

다중링크 가상사설망 부하 균등 기법

김정우* · 손주영**

*한국해양대학교 대학원, **한국해양대학교 컴퓨터공학과 교수

A Load Balancing Scheme for Multi-link VPNs

Jeong Woo Kim* · Jooyoung Son**

*Graduate school of Korea Maritime University, Busan 606-791, Korea

** Dept of Computer Engineering, Korea Maritime University, Busan 606-791, Korea

요 약 : 현재 다중링크 연결을 지원하는 가상사설망(VPN: Virtual Private Network) 장비들은 연결된 다중링크를 회선 장애 발생 시 회선간의 전이 기능을 위한 것으로만 활용한다. 그러나 실제 상황에서 회선 장애가 발생하는 경우는 매우 드물기 때문에 회선 자체의 활용도가 크게 떨어진다. 본 논문에서는 회선 장애가 없는 정상적인 상황에서 다중링크를 모두 이용하는 가상사설망을 형성하고, 회선간의 부하 균등을 기함으로써 회선의 활용도를 크게 높여 결과적으로 가상사설망의 대역폭을 높이는 효과를 얻을 수 있는 기법을 제안한다. 뿐만 아니라 회선 장애가 발생하였을 때는 기존의 가상사설망 장비가 시행하는 회선 전이 기술을 함께 적용하였다. 결론적으로 다중 링크로 연결되어 있는 가상사설망의 가용성을 유지하면서 대역폭을 크게 높이는 효과를 얻을 수 있었다.

핵심용어 : 가상사설망, 부하 균등, 다중링크, 키 인증

ABSTRACT : Nowadays, VPN devices supporting multi-link connections only utilize the second link to backup the fail-off primary link. In practice, however, the occurrence of the link fail-off is so rare that the capacity available on the second link is wasted. In this paper, a scheme of establishing a VPN with multi-links, and load balancing between the links under normal circumstances is proposed in order to take advantage of multi-links, and to eventually increase the effective bandwidth of the VPN. Additionally, the transition functionality is also applied for the link fail-off case like existing VPN devices. Consequently, the proposed scheme enables the VPN with multi-links not only to maintain the higher availability but also to highly increase the effective bandwidth.

KEY WORDS : VPN, Load Balancing, Multi-link, Key-Authentication

1. 서 론

VPN은 공중망을 이용하여 사설망의 효과를 얻기 위한 기술이다. 이는 전용선을 설치하기에는 부족한 재원을 가지고 있거나 전용선을 설치할 만큼 많은 통신 수요가 있지 않은 경우 사용되어 지고 있다. 따라서, VPN의 출현으로 비용을 절감 및 보안 증대의 효과를 얻고 있지만 향후 보다 강화된 보안 데이터와 멀티미디어 데이터 전송의 요구가 증가될 것이므로 VPN 회선 효율성의 최적화가 중요하다. 현재 단일 회선의 데이터 송수신으로 인한 데이터 손실률과 회선의 결합으로 인한 통신불능 가능성이 높아지게 되므로 이를 극복하기 위해서 다중 링크를 채택

2. 관련연구

VPN 서비스를 제공하기 위한 3 가지 기본 기술 요소는 터널링(Tunneling), 인증(Authentication), 암호화(Encryption) 이다[1]. VPN 구성방법에는 Layer2 프로토콜을 사용하는 L2TP(Layer2 Tunneling Protocol)와 PPTP(Point to Point Tunneling Protocol)이 있으며, Layer3 프로토콜을 사용하는 IPSec이 있다. 캡슐화는 Layer2 에서는 IP와 IPX, Layer3 에서는 IP를 사용하며, 패킷인증 및 암호화는 Layer2 에는 없는 반면, Layer3 에서는 AH헤더와 ESP헤더를 사용한다.[2, 3]

