

IOS Features

이 장에서는 CCIE Lab에서 자주 등장하였던 IOS Feature들에 대해 소개한다.

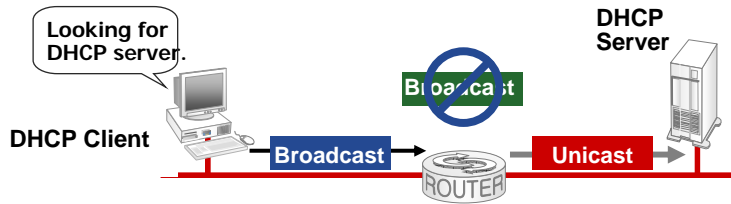
IP Helper-Address

1-2 © 2003, Cisco Systems, Inc. All rights reserved.

<http://www.lsfurion.com>

이 장에서는 IP Helper-Address의 기능과 특징을 소개한다.

IP Helper Address 개요



- Broadcast를 Unicast로 변환하여 Remote Network으로 전달 한다.
- Helper Address에 의해 지원되는 UDP, IP Packet은 다음과 같다.
 - 반드시 MAC Address가 ffff.ffff.ffff여야 한다.
 - 반드시 IP의 목적지 주소가 255.255.255.255 또는 Directed Broadcast 형식 이어야 한다.
 - 반드시 UDP를 사용하는 Packet이어야 한다. (protocol no. = 17)
 - TTL값은 최소한 2 보다 커야 한다.

1-3

<http://www.lsfurion.com>

IP Network에서 Broadcast를 이용하여 자신이 원하는 Resource를 찾아내는 것은 가장 일반적이고 구현이 간단한 방식이다. 하지만 이러한 방식은 Local Network의 범위 안에서만 국한되며, Router들은 특정 Subnet에서 발생한 Broadcast Traffic을 다른 Subnet으로 전달하지 않는다.

예를 들어 DHCP Client가 처음 부팅하면서 가장 먼저 검색하는 것이 DHCP Server의 주소이다. 하지만 위 그림처럼 DHCP Server가 Remote Network에 연결되어 있다면 DHCP Client는 IP 정보를 수신하지 못하게 될 것이다.

이런 경우, Router에서 IP Helper-Address란 기법을 사용하여 DHCP Client가 DHCP Server를 검색하는 Broadcast 주소를 Unicast 주소로 전환하여 전달 할 수 있는데, 이것을 BOOTP Relay Agent Solution이라 한다.

IP Helper Address의 특징은 다음과 같다.

- Broadcast를 Unicast로 변환하여 Remote Network으로 전달 한다.
- Helper Address에 의해 지원되는 UDP, IP Packet은 다음과 같다.
 - 반드시 MAC Address가 ffff.ffff.ffff여야 한다.
 - 반드시 IP의 목적지 주소가 255.255.255.255 또는 Directed Broadcast 형식 이어야 한다.
 - 반드시 UDP를 사용하는 Packet이어야 한다. (protocol no. = 17)
 - TTL값은 최소한 2 보다 커야 한다.
 - 기본적으로 다음과 같은 8개의 UDP port만을 허용한다.
UDP TFTP(69), DNS(53), Time Service(37), NetBIOS name service(137),
NetBIOS datagram service(138), BOOTP server(67), BOOTP client(68),
TACACS(49)

IP Helper Address Command

Router(config-if)#

ip helper-address address

- ◆ main UDP broadcast packet들을 명시된 Unicast Address로 Forwarding한다.
- ◆ Packet의 destination address를 broadcast에서 unicast 또는 directed broadcast address로 변경한다.
- ◆ 다음과 같은 8개의 port들이 자동으로 Open된다.
 - Trivial File Transfer (TFTP) (port 69)
 - Domain Name System (port 53)
 - Time service (port 37)
 - NetBIOS Name Server (port 137)
 - NetBIOS Datagram Server (port 138)
 - Boot Protocol (BOOTP) client and server datagrams (ports 67 and 68)
 - TACACS service (port 49)

Router(config)#

ip forward-protocol { udp [port] | nd | sdns }

- 이곳에 명시된 Packet들을 Forwarding 한다.

1-4

<http://www.lsfurion.com>

Helper-Address의 기본 명령어 문법은 다음과 같다.

Router(config-if)# ip helper-address {ip address}

- Unicast로 전환할 Broadcast가 수신되는 Interface에서 설정한다.
- IP Address 부분에 서버의 위치를 나타내는 Unicast 주소나 Subnet Broadcast(Directed Broadcast) 주소를 적을 수 있다. 이 명령어는 또한 하나 이상의 주소 또는 각 명령어가 다른 호스트 주소를 지칭할 수도 있다.

주요 UDP Broadcast 패킷들의 전달을 받을 서버의 목적지의 주소를 지정한다. 자동적으로 전달이 되도록 열리는 포트는 UDP TFTP(69), DNS(53), Time Service(37), NetBIOS name service(137), NetBIOS datagram service(138), BOOTP server(67)[\[1\]](#), BOOTP client(68)[\[2\]](#), 그리고 TACACS(49)등이다. 패킷의 목적지 주소를 Broadcast에서 Unicast나 Directed Broadcast로 바꾸어주고 서버에게 전달해 주며 Unicast로 결과를 받으면 다시 클라이언트에게는 Broadcast로 바꾸어 전달한다. 주의할 사항은 TCP가 아닌 UDP Broadcast만 전달하고 기본적으로 8개의 포트만 전달한다.

만약 추가적으로 다른 UDP port를 전달하고 싶으면 아래의 명령을 사용하면 된다.

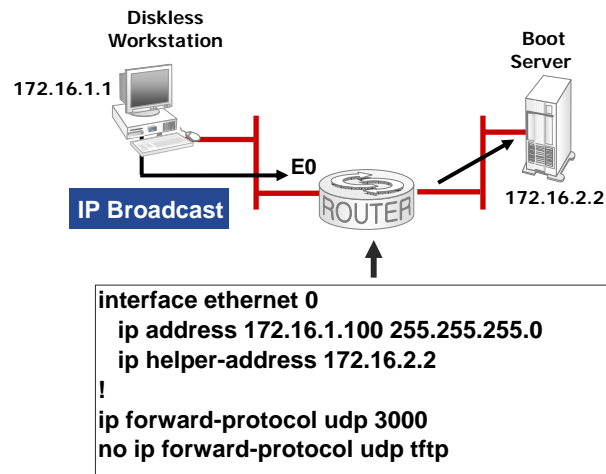
Router(config)# ip forward-protocol { udp [port] | nd | sdns }

기존에 미리 열려져 있는 포트를 닫고 싶으면,

Router(config)# no ip forward-protocol { udp [port] }

명령을 사용하면 된다. 예를 들면 no ip forward-protocol udp 53 면 DNS Client가 Host Name Resolution을 Broadcast로 요청했을 때 그것을 원격지로 전달하지 않는다.

Helper-Address 구성 예제#1



1-5

<http://www.lsfurion.com>

위 그림은 IP Helper Address의 구성 예제이다.

interface ethernet 0

ip address 172.16.1.100 255.255.255.0

ip helper-address 172.16.2.2

→ Ethernet0에서 수신되는 DHCP Discovery Broadcast Packet의
목적지 주소를 172.16.2.2로 변환하여 Forwarding한다.

!

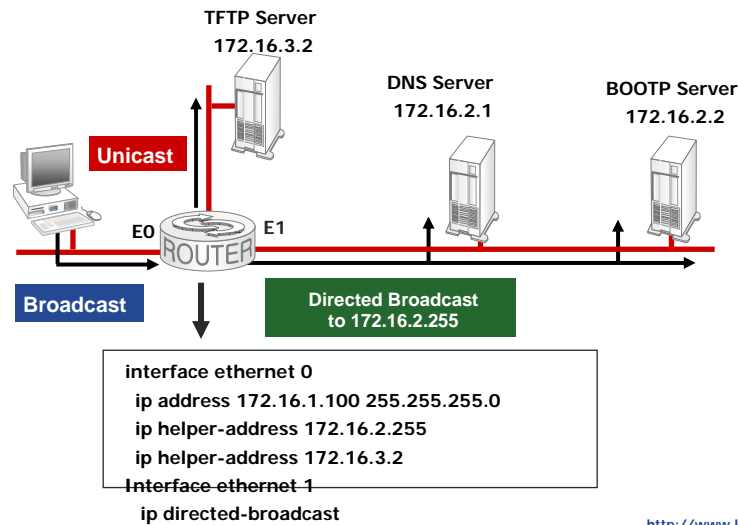
ip forward-protocol udp 3000

no ip forward-protocol udp tftp

→ TFTP를 위한 UDP Port를 Disable하고, 새로운 UDP 3000번을
추가한다.

Helper-Address 구성 예제#1

Directed Broadcast and Unicast



1-6

<http://www.lsfurion.com>

위 그림은 IP Helper-Address에서 목적지 주소를 Directed Broadcast로 변환하는 예제이다.

Directed Broadcast란, 예를 들어 172.16.2.255처럼 특정 Subnet을 명시한 Broadcast 주소이다. 참고로 IP Helper-Address에서 Directed Broadcast를 사용하기 위해서는 반드시 'no ip classless'가 설정되어 있어야 한다.

IP Directed Broadcast

Router는 특정 Interface구간, 즉 특정 subnet 구간 내에서 발생하는 Direct Broadcast를 허용한다. 하지만 외부에서 들어 오는 Packet의 목적지가 Directed Broadcast인 경우는 기본적으로 보안상의 이유로 허용하지 않도록 되어 있다.

예를 들어 위 그림의 Router의 Ethernet1 구간에서 172.16.2.255를 목적지로 하는 Broadcast Traffic이 발생하면 문제가 없겠으나 Ethernet0로부터 입력되는 Directed Broadcast를 허용하지 않는다.

이런 이유로 Ethernet1 Interface에서 Directed Broadcast를 허용하는 Command를 enable해야 한다.

예) router(config-if)#ip directed-broadcast

AutoInstall

- ◆ 정의: 네트워크 관리자가 자동적으로 장치들의 **Configuration**을 로드하게 하는 것
- ◆ 수행: 처음 라우터를 기동하거나 수동으로 **Configuration** 파일을 삭제 후 다시 시작할 때 **NVRAM**에 유효한 **Configuration** 파일이 없을 때 수행
- ◆ 두 가지 접근 방법
 - **Minimum Configuration: TFTP**
 - **Host Specific Full Configuration: TFTP, DHCP, DNS**

1-7

<http://www.lsfurion.com>

Autoinstall이란, Network에 새로 추가된 장비 또는 자동으로 구성 정보를 원하는 IOP Device들의 구성 작업을 자동화 하는 기능을 제공한다. 우리가 실습 중에 장비를 초기화하여 Reload하면 다음과 같은 메뉴를 본적이 있을 것이다.

Would you like to enter the initial configuration dialog? [yes]:

Would you like to terminate autoinstall? [yes]:

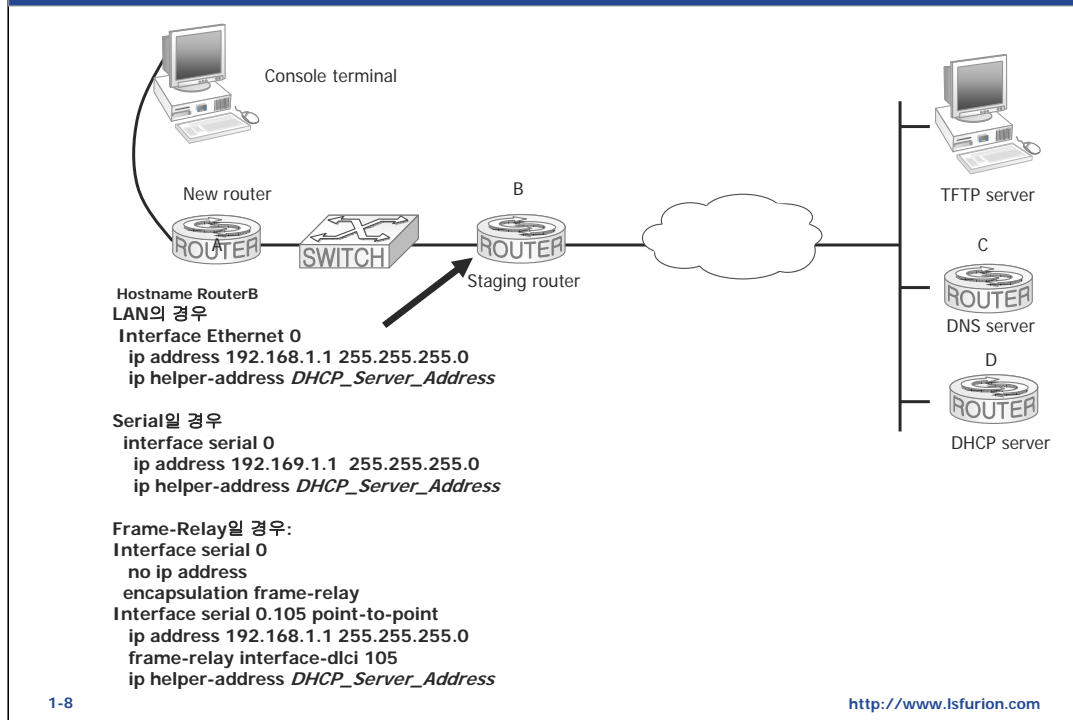
Autoinstall이 가능한 IOS Device들에게 구성 정보를 제공하는 방법에는 단순히 IOS Device들의 구성 정보를 저장한 TFTP Server를 사용하는 방식과 좀더 세분화된 구성 정보를 제공하기 위해 DHCP, DNS, TFTP Server를 이용하는 방식이 있다.

Autoinstall에 대한 자세한 내용은 www.cisco.com/univercd 사이트에서 아래와 같은 URL에서 확인 할 수 있다.

Using Autoinstall and Setup

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcp1/fcf002.htm

Staging 라우터의 설정



CCIE Lab에서는 Autoinstall을 수행하기 위해 필요한 Network상에 환경 설정을 묻게 되는데, 그 중에 위 그림에서 보이는 Staging Router에서 필요한 설정이 무엇인지를 묻는다.

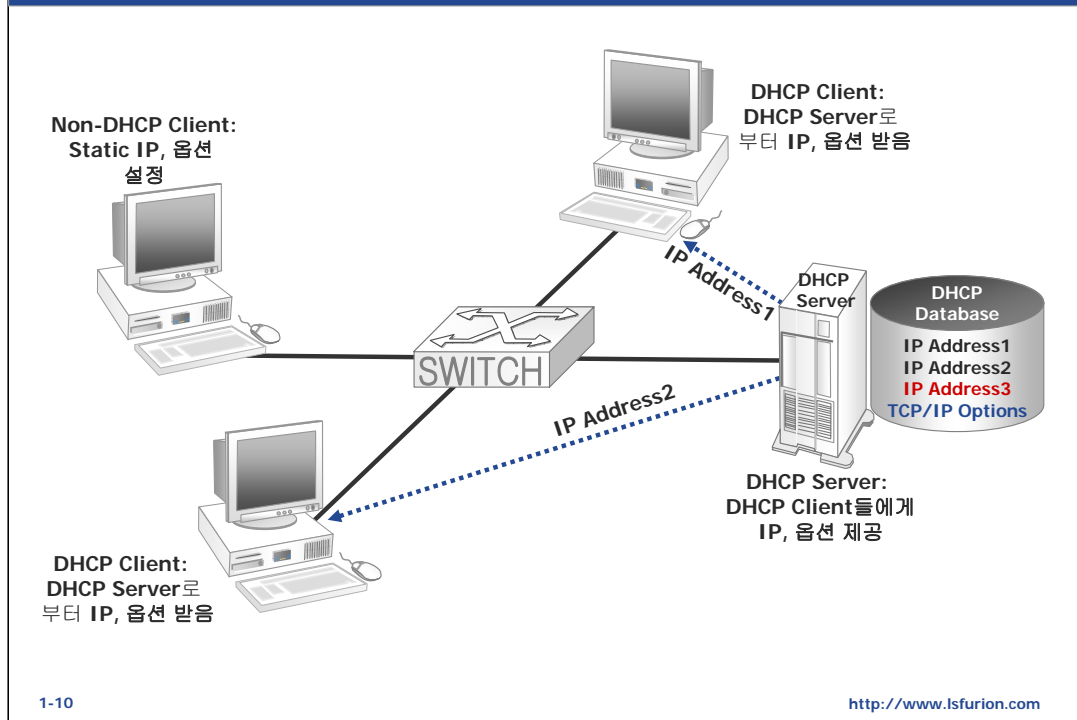
새로 추가 되는 IOS Device가 Autoinstall을 위해 DHCP Server를 검색하는 작업, 또는 TFTP Server를 연결해야 하는 작업을 해야 한다. 이를 위해 Autoinstall을 필요로 하는 Device와 연결된 Router에서 위 작업이 가능하도록 'ip helper-address' command를 사용하여 TFTP와 DHCP Server의 위치를 지정해야 한다.

DHCP

(Dynamic Host Configuration Protocol)

이 장에서는 IOS에서 제공하는 DHCP Service의 구성 방법을 소개한다.

DHCP 란 무엇인가?



DHCP (Dynamic Host Configuration Protocol)

TCP/IP Network에서는 통신에 참여하는 Device들마다 고유한 IP 주소를 가져야만 통신망에 접속이 가능하다. 또한 IP Network에 접근하는 Device들은 자신들에게 고유하게 배정되는 IP 주소 외에도 인터넷에 접속하기 위한 Default Gateway 주소, DNS의 IP, 도메인 이름 등, 기타 IP관련 정보들이 설정되어야 한다. DHCP는 네트워크 관리자들이 조직 내의 네트워크 상에서 IP 주소를 중앙에서 관리하고, 자동으로 할당해줄 수 있도록 해주는 프로토콜이다. DHCP를 사용하지 않는 경우에는, 각 컴퓨터마다 IP 주소가 수작업으로 입력되어야 하므로 관리상의 어려움과 문제 해결 시간이 길어지게 된다.

DHCP는 주어진 IP 주소가 일정한 시간 동안만 그 컴퓨터에 유효하도록 하는 "임대" 개념을 사용한다. DHCP는 영구적인 IP 주소를 필요로 하는 서버에 대해서는 정적인 주소를 제공할 수 있다.

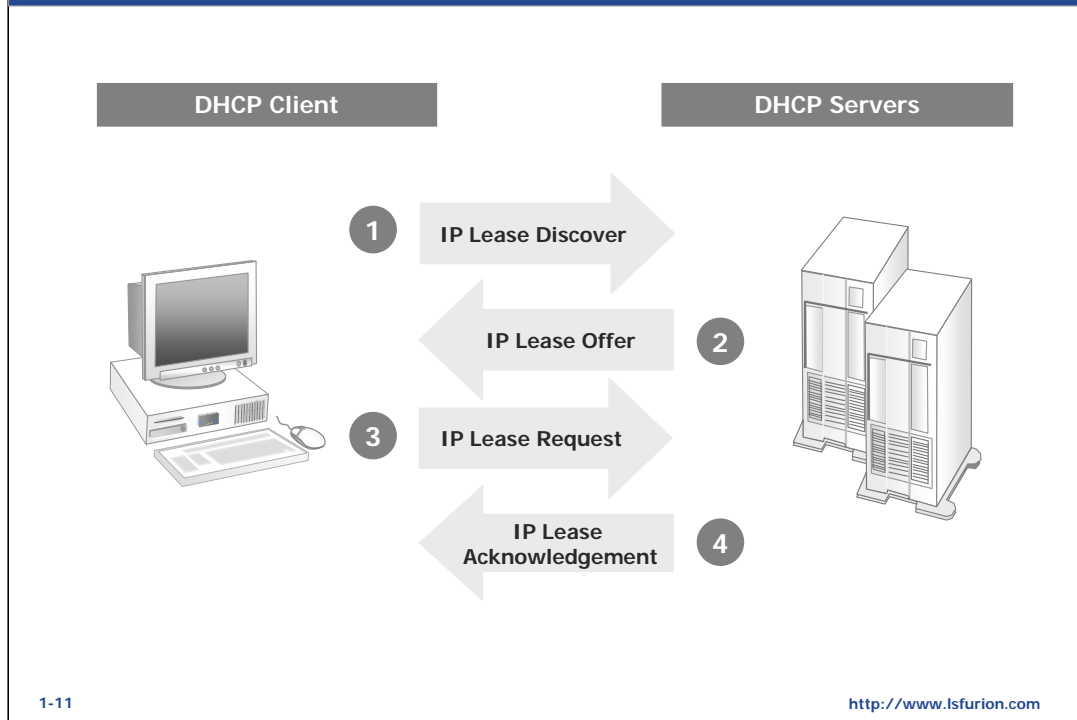
DHCP는 네트워크 IP 관리 프로토콜인 BOOTP (Bootstrap Protocol)의 대안으로 사용된다. DHCP가 더욱 진보된 프로토콜이지만, 두 개의 프로토콜 모두 일반적으로 사용된다. 어떤 조직에서는 두 개의 프로토콜 모두를 사용하지만, 동일한 조직에서 그것을 언제, 어떻게 사용할지를 이해하는 것이 무엇보다 중요하다. 윈도우NT와 같은 몇몇 운영체제에는 DHCP 서버가 달려 나온다. DHCP 또는 BOOTP 클라이언트는 네트워크가 구성될 수 있도록 각 컴퓨터에 위치하는 프로그램이다.

참고.

