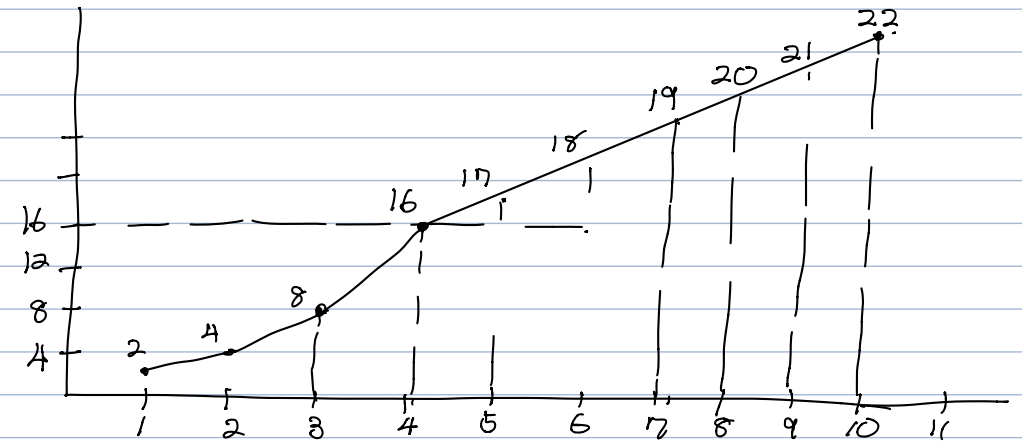
#1 2016112158 김희수

1-(1)

임계값 16 MSS

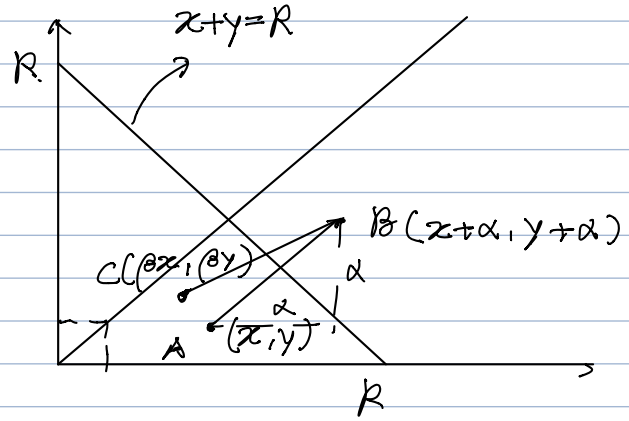
1 ~ 4 round: exponetially increase

5 ~ 10 round: linearly increase



22개

1-(2)



$x+y+2\alpha < R$

$x+$ A-B 기울기 : $\frac{y+\alpha-y}{x+\alpha-x} = 1$

$ex = \frac{x+\alpha-0}{2}$ C는 원점과 B의 중점

$ey = \frac{y+\alpha-0}{2}$

$\therefore$ B-C기울기 $= \frac{y+\alpha-\frac{y+\alpha}{2}}{x+\alpha-\frac{x+\alpha}{2}} = \frac{\frac{y+\alpha}{2}}{\frac{x+\alpha}{2}} = \frac{y+\alpha}{x+\alpha}$

#2

CIDR	32-x 비트들이 기관 내부에 같은 네트워크 프리픽스를 갖는 모든 장비를 구별 ⇒ subnet	서브넷에도 주소를 부여함으로 고갈을 가속시킬 수 있음
DHCP	서버로부터 주소를 동적으로 가져온다. 즉, 주소를 사용할 때만 빌리고 그렇지 않을땐 반환	DHCP 메세지가 차지하는 오버헤드 발생
NAT	local network의 인터페이스는 같은 동일 IP 주소를 사용. 포트넘버로 구별	변환테이블의 오버헤드 포트번호가 프로세스 주소지정에 사용됨
IPv6	IP 주소 크기를 32비트가 아닌 128비트로 확장	기존 IPv4 데이터그램을 처리할 수 없어서 변환해야 함

#3

20161121158 김희수

N'	$D(y), p(y)$	$D(z), p(z)$	$D(w), p(w)$	$D(v), p(v)$	$D(u), p(u)$
x	$1, x$	∞	$3, x$	$2, x$	$1, x$
xy		$3, y$	$2, y$	$2, x$	$1, x$
xyu		$3, y$	$2, y$	$2, x$	
$xyuv$		$3, y$	$2, y$		
$xyuvw$		$3, y$			
$xyuvwz$					

Destination	link
y	(x, y)
z	(x, y)
w	(x, y)
v	(x, v)
u	(x, w)

$x-y$
$x-y-z$
$x-y-w$
$x-v$
$x-u$

#4

- h3에서 h1, h2, h5, h6으로 가는건 반시계방향으로 포워딩
- h4에서 h1, h2, h5, h6 〃 시계 〃 〃

S3 flow table

	Match		Action
Ingress Port = 4	IP Src = 10.2.0.3	IP dst = 10.1.*.*	forward (3)
Ingress Port = 4	IP Src = 10.2.0.3	IP dst = 10.3.0.5	forward (2)
Ingress Port = 4	IP Src = 10.2.0.3	IP dst = 10.3.0.6	forward (1)
Ingress Port = 3	IP Src = 10.2.0.4	IP dst = 10.3.0.5	forward (2)
Ingress Port = 3	IP Src = 10.2.0.4	IP dst = 10.3.0.6	forward (1)

S1 flow table

	Match		Action
Ingress Port = 4	IP Src = 10.2.0.4	IP dst = 10.3.*.*	forward (1)
Ingress Port = 4	IP Src = 10.2.0.4	IP dst = 10.3.0.1	forward (2)
Ingress Port = 4	IP Src = 10.2.0.4	IP dst = 10.3.0.2	forward (3)
Ingress Port = 1	IP Src = 10.2.0.3	IP dst = 10.1.0.1	forward (2)
Ingress Port = 1	IP Src = 10.2.0.3	IP dst = 10.1.0.2	forward (3)

20161121158 김희수

#5	data Integrity	authentication	replay attack
PGP	MD5 해시 함수 digital signature	대칭키 암호화 digital signature 공개키 암호화, 해시함수	nonce 사용
SSL	MS로 생성된 두개의 암호화키 E_A, E_B 사용	MS로 생성된 두개의 MAC키 M_A, M_B 사용, handshaking	two nonce 사용 $MAC=(M_x, \underset{\#}{\text{sequence}} \| \text{data})$
IPSec	ESP 프로토콜 사용	AH 프로토콜 사용	sequence number 사용