข้า, ทางออกปลายทาง



input port มีสายต่อเข้ามา เชื่อมี data เข้ามา Data link อ่านข้อมูลแล้วเช็คว่า error ไหม ถ้าไม่จะถอด packet ออก แล้วส่งต่อไป queve
sw_f_ จะอ่านข้อมูลก่อน ว่าจะออกไปที่ไหน อ่านเสร็จก็ไปเทียบกับ routing table

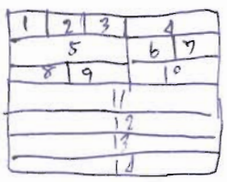


- Input Port Queuing
- Output Port จะรับได้ทีละ packet และ packet ที่ input อื่นๆ ที่ส่งมาเดียวกันนี้จะถูกยับยั้งไว้ เรียกว่า (HOL) Head_of_the_Line blocking แก้ไขโดย router จะ check packet ขับถัดไป หลังส่งก่อน

- การทำงานของ s_f_ (3 แบบ)
1. pc ทนท. เป็น router
2. Input, Output เชื่อมกันด้วย bus เร็วกว่า Mem
3. crossbar มีวงจรเชื่อม

Output Port queueing ถ้าทึบข้อมูลจนหายไป

Internet Network layer
IP datagram format



1. Version ชุดของเลขเวอร์ชั่นของ IP
2. head. len ความยาวของ header
3. type of service ลำดับชนิดรูปแบบในการจัดการกับข้อมูล
4. length ความยาวทั้งหมด
5. 16 bit identifier
6. flgs
7. fragment offset
ตัวชี้ตำแหน่ง offset ของข้อมูล
8. time to live อายุของ Datagram
9. upper layer ระบุชั้นของ Protocol
10. header checksum ตรวจสอบความถูกต้อง
11. 32 bit source IP address IP host ต้นทาง
12. 32 bit destination IP address ——→ ปลายทาง
13. Options (if any) ระบุลงในใช้ IP header เพื่อ option ต่างๆ ตามที่กำหนด
14. data

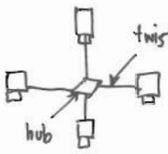
- IP Fragmentation & Reassembly
network layer จะมี MTU (ขนาดสูงสุดของเฟรม) IP Packet สามารถที่จะใหญ่ได้มากๆ แต่จุดมุ่งหมายคือ ในกรณีที่ผ่าน router 1 ไป router 1 link รองรับขนาดของ frame ได้ไม่ใหญ่เท่ากับขนาด IP Packet จะต้องแบ่งออกเป็นหลายๆ ส่วน หรือ fragment แต่ละส่วนจะมี IP header ของมันเอง และจะส่งไปที่ปลายทาง ถ้าผ่านไปยังปลายทาง แต่ละส่วนจะไม่รวมกัน จะรวมกันที่ (reassembly) เมื่อถึงปลายทาง

ความดี ทั้งชนะ ลงทั้งชนะ

418351 Friday, September 5, 2008 ชื่อ นาย มินา ทองนพเพ็ญ รหัสนิสิต 4921058๖.

12 ก.ย. 2551 บันทึกช่วยจำ

Hubs ใช้เชื่อมอุปกรณ์ com เข้าหากัน



"dumb" ไม่ฉลาด.

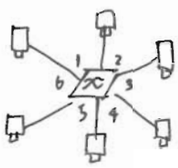
- ตอนรับ bit เข้ามา จะ copy link ที่เหลือ
- ไม่มีการ buffer frame โดยจะเก็บที่ตัวมันเอง
- ไม่ทำ CSMA/CD ทำแค่อุปกรณ์ขยายสัญญาณเพื่อระยะทางเดียว.

ข้อเสีย ไม่ช่วยลดการชนกันเลย.

Switch รับมาแล้วไปหน่อยก็ส่งแบบนั้น. (ตัวที่ทำให้เกิดการชนกันมี 2 ตัว 1. com 2. switch)

- ฉลาดกว่า Hub ไม่ต้องทำอะไร
- อ่าน frame ที่เข้ามาได้รู้ว่า MAC ต้นทางกับปลายทางคืออะไร?
- เลือก forward frame ไปที่ช่องใดช่องหนึ่งหรือหลายๆ ช่องได้.
- จะมีลักษณะ transparent (โปร่งใส) สำหรับ user คือ user ไม่ต้องไปอุ่งเกี่ยวด้วย ยังคงทำงานเหมือนเดิม.

Switch : ยอมให้มีการส่งพร้อมๆ กันได้หลายคู่



- แต่ละ link จะมีขอบเขตการเกิด collision.

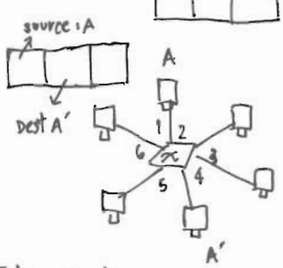
Switch Table

- ใช้กับ MAC Address ว่า MAC อันไหนอยู่กับ port ของอะไร
- รู้ว่าจะส่งไปที่ไหนเพราะมี switch table (ตอนแรกจะว่าง)

ประกอบด้วย

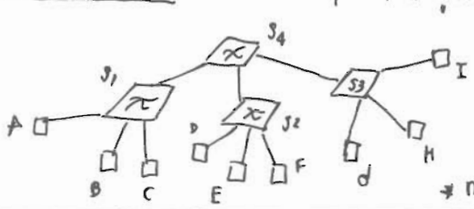
MAC	PORT	time

= interface (หัวเดียวกัน)



MAC Add	interface	TTL
A	1	60
A'	4	60

Interconnecting switches เอาสวิตช์มาต่อๆ กันได้. ทำให้รู้ว่าจะส่งไปทางไหนได้



broadcast ไปตามแต่ละเครื่อง.

* network ที่ต่อจากต้นไฮสต์ต้นหนึ่งของ router จะเป็นวง network เดียวกัน

Switches vs. Routers

- router เป็นอุปกรณ์ใน network layer
- switches เป็นอุปกรณ์ใน link layer.

Chapter 4

Network layer

- ส่ง segment ต้นทาง → ปลายทาง
- ตอนส่งเอา segment ไปใส่ capsul
- ส่งไปปลายทาง (ตอนรับ) จะแกะออกมา แล้วส่งไป transport layer.

* network layer เป็น layer ที่สูงที่สุดอยู่ใน com ทุกเครื่อง.

Two key Network-Layer Functions

Forwarding = การส่ง packet จาก router 1 → router 1

Routing = การหาเส้นทางว่าจะส่งไปทางไหนดี.

Interplay between routing and forwarding

- routing table ถูกสร้างโดย routing algorithm
- routing algor ตัวนี้ที่ update routing table
- IP Address มีความยาว 32 bit

routing algo	
local forwarding table	
header	output link
0100	3
0101	2
0111	2
4294	3

IP Address →

418351 Friday, September 5, 2008 ชื่อ นายเมธาวี จินดารักษ์ รหัสนิสิต 49210594

12 ก.ย. 2551 12 บันทึกช่วยจำ

IP Address มีขนาด 32 Bit เช่น xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

IP แบ่งเป็น 2 ส่วน < ส่วนหน้า Network Part
ส่วนหลัง Host Part

Class A	1.0.0.0 – 127.255.255.255
Class B	128.0.0.0 – 191.255.255.255
Class C	192.0.0.0 – 223.255.255.255
Class D	224.0.0.0 – 239.255.255.255

CIDR (Classless Inter Domain Routing)

- เป็นการอ้างอิงหมายเลข IP ตามมาตรฐาน โดยรู้เครื่องหมาย / ตามด้วยขนาดของมาร์ก (Mask)
- โดยแบ่งเครือข่าย = Prefix หมายเลขโฮสต์ = Suffix เช่น 128.10.0.0/16

DHCP (Dynamic Host Configuration Protocol)

คือ โปรโตคอลที่ใช้งานการกำหนด IP Address อัตโนมัติแก่เครื่องรับส่งบนระบบ

ที่ติดตั้ง TCP/IP

- DHCP Server มีหน้าที่กำหนด IP ให้แก่เครื่องรับส่งโดยไม่ซ้ำกัน เป็นการลดความผิดพลาด

NAT (Network Address Translation)

การแปลงที่อยู่ IP หลาย ๆ ตัวที่ใช้งานในเครือข่ายที่มีการต่อกับเครือข่ายอื่น โดยใช้ IP เดียวกัน

