네트워크 서비스 기반의 단일 웹 인증 설계

반경식* · 이재완** · 김형진***

A Design for Unified Web Authentication at Network Service Foundation

Kyung-sig Ban* · Jae-wan Lee** · Hyoung-Jin Kim***

요 약

최근 초고속통신망의 발달로 네트워크 보안 및 시스템 침해 사고에 대응하기 위한 다양한 인증 및 접근 제어 시스템이 도입되고 있다. 하지만 초고속인터넷 환경에서 보안 자체가 취약성을 보이고 있다. 따라서 인터넷 이용자의 다양한 욕구를 충족하고, 보다 안전하고 신뢰성있는 새로운 인증 시스템 도입이 필요한 시점이다.

본 논문에서는 다원화된 네트워크 환경에서 기술방식에 따라 차별적으로 적용하는 기존의 다양한 인증 체계를 하나로 통합하여 네트워크 보안을 강화하고, 보다 안정적인 서비스 제공 기반을 마련하기 위하여 단일 웹 인증 설계를 통한 새로운 인증 체계 방안을 제시하고자 한다.

ABSTRACT

Recently, Network companies have introduced security solutions to protect the network from intrusions, attacks and viruses but the network has still weakness and vulnerability. It is time to bring more stable and reliable authentication system that would meet the Internet user's need.

In this study, Current broadband networks don't have hierarchic and stable authentication solutions. And so, an integrated and hierarchic system is needed to provide a various kinds of application services. I'd like to present a new authentication system which is based on unified web authentication design. It will unify various authentication systems that have been deployed in various network environment and reinforce network security to provice a various kinds of application services in a stable and safe environment. that is a simple and more secure method for fighting a rise in card-not-present fraud

키워드

인증, 라우팅, VRRP

I. 서 론

최근 통신 인프라는 여러 가지 방법으로 사용자 데이터베이스를 관리하고, 보안 강화를 시도하고 있지만 자원관리, 접근 권한 등의 관리가 서로 다원화되어 있는 환경에서 다양한 사용자 관리의 어려움으로 인해 접근 인증과 같은 네트워크 보안에 취약점이 발생되고 있다.

기존의 접근방법은 네트워크 접근 허용 여부를 판단하는 단순 접근 인증만을 기반으로 네트워크 시스템에 일관된 자원 및 네트워크의 보안 체계 구축하여 서비스

* 군산대학교 전자정보공학부

** KT

*** 전북대학교 응용시스템 공학부 : 교신저자

접수일자 2008. 05. 27

를 제공하였다. 따라서 이러한 네트워크 환경의 신뢰성을 높여 중요한 자원들의 안전성 보장 및 관리가 필요하다는 인식을 통해 보안성 높은 접근 권한을 가진 사용자에 의해서만 접근이 가능토록 해야 한다. 즉 다양한 환경에서 네트워크 관리를 위해 사용자 인증 기반의 세분화된 접근 관리의 필요성이 부각되고 있다. 이에 안정성과 신뢰성을 확보할 수 있는 새로운 접근 제어가 필요 하다.

기존의 인증 시스템은 크게 인증 방식과 무인증 방식으로 구분할 수 있다.

인증 접근은 네트워크 기반의 인증 서비스를 제공하므로 기존 서비스들과 차별화가 가능하며, 서비스 인증과 통합하여 차별화된 서비스 제공이 가능하다. 그러나 사용자가 인증을 받기 위해 네트워크 인증 응용 프로그램이 요구되고, 네트워크 인증 응용 프로그램으로 인한 비용 및 유지 보수가 필요한 단점이 있다.

무인증 접근은 네트워크 접근 권한이 필요하지 않아 사용자가 네트워크를 통해 언제든지 웹 서비스 이용이 가능하다. 그러나 사용자를 위한 서비스의 차별화가 어려운 단점을 가지고 있다.

