Windows Server 2003 Network Infrastructure

Microsoft®

목 차

1. Windows Server 의 Network Infrastructure 의 기능 요약

1) DNS

A. DNS의 개요

DNS 는 Windows Server 2003 서버에서 이름을 분해하는 기본 방식입니다. DNS 는 Active Directory 배포를 위한 기본 요구 사항이기도 합니다. 하지만 DNS 배포 시에는 Active Directory 가 필요하지 않습니다. DNS 와 Active Directory 의 통합은 기업 이름 분해를 위한 최상의 보안, 성능 및 가용성을 제공합니다.

Windows Server 2003 DNS 는 다양한 운영 체제와 호환됩니다. 또한 DNS 는 계층식 명명 시스템을 구현하는 분산 데이터베이스를 사용합니다. 이 명명 시스템은 조직이 인터넷 상에서 자신의 입지를 확대하고 인터넷상에서나 TCP/IP 기반 인트라넷상에서 고유한 이름을 생성할 수 있게 해줍니다.

분산된 계층 구조를 가진 DNS 는 인터넷 이름 공간을 위해 전 세계적으로 사용됩니다. DNS 를 이용하여 인터넷상의 모든 컴퓨터는 인터넷 이름공간에 있는 다른 컴퓨터 이름을 찾을 수 있습니다. Windows Server 2003 Server 와 Windows 2000 을 실행하는 컴퓨터들도 DNS 를 이용하여 도메인 컨트롤러의 위치를 찾을 수 있습니다

DNS 를 Active Directory 와 함께 배포하면 Active Directory 의 멀티마스터 복제 토폴로지를 이용하여 이름 분해 성능과 무결성을 향상시킬 수 있습니다. Active Directory 통합 영역을 배포하면 별도의 단일 마스터인 일차/이차 영역 전송 토폴로지가 필요하지 않습니다. Active Directory 통합 영역은 영역 데이터를 Active Directory 데이터베이스에 저장합니다. Active Directory 에는 이차 영역을 저장할 수 없으므로 Active Directory 통합 영역을 사용하려면 도메인 컨트롤러에서 DNS 서버 서비스를 실행해야 하며 일차 영역을 독점적으로 사용해야 합니다. Active Directory 통합 영역을 배포할 경우 DNS 동적 업데이트 프로토콜의 확장 프로그램인 안전한 동적 업데이트(Secure Dynamic Update)를 구현함으로써 Active Directory 보안 모델을 활용할 수 있습니다.

DNS 를 배포할 경우, 전체 네트워크에서 리소스를 찾을 수 있는 확장형 메커니즘을 제공할 수 있게 됩니다. DNS 와 Active Directory 를 통합하면 DNS 의 보안과 성능이 강화됩니다.

B. Windows Server 2003에서 새로워진 기능

- **조건부 전달(Conditional forwarding).** 조건부 전달 기능은 쿼리되는 DNS 도메인 이름을 기반으로 DNS 쿼리를 전달할 수 있도록 합니다. 조건부 전달에 관한 추가 정보는 Windows Server 2003 Server 에 대한 도움말 및 지원 센터(Help and Support Center)를 참조하십시오.

- **스텁 영역(Stub zones).** 스텁 영역은 부모 영역을 호스트하는 DNS 서버와 각 자식 영역을 위해 인증된 DNS 서버를 동기화할 수 있도록 합니다. 스텁 영역에 대한 추가 정보는 Windows Server 2003 Server 에 대한 도움말 및 지원 센터(Help and Support Center)를 참조하십시오.
- **Active Directory 통합 영역.** Active Directory 통합 영역은 Active Directory 데이터베이스에 영역 데이터를 저장할 수 있도록 합니다. Active Directory 통합 영역에 있는 모든 일차 DNS 서버상의 영역 정보는 항상 복제됩니다. Active Directory 통합 영역에 관한 추가 정보는 Windows Server 2003 Server 에 대한 도움말 및 지원 센터를 참조하십시오.

C. 용어의 정의

다음은 몇 가지 주요 DNS 관련 용어들입니다.

- **승인된 이름 서버(Authoritative name server).** 특정 영역에 대한 DNS 쿼리를 분해할 수 있는 권한을 가진 서버. 승인된 이름 서버에는 영역 내에 있는 컴퓨터에 대한 리소스 기록의 로컬 영역 파일이 들어있습니다. 각 영역에는 적어도 하나의 승인된 이름 서버가 있습니다.
- **조건부 전달(Conditional forwarding).** 조건부 전달은 전달자가 쿼리에 지정된 도메인 이름과 관련되어 있는 내부 도메인 이름과 IP 주소를 지정할 수 있도록 합니다. Windows Server 2003 DNS 에서는 이름 기반 조건을 DNS 전달자에 추가하여 이름 분해 성능을 향상시킬 수 있습니다. 전달자가 쿼리에 지정된 도메인 이름과 조건에 지정된 도메인 이름을 매치시킬 때, 전달자는 지정된 도메인에 있는 DNS 서버에 쿼리를 전달합니다. 조건부 전달을 사용하도록 구성된 DNS 서버들은 재귀 기능(recursion)을 허용하지 않고도 이름 분해를 할 수 있습니다.
- **위임.** 도메인 이름에 대한 책임을 네트워크상의 각기 다른 DNS 서버에 분산시키는 프로세스. 위임되는 각 도메인 이름 별로 적어도 하나의 영역을 생성해야 합니다. 도메인을 더 많이 위임할수록 생성해야 하는 영역도 더 많아 집니다.
- **DNS 이름 공간.** 도메인 이름 트리의 계층 구조입니다. FQDN (fully qualified domain name)에 사용되는 각 도메인 라벨은 도메인 이름 공간 트리의 노드나 브랜치(branch)를 나타냅니다. 예를 들어, host1.contoso.com 은 인터넷 루트아래, 노드 com 아래, 노드 Contoso 아래에 있는 노드 host1 을 나타내는 FQDN 입니다.
- **DNS 분해자(resolver).** 클라이언트 컴퓨터에서 실행되며 DNS 쿼리를 DNS 서버에 전송하는 서비스 입니다.
- **DNS 서버.** DNS 서버 서비스를 실행하는 컴퓨터. DNS 서버는 일부 DNS 데이터베이스에 관한 정보를 유지 관리하고 DNS 쿼리를 분해합니다.

- **외부 이름 공간.** 인터넷과 같은 공용 이름 공간으로 연결된 모든 장치에서 액세스할 수 있습니다. 최 상위 수준 도메인 아래에 있는 ICANN(Internet Corporation for Assigned Names and Numbers)과 기타 인터넷 명명 기관들은 도메인을 ISP(Internet Service Providers)와 같은 조직에 위임하고 이들은 다시 그들 고객들에게 하위 도메인을 위임합니다.
- **FQDN (Fully qualified domain name).** DNS 이름 공간에 있는 노드를 독자적인 방식으로 식별하는 DNS 이름. 컴퓨터의 FQDN 은 컴퓨터 이름이 연결되어 있는 것이며(예, client1), 컴퓨터의 주 DNS 접미사(예, contoso.com)입니다.
- **내부 이름 공간.** 조직들이 액세스를 제어할 수 있는 이름 공간. 조직들은 내부 이름 공간을 이용하여 인터넷으로부터 그들의 내부 컴퓨터 이름과 IP 주소를 보호할 수 있습니다. 하나의 조직이 여러 개의 내부 이름 공간을 보유할 수 있습니다. 조직들은 필요에 따라 자체 루트 서버와 하위 도메인을 생성할 수 있습니다. 내부 이름 공간은 외부 이름 공간과 공존할 수 있습니다.
- **이름 서버.** 특정 영역 내에 있는 클라이언트로부터의 요청에 대해 DNS 분해자에게 응답하고 FQDN 을 IP 주소로 분해하는 DNS 서버. 영역에는 일차 및 이차 이름 서버가 포함될 수 있습니다.
- **마스터 이름 서버.** 영역에 대한 이름 분해 권한을 가지고 있는 서버. 마스터 이름 서버가 일차 이름 서버일 경우, 리소스 기록에 대한 로컬 영역 파일을 반드시 가지고 있어야 합니다. 마스터 이름 서버가 이차 이름 서버일 경우, 영역 전송 시 다른 마스터 이름 서버의 영역에 대한 리소스 기록을 반드시 확보해야 합니다.
- **일차 이름 서버.** 권한을 가지고 있는 영역에 대한 이름 분해를 담당하는 서버. 일차 이름 서버는 호스트 이름과 IP 주소를 매핑하는 리소스 기록의 마스터 DNS 데이터베이스를 가지고 있습니다. 마스터 DNS 데이터베이스 기록들은 로컬 영역 파일에 들어있습니다.
- **이차 이름 서버.** 영역 전송 시 마스터 이름 서버로부터 영역에 대한 리소스 기록을 확보해야 하는 서버. 이차 이름 서버는 로컬 영역 파일을 가지고 있지 않습니다. 이차 이름 서버가 마스터 이름 서버일 경우, 영역에 대한 이름 분해 권한을 가지지만 다른 마스터 이름 서버로부터 리소스 기록을 확보해야 합니다. 이차 이름 서버가 마스터 이름 서버가 아닌 경우, 이는 중복 작업과 로드 밸런싱에 사용될 수 있습니다.
- **리소스 기록(RR).** DNS 쿼리를 처리하는데 사용되는 정보를 포함하고 있는 표준 DNS 데이터베이스 구조. 예를 들어, (A)라는 주소의 리소스 기록에는 호스트 이름에 해당하는 IP 주소가 들어있습니다. 대부분의 기존 RR 유형은 RFC 1035, “도메인 이름-구현과 규정”에 정의되어 있지만 부수적인 RR 유형은 다른 RFC 에도 정의되어 있으며 DNS 에서 사용할 수 있도록 승인되었습니다.
- **스텁 영역.** DNS 서버에 의해 호스트 될 수 있는 영역의 부분 사본으로 재귀 또는 반복 쿼리를 분해하는데 사용됩니다. 스텁 영역에는 영역의 SOA(Start of Authority) 리소스

기록과 영역의 승인된 서버를 나타내는 DNS 리소스 기록 및 영역의 승인된 서버에 접속하는데 필요한 연결(glue) A(주소) 리소스 기록이 들어있습니다.

- **영역.** DNS 데이터베이스에서 DNS 서버에 의해 하나의 별개 항목으로 관리되는 DNS 트리의 연속되어 있는 부분. 영역에는 영역 내에 있는 모든 이름들에 대한 리소스 기록이 들어있습니다.
- **영역 파일.** 영역을 정의하는 DNS 데이터베이스 리소스 기록들로 구성된 파일. 각 일차 이름 서버에는 영역 파일이 들어있습니다.
- **영역전송.** 일차 이름 서버에 있는 영역 파일의 내용들을 이차 이름 서버로 이동시키는 프로세스. 영역 전송은 이차 이름 서버에 있는 영역 파일과 일차 이름 서버에 있는 영역 파일을 동기화 시킴으로써 내결함성을 제공합니다. 이차 이름 서버는 일차 이름 서버가 실패할 경우에도 이름 분해 작업을 계속 수행할 수 있습니다. 또한 영역 전송은 대용량 이름 분해 쿼리 기간 동안 일차 와 이차 이름 서버간에 네트워크 로드를 분할함으로써 로드 밸런싱을 제공합니다

D. DNS 배포

DNS 배포 프로세스

DNS 배포 작업에는 DNS 이름 공간, DNS 서버 배치, DNS 영역, DNS 클라이언트 구성을 비롯하여 DNS 인프라를 계획하고 설계하는 작업이 포함됩니다. 그 밖에도 Active Directory 와의 통합 수준을 계획해야 하며 자신의 생산 환경에 DNS 솔루션을 구현하기 전에 보안성, 확장성 및 성능 요구사항을 확인해야 합니다.

1. DNS 배포 도구

Windows Server 2003 에는 DNS 인프라를 배포하는데 도움이 되는 여러 가지 도구들이 있습니다.

1-1 Active Directory Sizer

Active Directory Sizer 는 조직의 프로파일, 도메인 정보 및 사이트 토폴로지를 기반으로 하여 Active Directory 를 배포할 때 필요한 하드웨어를 판단합니다. Active Directory Sizer 는 사용자 입력 사항과 내부 공식을 이용하여 다음과 같은 항목들의 수를 측정합니다.

- 사이트별 도메인별 도메인 컨트롤러.
- 사이트별 도메인별 글로벌 카탈로그 서버.
- 컴퓨터별 CPUs 와 CPU 유형.
- Active Directory 데이터 스토리지용으로 필요한 디스크.

Active Directory Sizer 는 다음 항목들도 측정합니다.

- 필요한 메모리 용량.
- 네트워크 대역폭 사용률.
- 도메인 데이터베이스 크기.
- 글로벌 카탈로그 데이터베이스 크기.
- 사이트간 복제에 필요한 대역폭.

1-2 Netdiag

Netdiag 도구는 네트워킹과 연결성 문제를 해결하는데 사용됩니다. Netdiag 는 네트워크 클라이언트의 상태를 확인하는데 사용되는 일련의 테스트를 실시합니다. Netdiag 에 관한 추가 정보는 Windows Server 2003 Server 에 대한 도움말 및 지원 센터에서 “지원 도구”를 참조하십시오.

1-3 Dnscmd.exe

Dnscmd.exe 명령줄 도구를 이용하면 DNS Microsoft Management Console (MMC) 스냅인에서 수행할 수 있는 대부분의 작업을 수행할 수 있습니다.

2. 현재 환경 조사하기

자신의 환경에 Windows Server 2003 DNS 를 배포하기 전에, 독자적인 DNS 인프라를 배포해야 하는지 혹은 DNS 관리를 아웃소싱할 것인지를 결정하기 위해 자신의 현재 요구 사항을 평가해봐야 합니다. 또한 조직의 현재 및 미래의 요구에 맞는 Windows Server 2003 DNS 배포 계획을 세워야 합니다.

2-1 인터넷 상태 확인하기

내부 도메인의 범위를 넘어서 이름 분해를 지원하려면, IP 주소와 DNS 도메인 이름이 인터넷 등록 기관에 등록되어야 합니다. 인터넷 등록기관들은 다음과 같은 일을 담당합니다.

- IP 주소 할당.
- DNS 도메인 이름 등록.
- 등록된 IP 주소와 도메인 이름의 공용 기록 보관

네트워크가 인터넷에 연결되어 있거나 연결될 예정인 경우, IP 주소의 등록 상태를 확인해야 합니다. 여러분의 네트워크에 있는 리소스를 찾기 위해 이 네트워크 IP 주소는 인터넷상의 다른 컴퓨터에 의해서도 사용될 것입니다.

이미 인터넷에 연결되어 있는 경우, 여러분의 네트워크는 ISP 네트워크의 서브넷이 됩니다. 여러분의 ISP 가 이 서브넷의 IP 주소를 인터넷 등록 기관에 등록하였는지 확인하십시오. ISP 가 여러분의 네트워크 IP 주소를 등록하였다면 직접 등록할 필요가 없습니다.

2-2 DNS 데이터 호스트 확인하기

DNS 데이터를 누가 호스팅할 것인지를 결정하십시오. DNS 데이터를 내부적으로 호스트할 수도 있고 외부 ISP 로 하여금 DNS 데이터를 호스트 하도록 할 수도 있습니다. 자신의 DNS 데이터를 호스트 함으로써 네트워크 리소스 할당과 보안을 완벽하게 제어할 수 있습니다. 자신의 네트워크가 당분간은 신속하게 확장되지 못하는 작은 규모일 경우에만 ISP 를 사용하십시오. DNS 데이터를 호스트 하기로 결정할 경우엔, DNS 클라이언트와 서버가 외부 호스트들을 위해 이름 분해를 하도록 ISP 의 DNS 서버를 사용할 수 있도록 할 것을 고려해 보야 합니다. 이러한 구성은 네트워크 전체에 대한 대역폭 활용도를 향상시킬 수 있습니다.

ISP 를 이용하여 DNS 데이터를 호스트 하기로 결정할 경우, ISP 의 DNS 서버 소프트웨어가 Windows Server 2003 DNS 와 호환되는지를 확인하여 ISP 의 DNS 인프라가 자신의 DNS 배포를 지원할 수 있는지 확인합니다. ISP 가 특정 Windows Server 2003 기능을 지원하도록 해야 하는 경우, 그 ISP 가 사용하는 DNS 버전이 이러한 기능들을 지원하는지를 확인합니다. 자신의 ISP 가 어떤 DNS 서버 소프트웨어를 사용하고 있는지 그리고 그 소프트웨어의 기능과 옵션들이 Windows Server 2003 DNS 와 어떻게 상호 작동되는지를 알고 있어야 합니다. 각기 다른 DNS 서버 소프트웨어 솔루션들은 각기 다른 기능과 옵션을 제공합니다.

조직에서 자신의 모든 DNS 데이터를 호스트 하는 경우엔 ISP 의 DNS 인프라에 대해 고려해볼 필요가 없습니다. ISP 의 도움 없이 자신의 DNS 데이터를 호스트하고 있는 경우에도 외부 호스트를 위한 이름 분해를 하기 위해선 자신의 DNS 클라이언트와 서버가 ISP 의 DNS 서버를 이용할 수 있도록 할 수 있다는 사실을 기억하십시오. 이 경우 자신의 ISP 에게 이 구성을 알릴 필요는 없습니다.

2-3 네트워크 토폴로지 분석하기

기존 네트워크 토폴로지를 분석하고 네트워크 설계를 통해 알 수 있는 서비스와 관리 목적을 확인합니다. DNS 이름 공간을 계획할 때, 조직의 서비스 및 관리 목적에 대해 설명해야 합니다. 처음 배포하는 도메인 이름간에 도메인 이름 개체틀(placeholders)을 포함시켜 자신의 DNS 계층에 있는 노드의 예상 확장 수를 참작합니다. 도메인 이름 자리값을 추가하면 추가되는 도메인 이름을 수용하기 위해 DNS 인프라를 재설계할 필요가 없게 됩니다.

변경된 컨텍스트에 사용될 수 있는 도메인 이름을 할당하여 자신의 비즈니스 모델에 대한 변경 가능성에 대해 사전에 준비합니다. 예를 들어 accounting.contoso.com 이라는 도메인 이름을 사용하지 않고 대신에 finance.contoso.com 을 사용하여 accounting 외에 financial 서비스도 추가될 수 있는 확장 가능성에 대해 준비합니다.

2-4 기존 DNS 인프라 도표 만들기

Windows Server2003 으로 업그레이드하거나 새로운 DNS 를 배포하거나 혹은 Windows Server 2003 DNS 와 Active Directory 서비스를 통합하는 경우, 기존 DNS 인프라를 변경할 필요가 없습니다. 하지만 써드 파티 DNS 인프라로부터 마이그레이션하거나 Windows Server 2003

DNS 를 기존 써드 파티 DNS 인프라와 통합하는 경우엔, 도메인, 서버 및 클라이언트가 포함된 기존 DNS 인프라에 대한 도표를 만들어야 합니다. 이 도표를 이용하면 Windows Server 2003 DNS 를 배포할 때 현재 DNS 인프라에 변경된 사항이 있는지 확인하는데 유용합니다.

2-5 보안 정책 확인하기

Windows Server 2003 DNS 인프라를 설계하고 배포하기 전에 조직의 보안 정책을 확인하고 문서화합니다. 이렇게 하면 자신의 DNS 서버와 영역 및 리소스 기록들이 이러한 정책을 지원하도록 할 수 있습니다. Windows Server 2003 DNS 에는 안전한 DNS 인프라를 배포할 수 있도록 해주는 기능들이 들어있습니다.

3.DNS 이름 공간 설계하기

DNS 인프라를 배포하기 전에 DNS 이름 공간을 설계해야 합니다. 여러분은 인터넷 사용자와 컴퓨터에게 공개되는 외부 이름 공간을 설계할 수도 있으며 내부 이름 공간에 있는 사용자와 컴퓨터만이 액세스할 수 있는 내부 이름 공간을 설계할 수도 있습니다.

3-1 자신의 DNS 이름 공간 요구 사항 확인하기

DNS 이름 공간을 설계하는 첫 번째 단계는 조직을 위한 새로운 이름 공간이 필요한지 혹은 기존 Windows 또는 써드 파티 DNS 이름 공간을 계속 사용할 것인지를 결정하는 것입니다.

이전 버전의 Windows 에서 Windows Server 2003 DNS 로 업그레이드하는 경우, Windows Internet Name Service (WINS)와 같은 기존 이름 분해 시스템을 지원하거나 Windows Server 2003 DNS 인프라로 대체해야 합니다. WINS 서버를 쿼리할 수 있도록 Windows Server 2003 DNS 서버를 DNS 영역 설정으로 구성하여 기존 WINS 배포를 지원할 수 있습니다.

Windows Server 2003 DNS 를 마이그레이션하거나 써드 파티 DNS 인프라와 통합하는 경우엔, 써드 파티 DNS 인프라에 사용되는 이름 공간 설계를 변경할 필요가 없습니다. 새로운 Windows Server 2003 DNS 인프라를 배포하는 경우엔, DNS 도메인과 컴퓨터 이름 전략을 생성해야 하며 이러한 이름들이 네트워크와 인터넷을 통해 어떻게 분해될 것인지를 계획해야 합니다.

Active Directory 를 지원하기 위해 Windows Server 2003 DNS 를 배포하는 경우, Active Directory 포리스트와 도메인 이름을 자신의 DNS 인프라에 통합해야 합니다. 예를 들어, Active Directory 도메인 컨트롤러, OU, 사이트 및 서브넷의 특정 이름들을 위치를 찾아야 하는 네트워크 리소스를 수용하기 위해 기존 DNS 이름 공간 설계를 변경할 수 있습니다.

표 3.1 DNS 이름 공간 설계 요구 사항

시나리오	설계 요구 사항
Windows Server 2003 Server 보다 이전 버전의 Windows 에서 기존 DNS 인프라를	DNS 이름 공간 설계는 그대로 유지됩니다.

업그레이드하고 있습니다.	
표준 DNS 도메인 명명 지침서를 준수하는 DNS 소프트웨어를 사용하는 써드 파티 DNS 인프라로부터 업그레이드하고 있습니다.	DNS 이름 공간 설계는 그대로 유지됩니다.
기본 DNS 소프트웨어가 표준 DNS 도메인 명명 지침서를 준수하지 않습니다.	Windows Server 2003 DNS 이름 공간을 배포하기 전에 기존 DNS 이름 공간 설계를 DNS 도메인 명명 지침서를 준수하도록 합니다.
기존 써드 파티 DNS 소프트웨어가 표준 DNS 도메인 명명 지침서를 준수합니다.	Windows Server 2003 DNS 를 현재 DNS 인프라와 통합합니다. 써드 파티 DNS 인프라나 기존 이름 공간의 이름 공간 설계를 변경하지 않아도 됩니다.
새로운 Windows Server 2003 DNS 인프라를 배포하고 있습니다.	DNS 도메인 명명 지침서를 기반으로 하여 자신의 DNS 이름 공간에 대한 논리적 명명 규약을 설계합니다.
Active Directory 를 지원하는 Windows Server 2003 DNS 를 배포하고 있습니다.	자신의 Active Directory 명명 규약을 기반으로 하는 DNS 이름 공간 설계를 만듭니다.
Active Directory 를 지원하도록 기존 DNS 이름 공간을 변경하고 있지만 자신의 DNS 이름 공간을 재설계하고 싶지는 않습니다.	Active Directory 도메인 이름과 기존 DNS 이름이 일치하도록 합니다. 이로써 여러분은 가장 간단한 관리 기술로 가장 높은 수준의 보안을 배포할 수 있습니다.

E.Windows Server 2003 DNS 구현하기

1.Windows Server 2003 DNS 배포 준비하기

서버와 영역을 비롯하여 변경하고자 하는 모든 것에 대한 안전한 백업을 만들어서 Windows Server 2003 DNS 배포를 위한 환경을 준비합니다. 배포 작업에 들어가기 전에 백업들을 테스트합니다. 데이터 소실, 서버 중단 및 네트워크 연결 실패와 같은 사고에 대한 복구 계획도 세웁니다.

DNS 배포를 전개하기 전에 배포하고자 하는 서버간에 라우팅 링크들이 갖추어져 있고 제대로 작동되는지 확인합니다. DNS 인프라가 구성된 방식에 따라 DNS 서버는 다음 항목들을 쿼리해야 할 수도 있습니다.

- 루트 서버
- 전달자
- 부모 영역을 호스트 하는 서버
- 자식 영역을 호스트 하는 서버
- 마스터 영역을 호스트 하는 서버
- Active Directory 통합 서버인 경우, 동일한 영역의 다른 Active Directory 통합 사본을 호스트 하는 서버
- 인터넷상의 서버들

클라이언트들이 인터넷상의 이름들을 쿼리할 것이라 예상하고 프록시 서버를 사용할 계획인 경우, 프록시 서버가 제자리에 배치되어 있는지 확인합니다.

편의상, Active Directory 설치작업 시 도메인 컨트롤러에 DNS 를 설치하도록 할 수도 있습니다. 이렇게 할 경우, Active Directory 가 컴퓨터에 설치된 후에는 컴퓨터 이름을 변경할 수 없다는 사실을 기억하십시오.

2. DNS Server 설치하기

DNS 를 설치하기 전에, 컴퓨터 이름이 정확한지 그리고 자신의 DNS 서버가 쿼리해야 할 네트워크상의 다른 컴퓨터들을 핑할 수 있는지 확인합니다. 클라이언트는 DNS 서버를 IP 주소로 찾기 때문에 각 DNS 서버에 고정 IP 주소를 제공해야 합니다.

아래의 네 가지 방식 중 한가지를 이용하여 DNS 서버를 설치할 수 있습니다.

- Active Directory 를 설치하는 Active Directory 설치 마법사를 이용하여 서버에 DNS 를 설치합니다.

  Active Directory 설치 마법사는 Active Directory 도메인 이름에 해당하는 정방향 조회 영역의 Active Directory 통합 사본을 자동으로 생성하며 안전한 동적 업데이트를 위한 영역을 구성합니다. 그 외에도 마법사는 DNS RFC 가 권장하는 표준 역방향 조회 영역을 생성합니다. 일부 경우, 마법사는 서버를 루트 서버로 구성하거나 루트 서버의 이름을 이용하여 루트 힌트를 초기화합니다.

  마법사가 질문하는 모든 질문들에 대한 답변이 들어있는 응답 파일(answer file)을 실행하여 Active Directory 설치 마법사를 시작할 수 있습니다. 응답 파일을 사용하는 방법에 대한 추가 정보는 Windows Server 2003 Server Resource Kit 의 분산 서비스 안내서에 있는 “Active Directory 데이터 스토리지"를 참조하십시오(또는 http://www.microsoft.com/windows/reskits/default.asp ENG 에서 “Active Directory 데이터 스토리지”를 참조하십시오.).

- 서버에 Active Directory 를 설치하기 전후, 프로그램 추가/삭제 도구[Add or Remove Programs]를 이용하여 DNS 서버 서비스를 설치하고 DNS 서버 마법사 구성하기[Configure DNS Server Wizard]를 실행하여 영역을 구성할 수 있습니다. Active Directory 설치 마법사를 이용할 때 DNS 서버 마법사 구성하기[Configure DNS Server Wizard]는 DNS RFC 가 권장하는 표준 역방향 조회 영역을 생성하고 서버를 루트 서버로 구성하거나 루트 힌트를 초기화합니다.
- 명령줄 도구 Dnscmd.exe 를 이용하여 DNS 서버를 구성할 수 있습니다.
- Windows Server 2003 서버에 포함되어 있는 WMI 제공자를 통해 VB Script 나 다른 스크립팅 언어를 사용할 수 있습니다.

DNS 서버를 설치한 후엔, 루트 힌트를 다시 살펴봅니다. 서버가 루트 서버로 구성되어있지만 여러분은 이 서버가 루트 서버가 되길 원치 않을 경우엔 루트 영역을 삭제합니다.

이러한 옵션에 대한 추가 정보와 Active Directory 설치 마법사와 DNS 서버 마법사 구성하기[Configure DNS Server Wizard]가 루트 힌트 초기화 여부를 확인하는 방식에 대한 정보는 Windows Server 2003 Server Resource Kit 의 네트워킹 안내서에 있는 “Windows Server 2003 DNS”를 참조하십시오(또는 http://www.microsoft.com/windows/reskits/default.asp ENG 에서 “Windows Server 2003 DNS”를 참조하십시오.

3. 영역 설치하기

Active Directory 설치 마법사를 이용하여 DNS 를 설치하는 경우 마법사는 여러분이 지정한 Active Directory 도메인에 해당하는 DNS 영역을 생성합니다. 배포 시 영역 계획 단계에서 지정했던 영역이 지금까지 남아있지 않다면 지금 다시 생성합니다.

마법사가 생성한 영역이 자신의 원하는 유형의 영역이 아닌 경우, 지금 변경합니다. 예를 들어, 표준 일차 영역을 Active Directory 통합 영역으로 전환해주어야 할 수도 있습니다. 설치 마법사가 영역을 생성하였지만 권한위임을 추가하지 않은 경우엔 지금 추가합니다.

생성한 각 영역에 대해 적절한 리소스 기록들을 추가해주고 필요에 따라 동적 업데이트나 안전한 동적 업데이트를 활성화 하거나 비활성화합니다. 업데이트를 영역에 대한 이차 서버에 밀어 넣기(Push) 하려는 경우엔, 일차 서버에서 DNS notify 를 구성합니다.

영역을 추가하고 삭제하는 방법에 대한 추가 정보는 Windows Server 2003 서버에 대한 도움말 및 지원 센터를 참조하십시오.

4.전달자 구성하기

서버가 쿼리를 다른 서버에 전달해야 하는 경우, 쿼리를 전달해야 하는 서버 상에서 전달 기능을 구성합니다. 서버가 쿼리에 지정된 DNS 접미사 별로 각기 다른 서버에 쿼리를 전달하도록 하려면, 조건부 전달 기능을 적절하게 구성합니다.

조건부 전달에 관한 추가 정보는 이 장에 소개된 "전달 기능 사용하기"와 Windows Server 2003 Server Resource Kit 의 네트워킹 안내서에 있는 "Windows Server 2003 DNS"를 참조하십시오(또는 http://www.microsoft.com/windows/reskits/default.asp ENG 에서 "Windows Server 2003 DNS"를 참조하십시오.).

4. 동적 업데이트를 위해 DNS 서버 구성하기

서버와 영역을 구성한 방식에 따라 영역이 이미 동적 업데이트나 안전한 동적 업데이트를 위해 구성되어 있을 수도 있습니다. 영역이 원하는 대로 구성되지 않은 경우엔 필요에 맞게 변경해줍니다.

동적 업데이트와 안전한 동적 업데이트 구성 방법에 관한 정보는 Windows Server 2003 Server 에 대한 도움말 및 지원 센터를 참조하십시오.

5. 에이징과 청소 기능 구성하기

동적 업데이트를 이용하면, 컴퓨터가 네트워크에 참여하고 DHCP 에 등록될 때마다, DNS 서버는 자동으로 기록을 영역에 추가합니다. 하지만, 경우에 따라서, DNS 서버는 이들을 자동으로 삭제하지 못하므로 오래된 기록이 될 수도 있습니다. 오래된 리소스 기록들은 서버의 공간을 차지하고 서버는 오래된 리소스 기록을 이용하여 쿼리에 응답할 수도 있습니다. 그 결과, DNS 서버 성능이 저하됩니다. 이러한 문제를 해결하기 위해 Windows Server 2003 DNS 서버는 오래된 기록들에 대한 데이터베이스를 검색하여 그러한 기록들을 삭제함으로써 오래된 기록들을 청소할 수 있습니다.

DNS Manager 에서 또는 Dnscmd.exe 를 이용하여 에이징 및 청소 기능을 구성할 수 있습니다.

에이징과 청소 기능을 이용하는 방법에 관한 추가 정보는 Windows Server 2003 Server Resource Kit 의 네트워킹 안내서에 있는 "Windows Server 2003 DNS"를 참조하십시오(또는 http://www.microsoft.com/windows/reskits/default.asp ENG 에서 "Windows Server 2003 DNS"를 참조하십시오.).

6. 영역 복제 구성하기

파일 기반의 일차 또는 이차 영역을 사용하는 경우엔, 영역에 대한 각 이차 서버에 영역 전송을 할 수 있도록 영역에 대한 각 마스터 서버를 구성해줍니다. 그런 다음 그 영역에 대한 마스터 서버 목록을 이용하여 영역에 대한 각 이차 서버를 구성해줍니다.

Windows Server 2003 도메인에서 Active Directory 복제를 이용하는 경우엔, 영역 복제 범위를 구성해줍니다. 어플리케이션 디렉터리 파티션을 이용하려는 경우엔, 영역 복제 범위를

구성하기 위해 기업 관리자 자격 증명을 보유하고 있어야 합니다. Active Directory 에서 기본 어플리케이션 디렉터리 파티션을 사용할 수 없고 DNS 서버가 이들을 자동으로 생성하지 않을 경우에도 기업 관리자 자격 증명을 보유하고 있어야 합니다.

Active Directory 에서의 DNS 영역 스토리지와 복제, DNS 어플리케이션 디렉터리 파티션에 DNS 서버 참여시키기, DNS 어플리케이션 디렉터리 파티션에서 DNS 서버 제거하기 또는 영역 복제 범위 변경하기에 관한 추가 정보는 Windows Server 2003 Server 에 대한 도움말 및 지원 센터를 참조하십시오.

7. DNS 서버가 제대로 작동되는지 확인하기

DNS 서버를 설치하고 구성한 다음엔, 서버가 제대로 작동되는지 확인합니다. 간단한 쿼리 테스트 또는 재귀 쿼리 테스트와 같은 DNS MMC 스냅 인의 모니터링 기능을 이용합니다. 이벤트 로그를 검사하거나 로그 파일을 디버그 하거나 명령줄 도구 Nslookup 을 이용하여 쿼리해 볼 수도 있습니다. DNS MMC 스냅 인의 모니터링 기능에 액세스하려면, **Action** 메뉴에서 **Properties** 를 클릭한 다음 **Monitoring** 탭을 클릭합니다.

DNS 서버 작동 확인에 관한 추가 정보는 Windows Server 2003 Server Resource Kit 의 네트워킹 안내서에서 “DNS 문제해결”을 참조하십시오(또는 http://www.microsoft.com/windows/reskits/default.asp ENG 에서 “DNS 문제 해결”을 참조하십시오.).

8. DNS 클라이언트 설치하기

다음 항목들을 이용하여 각 DNS 클라이언트를 설치합니다.

- 호스트 이름과 DNS 접미사
- 주 사용 DNS 서버와 대체 DNS 서버
- Proxy Auto-Configuration 파일이나 (프록시 클라이언트의 경우)이름 제외 목록 중에서 선택

다음 방법들을 이용하여 DNS 클라이언트를 설치할 수 있습니다.

- 클라이언트의 TCP/IP 설정 사용
- 그룹 정책을 이용하여 클라이언트 그룹 구성
- DHCP 서버 서비스를 이용하여 일부 클라이언트 설정을 자동으로 구성합니다.

DNS 클라이언트 설치 및 구성 방법에 관한 추가 정보는 Windows Server 2003 Server 에 대한 도움말 및 지원 센터를 참조하십시오.

9. 명령줄 도구 이용하여 DNS 배포하기

명령줄 도구 Dnscmd.exe 를 이용하면 DNS MMC 스냅 인에서 수행할 수 있는 모든 작업들을 수행할 수 있습니다. Dnscmd.exe 를 이용하여 영역과 기록들을 생성, 삭제 및 조회할 수 있으며 서버와 영역 속성을 재설정할 수 있습니다. 그 외에도 영역 생성 또는 업데이트하기, 영역 다시 로드하기, 영역 새로 고치기, 파일이나 Active Directory 에 영역 재 작성하기, 영역 중단 및 재개하기, 캐시 비우기, 루트 힌트에 기록 추가하기, DNS 서비스 중단 및 개시하기 및 통계 값 조회하기와 같은 일상적인 관리 작업을 수행할 수 있습니다.

그리고 Dnscmd.exe 를 이용하여 배치 파일 스크립트를 작성할 수도 있으며 원격 관리도 할 수 있습니다. Dnscmd.exe 에 관한 추가 정보는 도움말 및 지원 센터에서 **Tools** 를 클릭한 후 **Windows Support Tools** 를 클릭합니다. Windows Server 2003 Support Tools 와 Support Tools Help 를 설치하고 사용하는 것에 대한 정보는 Windows Server 2003 Server 운영 체제 CD 의 ₩Support₩Tools 폴더에 있는 Sreadme.doc 파일을 참조하십시오.

Nslookup.exe 를 이용하여 DNS 도메인 이름 공간의 쿼리 테스트를 실시하고 진단 정보를 표시할 수 있습니다.

F. DNS 서버 보안

1.DNS 보안 위협 확인하기

DNS 인프라는 다음과 같은 유형의 보안 위협에 취약합니다.

- **Footprinting.** 도메인 이름, 컴퓨터 이름 및 중요한 네트워크 리소스에 대한 IP 주소와 같은 DNS 영역 데이터를 확보하여 DNS 인프라의 도표나 footprint 를 만드는 프로세스. DNS 도메인과 컴퓨터 이름은 주로 도메인과 컴퓨터의 기능이나 위치를 나타냅니다.
- **서비스 거부 공격.** 침입자가 재귀 쿼리를 이용하여 네트워크에 하나 이상의 DNS 서버들이 초과하여 거주하도록 하여 네트워크 서비스 가용성을 거부하도록 하는 공격. DNS 서버에 쿼리가 초과될 때, CPU 사용률은 결과적으로 최대 한도에 도달하게 되고 DNS 서버 서비스를 사용할 수 없게 됩니다. 네트워크상에서 완벽하게 작동하는 DNS 서버가 없을 경우, 네트워크 사용자들은 DNS 서버를 이용하는 네트워크 서비스들을 이용할 수 없습니다.
- **데이트 변경.** 침입자가 데이터를 파괴시키고 다른 공격을 시도하기 위해 만든 IP 패킷에 있는 유효한 IP 주소를 사용하는 것. 데이터 변경은 이미 풋 프린트된(footprinted) DNS 인프라에서 주로 발생됩니다. 공격이 성공할 경우엔, 패킷이 네트워크 상의 유효한 IP 주소로부터 보내지는 것처럼 보입니다. 이는 주로 IP 스푸핑이라 불립니다. 유효한 IP 주소(서브넷의 IP 주소 영역에 있는 IP 주소)를 이용하여, 침입자는 네트워크에 액세스할 수 있게 됩니다.
- **리디렉션.** 칩입자가 제어할 수 있는 서버로 DNS 이름에 대한 쿼리들을 리디렉션할 수 있는 공격. 리디렉션 방법 중 한가지는 침입자가 제어할 수 있는 서버에 쿼리들이 보내지도록 잘못된 DNS 데이터를 이용하여 DNS 서버의 DNS 캐시를 손상시키는 것입니다. 예를 들어, example.contoso.com 에 대한 쿼리가 만들어지고 조회 응답이 contoso.com domain 외부에

있는 이름에 대한 기록을 제공하는 경우, DNS 서버는 캐시된 데이터를 이용하여 외부 이름에 대한 쿼리를 분해합니다. 리디렉션은 침입자가 불안정한 동적 업데이트를 이용할 때처럼 DNS 데이터에 쓰기 가능한 액세스를 할 때 이루어질 수 있습니다.

일반적인 공격 유형, 보안 정책 개발 및 자신의 위험 수준 평가에 대한 추가 정보는 디렉터리 및 보안 서비스 설계 및 배포에서 “인증 전략 설계하기”를 참조하십시오.

2. DNS 보안 정책 개발하기

DNS 데이터가 손상된 경우, 침입자는 다른 서비스를 손상시키는데 사용될 수 있는 네트워크 정보를 확보할 수 있습니다. 예를 들어, 침입자는 다음과 같은 방식으로 조직에 해를 끼칠 수 있습니다.

- 영역 전송을 이용하여 침입자는 여러분의 네트워크에 있는 모든 호스트와 그들의 IP 주소 목록을 가져올 수 있습니다.
- 서비스 거부 공격을 이용하여 침입자는 이 메일이 네트워크에서 오고 갈수 없도록 할 수 있으며 웹 서버를 볼 수 없도록 할 수도 있습니다.
- 침입자가 영역 데이터를 변경할 수 있을 경우엔, 가짜 웹 서버를 설치하거나 이 메일이 그들의 서버로 리디렉트되도록 할 수 있습니다.

여러분의 공격 위험은 인터넷에 얼마나 노출되어 있는 가에 따라 차이가 있습니다. 개인 이름 공간, 개인 주소 방식 및 효율적인 방화벽을 사용하는 개인 네트워크에 있는 DNS 서버의 경우, 공격 위험이 낮고 침입자를 발견할 확률이 높습니다. 인터넷에 노출되어 있는 DNS 서버의 경우 위험이 더 높습니다.

DNS 보안 정책 개발에는 다음과 같은 과정이 포함됩니다.

- 자신의 클라이언트가 필요로 하는 액세스가 무엇인지, 보안과 성능 중 어느 쪽에 더 비중을 둘 것인지 및 어떤 데이터를 가장 보호하고 싶은 지를 결정합니다.
- 내부 및 외부 DNS 서버에 일반적으로 발생하는 보안 문제들에 대해 알고 있어야 합니다.
- 어떤 클라이언트가 어떤 서버들을 쿼리할 수 있는지 알 수 있도록 자신의 이름 분해 트래픽에 대해 연구합니다.

낮은 수준, 중간 수준 또는 높은 수준의 보안 정책을 선택적으로 적용할 수 있습니다.

2-1 낮은 수준의 DNS 보안 정책

낮은 수준의 보안은 DNS 배포를 추가로 구성할 필요가 없습니다. DNS 데이터의 무결성에 아무런 문제가 없거나 외부 연결에 대한 책임이 없는 개인 네트워크와 같은 네트워크 환경에서는 이러한 수준의 DNS 보안을 사용합니다. 낮은 수준의 보안 정책은 다음과 같은 특성이 있습니다.

- 조직의 DNS 인프라가 인터넷에 완전히 노출되어 있습니다.
- 네트워크상의 모든 DNS 서버는 표준 DNS 분해를 실시합니다.
- 모든 DNS 서버들은 인터넷에 대한 루트 서버를 나타내는 루트 힌트를 이용하여 구성됩니다.
- 모든 DNS 서버들은 모든 서버에 영역 전송을 할 수 있도록 허용합니다.
- 모든 DNS 서버들은 자신의 모든 IP 주소를 수신하도록 구성됩니다.
- 모든 DNS 서버상에서 캐시 손상 방지 기능을 사용할 수 없습니다.
- 모든 DNS 영역에 동적 업데이트가 허용됩니다.
- User Datagram Protocol (UDP)과 TCP/IP 포트 53 은 소스 및 대상 주소에 대한 네트워크를 위한 방화벽에 공개됩니다.

2-2 중간 수준의 보안 정책

중간 수준의 DNS 보안은 도메인 컨트롤러에서 DNS 서버를 실행하지 않고 Active Directory 에 DNS 영역을 저장하지 않고도 사용할 수 있는 DNS 보안 기능들로 이루어져 있습니다. 중간 수준의 보안 정책은 다음과 같은 특성이 있습니다.

- 조직의 DNS 인프라는 인터넷에 대한 노출이 제한되어 있습니다.
- 모든 DNS 서버들은 이름을 로컬에서 분해할 수 없을 때 전달자를 이용하여 특정 내부 DNS 서버 목록을 나타내도록 구성됩니다.
- 모든 DNS 서버들은 그들 영역의 NS 기록에 나열되어 있는 서버로만 영역 전송되도록 제한합니다.
- DNS 서버는 특정 IP 주소만 수신하도록 구성됩니다.
- 모든 DNS 서버에서 캐시 손상 방지 기능을 사용할 수 있습니다.
- DNS 영역에 대해 동적 업데이트가 허용되지 않습니다.
- 내부 DNS 서버는 허용 된 소스와 대상 주소에 대한 제한된 목록을 가지고 방화벽 너머 외부 DNS 서버들과 통신합니다.
- 방화벽 앞에 있는 외부 DNS 서버들은 인터넷에 대한 루트 서버를 나타내는 루트 힌트를 이용하여 구성됩니다.
- 모든 인터넷 이름 분해는 프록시 서버와 게이트웨이를 이용하여 수행됩니다.

2-3 높은 수준의 DNS 보안 정책

높은 수준의 DNS 보안은 중간 수준의 보안과 동일한 구성을 사용하며 DNS 서버 서비스가 도메인 컨트롤러에서 실행되고 DNS 영역이 Active Directory 에 저장되어 있을 때 사용할 수

있는 보안 기능들을 사용합니다. 또한 높은 수준의 보안은 DNS 가 인터넷과 통신하는 것을 철저히 배제합니다. 이는 일반적인 구성은 아니지만 인터넷 연결이 필요하지 않을 경우엔 권장되는 구성입니다. 높은 수준의 보안 정책은 다음과 같은 특성이 있습니다.

- 조직의 DNS 인프라는 내부 DNS 서버를 이용하여 인터넷과 통신할 수 없습니다.
- 여러분의 네트워크는 DNS 영역에 대한 모든 권한이 내부적으로 유효한 내부 DNS 루트 및 이름 공간을 사용합니다.
- 전달자로 구성된 DNS 서버들은 내부 DNS 서버 IP 주소만을 사용합니다.
- 모든 DNS 서버들은 특정 IP 주소로 제한됩니다.
- DNS 서버는 지정된 IP 주소를 수신하도록 구성됩니다.
- 모든 DNS 서버에서 캐시 손상 방지 기능을 사용할 수 있습니다.
- 내부 DNS 서버들은 내부 이름 공간에 대한 루트 영역을 호스트 하는 내부 DNS 서버를 나타내는 루트 힌트를 이용하여 구성됩니다.
- 모든 DNS 서버들은 도메인 컨트롤러에서 실행됩니다. Discretionary Access Control List (DACL)는 특정 개인만이 DNS 서버 상의 관리 작업을 수행하도록 DNS 서버 서비스상에 구성됩니다.
- 모든 DNS 영역은 Active Directory 에 저장됩니다. DACL 은 특정 개인만이 DNS 영역을 생성, 삭제 및 변경할 수 있도록 구성됩니다.
- DACLs 는 특정 개인만이 DNS 데이터를 생성, 삭제 및 변경할 수 있도록 DNS 리소스 기록상에 구성됩니다.
- 안전한 동적 업데이트는 동적 업데이트를 결코 허용하지 않는 상위 수준 및 루트 영역을 제외하고 모든 DNS 영역에 대해 구성됩니다.

3.인터넷에 노출되어 있는 DNS 서버 보호하기

인터넷에 노출되어 있는 DNS 서버들은 공격에 특히 취약합니다. 다음과 같은 작업을 해줌으로써 인터넷에 노출되어 있는 DNS 서버를 보호할 수 있습니다.

- 이름 서버를 내부 네트워크 대신에 경계 네트워크상에 배치합니다.
- 경계 네트워크에 관한 추가 정보는 ISA(Internet Security and Acceleration)에 대한 내용을 참고하시기 바랍니다. .
- 경계 네트워크 내부에 있으며 공개적으로 액세스 되는 서비스를 위해 한 대의 DNS 서버를 사용하고 개인 내부 네트워크를 위해 별도의 DNS 서버를 사용합니다. 이는 중요한 이름 및 IP 주소를 인터넷 기반 사용자들에게 노출시킬 수 있는 개인 이름 공간의 노출 위험을 줄여줍니다. 그리고 DNS 서버상의 리소스 기록의 수를 줄여주므로 성능이 향상됩니다.

- 다른 서브넷, 네트워크 또는 ISP 에 이차 서버를 추가합니다. 이는 서비스 거부 공격이 발생하지 않도록 보호해줍니다.
- 라우터와 DNS 서버를 보호하고 DNS 서버들을 지역적으로 분산시킴으로써 단일 오류 지점이 생기지 않도록 합니다. 적어도 한 대의 외부 지역 DNS 서버에 영역의 이차 사본을 추가합니다.
- 인터넷 기반 사용자들이 이름과 IP 주소를 보지 못하도록 하기 위해 IPSec 이나 VPN 터널을 이용하여 영역 복제 트래픽을 암호화합니다.
- UDP 와 TCP 포트 53 에 패킷 필터링을 하도록 방화벽을 구성합니다.
- DNS 서버에서 영역 전송을 초기화하도록 허용된 DNS 서버의 목록을 제한합니다. 네트워크에 있는 각 영역들에 대해 이 작업을 실시합니다.
- Event Viewer 를 이용하여 DNS 로그와 외부 DNS 서버들을 모니터링 합니다.

4. 내부 DNS 서버 보호하기

내부 DNS 서버는 외부 DNS 서버들에 비해 공격에 덜 취약한 편이지만 그래도 이들을 보호해 줄 필요는 있습니다. 내부 DNS 서버를 보호하려면 다음과 같이 하십시오.

- 어떠한 오류도 발생하지 못하도록 합니다. 하지만 클라이언트가 네트워크 서비스에 액세스할 수 없을 경우엔 DNS 중복성이 아무런 도움이 되지 못한 다는 점을 기억하십시오. 각 DNS 영역의 클라이언트들이 어디에 배치될 지, 그리고 DNS 서버가 손상되어 쿼리에 응답할 수 없게 될 경우 어떻게 이름을 분해할 것인지에 대해 생각해 보십시오.
- 서버에 대해 인증되지 않은 액세스가 일어나지 않도록 합니다. 영역에 대해 안전한 동적 업데이트만을 허용하고 영역 전송을 확보하도록 허용된 DNS 서버의 목록을 제한합니다.
- Event Viewer 를 이용하여 DNS 로그와 내부 DNS 서버를 모니터링 합니다. 로그와 서버를 모니터링 하면 DNS 서버나 영역 파일에 대해 인증되지 않은 변경 사항을 발견하는데 유용합니다.
- 안전한 동적 업데이트를 이용하여 Active Directory 통합 영역을 구현합니다.

5.동적으로 업데이트된 DNS 영역 보호하기

불안정한 동적 업데이트를 사용할 경우 새로운 보안 위험이 발생합니다. 모든 컴퓨터는 기록을 변경할 수 있으므로 침입자는 영역 데이터를 변경하여 기존 서버로 가장할 수 있게 됩니다. 예를 들어, 웹 서버 web.contoso.com 을 설치하고 동적 업데이트를 이용하여 DNS 에 IP 주소를 등록하는 경우, 침입자는 이차 웹 서버를 설치하고 이 서버의 이름을 web.contoso.com 라 할 수 있으며 동적 업데이트를 이용하여 DNS 기록에 있는 해당 IP 주소를 변경할 수 있습니다. 이런 식으로 침입자는 본래의 웹 서버를 가장하고 보호되어 있는

정보를 확보할 수 있습니다. 이러한 이유로 인해 안전한 동적 업데이트를 구현하는 것이 중요합니다.

서버를 가장하지 못하도록 하려면 Active Directory 통합 영역을 사용하고 그들이 안전하게 동적 업데이트가 되도록 구성합니다. 안전한 동적 업데이트를 이용하면 ACL(access control list)에 지정된 컴퓨터와 사용자들만 영역 내에 개체를 생성하고 변경할 수 있습니다.

자신의 보안 정책이 보다 엄격한 보안을 요구하는 경우, 액세스를 더 강력하게 제한하도록 설정을 변경합니다. 컴퓨터, 그룹 또는 사용자 계정 별로 액세스를 제한하고 영역 내의 전체 DNS 영역에 대한 권한과 개별 DNS 이름에 대한 권한을 할당합니다.

6.DNS 영역 복제 보호하기

영역 복제는 영역 전송을 통해서 일어나거나 Active Directory 복제의 일부로 일어날 수 있습니다. 영역 복제를 보호하지 않을 경우, 컴퓨터의 이름과 IP 주소가 침입자에게 노출될 위험이 있습니다. 다음과 같은 작업을 통해 DNS 영역 복제를 보호할 수 있습니다.

- Active Directory 복제를 이용합니다.
- 인터넷과 같은 공용 네트워크를 통해 전송되는 영역 복제를 암호화합니다.
- 인증된 서버에만 영역 전송을 하도록 제한합니다.

6-1 Active Directory 복제 이용하기

Active Directory 복제 작업의 일부로서 영역을 복제할 경우엔 다음과 같은 보안 이점이 있습니다.

- Active Directory 복제 트래픽은 암호화되므로 영역 복제 트래픽도 자동으로 암호화됩니다.
- 제한된 사람만이 Active Directory 복제에 영향을 줄 수 있습니다. Active Directory 통합 영역을 호스트 하는 DNS 서버는 반드시 도메인 컨트롤러이어야 하며 이는 Active Directory 복제가 도메인 컨트롤러간에만 발생할 수 있다는 것을 의미합니다. 그러므로 도메인 컨트롤러를 관리하도록 인증된 관리자들만이 Active Directory 복제에 영향을 줄 수 있습니다.
- 복제를 수행하는 Active Directory 도메인 컨트롤러는 서로 간에 인증되어 있으며 서로를 가장할 수 없습니다.

참고 Active Directory 통합 영역은 파일 기반의 영역 전송에 비해 안전한 Active Directory 복제의 일부로서 복제되므로 가급적이면 Active Directory 통합 영역을 사용하도록 하십시오.

7.공용 네트워크를 통해 전송되는 복제 트래픽 암호화하기

IPSec 이나 VPN 터널을 이용하여 공용 네트워크를 통해 전송되는 모든 복제 트래픽을 암호화합니다. 공용 네트워크를 통해 전송되는 복제 트래픽을 암호화할 때에는 다음과 같이 하십시오.

- 자신의 서버가 지원할 수 있는 가장 강력한 수준의 암호화나 VPN 터널 인증을 사용합니다.
- Windows Server 2003 Server 라우팅 및 원격 액세스 서비스를 이용하여 IPSec 나 VPN 터널을 생성합니다.

8.인증된 서버에만 영역 전송되도록 제한하기

이차 서버를 가지고 있고 영역 전송을 이용하여 영역 데이터를 복제하는 경우, 자신의 서버가 영역 전송을 수신하도록 인증된 서버를 지정하도록 구성합니다. 이는 침입자가 영역 전송을 이용하여 영역 데이터를 다운로드 하지 못하도록 합니다. Active Directory 통합 영역을 사용하고 있다면 영역 전송을 허용하지 못하도록 서버를 구성합니다.

Windows Server 2003 DNS 를 배포할 때, DNS 서비스를 DHCP 와 WINS 와 같은 다른 Windows Server 2003 서비스와 통합해야 합니다.

G.DNS 와 다른 Windows Server 2003 서비스와 통합하기

1.DNS 와 DHCP 통합하기

Windows Server 2003 DNS 는 DNS 영역의 동적 업데이트를 이용하여 DHCP 를 지원합니다. DNS 배포 시 DHCP 와 DNS 를 통합함으로써, 네트워크 리소스에 DNS 에 저장되어 있는 동적 주소 처리 정보를 제공할 수 있습니다. 이러한 통합을 위해 Windows Server 2003 DHCP 서비스를 이용할 수 있습니다.

RFC 2136 “도메인 이름 시스템의 동적 업데이트”에 규정된 동적 업데이트 표준은 자동으로 DNS 기록을 업데이트합니다. Windows Server 2003 Server 와 Windows 2000 은 모두 동적 업데이트를 지원하며 클라이언트와 DHCP 서버는 그들의 IP 주소가 변경될 때 동적 업데이트를 전송합니다. 모든 클라이언트가 DNS 기록을 변경할 수 있으므로 동적 업데이트 자체는 안전하지 못합니다. 동적 업데이트를 보호하기 위해 Windows Server 2003 서버에서 제공되는 안전한 동적 업데이트를 사용할 수 있습니다. 오래된 기록을 삭제하기 위해 DNS 서버 에이징과 청소 기능을 사용할 수 있습니다.

동적 업데이트는 DHCP 서버가 DHCP 클라이언트를 대신하여 A 와 PTR 리소스 기록을 등록할 수 있도록 합니다. 이 프로세스는 DHCP 클라이언트 FQDN 옵션 81 을 사용하도록 요구합니다. 옵션 81 은 클라이언트가 자신의 FQDN 을 DHCP 서버에 제공하도록 합니다. 클라이언트 역시

서버에 DHCP 클라이언트를 대신하여 DNS 동적 업데이트를 처리하는 방법을 설명하는 지시 사항을 제공합니다.

옵션 81 이 정식 DHCP 클라이언트에 의해 발행될 때, 옵션 81 은 서버가 클라이언트를 대신하여 어떻게 업데이트를 초기화하는지 확인하기 위해 Windows Server 2003 DHCP 서버에 의해 처리되고 분석됩니다. 서버가 DNS 동적 업데이트를 실행하도록 구성되는 경우 다음 작업들 중 한가지를 수행합니다.

- 옵션 81 을 사용하는 클라이언트가 요청할 경우 DHCP 서버는 DNS A 와 PTR 기록을 모두 업데이트합니다.
- 클라이언트가 이 작업을 요청하건 안 하건 상관 없이 DHCP 서버는 DNS A 와 PTR 기록을 업데이트 합니다

또한, 서버에 옵션 81 을 전송할 수 없는 레거시 클라이언트를 대신하여 DHCP 서버는 동적으로 DNS A 와 PTR 기록을 업데이트할 수 있습니다. 클라이언트 임대(lease)가 삭제될 때 DHCP 서버가 클라이언트 A 와 PTR 기록을 폐기하도록 구성할 수도 있습니다. 이는 이러한 기록들을 수동으로 관리할 때 소요되는 시간을 줄여주고 동적 업데이트를 실행하지 못하는 DHCP 클라이언트를 지원합니다. 또한 동적 업데이트는 도메인 컨트롤러가 SRV 기록을 이용하여 동적으로 등록되도록 하여 Active Directory 의 설치 작업을 간소화합니다.

2.DNS 와 WINS 통합하기

이전 버전의 Windows 에서 Windows Server 2003 DNS 로 업그레이드할 때 기존 WINS 인프라를 계속 지원해야 할 수도 있습니다. Windows Server 2003 DNS 는 DNS 서버가 WINS 서버를 DNS 영역 설정으로 쿼리하도록 구성할 수 있도록 하여 기존 WINS 배포를 지원할 수 있도록 합니다.

WINS 는 동적 NetBIOS 이름 분해 기능을 제공합니다. 자신의 조직이 NetBIOS 이름 분해를 위해 WINS 를 사용하는 클라이언트와 프로그램을 지원하는 경우, WINS 를 계속 지원해야 합니다. 자신의 일부 클라이언트가 WINS 에 등록되어 있고 다른 클라이언트들은 자신의 이름을 분해해야 하지만 NetBIOS 이름 분해 기능을 이용할 수 없을 경우, WINS 조회 기능을 이용하여 자신의 DNS 서버가 WINS 이름 공간에 있는 이름을 조회할 수 있도록 할 수 있습니다.

이 기능은 NetBIOS 이름 분해를 요구하는 일부 클라이언트들이 WINS 를 사용할 수 없거나 일부 클라이언트들이 DNS 로 등록할 수 없는 경우(예, Microsoft Windows 95 나 Windows 98 클라이언트)에 특히 유용합니다. WINS 조회 기능은 일부 DNS 서버들이 WINS 조회와 WINS 역방향 조회에 사용될 리소스 기록을 지원하지 않을 경우 사용되는 방법입니다.

3.WINS 조회와 WINS 역방향 조회

WINS 조회를 위해 자신의 DNS 서버를 구성해줌으로써, DNS 가 이름 분해를 위해 WINS 를 쿼리하도록 할 수 있으므로 DNS 클라이언트는 WINS 클라이언트의 이름과 IP 주소를 조회할 수 있습니다. DNS 가 이름 분해를 위해 WINS 를 쿼리하도록 하려면, 인증된 영역에 WINS 조회 기록을 추가합니다. 이러한 영역에 대해 인증된 DNS 서버가 이름에 대한 쿼리를 수신할 때, 이는 인증된 영역을 검사합니다. DNS 서버가 그 이름을 인증된 영역에서 발견하지 못했지만 그 영역에 WINS 조회 기록이 들어있을 경우, DNS 서버는 WINS 서버를 쿼리합니다. 이름이 WINS 에 등록되어 있는 경우, WINS 서버는 관련 기록을 DNS 서버에 반환합니다.

그런 다음 DNS 서버는 본래 DNS 요청에 대한 응답으로 해당 DNS 기록을 컴파일하여 반환합니다. DNS 클라이언트는 클라이언트가 WINS 나 DNS 에 등록되었는지 여부를 반드시 알 필요는 없으며 이들은 WINS 서버를 쿼리할 필요가 없습니다.

WINS 역방향 조회를 위해 자신의 DNS 서버를 구성할 수도 있습니다. 존재하지 않는 PTR 기록을 위해 인증된 DNS 서버를 쿼리하고 인증된 영역에 WINS-R 기록이 들어있을 경우, DNS 서버는 NetBIOS 노드 어댑터 상태 조회를 이용합니다.

참고 내결함성을 위해 WINS 조회 기록에 여러 대의 WINS 서버를 지정할 수 있습니다. Windows 2000 이나 Windows Server 2003 DNS 서비스를 실행하는 서버는 목록에 지정된 순서로 WINS 서버를 검색하여 이름을 찾으려고 합니다.

4.WINS 조회 기능 구성하기

DNS 서버의 써드 파티 구현 제품을 실행하는 컴퓨터들은 WINS 조회나 WINS 역방향 조회에 사용되는 기록을 지원하지 않습니다. 이러한 기록이 들어있는 영역을 호스트 하기 위해 Microsoft 와 써드 파티 DNS 서버를 혼합하여 사용하려는 경우, 써드 파티 DNS 서버에서 데이터 오류가 발생하거나 영역 전송이 실패될 수 있습니다.

이렇게 혼합하여 사용하는 경우, WINS 조회를 이용하여 WINS 에 대한 DNS 조회를 참조하는 특별한 WINS 영역을 생성하고 위임할 수 있습니다. 이 영역은 등록이나 업데이트 작업을 수행하지 않습니다. 그런 다음 모든 DNS 클라이언트가 비정식 쿼리에 WINS 조회 영역 이름을 첨부하도록 구성합니다. 이런 식으로 클라이언트는 DNS 쿼리를 이용하여 DNS 와 WINS 를 동시에 쿼리할 수 있습니다. 관리 작업을 간소화하기 위해, DHCP 나 그룹 정책을 이용하여 클라이언트가 구성 작업을 수행하도록 구성할 수 있습니다.

DHCP 에 관한 추가 정보는 이 책에 들어 있는 “DHCP 배포하기”를 참조하십시오. 그룹 정책에 관한 추가 정보는 이 킷에 들어 있는 관리형 환경 설계하기에서 “그룹 정책 인프라 설계하기”를 참조하십시오.

참고 WINS 영역은 Windows Server 2003 이나 Windows 2000 DNS 서버상에서 호스트 되어야 하며 써드 파티 DNS 서버에 복제되어선 안됩니다. 써드 파티 DNS 서버는 WINS 리소스 기록을 지원하지 않으며 영역을 호스트하지 못할 수도 있습니다.

2) DHCP

A. DHCP 서버 도입의 이점

- 노트북 PC 및 Mobile Device 사용자에게 유연한 사무환경을 제공합니다.

노트북 PC(or Mobile Device)의 사용자의 증가는 지정된 자리 이외에서의 업무 증가를 의미합니다. 다른 부서(다른 Subnet)에서의 협업, 회의실에서의 네트워크 사용, 출장으로 인한 지방 사무실에서의 네트워크 사용 요구에 대처가 가능합니다.

- 네트워크 구성 정보 재구성 요구에 손쉽게 대처할 수 있습니다.

빠르게 변화하는 주변환경 또는 기업의 급속한 발전은 네트워크의 재구성을 요구합니다. 사무실 수의 증가, 조직 개편으로 인한 사무인원의 이동은 네트워크 구성정보의 재 배치를 요구하는 경우로 이어집니다.

- 사내 사용자 PC 의 관리 항목에서 네트워크 구성정보를 생각하지 않습니다

급격히 많아지고 있는 사용자 컴퓨터의 네트워크 구성정보를 개별적으로 점검해주는 것은 많은 시간을 필요로 합니다. 사용자가 많아진 만큼, 컴퓨터를 새로 설치하는 경우, IP 구성정보를 잘못 입력한 경우로, 네트워크 담당자의 도움을 청하는 경우가 많아집니다. 이러한 불필요한 지원이 사라지게 됩니다.

- 서버 또는 네트워크 장비의 재배치가 필요한 경우에도 쉽게 대처가 가능합니다.

DHCP 서버의 도입으로 다음과 같은 단점이 있을 수 있습니다.

- 직원 이외의 사용자에게 사내 네트워크 연결을 쉽게 허용합니다.

기업환경에서 일부 사무실의 환경이, 외부인의 출입이 자유로운 분위기에 젖어 있는 경우, 외부인에게 네트워크의 사용을 쉽게 허용하게 됩니다. 그러나 이러한 환경은 Static IP 를 배포하는 방법만으로 차단하기 어렵다는 점을 생각해야 합니다. 실제로 Static IP 를 사용하는 대부분의 네트워크 환경은, 사용자 컴퓨터 각각의 IP 주소를 관리하기 보다는, 특정 Static IP 영역을 사무공간 전체에 배포해 주는 의미를 갖습니다.

B. 이 문서에서는 다음과 같은 내용을 다룹니다.

- Multiple-subnet 기업환경에서 Windows 2000 컴퓨터이든 Windows 2000 컴퓨터가 아니든 IP Address와 Host 구성을 자동으로 구성한다. 이것은 이 시나리오의 주된 목적입니다.
- 만약 DHCP Server 이용이 불가능한 경우에 대비, 서버 이중화를 통한 fault tolerance 방법을 제공합니다.
- 권한 밖의 Windows 2000 DHCP Server의 사용을 제한 방법을 제공합니다.
- Desktop 컴퓨터와 IP 임대 기간이 다른 Portable 컴퓨터에 IP 임대를 하기 위해 User classes의 기능을 제공합니다.

C. Design Logic 은 목적을 달성하는 방법을 보여줍니다.

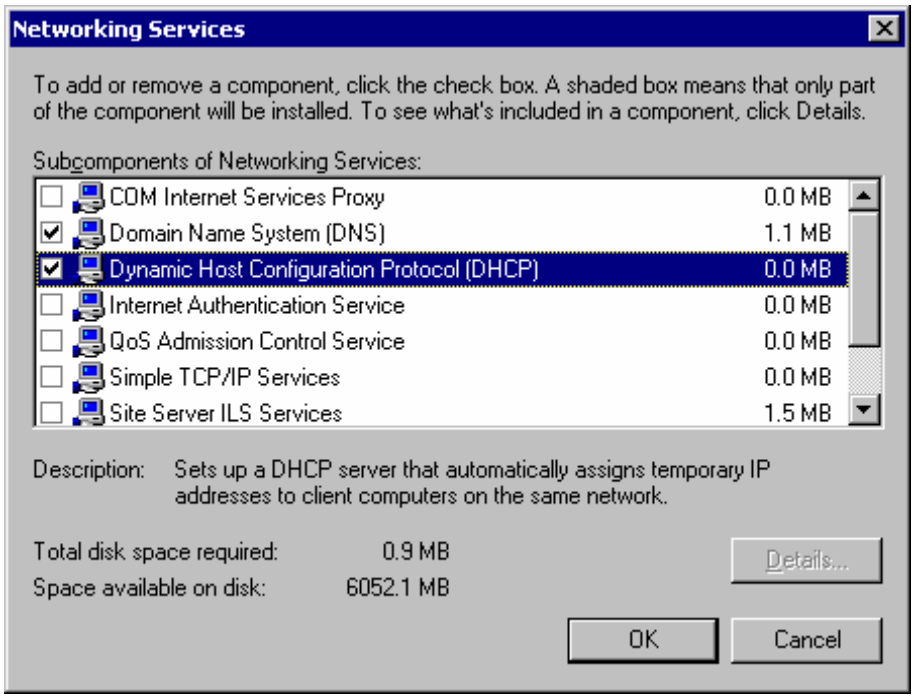
일반적으로, 기업은 DHCP 서버의 구성이 끝난 후에도, IP 주소, Subnet mask 그리고 적당한 Host 정보(DNS, WINS etc)와 같은 네트워크 정보를 자동으로 구성한 Windows 2000-Base 의 컴퓨터와 non-Windows 2000-Base 의 컴퓨터를 포함하는 여러 Subnet 으로 구성된 환경입니다. 또한, 각 Site 에는 네트워크 구성정보를 자동으로 구성하지 않고 수동으로 구성한 컴퓨터 또한 가지고 있습니다.

이것의 의미는 초기에 100% Static IP 로 구성된 기업환경에서 DHCP 서버를 사용한 점진적인 네트워크 자동 구성 환경으로 옮겨갈 수 있음을 의미합니다. 즉, 적용에 따른 부담을 최소화 할 수 있음을 뜻합니다.

우리는 DHCP 서버의 디자인과 이용에 영향을 주는, 기업의 물리적이고 논리적인 네트워크 구성을 충분히 검토해야 합니다. 네트워크 구성정보 자동설정 지역과 범위를 설정하고, DHCP Relay Agent Service 를 지원하는 Router 를 사용하고 있는지, 또는 DHCP Relay Agent Service 기능을 설정할 수 있는 NT 서버가 있는지, WAN Speed 는 충분한지 살펴 보아야 합니다.

1. IP Address and Host 구성을 자동으로 구성

Client PC 의 IP 주소와 Host 구성정보를 자동으로 구성하는 것은 간단한 TCP/IP 표준인 Dynamic Host Configuration Protocol 를 활용함으로써 이루어집니다. 네트워크에서 DHCP-Enable 된 Client PC 에 IP 주소와 다른 관계된 자세한 정보를 동적으로 할당하는 것은 Windows 2000 서버의 DHCP 네트워크 서비스 사용으로 간단히 제공됩니다.



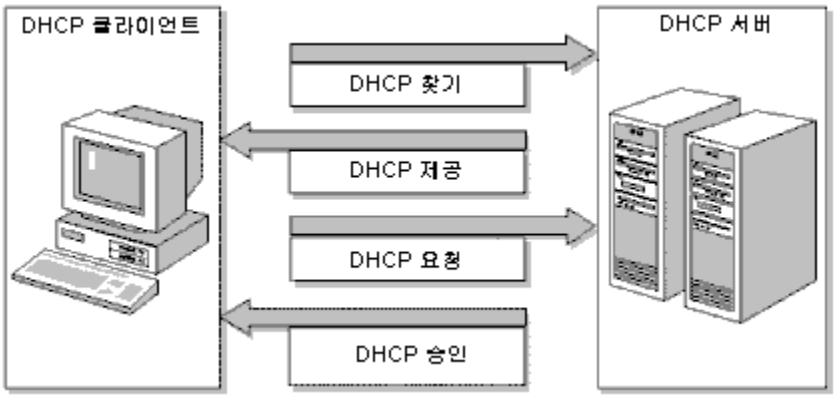
그리고, 이용 가능한 범위에서 몇몇 IP 주소는 DHCP 서버의 자동 구성 영역에서 제외되거나, 미래에 설치되어야 하는 Static Host 를 위해 예약되어야 합니다. 따라서 우리는 각 subnet 에 대해 네트워크 정보, 자동구성을 위해 이용 가능한 IP 주소와 제외주소를 결정해야 합니다.

Subnet	Range of Available IP Addresses	Range of Excluded IP Addresses

Site 에서 DHCP 서버의 위치는 이 솔루션의 이용에서 중요한 요소입니다. 네트워크 디자인에서 견고성을 유지하기 위해, 모든 DHCP 서버는 모든 subnet에 위치시키는 것을 원칙으로 합니다. 그리고 DHCP 서버와 DHCP Client사이의 모든 Router에 DHCP relay를 구성해서, DHCP relay agent를 client subnet에 제공해야 합니다.

Windows 2000 Server와 Cisco IOS version 12.0(10)는 subnet사이의 DHCP relay agent를 서비스를 제공합니다.

Client와 DHCP 서버 사이의 DHCP Packet은 아래와 같습니다.



2. 장애허용(Fault Tolerance)

임의의 site 에서 DHCP 서버로의 연결이 불가능한 것에 대비한, fault tolerance 는 DHCP Client 에 지속된 서비스를 제공합니다. 우리는 확실한 DHCP 서비스를 제공하기 위한 방법을 제공합니다.

- Fault tolerance를 위해 서로 분리된 subnet에, DHCP leases의 첫 번째 서버로써 동작하는 DHCP 서버와 두 번째(대기) 서버로써 동작하는 DHCP 서버를 위치시킵니다.
- 두 서버 사이에 배포 가능한 IP 주소의 범위를 나눕니다. 80 퍼센트의 DHCP Scope을 첫 DHCP 서버에, 20 퍼센트는 두 번째(대기) 서버에 생성시킵니다. (80/20 규칙)
- 보다 확실한 fault tolerance를 제공하기 위해, 대기서버를 실제로 두 대의 서버로 구성합니다. 두 대의 서버는 Cluster Node로써 Cluster 서비스를 실행하며, IP Scope와 다른 DHCP 데이터베이스 정보를 담은 공유디스크를 사용합니다.

일반적인 환경에서, IP 주소 할당과 renewal 에 대한 Client request 는 같은 subnet 에 있는 DHCP 서버에 의해 처리됩니다. 이 DHCP 서버에는 80 퍼센트의 이용 가능한 IP 주소를 사용하게 됩니다.

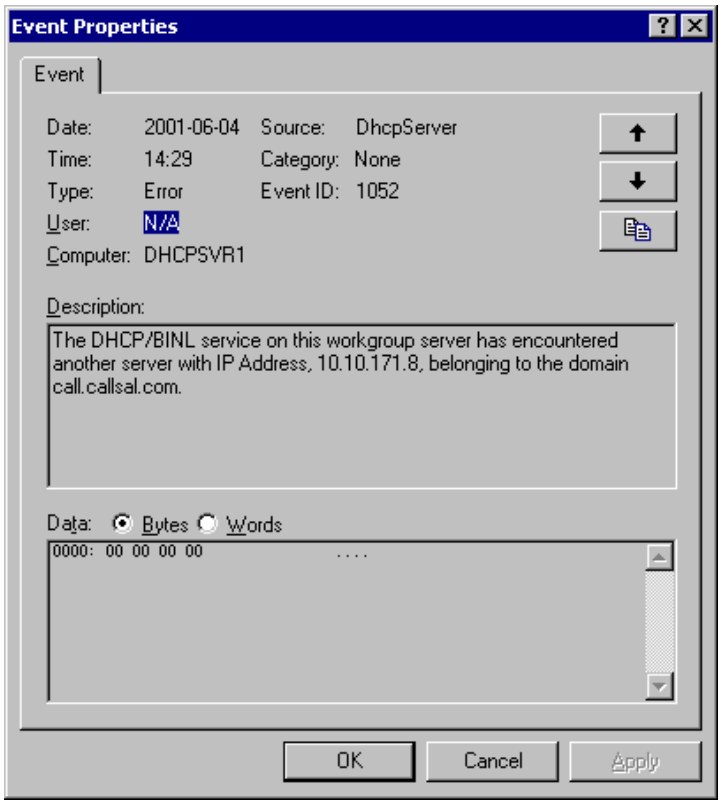
만약 같은 subnet 에 있는 DHCP 서버의 이용이 불가능할 경우, router 에 설정된 DHCP relay agent 서비스에 의해 다른 네트워크에 있는 대기 DHCP 서버로 전달되어 처리됩니다. 이 DHCP 서버에는 20 퍼센트의 이용 가능한 IP 주소가 설정되어 있습니다.

이 대기 서버는 cluster 서버로써 구성되어 있으며, 만약 cluster 의 한 node 가 이용이 불가능할 경우, cluster 서비스에 의해 자동으로 다른 node 에서 DHCP 서비스가 시작됩니다.

위와 같은 방법으로, DHCP 서버가 지역적으로 여러 지역에 설치될 수 있지만, 서버의 중앙 집중화된 설치와 관리를 유지할 수 있습니다. Windows 2000 의 terminal service 는 직접적인 기술지원이 어려운 원격 컴퓨터에 DHCP 서버의 초기 설치를 하는데 사용할 수 있으며, 설치를 끝내 후, DHCP Service 는 Microsoft Management Console(MMC)에 의해 관리할 수 있습니다.

3. 인증 받지 않은 DHCP 서버로부터 보호하기

Windows 2000 Server 의 쉬운 접근성은 네트워크 관리자가 모르는 사이에, 사내 네트워크에 DHCP 서버가 설치될 가능성이 있음을 의미합니다. 모든 Windows 2000-base 의 DHCP 서버는 Active 디렉터리에 등록하여 통합 관리함으로써, 네트워크에 허가되지 않은 Windows 2000-base DHCP 서버의 사용을 차단합니다. 새로 설치된 DHCP 서비스는, 네트워크에 이미 DHCP 서비스가 제공되는 경우, 아래와 같이 이벤트 로그에 기록하고 서비스를 시작하지 않습니다.



4. 사용자 클래스 지원

DHCP 서버를 사용할 때, 또 다른 요구는 보통 IP 임대기간을 짧게 사용하는 Portable PC 와 임대기간이 상대적을 긴 Desktop PC 에 의해 요청되는, DHCP request 을 다르게 처리하는 기능입니다. 이러한 요구 사항은 DHCP 서버의 옵션에서 user classes 의 사용으로 가능합니다. 부가적으로 Windows 2000 컴퓨터는 ipconfig /setclassid 명령을 사용하여 client 컴퓨터에 DHCP user class ID 설정이 가능합니다. Non-windows 2000 base client 는 사용자에게 이 기능을 제공하지 않기 때문에, 각 site 에 대한 scope option 을 사용해야 한다.

5. 시험운영(Deployment Test)

5-1 각 Subnet 에 대해 이용 가능한 IP 주소와 제외주소를 결정해야 합니다.

Subnet	Range of Available IP Addresses	Range of Excluded IP Addresses
10.10.171.0/254	10.10.171.23 – 10.10.171.27	

- Server가 위치하는 Local Subnet(10.10.10.X)을 먼저 결정합니다.
- 네트워크 구성정보의 자동설정 Subnet은 지리적으로 가까운 곳부터, 먼 곳으로 작업을 진행합니다.
- 환경이 Static 네트워크 구성에서 100% DHCP 환경이 아닌, Mixed (ex. Static Client 10% + DHCP Client 90%) 환경으로 전환하는 것임을 생각해야 합니다.
- 일반적으로 서버 및 Router 등의 네트워크 구성은 Static IP로 구성하고, Client PC 에 대해서만 자동구성 영역으로 할당합니다.

5-2 DHCP Scope에 대한 옵션

네트워크 구성 정보를 자동으로 구성하기 위해 사용되는 아래 내용을 결정합니다.

003	Router 10.10.10.1	Router의 IP 주소
006	DNS Servers 10.10.10.2 10.10.10.3	DNS 서버의 IP 주소
015	DNS Domain Name microsoft.co.kr	DNS domain name for client resolution
044	WINS/NBNS servers 10.10.10.26 10.10.10.25	WINS 서버의 IP주소
046	WINS/NBT node Type 1 = B node (Broadcast) 2 = P node (Peer) 4 = M node (Mixed) 8 = H node (Hybrid)	
047	NetBIOS Scope ID	같은 Scope ID를 사용하는 다른 NetBIOS hosts 와만 통신한다.

5-3 DHCP 서버의 수량과 방법을 결정합니다.

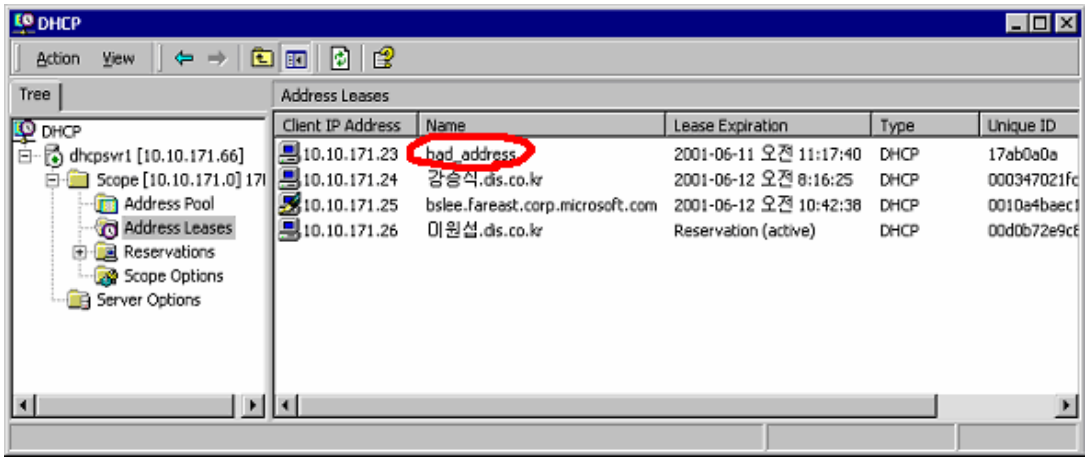
Computer Name	IP Addresses

DHCPSVR1.microsoft.com.co.kr	10.10.10.1

- WAN 의 신뢰성이 낮고, 사용자 수에 비해 Network Bandwidth가 불충분한 경우에만, DHCP 서버를 별도로 구성하는 것을 고려합니다.
- WAN 의 신뢰성이 높지만, 사용자 수가 적은 경우, Router 또는 NT(W2K)의 DHCP Server Relay Agent 서비스의 사용을 고려합니다.
- 본사에 중앙집중형식으로 DHCP서버를 구성하는 경우 DHCP Server의 Cluster Solution을 도입을 검토합니다.

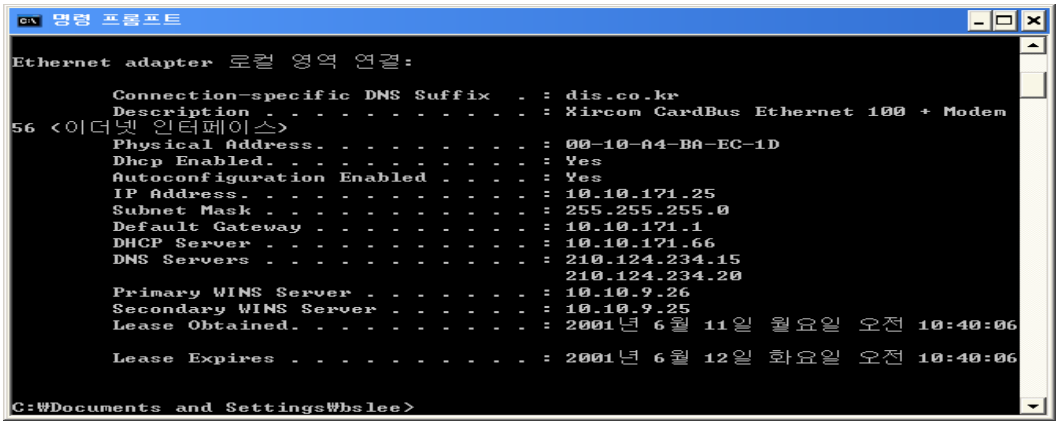
5-4 DHCP 서버와 같은 Subnet에 있는 Client PC가 네트워크 구성정보를 자동으로 구성하는 경우에 대해 검증합니다.

- DHCP 서버에서 네트워크 구성정보가 정상적으로 배포되는지 확인합니다



* bad_address는 이미 사용중인 Static IP가 있음을 뜻합니다. DHCP 서버는 이미 사용중인 주소는 bad_address로 표시하고, 같은 IP를 배포하지 않습니다.

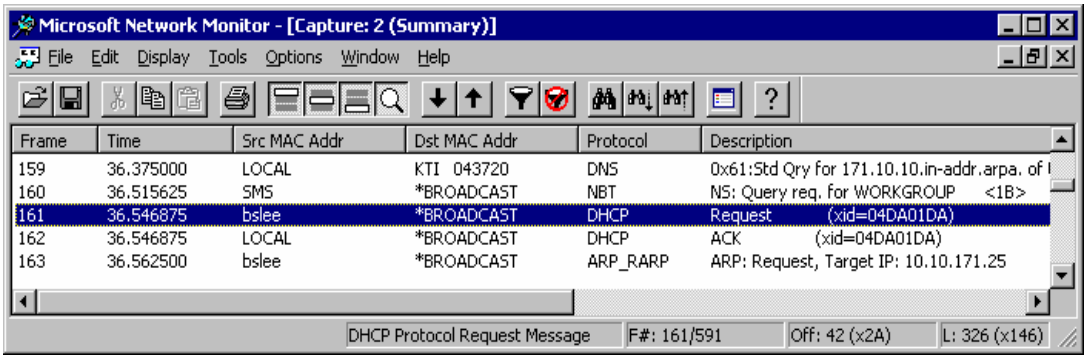
- Client PC의 네트워크 자동 구성정보가 정상인지 확인합니다.



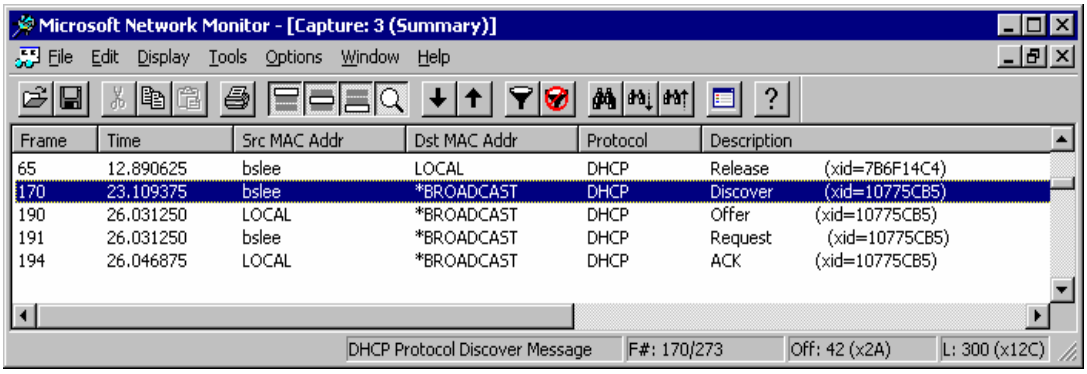
IP 주소, Default Gateway, DHCP server, DNS Server Lease 기간 등이 정상인지 확인

- 필요한 경우 네트워크 Packet를 Capture해 정상적으로 동작하는 지 검증합니다.

이미 네트워크 구성정보가 자동 구성된 PC가 Rebooting 하는 경우



Command Prompt에서 ipconfig /release & ipconfig /renew을 실행했을 경우
(또는 새로는 PC가 네트워크에 처음 접속하는 경우)



5-5 DHCP 서버가 Router로 분리된 다른 네트워크의 Client PC가 네트워크 구성정보를 자동으로 구성하는 경우에 대해 검증합니다.

1) 테스트 하고자 하는 네트워크의 Scope Range를 DHCP 서버에 설정합니다.
2) 네트워크 장비(Router & Power HUB)의 기본설정상태에서, Client PC가 DHCP 서버로부터 네트워크 구성정보를 받을 수 있는지 점검합니다
3) 구성된 네트워크 장비에서 BOOTP/ DHCP Relay Service를 Enable 합니다.
4) Client PC가 DHCP 서버로부터 네트워크 구성정보를 받는지 점검합니다.

```
The following part was recorded during router configuration:

lclmlab>enable
Password:
lclmlab#
lclmlab#write terminal
###
Current configuration:
!
version 10.2
```

```
!
hostname lclmlab
!
enable password lclmlab
!
!
interface Ethernet0
ip address 130.20.0.1 255.255.0.0
media-type 10BaseT
no mop enabled
!
interface Ethernet1
ip address 130.30.0.1 255.255.0.0
media-type 10BaseT
no mop enabled
!
interface Fddi0
no ip address
no keepalive
.
.
.

lclmlab#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.   End with CNTL/Z.
lclmlab(config)#ip forward-protocol udp 67
lclmlab(config)#interface ethernet 0
lclmlab(config-if)#ip helper-address 130.30.255.255
lclmlab(config-if)#interface ethernet 1
lclmlab(config-if)#ip helper-address 130.20.255.255
lclmlab(config-if)#^Z
lclmlab#write memory
####[OK]
lclmlab#write terminal
###
Current configuration:
!
```

```
version 10.2
!
hostname lclmlab
!
enable password lclmlab
!
!
interface Ethernet0
ip address 130.20.0.1 255.255.0.0
ip helper-address 130.30.255.255
media-type 10BaseT
no mop enabled
!
interface Ethernet1
ip address 130.30.0.1 255.255.0.0
ip helper-address 130.20.255.255
media-type 10BaseT
no mop enabled
!
interface Fddi0

lclmlab#
```

* Static IP 에서 자동구성으로 변경이 필요한 네트워크를 선정하여 하나씩 하나씩, 서서히 전환합니다.

6. 권고사항

지금까지의 테스트 결과에 의해 하드웨어, 소프트웨어에 대해, 아래와 같이 사용할 것을 권고합니다.

- DHCP Server 는 Windows server 2003 에서 제공하는 것을 사용합니다.
- DHCP Server 를 중앙집중식으로 구성하는 경우 Cluster 로 구성합니다.
- WAN 의 신뢰성이 높지만, 사용자 수가 적은 경우 DHCP Relay Agent 서비스를 enable 하여, 중앙 집중식으로 구성한 DHCP 서버를 사용합니다.
- Branch Office 가 WAN 의 신뢰성이 낮고, 사용자 수가 많고 Windows 2000 서버(프린터, 파일서버용)를 사용하고 있는 경우, DHCP 서버를 별도 설치하여 사용합니다 (80:20 Rule 적용). 관리는 MMC 를 사용하여

중앙에서 관리가 가능합니다. 물론 Router 의 BOOTP/ DHCP Relay Agent 서비스 역시 enable 합니다.

- 모든 네트워크의 분리는 BOOTP/ DHCP Relay Agent 서비스(RFC1542)를 enable 할 수 있는 Router 장비를 사용하도록 권고합니다.
- specifications for clustered DHCP server / 10,000 명

Minimum CPU	Minimum RAM	EDS/cluster	RAID Configuration
Dual P3 500Mhz	256 Mb	4 x 4GB	2 X RAID 1 4GB

http://www.microsoft.com/TechNet/showcase/deploy/w2kclust.asp 를 참조하세요. 이 자료에는 five DHCP servers managed roughly 80,000 address leases자의 내용 있습니다. 이것을 기준으로 생각하면 대략 1 대당 10,000 정도까지 가능합니다.

3) WINS

A.WINS 조회 사용

DNS 서버 서비스는 DNS 네임스페이스에서 이름을 찾지 못한 경우 WINS(Windows 인터넷 이름 서비스) 서버를 사용하여 WINS 에서 관리하는 NetBIOS 네임스페이스를 확인하고 이름을 조회할 수 있게 합니다.

WINS 조회 통합을 사용하려면 특수한 두 개의 RR(리소스 레코드)인 WINS 및 WINS-R 리소스 레코드를 사용할 수 있게 설정하고 영역에 추가해야 합니다. WINS RR 을 사용하면 영역에서 일치하는 호스트(A) RR 을 찾을 수 없는 DNS 쿼리는 WINS RR 에 구성되어 있는 WINS 서버로 전달됩니다. 역방향 조회 영역의 경우 WINS-R RR 을 사용할 수 있게 설정하여 역방향 in-addr.arpa 도메인에서 응답할 수 없는 역방향 쿼리에 대해 추가로 이름을 확인하는 유사한 이점을 제공할 수 있습니다.