418351 Friday, September ~~5~~ 12, 2008 ชื่อ [illegible]   รหัสนิสิต 49210644

12 ก.ย. 2551

บันทึกช่วยจำ

IP Address
- ขนาด 32bit เช่น 1111111 - 1111111 - 1111111 - 1111111
- แบ่งเป็น 2 ส่วน < ส่วนหน้าเรียก net part / ส่วนหลังเรียก host part

class A /8 1.0.0.0 - 127.255.255.255
— B /16 128.0.0.0 - 191. —
— C /24 192.0.0.0 - 223. —
— D /32 224. — - 239. —

192.168.100.0/27 → อยู่ในคลาส C /19 แสดงว่ายืม 3 bit
network IP = 192.168.100.111xxxxx
subnet mask = 255-31 = 224 = 255.255.255.224
จำนวน subnet $2^n - 2$ (n → bit ที่ยืม) = $2^3 - 2$ = 6 subnet
จำนวน host = $2^y - 2$ = $2^5 - 2$ = 30 host
broadcast IP = 192.168.100.255

CIDR (Classless InterDomain Routing)
- เป็นการจัดสรร IP ตามมาตรฐาน โดยใช้เครื่องหมาย / (slash) ตามด้วยจำนวนบิต
- โดยส่วนเครือข่าย = prefix และส่วน host = suffix เช่น 128.10.0.0/16

④ จากนั้นคำนวณ IP, TCP checksum ใหม่อีกครั้ง เพื่อตรวจสอบ ค.ถูกต้อง
* NAT → ป้องกันไวรัสไม่ได้
~~ → แก้ปัญหาการขาดแคลน Add_

IP datagram format

ver	head len	type of service	length
16-bit identifier		Flags	Fragment offset
TTL	upper layer	header checksum	
32 bit source IP address			
32 bit destination IP Add			
option (if any)			
data (varible length, typically a TCP or UDP segment)			

ผ่าน Router ลดลงทีละ 1 (TTL)

เช็คความถูกต้องของข้อมูลในส่วนหัว (header checksum)

DHCP (Dynamic host Configuration Protocol)
- เป็นโปรโตคอลที่ใช้ในการกำหนด IP Address อัตโนมัติ แก่เครื่องลูกข่ายบนระบบที่ติดตั้ง TCP/IP
- DHCP sever => จะแจก IP ในเครือข่ายไม่ให้ซ้ำ (เป็นการลดความซ้ำซ้อน)

#ขั้นตอนการต่อเครื่องลูกกับ DHCP_S
1) ลูกค้นหาเครื่อง DHCP. S_ ในเครือข่าย โดยส่ง DHCP discover เพื่อร้องขอ IP Add
2) DHCP S_ จะค้นหา IP ที่ว่างอยู่ในฐานข้อมูล แล้วส่ง DHCP offer กลับให้ลูก
3) เมื่อลูกได้รับ IP ก็จะส่งข้อความตอบกลับ DHCP Request ไปยังแม่ข่าย
4) DHCP. S_ ส่งข้อความ DHCP Ack ให้ลูก เพื่อแจ้งว่าเริ่มใช้งานได้

*NAT (Network Address Translation)
- รวมกลุ่มของ IP หลายๆตัวที่ใช้ภายในเครือข่าย ให้ติดต่อกับเครือข่ายอื่นโดยใช้ IP เดียวกัน

ขั้นตอนการทำงาน
- สร้างตารางภายใน ไว้เก็บ IP Address ของเครื่องในเครือข่ายภายในที่ส่ง Packet ผ่าน NAT device
- จากนั้นจะสร้างตาราง ไว้เก็บหมายเลข port ที่ถูกใช้ไป โดย outside IP_add และ:

เมื่อมีการส่ง Packet จากเครื่องใน → นอก NAT จะ:
① บันทึก source IP add และ s_port number ไว้ในตาราง
② แทนที่ IP ของ packet ด้วย IP ขาออกของ NATd-ice
③ assign และ port ใหม่ให้ Packet และบันทึก ch port นี้ไว้ในตาราง และเก็บหมายเลขร้องใน s-p_n_ ของ packet นั้น

[illegible]

12 ก.ย. 2551

418351 Friday, September 5, 2008 ชื่อ น.ส. อรภร นารชัย รหัสนิสิต 4921065?

บันทึกช่วยจำ

TCP → ยืนยันการส่ง, data มาครบไม่ครบ (ตรวจสอบก่อนส่งให้ upper layer)

UDP → ทำงานเร็วกว่า ตรวจสอบข้อมูลแบบง่ายๆ

IP Fragmentation & Reassembly

Network layer จะมี MTU (ขนาดสูงสุดของแต่ละเฟรม) IP packet ตามธรรมดาที่ผ่านไปได้ตามขนาด แต่ถ้าเป็นกรณีที่ต้องส่งจาก router ไป router ที่ link ระหว่างนั้นมีขนาดเล็กกว่า IP packet ที่ส่งมา ก็จะต้องแบ่งออกเป็นขนาดย่อย ๆ ตาม MTU ของ fragment แต่ละส่วนนั้นจะมี IP header ของตัวเอง และจะถูกส่งไปที่ปลายทางแต่ละส่วนจะไม่ถูกรวมกันจนกว่าจะถึงปลายทาง

IP Addressing : introduction

interface คือการเชื่อมต่อระหว่าง host/router กับ link ; routers มีหลาย interface ส่วน host มี interface เดียว IP address มีขนาดกี่ bit

Subnet

ในเครือข่ายที่ต่อกันแบบ subnet part เหมือนกันอยู่ในเน็ตเวิร์กเดียวกัน ที่ต่อกันจะโดยการมี Router หลายตัวในเครือข่าย network นั้น

IP addressing : CIDR

CIDR : Classless Inter Domain Routing

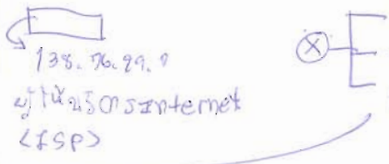
- วิธีการในการทำ Routing ที่ดูที่จำนวน bit ใน network part แบบไม่ตายตัว ดูส่วนของ subnet ตามความต้องการใช้ไม่เหมือนกัน ตามที่ผู้ดูแลระบบจะกำหนด

* ถ้าอยากได้ IP address ① ก็ code ตัวไปเซ็ตเลย window : control-panel-network → configuration → properties ← tcp

Unix : /etc/rc.config

② Protocal ที่ใช้ในการปรับค่าแบบ Dynamic address ที่ใช้ของ server ก็เหมือนกรณีที่โดนยกเลิกไป

NAT : network Address Translation



↳ Comsat > 1 เครื่อง ต้องการใช้ที่อยู่จะใช้ NAT ต่อสู่ข้อมูล ที่ web server ข้างนอก NAT ก็ทำหน้าที่แปล IP address ในส่วนของ network part เปลี่ยนเป็น

NAT ข้อดีคือ

- สามารถเปลี่ยน IP address ภายในเครือข่ายได้
- เปลี่ยนผู้ให้บริการ ISP ได้ โดยไม่ต้องไปยุ่งกับเครื่องในเครือข่าย
- ต่อกับ Internet ด้วย access เพียงอันเดียว (NAT ที่ต่อกับอินเตอร์เน็ต) หมายเลข IP address

NAT ข้อจำกัด เพื่อให้ข้อมูลออกไปข้างนอกได้ ต้องเป็น TCP ก็ได้ถูกเป็นระบบหมายเลข port ซึ่งแก้ปัญหาเรื่องนี้ NAT ต้องทำใน network layer ไปถึง port อยู่ใน header ของ TCP

② NAT ไปเปลี่ยน IP address ภายในเครือข่าย NAT ของตัวเองเท่านั้น ใช้ได้แค่ port ของตัวเอง

- NAT ทำปัญหาการกลับ address

Ex① ไฟรวันนี้ ทางผู้แปลของ ต้องการอะไรก็ได้ ก็ไม่ตอบ

Ex② ใช้ IP address ถูก 1 block ที่ IP address ถูกต่อกับอินเตอร์เน็ตได้ 120 ก็เอา NAT ถูกทำปัญหา