BOOTP (Bootstrap Protocol) ; 초기 적재 통신 규약

BOOTP는 네트워크 사용자의 시스템이 자동으로 구성되고(IP 주소를 받게), 사용자의 간섭 없이도 부트되는 운영체제를 가질 수 있게 해주는 프로토콜이다. X 터미널 등과 같이 하드 디스크를 갖지 않은 장치의 설정 정보를 자동적으로 할당, 관리하기 위해서 개발되었다. 네트워크 관리자에 의해 관리되는 BOOTP 서버는, 일정 시간 동안만 IP 주소를 자동으로 할당한다. BOOTP는 좀더 진보된 네트워크 관리 프로토콜인 DHCP의 기반이 된다.

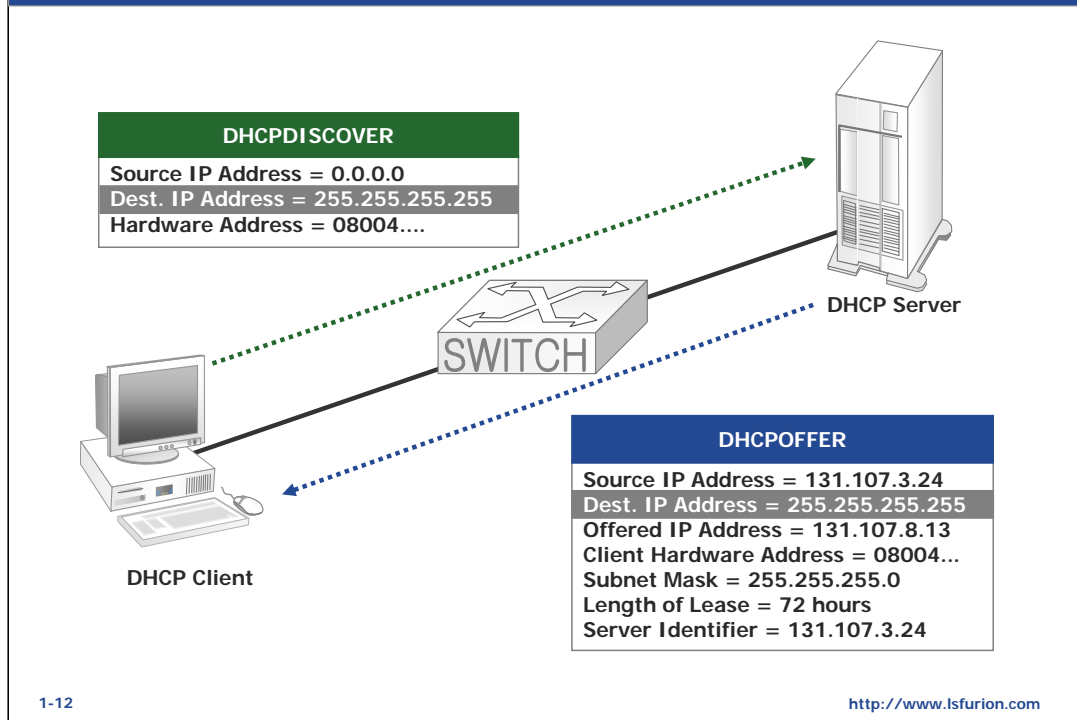
초기 DHCP 임대 요청(Lease Generation Process)



DHCP 임대 요청 절차(Lease Generation Process)절차란 DHCP 클라이언트가 DHCP 서버로부터 IP Address와 여러 가지 TCP/IP 옵션을 받기 위하여 클라이언트와 서버간에 전달되는 통신 패킷들의 종류와 순서를 말한다. 크게 아래와 같은 4개의 패킷에 의하여 모든 일이 처리된다.

- IP Lease Discover
- IP Lease Offer
- IP Lease Request
- IP Lease Acknowledgement

IP Lease Discover와 Offer



- **DHCPDISCOVER:** DHCP 클라이언트가 IP Address와 TCP/IP 옵션들을 DHCP 서버에게 요구하는 패킷의 이름이다. 패킷의 내용 중 핵심적인 것들은 아래와 같다.

Source IP Address = 0.0.0.0

→ IP Address가 아직 할당되지 않았으므로 정의되는 않은 것을 의미한다.

Dest. IP Address = 255.255.255.255

→ 서버의 위치를 모르기 때문에 전체 네트워크로 브로드캐스팅을 수행한다.

Hardware Address = 08004....

→ DHCP 클라이언트의 MAC Address를 패킷에 넣어 보낸다. 클라이언트의 MAC Address가 전달되기 때문에 나중에 이 MAC Address를 가진 클라이언트에게 특정(고정된) IP Address나 특정(고정된) TCP/IP 옵션들을 제공할 수 있다.

- **DHCPOFFER:** 클라이언트의 요청에 따라 DHCP 서버들이 보내는 답변이다.

Source IP Address = 131.107.3.24 → DHCP 서버의 주소이다.

Dest. IP Address = 255.255.255.255

→ 클라이언트가 아직 IP Address를 가지고 있지 않기 때문에 브로드캐스팅을 통해서 알려야 한다.

Offered IP Address = 131.107.8.13 → DHCP 서버가 클라이언트에게 제공하는 주소

Client Hardware Address = 08004...

→ DHCP 클라이언트의 MAC Address, 만약 하나의 물리적인 세그먼트에 DHCP 클라이언트가 여러 개 있어 동시에 요청을 했을 때 어느 클라이언트에게 어떤 IP Address를 제공했는지를 알려야 하기 때문이다. 이것이 없다면 여러 클라이언트들이 같은 IP Address를 갖게 되는 문제가 발생할 것이다. 클라이언트는 자신의 MAC Address를 통해 이 패킷이 자신의 것이라는 것을 인식한다.

Subnet Mask = 255.255.255.0

→ TCP/IP 옵션 중 Subnet Mask는 기본적으로 제공한다.

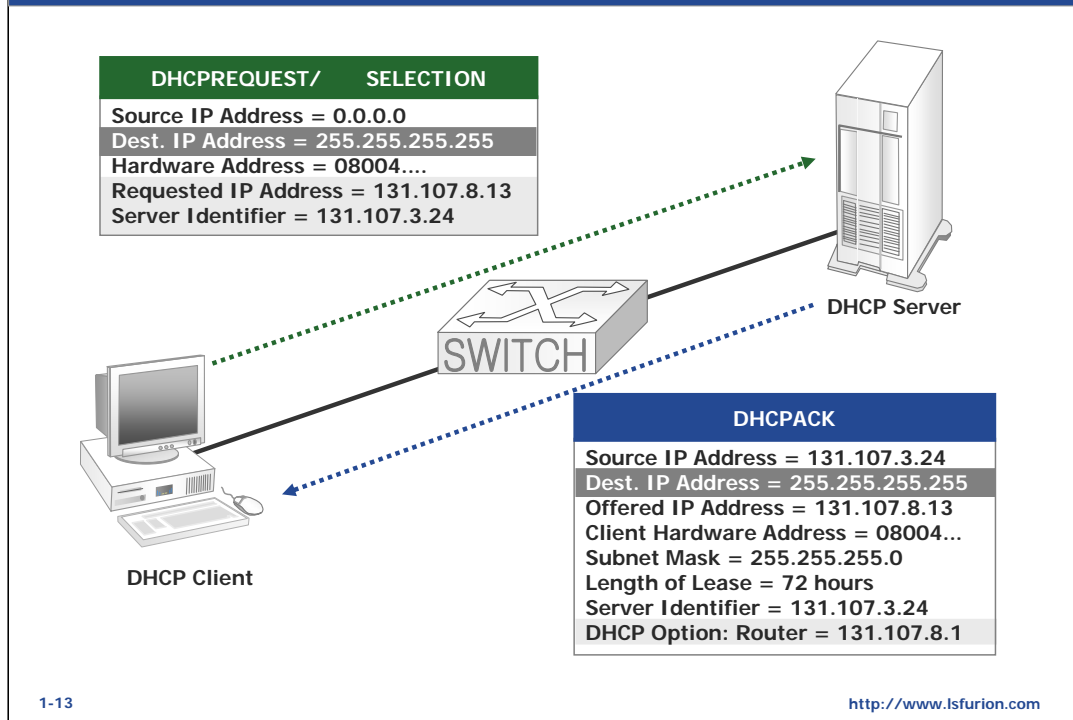
Length of Lease = 72 hours

→ IP Address와 TCP/IP 옵션들의 임대를 해 줄 수 있는 시간을 나타낸다.

Server Identifier = 131.107.3.24

→ 제공한 서버의 IP Address이다. 이것은 하나의 물리적인 세그먼트에 서버가 여러 대 있고, 여러 서버에 동시에 한 클라이언트에게 IP Address와 TCP/IP 옵션을 제공했을 때 각 서버들을 구별하기 위해서 필요하다.

IP Lease Request와 Acknowledgment



- **DHCPREQUEST와SELECTION:** 클라이언트가 여러 대의 DHCP 서버들로부터 받은 하나의 IP Address를 선택하여 자신이 사용하겠다고 제공한 DHCP 서버에게 요청하는 것을 말한다.

Source IP Address = 0.0.0.0

Dest. IP Address = 255.255.255.255

→ DHCPREQUEST에서 Server Identifier라는 서버의 주소를 받았음에도 불구하고 브로드 캐스팅을 계속하는 것은, 이것을 단지 선택 받은 서버에게만 보내는 것이 아니라 이 클라이언트에게 동시에 여러 대의 DHCP 서버들이 IP Address를 보냈을 경우, 그 모든 다른 DHCP 서버들에게 이 클라이언트가 특정 서버를 선택했다는 것을 알리기 위함이다.

Hardware Address = 08004....

→ 선택을 당하지 못한 DHCP 서버들이 이 MAC Address를 가진 클라이언트에게 제공한 IP Address를 수거한다.

Requested IP Address = 131.107.8.13

→ 클라이언트가 사용하겠다고 요청하는 IP Address

Server Identifier = 131.107.3.24

→ 선택된 서버의 IP Address를 말하면서 동시에 선택되지 않는 DHCP 서버들에게도 자신들이 선택되지 않았다는 것을 알리는 역할을 한다.

- **DHCPACK:** 선택된 서버가 요청한 클라이언트에게 최종적으로 그 IP Address의 사용을 허가하고 관련된 TCP/IP 옵션들을 제공하는 패킷이다. 이 시점에서 TCP/IP 옵션들이 제공된다.

Source IP Address = 131.107.3.24 → DHCP 서버의 주소

Dest. IP Address = 255.255.255.255

→ 여전히 아직 클라이언트는 IP Address사용의 확답을 받지 못했다.

Offered IP Address = 131.107.8.13 → 클라이언트에게 확답으로 제공할 IP Address

Client Hardware Address = 08004... → 클라이언트의 MAC Address

Subnet Mask = 255.255.255.0

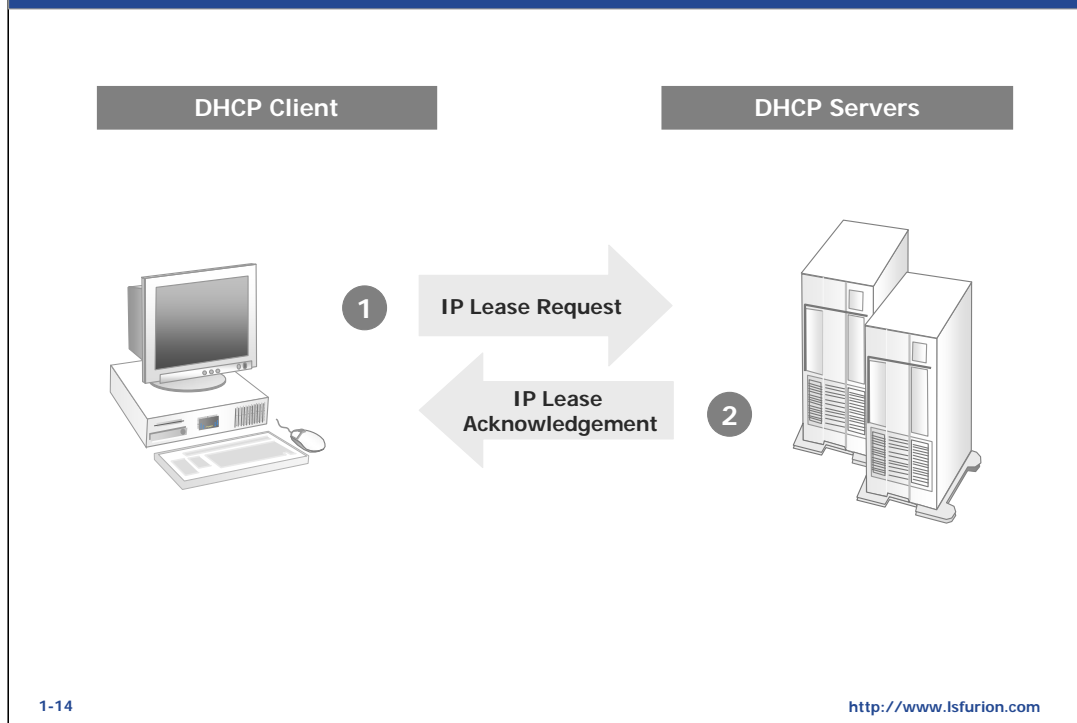
Length of Lease = 72 hours → 클라이언트가 사용할 수 있는 대여시간

Server Identifier = 131.107.3.24 → 서버의 IP Address

DHCP Option: Router = 131.107.8.1

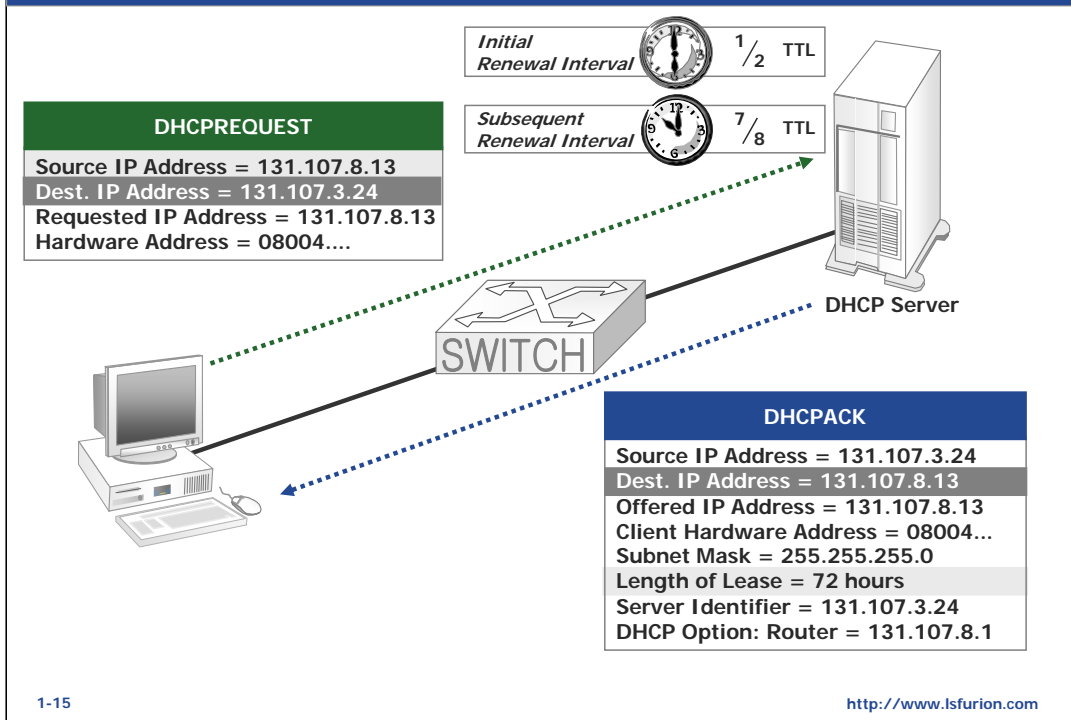
→ 최종적으로 TCP/IP 관련 옵션들을 제공한다. 여기는 Default Gateway 주소가 한 개 나왔지만, Domain Name, DNS Server 주소들, WINS 서버주소들, NetBIOS Name Node Type 등 다양한 옵션들을 제공할 수 있다.

DHCP Lease Renewal Process



DHCP Lease Renewal Process란 호스트가 DHCP 서버로부터 받은 Lease Time(임대기간)의 1/2의 시간이 지났거나 호스트가 재부팅을 수행하면 이전에 자신이 사용했던 IP Address와 TCP/IP 옵션들을 계속적으로 사용하기 위해서 확인하는 절차를 수행하는 것은 말한다.

IP Lease Renewal Request/ACK



• DHCPREQUEST: 클라이언트가 갱신을 요구한다.

Source IP Address = 131.107.8.13 → 이번에는 유니캐스팅 클라이언트 주소이다.

Dest. IP Address = 131.107.3.24 → DHCP 서버의 주소이다.

Requested IP Address = 131.107.8.13 → 자신이 계속 사용하고자 요청하는 주소이다.

Hardware Address = 08004....

→ 클라이언트의 MAC Address인데, DHCP 서버는 데이터베이스내에 이 MAC Address와 제공한 IP Address의 테이블을 가지고 있다.

• DHCPACK: 클라이언트 갱신 요청에 반응한다.

Source IP Address = 131.107.3.24 → DHCP 서버의 주소

Dest. IP Address = 131.107.8.13 → DHCP 클라이언트의 주소

Offered IP Address = 131.107.8.13

→ 계속 사용할 주소, DHCP 서버 쪽에서 이 주소를 폐기했다면 다른 주소가 올 수도 있다.

Client Hardware Address = 08004...

Subnet Mask = 255.255.255.0

Length of Lease = 72 hours

→ 새로운 임대 기간의 시작을 제공한다. 예를 들면, 클라이언트가 원래 72시간의 1/2인 36시간이 되었을 때 갱신 요청을 했을 것이고, 갱신에 대한 반응으로 새로운 72시간이 부여되면 나머지 36시간을 보내고 여기에 72시간을 더하는 방식이 아니라 위의 나머지 36시간은 무시하고 여기서 새로운 72시간이 시작된다.

Server Identifier = 131.107.3.24

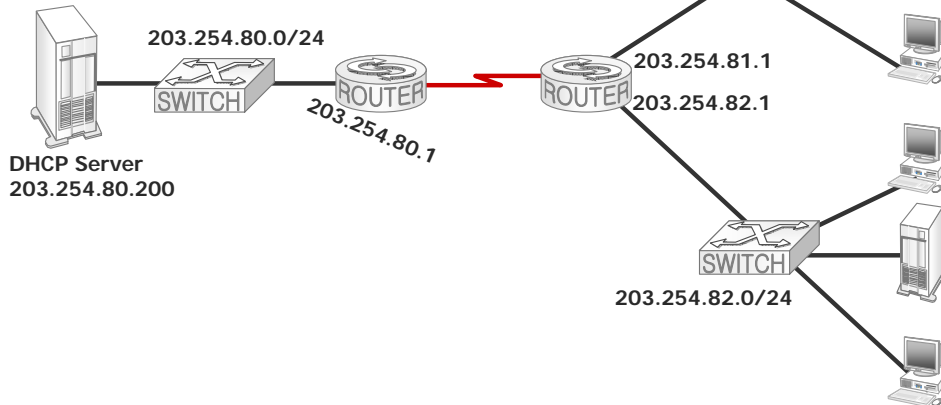
DHCP Option: Router = 131.107.8.1

→ 여기가 중요한데, 이때 서버 쪽에서 새로 변경된 TCP/IP 옵션들이 있으면 그것이 전달된다. 즉, 클라이언트는 기존에 자기가 사용하던 IP Address는 그대로 받지만 옵션은 새로운 것을 받아서 사용한다는 의미이다.

Scope 개관

컴퓨터들에 임대해 주기 위한 IP Address들과 옵션들의 집합

Scope
203.254.80.2~50
203.254.81.2~50
203.254.82.2~50



1-16

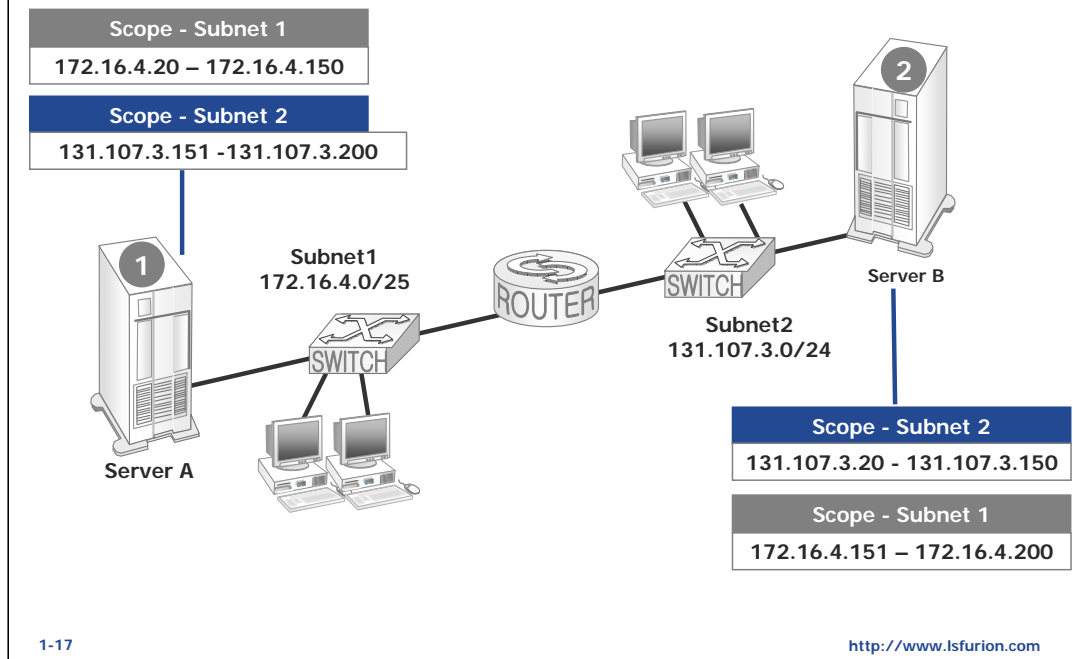
<http://www.lsfurion.com>

DHCP Scope란 DHCP 서버가 자신이 서비스를 제공한 여러 Subnet의 호스트들에 대해서 공급할 IP Address의 범위와 각 Subnet에 적합한 각종 TCP/IP 옵션들을 가지고 있는 것을 Scope라고 한다.