WINS 조회가 필요한 좋은 예는 DNS 이름 확인만 사용하는 UNIX 클라이언트와 NetBIOS 이름이 필요한 이전 버전 Microsoft 클라이언트로 구성된 혼합 모드 클라이언트 환경을 사용하는 경우입니다. 이러한 환경에서 WINS 조회는 UNIX DNS 클라이언트가 DNS 호스트 이름 확인을 WINS 에서 관리하는 NetBIOS 네임스페이스로 확장하여 WINS 클라이언트를 찾을 수 있게 방법을 제공합니다.

WINS 조회 통합 기능은 Windows DNS 서버에서만 지원합니다. Windows DNS 서버와 다른 DNS 서버를 혼합 사용하여 영역을 호스팅하면 WINS 조회 레코드를 사용할 때 모든 주 영역에 **이 레코드 복제 안 함** 확인란 옵션을 사용할 수 있도록 설정해야 합니다. 이렇게 하면 WINS 조회 레코드를 지원하지 않거나 인식하지 못하는 다른 DNS 서버로 영역을 전송할 때 이 레코드가 포함되지 않습니다. 로컬 서버에서만 사용되도록 WINS 조회 레코드를 사용할 수

있게 설정하지 않으면 영역을 복제하는 다른 DNS 서버 구현을 실행 중인 서버에서 영역 전송에 실패하거나 데이터 오류가 발생할 수 있습니다.

아래 섹션에서 WINS 조회 상호 운용성 고려 사항을 기술하고 아래와 같은 사항을 설명합니다.

- WINS 및 WINS-R 레코드에 사용하기 위해 캐시 TTL(Time-To-Live) 및 조회 시간 제한 값의 구성 방법
- DNS 서버 서비스에서 만든 영역 파일에 사용되는 WINS 및 WINS-R 리소스 레코드 형식

B. WINS 조회 상호 운용성

일반적으로 WINS 조회는 Windows DNS 서버를 사용할 때 가장 예측 가능하고 좋은 결과를 제공하며 Windows DNS 서버에서만 직접 사용할 수 있습니다. 하지만 다른 DNS 서버가 배치되어 있는 경우에도 상호 운용 솔루션으로 WINS 조회를 사용하고 그 이점을 얻을 수 있는 방법이 있습니다.

예를 들어 새 WINS 조회 사용 영역을 호스트 하는 Windows DNS 서버 추가를 고려하십시오. 영역을 만들고 명명할 때는 기존 DNS 도메인 네임스페이스에 추가되어 있고 DNS 네임스페이스에 추가된 WINS 에 특정한 조회만을 위해 사용되는 하위 도메인을 사용합니다.

예를 들어 example.microsoft.com 에 영역을 만들고 이 영역을 wins.example.microsoft.com 으로 명명합니다. 그런 다음 새로 만든 WINS 조회 영역을 다른 이전 DNS 영역에서 찾을 수 없는 이름을 가진 모든 WINS 사용 컴퓨터의 루트 영역으로 사용할 수 있습니다.

WINS 조회 영역을 사용하려면 클라이언트를 위한 DNS 접미사 검색 목록에 도메인 이름(wins.example.microsoft.com)을 지정해야 합니다. 접미사 목록은 클라이언트 연결을 위한 TCP/IP 속성의 일부분으로 구성할 수 있고 수동으로, DHCP 를 통해 또는 그룹 정책을 사용하여 업데이트할 수 있습니다. 도메인 접미사 목록에 WINS 조회 영역의 이름만 있으면 이전 영역에서 확인할 수 없는 모든 DNS 이름을 WINS 조회 하위 도메인을 사용하여 확인할 수 있습니다.

이름을 찾을 수 없는 경우 정상 조건에서는 다른 DNS 서버가 WINS 사용 영역을 호스팅하는 Windows DNS 서버로 재귀 쿼리를 보냅니다. 쿼리된 호스트 이름이 WINS 데이터베이스에 있는 NetBIOS 컴퓨터 이름과 일치하면 해당 WINS 데이터에 매핑되어 있는 IP 주소로 이름이 확인됩니다.

예에서 WINS 사용 영역은 WINS 조회에만 사용되기 때문에 다른 리소스 레코드를 추가할 필요가 없습니다. 일반적으로 WINS 레코드는 모든 정방향 조회 영역에 추가할 수 있습니다.

WINS 조회만을 위한 특정 하위 도메인을 사용하고 이름 확인과 검색에 사용될 정적 DNS 접미사 목록을 제공하면 서로 다른 FQDN 에 대한 DNS 쿼리 결과가 같은 WINS 클라이언트 이름과 IP 주소로 확인되는 비정상 상황이 발생하지 않게 할 수 있습니다. 네임스페이스의 각 수준에 많은 영역을 추가하여 구성하고 이들 각 영역에 WINS 조회 통합 사용을 설정하면 그와 같은 비정상 상황이 쉽게 발생할 수 있습니다.

예를 들어 WINS 조회를 사용하도록 구성된 두 영역이 있다고 가정합니다. 두 영역 모두 아래와 같은 DNS 도메인 이름에서 시작됩니다.

example1.microsoft.com.
example2.microsoft.com.

이 구성에서 이름이 HOST-A 인 WINS 클라이언트는 의도와 달리 아래 FQDN 중 하나로 확인될 수 있습니다.

host-a.example1.microsoft.com.
host-a.example2.microsoft.com.

C. WINS 리소스 레코드

설명: WINS 정방향 조회 리소스 레코드입니다. 영역에서 이름을 찾지 못한 DNS 쿼리를 이 레코드에 나열되고 구성되어 있는 WINS 서버로 보내어 추가 이름 확인을 제공하기 위해 영역에 사용됩니다. 이 레코드를 사용하는 경우 WINS 레코드는 영역 내 최상위 수준에만 적용되고 영역에 사용된 하위 도메인에는 적용되지 않습니다. 아래는 WINS RR에 사용되는 필드 중 일부입니다.

- *owner* 이 레코드의 소유자 도메인을 나타내며 현재 도메인과 영역 근원이 같음을 나타내도록 항상 "@"로 설정해야 합니다.
- *class* 이 레코드의 클래스를 나타내며, Windows Server 2003 을 실행하는 DNS 서버에 인터넷 클래스만 지원됨을 나타내도록 항상 "IN"으로 설정해야 합니다.
- LOCAL 이 필드가 사용되면 WINS RR 이 DNS 서버에서 로컬로만 사용되며 다른 DNS 서버로 영역을 복제할 때 이 RR 이 포함되지 않습니다. 이 필드는 DNS 콘솔에서 WINS 조회를 구성할 때 **이 레코드 복제 안 함** 확인란의 선택 여부에 해당합니다. 이 확인란의 선택을 취소하면 레코드를 영역에 쓸 때 이 필드가 포함되지 않습니다.
- *lookup_timeout* 이 레코드에 적용될 조회 시간 제한 값입니다. 자세한 내용은 WINS 조회의 고급 매개 변수를 참조하십시오.
- *cache_timeout* 이 레코드에 적용될 캐시 시간 제한 값입니다. 자세한 내용은 WINS 조회의 고급 매개 변수를 참조하십시오.
- *wins_ip_addresses* WINS 서버의 IP 주소 하나 이상을 지정하는 데 사용됩니다. 유효한 WINS 서버 IP 주소를 최소한 하나 지정해야 합니다.

구

문: *owner class* **WINS** [LOCAL] [L*lookup_timeout*] [Ccache_timeout] wins_ip_addresses

예:

@ IN WINS 10.0.0.1

@ IN WINS LOCAL L1 C10 10.10.10.1 10.10.10.2 10.10.10.3

참고

- 위의 예제 WINS 레코드에서 영역 루트는 현재 원본으로 가정합니다.

D. WINS-R 리소스 레코드

설명: WINS 역방향 조회 리소스 레코드입니다. 영역에서 찾지 못한 역방향 쿼리에 대해 쿼리된 IP 주소로 보낸 NetBIOS 어댑터 노드 상태 쿼리를 사용하여 추가로 이름 확인을 제공하기 위해 역방향 조회 영역에 사용됩니다. 이 레코드를 사용할 때 성공적인 역방향 조회가 발생하면 NetBIOS 컴퓨터 이름에 추가될 부모 도메인을 지정해야 합니다.
WINS-R 레코드에 사용되는 다른 필드는 위의 WINS 정방향 조회 레코드에서 설명한 것과 같습니다.

구문: *owner class* **WINS** [LOCAL] [L*lookup_timeout*] [Ccache_timeout] *Domain_to_append_to_returned_NetBIOS_names*

예:

@ IN WINS-R LOCAL L1 C10 example.microsoft.com.

@ IN WINS-R wins.example.microsoft.com.

참고

- 위의 예제 WINS-R 레코드에서 영역 루트는 현재 원본으로 가정합니다.

E. WINS 조회 고급 매개 변수

시간 제한과 관련된 아래 두 고급 매개 변수는 WINS 및 WINS-R 레코드에 사용됩니다.

- 캐시 시간 제한 값은 WINS 조회에 반환된 정보를 DNS 서버가 얼마 동안 캐시해야 하는지 나타냅니다. 기본적으로 이 값은 15 분으로 설정됩니다.
- 조회 시간 제한 값은 DNS 서버 서비스에서 수행하는 WINS 조회를 만료하기 전까지의 대기 시간을 지정합니다. 기본적으로 이 값은 2 초로 설정됩니다.

이 매개 변수는 영역을 구성할 때 영역 속성 대화 상자에서 **고급** 단추를 사용하여 구성합니다. 이 단추는 구성하는 영역이 정방향 조회 영역인지 역방향 조회 영역인지에 따라 WINS 또는 WINS-R 탭에 나타납니다.

WINS 또는 WINS-R 리소스 레코드를 사용하는 경우 영역의 SOA 레코드에 설정된 최소 TTL(Time-To-Live)은 이 레코드에 사용되는 기본 TTL 이 아니라는 점에 유의해야 합니다. 대신 WINS 조회에서 IP 주소나 호스트 이름이 확인되면 해당 정보는 WINS 캐시 시간 제한 값에 지정된 기간 동안 DNS 서버에 캐싱됩니다. 그런 다음 이 주소가 다른 DNS 서버로 전달되면 WINS 캐시 시간 제한 값 TTL 이 전송됩니다. WINS 데이터가 자주 변경되지 않는 경우에는 15 분인 기본 TTL 을 더 높일 수 있습니다.

참고

- 영역이 WINS 조회를 위해 구성되어 있으면 해당 영역에 대해 권한이 있는 모든 DNS 서버에 WINS 조회 능력이 있어야 하며 그렇지 않으면 조회 작업이 연속으로 수행되지 않습니다.
- WINS 및 WINS-R RR 이 다른 DNS 로 복제되지 않게 선택할 수 있기 때문에 WINS 조회가 사용되는 영역의 각 보조 서버에서 선택적으로 WINS 조회를 사용하고 구성할 수 있습니다. 영역의 주 서버에만 구성되는 다른 리소스 레코드 종류에서는 표준으로 이렇게 할 수 없습니다.

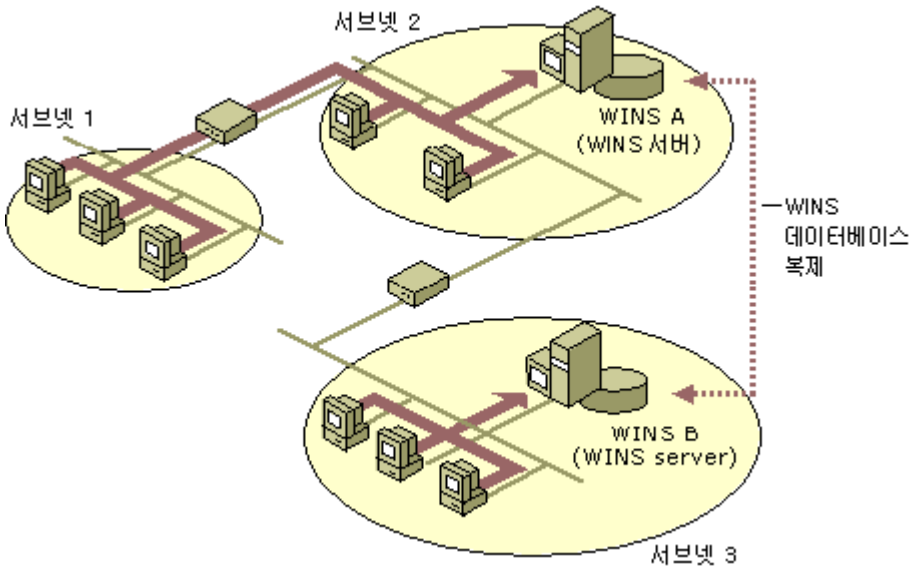
F. WINS 서버

WINS는 두 가지 주요 구성 요소인 WINS 서버와 WINS 클라이언트로 구성됩니다.

WINS 서버는 WINS 클라이언트의 이름 등록 요청을 처리하며 해당 이름과 IP 주소를 등록하고 클라이언트에서 제출한 NetBIOS 이름 쿼리에 응답하여 서버 데이터베이스에 해당 이름이 있으면 쿼리된 이름의 IP 주소를 반환합니다.

또한 아래 그림에서 설명된 대로 WINS 서버는 IP 주소에 대한 NetBIOS 컴퓨터 이름 매핑을 포함하는 자신의 데이터베이스 내용을 다른 WINS 서버에 복제할 수 있습니다. WINS 를 사용하는 클라이언트 컴퓨터(예: Subnet 1 이나 Subnet 2 의 워크스테이션 컴퓨터)가 네트워크에서 시작되면 자신의 컴퓨터 이름과 IP 주소를 등록하도록 요청하면서 구성된 주 WINS 서버인

WINS-A 로 직접 보냅니다. WINS-A 는 이 클라이언트들을 등록하는 서버이기 때문에 WINS 에서 해당 클라이언트의 레코드에 대한 소유자라고 합니다.



이 예제에서 WINS-A 서버에는 로컬 클라이언트(상주하는 Subnet 2 의 클라이언트)와 원격 클라이언트(Subnet 1 의 라우터를 통해 찾게 되는 클라이언트) 양쪽으로 등록되는 클라이언트가 있습니다. 둘째 WINS 서버인 WINS-B 는 Subnet 3 에 있으며 같은 서브넷에서 등록되는 로컬 클라이언트의 매핑만 소유합니다. WINS-A 와 WINS-B 는 나중에 자신의 데이터베이스 복제를 완료하여 세 서브넷 모두의 클라이언트 레코드가 두 서버의 WINS 데이터베이스에 있게 됩니다.

G. 주/보조 WINS 서버

WINS 서버는 주 WINS 서버와 보조 WINS 서버 중 어느 하나로 클라이언트에서 사용합니다.

WINS 에서 모든 기능적 목적이 동일하므로 주 WINS 서버와 보조 WINS 서버 간의 차이는 서버 방식에 근거하지 않습니다. 사용할 WINS 서버를 여러 개 제공했을 때 WINS 서버 목록을 구별하고 정렬하는 클라이언트에서 두드러진 특색이 나타납니다.

대부분의 경우 클라이언트는 모든 NetBIOS 이름 서비스 기능(이름 등록, 이름 갱신, 이름 등록 해제 및 이름 쿼리와 확인)을 제공받기 위해 주 WINS 서버에 접속합니다. 보조 WINS 서버가 사용되는 유일한 경우는 주 WINS 서버가 아래 경우 중 어느 하나에 해당되는 경우입니다.

a. 서비스 요청이 있을 때 네트워크에서 사용할 수 없는 경우
b. 클라이언트 이름을 확인할 수 없는 경우(이름 쿼리와 관련)

주 WINS 서버에 따른 실패인 경우 클라이언트는 같은 서비스 기능을 보조 WINS 서버에 요청합니다. 셋 이상의 WINS 서버가 클라이언트에 구성되어 있으면 목록이 소멸되거나 보조 WINS 서버 중 하나가 해당 요청의 처리와 응답에 성공할 때까지 추가된 WINS 서버들이 시도됩니다. 보조 WINS 서버가 사용된 후 클라이언트는 앞으로의 서비스 요청을 위해 주기적으로 주 WINS 서버로 다시 전환하려고 시도합니다.

최신의 WINS 클라이언트(Windows XP 및 Windows 2000)인 경우 최대 12 개까지의 보조 WINS 서버를 포함하는 목록이 TCP/IP 속성을 통해 수동으로 또는 DHCP 옵션 유형 44 를 사용하여 목록을 제공하는 DHCP 에 의해 동적으로 구성될 수 있습니다. 이 기능은 이동 클라이언트가 매우 많이 있고 NetBIOS 기반 리소스와 서비스가 자주 사용되는 환경에서 유용합니다. 이런 유형의 환경에서는 집중성 문제로 인해 WINS 데이터베이스가 WINS 서버의 네트워크 전반에 걸쳐서 일관되지 않을 수 있기 때문에 클라이언트에서 셋 이상의 WINS 서버를 조회할 수 있는 환경이 바람직합니다.

그러나 이 옵션은 추가된 WINS 서버를 목록에 나타냄으로써 내결함성 추가의 실제 이익과 관련하여 절충되기 때문에 필요 없이 지나치게 사용되지 않아야 합니다. 이 기능의 효용은 목록에 추가된 각 WINS 서버의 WINS 에서 쿼리 요청을 완전히 처리하는 시간이 결과 획득에 걸리는 시간보다 점차적으로 더 길어진다는 사실과 비교해야 합니다. 예를 들어 실패하기 전에 WINS 클라이언트가 셋 이상의 WINS 서버에 시도하면 로컬 Hosts 파일 검색이나 DNS 서버 쿼리와 같은 다른 확인 방법이 시도되기 전에 이름 쿼리의 처리를 실질적으로 지연시킬 수 있습니다.

H. WINS 클라이언트

WINS 클라이언트가 시작하거나 네트워크에 참가할 때 WINS 클라이언트는 WINS 서버에 이름 등록을 시도합니다. 그 이후에는 필요에 따라 클라이언트에서 WINS 서버를 쿼리하여 원격 이름을 확인합니다.

WINS 를 사용하는 클라이언트는 WINS 서버를 직접 사용하도록 구성될 수 있는 컴퓨터입니다. 일반적으로 대부분의 WINS 클라이언트에는 네트워크에서 사용하기 위해 등록해야 하는 NetBIOS 이름이 여러 개 있습니다. 이 이름은 각 컴퓨터에서 여러 방식으로 네트워크상의 다른 컴퓨터와 통신할 수 있는 Messenger 서비스나 Workstation 서비스와 같은 다양한 종류의 네트워크 서비스를 게시하는 데 사용됩니다.

Microsoft 는 아래 플랫폼을 실행하는 WINS 클라이언트를 지원합니다.

- Windows Server 2003, Datacenter Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Standard Edition

- Windows Server 2003, Web Edition
- Windows Server 2003, Datacenter Edition 64 비트 버전
- Windows Server 2003, Enterprise Edition 64 비트 버전
- Windows XP Professional
- Windows XP Home Edition
- Windows XP 64 비트 Edition
- Windows Millennium Edition
- Windows 2000 Datacenter Server
- Windows 2000 Advanced Server
- Windows 2000 Server
- Windows 2000 Professional
- Windows NT Server
- Windows NT Workstation
- Windows 98
- Windows 95
- Windows for Workgroups
- Microsoft LAN Manager
- MS-DOS 클라이언트
- OS/2 클라이언트
- Linux 클라이언트 및 UNIX 클라이언트(Samba 설치됨)

WINS 를 사용하는 클라이언트는 아래 작업을 위해 WINS 서버와 통신합니다.

- 클라이언트 이름을 WINS 데이터베이스에 등록합니다.
- WINS 데이터베이스에 있는 클라이언트 이름을 갱신합니다.
- WINS 데이터베이스에서 클라이언트 이름을 해제합니다.
- 사용자 이름, NetBIOS 이름, DNS 이름 및 IP 주소에 대한 매핑을 WINS 데이터베이스로부터 획득하여 이름을 확인합니다.

I. WINS 서버 역할: WINS 서버 구성

WINS(Windows 인터넷 이름 서비스) 서버는 IP 주소를 컴퓨터 이름(NetBIOS 이름)에 동적으로 매핑합니다. 이렇게 하면 사용자는 IP 주소 대신 컴퓨터 이름을 사용하여 리소스에 액세스할 수 있습니다. 컴퓨터에서 네트워크에 있는 다른 컴퓨터의 이름과 IP 주소를 추적하려면 이 컴퓨터를 WINS 서버로 구성합니다.

여기에서는 WINS 서버를 구성하는 기본 단계를 설명합니다. 기본적인 WINS 서버 설정이 끝나면 WINS 서버 용도에 따라 추가 구성 작업을 완료할 수 있습니다.

이 항목에서는 다음 내용을 설명합니다.

  - 시작하기 전에
- WINS 서버 구성
- 다음 단계: 추가 작업 완료

1. 시작하기 전에

컴퓨터를 WINS 서버로 구성하기 전에 다음을 확인합니다.

- NetBIOS 이름, WINS 서버, WINS 클라이언트, 복제 파트너 등의 WINS 개념을 잘 알고 있습니다.
- 운영 체제가 올바르게 구성되어 있습니다. Windows Server 2003 제품군에서 WINS 는 해당 운영 체제와 서비스의 구성을 따릅니다. Windows Server 2003 제품군의 제품을 새로 설치한 경우 기본 서비스 설정을 사용할 수 있습니다. 이런 경우에는 추가 조치가 필요 없습니다. Windows Server 2003 제품군의 제품으로 업그레이드한 경우 또는 최상의 성능 및 보안을 위해 서비스가 올바르게 구성되어 있는지 확인하려는 경우에는 서비스의 기본 설정의 표를 사용하여 서비스 설정을 검토합니다.
- 설치할 WINS 서버 수와 네트워크에서 각 서버의 위치를 알고 있습니다. WINS 서버 역할을 추가할 때 컴퓨터 이름과 IP 주소에 대한 데이터베이스를 유지하도록 이 서버를 구성합니다. 대규모 네트워크에서는 클라이언트 컴퓨터가 항상 하나 이상의 WINS 서버에 액세스할 수 있도록 하려면 WINS 서버 역할을 다른 서버에 추가해야 합니다.
- 이 컴퓨터는 고정 IP 주소를 가지고 있습니다.
- 기존의 모든 디스크 볼륨은 NTFS 파일 시스템을 사용합니다. FAT32 볼륨은 안전하지 않으며 파일과 폴더 압축, 디스크 할당량, 파일 암호화 또는 개별 파일 사용 권한을 지원하지 않습니다.

2. WINS 서버 구성

WINS 서버를 구성하려면 다음 중 하나를 수행하여 서버 구성 마법사를 시작합니다.

- 사용자 서버 관리에서 **역할 추가/제거**를 클릭합니다. 기본적으로 사용자 서버 관리는 로그온하면 자동으로 시작됩니다. 서버 관리를 열려면 **시작**, **제어판**을 차례로 클릭하고 **관리 도구**를 두 번 클릭한 다음 **사용자 서버 관리**를 두 번 클릭합니다.
- 서버 구성 마법사를 열려면 **시작**, **제어판**을 차례로 클릭하고 **관리 도구**를 두 번 클릭한 다음 **서버 구성 마법사**를 두 번 클릭합니다.

서버 역할 페이지에서 **WINS 서버**를 클릭한 후 **다음**을 클릭합니다.

- 선택 사항 요약
- 서버 구성 마법사 완료
- WINS 서버 역할 제거

1. 선택 사항 요약

선택 사항 요약 페이지에서 선택한 옵션을 보고 확인합니다. 이전 페이지에서 WINS 서버를 선택한 경우 다음 사항이 나타납니다.

- **WINS 설치**

선택 사항 요약 페이지에 표시된 선택 사항을 적용하려면 다음을 클릭합니다. 다음을 클릭하면 Windows 구성 요소 마법사의 구성 요소 구성 중 페이지가 표시된 다음 자동으로 닫힙니다. 이 페이지에서는 뒤로 또는 다음을 클릭할 수 없습니다. 서버 구성 마법사가 WINS 서버 서비스를 설치합니다. 다른 여러 서비스와 달리 WINS 서비스는 관리자 입력 없이 자동으로 설치됩니다.

서버 구성을 취소하면 WINS 서버 서비스가 설치되지 않습니다. 나중에 설치하려면 사용자 서버 관리를 다시 시작하고 WINS 역할을 추가합니다.

2. 서버 구성 마법사 완료

구성 요소를 구성하면 서버 구성 마법사는 이 서버는 이제 WINS 서버로 작동합니다 페이지를 표시합니다. 서버의 모든 변경 사항을 검토하거나 새 역할이 성공적으로 설치되었는지 확인하려면 서버 구성 로그를 클릭합니다. 서버 구성 마법사 로그는 *systemroot*₩Debug₩Configure Your Server.log 에 있습니다. 서버 구성 마법사를 닫으려면 마침을 클릭합니다.

3. WINS 서버 역할 제거

다른 역할을 위해 서버를 재구성해야 하는 경우 기존 서버 역할을 제거할 수 있습니다. WINS 서버 역할을 제거한 경우 이 서버가 클라이언트에서 컴퓨터 이름을 등록하고 확인하는 데 사용할 수 있는 유일한 WINS 서버이면 WINS 역할을 다른 서버에 추가해야 합니다. 또한 WINS 데이터베이스 정보를 다른 WINS 서버로 복제하도록 이 서버를 구성한 경우 해당 WINS 서버에 복제를 재구성해야 합니다.

WINS 서버 역할을 제거하려면 다음 중 하나를 수행하여 서버 구성 마법사를 다시 시작합니다.

- 사용자 서버 관리에서 **역할 추가/제거**를 클릭합니다. 기본적으로 사용자 서버 관리는 로그온하면 자동으로 시작됩니다. 서버 관리를 열려면 **시작**, **제어판**을 차례로 클릭하고 **관리 도구**를 두 번 클릭한 다음 **사용자 서버 관리**를 두 번 클릭합니다.
  - 서버 구성 마법사를 열려면 **시작**, **제어판**을 차례로 클릭하고 **관리 도구**를 두 번 클릭한 다음 **서버 구성 마법사**를 두 번 클릭합니다.

서버 역할 페이지에서 WINS 서버를 클릭한 후 다음을 클릭합니다. 역할 제거 확인 페이지에서 요약에 나열된 항목을 검토하고 WINS 서버 역할 제거 확인란을 선택한 후 다음을 클릭합니다. WINS 서버 역할 제거됨 페이지에서 마침을 클릭합니다.

4. 다음 단계: 추가 작업 완료

서버 구성 마법사를 완료하면 컴퓨터를 서버 IP 주소를 추적하고 클라이언트가 요청하는 정보를 제공할 수 있는 기본 WINS 서버로 사용할 수 있습니다. 지금까지 서버 하나에 WINS 서버 서비스를 설치하는 방법에 대해 설명했습니다. 복잡한 네트워크에서 WINS 클라이언트를 지원하려면 다른 서브넷에 추가 WINS 서버를 설치해야 합니다.

다음 표에는 WINS 서버에서 수행할 수 있는 몇 가지 추가 작업이 표시되어 있습니다.

작업	작업 목적
서버에 등록된 WINS 이름 레코드를 봅니다.	WINS 서버가 제대로 작동하는지 확인합니다.
WINS 서버 기본값을 수정합니다.	WINS는 WINS 서버 데이터베이스에서 NetBIOS 이름 레코드를 관리하는 방식을 결정하는 여러 개의 기본 서버 구성 매개 변수를 사용합니다. 일반적으로 이 매개 변수가 사용됩니다. 호스트 이름 변경을 해야 하는 경우 또는 클라이언트와 서버가 다른 IP 주소 집합을 사용하도록 네트워크 번호를 다시 설정하는 경우와 같이 특수한 환경에서는 이 매개 변수를 수정할 수 있습니다.
주 WINS 서버와 보조 WINS 서버에 대한 복제 설정을 구성합니다.	WINS 서버는 데이터베이스 변경 사항을 서로 복제하여 각 WINS 서버가 네트워크의 서버와 각 서버의 IP 주소에 대한 동일한 정보를 가지게 됩니다.

4) IAS (Internet Authentication Service)

A. IAS 기능

IAS 에는 다음과 같은 기능이 지원됩니다.

- 다양한 인증 방법

IAS 에는 여러 가지 인증 프로토콜이 지원되며 특정 인증 요구 사항을 충족하는 사용자 지정 방법을 추가할 수도 있습니다. 지원되는 인증 방법은 아래와 같습니다.

o 암호 기반의 PPP(지점간 프로토콜) 인증 프로토콜

PAP(암호 인증 프로토콜), CHAP(Challenge Handshake 인증 프로토콜), MS-CHAP(Microsoft Challenge Handshake 인증 프로토콜), MS-CHAP v2(MS-CHAP version 2) 등의 암호 기반 PPP 인증 프로토콜이 지원됩니다. 자세한 내용은 인증 방법을 참조하십시오.

o EAP(확장할 수 있는 인증 프로토콜)

인터넷 표준 기반의 구조로서 스마트 카드, 인증서, 일회용 암호, 토큰 카드 등 임의의 인증 방법을 추가할 수 있습니다. EAP 구조를 사용하는 특정한 인증 방법이 EAP 종류입니다. IAS 에서는 EAP-MD5(Message Digest 5)와 EAP-TLS(EAP-Transport Level Security)를 지원합니다. 자세한 내용은 EAP 를 참조하십시오.

- 다양한 권한 부여 방법

IAS 에는 여러 가지 권한 부여 프로토콜이 지원되며 특정 인증 요구 사항을 충족하는 사용자 지정 권한 부여 방법을 추가할 수도 있습니다. 지원되는 권한 부여 방법은 다음과 같습니다.

o DNIS(Dialed Number Identification Service)

호출된 전화 번호를 기반으로 연결 시도에 대해 권한을 부여합니다. DNIS 는 호출 수신자에게 호출된 전화 번호를 제공하며 대부분의 일반 전화 회사에서 제공합니다.

o ANI/CLI(Automatic Number Identification/Calling Line Identification)

호출자의 전화 번호를 기반으로 연결 시도에 대해 권한을 부여합니다. ANI/CLI 서비스는 호출 수신자에게 호출자의 전화 번호를 제공하며 대부분의 일반 전화 회사에서 제공합니다.

o 게스트 권한 부여

사용자 자격 증명(사용자 이름과 암호) 없이 연결하는 경우에 게스트 계정은 사용자의 ID 로 사용됩니다.

자세한 내용은 인증되지 않은 액세스를 참조하십시오.

- 유형이 다른 액세스 서버

IAS 에서는 RADIUS RFC 2865 및 2866 을 지원하는 액세스 서버를 지원합니다. 또한 네트워크 액세스 서버라고도 하는 전화 접속 액세스 서버와 함께 다음을 지원합니다.

o 무선 액세스 지점

원격 액세스 정책과 Wireless-IEEE 802.11 포트 종류 조건을 사용하면 무선 노드 인증 및 권한 부여를 위해 RADIUS 를 사용하는 무선 액세스 지점용 RADIUS 서버로 IAS 를 사용할 수 있습니다. 자세한 내용은 IAS 의 새로운 기능을 참조하십시오.

o 인증 스위치

원격 액세스 정책과 이더넷 포트 종류 조건을 사용하면 스위치 노드 인증 및 권한 부여를 위해 RADIUS 를 사용하는 이더넷 네트워크 스위치용 RADIUS 서버로 IAS 를 사용할 수 있습니다. 자세한 내용은 IAS 의 새로운 기능을 참조하십시오.

o 라우팅 및 원격 액세스 서비스와 통합

IAS 와 라우팅 및 원격 액세스 서비스는 원격 액세스 정책 및 로그 파일 기능을 공유합니다. 이러한 통합 방식을 통해 IAS 와 라우팅 및 원격 액세스 서비스를 일관되게 구현할 수 있습니다. 이렇게 하면 별도의 중앙 집중식 IAS 서버가 없이도 여러 소규모 사이트에 라우팅 및 원격 액세스를 배포할 수 있습니다. 또한 조직 내에 여러 대의 라우팅 및 원격 액세스 서버가 있는 경우에는 중앙 집중식 원격 액세스 관리 모델을 적용할 수 있습니다. 라우팅 및 원격 액세스 서버와 함께 IAS 를 사용하면 네트워크에 대한 아웃소싱 전화 걸기, 필요 시 전화 걸기 및 VPN 액세스 등의 원격 액세스에 사용할 수 있는 단일 관리 지점을 구현할 수 있습니다. 대규모의 중앙 집중식 사이트에 있는 IAS 의 정책을 소규모 사이트에 있는 별도의 라우팅 및 원격 액세스 서버로 내보낼 수 있습니다.

- RADIUS 프록시

IAS 에서는 인증 및 권한 부여 또는 계정을 처리하기 위해 들어오는 RADIUS 요청을 다른 RADIUS 서버로 전달할 수 있습니다. RADIUS 프록시로서 IAS 는 RADIUS 요청을 다른 RADIUS 서버로 라우팅해야 하는 경우에 사용될 수 있습니다. IAS 에서는 사용자 이름, 액세스 서버 IP

주소, 액세스 서버 식별자, 기타 조건을 기반으로 요청을 전달합니다. 자세한 내용은 IAS 의 새로운 기능을 참조하십시오.

- 아웃소싱 전화 접속 및 무선 네트워크 액세스

wholesale dialing 이라고도 알려진 아웃소싱한 전화 걸기는 조직(고객)과 ISP(인터넷 서비스 공급자) 간의 계약을 통해 이뤄집니다. ISP 를 사용하면 조직의 개인 네트워크로 연결되는 VPN 터널을 구축하기 전에 조직의 직원들이 조직 네트워크에 연결할 수 있습니다. 조직의 직원이 ISP 의 NAS 에 연결되면 인증 레코드와 사용 요약 레코드가 조직의 IAS 서버로 전달됩니다. IAS 서버를 통해 조직에서는 사용자 인증을 제어하고, 사용 요약을 추적하며, ISP 의 네트워크를 액세스할 수 있는 사용자를 결정합니다.

아웃소싱 전화 접속은 비용을 절감할 수 있다는 장점이 있습니다. 즉, 직접 구입하는 대신 ISP 의 라우터, 네트워크 액세스 서버 및 WAN(wide area network) 링크를 사용함으로써 하드웨어(구조) 비용을 매우 절약할 수 있습니다. 세계 전 지역에 연결망을 가진 ISP 에 전화를 걸면 장거리 전화 비용을 크게 줄일 수 있으며 여러 가지 지원 관련 사항을 공급자에게 맡겨 관리 비용을 없앨 수 있습니다.

또한 무선 액세스도 아웃소싱할 수 있습니다. 공급업체는 원격에서 무선 액세스를 제공하고 사용자가 제어할 수 있는 RADIUS 서버에 연결 요청을 전달하기 위해 사용자의 이름을 사용할 수 있습니다. 그 대표적인 예가 공항의 무선 인터넷 액세스입니다.

- 중앙 집중식 사용자 인증과 권한 부여

연결 요청을 인증하기 위해 IAS 에서는 연결 자격 증명이 로컬 SAM(보안 계정 관리자), Microsoft® Windows NT® Server 4.0 도메인 또는 Active Directory® 도메인의 사용자 계정과 맞는지 확인합니다. Active Directory 도메인의 경우 IAS 에서는 Active Directory UPN(사용자 이름)과 유니버설 그룹의 사용을 지원합니다.

연결 요청에 대한 권한을 부여하기 위해 IAS 에서는 연결 자격 증명 및 원격 액세스 정책과 일치하는 사용자 계정의 전화 접속 로그인 속성을 사용합니다. 각 사용자 계정의 원격 액세스 권한은 비교적 관리하기 쉽지만 조직의 규모가 커지면 이 방법은 그리 효율적이지 않습니다. 원격 액세스 정책은 원격 액세스 권한을 관리할 수 있는 강력하고 효율적인 방법을 제공합니다. 다음과 같은 다양한 조건을 기초로 네트워크 액세스 권한을 부여할 수 있습니다.

- 그룹의 사용자 계정 구성원
- 시간이나 요일

- 사용자가 연결하는 데 사용하는 미디어 종류(예: 무선, 이더넷 스위치, 모뎀, VPN)
- 사용자가 호출하는 전화 번호
- 요청을 보낸 액세스 서버

원격 액세스 정책의 프로필을 구성하면 다음과 같은 여러 연결 매개 변수를 제어할 수 있습니다.

- 특정한 인증 방법 사용
- 유휴 상태 시간 제한
- 최대 단일 세션 시간
- 멀티링크 세션의 연결 수
- 암호화 사용 및 강도
- 원격 액세스 사용자가 네트워크에 연결했을 때 액세스할 수 있는 리소스를 패킷 필터를 사용하여 관리. 예를 들어 필터를 사용하면 패킷을 보내거나 받는 데 사용자가 사용할 수 있는 IP 주소, 호스트 및 포트를 관리할 수 있습니다.
- 연결을 통해 전송되는 모든 패킷이 인터넷을 통해 안전하게 터널링되고 개인 네트워크에서 종료되도록 하는 강제 터널 작성
- 무선 또는 이더넷 연결을 위한 VLAN ID(Virtual Local Area Network Identifier)

- 모든 액세스 서버의 중앙 집중식 관리

IAS 는 RADIUS 표준을 지원하여 RADIUS 를 구현하는 액세스 서버의 연결 매개 변수를 제어할 수 있습니다. 또한 RADIUS 표준을 사용하면 개별 원격 액세스 공급업체에서 VSA(공급업체별 특성)라고 하는 고유한 확장 특성을 만들 수 있습니다. IAS 의 사전에는 여러 공급업체의 확장 특성이 통합되어 있습니다. 추가 VSA 는 개별 원격 액세스 정책의 프로필에 추가될 수 있습니다. 자세한 내용은 공급업체별 특성 개요를 참조하십시오.

- 중앙 집중식 감사 및 사용 요약 계정

IAS 는 RADIUS 표준을 지원하여 모든 액세스 서버에서 보낸 사용 요약(계정) 레코드를 특정 위치에 수집할 수 있습니다. 그리고 인증 성공 및 거부와 같은 감사 정보와 연결 및 연결 끊김 레코드와 같은 사용 요약 정보를 로그 파일에 저장합니다. IAS 는 데이터베이스로 직접 가져올 수 있는 로그 파일 형식을 지원합니다. 이러한 데이터는 모든 표준 데이터 분석 응용 프로그램을 사용하여 분석될 수 있습니다. 자세한 내용은 사용자 인증 및 계정 요청 로깅을 참조하십시오.

- 스냅인 기반의 관리 도구

IAS 에서는 인터넷 인증 서비스 스냅인이라고 하는 관리 도구를 제공합니다. 이 인터넷 인증 서비스를 관리 도구에서 실행하여 로컬 컴퓨터의 IAS 를 관리할 수 있습니다. 또는 로컬 컴퓨터나 원격 컴퓨터에서 실행하는 IAS 를 관리하기 위해 MMC(Microsoft Management Console)에 인터넷 인증 서비스 스냅인을 추가할 수 있습니다.

- Microsoft® Windows® Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition 및 Windows Server 2003, Datacenter Edition 에서 제공하는 도구를 사용한 로컬 또는 원격 모니터링

이벤트 뷰어, 시스템 모니터, SNMP(단순 네트워크 관리 프로토콜)를 포함한 Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition 및 Windows Server 2003, Datacenter Edition 에서 제공하는 도구를 사용하여 로컬 또는 원격 컴퓨터에서 IAS 를 모니터링할 수 있습니다. 또한 네트워크 모니터로 RADIUS 메시지를 캡쳐하여 자세한 트래픽 분석 및 문제 해결을 수행할 수 있습니다.

- 확장성

IAS 는 소규모 네트워크의 독립 실행형 서버에서 대규모 조직 및 ISP 네트워크에 이르기까지 다양한 크기와 종류의 네트워크 구성에 사용할 수 있습니다.

- 여러 IAS 서버 지원

Netsh 명령줄 도구를 사용하면 여러 IAS 서버의 구성을 동기화할 수 있습니다. 자세한 내용은 다른 서버에 IAS 구성 복사를 참조하십시오.

- 확장

Windows Server 2003 Platform SDK(소프트웨어 개발 키트)는 IAS SDK 와 EAP SDK 로 구분됩니다.

IAS SDK 는 다음과 같은 목적에 사용할 수 있습니다.

  - IAS 에서 반환하는 특성 이외의 사용자 지정 특성을 NAS 에 반환합니다. 예를 들어 IP 주소를 할당하는 사용자 지정 모듈을 만들 수 있습니다.

- o 사용자 네트워크 세션 수를 관리합니다.
- o 사용 요약 및 감사 데이터를 ODBC(개방형 데이터베이스 연결) 지원 데이터베이스로 직접 내보냅니다.
- o 사용자 지정한 권한 부여 모듈을 만듭니다.
- o 사용자 지정한 인증 모듈을 만듭니다(비 EAP).

5) IPSec

A. IPSec 소개

IPSec 은 장기적인 보안 네트워킹 방침으로 개인 네트워크 및 인터넷 공격으로부터 방어합니다.

IPSec 에는 두 가지 목적이 있습니다.

1. IP 패킷의 콘텐트 보호
2. 패킷 필터링 및 트러스트 된 통신의 강화를 통하여 네트워크 공격에 대한 방어 제공

두 가지 목적은 암호화 기반의 보호 서비스, 보안 프로토콜 및 동적인 키 관리의 사용으로 이뤄집니다. 이렇게 하면 강력한 힘과 융통성을 제공하여 개인 네트워크 컴퓨터, 도메인, 사이트, 원격 사이트, 엑스트라넷 및 전화 접속 클라이언트 사이의 통신을 보호합니다. 또한 특정 트래픽 유형의 확인 또는 전송의 차단에도 사용할 수 있습니다.

IPSec 은 엔드 투 엔드 보안 모델을 기준으로 하면서 원본 IP 에서 대상 IP 주소로 트러스트와 보안을 생성합니다. IP 주소 자체가 반드시 ID 로 여겨질 필요는 없으며 그보다는 IP 주소 뒤의 시스템이 인증 프로세스를 통해 유효한 ID 를 갖습니다. 보안할 트래픽에 관해 인식해야 하는 유일한 컴퓨터는 수신 및 송신 컴퓨터입니다. 각 컴퓨터는 통신이 발생하는 환경이 안전하지 않다는 가정 하에 각 끝 지점에서 보안을 해결합니다. 두 컴퓨터 간에 방화벽 형식의 패킷 필터링 또는 네트워크 주소 변환이 수행되지 않으면 원본에서 대상까지 데이터 경로만 정하는 컴퓨터는 IPSec 을 지원할 필요가 없습니다. 아래의 모델은 다음의 기업 시나리오에 대해 IPSec 이 성공적으로 배포되도록 합니다.

- LAN(Local Area Network): 클라이언트/서버, 피어 투 피어
- WAN(Widel Area Network): 라우터 간 및 게이트웨이 간
- 원격 액세스: 개인 네트워크에서 인터넷 액세스 및 전화 접속 클라이언트

B. IPSec 의 새로운 기능

IPSec(인터넷 프로토콜 보안)은 향상된 보안, 확장성, 가용성 및 쉬운 배포와 관리를 위해 다음과 같은 새로운 기능을 제공합니다.

1.IP 보안 모니터

Windows 2000 에서 IP 보안 모니터는 실행 프로그램(IPSecmon.exe)으로 구현되었으나 Windows XP 및 Windows Server 2003 제품군에서는 MMC(Microsoft Management Console)로 구현되며 기능이 향상되어 다음을 수행할 수 있습니다.

- 로컬 컴퓨터 및 원격 컴퓨터에 대한 IPSec 정보를 모니터링 합니다.
- 이름, 설명, 최종 수정 날짜, 저장소, 경로, 조직 구성 단위 및 그룹 정책 개체 이름을 포함하여 활성 IPSec 정책에 대한 세부 정보를 확인합니다.
- 주 모드 및 빠른 모드 일반 필터와 특정 필터를 확인합니다.
- 주 모드 및 빠른 모드 통계를 확인합니다. IP 보안 모니터에 표시되는 통계에 대한 자세한 내용은 IP 보안 모니터에서 주 모드 및 빠른 모드 통계 보기를 참조하십시오.
- 주 모드 및 빠른 모드 보안 연결을 확인합니다.
- 새로 고침 빈도를 사용자 지정하고 필터 및 보안 연결 출력에 대해 DNS 이름 확인을 사용합니다.
- 임의의 원본 또는 대상 IP 주소, 로컬 컴퓨터의 원본 또는 대상 IP 주소, 특정 원본 또는 대상 IP 주소와 일치하는 특정 주 모드 또는 빠른 모드 필터를 검색합니다.

IP 보안 모니터 스냅인 추가에 대한 자세한 내용은 IP 보안 모니터 스냅인 추가를 참조하십시오.

2.더 강력한 암호화 마스터 키(Diffie-Hellman)

보안을 강화하기 위해 IPSec 에서는 2048 비트 Diffie-Hellman 키 교환을 지원합니다. 더 강력한 Diffie-Hellman 그룹을 사용하면 Diffie-Hellman 교환에서 파생된 비밀 키가 더 강력해집니다. 강력한 Diffie-Hellman 그룹을 길이가 긴 키와 함께 사용하면 비밀 키를 알아내기가 훨씬 더 어려워집니다.

이 기능은 Windows Server 2003 제품군에서만 사용할 수 있습니다.

3.Netsh 를 사용한 명령줄 관리

Netsh IPSec 컨텍스트의 명령을 사용하면 정적 또는 동적 IPSec 주 모드 설정, 빠른 모드 설정, 규칙 및 구성 매개 변수를 구성할 수 있습니다. Netsh IPSec 컨텍스트를 입력하려면 명령 프롬프트에 **netsh -c ipsec** 을 입력합니다. Netsh IPSec 컨텍스트는 Windows 2000 Server Resource Kit 에 제공되는 Ipsecpol.exe 도구를 대신합니다. 이 기능을 사용하여 IPSec 구성을 스크립팅하고 자동화할 수 있습니다.

이 기능은 Windows Server 2003 제품군에서만 사용할 수 있습니다.

4.컴퓨터 시작 보안

보안을 강화하기 위해 IPSec 에서는 컴퓨터 시작 중에 네트워크 트래픽의 상태 저장 필터링을 제공합니다. 상태 저장 필터링을 사용하면 컴퓨터 시작 시 초기화된 아웃바운드 트래픽, 아웃바운드 트래픽에 대한 응답으로 전송된 인바운드 트래픽 및 DHCP 트래픽만 컴퓨터 시작 중에 허용됩니다. 상태 저장 필터링의 대안으로 IPSec 정책이 적용되기 전까지 모든 인바운드 및 아웃바운드 트래픽이 거부되도록 지정할 수 있습니다. 상태 저장 필터링을 사용하거나 컴퓨터 시작 중에 트래픽이 거부되도록 지정하면 컴퓨터 시작 중에 IPSec 필터링에서 제외시킬 트래픽 유형도 지정할 수 있습니다.

5.향상된 보안을 위한 영구 정책

로컬 IPSec 정책이나 Active Directory 기반 IPSec 정책을 적용할 수 없는 경우 영구적인 IPSec 정책을 만들고 할당하여 컴퓨터의 보안을 유지할 수 있습니다. 영구 정책을 만들어 할당하면 로컬 정책이나 Active Directory 기반 정책보다 먼저 적용되며 로컬 정책이나 Active Directory 기반 정책이 적용된 후에도 계속 유효합니다. 예를 들어 IPSec 정책이 손상되면 적용되지 않습니다.

- IP 보안 정책 관리 콘솔에서는 이 기능을 구성할 수 없습니다. 이 기능을 구성하려면 IPSec 의 Netsh 명령을 사용해야 합니다.

6.제거된 기본 트래픽 제외

Windows server 2003 및 Windows XP 에서는 기본적으로 모든 브로드캐스트, 멀티캐스트, IKE(인터넷 키 교환), Kerberos 및 RSVP(Resource Reservation Protocol) 트래픽이 IPSec 필터링에서 제외됩니다. 보안을 더 강화하기 위해 Windows Server 2003 제품군에서는 IKE 트래픽(IPSec 보안 통신 설정에 필요)만 IPSec 필터링에서 제외됩니다. 다른 모든 트래픽 유형은 현재 IPSec 필터에 일치하므로 멀티캐스트 및 브로드캐스트 트래픽에 대한 필터 동작을 구성, 거부 또는 허용할 수 있습니다. IPSec 은 멀티캐스트 및 브로드캐스트 트래픽에 대한 보안 연결을 협상하지 않습니다. 자세한 내용은 IPSec 특별 고려 사항을 참조하십시오.

7.네트워크 액세스 제어에 사용되는 IPSec 의 계정 매핑을 위한 인증서

Windows Server 2003 제품군에서 Kerberos V5 또는 인증서 인증을 사용하는 경우 연결할 수 있는 컴퓨터에 대해 제한 사항을 설정할 수 있습니다. 이 기능을 사용하면 IPSec 을 통해 Windows Server 2003 을 실행하는 서버에 대한 다음의 액세스를 허용하거나 거부할 수 있습니다.

- 특정 도메인의 구성원인 컴퓨터

- 특정 발급 인증 기관의 인증서가 있는 컴퓨터
- 특정 컴퓨터 그룹
- 특정 컴퓨터

IPSec 에서 계정 매핑에 대해 인증서를 사용하면 IKE 프로토콜은 Active Directory 도메인 또는 포리스트의 컴퓨터 계정에 컴퓨터 인증서를 연결(매핑)한 다음 액세스 토큰을 검색합니다. 이 액세스 토큰에는 컴퓨터에 할당된 사용자 권한 목록이 들어 있습니다. 그룹 정책 보안 설정을 구성하고 필요에 따라 **네트워크에서 이 컴퓨터 액세스** 사용자 권한이나 **네트워크에서 이 컴퓨터 액세스 거부** 사용자 권한을 개별 컴퓨터 또는 여러 컴퓨터에 할당하여 액세스를 제한할 수 있습니다.

IPSec 의 계정 매핑을 위한 인증서에 대한 자세한 내용은 인증 방법을 참조하십시오.

그룹 정책의 보안 설정 구성에 대한 자세한 내용은 보안 설정 개요를 참조하십시오.

- IPSec 의 계정 매핑을 위한 인증서는 Windows Server 2003 제품군에서만 사용할 수 있습니다.
- 포리스트 간에는 인증서 매핑이 지원되지 않습니다.

8.인증서 요청에서 CA 의 이름을 제외시키는 기능

보안을 강화하기 위해 인증서 인증을 사용하여 IPSec 피어 간에 트러스트를 설정할 경우 인증서 요청에서 CA(인증 기관) 이름을 제외시킬 수 있습니다. 인증서 요청에서 CA 의 이름을 제외시키고 내부 공개 키 구조를 사용하는 경우 컴퓨터를 소유하는 회사의 이름 및 컴퓨터의 도메인 구성원 같은 컴퓨터의 트러스트 관계에 대한 중요한 정보가 공격자에게 공개되지 않습니다.

9.IPSec 정책 필터에서 로컬 IP 구성의 논리 주소 허용

이제 IP 보안 정책 관리 콘솔을 사용하여 로컬 IPSec 정책이 DHCP 서버, DNS 서버, WINS 서버 및 기본 게이트웨이에 대한 주소로 해석하는 원본 또는 대상 주소 필드를 구성할 수 있습니다. 따라서 DHCP 또는 정적 IP 구성을 통해 서버의 IP 구성 변경 내용이 자동으로 IPSec 정책에 적용될 수 있습니다.

이 기능은 Windows Server 2003 제품군에서만 사용할 수 있습니다.

10.NAT 를 통한 IPSec 기능

IPSec ESP(Encapsulating Security Payload) 패킷은 UDP(User Datagram Protocol) 트래픽을 허용하는 NAT(네트워크 주소 변환)를 통해 전달될 수 있습니다. IKE 프로토콜을 사용하면 자동으로 NAT 의 존재를 감지하고 UDP-ESP 캡슐화를 사용하여 NAT 를 통해 IPSec 트래픽을 전달할 수 있습니다. 이 기능은 IPSec 에 대한 IETF(Internet Engineering Task Force) IP 보안 작업 그룹의 표준을 구현한 것입니다.

NAT 는 ICS(인터넷 연결 공유)와 호텔 및 항공 등 출장 중에 자주 이용하는 공용 인터넷 액세스 위치에서 널리 사용됩니다. 또한 일부 ISP(인터넷 서비스 공급자)는 중앙 NAT 를 사용하여 해당 클라이언트를 인터넷에 연결합니다.

NAT 를 통한 IPSec 기능을 사용하여 다음과 같은 일반적인 배포 시나리오에서 IPSec 보안 연결을 설정할 수 있습니다.

- NAT 를 이용하는 L2TP(계층 2 터널링 프로토콜)/IPSec VPN(가상 사설망) 클라이언트는 IPSec ESP 전송 모드를 사용하여 인터넷을 통해 회사 네트워크에 대해 IPSec 보안 연결을 설정할 수 있습니다.
- 라우팅 및 원격 액세스 기능을 실행하는 서버는 라우팅 및 원격 액세스를 실행하는 서버 중 하나가 NAT 를 이용할 때 게이트웨이 간 IPSec 터널을 설정할 수 있습니다.
- 이러한 컴퓨터 한 대 또는 두 대 모두 NAT 를 이용할 경우 클라이언트와 서버는 IPSec ESP 전송 모드를 사용하여 IPSec 보안 TCP 및 UDP 패킷을 다른 클라이언트나 서버로 전송할 수 있습니다. 예를 들어 주변 네트워크의 서버에서 실행되는 프로그램을 회사 네트워크에 연결하는 데 사용할 경우 해당 프로그램의 IPSec 보안이 유지될 수 있습니다.

VPN 및 IPSec 에 대한 자세한 내용은 IPSec 을 사용하는 가상 사설망을 참조하십시오.

11.네트워크 로드 균형 조정 기능과 IPSec 의 향상된 통합

네트워크 로드 균형 조정 기능과 IPSec 의 향상된 통합으로 네트워크 로드 균형 서버 그룹이 가용성이 높은 IPSec 기반 VPN 서비스를 제공할 수 있게 되었습니다. 네트워크 로드 균형 조정 기능으로 IPSec 보안 세션을 정확하게 추적할 수 있으며 IPSec IKE 프로토콜은 클러스터 서버와의 IPSec 보안 세션이 설정될 때를 감지하고 빠르게 장애 조치를 수행할 수 있습니다. 또한 네트워크 로드 균형 조정 기능은 클러스터의 호스트 수와 클라이언트를 호스트에 매핑하는 데 사용되는 알고리즘이 변경될 때에도 올바른 네트워크 로드 균형 조정 호스트와의 IPSec 보안 연결을 유지 관리할 수 있습니다. IKE 프로토콜은 자동으로 네트워크 로드 균형 조정 서비스를 감지하므로 이 기능을 사용하기 위한 추가 구성은 필요하지 않습니다.

이 기능은 Windows Server 2003, Enterprise Edition 및 Windows Server 2003, Datacenter Edition 에만 제공됩니다.

12.RSoP 용 IPSec 지원

IPSec 배포 및 문제 해결을 향상시키기 위해 IPSec 에서는 RSoP(정책 결과 집합) 콘솔에 대한 확장 기능을 제공합니다. RSoP 는 컴퓨터나 그룹 정책 컨테이너의 구성원을 위한 기존 IPSec 정책 할당을 확인하는 데 사용할 수 있는 그룹 정책 추가 요소입니다. 컴퓨터의 IPSec 정책 할당을 확인하려면 RSoP 로깅 모드 쿼리를 실행합니다. 그룹 정책 컨테이너 구성원의 IPSec 정책 할당을 확인하려면 RSoP 계획 모드 쿼리를 실행합니다. IPSec 정책 할당을 확인하는 방법에 대한 자세한 내용은 RSoP(정책 결과 집합)를 사용하여 IPSec 정책 할당 보기를 참조하십시오.

RSoP 로깅 모드 쿼리 또는 RSoP 계획 모드 쿼리를 실행하면 적용되는 IPSec 정책에 대한 자세한 설정(IPSec 정책이 만들어질 때 지정된 필터 규칙, 필터 동작, 인증 방법, 터널 종점 및 연결 유형)을 확인할 수 있습니다.

IPSec 에서 RSoP 를 사용하는 데 대한 자세한 내용은 정책 결과 집합을 사용하여 IPSec 정책 할당 보기를 참조하십시오.

13.IPSec 을 위한 보안 정보

조직에서 IPSec 을 배포하기 전에 다음 보안 문제를 고려합니다.

- 3DES 및 Microsoft® Windows® 2000 을 실행 중인 컴퓨터
- 인증 방법
- 방화벽 패킷 필터링
- AH 또는 ESP 를 사용하는 보호된 트래픽
- 기본 응답 규칙을 사용하는 보호되지 않은 트래픽
- Diffie-Hellman 그룹(Diffie-Hellman 그룹 1, 2 또는 2048 사용)

14.3DES 및 Windows 2000 을 실행 중인 컴퓨터

IPSec 정책에서는 더 뛰어난 보안성을 위해 DES 보다 더 강력한 암호화를 제공하는 강력한 암호화 알고리즘인 3DES 를 선택할 수 있습니다. Windows 2000 을 실행하는 컴퓨터가 3DES 알고리즘을 수행하려면 고급 암호화 팩 또는 서비스 팩 2 이상이 설치되어 있어야 합니다. 3DES 설정을 수신하는 Windows 2000 을 실행하는 컴퓨터에 고급 암호화 팩 또는 서비스 팩 2 이상이 설치되어 있지 않으면 보안 방법의 3DES 설정은 통신을 전면적으로 차단하기보다는 일정 수준의 기밀성을 유지할 수 있도록 보안이 약한 DES 로 설정됩니다. 그러나 일부 컴퓨터에서만 3DES 를 사용할 수 있는 환경에서는 DES 를 대체 옵션으로만 사용해야 합니다.

Windows XP 및 Windows Server 2003 제품군을 실행하는 컴퓨터에서는 3DES 를 지원하므로 고급 암호화 팩을 설치할 필요가 없습니다.

15.인증 방법

조직 내의 컴퓨터가 Active Directory® 도메인의 일부이면 기본 인증 방법(Kerberos V5)을 사용하여 IPSec 주 모드 인증을 얻을 수 있습니다. 인트라넷 통신을 위해 공개 키 인증서를 배포할 필요가 없습니다. 그러나 Windows XP Home Edition 을 실행하는 컴퓨터는 Kerberos V5 인증 방법을 지원하지 않습니다. 또한 컴퓨터가 인터넷에 연결되어 있으면 인증 방법으로 Kerberos V5 를 사용하지 않는 것이 좋습니다. Kerberos 인증이 사용되면 주 모드 협상 중에 각 IPSec 피어는 다른 피어에 해당 컴퓨터 ID 를 암호화되지 않은 형식으로 보냅니다. 주 모드 협상의 인증 단계 중에 전체 ID 페이로드 암호화가 수행될 때까지 컴퓨터 ID 가 암호화되지 않습니다. 공격자는 응답 IPSec 피어가 해당 컴퓨터 ID 와 도메인 구성원을 노출하게 하는 IKE(인터넷 키 교환) 패킷을 전송할 수 있습니다. 인터넷에 연결된 컴퓨터를 보호하기 위해서는 인증서 인증 방법도 권장됩니다.

미리 공유된 키 인증은 비교적 약한 인증 방법이므로 보안을 강화하기 위해서는 이 인증 방법은 사용하지 않는 것이 좋습니다. 또한 미리 공유된 키는 일반 텍스트로 저장됩니다. 미리 공유된 키 인증은 상호 운용성을 위해 제공되고 IPSec 표준을 준수합니다. 미리 공유된 키는 테스트용으로만 사용하는 것이 좋습니다.

16.방화벽 패킷 필터링

방화벽, 보안 게이트웨이, 라우터 또는 인터넷에 연결되어 주변 네트워크(완충 영역 또는 DMZ 이라고도 함)의 컴퓨터에 패킷 필터링 기능을 제공하는 다른 서버나 장치의 경우 해당 컴퓨터에서 특수한 필터링을 사용할 수 있어야 IPSec 으로 보안된 패킷을 주변 네트워크의 컴퓨터로 전달할 수 있습니다. 방화벽 또는 다른 장치는 통과하려면 일반적으로 다음 종류의 트래픽을 허용해야 합니다.

- IPSec ESP(Encapsulating Security Payload) 트래픽을 위한 IP 프로토콜 ID 50(0x32)
- IPSec AH(인증 헤더) 트래픽을 위한 IP 프로토콜 ID 51(0x33)
- IKE(인터넷 키 교환) 협상 트래픽을 위한 UDP 포트 500(0x1F4)

대부분의 패킷 필터링 소프트웨어를 사용하면 더 구체적으로 지정할 수 있습니다. 인바운드 트래픽(인바운드 필터), 아웃바운드 트래픽(아웃바운드 필터) 및 각 인터페이스에 별도의 패킷 필터를 정의할 수 있습니다. 또한 주변 네트워크의 IPSec 컴퓨터에 IP 주소를 지정할 수 있습니다. 주변 네트워크의 단일 IPSec 컴퓨터와 교환되는 IPSec 트래픽에 대해 가장 제한적인 패킷 필터는 다음 섹션에서 설명합니다.

17. 인터넷 인터페이스의 필터

다음의 인바운드 패킷 필터를 방화벽의 인터넷 인터페이스에 구성하여 특정 트래픽 종류를 허용합니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 대상 IP 주소 및 UDP 대상 포트 500(0x1F4)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에 IKE 트래픽을 보낼 수 있습니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 대상 IP 주소 및 IP 프로토콜 ID 50(0x32)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에 IPSec ESP 트래픽을 보낼 수 있습니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 대상 IP 주소 및 IP 프로토콜 ID 51(0x33)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에 IPSec AH 트래픽을 보낼 수 있습니다.

다음의 아웃 바운드 패킷 필터를 방화벽의 인터넷 인터페이스에 구성하여 특정 트래픽 종류를 허용합니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 원본 IP 주소 및 UDP 원본 포트 500(0x1F4)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에서 IKE 트래픽을 보낼 수 있습니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 원본 IP 주소 및 IP 프로토콜 ID 50(0x32)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에서 IPSec ESP 트래픽을 보낼 수 있습니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 원본 IP 주소 및 IP 프로토콜 ID 51(0x33)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에서 IPSec AH 트래픽을 보낼 수 있습니다.

18. 주변 네트워크 인터페이스의 필터

다음의 인바운드 패킷 필터를 방화벽의 주변 네트워크 인터페이스에 구성하여 특정 트래픽 종류를 허용합니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 원본 IP 주소 및 UDP 원본 포트 500(0x1F4)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에서 IKE 트래픽을 보낼 수 있습니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 원본 IP 주소 및 IP 프로토콜 ID 50(0x32)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에서 IPSec ESP 트래픽을 보낼 수 있습니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 원본 IP 주소 및 IP 프로토콜 ID 51(0x33)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에서 IPSec AH 트래픽을 보낼 수 있습니다.

다음의 아웃바운드 패킷 필터를 방화벽의 주변 네트워크 인터페이스에 구성하여 특정 트래픽 종류를 허용합니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 대상 IP 주소 및 UDP 대상 포트 500(0x1F4)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에 IKE 트래픽을 보낼 수 있습니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 대상 IP 주소 및 IP 프로토콜 ID 50(0x32)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에 IPSec ESP 트래픽을 보낼 수 있습니다.

- IPSec 컴퓨터의 주변 네트워크 인터페이스의 대상 IP 주소 및 IP 프로토콜 ID 51(0x33)

  이 필터를 사용하여 주변 네트워크의 IPSec 컴퓨터에 IPSec AH 트래픽을 보낼 수 있습니다.

19. AH 또는 ESP 를 사용하는 보호된 트래픽

IP 트래픽 보호에 AH 또는 ESP 를 사용할지 결정할 때 다음 사항을 고려합니다.

- AH 는 각 패킷에 대해 입력 해시를 계산하고 포함하여 데이터 인증 및 무결성 서비스를 모두 제공합니다. AH 를 사용할 경우 해시 계산에 전체 IP 패킷과 헤더가 포함됩니다. 전송할 때 변경할 수 있는 일부 필드는 제외됩니다. 패킷 재생 보호 서비스는 각 패킷의 시퀀스 번호를 포함하여 제공됩니다.
- ESP 는 각 패킷에 대해 입력 해시를 계산하고 포함하여 데이터 인증 및 무결성 서비스를 제공합니다. ESP 를 사용할 경우 해시 계산에 ESP 헤더, 트레일러 및 페이로드만 포함됩니다. IP 헤더는 해시로 보호되지 않습니다. ESP 는 DES(데이터 암호화 표준) 또는 3DES(Triple DES) 암호화 알고리즘으로 ESP 페이로드를 암호화하여 데이터 기밀성 서비스를 제공합니다. 패킷 재생 보호 서비스는 각 패킷의 시퀀스 번호를 포함하여 제공됩니다.

각 패킷을 암호화하고 해독하는 것보다 각 패킷의 해시를 확인하는 것이 CPU 를 덜 사용하게 됩니다. 성능을 상당히 고려할 경우 AH 를 사용하여 대부분의 트래픽을 보호할 수 있습니다. 기밀성이 필요하면 대신 ESP 를 사용할 수 있습니다. 예를 들어 인트라넷의 트래픽 보호에는 AH 를 사용하고 인터넷을 통해 보내는 트래픽에는 ESP 를 사용할 수 있습니다.

- 이 성능 고려 사항은 조직에서 IPSec 오프로드 네트워크 어댑터를 사용하고 있지 않다고 가정합니다. 오프로드 네트워크 어댑터는 어댑터 자체에서 해시와 암호화 및 해독 서비스의 계산 및 확인과 같은 암호화 계산을 수행하여 IPSec 보호 트래픽의 성능을 향상시킵니다.

20. 기본 응답 규칙을 사용하는 보호되지 않은 트래픽

특정한 서버 집합의 트래픽을 보안하는 IPSec 배포 시나리오는 다음과 같이 쉽게 구현할 수 있습니다.

1. 서버를 조직 단위에 두고 해당 조직 단위의 그룹 정책 개체에 서버와 다른 컴퓨터 간에 보안된 트래픽이 필요한 규칙이 있는 IPSec 정책을 할당합니다. 규칙의 필터 동작 안에서 보안된 서버가 보안되지 않은 통신을 받아들이지만 항상 IPSec 을 사용하여 응답할 수 있도록 합니다.
2. 클라이언트 컴퓨터를 조직 단위에 두고 해당 조직 단위의 그룹 정책 개체에 기본 응답 규칙만 사용하는 IPSec 정책을 할당합니다..

이 구성에서 클라이언트 컴퓨터와 보안된 서버 간의 다음 트래픽은 보안되지 않습니다.

- 클라이언트 컴퓨터에서 통신 설정을 위해 보낸 초기 요청(예: TCP SYN 패킷)은 클라이언트의 정책에 보안된 서버와 보안된 통신을 시작하는 규칙이 없으므로 보안되지 않습니다.
- 클라이언트 및 보안된 서버 컴퓨터 간에 보안된 통신이 협상된 후 계속해서 통신이 보안되더라도 트래픽에 보안 설정을 제공하는 빠른 모드 SA(보안 연결)는 결국 시간을 초과하여 보안된 서버와 클라이언트 컴퓨터에서 모두 제거될 수 있습니다. 이런 현상은 TCP 연결이 있고 클라이언트 컴퓨터와 보안된 서버 간에 오랜 시간 동안 트래픽이 전송되지 않을 경우 발생합니다. 기본 응답 규칙으로 클라이언트 컴퓨터에서 만든 동적 필터도 동적 필터가 시간 초과되면 제거됩니다.

보안된 서버가 기존 연결에서 새 데이터를 보낼 경우 보안된 서버에 이 서버와 다른 모든 컴퓨터 간의 트래픽을 보안하는 규칙이 있으므로 이 데이터를 클라이언트 컴퓨터에 보내기 전에 빠른 모드 SA 를 다시 협상합니다. 그러나 클라이언트 컴퓨터가 빠른 모드 SA 및 동적 필터 시간이 초과된 이후에 새 데이터를 보내면 클라이언트에 보안된 서버와 보안된 통신을 시작하는 규칙이 없으므로 새 데이터가 보안되지 않은 상태로 송신됩니다. TCP 연결의 경우 클라이언트 컴퓨터에서 하나 이상의 TCP 세그먼트를 보안되지 않은 상태로 보낼 수 있습니다. 클라이언트 컴퓨터에서 보안된 서버로 보안되지 않은 데이터를 보내지 않게 하려면 보안된 서버로 보안된 통신을 시작하는 추가 규칙으로 클라이언트 컴퓨터 IPSec 정책을 구성해야 합니다.

21. Diffie-Hellman 그룹(Diffie-Hellman 그룹 1, 2 또는 2048 사용)

Diffie-Hellman 그룹은 키 교환 프로세스에서 사용되는 기본 프라임 번호의 길이를 결정하는 데 사용합니다. 그룹 2048(높음)은 그룹 2(중간)보다 강력(보다 안전함)하며 그룹 2 는 그룹

1(낮음)보다 강력합니다. 그룹 1 은 768 비트, 그룹 2 는 1,024 비트, 그룹 2048 은 2,048 비트의 키 강도를 제공합니다.

강력한 Diffie-Hellman 그룹을 길이가 긴 키와 함께 사용하면 비밀 키를 알아내기가 훨씬 더 어려워집니다.

22. IPSec 특별 고려 사항

다음의 특별한 IPSec 고려 사항은 IPSec 정책 관리를 간단하게 만드는 데 도움을 줄 수 있습니다.

23. 권장되는 IPSec 시나리오 및 권장되지 않는 IPSec 시나리오

다음은 Windows Server 2003 제품군에서 구현된 IPSec 에 권장되는 시나리오와 권장되지 않는 시나리오입니다.

24. 권장되는 IPSec 시나리오

Windows Server 2003 제품군에 구현된 IPSec 은 다음과 같은 경우에 사용하는 것이 좋습니다.

- 패킷 필터링. IPSec 은 최종 시스템에 제한된 방화벽 기능을 제공합니다. 또한 인터넷 연결 방화벽과 라우팅 및 원격 액세스와 함께 IPSec 을 사용하여 인바운드 또는 아웃바운드 트래픽을 허용하거나 차단할 수 있습니다.
- 특정 경로의 호스트 간 트래픽 보안 유지. IPSec 을 사용하여 서버나 다른 정적 IP 주소 또는 서브넷 간의 트래픽에 상호 인증 및 암호화 보호 기능을 제공할 수 있습니다. 예를 들어 IPSec 은 도메인 컨트롤러 사이트나 포리스트 간 또는 웹 서버와 데이터베이스 서버 간 트래픽의 보안을 유지할 수 있습니다.
- 서버로의 트래픽 보안 유지. IPSec 을 사용하여 서버에 액세스하는 모든 클라이언트 컴퓨터의 상호 인증을 요청할 수 있습니다. 또한 Windows Server 2003 제품군을 실행하는 서버에 연결할 수 있는 컴퓨터에 대해 제한을 설정할 수 있습니다.
- VPN 연결에 L2TP/IPSec 터널링 사용. 모든 가상 사설망 VPN 시나리오에 L2TP(계층 2 터널링 프로토콜) 및 IPSec(L2TP/IPSec) 조합을 사용할 수 있습니다.
- 터널 모드에서 게이트웨이 간 터널에 IPSec 사용. L2TP/IPSec 또는 PPTP VPN 터널링을 지원하지 않는 다른 라우터, 게이트웨이 또는 최종 시스템과의 상호 운용성을 위해 터널 모드에서 게이트웨이 간 터널에 IPSec 을 사용할 수 있습니다.
-

25. 권장되지 않는 IPSec 시나리오

IPSec 인증 및 데이터 보호 기능을 사용하면 Windows 2000, Windows XP 및 Windows Server 2003 제품군의 정책 관리 모델은 하나의 종점이 정적 주소를 갖는 서버 간 시나리오 및

클라이언트와 서버 간 시나리오에 가장 적합한 것이 됩니다. 양쪽 최종 시스템이 정적 주소를 갖는 대규모 네트워크 배포 및 이동성을 구현해야 하는 상황에서 정책 관리가 복잡하면 IPSec 배포가 어려울 수 있습니다. 이러한 이유로 다음과 같은 경우에는 IPSec 을 사용하는 것이 권장되지 않습니다.

- 도메인 구성원과 해당 도메인 컨트롤러 간 통신 보안 유지. 이 시나리오에 요구되는 IPSec 정책 구성 및 관리가 복잡하기 때문에 IPSec 을 사용하여 도메인 구성원과 해당 도메인 컨트롤러 간 통신의 보안을 유지하는 것은 좋지 않습니다.
- 네트워크에서 모든 트래픽의 보안 유지. 네트워크의 많은 컴퓨터의 보안을 유지하기 위해 모든 클라이언트 컴퓨터와 모든 서버 간 IPSec 통신을 구성하는 것은 어려운 일입니다. IPSec 은 멀티캐스트 및 브로드캐스트 트래픽의 보안을 협상할 수 없습니다. 실시간 통신으로 발생한 트래픽, ICMP 를 필요로 하는 응용 프로그램 및 피어 투 피어 응용 프로그램은 IPSec 과 호환될 수 없습니다. 이러한 이유로 IPSec 을 사용하여 네트워크의 모든 트래픽에 대해 보안을 유지하는 것은 바람직하지 않습니다.

  또한 IPSec 프로토콜 및 구현을 사용하는 경우 다른 시나리오에서 다음과 같은 사항을 특별히 고려해야 합니다.

- 무선 802.11 네트워크를 통한 트래픽의 보안 유지. IPSec 정책은 이동 클라이언트의 구성에 맞게 최적화되어 있지 않습니다. 이러한 이유로 IPSec 은 무선 802.11 네트워크를 통해 보낸 트래픽의 보안을 유지하는 방법으로 권장되지 않습니다. 대신 IEEE 802.1x 인증을 사용하는 것이 좋습니다. 802.1x 는 중앙 사용자 ID, 인증, 동적 키 관리 및 계정을 제공하여 보안을 강화하며 배포를 용이하게 해 줍니다. 클라이언트가 같은 네트워크의 액세스 지점 간을 이동하는 경우 802.11 및 802.1x 와 함께 IPSec 을 사용할 수 있습니다. 이동 시 클라이언트 IP 주소가 변경되는 경우에는 IPSec 보안 연결이 무효화되며 새 보안 연결이 다시 협상됩니다.
- 터널 모드에서 원격 액세스 VPN 연결에 IPSec 사용. 터널 모드에서 원격 액세스 VPN 시나리오에 IPSec 을 사용하는 것은 권장되지 않습니다. 대신 원격 액세스 VPN 연결에 L2TP/IPSec 또는 PPTP 를 사용하십시오.

26. Windows Server 2003 제품군에서만 사용할 수 있는 새 기능을 사용하는 정책 관리

다음 기능은 Windows Server 2003 제품군에 구현된 IPSec 에서만 사용할 수 있습니다.

- 필터를 정의하기 위한 새 원본 및 대상 주소 옵션. 예를 들어 다음을 만들 수 있습니다.
  - **모든 IP 주소**의 대상 주소 및 원본 주소를 포함하는 필터
  - 비표준 서브넷 클래스를 원본 주소 또는 대상 주소로 사용하는 필터
  - 멀티캐스트 또는 브로드캐스트 주소를 대상 주소로 사용하는 필터

  - DNS 서버, WINS 서버 및 DHCP 서버와 필터가 적용되는 컴퓨터의 기본 게이트웨이에 대한 로컬 IP 구성에 해당하는 원본 주소 또는 대상 주소를 포함하는 필터
- 인증서 요청에서 CA(인증 기관)의 이름을 제외시키는 기능
- 네트워크 액세스 컨트롤을 위한 인증서에서 계정으로의 매핑
- 확장된 ASCII 문자 집합에 나타나는 루트 CA 이름에 대한 지원
- 강력한 Diffie-Hellman 그룹(2048 비트 Diffie-Hellman 키 교환)

Windows XP 및 Windows 2000 을 실행하는 컴퓨터는 이러한 새 정책 설정을 사용할 수 없습니다. Windows Server 2003 제품군에서만 사용할 수 있는 기능을 사용하는 Active Directory 기반 IPSec 정책을 적용하려는 경우 Windows Server 2003 제품군 버전의 IP 보안 정책 관리 콘솔을 사용하여 이 정책을 관리하십시오. Windows XP 또는 Windows 2000 버전의 IP 보안 정책 관리 콘솔을 사용하여 이러한 정책을 관리하면 이전 버전의 IP 보안 정책 관리 콘솔이 새로운 기능 설정을 삭제합니다.

또한 다른 버전의 Windows 를 실행하는 컴퓨터에 동일한 IPSec 정책을 적용하려면 Windows Server 2003 을 실행하는 서버와 Windows XP 또는 Windows 2000 을 실행하는 컴퓨터에서 모두 해당 정책이 예상대로 작동하는지 확인합니다.

Windows Server 2003 제품군에 구현된 IPSec 에서 사용할 수 있는 새 기능에 대한 내용은 IPSec 의 새로운 기능을 참조하십시오

27. IP 필터

IP 필터 구성 시 다음을 고려하십시오.

- 단일 필터를 컴퓨터 그룹에 적용하려면 일반 필터를 사용합니다. 예를 들어 필터를 구성할 때 특정 컴퓨터의 원본 및 대상 IP 주소를 지정하는 대신 **내 IP 주소**, **모든 IP 주소** 또는 서브넷 주소를 사용합니다.
- 네트워크 안에서 논리적으로 연결된 세그먼트 또는 서브넷에서 트래픽을 그룹화하고 보안할 수 있는 필터를 정의합니다.
- IPSec 정책을 볼 때 필터가 적용되는 순서는 표시되는 순서와 관계가 없습니다. IPSec 정책 에이전트가 IPSec 정책을 읽을 때 필터는 가장 구체적인 것부터 일반적인 것으로 순서대로 처리됩니다. IP 보안 모니터 콘솔을 사용하여 가중치별로 정렬된 필터를 볼 수 있습니다. 가중치가 동일한 필터는 필터 간 상대적 순서로 표시될 수 있습니다.

정책 업데이트 중에 IPSec 정책 에이전트는 정렬 순서를 다시 계산하고 변경된 내용만으로 IPSec 드라이버를 업데이트합니다. 필터가 삭제되거나 필터에 대한 필터 동작이 변경되면 해당

필터와 관련된 모든 보안 연결이 삭제됩니다. 따라서 새 보안 연결이 협상될 때 일부 패킷이 손실됩니다. 그러나 손실된 패킷을 다시 전송하여 즉시 TCP 연결을 복구해야 합니다.

- Kerberos 트래픽의 보안을 유지하도록 IPSec 정책을 구성하는 경우 인증 방법에 Kerberos 가 사용되지 않으면 IPSec 은 보안 연결만 협상할 수 있습니다. 도메인 구성원 간의 인증을 위해 Kerberos 가 필요한 경우 도메인 구성원과 도메인 컨트롤러 간의 Kerberos 에 요구되는 트래픽에 대해 고려해야 할 사항이 있으며 다음 요구 사항을 충족해야 합니다.
  - 도메인 구성원과 도메인 컨트롤러가 다른 도메인의 구성원인 경우 도메인 간에 양방향 트러스트가 형성되어야 하며 그렇게 하지 않으면 IKE(인터넷 키 교환) 키 다시 대조가 실패합니다.
  - 클라이언트 컴퓨터 또는 도메인의 서버가 Kerberos 인증을 사용하여 모든 피어와 IPSec 을 협상하는 경우 모든 도메인 컨트롤러로 전송되는 모든 Kerberos 종속 트래픽에 대해 미러링된 허용 필터를 만들어야 합니다. 도메인 구성원의 도메인에서 각 도메인 컨트롤러 IP 주소에 대한 모든 트래픽을 제외시키는 허용 필터를 만드는 것이 좋습니다. 트러스트된 모든 도메인 컨트롤러 IP 주소에 대한 모든 트래픽을 제외시키는 허용 필터는 만들 필요가 없습니다. 대신 컴퓨터 사이에 있는 트러스트 경로의 모든 도메인 컨트롤러 IP 주소에 대한 Kerberos 트래픽 및 도메인 컨트롤러 사이트 위치(LDAP) 쿼리만 제외시키는 허용 필터를 만드십시오. 도메인 컨트롤러(이미 모든 트래픽이 허용된)에서 DNS 서비스를 제공하지 않으면 도메인 컨트롤러 검색에 DNS 를 사용할 수 있도록 DNS 서버 IP 주소에 대한 DNS 트래픽도 제외시켜야 합니다.

    IPSec 정책에서 이러한 트래픽 유형을 제외시키려면 각각 허용 필터 동작을 갖는 다음 필터를 만듭니다.

    - **내 도메인 컨트롤러로의 모든 트래픽**
      - 미러됨
      - 원본 주소 = **내 IP 주소**
      - 대상 주소 = **특정 IP 주소**(여기서 **특정 IP 주소**는 도메인에 있는 각 도메인 컨트롤의 정적 IP 주소임)
      - 프로토콜 = **모두**

        이 필터는 LDAP 사이트 위치 쿼리와 ICMP, DNS 및 Kerberos 트래픽을 허용합니다. 또한 RPC(원격 프로시저 호출) 트래픽 및 Active Directory 기반 IPSec 정책을 관리하는 데 필요한 그룹 정책 다운로드를 허용합니다.

    - Kerberos
      - 미러됨

- 원본 주소 = **내 IP 주소**
- 대상 주소 = **특정 IP 주소**(여기서 **특정 IP 주소**는 트러스트된 도메인에 있는 각 도메인 컨트롤의 정적 IP 주소임)
- 프로토콜 = UDP
- 원본 포트 = **모두**
- 대상 포트 = 88

이 필터를 만든 후 동일한 설정으로 다른 필터를 만듭니다. 그러나 프로토콜에 대해 TCP 를 지정합니다.

- **도메인 컨트롤러 사이트 위치(LDAP) 쿼리**
  - 미러됨
  - 원본 주소 = **내 IP 주소**
  - 대상 주소 = **특정 IP 주소**(여기서 **특정 IP 주소**는 도메인에 있는 각 도메인 컨트롤의 정적 IP 주소임)
  - 프로토콜 = UDP
  - 원본 포트 = **모두**
  - 대상 포트 = 389
- **DNS 클라이언트 쿼리**
  - 미러됨
  - 원본 주소 = **내 IP 주소**
  - 대상 주소 = **DNS 서버 <동적>**(또는 **특정 IP 주소**. 여기서 IP 주소는 네트워크에 있는 각 DNS 서버의 IP 주소임)
  - 프로토콜 = UDP
  - 원본 포트 = **모두**
  - 대상 포트 = 53

이 필터를 만든 후 동일한 설정으로 다른 필터를 만듭니다. 그러나 프로토콜에 대해 TCP 를 지정합니다.

- 주의
  - 네트워크의 공격 취약성을 최소화하려면 도메인 컨트롤러 및 DNS 서버의 특정 IP 주소에 대해서만 이러한 예외를 허용해야 합니다.

o ICMP 트래픽을 보안하거나 차단하도록 IPSec 정책을 설계할 때 해당 정책을 주의 깊게 계획하고 테스트한 후에 실제 환경에서 구현해야 합니다. 다음과 같은 시나리오에 ICMP 가 필요합니다.

- 링크 프레임 크기가 다른 네트워크를 이동하는 아웃바운드 TCP 연결은 PMTU(경로 최대 전송 단위) 검색을 요구합니다. PMTU 검색이 올바르게

수행되려면 라우터 및 기타 게이트웨이에서의 인바운드 ICMP 트래픽이 수신되어야 합니다.

- **tracert** 명령은 대상으로 가는 경로를 결정하기 위해 ICMP 트래픽을 요구합니다. 그러나 IPSec 이 ICMP 트래픽을 보호하는 경우 **tracert** 출력 결과로 중간 라우터의 경로가 아닌 대상 컴퓨터만 표시됩니다.
- 파일 공유 및 기타 응용 프로그램은 ICMP 트래픽을 사용하여 대상 IP 주소에 도달할 수 있는지 여부를 결정합니다.
- 네트워크 로그온 및 그룹 정책은 각 도메인 컨트롤러 IP 주소에 대한 ICMP 응답 횟수를 측정합니다. 이 작업은 네트워크 로그온을 제공하고 저속 연결에 대해 그룹 정책 설정을 적용할지 여부를 결정하는 도메인 컨트롤러를 선택할 때 도움을 주기 위해 수행됩니다.

일부 경우에는 낮은 수준의 SA(보안되지 않은 연결)가 설정되기 전에 3 초 정도 지연되는 것조차도 빠른 ICMP 응답을 요구하는 상위 계층 통신에 영향을 줄 수 있습니다.

o Windows 2000 및 Windows XP 에서는 기본적으로 브로드캐스트, 멀티캐스트, Kerberos, IKE(인터넷 키 교환) 및 RSVP(Resource Reservation Protocol) 트래픽이 필터 검색에서 제외됩니다. 기본적으로 Windows Server 2003 제품군에서 브로드캐스트, 멀티캐스트, Kerberos 및 RSVP 트래픽은 필터 검색에서 제외되지 않으며 IKE 트래픽만 제외됩니다. 브로드캐스트 및 멀티캐스트 패킷은 보안을 협상하기 위한 필터 동작을 갖는 필터와 일치할 경우 삭제됩니다. 기본적으로 Windows Server 2003 제품군은 브로드캐스트 및 멀티캐스트 트래픽의 필터링을 제한적으로 지원합니다. 원본 주소가 **모든 IP 주소**인 필터는 멀티캐스트 및 브로드캐스트 주소를 찾습니다. 원본 주소가 **모든 IP 주소**이고 대상 주소가 **모든 IP 주소**인 필터는 인바운드 및 아웃바운드 멀티캐스트 주소를 찾습니다. 이러한 필터를 사용하여 모든 트래픽을 차단할 수 있습니다. 그러나 특정 멀티캐스트 또는 브로드캐스트 트래픽을 차단하거나 허용하는 데 사용되는 단방향 필터는 지원되지 않습니다.

Windows Server 2003 제품군에서 구현된 IPSec 에 대한 기본 예외 동작이 변경되었으므로 Windows 2000 또는 Windows XP 용으로 설계된 IPSec 정책의 동작을 확인하고 특정 트래픽 유형을 허용하도록 명시적인 허용 필터를 구성할지 여부를 결정해야 합니다. Windows 2000 및 Windows XP 에서 나타나는 IPSec 정책의 기본 동작을 복원하려면 **netsh ipsec dynamic set config 명령**을 사용하거나 레지스트리를 수정할 수 있습니다.

주의

- IPSec 을 위한 Windows 2000 및 Windows XP 기본 예외 설정은 공격받을 위험이 적은 회사 LAN 환경을 위해 설계되었습니다. 이러한 이유로 위험이 적은

환경에서 문제를 해결해야 하는 경우 또는 IPSec 정책에서 명시적으로 필터를 구성하여 프로그램 호환성 문제를 해결할 수 없을 때만 Windows 2000 및 Windows XP 의 기본 예외 설정을 사용해야 합니다.

28. 안전 모드(네트워킹 사용)

안전 모드(네트워킹 사용)로 컴퓨터를 시작하는 경우 다음을 고려하십시오.

- 안전 모드(네트워킹 사용)로 컴퓨터를 시작하면 IPSec 서비스는 IPSec 정책의 필터를 적용하거나 IP 보안을 협상할 수 없습니다. 따라서 디렉터리 서비스 복원 모드 작업이 진행 중일 때 IPSec 을 요구하는 IPSec 정책을 실행하는 원격 도메인 컨트롤러나 네트워크 백업 장치와의 통신이 발생되지 않습니다.
- 컴퓨터가 시작 중에 Windows 운영 체제를 로드하면 IPSec 드라이버는 TCP/IP 드라이버와 동시에 로드됩니다. IPSec 정책이 컴퓨터에 할당되고 자동 시작을 위해 IPSec 서비스가 구성되면 기본적으로 IPSec 드라이버 시작 모드가 상태 저장 필터링을 수행하도록 변경됩니다. 상태 저장 필터링이 수행되면 모든 아웃바운드 트래픽이 허용되지만 모든 인바운드 트래픽이 차단됩니다. 이때 DHCP 트래픽 및 컴퓨터 시작 중 시작된 아웃바운드 트래픽에 대한 응답으로 보내진 트래픽은 예외입니다. IPSec 드라이버는 아웃바운드 트래픽에 대한 응답을 허용하도록 인바운드 필터를 자동으로 만듭니다. 그러나 IPSec 서비스 자체는 시작되지 않습니다. 따라서 비영구적 또는 로컬 IPSec 정책이나 Active Directory 기반 IPSec 정책을 적용할 수 있습니다.
- 컴퓨터가 안전 모드(네트워킹 사용)인 경우 특정 트래픽의 인바운드 예외를 구성하여 IPSec 드라이버에서 상태 저장 필터링 보호 기능을 계속 제공하도록 할 수 있습니다. 또는 IPSec 드라이버에서 모든 트래픽을 허용하도록 할 수 있습니다.
- 특정 트래픽에 대해 안바운드 예외를 구성하려면 정상적으로 컴퓨터를 다시 시작하고(안전 모드가 아닌 모드로) netsh ipsec dynamic set config bootexemptions 명령을 사용하여 컴퓨터 시작 중에 제외시킬 트래픽 유형을 지정한 다음 컴퓨터를 다시 시작합니다. 컴퓨터가 다시 시작될 때 새로운 예외가 적용되며 삭제 또는 변경될 때까지 계속 적용됩니다.
- IPSec 드라이버에서 특정 트래픽에 대해 인바운드 예외를 구성하도록 할 경우 예외를 적절히 구성하지 않으면 다음과 같은 문제가 발생할 수 있습니다.
  - 원격 데스크톱 연결 및 원격 지원과 같은 네트워크 서비스에 대한 인바운드 연결이 차단되므로 연결을 수신하기 위해 포트가 열립니다. 클라이언트에서 원격 데스크톱 연결 또는 원격 지원을 사용하게 하려면 TCP 포트 3389 에 대한 인바운드 트래픽을 허용하도록 예외를 구성해야 합니다. 이 예외를 구성하려면 다음 Netsh 명령을 사용하십시오.

    netsh ipsec dynamic set config bootexemptions TCP:any:3389:inbound

- PMTU 검색을 요구하는 연결 같은 일부 아웃바운드 TCP 연결이 작동하지 않을 수 있습니다. TCP PMTU 검색을 사용하도록 설정하려면 인바운드 ICMP 트래픽을 허용하도록 예외를 구성해야 합니다. 이 예외를 구성하려면 다음 Netsh 명령을 사용하십시오.

  netsh ipsec dynamic set config bootexemptions ICMP:inbound

o 중요

- bootexemptions= 매개 변수를 수정하여 시작 보안에서 제외되는 IPSec 트래픽 예외를 수정할 경우 시작 보안의 이전 예외를 모두 덮어쓰게 됩니다.

컴퓨터가 안전 모드(네트워킹 사용)인 동안 IPsec 드라이버에서 모든 인바운드 트래픽을 허용하게 하려면 수동 시작을 위해 IPSec 서비스를 구성하거나 IPSec 서비스를 비활성화한 다음 안전 모드(네트워킹 사용)로 컴퓨터를 다시 시작해야 합니다.