본 논문에서는 기존의 인증 시스템에서 나타난 문제점을 해결하기 위해 네트워크 접근 제어를 기반으로 웹 기반의 인증 서버를 구현하여 사용자 요구사항을 능동적으로 수용할 수 있도록 하고자 한다. 또한 기존의 인증 시스템을 하나로 통합하여 접근 보안을 강화하고 보다 안정성이 고려된 새로운 인증 체계 개선 방안을 제시하고자 한다. 이에 기존의 인증 시스템을 단일 웹 인증 기반이라 정의한다. 이에

따라서 이를 위해 라우터 간 이원화된 운용 체계를 VRRP(Virtual Router Redundancy Protocol) 프로토콜을 이용하여 단일 웹 인증 체계를 설계하고자 한다.

이를 위해 본 논문에서는 2장에서는 인증 절차를 보이고 3장에서는 제안 기법에 대해 설계한다. 그리고 4장에서는 시뮬레이션을 통해 본 논문의 우수함을 보이고 마지막 5장에서 결론을 맺는다.

Ⅱ. 네트워크 망에서의 인증 절차

네트워크 망에서의 인증 절차는 접근 방식에 따라 인증 알고리즘을 Explicit, Implicit 인증 및 무선인증으로 구분한다.

Explicit 인증은 일반적 의미의 인증으로 웹 서버를 이용하여 이용자의 ID · Password를 확인하여 접속권한을 부여하고, 이용자의 요구에 따라 매 login시 접속권한을 부여하는 수동 인증 방법이다.

Implicit 인증은 무인증으로서 인식되고 있는 자동인증 방법으로 시설과 단말기를 확인함으로써 시스템이 내부적으로 인증하는 방법이다. 그리고 접속 시 이용자의 MAC 주소를 통해 인증함으로써 MAC 스프핑시 시스템의 부하를 가중시킬 수 있고, 부가서비스 자원의 사용을 허용할 수 있다.

무선인증은 웹 서버를 사용하지 않고 MAC 주소와 EAP-MD5 인증 방식을 적용한다.

따라서 단일 웹 인증 방식은 사용자의 단말기의 MAC 주소를 등록 후 IP 할당 시 인지된 정보를 기반으로 Implicit 인증 방법과 웹을 통하여 ID · PWD로 접속하는 Explicit 인증 방법을 통합 적용하고자 한다. 이에 그림 1은 단일 웹 인증 절차를 보여주고 있다.

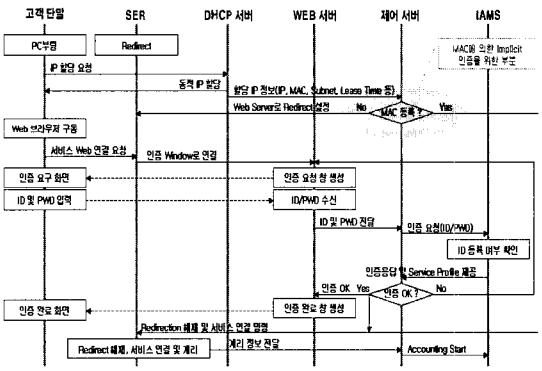

그림 1. 단일 웹 인증 절차
Fig. 1 Unified Web Authentication Process

Ⅲ. 단일 웹 인증 설계

3.1 VRRP 프로토콜

동적 라우팅은 라우팅 프로토콜을 사용해 최단의 거리를 자동으로 설정해 주므로 네트워크가 커진 경우에 상당히 편리한 작용을 하지만 계속적인 라우팅 정보를 갱신하기 때문에 부하가 커지기도 한다. 정적 라우팅은 프로토콜을 설정해주는 것이 아니라 어떤 패킷이 들어올 경우에 패킷을 지정된 장소로 보내는 것으로, 정적 라

우팅 환경에서는 한 개의 라우터가 잘못되었을 경우에 그것을 통해 나가는 모든 호스트들은 통신장애가 발생한다. 이러한 통신장애가 발생했을 경우에 백업기능으로 구현된 것이 VRRP 프로토콜이다.