ปิดไฟ, พัดลม, TV ก่อนออกจากห้อง ประหยัดพลังงาน ดีๆ

418351 Friday, September 5, 2008 ชื่อ น.ส. วิภาวัลย์ เพชรสม้ากญงค์ รหัสนิสิต 4992106 93

12 ก.ย. 2551

บันทึกช่วยจำ

IP Address multicast = มีผู้รับหลายคน

interface = จุดเชื่อมต่อระหว่าง router กับ link

subnet คือ หนึ่งในเครือข่ายที่มีส่วนของ subnet part

เหมือนกัน คือ อยู่ใน network/subnet เดียวกัน = network เดียวกัน

สามารถดูได้ที่ IP Add (Ex. 223.1.1.8, 223.1.1.10)

IP Addressing : CIDR

เป็นวิธีการกำหนด Routing แบบกำหนดจำนวน bit ใน network part แบบไม่คงที่

→ มี protocol อื่นนอก protocol ที่ใช้ส่งกลับประเภท Dynamic อย่างการแจกแจง IP

DHCP (Dynamic Host Configuration Protocol)

→ ต้องมี DHCP โดยการ broadcast ~> " DHCP discover"

DHCP ตอบกลับ " DHCP offer"

Host ขอ IP Add "DHCP request"

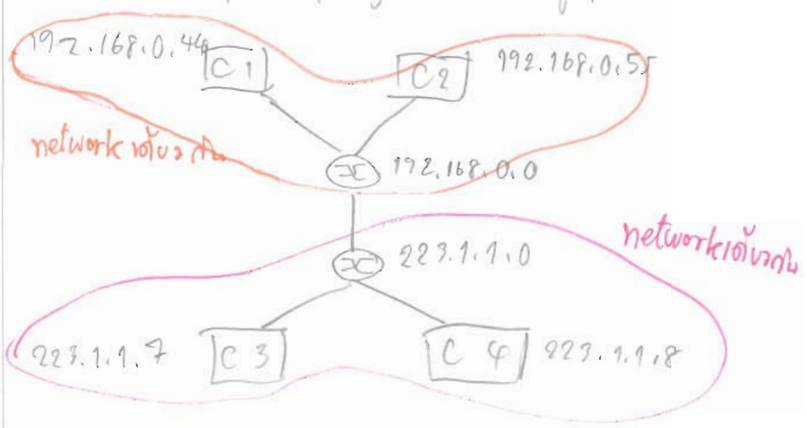
ตัวแม่ข่ายของตอบกลับโดย "DHCP Ack"

NAT → ถ้าจะ com ภายนอก เครื่องที่จะไปสามารถใช้ได้ทั้งหมดต้องใช้ NAT ช่วย

≥ สามารถเปลี่ยน IP เองเครื่องได้ (IP เก็บไว้ใน table) ← หมดเวลาต่อไม่ได้

- อย่างการแปะหัว (ปลอมตัวเพื่อหลบ)
- สามารถส่งกลับ port เดิมได้

* สรุปใน network layer ไม่ควรไปดู port ใน header ของ TCP



มาเรียนเช้าสม่ำเสมอ สีหน้าไม่สดชื่นครับคุณ

418351 Friday, September 5, 2008 ชื่อ แขมสิรยุ พิมพ์ใบ รหัสนิสิต 4921078Y

12 ก.ย. 2551 บันทึกช่วยจำ

- เรื่อง host ใช้การ Dijkstra's
ทุก node ต้องมี node A ครบในโครงข่ายรู้จัก
ทำให้คำนวณหาเส้นทางทั้ง network topology
ต้องใช้การส่งข้อมูลสั้นๆ ทุก node บางครั้งก็ล้มเหลวได้
- link state algorithm มี R ในแต่ละห้องสำหรับในแต่ละ
- เครื่องคอมกับเครื่อง host ก็ใช้ ICMP ช่วยกัน
มีการส่ง error report ถ้าส่งข้อมูลไปไม่ถึง R จะส่งกลับ
ICMP ส่วน message มา 1 อัน คือกรณี TTL expired

-IPv6
เราคาดหวัง IPv4 3 ปี ก็ไม่เลิกใช้ ต้องมีช่วงให้ครบก่อนไม่งั้นก็ล่ม
R ต้องทำงานเพิ่มขึ้น แพ็กเกจเข้ามาต้องประมวลผลส่งเข้า-ออกไม่เร็ว
40 byte header
ไม่มีการ fragmentation

ที่เปลี่ยนจาก IPv4
check sum ไม่ทำ
option ยังมีอยู่ได้ แต่ว่าจะอ้างถึงจะต้องอยู่ใน header หรือเอาไปใส่ใน data
ICMPv6 เวอร์ชั่นใหม่ของ ICMP ไม่แบ่งออกเป็น 3 fragment

IRIB คือ v4 ใช้ร่วมกันได้ ต้องมีซอฟต์แวร์ มี ตัวR
ทำให้ 2 R เรื่องกันอยู่
- global ต้องการเห็น R ของทุกเครือข่ายที่ดีที่สุด

ความดี
ง่ายเพิ่มขนาดของไปเกิ่มใช้ที่นี่

IPv6 ver 4bit Pri ความสำคัญ flow label ใช้ระบุการไหลเวียนของข้อมูล
Payload len ความยาวของข้อมูล next hdr ข้อมูลนี้จะไปที่ไหนต่อ
hop limit / source add / dest add 16byte / data

12 ก.ย. 2551

418351 Friday, September 5, 2008 ชื่อ น.ส. ศิริพร นวช่ทอง รหัสนิสิต 49210768

บันทึกช่วยจำ

IP Add multicast - มีหมู่ใช้หลายคน

interface - รูตเชื่อมต่อระหว่าง router กับ link

subnet คือ หนึ่งในเครือข่ายที่มีส่วนของ subnet part เหมือนกัน คือ อยู่ใน network (subnet) เดียวกัน ถ้าส่งไป network เดียวกัน ใช้ไม่ต้องผ่าน router = ทพ. เดียวกัน

IP Addressing : CIDR → เป็นวิธีการทำ routing แบบหนึ่ง

จำนวน bit ใน ทพ-part แบบไม่คงที่

- router → ดูความยาวได้ ไม่แน่นอน ต้องดูที่ข้างในตัวเลข

Q → ซ่ายยกได้ IP Add

→ ใช่ set เอง แต่ไม่ดี ∴ ถ้า 2 เครื่อง set ตัวเลขเหมือนกัน จะเกิดปัญหา

→ มีโปรโตคอลที่ใช้ส่ง Dynamic Add ที่ได้มา Server จะจัดการหมดให้เลย

DHCP (Dynamic Host Configuration Protocol)

- Com จะค้นหา DHCP โดยการ broadcast ว่า "DHCP discover"
- DHCP server ตอบกลับมาด้วย "DHCP offer"
- host ของ IP add ร้องขอความ "DHCP request"
- พอได้ตอบกลับ "DHCP ack"

DHCP Client - server scenario

Com → ส่งไป port ที่ต้องการ ใช้ยกก broadcast → เราตอบกลับ

→ ทำการขอใช้ → server ตอบกลับยินยอม

ISP = ผู้ให้บริการ server.

NAT

ถ้ามี Com มากกว่า 1 เครื่อง เครื่องที่จองไม่สามารถใช้ได้ทั้งหมด ต้องใช้ NAT ช่วย

NAT → สามารถเปลี่ยน IP ของเครื่องในหน่วยความจำได้

→ Com ส่งให้ NAT → NAT ทำการเปลี่ยน IP ที่เก็บอยู่ใน table → ส่งไปปลายทาง

กลับ → NAT ดูที่ปลายทางที่ส่งมาหลังทำการค้นหาใน table ว่าจะส่งไปให้ port ใด ที่เป็น port เดิม

NAT → ใช้ packet ถัดไป สร้าง table หลังหา เลข port ที่ไม่ซ้ำกับใครใน table แล้ว NAT จะจำว่าต้นทางเป็นเลขอะไร

พอจะส่งกลับ NAT จะดูจำปลายทางส่งไปที่ใด ถัดไปดูที่ table ว่าจะส่งกลับไปที่ port ใด.

port-number → หมายเลขน้อยหักที่เราอยู่

การจองเลขหนึ่ง เพื่อให้ข้อมูลมีตัวเลขที่ไม่ซ้ำใคร

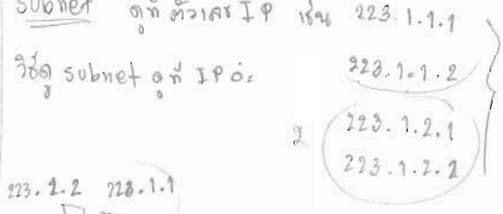
เพื่อเวลาจะส่งกลับ TCP จะได้ส่งไปที่ bit ถูก (ของ NAT).