VPN 기술별 트래픽 부하 실험결과, PPTP는 Ping과

을 구성하기 때문이다. 따라서, 보안을 중시하는 응용은 패킷의 무결성 보장을 위해 L2TP/IPSec 기술을 채택한 VPN 사용을 권장하며, 시간 제약적인 실시간/멀티미디어를 중시하는 응용은 L2TP에 의한 VPN 사용을 권장한다. 계층 3 기반 라우팅 정보를 이용하는 부하 균등 기법은 크게 2 가지 방식이 있다.[11] 목적지 주소에 의거한 목적지별 부하 균등과 패킷 단위로 이루어지는 패킷별 부하 균등이다. 목적지별 부하 균등은 링크의 사용 빈도가 불균형을 이룰 수 있고, 패킷별 부하 균등에서는 패킷의 도착 순서가 뒤섞이는 현상이 발생할 수 있는 단점을 가진다. 현존하는 부하 균등 기법은 응용과 링크의 특성을 고려하지 않는 문제가 있다. 따라서 응용에 따른 동적인 링크 부하 균등 기법은 전체 링크들간에 부하 균등을 이루면서 응용의 특성을 고려하고, 즉각적인 링크 상황을 반영할 수 있다는 점에서 유리한 기법이다.

3. 다중 링크 VPN 부하균등

3.1 다중 링크 VPN 인증 기법

그림 1과 같이 VPN 클라이언트에 두개의 회선을 설치한 후 다중 링크 VPN 부하균등 수행 시 A:주(Master), B:부(Slave)가 되고 회선 단절(Fail-Off)에 대비한 A와 B간의 상호 이전(transition)이 원활해야 한다.



Fig. 1. Architecture of Multi-link VPN

그러나 현존하는 장비는 VPN 센터와 VPN 클라이언트 간에 서로 1:1이라는 정형화된 구성으로 밖에 인식이 되지 않으므로 다중 링크를 채택한 VPN에서의 부하균등이 이루어지지 않는다.[5] 즉, 하나의 장비에 두개의 키 인증을 할 수 없는 것이 문제인 것이다.

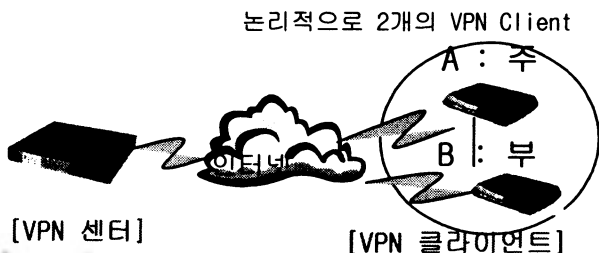


Fig. 2. Load balancing on Multi-link VPN

행한다.

Table 1. Multi-link VPN Key Authentication Algorithm

1. VPN 센터에서 클라이언트 정보 입력
2. 클라이언트에 키 값을 미리 할당
3. 클라이언트는 자신의 정보를 메모리에 할당하여 클라이언트2 개체를 복제
4. 소프트웨어 복제 시 일정 순서에 의한 값을 할당
5. 각 할당된 키 인증 값이 상호 일치할 때 각각의 클라이언트를 분리된 독립 개체로 인식하여, 다중 링크 VPN 통신이 가능

그림 2와 표 1을 바탕으로 그림 3과 같이 부하균등을 위한 인증 과정을 거쳐 VPN이 형성된다.[6,7]

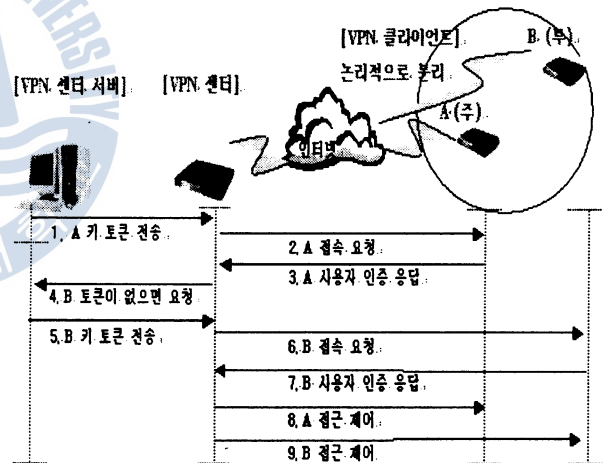


Fig. 3. Authentication Procedure for the Load-balancing

3.2 다중 링크 VPN 부하균등 알고리즘

VPN 클라이언트 사이에 부하균등을 위해 집합 분할(set partition) 알고리즘을 적용하였다. 패킷의 원활한 흐름과 VPN 클라이언트 주/부간의 부하 차이를 최소화할 수 있게 하여 링크 효율성을 증대 시킬 수 있다.