VRRP는 LAN상에서 정적으로 설정된 기본적으로 하나의 라우터를 사용하고 있을 때, 하나 이상의 또 다른 백업 라우터를 가질 수 있는 방법을 제공하는 인터넷 프로토콜의 하나이다.

네트워크 구성에서 가장 일반적인 배치는 근거리통신망 상의 호스트 그룹으로부터 전달되는 패킷들을 하나의 라우터가 관리하고 서비스하도록 설정하는 것이다. 그러나 만약 이 라우터가 고장이 나면, 다른 라우터를 백업으로 사용할 수 있는 방법이 없다. VRRP를 사용하면 하나의 가상 IP 주소가 기본으로 설정된다. 가상의 IP 주소는 하나는 마스터 라우터로, 다른 것은 백업들로 지정되는 라우터들 간에 공유된다. 마스터 모드에 문제가 발생하는 경우에 가상 IP 주소는 백업 라우터의 IP 주소로 바로 천이된다. 또한 VRRP는 네트워크 부하조절에도 사용될 수 있으며, 대상 프로토콜은 IPv4와 IPv6 모두에 적용된다.

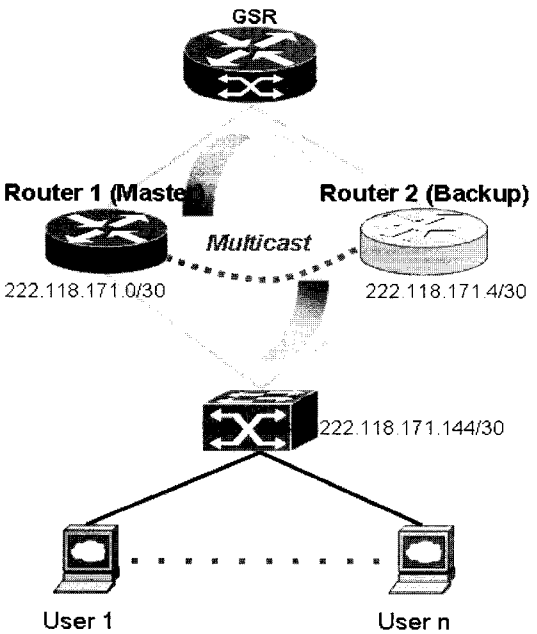

그림 2. VRRP 기본 구성도
Fig. 2 Basic Format of VRRP

VRRP 기본 구성도는 그림 3과 같다.

그림 3에서 보면 router1 과 router2는 VRRP 그룹으로 구성돼 클라이언트들에게 라우팅 서비스를 제공한다. VRRP 에서는 마스터・백업 개념이 사용되며 동일한 VRRP 그룹에 속하는 라우터 그룹은 priority 등의 우선권으로 각각 마스터 또는 백업 동작을 결정하게 된다. 또한 VRRP는 이더넷 인터페이스에서 사용할 수 있는 기능이며, 멀티캐스트 기반의 프로토콜이다.

따라서 본 논문에서 VRRP 구현을 위한 단일 웹 인증 기반의 인증 시스템 설계는 그림 3과 같다. 또한 이 테스트 베드 스몰 망의 SER - RS38K 라우터간 라우팅 프로토콜은 BGP/IS-IS를 적용하였다

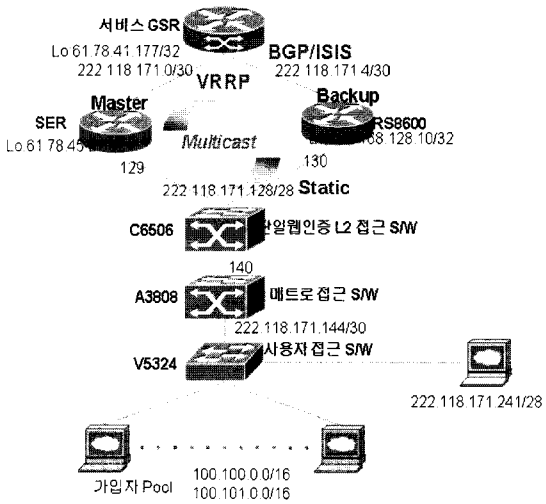

그림 3. VRRP 스몰 망 설계
Fig. 3 A Small Network Design of VRRP

본 논문에서 제안한 절차는 다음과 같다.