Scope 옵션이란 각각의 DHCP Scope에 적합한 TCP/IP 옵션들을 설정하는 것을 말한다. Scope는 대부분 TCP/IP Subnet마다 따로 할당됨으로 TCP/IP Subnet이 다르다면 대표적으로 Default Gateway와 같은 옵션들은 반드시 다르게 지정되어야만 한다.

이밖에 DHCP에 의해서 지원될 수 있는 TCP/IP 옵션들은 Default Gateway(Router)의 주소, DNS Server의 IP 주소, DNS Domain Name, WINS Server의 IP 주소, NetBIOS over TCP/IP Name Resolution의 형태등, 다양한 옵션들을 제공할 수 있다.

DHCP Server의 결함허용과 부하분산



DHCP 서버도 다운되어서는 안 되는 기업의 핵심적인 서버 중의 하나이다. 설사 다운되는 상황이 발생되어 정상적인 서비스를 할 수 없는 상황이 되더라도 기존에 이미 IP Address와 TCP/IP 옵션들을 받은 호스트들은 Lease Time이 만료될 때 까지는 문제가 없다.

그러나, 새로 부팅하는 클라이언트들은 DHCP 서비스를 받지 못하면 169.254.x.x의 Automatic Private IP Address가 설정됨으로써 로컬 서브넷외에는 외부로 통신을 수행할 수가 없을 것이다. 이런 이유로 중앙집중적인 IP Address와 TCP/IP 옵션관리가 중요할 지라도 DHCP 서버를 한대만 운영하는 것은 결함허용(Fault Tolerance)나 부하분산(Load Balancing)의 측면에서 바람직하지 못하다.

그래서 권장하는 바는 적어도 두 대 정도의 DHCP 서버를 다른 서브넷상에 배치하는 것이 좋다. 문제는 Scope의 IP Address의 영역을 지정하는 것인데 절대 특정 Scope의 IP Address의 같은 영역을 가지고 있으면 안 된다. 만약 같은 영역을 가지고 있다가 다른 클라이언트에 같은 주소를 부여하면 DHCP 클라이언트들이 IP Address 충돌 현상을 일으킬 것이다. IP SCOPE POOL 배정시 75 vs. 25의 규칙을 사용하면 좋다.

하나의 DHCP 서버에 같은 Scope의 IP Address 범위의 75%를 가지고 있고 다른 DHCP 서버에 이 Scope의 IP Address의 다른 범위의 25%를 가지고 있게 하는 것이다. 이러한 식으로 모든 Scope를 정의하면 되는 것이다. 물론 75%와 25%를 가지고 있는 전체적인 Scope의 양을 균형을 유지하는 것이 좋다. 예를 들면 DHCP1 서버는 A Scope의 75%와 B Scope의 25%를 가지고 있고 DHCP2 서버는 A Scope의 25%와 B Scope의 75%를 가지고 있는 식이다. 이러한 Scope들을 적절하게 나누어 두 대 이상의 서버가 가지고 있으면 부하분산이 가능하면서 둘 중 한 서버가 죽더라도 다른 서버가 나머지 Scope영역을 가지고 서비스를 계속할 수 있어서 결함허용의 효과까지 얻을 수 있다.

Superscope를 이용해서 Scope 결합

The diagram illustrates a network setup for IP address aggregation using Superscope. A central SWITCH is connected to four desktop computers and a DHCP Server. The DHCP Server is also connected to a ROUTER. The SWITCH is configured with two scopes: Scope1 (192.168.1.2 to 192.168.1.254) and Scope2 (192.168.2.2 to 192.168.2.254). The SWITCH's Interface Ethernet0 is configured with the primary IP address 192.168.1.1 and the secondary IP address 192.168.2.2. The four desktop computers are labeled with their respective IP addresses: 192.168.1.2, 192.168.1.254, 192.168.2.2, and 192.168.2.254.

SuperscopeA

- Scope1**
192.168.1.2
⋮
192.168.1.254
- Scope2**
192.168.2.2
⋮
192.168.2.254

SWITCH

DHCP Server

ROUTER

Interface Ethernet0
ip address 192.168.1.1 255.255.255.0
ip Address 192.168.2.2 255.255.255.0 secondary

192.168.1.2 **192.168.1.254** **192.168.2.2** **192.168.2.254**

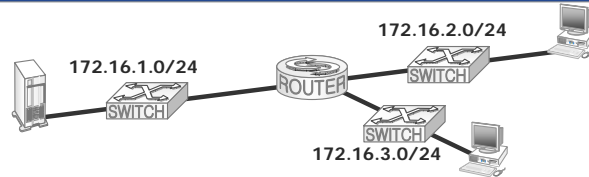
1-18

<http://www.lsfunion.com>

Superscope란 두 개 이상의 다른 서브넷을 결합해서 마치 하나의 Scope처럼 DHCP 서버가 생각하게 하는 것이다. 그래서 하나의 서브넷을 위한 IP Address가 소진되었을 때 다른 Scope의 IP Address와 TCP/IP 옵션들을 줄 수 있는 기능을 수행한다.

18

Cisco Router에서 DHCP Server 설정 예



```

service dhcp
!
ip dhcp excluded-address 172.16.1.1
ip dhcp excluded-address 172.16.2.1
ip dhcp excluded-address 172.16.3.1
!
ip dhcp pool Scope_172.16.0.0_Network
network 172.16.0.0 255.255.0.0
domain-name lns.co.kr
dns-server 172.16.51.200 10.1.1.1
netbios-name-server 172.16.51.201
netbios-node-type h-node
lease 8
!
ip dhcp pool Scope_172.16.1.0_Subnet
network 172.16.1.0 255.255.255.0
default-router 172.16.1.1
!
ip dhcp pool Scope_172.16.2.0_Subnet
network 172.16.2.0 255.255.255.0
default-router 172.16.2.1

```

```

ip dhcp pool Scope_172.16.3.0_Subnet
network 172.16.3.0 255.255.255.0
default-router 172.16.3.1
!
ip dhcp pool Scope_172.16.1.100_Host
host 172.16.1.100 255.255.255.0
client-identifier 0100.a024.2b2a.60
domain-name sales.lns.co.kr
client-name instructor
!
interface Ethernet 1
IP Address 172.16.1.1 255.255.255.0
!
interface Ethernet 2
IP Address 172.16.2.1 255.255.255.0
!
interface Ethernet 3
IP Address 172.16.3.1 255.255.255.0

```

1-19

<http://www.lsfurion.com>

Cisco IOS에서 제공하는 DHCP Service는 다음과 같이 구성한다.

1.DHCP Service를 Enable한다.

예) router(config)#ip dhcp service

2.DHCP Service에서 제외시켜야 하는 하는 IP 주소들을 설정한다.

예) router(config)#ip dhcp excluded-address 172.16.1.1

→ Default Gateway 또는 이미 배정된 고정 IP들을 선언해 준다.

3.DHCP Pool을 생성하고 필요한 IP Option을 설정한다.

예)

ip dhcp pool Scope_172.16.0.0_Network

→ 네트워크 전체를 커버할 수 있는 Scope를 만들었다.

network 172.16.0.0 255.255.0.0

→ 전체 네트워크를 선언합니다. IP Address의 범위를 지정하는 것과 같다.

domain-name learningsharing.co.kr

→ Windows 2000/2003시리즈 DHCP서버의 Server Level 옵션들을 지정하는 것으로 DNS domain-name을 지정한다.

dns-server 172.16.51.200 → DNS Server의 주소를 지정한다.

netbios-name-server 172.16.51.201 → WINS Server의 주소를 지정한다.

netbios-node-type h-node → NetBIOS Name Query의 형식을 지정한다.

lease 8 → IP Address와 TCP/IP 옵션들의 임대기간을 지정한다.

ip dhcp pool Scope_172.16.1.0_Subnet

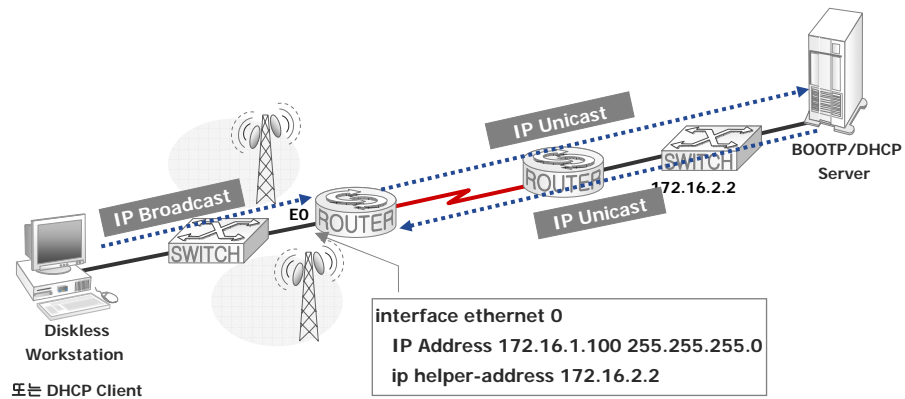
→ 전체 네트워크 중에서 일부 Subnet에 할당될 주소영역과 옵션들을 지정한다.

network 172.16.1.0 255.255.255.0

→ 할당할 subnet의 IP Address의 범위를 지정한다.

default-router 172.16.1.1

라우터의 BOOTP Relay Agent



- ◆ 라우터는 원래 Broadcast를 전달하지 않음 → Switch의 VLAN과 더불어 Broadcast Domain을 나눔
- ◆ Helper address를 UDP Broadcast 중 선택적으로 전달해 줌
- ◆ DHCP와 관련해 Cisco Router에서는 BootP Relay Agent 기능을 수행

1-20

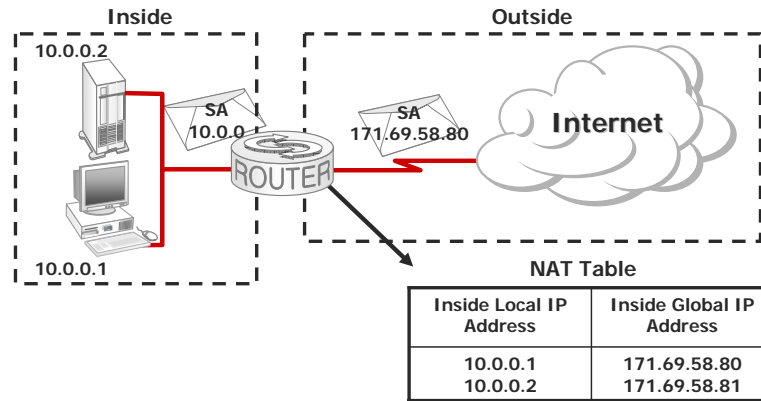
<http://www.lsfurion.com>

위 그림은 Remote Network의 DHCP Server로 부터 IP 정보를 수신 할 수 있도록 Router에서 IP Helper Address를 이용한 Bootp Relay Agent를 설정한 예제이다.

IOS를 이용한 NAT Service

이 장에서는 NAT의 기본적인 기능과 특징, 그리고 IOS에서 NAT를 구성하는 방법에 대해 소개한다.

Network Address Translation



- IP 자원을 절약 할 수 있다.
- 내부 **Network** 구조를 감추고, 외부로부터 보호 할 수 있다.

1-22

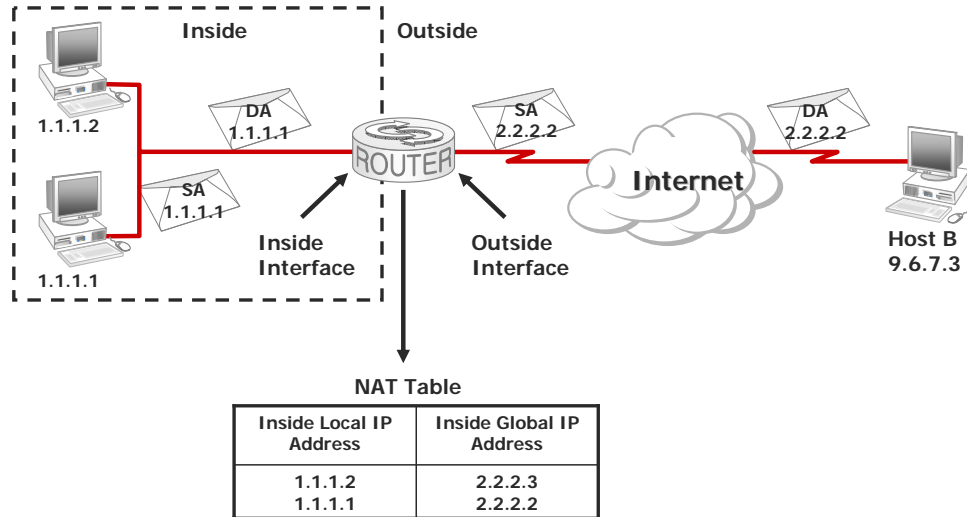
<http://www.lsfurion.com>

NAT를 사용하는 목적에는 2가지가 있는데, 첫째는 인터넷의 공인 IP주소를 절약할 수 있다는 점이고, 둘째는 인터넷이란 공공망과 연결되는 내부 Network를 외부 침입자들로부터 보호할 수 있다는 점이다.

인터넷의 공인 IP주소는 한정되어 있기 때문에 가급적 이를 공유할 수 있도록 하는 것이 필요한데, NAT를 이용하면 사설 IP주소를 사용하면서 이를 공인 IP주소와 상호 변환할 수 있도록 하기 때문에 공인 IP주소를 사설 IP를 가진 다수의 사용자들이 함께 사용할 수 있도록 한다.

CCIE Lab에서 NAT를 대상으로 하는 문제가 나온다면, NAT의 두 가지 목적을 모두 만족시킬 수 있는 구성을 설정 할 수 있어야 한다.

Translating Inside Source Addresses



1-23

<http://www.lsfurion.com>

NAT와 관련된 용어들은 다음과 같은 것들이 있다.

내부(inside) : 어드레스 변환의 대상이 되는 내부 사설 네트워크 군이다.

외부(outside) : 다른 네트워크를 의미한다. 통상적으로 인터넷을 의미한다.

내부로컬 IP Address(inside Local IP Address) : 내부 네트워크의 단말기 또는 호스트 사설 IP Address로서 내부적으로 중복되지 않는 어드레스이다. 내부 IP는 RFC 1918의 어드레스 스페이스에 할당된 프라이빗 어드레스를 사용하기를 권장한다. Private Address는 외부(인터넷)로 라우팅이 안되지만 비공인 IP Address를 그냥 사용한다면 인터넷에서 IP충돌로 인한 문제가 발생할 수 있다.

내부 글로벌 IP Address(Inside Global IP Address) : 내부 호스트의 IP Address와 대응되는 외부의 공인 IP Address이다. 내부 사용자의 IP Address가 이 공인 어드레스로 변환되어 나간다.

단순 변환 엔트리(Simple Translation Entry) : 기존 IP Address와 다른 IP Address를 대응시키는 변환 테이블의 엔트리이다.

확장 변환 엔트리(Extended Translation Entry) : IP Address와 포트번호 쌍을 대응시키는 변환 테이블의 엔트리이다.

NAT가 제공하는 주용 기능은 다음과 같다.

고정 어드레스 변환(Static Address Translation) : 내부 로컬 어드레스와 글로벌 어드레스를 1 대 1로 매핑하여 설정할 수 있다.

동적 소스 어드레스 변화(Dynamic Source Address Translation) : 내부 로컬 어드레스와 글로벌 어드레스의 매핑을 동적으로 작성할 수 있다. 글로벌 어드레스에 할당된 어드레스는 어드레스 풀(Address Pools)에 저장한다. 로컬 어드레스가 자신의 소스 어드레스를 어드레스 풀에 있는 글로벌 어드레스로 변환시킨다. 그리고 변환된 어드레스는 변환 테이블의 엔트리에 등록된다.

동적 포트 변화(Dynamic Port Translation) : 글로벌 어드레스 풀에 있는 어드레스를 절약하기 위해 TCP 또는 UDP의 소스 포트를 사용해서 변환할 수 있다. 여러개의 로컬 어드레스가 동일한 글로벌 어드레스를 사용하더라도 포트번호로 구분할 수 있다. 따라서 변환이 필요할 때에는 Berkeley Standard Distribution의 협정에 따라서 오리지널과 같은 영역(1-511, 512-1023, 1024-4999, 5000-65535)에 있는 새로운 포트 번호를 선택한다.

도착지 어드레스 로타리 변환(Destination Address Rotary Translation) : 동적 도착지 변환은 외부에서 내부로 특정 트래픽이 통과하도록 설정할 수 있다. 매핑이 설정되면 Access List의 어드레스와 매치되는 도착지 어드레스는 로컬 풀에 있는 어드레스로 치환된다. 이 어드레스의 할당에는 외부에서 내부로 새로운 커넥션이 확립될 때만 라운드 로빈 방식으로 할당된다.

Static Translation 설정하기

```
Router(config)#ip nat inside source static local-ip global-ip
```

- **inside local address** 와 **inside global address**의 **Mapping** 관계를 수동으로 설정한다.

```
Router(config-if)#ip nat inside
```

- 해당 **Interface**가 내부 **Network**에 연결되어 있음을 설정한다.

```
Router(config-if)#ip nat outside
```

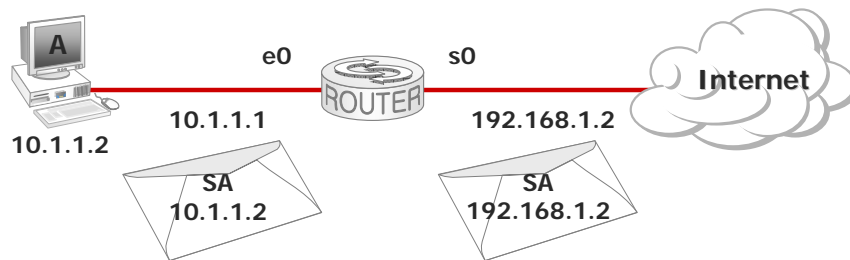
- 해당 **Interface**가 외부 **Network**에 연결되어 있음을 설정한다.

1-24

<http://www.lsfurion.com>

위 명령어는 고정 어드레스 변환(Static Address Translation)을 수행하기 위해 필요한 명령어이다.

Static NAT Address Mapping 예제



```
Interface s0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
Interface e0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
Ip nat inside source static 10.1.1.2 192.168.1.2
```

1-25

<http://www.lsfurion.com>

위 그림은 1:1 Mapping 관계를 설정하여 NAT 서비스를 지원하는 예제이다. PC A가 외부 Network으로 IP Packet을 전송하면, Router는 해당 Packet의 Source Address를 192.168.1.2로 변환하여 전달한다.

Dynamic Translation 설정하기

```
Router(config)#ip nat pool name start-ip end-ip  
{netmask netmask | prefix-length prefix-length}
```

- NAT가 제공하는 pool을 정의한다.

```
Router(config)#access-list access-list-number permit  
source [source-wildcard]
```

- NAT의 서비스를 받아야 하는 Inside Local의 Source Network을 위한 Standard ACL을 정의한다.

```
Router(config)#ip nat inside source list  
access-list-number pool name
```

- dynamic source translation의 대상이 되는 access list Number를 설정한다.

1-26

<http://www.lsfurion.com>

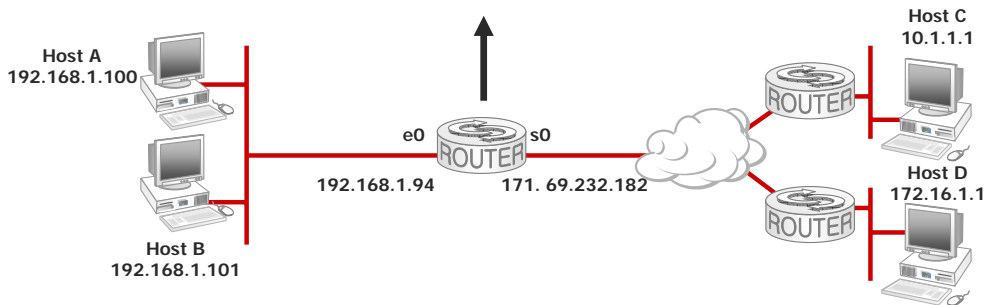
위 그림은 Dynamic NAT Service를 위한 기본 구성의 예제이다.

아래는 NAT 설정과 관련된 Global Command들이다.