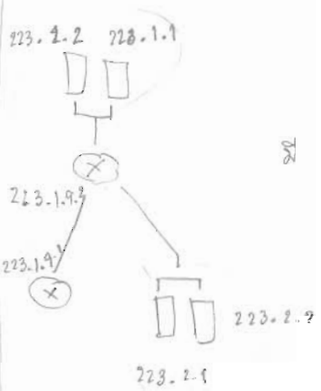
NAT → ทำงานใน ทพ layer ไม่ควรไปดู port ใน header ของ TCP

NAT ใช้แก้ปัญหาเฉพาะหน้าได้, ใช้ในกรณีที่มี add (IP) ไม่พอ.

subnet ดูที่ ตัวเลข IP เช่น 223.1.1.1

วิธีดู subnet ดูที่ IP ว่า:





มี 3 network

12 ก.ย. 2551 12

418351 Friday, September 5, 2008 ชื่อ นาย ศักดิ์ชัย นามสกุล รหัสนิสิต 4921078

บันทึกช่วยจำ

IP Address

ขนาด 32 bit แบ่ง |||||||. |||||||. |||||||. |||||||

IP แบ่งออกเป็น 2 ส่วน – ส่วนหน้าเรียกว่า Net work part
ส่วนหลังเรียกว่า host part

Class A /8 0xxx. → 127. 255.256.255
Class B /16 128.00.0 → 191. 255.255.255.
Class C /24 192.0.0.0 → 223. 255.255.255
Class D /32 224.0.0.0 → 239. 255.255.255.

192. 168.100. 0/27 อยู่ใน Class C/19 เหลือสำรอง 3 bit

Network IP = 192. 168. 100. 111xxxxx (31)
Subnet mask = 255.→31 = 224 = 256. 255. 255. 224
จำนวน subnet = $2^{n}-2$ → bit ที่ยืม = $2^{3}-2$ = 6 subnet
จำนวน host = $2^{x}-2$ → จน.ที่เหลือไปหา = $2^{5}-2$ = 30 host
Broadcast IP = 192. 168. 100. 255
Rangehost IP =

Subnet zero	192.168. 100.0	– 192.168.100.31
1	192.168. 100.32	– 192.168. 100. 63
2	192.168. 100.64	– 192.168. 100 95
3	192.168.100. 96	– 192.168.100. 127
4	192.168.100.128	– 192.168. 100. 159
5	192.168.100 .160	– 192.168 .100. 191
6	192.168.100 .192	– 192.168 .100 223
Broadcast	192.168. 100 .224	– 192. 168. 100. 255

Subnet mask = ตัวเลข bit ด้านซ้ายมือจนถึง bit ที่ยืมมาเป็นเลขฐาน
CIDR (Classless Inter Domain Routing)
- เป็นการอ้างอิงตำแหน่งเลข IP ตามจำนวนฐาน โดยใช้สัญลักษณ์ ขีดทับ (Slash) ตามด้วยขนาดของ มาสก์
- โดยแบ่งเครือข่าย = Prefix และ เครื่อง = Suffix
เช่น 128.10.0.0/16

* DHCP (Dynamic Host Configuration Protocol)
คือ โปรโตคอลที่ใช้ในการแจก IP Address อัตโนมัติ แก่เครื่องลูกข่ายในระบบเครือข่าย ที่ใช้งาน TCP/IP
- DHCP sever → มีหน้าที่แจก IP ในเครือข่าย ไปให้เครื่องในการติดต่อสื่อสาร

-ขั้นตอนการต่อ เครื่องลูกข่าย DHCP sever

① ลูกข่าย เครื่อง DHCP S_ ในเครือข่าย โดยส่ง DHCP discover เพื่อร้องขอ IP add_
② DHCP S_ จะตอบกลับ IP ที่ว่างอยู่ในฐานข้อมูล แล้วส่ง DHCP offer กลับไปให้ลูก
③ เมื่อลูกได้รับ IP ก็จะส่งข้อความกลับ DHCP Request ไปให้แม่ข่าย
④ DHCP S_ ส่งข้อความ DHCP Ack ให้ลูก เพื่อแจ้งว่าให้ใช้งานได้

* NAT (Network Address Translation)
- สามารถแปลง IP แหล่งต้นทางที่ใช้งานในเครือข่าย ให้สื่อสารต่อกับเครือข่ายอื่นโดยใช้ IP เดียวกัน

-ขั้นตอนการทำงาน
เมื่อ NAT เริ่มทำงาน มันจะสร้าง ตาราง การแปล ซึ่งมีไว้เก็บ แม็ป เลขที่อยู่ IP Add ของเครื่อง ในเครือข่าย ที่ส่ง packet ผ่าน NAT device และจากนั้น มันจะสร้าง ตารางไว้เก็บบันทึกเลข Port ที่ถูกใช้ไปโดย Outside IP add_ ตอนเมื่อมีการส่ง Packet จาก เครือข่าย ใน → นอก NAT ดังนี้
① บันทึกข้อมูล source IP add_ และ S_ port number ไว้ในตารางที่เตรียมไว้
② แทนที่ IP ของ packet ด้วย IP ของNAT ด้วยตัวเอง
③ สลับหมายเลข Port ในส่วน packet และบันทึกค่า Port นี้ ไว้ใน ตาราง เพื่อทำแบบเดียวกันในส่วน S_P_N_ ของ packet ขาเข้า
④ คำนวณใหม่ค่าของ IP, TCP checksum ขึ้นมาใหม่ เพื่อตรวจสอบ ความถูกต้อง

* NAT → ป้องกันไวรัสไม่ได้
* → แก้ปัญหาการขาด แคลน Add_

ตอนจบ : ไปส่งเพื่อนที่เดินทางกลับบ้านกลับบ้าน

12 ก.ย. 2551 12

418351 Friday, September 5, 2008 ชื่อ นายกฤตสมาส์ สวนโยลว รหัสนิสิต 4921079Z

บันทึกช่วยจำ

Chapter 4

host กะ com ใช้ ICMP ร่วมกัน

ส่ง error report - ถ้า host ส่งข้อมูลไม่ถึง

router ปลายทางจะ ตอบกลับมาให้

ตอบกลับ ICMP สร้าง message 1 อัน TTL expired

message ส่งออกเส้นเดิมตรง

IPv6 มาตรฐานที่ IPv4 32 บิต ไม่พอใช้

IPv6 มี 128 บิต

router ช่วยทำงานหนัก ถ้า packet เข้ามาหลายทาง

ช่วยคำนวณให้เร็วขึ้น

IPv6 มี 46 byte header ไม่ให้ทำ fragmentation

V. 4 bit Pri ลำดับสำคัญ

flow label . IP มาจาก flow เดียวกัน

payload len ความยาวของ data ข้างล่าง

next header ข้อมูลเช่น protocol อะไร hoplimit

IPv6 ทำเปลี่ยนแปลงจาก IPv4

Checksum ไม่ทำ

Option ถ้ามีอยู่ ไม่มีอยู่ในส่วนของ header

แยกอยู่ใน data

ICMPv6 เวอร์ชันใหม่ของ ICMP ไม่ยอมออก

เป็น 3 flagment

MTU → Maximum Transfer Unit

IPv6 กะ IPv4 ใช้ร่วมกันได้ต้องใช้อุโมง

มี delay นิดนึง ทำให้ 2 router เชื่อมต่อกัน 2 IP

IPv6 ทำงานได้เกือบทุกอย่างที่ IPv4 ทำได้

Global ช่วยการข้อมูลของ router และการ

เลือกทางที่ดีที่สุด

อัลกอริทึม Dijkstra's

- จาก node ตัวเอง ไปยัง node ต่างๆ เลือกเส้นทาง

ที่ใกล้ที่สุด

- ทำยังไงจะได้ภาพล่าสุดของทั้ง network topology

- ต้องใช้การส่งข้อมูลไปทุกๆ node

- คำนวณเส้นทางที่น้อยที่สุด

- ถ้ามี router ใหม่ ลงต้องคำนวณใหม่ทุก

router

ข้อสอบไล่อัลกอริทึม

ความดีที่ทำในวันนี้

ไม่รบกวนการสอนของอาจารย์ โดยการขอยกเลิกเรียนทั้งตามเส้นย เรียน

12 ก.ย. 2551

418351 Friday, September 5, 2008 ชื่อ น.ส.สุพิชา เชื้องจันทร์ รหัสนิสิต 49270500

บันทึกช่วยจำ

CSMA/CD efficiency

T_{prop} = เวลาที่สัญญาณเดินทางจากจุดหนึ่งไปยังจุดหนึ่งที่ห่างกันมากที่สุด เช่น รถไปรับเพื่อน