① 망 모형에서 SER - RS38K 라우터간 VRRP 그룹을 구성한다.

② 라우팅 프로터콜(BGP,IS-IS)을 적용하고, SER - RS38K 라우터간 인터페이스 config 작업을 수행한다.

③ VRRP 그룹 구성 후 트래픽 라우팅 흐름을 측정・비교한다.

④ 웹 stress를 이용한 트래픽 발생, 점유 및 흐름을 비교・분석한다.

⑤ 시뮬레이션 수행 후 결과를 확인・분석한다.

Ⅳ. 성능평가

4.1 시뮬레이션 환경

VRRP 스몰 망에 라우팅 프로토콜(ISIS, BGP, Static)을 적용・구현된 모형 망에서 라우팅 흐름을 측정・비교・분석한다. 시뮬레이션에서 사용된 장비는 Cisco 서비스 GSR(12416) 1대, SER(Catalyst6509) 1대, RS38K (RS8600) 1대, Alphine3808, Catalyst6506, Dasan V5324, 광케이블 등이다.

그림 3은 Master-backup 환경에서 SER은 primary(주), RS8600은 secondary(예비)로 설정하고, primary 장애시 secondary로 자동 절체되도록 구성하였다. 또 A3808은 VRRP의 VIP로 static 라우팅을 하도록 구성한다.

master-backup 라우터간에 시뮬레이션 환경은 다음과 같이 정의한다.

① 동일한 VRRP 그룹에서 ID와 IP 주소를 설정한다.
② 그룹 내 높은 priority 값으로 마스터를 결정한다.
③ 이더넷 기반에서 사용하며, 멀티케스트를 통한 VRRP 정보를 전달한다.

4.2 VRRP 실험 및 결과

VRRP 시험을 위한 트래픽 측정 툴은 다음 그림 4에서 보여주는 바와 같이 웹 application stress를 사용하였으며 트래픽 발생 유형은 패킷 제너레이터 형태로 발생한다.

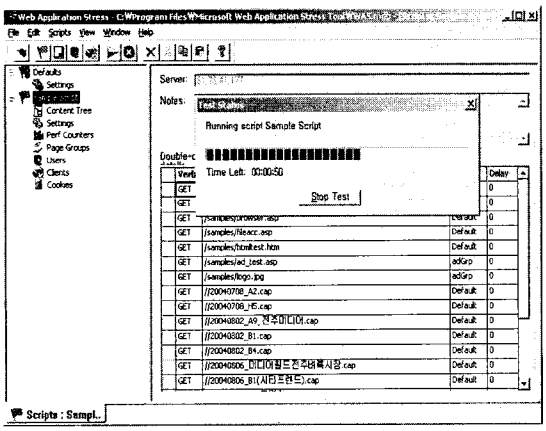

그림 4. VRRP 트래픽 발생 툴
Fig. 4 VRRP traffic generated Tool

다음은 VRRP 트래픽 발생 툴에 실제 트래픽을 유발시켜 SER-RS38K간 동작 모드의 천이 과정과 모드 변경 전, 후에 대한 트래픽 흐름을 측정하고 분석하였다.

1) 동작 모드 변경전, C6509 및 RS8600의 트래픽 흐름 비교는 다음과 같다.