29. 필터 동작

IP 필터 동작을 구성할 때 다음 특별 요구 사항을 고려합니다.

- 유효하지 않은 주소 또는 특정한 TCP 포트와의 트래픽과 같이 항상 차단하려는 특정한 트래픽이 있으면 **보안 방법**을 **거부**로 설정하여 거부 필터 동작을 만듭니다.
- 항상 보안하지 않으려는 특정한 트래픽이 있으면 **보안 방법**을 **허용**으로 설정하여 허용 필터 동작을 만듭니다.
- 암호화된 트래픽에 사용자 지정 보안 방법을 구성할 경우 더 높은 층의 프로토콜로 데이터 암호화를 제공하려면 ESP 기밀성 선택을 **<없음>**으로 설정해야 합니다.
- 지점 간의 IPSec 터널링과 같은 인터넷 시나리오를 계획하고 있을 경우 세션 키에 3DES 와 같은 높은 수준의 보안, 짧은 키 수명(50MB 미만) 및 PFS(전달 완전 보안)를 지정하는 보안 방법 목록의 사용을 고려합니다. 이렇게 하면 알려진 키 공격으로부터 보호할 수 있습니다.

참고

- Windows 2000 을 실행하는 컴퓨터는 3DES 알고리즘을 사용하려면 고급 암호화 팩 또는 서비스 팩 2 이상이 설치되어 있어야 합니다. Windows 2000 을 실행하는 컴퓨터에 3DES 가 설정되어 있지만 고급 암호화 팩 또는 서비스 팩 2 이상이 설치되어 있지 않으면 보안 방법의 3DES 설정은 통신을 전면적으로 차단하기보다는 일정 수준의 기밀성을 유지할 수 있도록 약하게 설정됩니다. 그러나 일부 컴퓨터에서만 3DES 를 사용할 수 있는 환경에서는 DES 를 폴백 옵션으로만 사용해야 합니다. Windows XP

또는 Windows Server 2003 운영 체제를 실행하는 컴퓨터에서는 3DES 를 지원하므로 고급 암호화 팩을 설치할 필요가 없습니다.

6) IPv6

A. IPv6 라우팅

라우팅은 연결된 네트워크 세그먼트 사이에서 패킷을 전달하는 과정입니다. IPv6 기반 네트워크의 경우 라우팅은 더 큰 IPv6 기반 네트워크 내 별도의 세그먼트에 있는 호스트 사이에서 전달 기능을 제공하는 IPv6 의 일부입니다.

IPv6 은 IPv6 데이터 정렬 및 배달이 이루어지는 메일룸입니다. 들어오거나 나가는 각각의 패킷을 IPv6 패킷이라고 합니다. IPv6 패킷에는 보내는 호스트의 원본 주소와 받는 호스트의 대상 주소가 모두 들어 있습니다. 연결 계층 주소와 달리 IPv6 헤더의 IPv6 주소는 일반적으로 IPv6 네트워크에서 패킷이 이동하는 것과 같습니다.

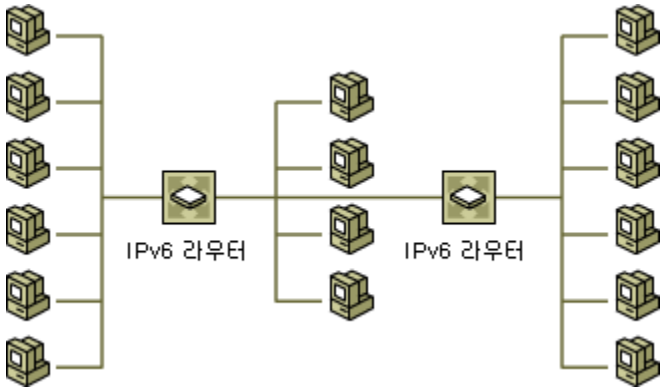
라우팅은 IPv6 의 주 기능입니다. IPv6 패킷은 인터넷 계층에서 IPv6 을 사용하여 각 호스트에서 교환되고 처리됩니다.

IPv6 계층 위에서 원본 호스트의 전송 서비스는 TCP 세그먼트 또는 UDP 메시지 유형으로 IPv6 계층에 데이터를 전달합니다. IPv6 계층에서는 네트워크를 통해 데이터의 경로를 정하는 데 사용되는 원본 및 대상 주소와 함께 IPv6 패킷을 만듭니다. 그런 다음 IPv6 계층은 패킷을 연결 계층으로 전달하고 연결 계층에서 IPv6 패킷은 실제 네트워크의 네트워크별 미디어를 통해 전송할 수 있는 프레임으로 변환됩니다. 대상 호스트에서는 이러한 과정이 반대의 순서로 발생합니다.

보내는 각 호스트의 IPv6 계층 서비스는 각 패킷의 대상 주소를 조사하고 그 주소를 로컬로 유지 관리되는 라우팅 테이블과 비교한 다음 추가 전달 작업이 필요한지 결정합니다. IPv6 라우터는 서로 간에 패킷을 전달할 수 있는 여러 IPv6 네트워크 세그먼트에 연결되어 있습니다.

B. IPv6 라우터

링크 또는 서브넷이라고도 하는 IPv6 네트워크 세그먼트는 IPv6 라우터로 연결되며 IPv6 라우터는 네트워크 세그먼트 사이에서 IPv6 패킷을 전달하는 장치입니다. 이러한 과정을 IPv6 라우팅이라고 하며 다음 그림에 표시되어 있습니다.



IPv6 라우터는 실제로 분리된 여러 IPv6 네트워크 세그먼트를 결합하는 주요 방법을 제공합니다. 모든 IPv6 라우터에는 다음과 같은 특징이 있습니다.

- IPv6 라우터는 물리적 다중홈 호스트입니다.

  물리적 다중홈 호스트는 여러 네트워크 연결 인터페이스를 사용하여 실제로 분리된 각 네트워크 세그먼트를 연결하는 네트워크 호스트입니다.

- IPv6 라우터는 다른 IPv6 호스트에 패킷 전달을 제공합니다.

  IPv6 라우터는 다중홈을 사용하는 다른 호스트와 구별됩니다. IPv6 라우터는 다른 IPv6 네트워크 호스트에 네트워크 사이의 IPv6 기반 통신을 전달할 수 있어야 합니다.

IPv6 프로토콜로 Windows Server 2003 제품군을 실행하는 컴퓨터를 포함하여 다양한 하드웨어 및 소프트웨어 제품을 사용하여 IPv6 라우터를 구현할 수 있습니다. 전문 소프트웨어를 실행하는 전용 하드웨어 장치인 라우터가 일반적입니다. 사용하는 IPv6 라우터의 종류에 관계없이 모든 IPv6 라우팅은 라우팅 테이블을 사용하여 네트워크 세그먼트 사이에서 통신합니다.

C.라우팅 테이블

IPv6 호스트는 라우팅 테이블을 사용하여 다른 IPv6 네트워크 및 IPv6 호스트에 대한 정보를 유지 관리합니다. IPv6 네트워크 접두사와 접두사 길이를 사용하여 네트워크 세그먼트를 식별합니다. 또한 라우팅 테이블은 원격 네트워크 및 호스트와 통신하는 방법과 관련하여 중요한 정보를 각 로컬 호스트에 제공합니다.

IPv6 네트워크의 각 컴퓨터에 대해서는 로컬 컴퓨터와 통신하는 네트워크나 다른 모든 컴퓨터의 항목이 들어 있는 라우팅 테이블을 유지 관리할 수 있습니다. 일반적으로 이 방법은 실용적이지 않으므로 기본 라우터가 사용됩니다.

컴퓨터에서는 IPv6 패킷을 전달하기 전에 원본 IPv6 주소와 받는 사람에 대한 대상 IPv6 주소를 IPv6 헤더에 삽입합니다. 그런 다음 컴퓨터는 대상 IPv6 주소를 조사하고 그 주소를 로컬로 유지 관리되는 IPv6 라우팅 테이블과 비교한 다음 적절한 작업을 수행합니다. 컴퓨터는 아래의 세 가지 중 하나를 실행합니다.

- 패킷을 로컬 호스트의 IPv6 위에 있는 프로토콜 계층으로 보냅니다.
- 연결된 네트워크 인터페이스 중 하나를 통해 패킷을 전달합니다.
- 패킷을 버립니다.

IPv6 은 라우팅 테이블에서 대상 IPv6 주소와 가장 가깝게 일치하는 경로를 검색합니다. 가장 구체적인 경로에서 가장 구체적이지 않은 경로의 순서는 아래와 같습니다.

1. 대상 IPv6 주소와 일치하는 경로(접두사 길이가 128 비트인 호스트 경로)
2. 접두사 길이가 가장 긴 대상과 일치하는 경로
3. 기본 경로(네트워크 접두사 ::/0)

일치하는 경로를 찾지 못하면 그 대상은 온링크 대상으로 결정됩니다.

D. IPv6 구성 항목

IPv6 프로토콜에 대해 다음 항목을 구성할 수 있습니다.

- IPv6 주소
- 기본 라우터
- DNS 서버

1. IPv6 주소

기본적으로 로컬 링크 주소는 고유한 로컬 링크 IPv6 주소가 있는 각각의 IPv6 노드(호스트 또는 라우터)에서 각 인터페이스에 대해 자동으로 구성됩니다. 연결된 링크에 없는 IPv6 노드와 통신하려면 호스트에 추가 로컬 사이트 주소나 글로벌 유니캐스트 주소가 있어야 합니다. 호스트의 추가 주소는 라우터가 보낸 라우터 알림에서 가져오거나 수동으로 할당됩니다. 라우터의 추가 주소는 수동으로 할당해야 합니다.

2. 기본 라우터

다른 네트워크 세그먼트에 있는 IPv6 노드와 통신하려면 IPv6 은 기본 라우터를 사용해야 합니다. 기본 라우터는 라우터 알림을 받으면 자동으로 할당됩니다. 또한 IPv6 라우팅 테이블에 기본 라우터를 추가할 수 있습니다. 단일 네트워크 세그먼트로 구성된 네트워크에 대해서는 기본 라우터를 구성하지 않아도 됩니다.

3. DNS 서버

DNS(Domain Name System) 서버를 사용하여 IPv6 주소의 호스트 이름을 확인할 수 있습니다. IPv6 호스트를 DNS 서버 주소로 구성하면 호스트는 DNS 이름 쿼리를 서버로 보내 확인합니다. DNS 서버에 저장되어 있는 4A(AAAA) 리소스 레코드를 사용하여 호스트 이름에서 IPv6 주소로 매핑할 수 있습니다.

DNS 이름 확인을 사용하려면 전달을 사용 가능하게 하고 클라이언트에 알리는 글로벌 접두사를 사용하여 IPv6 라우터를 구성합니다. **netsh interface ipv6 add route** 및 **netsh interface ipv6 set interface** 명령을 사용하여 이 작업을 수행할 수 있습니다. 기본적으로 DNS 는 DNS 동적 업데이트를 할 수 있도록 구성됩니다. DNS 와 함께 IPv6 을 사용할 때 동적 업데이트를 사용 가능하게 하거나 IPv6 클라이언트에 대해 DNS 레코드를 수동으로 추가할 수 있습니다.

3-1 DNS 서버 주소로 클라이언트 구성

DNS 클라이언트와 서버 간에 통신을 제공하려면 DNS 서버의 IPv6 주소로 클라이언트를 구성하거나 모든 IPv6 클라이언트에서 자동으로 구성되는 세 가지 기본 DNS 서버 IPv6 주소 중 하나로 DNS 서버를 구성할 수 있습니다.

각 클라이언트 컴퓨터에서 **netsh interface ipv6 add dns** 명령을 사용하거나 클라이언트가 네트워크에 로그온할 때마다 실행되는 로그온 스크립트에서 DNS 서버의 IPv6 주소로 클라이언트를 구성할 수 있습니다.

기본적으로 IPv6 클라이언트 컴퓨터에서 사용할 수 있는 세 가지 IPv6 주소 중 하나로 DNS 서버를 구성하려면 **netsh interface ipv6 add address** 명령을 사용합니다. 세 가지 기본 DNS 서버 주소는 다음과 같습니다.

- FEC0:0:0: FFFF::1
- FEC0:0:0: FFFF::2
- FEC0:0:0:FFFF::3

DNS 서버가 IPv6 클라이언트와는 다른 서브넷에 있는 경우 DNS 서버의 서브넷에서 사용할 수 있는 IPv6 라우터의 DNS 서버에 대한 정적 경로를 구성합니다.

3-2. IPv6 에서 수신 대기하도록 DNS 구성

IPv6 을 통해 DNS 이름 등록과 확인 요청을 수신 대기하도록 DNS 서버를 구성할 수 있습니다. DNS 서버가 IPv4 와 IPv6 에서 모두 수신 대기하도록 구성된 경우 다음이 수행됩니다.

- IPv6 에서는 작동하지만 IPv4 에서는 작동하지 않는 장치는 DNS 서버에서 제대로 작동합니다.
- IPv4 와 IPv6 을 모두 사용하여 구성된 컴퓨터와 기타 장치는 기본적으로 IPv6 을 사용합니다.

IPv6 을 통해 수신 대기하도록 DNS 서버를 구성하려면 다음을 수행하십시오.

1. Windows 지원 도구를 설치합니다.

   자세한 내용은 Windows 지원 도구 설치를 참조하십시오.

2. 명령 프롬프트를 엽니다.
3. 다음 명령을 입력합니다.

   dnscmd /config /EnableIPv6 1

4. DNS 서버 서비스를 다시 시작합니다.

   자세한 내용은 DNS 서버 시작 또는 중지를 참조하십시오.

3-3. IPv6 프로토콜 기능

Microsoft® Windows® Server 2003 제품군의 IPv6 프로토콜에는 다음 기능이 있습니다.

a. 6to4 터널링

6to4 는 RFC 3056 에서 설명하는 터널링 기법입니다. 6to4 호스트는 수동 구성을 요구하지 않으며 표준 자동 구성을 사용하여 6to4 주소를 만듭니다. 6to4 는 글로벌 주소 접두사 2002:*WWXX*:*YYZZ*::/48 을 사용하며 여기서 *WWXX*:*YYZZ* 는 사이트나 호스트에 할당된 공용 IPv4 주소(*w.x.y.z*)를 콜론으로 구분한 16 진수 표시법입니다. WWXX:YYZZ 는 6to4 주소의 NLA(Next Level Aggregator) 부분입니다.

6to4 를 사용하면 IPv6 사용 가능 사이트와 호스트는 유니캐스트 IPv6 을 사용하여 통신할 수 있습니다. IPv6 사이트와 호스트는 6to4 주소 접두사와 인터넷을 사용하여 인터넷 서비스 공급자로부터 IPv6 글로벌 주소 접두사를 얻거나 IPv6 인터넷에 연결하지 않고 통신할 수 있습니다.

b. ISATAP(Intrasite Automatic Tunnel Addressing Protocol)

ISATAP(Intrasite Automatic Tunnel Addressing Protocol)는 IPv4 사이트 내 IPv6/IPv4 노드 간 통신에 사용하는 주소 할당 및 터널링 기술입니다. 이 기술은 "Intra-Site Automatic Tunnel

Addressing Protocol (ISATAP)"(draft-ietf-ngtrans-isatap-0*x*.txt)이라는 제목으로 인터넷 기초에 설명되어 있습니다.

c. 임시 주소

인터넷 리소스에 액세스할 때 익명 수준을 제공하려면 임의의 숫자를 사용하여 임시 글로벌 주소를 만들어 글로벌 IPv6 주소의 64 비트 인터페이스 식별자를 파생시킵니다.

d. 라우터 알림의 사이트 접두사

게시된 온링크 접두사는 "Site prefixes in Neighbor Discovery"(draft-ietf-ipngwg-site-prefixes-0*x*.txt)라는 제목으로 인터넷 기초에 설명된 대로 사이트 접두사 길이로 구성할 수 있습니다. **netsh interface ipv6 add route** 명령을 사용하여 주소 접두사와 함께 사이트 접두사 길이를 포함할 수 있습니다.

사이트 접두사를 지정하는 접두사 정보 옵션을 받으면 사이트 접두사 테이블에 항목이 만들어집니다. **netsh interface ipv6 show siteprefixes** 명령을 사용하여 이 테이블을 볼 수 있습니다. 사이트 접두사 테이블을 사용하여 **getaddrinfo()** Windows 소켓 함수에서 반환한 주소에서 부적절한 로컬 사이트 주소를 제거할 수 있습니다.

e. DNS 지원

RFC 1886, "DNS Extensions to support IP version 6"에서 정의된, AAAA 또는 4A 리소스 레코드라고도 하는 DNS(Domain Name System) IPv6 호스트 레코드 처리는 Microsoft® Windows® XP 및 Windows Server 2003 제품군의 DNS 확인자(클라이언트) 및 Windows Server 2003 제품군과 Windows 2000 의 DNS 서버 서비스에서 지원합니다. 모든 DNS 트래픽은 IPv4 나 IPv6 을 통해 전달됩니다.

f. IPSec 지원

MD5(Message Digest 5) 해시를 사용한 AH(인증 헤더)의 처리 및 NULL ESP 헤더와 MD5 해시를 사용한 ESP(Encapsulating Security Payload)가 지원됩니다. ESP 데이터 암호화는 지원되지 않습니다.

주의

- 이러한 IPv6 의 IPSec 구현은 정적 키 입력에 의존하며 시퀀스 번호 재사용 시 키를 업데이트할 규정이 없기 때문에 프로덕션 환경에 사용하지 않는 것이 좋습니다.

g. 응용 프로그램 지원

Windows Server 2003 제품군과 함께 제공되며 IPv6 사용을 지원하는 응용 프로그램과 구성 요소는 다음과 같습니다.

- DCOM(Distributed Component Object Model)
- DFS(분산 파일 시스템)
- DNS(Domain Name System) 서버 및 클라이언트
- 파일 및 인쇄 공유
- FTP(파일 전송 프로토콜) 클라이언트
- Internet Explorer
- Microsoft .NET Framework
- 네트워크 모니터
- 텔넷 서버 및 텔넷 클라이언트
- Windows Media 서비스
- Windows 소켓

h. RPC 지원

네트워크를 통해 원격 시스템으로 응용 프로그램 기능 호출을 전달하는 데 사용되는 RPC(원격 프로시저 호출) 기능은 IPv6 을 통해 사용할 수 있습니다. 일반적으로 RPC 는 원격 관리에 사용됩니다.

I. 정적 라우터 지원

Windows Server 2003 제품군의 구성원을 실행하는 컴퓨터는 IPv6 라우팅 테이블의 내용을 기반으로 하는 인터페이스 사이에서 IPv6 패킷을 전달하는 정적 IPv6 라우터 역할을 합니다. **netsh interface ipv6 add route** 명령으로 정적 경로를 구성할 수 있습니다. 현재 IPv6 라우팅 프로토콜은 지원되지 않습니다.

Windows Server 2003 제품군의 구성원을 실행하는 컴퓨터는 라우터 알림을 보낼 수 있습니다. 라우터 알림의 내용은 라우팅 테이블에 게시된 경로에서 자동으로 파생됩니다. 게시되지 않은 경로는 라우팅에 사용되지만 라우터 알림에서 전달되지는 않습니다. 라우터 알림에는 항상 원본 연결 계층 주소 옵션과 MTU 옵션이 있습니다. MTU 옵션 값은 보내는 인터페이스의 현재 링크 MTU 에서 가져옵니다. 다음 Netsh 명령을 사용하여 이 값을 변경할 수 있습니다.

netsh interface ipv6 set interface [**interface=**]*String* [[**mtu=**]*Integer*]

Windows Server 2003 제품군의 구성원을 실행하는 컴퓨터는 게시되도록 구성된 기본 경로가 있는 경우 0 이 아닌 라우터 수명과 함께 라우터 알림을 사용하여 기본 라우터로 자신을 알리기만 합니다.

j. 명령줄 도구 지원

다음 명령줄 도구가 Windows Server 2003 제품군에 제공되며 IPv6 사용과 구성을 지원합니다.

- 인터페이스 IPv6 에 대한 netsh 명령
- 인터페이스 Portproxy 에 대한 netsh 명령
- Ipconfig
- Pathping
- Ping
- Route
- Tracert
- Netstat

Windows Server 2003 제품군과 Windows XP 에 제공되는 Netstat 명령줄 도구에는 IPv6 관련 통계 지원이 들어 있습니다. 네 가지의 통계 범주가 있습니다.

1. IPv6 통계
2. ICMPv6 통계
3. TCP 연결에 대한 IPv6 통계
4. UDP 트래픽에 대한 IPv6 통계

k. 6over4 터널링

IPv4 멀티캐스트 터널링이라고도 하는 6over4 는 RFC 2529 에서 설명하는 터널링 기술입니다. 6over4 를 사용하면 IPv6 및 IPv4 노드는 IPv4 하부 구조를 통해 IPv6 을 사용하여 통신할 수 있습니다. 6over4 는 IPv4 하부 구조를 멀티캐스트 가능 링크로 사용합니다. 6over4 가 제대로 작동하려면 IPv4 하부 구조는 IPv4 멀티캐스트가 가능해야 합니다.

E. IPv6 구성 방법

IPv6 프로토콜에서는 다음 구성 방법을 사용할 수 있습니다.

- 상태 비저장 주소를 사용하는 자동 구성
- 수동 구성

1. 자동 구성

IPv6 프로토콜은 RFC 2462, "IPv6 Stateless Address Autoconfiguration"에 정의된 대로 상태 비저장 주소에 대한 주소 자동 구성을 지원합니다. IPv6 노드(호스트 및 라우터)는 이더넷이나 FDDI 인터페이스로 나타나는 모든 LAN 인터페이스에 대해 고유한 로컬 링크 주소를 자동으로 만듭니다. IPv6 호스트는 받은 라우터 알림 메시지를 사용하여 자동으로 다음을 구성합니다.

- 기본 라우터
- IPv6 헤더 홉 제한 시간 필드의 기본 설정
- 주소 및 기타 구성에 필요한 요구 사항으로 노드에서 DHCPv6(Dynamic Host Configuration Protocol for IPv6) 같은 상태 저장 주소 구성 프로토콜을 사용해야 하는지 여부의 결정입니다. Windows Server 2003 제품군의 IPv6 프로토콜은 DHCPv6 이나 다른 상태 저장 주소 구성 프로토콜을 현재 지원하지 않습니다.
- 인접 탐색 과정에 사용되는 타이머
- 로컬 링크의 MTU(최대 전송 단위)
- 링크에 대해 정의된 네트워크 접두사 목록입니다. 각 네트워크 접두사에는 IPv6 네트워크 접두사와 유효 및 기본 수명이 모두 포함됩니다. 표시되는 경우 네트워크 접두사는 인터페이스 식별자와 결합하여 받는 인터페이스에 대해 상태 비저장 IPv6 주소 구성을 만듭니다. 네트워크 접두사도 로컬 링크에 있는 노드의 주소 범위를 정의합니다.

또한 Windows Server 2003 제품군의 IPv6 프로토콜은 자동으로 다음을 구성합니다.

- 컴퓨터에 할당된 모든 공용 IPv4 주소에 대해 6to4 터널링 인터페이스의 6to4 주소(라우터 알림을 받지 못하고 컴퓨터가 공용 IPv4 주소로 구성된 경우)
- 컴퓨터에 할당된 모든 IPv4 주소에 대한 자동 터널링 의사 인터페이스에 ISATAP(Intrasite Automatic Tunnel Addressing Protocol) 주소
- Windows Server 2003 제품군의 구성원을 실행하는 라우터에서 오프링크 주소 접두사를 알려 준 경우 오프링크 접두사에 대한 경로

2. IPv6 주소 자동 구성

IPv6 의 매우 유용한 측면은 DHCPv6(Dynamic Host Configuration Protocol for IPv6) 같은 상태 저장 구성 프로토콜을 사용하지 않고 자동으로 IPv6 주소를 구성할 수 있는 기능입니다. 기본적으로 IPv6 호스트는 각 인터페이스에 대해 로컬 링크 주소를 구성할 수 있습니다. 또한 라우터 검색을 사용하여 호스트는 라우터 주소, 추가 주소 및 기타 구성 매개 변수를 결정할 수도 있습니다. 상태 저장 주소 구성 프로토콜을 사용해야 하는지 여부를 나타내는 표시는 라우터 알림 메시지에 포함됩니다.

주소 자동 구성은 멀티캐스트 가능한 인터페이스에서만 수행할 수 있습니다. 주소 자동 구성은 RFC 2462, "IPv6 Stateless Address Autoconfiguration"에 설명되어 있습니다.

3. 자동 구성된 주소 상태

자동 구성된 주소는 다음 상태 중 하나 이상이 될 수 있습니다.

- 미정

  고유한 주소인지 확인 중에 있는 주소입니다. 중복되는 주소 검색을 통해 확인합니다.

- 기본

  고유성이 확인된 주소입니다. 한 노드에서 기본 주소 간의 유니캐스트 트래픽을 주고 받을 수 있습니다. 주소가 미정과 기본 상태로 유지될 수 있는 기간은 라우터 알림 메시지에 포함되어 있습니다.

- 사용하지 않음

  아직까지는 유효하지만 새 통신에는 사용하지 않는 것이 좋은 주소입니다. 기존의 통신 세션에서는 사용하지 않는 주소를 계속 사용할 수 있습니다. 한 노드에서 사용하지 않는 주소 간에 유니캐스트 트래픽을 주고 받을 수 있습니다.

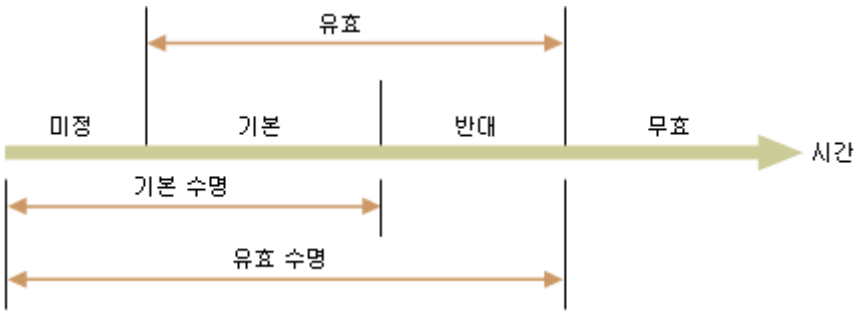
- 유효

  유니캐스트 트래픽을 주고 받을 수 있는 주소입니다. 유효 상태는 기본 및 사용하지 않음 상태를 모두 포괄합니다. 주소가 미정과 유효 상태로 유지될 수 있는 기간은 라우터 알림 메시지에 포함되어 있습니다. 유효 상태의 수명은 기본 상태 수명보다 길거나 같아야 합니다.

- 유효하지 않음

  노드에서 더 이상 유니캐스트 트래픽을 주고 받을 수 없는 주소입니다. 유효 상태의 수명이 만료되면 주소는 유효하지 않음 상태가 됩니다.

자동 구성된 주소 상태 사이의 관계와 기본 수명 및 유효 수명이 다음 그림에 표시되어 있습니다.



참고

- 로컬 링크 주소를 제외하면 주소 자동 구성은 호스트에 대해서만 지정됩니다. 라우터는 수동 구성 같은 다른 방법을 통해 주소 및 구성 매개 변수를 얻어야 합니다.

4. 자동 구성의 종류

다음과 같은 세 종류의 자동 구성이 있습니다.

1. 상태 비저장

주소 구성은 라우터 알림 메시지 수신을 기초로 합니다. 이 메시지에는 상태 비저장 주소 접두사가 포함되어 있으며 호스트는 상태 저장 주소 구성 프로토콜을 사용하지 않습니다.

2. 상태 저장

구성은 DHCPv6 같은 상태 저장 주소 구성 프로토콜을 기초로 하여 주소 및 다른 구성 옵션을 가져옵니다. 호스트는 주소 접두사가 없는 라우터 알림 메시지를 받을 때 상태 저장 주소 구성을 사용하며 호스트는 상태 저장 주소 구성 프로토콜을 사용합니다. 또한 호스트는 로컬 링크에 나타나는 라우터가 없을 때 상태 저장 주소 구성 프로토콜을 사용하게 됩니다.

3. 모두

주소 구성은 라우터 알림 메시지 수신을 기초로 합니다. 이 메시지에는 상태 비저장 주소 접두사가 포함되어 있고 호스트는 상태 저장 주소 구성 프로토콜을 사용합니다.

자동 구성 종류 모두에 대해 로컬 링크 주소를 항상 구성할 수 있습니다.

5. 자동 구성 과정

IPv6 노드의 주소 자동 구성 과정은 다음과 같습니다.

1. 미정 로컬 링크 주소는 로컬 링크 접두사 FE80::/64 와 64 비트 인터페이스 식별자를 기준으로 파생됩니다.
2. 중복되는 주소 검색을 수행하여 미정 로컬 링크 주소의 고유성을 확인합니다.
3. 중복되는 주소 검색에 실패하면 노드에서 수동으로 구성해야 합니다.
4. 중복되는 주소 검색에 성공하면 미정 로컬 링크 주소는 고유하며 유효한 것으로 간주됩니다. 로컬 링크 주소는 인터페이스에 대해 초기화됩니다. 대응하는 요청된 노드 멀티캐스트 링크 계층 주소는 네트워크 어댑터로 등록됩니다.

IPv6 호스트의 경우 주소 자동 구성은 다음과 같이 진행됩니다.

1. 호스트는 라우터 요청 메시지를 보냅니다.
2. 라우터 알림 메시지를 받지 못하면 호스트는 상태 저장 주소 구성 프로토콜을 사용하여 주소 및 다른 구성 매개 변수를 얻습니다. Windows Server 2003 제품군과 Windows XP 의 IPv6 프로토콜은 상태 저장 주소 구성 프로토콜의 사용을 지원하지 않습니다.
3. 라우터 알림 메시지를 받으면 메시지에 포함된 구성 정보는 호스트에서 설정합니다.
4. 각 상태 비저장 자동 구성 주소 접두사는 다음과 같습니다.
    - 주소 접두사와 적절한 64 비트 인터페이스 식별자를 사용하여 미정 주소를 파생시킵니다.
    - 중복되는 주소 검색을 사용하여 미정 주소의 고유성을 확인합니다.
        - 미정 주소를 사용하고 있으면 주소는 인터페이스에 대해 초기화되지 않습니다.
        - 미정 주소를 사용하지 않으면 주소가 초기화됩니다. 라우터 알림 메시지에 포함된 정보를 기준으로 하는 유효 수명 및 기본 수명을 포함합니다.
5. 라우터 알림 메시지에서 지정하면 호스트는 상태 저장 주소 구성 프로토콜을 사용하여 추가 주소나 구성 매개 변수를 가져옵니다.

참고

- IPv6 은 업계 표준으로 빠르게 발전하고 있습니다. 여기서 언급한 RFC 는 최신 RFC 로 대체되었을 수도 있습니다.
- IPv6 의 상태 저장 주소 구성 표준은 현재 개발 중입니다. Windows Server 2003 제품군과 Windows XP 의 IPv6 프로토콜은 상태 저장 주소 구성 또는 DHCPv6 프로토콜을 지원하지 않습니다.

6. 수동 구성

IPv6 명령줄 도구의 Netsh 명령을 사용하여 IPv6 주소 및 경로를 수동으로 구성할 수 있습니다. 수동 구성은 라우터가 라우터 알림을 보내도록 구성되지 않은 여러 IPv6 네트워크 세그먼트가 있는 네트워크에 필요할 수 있습니다. 다음은 수동으로 구성하는 방법입니다.

수동으로 IPv6 주소를 구성하려면

1. 명령 프롬프트를 엽니다.
2. 명령 프롬프트에서 **netsh** 를 입력한 다음 Enter 키를 누릅니다.
3. **interface ipv6** 을 입력한 다음 Enter 키를 누릅니다.
4. **add address** [**interface=**]*String* [**address=**]*IPv6Address* 를 입력합니다.

   여기에서

   [**interface=**]*String*
   인터페이스 이름을 지정합니다.
   [**address=**]*IPv6Address*
   IPv6 주소를 지정합니다.

7. IPv6 연결 테스트

Ping 명령을 사용하여 IPv6 연결을 테스트하려면

1. 컴퓨터의 IPv6 구성을 보려면 명령 프롬프트를 열고 **netsh interface ipv6 show interface** *InterfaceName* 을 입력합니다. 여기서 *InterfaceName* 은 컴퓨터의 인터페이스 이름입니다. 예를 들어 로컬 영역 연결이라는 인터페이스가 있는 경우 다음 명령을 입력합니다.

   netsh interface ipv6 show interface "Local Area Connection"

   IPv6이 설치되어 있지 않으면 관련 항목을 참조하십시오.

2. 다음 명령을 사용하여 다른 IPv6 노드를 ping 합니다.
   - 서브넷이라고도 하는 링크에서 다른 노드의 로컬 링크 주소를 ping 하려면 다음을 입력합니다.

     ping *Address***%***ZoneID*

     여기서 *Address* 는 다른 노드의 로컬 링크 주소이고 *ZoneID* 는 ping 패킷을 전달하려는 인터페이스의 인터페이스 색인입니다. **netsh interface ipv6 show interface** 명령 결과 표시된 화면에서 인터페이스 색인을 가져올 수 있습니다.

     ping 명령이 실패한 경우에는 다른 노드 및 영역 ID 의 로컬 링크 주소를 확인하십시오.

- 다른 노드의 로컬 사이트 주소를 ping 하려면 다음을 입력합니다.

  ping *Address*%*ZoneID*

  여기서 *Address* 는 다른 노드의 로컬 사이트 주소이고 *ZoneID* 는 **netsh interface ipv6 show interface level=verbose** 명령 결과 화면에 표시되는 부분에서 가져온 사이트 식별자(사이트의 영역 ID)입니다. 사이트 식별자를 사용하지 않거나 단일 사이트만 있는 경우에는 명령에서 **%***ZoneID* 부분이 필요 없습니다.

  Ping 명령이 실패한 경우에는 다른 `노드 및 영역 ID 의 로컬 사이트 주소를 확인하십시오.

- 다른 글로벌 노드의 주소를 ping 하려면 다음을 입력합니다.

  ping *Address*

  여기서 *Address* 는 다른 글로벌 노드의 주소입니다.

  ping 명령이 실패한 경우에는 다른 글로벌 노드의 주소를 확인하십시오.

- 다른 노드를 이름별로 ping 하려면 다음을 입력합니다.

  ping -6 *Name*

  여기서 *Name* 은 로컬 호스트 파일의 항목이나 DNS(Domain Name System) 하부 구조에 있는 AAAA 리소스 레코드를 통해 IPv6 주소로 확인될 수 있는 이름입니다. IPv6 주소 대신 이름으로 대상 호스트를 확인할 때는 IPv6 주소를 사용하도록 명령에 매개 변수 **-6** 을 포함해야 합니다.

  Ping 명령이 실패한 경우에는 이름이 IPv6 주소로 확인될 수 있는지 확인하십시오.

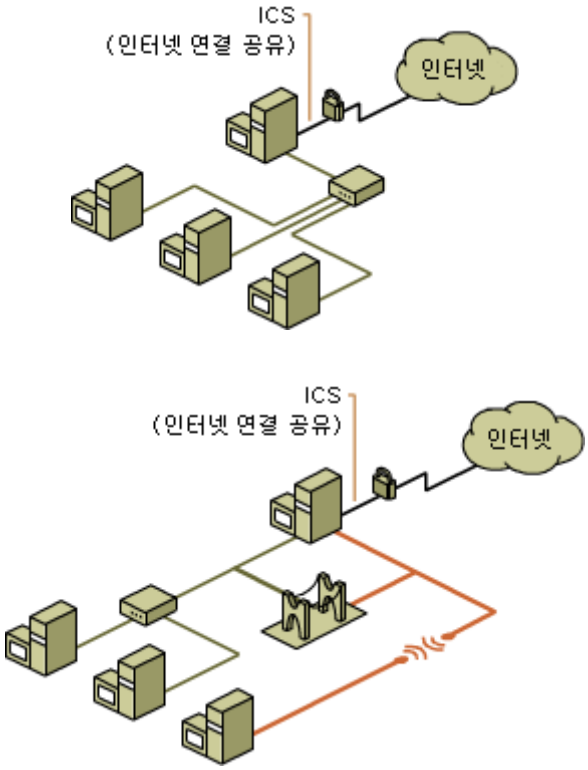
7) 인터넷 연결 방화벽

A. 인터넷 연결 방화벽의 개요

홈 네트워크 및 소규모 네트워크는 인터넷에 직접 연결된 컴퓨터에 방화벽 보호로 추가 보안을 제공합니다. ICF(인터넷 연결 방화벽)는 네트워크와 인터넷 사이의 연결을 통과하는 모든 통신을 검사하고, 인터넷을 통해 받을 수 있는 응답을 선택합니다.

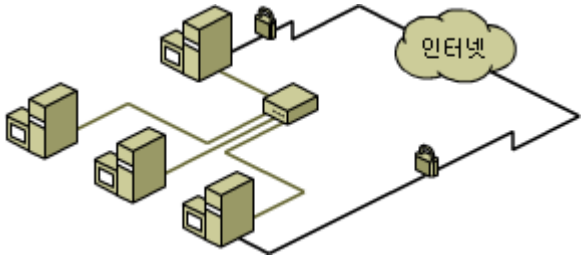
B. 권장 토폴로지

ICS(인터넷 연결 공유)는 사용자 네트워크에서 하나의 인터넷 연결에만 사용할 수 있으며 ICF 를 사용하여 이 연결을 보호해야 합니다. ICF 는 ICF 가 설정된 인터넷 연결을 통과하는 통신만 확인할 수 있습니다. 이러한 유형의 네트워크 토폴로지가 안전하고 가장 바람직합니다.

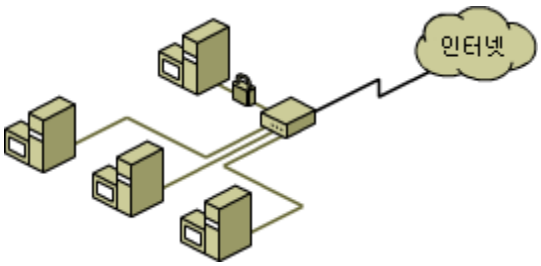


C. 권장되지 않는 토폴로지

여러 인터넷 연결에서 토폴로지를 사용하는 것을 피해야 합니다. 네트워크에 여러 개의 직접 인터넷 연결이 필요한 경우에는 다음 설명과 같이 네트워크를 보호할 수 있도록 직접 인터넷 연결마다 ICF 를 사용할 수 있게 설정해야 합니다. 그러나 ICF 가 연결에 따라 작동하기 때문에 모든 인터넷 연결의 지속적 보호를 보장할 수 있는 중앙 관리 지점이 있어야 하는 데, 이 토폴로지에는 이러한 중앙 관리 지점이 없으므로 사용하지 않는 것이 좋습니다.



마찬가지로 네트워크 허브를 인터넷에 직접 연결하여 네트워크에 인터넷 연결을 제공하는 토폴로지도 외부 공격을 받기 쉬우므로 사용하지 않는 것이 좋습니다.



이 유형의 네트워크 토폴로지에 ICF 를 사용할 수 있게 설정하면 일부 네트워크 통신이 중단되고 ICF 를 사용할 수 있게 설정한 컴퓨터만 보호됩니다. 다른 컴퓨터는 허브를 통해 인터넷에 직접 연결되며 보호되지 않습니다.

D. 연결 아이콘

ICF 가 네트워크 연결에 사용되면 네트워크 연결에 다음과 같은 네트워크 연결 아이콘

이 나타납니다. ICF 의 사용 여부를 확인하거나 ICF 를 사용할 수 있게 설정하려면 다음과 같이 작업합니다.

1. 네트워크 연결을 엽니다.
2. **전화 접속** 또는 **LAN 또는 고속 인터넷**에서 보호할 연결을 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **고급** 탭의 **인터넷 연결 방화벽** 아래에서 다음 중 하나를 수행합니다.
    - o ICF(인터넷 연결 방화벽)를 사용하려면 **인터넷에서 이 컴퓨터에 액세스하는 것을 제한하거나 금지하여 내 컴퓨터 및 네트워크 보호** 확인란을 선택합니다.
    - o ICF 를 해제하려면 **인터넷에서 이 컴퓨터에 액세스하는 것을 제한하거나 금지하여 내 컴퓨터 및 네트워크 보호** 확인란 선택을 취소합니다

주의

- **인터넷에서 이 컴퓨터에 액세스하는 것을 제한하거나 금지하여 내 컴퓨터 및 네트워크 보호** 확인란의 선택을 취소하면 해당 연결에서 방화벽을 사용할 수 없게 됩니다. 방화벽을 사용하지 않으면 컴퓨터가 보호되지 않은 연결을 통한 외부 공격에 노출될 수 있습니다.

네트워크 연결에 ICS 가 사용할 수 있게 설정되면 네트워크 연결에 공유 인터넷 연결 아이콘  으로 나타납니다. ICS 의 사용 여부를 확인하거나 ICS 를 사용하려면 다음과 같은 방법을 이용합니다.

1. 네트워크 연결을 엽니다.
2. **전화 접속** 또는 **LAN 또는 고속 인터넷**에서 ICS 를 사용할 수 있게 설정할 연결을 마우스 오른쪽 단추로 클릭한 다음 **속성**를 클릭합니다.
3. **고급** 탭의 **인터넷 연결 공유** 아래에서 **다른 네트워크 사용자가 이 컴퓨터의 인터넷 연결을 통해 연결할 수 있도록 허용** 확인란을 선택합니다.
4. **홈 네트워킹 연결**(있는 경우)의 **개인 네트워크 연결 선택** 드롭다운 상자에서 네트워크에 직접 연결되는 연결을 선택합니다.

중요

- ICS 는 네트워크 어댑터가 둘 이상 설치되어 있을 때만 사용할 수 있습니다.
- 개인 LAN 세그먼트에 연결된 개인 연결이 여러 개 있는 컴퓨터의 경우 ICS 를 사용하기 전에 개인 연결을 브리지해야 합니다. 네트워크 브리지를 설치하는 방법에 대한 자세한 내용은 관련 항목을 참조하십시오.
- ICS 를 사용할 수 있게 설정하면 ICS 호스트의 개인 연결에 자동으로 IP 주소가 제공됩니다.

E. ICF 사용에 대한 권장사항

모든 인터넷 연결에 ICF 를 사용할 수 있게 설정해야 합니다. VPN(가상 사설망) 연결 또는 네트워크 클라이언트 컴퓨터에서는 ICF 가 파일 및 프린터 공유와 같은 일부 유형의 네트워크 활동을 방해하므로 ICF 를 사용할 수 없게 설정해야 합니다. 비슷한 이유로 ICS 는 ICS 호스트 컴퓨터의 개인 연결 및 ICS 호스트를 ICS 클라이언트 컴퓨터에 연결하는 연결에서도 ICF 의 사용을 금지합니다. 이 위치의 방화벽은 네트워크 통신을 완전히 차단합니다. 인터넷에 직접 연결된 모든 연결에 ICF 를 사용할 수 없게 설정해야 합니다. 인터넷 연결에 이미 방화벽이나 프록시 서버가 실행되고 있으면 ICF 가 필요하지 않습니다.

F. ICF 및 알림 메시지

ICF 는 모든 들어오는 통신을 검사하므로 전자 메일 프로그램과 같은 일부 프로그램은 ICF 를 사용하는 경우 다르게 작동할 수 있습니다. 새 메일에 대해 전자 메일 서버를 정기적으로 폴링하는 전자 메일 프로그램도 있고 전자 메일 서버의 알림을 기다리는 전자 메일 프로그램도

있습니다. 예를 들어 Outlook Express 는 타이머가 알려 주는 시점에 새 전자 메일을 자동으로 확인합니다. 새 전자 메일이 있으면 Outlook Express 는 사용자에게 새 전자 메일 알림을 통해 알립니다. 새 전자 메일 알림 요청은 방화벽 내에서 시작되므로 ICF 는 이 프로그램의 동작에 영향을 주지 않습니다. 해당 방화벽은 메일 서버에 대한 아웃바운드 통신을 나타내는 표에 항목을 만듭니다. 메일 서버가 새 전자 메일에 대한 응답을 반환하면 방화벽은 표에서 연결된 항목을 찾아 통신 전달을 허용합니다. 그러면 사용자는 새 전자 메일이 도착했다는 알림을 받습니다.

그러나 Outlook 2000 은 RPC(원격 프로시저 호출)를 사용하여 클라이언트 컴퓨터에게 새 전자 메일 알림을 보내는 Microsoft Exchange Server 에 연결됩니다. Exchange Server 에 연결된 Outlook 2000 은 새 전자 메일을 자동으로 확인하지 않습니다. Exchange Server 는 Outlook 2000 에 새 전자 메일의 도착 시간을 알립니다. RPC 알림은 방화벽 내부의 Outlook 2000 이 아닌 방화벽 외부의 Exchange Server 에서 초기화되므로 ICF 는 표에서 해당 항목을 찾을 수 없으며 RPC 메시지는 인터넷에서 홈 네트워크 또는 소규모 네트워크로 통과되지 않습니다. RPC 알림 메시지는 삭제됩니다. 사용자는 전자 메일을 주고 받을 수 있지만 받은 새 전자 메일은 편지함에서 수동으로 확인해야 합니다.

G.고급 ICF 설정

ICF 보안 로깅 기능을 사용하여 방화벽 작업에 대한 보안 로그를 작성할 수 있습니다. ICF 는 승인된 트래픽과 거부된 트래픽을 모두 기록할 수 있습니다. 예를 들어 기본적으로 방화벽은 인터넷에서 들어오는 에코 요청을 허용하지 않습니다. ICMP(Internet Control Message Protocol) **수신 에코 요청 허용**을 사용하지 않으면 인바운드 요청이 실패하며 실패한 인바운드 시도를 기록하는 로그 항목이 생성됩니다.

ICMP 를 사용하면 **수신 에코 요청 허용**, **수신 타임스탬프 요청 허용**, **수신 라우터 요청 허용** 및 **방향 전환 허용**과 같은 여러 ICMP 옵션을 활성화하여 방화벽 동작을 수정할 수 있습니다.

ICF 를 한 대의 컴퓨터에서 둘 이상의 연결에 사용하면 ICMP 옵션의 설정은 연결에 따라 다릅니다. ICF 를 사용할 수 있게 설정한 모든 연결에서 ICMP 옵션의 설정을 변경하거나 설정하면 해당 설정이 사용자 컴퓨터의 다른 ICF 방화벽에 적용되지 않습니다. 허용할 ICF 보안 로그 크기를 설정하여 DoS(Denial-of-Service) 공격으로 인해 발생할 수 있는 잠재된 오버플로를 방지할 수 있습니다. 이벤트 로깅은 W3C(World Wide Web Consortium)에서 설정한 바와 같이 확장 로그 파일 형식으로 생성됩니다.

이러한 ICF(인터넷 연결 방화벽) 보안 는 다음의 2 가지를 위하여 사용될 수 있습니다.

- **손실된 패킷 로그에 기록** 홈 네트워크나 소규모 네트워크 또는 인터넷에서 시작된 손실 패킷을 모두 로그에 기록합니다.

- **성공적인 연결 로그에 기록** 홈 네트워크나 소규모 네트워크 또는 인터넷에서 시작된 성공적인 연결을 모두 로그에 기록합니다.

손실된 패킷 로그에 기록 확인란을 선택하면 ICF 에서 트래픽 시도를 감지하여 거부할 때마다 정보가 수집됩니다. 예를 들어 ICMP(Internet Control Message Protocol) 설정이 **ping** 에서 내보내는 것과 같은 수신 에코 요청 및 **tracert** 명령을 허용하지 않고 네트워크 외부에서 에코 요청을 받으면 해당 에코 요청은 삭제되며 하나의 항목이 로그에 생성됩니다.

성공적인 연결 로그에 기록 확인란을 선택하면 ICF 에서 트래픽 시도를 감지하여 허용할 때마다 정보가 수집됩니다. 예를 들어 네트워크상의 한 컴퓨터가 웹 사이트 연결에 성공하면 하나의 항목이 로그에 생성됩니다.

또한 ICF 보안 로그에는 두 섹션이 있습니다:

- 머리글은 ICF 보안 로그의 버전 및 데이터 항목에 사용 가능한 필드 정보를 제공합니다. 머리글 정보는 고정 목록으로 제공됩니다.
- 본문에는 방화벽을 통과하려는 트래픽의 결과로 입력되는 컴파일된 데이터가 들어 있습니다. ICF 보안 로그 본문의 필드는 페이지의 왼쪽에서 오른쪽으로 입력됩니다. ICF 보안 로그의 본문은 동적 목록이며 새 데이터 항목은 로그의 맨 아래에 입력됩니다.

다음 표는 ICF 보안 로그에 들어 있는 정보에 대한 정의입니다.

머리글 항목

항목	설명	예제
#Version	설치된 ICF 보안 로그의 버전을 표시합니다.	1.0
#Software	ICF 보안 로그의 이름을 제공합니다.	Microsoft 인터넷 연결 방화벽
#Time	로그에 있는 모든 타임스탬프가 현지 시간임을 나타냅니다.	현지 시간
#Fields	데이터가 사용 가능한 경우 ICF 보안 로그 항목에 대해 사용 가능한 필드의 고정 목록을 표시합니다. 필드로는 date, time, action, protocol, src-ip, dst-ip, src-port, dst-port, size, tcpflags, tcpsyn, tcpack, tcpwin, icmptype, icmpcode, info 등이 있습니다.	Src-port, dst-port, size

본문 데이터

필드	설명	예제
Date	기록된 트랜잭션이 발생한 년, 월, 일을 지정합니다. 날짜는 다음과 같은 형식으로 기록됩니다. YY-MM-DD 여기서 YY는 년, MM은 월, DD는 일을 나타냅니다.	2001-01-27
Time	기록된 트랜잭션이 발생한 시간, 분, 초를 지정합니다. 시간은 다음과 같은 형식으로 기록됩니다. HH:MM:SS 여기서 HH는 24시간 형식의 시간, MM은 분, SS는 초를 나타냅니다.	21:36:59
Action	방화벽에서 관찰하는 작업을 지정합니다. 방화벽에 사용 가능한 옵션은 OPEN, CLOSE, DROP 및 INFO-EVENTS-LOST입니다. INFO-EVENTS-LOST 작업은 이벤트가 발생했지만 로그에 기록되지 않은 이벤트 수를 가리킵니다.	DROP
Protocol	통신에 사용된 프로토콜을 지정합니다. 프로토콜로 TCP, UDP 및 ICMP가 지정될 수 있으며, 이들 프로토콜을 사용하지 않은 경우에는 숫자가 지정될 수도 있습니다.	ICMP
Src-ip	원본 IP 주소 즉, 통신을 설정하려는 컴퓨터의 IP 주소를 지정합니다. 원본 IP는 다음과 같이 점으로 구분된 형식으로 기록됩니다. (숫자).(숫자).(숫자).(숫자)	192.168.0.0
Dst-ip	통신 시도 대상의 IP 주소를 지정합니다. 대상 IP는 다음과 같이 점으로 구분된 형식으로 기록됩니다. (숫자).(숫자).(숫자).(숫자)	192.168.0.1
src-port	송신 컴퓨터의 원본 포트 번호를 지정합니다. src-port 항목은 1부터 65,535까지의 정수로 기록됩니다. TCP와 UDP만 유효한 src-port 항목을 반환합니다. 다른 모든 프로토콜은 src-port에 대해 유효하지 않으며 -항목을 생성합니다.	4039
Dst-port	대상 컴퓨터의 포트 번호를 지정합니다. dst-port 항목은 1부터 65,535까지의 정수로 기록됩니다. TCP와 UDP만 유효한 dst-port 항목을 반환합니다. 다른 모든 프로토콜은 dst-port에 대해 유효하지 않으며 -항목을 생성합니다.	53
Size	패킷 크기를 바이트로 지정합니다.	60
Tcpflags	IP 패킷의 TCP 머리글에 있는 TCP 제어 플래그를 지정합니다.	AFP

	• Ack-중요한 승인 필드 • Fin-더 이상 보낸 사람의 데이터 없음 • Psh-Push 함수 • Rst-연결 다시 설정 • Syn-시퀀스 번호 동기화 • Urg-중요한 긴급 지점 필드 플래그는 대문자로 기록됩니다. tcpflags의 항목 정보는 사용자에게 TCP(전송 제어 프로토콜)에 대한 자세한 내용을 제공합니다. TCP에 대한 추가 정보는 RFC 793에 나와 있습니다.	
Tcpsyn	패킷의 TCP 시퀀스 번호를 지정합니다. tcpsyn의 항목 정보는 사용자에게 TCP에 대한 자세한 내용을 제공합니다.	1315819770
Tcpack	패킷의 TCP 승인 번호를 지정합니다. tcpack의 항목 정보는 사용자에게 TCP에 대한 자세한 내용을 제공합니다.	0
Tcpwin	패킷의 TCP 창 크기를 지정합니다. 이 크기는 바이트로 지정됩니다. tcpack의 항목 정보는 사용자에게 TCP에 대한 자세한 내용을 제공합니다.	64240
Icmptype	ICMP 메시지의 형식 필드를 나타내는 숫자를 지정합니다.	8
Icmpcode	ICMP 메시지의 코드 필드를 나타내는 숫자를 지정합니다.	0
Info	발생한 작업 유형에 따라 달라지는 정보 항목을 지정합니다. 예를 들어 INFO-EVENTS-LOST 작업은 이벤트가 발생했지만 해당 이벤트 유형이 마지막으로 발생한 이후 로그에 기록되지 않은 이벤트 수를 표시합니다.	23

필드에 사용할 수 있는 정보가 없으면 (-) 문자가 입력됩니다.

ICF 를 한 대의 컴퓨터에서 둘 이상의 연결에 사용하면 ICF 설정이 전역 설정이 됩니다. ICF 가 사용되는 연결 중 하나에서 **로그 옵션** 또는 **서비스**의 설정을 선택하거나 변경하면 해당 설정이 컴퓨터의 모든 ICF 방화벽에 적용됩니다.

ICF 를 한 대의 컴퓨터에서 둘 이상의 연결에 사용하면 ICF 설정이 전역 설정이 됩니다. ICF 가 사용되는 연결 중 하나에서 **로그 옵션** 또는 **서비스**의 설정을 변경하거나 선택하면 해당 설정이 컴퓨터의 모든 ICF 방화벽에 적용됩니다.

참고

- 인터넷 연결 공유, 인터넷 연결 방화벽 및 네트워크 브리지는 Windows Server 2003, Standard Edition 및 32 비트 버전의 Windows Server 2003, Enterprise Edition 에만 포함되며 Windows Server 2003, Web Edition, 32 비트 버전의 Windows Server 2003, Datacenter Edition 또는 64 비트 버전의 Windows Server 2003 제품군에는 포함되지 않습니다.

8) 라우팅 및 원격 액세스 제어

라우팅 및 원격 액세스는 Windows NT 4.0 에 있는 RRAS(라우팅 및 원격 액세스 서비스)와 RAS(원격 액세스 서비스)를 대신합니다. 라우팅 및 원격 액세스는 전화 접속이나 VPN 클라이언트에서 연결을 종료하거나 라우팅(IP, IPX 및 AppleTalk) 또는 이 두 가지를 모두 제공하는 통합된 단일 서비스입니다. 라우팅 및 원격 액세스를 사용하여 서버에서 원격 액세스 서버, VPN 서버, 게이트웨이 또는 지점 라우터 기능을 수행할 수 있습니다. 정리해 보면,

Microsoft® Windows® Server 2003 제품군의 라우팅 및 원격 액세스 서비스가 제공하는 기능은 다음과 같습니다.

- 멀티프로토콜 LAN 대 LAN, LAN 대 WAN, VPN(가상 사설망) 및 NAT(네트워크 주소 변환) 라우팅 서비스.
- 전화 접속 및 VPN 원격 액세스 서비스.

라우팅 및 원격 액세스의 기능

- 라우팅 및 원격 액세스

  라우팅을 구성하기 위한 기본 관리 도구는 **제어판**의 **관리 도구** 폴더에서 사용할 수 있는 라우팅 및 원격 액세스입니다.

  라우팅 및 원격 액세스를 사용하여 다음과 같은 작업을 할 수 있습니다.

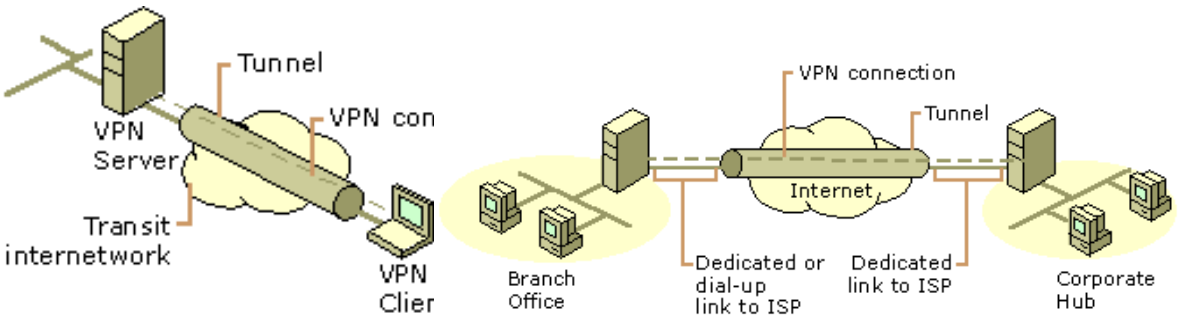
  - 라우팅 및 원격 액세스 서비스를 구성하여 사용하거나, 사용을 해제하거나, 시작하거나, 중지합니다.
  - 로컬 및 원격 라우터를 관리합니다.
  - 라우팅 동작 및 라우팅 프로토콜을 구성합니다.
  - 필요 시 전화 접속 라우팅 동작을 구성합니다.
  - 원격 액세스 정책을 구성합니다.
  - 활성 연결을 모니터링합니다.
  - 로컬 로깅 동작을 구성합니다.

Administrators 그룹의 구성원은 라우팅 및 원격 액세스를 사용할 수 있습니다. 컴퓨터가 도메인의 구성원인 경우 Domain Administrators 그룹의 구성원은 라우팅 및 원격 액세스를 사용할 수 있습니다.

9) VPN 기능

A.VPN 의 정의

가상 사설망(VPN)은 인터넷과 같은 공용 네트워크를 통해 사무실 네트워크 등의 개인 네트워크에 연결할 수 있게 해주는 방법으로 전화 접속 서버에 대한 전화접속 연결의 이점 뿐 아니라 인터넷 연결의 편리함과 융통성도 제공합니다. 인터넷 연결을 통해 전세계 어디로나 이동할 수 있으며 대부분의 장소에서 가까운 지역의 인터넷 지역의 인터넷 서비스 공급자(ISAP)에 전화를 걸어 자신의 사무실에 연결할 수 있습니다. 사용자 컴퓨터와 사무실 컴퓨터에 고속 인터넷 연결이 설치되어 있으면 아날로그 모뎀을 통한 전화접속 연결과는 비교도 안되는 바른 인터넷 속도로 사무실에 연결할 수



있습니다. VPN 에서는 인증된 링크를 사용하여 권한있는 사용자만 네트워크에 연결할 수 있도록 합니다. 사용자는 암호화를 사용하여 다른 사용자가 인터넷을 통해 이동되는 데이터를 가로채서 사용하는 것을 막습니다 Windows 에서는 PPTP(지점간 터널링 프로토콜)와 L2TP(계층 2 터널링 프로토콜)를 사용하여 이러한 보안을 구현합니다. 위의 그림은 VPN 의 개념에 대한 것입니다.

VPN 기술을 사용하면 회사에서 보안 통신을 유지하면서 인터넷과 같은 공용 네트워크를 통해 지사나 다른 회사에 연결할 수 있습니다. 인터넷을 통한 VPN 연결은 논리적 측면에서 볼 때 전용 WAN 링크로 작동합니다.

1. VPN 구성요소

Windows Server 2003 을 실행하는 서버의 VPN 은 VPN 서버, VPN 클라이언트, VPN 연결(데이터가 암호화되는 연결의 부분) 및 터널(데이터가 캡슐화되는 연결의 부분)로 구성됩니다. 터널링은 Windows Server2003 을 실행하는 서버에 포함된 터널링 프로토콜 중 하나를 통해 수행됩니다. Windows Server 2003 을 실행하는 서버에 포함된 두 터널링 프로토콜 모두 라우팅 및 원격 액세스 서비스와 함께 설치됩니다. 라우팅 및 원격 액세스 서비스는 Windows Server 2003 을 설치하는 동안 자동으로 설치되지만 기본적으로 활성화되지 않습니다. Windows 에 포함된 두 터널링 프로토콜은 다음과 같습니다.

- PPTP(지점간 터널링 프로토콜) : Microsoft Point-to-Point 암호화를 사용하여 데이터 암호화를 제공합니다.
- L2TP(계층 2 터널링 프로토콜) : IPSec 를 사용하여 데이터 암호화, 인증 및 무결성을 제공합니다.

인터넷 연결에는 T1, 부분적 T1 또는 프레임 릴레이와 같은 전용회선을 사용해야 하며 도메인에 할당되었거나 인터넷 서비스 공급자(ISP)가 제공한 IP 주소와 서브넷 마스크를 사용하여 WAN 어댑터를 구성해야 합니다. 또한 WAN 어댑터를 ISP 라우터의 기본 게이트웨이로 구성해야 합니다.

- 암호화 비교

다음 표는 전화 접속 및 PPTP 와 IPSec 를 통한 L2TP 의 VPN 연결 형식에 사용된 암호화 형식을 비교한 것입니다.

	전화 접속 및 PPTP	**IPSec 을 통한 L2TP**
기본 암호화	40 비트 MPPE	56 비트 DES
강력한 암호화	56 비트 MPPE	56 비트 DES
가장 강력한 암호화	128 비트 MPPE	3DES (56 비트 키 3 개)

- 패킷 비교

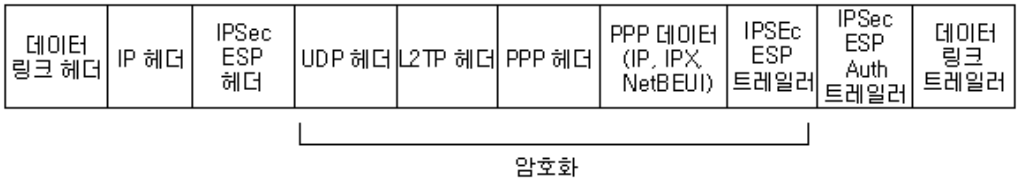
아래의 그림 5 는 PPTP 데이터 패킷이 터널을 통해 이동할 때 모습을 나타낸 것입니다. 우선 암호화된 PPP 데이터를 PPP 헤더로 캡슐화하여 PPP 프레임이 만들어집니다. 그런 다음 PPP 프레임은 GRE 헤더로 캡슐화됩니다. 그러면 결과 페이로드는 원본과 대상 IP 주소에 대한 정보가 들어 있는 IP 헤더로 캡슐화됩니다. 마지막으로 이 IP 데이터그램은 데이터 링크 계층 헤더와 트레일러로 캡슐화됩니다. 데이터 링크 계층 헤더와 트레일러는 사용 기술에 따라 다양합니다. 예를 들어, 이더넷 네트워크를 사용할 경우 IP 데이터그램은 이더넷 헤더 및

트레일러로 캡슐화되고, 아날로그 전화선을 사용할 경우 IP 데이터그램은 PPP 헤더와 트레일러로 캡슐화됩니다. 패킷이 대상에 도달하면 헤더는 반대 순서로 차례대로 스트립됩니다. 우선 데이터 링크 계층 헤더와 트레일러가 제거되고 그 다음에 IP, GRE 및 PPP 헤더가 스트립됩니다. 마지막으로 PPP 데이터 암호화가 해제됩니다. 아래 글;a 은 PPTP 패킷구조를 나타냅니다.

데이터 링크 헤더	IP 헤더	GRE 헤더	PPP 헤더	암호화된 PPP 데이터 (IP, IPX, NetBEUI)	데이터 링크 트레일러

L2TP 패킷 구조

L2TP 의 패킷 구조는 헤더가 PPP 데이터에 추가된 PPTP 와 유사합니다. 그림 6 은 L2TP 패킷의 모습을 보여줍니다. UDP 헤더와 IPSec 트레일러 사이의 모든 것이 암호화된다는 점에 유념하십시오



■ **연결 생성 메커니즘**

VPN 사용에 있어서 가장 중요한 것이 바로, 네트워크를 통한 데이터 통신간의 보안입니다. 이를 위해 VPN 서버에서는 위의 VPN의 개념에서 언급한 터널링(Tunneling) 메커니즘을 사용하고 이 터널링 메커니즘은 다음과 같이 2가지 종류로 구분됩니다.

Voluntary Tunneling

사용자나 클라이언트 컴퓨터가 VPN 연결을 요청하고 이에 자발적으로 터널이 생성되는 방식으로, 이 때 사용자 컴퓨터는 터널상의 종점이 되며 터널 클라이언트로 작동합니다. 원격 액세스 사용자는 보통 VPN 서버에 직접 Voluntary Tunneling을 생성하게 됩니다. 즉, 사용자가 VPN 서버에 접근하여 VPN 연결에 대한 보안 설정이나 암호화 설정을 하게 되는 것입니다.

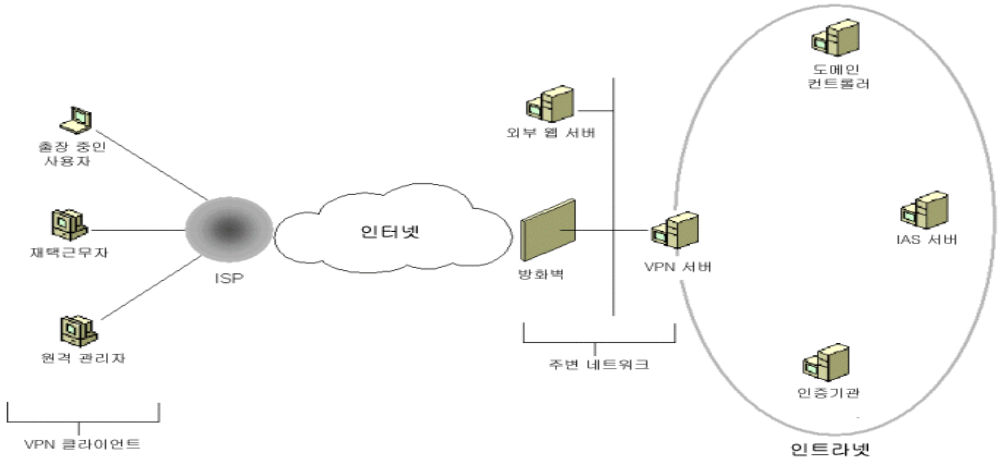
Compulsory Tunneling

Voluntary Tunneling과 달리, VPN 서버가 터널을 구성하는 방식을 말합니다. 이는 사용자 컴퓨터가 터널상의 종점이 되는 것이 아니라 사용자 컴퓨터와 터널 서버 사이에 있는 원격 액세스 서버가 터널의 종점이 되며 터널 클라이언트로 동작합니다. 이 의무적 터널링은 라우터의 역할을 하는 VPN 서버간에 구성되기도 하고 이에 따라 회사의 본사와 지사를 연결하는 경우에 특히 유용합니다.

● **VPN 연결을 위한 구성 요소**

1. VPN 클라이언트

2. 인터넷 인프라
3. VPN 서버
4. 인트라넷 인프라
5. 인증, 권한 및 계정(AAA) 인프라
6. 인증서 인프라



[그림] Windows Server 2003 원격 액세스 VPN 구성 요소

2. VPN 클라이언트

VPN 클라이언트는 MMPE(마이크로소프트 지점간 암호화)를 사용하여 PPTP 를 설정하거나 IPSec 암호화를 사용하여 L2TP(Layer2 터널링 프로토콜)를 설정할 수 있는 경우 어떤 컴퓨터라도 상관없습니다.

VPN 터널링 프로토콜	Microsoft 운영 체제
PPTP	Windows XP, Windows 2000, Windows NT version 4.0, Windows ME, Windows 98, Windows 95(Windows 전화 접속 네트워킹 1.3 이상의 성능 및 보안 업데이트)
L2TP/IPSec	Windows XP, Windows 2000

[표 2] VPN 기능을 하는 마이크로소프트 데스크톱 운영체제

3. 인터넷 인프라 – VPN프로토콜

VPN 프로토콜은 위에서 본 바와 같이 지점간 터널링 프로토콜 (PPTP)과 인터넷 프로토콜 보안(IPSec)가 있는 계층 2 터널링 프로토콜(L2TP)로 구성 되며 설계시 다음과 같은 차이점을 보입니다.

설계 사항 : L2TP와 PPTP

- PPTP 는 Windows XP, Windows 2000, Windows NT 버전 4.0, Windows ME, Windows 98, Windows 95(Windows 전화 접속 네트워킹 1.3 이상의 성능 및 보안 업데이트)를 포함하여 다양한 Microsoft 클라이언트에서 사용할 수 있으며 PPTP 에서는 사용자 ID 와 패스워드로 인증을 하기 때문에 컴퓨터 인증서를 발행하기 위한 인증서 인프라가 필요하지 않습니다.
- PPTP 기반 VPN 연결은 데이터 기밀을 제공합니다 (캡쳐된 패킷에 암호화 키가 없는 경우 해석될 수 없음). 그러나 PPTP VPN 연결은 전송 중 데이터가 변경되지 않도록 보장하는 데이터 무결성 또는 데이터 전송자의 자격을 증명하는 데이터 인증을 제공하지는 않습니다.
- NAT 에 PPTP 로 터널링한 데이터를 적절히 변환할 수 있는 NAT 편집기가 있는 경우 PPTP 기반 VPN 클라이언트를 NAT 의 뒤에 위치시킬 수 있습니다. 예를 들어 네트워크 및 전화 접속 연결 폴더의 인터넷 연결 공유(ICS) 기능과 라우팅 및 원격 액세스 서비스에 NAT 뒤에 위치한 PPTP 클라이언트에서 수신되는 PPTP 트래픽을 변환하는 NAT 편집기가 포함될 수 있습니다. 복수의 IP 주소가 있지 않으며 공용 IP 주소에서 VPN 서버의 개인 IP 주소로의 일대일 매핑이 있지 않는 한, 또는 하나의 공용 주소만 있거나 NAT 가 PPTP 로 터널링된 데이터를 변환하여 VPN 서버로 전달하도록 구성된 경우, VPN 서버는 NAT 뒤에 위치할 수 없습니다. ICS 와 NAT 라이팅 프로토콜 구성 요소를 포함하여 하나의 공용 IP 주소를 사용하는 대부분의 NAT 는 IP 주소와 TCP 및 UDP 포트를 기반으로 수신되는 트래픽을 허용하도록 구성될 수 지만, PPTP 로 터널링된 데이터는 TCP 또는 UDP 헤더를 사용할 수 없다. 따라서 VPN 서버는 하나의 IP 주소를 사용할 경우 ICS 나 NAT 라우팅 프로토콜 구성 요소를 사용하는 컴퓨터 뒤에 위치할 수 없습니다.
- Windows 2000 IPSec 보안 연결을 협상하는 프로토콜인 인터넷 키 교환(IKE)과 IPSec 로 보호된 트래픽은 NAT 로 변환할 수 없으므로 L2TP 기반 VPN 클라이언트 또는 서버는 NAT 의 뒤에 위치할 수 없습니다.
- L2TP 는 Windows XP 및 Windows 2000 과 함께 사용할 수 있으며 IPSec 용 인증 수단으로 컴퓨터 인증서를 지원합니다. 컴퓨터 인증서 인증에는 VPN 서버 컴퓨터와 모든 VPN 클라이언트 컴퓨터에 컴퓨터 인증서를 발행하는 인증서 인프라가 필요합니다.
- L2TP 기반 VPN 인증은 IPSec 를 사용하여 데이터 기밀, 데이터 무결성, 데이터 인증 및 회신 보호를 제공합니다.
- PPTP 와 L2TP 중에서 하나만 선택해야 하는 것은 아닙니다. 기본적으로 Windows 2000 VPN 서버는 PPTP 와 L2TP 연결을 동시에 지원합니다. PPTP 를 어떤 원격 액세스 VPN 연결(Windows XP 또는 Windows 2000 에서 실행되지 않으며 설치된 컴퓨터 인증서가 없는 VPN 클라이언트)에 사용하는 동시에 L2TP 를 다른 원격 액세스 VPN 연결(Windows

XP 또는 Windows 2000 에서 실행되며 설치된 컴퓨터 인증서가 있는 VPN 클라이언트)에 사용할 수 있습니다.

- PPTP 와 L2TP 를 모두 사용할 경우 PPTP 와 L2TP 연결용으로 다른 연결을 정의하는 별도의 원격 액세스 정책을 만들 수 있습니다.

4. VPN 서버

VPN 서버는 Windows Server 2003 서버와 라우팅 및 원격 액세스 서비스가 실행되는 컴퓨터로 다음과 같은 기능을 수행합니다.

- PPTP 연결 시도와 L2TP 연결 시도를 위한 IPSec SA 협상 감시
- 데이터 흐름 허용에 앞서 VPN 연결 인증 및 권한 부여
- VPN 클라이언트 간 데이터 및 인트라넷 리소스를 전달하는 라우터 역할
- 터널 클라이언트(보통 VPN 클라이언트)에서의 VPN 터널 끝점 역할
- VPN 클라이언트에서의 VPN 연결 끝점 역할

5. 인증서 인프라

인증서 인프라는 L2TP Over IPSec과 함께 사용되는 인증 인프라입니다. 이 것은 Windows2000 서버에 기본으로 내장되어 있는 마이크로소프트 인증서버 (Certificate Authority)가 반드시 설치되어야 함을 전제로 합니다. 인증서 서비스에 대한 추가적인 사항은 다음 내용에서 다루기로 하겠습니다.

2.Windows Server 의 Network Infrastructure 의 기능 요약

1) 보다 쉬워진 설치, 구성 및 배포

A.네트워크 진단 기능들

Windows Server 2003 제품군에 추가된 네트워크 진단 기능들이 네트워크 상의 여러 가지 문제들을 진단해 줍니다.
네트워크 진단 웹 페이지는 도움말 및 지원의 **도구** 부분이나 문제 해결 혹은 네트워킹 상의 도움말 및 지원 상세 정보 부분에서 살펴볼 수 있습니다. 이 웹 페이지를 통해 로컬 컴퓨터나 그것이 연결되어 있는 네트워크에 대한 중요한 정보를 쉽게 검색해 볼 수 있습니다.

Netsh diag 명령 -새로운 Netsh helper DLL 은 **netsh diag** 컨텍스트에서 명령들을 제공하여 여러분이 광범위한 네트워크 진단 정보를 살펴보고 명령줄에서 진단 기능들을 수행할 수 있도록 해줍니다. Netsh 진단 명령을 실행하려면 명령 프롬프트에서 **netsh -c diag** 라고 입력하십시오.

네트워크 연결을 위한 **복구** 메뉴 옵션 –때때로 컴퓨터의 네트워크 구성이 네트워크 간 커뮤니케이션을 막는 경우가 있습니다. 그러나 이런 경우도 IP 주소 구성이나 DNS 이름 등록을 갱신하는 등의 일반 프로시저들을 통해 복구될 수 있습니다. 그러나 이런 절차들을 수동으로 일일이 처리하고 싶지 않을 경우엔 각 네트워크 연결 컨텍스트 메뉴 상에 있는 **복구** 옵션을 사용할 수 있습니다. 이 옵션을 선택해 일련의 단계들을 취함으로써, 더 이상의 심각한 문제는 야기하지 않는 것으로 알려진 단순한 커뮤니케이션 문제들 정도는 해결할 수 있습니다.

네트워크 연결을 위한 **지원** 탭–네트워크 연결 폴더 내에 있는 각각의 네트워크 연결을 위한 **상태** 대화상자는 이제 **지원** 탭을 포함하고 있습니다. 이 탭에서 TCP/IP 구성 정보를 볼 수 있습니다. 또한 이 **지원** 탭에는 **복구** 버튼이 포함되어 있으며 이는 네트워크 연결 상의 **복구** 컨텍스트 메뉴 옵션과 같은 것입니다.

작업 관리자를 위한 **네트워킹** 탭 –이제 작업 관리자에는 시스템에서 각 네트워크 어댑터를 위한 실시간 네트워킹 메트릭스를 보여주는 **네트워킹** 탭이 포함되어 있습니다. 이 탭에서는 네트워크가 어떻게 작업을 수행하는지에 대한 간략한 개요를 보여줍니다.

업데이트된 Netdiag.exe 명령줄 네트워크 진단 도구 –Windows Server 2003 제품군 CD-ROM 에서 제공되는 지원 도구들에는 Netdiag.exe 가 들어 있는데 이는 Windows 2000 Resource Kit 에서 제공되던 진단 도구의 보다 강화된 버전입니다. 이 지원 도구를 설치하려면 Windows Server 2003 제품군 CD-ROM 의 지원₩도구 폴더에서 Support.msi 파일을 실행합니다.

원격 액세스 로그인을 가능하게 해주는 메뉴 옵션 – 새 **진단** 탭이 네트워크 연결 폴더의 **원격 액세스 설정** 대화 상자에 추가되어 원격 액세스 연결에 대한 활성화, 보기 및 로그인 제어 등을 할 수 있게 합니다. **원격 액세스 설정** 대화 상자를 살펴보기 위해서는 **고급**을 클릭한 후 네트워크 연결 폴더에 있는 **원격 액세스 설정**을 클릭합니다.

더 자세한 정보는 Windows Server 2003 제품군 도움말 및 지원 센터에서 살펴보실 수 있습니다.

- **네트워크 위치 인식**

네트워크 위치 인식은 Windows Server 2003 제품군에서 실행되는 컴퓨터가 자신이 연결되어 있는 네트워크에 대한 정보를 검색할 수 있게 해 줍니다. 또한 해당 위치에 대한 네트워크 스택의 유연한 구성도 가능합니다. 이 정보는 Windows Sockets API를 통해서도 알 수 있는데, 이를 통해 어플리케이션은 현재 네트워크에 대한 정보를 검색하거나 네트워크 정보가 변경되었을 때 해당 사항을 통보받게 됩니다.

Windows Server 2003 제품군의 구성요소들은 또한 적절한 서비스를 제공하기 위해 네트워크 위치를 사용합니다. 예를 들어 인터넷 연결 공유(ICS), 인터넷 연결 방화벽(ICF), 네트워크 브리지(Network Bridge) 기능들을 활성화 내지는 비활성화하는 새 그룹 정책 설정들은 네트워크 위치를 인식합니다. 그리고 이 정책들은 컴퓨터가 일련의 설정이 적용되어 있는 네트워크에 연결할 때에만 적용됩니다. 즉 랩톱 컴퓨터가 기업 네트워크에 연결되는 동안에는 이러한 기능들을 비활성화 하라는 내용의 새로운 그룹 정책 설정 내용을 수신했더라도, 홈 네트워크에 연결되는 동

안에는 그 그룹 정책 설정을 따르지 않기 때문에 여전히 그 기능들을 사용합니다.

- **무선 LAN 에 있어 강화된 기능들**

몇몇 새로운 기능들 및 강화된 사항들이 Windows Server 2003 제품군에 추가되어, LAN 액세스에 대한 중요 자동 관리 기능과 사용자 인증 및 권한 등을 포함해 여러 가지 무선 LAN 네트워크 구축과 관련된 내용들을 개선합니다. 자세한 내용은 아래와 같습니다.

- **강화된 이더넷 및 무선 보안(IEEE 802.1X 지원)** –이전에 무선 LAN 네트워킹에는 중요 관리 시스템을 통한 구축이 간편한 보안 솔루션이 부족했습니다. 따라서 Microsoft 와 몇몇 무선 LAN 및 PC 업체들은 이더넷과 무선 LAN 모두에 적용되는 포트 기반 네트워크 액세스 제어를 위한 표준인 IEEE 802.1X 를 정의하기 위해 함께 노력하였습니다. Microsoft 는 Windows XP 에서 IEEE 802.1X 를 지원하며, 무선 LAN 업체와 협력하여 액세스 포인트에 있어서 표준을 지원합니다.

- **무선 제로 구성(Zero Configuration)** –무선 네트워크 어댑터와 관련해 Windows Server 2003 제품군은 사용자 개입 없이도 선호하는 네트워크에 연결을 구축하기 위해 무선 네트워크에서 여러 가지 다양한 선택을 할 수 있습니다. 특정 네트워크에 대한 설정은 저장되어, 다음 번에 무선 네트워크가 특정 네트워크에 연결될 때 자동적으로 사용됩니다. 또한 Windows Server 2003 제품군은 인프라 네트워크 없이도 임시 모드를 사용하기 위해 무선 어댑터를 구성할 수 있습니다.

- **무선 로밍 지원** – Windows 2000 은 네트워크 가용성을 파악하고 적절하게 대처하기 위해 여러 개선 사항들을 제공했습니다. 이 개선 내용들은 Windows Server 2003 제품군에서 확대되고 보완되어 무선 네트워크의 변환적인 성향을 지원합니다. Windows Server 2003 에 추가된 기능들에는 재연결시 DHCP 구성 갱신, 필요 시 재인증, 컴퓨터가 연결되어 있는 네트워크를 기반으로 한 다양한 구성 옵션 선택 기능들이 있습니다.

- **무선 모니터 스냅인** – Windows Server 2003 제품군에는 무선 액세스 포인트(AP)나 무선 클라이언트 구성 및 통계 정보를 살펴볼 수 있는 새로운 무선 모니터 스냅인이 포함되어 있습니다.

- **안전한 무선 연결을 위한 암호 기반 인증** – Windows Server 2003 제품군에는 무선 네트워크 연결을 위한 Protected Extensible Authentication Protocol (PEAP) 지원 기능이 포함되어 있습니다. PEAP 과 함께 암호 기반 인증 수단을 사용함으로써 안전하게 무선 연결을 인증할 수 있습니다. PEAP 은 인증 프로세스가 시작되기 전에 암호화된 채널을 구성합니다. 따라서 암호 기반 인증 교환은 오프라인 사전 공격이 아닙니다. MS-CHAP v2(Microsoft Challenge Handshake Authentication Protocol version 2)는 이제 EAP 인증 형태로 사용할 수 있습니다. MS-CHAP v2 의 EAP 버전과 함께 PEAP 은 PKI(공개키 인프라)라고 알려져 있는 인증서 인프라를 구축하지 않고도 안전한 무선 인증을 확보할 수 있게 해주며 각 무선 클라이언트에 인증서를 설치합니다. Internet Authentication Service (IAS)라고 알려져 있는 Windows Server 2003 제품군의 RADIUS(Remote Authentication Dial-in User Service)

서버 역시 PEAP 를 지원하기 위해 강화되었습니다.

- **무선 네트워크 정책을 위한 그룹 정책 확장** – 새로운 Wireless Network (IEEE 802.11) Policies 그룹 정책 확장은 컴퓨터 구성을 위한 그룹 정책의 일부인 무선 네트워크 설정을 구성할 수 있게 해줍니다. 무선 네트워크 설정에는 선호하는 네트워크의 목록, Wired Equivalent Privacy (WEP) 설정 및 IEEE 802.1X 설정이 포함됩니다. 이러한 설정들은 도메인 멤버에 다운로드되어, 무선 클라이언트 컴퓨터에 안전한 무선 연결을 하기 위한 특정 구성 배포 작업을 보다 쉽게 만들어 줍니다. 또한 그룹 정책 스냅인의 Computer Configuration/Windows Settings/Security Settings/Wireless Network (IEEE 802.11) Policies 노드에서 무선 정책을 정할 수 있습니다.

- **무선 LAN 연결을 위한 인증되지 않은 액세스** – Windows Server 2003 제품군의 무선 클라이언트와 IAS 둘다 인증되지 않은 무선 연결을 지원합니다. 이 경우에는 EAP-TLS(Extensible Authentication Protocol-Transport Level Security)가 사용되어 IAS 서버 인증서의 단방향 인증이 수행되며, 무선 클라이언트는 사용자 이름이나 사용자 자격 증명을 보내지 않습니다. 무선 클라이언트를 위해 인증되지 않은 액세스를 가능하게 하려면 네트워크 연결 폴더에 있는 무선 연결 속성의 Authentication(인증) 탭에서 Authenticate as guest when user or computer information is available 를 선택합니다. IAS 서버를 위한 인증되지 않은 액세스를 가능하게 하려면 게스트 계정을 활성화하고, 게스트 계정이 포함된 그룹을 사용하는 EAP-TLS 연결에 대핸 인증되지 않은 액세스를 허용하도록 원격 액세스 정책을 구성해야 합니다.

이러한 개선 내용들을 통해 다음이 가능합니다:

- 이동중인 사용자가 공항에서도 무선이나 이더넷 연결을 통해 안전한 인터넷 연결을 할 수 있습니다.
- IT 관리자들은 이런 강화된 기능들을 사용해 무선 LAN 으로 안전한 연결을 구축합니다. IT 관리자들은 또한 IAS 가 사용하는 원격 액세스 정책에 기반한 자동 등록 및 권한을 통해 구축된 인증서를 요구합니다.
- IT 관리자는 데이터 암호화를 요구하지 않고도 이 기능들을 사용해 유선 기반 이더넷 LAN 에 대한 인증되고 증명된 액세스를 구성할 수 있습니다.

● 라우팅 및 원격 액세스 서비스에 있어 강화된 기능들

Windows Server 2003 제품군에는 다음과 같은 라우팅 및 원격 액세스 서비스 강화 기능들이 추가되었습니다.

- 스냅인 및 설치 마법사 강화

라우팅 및 원격 액세스 서버 설치 마법사는 라우팅 및 원격 액세스 서비스의 초기 구성을 쉽게 할 수 있도록 수정되었습니다.

- EAP-TLS 속성을 위한 향상된 구성

Smart Card or other Certificate Properties 대화 상자는 다양한 RADIUS 서버 구성 및 여러 최상위 인증 기관(Root CA)들을 허용하도록 향상되었습니다. 이를 통해 여러 유무선 네트워크나 다양한 RADIUS 서버를 사용하는 대규모 네트워크들과의 유연한 연결을 제공합니다. Smart Card or other Certificate Properties 대화상자를 열기 위해서는 네트워크 연결 폴더 내에 있는 LAN 연결 속성의 Authentication(인증) 탭에서 Smart Card or other Certificate EAP type을 선택하고 Properties(속성)을 클릭합니다.

- NetBIOS over TCP/IP Name Resolution Proxy (NetBT 이름 분해 프록시)

새로운 NetBT(NetBIOS over TCP/IP) 프록시는 라우팅 및 원격 액세스 서비스에 내장되어, 단일 라우터(Windows Server 2003 제품군 중 하나를 실행하는 원격 액세스 서버 컴퓨터)를 가진 하나 또는 여러 서브넷으로 구성된 네트워크에 연결된 원격 액세스 클라이언트가 DNS나 WINS 서버를 사용하지 않고도 이름을 분해할 수 있도록 해줍니다.
이 새로운 기능을 사용해 소규모 업체들은 원격 액세스나 VPN 서버를 구성함으로써, 직원들이 집에서도 일할 수 있게 되었습니다. NetBT 프록시 활성화를 통해 원격으로 연결되어 있는 클라이언트들은 이제 따로 DNS나 WINS 서버를 배포하지 않고도 소규모 네트워크 상에서 컴퓨터 이름을 분해할 수 있게 되었습니다.

- 서버와 라우팅 및 원격 액세스 서비스 통합 관리

이 기능은 Manage Your Server 기능을 사용하는 라우팅 및 원격 액세스 서비스의 NAT/Basic 방화벽 구성요소를 구성하기 위해 통합된 방법을 제공합니다. 또한 IT 관리자들은 이 기능을 사용해 동일한 설치 과정 중에 Windows Server 2003 제품 서버와 라우팅 및 원격 액세스 서비스 NAT/Basic 방화벽 구성요소를 구성할 수 있습니다.

- NAT 사설 인터페이스로서 라우팅 및 원격 액세스 서비스 내부 인터페이스를 활성화하는 기능

사설 인트라넷에 원격 액세스를 제공하고 인터넷으로의 액세스를 제공하기 위해 NAT(Network Address Translator)으로서 작동하는 Windows 2000 Server를 운영하는 컴퓨터에게는 연결되어 있는 원격 액세스 클라이언트에게 인터넷 액세스를 제공할 방법이 없습니다. Windows Server 2003 제품군 중 하나를 운영하는 컴퓨터들은 이제 라우팅 및 원격 액세스 서비스의 NAT 구성요소에 대한 개인 인터페이스로서 **내부** 인터페이스를 추가할 수 있도록 해 줍니다. 이를 통해 연결된 원격 액세스 클라이언트는 인터넷에 액세스할 수 있습니다.

- 전화 연결 접속을 통해서도 사용할 수 있는 PPPoE

이 기능은 필요시 전화접속 연결(dial-on-demand connections로도 알려져 있음)을 위해 PPPoE를 사용할 수 있게 해 줍니다. Demand-dial connections은 패킷들이 라우트되는 LAN

사이에서 지점간(point-to-point) 연결을 하기 위해 라우팅 및 원격 액세스 서비스가 사용하는 것입니다. 이 기능은 Demand-Dial 인터페이스 마법사의 **Connection Type(연결 형식)** 대화상자에 있는 **Connect using PPP over Ethernet (PPPoE)** 옵션을 선택하여 사용할 수 있습니다.
Demand-dial 연결을 위한 연결 형식으로 PPPoE를 사용함으로써 소규모 업체들은 이제 라우팅 및 원격 액세스 서비스의 NAT/Basic 방화벽과 자신들의 광대역 인터넷 연결을 사용하여 인터넷에 연결할 수 있습니다.

- 내부 및 인터넷 인터페이스를 위한 Default Behavior(기본 동작)의 개선점들

VPN 서버의 이름을 분해하고 VPN 서버 상에서 실행되는 서비스에 액세스 하는 것과 관련된 문제가 일어나는 것을 미리 방지하기 위하여, 라우팅 및 원격 액세스 서비스는 디폴트로 내부 인터페이스를 위한 동적 DNS 등록을 비활성화 시키고, 더불어 라우팅 및 원격 액세스 서버 설치 마법사에서 인터넷 인터페이스로서 나타나는 인터페이스를 위한 동적 DNS 및 NetBT(NetBIOS over TCP/IP)도 역시 비활성화시킵니다.

- Windows Server 2003, Web Edition 을 위한 VPN Connection Limit(연결 제한)

Web Edition에서 허용된 VPN 연결 수는 VPN 연결 하나입니다(PPTP 또는 L2TP 기반의 연결). 이는 Windows XP Professional과 Windows XP Home Edition에도 적용되는 제한 사항입니다. 하나 이상의 VPN 연결을 지원하려면 반드시 Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition, 또는 Windows Server 2003, Datacenter Edition을 사용해야 합니다.