- ip nat pool <name> <start-ip> <end-ip> { netmask <netmask> | prefix-length <prefix-length> } [<type {rotary}]
 - Pool의 정의
 - Pool에 있는 어드레스는 start address, end address 와 netmask를 사용해서 정의한다. 이들 어드레스는 필요에 따라서 할당된다.
- ip nat inside source { list <acl> pool <name> [overload] | static <local-ip> <global-ip> }
 - 내부 소스 어드레스를 변환 가능하게 한다.
 - 최초의 명령은 동적 변환을 설정하는 명령이다. 이 간단한 access list에 해당하는 어드레스가 있으면 지정된 풀에서 할당된 글로벌 어드레스를 사용해서 변환한다. 옵션의 키워드를 사용해서 UDP와 TCP의 포트 변환도 가능하다.
- ip nat inside destination { list <acl> pool <name> | static <global-ip> <local-ip> }
 - 내부 도착지 어드레스의 변환을 가능하게 한다.
 - 이 명령어는 소스변환 명령과 유사하다. 동적 변환과 같이 pool은 로컬 타입으로 한다.
- ip nat outside source { list <acl> pool <name> | static <global-ip> <local-ip> }
 - 외부 소스 어드레스의 변환을 가능하게 한다.
 - 최초의 명령(list ... pool ...)은 동적변환을 가능하도록 설정한다. 패킷의 어드레스가 이 access list에 있는 어드레스와 매칭이 되면 지정된 pool에서 할당된 로컬 어드레스를 사용해서 변환시킨다.
 - Static Option은 정적 변환을 설정하는 명령어이다.

Dynamic Address Translation 예제

```
ip nat pool net-208 208.69.233.210 208.69.233.250 netmask 255.255.255.0
ip nat inside source list 1 pool net-208 [overload]
!
interface serial 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```



1-27

<http://www.lsfurion.com>

위 그림의 예제는 Dynamic NAT의 전형적인 예제이다.

위 예제의 Router는 다음과 같은 구성을 기반으로 192.168.1.0/24 Network에 대해서만 NAT 서비스를 수행하고 있다.

```
ip nat pool net-208 208.69.233.210 208.69.233.250 netmask 255.255.255.0
```

→ NAT Pool의 이름은 'net-208'이며, 현재 이 Pool에는 Address Translation을 위한 주소 범위를 208.69.233.10에서 208.69.233.50까지 제공할 것이다.

```
ip nat inside source list 1 pool net-208 [overload]
```

→ NAT Pool의 자원을 access-list 1에서 정의한 Source Network에게만 제공한다.

NAT Pool은 순차적으로 IP 자원을 배포하며, NAT Pool에서 IP 자원이 고갈되면, 이후에 외부 Network으로 Packet을 전송하려고 하는 PC는 NAT 서비스를 제공 받지 못하게 된다.

만약 IP 자원이 부족하여도 기존에 할당된 IP를 다른 노드들과 공유하여 사용할길 바란다면 'overload' option을 추가 할 수 있다.

!

Interface serial 0

```
ip address 171.69.232.182 255.255.255.240
```

ip nat outside → 외부 Network에 연결된 interface임을 표시한다.

!

Interface ethernet 0

```
ip address 192.168.1.94 255.255.255.0
```

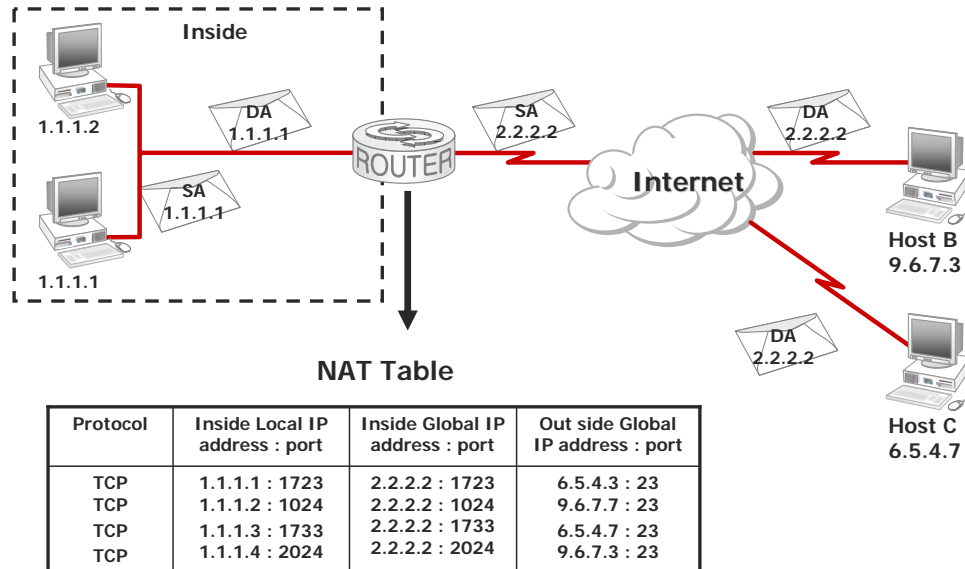
ip nat inside → 내부 Network에 연결된 interface임을 표시한다.

!

```
Access-list 1 permit 192.168.1.0 0.0.0.255
```

→ NAT Pool의 서비스 대상이 되는 Source Network을 정의한다.

Inside Global Address의 Overloading



1-28

<http://www.lsfurion.com>

NAT는 IP 공유기의 개념처럼 소수의 공용 IP를 다수의 사설 IP를 가진 시스템들이 공유하는 환경에서 많이 적용된다.

예를 들어 30명의 직원이 있는 회사가 인터넷 연결을 위한 1개의 공용 IP만을 가진 상황이라면, NAT를 통해 1개의 공인 IP를 30명이 공유할 수 있도록 설정할 수 있다.

이런 상황에서 NAT Service를 수행하는 Router는 사설 IP와 공인 IP간의 Mapping 정보 말고도 TCP와 같은 상위 Layer의 port 정보를 기반으로 Inside Local Address와 Inside Global Address간의 연결 정보를 관리하게 된다.

Overloading 설정하기

```
Router(config)#access-list access-list-number permit  
source source-wildcard
```

- **dynamic source translation**의 대상이 되는 **access list Number**를 설정한다.

```
Router(config)#ip nat inside source list  
access-list-number interface interface overload
```

- **NAT Service**를 제공해야 하는 **Source Network**과 사설 노드 들이 공유하는 **Interface**의 **point**을 설정한다.

1-29

<http://www.lsfurion.com>

NAT Overloading 구성을 위해 필요한 명령어는 다음과 같다.

1.dynamic source translation의 대상이 되는 access list Number를 설정한다.

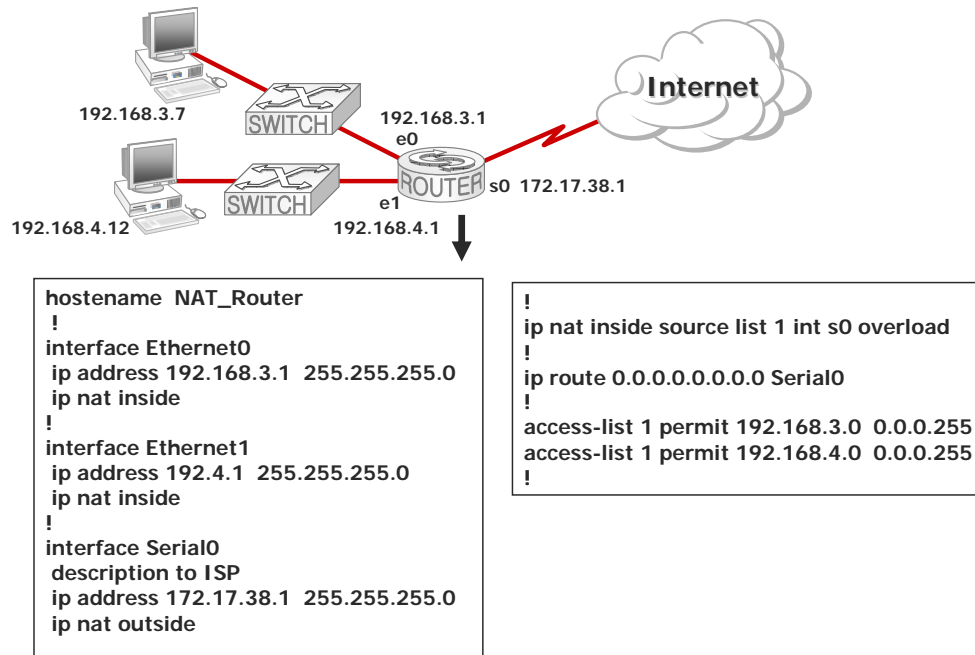
```
Router(config)#access-list access-list-number permit source source-wildcard
```

2.NAT Service를 제공해야 하는 Source Network과 사설 노드 들이 공유하는

Interface의 point을 설정한다.

```
Router(config)#ip nat inside source list access-list-number interface interface overload
```

Overloading an Inside



1-30

<http://www.lsfurion.com>

위 그림은 Overloading을 이용한 구성 예제이다.

```
Router#show ip nat translations
```

- Displays active translations

```
Router#show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.131.1        10.10.10.1        ---                ---
```

```
Router#show ip nat statistics
```

- Displays translation statistics

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Ethernet0, Serial2.7
Inside interfaces:
Ethernet1
Hits: 5 Misses: 0
...
```

show ip nat translation [verbose] - 액티브한 변환을 확인한다.

show ip nat statics - 변환 통계를 확인한다.

clear ip nat translation * - 전 동적 변환을 해제한다.

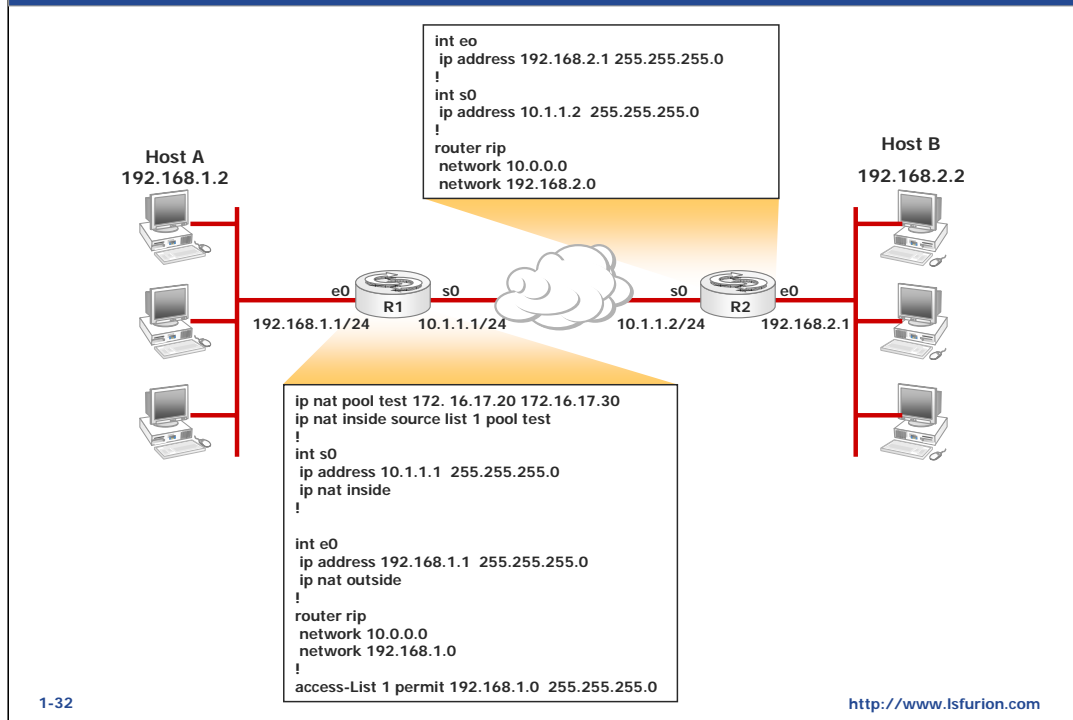
clear ip nat translation <global-ip> - 단순한 동적 변환을 해제한다.

clear ip nat translation <global-ip> <local-ip> <proto> <global-port> <local-port>

- 특정의 동적 변환만을 해제한다.

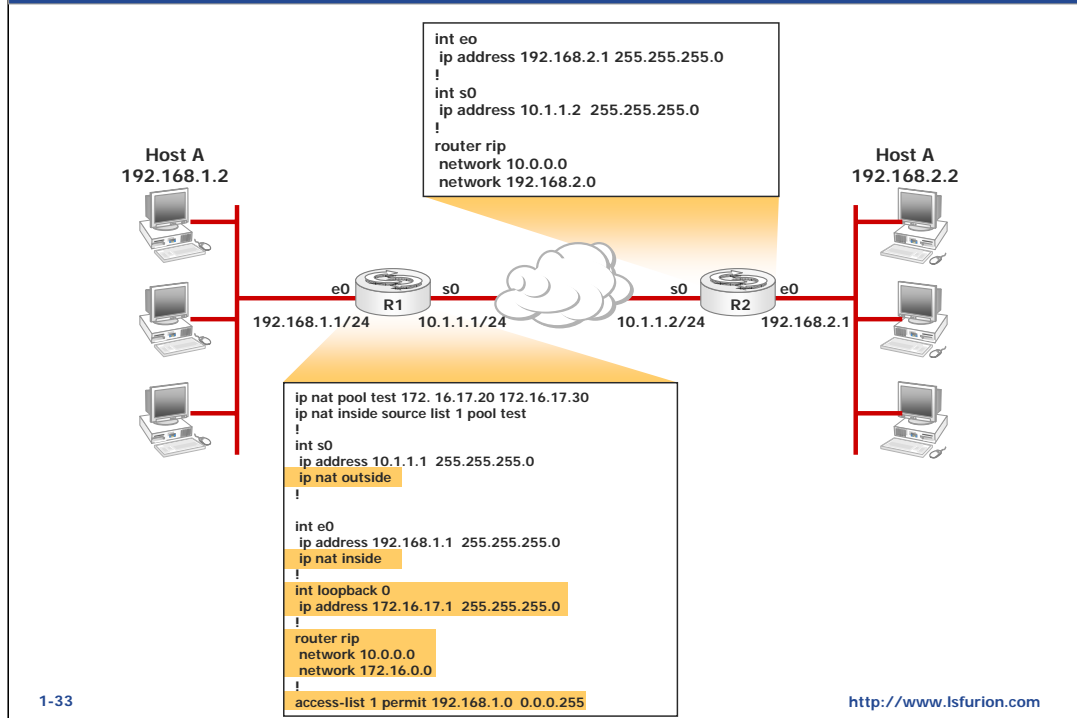
debug ip nat [<list>] [detailed] - 디버그

NAT 환경에서 문제점 해결 예제



위 그림의 R1과 R2의 구성 정보를 보고 어떤 문제점들이 있는 지를 살펴보자.
 위 예제에서 잘못된 설정들을 수정하지 않으면 HostA와 HostB는 상호 IP 통
 신을 할 수 없는 상황이 될 것이다.

NAT 환경에서 문제점 해결 예제(계속)



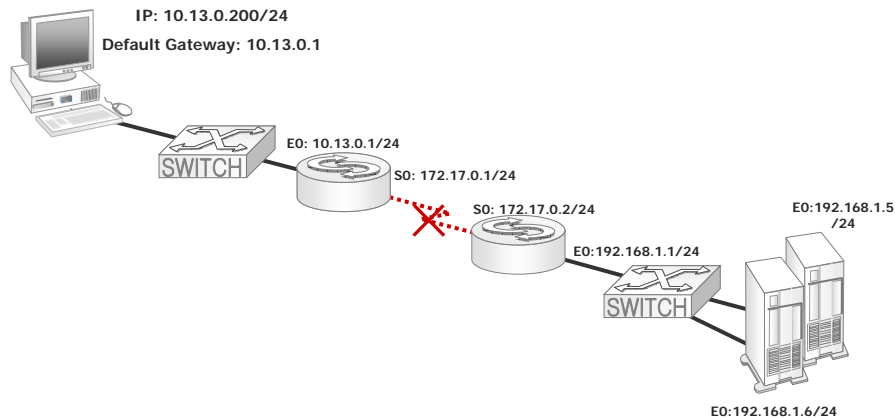
위 그림은 앞 페이지에서 언급한 문제점들을 해결한 결과이다.

특히 R1의 Routing 설정을 이해해야 한다. NAT는 IP 자원을 절약 할 수 있다는 이점 말고도 내부 Network 구조를 감추기 위한 용도로도 사용된다는 것을 잊지 말아야 한다.

Default Gateway Redundancy

이 장에서는 다수의 Default gateway를 소유한 Network에서 다수의 Default gateway에 대한 Redundancy Solution들과 문제점들을 살펴본다.

One Default Gateway = No Fault Tolerance



One Default Gateway = One Default Route → NO Fault Tolerance

1-35

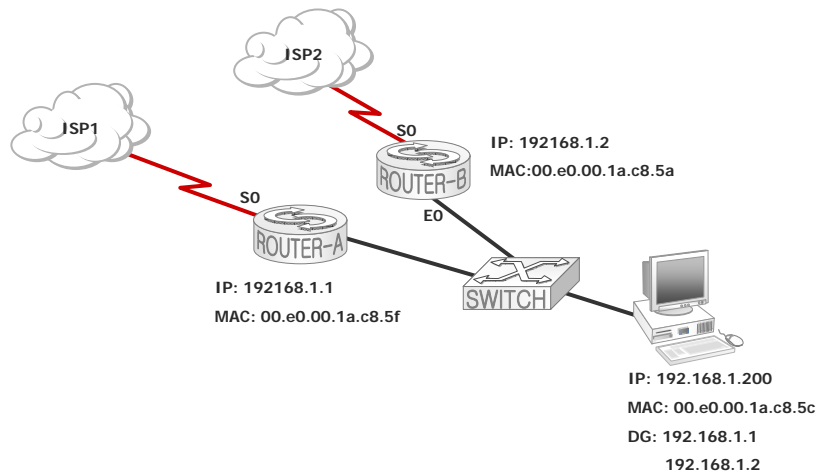
<http://www.lsfurion.com>

단일 Default Gateway를 갖는 환경에서는 Router의 Fail로 인해 모든 Node의 통신이 두절된다.

현재 IPv4를 사용하는 노드들은 자신들이 사용하는 Default Gateway의 존재를 자동으로 인지 하지 않으며, Default Gateway의 Fail을 감지하는 특정한 Process를 취급하지도 않는다. 따라서

또한 위 그림처럼 Router의 Ethernet이 아닌 Serial 구간에 문제가 발생하면, 해당 Link에 연결된 Router를 제외한 나머지 Switch 들이나 일반 노드들은 이 사실을 인지하지 못한다.

솔루션1: Two Default Gateway = Two Default Route ?



1-36

<http://www.lsfurion.com>

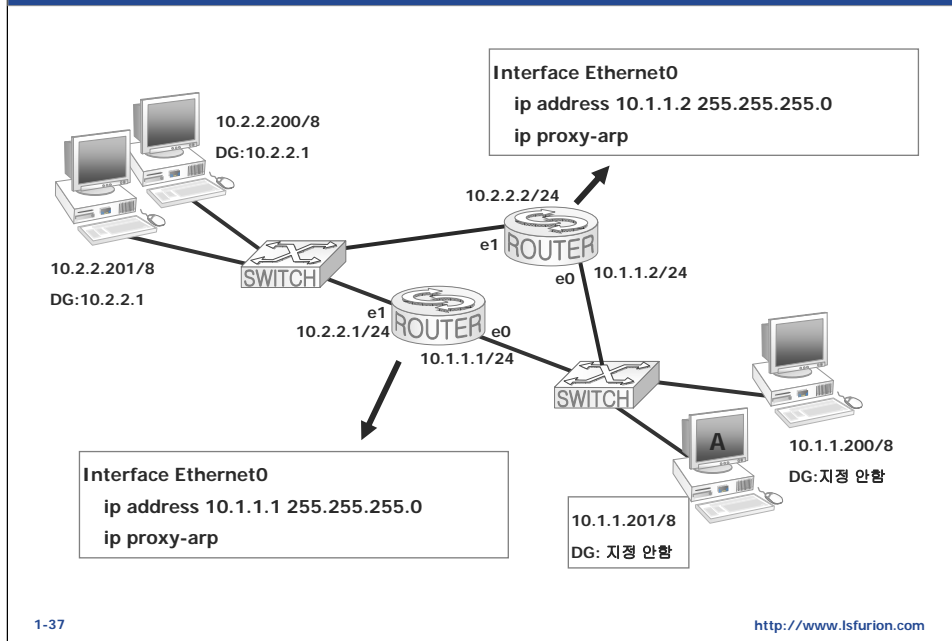
위 그림은 하나의 Subnet에 두 개의 Default Gateway를 설치하고, PC에서도 두 개의 Default Gateway를 설정하고 있다.

현재 IPv4를 사용하는 Node들은 하나 이상의 Default Gateway를 설정해 줄 수는 있지만, 이중에 누가 더 우선되는 Default Gateway인지, 어떤 Default Gateway가 fail되었는지를 설정하는 Option들은 제공하지 않고 있다. 따라서 위 그림의 PC는 자신에게 설정된 두 개의 Default Gateway를 효율적으로 관리 할 수 있는 능력을 전혀 제공하지 않을 것이다.

만약 PC가 Router-A를 Primary로 선택하여 사용하다가 어느 순간에 Router-A가 fail되면 PC는 Router-B를 자동으로 Default Gateway로 설정하여 사용 할 수 있을 것인가?