첫째, priority 값(120)에 따라 C6509를 마스터 모드로 설정(①)하고 마스터 모드에서 트래픽 흐름을 측정하였다. 따라서 마스터 모드인 C6509(primary)에는 트래픽이 점유(②)되었고, 백업 모드인 RS8600(secondary)에서는 입・출력 모두 트래픽 점유가 없었음(③)을 알 수 있다.

C6509#sh vrrp detail
GigabitEthernet4/2 - Group 1

① State is Master
Virtual IP address is 222.118.171.131
Priority 120

gsr01#sh int g2/2(C6509로 가는 Interface)
GigabitEthernet2/2 is up, line protocol is up
Hardware is GigMac 3 Port GigabitEthernet, address is 000c.3129.ae02 (bia 000c.3129.ae02)
Internet address is 222.118.171.1/30
・・・ 중 략 ・・・

② 5 minute input rate 67000 bits/sec, 67 packets/sec
5 minute output rate 41000 bits/sec, 46 packets/sec

・・・ 생 략 ・・・
gsr01#sh int g2/0(RS8600으로 가는 Interface)
GigabitEthernet2/0 is up, line protocol is up
Hardware is GigMac 3 Port GigabitEthernet, address is 000c.3129.ae00 (bia 000c.3129.ae00)
Internet address is 222.118.171.5/30
・・・ 중 략 ・・・

③ 5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec

・・・・ 생 략 ・・・

둘째, RS8600을 VRRP 백업 모드로 설정(④)하고 VRRP 트래픽 흐름을 측정하였다. 측정 결과 마스터 모드인 C6509(primary)에서만 트래픽이 점유(⑤)되었고, 백업 모드인 RS8600(secondary)에는 트래픽 점유가 없음(⑥)을 알 수 있다.

따라서 VRRP 그룹에서 master-backup 라우터가 정

상 모드로 동작할 경우 마스터인 primary 라우터에만 트래픽 점유가 발생하고, 백업 모드인 secondary 에서는 입·출력 모두 트래픽이 발생되지 않는 것으로 측정되었다.

RS8600# ip-redundancy show vrrp sum

④ Virtual Router Interface Primary Address Associated Address **State**

---
1 to_alpine 222.118.171.130 222.118.171.131 **Backup**

gsr01#sh int g2/2(C6509로 가는 Interface)
GigabitEthernet2/2 is up, line protocol is up
Hardware is GigMac 3 Port GigabitEthernet, address is
000c.3129.ae02 (bia 000c.3129.ae02)
Internet address is 222.118.171.1/30
··· 중 략 ···

⑤ 5 minute input rate 67000 bits/sec, 67 packets/sec
5 minute output rate 41000 bits/sec, 46 packets/sec

···· 생 략 ····
gsr01#sh int g2/0(RS8600으로 가는 Interface)
GigabitEthernet2/0 is up, line protocol is up
Hardware is GigMac 3 Port GigabitEthernet, address is
000c.3129.ae00 (bia 000c.3129.ae00)
Internet address is 222.118.171.5/30
····· 중 략 ···

⑥ 5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec

···· 생 략 ···

2) 동작 모드 변경후, C6509 및 RS8600의 트래픽 흐름 비교는 다음과 같다.

첫째, 우선순위 priority 값(90)에 따라 C6509를 VRRP 백업 모드로 설정(ⓐ)하고, RS8600이 VRRP의 마스터 모드로 천이후 트래픽 흐름을 측정하였다. 그 결과 백업 모드로 변경된 C6509는 트래픽 점유가 없었고(ⓑ), 마스터 모드로 천이된RS8600에는 입·출력 모두 트래픽 점유가 발생되었음을 알 수 있다(ⓒ).

둘째, RS8600이 VRRP의 마스터 모드로 천이(ⓓ)된 후 VRRP 트래픽 흐름을 측정하였다. 그 결과 백업 모드로 천이된 C6509에서는 트래픽 점유(ⓔ)가 없었으며, 마스터 모드인 RS8600에서는 입·출력 모두 트래픽 점유가 발생하였음(ⓕ)을 알 수 있다.