- NAT 과 방화벽 통합

라우팅 및 원격 액세스 서비스의 NAT/Basic 방화벽 구성요소는 Windows XP에서 제공되는 인터넷 연결 방화벽에서 사용된 것과 동일한 기술을 사용해 기본 방화벽을 지원하기 위해 보다 강화되었습니다. 이 기능을 통해 여러분은 인터넷에 액세스하기 위해 NAT(Network Address Translator)을 이용하며 Windows Server 2003 제품군 중 하나를 실행하는 컴퓨터의 공용 인터페이스를 보호할 수 있습니다. NAT을 사용하면 사설 네트워크 클라이언트가 트래픽을 요청하지 않는 한은 NAT 컴퓨터가 인터넷으로부터 트래픽을 전송하지 않기 때문에 사설 네트워크 상의 컴퓨터들이 보호됩니다. 그러나 사실상 NAT 컴퓨터는 그 컴퓨터 자체가 공격에 취약합니다. NAT 컴퓨터의 공용 인터페이스 상에서 기본 방화벽을 활성화하면, 이제 NAT 컴퓨터가 요구하는 트래픽(컴퓨터 자체를 위한 또는 사설 인트라넷 클라이언트를 위한)과 일치하지 않는 인터넷 인터페이스 상의 모든 패킷들은 버려집니다.
라우팅 및 원격 액세스 서비스의 NAT/Basic 방화벽 IP 라우팅 프로토콜을 사용하도록 구성된 사설 인터페이스 속성의 **NAT/Basic Firewall** 탭에서 이 새로운 기능을 활용할 수 있습니다.

- L2TP/IPSec NAT Traversal

Windows 2000과 함께 Internet Key Exchange (IKE)와 Encapsulating Security Payload (ESP)

트래픽은 NAT을 통과할 수 없습니다. 왜냐하면 NAT이 IP 주소나 패킷의 포트를 변환할 경우 패킷의 보안을 무효화하기 때문입니다. 이는 NAT 밖에서는 L2TP/IPSec 연결을 구축할 수 없으며 VPN 연결을 위해 Point-to-Point Tunneling Protocol (PPTP)을 사용해야만 한다는 것을 의미합니다.

Windows Server 2003 제품군은 이제 NAT을 통해 IKE 및 ESP 트래픽이 통과할 수 있도록 Internet Protocol security (IPSec) 패킷의 UDP 캡슐화를 지원합니다. 그리고 이를 통해 하나 또는 여러 개의 NAT 밖에 위치하며 Windows Server 2003 제품군 중 하나를 실행하는 Windows XP 또는 Windows 2000 Professional 기반 컴퓨터와 서버 컴퓨터에서 L2TP/IPSec 연결이 이루어질 수 있습니다.

Windows Server 2003 제품군에서 지원되는 IPSec 트래픽을 위한 NAT traversal은 "UDP Encapsulation of IPSec Packets" (draft-ietf-ipsec-udp-encaps-02.txt)와 "Negotiation of NAT-Traversal in the IKE" (draft-ietf-ipsec-nat-t-ike-02.txt)에 자세히 나와 있습니다.

- L2TP/IPSec 트래픽을 위한 NLB 지원

Windows 2000에서 Network Load Balancing (NLB) 서비스는 다양한 서버 상의 IPSec security associations (SAs)를 관리할 능력이 없습니다. 클러스터에 있는 서버가 사용할 수 없는 상황이 되면 클러스터에 의해 관리되는 SAs는 소속이 없어지고 결국에는 종료됩니다. 이는 결국 L2TP/IPSec VPN 서버를 클러스터할 수 없다는 것을 의미합니다. 여러 개의 L2TP/IPSec VPN 서버들 상의 부하 분산을 위한 DNS 순차 순환 방식을 사용할 수는 있지만 는 결함 허용은 되지 않습니다.

Windows Server 2003 제품군에서 NLB 서비스는 IPSec security associations (SAs)를 위해 클러스터링 지원을 제공하고자 향상되었습니다. 이는 L2TP/IPSec VPN 서버의 클러스터를 생성할 수 있으며 NLB 서비스가 L2TP/IPSec 트래픽을 위한 로드 밸런싱과 결함 허용을 제공할 것이라는 것을 의미합니다.

이 기능은 Enterprise Edition과 Datacenter Edition의 32-bit 및 64-bit 버전에서만 제공됩니다.

- L2TP/IPSEC 연결을 위한 Preshared Key 구성

Windows Server 2003 제품군은 L2TP 연결을 위한 IP Security (IPSec) security association 을 구축하기 위한 인증 방법으로 컴퓨터 인증서와 preshared key를 지원합니다. Preshared key는 VPN 클라이언트와 VPN 서버에 구성된 일련의 텍스트입니다. 이는 상대적으로 미약한 인증 방법입니다: 따라서 Preshared key 인증은 단지 여러분의 PKI(공개키 인프라)가 컴퓨터 인증서를 확보하도록 구축된 경우나 혹은 VPN 클라이언트가 Preshared key 인증을 요구할 때에만 사용할 것을 권합니다. 여러분은 L2TP 연결을 위해 Preshared key 사용을 활성화하거나, 라우팅 및 원격 액세스 스냅인의 서버 속성 창의 **Security(보안)** 탭에서 Preshared key를 지정할 수 있습니다.

Windows XP와 Windows Server 2003 제품군 원격 액세스 VPN 클라이언트는 preshared key 인증도 지원합니다. 네트워크 연결의 VPN 연결 속성에 있는 **Security(보안)** 탭 상의 **IPSec settings**에서 Preshared key 인증을 활성화하고 preshared key를 구성할 수 있습니다.

Preshared key 인증은 Windows Server 2003 family router-to-router VPN 연결(Windows Server 2003 제품군 라우터 간 VPN 연결)을 위해 지원됩니다. 라우팅 및 원격 액세스 스냅인의 demand-dial 인터페이스 속성에 있는 **Security(보안)** 탭 상의 **IPSec settings**에서 demand-dial 인터페이스를 위한 preshared key를 구성하고 Preshared key 인증을 활성화할 수 있습니다.

- **Connection Manager(연결 관리자) 강화**

Windows Server 2003 제품군에서는 Connection Manager와 Connection Manager Administrator Kit이 다음과 같이 강화되었습니다.

- Connection Manager 즐겨찾기

Connection Manager 즐겨찾기 기능을 이용해 사용자는 일반적인 전화 걸기 위치를 변경할 때 Connection Manager 속성의 반복되는 구성을 생략할 수 있습니다. 이 기능은 저장 및 간편한 액세스 설정을 위한 방법들을 제공하며 다음과 같은 시나리오에서 사용됩니다:
a. 회사 사무실과 제휴사의 사이트 사이를 자주 왕래하는 사용자가 있습니다. 이 사용자는 각 위치에 대한 Connection Manager 설정을 구성하는데 여기에는 가장 가까운 액세스 전화 번호, 지역번호 및 전화 걸기 규칙들이 들어 있습니다. 또한 이는 각기 고유한 이름도 가집니다. 사용자는 이제 저장된 설정들 중에서 하나를 선택하여 각 위치에 따라 네트워크 연결을 재빠르게 설정할 수 있습니다.

- 자동 프록시 구성

자동 프록시 구성 기능은 사용자의 컴퓨터가 기업 네트워크에 연결되어 있는 동안 내부 및 외부 리소스에 대해 적절하게 액세스하고 있는지 확인하기 위해, Connection Manager 프로필을 생성할 수 있는 능력을 부여합니다. 이 기능은 Internet Explorer 4.0 이상을 실행할 때 사용할 수 있습니다.
예를 들어 한 직원이 집에서 쓰는 컴퓨터에 프록시 설정 없이 인터넷을 검색하도록 설정해 두었다고 가정합시다. 이러한 구성은 사용자가 기업의 네트워크에 연결했을 때 문제를 일으키게 됩니다. IT 관리자는 사용자가 기업 네트워크에 연결될 때마다 사용하도록 적절한 프록시 설정을 제공하는 Connection Manager 프로필을 만들 수 있습니다.

- 클라이언트 로그 파일

이 기능은 Connection Manager 연결을 이용해 문제들을 재빠르고 정확하게 해결할 수 있도록 로그 파일을 실행시킬 수 있는 능력을 제공합니다. 예를 들어 사용자는 IT 관리자가 만든 Connection Manger 프로필을 사용하는 네트워크에 연결할 때 여러 문제들을 경험할 수 있습니다. 로그 파일이 사용자의 컴퓨터 상에 생성되며, 사용자는 이를 IT 관리자에게 보내 문제 해결 프로세스를 실행하도록 할 수 있습니다.

- VPN 서버 선택 지원

Windows Server 2003 제품군에서 제공되는 강화된 Connection Manager Administration Kit을 사용하여, 사용자들이 기업 네트워크에 연결할 때 사용할 VPN 서버를 선택하도록 Connection Manager 프로필을 구성할 수 있습니다. 이를 통해 다음과 같은 시나리오에서 VPN 연결이 성립할 수 있습니다:

a. 전세계 여러 지역에 VPN 서버를 보유하고 있는 수많은 지사를 가진 회사의 IT 관리자는 이동중인 사용자가 연결을 시도할 때 자신의 연결 방식에 가장 부합하는 VPN 서버를 선택할 수 있도록 Connection Manager 프로필을 구성할 수 있습니다.

b. 기업 VPN 서버는 유지관리를 위해 오프라인이 될 수 있습니다. 이런 시기에 사용자는 연결을 위해 다른 VPN 서버를 선택할 수 있습니다.

- **Connection Manager Administration Kit 마법사 개선 사항**

Connection Manager Administration Kit (CMAK)은 확장된 마법사 기능을 가지고 있으며 보다 개선된 대화상자와 사용자 프로필을 작성하기 전에 최상의 사용자 지정 작업을 수행할 수 있는 능력을 보유하고 있습니다. 이러한 개선 사항들은 사용자 지정 클라이언트 연결 패키지 구축 과정을 유연하게 해주며 최고의 사용자 지정 요구사항을 위해 .cms 또는 .cmp 파일을 편집해야 하는 수고를 덜어줄 수 있습니다. 이런 다양한 사용자 지정 작업은 CMAK 마법사에서 가능하며 여기에는 VPN 연결을 위해 특별히 고안된 사용자 지정 작업도 포함됩니다. 예를 들어, IT 관리자는 단일 프로필을 구성하여 다양한 클라이언트 운영체제에 보안 설정을 적용할 수 있으며, 또는 콜백이나 터미널 서비스 사용과 같은 원격 액세스 서버 기능을 활용하기 위해 프로필을 구성할 수 있습니다.

- Pre-Shared Key 구성

이 기능을 통해 IT 관리자는 CMAK를 사용하여 연결 관리자 프로필을 만들 수 있는데, 여기에는 VPN 서버의 preshared key가 들어 있어 L2TP/IPSec 연결을 인증할 때 이를 활용할 수 있습니다.

- VPN 연결을 위한 인트라넷 및 인터넷 동시 액세스 경로 관리

Windows XP와 Windows Server 2003 제품군이 나오기 전에는, Microsoft VPN 클라이언트가 자동으로 VPN 터널을 통해 모든 디폴트 경로 트래픽을 전송하는 디폴트 경로를 생성하였습니다. 비록 이를 통해 VPN 클라이언트가 자신의 기업 인트라넷에 액세스할 수 있다 하더라도, 클라이언트는 오로지 VPN 연결을 통해 기업의 인트라넷에 대한 인터넷 액세스가 가능할 경우 VPN 연결이 활성화된 동안에만 인터넷 리소스에 액세스할 수 있습니다. Windows XP와 Windows Server 2003의 새로운 Connection Manager 지원 기능을 통해 다음과 같은 작업이 이루어집니다.

- VPN 연결이 이루어지면, 디폴트 경로가 변경되는 대신 기업 인트라넷을 위한 특정 경로가

VPN 클라이언트의 라우팅 테이블(경로표)에 추가됩니다. 그리고 이로 인해 기업 인트라넷을 통한 인터넷 트래픽을 거치지 않고도 인트라넷(특정 경로를 사용하여)과 인터넷(기본 경로를 사용하여) 리소스에 동시에 액세스할 수 있게 됩니다.

Connection Manager Administration Kit을 사용하면 VPN 사용자들에게 배포된 connection manager 프로필의 일부로서 특정 경로를 구성할 수 있습니다. 또한 프로필에 구성되어 있는 것들 이외에도 현재 기업 인트라넷 경로나 추가 경로들을 포함한 Uniform Resource Locator (URL)도 지정할 수 있습니다.

2) 인터넷 연결 개선 사항

Windows Server 2003에서는 인터넷 연결에 대해 다음과 같은 개선 사항들이 이루어졌습니다.

- **Internet Connection Firewall (ICF: 인터넷 연결 방화벽)**

컴퓨터가 인터넷이나 또는 다른 측면의 경로에 연결되어 있다면, 이 때문에 컴퓨터나 그 안에 있는 데이터에 인증되지 않은 액세스 시도라는 위협을 받을 수 있습니다. 외부 네트워크에 연결되어 있는 컴퓨터가 독립형 컴퓨터이든 아니면 네트워크를 위한 게이트웨이로서 작동하고 있든(예를 들어, 인터넷 연결 공유 기능이 사용될 때) 간에 방화벽은 네트워크 트래픽이 통과할 때 안전하지 못한 네트워크 트래픽에 대해 홈 네트워크를 보호합니다.

Windows Server 2003 제품군은 그러한 방식으로 연결되어 있는 여러분의 컴퓨터나 홈 네트워크를 보호하기 위해 ICF(Internet Connection Firewall; 인터넷 연결 방화벽)를 포함하고 있습니다. ICF는 새로운 연결 마법사가 실행될 때, 대부분의 네트워크에 대해 무리 없이 작동할 수 있도록 기본 설정에 방화벽을 설정하면서 전화접속 연결이나 광대역 연결을 위해 자동으로 활성화됩니다. 방화벽은 또한 네트워크 연결(Network Connections) 폴더를 통한 연결을 위해 수동으로 활성화 혹은 비활성화될 수 있습니다.

ICF는 외부 네트워크의 어떤 트래픽이 허용되어야 하는지 결정하기 위해 방화벽 내부에서 이루어지는 커뮤니케이션을 모니터합니다. 외부 네트워크에서 온 트래픽은 기본값으로 방화벽에서는 허용되지 않습니다. 만약 방화벽 뒤에서 서비스나 프로그램(웹 서버와 같은)을 호스트할 경우엔 ICF 설정은 여러분의 필요에 맞게 변경할 수 있습니다.

ICF는 ISP(Internet service provider)에 직접 전화를 걸 때 원격 액세스 연결을 보호하기 위해 사용되기도 하며 DSL(Digital Subscriber Line)이나 케이블 모뎀을 통해 연결되는 LAN 연결을 보호하기 위해 사용될 수도 있습니다.

이 기능은 단지 Standard Edition, Enterprise Edition 및 Web Edition의 32-bit 버전에서 제공될 수 있습니다.

- **네트워크 연결 개선사항**

Windows Server 2003 제품군에서는 네트워크 연결에 대해 다음과 같은 내용들이 강화되었습니다.

A. 네트워크 및 전화 접속 연결을 위해 업데이트된 그룹 정책

이 기능은 Windows XP Professional 또는 Windows Server 2003 제품군 중 하나를 운영하는 컴퓨터 사용자들을 위해 네트워킹 기능의 여러 구성 요소들을 설정하는데 그룹 정책을 적용할 수 있게 해줍니다. 이러한 기능들이 다음 시나리오를 가능하게 만들어줍니다.

- IT 관리자들은 사용자를 Network Configuration Operators Group 의 한 구성원으로 만들 수 있는데, 이 Network Configuration Operators Group 의 구성원은 LAN 연결을 위해 Transmission Control Protocol/Internet Protocol (TCP/IP) 속성에 액세스할 수 있고 자신만의 고유 IP 주소를 구성할 수 있습니다.

- 사용자 계정이 컴퓨터 상의 로컬 Administrators 그룹의 구성원일 경우, 사용자는 ICS, ICF, Network Bridge 및 네트워크 연결 속성을 활성화하고 구성할 수 있습니다. 이러한 기능들은 활성화하거나 재구성하는 것은 네트워크 연결을 손상시킬 수도 있습니다. 반면 IT 관리자들은 이 기능을 사용해 로컬 관리자들마저도 이러한 기능들을 구성하지 못하도록 막는 정책을 활성화할 수 있습니다.

B. 광대역 인터넷 연결을 위한 PPPoE 클라이언트

Windows Server 2003 제품군은 PPPoE(Point-to-Point Protocol over Ethernet)를 사용해 연결을 구축할 수 있는 기능을 포함하고 있습니다. PPPoE와 DSL이나 케이블 모뎀 같은 광대역 인터넷 연결을 사용해 사용자들은 고속 데이터 네트워크에 대해 개별적인 인증 액세스를 확보할 수 있습니다. Windows의 이전 버전들에서 사용자는 ISP에 의해 공급되는 개별 소프트웨어를 설치해야만 했지만 이제는 이러한 지원들이 운영 체제 내에 내장되어 제공됩니다.
PPPoE 클라이언트 지원을 통해 다음과 같은 작업들이 가능해졌습니다:

- 인터넷에 연결하기 위해 PPPoE 로그인을 요구하는 광대역 연결을 보유하고 있는 가정 사용자가 있습니다. 내장된 PPPoE 클라이언트와 새 연결 마법사(New Connection Wizard)를 사용해 사용자는 완전히 통합된 인터넷 연결을 구축할 수 있습니다.

- IT 관리자는 이러한 기능을 사용해 내부 네트워크에 대한 액세스를 보다 안전하게 할 수 있으며 여기 사용되는 PPPoE 는 회의실이나 로비와 같은 회사의 공공 장소로부터의 모든 네트워크 액세스를 인증합니다.

Windows Server 2003 제품군에 내장된 이러한 기능을 통해 여러분은 ICS(다른 컴퓨터와의 광대역 연결을 공유하기 위해) 및 ICF(인터넷 공격으로부터 PPPoE 연결을 보호하기 위해)와 같은 여러 다른 기능들을 활용할 수 있습니다. PPPoE 연결은 또한 Internet Explorer와 다른 Windows 기반 구성요소 혹은 어플리케이션에서도 선택할 수 있는 방식입니다.

3) 기타 네트워크 액세스 옵션

Windows Server 2003 제품군에서는 네트워크 액세스에 대해 다음과 같은 개선들이 이루어졌습

니다.

■ 네트워크 브리지

가정에서나 소규모 사무실에서 네트워크를 구축할 경우 특정 네트워크 수단이 네트워크의 한 영역이나 또는 다른 곳에서 유난히 잘 작동하는 것을 발견할 수 있습니다. 예를 들어 몇몇 컴퓨터들은 전화 연결 잭 가까이에 위치하여 전화선 네트워킹 장치를 사용해 연결할 수 있습니다. 또 다른 컴퓨터들은 전화 연결 잭 근처에 있지 않기 때문에 무선과 같은 다른 네트워크 수단을 사용해야 하기도 합니다. Windows Server 2003에서는 이더넷이나 전화선, IEEE 802.11b wireless 및 IEEE 1394 등 여러 매체들이 지원됩니다. 특정 네트워킹 기술을 사용하여 커뮤니케이션할 수 있는 컴퓨터들이 LAN 세그먼트를 정의합니다.

전통적으로 TCP/IP를 사용해 이런 개별적인 LAN 세그먼트에 연결하려면 다른 매체들을 함께 연결하기 위해 다양한 서브넷 주소나 라우터를 구성해야 합니다. 네트워크 브리지(Network Bridge)는 Windows Server 2003 제품군 중 하나를 실행하는 컴퓨터를 활성화하여 단일 서브넷을 구축하기 위해 다양한 네트워크 세그먼트들을 연결시킵니다. 브리지 컴퓨터에서 다양한 LAN 세그먼트를 연결(브리징)하는 것은 Network Connections 폴더에서 다양한 연결을 선택하는 것만큼 쉽습니다. 단순히 연결 중 하나를 오른쪽 클릭하고 Bridge Connections을 클릭하기만 하면 됩니다.

네트워크 브리지(Network Bridge)를 사용하면 모든 네트워크 매체와 연결되며 간편하게 구성된 단일 서브넷으로 이루어진 네트워크를 구성할 수 있습니다. 브리지 컴퓨터는 어떤 컴퓨터가 어떤 LAN 세그먼트에 있는지에 대한 정보를 조사하고 보유하여 적절한 LAN 세그먼트 사이에 패킷을 전송하게 됩니다.

■ 자격증명 관리자 “Key Ring”을 사용하는 원격 액세스

Windows Server 2003 제품군에는 그 동안 시스템에서 사용되어온 다양한 자격 증명 모음이 들어있는 “key ring”을 포함된 Credential Manager Key Ring 기능이 있습니다. 이를 통해 여러분은 다양한 네트워크(사용자 이름과 암호를 포함하는 다양한 자격 증명을 가지고 있는 네트워크)에 동시에 액세스할 수 있으며 각 프롬프트에 대해 계속해서 자격 증명을 입력할 필요가 없습니다. 여러분이 연결을 시도하고 있는 네트워크 리소스에 대한 정보(서버이름과 도메인 이름과 같은 정보)는 key ring에서 적절한 자격 증명을 선택하기데 사용됩니다. 원격 액세스는 전화접속이나 VPN 연결이 성공적으로 성립할 때마다 임시 디폴트 자격 증명을 추가함으로써 Key Ring에 속하게 됩니다. 이 자격 증명은 연결을 설정할 때 사용되었던 사용자 이름과 암호를 포함하고 있는데, 이는 종종 네트워크 상의 리소스에 액세스할 수 있는 동일한 자격 증명이 되기 때문입니다. 이를 통해 원격 네트워크에 연결하고 그 해당 네트워크와 로컬 네트워크 상의 리소스를 유연하게 사용할 수 있게 됩니다.

■ All-User Remote Access Credential (모든 사용자 원격 액세스 자격 증명)

모든 사용자 원격 액세스 자격 증명 기능은 해당 컴퓨터 상의 모든 사용자들이 사용할 수 있는

사용자 이름과 암호를 포함해, 자격 증명 모음을 사용해 연결을 구축할 수 있는 능력을 제공합니다.
예를 들어 사용자가 자신의 집에서 로컬 ISP로 네트워크 연결을 보유하고 있다고 가정해 봅시다. 사용자는 이 연결이 모든 사용자 연결인지의 여부를 New Connection Wizard(새로운 연결 마법사)가 기동되는 동안 지정하고 모든 사용자를 위한 자격 증명을 저장합니다. 다른 구성원들은 이제 ISP에 연결할 때 사용자 이름이나 암호를 기억할 필요 없이 이 연결을 사용할 수 있습니다.

■ Internet Protocol over IEEE 1394 (IP/1394) 지원

Windows Server 2003 제품군은 100에서 400Mbps를 지원하는 직렬 통신 버스 매체인 IEEE 1394 매체를 통해 TCP/IP 패킷의 송수신을 지원합니다. IEEE 1394는 일반적으로 오디오와 비디오 장치를 연결하는데 사용됩니다. IEEE 1394에 대한 지원은 또한 네트워크 브리지를 위한 IEEE 1394 프레임의 처리도 포함합니다.
IEEE 1394 링크를 위해 필요한 구성은 따로 없습니다. 이들은 자동으로 검색되고 구성됩니다.

4) 프로토콜에 대한 변경

■ TCP/IP 변경과 개선 사항

Windows Server 2003 제품군을 위한 TCP/IP 프로토콜에 대해 다음과 같은 변경과 개선 사항들이 이루어졌습니다.

- 제거될 수 없는 TCP/IP 프로토콜

TCP/IP 프로토콜(네트워크 연결 폴더의 연결 속성에서 Internet Protocol (TCP/IP)라고 명명된)은 디폴트로 설치되며 제거될 수 없습니다. 발생 가능한 TCP/IP 구성 문제 해결의 첫 번째 단계는 TCP/IP 프로토콜을 제거하고 이를 재설치하는 것이었습니다. 그러나 이제 Windows Server 2003 제품군에서는 이것이 더 이상 가능하지 않습니다. 대신 새로운 netsh 명령을 사용하여 설치 기본값에 TCP/IP 구성을 재설정할 수 있습니다.

- 다중 네트워크 연결을 위한 자동 선택 구성

여러분은 선택 구성을 통해 컴퓨터가 DHCP(Dynamic Host Configuration Protocol) 클라이언트이거나 컴퓨터 시작 시 어떤 DHCP 서버도 찾을 수 없을 때 수동으로 고정 TCP/IP를 설정할 수 있습니다. Windows 2000, Windows 98 및 Windows Millennium Edition을 운영하며 DHCP 클라이언트로 구성된 컴퓨터가 DHCP 서버를 찾을 수 없을 때, Automatic Private IP Addressing(APIPA)은 자동으로 169.254.0.0.16 주소 공간에서 고유의 주소를 할당하게 됩니다. APIPA가 TCP/IP를 시작하는 동안에는 기본 게이트웨이 주소, DNS(Domain Name System) 서버 IP 주소를 할당하거나 또는 인터넷이나 인트라넷 상의 커뮤니케이션을 위해 필수적인 다른 설정들을 하지 않습니다. 선택 구성은 컴퓨터가 하나 이상의 네트워크에서 사용되며 그런 네트

워크 중 하나가 DHCP 서버를 가지고 있지 않고 APIPA 주소 방식 구성이 요구되지 않는 상황에서 유용합니다.
예를 들어 사용자가 집과 사무실에서 사용하는 랩톱 컴퓨터를 가지고 있을 경우, 사무실에서는 DHCP 할당 TCP/IP 구성을 사용하고 집에서는 DHCP 서버가 없기 때문에 자동으로 선택 구성을 사용하여 홈 네트워크 및 인터넷에 쉽게 액세스하게 됩니다. 선택 구성을 이용하면 랩톱 컴퓨터가 사무실이나 홈 네트워크에 연결될 때 수동으로 TCP/IP 설정을 재 구성할 필요가 없습니다.
TCP/IP 선택 구성은 네트워크 연결 폴더의 LAN 연결 속성에 있는 **Internet Protocol (TCP/IP)** 프로토콜 속성의 **Alternate Configuration**(선택 구성) 탭에서 구성할 수 있습니다.

- TCP/IP 디폴트를 재설정하는 Netsh 명령

Windows Server 2003 제품군에 추가된 이 새로운 netsh 명령은 원래의 기본값에 여러분의 TCP/IP 구성을 재설정하도록 해 줍니다. 새로운 netsh 명령은 **netsh interface ip reset**이며 명령 프롬프트에서 입력합니다.
Windows의 초기 버전에서 여러분은 **Internet Protocol (TCP/IP)** 프로토콜을 제거하거나 재설치할 수 있었습니다. Windows Server 2003 제품군에서 TCP/IP는 디폴트로 설치되며 제거될 수 없습니다. 이 기능은 IT 관리자가 컴퓨터 사용자 임의로 TCP/IP 구성을 변경했는지 알고자 할 때 유용하게 사용됩니다.

- Display TCP Port Ownership 에 대한 새로운 Netstat 옵션

Netstat 도구에 새로이 추가된 옵션은 활성화된 TCP 연결을 보여주며 각 연결에 대한 PID(process identifier)를 포함합니다. Windows 작업 관리자의 **프로세스** 탭에서 PID에 기반한 어플리케이션을 찾을 수 있습니다. 기본값으로 PID는 Windows 작업 관리자에는 나타나지 않습니다. Windows 작업 관리자가 PID를 보여주도록 구성하려면 **View (보기)**를 선택하고 **Select Columns (열 선택)**를 선택한 다음 다시 목록에서 **PID (Process Identifier)**를 클릭하고 OK (확인)를 클릭합니다.

- IGMP version 3

IGMPv3는 소스 기반의 멀티캐스트 그룹 멤버십 보고 기능을 제공합니다. 호스트는 지정된 소스나 특정 소스 모음에서 멀티캐스트 트래픽을 수신하도록 요청할 수 있습니다. 소스 지정식의 보고 기능은 멀태캐스트 가능 라우터가 멀티캐스트 트래픽 소스를 위한 수신 호스트가 없는 서브넷에 멀티캐스트 트래픽을 전송하지 못하도록 해줍니다. IGMPv3 지원 기능은 디폴트로 활성화되며 별도의 구성이 필요하지 않습니다.

- 인터페이스 속도에 기반한 라우팅 메트릭스 자동 결정

이 기능을 통해 TCP/IP 프로토콜은 관련된 인터페이스의 속도 기반 TCP/IP 구성에서 파생한 경로를 위해 라우팅 메트릭을 자동으로 결정할 수 있습니다. 예를 들어 10 Mbps 이더넷 네트

워크 어댑터의 TCP/IP 구성에서 파생된 경로들은 30개의 라우팅 메트릭을 보유하고 있으며 100 Mbps 이더넷 네트워크 어댑터의 TCP/IP 구성에서 파생된 경로들은 20 개의 라우팅 메트릭을 보유하고 있습니다.

이 기능은 동일한 디폴트 게이트웨이를 사용하도록 구성된 서로 다른 속도의 다중 인터페이스를 보유하고 있는 경우, 가장 빠른 인터페이스가 기본 경로로 가장 낮은 라우팅 메트릭을 보유하고, 자신의 디폴트 게이트웨이로 트래픽을 전송하기 위해 사용될 때 매우 유용합니다. 가장 빠른 속도의 다중 인터페이스의 경우, 바인딩 순서에서 가장 먼저 나와 있는 인터페이스가 디폴트 게이트웨이로 트래픽을 전송하는 데 사용됩니다.

인터페이스 메트릭 자동 결정은 **IP 설정** 탭의 **Automatic metric (자동 메트릭)** 체크박스에서 디폴트로 활성화되고 더불어 네트워크 연결 폴더의 연결에서 **Internet Protocol (TCP/IP)** 프로토콜 속성의 **Advanced TCP/IP Settings(고급 TCP/IP 설정)** 에서 디폴트 게이트웨이를 수동으로 구성할 때 활성화됩니다.

- 로컬 네트워크 어댑터에 의해 결정되는 창 크기를 받아들이는 TCP

창 크기는 별도의 승인 없이 전송될 수 있는 바이트의 최대 값을 결정합니다. 느린 속도의 전화 접속 네트워크 연결에서 창 크기는 원격 액세스 서버 상의 대기열 크기와 거의 동일합니다. 대기열이 한 TCP 연결의 TCP 세그먼트들로 가득 차면, 새로운 TCP 연결은 모든 패킷이 보내질 때까지는 성립될 수 없습니다. 게다가 새로운 연결의 느린 TCP 시작 알고리즘은 상황을 더욱 악화시킵니다. 이 기능과 더불어 ICS가 가능한 컴퓨터 상의 QoS(Quality of Service) 패킷 스케줄러가 전화접속 네트워크 연결 속도에 맞도록 창 크기를 조정할 것입니다. 이는 원격 액세스 서버에서 대기열 길이를 줄여주며 새로운 연결들이 보다 잘 작동할 수 있도록 해 줍니다. 홈 네트워크에서 모든 홈 컴퓨터들은 일반적으로 높은 속도의 LAN 상에서 운영되며 ICS 컴퓨터를 통해 인터넷에 연결됩니다. ICS 컴퓨터는 전화 접속 모뎀을 사용해 인터넷에 연결됩니다. 홈 컴퓨터가 용량이 큰 파일 전송을 시도하면 다른 홈 컴퓨터들은 인터넷 연결이 다소 느려질 것입니다(예를 들어 웹 브라우저를 사용할 때). 이 기능을 사용함으로써 다른 홈 컴퓨터들의 새로운 인터넷 TCP 연결이 보다 빨라질 것입니다.

이 기능은 단지 ICS가 사용되고 별도의 다른 구성을 요구하지 않을 때만 디폴트로 활성화됩니다.

■ IPv6 프로토콜 스택

Windows Server 2003 제품군에는 생산시 사용을 목적으로 고안된 IPv6 프로토콜 스택이 들어 있습니다. Windows Server 2003 제품군의 IPv6프로토콜은 다음과 같은 기능들을 가지고 있습니다.

- Windows Sockets 지원
- 6to4 터널링
- Intrasite Automatic Tunnel Addressing Protocol
- PortProxy

- Site prefixes in router advertisements
- DNS 지원
- IPSec 지원
- 어플리케이션 지원
- RPC 지원
- 고정 라우터 지원

이제부터 각각의 기능에 대해 자세히 살펴보겠습니다.

a. Windows Sockets 지원

Windows Server 2003 제품군은 RFC 2553에 기술된 것처럼 Windows Sockets 어플리케이션을 위한 이름 대 주소, 주소 대 이름 분해를 수행하는 새로운 Windows Sockets 함수 GetaddrInfo()과 GetnameInfo()를 지원합니다. Gethostbyname()과 Getaddrbyname()대신 이 함수들을 사용함으로써 여러분은 Windows Sockets 어플리케이션을 컴퓨터에서 운영되고 있는 IP 버전 (IPv4 또는 IPv6)과는 독립적으로 만들 수 있습니다.

b. 6to4 터널링

6to4 터널링은 RFC 3056에 기술되어 있는 터널링 기술입니다. Windows Server 2003 제품군의 IPv6 프로토콜 구성요소 중 하나인 6to4는 IPv4 인트라넷을 통한 IPv6/IPv4 호스트들 간에 IPv6 연결과 자동 터널링을 허용합니다. 6to4 호스트는 IPv4 공용 주소에서 파생된 IPv6 주소를 사용합니다. 6to4와 더불어, IPv6 사이트와 호스트들은 6to4 기반 주소와 IPv4 인터넷을 사용해 ISP(Internet service provider)에게서 IPv6 전체 주소 식별번호를 확보하여 IPv6 인터넷에 연결할 필요 없이 통신을 할 수 있습니다.

c. Intrasite Automatic Tunnel Addressing Protocol(ISATAP)

Intrasite Automatic Tunnel Addressing Protocol (ISATAP)이란 사이트의 IPv4 인프라 내에 있는 IPv6/IPv4 노드가 IPv6를 사용해 서로 간에 또는 IPv6 활성화 네트워크 상의 노드들과, 사이트 내에서나 혹은 IPv6 인터넷 내에서 통신할 수 있게 하는 주소 할당 및 자동 터널링 매커니즘을 말합니다. ISATAP은 Internet draft "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)"에 기술되어 있습니다.

d. PortProxy

PortProxy 구성요소는 일반적인 인터넷 계층 프로토콜(IPv4 또는 IPv6)을 사용해서는 연결할 수 없는 노드나 어플리케이션 사이에 통신을 용이하게 해 줍니다. PortProxy는 다음에 대한 TCP 트래픽의 프록싱을 허용합니다:

- IPv4 전용 노드는 IPv6 전용 노드에 액세스할 수 있습니다.

- IPv6 전용 노드는 IPv4 전용 노드에 액세스할 수 있습니다.
- IPv6 노드는 IPv6/IPv4 노드 상에서 실행되는 IPv4 전용 서비스에 액세스할 수 있습니다.

이 마지막 시나리오는 Windows Server 2003 제품군의 IPv6 프로토콜을 실행하는 컴퓨터들이 IPv6을 사용해 Windows 2000 Server 제품군과 IIS(Internet Information Services)를 실행하는 컴퓨터 상의 웹 페이지들에 액세스할 수 있도록 합니다. Windows 2000 IIS는 IPv6을 지원하지 않습니다. 따라서 이에 액세스하는 유일한 방법은 IPv4를 사용하는 것입니다. PortProxy가 Windows Server 2003 제품군을 실행하는 컴퓨터 상에 구성되었을 때, 들어오는 IPv6 기반 웹 요청들은 Windows 2000 IIS 서버로 프록시되며 이는 IIS 서버가 IPv6이 활성화된 웹 브라우저와 간접적으로 통신할 수 있게 해 줍니다.
PortProxy 서비스를 구성하려면 netsh interface portproxy add|set|delete v4tov4|v4tov6|v6tov4|v6tov6 명령을 사용하십시오.

e. Router Advertisements 의 사이트 접두사

게시된 온-링크 접두사는 사이트 접두사 길이를 사용해 구성될 수 있으며 이는 Internet draft "Site prefixes in Neighbor Discovery"에 기술되어 있습니다. 여러분은 주소 접두사에 사이트 접두사 길이를 포함하기 위해 **netsh interface ipv6 add|set route** 명령을 사용할 수 있습니다.
사이트 접두사를 지정하는 접두사 정보 옵션이 송신되면 항목이 사이트 접두사 표에 생성됩니다. **netsh interface ipv6 siteprefixes** 명령을 사용해 이 표를 볼 수 있습니다. 이 사이트 접두사 표를 사용하여 Getaddrinfo() Windows sockets 함수에 의해 반송되는 내용에서 적절하지 못한 사이트-로컬 주소를 제거합니다.

■ DNS 지원

RFC 1886, "DNS Extensions to support IP version 6"에 기술되어 있는 Domain Name System (DNS) IPv6 호스트 레코드 처리(AAAA 또는 quad-A 리소스 레크드로 알려져 있음) 및 AAAA 레코드의 동적 등록은 Windows Server 2003 제품군의 DNS resolver (클라이언트)와 Windows Server 2003 제품군 및 Windows 2000의 DNS Server 서비스에 의해 지원됩니다. DNS 트래픽은 IPv6과 IPv4에서 지원됩니다.

- IPSec 지원

Message Digest 5 (MD5) 해시를 사용한 Authentication Header (AH) 처리와 NULL ESP 헤더 및 MD5 해시를 사용한 Encapsulating Security Payload (ESP) 처리가 지원됩니다. ESP 데이터 암호화와 IKE 프로토콜에 대해서는 어떤 지원도 이루어지지 않습니다. IPSec 보안 정책, 보안 연계 및 암호화 키는 Ipsec6.exe 도구를 사용해 반드시 수동으로 구성되어야 합니다.

- 운영 체제 구성요소 및 어플리케이션 지원

IPv6 의 사용을 지원하는 Windows Server 2003 제품군에 포함된 시스템 구성요소와 어플리케

이션들은 Internet Explorer, Telnet client (Telnet.exe), FTP client (Ftp.exe), IIS 6.0, 파일 및 프린트 공유(서버와 워크스테이션 서비스), Windows Media™ Services 및 Network Monitor를 포함합니다.

- RPC 지원 <<add DCOM support>>

RPC 함수들은 어플리케이션 함수 호출을 네트워크를 통해 원격 시스템에 전송하는데 사용됩니다. Windows Server 2003 제품군에 들어 있는 RPC 구성요소들은 IPv6이 활성화되어 있습니다. RPC 구성요소들은 업데이트된 Windows Socket들을 사용하도록 변경되어 왔으며 이는 RPC가 IPv4와 IPv6 양쪽에서 다 작동할 수 있도록 해줍니다.

- IP Helper API 지원

Internet Protocol Helper (IP Helper)는 로컬 컴퓨터 네트워크 구성의 관리에서 지원되는 API 입니다. IP Helper를 사용하면 로컬 컴퓨터의 네트워크 구성에 대한 정보를 검색할 수 있고 또한 그 구성을 수정할 수 있습니다. IP Helper는 또한 알림 매커니즘을 제공하여 로컬 컴퓨터에서 네트워크 구성의 일부분이 변경되었을 때 어플리케이션이 이를 통보받을 수 있게 합니다. Windows Server 2003 제품군의 IP Helper는 IPv6과 그 구성요소들을 위한 정보 검색을 허용하도록 확대되어 왔습니다.

■ 고정 라우터 지원

Windows Server 2003 제품군을 실행하는 컴퓨터는 IPv6 라우팅 테이블의 컨텐츠에 기반하고 있는 인터페이스들 사이에서 IPv6 패킷을 전송하는 고정 IPv6 라우터로서 작동할 수 있습니다. **netsh interface ipv6 add route** 명령을 사용해 고정 경로를 구성할 수 있습니다. 라우팅 및 원격 액세스 서비스를 위해서는 어떤 IPv6 라우팅 프로토콜도 제공되지 않습니다.
Windows Server 2003 제품군을 운영하는 컴퓨터는 router advertisements를 전송할 수 있습니다. router advertisements의 컨텐츠는 라우팅 테이블에 나와 있는 경로에서 자동으로 파생됩니다. 게시되어 있지 않은 경로도 라우팅을 위해 사용될 수는 있으나 router advertisements에 전송되지는 않습니다. Router advertisements는 항상 소스 링크 계층 주소 옵션과 MTU 옵션을 포함하고 있습니다. 이 MTU 옵션의 값은 보내는 인터페이스의 현재 링크 MTU로부터 매겨집니다. 그리고 **netsh interface ipv6 set interface** 명령을 사용해 이 값을 변경할 수 있습니다. 게시되도록 구성된 기본 경로가 있을 경우에는 Windows Server 2003 제품군을 실행하는 컴퓨터만이 자신을 디폴트 라우터로 알릴 것입니다(0 이상의 라우터 주기를 가진 router advertisement를 사용하여).

- 웹 트래픽의 커널 모드 프로세싱

HTTP.SYS는 HyperText Transfer Protocol (HTTP)의 클라이언트 및 서버 양측의 커널 모드의 구현입니다. 이는 확장적이고 효율적인 HTTP의 구현을 목적으로 하며, 완료 포트에 요청과 응답 완료를 바인드하는 능력을 포함하여 진정한 Win32® asynchronous I/O 사용을 허용합니다.

클라이언트 측을 위한 사용자 모드 API는 WinHTTP나 .NET Framework Classes와 같은 기존 API들을 통해 나타날 것입니다. 서버 측HTTP.SYS는 Windows Server 2003 제품군에서 제공되며 IIS 6.0에 의해 사용됩니다. 클라이언트와 서버 모두를 포함하는 HTTP.SYS의 완전한 버전은 Windows의 향후 버전에서 제공될 것입니다.

■ Quality of Service 강화

Windows Server 2003 제품군에서는 Quality of Service (QoS)와 관련하여 다음과 같은 내용들이 개선되었습니다.

- 홈 네트워크를 위한 창 크기를 수신하는 TCP

홈 네트워크가 기업 또는 다른 네트워크에 전화 접속 라인과 같은 저속 링크를 통해 연결되었을 때 저속 링크를 통과하는 트래픽에 지연 현상이 일어날 수 있습니다.
수신하는 클라이언트가 (ICS 박스를 넘어) 상대적으로 빠른 네트워크(예, 100 Mbps 이더넷)에서 실행되고, 원격 액세스 박스를 뛰어넘어 리시버(수신자)가 통신하고 있는 서버가 빠른 네트워크를 사용하고 있을 경우, 일종의 불일치가 일어납니다. 이 시나리오에서 수신자의 수신 창은 연결 속도에 따른 큰 값으로 설정됩니다. 송신자는 낮은 비율부터 송신을 시작하지만 패킷이 손실되지 않기 때문에 결국엔 거의 창 크기만큼의 패킷을 전송하게 됩니다.
이는 같은 네트워크를 가로지르는 다른 TCP 연결 성능에 영향을 주며, 이들의 패킷을 사실상 이러한 대규모의 대기열에서 기다리게 만듭니다. 패킷 손실이 일어나면 원래 창의 크기가 재송신되어야 하며 이는 또 다른 링크 정체를 가져옵니다.
이에 대한 해결책은 네트워크 집합 상의 ICS 컴퓨터가 수신 창을 저속 링크에 알맞은 작은 사이즈로 조정하는 것이며, 이는 수신자의 설정 내용(수신자가 지정했던 내용)을 무효화합니다. 반대로 이 설정은 수신자가 저속 링크에 직접 연결되었을 경우엔 창 크기가 그에 맞게 설정될 것이기 때문에 트래픽에 영향을 주지 않을 것입니다. ICS 컴퓨터에서 실행되고 있는 QoS 패킷 스케줄러 구성요소가 이러한 창의 조정을 행합니다.
QoS 패킷 스케줄러에 관한 자세한 정보는 Windows XP 도움말을 살펴보십시오. QoS에 관한 추가 정보는 다음의 Windows 2000 Networking and Communications Services(Windows 2000 네트워킹 및 커뮤니케이션 서비스) 웹 사이트에서 찾아보실 수 있습니다:
http://www.microsoft.com/windows2000/technologies/communications/default.asp.

5)향상된 네트워크 장치 지원

Windows Server 2003 제품군에서는 네트워크 장치 지원에 있어 다음과 같은 점들을 개선하였습니다.

A. Permanent Virtual Circuit Encapsulation (고정 가상 회선 캡슐화)

Windows Server 2003 제품군은 RFC 2684의 사안을 구현합니다. 이는 업체들이 DSL을 보다 쉽게 구현할 수 있도록 추가되었습니다. 이것의 구현 내용은 NDIS intermediate driver(중간 드라이버)로, 이는 마치 이더넷 인터페이스처럼 보이지만 DSL/Asynchronous Transfer Mode

(ATM) permanent virtual circuit (PVC)를 사용하여 이더넷(또는 TCP/IP 전용) 프레임을 수행합니다. 이런 매커니즘은 일반적으로 업계에서 DSL을 구축하는 사업자들에 의해 사용됩니다. Windows Server 2003 제품군과 DSL 장치를 위한 ATM miniport driver를 이용해 DSL 배포에는 다음의 프로토콜 구성들을 사용할 수 있습니다.

- 업체 DSL ATM miniport driver 를 사용하는 PPP over ATM (PPPoA) 상의 TCP/IP
- 업체 DSL ATM miniport driver 를 사용하는 RFC 2684 (4 개의 캡슐화 형식) 상의 TCP/IP
- 업체 DSL ATM miniport driver 를 사용하는 RFC 2684 (4 개의 캡슐화 형식) 상의 PPPoE 를 통한 TCP/IP

추가로 802.1X 인증이 RFC 2684 이더넷 인터페이스에 추가될 수 있습니다. 이러한 선택의 다양성은 다수의 DSL 배포를 위해 필요합니다. 더 자세한 정보는 RFC 2684를 참고하시기 바랍니다.

B. NDIS 5.1 및 원격 NDIS

Enhancements include: 물리적 네트워크를 운영체제와 프로토콜에서 사용할 수 있도록 해주는 인터페이스 네트워크 카드와 이들의 드라이버는 Windows Server 2003 제품군에서 보다 강화되었습니다. 그 내용은 다음과 같습니다.

- **플러그 앤 플레이 및 전원 상태 알림** –네트워크 카드 미니포트 드라이버(miniport drivers)를 활성화하여 전원이나 플러그 앤 플레이 상태를 통보받을 수 있습니다. 그 결과 이러한 이벤트 중에 클리너 시스템 작동이 이루어집니다.
- **전송 취소 지원** –네트워크 프로토콜은 네트워크 패킷 전송 요청이 완료될 때까지 오랜 시간 기다릴 필요가 없어졌습니다.
- **향상된 통계 용량(64-bit 통계 카운터)** –이러한 개선 사항을 통해 고속의 네트워크 미디어에서 정확한 네트워크 통계를 보여줄 수 있게 되었습니다.
- **성능 강화** –몇 가지 개선 사항들을 통해 중요한 네트워크 데이터 경로가 보다 더 효율적이 되었으며 불필요한 패킷 사본들도 생략할 수 있게 해 주었습니다.
- **Wake on LAN 변경** –Wake on LAN 에 이루어진 변경 사항을 통해 여러분은 wake up 패킷을 단지 magic packet(매직 패킷)으로 한정할 수 있게 되었습니다(프로토콜 등록 패킷 패턴 대신에). 이는 네트워크 어댑터 속성의 **Power Management (전원 관리)** 탭에서 구성할 수 있습니다.
- **부수적인 변경들** –이 밖에도 몇몇의 추가적인 변경들이 이루어져 드라이버 개발자들의 일반적인 필요나 요구를 충족시켰으며 또한 드라이버 완전성을 향상시켰습니다.

원격 NDIS 역시 Windows Server 2003 제품군에 포함되었습니다. 원격 NDIS는 써드 파티 드라이버 설치 없이도 USB 부착 네트워크 장치를 지원할 수 있게 하였습니다. Microsoft는 네트워크 장치들과 통신할 수 있는 드라이버들을 제공합니다. 이를 통해 설치가 간편해졌으며 제대로

갖추어지지 않았거나 테스트되지 못한 드라이버 때문에 일어나는 시스템 중단의 문제도 줄일 수 있습니다.

NDIS 5.1 및 원격 NDIS에 관한 추가 정보는 Windows Server 2003 family DDK와 다음 웹 페이지를 참조하시기 바랍니다:

http://www.microsoft.com/hwdev/network/NDIS51.htm

http://www.microsoft.com/hwdev/network/rmNDIS.htm

C. 향상된 네트워크 미디어 지원

몇몇 최신 네트워크 장치에 대한 지원 내용이 Windows Server 2003 제품군에 추가되었습니다. 여기에는 여러 가지 새로운 네트워킹 장치에 대한 지원도 포함됩니다. 새로운 HomePNA (전화선) 장치의 대부분이 지원됩니다. 대부분의 USB 연결 네트워크 장치 역시 Windows Server 2003 제품군에서 지원되며, 몇몇은 추가 드라이버가 필요 없는 원격 NDIS를 사용합니다. 802.11 무선 장치에 대한 지원도 보다 강화되었습니다. 이들 장치 대부분이 또한 Windows Server 2003 제품군에서 무선 제로 구성(zero configuration) 및 로밍 기능을 지원합니다. Windows의 모뎀 지원 역시 많은 소프트 모뎀들을 포함하도록 Windows Server 2003 제품군에서 확대되었습니다.

D. CardBus Wake on LAN

이 기능을 사용해 컴퓨터는 CardBus LAN 카드에 의한 대기 상태에서 다시 복구될 수 있습니다. IT 관리자는 서버 그룹 관리를 보조하기 위해 이 기능을 사용할 수 있습니다.

E. 장치 드라이버 강화

이 기능은 홈 네트워킹에서 일반적으로 사용되며 더 이상 관련이 없는 레거시 장치 드라이버를 제거하기 위해 사용되는 네트워크 장치 드라이버에 추가되었습니다. 이는 또한 네트워킹 드라이버의 품질을 향상시켰습니다.

- **LAN 네트워크 드라이버** –10/100 Network Interface Cards (NICs), IEEE 802.11 및 Home Phoneline Networking Alliance (HomePNA)를 포함.
- **광대역** –케이블 모뎀, Asymmetric Digital Subscriber Line (ADSL) 및 Integrated Services Digital Network (ISDN)를 포함.
- **모뎀** 드라이버 기반 모뎀 및 56kbps V.90 모뎀 포함.

Windows Server 2003 제품군 중 하나로 자신의 컴퓨터를 업그레이드한 가정 사용자는 자신들이 최근에 사용한 네트워크 장치들이 이미 이 새로운 운영 체제에서 지원되고 있다는 사실을 눈치챘을 것입니다.

F. Wake on LAN: Select Wake Event 개선 사항

Windows 2000에서 처음 소개된 Wake on LAN (WOL) 기능은 네트워크 패킷에서 특정 패턴 수신 시에 NIC이 버스 전원 관리 wake-up 이벤트를 작동시킬 수 있게 해주는 WOL-활성화 네트워크 어댑터의 하드웨어 능력을 뜻합니다. 이 기능에서는 다음과 같은 사항들이 개선되었습니다.

- wake-up 이벤트를 야기하는 모든 패킷 패턴으로 완전히 활성화된 WOL.
- wake-up 이벤트를 야기하는 Magic Packets(매직 패킷)만으로 활성화된 WOL.
- 완전히 비활성화된 WOL.

이 새로운 기능들은 다음 시나리오를 가능하게 합니다.

- 컴퓨터의 전력 사용을 절약하고자 하는 사용자는 전원 상태를 대기 모드 상태로 둘 수 있습니다. 그러나 이 사용자는 동시에 네트워크 상의 다른 컴퓨터가 자기 컴퓨터 상의 서비스를 사용하거나 관리 작업을 수행하고자 할 경우 바로 대기 모드에서 돌아오도록 합니다.
- IT 관리자는 컴퓨터 상의 WOL 을 통제할 수 있도록 이 기능을 WOL 를 완전히 활성화하는 상태로 설정해 둡니다.

G. IrDA 를 위한 IrCOMM 모뎀 드라이버

사용자는 IrCOMM 모뎀 드라이버를 사용하면 적외선 기능을 사용할 수 있는 자신의 이동전화를 모뎀으로서 사용할 수 있습니다. 이동 전화를 적외선 포트 옆에 두면 이는 적합한 드라이버를 찾아 설치합니다(또는 적당한 모델이 발견되지 않으면 일반적인 드라이버를 사용). 이런 작업이 끝나고 나면 이제 이동 전화를 네트워크 연결을 구축하기 위한 모뎀처럼 사용할 수 있습니다. 이 드라이버를 통해 다음과 같은 일들이 가능해 집니다:

- IrCOMM 프로토콜과 적외선 기능을 사용할 수 있는 이동 전화를 가지고 있는 사용자는 이 전화를 인터넷에 액세스할 수 있는 모뎀으로 사용하고자 합니다. 위 기능을 사용하면 휴대용 컴퓨터가 이 이동 전화를 인식하고 이를 찾아 모뎀으로서 설치합니다. 사용자는 내장된 모뎀을 사용하는 것과 같은 방식으로 전화를 걸어 인터넷에 접속합니다.

이 기능은 단지 Enterprise Edition과 Web Edition에서만 제공됩니다.

6)새로운 네트워크 서비스 지원

Windows Server 2003 제품군에서는 네트워크 서비스 지원에 있어 다음과 같은 내용들이 강화되었습니다.

A. TAPI 3.1 및 TAPI Service Providers (TSP)

과거의 Windows 운영체제들은 Telephony API (TAPI)의 이전 버전들을 장착했었고, 가장 최근의 Windows 2000은 TAPI 3.0을 장착하였습니다. TAPI는 어플리케이션이 사용자에게 다양한 형

식의 telephony 서비스를 제공할 수 있도록 해줍니다.

TAPI 3.1은 Microsoft Component Object Model (COM)을 지원하며 프로그래머에게 COM 개체 모음을 제공합니다. 이는 모든 COM 호환 프로그래밍 어플리케이션과 스크립팅 언어를 사용하여 telephony 어플리케이션을 작성할 수 있게 해 줍니다.

Windows XP에 포함되어 있는 TAPI service providers (TSPs)는 IP telephony에 기반하여 H.323을 위한 기능들을 제공하며 더불어 TCP/IP 네트워크에서 IP 멀티캐스트 오디오 및 비디오 회의를 할 수 있게 해줍니다. 이는 또한 이전 Windows 버전들에서 제공되는 TSPs에 추가됩니다. H.323 TSP 및 media service provider (MSP: 미디어 서비스 제공자)는 H.323 version 2 기능을 지원합니다.

또한 다음의 사항들이 TAPI 3.1와 함께 제공됩니다:

파일 터미널: 어플리케이션들이 파일에 스트리밍 데이터를 기록하여 이 기록된 데이터를 다시 스트림으로 재생할 수 있도록 해줍니다.

Pluggable Terminals(플러그 가능한 터미널): 써드 파티가 MSP에 의해 사용될 수 있는 새로운 터미널 개체를 추가하도록 해 줍니다.

USB Phone TSP: 어플리케이션이 USB phone을 제어하고 이를 스트리밍 종점으로 사용할 수 있게 해줍니다.

TAPI Server의 자동 발견: 클라이언트가 네트워크에서 사용 가능한 telephony 서버를 찾도록 해줍니다.

추가로 H.323을 위해 다음과 같은 부수적인 서비스(보다 다양한 호출 통제 기능)들이 제공됩니다.

Call Hold Service (ITU-T Recommendation H.450-2)

Call Transfer Service (ITU-T Recommendation H.450-2)

Call Diversion Services (ITU-T Recommendation H.450-3)

Call Park and Pickup Service (ITU-T Recommendation H.450-5)

B. Real Time Communication (RTC) Client APIs

Real Time Communications (RTC) Client Application Programming Interfaces (APIs) 기능은 Session Initiation Protocol (SIP)에 기반한 차세대 통신 플랫폼을 제공합니다. SIP은 호출자의 위치를 알 필요 없이 전자메일 주소를 사용하여 일반 세션을 구축하는 프로토콜을 제공합니다. 결국 이는 커뮤니케이션에 보다 효율적인 수단을 제공하는 것입니다. RTC는 음성, 비디오 및 데이터 공동 작업 어플리케이션과 같이 기능들이 집중되어 있는 어플리케이션을 통해 보다 강화된 인터넷 어플리케이션을 신속하게 배포할 수 있도록 해 줍니다.

Windows Server 2003 제품군은 RTC client APIs를 포함하는데 여기에는 buddy-list 관리, 사용자 실행 탐지, 인스턴트 메세징 세션 구축 능력, 양 클라이언트 간의 오디오 및 비디오 세션, 모든 전화 번호에 대한 전화 호출, 어플리케이션 공유 및 화이트보드 세션들이 포함됩니다. 클라이언트 APIs는 Secure Sockets Layer (SSL) 상의 SIP 서버에 대한 방화벽 터널링, 사용자 및 기본 인증 방식, 그리고 Universal Plug and Play (UPNP)가 활성화된 NATs를 통한 실시간 통신 세션을 가능케 하는 NAT 로직 등을 포함합니다. APIs는 고성능 오디오 및 비디오 미디어 스택

에 대한 액세스를 제공합니다. 오디오 및 비디오 품질은 다음과 같은 새로운 기능들에 의해 매우 향상되었습니다:

- Acoustic Echo Cancellation(AEC) –음성 호출을 하기 위해 헤드셋이 필요하지 않으며 내장되어 있는 echo cancellation(반향 소거) 기능이 높은 품질의 통신을 제공합니다.
- Quality control(품질 관리) –이 새로운 알고리즘은 네트워크 상태에 있어 감지된 변화들에 기반해 오디오 빛 비디오 설정을 적절하게 변경합니다.
- Forward Error Correction (FEC)는 네트워크 정체에 따른 패킷 손실을 보충하기 위해 사용됩니다.
- Dynamic Jitter buffers 는 수신된 패킷들 사이에서 지연으로 인해 발생한 변동에 따른 효과들을 제거하기 위해 수신된 오디오(음성, 음향 등등)를 부드럽게 하는데 사용됩니다.

RTC client APIs 를 통해 다음과 같은 일들이 가능해졌습니다:

- 게임을 개발하는 ISV 는 RTC client APIs 를 사용해 자신의 새로운 게임에 buddy lists, 인스턴트 메세징 및 오디오/비디오를 추가할 수 있습니다. 이에 따라 게임을 하는 동안 다른 사람들과 메시지를 주고 받으며 화상 채팅을 할 수도 있습니다.
- IT 관리자들은 소규모 어플리케이션을 구축해 메일 서버의 모든 사용자들에게 유지 관리를 위해 잠시 오프라인 상태가 됨을 미리 알려 줄 수 있습니다.
- 예산 관리 및 인사 관리 어플리케이션을 판매하는 ISV 는 RTC client APIs 를 사용해 ActiveX 컨트롤을 구축할 수 있습니다. 부서 관리를 위한 서버 웹 페이지에 컨트롤을 추가하여 직원 연락처 및 연락 상황을 살펴보거나 인스턴트 메시지나 오디오를 통해 예산에 관한 질문을 해결하며, 어플리케이션 공유를 통해 예산에 대해 함께 분석해 볼 수도 있습니다.

이 기능은 Web Edition의 32-bit 버전에서는 제공되지 않습니다.

C. DHCP

Windows Server 2003 제품군에서는 Dynamic Host Configuration Protocol (DHCP)에 대해 다음과 같은 개선이 이루어졌습니다.

D. DHCP 를 통한 백업 및 복구

DHCP 스냅인은 이제 DHCP 데이터베이스 백업 및 복구를 위한 새로운 메뉴 항목들을 제공합니다. 사용자가 이러한 메뉴 항목들을 선택할 때 브라우저 창이 나타나 위치를 선택하도록 한다거나 새로운 폴더가 생성된다거나 할 수 있습니다. IT 관리자는 이 기능을 이용해 Windows Server 2003 제품군을 실행하는 서버에서 백업과 복원을 수행할 수 있습니다.
이 기능은 Web Edition에서는 제공되지 않습니다.

E. Classless Static Route Option (클래스가 없는 고정 경로 옵션)

DHCP 클라이언트는 자신들의 라우팅 테이블에 추가할 수 있도록 이 옵션이 경로 목록과 함께 제공되도록 요청할 수 있습니다. 이는 원격 액세스와 VPN 클라이언트들이 원격 네트워크에 연결될 때 분할 터널링을 수행할 수 있도록 해줍니다. 또한 LAN 클라이언트들이 추가 라우팅 정보를 얻을 수도 있습니다.

예를 들어, IT 관리자들은 이 기능을 사용하여 클라이언트들이 VPN 연결이나 인터넷을 통해 분할 터널링 하도록 할 수 있습니다. 또한 인터넷으로 향하는 트래픽이 VPN 연결을 통해 가는 것을 막을 수 있으며, 이는 결국 사용자가 자기 회사나 조직의 사설 네트워크 리소스에 액세스할 수 있게 해줍니다.

F. Netsh 를 이용한 DHCP 데이터베이스 마이그레이션

이 기능을 사용해 한 서버에서 다른 서버로 DHCP 데이터베이스를 쉽게 마이그레이션 할 수 있습니다. 이는 수동으로 레지스트리를 편집하거나 범위를 재설정하는 것과 같은 대부분의 수동 구성 작업을 없애줍니다. Netsh는 로컬에서 서버나 라우터를 구성하는 데 이용되며 스크립트 파일을 사용해 구성 작업을 자동화할 수 있습니다. 이는 다음의 경우에 사용됩니다:

- IT 관리자가 DHCP 서버에서 디스크 오류 메시지를 발견하고 이 디스크가 완전히 중단되기 전에 DHCP 서비스를 이동하기로 결정합니다.
- DHCP 서버가 위치하고 있는 네트워크 세그먼트의 성능 문제 때문에 IT 관리자는 DHCP 서버를 분리해야 합니다. IT 관리자는 이 기능을 사용함으로써 DHCP 데이터베이스의 부분들을 다른 컴퓨터로 이동시킬 수 있습니다.

G. Netsh 를 이용한 DHCP Lease Deletion

새로운 **netsh dhcp server scope** *ScopeAddress* **delete lease**를 사용하여 명령줄에서 DHCP lease를 삭제할 수 있습니다. 이 기능은 DHCP 스냅인을 사용해 lease를 삭제하기 보다는 명령줄과 스크립트를 사용함으로써 DHCP 서버 작동을 쉽게 관리할 수 있도록 해줍니다.

H. DNS

Windows Server 2003 제품군에서는 DNS에 대해서도 다음과 같은 개선이 이루어졌습니다.

어플리케이션 파티션에 저장된 Active Directory 통합 DNS 영역

이 기능은 어플리케이션 파티션의 Active Directory® 서비스에 저장된 Domain Name System (DNS) 영역의 저장과 복제를 가능하게 하였습니다. DNS 데이터를 저장하는 어플리케이션 파티션을 사용하면 글로벌 카탈로그에 저장된 개체 수가 줄어듭니다. 게다가 DNS 영역 데이터가 어플리케이션 파티션에 저장될 때, 이는 단지 어플리케이션 파티션에 지정되어 있는 도메인의 도메인 컨트롤러 하위집합에만 복제됩니다. 기본적으로 DNS 지정 어플리케이션 파티션들은 오로지 DNS 서버를 운영하는 도메인 컨트롤러(Domain Controllers)들만을 포함합니다. 더불어 어

플리케이션 파티션에 DNS 영역 데이터를 저장함으로써 Active Directory 포리스트의 서로 다른 도메인들의 도메인 컨트롤러에서 운영되고 있는 DNS 서버에 대한DNS 영역의 복제를 수행할 수 있습니다.
IT 관리자는 이 기능을 사용하여 어플리케이션 파티션에 DNS 영역을 저장할 수 있습니다. 이는 Active Directory 통합 DNS 영역이 반드시 Windows Server 2003 제품군 중 하나를 실행하는 DNS 서버에 의해 호스트되어야만 할 때 권장되는 방식입니다.

I. DNS Security Extensions 에 대한 기본 승인

Windows Server 2003 제품군 중 하나를 실행하는 DNS 서버는 RFC 2535에서 정의된 Internet Engineering Task Force (IETF) standard DNS Security Extensions 프로토콜에 대한 기본 승인을 제공합니다. DNS 서버는 IETF 표준에서 정의된 레코드 형식(KEY, SIG, and NXT)들을 저장할 수 있으며 RFC 2535에 따라 쿼리에 대한 응답을 할 때 이러한 레코드들을 포함할 수 있습니다. 또한 서버는 써드 파티 소프트웨어에 의해 생성된 표준 KEY 및 SIG 기록을 저장하여 사용할 수도 있습니다.
IT 관리자는 DNS Security Extensions (per RFC 2535)을 완벽하게 지원하는 서버 상의 1차 사본과 함께 Windows Server 2003 제품군 중 하나를 운영하는 DNS 서버를 서명된 영역을 위한 2차 서버로서 사용할 수 있습니다.

J. 부적적하게 구성된 DNS 를 찾기 위해 도메인 합류 절차 강화

이 기능은 부정확한 DNS 구성의 보고 및 디버깅을 간단히 해주며 컴퓨터가 도메인에 합류하는데 필요한 DNS 인프라를 적절히 구성할 수 있도록 도와줍니다. Active Directory 도메인에 합류하려고 하는 컴퓨터가 도메인 컨트롤러를 찾을 수 없을 때(DNS가 잘못 구성되었거나 도메인 컨트롤러가 사용 가능한 상태가 아니라서)는 DNS 인프라의 디버깅이 이루어집니다. 또한 실패의 원인을 알려주고 어떻게 문제를 해결할 수 있는 지 설명해 주는 보고서를 생성합니다.
컴퓨터가 도메인에 합류할 수 있도록 DNS 인프라가 적절히 구성되었다면, IT 관리자는 이러한 기능이 존재한다는 사실을 발견하지 못할 것입니다. 그러나 DNS 인프라가 잘못 구성되었고 컴퓨터가 도메인 컨트롤러를 찾아 도메인에 합류하는 것을 막고 있을 경우, IT 관리자는 컴퓨터를 도메인에 합류시키기 위해 이 기능에 관심을 갖게 될 것입니다.

K. 그룹 정책을 사용하여 DNS 클라이언트 관리

이 기능을 통해 관리자는 Windows Server 2003 제품군 중 하나를 운영하는 컴퓨터에 그룹 정책을 사용해 DNS 클라이언트 설정을 구성할 수 있습니다. 이는 클라이언트에 의한 DNS 레코드의 동적 등록을 가능하게 하고 또 비활성화하는 것과 같이 DNS 클라이언트 설정을 조정할 때, 이름 분해 시 주 DNS 접미사의 위임 기능을 사용할 때, DNS 접미사 검색 목록을 추가할 때 도메인 멤버를 구성하는 데 필요한 단계들을 간단하게 해 줍니다. 단순한 관리 기능들과 더불어 DNS 접미사 검색 목록을 위한 그룹 정책 지원 또한 중요한 기능이며, NetBIOS가 없는 환경으로 변환 시 필요합니다.

IT 관리자들은 이 그룹 정책 기능을 사용해 DNS 클라이언트를 구성할 수 있습니다.

L. Stub Zones (스텁 영역) 및 Conditional Forwarding (조건부 전달)

Stub zones(스텁 영역)과 조건부 전달은 두 개의 DNS 서버 기능으로, 이는 네트워크 상에서 DNS 트래픽의 라우팅을 제어하는 능력을 제공합니다. Stub zones은 DNS 서버가 영역 내에 있는 모든 사본을 다 갖추지 않고도 또는 DNS 루트 서버에 쿼리를 전송하지 않고도 영역의 모든 사본에 대해 인증된 서버들의 이름과 주소를 알 수 있도록 해 줍니다. Windows 2000을 운영하는 DNS서버는 DNS 쿼리를 DNS 서버 집합으로 전송하도록 구성될 수 있습니다. Windows Server 2003 제품군의 조건부 전달 기능은 이름을 의존하는 전달에 대한 지원을 강화하였습니다. 예를 들어 DNS 서버는 동시에 다음과 같이 구성될 수 있습니다:

- usa.microsoft.com 으로 끝나는 이름에 대한 쿼리를 첫 번째 DNS 서버들의 집합으로 전송하도록.
- europe,microsoft.com 으로 끝나는 이름에 대한 쿼리를 두 번째 DNS 서버들의 집합으로 전송하도록.
- 기타 다른 모든 쿼리들은 세 번째 DNS 서버들의 집합으로 전송하도록.

IT 관리자들은 이 기능을 사용하여 네트워크 상에서 DNS 트래픽의 라우팅을 통제할 수 있습니다.

M. EDNS0 프로토콜 지원

RFC 2671 에 정의되어 있는 EDNS0 프로토콜은 DNS 서버들이 512옥텟 보다 더 큰 페이로드 크기로 UDP DNS 메시지를 수신 및 전송할 수 있게 해 줍니다. 이 기능은 로컬 Active Directory 도메인 컨트롤러에 대한 Service Resources Record (SRV) 쿼리와 같은 DNS 응답이 512 옥텟보다 큰 경우에 유용합니다. Windows Server 2003 제품군 이전에는 이러한 응답들이 TCP 세션을 구축하고 분리하도록 추가적인 왕복 시간이 필요했습니다. 그러나 이제 Windows Server 2003 제품군에서는 EDNS0 프로토콜을 사용함으로써 이런 많은 응답들이 TCP 세션의 구축과 분리 없이도 단일 UDP 왕복으로 완료될 수 있습니다.

O. 그 밖의 강화된 기능들

Windows Server 2003 제품군의 DNS Server 서비스는 그 밖에도 다음과 같은 여러 추가적인 강화 기능들을 제공합니다.

- 모든 RR (resource record; 리소스 레코드) 형식을 위한 순환 순서 방식(Round-robin) 지원

  디폴트로 DNS Server 서비스는 모든 RR 형식을 위한 순환 순서 방식(Round-robin) 회전을 수행할 것입니다.

- 강화된 디버그 로깅

DNS 문제들을 해결하기 위해 강화된 DNS Server 서비스 디버그 로깅 설정을 사용

- 서버와 영역 기반에서 자동 Name Server (NS) resource record registration(NS 리소스 레코드 등록)을 통제하는 능력

◆ WINS

Windows Server 2003 제품군에서는 Windows Internet Name Service (WINS)에 대해 다음과 같은 점들이 개선되었습니다.

◆ 필터링 레코드

강화된 필터링과 새로운 검색 기능은 여러분이 지정한 기준에 부합한 레코드들을 보여 주면서 이들이 어디에 위치해 있는지 찾을 수 있도록 해줍니다. 이러한 기능들은 매우 큰 규모의 WINS 데이터베이스를 분석하는데 특히 유용합니다. 여러분은 다양한 기준을 사용하여 WINS 데이터베이스 레코드들을 대상으로 고급 검색을 수행할 수 있습니다. 이러한 향상된 필터링 기능을 사용하여 여러분은 사용자 지정된 정확한 쿼리 결과를 얻을 수 있도록 필터들을 결합시킬 수 있습니다. 사용 가능한 필터들에는 레코드 소유자, 레코드 형식, NetBIOS 이름, 그리고 서브넷 마스크가 있는 혹은 없는 IP 주소들이 포함됩니다.
여러분은 이제 쿼리 결과를 로컬 컴퓨터의 메모리 캐시에 저장할 수 있기 때문에 이후의 쿼리 성능은 보다 향상되며 네트워크 트래픽은 줄어들 것입니다.

◆ 복제 파트너 수용

여러분은 기업의 복제 전략을 결정하면서 WINS 서버간의 pull replication(끌어오기 복제) 시에 들어오는 이름 레코드의 소스를 제어하는 목록을 만들 수 있습니다. 특정한 복제 파트너로부터의 이름 레코드를 차단할 뿐만 아니라 복제 시에 특정 WINS 서버가 소유한 이름 레코드를 받아들이도록 할 수도 있습니다. (단, 목록에 있지 않는 모든 서버의 이름 레코드를 제외함)

◆ IAS

Windows Server 2003 제품군에서는 IAS가 다음과 같이 강화되었습니다. IAS는 Web Edition에서 제공됩니다.

◆ 안전한 무선 및 LAN 을 위한 IEEE 802.1x 인증 지원

IAS는 IEEE 802.1X 인증을 사용하여 IEEE 802.11b 무선 액세스 포인트와 이더넷 스위치에 접속하는 사용자와 컴퓨터의 인증 및 자격 증명을 허용하도록 강화되었습니다. 이제 원격 액세스 정책 NAS-Port-Type 조건은 무선과 이더넷 연결 형식을 선택하는 능력 또한 갖추게 되었습니다.
안전한 무선 및 이더넷 연결을 위해서 여러분은 Protected EAP (PEAP) 및 MS-CHAP v2 인증

으로 보호되는 인증서(EAP-TLS)나 암호를 사용해야 합니다. EAP-TLS는 인증서를 이용하여 자격 증명을 인증하고 암호화 키 관련 자료를 제공합니다. EAP-TLS는 IAS 서버와 무선 또는 이더넷 클라이언트에 대한 인증서를 발행하는 인증서 인프라를 필요로 합니다. PEAP 및 MS-CHAP v2를 사용해 여러분은 암호 기반 인증을 안전하게 사용할 수 있습니다. 그것은 MS-CHAP v2 인증 교환이 안전한 TLS 채널에 의해 암호화 되었으며 사용자 암호에 대한 오프라인 사전 공격을 막아주기 때문입니다. PEAP 인증 교환은 또한 암호화 키 관련 자료를 생성합니다. MS-CHAP v2를 사용하는 PEAP은 단지 IAS 서버에만 설치되는 인증서를 요구합니다.

PEAP은 초기 PEAP 인증에서 생성된 TLS 세션의 재개를 허용합니다. 이러한 PEAP의 기능은 “fast reconnect(빠른 재연결)”으로 알려져 있는데 이는 TLS 세션에 기반하여 향후 계속되는 인증들이 완벽한 PEAP 인증의 대부분의 메시지가 전송되지 않을 만큼 매우 빨리 일어날 수 있도록 해 줍니다. PEAP fast reconnect는 연결과 인증 시간을 최소화하며 사용자에게 사용자 이름이나 암호 같은 인증 자격 증명을 재전송하도록 요구하지 않습니다. 예를 들어 한 무선 인증 프로토콜에서 다른 무선 인증 프로토콜로 로밍하는 무선 클라이언트들은 보다 유연한 네트워크 연결을 보유하며 인증 자격 증명을 요구 당하지 않습니다.

IAS에서 MS-CHAP v2를 사용하는 PEAP을 선택하려면 Internet Authentication Service 스냅인에서 원격 액세스 정책의 프로필 속성에 있는 **Authentication** 탭 상의 **EAP Methods**를 클릭합니다. **Select EAP Providers** 대화 상자에서 **Protected Extensible Authentication Protocol (PEAP)**를 클릭하여 그것의 속성을 편집하거나 또는 그것을 EAP 형식 목록의 가장 위로 이동시킵니다.

- **계정 제한 사항을 반영하는 세션시간**

IAS는 이제 사용자나 컴퓨터의 만료 시간 및 허용 로그온 시간에 기반하여 연결에 필요한 세션 시간을 산정할 수 있습니다. 예를 들어 사용자 계정이 월요일에서 금요일, 오전 9시에서 오후 5시 까지만 로그온 하도록 제한되어 있다고 가정해 봅시다. 만약 금요일 오후 4시에 그 사용자의 계정을 사용해 연결이 이루어진다면, IAS는 자동으로 연결을 위해 1 시간이라는 최대 세션 시간을 설정하며 이 최대 세션 시간을 RADIUS 특성으로서 액세스 서버에 전송합니다. 오후 5시, 액세스 서버는 연결을 종료합니다. 이 새로운 기능은 계정의 로그온 일자 및 시간 제한과 일치하는 일관된 네트워크 액세스 작동을 제공하게 됩니다.

- **IAS 및 교차 포리스트 인증**

Active Directory 포리스트들이 양방향 트러스트의 교차 포리스트 모드라면, IAS는 다른 포리스트에서 사용자 계정을 인증할 수 있습니다. IT 관리자들은 이 기능을 사용하여 교차 포리스트 모드에 있는 다른 양방향 트러스트 Active Directory 포리스트 내에 계정을 위한 인증 및 권한을 제공할 수 있습니다.

- **RADIUS Proxy 로서의 IAS**

이 기능을 통해 IAS 는 액세스 서버와 RADIUS 서버 사이에서 RADIUS 인증 및 계정 메시지를 전송합니다. 기능들은 다음과 같습니다:

- 유연한 규칙 기반의 전송.
- 여러 개의 RADIUS 서버들 사이의 로드 밸런싱과 장애 조치 및 RADIUS 요청들의 로드 밸런싱.
- 액세스 클라이언트로 하여금 사용자 인증을 사용해 또는 사용자 인증 없이 의무 터널을 사용하도록 하는 능력.
- 다양한 RADIUS 서버들로의 선택적인 인증 및 계정 요청 전송.

이 기능을 통해 다음이 가능해졌습니다.

- IT 관리자들은 한 도메인에 위치하는 IAS 기반 RADIUS 프록시를 생성하여 트러스트 관계를 맺지 않고 오직 단방향 트러스트 관계만을 갖고 있는 다른 도메인에서나 또는 다른 포리스트의 도메인에서도 사용자들을 인증할 수 있게 합니다.
- 기업에 대한 무선 서비스 또는 VPN, ISP offering outsourced dial-up(ISP 제품을 사용하는 dial-up)은 사용자 인증이나 계정 요구를 기업 RADIUS 서버로 전송합니다.
- 일부 경계 네트워크 구성에 있어 IT 관리자는 네트워크 경계에 IAS 프록시를 설치할 수 있습니다. 요청들이 ISP 의 IAS 프록시에서 기업 네트워크의 IAS 서버로 전송될 수 있습니다.
- 파트너 ISP 나 네트워크 인프라 제공자와 함께 작업하는 ISP 들은 로밍 컨소시엄에 있어서 IAS RADIUS 프록시를 사용할 수 있습니다.
- IT 관리자는 파트너 네트워크와 연결되는 기업 네트워크를 위해 IAS 를 사용함으로써 다른 기업의 사용자 인증을 자신들의 사용자 계정 데이터베이스로 전송할 수 있습니다.

● SQL 데이터베이스에 대한 RADIUS 정보 로깅

IAS는 계정 요청, 인증 요청 및 Structured Query Language (SQL) 서버의 주기적 상태에 대한 로깅 정보를 전송하도록 구성될 수 있습니다. 이를 통해 IT 관리자들은 SQL 쿼리를 사용하여 인증을 위해 RADIUS를 사용하는 연결 시도에 대한 과거 및 실시간 정보를 확보할 수 있습니다. 이를 구성하기 위해서, Internet Authentication Service 스냅인의 **Remote Access Logging** 폴더에서 **SQL Server** 로깅 메소드에 관한 속성을 확보하십시오.

● EAP-TLS Unauthenticated Access (EAP-TLS 인증되지 않은 액세스)

EAP-TLS unauthenticated access는 인증서를 설치하지 않은 무선 혹은 스위치 클라이언트를 위한 게스트 액세스를 가능하게 하는 방법을 제공합니다. 네트워크 액세스 클라이언트가 자격 증명을 제공하지 않는다면, IAS가 연결 시도에 맞는 원격 액세스 정책에서 인증되지 않은 액세스를 활성화할지 여부를 결정하게 됩니다. EAP-TLS는 클라이언트가 자격 증명을 전송하지 않는 인증되지 않은 액세스 또는 단방향 인증을 지원합니다.

이 기능을 사용해 다음과 같은 일들이 가능해집니다:

- IT 관리자는 이 기능을 사용해 인증서를 가지고 있지 않은 무선 또는 스위치 클라이언트가 초기 적재 구성을 위해 제한된 VLAN(virtual local area network)에 연결되도록 할 수 있습니다.
- IT 관리자는 이 기능을 사용해 기업 네트워크로의 방문객 혹은 비즈니스 파트너에게 액세스를 허용함으로써 인터넷에 액세스할 수 있도록 줍니다.
- 무선 ISP 는 이 기능을 사용해 잠재적인 가입자들에게 액세스를 허용합니다. 이 잠재적인 가입자들은 지역 정보를 이용해 제한된 VLAN 에 액세스할 수 있습니다. 사용자가 인터넷 액세스를 위해 가입을 한 후에야 클라이언트가 인터넷에 연결될 수 있습니다.

● IP 주소들을 지원하는 RADIUS 클라이언트 구성

동일한 서브넷 또는 동일한 IP 주소 공간 내에 수많은 무선 액세스 지점이 있을 경우 Remote Authentication Dial-In User Server (RADIUS) 클라이언트를 단순화시키기 위해 IAS는 RADIUS 클라이언트를 위해 일련의 주소들을 구성할 수 있도록 해줍니다.

RADIUS 클라이언트들을 위한 주소 범위는 네트워크 접두사 길이 표기법인 *w.x.y.z/p* 형태로 표기됩니다. *w.x.y.z*는 주소 접두사의 십진 표기법이며 *p*는 접두사 길이(네트워크 접두사를 정의하는 높은 명령 비트 수)입니다. 이는 또한 CIDR(Classless Inter-Domain Routing) 표기법이라고도 알려져 있습니다. 예를 들어 192.168.21.0/24와 같은 형태입니다. 서브넷 마스크 표기법에서 네트워크 접두사 길이 표기법으로 변환할 경우, *p*는 서브넷 마스크에서의 높은 명령 비트 수입니다.

IT 관리자는 이 기능을 사용하여 무선 액세스 지점 관리를 간편하게 할 수 있습니다.

● EAP 인증 방법 결정에 대한 개선사항

이 기능을 사용해 여러분은 원격 액세스 정책을 구성할 때 여러 개의 EAP 형식을 선택할 수 있습니다. 이를 통해 IAS 는 여러 개의 선택된 EAP 방식에서 클라이언트와 EAP 인증 방식을 협의할 수 있습니다. IT 관리자는 네트워크 액세스 클라이언트가 다양한 EAP 인증 방식을 사용할 때 이 기능을 사용할 수 있으며, 허용된 EAP 인증 방식 목록을 구성하도록 서버를 구성할 수 있습니다.

● 사용자 인증서 및 스마트 카드를 위한 Object Identifier Checking(개체 식별자 검사)

특정 형식의 연결을 위한 특별한 형식의 사용자 수준 인증서를 확보하기 위해, IAS는 액세스 클라이언트 인증서에 원격 액세스 정책 프로필 설정의 일부로서 포함되어야만 하는 개별 인증서 발급 정책 개체 식별자(OIDs) 요구사항을 지원합니다. 예를 들어 IT 관리자가 원격 액세스 VPN 연결이 자체적으로 설치되어 있는 사용자 인증서보다는 스마트 카드 인증서를 사용하도록 하고자 한다면, 이 관리자는 스마트 카드 로그온 인증서 발급 정책이 원격 액세스 VPN 클라이

언트가 제공하는 인증서에 나타나도록 요청하는 내용의 적절한 원격 액세스 정책을 구성해야 합니다.

원격 액세스 정책 프로필 속성의 Advanced 탭에서 Allow certificates with these OIDs 특성을 사용하여 액세스 클라이언트가 요구하는 사용자 인증서에 들어있어야 하는 개체 식별자 목록을 구성할 수 있습니다. 필요한 어떤 개체 식별자도 디폴트로 지정되지 않습니다.

- **RADIUS Proxy 로의 로드 밸런싱**

이 기능은 IAS가 RADIUS 프록시로서 사용될 때 여러 개의 RADIUS 서버들에서 인증 로드의 균형을 맞추는 능력을 제공합니다. 이는 수직 확장 기능도 제공하며 지리적 장애 조치를 수행할 수 있습니다. IAS RADIUS 프록시는 여러 개의 RADIUS 서버에서 동적으로 계정 요청 및 연결 로드의 균형을 맞추며 초당 처리할 수 있는 RADIUS 클라이언트 및 인증 수를 증가시킵니다. 추가적으로 RADIUS 프록시는 특정 RADIUS 서버들이 높은 성능을 내도록 구성할 수 있습니다. 낮은 성능의 RADIUS 서버는 그보다 높은 성능의 서버를 사용할 수 있을 때는 사용되지 않습니다.

이 기능을 이용해 다음과 같은 일을 할 수 있습니다:

- IT 관리자는 이 기능을 사용해 무선, VPN(virtual private network), 전화 접속 인증을 수직 확장하여 여러 개의 RADIUS 서버들을 사용하는 다수의 연결 요청을 처리합니다.
- IT 관리자는 이 기능을 사용해 연결 요청이 가까이에 있는 사용 가능한 RADIUS 서버들에 장애 조치를 하고 RADIUS 서버들을 원격 사이트에서 백업 RADIUS 서버들로 구성할 수 있습니다.

- **계정의 다이얼 인 속성 무시하기**

원격 액세스 정책의 프로필 속성에서 계정의 다이얼 인 속성을 무시하도록 RADIUS 특성을 구성할 수 있습니다:

- Remote access permission (원격 액세스 허용)
- Caller-ID (호출자 ID)
- Callback options (콜백 옵션)
- Static IP address (고정 IP 주소)
- Static routes (고정 라우트)

IAS가 인증과 권한을 제공하는 다양한 연결 형태를 지원하기 위해서는 계정 다이얼 인 속성 처리를 비활성화하는 것이 필요합니다. 이는 특정 다이얼 인 속성이 필요하지 않은 시나리오를 지원하기 위한 사항입니다.

예를 들어 caller-ID(호출자 ID), callback(콜백), static IP address(고정 IP 주소) 및 static routes(고정 라우트) 속성들은 NAS(network access server)에 전화 걸기하는 클라이언트를 위해

설계되었습니다. 이러한 설정들은 무선 액세스 지점(AP)들을 위해서 설계된 것이 아닙니다. IAS 서버로부터 RADIUS 메시지의 이런 설정을 전송 받은 무선 AP는 이들을 처리하지 못할 수도 있으며 이는 무선 클라이언트의 연결을 중단시킬 수 있습니다. IAS가 무선 기술을 사용해 기업 네트워크에 액세스하고 다이얼 인하는 사용자들에게 인증과 권한을 제공할 때, 다이얼 인 속성은 반드시 다이얼 인 연결(다이얼 인 속성을 설정함으로써)이나 무선 연결(다이얼 인 속성을 설정하지 않음으로써)을 지원하도록 구성되어야 합니다.

IAS를 사용하여 몇몇 상황(예를 들어 다이얼 인 같은)에서는 사용자 계정을 위한 다이얼 인 속성을 활성화하고 또 다른 상황(무선 및 스위치 인증 같은)에서는 사용자 계정 다이얼 인 속성을 위해 다이얼 인 속성 처리를 비활성화할 수 있습니다. 이는 원격 액세스 정책을 위한 프로필 설정에서 Advanced 탭의 Ignore-User-Dialin-Properties 특성을 구성함으로써 가능합니다:

- 계정 다이얼 인 속성 처리를 활성화하기 위해서는 Ignore-User-Dialin-Properties 특성을 제거하거나 이를 False 로 설정하십시오. 예를 들어 다이얼 인 연결을 위해 설계된 원격 액세스 정책에 대해서는 어떤 추가 구성도 요구되지 않습니다.

- 사용자 계정 다이얼 인 속성 처리를 비활성화하기 위해서는 Ignore-User-Dialin-Properties 특성을 True 로 설정하십시오. 예를 들어 이는 무선 또는 스위치 인증 연결을 위해 고안된 원격 액세스 정책에 대한 설정입니다. 사용자 계정의 다이얼 인 속성이 무시되면 원격 액세스 허용은 원격 액세스 정책에 대한 원격 액세스 허용 설정 내용에 따라 결정됩니다.

여러분은 또한 이 특성을 사용해 원격 액세스 정책 상의 원격 액세스 허용과 그룹을 통해 네트워크 액세스 제어를 관리할 수 있습니다. Ignore-User-Dialin-Properties 특성을 True 값으로 설정함으로써 사용자 계정의 원격 액세스 허용은 무시됩니다. 이런 방식으로 Ignore-User-Dialin-Properties 특성을 사용하면 여러분은 해당 원격 액세스 정책에 부합하는 연결을 위한 caller-ID(호출자 ID), callback(콜백), static IP address(고정 IP 주소) 및 static routes(고정 라우트)의 추가적인 다이얼 인 속성을 사용할 수 없게 됩니다.

● 컴퓨터 인증 지원

Active Directory와 IAS는 표준 사용자 인증 방식을 사용하여 컴퓨터 계정 인증을 지원합니다. 이를 통해 컴퓨터와 그 컴퓨터의 자격 증명이 무선 또는 스위치 인증 액세스 클라이언트에 대하여 인증됩니다.

● 인증 형식 원격 액세스 정책 조건을 위한 지원

Authentication Type(인증 형식) 조건을 사용하여 원격 액세스 정책을 구축할 수 있습니다. 이 새로운 조건을 통해 여러분은 액세스 클라이언트를 확인하는데 사용되는 인증 프로토콜 및 방식에 기반한 연결 제약 조건들을 설정할 수 있습니다.

● 강화된 IAS SDK

Windows Server 2003 Platform Software Development Kit (SDK)에는 IAS SDK와 EAP SDK라는

두 개의 소규모 네트워킹 SDK가 포함되어 있습니다. IAS SDK 는 사용자 네트워크 세션 수를 제어하고 사용 및 감사 데이터를 곧장 Open Database Connectivity (ODBC)에 맞는 데이터베이스로 내보내며 사용자 지정된 권한 모듈 및 인증 모듈을 생성하기 위해 IAS에 의해 리턴되는 것들 뿐 아니라 액세스 서버로 사용자 지정 특성을 리턴하는데 사용될 수 있습니다. EAP SDK는 EAP 형식을 생성하는데 사용됩니다.

개발자들은 IAS SDK의 강화된 기능들을 사용하여 RADIUS 특성을 수정하거나 삭제할 수 있고 Access-Rejects를 Access-Accepts로 전환할 수 있습니다. ISV 또는 VAR은 이 기능을 사용해 IAS를 갖춘 보다 강화된 솔루션을 구축할 수 있습니다. IT 관리자도 이 기능을 사용해 IAS를 위한 사용자 지정 솔루션을 구축할 수 있습니다.

- **IAS 를 구성하기 위한 Scriptable API**

이 기능은 IAS Platform Software Developers Kit (SDK)에서 IAS를 구성할 수 있게 하는 scriptable API를 사용할 수 있게 해줍니다. 이 기능을 사용해 ISV는 IAS 인프라에서 부가가치 서비스를 제공하며, IT 관리자들은 자신들의 IAS를 자신들만의 자체 서비스 관리 인프라에 통합시킬 수 있습니다.

- **원격 액세스 정책을 위해 강화된 EAP 구성**

Windows 2000에서는 원격 액세스 정책을 위해 단일 EAP만을 선택할 수 있습니다. 이는 정책 조건에 맞은 모든 연결이 반드시 정책 프로필 설정에서 선택된 단일 EAP 형식만을 사용해야 한다는 것을 의미합니다. 이러한 제약 조건들은 여러분이 각 정책의 EAP 형식을 위한 속성을 개별적으로 구성하기 원할 때 또는 그룹 당 혹은 네트워크 연결 형식을 위해 여러 개의 EAP 형식을 선택하고자 할 때 문제를 일으킬 수 있습니다. 이러한 제약 조건들은 Windows Server 2003 제품군에서는 IAS를 위해 제거되었습니다. 예를 들어 여러분은 VPN 연결에 비교해, 무선 연결을 위한 EAP-TLS 인증에 대해 서로 다른 컴퓨터 인증서를 선택하고자 할 수도 있고, 또는 여러분의 무선 클라이언트의 일부는 EAP-TLS 인증을 사용하고 나머지 다른 것들은 MS-CHAP v2과 함께 PEAP을 사용하기 때문에 무선 연결을 위해 여러 개의 EAP 형식을 선택하고자 할 수도 있습니다.