위 예제와 같은 Network 환경에서는 이 질문에 대해 그 어떠한 뚜렷한 동작을 기대 할 수 없을 것이다. 설사 PC가 시간이 지남에 따라 Router-B를 이용하여 외부 Network에 Packet을 전달 할 수는 있겠지만, 분명한 건 두 Default Gateway사이의 failover time에 대한 보장이 없다는 것이다.

솔루션2: Proxy ARP



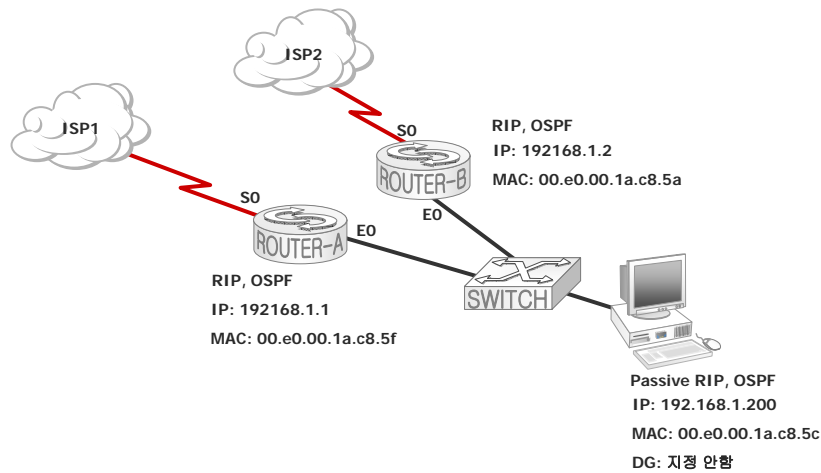
PC들은 자신들이 통신하는 대상 노드가 다른 Subnet상에 존재한다는 것을 인지하면, Default Gateway의 IP 주소를 이용하여 ARP를 수행한다. 따라서 일반적인 상황에서는 반드시 PC의 IP 구성 정보에는 Default Gateway의 IP가 설정되어 있어야 한다.

하지만 Router에 Proxy ARP를 Enable하면, PC들은 별도로 Default Gateway의 IP를 알지 못해도 외부와 통신이 가능하게 된다. 예를 들어 PC A가 10.1.1.201에 대한 ARP Request Broadcast를 전송하면, 이를 Proxy ARP를 지원하는 Router가 듣고, 자신의 Ethernet의 MAC Address를 대신 알려 준다.

위 Network에서는 PC는 먼저 ARP Request에 응답한 Router를 Default Gateway로 사용 할 것이다. 하지만 만약 해당 Router가 죽으면 다른 Router를 바로 사용 할 수 있는 것은 아니다. 이전 Router의 MAC Address정보가 아직 ARP Cache에 남아 있기 때문이다.

위 Solution은 PC들에게 수동으로 다수의 Default Gateway를 설정하지 않아도 된다는 장점은 있지만, failover time의 속도가 너무 늦고, Load Sharing을 적용 할 수 없다는 것이 단점이다.

솔루션3: Dynamic Routing Protocol



1-38

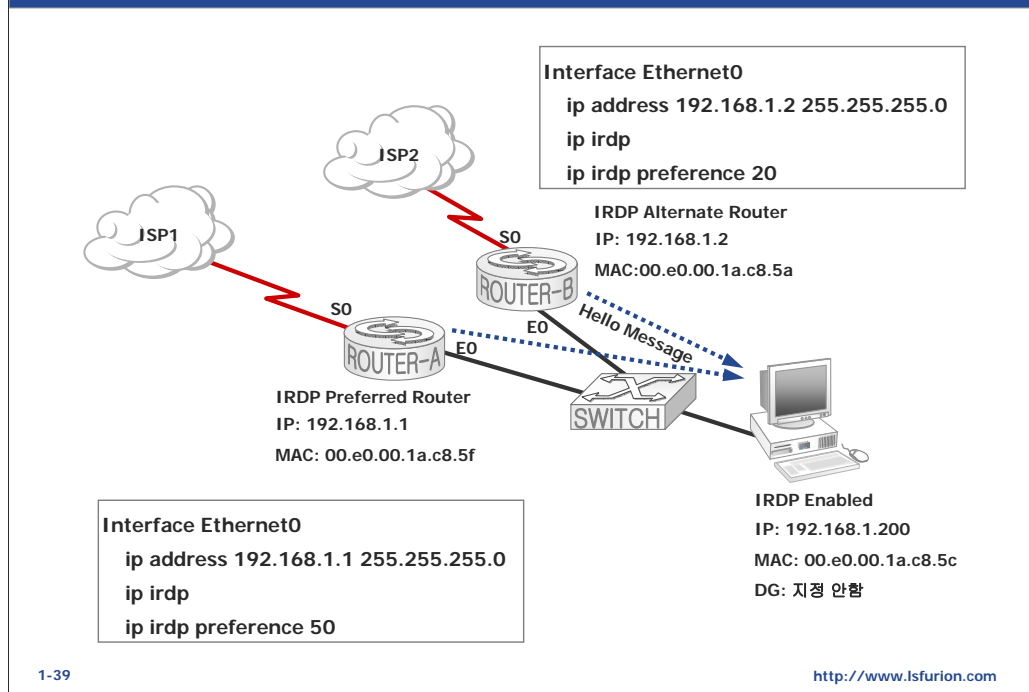
<http://www.lsfurion.com>

다수의 Default gateway를 가진 Network상에 모든 PC들이 Dynamic Routing Protocol을 이용하여 서로 다른 망과 연결될 수 있다.

이론적으로는 PC들이 Routing Protocol을 수행하여 Network상의 변화를 감지할 수 있는 능력을 가지게 된다면, Routing Protocol이 제공하는 Convergence Time 수준으로 failover time이 결정될 것이며, Metric이 동일한 경로에 대해 Load Sharing도 구사하게 될 것이다.

하지만 모든 PC들이 Routing Table을 관리해야 한다는 부담감과 PC들이 Routing Protocol을 수행하기 위해 높은 수준의 운영체제를 사용해야 한다는 단점도 있다. 다량의 PC들이 Network 상에 존재할 경우 Routing Protocol에게 영향을 줄 수 있다.

솔루션4: IRDP(ICMP Router Discovery Protocol)



IRDP는 IPv4 Node들이 Default Gateway(Router)를 검색 할 수 있도록 하는 기능을 제공하기 위해 ICMP에 확장된 기능을 추가한 Protocol이다.

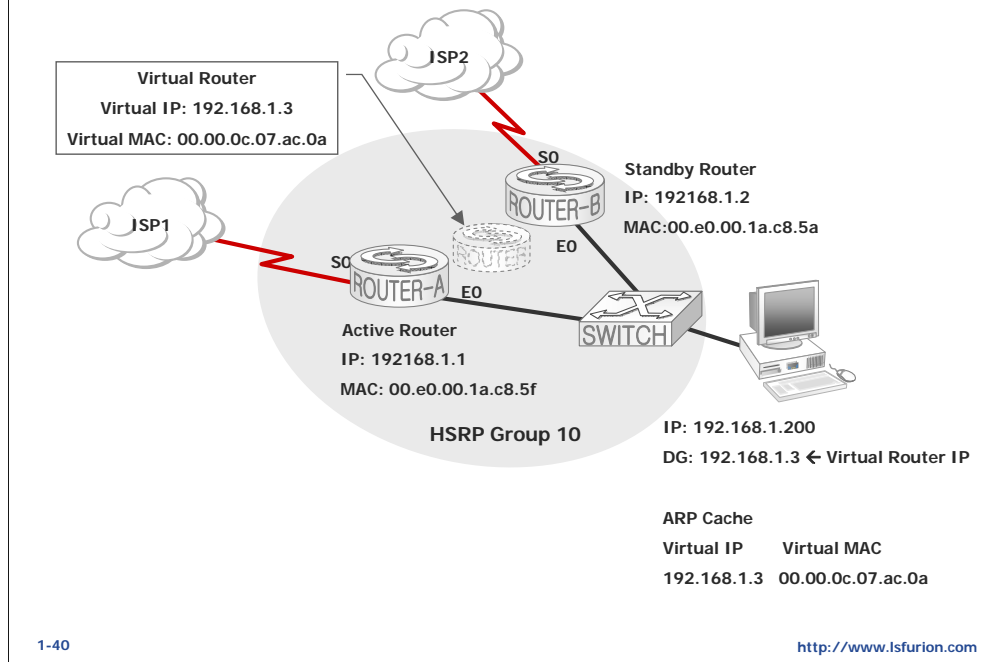
IRDP를 사용하기 위해서는 Router와 PC 모두가 IRDP를 지원해야 하며, 특히 Windows 운영체제를 사용하는 PC같은 경우에는 레지스트리 정보를 수정해야 IRDP 사용이 가능할 것이다.

IRDP가 Router의 특정 Interface에 enable되면, Router는 해당 Interface에서 주기적인 Hello packet을 전송한다. 그러면 IRDP Client들은 이 Hello Packet을 전송하는 Router들의 존재를 인지하고, 이 중에 먼저 Hello Packet을 수신한 Router를 Default Gateway로 선택하게 된다. 하지만 Router관리자는 IRDP를 수행하는 Router들의 우선순위를 결정하여 IRDP Client들에게 어떤 Router를 먼저 선택해야 하는지를 알려 줄 수 있다.

IRDP환경에서는 주기적인 Hello Packet을 전송하여 Router의 상태 정보를 확인하며, 만약 먼저 선택된 Router가 fail되어, 일정 시간 Hello Packet이 수신되지 않으면, 그 다음 Router를 선택하여 사용한다.

Failover time은 IRDP Router와 IRDP Client사이에 Hello Packet을 교환하는 주기에 따라 다르며, 효과적인 Load Sharing을 적용 할 수 없다.

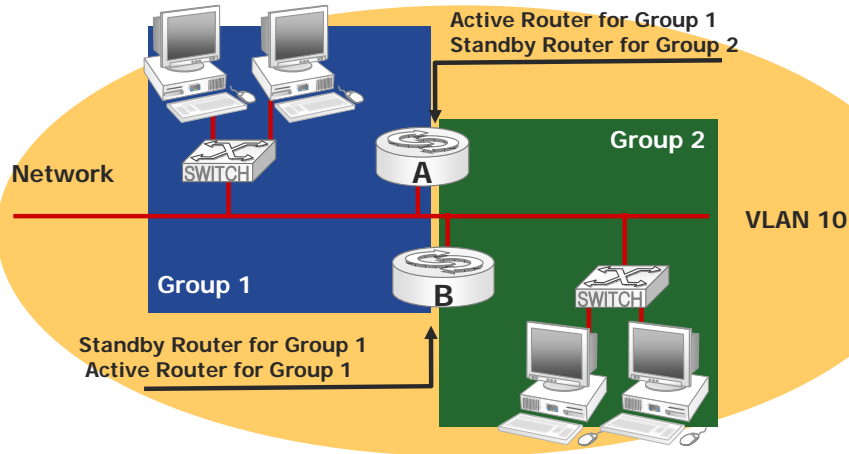
솔루션5: Cisco HSRP(Hot Standby Router Protocol)



HSRP는 다수의 물리적인 Router들을 하나의 논리적인 Router로 구성 하는 방식으로, 실제 PC 사용자들은 물리적인 Router들의 존재 여부에 상관없이 오직 논리적인 Router의 IP를 Default Gateway로 인지하여 사용하면 된다.

HSRP는 논리적인 Router의 존재를 Client들에게 알리기 위해 가상의 IP와 가상의 MAC Address를 제공한다. 또한 논리적인 Router는 실제 물리적인 Router들의 성능이 허락하는 만큼 다수의 논리적인 Router들을 만들 수 있으며, 이들 논리적인 Router들이 지원하는 Network 영역들을 HSRP Group 이란 개념으로 식별하고, 관리한다.

Multiple HSRP Groups



- Routers can belong to multiple groups on the same subnet in a VLAN.

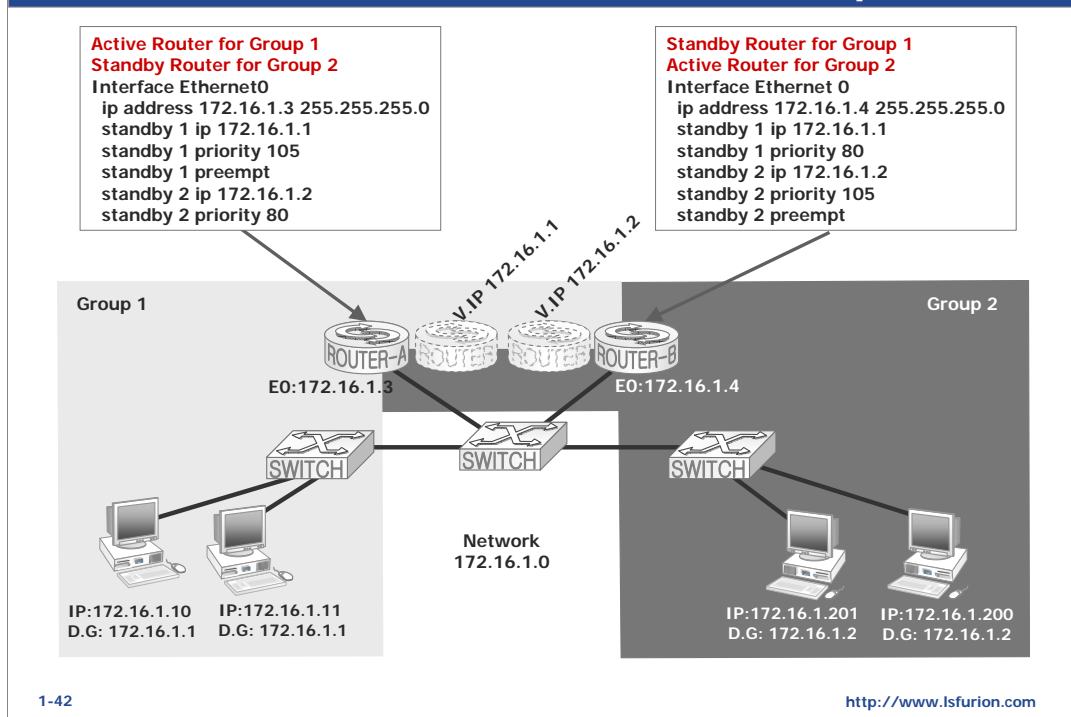
1-41

<http://www.lsfurion.com>

HSRP에서 생성된 하나의 논리 Router는 특정 Subnet을 위한 Default Router가 될 것이다. 이렇게 논리 Router 하나가 지원하는 대상 Subnet영역을 HSRP Group이라 하며, 이러한 HSRP Group은 경우에 따라서 다수가 존재 할 수 있다.

또한 하나의 Subnet에 하나 이상의 논리 Router가 배정될 수도 있다. 즉 다수의 가상 Router와 그에 따른 가상 IP, 가상의 MAC Address가 존재 할 수 있다는 것이다.

HSRP Group 구성 예제



위 그림은 하나의 Subnet에 연결된 노드들을 위해 두 개의 논리 Router, 즉 두 개의 Virtual Router (HSRP Group)를 설정한 구성 예제이다.

다음은 Router-A와 Router-B 에서 Group1을 위한 논리 Router의 설정이다.

Router-A

interface Ethernet0

ip address 172.16.1.3 255.255.255.0

standby 1 ip 172.16.1.1

standby 1 priority 105

standby 1 preempt

- Group1의 가상 Router가 사용하는 가상의 IP를 172.16.1.1로 설정했다.

- Router-A를 Group1의 Active Router로 설정하기 위해 priority값을 '105'로 설정했다.

- Router-A가 fail되었다가 복구되면, 원래의 Active Router역할을 수행하기 위해 'Preempt' option을 설정하였다.

Router-B

interface Ethernet0

ip address 172.16.1.4 255.255.255.0

standby 1 ip 172.16.1.1

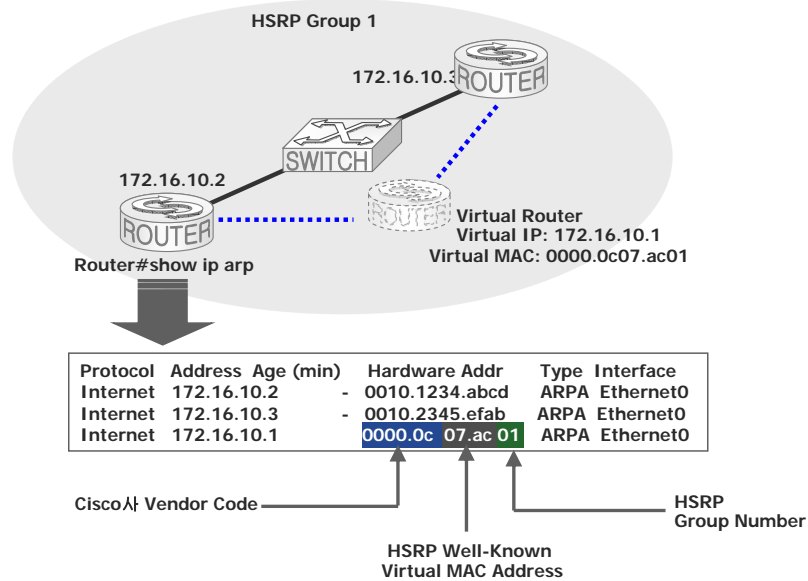
standby 1 priority 80

- Group1의 가상 Router가 사용하는 가상의 IP를 172.16.1.1로 설정했다.

- Router-A를 Group1의 Standby Router로 설정하기 위해 priority값을 '80'으로 설정했다.

위 구성과 마찬가지로 나머지 Group2도 Router-B를 Active로 하고, Router-A를 Standby Router로 설정하고 있다. 이처럼 HSRP는 다수의 Group을 통해 Fault-Tolerance와 Load Sharing이라는 Solution을 제공한다.

HSRP Virtual MAC Address



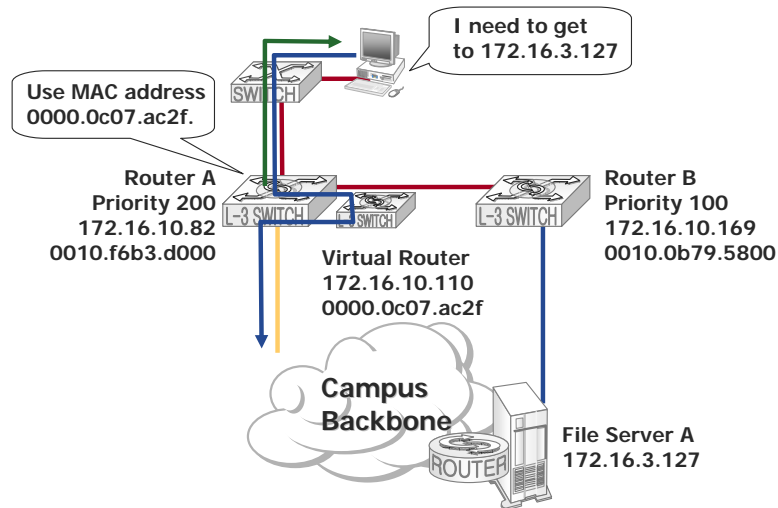
1-43

<http://www.lsfurion.com>

위 그림은 HSRP에서 설정한 가상의 IP를 위해 배정된 가상의 MAC Address를 확인 하는 예제이다.

HSRP가 적용된 Network에서 'show ip arp'command를 이용하면 위 그림에서 보여주는 MAC Address를 확인 할 수 있을 것이다.

Active Router의 역할



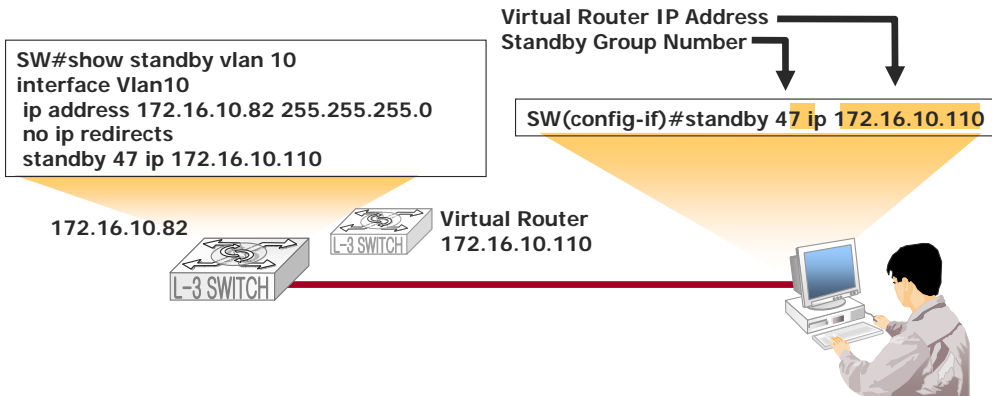
1-44

<http://www.lsfurion.com>

Priority값에 의해 각 HSRP Group을 위한 Active Router가 선출되면, 해당 Router는 Client들의 ARP Request에 대한 응답이나, Remote Traffic들을 처리하게 된다.

Active Router는 Standby Router와 주기적인 Hello Packet을 교환하면서, 서로의 상태 정보를 확인하며, Standby Router는 일정 시간(Hold Time) 동안 Active Router에게서 Hello Packet을 수신하지 못하면, 자신이 Active Router의 역할을 수행하게 된다.

HSRP Standby Interface 설정하기



- HSRP가 특정 Interface상에서 Enable되면 자동적으로 ICMP redirects 가능은 해제될 것이다.

1-45

<http://www.lsfurion.com>

위 그림은 HSRP Service를 수행해야 하는 Router의 Interface에서 HSRP Group Number와 Priority 값을 설정하는 예제이다.