C6509#sh vrrp detail
GigabitEthernet4/2 - Group 1

ⓐ State is Backup
Virtual IP address is 222.118.171.131
Priority 90

gsr01#sh int g2/2(C6509로 가는 Interface)
GigabitEthernet2/2 is up, line protocol is up
Hardware is GigMac 3 Port GigabitEthernet, address is
000c.3129.ae02 (bia 000c.3129.ae02)
Internet address is 222.118.171.1/30
··· 중 략 ···

ⓑ 5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec

··· 생 략 ···
gsr01#sh int g2/0(RS8600으로 가는 Interface)
GigabitEthernet2/0 is up, line protocol is up
Hardware is GigMac 3 Port GigabitEthernet, address is
000c.3129.ae00 (bia 000c.3129.ae00)
Internet address is 222.118.171.5/30
··· 중 략 ···

ⓒ 5 minute input rate 40000 bits/sec, 38 packets/sec
5 minute output rate 22000 bits/sec, 22 packets/sec

··· 생 략 ···

RS8600# ip-redundancy show vrrp sum

ⓓ Virtual Router Interface Primary Address Associated Address **State**

---
1 to_alpine 222.118.171.130 222.118.171.131 **Master**

gsr01#sh int g2/2(C6509로 가는 Interface)
GigabitEthernet2/2 is up, line protocol is up
Hardware is GigMac 3 Port GigabitEthernet, address is
000c.3129.ae02 (bia 000c.3129.ae02)
Internet address is 222.118.171.1/30
··· 중 략 ···

ⓔ 5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec

··· 생 략 ···
gsr01#sh int g2/0(RS8600으로 가는 Interface)
GigabitEthernet2/0 is up, line protocol is up
Hardware is GigMac 3 Port GigabitEthernet, address is
000c.3129.ae00 (bia 000c.3129.ae00)
Internet address is 222.118.171.5/30
··· 중 략 ···

ⓕ 5 minute input rate 40000 bits/sec, 38 packets/sec
5 minute output rate 22000 bits/sec, 22 packets/sec

··· 생 략 ···

지금까지 VRRP그룹의 master-backup 라우터간에 마스터 모드(primary)와 백업 모드(secondary) 환경에서 트래픽 흐름을 측정하고 비교하였다. 그 측정 결과는 다음과 같다.

첫째, 마스터 모드로 동작중인 라우터에서만 트래픽 점유가 발생한다.

둘째, 백업 모드에서는 입·출력 모두에 트래픽 점유가 없음을 알 수 있다.

다음은 VRRP그룹의 천이 과정 중에 서비스 GSR은 어떻게 동작하는가를 GSR 라우팅 표를 이용하여 트래픽 흐름을 비교·분석하였다. 측정 결과는 다음 2가지로 분석할 수 있다.

첫째, 동작 모드 변경전(①) 가입자 pool에 대한 Next-hop(100.100/101.0.0)이 SER의 loopback IP(61.78.45.21) 주소로 지정되어 있음을 알 수 있다.