- **IAS Proxy 를 위한 인증과 권한의 분리**

Windows Server 2003 제품군에서 IAS의 프록시 구성요소는 액세스 서버로부터 연결 요청에 대한 인증 및 권한을 분리하는 기능을 지원합니다. IAS 프록시는 인증을 위해 사용자 자격 증명을 외부 RADIUS 서버로 전송할 수 있고, Active Directory 도메인에 위치하며 로컬로 원격 액세스 정책을 구성한 사용자 계정을 사용해 자체 인증을 수행할 수 있습니다. 이 기능을 활용해 대체 사용자 인증 데이터베이스를 사용할 수는 있으나, 연결 인증 및 제약 사항들이 로컬 관리를 통해 결정될 수 있습니다.

이 기능을 사용해 다음과 같은 일들이 가능해졌습니다:

- 기업 네트워크 방문자는 방문객 자격 증명을 사용해 자신들을 인증하고 신뢰되지 않는

방문객 Active Directory 도메인에 있는 사용자 계정과 IAS 프록시에 구성된 원격 액세스 정책을 사용해 연결을 승인함으로써 게스트 LAN에 대한 액세스 허가를 받을 수 있습니다.

- 공용 무선 네트워크는 대체 사용자 데이터베이스를 사용해 무선 액세스를 인증하고 Active Directory 도메인에 있는 로컬 사용자 계정을 통해 이들을 허용할 수 있습니다.

이 새로운 기능은 연결 요청 정책의 고급 속성에 있는 **Remote-RADIUS-to-Windows-User-Mapping** 설정을 사용해 구성됩니다.

● IPSec

Windows Server 2003 제품군에서는 IPSec에 대해 다음과 같은 개선이 이루어졌습니다.

● 새로운 IP Security Monitor 스냅인

새로운 IP Security Monitor 스냅인은 세부적인 IPSec 정책 구성과 활성화된 보안 상태를 보여줍니다. 이는 Windows 2000에서 제공되던 Ipsecmon.exe 툴을 대체합니다. IPSec 정책은 주요 모드 정책 모음, 빠른 모드 정책 모음, 주요 모드 정책과 관련이 있는 주요 모드 필터 모음, 그리고 빠른 모드 정책과 관련이 있는 빠른 모드 필터(투명 및 터널 모드) 모음으로 구성됩니다. 활성화된 보안 상태는 활성화된 주요 모드와 빠른 모드 보안 결합 및 IPSec-protected 트래픽에 대한 통계치로 구성되어 있습니다. IT 관리자는 이 새로운 스냅인을 사용해 IPSec 모니터링과 문제 해결 기능을 향상시킬 수 있습니다.

● Netsh 를 통한 명령줄 관리

netsh ipsec 컨텍스트식의 명령을 사용하여 여러분은 정적 혹은 동적 IPSec 주요 모드 설정, 빠른 모드 설정, 규칙 및 구성 매개변수를 구성할 수 있습니다. **netsh ipsec** 컨텍스트에 들어가려면 명령 프롬프트에서 **netsh -c ipsec**라고 입력합니다. **netsh ipsec** 컨텍스트는 Windows 2000 Server Resource Kits에서 제공되는 Ipsecpol.exe 툴을 대체합니다. IT 관리자는 이 기능을 사용해 IPSec 구성을 설정하고 자동화할 수 있습니다.

● IP 보안 및 네트워크 로드 밸런싱 통합

이 기능을 통해 Network Load Balancing (NLB)을 사용하는 서버들의 그룹은 높은 가용성을 지닌 IPSec 기반의 VPN 서비스를 제공합니다. 또한 하위 수준 L2TP/IPSec 클라이언트도 이를 지원합니다. 이 기능은 보다 빠른 IPSec 장애조치 역시 가능하게 해줍니다.
IT 관리자는 이 기능을 사용해 보다 안전하고 안정적인 네트워크 서비스를 위해 NLB와 IPSec 기반의 VPN 서비스를 통합할 수 있습니다. IKE 프로토콜이 자동으로 NLB 서비스를 검색하기 때문에 이 기능을 사용하기 위해서는 어떤 추가 구성도 필요하지 않습니다.
이 기능은 오로지 Enterprise Edition과 Datacenter Edition에서만 제공됩니다.

- **RSoP 을 위한 IPSec 지원**

IPSec 구축과 문제 해결 기능을 강화하기 위해서 IPSec은 이제 Resultant Set of Policy (RSoP) 스냅인을 확장하였습니다. RSoP은 그룹 정책(Group Policy)에 대한 추가 내용으로서, 여러분은 이를 사용하여 기존 IPSec 정책 지정을 살펴볼 수 있고 컴퓨터나 사용자를 위해 계획된 IPSec 정책 지정을 시뮬레이션해볼 수 있습니다. 기존 정책 지정을 살펴보기 위해 여러분은 RSoP 로깅 모드 쿼리를 실행할 수 있습니다. 계획된 IPSec 정책 지정을 시뮬레이션하기 위해 RSoP 계획 모드 쿼리를 실행할 수 있습니다.

로깅 모드 쿼리는 IPSec 정책을 위한 문제 해결 우선 순위 결정에 있어 유용합니다. 로깅 모드 쿼리의 결과는 IPSec 클라이언트에 지정된 모든 IPSec 정책과 각 정책의 순위를 보여줍니다. 계획 모드 쿼리는 이들이 다양한 IPSec 정책 설정들을 시뮬레이션하기 때문에 배포 계획에 있어 유용합니다. 서로 다른 IPSec 정책 설정을 시뮬레이션함으로써 실질적으로 구현하기 전에 미리 변경된 정책 설정 내용의 효과를 평가해볼 수도 있고 더불어 최상의 설정 내용을 예측해 볼 수도 있습니다. RSoP 로깅 모드 쿼리 또는 RSoP 계획 모드 쿼리를 실행한 후에 여러분은 앞으로 적용할 IPSec 정책에 대한 자세한 설정 내용(필터 규칙, 필터 동작, 인증 방식, 터널 종단점 및 IPSec 정책이 만들어질 때 지정되는 연결 형식 등)을 살펴볼 수 있습니다.

- **IPSec NAT Traversal**

이 기능을 사용하면 IKE 및 ESP-protected 트래픽이 NAT을 통과할 수 있습니다. IKE는 자동으로 NAT이 존재하는지 검사하며 User Datagram Protocol-Encapsulating Security Payload (UDP-ESP) 캡슐화를 사용하여 ESP-protected IPSec 트래픽이 NAT을 통과할 수 있도록 합니다. Windows Server 2003 제품군에서의 IPSec NAT traversal 지원에 관해서는 Internet Draft "UDP Encapsulation of IPSec Packets" (draft-ietf-ipsec-udp-encaps-02.txt)와 "Negotiation of NAT-Traversal in the IKE" (draft-ietf-ipsec-nat-t-ike-02.txt)에 기술되어 있습니다.

이런 지원 기능을 통해 기업의 직원들은 호텔이나 홈 네트워크 같은 개인 네트워크에 연결할 때 L2TP/IPSec을 사용할 수 있습니다. 이 기능은 또한 NAT 에서의 일반적인 IPSec ESP 전송과 모드 보안 결합을 지원합니다. 관리자는 이 기능을 사용해 Windows Server 2003 제품군을 운영하는 두 컴퓨터 사이의 게이트웨이 간 IPSec 터널을 구성할 수 있고, 이 컴퓨터 중 하나 혹은 두 대 모두가 NAT 외부에 있을 때 원격 액세스 서비스를 구성할 수도 있습니다. 그리고 NAT 에서 내부 네트워크 서버와 통신하는 경계 네트워크 상의 서버 같은 서버 간 IPSec 연결도 허용합니다.

- **Network Address Translation Hardware Acceleration**

IPSec은 이제 정상적인 ESP 트래픽을 위해 NAT hardware acceleration를 지원합니다. 이 기능을 사용해 다음과 같은 작업을 할 수 있습니다:

- IT 관리자는 이 기능을 사용해 IPSec over NAT 이 사용될 때 L2TP/IPSec 과 정상적인 IPSec 연결을 조정할 수 있습니다.
- IHV 는 이 기능을 사용해 새로운 캡슐화를 사용하도록 새로운 카드를 구축하거나 구형

펌웨어를 업데이트할 수 있습니다.

IPSec hardware acceleration 인터페이스는 TCP/IP Task Offload의 일부로서 플랫폼 DDK에 잘 설명되어 있습니다.

- **로컬 IP 구성을 위해 논리적 주소를 허용하는 IPSec 정책 필터**

IP Security Policies(IP 보안 정책) 스냅인은 이제 로컬 IPSec 정책 서비스를 사용해 소스나 대상 주소 부분을 DHCP 서버, DNS 서버, WINS 서버 및 기본 게이트웨이를 위한 주소들로 바꿀 수 있습니다. 따라서 IPSec 정책은 이제 DHCP나 고정 IP 구성을 사용해 자동으로 서버의 IP 구성에 대한 변경 사항을 적용할 수 있습니다. Windows 2000 또는 Windows XP를 운영하는 컴퓨터들은 IPSec 정책에 대한 이러한 확장된 기능을 무시합니다.

- **액세스 컨트롤을 제공하는 액티브 디렉터리 컴퓨터 계정으로의 인증서 매핑**

IP Security Policies 스냅인은 Active Directory 포리스트 안에 있는 컴퓨터 계정에 대한 컴퓨터 인증서를 매핑하도록 구성할 수 있습니다. 네트워크 관리자는 이제 IPSec을 사용하며 Windows Server 2003 제품군 중 하나를 운영하는 컴퓨터에 대한 액세스를 제한하여 특정 도메인 상의 컴퓨터나 특정 인증 기관의 인증서를 보유한 컴퓨터, 특정 컴퓨터 그룹, 심지어 단일 컴퓨터에 대해서만 액세스를 허용하도록 만들 수 있습니다. Windows 2000 또는 Windows XP를 운영하는 컴퓨터들은 IPSec 정책에 대한 이러한 확장된 기능을 무시합니다.

- **Internet Key Exchange (IKE)를 위한 더 강력해진 Diffie-Hellman 그룹**

IPSec은 이제 2048-bit Diffie-Hellman 키 교환 사용을 지원하며 이는 Internet Draft "More MODP Diffie-Hellman groups for IKE."에 대한 지원을 제공합니다. 보다 강력한 Diffie-Hellman 그룹과 함께 Diffie-Hellman 교환에서 파생된 비밀 키는 더 강력합니다. IP Security Policies 스냅인에서 로컬 및 도메인 기반 IPSec 정책 모두를 위한 이 새로운 Diffie-Hellman 그룹 설정을 구성할 수 있습니다. Windows 2000과 Windows XP를 운영하는 컴퓨터들은 이 설정을 무시합니다

- **IKE 를 위해 보다 나아진 서비스 거부 공격 보호**

Windows Server 2003 제품군의 IKE는 IKE 트래픽을 포함한 서비스 거부 공격에 보다 잘 대처하기 위해 수정되었습니다. 대부분의 일반적인 공격은 잘못된 패킷을 UDP 포트 500으로 전송하는 식이었습니다. 패킷을 확인하는 IKE 는 유입되는 패킷이 너무 많아지면 점차 패킷을 버리기 시작합니다. 그리고 전송 비율이 떨어지면 다시 IKE 패킷 확인 작업을 재개합니다. 가장 방어하기 힘든 공격은 악의적인 의도를 가진 사용자가 정상적인 IKE 게시 메시지를 IKE 응답기에 (메시지의 출처에 대한) 잘못된 IP 주소와 함께 전송한다든가 또는 정확한 IP 주소이긴 하나 너무 빨리 전송한다는가 하는 방식의 공격입니다. 이 공격은 TCP/IP 기반 서버에 대한 TCP Synchronize (SYN) 공격과 유사합니다. 새로운 방어 기능을 이용해 IKE 응답기는 Responder

Cookie 영역에 특별 값을 포함하고 있는 IKE 메시지가 들어 있는 적절한 IKE 게시 메시지에만 응답을 합니다. IKE 게시자가 적절하게 설정된 Responder Cookie 영역을 통해 다음 메시지를 전송하지 않는다면 IKE exchange는 무시됩니다. Windows Server 2003이 IKE 게시자일 때에 그것은 적절하게 작동을 시작할 것입니다. IPSec IKE 모듈은 적절하게 설정된 Responder Cookie 영역을 포함한 응답을 받을 때까지는 IKE negotiation에 대한 어떤 상태도 보존하지 않습니다. 이는 Windows 2000이나 Windows XP, 써드 파티 IPSec 구현 기능(제품)들을 운영하는 컴퓨터와 호환되며, 심지어 응답기가 제한된 공격을 받고 있는 상황에도 적법한 게시자가 성공적으로 협상할 수 있는 기회를 증가시켜 줍니다.

7) 그 밖의 새로운 기능

- **Winsock API에 대한 변경**

Windows Server 2003 제품군에서는 Windows Sockets API에 대해 다음과 같은 변경이 이루어졌습니다.

- **AF_NETBIOS를 위한 지원 제거(64-bit만을 위함)**

AF_NETBIOS는 Enterprise Edition과 Datacenter Edition의 64-bit 버전에서는 지원되지 않습니다. 어플리케이션은 이에 대한 대체 사항으로 TCP 또는 UDP를 사용해야 합니다. 기능들은 32-bit 써드 파티 어플리케이션들을 위해 유지됩니다.

- **ConnectEx/TransmitPackets 및 TCP/IP**

다음의 두 함수가 Windows Sockets 2 형식에 대한 Microsoft 만의 고유한 확장자입니다:
Windows Sockets ConnectEx() 함수는 다른 소켓 어플리케이션에 대한 연결을 구축하고 연결이 성립된 이후 선택적으로 데이터 블록을 전송합니다.

Windows Sockets TransmitPackets() 함수는 연결된 소켓(데이터그램 또는 스트림) 상의 메모리 및/또는 파일 데이터로 전송됩니다. 운영 체제의 캐시 관리자는 파일을 검사하는 데 사용되며 이를 전송하기 위해 요구되는 최소한의 시간 동안 메모리를 잠궈 둡니다. 이는 소켓 상의 파일 및 메모리 데이터 전송을 위해 높은 성능과 효율성을 제공합니다.

- **System Area Network를 위한 Windows Sockets Direct 경로**

Windows Server 2003 제품군에서는 SAN(System Area Networks)을 위한 Windows Sockets Direct (WSDP)에 다양한 성능 향상이 이루어졌습니다. WSD는 SOCK_STREAM을 위해 쓰여진 Windows Sockets 어플리케이션을 활성화하여 어플리케이션 수정 없이도 SAN의 성능 이점을 이용할 수 있게 해줍니다. 이 기술의 기본적인 구성요소는 기본 SAN 서비스 제공자를 통해 TCP/IP 의미를 에뮬레이트하는 WinSock 스위치입니다. Windows 2000 Server 제품군에서는 오직 Windows 2000 Advanced Server 및 Windows 2000 Datacenter Server에서만 WSD 지원이

이루어집니다. WSD 지원은 Windows Server 2003 제품군의 모든 제품에 포함되어 있습니다. Windows Sockets API 에 관한 더 자세한 정보는 Microsoft Platform SDK를 참고하시기 바랍니다.

- **Legacy Networking Protocol 제거**

다음과 같은 레거시 네트워킹 프로토콜이 제거되었습니다:

- Data Link Control (DLC).
- NetBIOS Extended User Interface (NetBEUI).

다음의 레거시 네트워킹 프로토콜은 운영체제 64-bit 버전에서 제거되었습니다:

- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)와 IPX-dependent services.
- Infrared Data Association (IrDA).
- Open Shortest Path First (OSPF).

- **잘 쓰이지 않는 RPC 프로토콜 제거**

다음과 같은 레거시 RPC 프로토콜들이 TCP로 대체되었습니다:

- Remote Procedure Call (RPC) over NetBEUI.
- RPC over NetBIOS over TCP/IP (NetBT).
- RPC over NetBIOS over IPX (NBIPX).
- RPC over SPX (64-bit only).
- RPC over AppleTalk (64-bit only).

UDP에 의해 대체된 레거시 프로토콜:

- RPC over IPX.
- RPC over Message Queuing (MSMQ).

- **명령줄 도구**

새로운 명령줄이나 유틸리티가 제공되어 컴퓨터의 유지 관리를 향상시켰습니다. 새로이 업데이트 된 명령줄 도움말 파일(A-Z)은 :

- Bootcfg.exe -로컬 혹은 원격 서버(64-bit 버전에서 지원되지 않음) 상의 boot.ini 파일 속성(debug on/off 같은)을 살펴보거나 설정하기 위해 사용됩니다.
- DriverQuery.exe - 최근 로드된 장치 드라이버와 이들의 메모리 사용을 살펴보기 위해

사용됩니다.

- Dsadd.exe – Active Directory 에 지정된 형식의 개체 인스턴스를 생성하기 위해 사용됩니다.
- Dsmod.exe – Active Directory 내에 있는 기존 개체의 선택된 특성을 수정하기 위해 사용됩니다.
- Dsrm.exe – Active Directory 의 개체 하에서 완전한 하위 트리나 개체를 제거하기 위해 사용됩니다.
- Dsmove.exe – 개체를 현재 위치에서 동일한 명명 컨텍스트 내에 있는 새로운 부모 위치로 옮기거나 Active Directory 에서 개체 이름을 다시 정하기 위해 사용됩니다.
- Dsquery.exe – Active Directory 에서 지정해 둔 검색 기준에 부합하는 개체를 찾을 때 사용됩니다.
- Dsget.exe – 살펴볼 수 있는 개체의 위치가 특별히 명시되어 있을 때 Active Directory 내에 있는 기존 개체의 선택된 속성을 확보하거나 살펴보기 위해 사용됩니다.
- Eventtriggers.exe – 이벤트 로그에 기록된 이벤트 발생에 기반한 프로세스를 시작하기 위해 사용됩니다.
- Eventquery.vbs – 이벤트 로그로부터 추출해낼 수 있는 이벤트 형식을 지정하기 위해 사용됩니다. 선택된 이벤트는 화면 상에서 보여줄 수도 있고 파일에 저장할 수도 있습니다.
- Eventcreate.exe – 모든 이벤트 로그에 사용자 정의된 이벤트를 기록할 때 사용됩니다.
- GPresult.exe – 컴퓨터에 적용할 정책 목록과 Resulting Set of Policies (RSoP)을 살펴보기 위해 사용할 수 있습니다.
- IIS scripts – 여러 새로운 스크립들(IISWeb.vbs, IISVdir.vbs 등등)이 IIS 와 Active Server Pages (ASP) 어플리케이션을 운영하는 서버를 구성, 준비, 관리하기 위해 명령줄을 제공합니다.
- Netsh.exe – 확장 네트워크 구성 툴은 이전 NetDiag.exe 툴에 의해 제공되던 기본 네트워크 진단 기능을 추가합니다.
- Openfiles.exe – 컴퓨터의 공유마다 사용되는 연결된 사용자와 파일들의 목록을 보여주기 위해 사용됩니다.
- Pagefileconfig.vbs – 현 pagefile 크기를 알아보거나 새로운 pagefile 크기를 설정하기 위해 사용됩니다.
- Print scripts – 프린터 서비스, 드라이버 및 대기열을 관리하기 위해 사용되는 많은 새로운 스크립트들(prncnfg.vbs, prnjobs.vbs 등등)
- Reg.exe – 레지스트리 키를 살펴보고 설정 및 편집하기 위해 사용됩니다.

- SC.exe – Win32 서비스를 시작/중지하고 관리하기 위해 사용됩니다.
- Schtasks.exe – 기존의 Win32 스케줄링 서비스를 사용하여 예정된 작업들을 알아보거나 새로 설정하고 편집하기 위해 사용됩니다.
- Systeminfo.exe – 기기의 기본 속성(CPU 나 메모리 같은 속성)을 살펴보기 위해 사용됩니다.
- Taskkill.exe – 실행 중인 프로세스를 중단하거나 종료하기 위해 사용됩니다.
- Tasklist.exe – PID 와 함께 실행되는 모든 프로세스를 살펴보거나 확인하기 위해 사용됩니다.
- Tsecimp.exe – Telephony Application Programming Interface (TAPI) 사용자 계정 속성 및 액세스 권한을 가져오기 위해 사용됩니다.

IT 관리자는 Visual Basic® scripting 또는 명령줄 배치 파일들을 통해 고용량 내지는 일반 서버 관리 작업을 자동화할 수 있도록 명령줄 도구를 사용할 수 있습니다. 이는 GUI 관리 도구에 의한 on-off 작동을 배제하고 IT 관리 비용을 절감할 수 있습니다.

- **Services for Macintosh 를 위한 강력한 인증**

Services for Macintosh (SFM)을 실행하고 Microsoft user authentication module (MSUAM: Microsoft 사용자 인증 모듈)을 사용하는 컴퓨터에 대해서는 새로운 **Require strong authentication (NTLMv2)** 체크박스가 나타나며 MSUAM 인터페이스에서 기본값으로 활성화됩니다. 이 옵션을 선택하면 사용자는 오로지NTLMv2를 구현하는 서버에 대해서만 인증을 합니다. 즉 이는 NTLMv2를 사용하여 인증할 수 없는 이전 서버들과 Windows NT® 4.0은 제외합니다. **Require strong authentication (NTLMv2)** 체크박스를 선택 해제하면 이런 구형 서버들도 인증할 수 있습니다.

3. 주요 Network 기능 구성하기

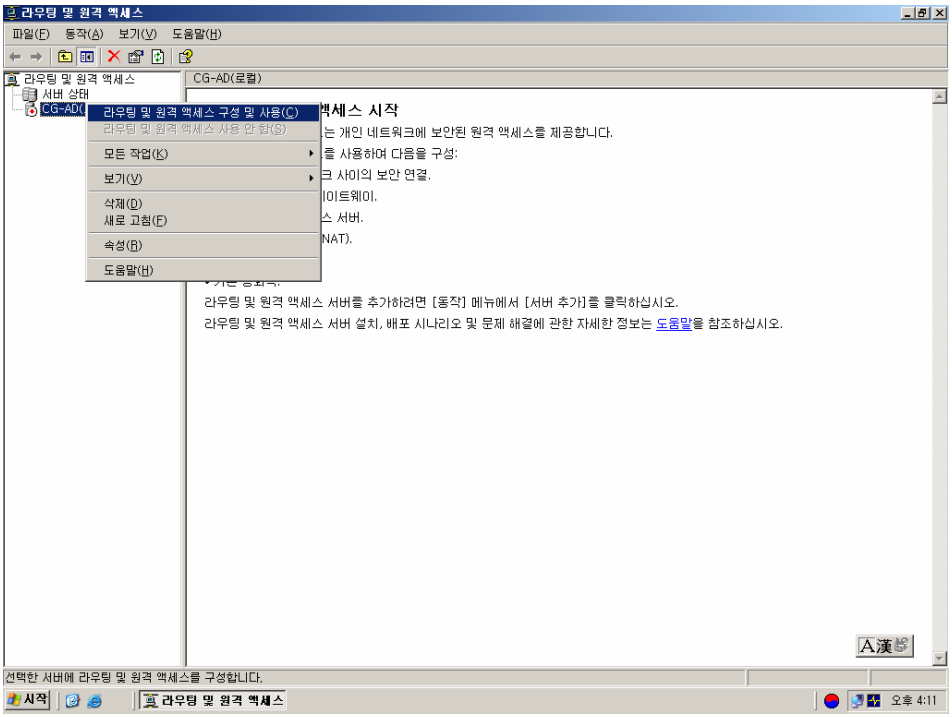
1) VPN Service – 서버

1.VPN 서버 설치 및 활성화

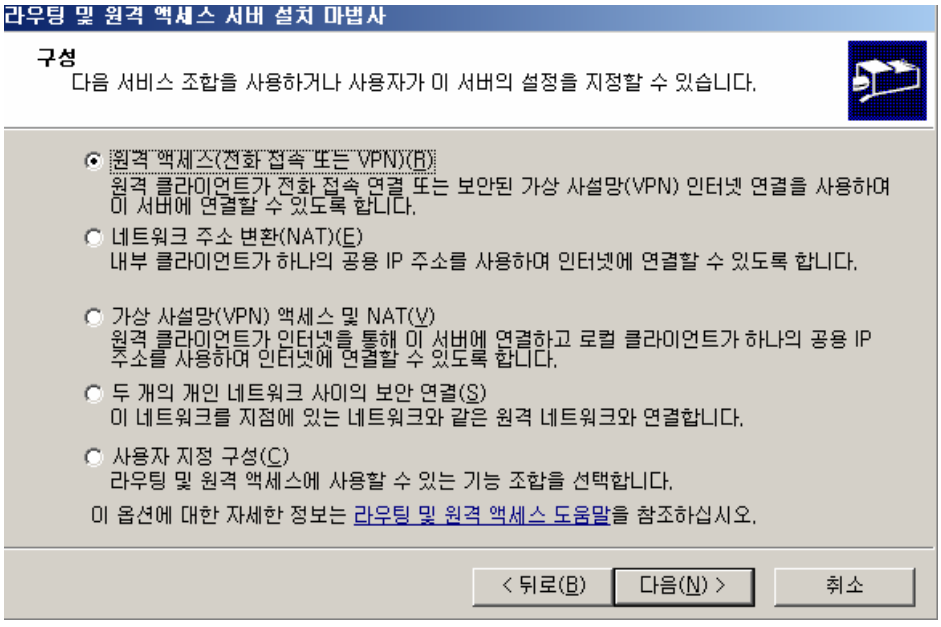
1-1 Start 를 누르고 Administrative Tools 를 가리킨 다음 라우팅 및 원격 액세스를 선택합니다.

1-2 콘솔의 왼쪽 창에서 로컬 서버 이름과 일치하는 서버 아이콘을 누른다. 아이콘의 왼쪽 아래 모서리에 빨간색 원이 있으면 라우팅 및 원격 액세스 서비스가 활성화되지 않은 것이고 아이콘의 왼쪽 아래 모서리에 녹색 위쪽 화살표가 있으면 라우팅 및 원격 액세스 서비스가 활성화된 것입니다. 라우팅 및 원격 액세스 서비스를 이전에 활성화한 경우에는 서버를 다시 구성해야할 수도 있습니다. 서버를 다시 구성하려면 다음과 같이 합니다

a. 서버 개체를 마우스 오른쪽 버튼으로 누른다음 Disable Routing and Remote Access 를 누릅니다. 정보 메시지를 제공하는 프로프트가 나타나면 Yes 를 눌러 계속합니다.

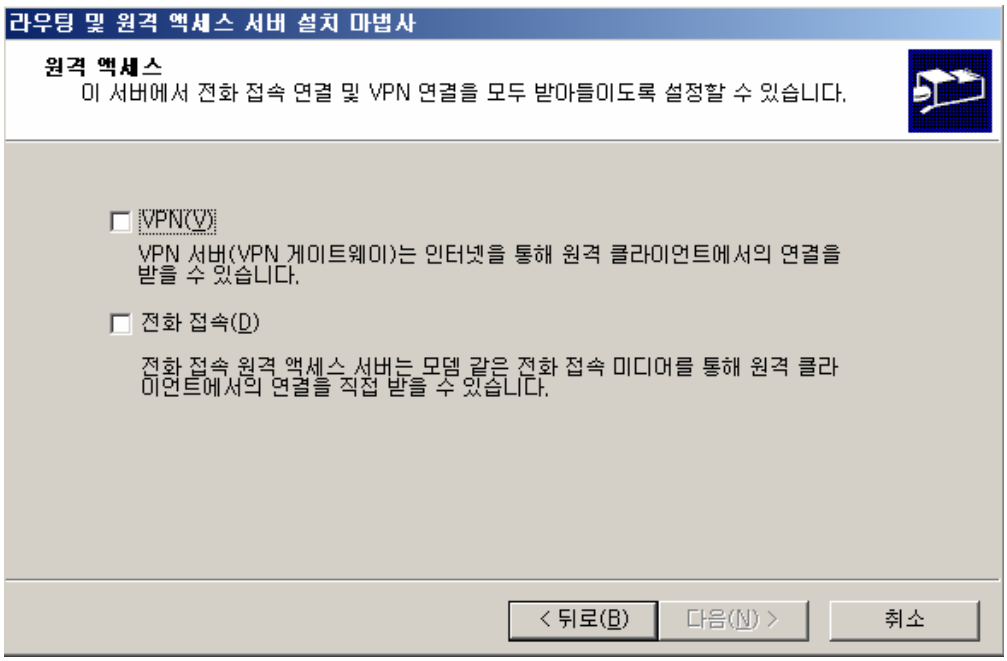


b. 서버 아이콘을 마우스 오른쪽 단추로 누른다음 라우팅 및 원격 액세스 구성 및 사용을 눌러 라우팅 및 원격 액세스 서버 설치 마법사 를 시작합니다. 다음을 눌러서 계속합니다.

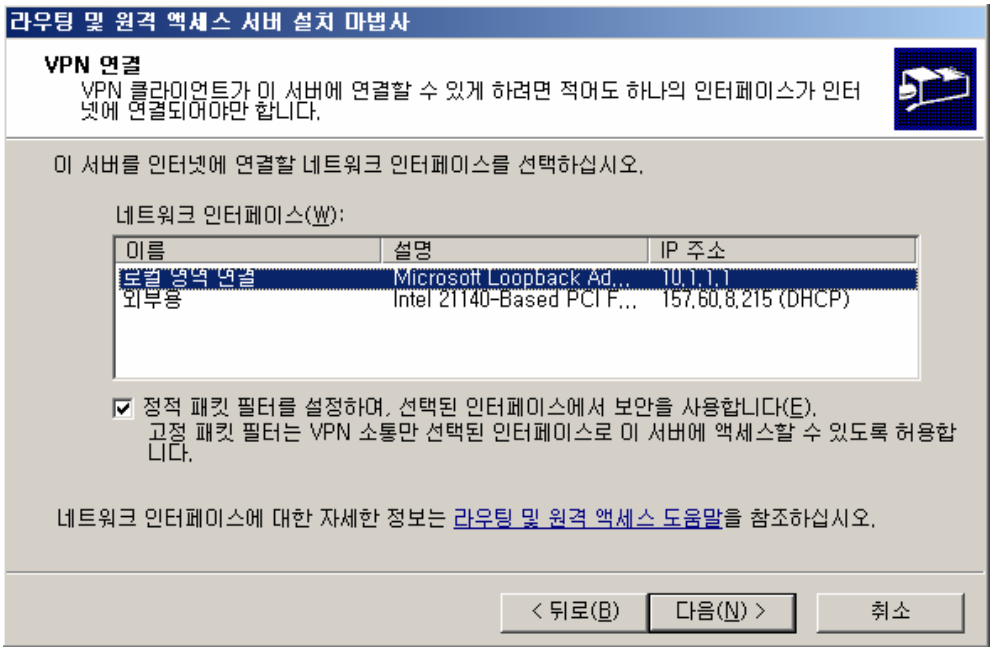


c.원격 액세스(전화접속 또는 VPN)을 눌러 인터넷을 통해 이 네트워크에 전화 접속하거나 연결할 원격 컴퓨터를 활성화합니다. 다음를 눌러 계속합니다.

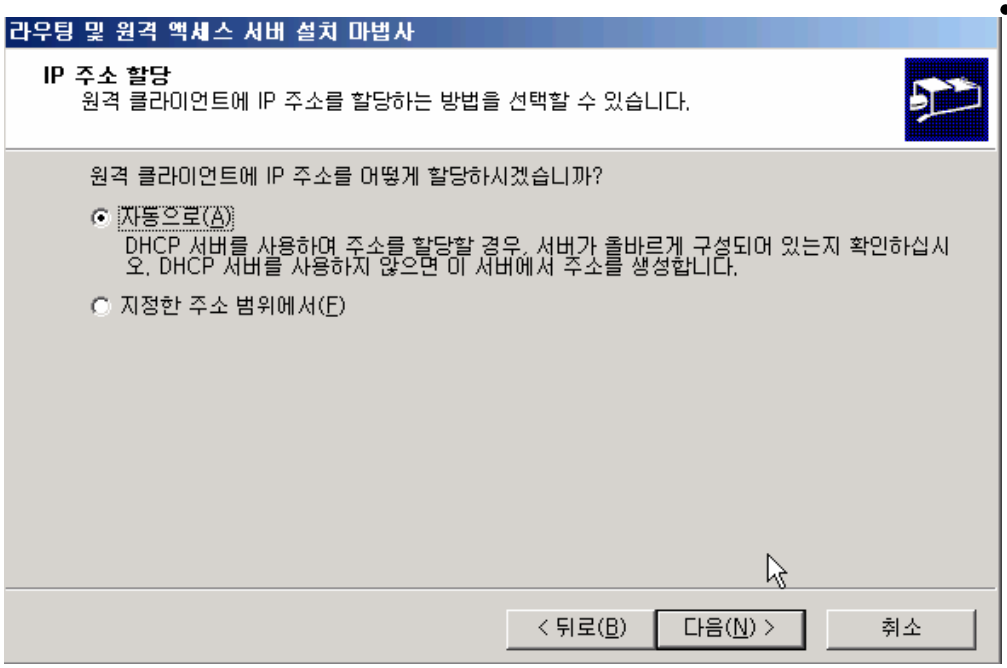
1-3 이 서버에 할당할 역할에 따라 VPN 또는 전화접속 을 선택합니다.



1-4 VPN 연결 창에서 인터넷에 연결된 네트워크 인터페이스를 누른 다음 다음을 누릅니다.



1-5 IP 주소 할당 창에서 DHCP 서버를 사용하여 원격 클라이언트에 주소를 할당할 경우에는 Automatically 를 선택하고, 원격 클라이언트에 미리 정의한 풀의 주소만 부여할 경우에는 지정한 주소 범위에서 누릅니다. 대부분의 경우 DHCP 옵션이 더 관리하기 쉽습니다. 단, DHCP 를 사용할 수 없으면 정적 주소 범위를 지정해야 합니다. 다음을 눌러 계속합니다.



1-6 지정한 주소 범위에서 누른 경우에는 주소 범위 할당 대화 상자가 열립니다. New 를 누릅니다. 정적 IP 주소 상자에 사용할 주소 범위의 첫 번째 IP 주소를 입력합니다. End IP Address 상자에 사용할 주소 범위의 마지막 IP 주소를 입력합니다. 그러면 주소 수가 자동으로 계산됩니다. 확인을 눌러 주소 범위 할당 창으로 돌아갑니다. 다음 버튼을 눌러 계속합니다.

1-7 기본값인 No, User Routing and Remote Access to authenticate connection requests 를 그대로 선택한 다음 다음을 눌러 계속합니다. Finish 를 눌러 라우팅 및 원격 액세스 서비스를 활성화하고 해당 서버를 원격 액세스 서버로 구성합니다.

2. VPN 서버를 구성하는 방법

필요한 경우, VPN 서버 구성을 하려면 다음과 같이 하십시오

- 원격 액세스 서버를 라우터로 구성하는 방법

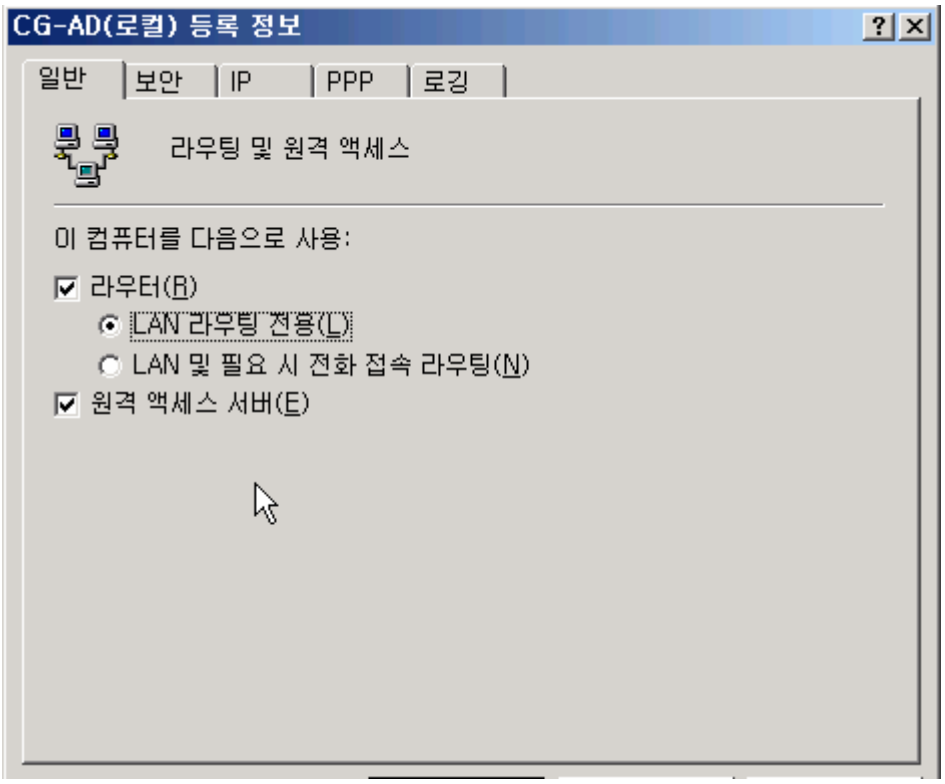
원격 액세스 서버가 네트워크 소통량을 원활하게 전달하려면 정적 라우트 또는 라우팅 프로토콜을 통해 해당 서버를 라우터로 구성하여 원격 액세스 서버에서 인트라넷의 모든 위치에 연결할 수 있도록 해야 합니다.

다음은 서버를 라우터로 구성하는 방법입니다.

1) 시작을 누르고 관리 도구를 가리킨 다음 라우팅 및 원격 액세스를 누릅니다.

2) 서버 이름을 마우스 오른쪽 단추로 누른 다음 속성을 누릅니다.

3) 일반 탭을 누른 다음 이 컴퓨터를 다음으로 사용 아래에서 LAN 라우팅 전용을 선택합니다.



4) LAN 라우팅 전용이나 LAN 및 필요시 전화접속 라우팅 을 누른 다음 확인을 눌러 속성 대화상자를 닫습니다.

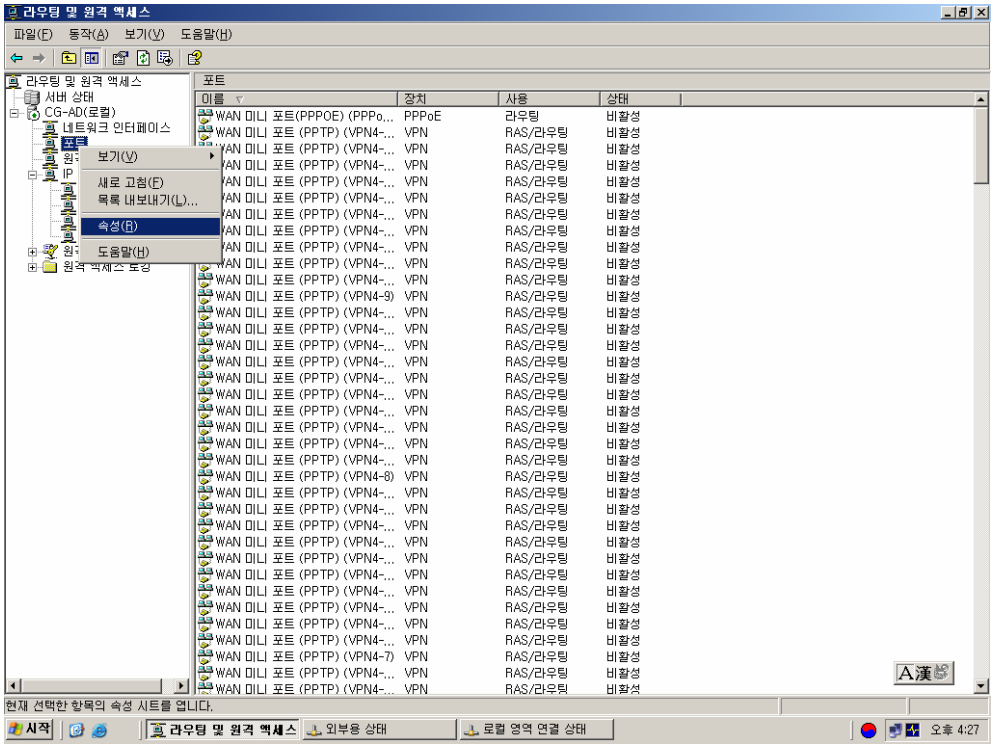
- 동시 연결 수를 수정하는 방법

전화접속 모뎀 연결 수는 서버에 설치된 모뎀수에 따라 다릅니다. 예를 들어, 서버에 설치된 모뎀이 한 개뿐이면 모뎀 연결이 한번에 하나씩만 가능합니다.

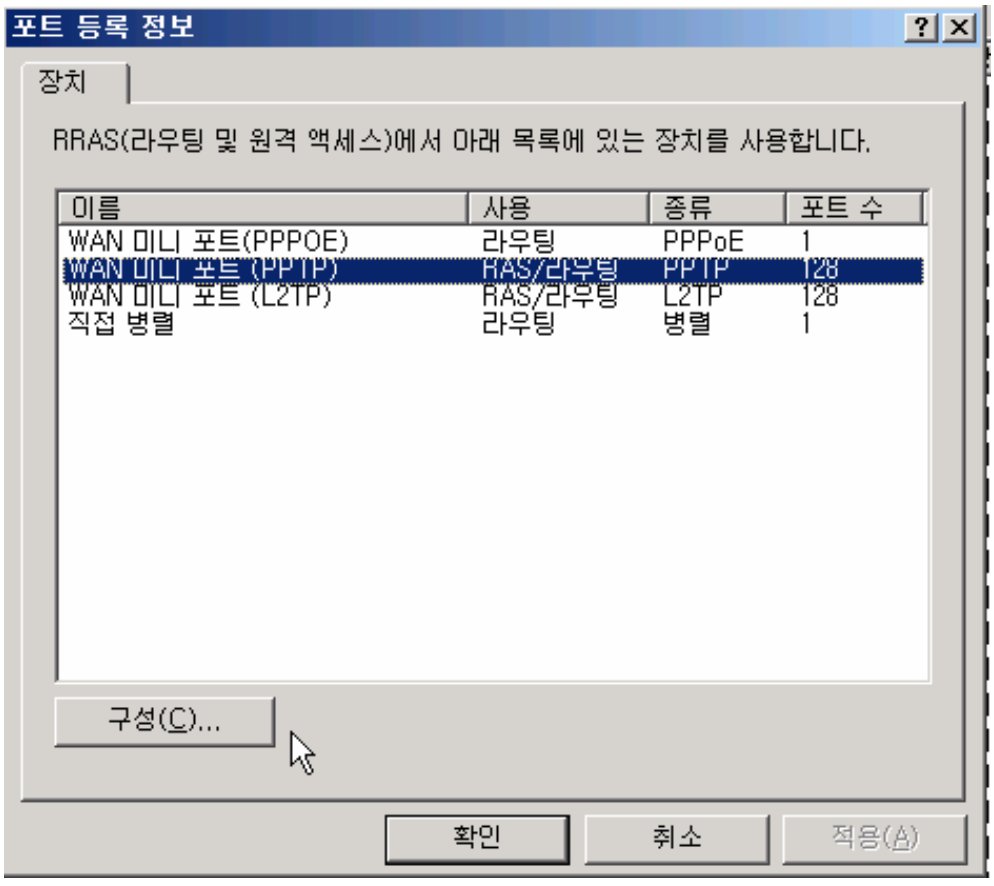
전화접속 VPN 연결수는 허용된 동시 사용자 수에 따라 다릅니다. 기본적으로 이 문서에서 설명하는 절차에 따르면 128 개의 연결이 허용됩니다. 동시 연결 수를 변경하려면 다음과 같이 하십시오

1) 시작을 누르고 관리도구를 가리킨 다음 라우팅 및 원격 액세스를 누릅니다.

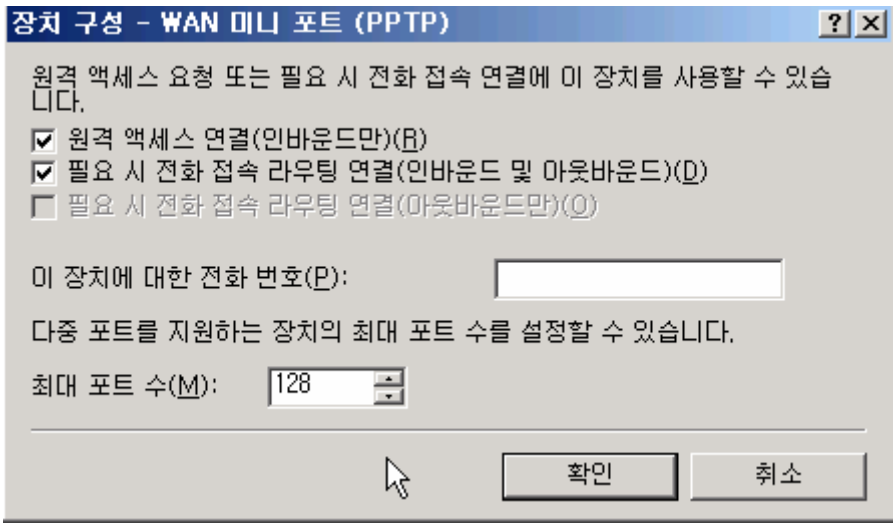
2) 서버 개체를 두 번 누르고 포트를 마우스 오른쪽 단추로 누른 다음 속성을 누릅니다.



3) 포트 속성 대화상자에서 WAN Monitor(PPTP)를 누른 다음 구성 버튼을 누릅니다.



4) 최대 포트수 상자에 허용할 VPN 연결 수를 입력합니다.



5) 확인을 누르고 확인을 다시 누른 다음 라우팅 및 원격 액세스를 닫습니다.

3. 주소 및 이름 서버를 관리하는 방법

VPN 서버에는 연결 프로세스의 IPCP(IP Control Protocol) 협상 단계가 진행되는 동안 VPN 서버의 가상 인터페이스와 VPN 클라이언트에 IP 주소를 할당할 수 있도록 사용 가능한 IP 주소가 있어야 합니다. VPN 클라이언트에 할당된 IP 주소는 VPN 클라이언트의 가상 인터페이스에 할당됩니다.

Windows Server 2003 기반 VPN 서버의 경우, VPN 클라이언트에 할당되는 IP 주소는 기본적으로 DHCP 를 통해 얻어집니다. 정적 IP 주소 풀을 구성할 수도 있고 또한 IPCP 협상이 진행되는 동안 VPN 클라이언트에 할당할 수 있도록 이름 확인 서버 (대개 DNS 및 WINS 서버 주소)를 사용하여 VPN 서버를 구성해야 합니다.

4. 액세스를 관리하는 방법

전화 접속 네트워킹 액세스와 VPN 연결 액세스를 관리하려면 사용자 계정과 원격 액세스 정책에 대한 전화 접속 속성을 구성하십시오. 기본적으로 사용자의 전화 네트워킹 액세스는 거부됩니다.

- 사용자 계정 별 액세스

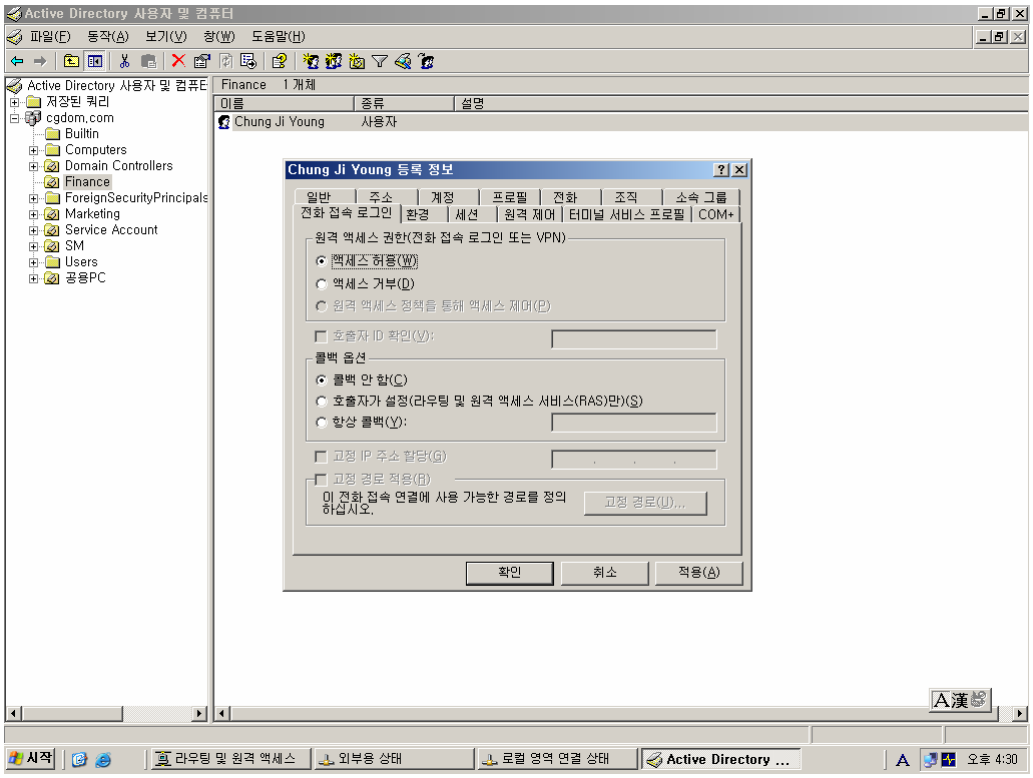
원격 액세스를 사용자 별로 관리할 경우 사용자 계정에 전화 접속 액세스 권한을 부여하려면 다음과 같이 하십시오

1) 시작을 누르고 관리도구를 가리킨 다음 Active Directory Users and Computers 를 누릅니다.

2) 사용자 계정을 마우스 오른쪽 단추로 누른 다음 속성을 누릅니다.

3) 전화접속 로그인 탭을 누릅니다.

4) 액세스 허용을 눌러 전화 접속할 수 있는 사용자 권한을 부여한 다음 확인을 누릅니다.



● 그룹 구성원 별 액세스

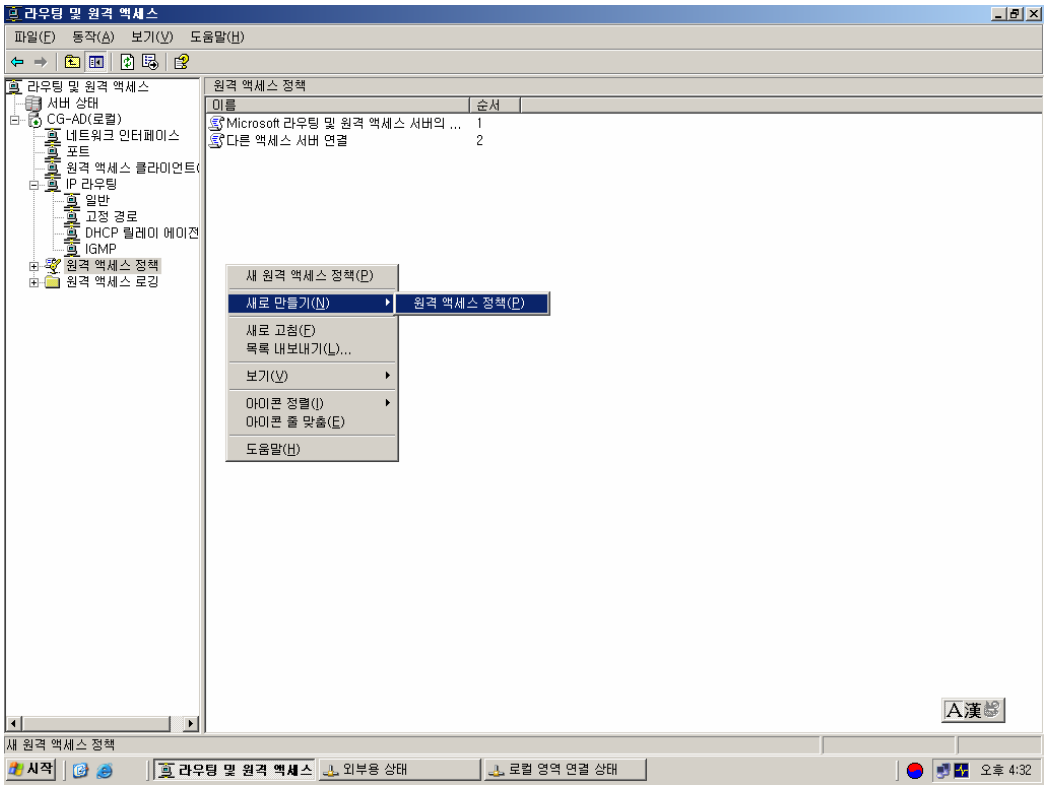
원격 액세스를 그룹별로 관리하는 경우에는 다음과 같이 하십시오

1) VPN 연결을 만들 수 있는 구성원 그룹을 만듭니다.

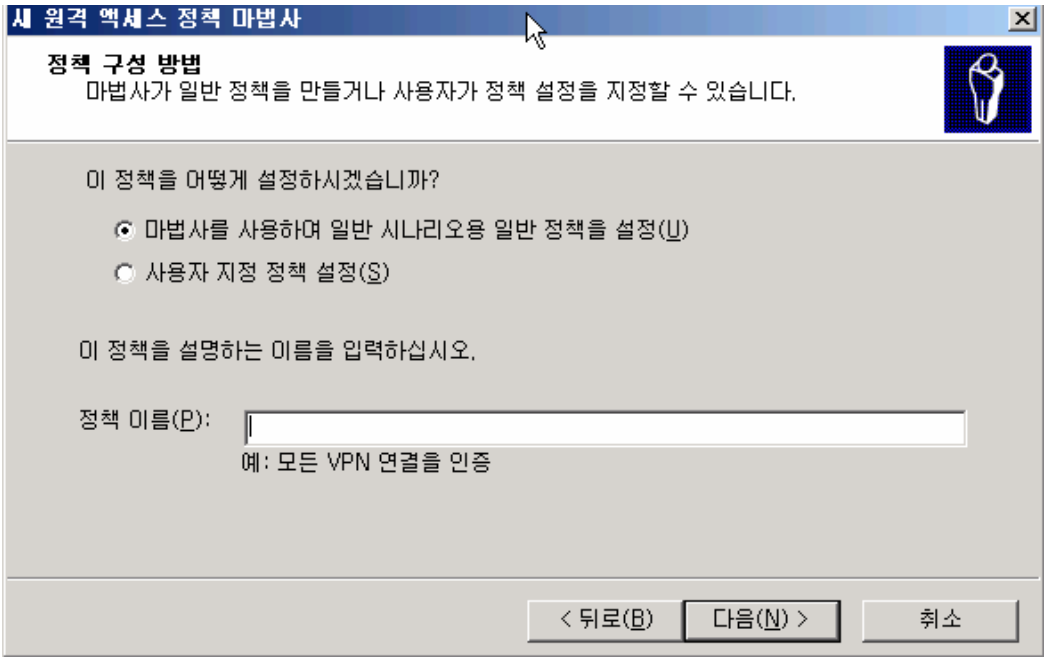
2) 시작을 누르고 관리도구를 가리킨 다음 라우팅 및 원격 액세스를 누릅니다.

3) 콘솔 트리에서 라우팅 및 원격 액세스를 확장하고 서버 이름을 확장한 다음 원격 액세스 정책을 누릅니다.

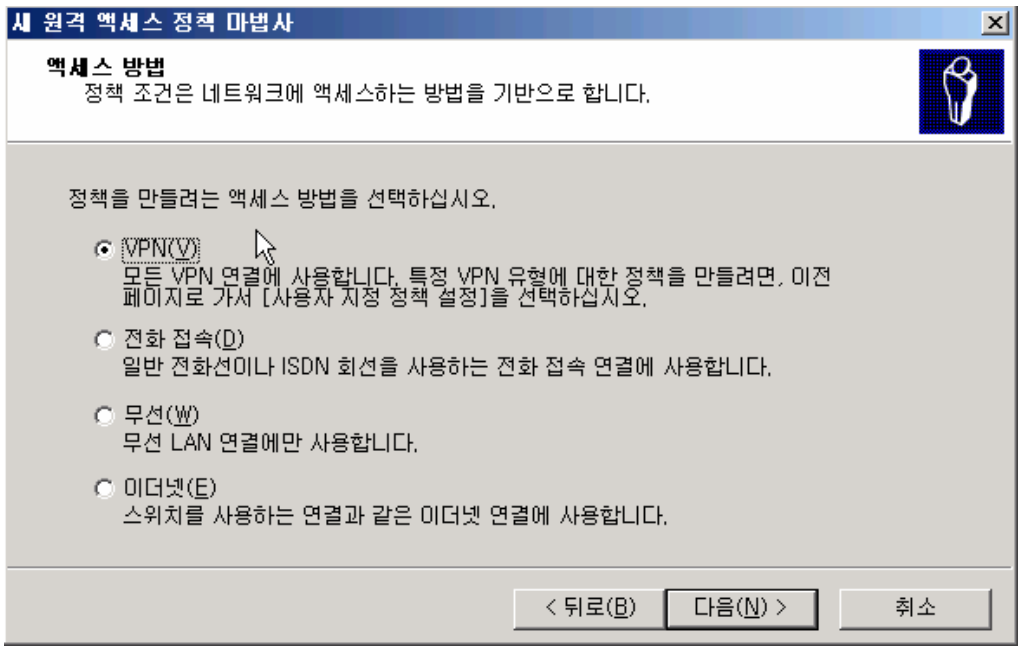
4) 오른쪽 창안의 어느 곳이나 마우스 오른쪽 단추로 누르고 새로 만들기를 가리킨 다음 원격 액세스 정책을 누릅니다.



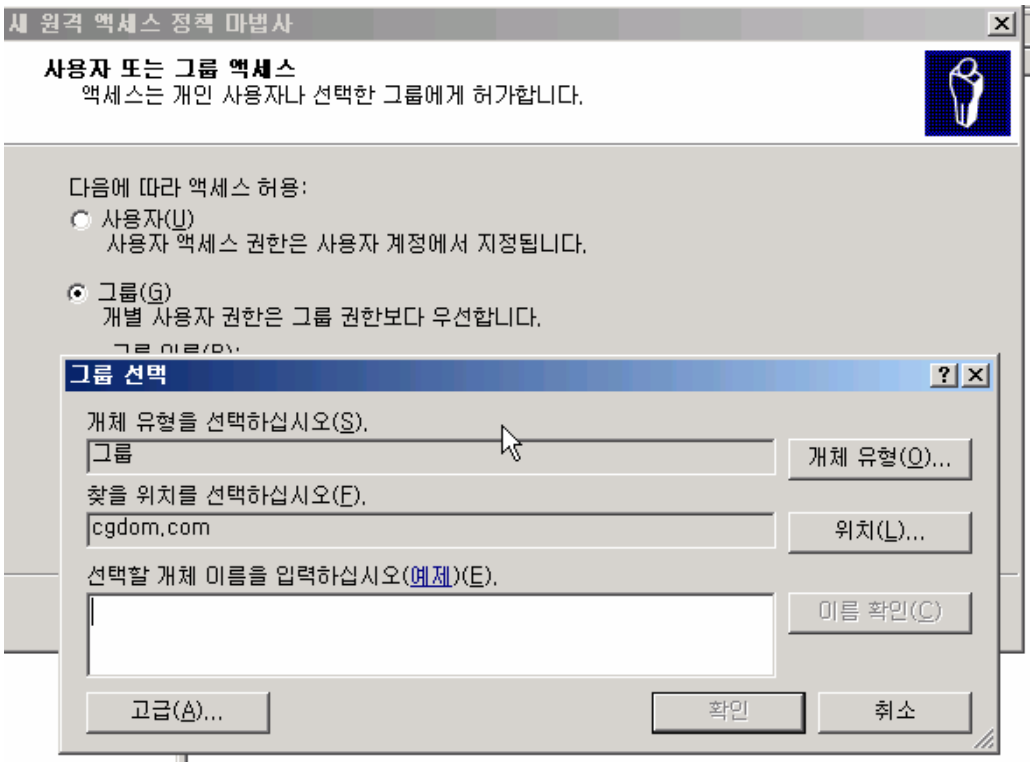
5) 다음을 누르고 정책 이름을 입력한 다음, 다음을 누릅니다.



6) VPN(가상 사설망 액세스를 허용할 경우) 또는 전화 접속(전화 접속 액세스를 허용할 경우)을 누른 다음 다음을 누릅니다.



7) 추가를 누르고 1 단계에서 만든 그룹의 이름을 입력한 다음 다음을 누릅니다.



8) 화면의 지침에 따라 마법사를 완료합니다.

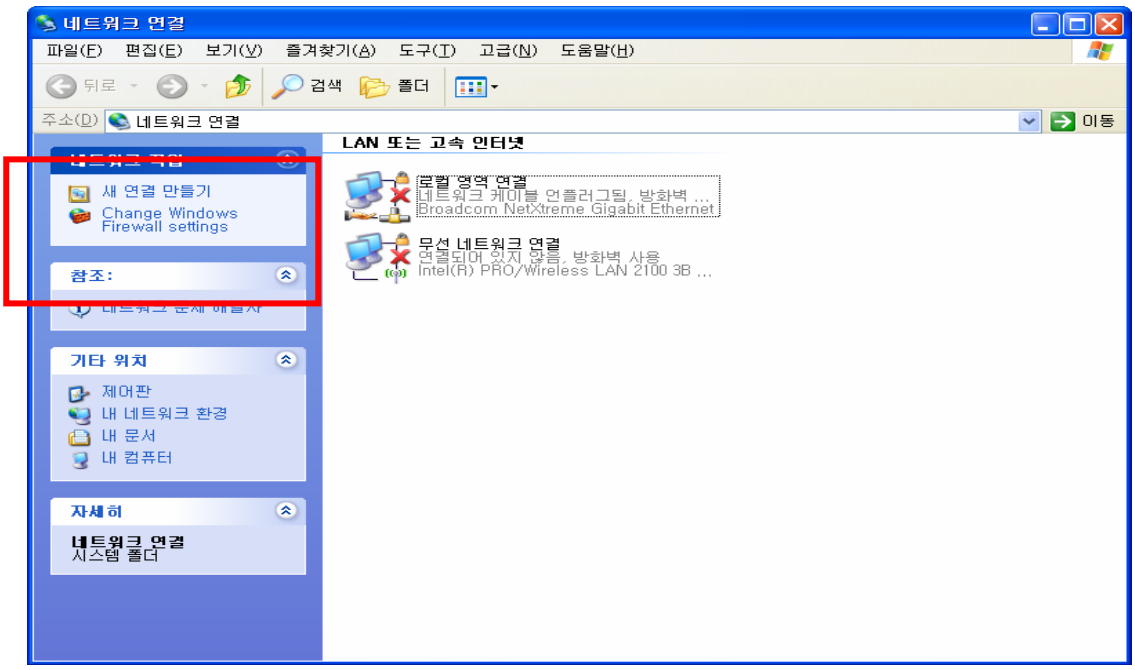
VPN 서버에서 전화 접속 네트워킹 원격 액세스 서비스를 이미 허용한 경우에는 기본 정책을 삭제하지 말고 마지막 정책으로 평가되도록 이동하십시오.

5.VPN 클라이언트 설치 및 활성화

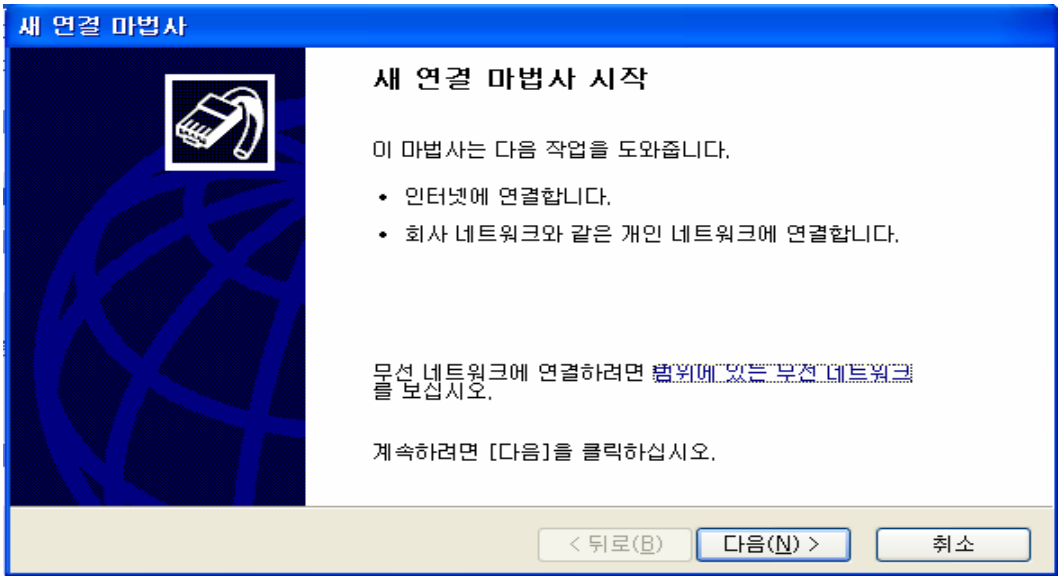
VPN 연결을 설정하려면 다음과 같이 하십시오. 가상 사설망에 액세스할 수 있도록 클라이언트를 설정하려면 클라이언트 워크스테이션에서 다음과 같이 하십시오 (아래의 작업을 하기 위해서는 데스크톱의 관리자 그룹의 구성원이어야 하며, 설치된 데스크톱 운영체제에 따라서 절차가 약간 다를 수도 있습니다.)

1) 클라이언트 컴퓨터에서 인터넷 연결이 제대로 구성되어 있는지 확인합니다.

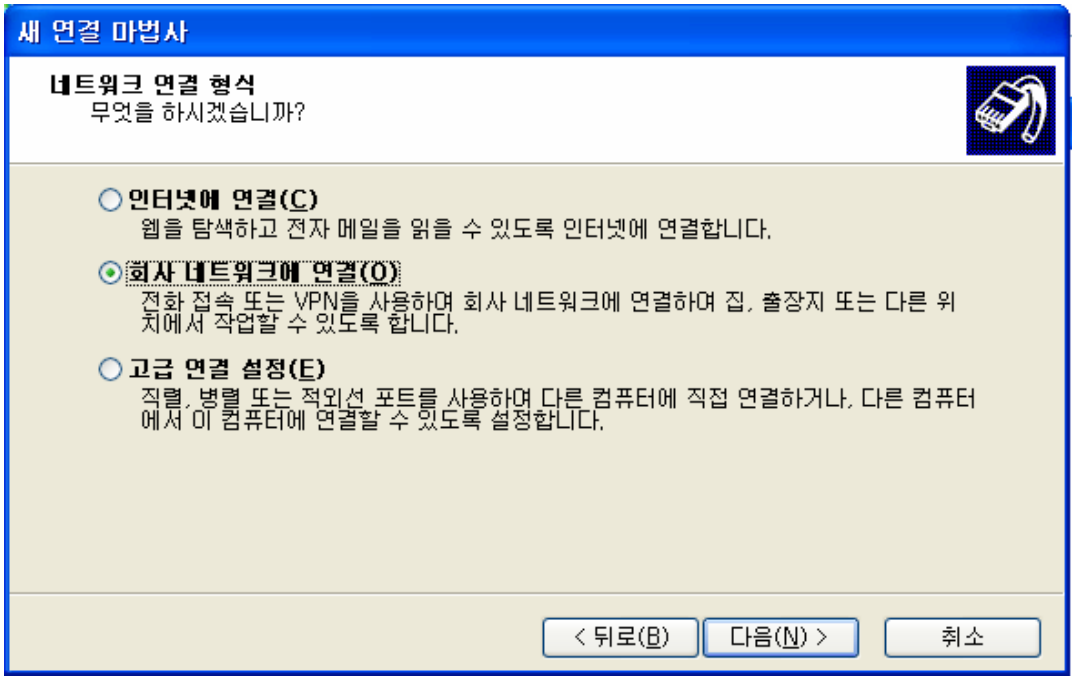
2) 시작을 누르고 제어판을 누른 다음 네트워크 연결을 누릅니다. 네트워크 작업 아래에서 새 연결 생성을 누른 다음 다음을 누릅니다.



3) 새 연결 마법사가 시작되면 다음을 누릅니다.

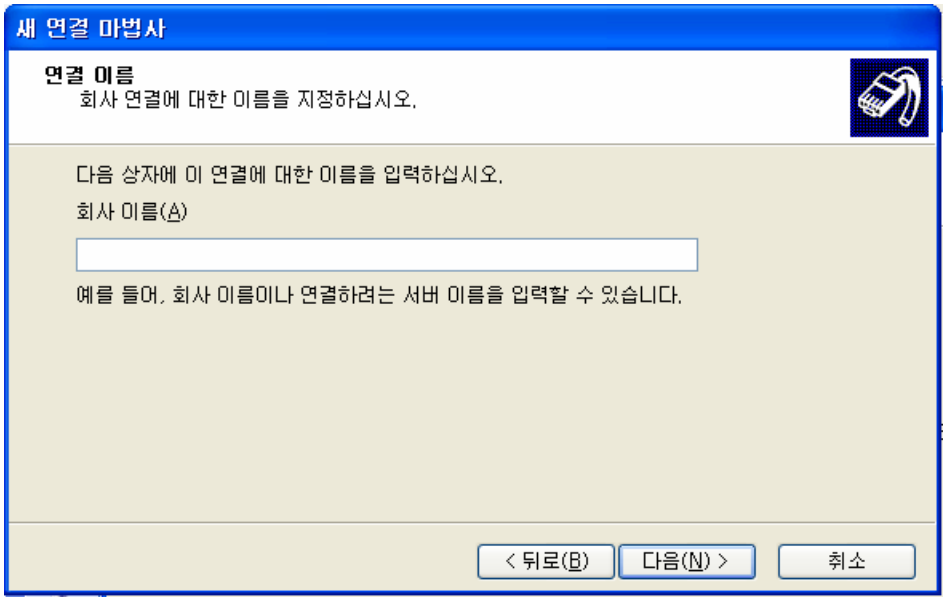


4) 네트워크 연결형식에서 회사네트워크에 연결을 선택하고 다음을 누릅니다.

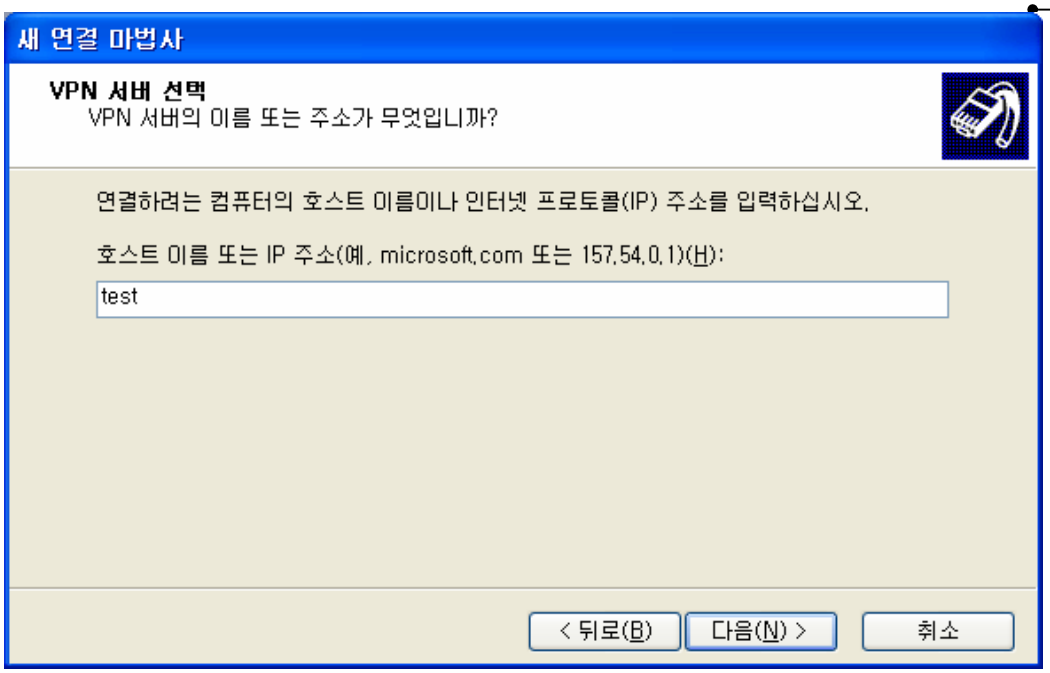


5) 네트워크 연결 항목에서 VPN 을 선택하고 다음을 누릅니다.

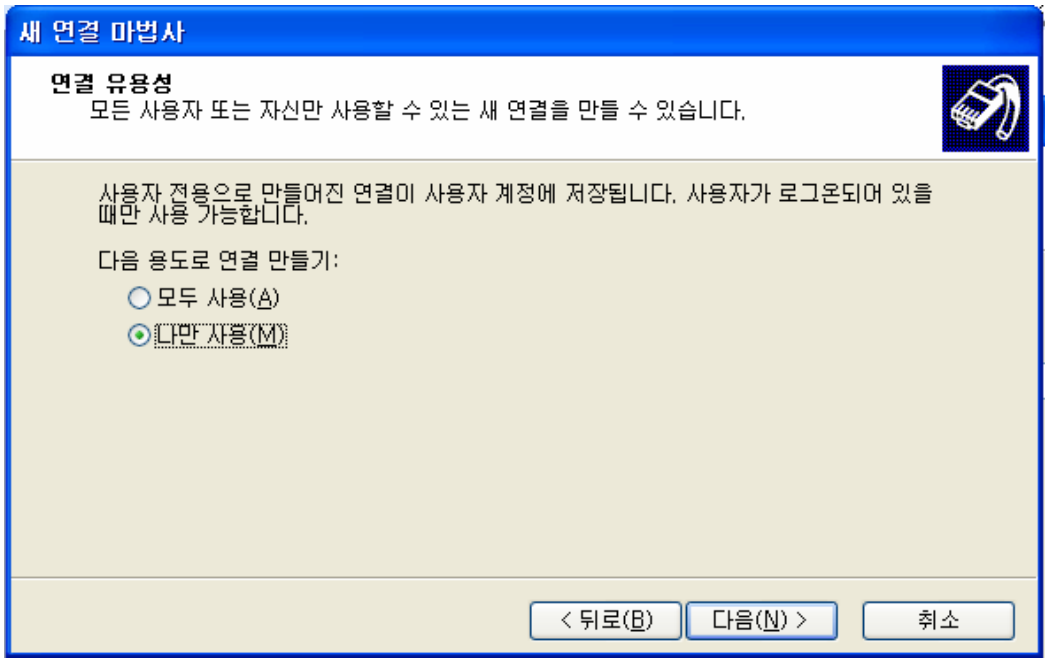
6) 연결 이름 창에서 이 연결의 설명이 포함된 이름을 입력한 다음 다음을 누릅니다.



7) VPN 서버 컴퓨터의 서버이름(호스트 이름) 또는 IP 주소를 입력합니다.



8) 연결 유용성에서 모든 사용자가 이 연결을 사용할 것인지 또는 로그인한 사용자만이 사용할 수 있도록 할 것인지 결정한 다음, 해당하는 항목을 선택하고 다음을 누릅니다.



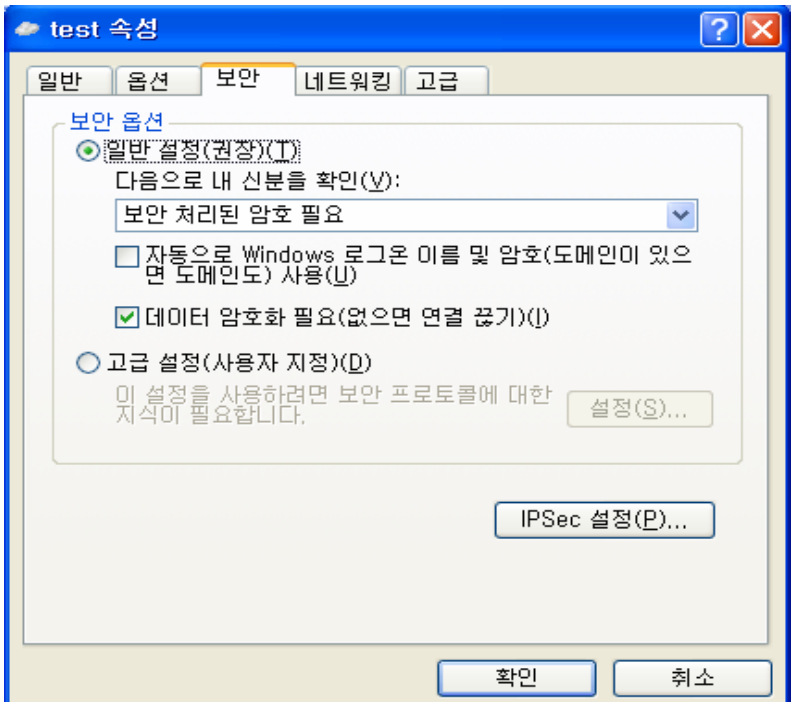
9) 마침을 눌러 연결을 저장합니다.

10) 시작을 누르고 제어판에서 다시 네트워크 연결을 누릅니다.

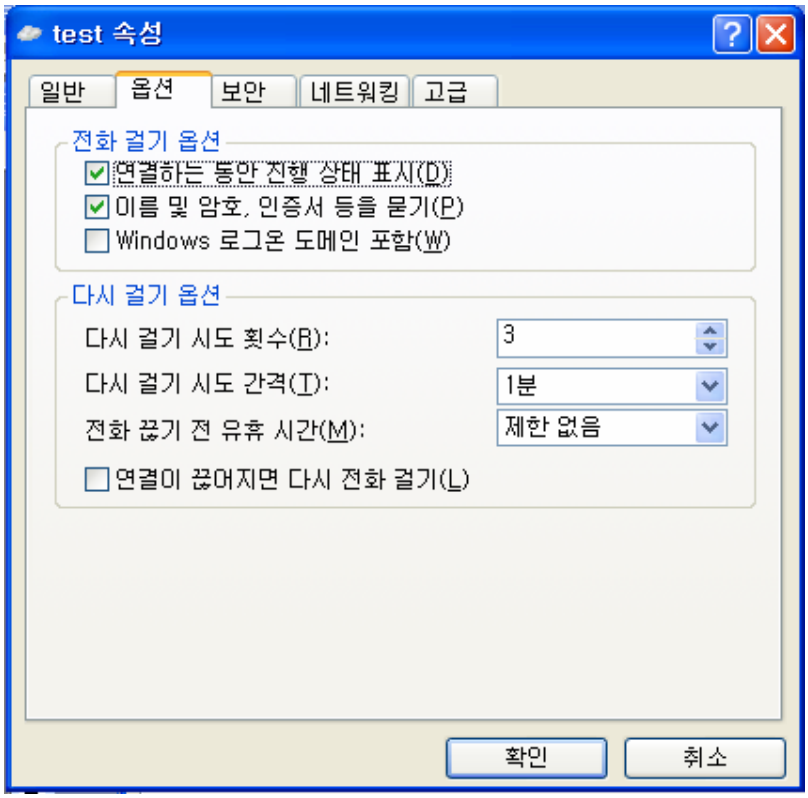
11) 방금 전에 만든 새 연결을 두 번 누르고 속성 버튼을 선택합니다.

12) 속성 화면에서 다음과 같이 연결 옵션을 구성합니다.

A. 보안 탭에서 인증 종류를 선택합니다. (로그온 아이디를 이용할 것인지 또는 스마트카드를 이용할 것인지 해당하는 종류를 선택합니다.) 고급 설정 버튼을 누르면 지정된 암호화 방식을 선택할 수도 있습니다.



B. 옵션 탭에서 전화 걸기 옵션이나 다시 걸기 옵션에 대한 항목을 설정할 수 있습니다.

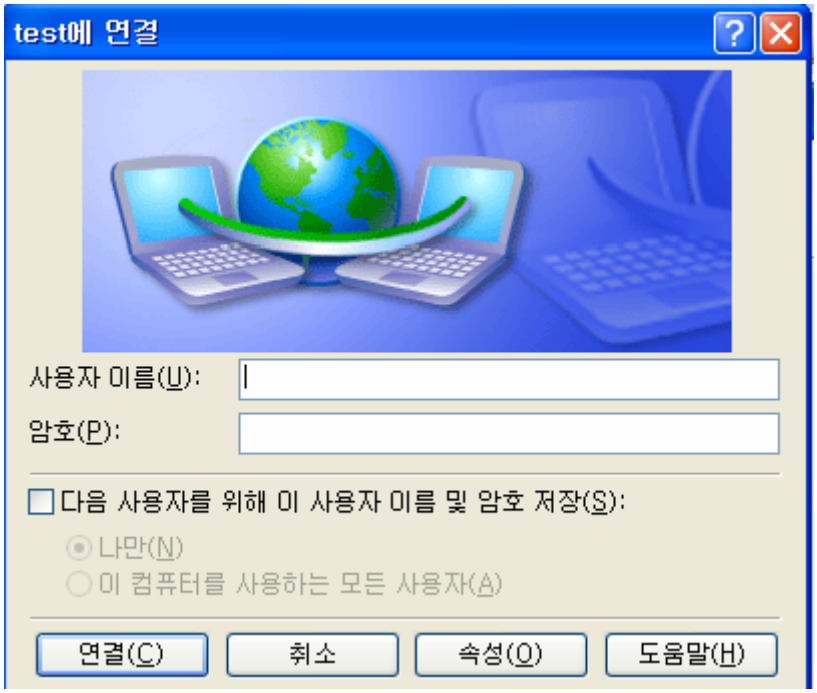


연결을 사용하려면 다음과 같이 합니다.

1) 시작을 누르고 연결 대상에서 만들어진 VPN 이름을 선택합니다.

2) 현재 인터넷에 연결되어 있지 않으면 자동으로 인터넷에 연결됩니다.

3) 인터넷에 연결되면 사용자 이름과 암호를 묻는 메시지가 나타납니다. 이름과 암호를 입력한 다음 연결을 누릅니다. VPN 연결을 끊으려면 해당 연결 아이콘을 마우스 오른쪽 단추로 누른 다음 연결 끊기를 누릅니다.



2) 인증서 서비스 설치하기

1. Windows Server 2003 에 루트 CA(Certificate Authority) 설치하기

1-1 공개 키 구조

이제 컴퓨터 네트워크는 사용자가 단순히 네트워크에 있다는 사실만으로도 신원이 보증될 수 있었던 예전의 폐쇄적인 시스템이 아닙니다. 오늘날과 같이 정보가 복잡하게 연결되어 있는 시대에는 조직들의 네트워크가 인트라넷, 인터넷 사이트, 엑스트라넷 등으로 다양하게 구성됩니다. 그리고 이들은 모두 악의적으로 조직의 디지털 정보 자산을 보거나 변경하려는 무단 침입자의 액세스로부터 자유롭지 못합니다.

침입자가 네트워크의 정보에 무단으로 액세스할 가능성은 얼마든지 있습니다. 전자 메일, 전자 상거래, 파일 전송과 같은 정보의 흐름을 모니터링 하거나 변경하려는 시도가 있을 수

있습니다. 조직들은 정해진 범위와 기간 내에서 프로젝트 파트너와 협력해야 할 수도 있고 신상에 대해 전혀 모르는 직원과 일하면서 이들에게 조직의 정보 리소스에 대한 액세스 권한을 제공해야 할 수도 있습니다. 각기 다른 보안 시스템에 액세스하기 위해 여러 개의 암호를 기억해야 하는 경우 사용자들은 좀 더 기억하기 쉬운 평범한 암호를 선택하려 합니다. 이처럼 평범한 암호를 선택하면 침입자가 손쉽게 암호를 해독하고 많은 보안 시스템 및 저장 데이터에 침투할 수 있습니다.

따라서 시스템 관리자가 정보에 액세스하는 사람의 신원을 확인하고 그에 따라 그 사람이 액세스할 수 있는 정보를 제어할 수 있는 방법이 있어야 합니다. 또한 조직 전체에 걸쳐 ID 자격 증명을 안전하고 쉽게 배포 및 관리할 수 있는 방법이 있어야 합니다. 이러한 모든 문제는 공개 키 구조를 체계적으로 계획하여 해결할 수 있습니다.

PKI(공개 키 구조)는 디지털 인증서, CA(인증 기관) 및 공개 키 암호화를 사용하여 전자 거래에 관련된 당사자들의 유효성을 확인하고 인증하는 기타 등록 기관으로 구성된 시스템입니다. 전자 상거래의 필수 요소로 널리 구현되고 있음에도 불구하고 PKI 에 대한 표준은 아직까지 계속 발전하는 상태입니다.

조직이 Windows 를 사용하여 PKI 를 배포하는 데는 아래와 같은 여러 가지 이유가 있습니다.

- **강력한 보안** 스마트 카드를 사용하여 강력한 인증 프로세스를 구현할 수 있습니다. 또한 인터넷 프로토콜 보안을 사용함으로써 공용 네트워크를 통해 전송되는 데이터의 기밀과 무결성을 유지하고 EFS(암호화 파일 시스템)를 사용함으로써 저장된 데이터의 기밀을 유지할 수 있습니다.
- **관리의 간소화** 조직에서는 인증서를 발급하고 다른 기술과 결합시켜 암호의 사용을 제거할 수 있습니다. 그리고 필요하면 인증서를 해지하고 CRL(인증서 해지 목록)을 게시할 수 있습니다. 인증서를 사용하여 신뢰 관계를 엔터프라이즈 전반에 걸쳐 확대할 수 있습니다. 또한 Active Directory 디렉터리 서비스와 정책을 인증서 서비스와 통합할 때의 장점을 활용할 수 있습니다. 인증서를 사용자 계정에 매핑하는 기능 역시 유용합니다.
- **새로운 기회** 인터넷과 같은 공용 네트워크를 통해 파일과 데이터를 안전하게 교환할 수 있습니다. S/MIME(Secure Multipurpose Internet Mail Extensions)을 사용하여 보안 전자 메일을 구현하고 SSL(Secure Sockets Layer) 또는 TLS(Transport Layer Security)를 사용하여 보안 웹 연결을 구현할 수 있습니다. 또한 무선 네트워킹에 대한 보안 향상을 구현할 수 있습니다.

공개 키 구조를 구현하는 데 유용한 Windows Server 2003 제품군의 기능은 아래와 같습니다.

- **인증서** 인증서는 기본적으로 인증서 보유자의 신원을 보증하는 기관에서 발급하는 디지털 문서입니다. 인증서는 해당 개인 키를 보유한 개인, 컴퓨터 또는 서비스의 ID 와 공개 키를 연결합니다. 인터넷과 같은 네트워크 전체에 걸쳐 인증, 데이터 무결성,

보안 통신을 제공하는 다양한 공개 키 보안 서비스 및 응용 프로그램에서 인증서를 사용합니다.

Windows 인증서 기반 프로세스에 사용되는 표준 인증서 형식은 X.509 v3 입니다. X.509 인증서에는 인증서를 발급 받는 개인 또는 엔터티에 대한 정보, 인증서에 대한 정보, 인증서를 발급하는 인증 기관에 대한 선택적 정보가 포함됩니다. 주체 정보에는 엔터티의 이름, 공개 키 및 공개 키 알고리즘이 포함될 수 있습니다.

사용자는 인증서 MMC 콘솔을 사용하여 인증서를 관리할 수 있습니다. 사용자는 인증서 자동 등록을 통해 자신의 인증서를 자동으로 관리할 수도 있습니다.

- **인증서 서비스** Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition 및 Windows Server 2003, Datacenter Edition 에서 인증서 서비스는 CA(인증 기관)를 만들고 관리하는 데 사용되는 구성 요소입니다. CA 는 인증서 보유자의 ID 를 설정하고 보증합니다. 또한 인증서가 더 이상 유효하지 않은 경우 인증서를 해지하고 인증서 확인자를 위해 CRL(인증서 해지 목록)을 게시합니다. 가장 단순한 PKI 에는 루트 CA 하나만 있습니다. 그러나 실제로 PKI 를 배포하는 조직은 대부분 많은 CA 를 사용하며 이를 인증서 계층 구조로 구성합니다.

  관리자는 인증 기관 MMC 콘솔을 사용하여 인증서 서비스를 관리할 수 있습니다.

- **인증서 템플릿** 인증서는 인증서 요청에 제공된 정보 및 인증서 템플릿에 포함된 설정을 기반으로 하여 CA 에서 발급합니다. 인증서 템플릿은 수신하는 인증서 요청에 적용되는 규칙 및 설정 집합입니다. 엔터프라이즈 CA 가 발급할 수 있는 각 유형의 인증서에 대해 인증서 템플릿을 구성해야 합니다.

  인증서 템플릿은 Windows Server 2003, Enterprise Edition 및 Windows Server 2003, Datacenter Edition 엔터프라이즈 CA 에서 사용자 지정할 수 있으며 포리스트의 모든 CA 가 사용할 수 있도록 Active Directory 에 저장됩니다. 이를 통해 관리자는 인증서 서비스에 설치된 기본 템플릿 중 하나 이상을 선택하거나 특정 작업이나 역할에 맞게 사용자 지정된 템플릿을 만들 수도 있습니다.

  관리자는 인증서 템플릿 MMC 콘솔을 사용하여 인증서 템플릿을 관리할 수 있습니다.

- **인증서 자동 등록** 자동 등록을 통해 관리자는 주체를 상호 작용 없이도 인증서에 자동 등록하고 발급된 인증서를 검색하며 만료되는 인증서를 갱신할 수 있도록 구성할 수 있습니다. 이 작업을 할 때 인증서 템플릿이 주체와 상호 작용하도록 구성되었거나 CSP 에 상호 작용(스마트 카드 CSP 처럼)하도록 구성된 경우 이외에는 인증서 작업에 대한 별다른 지식이 없어도 됩니다. 따라서 클라이언트의 인증서 사용법이 단순화되고 관리 작업도 최소화됩니다.

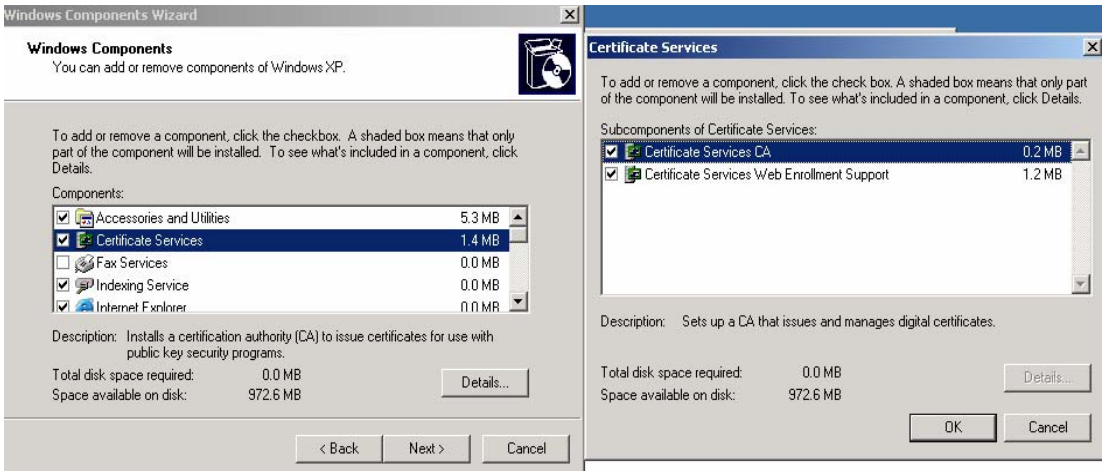
관리자는 인증서 템플릿 및 CA 설정의 구성을 통해 자동 등록을 구성할 수 있습니다.