HSRP Standby Priority 설정하기

```
Switch#show standby vlan 10
interface Vlan10
ip address 172.16.10.82 255.255.255.0
no ip redirects

standby 47 priority 150
standby 47 ip 172.16.10.110
```

Assigned Priority
Standby Group Number


```
Switch(config-if)#standby 47 priority 150
```

172.16.10.82

L-3 SWITCH

Virtual Router
172.16.10.110

L-3 SWITCH



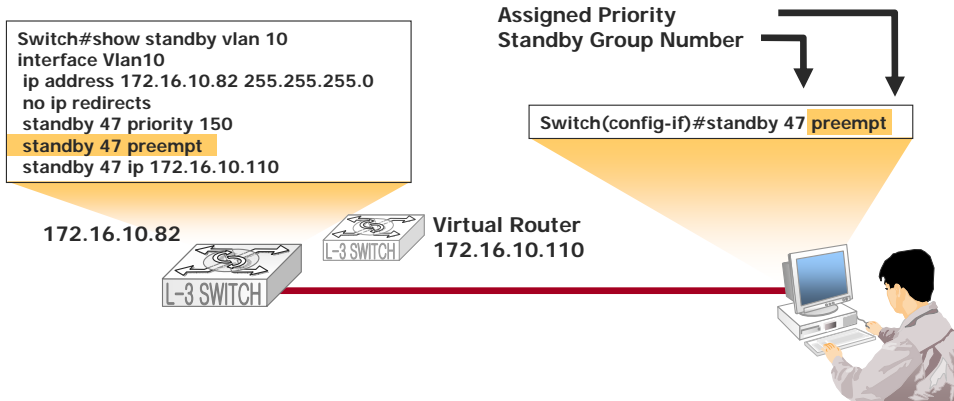
- HSRP group에서 priority가 높은 Router가 Active Router 역할을 수행한다.
- Default priority값은 '100'이다.

1-46

<http://www.lsfurion.com>

46

HSRP Standby Preempt 설정하기



- **Preempt**는 **Active Router**의 복원 후에 자신의 원래 역할을 수행하게 한다.

1-47

<http://www.lsfurion.com>

Active Router가 Fail되어 동작을 멈춘 상태에서는 그만큼 Standby Router에게 부담스런 시간이 될 것이다. 따라서 **Preempt** 설정은 Active Router의 복원 되면, Standby Router에게 전이되었던 Traffic처리 업무를 되찾아야 한다.

기본적으로 **Preempt**는 Active Router에서 필요한 Option이다. **Preempt**는 원칙적으로 Priority값이 높은 Router를 즉시 Active Router로 동작시키겠다는 의미이다. 따라서 평소 Standby 역할을 수행하는 Router가 경우에 따라서 자신의 Priority값이 다른 Router들보다 높게 되어 Active Router가 되어야 한다면, Standby Router의 Interface에서도 **Preempt**를 enable할 필요가 있다.

Hello Message Timer 설정

Building configuration...

Current configuration:
(text deleted)

!

```
interface Vlan10
ip address 172.16.10.82 255.255.255.0
no ip redirects
standby 47 timers 5 15
standby 47 ip 172.16.10.10
```

172.16.10.82



Virtual Router
172.16.10.110

holdtime
hellotime

Switch(config-if)#standby 47 timers 5 15



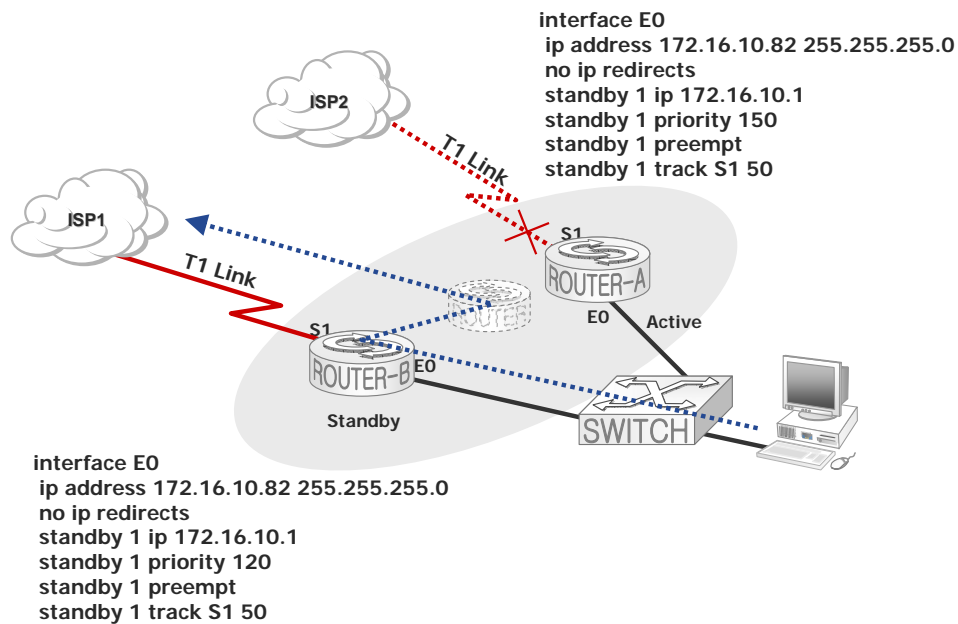
- Holdtime은 적어도 Hello Time의 3배 정도를 설정하는 것이 좋다.

1-48

<http://www.lsfurion.com>

Active와 Standby Router 사이에서 서로의 동작을 확인하기 위해 주기적으로 교환하는 Hello Message의 주기 시간을 위 그림과 같이 조정 할 수 있다.

HSRP 인터페이스 추적(Tracking)



1-49

<http://www.lsfurion.com>

HSRP는 Default Gateway의 Full Redundancy 설정 말고도, WAN Link구간의 Fail을 감지 할 수 있는 Option을 제공한다. 물론 HSRP를 수행하고 있는 Router들에 직접 연결되어 있는 구간만 감지 할 수 있으며, 그 외에 Remote 경로의 감지는 지원하지 않는다

Router-A의 Interface Tracking을 살펴보자.

```
interface E0
ip address 172.16.10.82 255.255.255.0
no ip redirects
standby 1 ip 172.16.10.1
standby 1 priority 150
standby 1 preempt
standby 1 track S1 50
```

→ Router-A의 Serial1 Interface가 fail되면, 기존 Priority값 '150'에서 '50'을 감하여, Priority값을 '100'으로 재조정하겠다는 의미를 가진다.
따라서 Router-A에서 Serial1 Interface가 down되면, 기존 Group1의 Priority값이 '100'이 되므로, Router-B의 Group1이 Active된다.

Standby Brief Status

```
Switch#show standby brief
```

P indicates configured to preempt.

Interface	Grp	Prio	P	State	Active addr	Standby addr	Group addr
Vl11	11	110		Active	local	172.16.11.114	172.16.11.115

```
Switch#debug standby
```

```
*Mar 1 00:22:30.443: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:22:32.019: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:22:33.331: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:22:34.927: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:22:36.231: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:22:37.823: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:22:39.163: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:22:40.735: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:22:42.119: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:22:43.663: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:22:45.067: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:22:46.567: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
```

1-50

<http://www.lsfurion.com>

‘show standby brief’ command는 어떤 Router가 Active 또는 Standby Router인지를 알려 준다.

‘debug standby’ command는 Active Router와 Standby Router사이에서 교환되는 Hello Message의 상황을 확인 할 수 있다.

NTP(Network Time Protocol)

이 장에서는 IOS에서 NTP Service관련 설정을 어떻게 구성해야 하는지를 소개한다.

◆ NTP(Network Time Protocol)

- 네트워크 장비들의 시간을 동기화시키기 위해서 Time Server와 장비들간에 통신하는 프로토콜
- IP Network에서는 UDP Port#123 으로 통신

◆ Clock

- H/W Clock-System Clock, Calendar Command
- S/W Clock- Clock Command

◆ 관련 프로토콜

- Daytime Protocol
- Time Protocol (NTP, SNTP, VINES Time Service, Manual)
- ICMP timestamp

◆ 관련된 서비스

- Digital Time Service

◆ NTP Version

- Version 1: RFC 958
- Version 3: RFC 1305
- SNTP (Simple Network Time Protocol): NTP Version 3이 적용된 NTP Subnet-No Authentication, No statistics mechanism
- SNTP Version 4: IPv6 Header와 OSI Addressing 포함

1-52

<http://www.lsfurion.com>

NTP는 네트워크에 연결된 여러 컴퓨터의 시간을 서로 동기화하여, 시간이 서로 달라서 생기는 혼란을 최소화하려고 고안된 프로토콜이다.

네트워크에 연결되어 있는 시스템에서 "시간"은 중요한 요소이다. 만약 네트워크에 연결된 시스템들의 설정 시간이 서로 다르면, 시스템들 사이에서 특정한 주기를 두고 통신해야 하는 서비스들의 통신 상태가 일관성 없이 진행되므로 예기치 않은 문제들이 발생하게 된다. NTP는 이러한 문제들을 해결하기 위해 Time Server를 별도로 정의하고, 이 Time Server에서 받아온 시간을 통하여 지역 시스템의 시간을 관리하기 때문에 여러 시스템의 시간을 동일하게 유지 할 수 있게 되었다.

- 시스템마다 시간의 차이로 인한 문제점
 - 시스템에서 구동하는 여러 애플리케이션, 그 중에서도 네트워크 응용프로그램 들은 더욱 정확한 시간을 필요로 한다.
 - 시스템의 로그 파일을 분석하는데, 시간이 잘못되어 있다면 분석에 어려움이 많게 된다.

- Clock 정보는 H/W 또는 S/W로 설정 될 수 있다.

- NTP말고도 다양한 Time관련 Protocol들이 사용될 수 있다.

Daytime Protocol

Time Protocol (NTP, SNTP, VINES Time Service, Manual)

ICMP timestamp

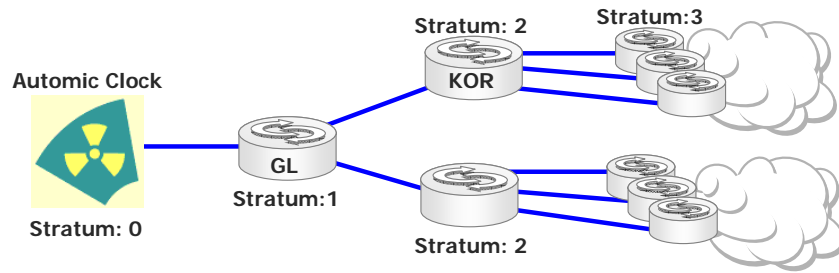
- 다음과 같은 NTP Version들을 제공한다.

Version 1: RFC 958

Version 3: RFC 1305

SNTP (Simple Network Time Protocol): NTP Version 3이 적용된 NTP Subnet-No Authentication, No statistics mechanism

SNTP Version 4: IPv6 Header와 OSI Addressing 포함



- ◆ **Stratum: Authoritative Time Source**로 부터 **NTP Machine**이 얼마나 떨어져 있는(**Hop**)
 - 원자시계: 1 → First Sync.ed NTP1 3 → Second Sync.ed NTP2 6...
- ◆ **Clock offset**: 참조시간에 대응하여 클라이언트의 지역시간을 조정할 시간의 양
- ◆ **Round-trip delay**: 시간에 동기화되기 위해서 통신할 때의 **Delay**
- ◆ **Dispersion(분산)**: 참조시간에 대한 지역시간의 최대 에러

1-53

<http://www.lsfurion.com>

Cisco IOS에서 NTP 설정을 위한 기본 용어는 다음과 같다.

- **Stratum**:
Authoritative Time Source로부터 NTP Machine이 얼마나 떨어져 있는(Hop)을 의미.
예)원자시계: 1 → First Sync.ed NTP1 3 → Second Sync.ed NTP2 6...
- **Clock offset**: 참조시간에 대응하여 클라이언트의 지역시간을 조정할 시간의 양
- **Round-trip delay**: 시간에 동기화되기 위해서 통신할 때의 **Delay**
- **Dispersion(분산)**: 참조시간에 대한 지역시간의 최대 에러

NTP는 Network에서 다음과 같은 이점을 제공한다.

- 시간 차이로 인한 링크나 인접관계의 실패를 방지
- **Time-range** 응용: 예)시간대별 대역폭 할당
- 여러 대의 네트워크 장비의 로그나 디버깅 정보의 정확한 시간 표현
- 각종 Network Management System들이 네트워크의 활동 사항을 정확하게 보고할 수 있다.
- 각종 서버들과 클라이언트들의 시간 정보 동기화 가능

IOS에서 Clock 설정하기

```
Router(config)#clock ?  
    summer-time  Configure summer (daylight savings) time  
    timezone      Configure time zone  
Router(config)#clock timezone ?  
    WORD          name of time zone  
Router(config)#clock timezone KOR ?  
    <-23 - 23>    Hours offset from UTC  
Router(config)#clock timezone KOR +9
```

```
Router#clock ?  
    set          Set the time and date  
Router#clock set ?  
    hh:mm:ss     Current Time  
Router#clock set 10:00:00 ?  
    <1-31>        Day of the month  
    MONTH        Month of the year  
Router#clock set 10:00:00 1 ?  
    MONTH        Month of the year  
Router#clock set 10:00:00 1 aug ?  
    <1993-2035>   Year  
Router#clock set 10:00:00 1 aug 2005 ?  
    <cr>  
Router#clock set 10:00:00 1 aug 2005  
Router#show clock  
10:00:11.527 KOR Mon Aug 1 2005
```

1-54

<http://www.lsfurion.com>

위 그림은 IOS Device에서 수동으로 Clock 설정을 보여주는 예제이다.

시간 설정은 Time Zone과 실제 Clock 설정이 필요하다.

Time Zone 설정

```
Router(config)#clock timezone KOR +9
```

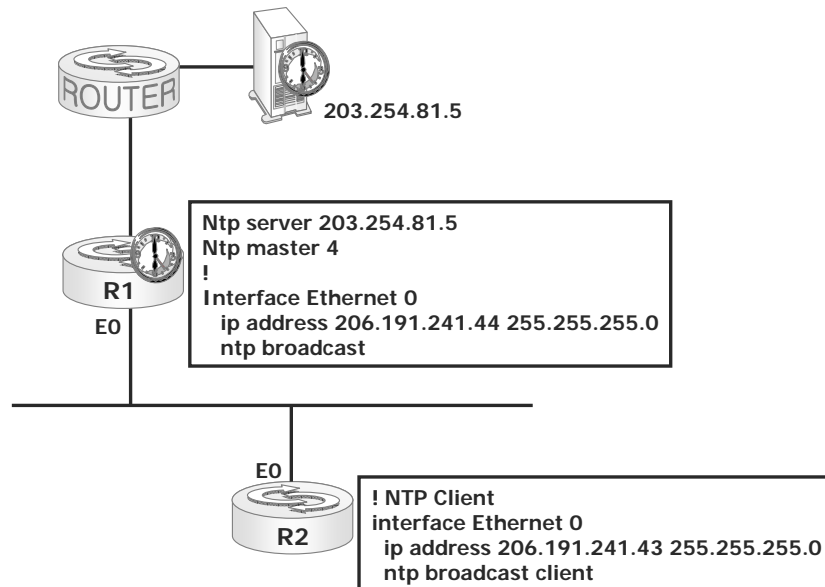
Clock 설정

```
Router#clock set 10:00:00 1 aug 2005
```

```
Router#show clock
```

```
10:00:11.527 KOR Mon Aug 1 2005
```

NTP Broadcast Client Mode



1-55

<http://www.lsfurion.com>

위 그림은 NTP Broadcast Client Mode의 설정 예제이다.

- R1은 다음과 같은 설정으로 NTP Server로 구성되었다.

ntp server 203.254.81.5

→ 시간 정보를 참조하는 상위 Time Server를 설정한다.

ntp master 4

→ R1 자신이 NTP Server임을 설정하고 Stratum level은 4로 설정되었다.

!

interface Ethernet 0

ip address 206.191.241.44 255.255.255.0

ntp broadcast

→ 특정 Interface에서 시간 정보를 전송한다.

- R2는 다음과 같은 방식으로 Time Server를 참조한다.

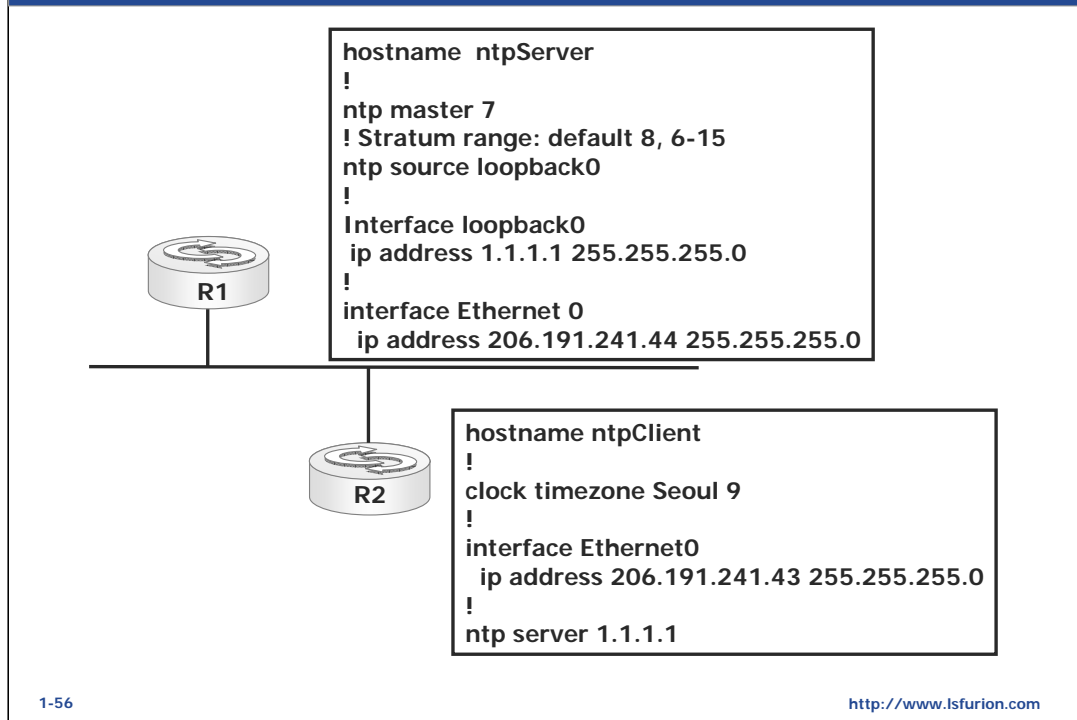
interface Ethernet 0

ip address 206.191.241.43 255.255.255.0

ntp broadcast client

→ 시간 정보를 수신할 Interface에서 NTP Client 기능을 Enable한다.

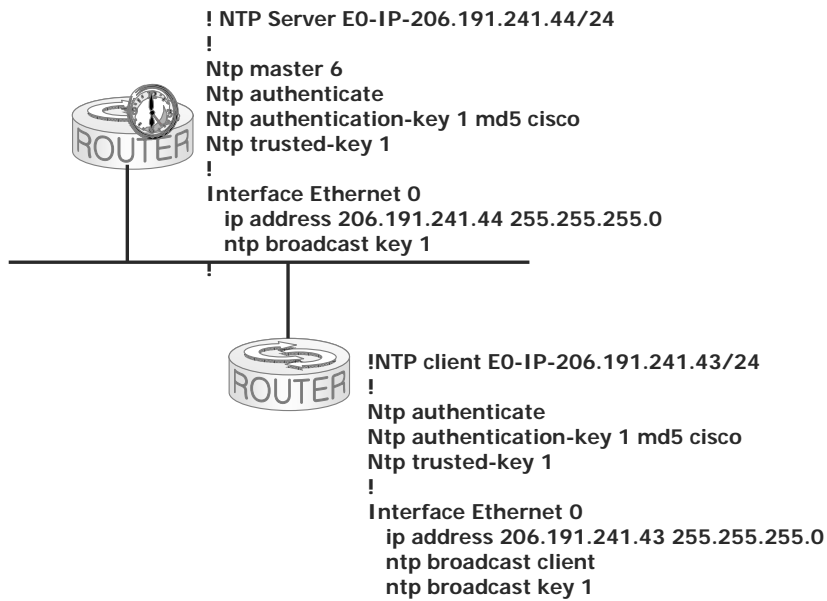
NTP Static Client Mode



위 그림은 NTP Static Client Mode의 구성 예제이다. NTP Client에서 특정 NTP Server의 IP를 정의하고 있다.

R1은 다른 Time Source를 참조하지 않고, 자기 자신을 NTP Master로 설정하였다. R1은 자기 자신이 가진 Clock 정보를 Source로 하여 다른 NTP Client에게 시간 정보를 전송하므로, R1의 시간 정보(Time-Zone, Clock)는 정확해야 한다. 또한 NTP Client에서는 NTP Server가 자신과 같은 Time Zone에 있지 않다면, Time Zone 설정이 필요하다.

NTP Authentication



1-57

<http://www.lsfurion.com>

위 구성은 NTP Authentication 설정 예제이다. NTP는 Open된 Protocol이므로, 인증되지 않은 잘못된 시간 정보에 의한 Network의 혼란을 경험 할 수도 있다. 따라서 Network에 연결된 시스템들은 인증된 시간 서버에서만 시간 정보를 받아올 필요가 있다.