둘째, 동작 모드 변경후(②) 가입자 pool에 대한 Next-hop(100.100/101.0.0)이 RS8600의 loopback IP(192.168.128.10) 주소로 변경 되는 것으로 나타났다.

```
gsr01#sh ip ro
Codes: C - connected,S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR

Gateway of last resort is not set
  222.118.171.0/24 is variably subnetted, 5 subnets, 3 masks
C  222.118.171.0/30 is directly connected, GigabitEthernet2/2
C  222.118.171.4/30 is directly connected, GigabitEthernet2/0
B  222.118.171.128/28 [200/0] via 61.78.45.21, 00:00:48
S  222.118.171.135/32 [1/0] via 222.118.171.6

① B  222.118.171.240/28 [200/0] via 61.78.45.21, 00:00:48
     100.0.0.0/16 is subnetted, 2 subnets
  B  100.100.0.0 [200/0] via 61.78.45.21, 00:00:48
  B  100.101.0.0 [200/0] via 61.78.45.21, 00:00:48

  192.168.128.0/32 is subnetted, 1 subnets
i L1192.168.128.10 [70/10] via 222.118.171.6, GigabitEthernet2/0
  172.25.0.0/24 is subnetted, 1 subnets
C  172.25.234.0 is directly connected, Ethernet0
  61.0.0.0/32 is subnetted, 2 subnets
i L1 61.78.45.21 [70/100] via 222.118.171.2, GigabitEthernet2/2
C  61.78.41.177 is directly connected, Loopback0

gsr01#sh ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia-IS-IS inter area
* - candidate default, U - per-user static route, o - ODR

Gateway of last resort is not set
  222.118.171.0/24 is variably subnetted, 5 subnets, 3 masks
C  222.118.171.0/30 is directly connected, GigabitEthernet2/2
C  222.118.171.4/30 is directly connected, GigabitEthernet2/0
B  222.118.171.128/28 [200/0] via 61.78.45.21, 00:05:56
S  222.118.171.135/32 [1/0] via 222.118.171.6

② B  222.118.171.240/28 [200/0] via 192.168.128.10, 00:05:56
     100.0.0.0/16 is subnetted, 2 subnets
  B  100.100.0.0 [200/0] via 192.168.128.10, 00:05:56
  B  100.101.0.0 [200/0] via 192.168.128.10, 00:05:56

  192.168.128.0/32 is subnetted, 1 subnets
i L1192.168.128.10 [70/10] via 222.118.171.6, GigabitEthernet2/0
  172.25.0.0/24 is subnetted, 1 subnets
C  172.25.234.0 is directly connected, Ethernet0
  61.0.0.0/32 is subnetted, 2 subnets
i L1 61.78.45.21 [70/100] via 222.118.171.2, GigabitEthernet2/2
C  61.78.41.177 is directly connected, Loopback0
```

VRRP 구현후 다음 그림 5에서와 같이 사용자 PC에서 서비스 GSR loopback IP(61.78.41.177)로 ping 시험을 수행하였다.

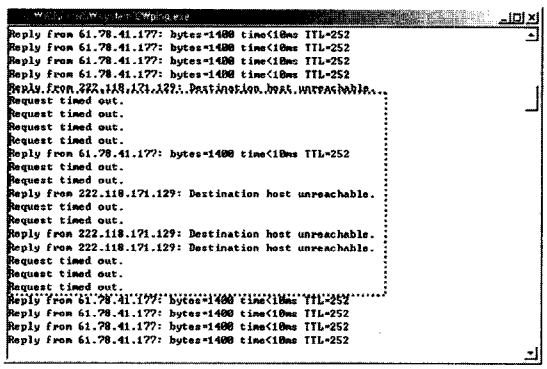

그림 5. VRRP ping 실험 결과
Fig. 5 VRRP ping test result

ping 시험 조건은 VRRP 그룹의 master-backup 라우터간에 마스터 모드(primary)는 RS38K(222.118.171. 130)로 설정 하고, 백업 모드(secondary)는 SER(222.118.171.129)로 하였다. 그 시험 결과는 다음과 같다.

첫째, 라우팅 흐름은 마스터 모드(primary)인 RS38K (222.118.171.130)로 이루어지고 GSR loopback IP(61.78. 41.177)로의 성공적인 트래픽 흐름을 보였다.

둘째, 라우팅 흐름 경로가 백업 모드(secondary)인 SER(222.118.171.129)로 이루어질 때는 라우팅 목적지에 도착 및 응답이 발생되지 않음을 알 수 있다.

따라서 ping 시험 결과 14초 정도의 손실(loss)이 발생한 것으로 나타나 VRRP 구현을 통한 단일 인증 기반의 이중화 제어가 가능함을 증명하였다.