- **웹 등록 페이지** 인증서 서비스에는 별도의 구성 요소가 있습니다. 이러한 웹 페이지는 CA 를 설치하고 웹 브라우저를 사용하여 인증서 요청을 제출할 수 있는 권한을 인증서 요청자에게 허용할 때 기본값으로 설치됩니다. 또한 CA 웹 페이지는 인증 기관이 설치되지 않은 Windows 를 실행하는 서버에 설치할 수 있습니다. 이런 경우 어떠한 이유로든 요청자들의 직접적인 액세스를 허용해서는 안 되는 CA 에 인증서 요청을 보내기 위해 웹 페이지가 사용됩니다. 조직이 CA 에 액세스할 수 있도록 사용자 지정 웹 페이지를 만들려는 경우 운영 체제에서 제공되는 웹 페이지를 예제로 사용할 수 있습니다. 인증서 서비스 및 CA 웹 페이지 사용자 지정에 대한 자세한 내용은 Microsoft 플랫폼 소프트웨어 개발 키트를 참조하십시오.
  - **스마트 카드 지원** Windows 에서는 스마트 카드를 사용하여 인증서 및 개인 키를 저장하는 것 이외에도 스마트 카드의 인증서를 통한 로그온도 지원합니다. 스마트 카드는 웹 인증, 전자 메일 보안, 무선 네트워킹 및 기타 공개 키 암호화 관련 작업에 사용됩니다.
  - **공개 키 정책** Windows 의 그룹 정책을 사용하여 주체에게 인증서를 자동으로 배포하고 일반적인 신뢰할 수 있는 인증 기관을 설정하고 EFS(암호화 파일 시스템)에 대한 복구 정책을 관리할 수 있습니다..

1-2 CA 서비스 설치하고 환경설정하기

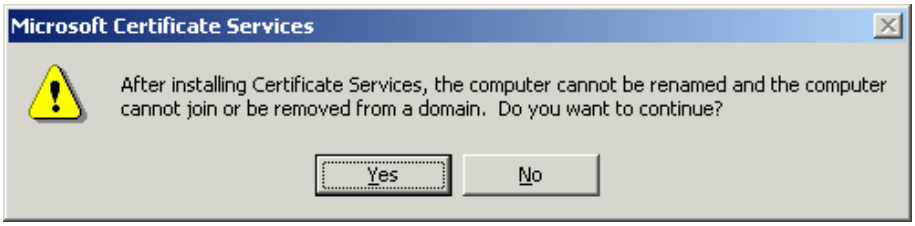
1) CA 서비스를 설치하기 위하여 설치 CD 를 넣거나 설치 CD 가 있는 공유포인트에 연결합니다.

2) 시작의 제어판을 누르고 프로그램 추가/삭제를 더블 클릭한 뒤 윈도우 구성요서 추가 삭제 버튼을 선택하고 Certificate Service(인증서 서비스)를 선택합니다.



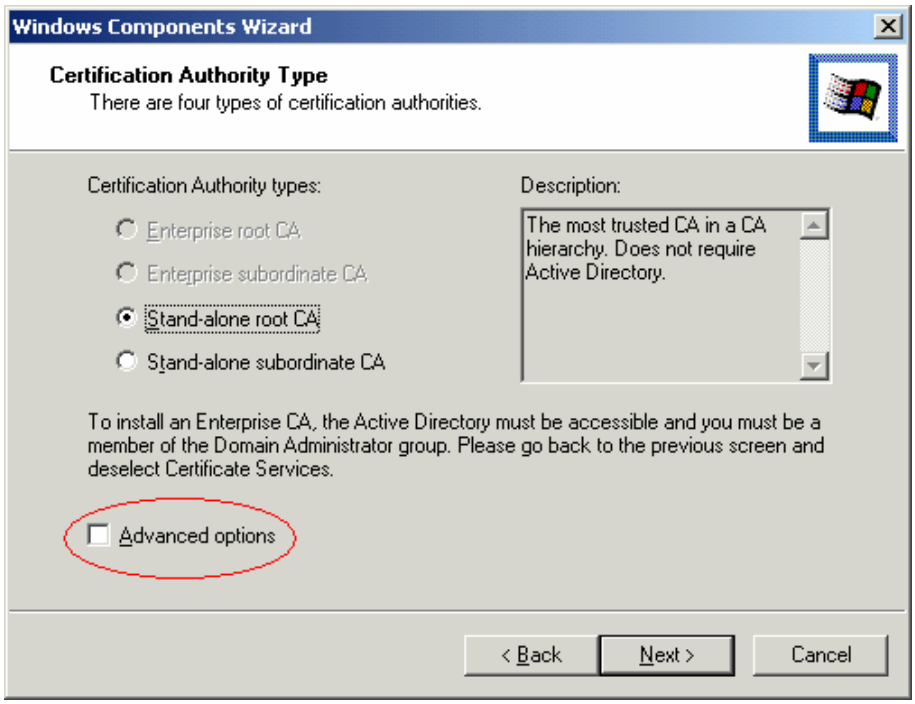
3) 계속한다는 메시지를 따라서 예를 선택한다.

독립형 루트 CA 옵션을 선택하고 고급옵션 체크박스를 활성화하여 인증 기관 종류 선택 합니다.

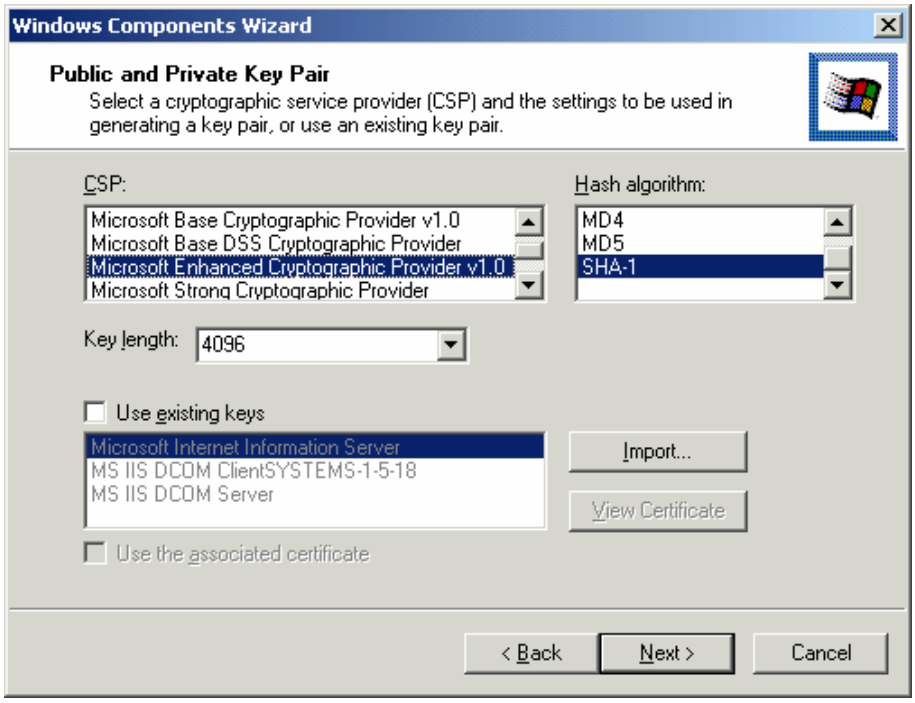


참고 : 인증서 서비스를 설치할 때 아래와 같은 종류의 CA(인증 기관)를 선택하여 설치할 수 있습니다.

인증 기관 종류	설명
엔터프라이즈 루트 CA	엔터프라이즈 루트 CA는 인증서 계층 구조에서 최상위 수준 CA입니다. 엔터프라이즈 루트 CA에는 Active Directory 디렉터리 서비스가 필요합니다. 엔터프라이즈 루트 CA는 자신의 CA 인증서에 자체 서명하고 그룹 정책을 사용하여 도메인에 있는 모든 서버 및 워크스테이션의 신뢰할 수 있는 루트 인증 기관 저장소에 해당 인증서를 게시합니다. 일반적으로 엔터프라이즈 루트 CA는 사용자 및 컴퓨터 인증서에 대해 리소스를 직접 제공하지는 않지만 인증서 계층 구조의 기본 토대입니다. 자세한 내용은 엔터프라이즈 인증 기관을 참조하십시오.
엔터프라이즈 하위 CA	엔터프라이즈 하위 CA는 다른 CA로부터 CA 인증서를 받아야 합니다. 엔터프라이즈 하위 CA에는 Active Directory가 필요합니다. Active Directory, 인증서 템플릿 및 스마트 카드 로그온을 Windows XP 및 Windows Server 2003 제품군 운영 체제를 실행하는 컴퓨터에서 이용하려면 엔트프라이즈 하위 CA를 사용합니다.
독립실행형 루트 CA	독립 실행형 루트 CA는 인증서 계층 구조에서 최상위 수준 CA입니다. 독립 실행형 루트 CA는 도메인의 구성원일 수도 있고 아닐 수도 있으므로 Active Directory를 필요로 하지 않습니다. 그러나 Active Directory가 있을 경우 이를 사용하여 인증서와 인증서 해지 목록을 게시합니다. 독립 실행형 루트 CA는 Active Directory를 필요로 하지 않기 때문에 네트워크에서 손쉽게 제거하여 보안 영역에 배치할 수 있습니다. 이는 보안 오프라인 루트 CA를 만들 때 유용합니다. 자세한 내용은 독립 실행형 인증 기관을 참조하십시오.
독립 실행형 하위 CA	독립 실행형 하위 CA는 다른 CA로부터 CA 인증서를 받아야 합니다. 독립 실행형 하위 CA는 도메인의 구성원일 수도 있고 아닐 수도 있으므로 Active Directory를 필요로 하지 않습니다. 그러나 Active Directory가 있을 경우 이를 사용하여 인증서와 인증서 해지 목록을 게시합니다. 독립 실행형 하위 CA는 다른 CA로부터 CA 인증서를



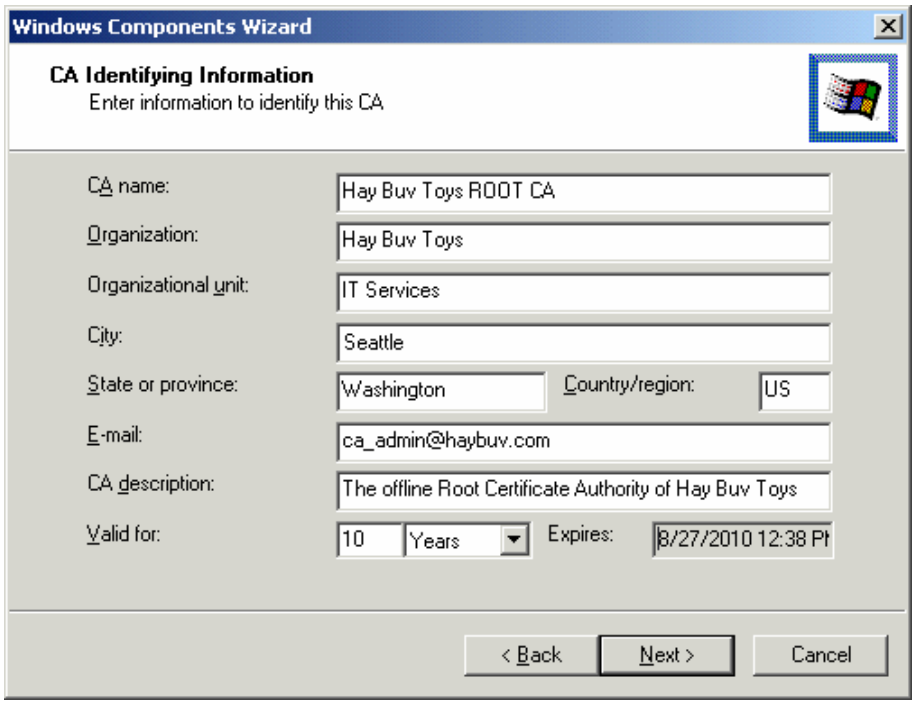
4)공개키/개인키 암호화부분에서 추가적인 Cryptographic Service Provider(CSP)를 선택할 수 있습니다. 이 중에서 가장일반적으로 Microsoft Enhanced Cryptographic Provider Version1.0 을 선택하여 설치하고 사이즈는 10225-4096 을 사용합니다.



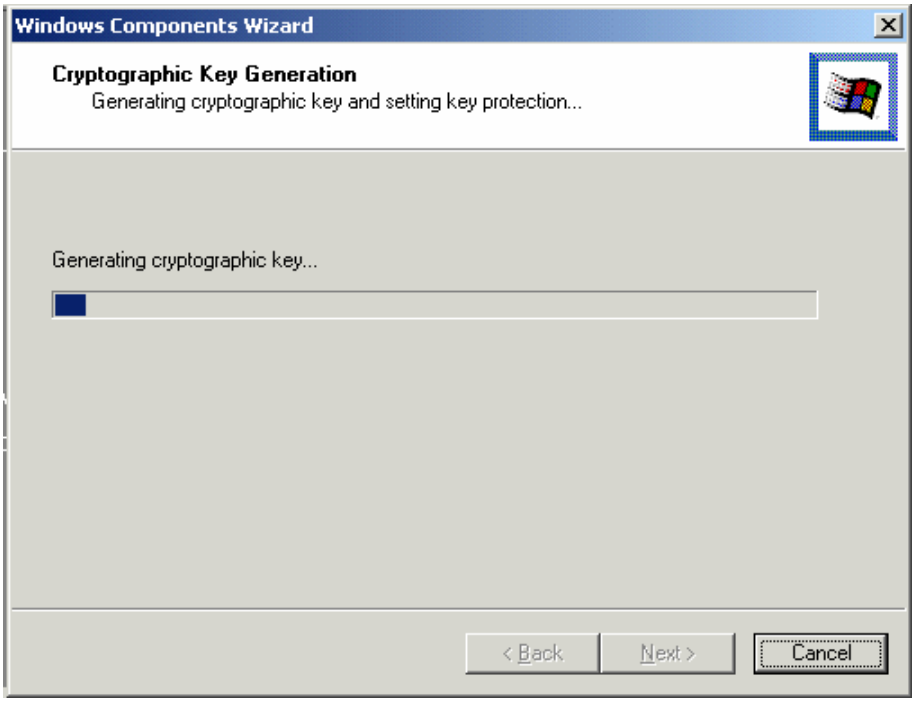
5) 다음은 CA 서버의 이름을 지정하고 CA 서버의 유효기간(라이프 타임)을 설정합니다.

팁 : 인증서 서비스를 설치할 때 CA 식별 정보를 제공하는 방법에 대한 몇 가지 지침입니다.

필드	설명
CA 이름	CA 에 사용할 이름입니다. 모든 유니코드 문자를 사용하여 문자열을 입력할 수 있습니다. CA 이름은 Active Directory 에 사용되는 CA 의 고유 이름에 대한 공통 이름이기도 합니다. CA 이름에 특수 문자가 포함된 경우 수정되지 않은 CA 이름을 사용할 수 없는 작업에 삭제된 CA 이름이 사용됩니다. 삭제된 CA 이름이란 파일 이름, CryptoAPI 키 컨테이너 이름 및 Active Directory 개체 이름에 사용할 수 있는 형식으로 인코딩된 모든 특수 문자로 된 CA 이름을 말합니다. 특수 문자는 이러한 이름 중 하나 이상에 사용할 수 없는 문자이며 목록에는 ASCII 문자가 아닌 모든 문자 및 많은 ASCII 문장 부호가 포함됩니다. 뿐만 아니라 Active Directory 개체 이름은 LDAP(Lightweight Directory Access Protocol) 표준에 따라 64 문자로 제한됩니다. 이러한 제한 때문에 Active Directory 개체 이름은 삭제된 이름을 자른 다음 삭제된 부분만큼 계산된 해시를 추가하여 구성됩니다. 고유 이름 접미사 필드는 Active Directory 도메인의 고유 이름으로 자동으로 채워집니다. 이 고유 이름을 편집할 때는 LDAP 표준을 준수해야 합니다. 명령줄 프롬프트에서 인수 없이 **certutil.exe** 를 입력하여 게시된 모든 CA 의 삭제된 이름을 표시할 수 있습니다. **certutil.exe –v –ds** 를 입력하면 CA 관련 Active Directory 이름을 모두 표시할 수 있습니다. 첫째 열은 잘린 다음 해시가 추가된 CA 이름입니다. 이는 원래 형식으로 다시 전환된 특수 문자를 사용하는 실제 Active Directory 개체의 컨테이너 이름입니다. 잘려서 삭제된 이름이 잘린 CA 이름과 일치하지 않고 실제 Active Directory 개체의 컨테이너 이름인 경우에만 둘째 열이 표시됩니다.
고유 이름 접미사	CA 이름에 추가될 X.500 고유 이름 접미사입니다.
유효 기간	CA의 인증서가 유효한 기간입니다. CA는 이 기간 동안 유효한 인증서를 얻으며 이 인증서의 개인 키를 발급된 인증서 및 인증서 해제 목록에 서명하는 데 사용합니다.



6) 서비스 환경 설정 및 CA 는 생성될 것입니다. 루트 인증서는 루트 CA 에 의하여 스스로 사인됩니다.



데이터베이스 7) 장소와 로그를 저장할 장소를 지정합니다.

CA 서버를 복구하기 위한 백업은 공유 폴터 라고 하는 곳에 지정합니다.

인증서 서비스는 로컬 저장소를 사용하여 데이터베이스, 구성 데이터, 백업 데이터 및 로그 데이터를 저장합니다. CA 를 설치할 때 데이터베이스 및 로그의 위치를 지정할 수 있습니다. 기본값으로 CA 가 발급하는 인증서는 아래 위치에 저장됩니다.

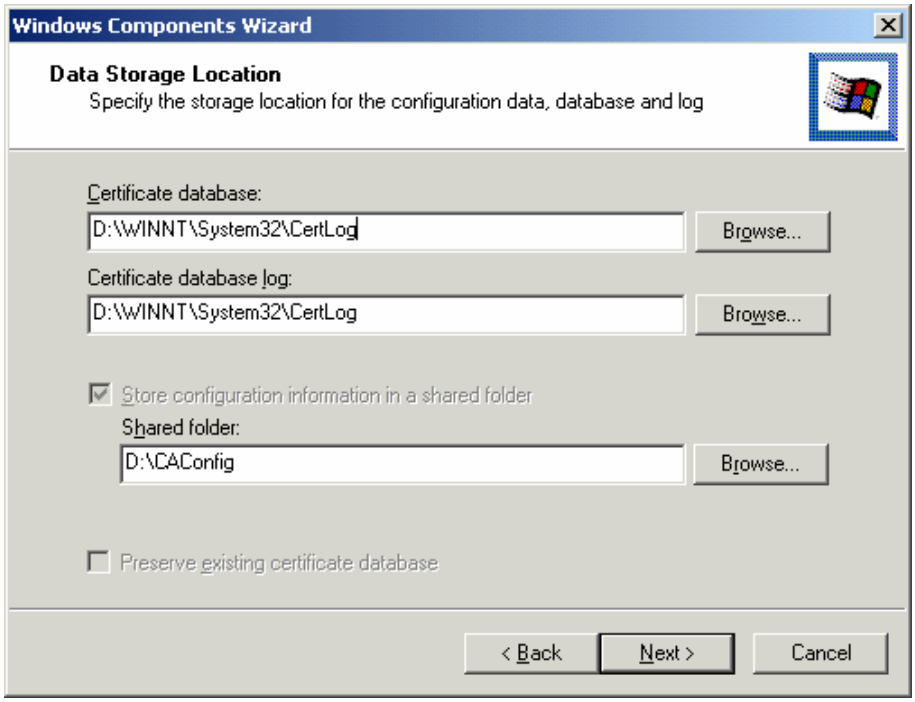
₩*Systemroot*₩system32₩certlog

최고의 성능을 위해서는 데이터베이스와 로그 파일을 별도의 실제 디스크 드라이브에 저장해야 하며 별도의 디스크 컨트롤러를 사용하면 더 좋습니다. 그러면 디스크 처리량이 극대화되고 CA 성능이 향상됩니다.

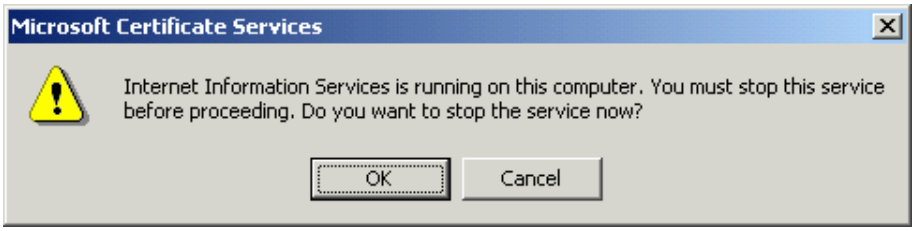
CA 를 설치할 때 공유 폴더를 지정할 수도 있습니다. 공유 폴더는 컴퓨터 사용자가 인증 기관에 대한 정보를 찾을 수 있는 위치입니다. 이 옵션은 Active Directory 를 사용하지 않고 독립 실행형 CA 를 설치하는 경우에만 유용합니다.

인증서 서비스의 호스트 컴퓨터가 도메인의 구성원인 경우 CA 에 대한 정보가 자동으로 Active Directory 에 게시됩니다. 그러나 Active Directory 는 인증서 서비스의 데이터베이스로 동작하지 않습니다. 이 기능은 로컬 컴퓨터에 유지됩니다.

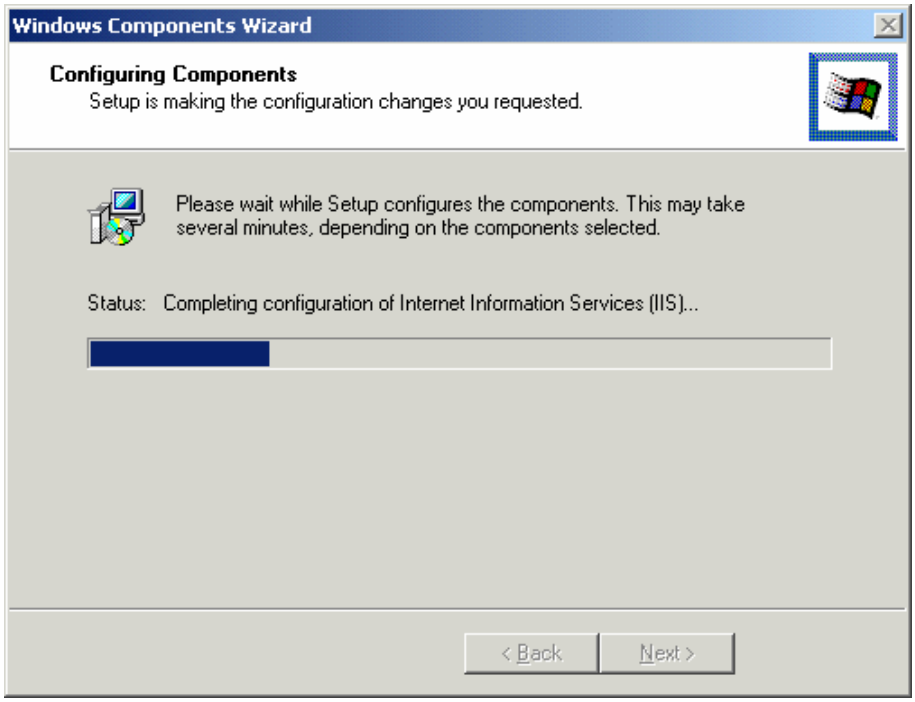
CA 서버는 99.999 의 가용성을 보장하기 위하여 NTFS 로 포맷되어야 하며 Raid5 로 구성될 것을 권장합니다. 데이터베이스는 Small – Medium 사이즈의 기업인 경우 환경의 최적화와 Fault-Tolerance 를 위하여 20GB 를 권장합니다.



8) 마이크로소프트 Internet Information Service (IIS) 서비스는 중지되었다가 다시 시작됩니다.



9) IIS 관련 서비스들이 갱신되고 추가됩니다.

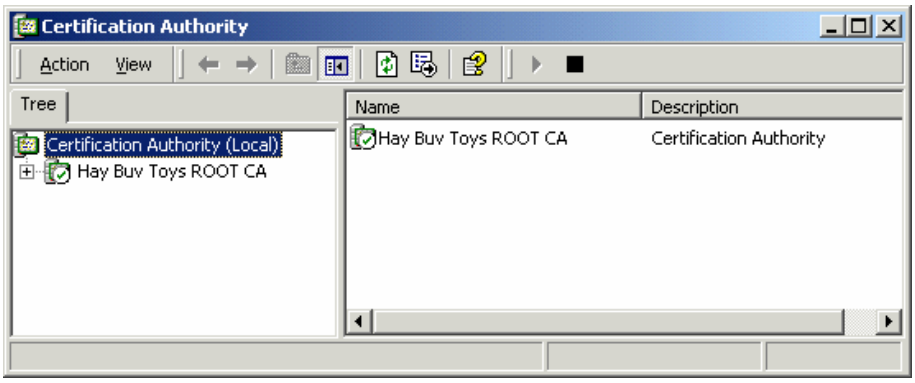


이제 설치가 모두 끝났습니다. 이제 인증서를 발행하는 인증서 서비스를 사용할 준비가 되었습니다.

1-3 인증서 서비스 환경설정하기

CA 서버를 이용하여 사용자에게 인증서를 발급할 수 있도록 설치가 되었습니다. 하지만, 이렇게 하기 전에 Certificate Revocation List(CRL) 의 장소를 지정하고 또한 Authority Information Access(AIA)의 장소를 지정할 필요가 있습니다. 강력한 PKI 어플리케이션은 인증서 취소 상태를 확인하거나 공인키를 다운로드 하는 상태를 확인하기 위하여 위의 장소를 확인합니다.

CA 가 속해 있는 Microsoft Management Console (MMC) 을 실행하십시오 아래의 그림에서 서비스가 실행중인 것을 초록색 체크마크를 보고 확인할 수 있습니다.



정책 모듈 / 구성 / X.509 를 선택하고 지정되어 있는 다른 장소들을 지우십시오. 체크를 하지 않거나 모두 삭제할 수 있는 옵션을 제공합니다.

루트 CA 서버는 네트워크 상에서 객체로 보여지지 않기 때문에 CRL 과 CRT 파일은은 모두 웹 서버에 수동으로 복사해야 합니다. 웹 서버는 DNS 에서 해석 가능한 이름으로 사용되어야 합니다.

1-4 참고

만약에 루트 CA 가 또한 Certificate Distribution Point(CDP)이며 루트 CA 를 위하여 스스로 사인된 CDP 장소가 있다면 루트 CA 를 capolicy.inf 파일을 이용해서 생성할 필요가 있습니다. 이것은 또한 루트 CA 인증서에서 Practice Statement URL 을 세팅하기 위하여도 필요합니다. Capolicy.inf 파일은 ₩windows 디렉터리에 있고 다음과 같습니다.

[Version]

Signature= "$Windows NT$"

[CAPolicy]

Policies = LegalPolicy, LimitedUsePolicy, ExtraPolicy, OIDPolicy

[LegalPolicy]

OID = 1.3.6.1.4.1.311.21.43

Notice = "Legal policy statement text."

[LimitedUsePolicy]

OID = 1.3.6.1.4.1.311.21.47

URL = "http://http.site.com/some where/default.asp"

URL = "ftp://ftp.site.com/some where else/default.asp"

Notice = "Limited use policy statement text."

URL = "ldap://ldap.site.com/some where else again/default.asp"

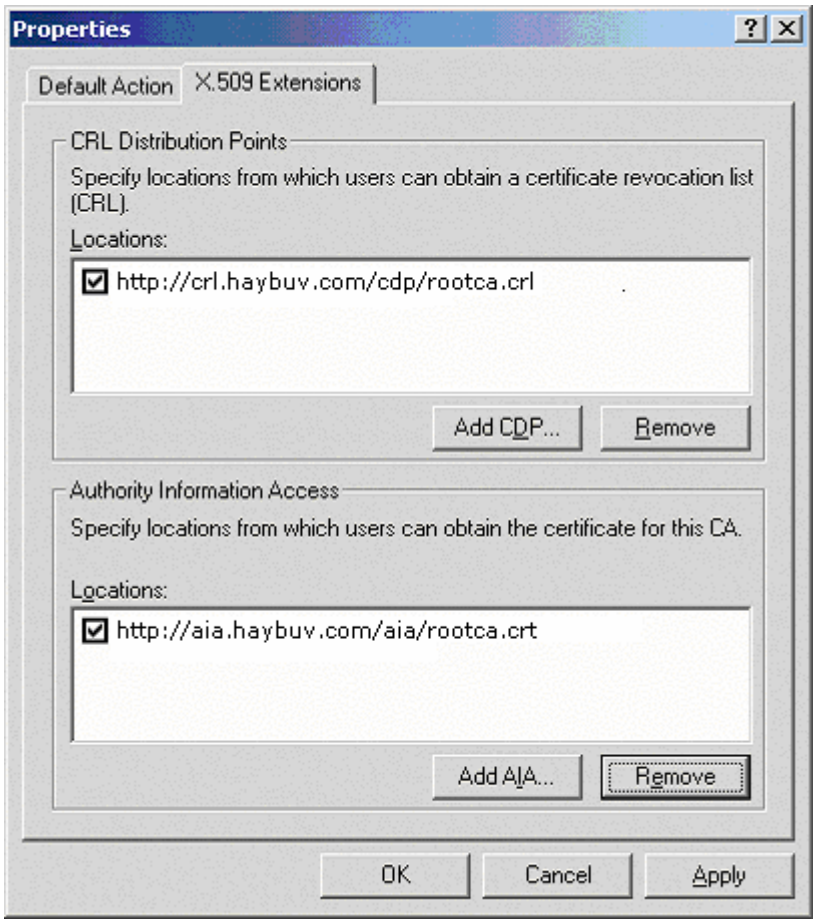
[ExtraPolicy]

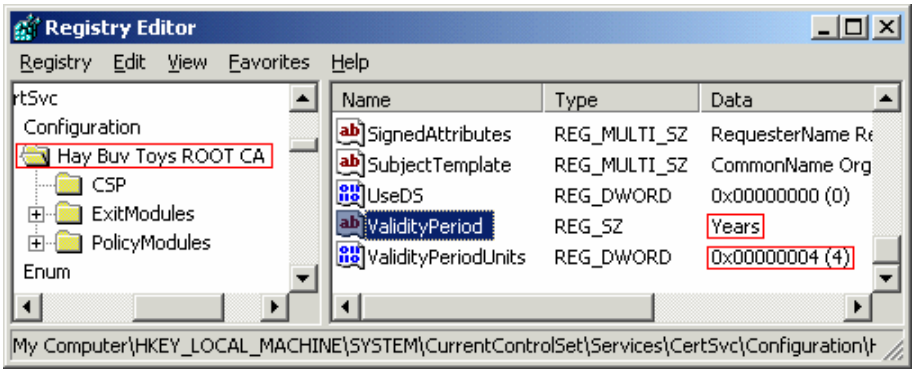
OID = 1.3.6.1.4.1.311.21.53

URL = http://extra.site.com/Extra Policy/default.asp

[oidpolicy]

OID = 1.3.6.1.4.1.311.21.55



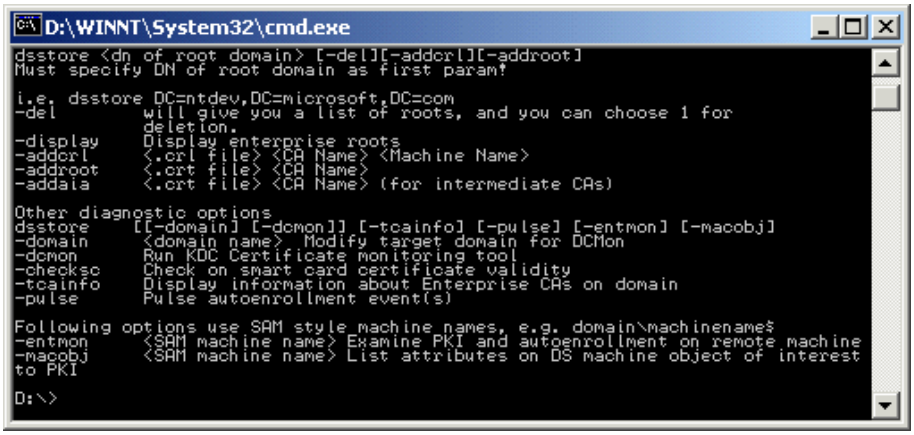


이제 루트 인증서를 Active Directory 에 퍼블리시할 준비가 되었습니다. 완료되면 인증서 계층 구조를 세팅하게 됩니다. 이제부터는 서버의 실행시간이 중요한 요소가 됩니다. 왜냐하면 루트가 실행되지 않고 있으면 트러스트가 깨지기 때문입니다.

퍼블리시하기 위하여 리소스킷에 있는 Dsstore.exe 를 실행합니다. :

dsstore.exe DC=haybuv,DC=com –addroot ROOTCA.CRT “Hay Buv Toys ROOT CA”

프로덕션에 퍼블리시되면 DSSTORE –pulse 명령으로 복제를 합니다.



1-5 Subordinate Certificate Authority 설치하기

마이크로소프트 인증서버는 이미 언급한 대로 다중의 Subordinate Certificate Authority 를 루트밑에 둘 수 있습니다. 사용하는 예를 들면, 하나는 스마트카드 로그온 용으로, 또 다른 하나는 컴퓨터 계정용으로 사용하는 인증서 서버를 둘 수가 있습니다.

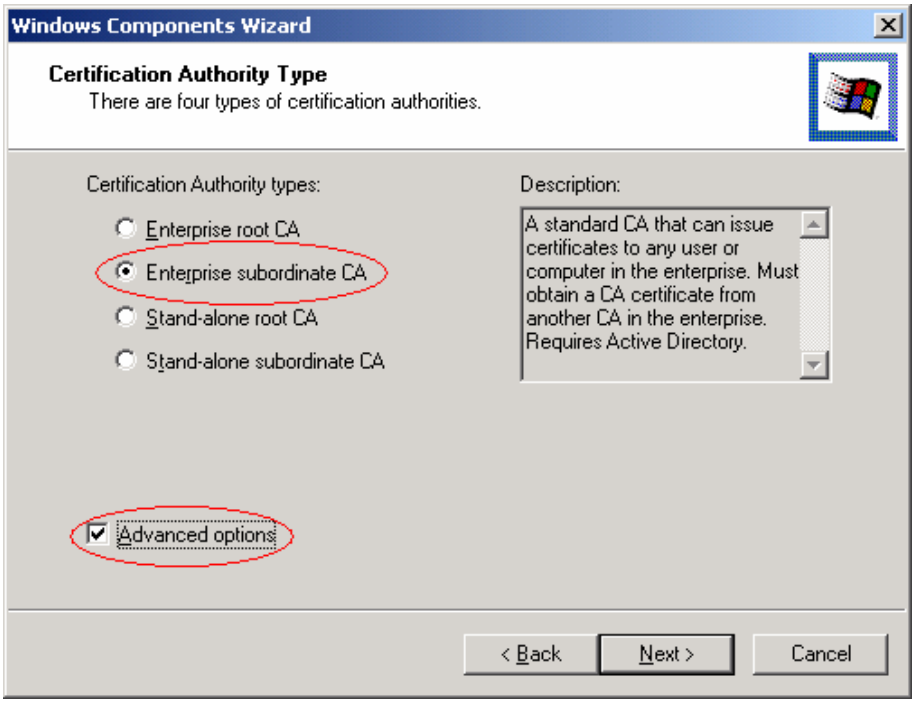
루트 Authority 는 Subordinate authority 와 SRL 이나 AIA 를 LDAP Query 기능을 하는 Active Directory 에 저장하는 측면에서 다릅니다..

Subordinate CA 를 설치하는 프로세스는 루트 CA 를 설치하는 것와 매우 유사한 프로세스입니다. 그리고 모든 Subordinate 는 반드시 생성되는 것이 바람직합니다. 이러한 온라인 상태의 authority 는 기업 내에서 가능하게 하기 위하여 오프라인 루트에 사인을 하게 됩니다.

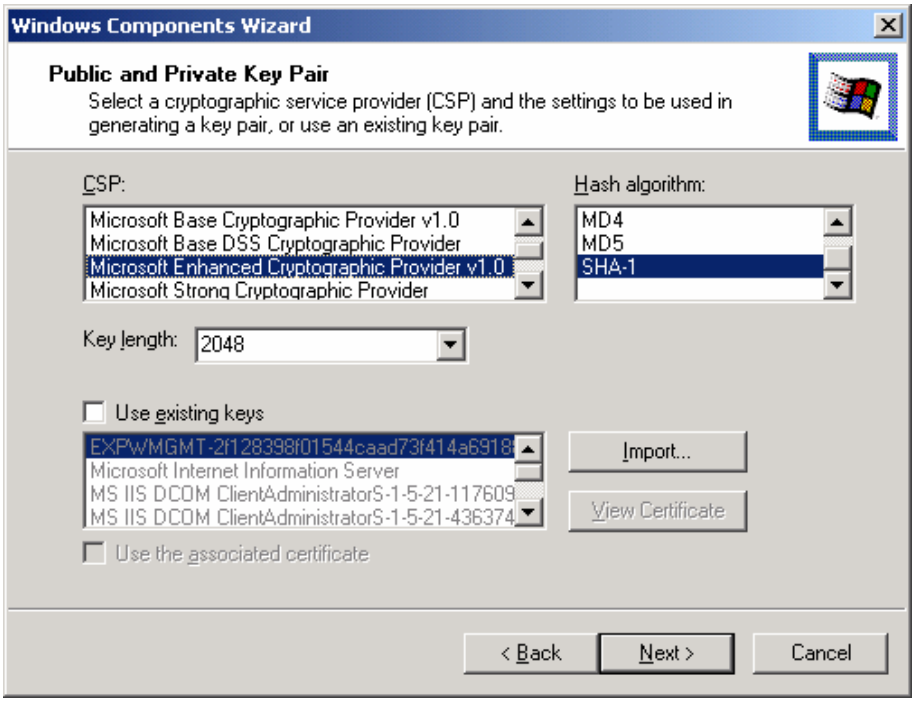
설치를 시작하기 전에 Subordinate authority 가 적용될 컴퓨터에 엔터프라이즈 급 관리자로 로그인하고 다음을 실행합니다.

1) 제어판을 열고 프로그램 추가 / 삭제에서 윈도우 컴포넌트 추가/삭제를 선택하고 여러 가지 리스트 중에 인증서 설치를 선택합니다.

2) 엔터프라이즈 Subordinate CA 를 선택하고 고급옵션을 클릭합니다.

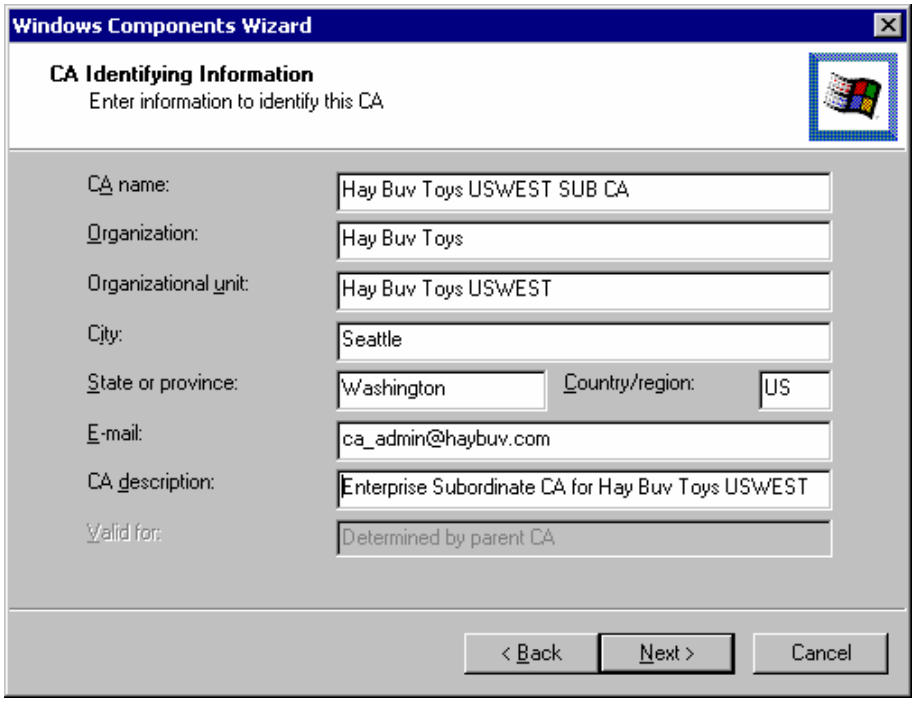


3) 루트 CA 와 같은 CSP 를 선택하고 해쉬 알고리즘을 지정합니다.

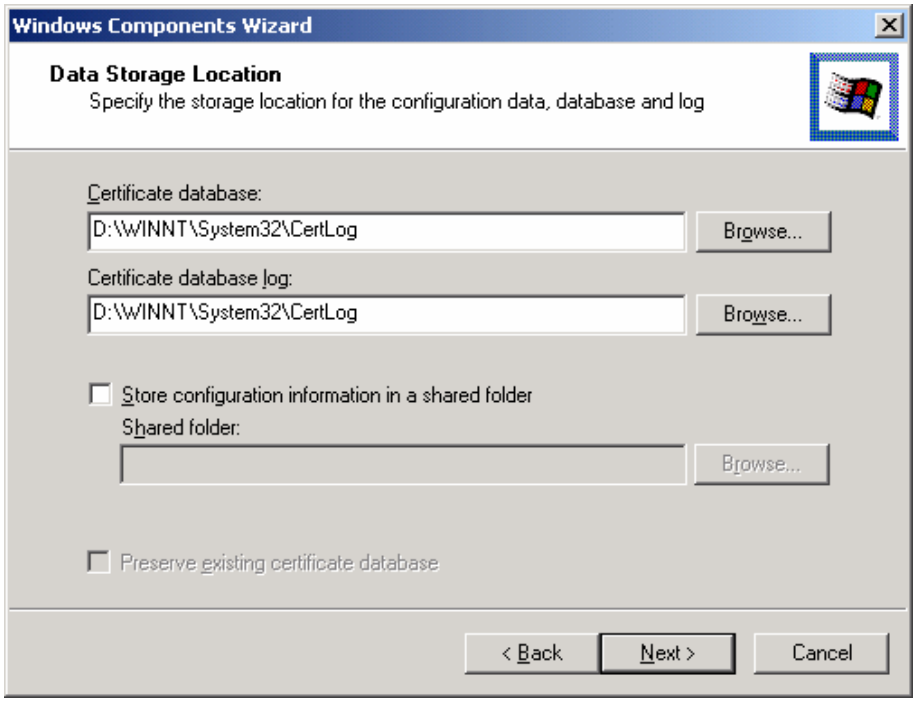


4) 기본 유효기간을 설정합니다. 기본으로 제공하는 기간은 1 년이고 역시 새롭게 갱신될 수 있습니다. 기간을 새롭게 갱신하는 경우 다음 방법과 같이 레지스트리를 수정해서도 가능합니다.

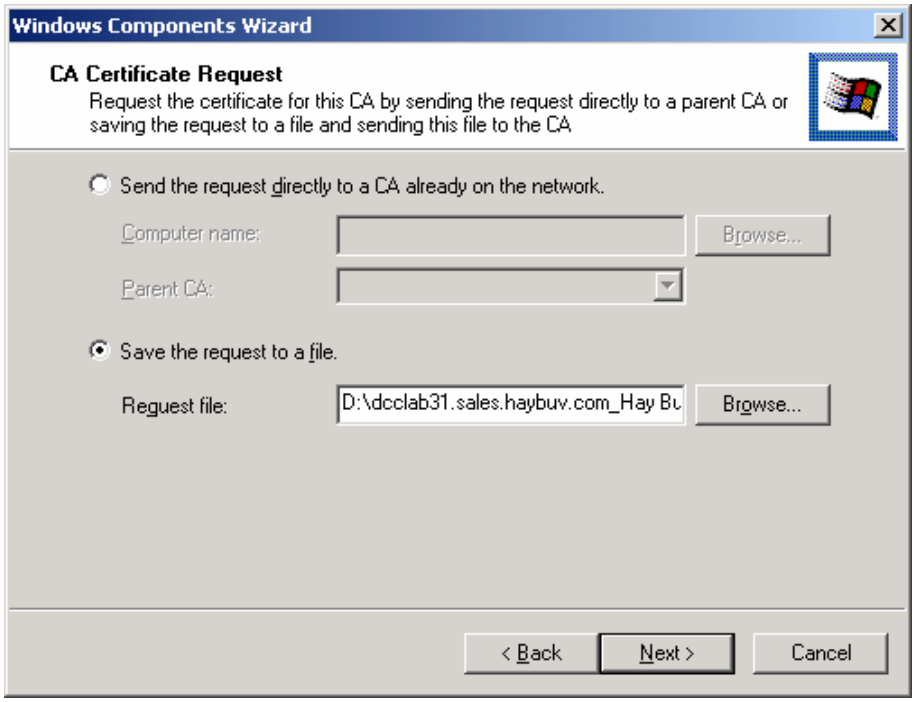
HKLM₩SYSTEM₩CurrentControlSet₩Services₩CertSvc₩Configuration₩<name of the root CA>₩ValidityPeriod



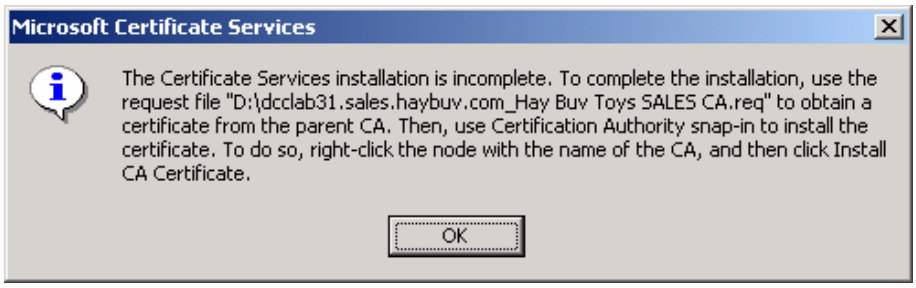
5) 데이터베이스와 로그를 저장하기 위한 장소를 선택합니다.



6) 루트에 의하여 사인된 subordinate 인증서를 갖기 위하여 다음과 같이 2 가지 옵션을 제공합니다. 직접 요청을 루트로 보낼 수도 있고 처리를 위하여 파일을 만든 다음 그 파일을 루트에 보낼 수도 있습니다. 2 가지 옵션을 선택하는 기준은 루트 CA 와 통신이 가능한지에 따라 선택하면 됩니다. 즉, 인터넷이 되지 않는 경우에는 아래 그림과 같이 위의 2 가지 방법 중 2 번째로 설치하면 됩니다.



7) 완료가 되면 마법사는 프로세스가 생성되었다는 메시지를 보여줍니다.



1-6 루트 Authority에 의하여 사인된 인증서 요청

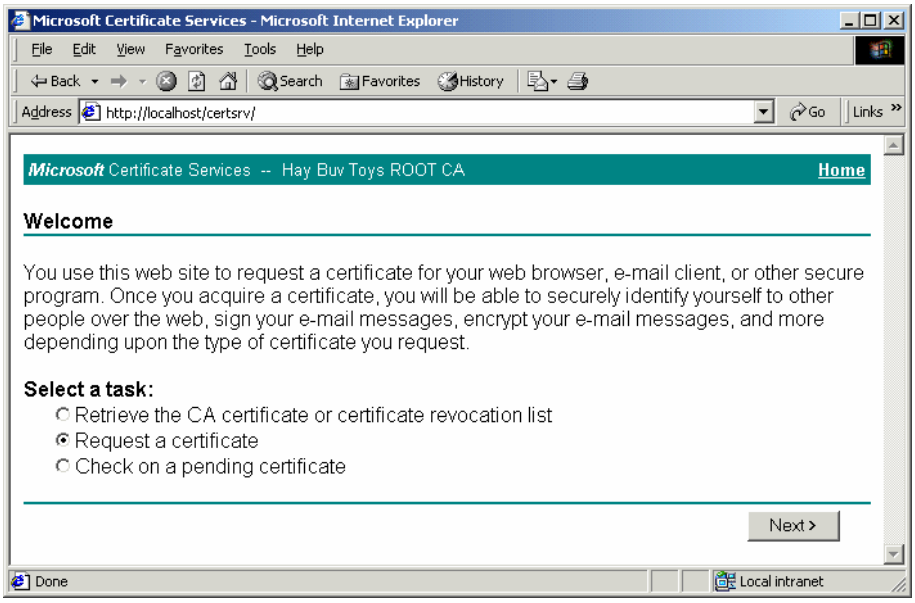
루트에 의하여 사인된 Subordinate 인증서를 받기 위해서는 루트 CA 가 설치된 컴퓨터에서 작업해야 합니다. 루트 CA 에서 다음과 같이 합니다.

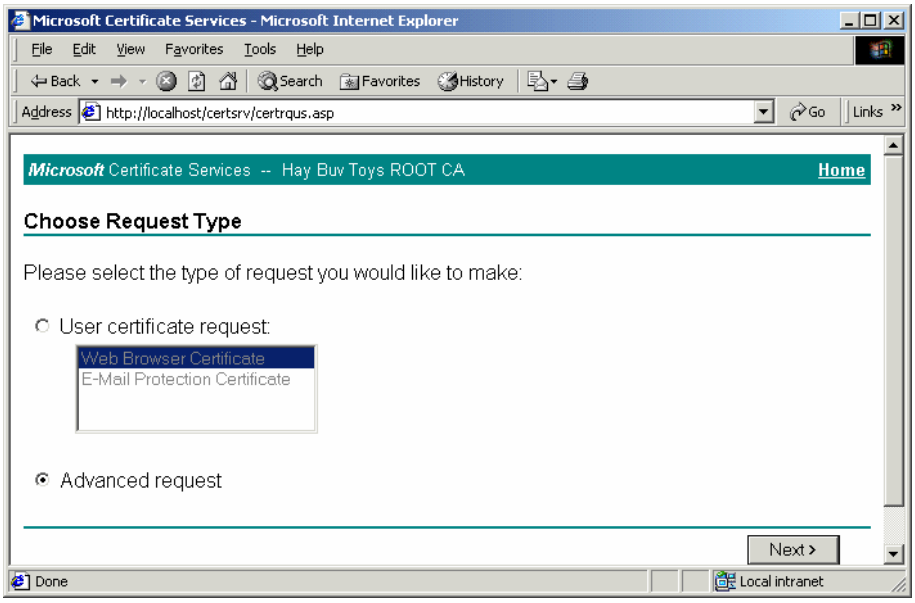
인터넷 브라우저를 열고 Tools/Internet Options/Security/Trusted Siteds 에서 Sites 를 선택하고 Require Server verification 옵션 박스를 선택하지 않습니다. 그리고 Add this server to the web site filed 항목을 다음과 같은 포맷으로 로컬호스트 라고 하거나 서버 이름을 입력합니다.

http://localhost

추가 버튼을 클릭하고 완료 버튼을 눌러서 완료합니다.

1) 브라우저에서 로컬호스트 인증서 서비스를 호출합니다. 그리고 가능한 작업 리스트에서 인증서 요청을 선택합니다.

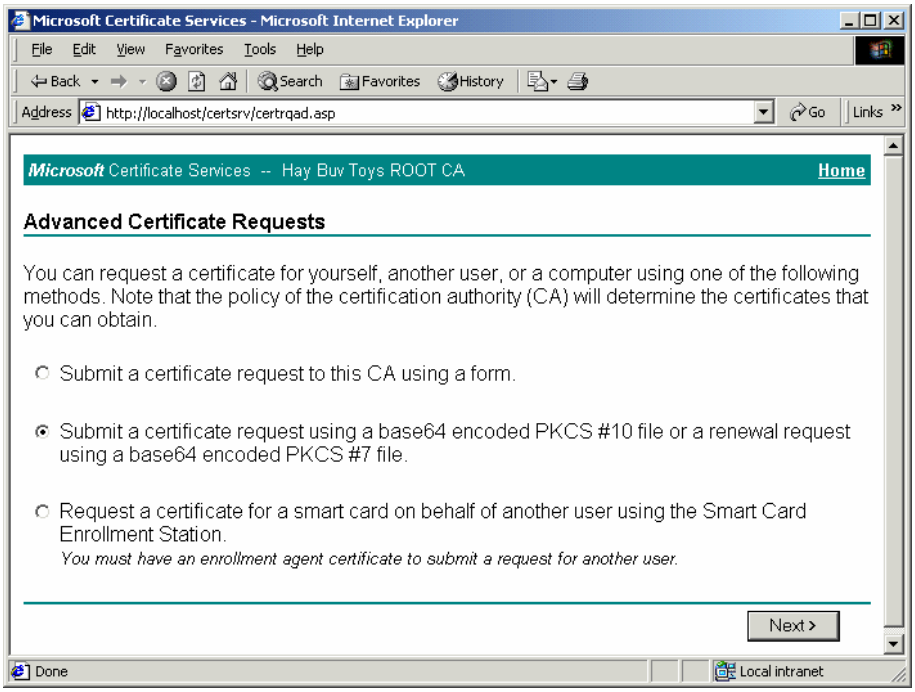




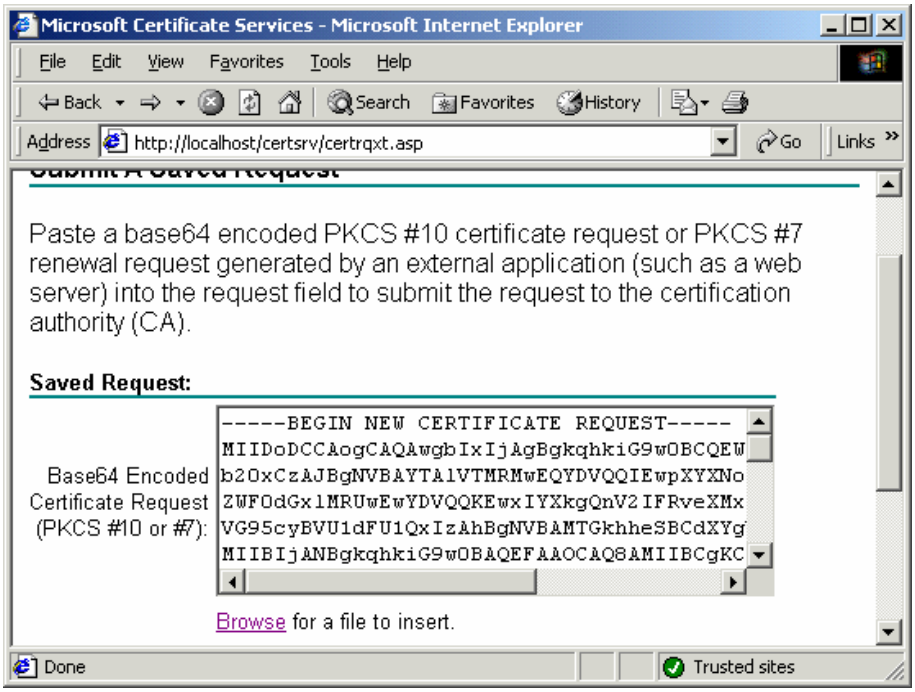
2) 고급 옵션을 선택합니다.

3) standard PKCS 10-base 64 encoded file 을 제출합니다.

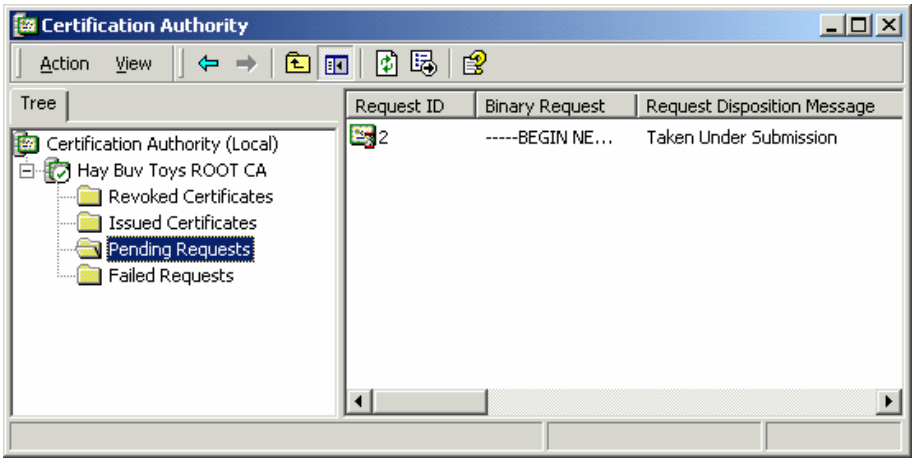
Note 실제로 인증서 서비스를 사용할 경우 만약에 루트 CA 가 기업의 네트워크에 있지 않으면 기밀성을 위하여 반드시 높은 수준의 암호화를 하고 인증서 요청을 수동으로 할 것을 요청합니다.



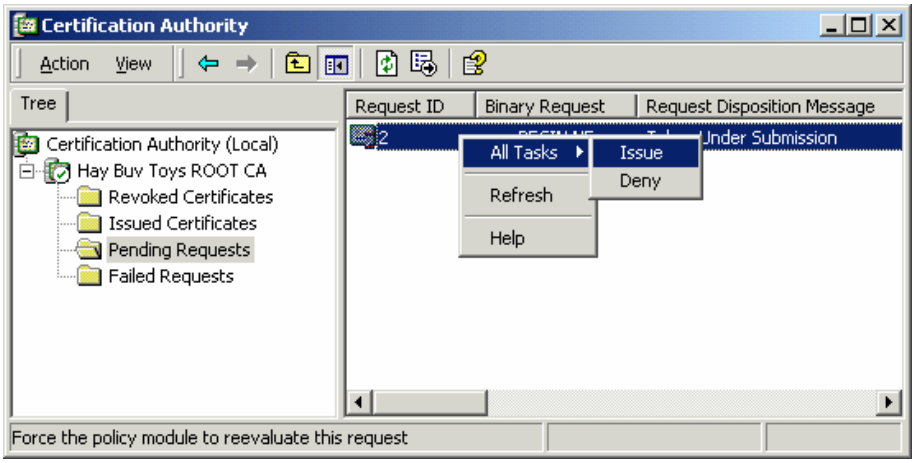
4) Base64 인코드 문서를 붙여 넣는 옵션입니다. 완성이 되면 제출(Submit) 버튼을 선택하십시오.



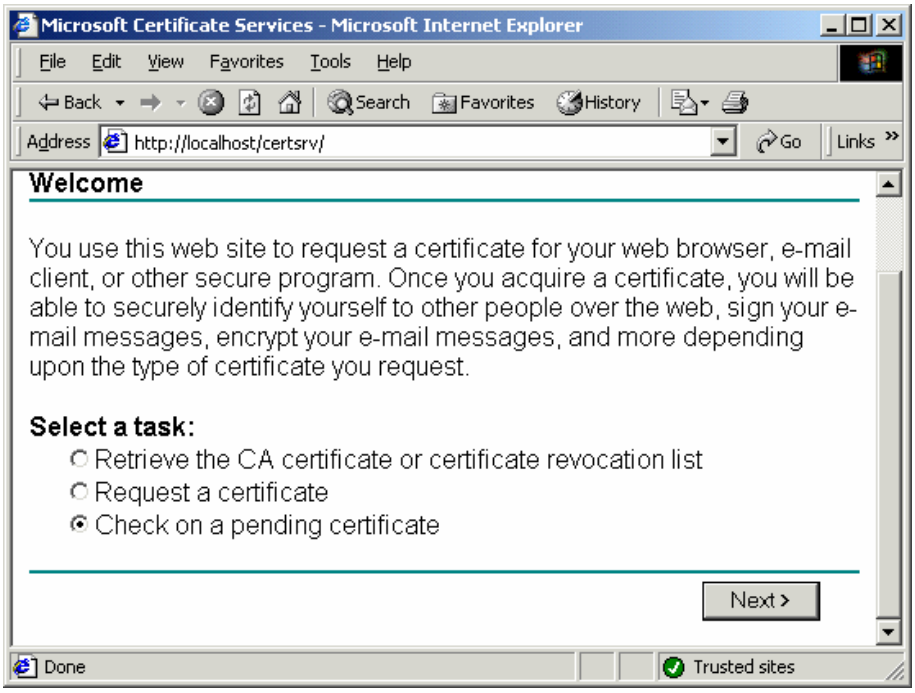
5) 루트 CA 의 MMC 콘솔을 실행하고 대기요청을 선택하십시오.



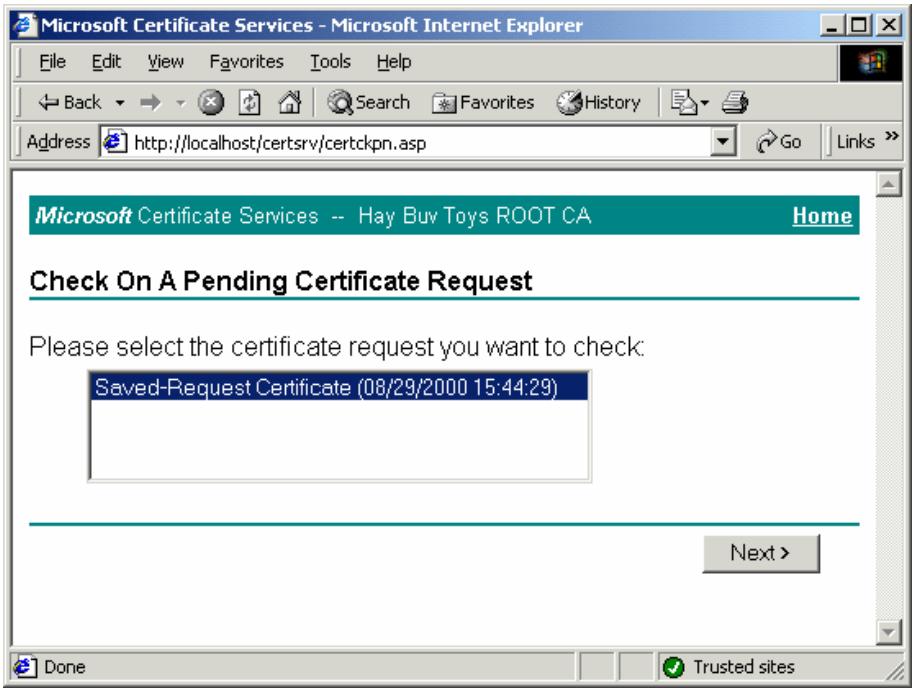
6) 대기 요청을 오른 버튼 클릭하면 발행할 것이지 거절할 것인지를 선택할 수 있습니다. 발행(Issue) 버튼을 클릭하십시오.



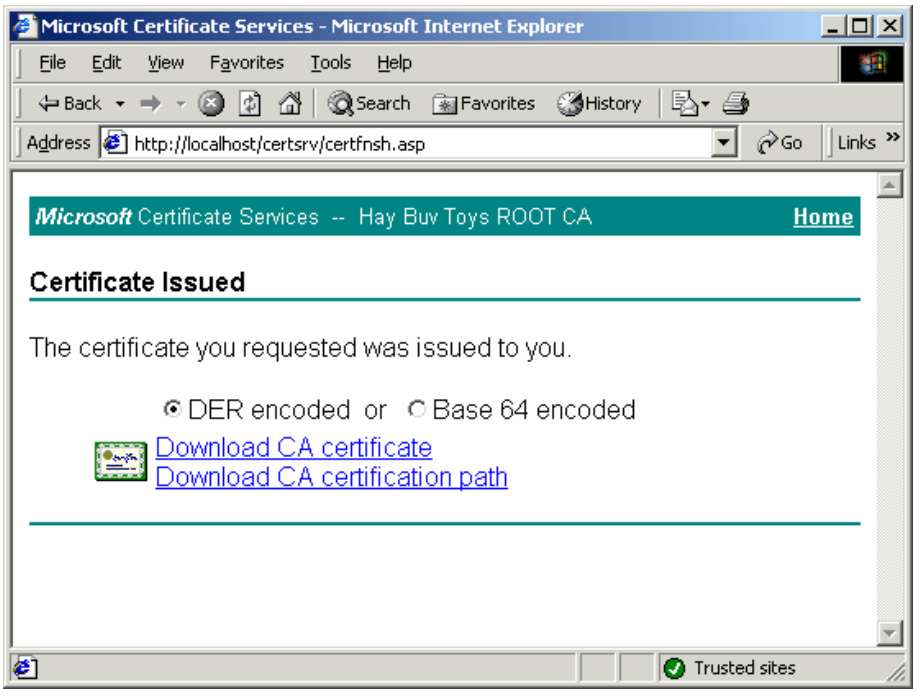
7) 루트의 Enrollment(발급) 페이지로 가서, 대기된 요청의 상태를 확인하십시오.



8) 요청에 대한 상태를 확인할 수 있습니다.

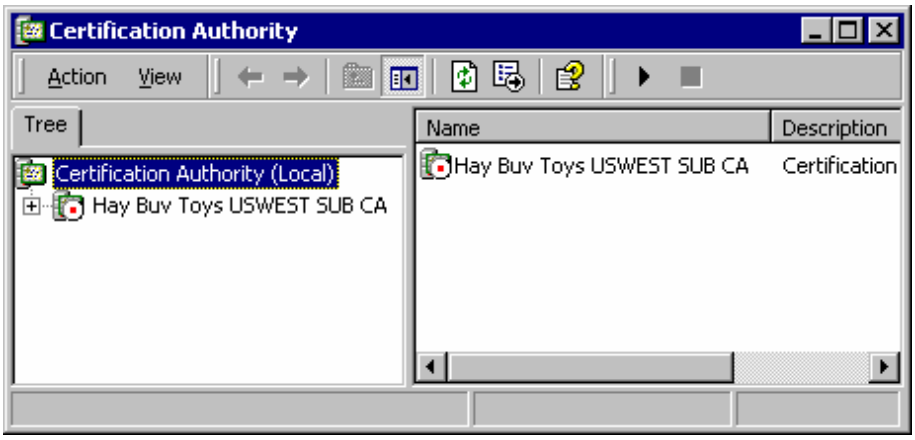


9) 아래 그림에서 보듯이 다운로드 패스를 지정하던지 또는 플로피 같은 저장 장치를 통해서 다운로드 할 것인지에 대한 옵션을 볼 수 있습니다. 발급된 인증서는 옵션에 따라서 리모트 사이트에서 요구하는 방식대로 직접 플로피 등에 담아서 전달할 수 있습니다.

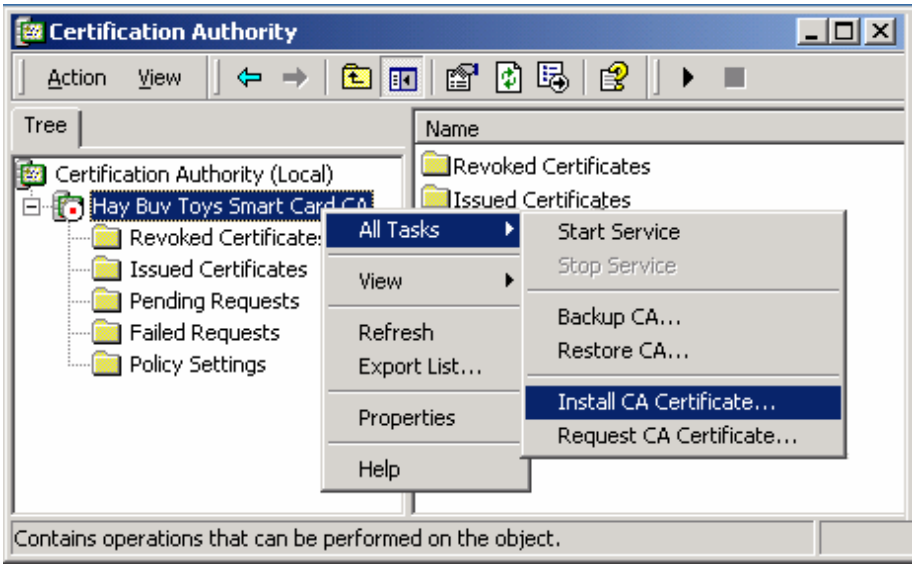


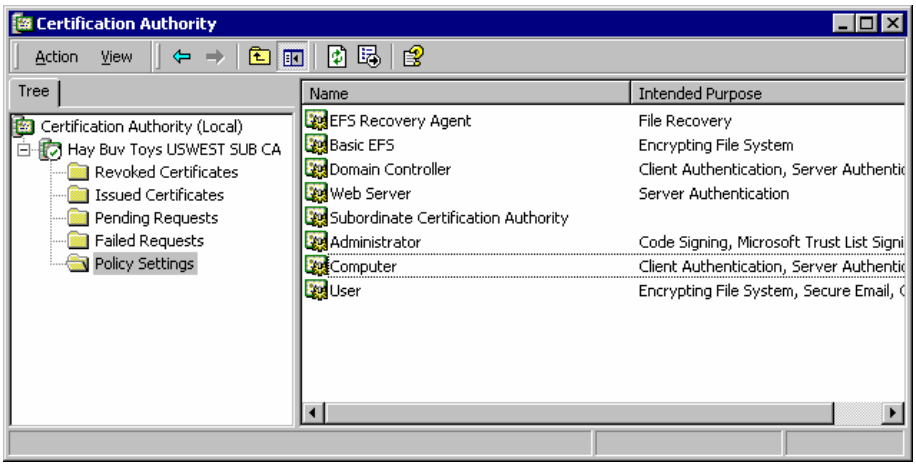
1-7 Subordinate CA 설치하고 활성화하기

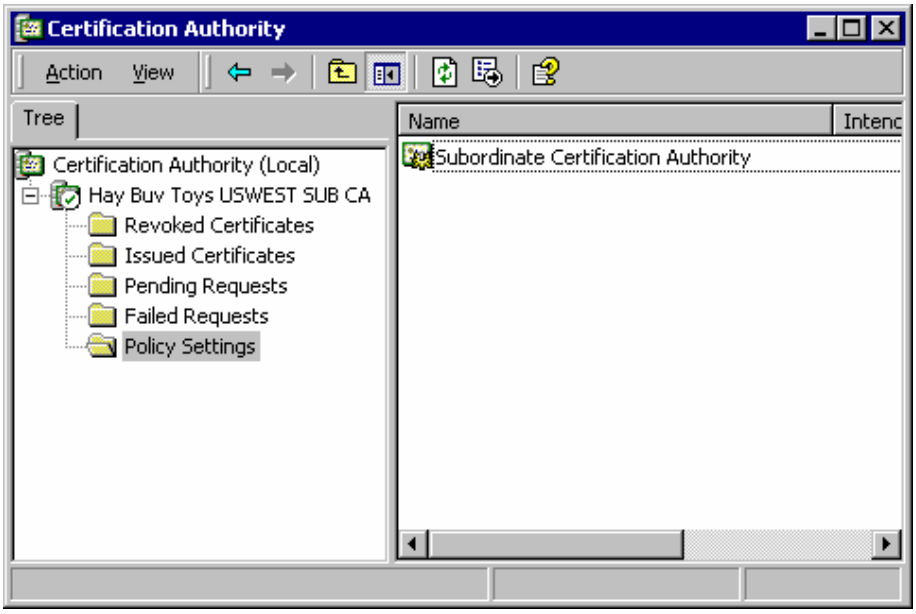
1) subordinate CA 로 돌아와서 MMC 콘솔을 실행합니다. MMC 콘솔에서는 Subordinate CA 서비스가 현재 실행 중인지의 여부를 볼 수 있습니다.



2) Subordinate CA 를 오른 버튼 클릭하고 작업 리스트 중에서 인증서 설치(Install CA Certificate) 옵션을 선택합니다.



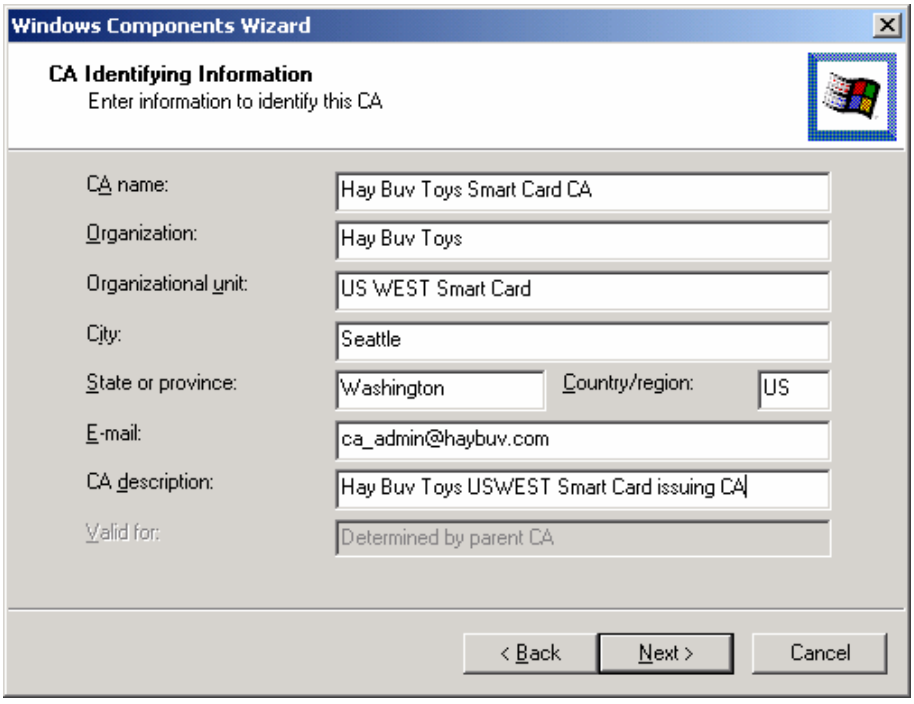




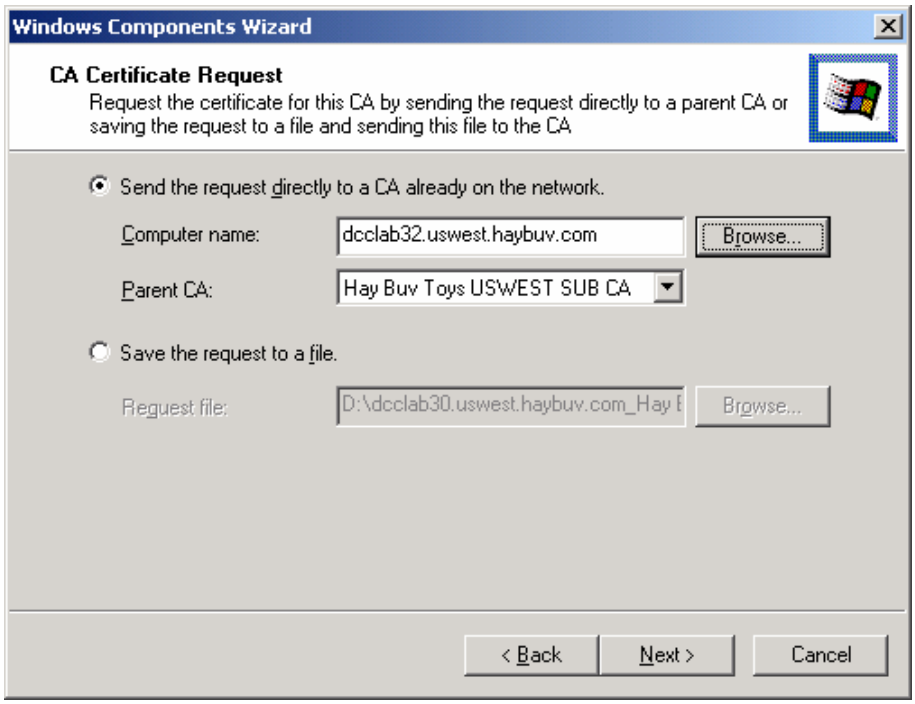
1-8 추가적인 Subordinate CA 설치하기

위에서 언급한 방식대로 계속해서 루트 밑에 Subordinate CA 를 설치할 수 있습니다.

1) 아래 그림은 위에서 언급한 방식과 마찬가지로 루트 CA 에 Subordinate 를 생성하는 화면입니다.



2) 첫 번째 Sub CA 설치 방식과 다르게 네트워크상에 이미 존재하는 CA 서버로 요청 보내기를 선택합니다.



3)무선 액세스– IAS 서버 구성하기

1. 개요

AP을 이용한 무선 액세스 서비스를 Windows Server 2003에 구축하기 위해서는 다음과 같은 기능이 서버에 설치되어야 합니다.

1) Active Directory (Domain Controller)
2) DHCP
3) DNS
4) 라우팅 및 원격 액세스
5) Internet Information Service (IIS)
6) IAS(Internet Authentication Service)

2. Windows Server 2003 설치하기

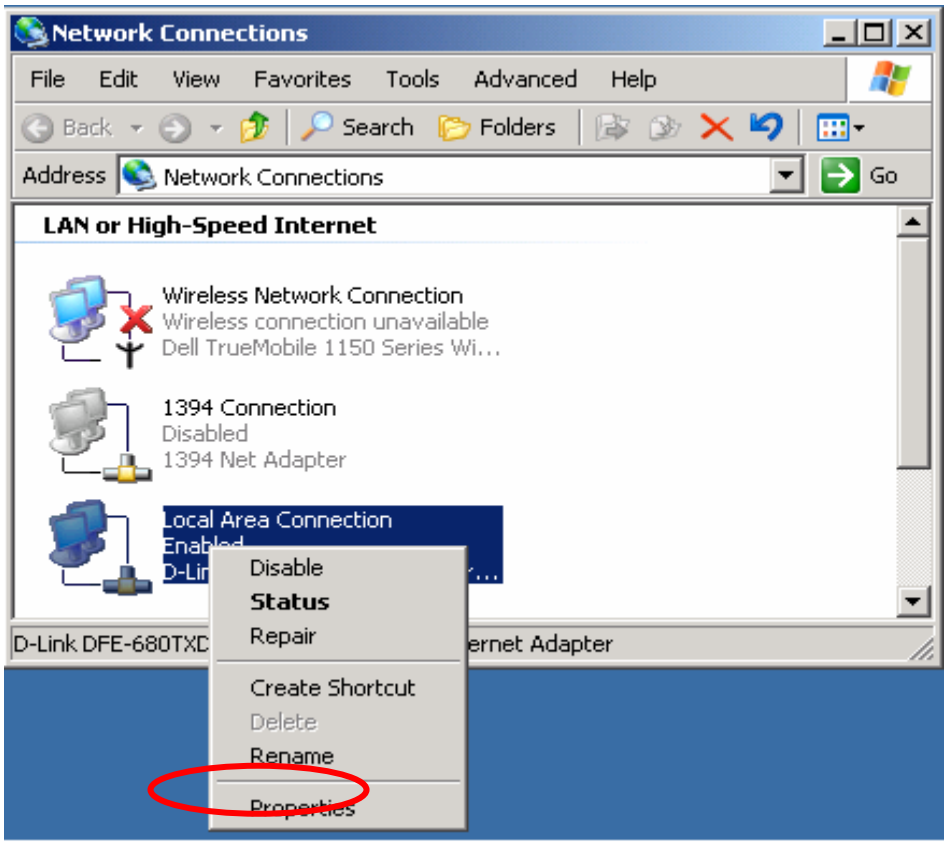
Windows Server 2003 설치하기: (Standard Server, Enterprise Server– Standard edition과 enterprise edition을 선택하는 기준은 동시 연결 수에 따라 선택하면 됩니다. Standard edition은 동시 연결을 25개까지 지원합니다.)

1. NTFS 파티션에 운영체제를 설치합니다. FAT32 를 사용하고 있다면 도메인컨트롤러로 만들기 전에 NTFS 로 전환할 것을 권고합니다. (Convert cL/fs:ntfs)

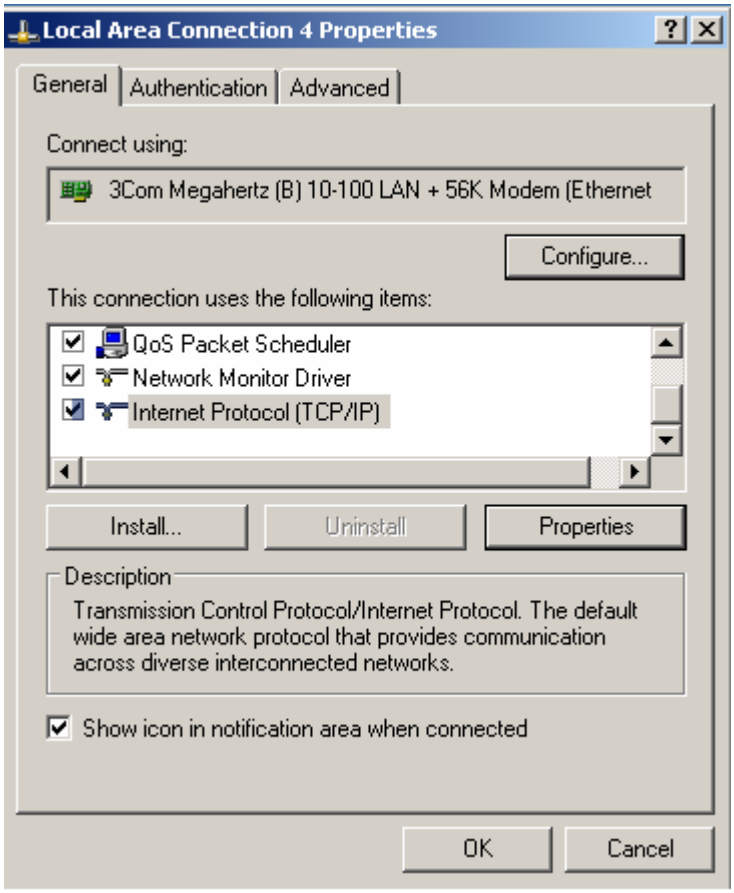
2. 네트워크의 로컬 인터페이스에 IP 주소를 할당합니다.

"네트워크 연결" 실행 : 시작 → 세팅 → 네트워크 연결.

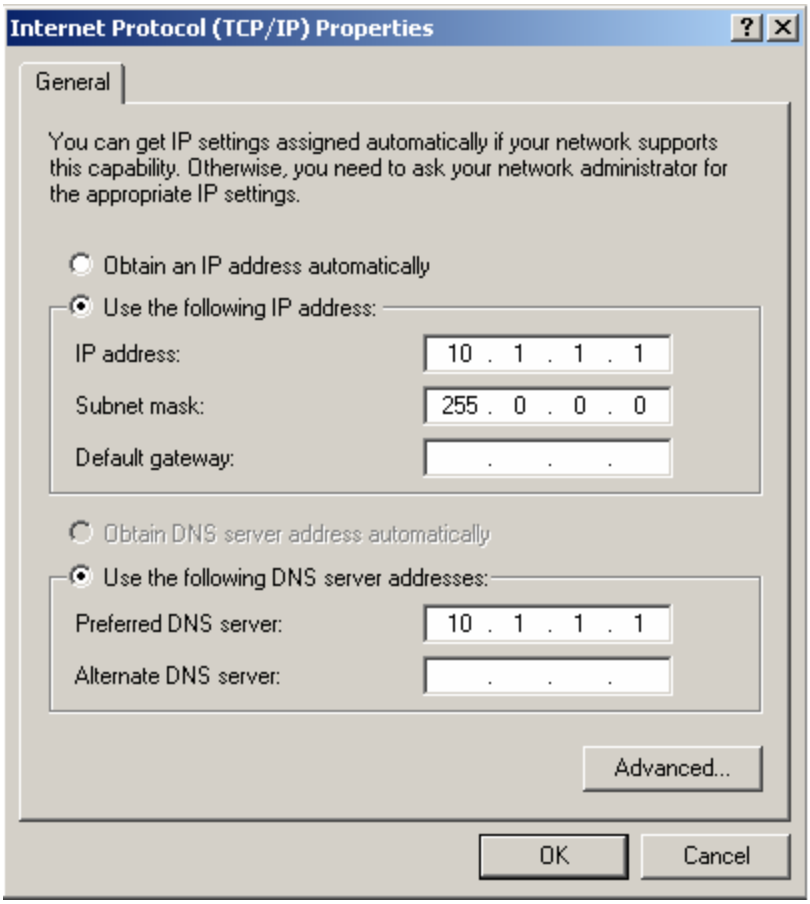
3. 사설망에 액세스하려고 하는 인터페이스를 선택하고 오른 버튼을 클릭해서 속성을 선택합니다.



4. Internet Protocol (TCP/IP)을 선택하고 속성 버튼을 클릭합니다.



5. 라디오 버튼 중에 다음 IP 주소 사용을 클릭하고 IP 주소를 적절한 서브넷 주소와 함께 입력합니다. 그리고 DNS 서비스를 구성해야 하기 때문에 다음 DNS 서버 주소 사용에 IP 주소를 입력합니다 .입력을 완료한 다음 로컬 영역 연결 속성 페이지를 닫습니다.

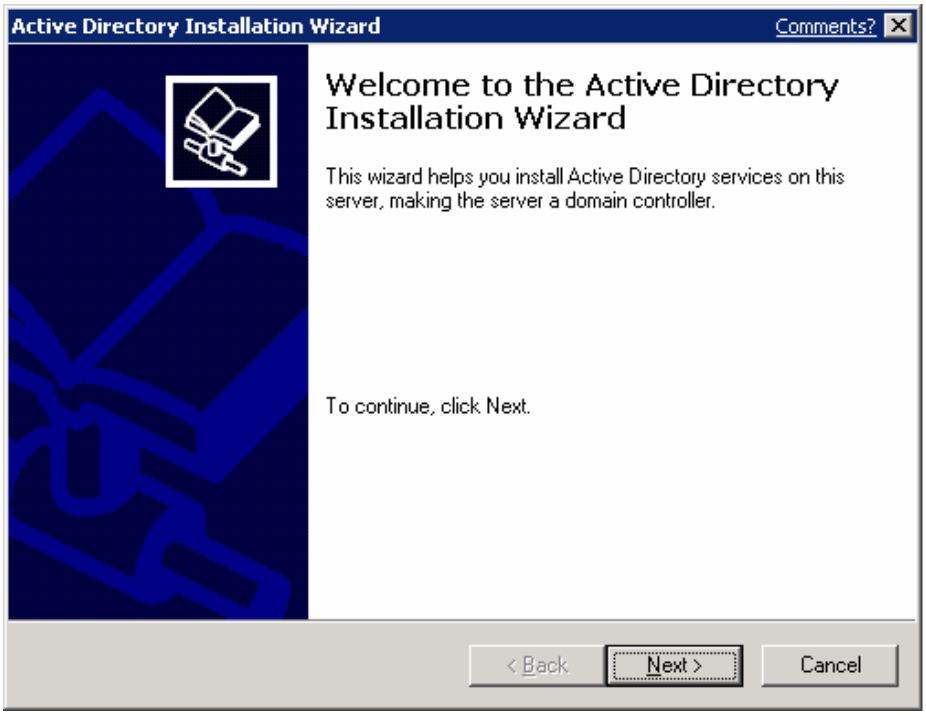


6. 네트워크 연결을 닫습니다.

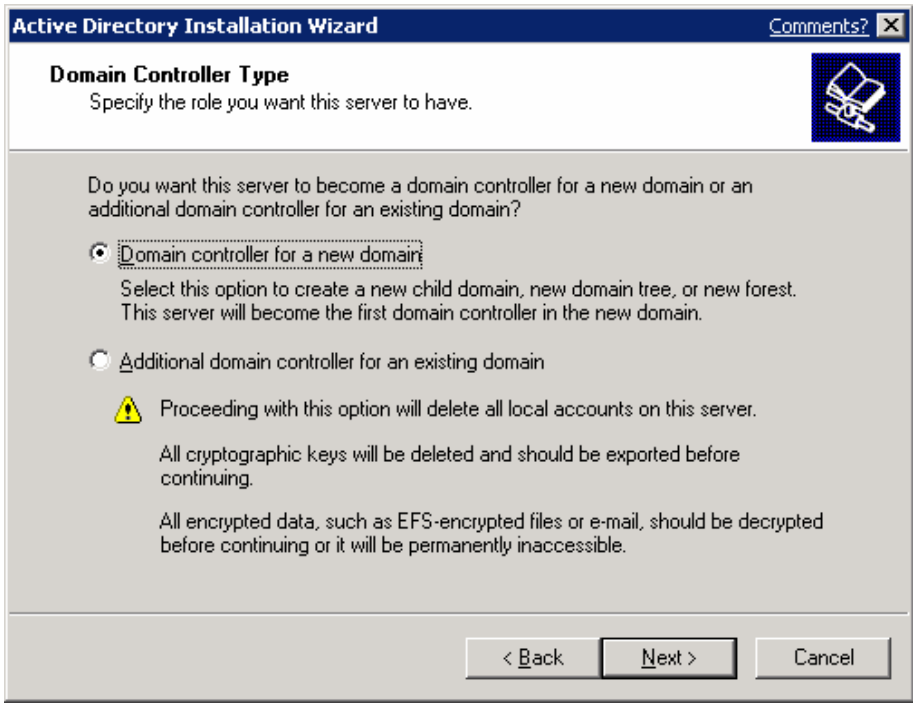
3. 부모 도메인 설치하기

4. 해당 컴퓨터를 도메인 컨트롤러로 승격하기

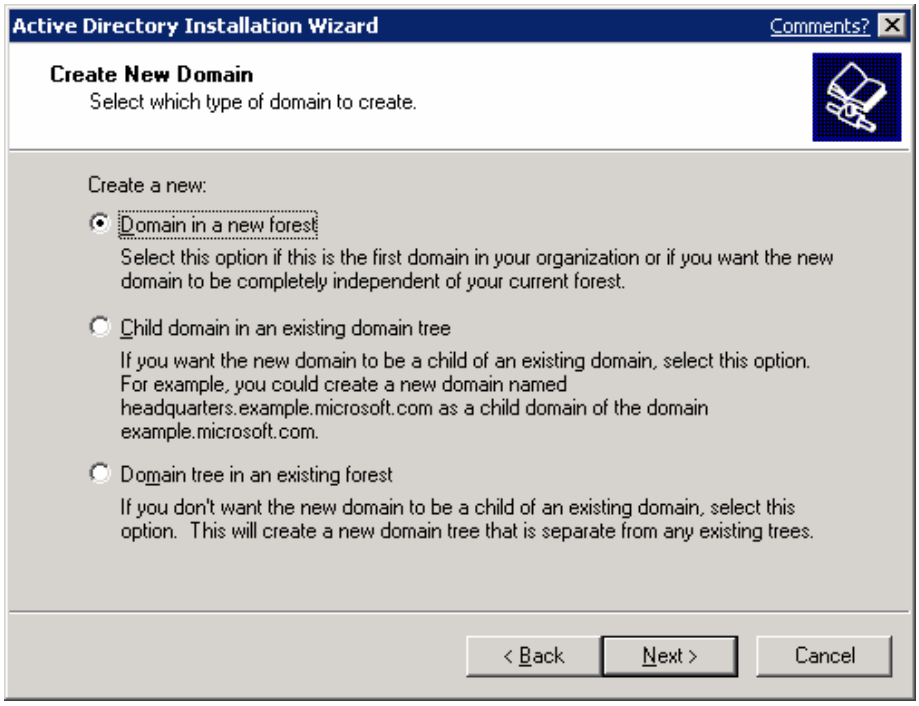
Active Directory 마법사를 실행하기 위하여 Command 라인 화면을 연고 Dcpromo 를 입력합니다. 마법사 시작 화면이 실행되면 다음 버튼을 클릭합니다.