(1) 집합 분할 알고리즘의 개요

집합(Set) $[n] = \{1, 2, \dots, n\}$ 에 대해 $[n]$ 의 부분집합(Subset)은 B_0, B_1, \dots, B_j 들로 나타낼 수 있으며, B_0, B_1, \dots, B_j 는 블록(Block)이라고 한다. 각각의 파티션 집합은 순차적으로 블록이 증가를 할 때, 하위의 블록에 포함된 원소(Element)는 포함이 되지 않는다. 이것을 Partitioning Set이라고 한다. 각각의 파티션 집합은 순차적으로 블록이 증가를 할 때, 하위의 블록에 포함된 원소(Element)는 포함이 되지 않는다. 이것을 Partitioning Set이라고 한다.

에 패킷을 할당하는 기준이다. 기본적인 기준은 패킷을 발생시키는 응용에 기반한다. 이러한 부하균등 알고리즘을 주기적으로 적용하는 것을 원칙으로 한다. 이때 얼마나 자주 알고리즘을 적용해서 링크에 할당되는 패킷을 결정해야 VPN 라우터에서의 부하와 부하균등 정도 면에서 가장 최적인 것인지를 실험과 분석 과정을 거쳐 파악한다. 나아가 포트 또는 패킷별 부하균등과 같은 강제적 부하균등이 아니라 패킷의 시간대별 흐름을 분석한 후 패킷 및 포트와는 상관없이 회선에 가장 적합한 부하균등을 제공함으로써 부하균등 정책을 실시간적이며 유연성 있게 적용할 수 있게 한다.

실험에서 사용되는 기준값(port)은 다음과 같다.

$$[n] = \{pop3, Domain, Http, SMTP, Ms-sql\}$$

여기서 [n]에 포함된 각각의 값들은 시간대별 패킷 분석 결과 가장 많이 사용되어지는 값들로서 회선의 대부분을 차지하는 값들이다. 블록은 실험에서 부하균등을 위해 고려 중인 회선이 2 개이므로 2 블록을 사용하게 된다. 실험 결과의 성능은 각 시간별 집합 분할에 의해 얻은 파티션 값(원소로 지정된 포트에 전송되는 패킷의 양)간의 차이로써 구해지며, 각 결과 값의 분포도상 전체 표면량이 가장 적은 표면 분포값을 나타내는 것이 가장 성능이 가장 우수한 것이 된다.

이를 실험적으로 구현한 부하균등 VPN 라우터 시뮬레이터를 제작하였다.

(3) 부하균등 VPN 라우터 시뮬레이터

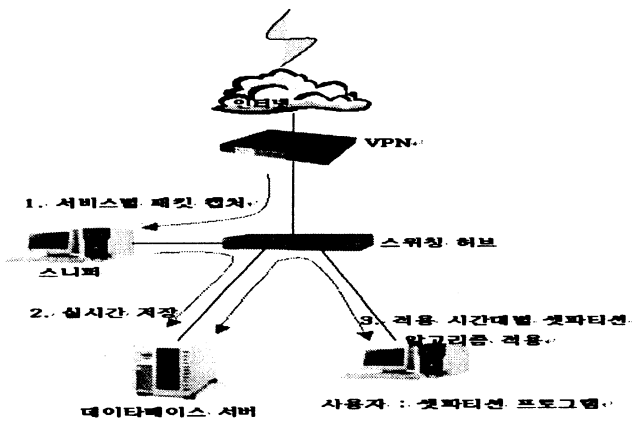


Fig. 4. Simulation of the Load-balancing VPN

7월 4와 같이 시뮬레이션 운영 환경은 윈도우 95 이

스 종류와 크기를 파악한다.

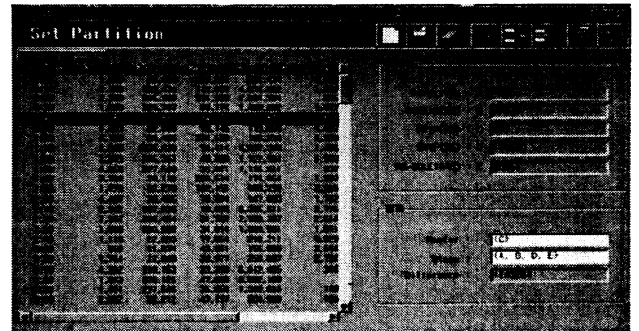


Fig. 5. Snapshot of the Simulator working

둘째, 분석이 완료된 서비스는 실시간으로 데이터베이스 서버에 저장하며 마지막으로 집합 분할 VPN 시뮬레이터는 미리 설정된 시간 간격에 맞춰 주기적으로 데이터베이스 서버로부터 해당 로그 데이터를 가져온 후 각 링크에 포트를 할당하고, 링크에 할당된 패킷 양간의 차이값을 산출한다. 이때 얻은 차이값은 다시 해당 데이터베이스 결과 및 결과 이력 테이블에 저장된다