T_{trans} = เวลาที่ใช้ในการส่ง frame ที่ใหญ่ที่สุด ขนาดจะต่างกันที่ data เช่น สามารถเอาคนขับใส่รถไปได้มากแค่ไหน

$$efficiency = \frac{1}{1 + 5t_{prop} + t_{trans}}$$

tran น้อย collision น้อย

tran มาก collision มาก

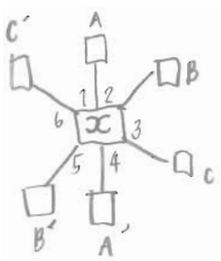
- Hub => "dump" ไม่ฉลาด ตอบรับ bit เข้ามาจะ copy link ทั้งหมด ไม่มีการ buffer fram เก็บที่ตัวมันเอง ไม่ช่วยลด การ collision ไม่ทำ CSMA/CD ทำแต่อุปกรณ์ขยายสัญญาณเพื่องอย่างเดียว
- Switch => ตัวที่ทำให้เกิดการแชร์กันมี 2 ตัว คือ

1. com 2. switch
   - อ่าน frame ที่เข้ามาได้
   - เลือก forward fram ไปช่องใดช่องหนึ่งได้

ข้อดี transparent => โปร่งแสง

คือ user ไม่ต้องรู้เกี่ยวกับอุปกรณ์ในการทำงานเหมือนเดิม

- ของมีให้ส่งข้อมูลกันหลายๆ คู่ แต่ link จะมีขอบเขตของการเกิด collision



- Switch Table => ตารางเอาไว้เก็บ MAC address ว่า MAC อะไรอยู่ที่ port เบอร์อะไร
- Interconnecting switches => เอาสวิทช์มาต่อกัน ก็ไม่รู้ไง broadcast ไปแต่ละเครื่อง
- Institutional network => network ที่ต่อจากด้านใดด้านหนึ่งของ Router จะเป็นของ network เดียวกัน

@ chapter 4

- Network layer => ส่ง segment จากเครื่องต้นทางไปยังปลายทาง (segment => ชื่อเรียกก้อนข้อมูล)
- Two Key Network-Layer Functions
  - forwarding => ส่ง packet จาก router หนึ่งไปอีก router หนึ่ง
  - routing => ก่อนทำก่อน forwarding คือ การหาเส้นทางที่จะส่งไปทางไหนดี

@ Virtual circuits => เรียก setup

-Virtual circuits : signaling protocols

ATM => Asynchronize Transfer Mode

@ Datagram or VC network

Datagram	VC network
- การส่ง data ของ com ขัดหน่อย, ไม่สามารถการันตีเวลาในการส่งมาถึงได้	- กำหนดการร้องเวลาในการส่งที่แน่นอนได้, เชื่อถือได้
- อุปกรณ์ตรงไม่ซับซ้อน แต่อุปกรณ์ที่ต่อต่างกัน ผู้ใช้จะฉลาด	- ข้างนอก dump ไม่ฉลาด - ข้างใน ฉลาด กว่า

ความดี " ขี้งบ: ลงดังบ: "

12 ก.ย. 2551

418351 Friday, September 5, 2008 ชื่อ น.ส. สุนิสา ของชัยทอง รหัสนิสิต 49210818

บันทึกช่วยจำ

-IP add
สัมผัส 32 bit แบ่ง ๔ ส่วน | IP แบ่ง ๒ ส่วน (ส่วนหน้า = network part, หลัง = host part)

A /8 1.0.0.0 → 127.255.255.255
B /16 128.0.0.0 → 191.๑.๑.๑
C /24 192.0.0.0 → 223.๑.๑.๑
D /32 224.0.0.0 → 239.๑.๑.๑
E ex 192.168.100.0 /27 → อยู่ C / 27 แสดงว่ายืม 3 bit
Network IP = 192.168.100.111xxxxx
Subnet mask = 255.255.255.224 = 255.๑.๑.224
จน. subnet = $2^n - 2$ → bit ที่ยืม = $2^3 - 2 = 6$ subnet
จน. host = $2^5 - 2 = 30$ host
Broadcast IP = 192.168.100.255
Range host IP subnet zero 192.168.100.๑ — 192.168.100.31

1	32 –	63
2	64 –	95
3	96 –	127
4	128 –	159
5	160 –	191
6	192 –	223
Broadcast	224 –	255

sub-net = ตัวแสดง bit ที่ยืมส่วนของ bit ที่ยืมออกเป็น network

* CIDR classless Interdomain Routing
- เป็นการอ้างอิงแทนการแบ่ง IP ตามคลาสการใช้ /(slash) ตามด้วยจำนวนของ subnet
- ใช้แสดงหมายเลข = prefix และ เครื่องหมาย = suffix
เช่น 128.10.๐.๐ /16
* DHCP (Dynamic Host configuration protocol)
คือโปรโตคอลที่ใช้กำหนดค่า IP Address อัตโนมัติ แก่คอมพิวเตอร์ในระบบที่ตั้งค่า TCP/IP
* DHCP sever → สำหรับเก็บ แจก IP ในเครือข่าย ไม่ใช้สำหรับการ Add ครั้งต่อไป
- ขั้นตอน การทำงานของเครื่องลูกกับ DHCP s—
① ลูกข่าย ส่งเครื่อง DHCP s— ในเครือข่าย โดยส่ง DHCP discover เพื่อร้องขอ IP add—
② DHCP s— ค้นหา IP ที่ว่างอยู่ในฐานข้อมูล แล้วส่ง DHCP offer กลับให้ลูก
③ เครื่องลูกได้รับ IP ก็จะส่งข้อความตอบกลับ DHCP Request ไปให้แน่ใจ
④ DHCP s— ส่งข้อมูลการ DHCP Act ให้ลูก เพื่อเสร็จสิ้นการใช้งานได้

ตำแหน่งข้อมูลแต่ละส่วน ต้องบอกตำแหน่งที่ของตัวเอง offset ตำแหน่งข้อมูล fragment ชิ้นนี้อยู่ตรงไหนของ Datagram เดิม

1440/8 = offset ต้องเป็น 8byte เท่านั้น ถึงจะ, เพราะ บิตสุดท้ายคือ flag

NAT (Net Add— Translation)
- ต้องการแปลง IP ภายในองค์กรที่ใช้ ติดต่อกับเครือข่ายอื่นโดยใช้ IP เฉพาะตัว
-ขั้นตอนการทำงาน
เครื่อง NAT จะต้องทำงาน ร่วมกับเราเตอร์ ซึ่งผู้ใช้งานจะใส่ IP Add— ของเครื่องในเครือข่ายภายในที่ต้องการ packet ผ่าน NAT device และมีการกำหนด ช่วง port ที่ถูกใช้ไปโดย outside IP add— และเมื่อมีการส่ง Packet ออกจากเครื่องภายใน → นอก NAT จะ
① บันทึกโดยดู source IP add— และ s— port number ไว้ในตารางที่กำหนดไว้
② เปลี่ยน IP ของ packet ด้วย IP ของ NAT d— แทน
③ assign และ port ใหม่ให้ pac— และบันทึกค่า Port ไว้ในตาราง และเพิ่มค่าลงในช่อง s— p— n— ของ Packet นั้น
④ ยกเว้น จะต้องแก้ IP, TCP checksum ด้วยเพื่อความถูกต้อง
* NAT → ข้องกันไฟร์วอลล์ได้
แก้ปัญหาการขาดแคลน Add—

*IP datagram format

① Ver. = เลขของรุ่นของ IP (20byte)
② head len = ความยาวของ header
③ type of service = กำหนดรูปแบบการให้บริการกับข้อมูล
④ length = ความยาวของ IP pa— (65535)
⑤ 16-bit identifier = ทำ fragmentation
⑥ flgs = กำหนด data ในการทำ fragment ว่าได้แยกส่งหรือไม่
⑦. fragment offset = ตำแหน่ง offset ของข้อมูล
⑧. time to live = อายุของ data —
⑨ upper layer = ระบุชนิดของโปรโตคอล
⑩ header checksum = ตรวจสอบ error ของ h—
⑪ 32 bit source IP add— = ต้นทาง
⑫ ความยาว destination = ปลายทาง
⑬ options = ของเพิ่มให้ IP ใช้— เพิ่ม op— สำหรับการทดสอบ
⑭ data = field ข้อมูล

20 TCP } 40 + applayer overhead
20 IP } * ถ้าไม่มี TCP ไม่ต้อง + เท่ากัน

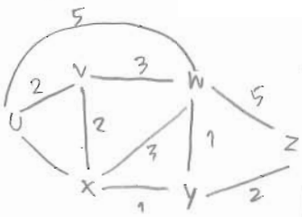
กรอบสี่ เสี่ยงสุขสิงให้คนรู้จัก ทำบุญปล่อยปลา

CIDR
- เป็นการอ้างอิง หมายเลข IP ตามมาตรฐาน โดยใช้เครื่องหมาย / ตามด้วยจำนวนบิตของ subnet
- โดยเลขเครือข่าย = Prefix และ เลข host = suffix
เช่น 128.10.0.0/16.