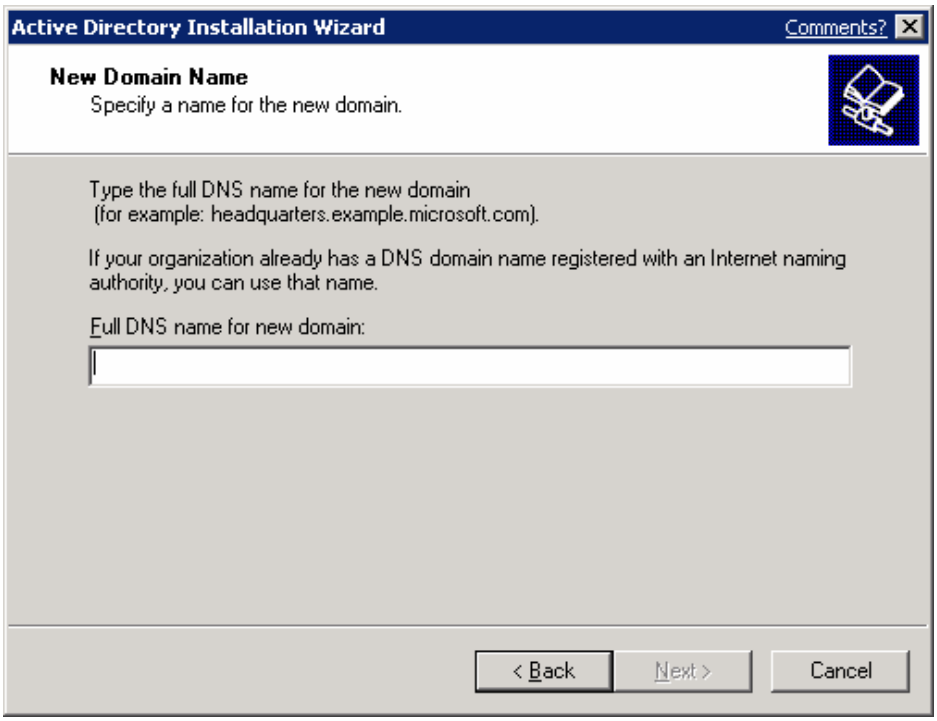
선택: 새로운 도메인을 위한 도메인 컨트롤러(Domain controller for a new domain)을 선택하고 다음 버튼을 클릭합니다.



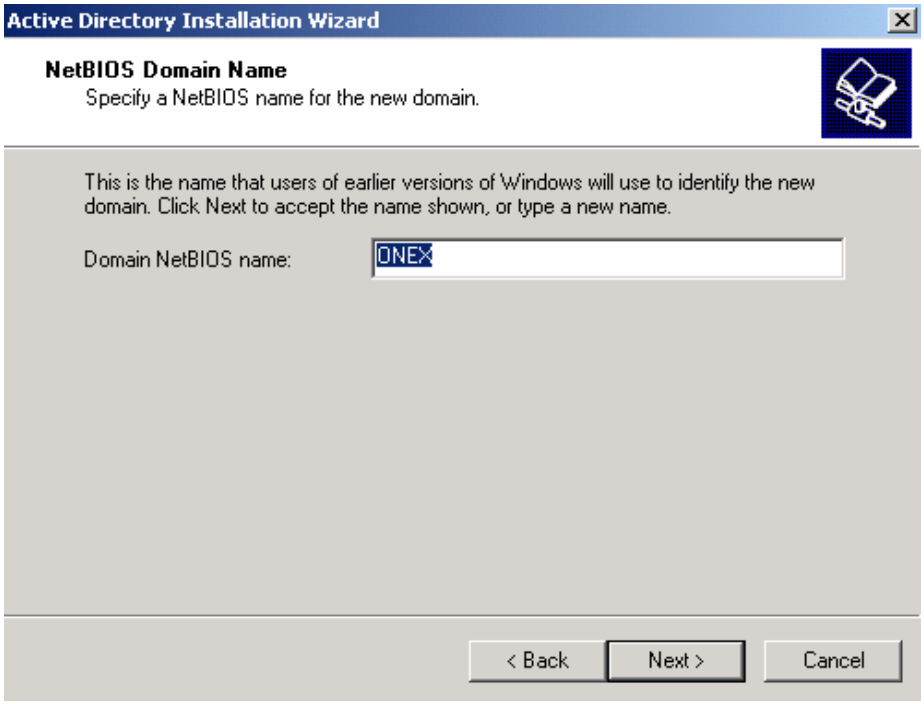
1. 선택: 새로운 포리스트에 도메인을 생성, 다음을 누릅니다.



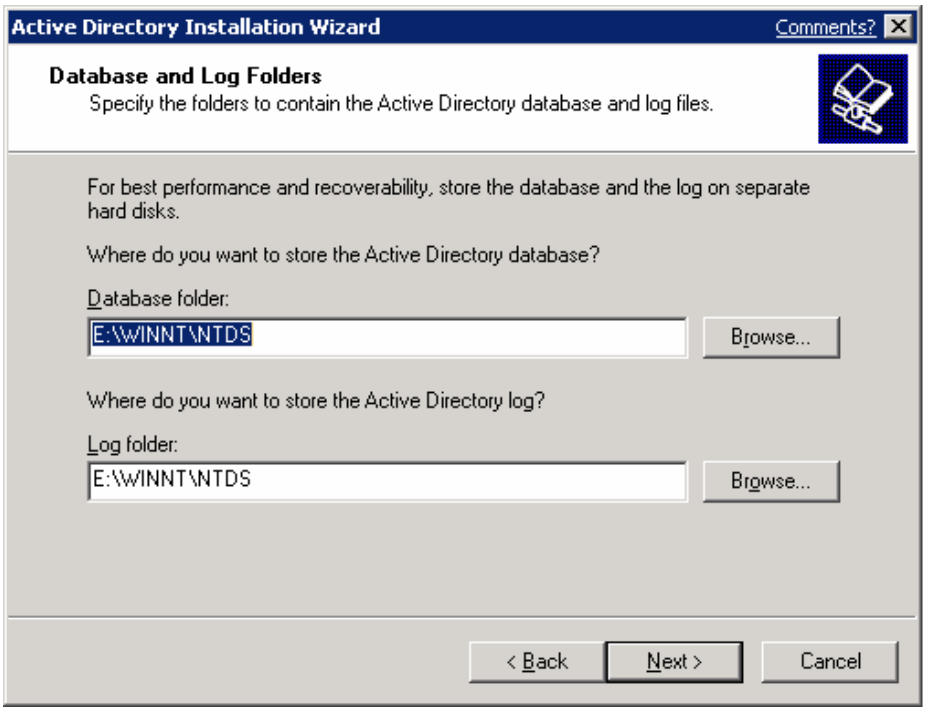
2. 새로운 도메인을 위한 FQDN 을 입력합니다. (ex, Microsoft.com), 다음을 누릅니다.



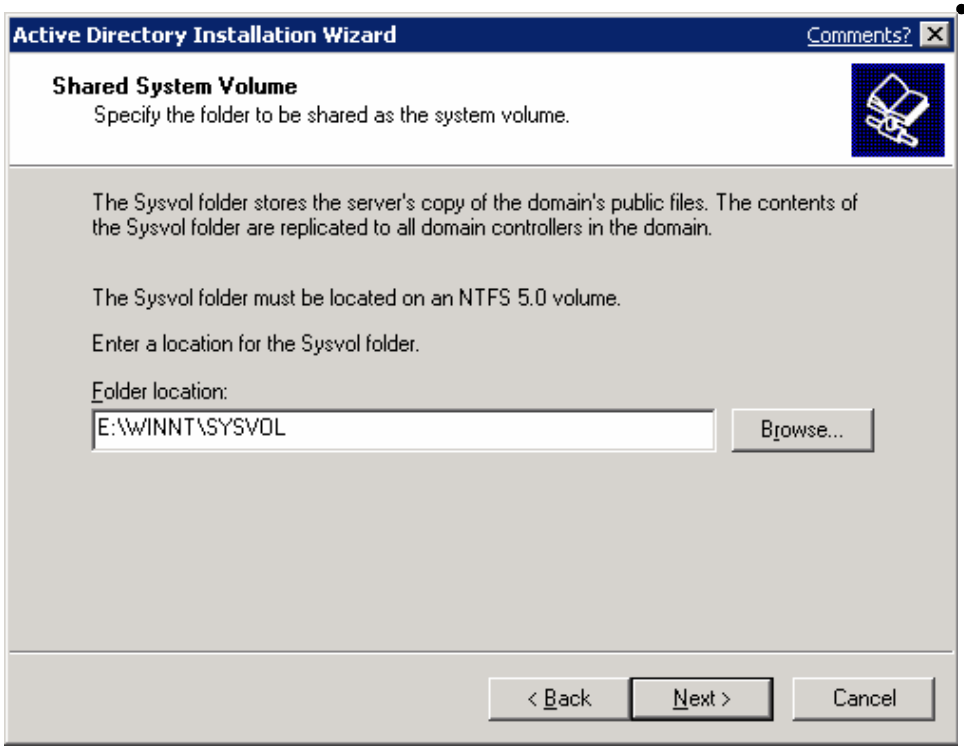
3. NetBIOS 도메인 이름을 입력합니다. (ex, MICROSOFT), 다음을 누릅니다.



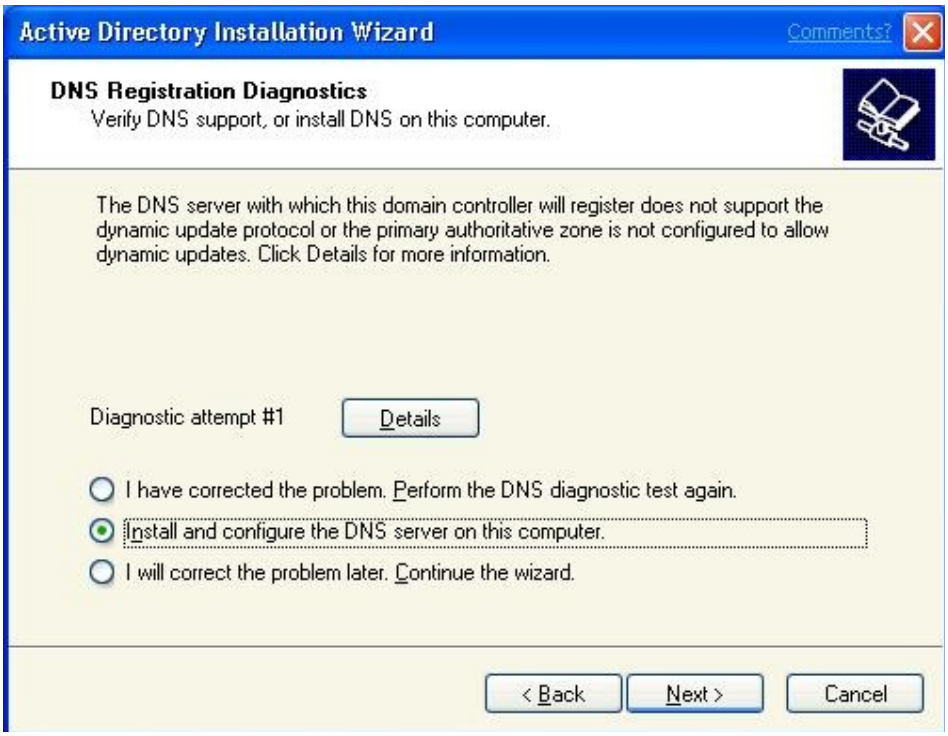
4. 기본값을 수락합니다. 다음을 누릅니다.



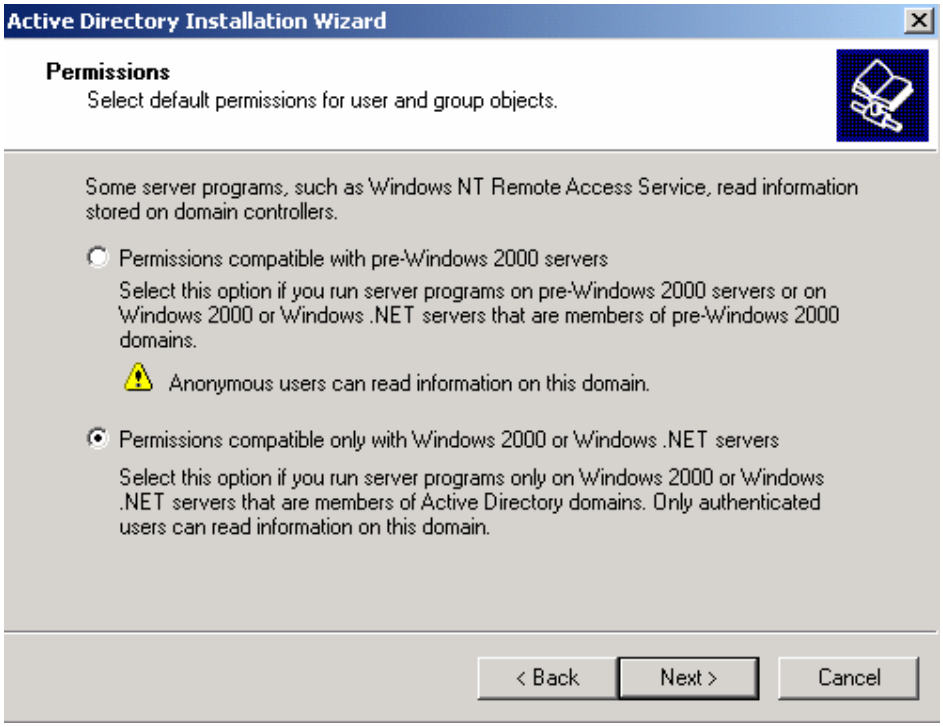
5. 기본값을 수락하고 다음을 누릅니다.



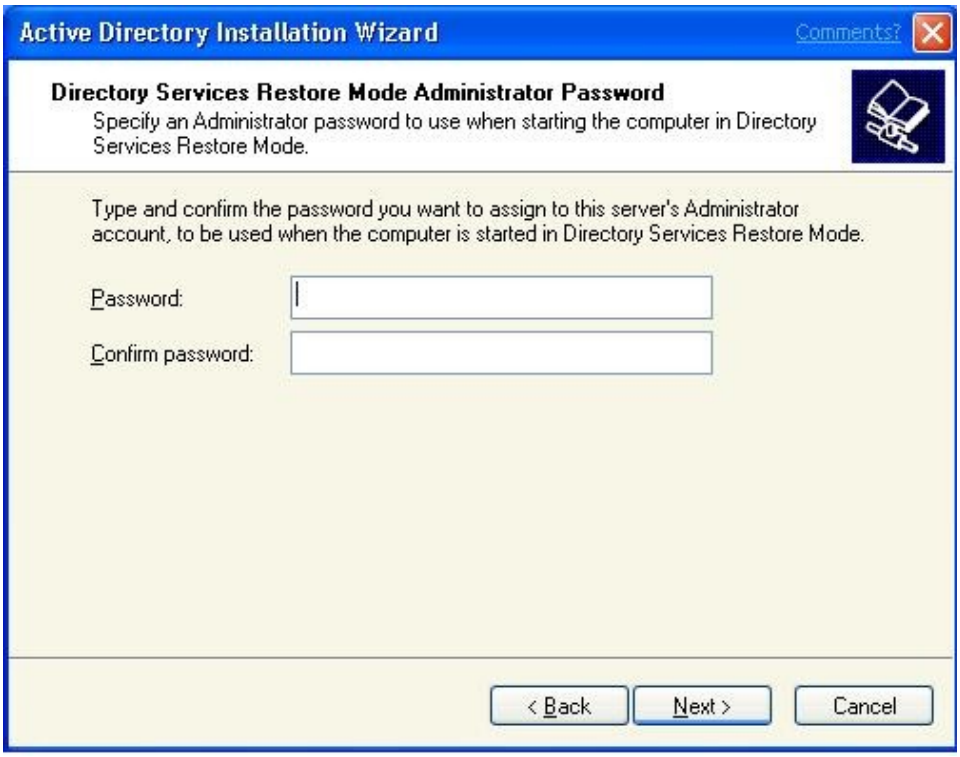
5. DNS 설치



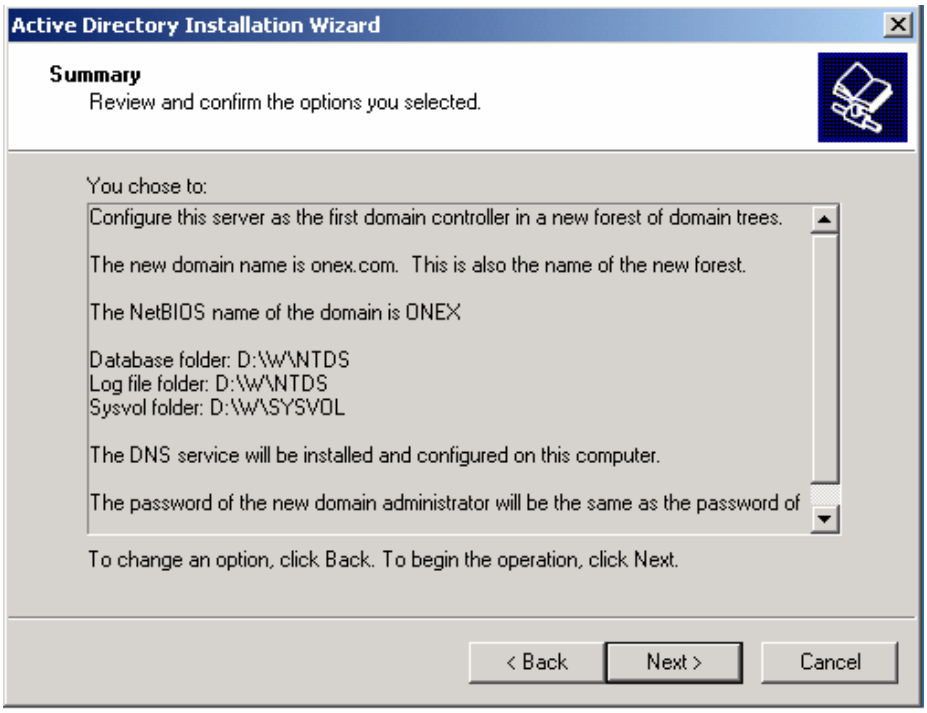
6.선택: Permissions compatible only with Windows 2000 servers. 다음을 누릅니다.



7. 디렉터리 서비스 복구를 위한 관리자 패스워드를 입력하고 다음을 누릅니다.



8.Active Directory 마법사가 데이터베이스 및 로그 파일 세팅을 위한 화면을 보여줍니다. 다음을 누릅니다.



Active Directory 구성을 계속합니다. 이 프로세스는 몇분정도 소요됩니다. Active Directory가 완료되면 완료버튼을 클릭합니다.

9. 아래 화면에 따라서 재 시작합니다.

4-1서비스 설치하고 구성하기

제어판의 프로그램 추가/삭제를 통해서 다음 서비스들을 추가합니다.

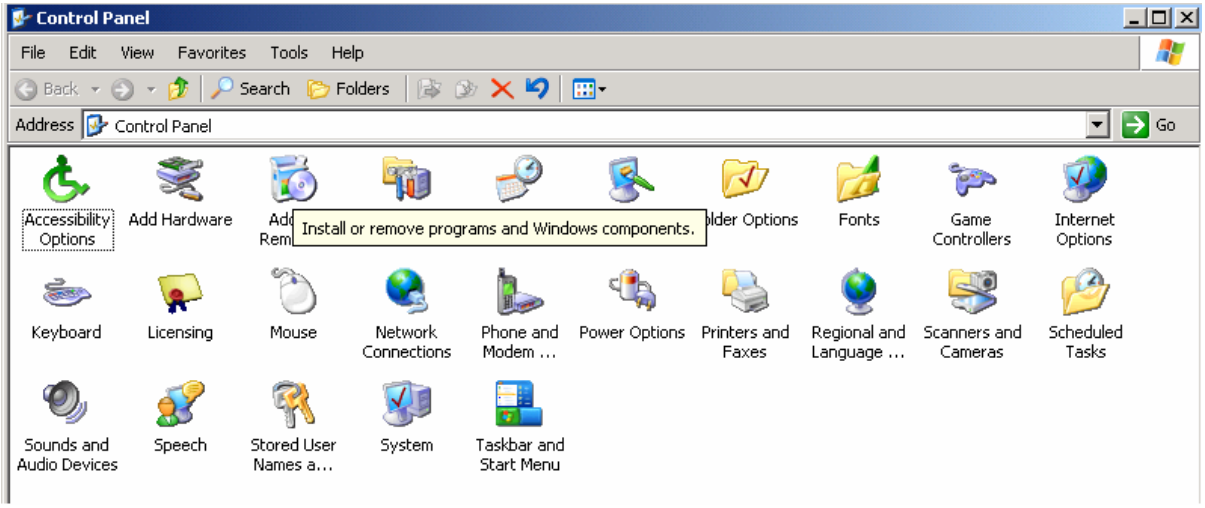
인증서 서비스 (Certificate services)

Internet Information Services – IIS

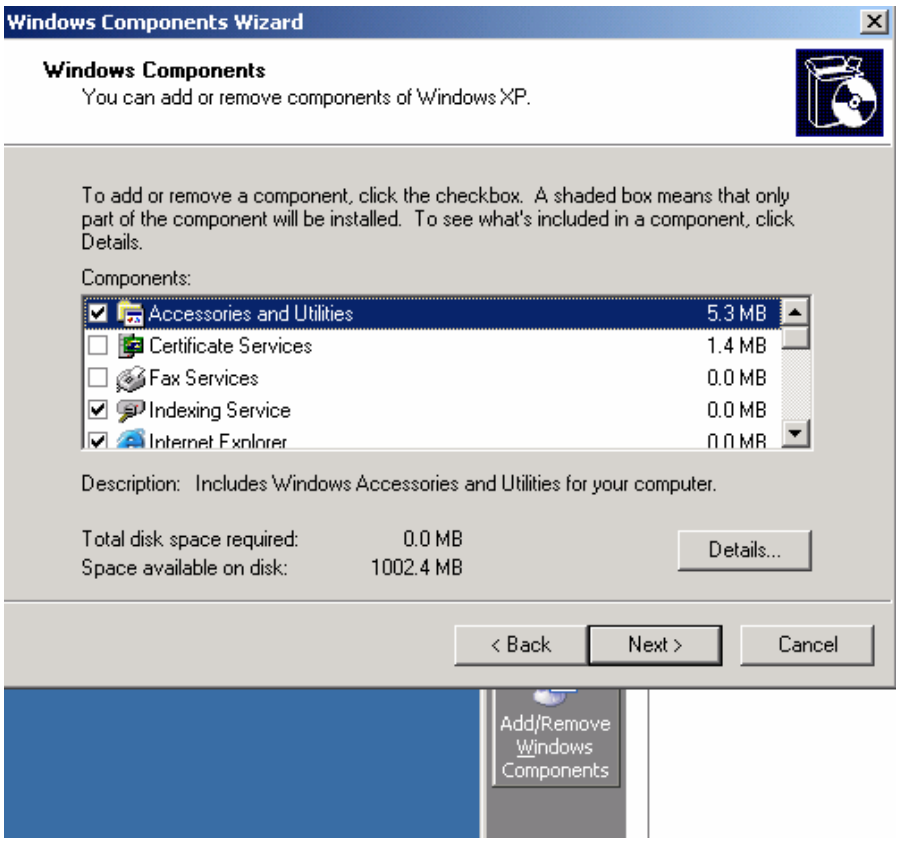
네트워킹 서비스에 속해있는: Internet Authentication Service (IAS)

Note: 만약에 IIS가 선택되어 있으면 서비스가 이미 시작된 것입니다.

1. 제어판을 엽니다.
   시작 → 세팅 → 제어판

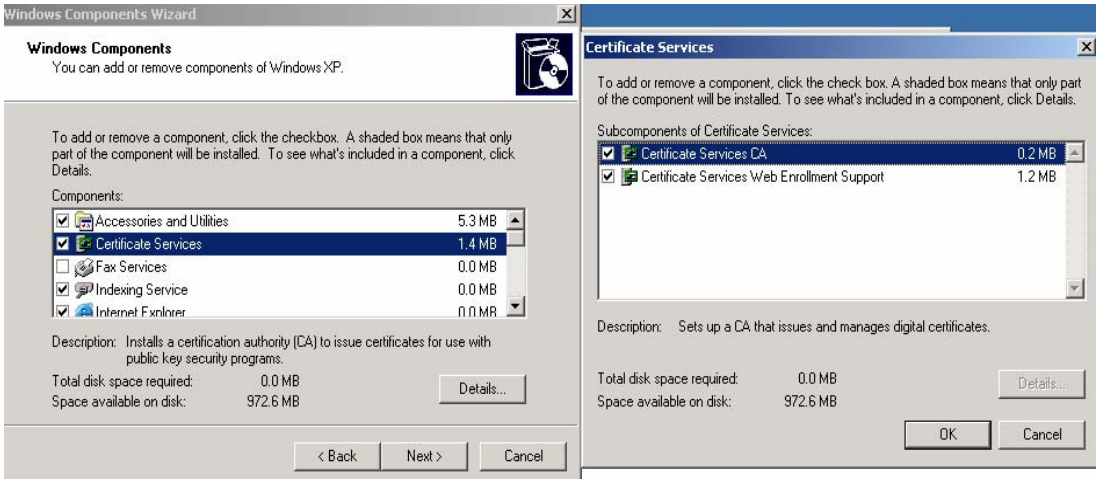


2.프로그램 추가/삭제를 더블 클릭하고 윈도우 구성요소 마법사를 실행하기 위하여 윈도우 컴포넌트 추가/삭제를 클릭합니다.



3.다음 구성요소를 설치합니다.

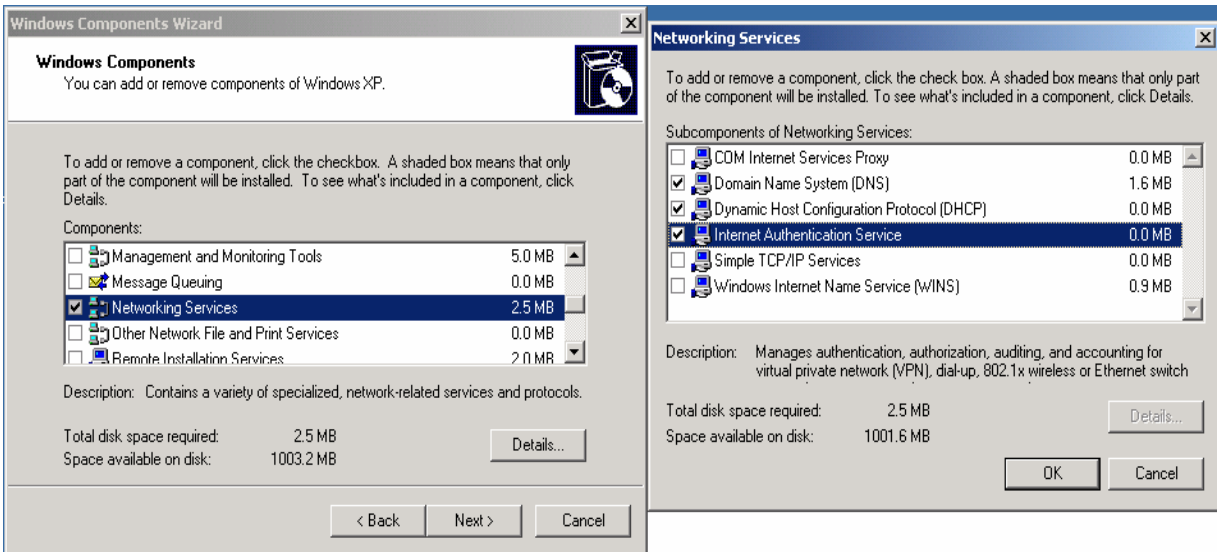
인증서 서비스



4.왼쪽의 인증서 서비스박스를 선택하고 자세히(details) 버튼을 클릭합니다. 이 버튼을 클릭하면 하부 구성요소 윈도우가 열리게 되고 모든 구성요소를 선택한 다음 확인 버튼을 클릭합니다.

5.다음, 네트워킹 서비스를 선택하고 하부 컴포넌트를 보기 위하여 자세히(detail)버튼을 클릭합니다. 하부 구성요소 화면세어 DNS, DHCP, Internet Authentication 서비스가 모두

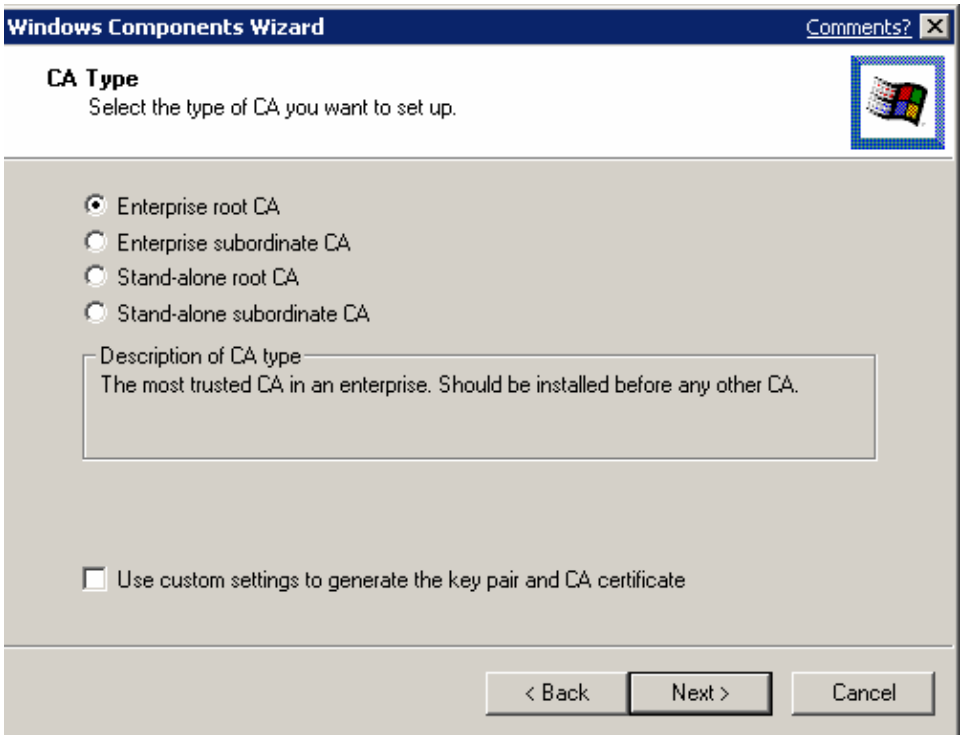
선택되었는지 확인하고 확인 버튼을 누릅니다. 그리고 윈도우 구성요소 창에서 다음 버튼을 누릅니다.



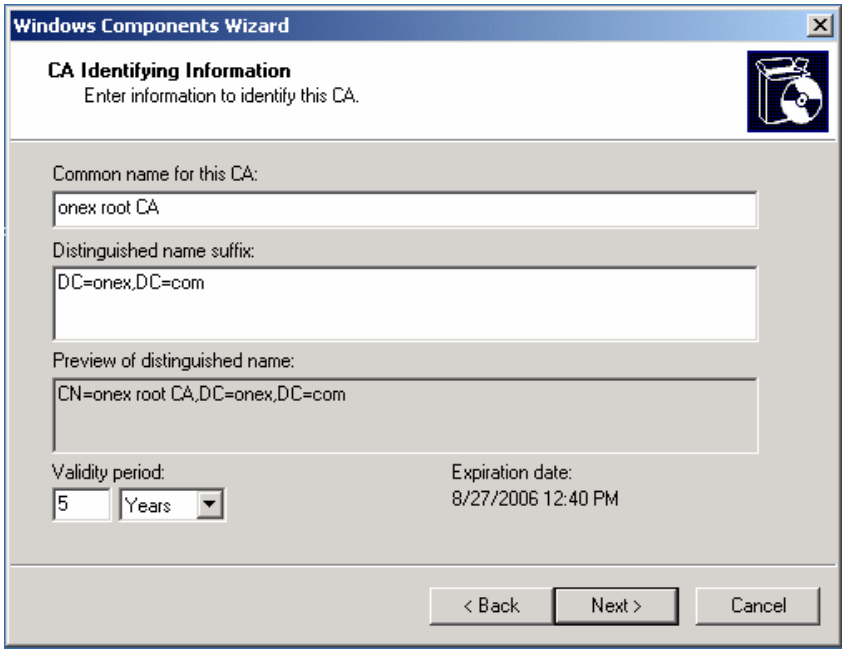
6.구성요소 마법사는 선택된 구성요소를 설치하기 위하여 프로세싱합니다.

인증서 서비스 설치 화면

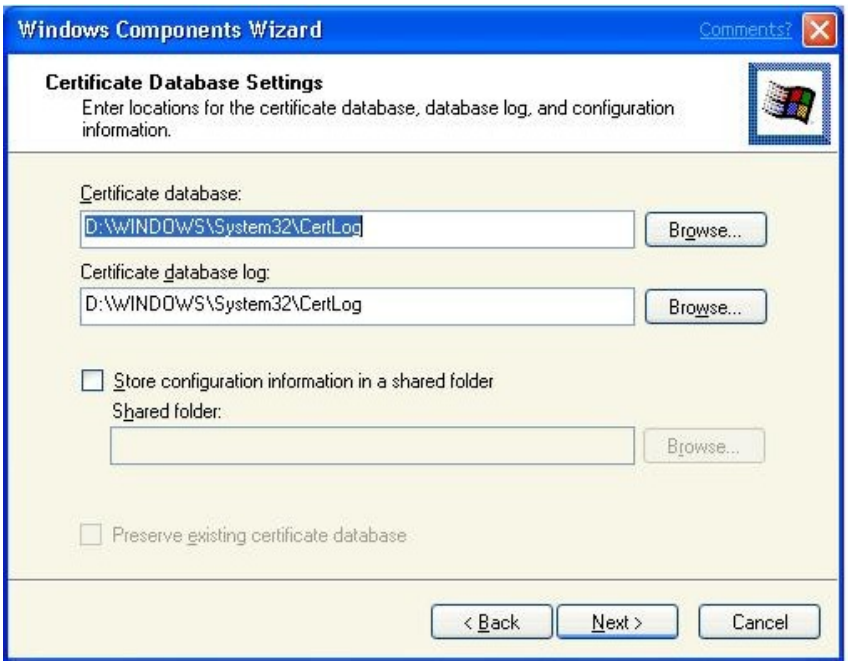
7.엔터프라이즈 루트 CA 를 선택하고 다음버튼을 클릭합니다.



8. CA 정보를 입력하고 다음 버튼을 클릭합니다.

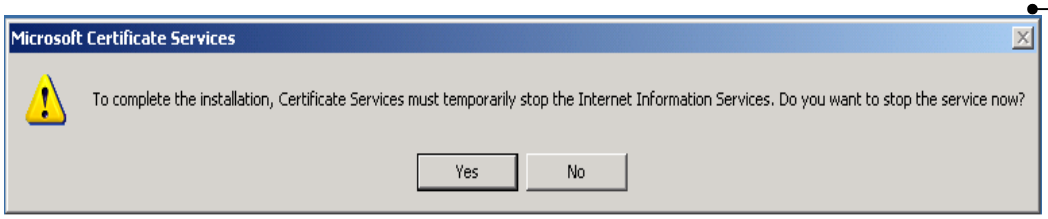


9. 기본값을 수락하거나 데이터 저장 장소를 다르게 입력합니다. PATH 또는 UNC Path 를 사용해야 합니다.

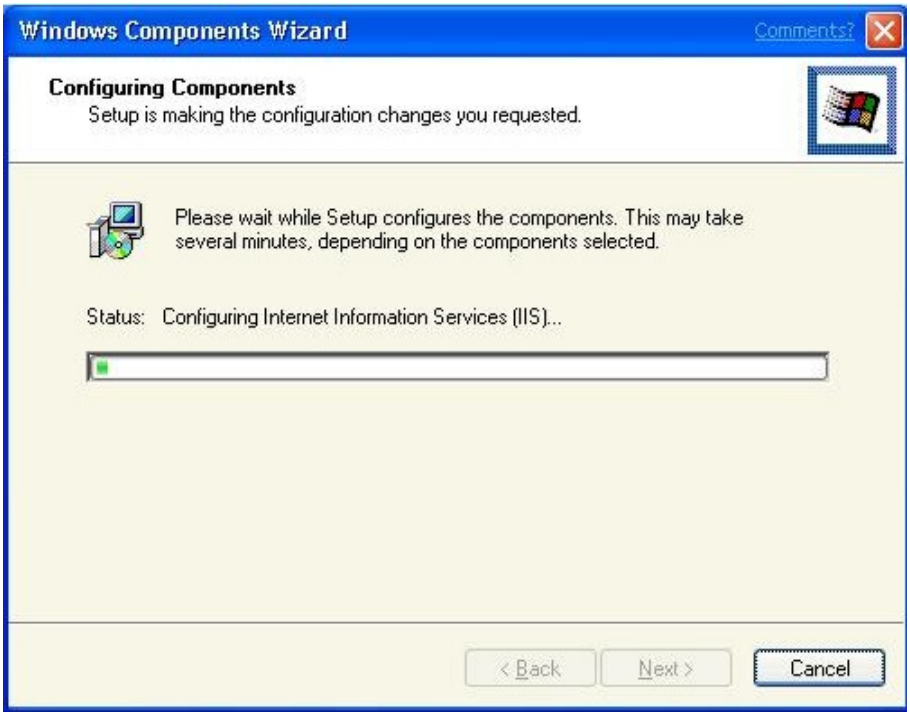


10.다음을 클릭하고 완료 버튼을 누릅니다.

Note: Certificate Service 구성을 완료합니다.



11. 윈도우 구성요소 마법사가 IIS 를 구성하도록 예(Yes)를 클릭합니다.

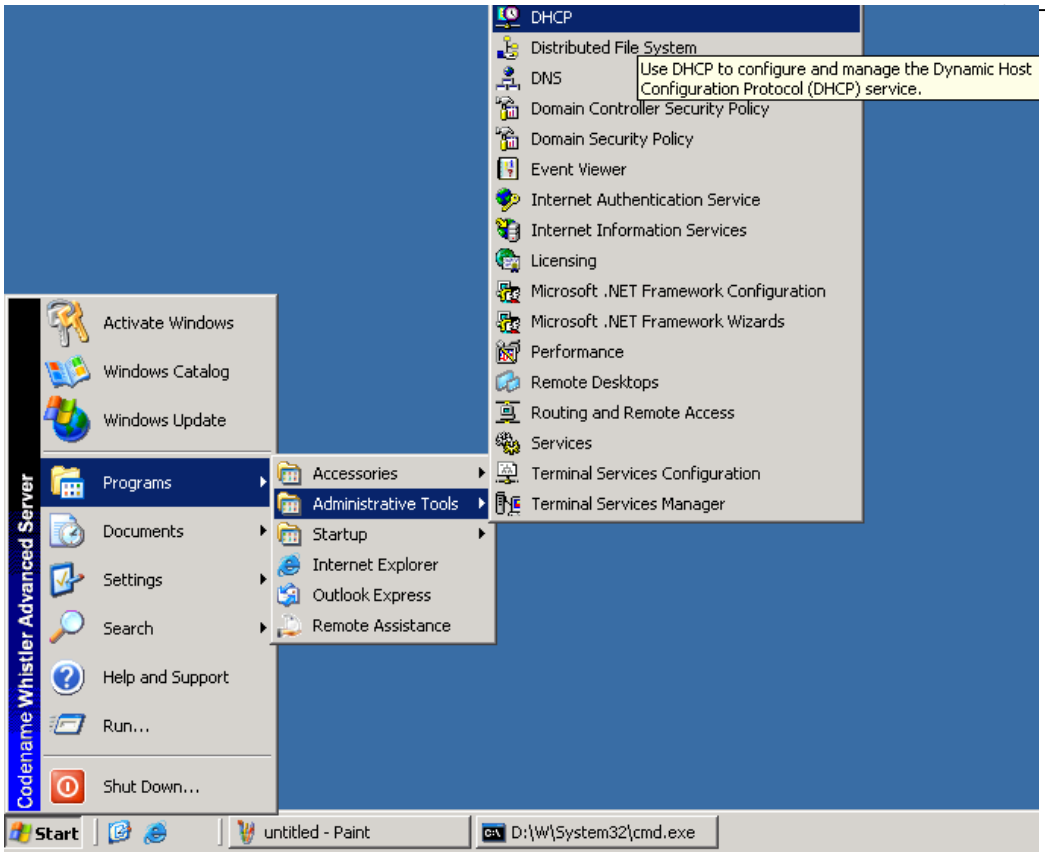


12. 마법사의 완료버튼을 눌러서 설치를 완료합니다.

4-2 DHCP 서버 구성하기

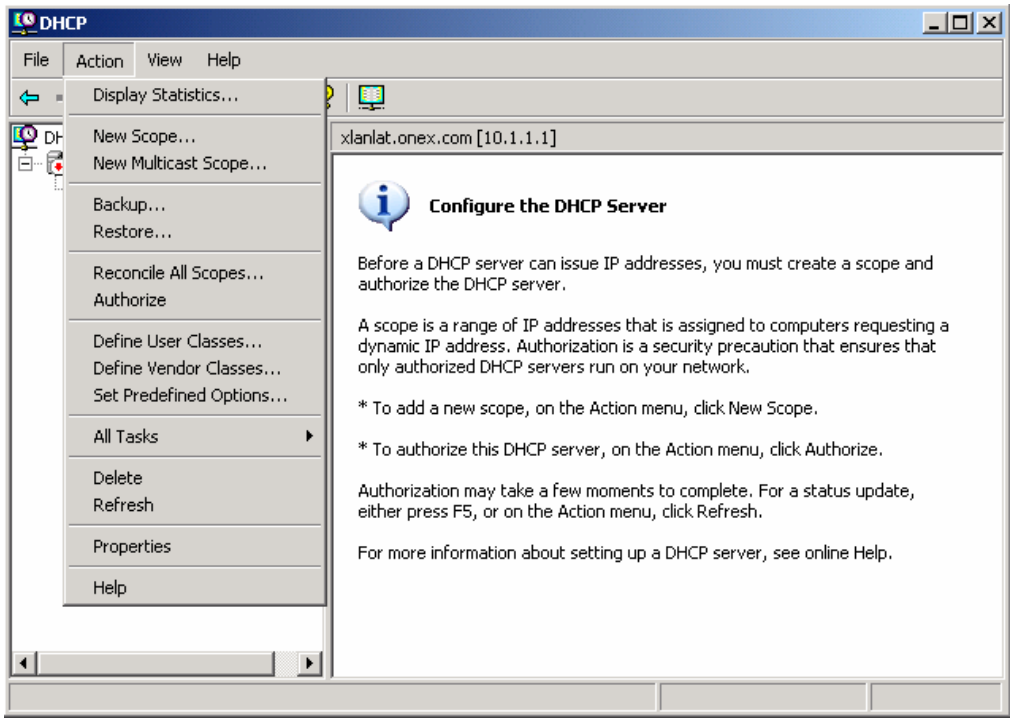
로컬 네트워크 영역에 IP 주소를 입력하지 않았다면 정적 주소를 입력하기 위하여 앞부분에 설명되어 있는 “Windows Server 2003 설치하기”로 돌아갑니다.

1. DHCP 서비스를 엽니다. 시작 → 프로그램 → 관리 도구 → DHCP.

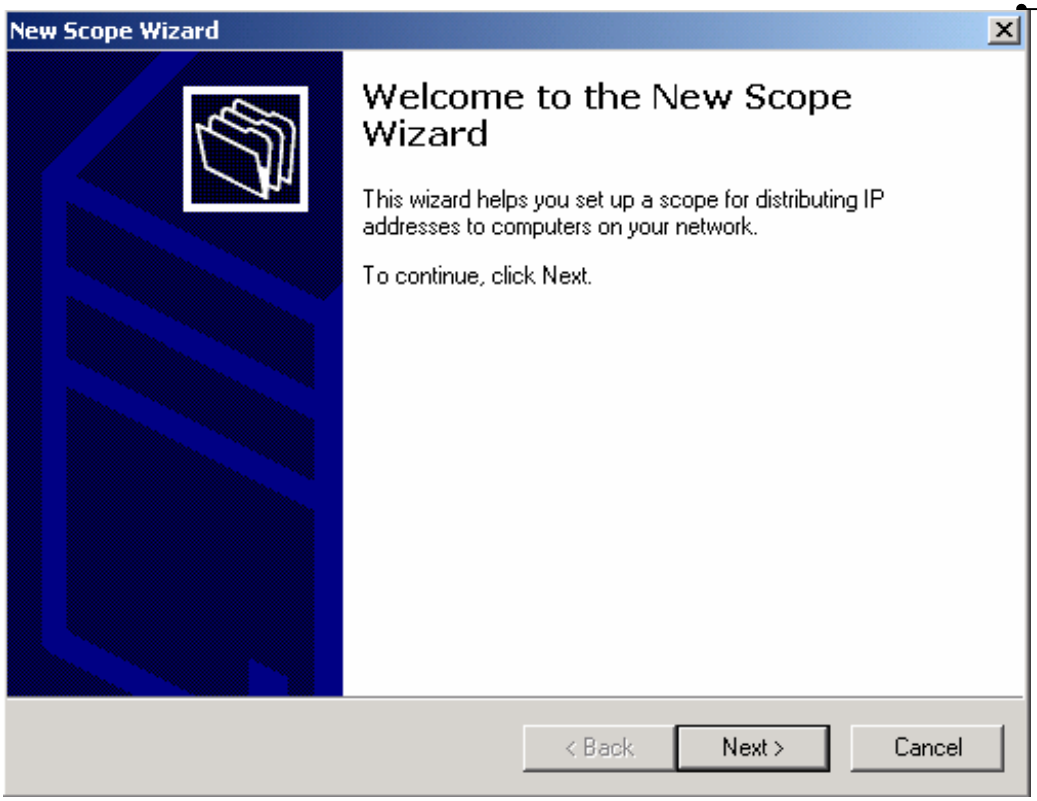


2. 단일 영역을 생성합니다 –예) 10.1.1.2 – 10.1.1.254

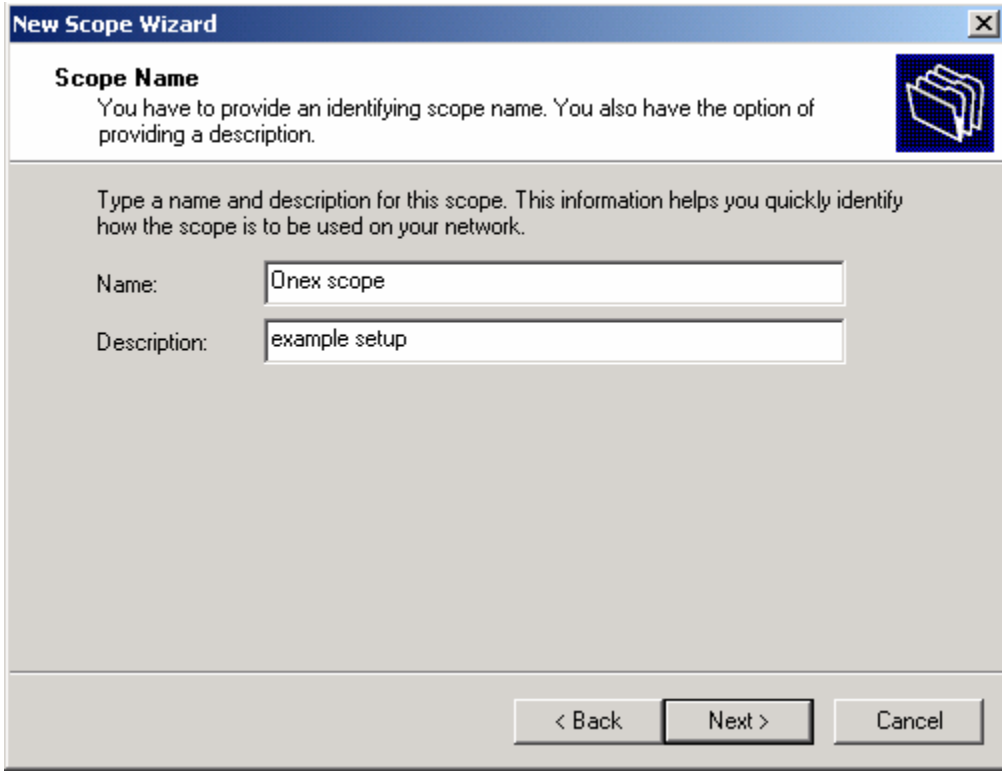
서버 이름을 하이라이트하고 Action –> 새로운 영역 (New scope)을 클릭합니다.



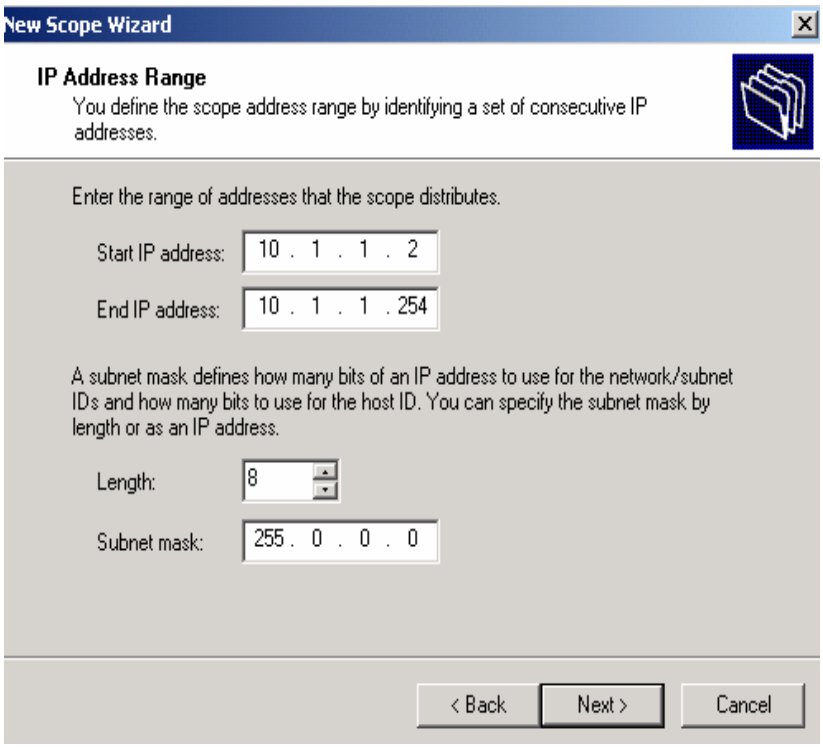
3.새 영역 마법사가 실행되면 다음 버튼을 누릅니다.



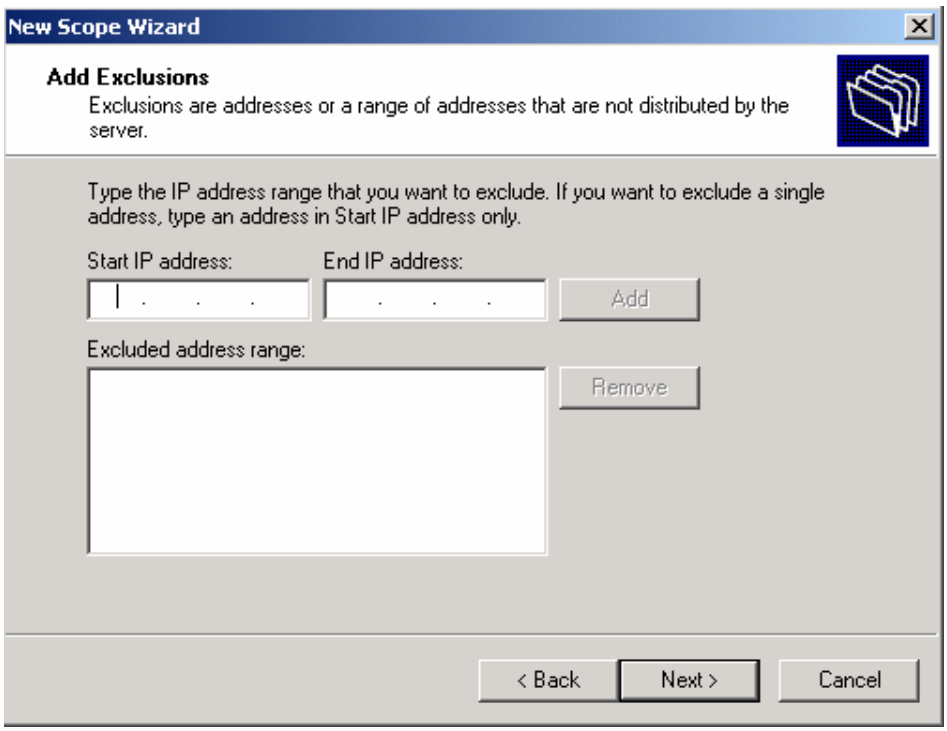
4. 영역 이름과 적절한 설명을 입력하고 다음을 클릭합니다. , and description, click next.



5. IP 주소 범위를 입력합니다. (같은 서브넷위에 서버 주소가 있어야 합니다.)

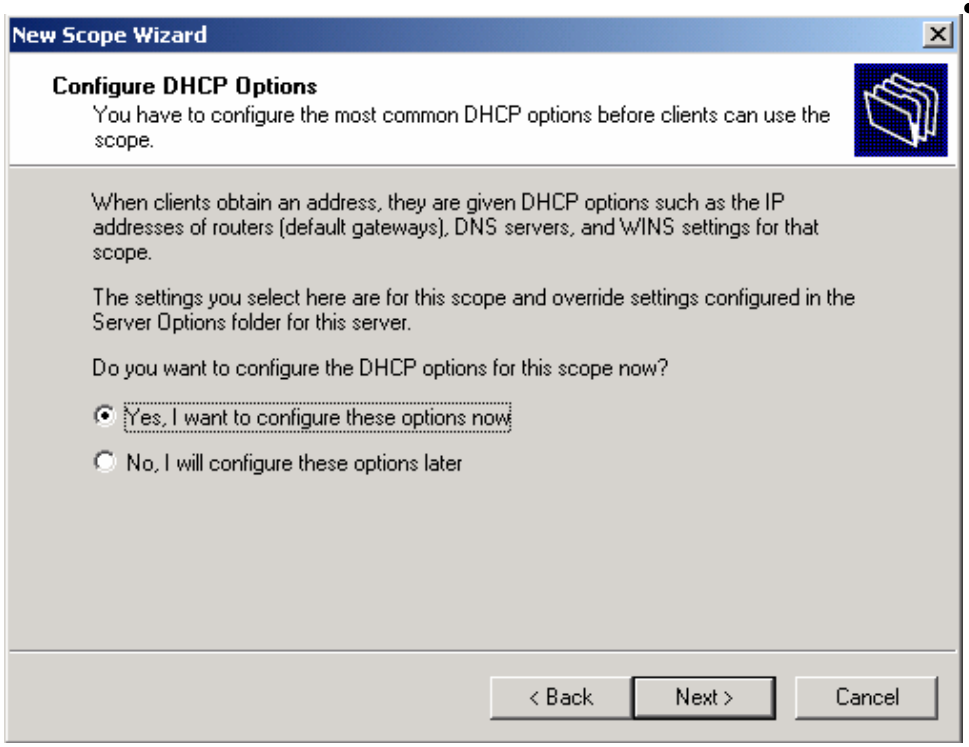


6. 주소 범위 참에서 제외(exclusion)를 클릭합니다. 이 제외 안에는 Access Point, 스위치 등이 가지고 있는 정적 주소가 포함되어야 합니다.) 입력을 완료한 다음, 다음 버튼을 클릭합니다.



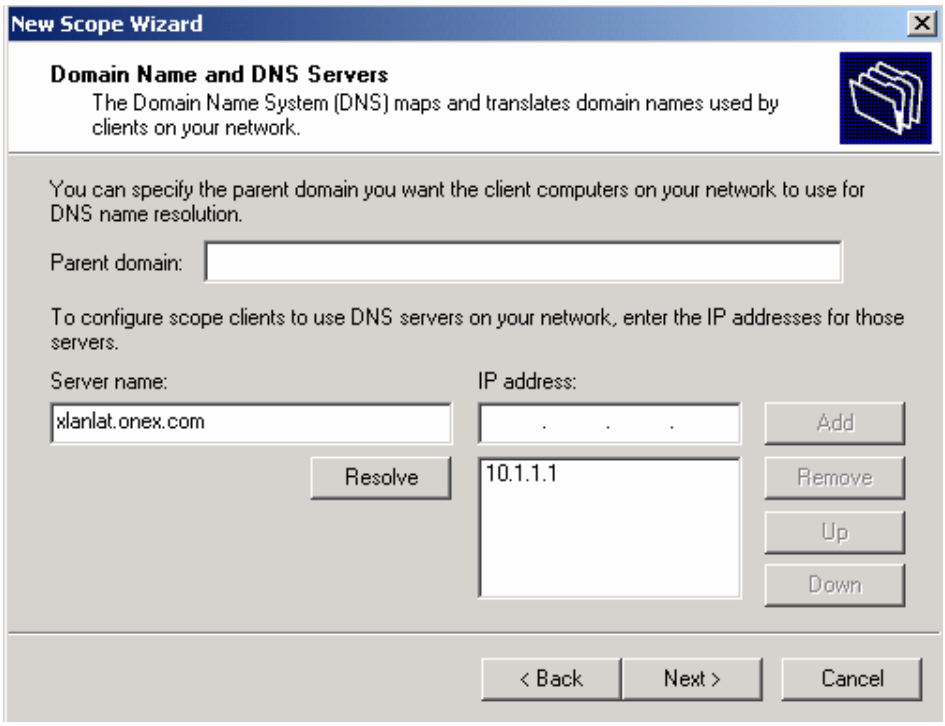
7. 대여 기간을 입력하거나 기본값을 수락하고 다름을 클릭합니다.

8. DHCP 옵션을 선택하고 다음을 클릭합니다.



9. Router default gateway – 802.1X 테스트에는 이 옵션이 필요하지 않습니다. 다음을 클릭합니다.

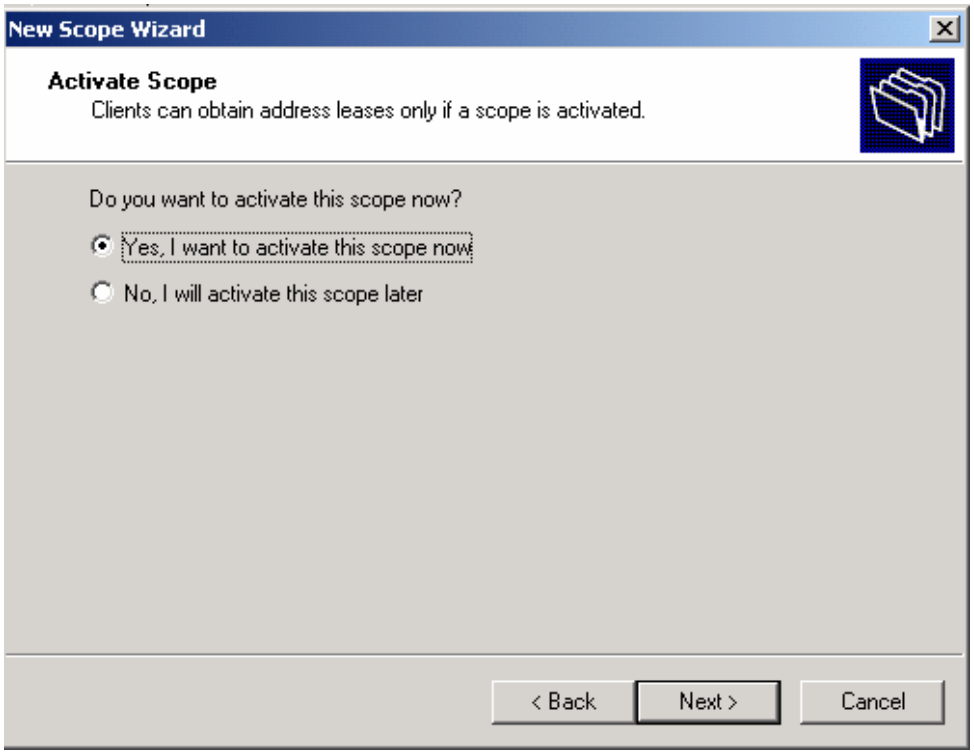
10. 도메인 이름 및 DNS 세팅
부모 도메인(Parent domain)란은 입력하지 않아도 되지만 서버이름과 IP 주소를 입력하고 추가버튼을 누릅니다.



11.Wins 는 1X 테스트라면 입력할 필요가 없습니다. 다음을 클릭합니다.

12.만들어진 영역을 활성화 합니다. .

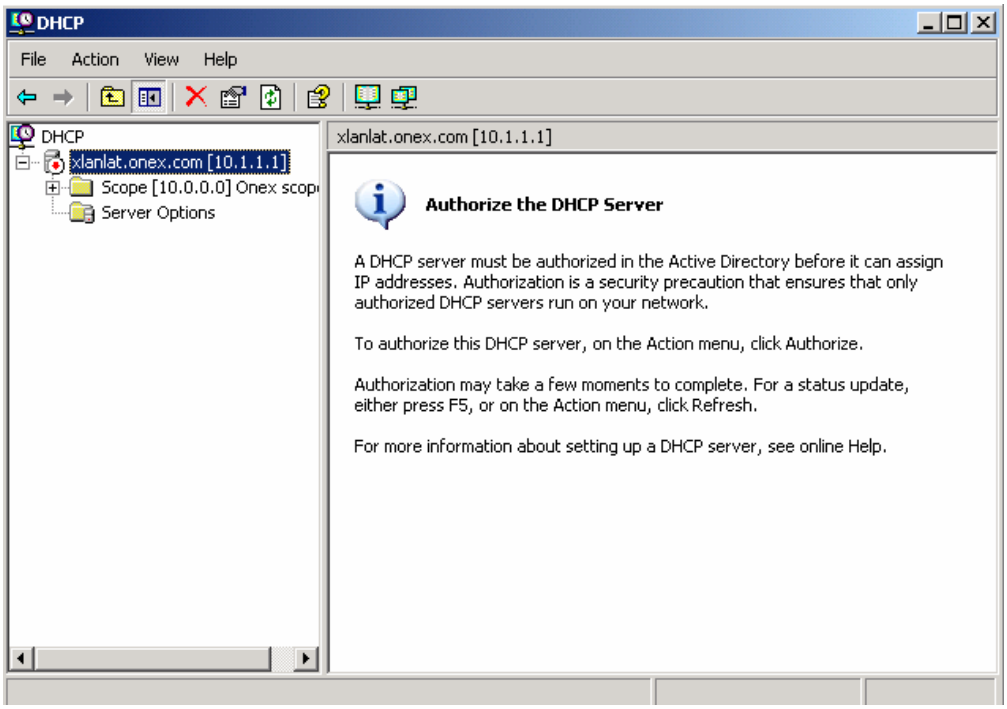
예, 이 영역을 활성화 하고자 합니다.(Yes, I want to active this scope) 를 선택하고 다음을 클릭합니다.



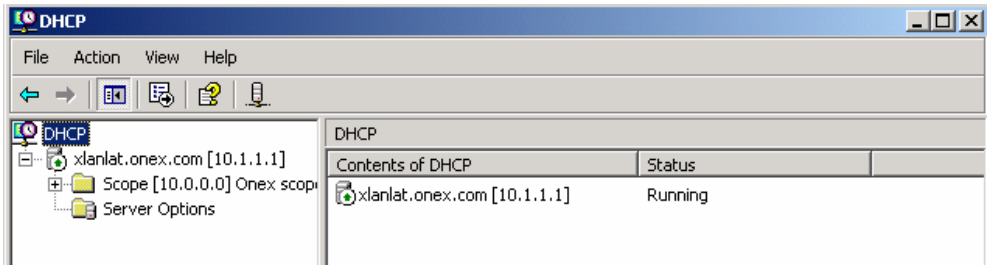
13.완료버튼을 클릭합니다.

14.서버 인증하기

서버 이름을 하이라이트 하고 Action -> Authorize를 클릭합니다. 화면을 갱신하기 위하여 몇 분 정도 소요될 수 있습니다.



15.서버에 인증하고 난 후 서버에 초록색 화살표가 있는 것을 볼 수 있습니다. 서비스가 아무런 문제없이 동작하고 있음을 나타냅니다.

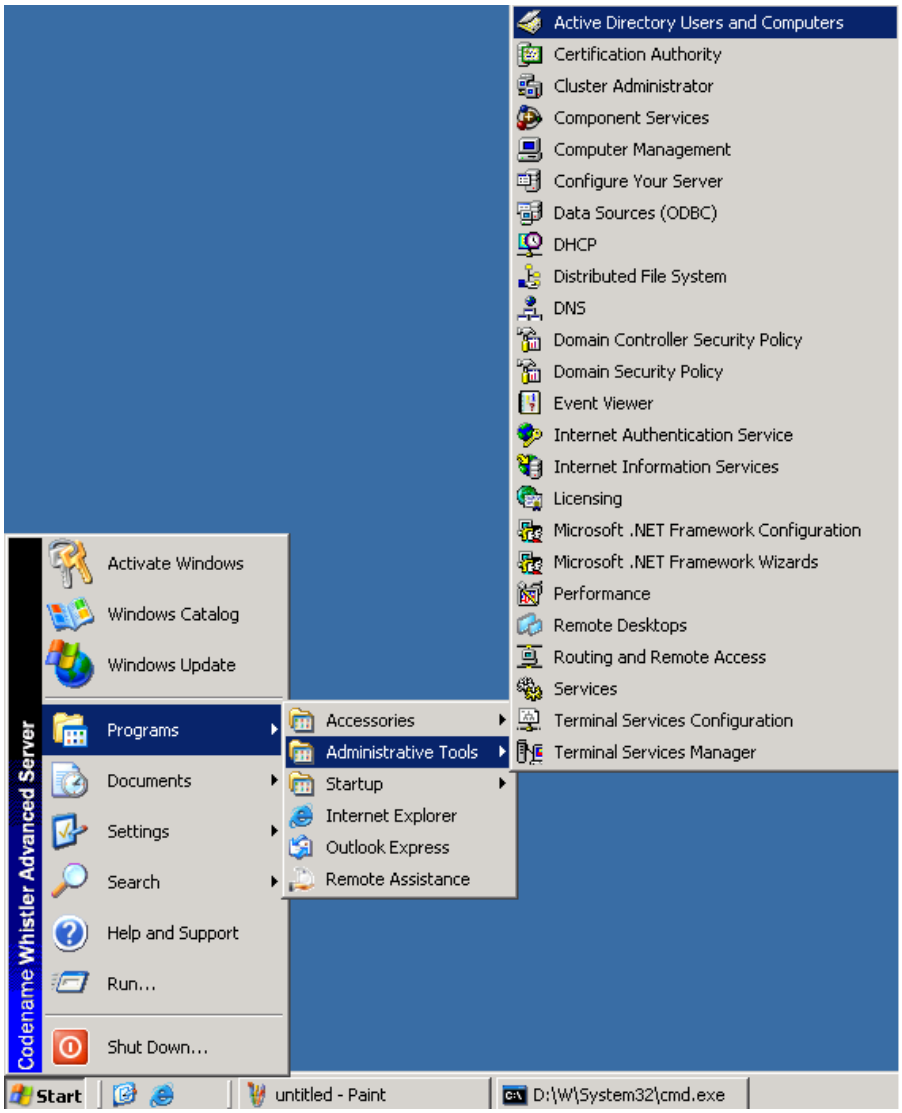


16.DHCP server 를 닫고 클라이언트가 서버로부터 받은 사설 네트워크에 있음을 확인합니다. IPConfig/release, IPconfig/renew 명령어를 사용합니다.

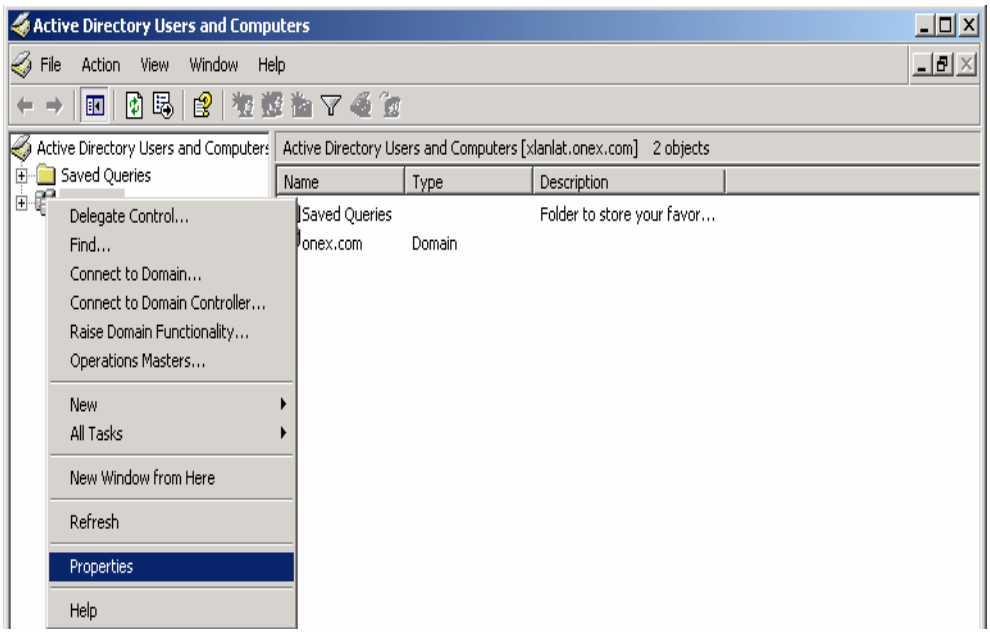
4-3 MD5 알고리즘을 위하여 Active Directory 구성하기

DC를 위해서 모든 사용자의 패스워드가 reversible encryption되어 저장될 수 있도록 구성할 필요가 있습니다.

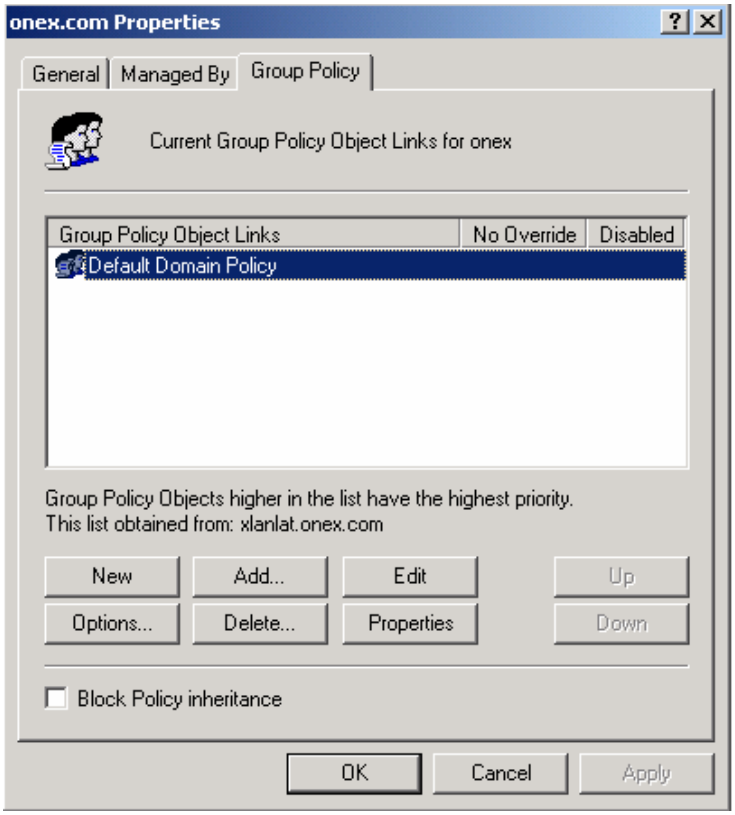
1. Active Directory 사용자 및 컴퓨터를 실행합니다.
   시작 → 프로그램 → 관리 도구 → Active Directory 사용자 및 컴퓨터.



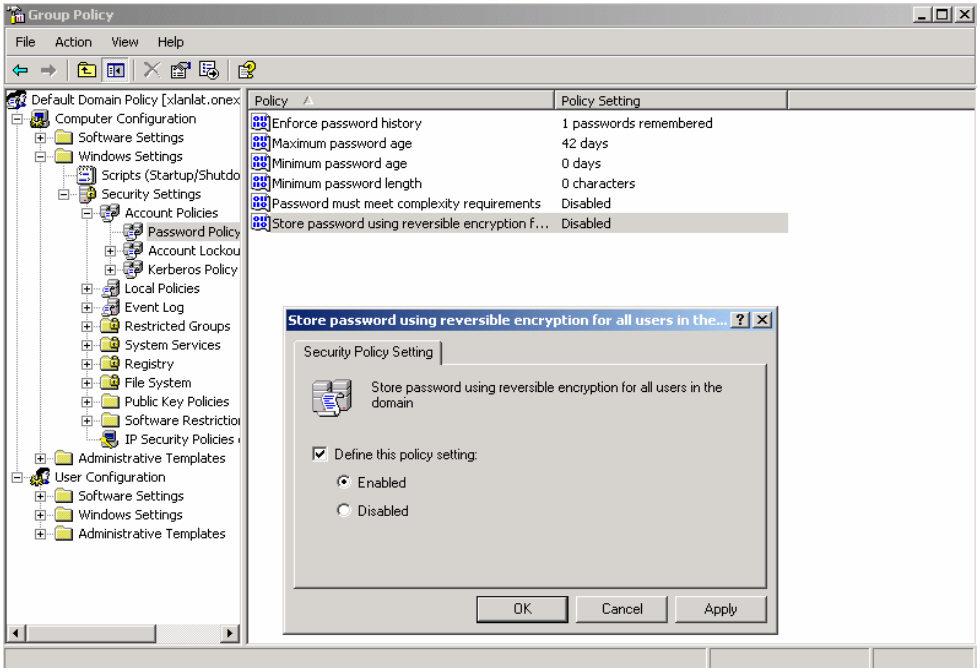
2.도메인 이름을 오른 버튼 클릭하고 속성을 누릅니다.



3.속성화면에서, 그룹정책 탭을 클릭하고 Default Domain 정책을 클릭한 다음 편집 버튼을 클릭합니다.



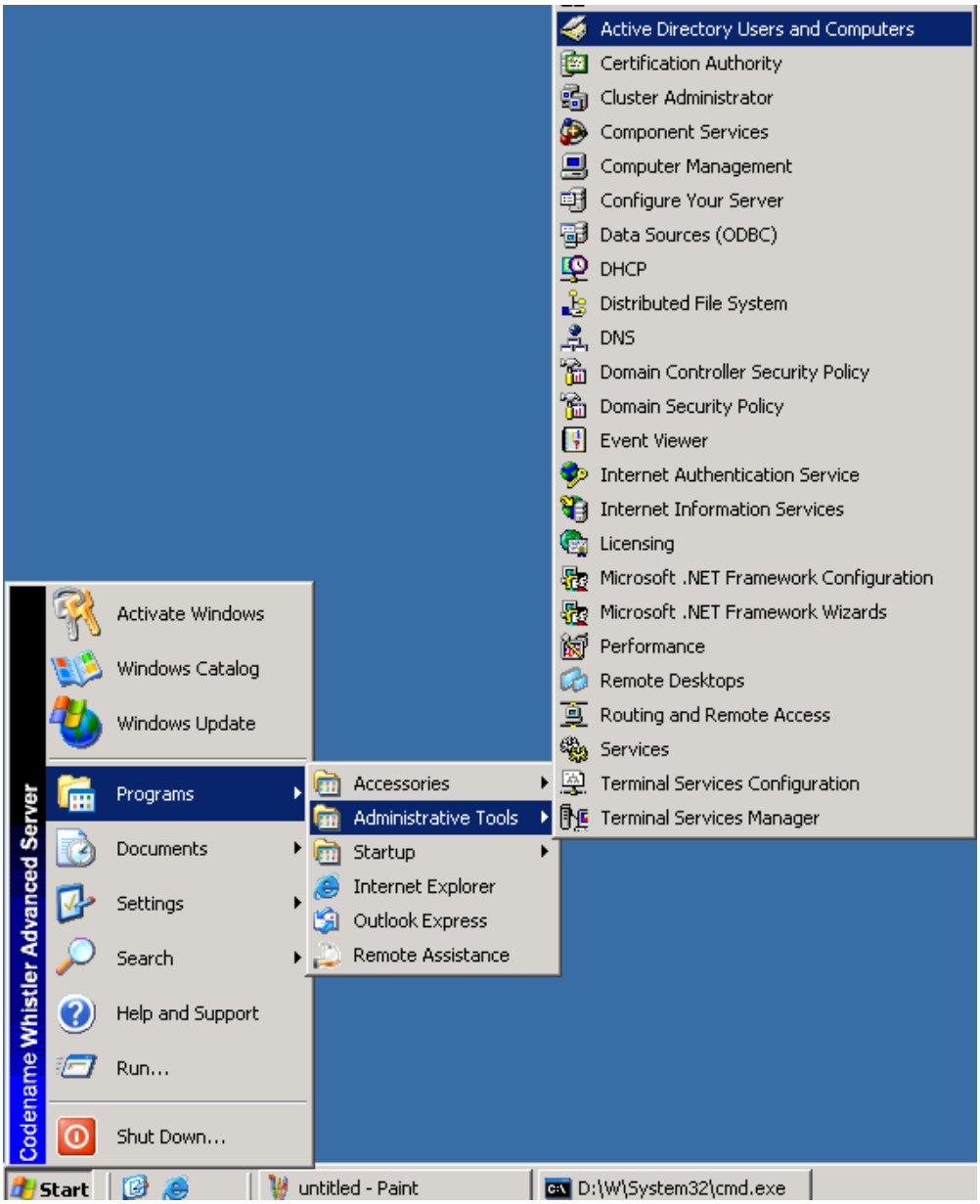
4.Store password using reversible encryption 을 오른 버튼 클릭합니다. Enable -> 확인 -> 확인 Active Directory 화면을 닫습니다.



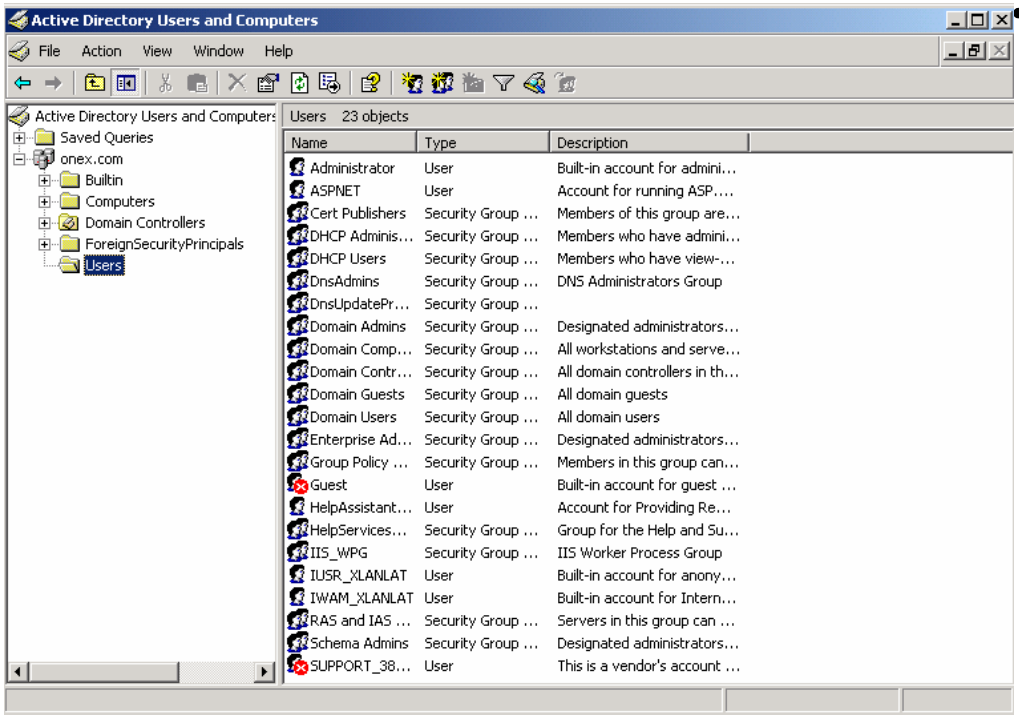
4-4 사용자 생성하기

1. Active Directory 사용자 및 컴퓨터를 실행합니다.

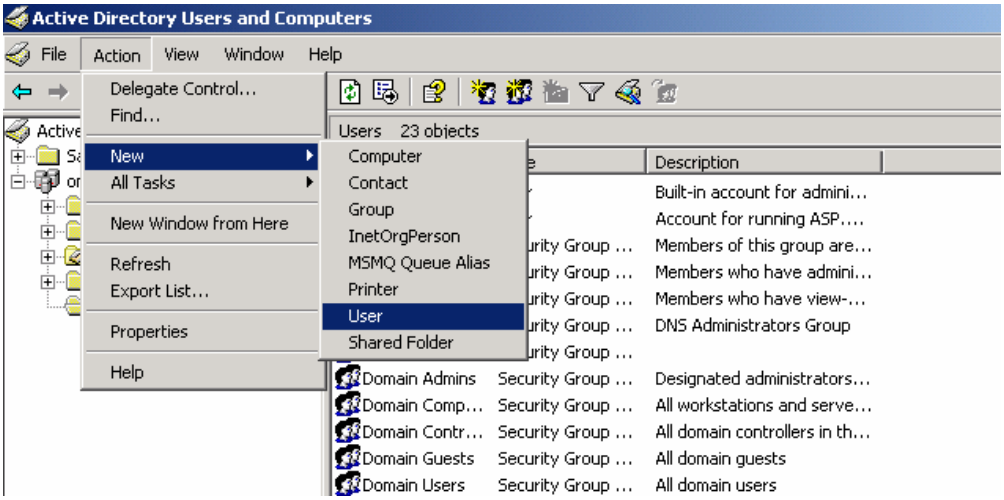
시작→ 프로그램 → 관리도구 → Active Directory 사용자 및 컴퓨터



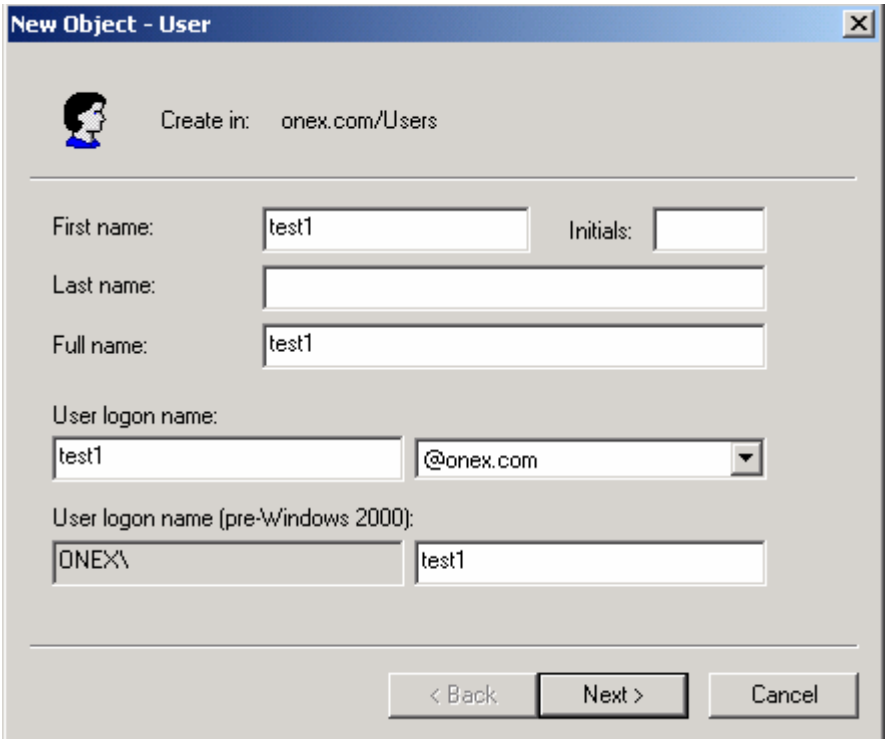
2. 도메인 이름을 확장 하고 사용자를 하이라이트 합니다.



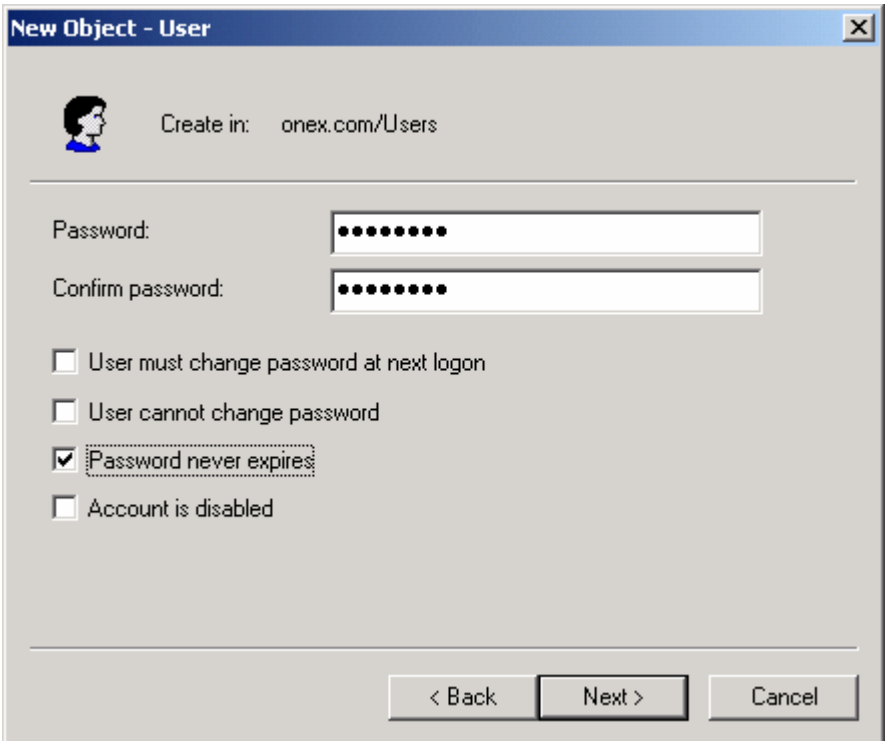
3. Action → 추가 → 사용자를 클릭합니다. .



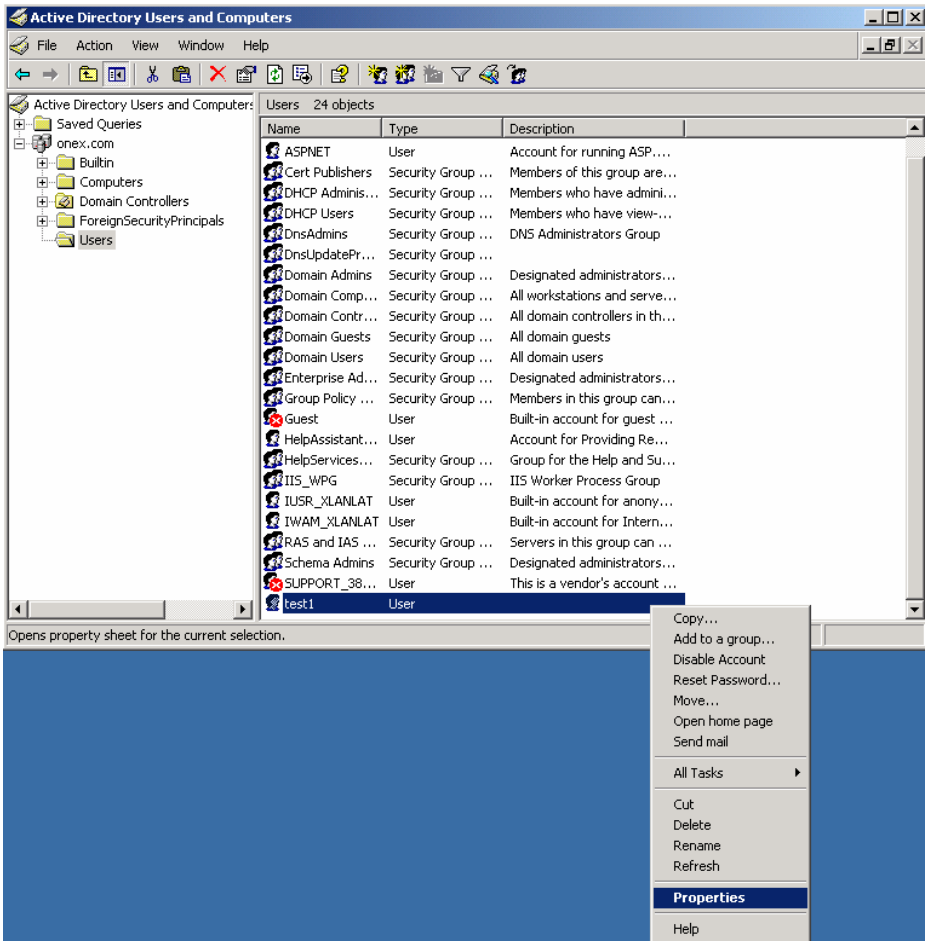
4. 사용자 정보를 입력하고 다음을 클릭합니다.



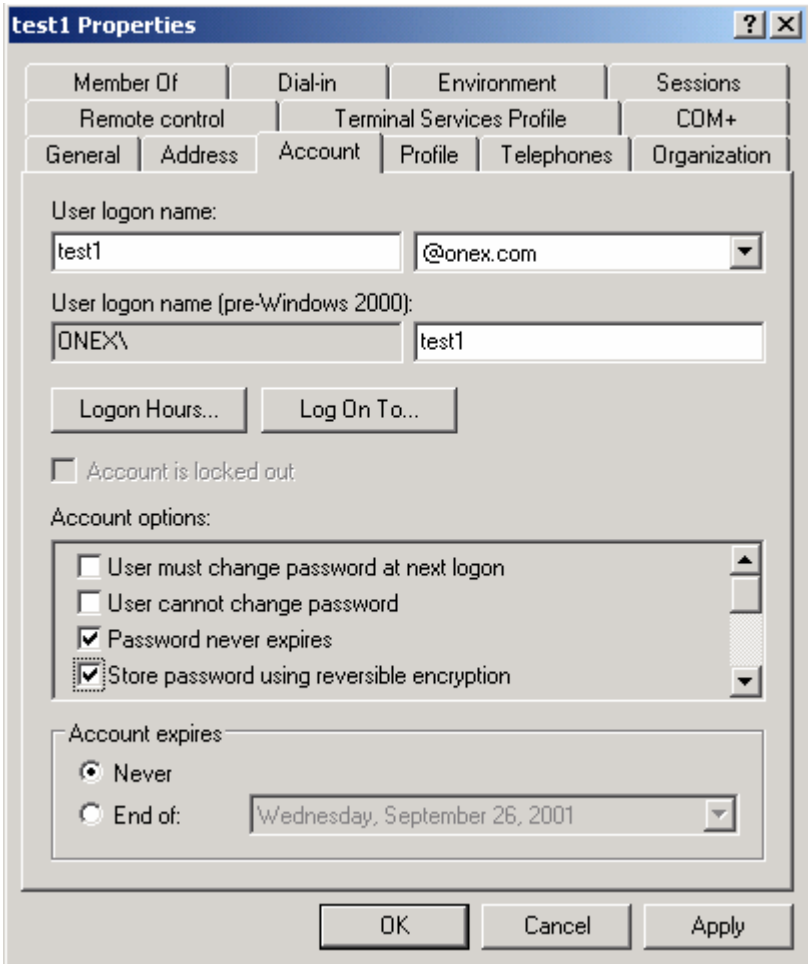
5. 패스워드, 패트워드 확인 란에 패스워드를 입력하고 다음을 누른 다음 완료합니다.