이러한 일련의 과정을 거쳐 생성된 데이터는 다음의 분석 과정을 거쳐 부하균등 알고리즘을 적용하기 위한 가장 최적의 주기시간을 얻었다.

3.3 시간대별 부하균등 시뮬레이션 결과

부하균등 VPN 시뮬레이션은 모두 15일 동안 실행되었다. 각 하루 24시간동안 1분에서 60분까지 부하균등 적용 간격(주기)을 달리하여 실행하였다. 각각의 적용 간격(주기) 시간별로 계산된 결과의 차이값(Difference)들을 평균한 후 간격별로 표시하면 그림 6과 같다.

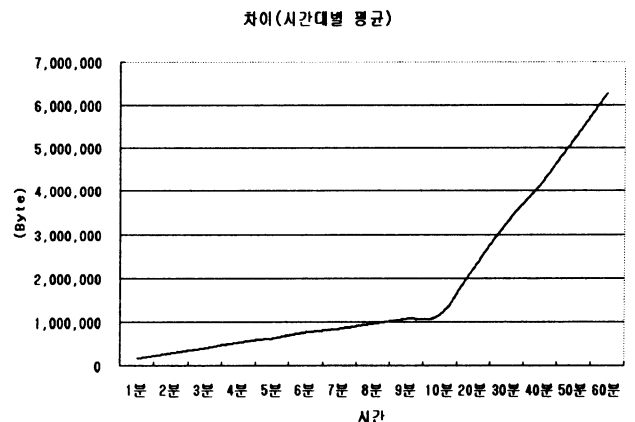


Fig. 6. Difference Averages

되고, 소비 시간이 발생하게 된다. 따라서 부하균등 적용의 가장 적합한 시간을 찾아내기 위해서는 처리지연시간(Processing Delay)을 함께 고려하여야 한다. 이것은 다음과 같이 구할 수 있다.

명령문 수[Instructions]/컴퓨터처리능력[mips]

[명령문의 수]를 계산할 때 프로그램의 흐름에서 가능한 경우의 수를 모두 고려하여야 한다. 전체 프로그램의 흐름은 입력값 5가지를 받게 되면, 다음으로 집합이 부분 집합으로 분할될 수 있는 각각의 경우에 대한 링크 부하값을 계산한 후, 각 경우에 대해 비교 작업을 한다. 그런 후 가장 작은 차이값을 가지는 분할 결과에 따라 각각의 링크로 구분하여 할당된 패킷들을 전송하는 것이다. 본 실험에서 발생할 수 있는 부하균등 시 결과는 입력값이 5가지이고 분할되는 부분집합의 개수가 2이므로 총 15가지의 경우의 수를 가진다. 정리하면 가능한 분할 경우의 수가 15가지, 각각의 차이값에 대해 비교하는 경우의 수가 14가지, 끝으로 회선을 분리하기 위한 과정이 2가지이므로 총 31번의 비교 작업이 수행되어야 한다.[10]

따라서, 비교 동작을 하나의 명령어로 처리할 수 있다고 가정하고, VPN 라우터의 CPU 처리능력이 1 mips라고 할 때, 전체 1회 부하균등 알고리즘 실행 시간은 약 $31/10^6$ 초이며, 이것은 약 0.000031 초의 처리지연시간이 필요함을 나타낸다. 이것을 1분에서 60분 단위로 전체 24 시간동안 적용하였을 때, 누적되는 처리지연시간을 그림 3.7에 나타내었다. 이 그림에서는 앞서 3.6에서 구한 각 간격별로 구한 평균 차이값과 함께 표현하여 처리지연시간과의 상호 비교를 하였다.