DHCP
- โปรโตคอลที่ใช้ในการกำหนด IP address อัตโนมัติในเครื่องลูกข่ายขนาดเล็กที่ติดตั้ง TCP/IP
DHCP Server → มีหน้าที่แจก IP ในเครือข่ายไม่ให้ซ้ำ เป็นการลดความซ้ำซ้อน

NAT
- สามารถแปลง IP หลายๆตัวที่ใช้ภายในเครือข่าย ให้ติดต่อกับเครือข่ายอื่นโดยใช้ IP เดียวกัน ในขณะการทำงาน.
เมื่อ NAT เริ่มทำงานมันจะสร้างตารางภายใน ซึ่งมีไว้สำหรับเก็บข้อมูล IP address ของเครื่องในเครือข่ายภายในที่ส่ง packet ผ่าน NAT device และจากนั้นมันจะสร้างตารางไว้เก็บหมายเลข Port ที่ถูกใช้ไปโดย outside IP address และเมื่อมีการส่ง Packet จากเครือข่ายใน ไป นอก
NAT มี 2
1. บันทึกข้อมูล source IP address และ subnet number ไว้ในตารางที่เกี่ยวข้อง
2. แทนที่ IP ของ packet ด้วย IP ออกของ NAT ของ
3 assign เลข Port ใหม่ให้ Packet และบันทึกค่า Port นี้ไว้ในตาง และทำการแทนค่าหมายเลข Subnet port ของ packet นั้น
④ จากนั้นจะคำนวณหา IP, TCP checksum อีกครั้ง เพื่อตรวจสอบความถูกต้อง.

Step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	4,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					4,y



DST	PRE	COST
x	u	1
y	x	2
v	u	2
w	v	3
z	y	4

IP หน่วย — ส่วนหน้าเรียก network part
ส่วนหลัง — host part

class A	18	0.00 → 127.255.255.255
B	16	128.00 → 191. — —
C	24	192.00 → 223
d	32	224 — → 239.

192.168.100.0/27 → อยู่ใน class C/19 ยืม 3 บิต
Network IP = 192.168.100.111 xxxxx
subnet mask = 255-31 = 224 = 225.255.255.224
จำนวน subnet
จำนวน host
Broadcast IP
Range host IP

418351 Friday, September 5, 2008 ชื่อ สุรเดชรัฐ แซ่จึง รหัสนิสิต 4921085?

12 ก.ย. 2551 บันทึกช่วยจำ

IP Addressing ขนาด 32 bit

IP แบ่งออกเป็น 2 ส่วน { ส่วนหน้า network part / ส่วนหลัง host part

Class

A	/8	1.0.0.0	→ 127.255.255.255
B	/16	128.0.0.0	→ 191
C	/24	192.0.0.0	→ 223
D	/32	224.0.0.0	→ 239

192.168.100.0/24 → อยู่ในคลาส C /24 หมายถึงยืม 3 bit

Network IP : 192.168.100.111 xxxxx

subnet mask : 255-31 = 224 = 255.255.255.224

จำนวน subnet : $2^n - 2$ (n = จำนวนบิตที่ยืม) $= 2^3 - 2 = 6$ subnet

จำนวน host $= 2^5 - 2 = 30$ host

Broadcast IP : 192.168.100.255

Forgehost IP

subnet zero	192.168.100.0 —	192.168.100.31
1	32 —	63
2	64 —	95
3	96 —	127
4	128 —	159
5	160 —	191
6	192 —	223
Broadcast	224 —	255

subnet mask : ตัวเลข bit ด้านซ้ายมือจนถึง bit ที่ยืมมาสุดท้าย

CIDR (Classless InterDomainRouting)

- แบ่งการจัดสรรและการกำหนด IP ตามความต้องการใช้งาน / ตามขนาดของ mask
- โครงสร้างเครือข่าย : Prefix คือ network + suffix

เช่น 128.10.0.0/16

DHCP (Dynamic Host Configuration Protocol)

คือโปรโตคอลที่ใช้ในการกำหนด IP Address อัตโนมัติ เครื่องลูกข่าย และแม่ข่ายที่ติดตั้ง TCP/IP

- DHCP server → มีหน้าที่แจก IP ในเครือข่ายให้กับเครื่องลูกข่ายที่ร้องขอ
- ขั้นตอนการทำงานของ DHCP server

① ลูกข่ายที่ต้อง DHCP ส่ง ในเครือข่ายไปยังเครื่อง DHCP discover เพื่อร้องขอ IP Add

② DHCP ส่ง ตอบกลับ IP ที่ว่างอยู่ในฐานข้อมูลกลับไปยังลูกข่าย DHCP offer กลับไปให้ลูก

③ เมื่อลูกข่ายได้รับ IP จะส่งข้อมูลยืนยันกลับไปยัง DHCP Request ไปที่เครื่องแม่ข่าย

④ DHCP ส่ง ข้อมูลยืนยัน DHCP Ack ให้ลูกข่าย เพื่อยืนยันว่าเครื่องนี้ใช้งานได้

NAT (Network Address Translation)

- สามารถแปลง IP ของเครื่องที่ใช้งานในเครือข่ายให้ติดต่อกับเครือข่ายอื่นได้ โดยใช้ IP เดียวกัน
- ขั้นตอนการทำงาน

เมื่อ NAT เริ่มทำงานครั้งแรก จะสร้างตารางภายในขึ้นมาเพื่อใช้สำหรับเก็บข้อมูล IP Add ของเครื่องในเครือข่าย ขณะที่ส่ง Packet ผ่าน NAT device และจากนั้นจะสร้างตารางใช้เก็บหมายเลข Port ที่ถูกใช้ไปกับ outside IP Add และขั้นตอนการส่ง Packet จากเครื่องข่ายใน → นอก NAT มี

① ย้ายที่อยู่ source IP Add และ S_Port number ไปไว้ในตารางที่เตรียมไว้

② แทนที่ IP ของ Packet ด้วย IP ของตัว NAT เอง

③ assign เลข Port ใหม่ ให้ Packet และบันทึกค่า Port ที่ใช้ไว้ในตาราง และค่าของค่าที่เปลี่ยนใน S_P_n ของ Packet นั้น

④ จากนั้นจะคำนวณค่า IP, TCP checksum อีกครั้งเพื่อตรวจสอบความถูกต้อง

NAT → ฝั่งต้นไม่รู้จักใช่ไม่ได้

→ แก้ปัญหาการขาดแคลน Add

IP datagram format

① เลข ver. ของ IP

② head len = ความยาวของ header (20byte)

③ type of service = กำหนดรูปแบบการให้บริการจัดลำดับ

④ length = ความยาวทั้งหมดของ IP Pa (65535

⑤ 16 bit identifier

⑥ flags กำหนด data ในการทำ fragment ว่าเป็นแบบสุดท้าย

⑦ fragment offset : ชี้ตำแหน่ง offset ของข้อมูล

⑧ TTL : อายุของ data

⑨ upper layer ระบุชนิด Protocol

⑩ reader checksum ตรวจสอบความถูกต้องของ h

⑪ 32 bit source IP add ต้นทาง

⑫ 32 bit des ปลายทาง

⑬ options : ของใน IP h เพื่อ op ต่างๆตามที่กำหนด

⑭ data : field สุดท้าย

20 TCP
20 IP
} ตอ + app layer overhead

* ถ้าใช้ TCP ใส่ต้อง + ให้ด้วย

ค.ศ. ปีพ.ศ. ในหลวงแก้ว (ตอนเรียน)