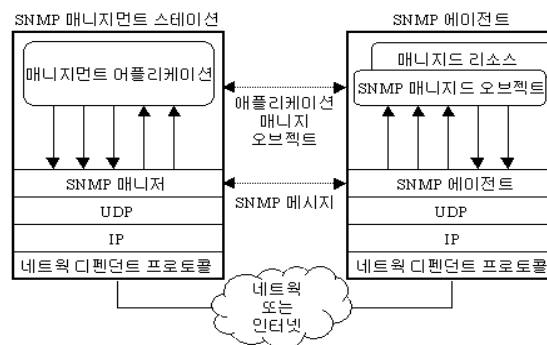
SNMP & RMON

이 장에서는 IOS Device에서 SNMP Agent와 RMON 설정을 소개한다.

◆ 개요 (Simple Network Management Protocol)

- Internet Activities Board 에서 개발한 Network 관리 프로토콜
- 처음에는 TCP/IP 네트워크를 관리 하기위해 설계
- IP 스택에 존재하지만 비 TCP/IP장비를 포함한 어떤 형태의 네트워크 트래픽도 관리 가능하고 모니터링 가능
- 관리 표준 프로토콜로 지정

◆ SNMP 프로토콜 아키텍처



1-59

<http://www.lsfurion.com>

SNMP 정의 (Simple Network Management Protocol)

단순 네트워크 관리 프로토콜(SNMP)은 TCP/IP 네트워크에서 사용되는 네트워크 관리 표준 Protocol이다.

SNMP는 아래와 같이 사용될 수 있다.

- 원격 장치 구성
구성 정보는 관리 시스템에서 네트워크로 연결된 각 호스트로 보내질 수 있다.
- 네트워크 성능 모니터링
처리 속도와 네트워크 처리량을 추적하고 데이터 전송 성공에 대한 정보를 수집할 수 있다.
- 네트워크 결함이나 부적절한 액세스 감지
특정 이벤트가 발생하면 네트워크 장치에서 경고를 호출하도록 구성할 수 있다. 경고가 호출되면 장치는 이벤트 메시지를 관리 시스템으로 전달한다.
- 네트워크 사용 감시
사용자나 그룹 액세스를 식별하기 위한 전체적인 네트워크 사용 및 네트워크 장치와 서비스 사용 유형을 모두 모니터링할 수 있다.

SNMP 관리 시스템과 에이전트 / SNMP를 사용하려면 아래와 같은 두 가지 구성 요소가 필요하다.

SNMP 관리 시스템

관리 콘솔이라고도 하는 관리 시스템은 SNMP 에이전트에 정보와 업데이트 요청을 교환한다. SNMP 관리 시스템은 SNMP 에이전트라는 관리 대상 컴퓨터로부터 사용 가능한 하드 디스크 공간이나 활성 세션 수 등의 정보 등을 요청할 수 있다. 관리 시스템이 에이전트에 대한 쓰기 액세스를 부여 받은 경우 에이전트의 구성을 변경할 수도 있다.

SNMP Agent

관리 대상 장비들에서 동작하는 소프트웨어이며, 드라이버 또는 Firmware형태로 존재한다. Agents는 자신이 동작하는 Device의 관리 요소들에 대한 정보들을 SNMP 관리 시스템에게 알려 주거나 특정한 요청을 받아 들여 작업을 수행한다.

SNMP Manager들과 Agent들

◆ SNMP Manager

- SNMP Agent를 통해 수집한 정보들을 Database에 저장하여 중앙집중적이고 벤더 독립적인 시스템과 네트워크 관리를 수행하는 응용프로그램
- 종류
 - ◆ HP OpenView
 - ◆ IBM NetView, Tivoli
 - ◆ Novell ManageWiser
 - ◆ CA Unicenter TNG
 - ◆ CiscoWorks 2000

◆ SNMP Agent

- MIB(Management Information Base)에서 지정한 특정 정보들을 시스템에서 추출하여 SNMP Manager의 요청에 응답하는 서비스
- 시스템에 문제가 발생하면 능동적으로 Trap Destination에게 메시지를 송신한다.
- SNMP Manager가 지정된 설정 값을 보내면 그 값을 이용하여 자신의 시스템을 변경
- Windows 운영체제인 경우 SNMP Agent, Trap 서비스들이 내장
- Network Device나 Server와 같은 하드웨어 장비에는 Firmware 또는 Driver형태로 내장되어있어 사용자의 설정에 의하여 그 기능을 수행

1-60

<http://www.lsfurion.com>

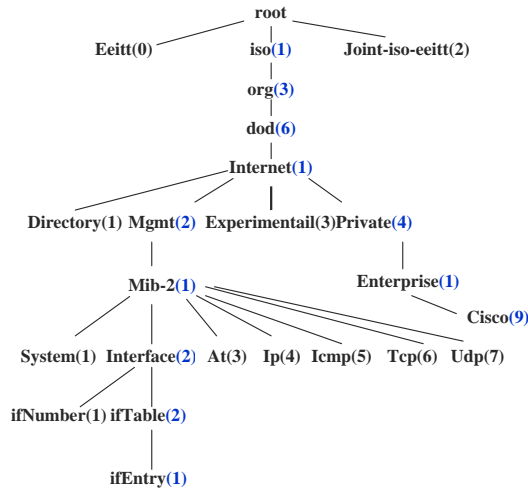
SNMP Manager

SNMP를 이용한 관리용 소프트웨어를 의미한다. 일반적으로 각 벤더마다 자신들의 관리용 소프트웨어를 제공한다.

SNMP Agent

관리 대상 장비들에서 동작하며, SNMP Manager와 관리상에 필요한 모든 Action을 교환한다.

◆ MIB 구조



◆ 기본 관리대상 항목의 OID 값 예제

- ◆ ifInOctects
- ◆ (1.3.6.1.2.1.2.2.1.10)
- ◆ ifOutOctects
- ◆ (1.3.6.1.2.1.2.2.1.16)
- ◆ ifInErrors
- ◆ (1.3.6.1.2.1.2.2.1.14)
- ◆ ifOutErrors
- ◆ (1.3.6.1.2.1.2.2.1.20)
- ◆ loclIfInCRC
- ◆ (1.3.6.1.4.1.9.2.2.1.1.12)

1-61

<http://www.lsfurion.com>

- MIB (Management Information Base)

MIB 이란 TCP/IP를 기초로 하는 관리 모델에서 각 대상 장비의 관리 되어질 요소들에 대한 정보를 정의하고 있는 데이터 베이스이다.

- MIB의 구조

- 관리되어지고 있는 각 정보들을 객체, 즉 오브젝트라고 함
- 각각의 객체는 객체 식별자(OID: Object Identifier)로 구분
- 정의된 오브젝트의 집합은 트리 구조를 가짐
- 각 오브젝트들은 정수의 연속된 나열로 표시 (예: .1.3.1.2.1.2.2.1.10)

- MIB 버전별 기능

- MIB-1 : 네트워크 관리에 필요한 최소한의 관리 정보를 정의(object 114 개)
- MIB-2 : MIB-1의 확장판으로 현재 대부분의 제품이 MIB-2를 지원 (MIB-1 object 포함하여 object 171 개)
- 확장 MIB : 표준 MIB에 규정되어 있지 않은 각 장비 제조사의 독자적 기능을 상세히 관리하기 위한 항목들을 정의

SNMP에서 관리 정보로 활용하는 MIB 정보의 예)

ifInOctets : 인터페이스에 수신된 바이트의 총수

ifOutOctets : 인터페이스에서 송신되는 바이트의 총수

IpSpeed : bps 단위로 인터페이스의 현재 대역폭

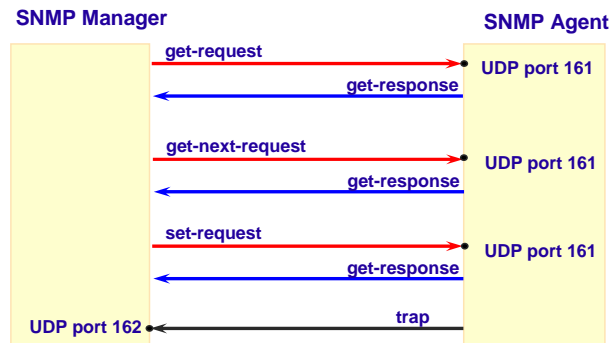
sysUpTime : 시스템의 네트워크 관리대상이 마지막으로 재초기화된 이후의 시간

ifType : 물리/데이터 링크 계층 프로토콜에 따라 구별되는 인터페이스의 유형

기타 등등....

◆ SNMP 동작 (Process)

- UDP port 번호 161번을 이용한 정보 교류
- 3가지 연산(Get, Set, Trap)을 통한 7가지 형태의 메시지로 정보 교류 수행
any version : get-request, get-next-request, set-request, get-response, trap
version 2 : get-bulk, get-info-req
- Manager와 agent의 동작도



1-62

<http://www.lsfurion.com>

위의 각 PDU들의 기능은 다음과 같다.

GetRequest : SNMP manager가 값을 얻고자 하는 변수들을 SNMP agent에게 알린다.

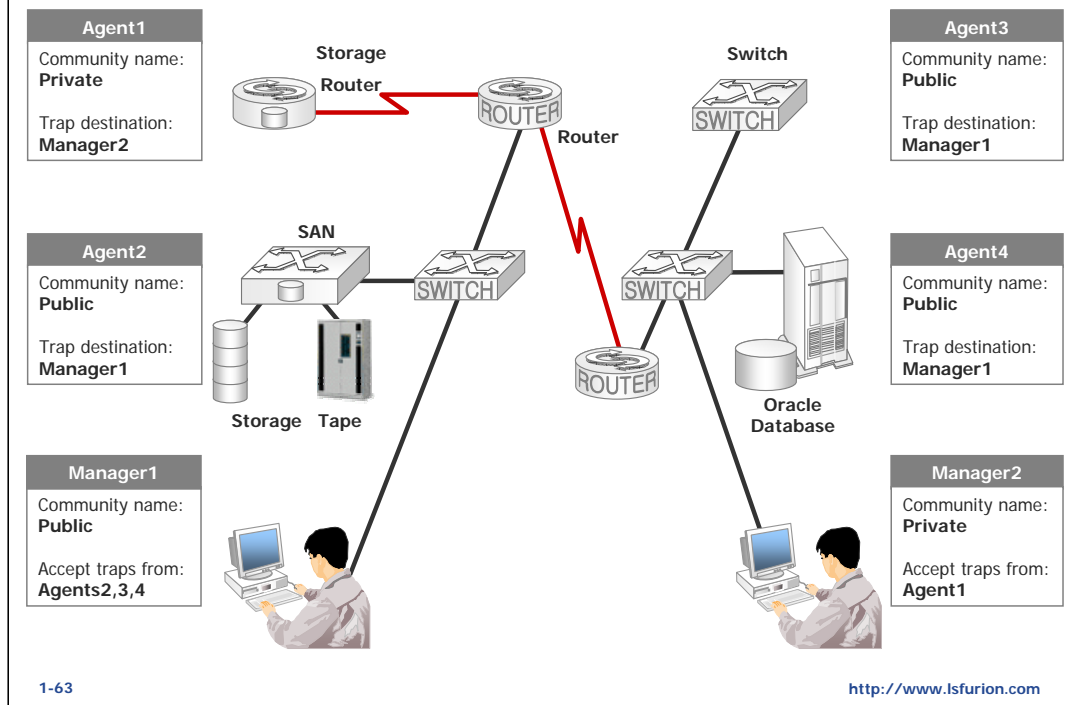
GetNextRequest : SNMP manager가 연속해서 값을 얻고자 하는 변수들을 SNMP agent에게 알린다.

SetRequest : SNMP manager가 변수들에 대해 지정하고자 하는 값을 SNMP agent에게 알린다.

GetResponse : GetRequest, GetNextRequest, SetRequest 등에 대한 응답을 보낸다.

기본적으로 GET, GET NEXT를 통한 데이터요청은 일정한 polling시간을 가지고 manager에서 agent로 필요한 정보를 요청하는 방식이다. 그러나 이것을 이용해서는 비동기적으로 발생하는 정보를 수집할 수는 없다. 이러한 비동기적인 정보는 여러 형태가 있는데, 예를 들어 특정 네트워크 세그먼트에 문제가 생겼다거나 디스크나 메모리용량을 과다하게 사용하고 있다거나 하는 사건들은 비동기적으로 발생할 것이다. 이런 경우에는 agent에서 manager측으로 사건을 통보해야 하는데 이렇게 agent에서 manager측으로 비동기적으로 사건을 통보하는 것을 SNMP TRAP라고 한다.(간단히 말해서 경고메시지를 전송한다.)

SNMP Community의 정의



커뮤니티 정의

에이전트와 관리 시스템의 제한된 보안 검사나 관리상의 목적으로 호스트 그룹을 단순 네트워크 관리 프로토콜(SNMP) 커뮤니티에 지정할 수 있다. 커뮤니티는 사용자가 지정하는 커뮤니티 이름으로 식별되며, 호스트는 동시에 여러 커뮤니티에 속할 수 있지만 에이전트는 허용되는 커뮤니티 이름 목록에 없는 관리 시스템으로부터의 요청을 받아들이지 않는다.

SNMP 설정 시 Community와 함께 권한을 설정하게 되는데 일반적으로 다음과 같은 권한의 종류가 있다.

RO(Read Only)

SNMP Manager가 SNMP Agent를 통해 관리용 정보를 수집할 수는 있지만, SNMP Agent를 통해 대상 시스템의 구성 정보를 설정할 수는 없다.

RW(Read Write)

SNMP Manager가 SNMP Agent를 통해 관리용 정보를 수집하고, SNMP Agent를 통해 대상 시스템의 구성 정보를 설정할 수 있다.

◆ 개요

- 분산 LAN 환경에 위치한 원격 모니터링 장비의 네트워크 데이터를 수집, 저장 방법을 규정한 표준
- 기존 SNMP 대비 랜 환경에서의 통신량의 특성이나 사용량 측정에 초점
- 새로운 관리 대상 객체(관리항목)들을 정의하기 위해서 추가된 MIB을 가짐
- 관리자와의 통신은 SNMP 전송 메커니즘과 커맨드를 이용

◆ 목적(용도)

- Off-line 동작
 - ◆ 통신 두절 등의 원인으로 Manager와의 지속적인 연결이 이루어지지 않을 경우에도 Agent가 통계 데이터를 수집
- 사전동작 감시
 - ◆ 특정 에러 상태와 트래픽 과잉 등의 문제 발생의 기록과 관리
- 문제 검출 및 보고
 - ◆ Agent가 어떤 상태값의 설정 임계치를 넘을 경우 Manager에게 여러 가지 방법으로 통보
- Value-added 데이터
 - ◆ 해당네트워크에서 수집한 정보를 이용하여 부가가치 있는 정보로 가공(예: Top-N 트래픽 유발 호스트 알림)
- 다중관리자
 - ◆ 동시에 용도가 틀린 두개 이상의 Manager에게 정보 제공 가능

1-64

<http://www.lsfurion.com>

RMON은 중앙 사이트로부터 T-1/E-1과 T-2/E-3 회선들이 서로 연결되어 있는 분산 근거리 통신망 그룹을 감시, 분석 및 고장 처리하는데 사용될 수 있는 표준 정보를 네트워크 관리자에게 제공한다. 명확히 말하면 RMON은, 어떠한 네트워크 감시 시스템이라도 제공할 수 있을 정보를 명백히 보여준다. 이것은 SNMP의 확장판으로서 RFC 1757에 정의된 MIB의 일부로 정의되어 있다. 최신판은 때로 "RMON 2"라고도 불리는 RMON Version 2이다.

RMON은 프로브라고 불리는 하드웨어 감시 장치나, 소프트웨어 또는 그 조합에 의해 지원된다. 예를 들면, 시스코의 LAN 스위치 계열에는 각 스위치가 MIB 내를 통과하는 트래픽 정보를 잡고, 기록할 수 있는 소프트웨어가 포함된다. 소프트웨어 에이전트는 네트워크 관리자에게 GUI 형태로 보여주기 위해 정보를 모을 수 있다. 많은 공급회사들이 RMON을 지원하는 다양한 종류의 제품을 제공한다.

RMON은 보내진 패킷의 수, 바이트 수, 없어진 패킷의 수, 호스트별 통계, 주고받은 주소지별 통계, 다양한 종류의 이벤트 발생 내역 등 9가지 종류의 정보를 수집한다. 네트워크 관리자는 네트워크 상에서 각 사용자들이 부과하는 대역폭이나 트래픽 양이 얼마나 되는지, 어떤 웹 사이트들이 액세스되고 있는지 등을 알아낼 수 있다. 절박한 문제점들을 알리기 위하여 경고 신호가 보내질 수 있다.

표준 SNMP에서는 전송 구조와 명령을 이용하여 분산된 랜(LAN) 환경에서 원격 모니터링 장비가 어떻게 통신망 데이터를 수집하여 저장할 것인지를 규정했다. 하지만 기존의 기능은 각 통신장비의 연결에만 초점을 두고 있었기 때문에 랜 환경에서의 통신량의 특성이나 사용량과 같은 필요한 정보를 얻을 수 없었다. 그러나 RMON은 LAN Protocol 분석기의 개념을 확대 발전시켜, 각 통신장비에 원격 모니터링 기능을 설치하여 해당 통신장비의 정보를 수집한 후 관리하는 곳으로 전달한다.

RMON은 분산 랜 환경의 상태를 감시하는 장비의 기본 기능과 호환될 수 있는 표준을 가지도록 개발되었으며, 이더넷과 토큰링의 OSI 7계층모델 중 1, 2 계층에 대한 원격지 감시 기능도 제공한다. 그러나 수집한 정보에 대한 표현 방법은 규정하지 않고 있다. 앞으로 FDDI와 WAN 네트워크에로의 확장성을 고려하여 설계되었다

SNMP 기본 설정

Command	Purpose
Router(config)# snmp-server community string [view view-name] [ro rw] [number]	Defines the community access string.
Router(config)# snmp-server host host-id [traps informs][version {1 2c 3} [auth noauth priv]] community-string [udp-port port-number] [notification-type]	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.
Router(config)# snmp-server system-shutdown	Enables system shutdown using the SNMP message reload feature
Router(config)# snmp-server enable traps [notification-type [notification-options]]	Enables sending of traps or informs, and specifies the type of notifications to be sent. If a <i>notification-type</i> is not specified, all supported notification will be enabled on the router. To discover which notifications are available on your router, enter the snmp-server enable traps ? command.
Router> show snmp	Monitors SNMP status.

1-65

<http://www.lsfurion.com>

위 그림은 RMON 설정을 위해 필요한 명령어의 설명이다.

SNMP Agent Sample#1

```
Router(config)#snmp-server community public RW
Router(config)# snmp-server system-shutdown
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server enable traps isdn call-information
Router(config)# snmp-server enable traps config
Router(config)# snmp-server enable traps entity
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server enable traps rtr
Router(config)# snmp-server enable traps frame-relay
Router(config)# snmp-server enable traps syslog
Router(config)# snmp-server enable traps tty
Router(config)# snmp-server host 203.254.82.126 traps public tty
frame-relay isdn x25 config entity envmon bgp syslog sdhc snmp
```

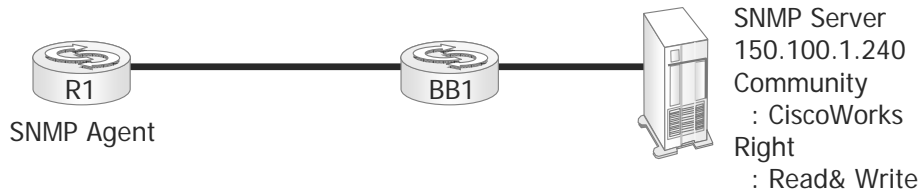
1-66

<http://www.lsfurion.com>

위 그림은 SNMP Agent 설정의 전형적인 예제이다. SNMP 설정을 위한 작업 단계는 다음과 같다.

- 1.SNMP Community와 권한을 설정한다.
snmp-server community public RW
- 2.SNMP Manager가 해당 시스템을 원격에서 재부팅 할 수 있도록 허용한다.
snmp-server system-shutdown
- 3.SNMP Manager에게 전달할 Trap들을 설정한다.
snmp-server enable traps → 모든 Trap을 Enable한다.
snmp-server enable traps bgp → 특정 Trap을 Enable한다.
- 4.SNMP Server와 해당 Server에게 전달할 Trap을 설정한다.
snmp-server host 203.254.82.126 traps public

SNMP Agent Sample#2



```
# configure terminal
config# snmp-server community CiscoWorks RW 20
config#
config# access-list 20 permit 150.100.1.240
config#
config# snmp-server enable traps BGP
config# no snmp-server enable traps tty
config# snmp-server host 150.100.1.240 traps CiscoWorks
BGP
config# snmp-server system-shutdown
config# end
#
```

1-67

<http://www.lsfurion.com>

위 예제는 R1에서 다음과 같은 조건을 기반으로 구성된 것이다.

- SNMP Server는 150.100.1.240 이다. 기본적인 보안의 이유로 오직 그 서버만이 SNMP 동작을 R1에게 요청할 수 있도록 설정한다.
- Community String은 “CiscoWorks”로 모두 Read/Write가 권한을 가지도록 한다.
- R1은 오직 BGP Trap만을 SNMP 서버에 보내도록 한다.
- NMS 관리자가 R1을 Reboot 시킬 수 있도록 하고, Trap을 보낼 때는 Community String을 같이 보낼 수 있도록 한다.