적용시간대별 부하량을 구하기 위해서 다음과 같은 수식이 적용된다.

$$[\text{처리부하(Byte)}] = (\text{전체 Byte량} \times (\text{처리지연시간} \times \text{시간대별적용횟수}))$$

전체 바이트량을 적용함으로써 적용시간대별 평균차이값을 구하기 위해 사용된 데이터를 처리함에 있어 동일한 조건을 적용하여 적용시간대별 부하량을 얻기 위함이다. 이는 하루 24시간동안 적용시간대별 부하균등이 실행될 경우를 고려한 것이다. 따라서, 시간대별적용을 할 경우 실행 되어져야 하는 횟수를 적용하면 그림 7과 같이 나타내어 진다.

이 다양하지 못함으로 인해 발생할 수 있는 부하균등에 따른 링크간의 부하 차이값이 클 경우가 될 것이고, 반대로 다양한 응용들을 골고루 사용하는 경우는 10분 전후가 가장 적정할 것으로 예상된다.

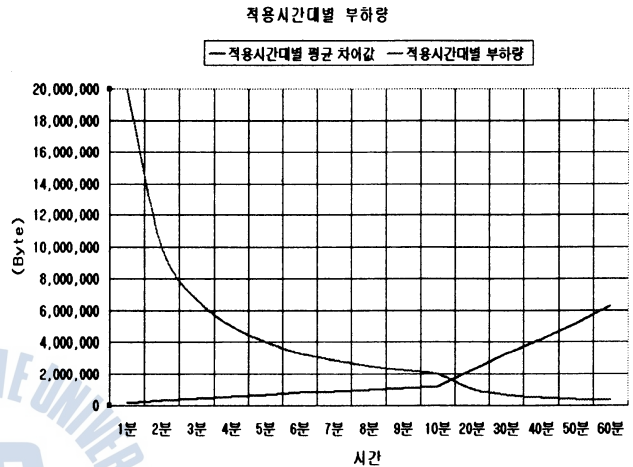


Fig. 7. Difference Averages vs. Processing Time

따라서, 이런 시간대가 부하균등 시 VPN 장비의 부하를 최소화 하면서, 원활한 부하균등을 수행할 수 있는 시간이 될 것이므로 부하균등 적용 시 사용그룹의 성향이 먼저 파악되어져야 할 것이다. 그리고, 여기서 고려되어야 하는 사항은 서비스의 포트별 경우의 수가 일정하지 않을 경우인데 이 경우 적용시간대별 처리 지연시간의 등락 폭이 일정하지 않게 될 것이고 이는 부하균등 정책을 수행함에 있어 적용시간 역시 달라질 수 있는 것을 의미한다.

3.4 부하균등 적용 시 세션 처리

응용별로 부하균등정책을 적용할 때 하나의 세션을 이루는 패킷들을 다른 링크로 할당할 경우 세션의 연속성을 확보하여야만 한다. 다시 말해 응용별 VPN의 부하균등을 하기위해선 세션별 부하균등 정책 역시 중요하다. 세션별 부하균등을 처리함에 있어 보다 구체적인 방법은 송·수신측 IP 주소를 세션과 동시에 판별하여 적용하는 방법이 있지만 본 논문에서는 현재 시간별 응용별 현황을 적용한다. 따라서, VPN은 집합분할(Set Partition)을 응용별로 적용한 결과와 앞으로 적용할 결과를 동시에 처리하게 된다. 아래 표 2는 응용별 세션 부하균등 적용 시 처리방법을 설명하기 위한 값으로써 이는 실험을 위해 실제 사용된 값을 기초로써 표본을 추출하였다. 표본을 추출함에 있어 모든 세션별 부하균등에 있어서 적용되는 방법은

종료됨을 의미한다.

순번 1이 집합분할되어 부하균등이 적용이 되었을 경우 다음으로 순번 2의 경우를 VPN은 부하균등을 적용하려 할 것이다. 이때 순번 2에 대한 집합분할이 적용될 때 {53}과 {1175}가 세션이 계속 유지되고 있고 또 같은 회선으로의 부하균등을 지속적으로 할 수 있다. 하지만 순번 2와 순번 3의 경우를 보면, 순번 2의 {53}은 B 회선으로의 집합분할 결과가 주어지게 됨을 알 수 있다. 이런 경우 집합분할 부하균등을 적용하게 되면 세션이 종료되어 응용 프로그램이 종료가 되는 것이다.