418351 Friday, September 5, 2008 ชื่อ ไกรณ รหัสนิสิต 4921087 5

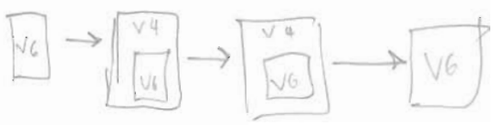
12 ก.ย. 2551 บันทึกช่วยจำ

IP ver. 6

- IP ver.4 32bit ได้ IP 4,000ล้านIP ปัจจุบันใช้หมดแล้ว
- V.6 มี header ขนาด 40 bytes
- ไม่มีการ fragment
- V6 ไม่มีส่วน ของ option เป็นส่วนหนึ่งของ Header

ทางไม่ดี ไม่ใช้ V6 ทั้งหมดเลย = ไม่สามารถเปลี่ยนของใครๆ ทุกๆคนในโลกได้ ต้องใช้ทางเลือก

- การเริ่มใช้ IP v.6 ไปใช้กับ v.4 จะทำให้เกิด Delay ขึ้นตามมา



G = (N,E)

N = จำนวนโหนด ; A,B

E = เส้นเชื่อม ; (AB)(CV)

C = Cost หรือ ระยะทางที่ใช้จากnodeถึง node ; C(AB) = 5

distance vector → cost — การหาเส้นทางโดยการดูจากnode ข้างๆแล้วนำมาคำนวณหาเส้นทางที่สั้นที่สุด (ไม่รู้ภาพเส้นทาง)

Dijkstra — ทุกnodeจะรู้ทางไปถึงทุกnode ที่จะได้เส้นทางเหมือนกัน (ได้ภาพเส้นทาง)

C(x,y) = ค่าเลน (ถ้าไม่มีเชื่อมจะเป็น ∞)

D(v) = ค่าของcostของnodeไป node ; A → B → C = D(C)

P(v) = จำ node ก่อนหน้าของ V

N' = set ของ node ที่ผ่านไปแล้ว

```
1  initialization
2  N' = {u}
3  for all nodes v
4    if v adjacent to u
5    then D(v) = C(u,v)
6    else D(v) = ∞
7
8    Loop
9    find N'
10   add w to N'
11   update D(v)
12   D(v) = min(D(v), D(w) + C(w,v))
13 until all node in N'
```

Application

Ex

step	N'	D(v),P(v)	D(w),P(w)	D(x),P(x)	D(y),P(y)
0	u	2,u	5,u	∞	∞
1	uv	2,u	5,u	4,x	∞
2	uvx	2,u	5,u	4,x	11,x
3	uvxw	2,u	5,u	4,x	11,x

การสร้าง Routing Table

Ex

destination	link
v	(u,v) 1
x	(u,x) 2
y	(u,x) 2
w	(u,x) 3
z	(u,x) 4

ICMP : Internet Control Message Protocol

...

...

IPv6

... → ... 128 bit, ... 40 byte header

IPv6 ... IPv4

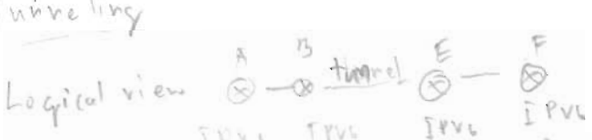
- no "flag days" (check same ... 7), IPv6 ... IPv4

IPv6 ... ICMP ... fragment

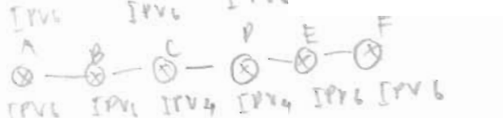
IPv6 ... IPv4 ...

Tunneling

Logical view



Physical view



Graph abstraction

graph : G = (N, E)

N = set of routers = {u, v, w, x, y, z}

E = set of link {(u,v), (u,x), (v,x), (v,w), (x,w), (x,y), (w,y), (w,z), (y,z)}

...

...

Switch จะออกไปที่สถานีส่งเพื่อเดินไปยังปลายทางคู่

- switch เป็นต้นทางของข้อมูล
- ปัญหาจะเกิดขึ้น 2 เหตุการณ์นี้
  - ปลาย link จะมีจานเพจของการเกิด collision

switch table คู่กับ MAC address

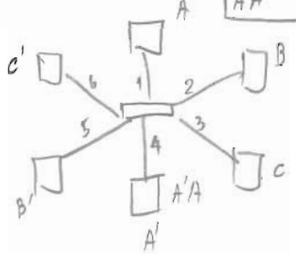
MAC	PORT

- switch จะรู้ได้ว่าแต่ละเครื่องอยู่ของใคร ∴ มี switch table
- time stamp = ของเวลาที่ใน MAC address เข้ามา
- ลักษณะคล้าย routing table

switch : Self-learning เรียนรู้ได้ด้วยตัวเอง

MAC addr.	interface	TTL
A	1	60
A'	4	60

source : A
Dest : A'
AA'



network ที่ต่างกันคือด้านหนึ่งของ router จะเป็น 2 network เสมอกัน

Switch vs Router

- router ⇒ อุปกรณ์ใน network layer
- switches ⇒ อุปกรณ์ใน link layer

บทที่ 4 Network Layer

Network layer

- ส่ง segment จากต้น → ปลาย
- ในขาจะ encapsulates

Two key Network-Layer Functions

- forwarding = ส่ง packet จาก router 1 → 1
- routing = หาเส้นทางที่จะส่งไปปลายทางใน

Interplay between routing and forwarding

router หาผ่านไปแต่ละ router ใน

ในคู่ใน routing table

Network layer connection and connection-less service

- เป็น network protocal ที่ให้บริการ connectionless

virtual circuit and datagram networks

- datagram network ให้บริการ connectionless
- vc ให้บริการ connection

- VC : signaling protocols
  - ต้น → ปลาย ของส่ง หลังปลายทางของสัญญาณส่ง
- Datagrame network (จะส่งเลย)
  - แบบ connectionless
  - ทางผ่าน router ไม่รู้จักจะต้นทางปลายทาง เช่น ส่ง e-mail

Forwarding table

ถ้า IP จากหน้าตาเหมือนสัญญาณ ที่จากจะ 0,1 ก็จะไปที่ link นั้นๆ เรียกว่า Prefix match

- Langest watching

forward packet ในขาใน address ปลาย กับ address ที่อยู่ใน routing table ในคู่จาก คน. bit ที่ตรงกันต่อกัน

ก้องภาคูณ 12, 2008

418351 Friday, September 5, 2008 ชื่อ น.ส. อัธรา ขุยมาเลิศ รหัสนิสิต 4912109127

12 ก.ย. 2551

บันทึกช่วยจำ

Router Architecture overview

แบ่งได้ 3 ส่วนหลัก ① Input ② output ③ การทำงาน

Switching Fabric: ตัวนำ forward data ที่มีทางเข้าและทางออกหลายทาง

Input Port: มีสายต่อเข้ามาเมื่อ data เข้ามา Data link ที่อ่านข้อมูลแก้ไข error ถ้าไม่ error ก็ส่ง Packet ออกไปเก็บที่ queue (queue มีเพื่อช่วย switch fabric ทำงานไม่ทัน) switch fabric จะผ่านขึ้นอยู่กับว่าจะไปออกที่ไหนแล้วจะเทียบกับ routing table ว่าออกออก output port ไหน

Input Port Queuing

Switch fabric ทำงานไม่ทันจะมีการใช้ queues ก่อนตัว queue เต็มข้อมูลจะสูญหาย

ถ้า port ที่แลว่างจะออกทางเดียวกันทำงานพร้อมกันไม่ได้ต้องรอไปก่อน

การทำงานของ switch fabrics มี 3 แบบ

① PC เป็น router

② in/out put เชื่อมกันผ่าน bus เข้าหา memory

③ มีวงจรเชื่อม Input output ผ่านตารางเชื่อมต่อกับทุก output port

Output Ports มี queue ทางฝั่ง router

จากที่มาเชื่อมต่อที่สายส่งข้อมูลกลับ

Buffering

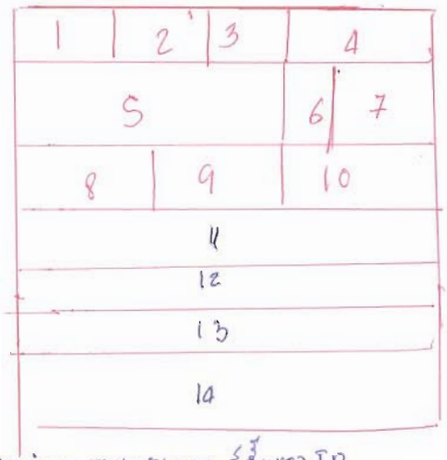
Scheduling

output Port queueing ตัดสินใจข้อมูลออกมาได้

* Binary exponential Backoff → อัลกอริทึมทำให้โอกาสในการชนกันของข้อมูลมีน้อยลง เมื่อจำนวนครั้งของการชนกันมากเครื่องของข้อมูลมีมากขึ้น