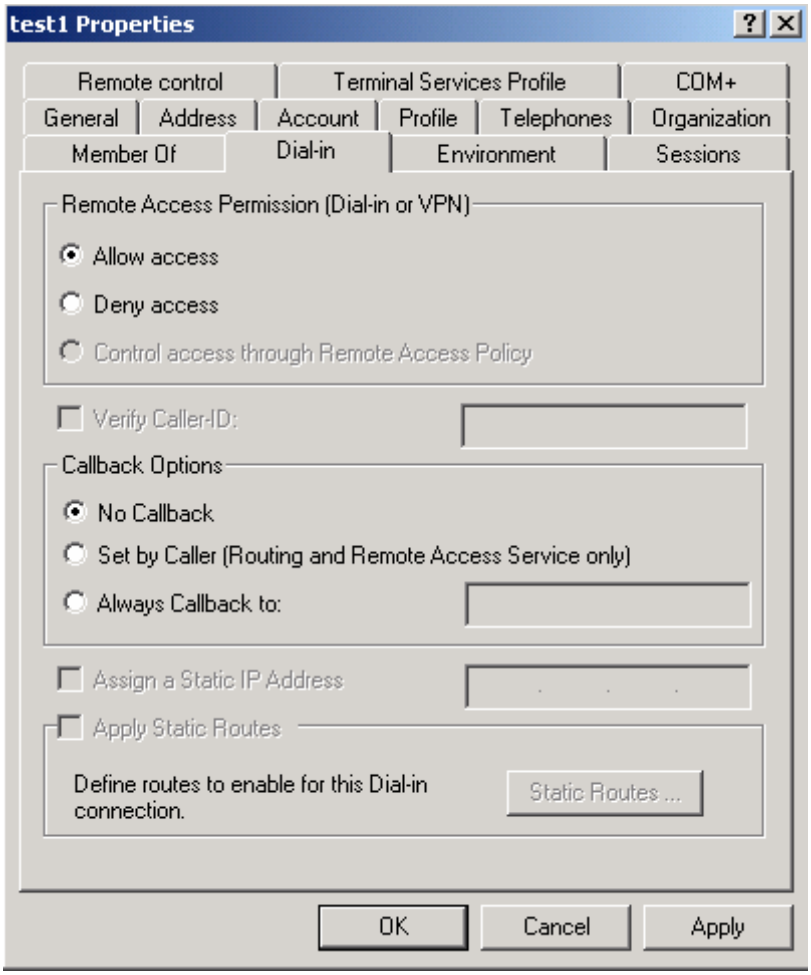
6. 사용자 이름을 하이라이트 → 이름을 오른 버튼 클릭 → 속성 선택.



7. 사용자 계정 정보 창에서 계정(Account)탭을 클릭한 다음, store password reversibly encrypted 체크 박스를 선택합니다.



8. 전화접속(Dial-in) 란을 선택하고 원격 액세스 권한을 허락합니다.



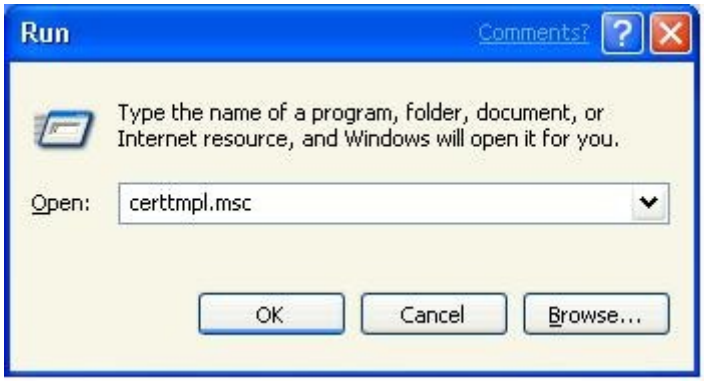
9. 확인을 클릭하고 화면을 닫습니다.

5. 인증서 서비스(Certificate Service) 구성하기

6. 엔터프라이즈 인증서 템플릿을 설치하고 구성하기

6-1 처음으로 엔터프라이즈 인증서 템플릿을설치하기

1. 인증서 템플릿 관리 콘솔을 실행합니다. 시작 → 실행 (certtmpl.msc 입력, 확인 클릭



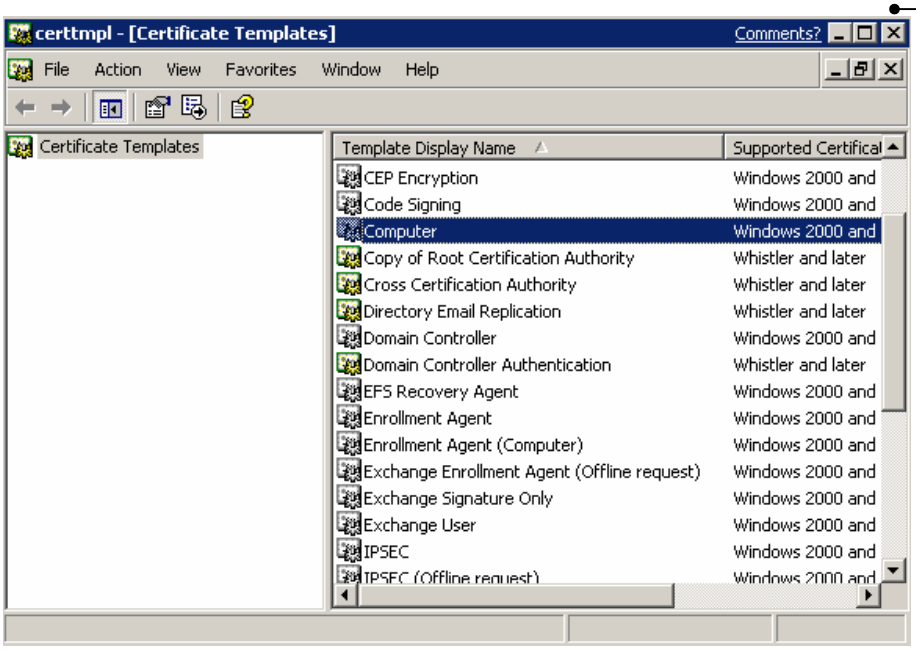
2. 엔터프라이즈 관리자 이거나 부모 도메인 관리자 이어야 Active Directory 에 템플릿을 양식시킬 수 있습니다. 확인을 클릭하십시오

3. 올바른 인증정보를 가지고 있다면 아래와 같은 화면을 볼 수 있습니다. 확인을 클릭하십시오

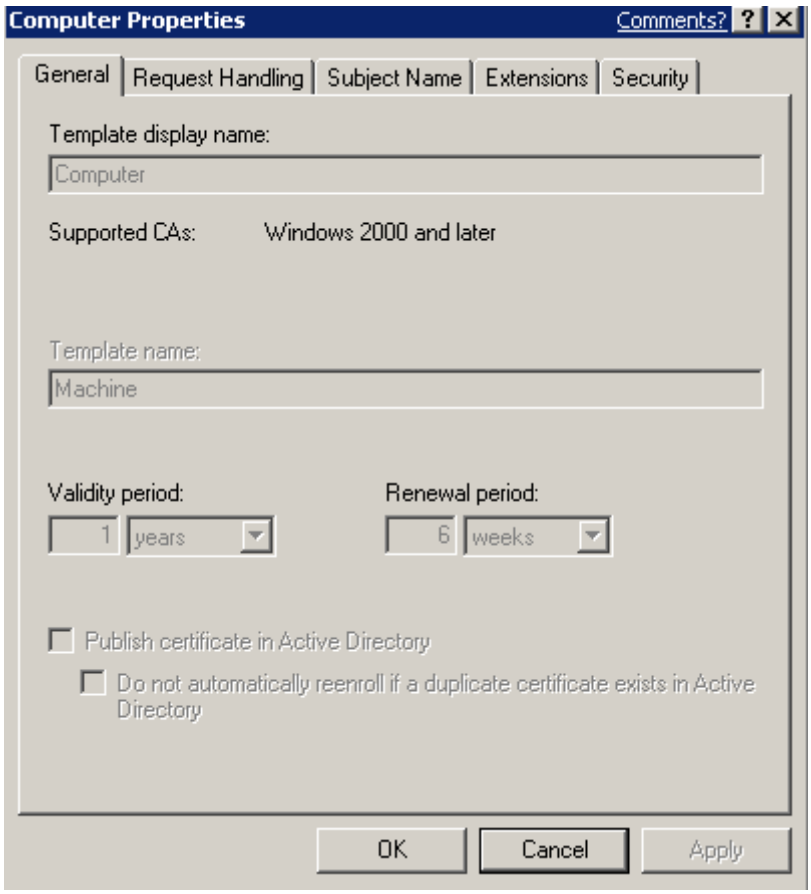
Note: 확인을 클릭하면 인증서 템플릿 관리 콘솔이 열리기 됩니다.

6-2 엔터프라이즈 인증서 템플릿 구성하기

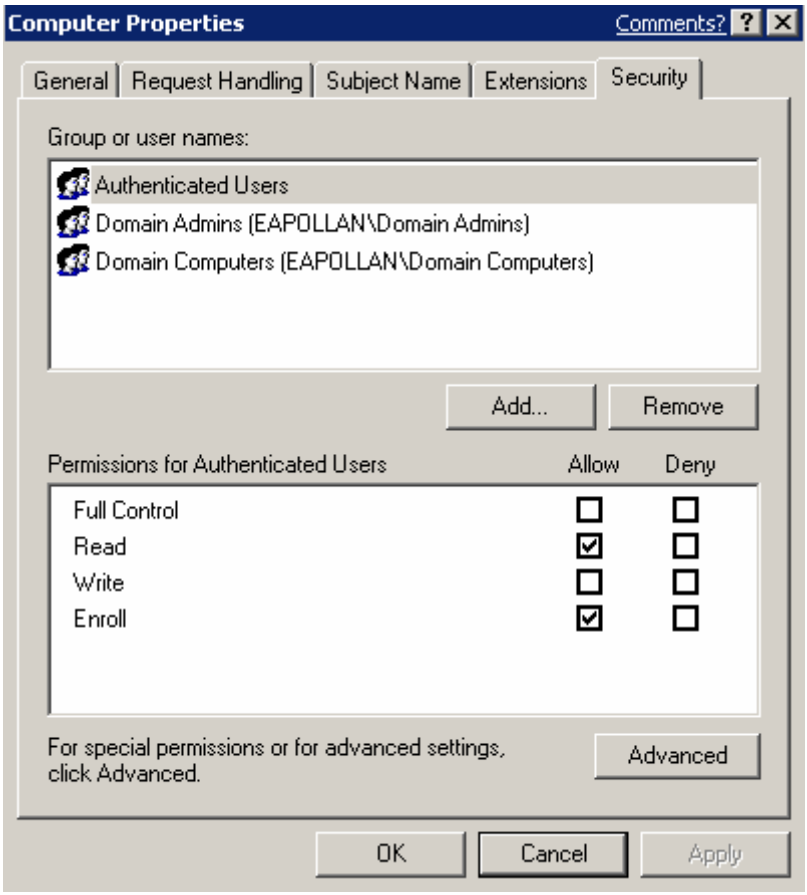
1. 인증 받은 사용자에게 발급 권한을 부여하도록 컴퓨터 템플릿을 세팅합니다.
컴퓨터 인증서의 속성을 열기 위하여 컴퓨터 인증서를 더블 클릭합니다.



2. 보안 탭을 선택합니다.



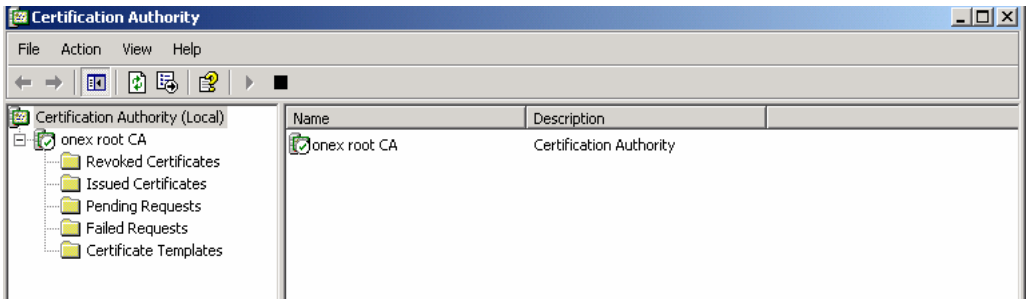
3. 인증 받을 사용자에게 발급 권한을 주기 위하여 체크하고 확인버튼을 클릭합니다.



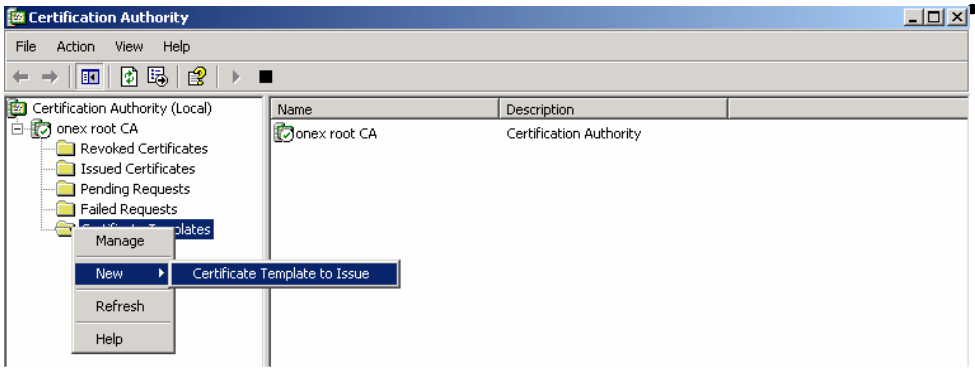
4. 스텝 1 에 있는 사용자 템플릿을 선택하고 계속해서 위의 절차를 반복합니다.

6-3 템플릿을 발급하도록 Certificate Authority를 구성하기

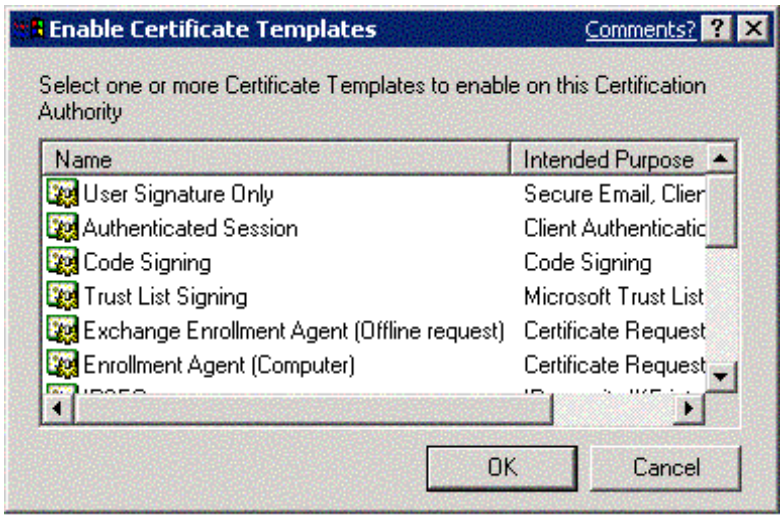
1. 시작 → 프로그램 → 관리 도구 → Certificate Authority. Root CA 를 확장합니다.



2. 인증서 템플릿을 오른쪽 버튼 클릭합니다. → 발행할 새 인증서 선택.



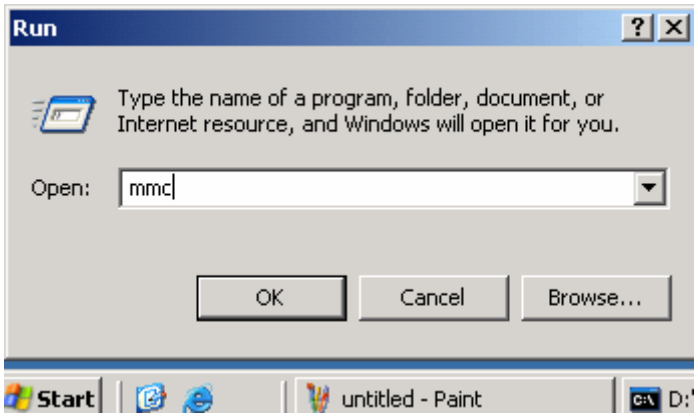
3. 모든 인증서를 선택합니다. 첫 번째 템플릿을 하이라이트 -> 마지막 템플릿 리스트까지 scroll down Shift 키를 누르고 선택된 모든 템플릿중에 마지막 템플릿을 클릭하고 확인 키를 누릅니다. Certificate Authority 를 닫습니다.



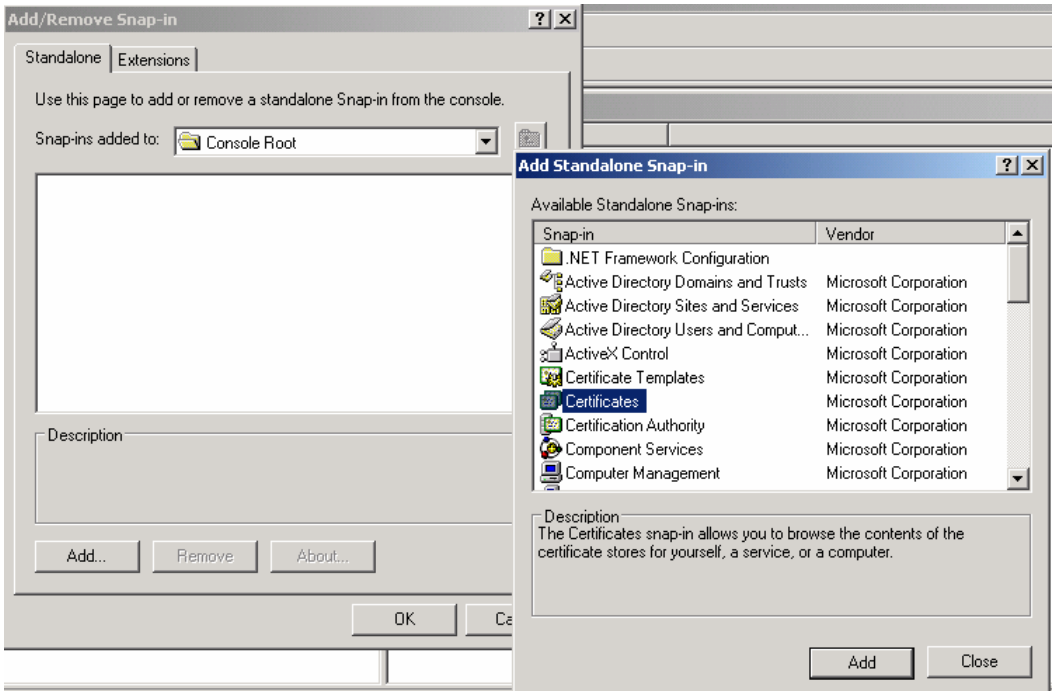
4. 서버 컴퓨터를 위한 컴퓨터 인증서를 생성하기 위하여 gpupdate /force 라고 하는 command 를 prompt 상에서 입력합니다.

6-4 서버 인증서 체크하기

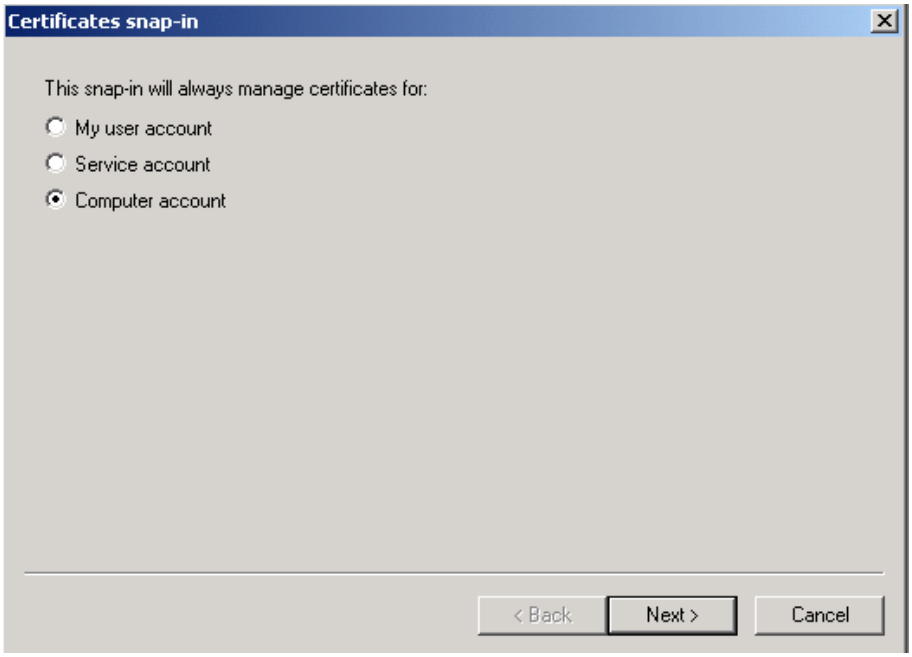
1. 시작→ 실행 → 입력 : MMC, 확인 키를 누릅니다.



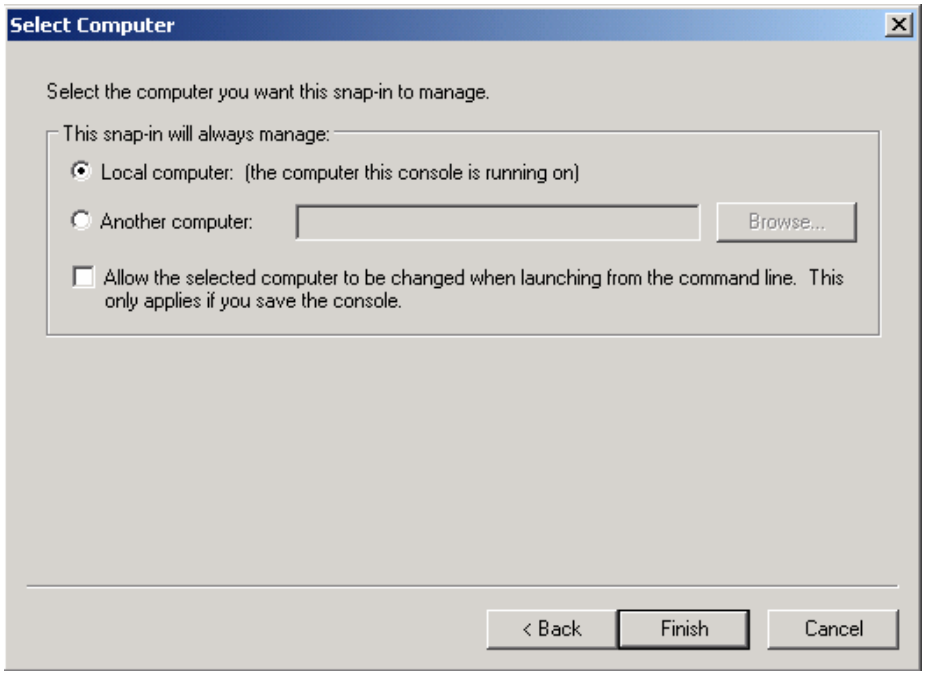
2. 파일 메뉴 → 스냅인 추가/삭제. 추가 버튼 -> Certificates from the Add standalone snap-in 창 선택 -> 추가 버튼 클릭.



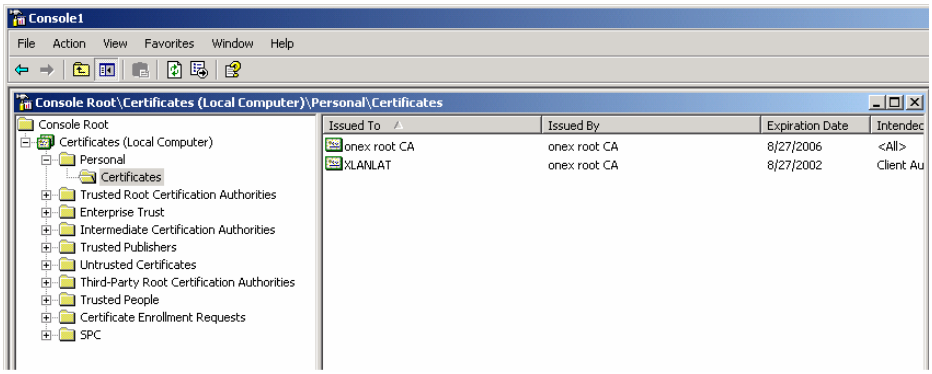
3. 내 컴퓨터 계정 닫기 → 다음 버튼 클릭.



4. 관리할 스냅 인 선택 : 로컬 컴퓨터. Standalone 스냅인을 닫습니다. -> 스냅인 추가/삭제 창을 닫기 위하여 확인을 선택합니다.



5. 오른쪽 패널에 있는 로컬 컴퓨터의 인증서를 더블 클릭합니다.
개인 더블 클릭 -> 인증서 더블 클릭. 클라이언트를 인증하기 위해서 컴퓨터 인증서와 루트 CA 인증서를 받드시 가지고 있어야 합니다.



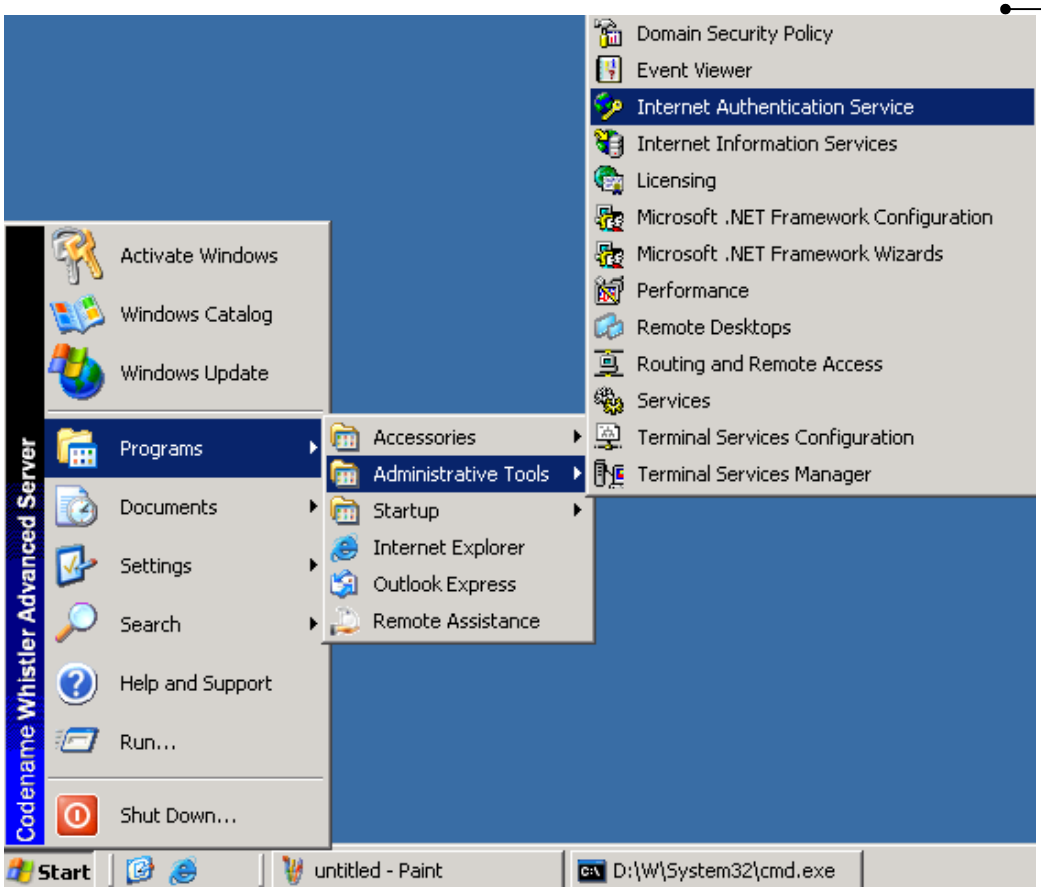
6. 추후에 편하게 관리하기 위해서 화면을 저장합니다.

6-5 INTERNET AUTHENTICATION SERVICES (인터넷 인증 서비스) 구성하기

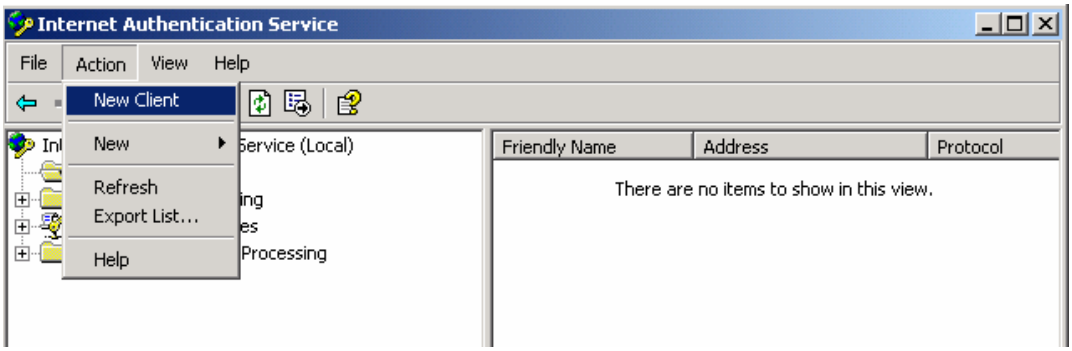
IAS를 구성하기 전에 네트워크에 있는 Access Point에 연결할 필요가 있습니다. AP는 DHCP에서 IP 주소를 획득할 수도 있고 정적 주소를 사용할 수도 있습니다. 추후에 Radius 클라이언트를 생성할 때 이 IP주소가 필요합니다.

6-6 Radius 클라이언트 생성하기

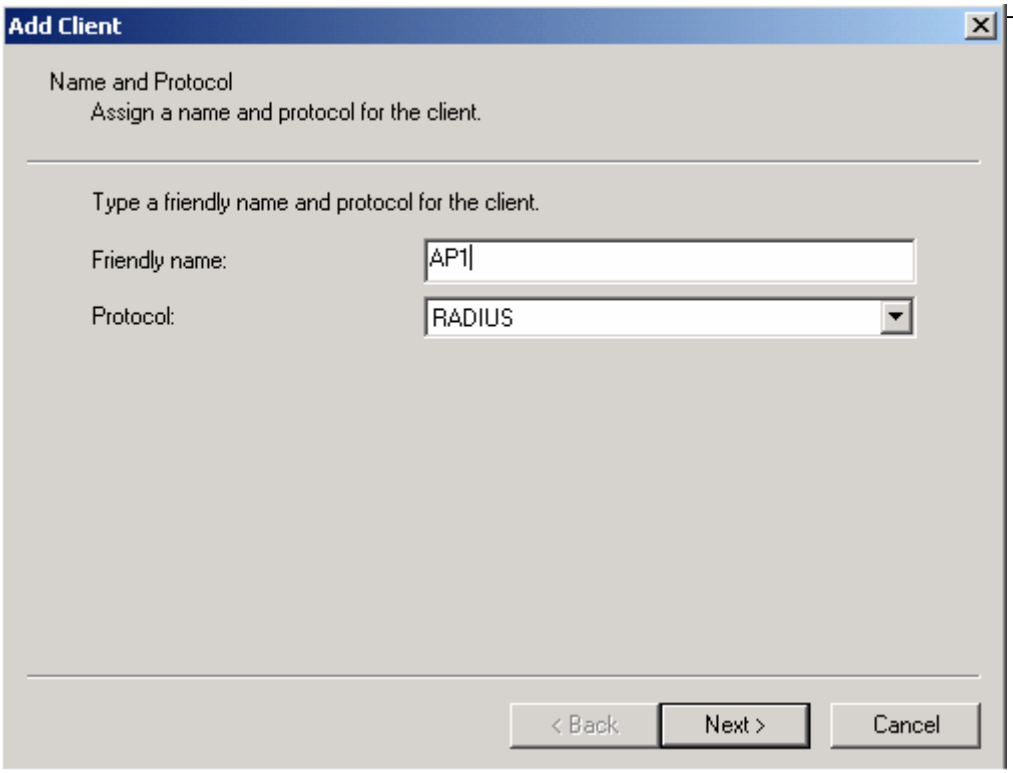
1. 시작→ 프로그램 → 관리 도구 → Internet Authentication Service. (인터넷 인증 서비스)



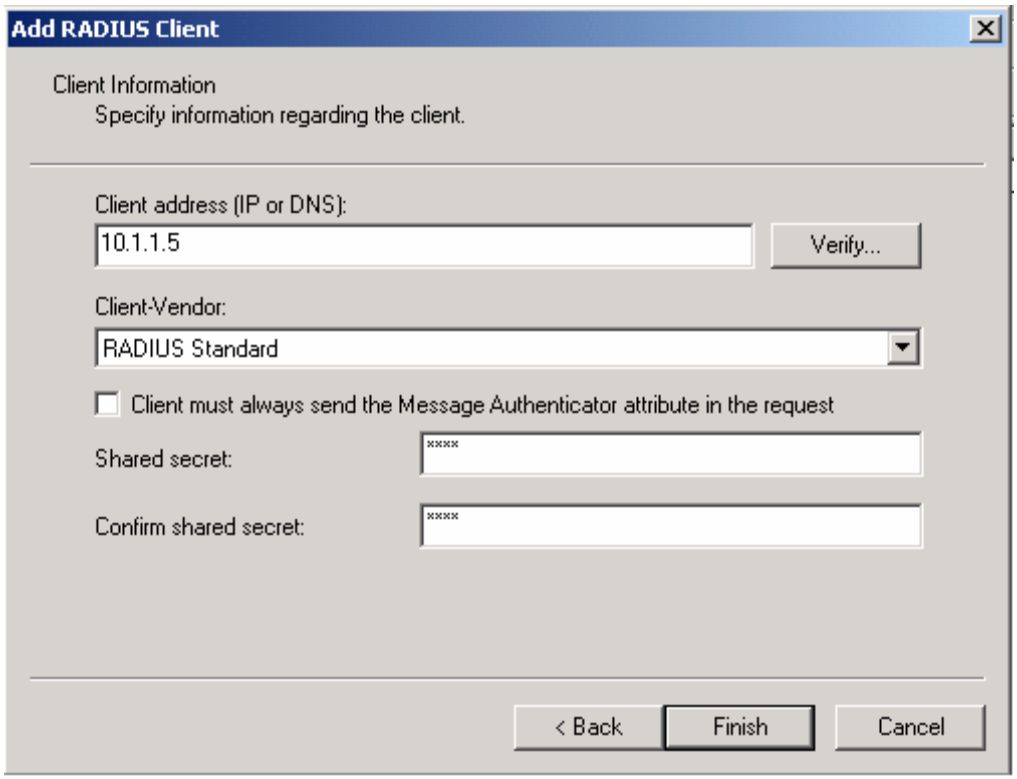
2.클라이언트 하이라이트 → Action → 새 클라이언트



3.친숙한 이름 입력. 프로토콜은 Radius 로 지정.



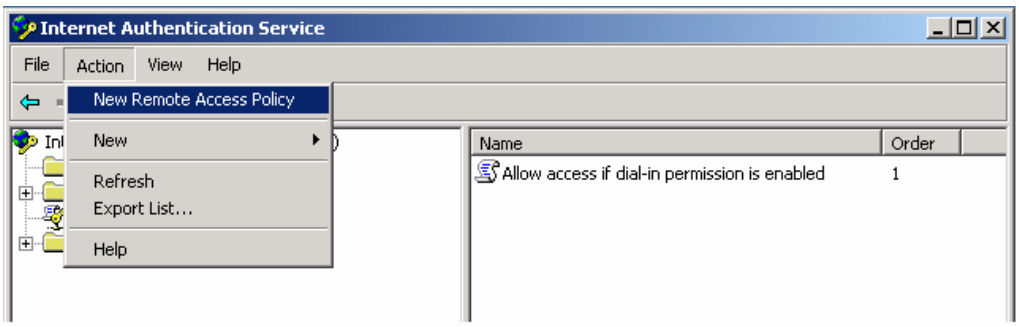
4.Radius 클라이언트를 위한 IP 주소 입력 하고 shard secret 를 위한 패스워드를 입력합니다. (중요) 이 패스워드는 Radius 서버와 Access Point 둘 다 모두 동일 하게 사용해야 합니다.



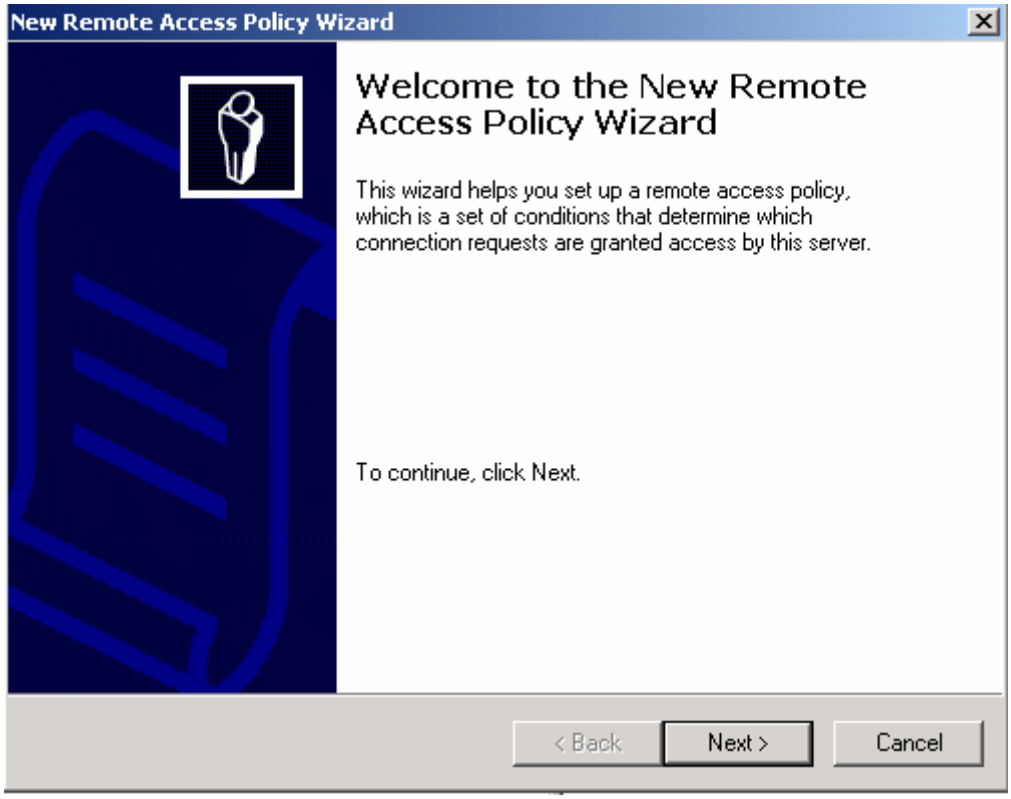
5.완료버튼 클릭

6-7 Radius 클라이언트를 위한 원격 액세스 정책 만들기

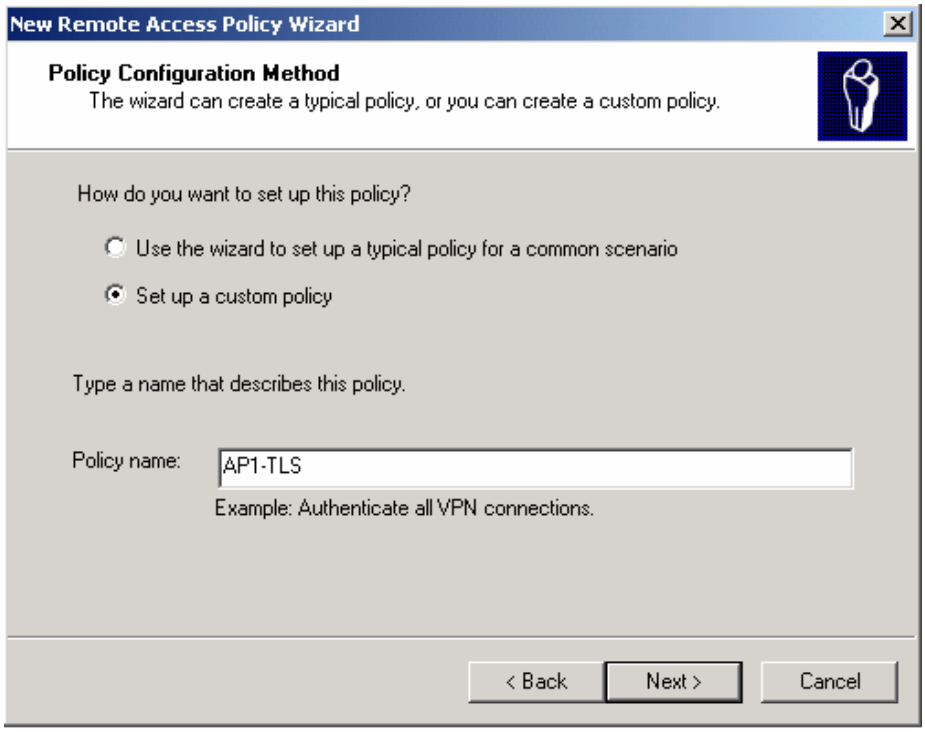
1. 액세스 정책 → Action → 새 원격 액세스 정책



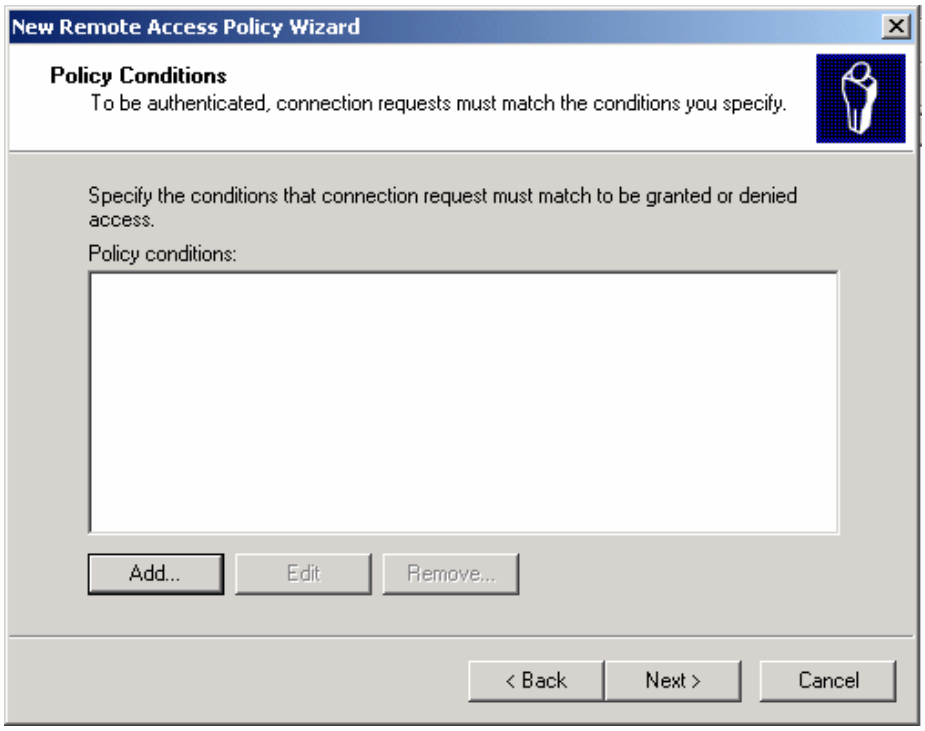
2. 원격 액세스 정책 마법사를 실행합니다. 다음을 클릭합니다.



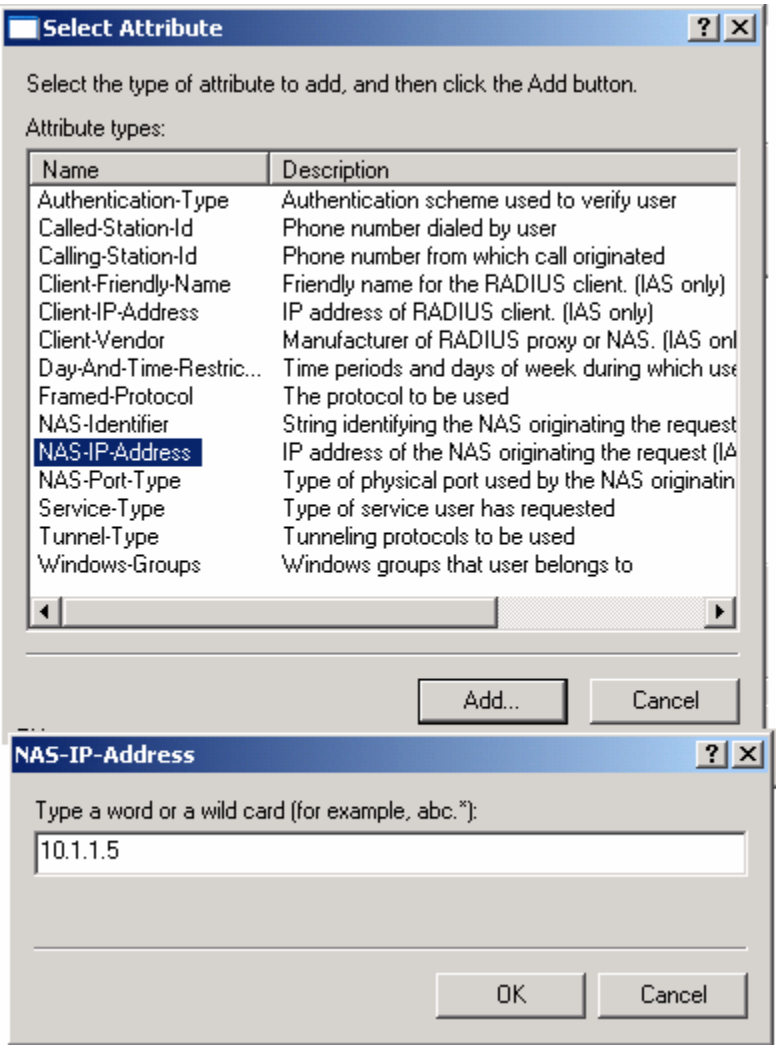
3. Set up a custom policy 을 클릭하고 정책의 이름을 입력한 뒤, 다음을 클릭합니다.



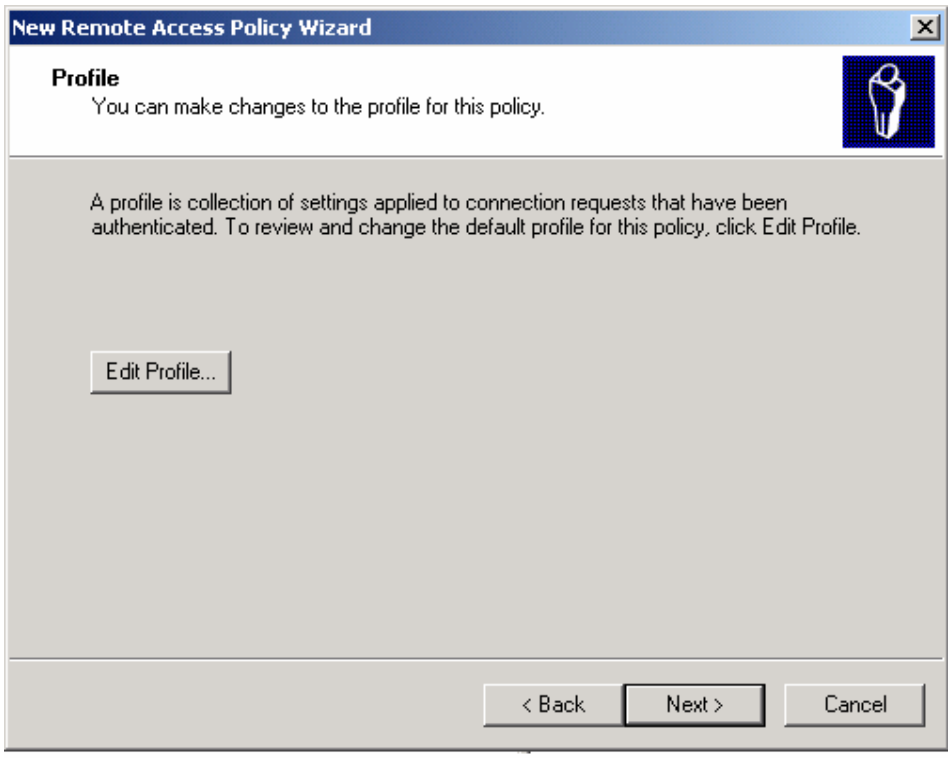
4. Policy Conditions 화면에서 추가 버튼을 클릭합니다.



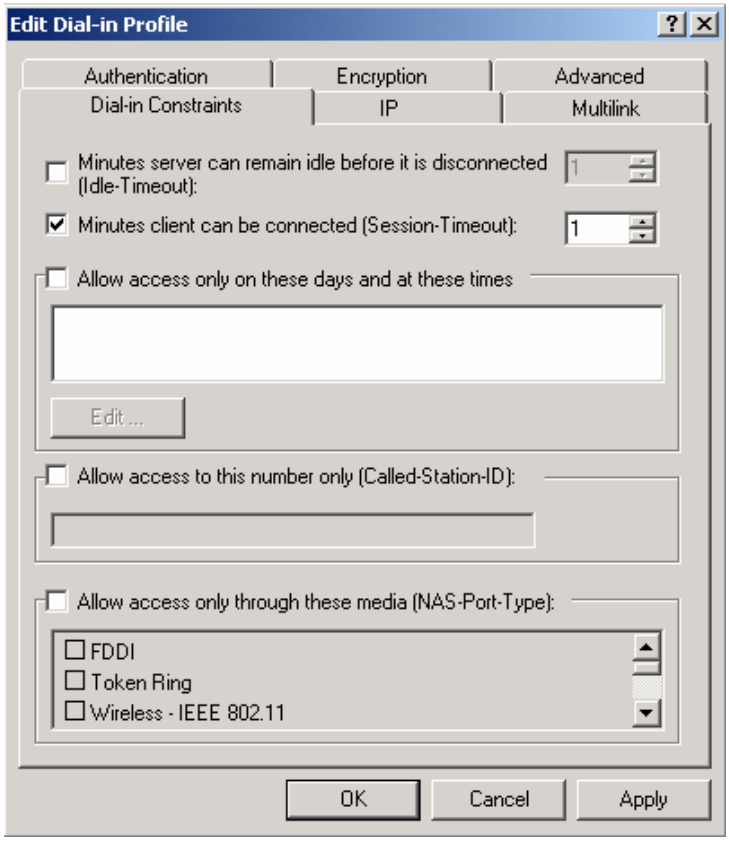
5. NAS-IP-Address 를 Attribute list 로부터 선택하고 정책이 적용될 Radius 클라이언트의 IP 주소를 입력합니다.



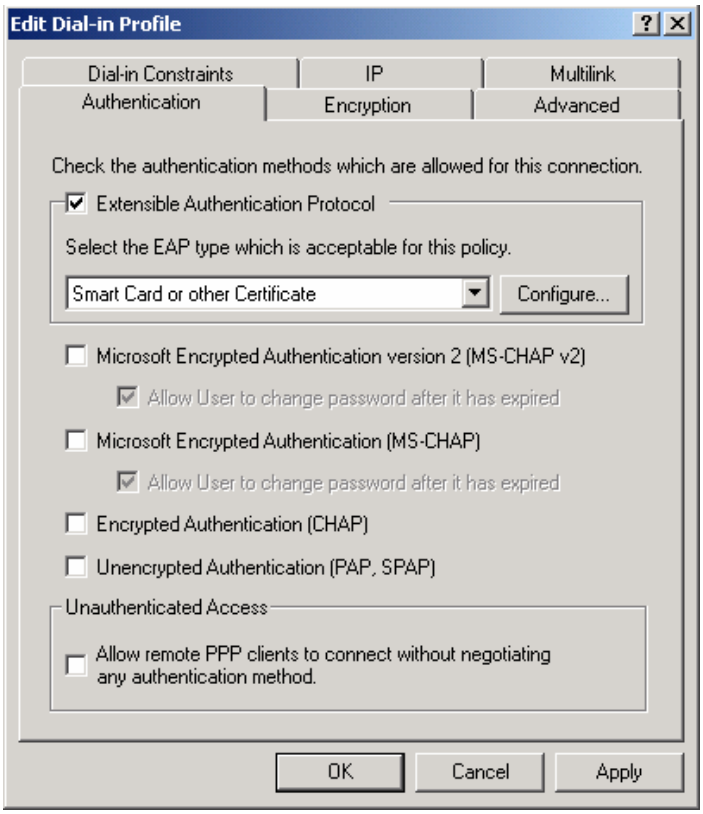
6. 정책 편집을 클릭합니다.



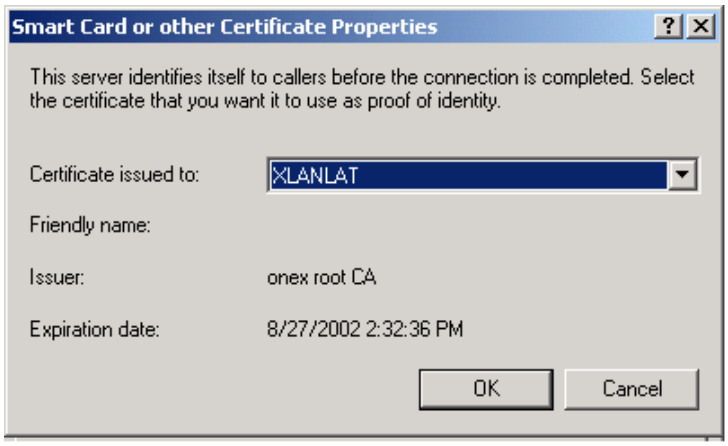
7. Radius 세션 타임 아웃을 구성하기 위하여 전화접속(Dial-in) 제약사항을 구성합니다. 테스트 환경을 위하여 1 분을 설정합니다.



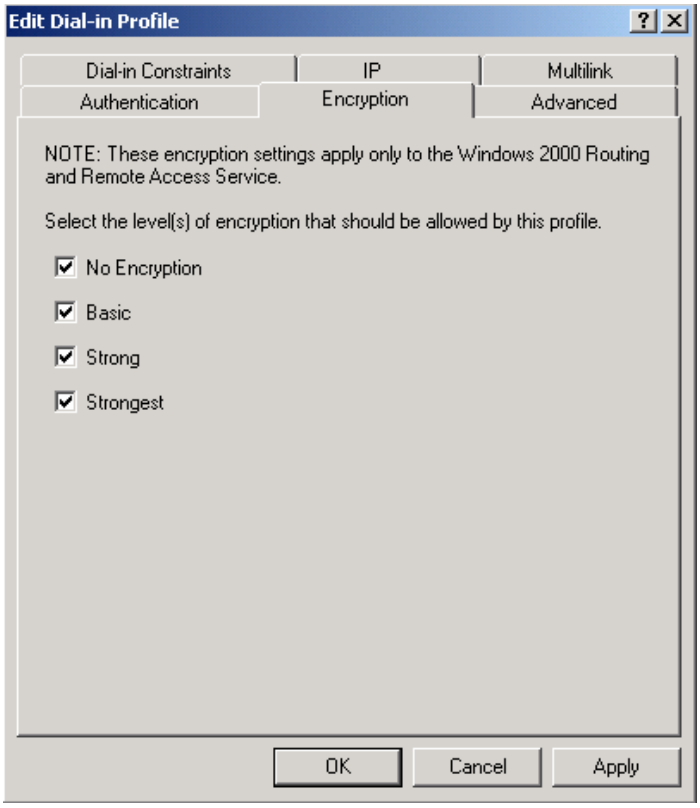
8. 인증 탭을 클릭합니다. 확장 가능한 박스를 선택 -> 모든 다른 인증 타입에 되어있는 체크를 지웁니다. -> 스마트카드 또는 다른 인증서를 선택합니다. -> 구성(configure)를 클릭합니다.



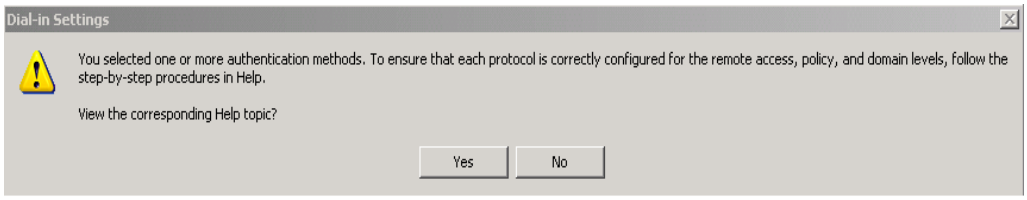
9. 클라이언트 인증을 위하여 서버의 인증서를 봅니다.



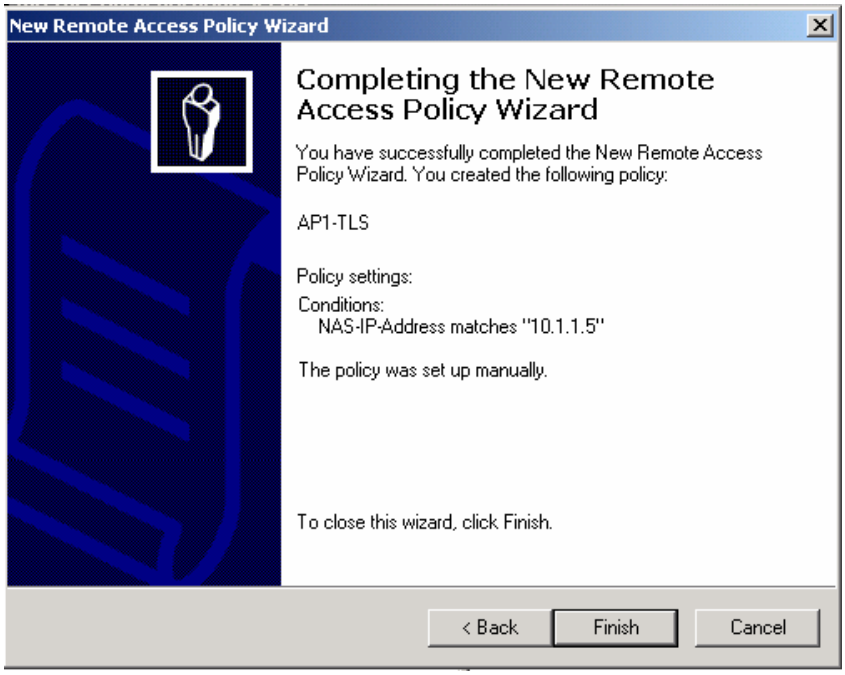
10. 암호화(Encryption) 탭을 클릭하고 모든 다른 테스트 시나리오를 위하여 체크되어있는지를 확인합니다.



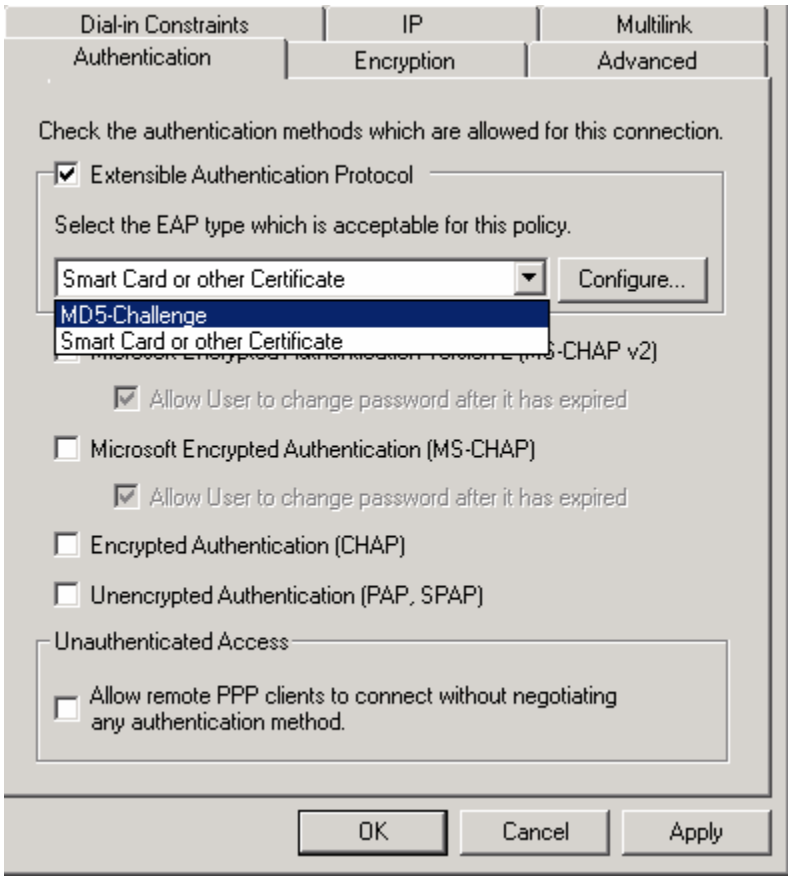
11. 다음과 같은 메시지를 볼 수 있습니다. 만약에 인증 방법에 대하여 배우고자 한다면 “예”버튼을 그렇지 않고 계속하길 원하면 “아니오”버튼을 클릭하십시오.



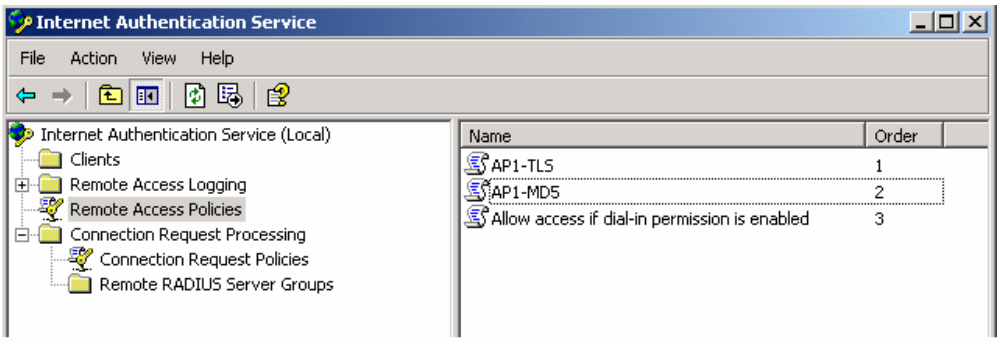
12. 다음을 클릭하고 완료를 클릭하십시오



13. 위와 같은 스템으로 MD5 를 위한 정책을 생성하십시오. MD5 대신 스마트 카드나 인증서를 인증 탭에서 대신 선택해도 됩니다.

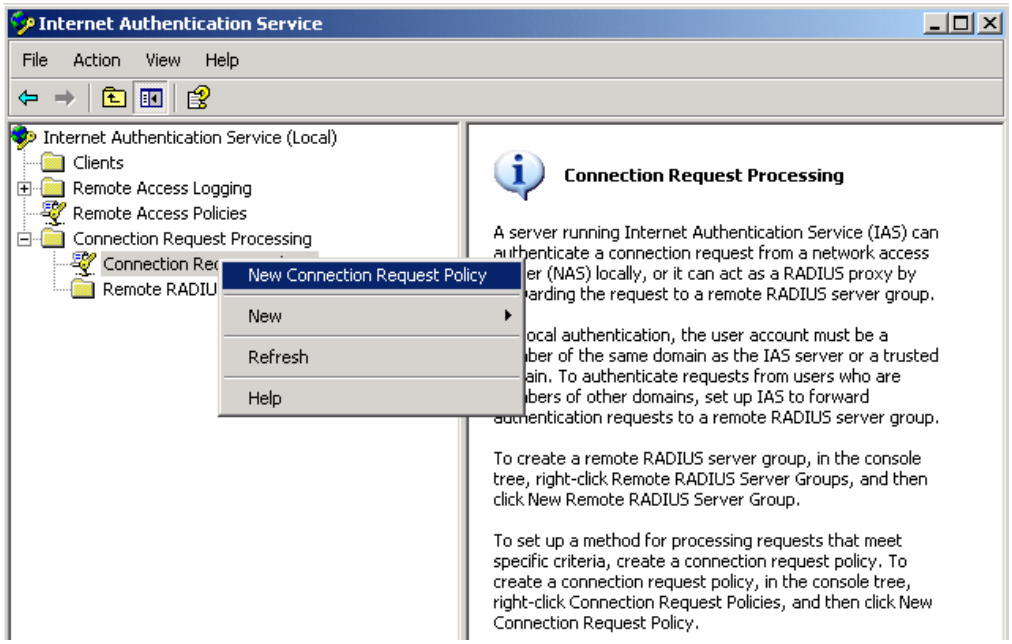


14. 적용될 정책에 대한 리스트를 아래와 같이 볼 수 있습니다. 이 리스트는 위에서부터 순서대로 적용됨을 기억하십시오. 다시 말하면 만약에 TLS 대신 MD5 암호화를 적용한 정책을 사용하시려고 한다면 순서를 바꾸어야지만 올바르게 동작합니다.

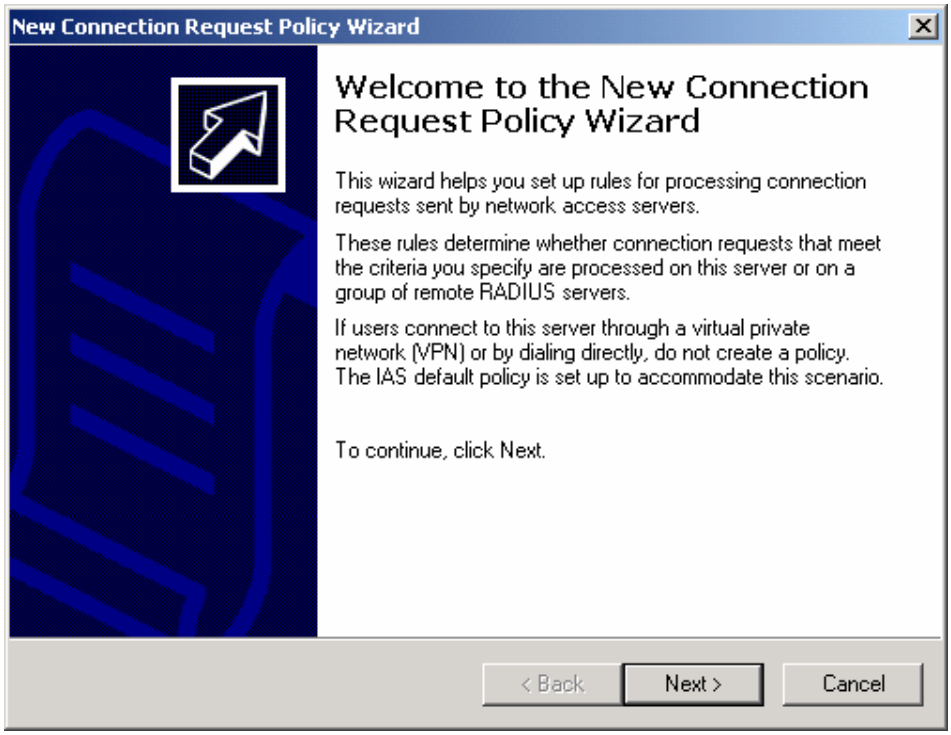


6-8 연결 정책 구성하기

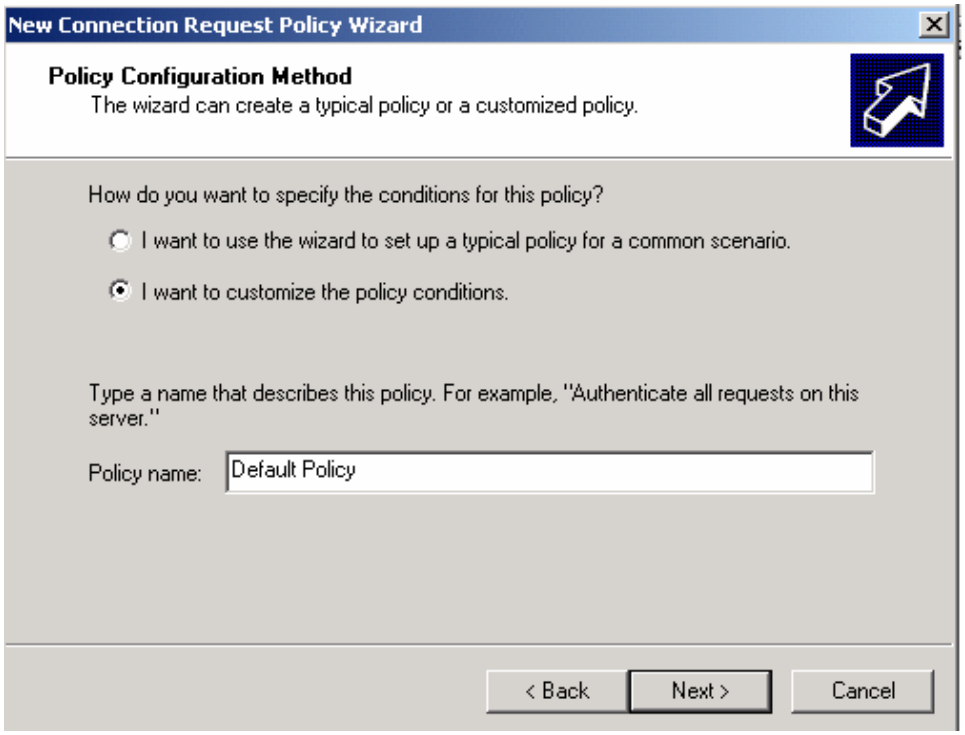
1. Connection Request Processing 확장 → Connection Request policy 를 오른 버튼 클릭



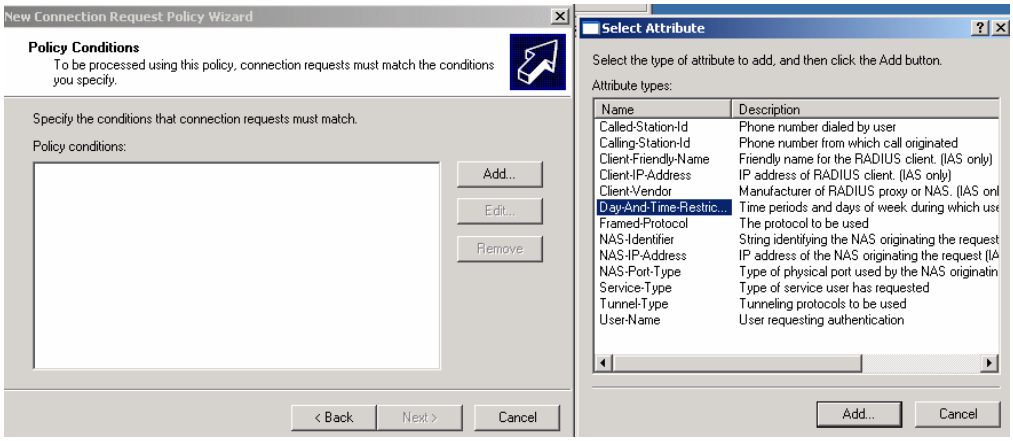
2. Connection Request 마법사가 실행됩니다. 다음을 클릭하십시오.



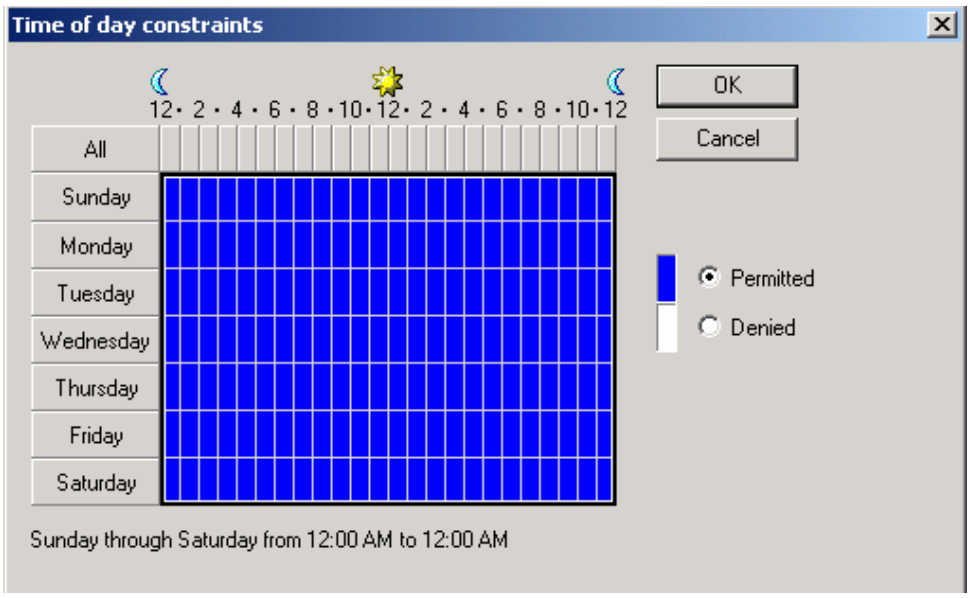
3. I want a custom policy 를 선택하고 정책이름을 입력한 후 다음 버튼을 클릭합니다.



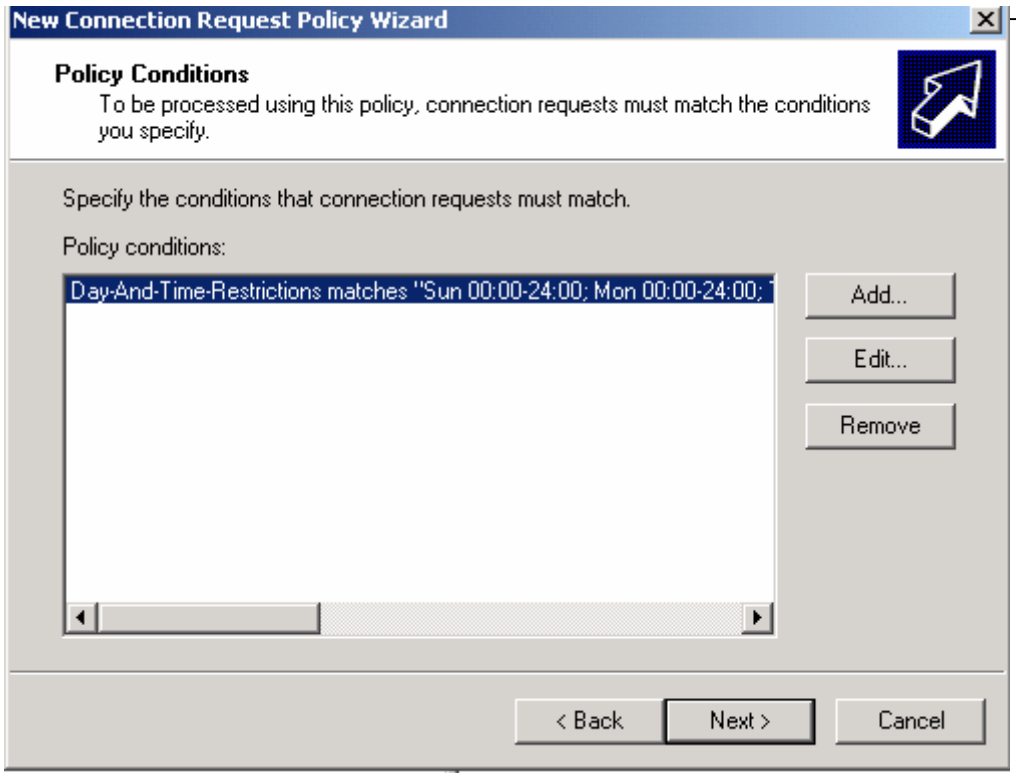
4. 정책 조건 화면에서 추가 버튼을 클릭하고 적당한 Attribute 를 선택합니다. 그리고 추가 버튼을 한번 더 누릅니다.



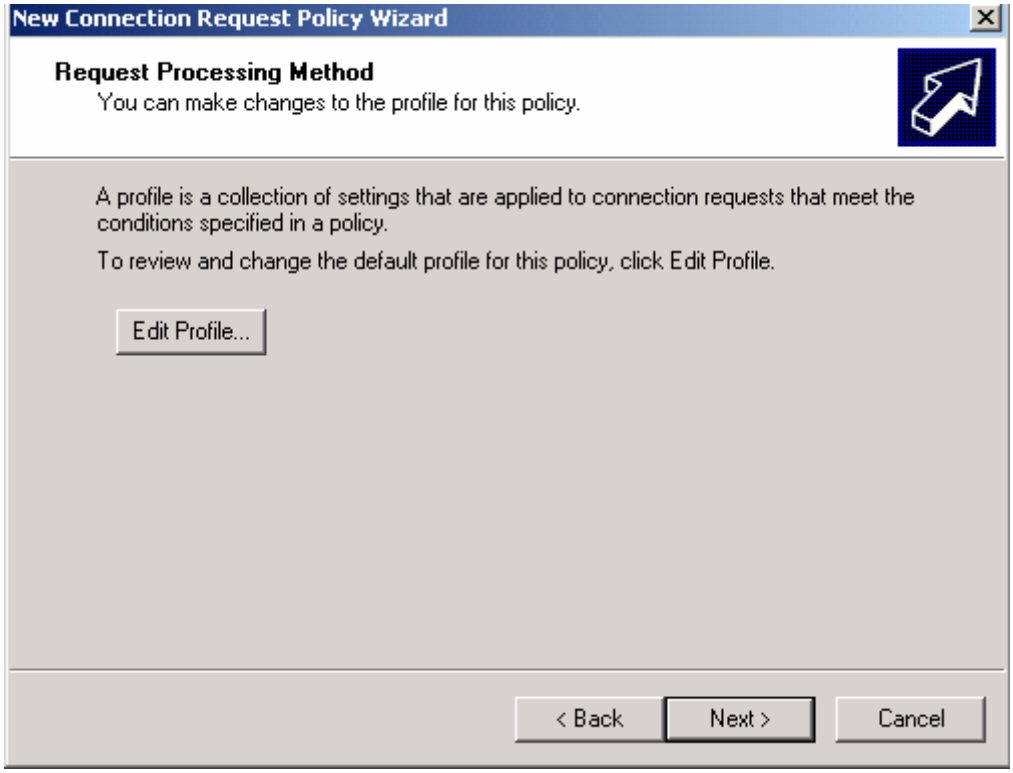
5. Day and Time 과 24X7 액세스 허용을 선택합니다.



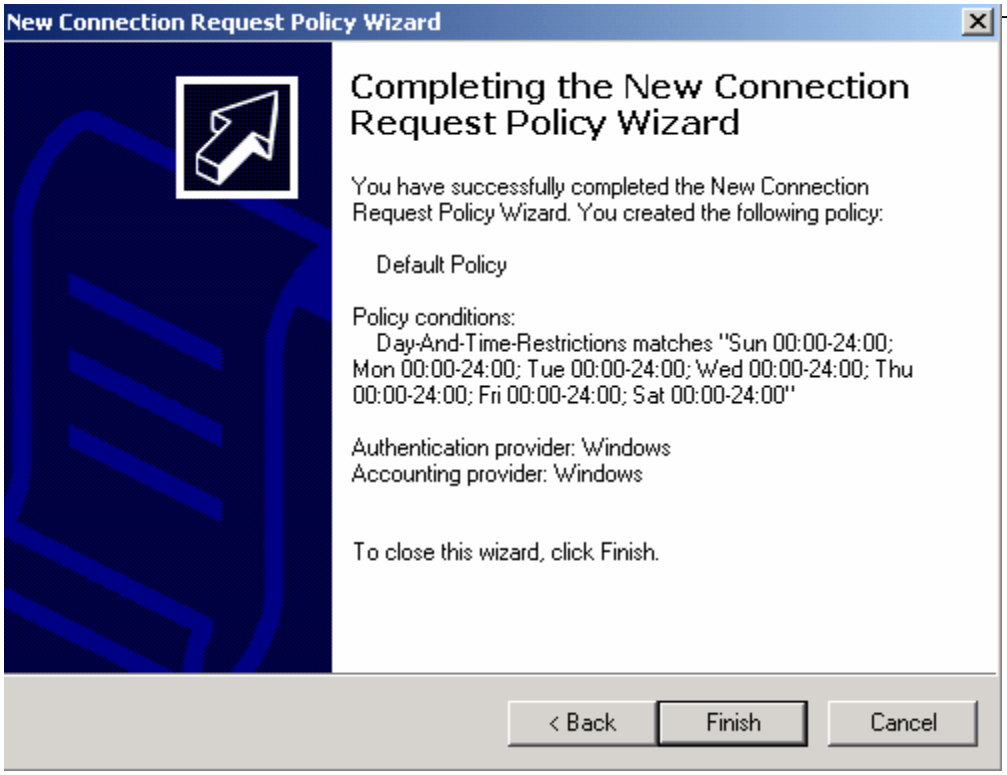
6. 다음을 클릭합니다.



7. 다음을 클릭해서 프로파일 기본값을 제외합니다.



8. 완료를 클릭하고 Internet Authentication Service 를 닫습니다.



4) 스마트카드 인증 시스템 구현

위의 내용에서 이미 아래 부분에 대한 설정을 알아보았습니다.

A. Active Directory 구성
B. 인증서 서비스 구성 및 관리
C. 고급 및 사용자 인증서 관리

- **지원되는 카드 리더**

스마트카드를 사용하기 전에 호스트 컴퓨터에 스마트카드 리더를 설치해야 합니다. 마이크로소프트 Windows Server 에는 다음과 같은 스마트카드 리더 디바이스 용 드라이버가 포함되어있습니다만 Plug and Play 로 자동 발견되는 장비가 설치됩니다. (하드웨어 업체에 따라 차기 버전의 드라이버가 지원될 수도 있습니다.)

Manufacturer	Smart Card Reader	Interface	Device Driver
Bull CP8	Smart TLP3	RS-232	bulltlp3.sys
Gemplus	GCR410P	RS-232	gcr410p.sys

Gemplus	GPR400	PCMCIA	gpr400.sys
Litronic	220P	RS-232	lit220p.sys
Rainbow Technologies	3531	RS-232	rnbo3531.sys
SCM Microsystems	SwapSmart	RS-232	scmstcs.sys
SCM Microsystems	SwapSmart	PCMCIA	pscr.sys

이 문서에서는 Plug and Play 스마트 카드 리더기를 설치하고 사용하는 방법을 알아보고 Plug and Play 를 지원하지 않는 스마트카드 리더기는 윈도우 플랫폼 상에서 권고하지 않습니다. 해당 스마트 카드 리더기를 설치하려면 리더기 제조 업체로부터 소프트웨어 및 설명서를 직접 받아야 합니다.

마이크로소프트는 다른 하드웨어 디바이스와 마찬가지로 스마트카드 리더기를 위하여 직접 로고 프로그램을 개발하였습니다. 이 프로그램은 고객이 최상의 하드웨어 경험으로 사용할 수 있도록 배려한 것이며 Personal computer.smart card (PC/SC0 규격을 잘 지켰는지 와 윈도우 플랫폼에서의 상호 운용성을 근간으로 마련되었습니다. 자세한 것은 Windows Hardware Compatibility List 를 확인하십시오

- **지원되는 스마트카드**

Windows Server 를 설치하면 Gemplus 의 GemSAFE 와 schlumberger ctyptoflex cryptographic smart card 가 기본 설치에 포함되어 있습니다. 포함되어 있는 카드를 사용하기 위하여 서버나 클라이언트에서 어떠한 작업도 수행할 필요가 없습니다.

아래 테이블은 지원되는 스마트카드에 대한 정보를 제공합니다.

Smart Card	Default PIN	Contact Shape	CSP
Gemplus GemSAFE	1234	oval	Gemplus GemaSAFE Card CSP v1.0
Schlumberger Cryptoflex	00000000	rectangular	Schlumberger Cryptographic Service Provider

- **스마트카드 리더 설치하기**
- **스마트 카드 리더 연결하기**

1. 컴퓨터를 shutdown 하고 전원을 끕니다.
2. 카드 리더를 가능한 시리얼 포트에 연결하거나 PC 카드를 PCMCIA 타입의 슬럿에 삽입합니다.
3. 만약에 시리얼 리더가 보조 PS/2 cable/connector 를 가지고 있다면 키보드 또는 마우스 connector 를 연결합니다. 그리고 컴퓨터의 키보드나 마우스 포트에 플러그 합니다.
4. 컴퓨터를 재 시작하고 관리자 권한을 가진 사용자로 로그온 합니다.

- **스마트카드 리더 디바이스 드라이브 설치하기**

스마트카드 리더가 인식되고 설치되었다면 윈도우 로그온 화면이 자동으로 인식해서 바뀔 것입니다. 만약에 인식이 되지 않았다면 다음과 같이 하십시오

Windows CD 또는 하드웨어 업체로부터 받은 미디어를 준비하십시오

1. 데스크톱의 내 컴퓨터를 오른 버튼 클릭하고 관리 메뉴를 클릭합니다.
2. 서비스와 어플리케이션 노드를 확장하고 서비스를 클릭합니다.
3. 오른쪽 화면에서 스마트카드를 오른 버튼 클릭하고 속성을 선택합니다.
4. 일반 탭에서 시작 타입을 자동으로 선택하고 확인 키를 누릅니다.
5. 컴퓨터를 재 시작합니다.

그래도 하드웨어 마법사에서 자동으로 인식하지 못하면 스마트카드는 Plug and Play 가 아닐 수 있습니다. 마이크로소프트는 Plug and Play 디바이스 사용을 권고합니다.

- **스마트카드 인증서 발급**

관리자로부터 적당한 권한을 부여 받지 않은 도메인 사용자는 스마트카드 로그온을 발급할 수 없거나 스마트마드 사용자 인증서를 발급할 수 없음을 기억하십시오

엔터프라이즈 CA 가 설치되면 설치는 stantion 상에서의 enroll-on-behalf 기능이 포함되어 있습니다. 그렇게 되면 해당 스테이션에서 관리자가 특정사용자에게 스마트카드 로그온이나 스마트카드 사용자 용 인증서를 발급할 수 있게 됩니다. 그러나 이 스테이션은 카드를 개인화하는 기능을 포함하고 있지는 않습니다. 이것은 스마트카드 제조업체에서 만든 특정 소프트웨어를 설치해야만 가능합니다.

- **스마트카드 인증서 발급하기**

1. 인터넷 익스플로러를 실행합니다.

2. CA 서버에 연결하기 위하여 http://*machine-name*/certsrv 를 주소란 창에 입력합니다.
3. 마이크로소프트 인증서 서비스 페이지가 나타나면 “인증서 요청”을 선택하고 다음버튼을 클릭합니다.
4. 요청 형태를 선택하고 고급요청버튼을 누른 후 다음 버튼을 클릭합니다.
5. 고급 인증서 요청 페이지가 나타나면 스마트카드 발급 스테이션을 이용하여 Request a certificate for a smart card on behalf of another user” 을 선택한 후 다음을 클릭합니다.
6. 맨 처음 스마트카드 발급 스테이션을 사용할 경우, 디지털로 사인된 마이크로소프트 ActiveX 컨트롤이 CA 서버로부터 다운로드 되고 이것을 발급 스테이션이 사용하게 됩니다. 보안 경고 창에서 “예”를 선택해서 컨트롤을 설치합니다.
7. 스마트카드 발급 스테이션 페이지가 나타나면, 이 페이지상에서 인증서를 요청하기 전에 다음을 반드시 해야 합니다.

   - **스마트카드 로그온이나 스마트카드 사용자 인증서 템플릿을 선택합니다.**
   - Certification Authority 를 선택합니다.
   - Cryptographic Service Provider 를 선택합니다.
   - Administrator Signing Certificate. 을 선택합니다.
   - 발급할 사용자를 선택합니다.

   위의 사항을 각 드롭다운 리스트 박스를 이용하여 선택합니다.

8. 인증서 템플릿, CA, 그리고 CSP 를 선택한 다음 선택된 인증서를 클릭해서 서명된 관리자 인증서를 선택합니다. 인증서를 요청하면 인증서 내용을 볼 수도 있고 취소할 수도 있습니다.
9. 또한 인증서를 발급할 사용자를 선택합니다. .
10. 인제 Enroll(발급)버튼을 눌러서 인증서를 발급할 수 있습니다.
11. 만약에 대상 스마트카드가 리더기에 없으면 스마트카드를 요청하는 다이알로그 박스가 나타날 것입니다. 카드를 삽입한 다음 재시도 버튼을 누르십시오.
12. 인증서 발급 프로세스의 한 부분으로 이 요청은 반드시 인증을 요청하는 것에 포함되는 공인 키에 맞는 개인키로 디지털 사인이 되어야 합니다. 개인키는 스마트카드에 저장되므로 디지털 사인은 스마트카드의 주인을 확인하기 위하여 인증할 필요가 있습니다. 카드의 PIN 번호를 입력한 후 확인 키를 선택하십시오

또한 사용자는 변경 버튼을 눌러서 PIN 번호를 바꿀 수도 있습니다. 사용자는 다이알로그 박스에서 숫자로 된 핀을 입력한 후 원하는 PIN 번호로 바꿉니다.

- **스마트카드로 로그인하기**

패스워드 기반의 로그온은 Ctrl+Alt+Del 키를 누르고 입력하게 되어있습니다. 스마트카드 로그온은 사용자가 스마트카드를 리더기에 삽입하고 안전한 로그온 프로세스 절차에 따라서 사용자 이름과 패스워드 대신 PIN 숫자를 입력합니다.

스마트카드 로그온을 지원하도록 구성된 Windows 도메인에 로그온하기 위하여

1. 스마트카드를 삽입합니다.
2. PIN 숫자를 입력하고 확인키를 누릅니다.

- Gemplus GemSAFE 의 기본 PIN 값은 1234 입니다.
- Schlumberger Cryptoflex 의 기본값은 **00000000 입니다.**

화면은 Windows 2000 Professional 기준입니다.

시스템이 로그온하지 못하면 인증정보가 확인되지 않은 것입니다.

스마트카드를 이용하여 잠금 기능과 해제기능

- **컴퓨터를 잠그기 위하여 (로그아웃 대신)**

- Ctrl+Alt+Del 키를 동시에 누르고 컴퓨터 잠금을 선택합니다.

- **잠긴 컴퓨터를 해제하기 위하여**

- 스마트카드를 리더기에 삽입하고 PIN 숫자를 입력합니다.