Table 2. Sessions of the Different Applications

시간	응용	크기(Byte)
14:28:04	53(DNS)	1320
14:28:04	135(epmap)	84
14:28:04	1175(Unassigned)	200
14:28:05	80(HTTP)	142
14:28:05	135(epmap)	195
14:28:05	53(DNS)	884
14:28:05	1175(Unassigned)	65
14:28:06	25(SMTP)	504
14:28:06	1175(Unassigned)	505
14:28:06	135(epmap)	99
14:28:06	1437(Tabula)	116
14:28:06	137(NetBios)	1332
14:28:06	80(HTTP)	44
14:28:06	53(DNS)	634
14:28:06	1026(Unassigned)	78
14:28:06	1026(Unassigned)	72

Table 3. Results of Set Partition on data in Table 2

순번	시간	셋 파티션 결과(응용별)	
		A 회선	B 회선
1	14:28:04	{53}	{137, 1175}
2	14:28:05	{53}	{80, 135, 1175}
3	14:28:06	{25, 137}	{1175, 135, 1437, 80 ...}

따라서 부하균등은 적용하기에 앞서 부하균등 적용 중

순번 3을 다시 집합분할한 결과는 표 4와 같다. 위와 같이 다시 집합분할을 적용하여 가장 좋은 방법을 다음 단계에서 찾는다. 즉, 최상의 조건을 찾아 부하균등을 하는 것이다. 이로 인해 세션 단절 없이 지속적이면서 안정성 있는 부하균등이 가능하다.

Table 4. Result of the reapplication of Set Partition on #3 in Table 3

순번	시간	셋 파티션 결과(응용별)	
		A 회선	B 회선
3	14:28:06	{53, 137}	{25, 1175, 135, 1437, ...}

4. 결론 및 향후 연구과제

하나의 VPN 장비에 2개 회선 이상이 연결되게 되면 이중 투자 비용의 감소 및 안정성 있는 서비스가 가능할 것이다. 이는 현재 VPN을 사용하고 있고, 앞으로 사용할 기업 및 인터넷 회선을 사용하는 대부분의 장소에 위와 같은 부하 균등 기능이 포함된 다중 링크 VPN이 적용될 것으로 예상된다.

향후 완벽한 QoS를 보장하기 위해서는 VPN은 부하균등이라는 과정을 거쳐야 할 것이며, 나아가 송/수신 시 패킷의 안정성도 높아져야 할 것이다. 본 연구 결과로써 VPN 한 장비에 멀티포인트 회선의 사용 시 부하균등 정책을 적용하여 시스템자원의 이중 낭비를 막고, 제안된 실시간적인 부하균등 알고리즘을 통하여 가장 효율적이며, 적응력을 높일 수 있는 방법을 제안하였다.

향후 연구 과제로는 부하균등 적용 시 패킷 손실을 최소화하는 방법에 대하여 연구할 계획이다.

본 논문은 해양대 산학연컨소시엄사업단이 지원하였음

참 고 문 헌

- [1]"Understanding Virtual Private Network", pp.10~11, ADTRAN Inc, 2001
- [2]김광호, 임채훈 "PPTP 와 L2TP 의 비교 분석", Cryptography & Network Security Center, Future Systems, Inc, Technical Report, p.3, pp.15-17, Sep. 25, 2000

- [5] "Network Load Balancing Technical Overview", pp.3-4, pp.12-13, Microsoft Windows2000 Server, White Paper, 2000
- [6] Stamatis Karnouskos, Ingo Busse, Stefan Covaci, "Place Oriented Virtual Private Networks", pp.3-4, 33rd Hawaii International Conference on System Sciences, 2000
- [7] Eli Herscovitz, "Secure Virtual Private Networks: The Future of Data Communications", pp.2-3, p.5, International Journal of network management, 1999
- [8] P.C Chu and J.E.Beasley, "A genetic Algorithm for the set partitioning Problem", pp.1-2, The Management School Imperial College, April. 1995
- [9] Zbigniew J.Czech, "Heuristic algorithms for solving the set-partitioning problem" p.1, Silesia Univ. of Technology, June. 1997
- [10] Huican Ahu, Oscar H.Ibarra, "On Some Approximation Algorithms for the Set Partition Problem", p.2, pp.6-7, California Univ. USA
- [11] Jeff Doyle, "Routing TCP/IP Vol.1, pp.109~112, Cisco Press, 1998.