Internet Network layer

IP datagram Format



1 > version. ของ IP

2 > head len ความยาวของ header

3 > type of service กำหนดชนิดของข้อมูลที่ส่งไป

4 > length ความยาวทั้งหมด หน่วยเป็น 16 bit

5 > 16 bit identifier

6 > flags } ตัวบอกตำแหน่ง offset ของข้อมูล

7 > fragment offset

8 > time to live อายุของ datagram

9 > upper layer ระบุโปรโตคอล Protocol

10 > header checksum ตรวจข้อผิดพลาดของข้อมูล

11 > 32 bit source IP address → IP host

12 > 32 bit destination IP add. → IP host ปลายทาง

13 > options (if any) ของ IP header

14 > data

* Binary exponential Backoff → อัลกอริทึมทำให้โอกาสในการชนกันของข้อมูลมีน้อยลง เมื่อจำนวนครั้งของการชนกันมากเครื่องของข้อมูลมีมากขึ้น

418351 Friday, September 5, 2008 ชื่อ [illegible] รหัสนิสิต [illegible]

12 ก.ย. 2551 บันทึกช่วยจำ

NAT : network address Translation
- การแปลง IP ที่ router ไม่ต้องยุ่ง
- เหมือนเป็นเครื่องเดียวกับ IP ที่ได้รับ

ICMP : ใช้โดย host และ router เพื่อ
ติดต่อ network-level
- แจ้งกลับ router ปลายทาง ไม่ได้
echo request (ping) ใช้ตรวจสอบ
ว่าเครื่องปลายทางยังเปิดอยู่

Traceroute
ส่ง UDP ไปปลายทาง และจะถูก drop
router TTL

ICMP
ตัวอย่างที่ได้การใช้ drop
ข้อความ ICMP
- ถูก drop
- ส่ง host ไปแจ้ง error

IPv6
- ขยายจาก IPv4
- ปรับปรุงคุณภาพการให้บริการ
สิ่งที่ไม่มีใน IPv4
- ไม่มี checksum
- ไม่มีก็ต้องเพิ่มขึ้นมาที่ header
(option)
- มี ICMP เพิ่มขึ้นมาสำหรับ v.นี้

เปรียบเทียบ IPv6 และ IPv4
- ไม่สามารถเปลี่ยนได้ง่ายเหมือนที่ได้ยาก
- มีปัญหาว่า IPv4 กับ IPv6 ใช้ด้วยกันได้
ต้อง Tunnelling ที่ router 2 ตัว
ตามทางเรื่องนี้ต้องมีคนใช้ IPv6 ด้วย

Routing Algorithm
- router ทุก router เพื่อนบ้านของ network (complete topology)
- ไม่ได้แปลว่าต้องเก็บ ทั้งหมดแต่ต้องใช้การ
ประมาณค่า จาก Information ของ router ที่ใกล้ๆ
(link state)

static or dynamic

~~static~~
static - router table ถูกเพิ่มเข้าไป
แก้ไขได้ด้วยมือ โดยคน
dynamic - เมื่อทาง router ถูกเปลี่ยนไปเรื่อยๆ

dijkstra's algorithm
- ทุก router เพื่อนบ้านของมัน ว่าตัวเองมี link
กับ cost เท่าไร แล้วส่ง link state
broadcast ไป ทุก node ถึงแม้ว่าจะไม่ได้ forwarding table
ของมัน

418351 Friday, September 5, 2008 ชื่อ อารยา ขุนพลพิทักษ์ รหัสนิสิต 49210925

บันทึกช่วยจำ

IP addressing.

ขนาด 32 bit เช่น 11111111.11111111.11111111.11111111

IP แบ่งออกเป็น 2 ส่วน < ส่วนหน้าเรียก Network part
ส่วนสุดเรียก host part

class A /8 1.0.0.0 → 127.255.255.255.

class B / 16 128.0.0.0 → 191.255.255.255.

class C / 24 192.0.0.0 223.255.255.255

class D / 32 224.0.0.0 239.255.255.255

192.168.100.0 / 27 → อยู่ใน class C /19 แสดงว่ายืมมา 3 bit

network IP = 192.168.100.111 (3) xxxxx

subnet mask = 255-31 = 224 = 255.255.255.224

จำนวน Subnet = $2^{\text{จำนวน bit ที่ยืมมา}} - 2$ $= 2^3 - 2 = 6$ subnet

จำนวน host $= 2^x - 2 = 2^5 - 2 = 30$ host

brord cast IP = 192.168.100.255

subnet zero	192.168.100.0 –	192.168.100.31
1	192. —— .32 – ——	63
2	192 —— .64 – ——	95
3	—— 96 – ——	127
4	—— 128 – ——	159
5	—— 160 – ——	191
6	—— 192 – ——	223
Broad cast	—— 224 – ——	255

subnet mask. = ตัวเลข bit ด้านซ้าย มีค่าเป็น 1 กี่ตัว bit ที่ยืมมาเป็นเลข

CIDR

- เป็นการอ้างอิงเลขหมายเลข IP ตามมาตรฐาน โดยให้เครื่อง ของ / ตามด้วยจำนวนของเลขฐานสอง
- โดยเฉพาะเครือข่าย = Prefix และเลขโฮสต์ = Suffix
เช่น 128.10.0.6 /16

DHCP

คือ โปรโตคอลที่ใช้ในการกำหนด IP Address อัตโนมัติ ให้กับเครื่องลูกข่าย ในระบบที่ใช้ TCP/IP

- DHCP Sever มีหน้าที่แจก IP ในเครือข่าย ไม่ให้ซ้ำ เป็นการลดความซับซ้อน

- ขั้นตอนการทำงานเครื่องลูกกับ DHCP Sever

(1) ลูกข่ายเครื่อง DHCP C_ ในเครือข่าย โดยส่ง DHCP discover เพื่อร้องขอ IP add-

(2) DHCP S_ จะค้นหา IP ที่ว่างอยู่ในฐานข้อมูล แล้วส่ง DHCP offer กลับไปยัง

(3) เมื่อได้รับ IP ก็จะส่ง สัญญาณตอบกลับ DHCP Request ไปยังแม่ข่าย

(4) DHCP S_ ส่งสัญญาณ DHCP Ack ไปยืนยันว่าเครื่องว่างเช่นใช้งานได้

* NAT

- สามารถแปลง IP หลายๆ ตัวนำไปใช้ในเครือข่าย ไม่ซ้ำกับเครือข่ายอื่น โดยใช้ IP เดียวกัน

- ขั้นตอนการทำงาน

เมื่อ NAT เริ่มทำงานมันจะกำหนดช่วงไว้ สำหรับเก็บข้อมูล IP address ของเครื่องในเครือข่าย ตรงนี้เรียก Packet ผ่าน NAT device และจากนั้นมันจะกำหนดไว้เก็บหมายเลข Port ที่ถูกใช้โดย outside IP add- และเมื่อมีการส่ง Packet ออกจากเครือข่ายไปยัง NAT ดว

① - มันจะเก็บข้อมูล source IP add- และ S_ port number ไว้ในตารางที่กำหนดไว้

② แทนที่ IP ของ packet ด้วย IP ของ NAT d-ice

③ assign เลข Port ใหม่ใน Packet และบันทึกค่า Port นี้ไว้ใน ตาราง และกำหนดค่าให้ S_P_N_ ของ packet นั้น

④ ตามนั้นจะคำนวณหา IP, TCP checksum อีกครั้งเพื่อตรวจสอบความถูกต้อง

* NAT → ข้อจำกัดในการใช้งาน

" → ถ้ามีปัญหาการขยายแคลน Add-

ความดี ; มาเรียนตรงเวลา