Ⅳ. 결 론

본 논문에서는 단일 웹 인증 기반에 적합한 Test Bed 스몰 망을 구성하여 접근·인증 절차를 제시하고, VRRP 프로토콜을 활용하여 Test Bed 시험 망을 설계하여 VRRP 그룹의 트래픽 흐름을 시뮬레이션을 통해서 비교·분석하였다. 단일 웹 인증 기반에서 VRRP 구현 결과는 다음과 같다.

① VRRP 그룹, 즉 SER과 RS8600간 이중화 기능 구현으로 접속 제어 기반의 서비스 제공이 가능하다.
② 라우팅 프로토콜(BGP/IS-IS) 표준안 적용으로 단일 인증 수용 장비별 라우팅 프로토콜 적용이 가능하다.
③ priority값 조정 및 링크 장애(trouble, down)에 따른 동작 모드의 자동 절체와 이중화 구현으로 패킷 라우팅 절체가 가능하다.

따라서 본 논문에서는 단일 인증 기반의 SER - RS38K 라우터간 물리적인 이원화 운용 체계에 VRRP 프로토콜 기술을 구현하여 네트워크 로드 밸런싱은 물론 자동 장애복구가 가능하고 보안성, 안전성 및 신뢰성을 확보할 수 있는 인증 체계이다.

참 고 문 헌

[1] http://www.mic.go.kr.
[2] Korea Information Security Agency, "An Introduction Computer Security:The NIST Handbook(NIST Special Publication 800-12)", 1999.
[3] Meyer C.H., and S. M. Matyas, "Cryptography: A New Dimension in Computer Data Security", John Wiley & Sons, 1982.
[4] Murray W.H., "Security Considerations for Personal Computers". Tutorial;Computer and Network Security, Oakland, 1986.
[5] National Institute of Standards and Technology, "Guideline for the Advanced Authentication Technology Alternatives", October 1994..
[6] National Institute of Standards and Technology, "Data Encryption Standard", Federal Information Processing Standard Publication 46-2. December 1993.
[7] Denning P., and D. Denning, "The Clipper and Capstone Encryption Systems", American Scientist, 81(4), 1993.
[8] Rivest R., A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol. 21, No. 2, 1978.
[9] Schneier B., "A Taxonomy of Encryption Algorithms", Computer Security Journal, Vol. 9, No. 1, 1993.
[10] 이재완, 고남영, "SPAM 서버를 이용한 초고속 IP 기반의 인증시스템 구축" 한국해양정보통신학회논문지, Vol.8, No.7, 2004.
[11] 이재완, 고남영, 김형진, "초고속 IP 기반에서 GRE 터널링 기법을 이용한 접속 제어 연구", 한국해양정보통신학회논문지, Vol.10, No.6, 2006.

저자소개

반경식(Kyung-sig Ban)

2003년 한남대학교 정보통신공학과(석사졸업)
2005년 군산대학교 전자정보공학부 박사수료

1988 ~현재 : 정보통신부(충청체신청) 재직
※ 관심분야 : 유·무선 통신, 통신정책, 북한통신

이제완(Jae-wan Lee)

1989년 전북대학교 공학사
1996년 군산대학교 공학석사
2004년 군산대학교 공학박사

※ 관심분야 : 초고속인터넷 응용, 유·무선 네트워크, 북한통신

김형진(Hyoung-Jin Kim)

1997년 호원대학교 전자계산학과 이학사
1999년 군산대학교 정보통신공학과 공학석사
2004년 군산대학교 정보통신공학과 공학박사
2004. 9~2005 군산대학교 전자정보공학부 계약교수
2005. 4~2008. 2 익산대학 정보통신과 조교수
2008. 3~현재 전북대학교 응용시스템공학부 조교수
※ 관심분야 : 멀티미디어 DBMS, 멀티미디어 통신 시스템, 북한통신