RMON 기본 설정

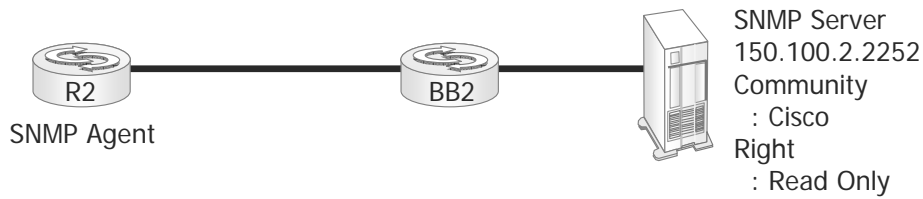
Command	Purpose
Router(config-if)# rmon {native promiscuous}	특정 Interface에서 RMON을 Enable한다.
Router(config)# rmon alarm <i>number variable interval</i> {delta absolute} rising-threshold <i>value</i> [<i>event-number</i>] falling-threshold <i>value</i> [<i>event-number</i>] [<i>owner string</i>]	특정 MIB object에 대한 Alarm 조건을 설정한다.
Router(config)# rmon event <i>number</i> [log] [trap <i>community</i>] [description <i>string</i>] [owner <i>string</i>]	RMON event table에 RMON Alarm 설정을 추가 또는 제거한다.
Router> show rmon	Displays general RMON statistics.
Router> show rmon alarms	Displays the RMON alarm table.

1-68

<http://www.lsfurion.com>

위 구성은 RMON을 설정하기 위한 작업 단계를 보여준다.

RMON 설정 예



R2의 CPU Utilization이 1분 동안 평균 70%이상 , 또는 40%이하인 경우
SNMP Server Trap을 전달하고 싶다.

```
Config t
!
snmp-server community cisco RO
snmp-server host 150.100.2.252 trap cisco
snmp-server enable trap
rmon event 1 log trap cisco description "over 70%" owner config
rmon event 2 log trap cisco description "under 40%" owner config
rmon alarm 1 lsystem.57.0 60 absolute rising-threshold 70 1 falling-threshold 40 2 owner
```

1-69

<http://www.lsfurion.com>

RMON을 이용한 특정 MIB 개체의 모니터링과 알람 설정을 위해 반드시
SNMP의 도움을 받아야 한다.

위 예제는 다음과 같은 조건을 기반으로 설정되었다.

- CPU 사용도(Utilization)가 1분 동안 평균적으로 70%을 넘거나, 40% 아래로 다시 떨어지면 자동적으로 로그와 트랩을 생성할 수 있도록 R2를 구성한다.
- 호스트 150.100.1.240으로 Trap을 보낼 것이며, Community String은 'cisco'로 설정한다.
- OID: 1.2.6.1.4.1.9.2.1.57.0 또는 lsystem.57.0을 사용한다.

Syslog

D1 장에서는 Syslog에 대해 소개한다.

Syslog Service란?

- ◆ 라우터나 스위치에서 발생하는 시스템 에러 메시지나 **Debugging** 정보를 처리하는 서비스
- ◆ Syslog 목적지
 - Console
 - Buffer
 - Terminal Line
 - Syslog Application
- ◆ Cisco사의 Syslog Format
 - BSD Unix 4.3 Syslog와 호환됨

```
config t
!
logging on
!
logging console
logging buffered
[size]
logging monitor
logging host
!
show logging
clear logging
```

1-71

<http://www.lsfurion.com>

라우터나 스위치에서 발생하는 시스템 에러 메시지나 **Debugging** 정보를 처리하는 서비스를 말한다.

Syslog 목적지는 다음과 같다.

- Console
Console Terminal상에 메시지를 표현한다.
- Buffer
Memory상에 메시지를 저장 한다.
- Terminal Line
Telnet Teminal상에 메시지를 표현한다.
- Syslog Application
특정 서버에 메시지들을 전송한다.

Cisco사의 Syslog Format

BSD Unix 4.3 Syslog와 호환됨

Logging 수준의 제한

◆ 메시지 숫자와 수준을 제한

- **Router(config)#logging console *level***
 - ◆ 콘솔로 로그되는 메시지 숫자의 제한
- **Router(config)#logging monitor *level***
 - ◆ 터미널 라인으로 로그되는 메시지의 제한
- **Router(config)#logging trap *level***
 - ◆ Syslog server로 로그되는 메시지 제한

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

1-72

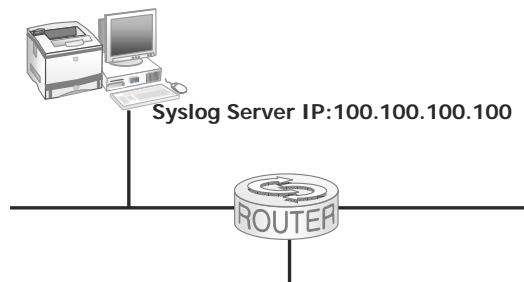
<http://www.lsfurion.com>

Syslog에 의해 표현되는 다양한 이벤트에 따른 메시지들은 그 등급에 따라 표현되는 이벤트와 메시지 형식이 다르게 되어 있다.

위 그림에서 보이는 메시지들의 등급은 상위 등급으로 올라 갈수록 하위 등급의 메시지들도 함께 표현할 수 있다. 예를 들어 메시지 등급이 'errors' 수준 이라면 emergencies, alerts, critical과 같은 등급의 메시지들도 함께 표현한다. 메시지 형식의 수준을 제어하기 위해서는 다음과 같은 명령어를 사용한다.

- **Router(config)#logging console *level***
콘솔로 로그되는 메시지 숫자의 제한
- **Router(config)#logging monitor *level***
터미널 라인으로 로그되는 메시지의 수준 제한
- **Router(config)#logging trap *level***
Syslog server로 로그되는 메시지 수준 제한

Syslog Server를 이용한 Logging 서비스 설정



```
Router(config)#logging on
Router(config)#logging host 100.100.100.100
Router(config)#logging source-interface loopback 0
Router(config)#logging trap ?
<0-7>      Logging severity level
alerts      Immediate action needed      (severity=1)
critical    Critical conditions           (severity=2)
debugging   Debugging messages           (severity=7)
emergencies System is unusable           (severity=0)
errors      Error conditions             (severity=3)
informational Informational messages       (severity=6)
notifications Normal but significant conditions (severity=5)
warnings    Warning conditions           (severity=4)
```

1-73

<http://www.lsfurion.com>

위 구성은 Syslog Server에 Logging 서비스를 수행하기 위한 구성의 예제이다.

Router(config)#logging on

→ Logging Service를 Enable한다.

Router(config)#logging host 100.100.100.100

→ Syslog Server의 IP를 기술했다.

Router(config)#logging source-interface loopback 0

→ Syslog Server에 Logging 메시지를 전달 할때 사용할 source IP 주소.

Router(config)#logging trap ?

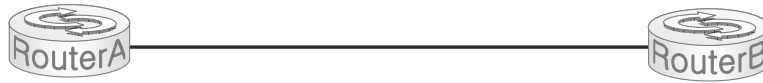
→ Logging 메시지의 수준을 설정한다.

<0-7> Logging severity level

alerts	Immediate action needed	(severity=1)
critical	Critical conditions	(severity=2)
debugging	Debugging messages	(severity=7)
emergencies	System is unusable	(severity=0)
errors	Error conditions	(severity=3)
informational	Informational messages	(severity=6)
notifications	Normal but significant conditions	(severity=5)
warnings	Warning conditions	(severity=4)

기타 Features

Hiding Telnet Addresses



- ◆ 외부로 Telnet을 수행 시 표시되는 원격호스트의 IP Address를 숨기는 기능.
- ◆ Telnet Session이 설립되는 동안의 각종 메시지에 출력되는 원격 호스트의 IP Address를 숨김.
- ◆ 형식
 - Router(config)#service hide-telnet-address

```
!  
Hostname RouterA  
Service hide-telnet-address  
Ip host RouterB 192.168.1.2  
!  
Interface Ethernet 0  
ip address 192.168.1.1 255.255.255.0  
!  
  
RouterA#telnet RouterB  
...  
RouterB>
```

```
!  
Hostname RouterB  
!  
Interface Ethernet 0  
ip address 192.168.1.2 255.255.255.0  
!  
Line vty 0 4  
login  
password cisco  
!
```

1-75

<http://www.lsfurion.com>

Hide telnet address기능은 IOS Device에서 remote hostname로 telnet 접근 시 remote hostname과 mapping되는 IP 정보를 보이지 않게 한다.

◆ Idle Terminal Message

- 콘솔이나 터미널들이 사용 중이 아닐 때 시스템이 표시하도록 설정하는 것, 다른 말로 **vacant message** 라고도 함
- 형식
 - ◆ Router(config-line)#vacant-message [d message d]
 - ◆ “d” → 종료문자로 message 내에서 사용되지 않는 어떤 문자

◆ “Line in Use” Message

- **Incoming** 연결을 요청한 클라이언트에게 모든 **rotary group**이나 라인이 사용 중일때 원격 클라이언트에게 보내 줄 메시지
- 형식
 - ◆ Router(config-line)#refuse-message d message d

◆ “Host Failed” Message

- 다른 원격 호스트로 Telnet 접속을 시도했으나 실패했을 때 **Local Telnet Client**에게 보여 줄 메시지를 지정
- 형식
 - ◆ Router(config)#ip host *hostname ip_address*
 - ◆ Router(config)#busy-message *hostname d message d*

1-76

<http://www.lsfurion.com>

다음은 IOS Device에서 관리자가 직접 정의할 수 있는 Terminal Message의 종류들이다.

• Idle Terminal Message

콘솔이나 터미널들이 사용 중이 아닐 때 시스템이 표시하도록 설정하는 것, 다른 말로 vacant message 라고도 함.
명령어 형식

Router(config-line)#vacant-message [d message d]

“d” → 종료문자로 message 내에서 사용되지 않는 어떤 문자

• “Line in Use” Message

Incoming 연결을 요청한 클라이언트에게 모든 rotary group이나 라인이 사용 중일때 원격 클라이언트에게 보내 줄 메시지
명령어 형식

Router(config-line)#refuse-message d message d

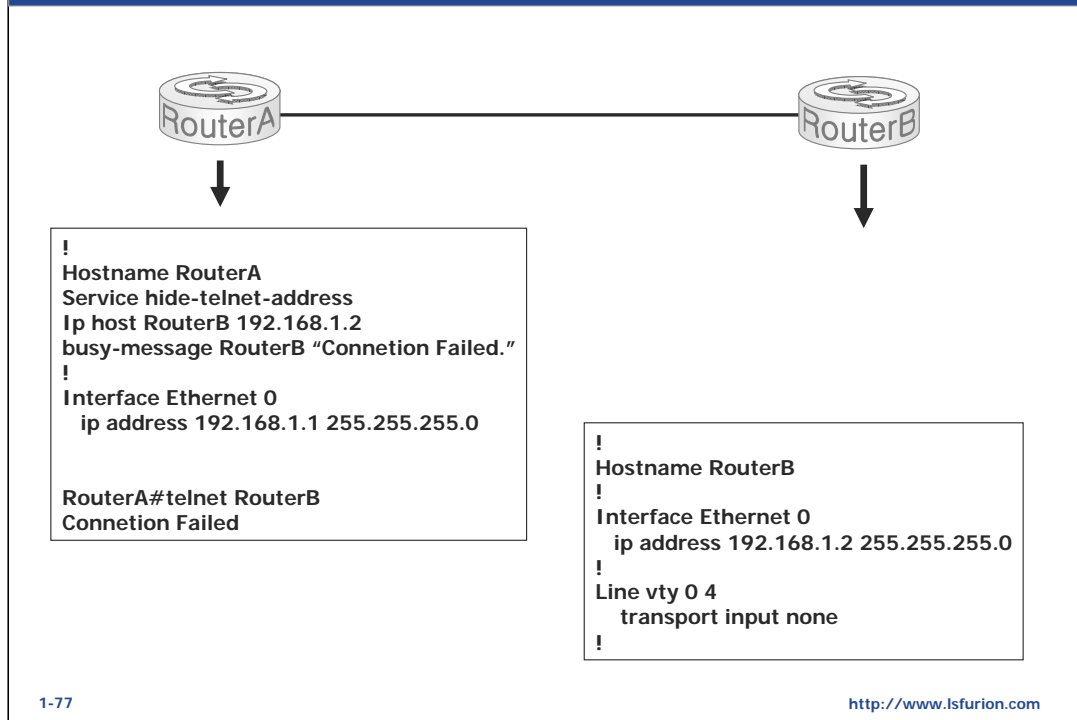
• “Host Failed” Message

다른 원격 호스트로 Telnet 접속을 시도했으나 실패했을 때 Local Telnet Client에게 보여 줄 메시지를 지정
형식

Router(config)#ip host *hostname ip_address*

Router(config)#busy-message *hostname d message d*

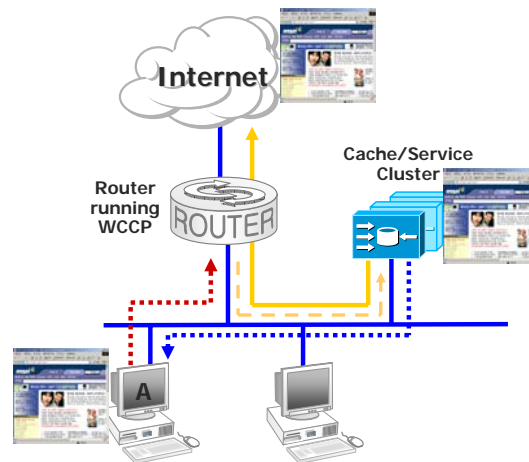
"Host Failed" Message 구성 예제



위 그림에서 Router-B는 외부에서 접근하는 Telnet을 Disable하기 위해 line configuration mode에서 'transport input none' command를 설정하였다.

Router-A는 RouterB를 위한 host table에 등록하고, RouterB에 telnet연결 시 문제가 발생하면 관리자가 정의한 문구가 콘솔 화면에 표시되도록 busy-message를 설정하였다.

WCCP (Web Cache Communication Protocol)



- WCCP는 Router와 Cisco WEB Cache Device사이에서 동작한다.
- Router는 HTTP Request Traffic들을 WEB Cache로 전달 한다.
- Cisco WEB Cache는 User들이 자주 참조 하는 WEB Content를 저장하고, 이를 Local Network에서 제공한다.

1-78

<http://www.lsfurion.com>

Web Cache란, 자주 참조하는 WEB Site의 Content들을 미리 Local Network에 저장하고 있다가 사용자들의 HTTP Request에 대해 대신 Content를 제공하는 기능을 의미한다. 이러한 기능으로 인터넷으로 나가는 HTTP Traffic을 줄일 수 있어 Bandwidth를 절약하고, Web Content를 요구하는 사용자들에게 좀 더 빠른 응답을 제공할 수 있다.

WCCP는 Cisco Router와 Cisco Web Cache사이에서 사용하는 전용 Protocol이며, Router는 자신에게 입력되는 HTTP pattern의 Traffic들을 WCCP를 통해 Web Cache에게 알려 준다.

Web Cache는 자신의 Local Cache를 검색하여, 사용자들이 원하는 WEB Content가 있는지 확인한다. 만약 사용자들이 요구하는 Content를 Web Cache가 가지고 있다면 Local Network 수준에서 정보가 제공되며, 만약 사용자들이 원하는 정보가 없다면 Web Cache 스스로가 해당 사이트에 접근하여 필요한 Content를 받아서 자신의 Local Cache에 기록 후 사용자들에게 서비스한다.

CCIE Lab에서는 Web Cache가 특정 Network에 있는 것으로 간주하고, 특정 Router가 WEB Cache와 연동할 수 있도록 구성하는 문제가 출제된다.

WCCP Router 설정 예제

WCCP-Router(config)#

```
ip wccp {web-cache | service-number} [group-address  
multicast-address] [redirect-list access-list] [group-list  
access-list] [password password]
```

- To direct a router to enable or disable the support for a cache engine service group

WCCP-Router(config)#

```
ip wccp version {1 | 2}
```

- To specify which version of WCCP you want to configure on your router

WCCP-Router(config-if)#

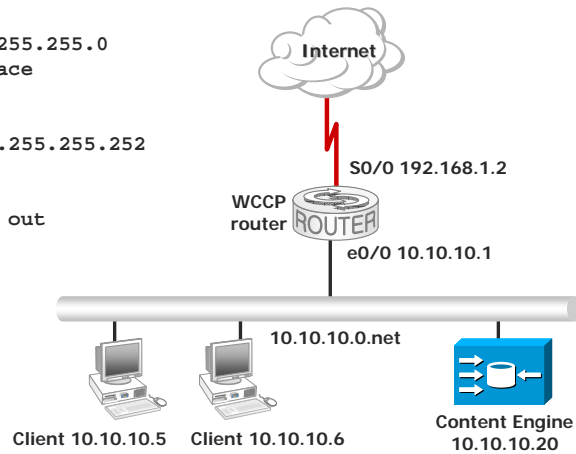
```
ip wccp service redirect {out | in}
```

- To enable packet redirection on an outbound or inbound interface using WCCP

위 그림은 Router에서 WCCP를 설정하는 명령어들에 대한 예제이다.

Web Cache가 같은 Subnet에 있는 경우

```
hostname WCCP-Router
!
!
ip wccp web-cache
!
interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 ip route-cache same-interface
!
interface Serial0
 ip address 192.168.1.2 255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
 ip wccp web-cache redirect out
!
end
```



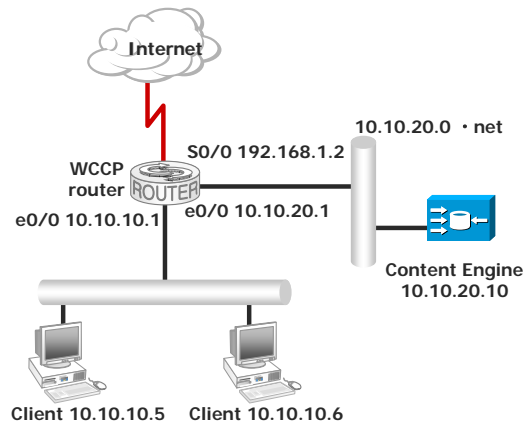
1-80

<http://www.lsfurion.com>

위 그림은 WEB Cache가 HTTP Client들과 같은 Subnet에 있는 상황에서, Router에 WCCP를 설정한 예제이다.

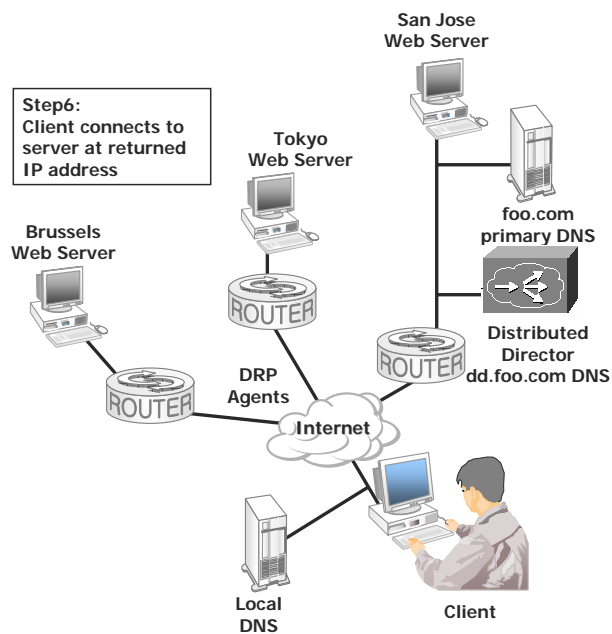
Transparent Caching WCCP Router Configuration Example 2

```
!  
hostname WCCP-Router  
!  
ip subnet-zero  
!  
ip wccp web-cache  
!  
interface Ethernet0  
  ip address 10.10.10.1 255.255.255.0  
!  
interface Ethernet1  
  ip address 10.10.20.1 255.255.255.0  
!  
interface Serial0  
  ip address 192.168.1.2 255.255.255.252  
  ip wccp web-cache redirect out  
!  
end
```



위 그림은 WEB Cache가 HTTP Client가 다른 Subnet에 있는 경우 설정 예제이다.

Cisco Distribute Director



1-82

<http://www.lsfurion.com>

Cisco Distribute Director란, user들의 DNS Name Query 또는 HTTP Request의 URL 정보와 대응하는 IP 정보들을 자신의 Local Cache에 저장하고 있다. 이를 위해서는 Cisco Distributed Director Service를 지원하는 특정 장치가 필요하며, Router들과는 DRP(Director Response Protocol)을 이용하여 통신한다. Cisco Distributed Director와 Router사이에 DRP를 이용한 통신이 가능 하려면 Router를 DRP Agent로 설정해야 한다.

```
!  
hostname DRPWest  
!  
key chain KEY-CHAIN-NAME  
key 1  
key-string my_keychain_password  
!  
!  
!  
interface FastEthernet0/0  
ip address 192.168.134.235 255.255.255.248  
no ip directed-broadcast  
no ip mroute-cache  
full-duplex  
!  
!  
ip drp authentication key-chain KEY-CHAIN-NAME  
ip drp server  
!
```

단순히 Router를 DRP Agent로 설정하는 경우에는 ‘ip drp server’ command라는 설정만 있으면 된다. 위 그림은 DRP Agent와 Distributed Director 사이에 인증된 DRP 정보를 교환하기 위해 별도의 키를 사용한 인증의 예제이다.