iSCSI 소개

개요

이 백서에서는 iSCSI(Internet Small Computer Systems Interface) 프로토콜에 대한 기본적인 작업 지식을 설명합니다. iSCSI는 TCP/IP 네트워크를 통해 블록 중심형 스토리지 데이터를 맵핑하기 위한 SCSI 전송 프로토콜입니다. 이 문서에서는 주로 iSCSI에 대해 설명하므로 SCSI와 SAN(Storage-Area Network) 프로토콜 및 아키텍처에 대한 배경 지식이 필요합니다. 이러한 영역을 다루는 백서 목록은 이 문서의 끝 부분을 참조하십시오.

이 문서에서 제공하는 iSCSI 프로토콜에 대한 설명은 인터넷 엔지니어링 태스크포스(IETF)의 IP Storage(IPS) iSCSI 초안 10을 기초로 합니다. 자세한 내용을 보려면 이 문서의 끝 부분에 있는 참조 URL을 이용하십시오.

이 문서에는 iSCSI 프로토콜 및 프로세스에 대한 분류와 iSCSI 보안 및 관리상의 고려사항 및 기본적인 구현 정보가 포함되어 있습니다. 또한 iSCSI 프로토콜과 관련된 용어와 약어에 대한 정의도 포함되어 있습니다.

iSCSI 전망

iSCSI에 대한 기본 개념

개념적으로 iSCSI+TCP+IP는 병렬 SCSI 케이블이나 FCP(Fibre Channel Protocol: 파이버 채널을 통한 SCSI)의 대체 방법이 아니라 Layer3/4 네트워크 전송과 동일한 방법입니다. iSCSI의 기본 개념은 기존 IP 네트워크에의 투자를 활용하여 SAN을 촉진하고 확장하는 것입니다. 이를 위해 호스트와 SAN 노드 사이에서 TCP/IP 프로토콜을 사용하여 SCSI 명령과 데이터를 전송합니다.

일반적으로 SAN에서는 호스트와 스토리지 시스템을 상호 연결하는 별도의 전용 인프라가 필요했습니다. 이러한 상호 연결을 위한 기본 수단은 SCSI 전송을 제공하는 파이버 채널 네트워크이기 때문에 결과적으로 IP 애플리케이션과 관련 스토리지를 지원하기 위해 별도의 병렬 네트워크를 구축해야 합니다. 또한 파이버 채널은 원시 형태로 낮은 대역폭의 WAN 네트워크를 통해 전송될 수 없으므로 특수한 하드웨어와 처리가 필요합니다. 하지만 IP 네트워크에서 iSCSI를 사용하면 파이버 채널 네트워크를 교체하지 않아도 IP로 연결된 호스트가 파이버 채널 기반 SAN에 도달할 수 있습니다.

IP 네트워크 인프라는 서버와 블록 지향형 스토리지 장치를 효율적으로 상호 연결할 수 있다는 장점이 있습니다. IP 네트워크는 비용면에서 효율적이며 보안과 확장성, 호환성, 네트워크 관리 및 스토리지 관리 기능을 제공합니다.

IP 네트워크는 다음과 같은 장점이 있습니다.

- IP 네트워크는 관리, 보안 및 서비스 품질(QoS)을 위한 미들웨어 및 네트워크 프로토콜에 대한 가용성이 높습니다.
- IP 네트워크의 설계 및 관리에서 개발된 기술을 IP SAN에 적용할 수 있습니다. 경험 많고 숙련된 IP 네트워킹 직원을 활용하여 이 네트워크를 설치하고 운영할 수 있습니다.
- IP 네트워크에서는 전체 조직이 표준 IP 인프라, 제품 및 서비스를 사용함으로써 경제적인 이득을 얻을 수 있습니다.
- iSCSI는 기존의 IP LAN 및 WAN 인프라와 호환됩니다.
- 거리를 제한하는 것은 IP 네트워크가 아니라 애플리케이션 시간 종료 때문입니다.

iSCSI의 가치

기존의 IP 네트워크에 구축하기 때문에 호스트를 스토리지 장치에 연결하기 위해 호스트 어댑터를 추가할 필요가 없고 스토리지 리소스를 보다 잘 이용할 수 있으며 별도의 WAN 인프라가 필요하지 않습니다. iSCSI에서는 SCSI에 대한 전송 수단으로 TCP/IP를 사용하므로 주로 이더넷으로 연결되는 기존의 IP 기반 호스트 연결을 통해 정보를 전달할 수 있습니다. 이외에도 기존의 스토리지 리소스를 보다 잘 활용할 수 있다는 장점이 있습니다. 호스트에서 기존의 IP/이더넷 네트워크 연결을 사용하여 스토리지 요소에 액세스할 수 있으므로 스토리지를 통합하고 활용도를 높이기가 쉬워졌습니다. 앞에서 설명한 대로 과거의 SAN에서는 WAN 연결을 별도로 제공해야 했습니다. 이제 기존의 WAN 연결을 사용하여 호스트가 IP를 통해 스토리지에 액세스함으로써 비용을 상당히 절약할 수 있습니다.

다른 IP SAN 프로토콜

IP 네트워크를 통한 스토리지 트래픽 전송에 관해 제안된 다른 초안들도 있습니다. 여기에는 FCIP(Fibre Channel over IP), iFCP(Internet Fibre Channel) 및 iSNS(Internet Storage Name Service) 등이 있습니다. 이러한 프로토콜은 이 문서의 범위를 벗어나지만 참고 자료에서 자세한 내용을 확인할 수 있습니다.

iSCSI 표준 트랙

iSCSI 초안은 IETF의 작업 그룹인 IPS(IP Storage)에서 개발 중인 여러 프로토콜 중 하나입니다. 시스코, IBM, HP와 같은 업계 선두 업체들은 초안을 표준화하기 위해 노력하고 있습니다. 현재 릴리즈는 2002년 6월 1일에 발표된 draft-ietf-ips-iscsi-14입니다. iSCSI 초안은 금년 후반기에 인터넷 엔지니어링 스티어링 그룹(IESG)에 제출되어 제안된 표준으로서 검토될 예정입니다. 수많은 공급 업체들이 현재의 초안 표준에 따라 제품을 개발하고 있습니다. 사전 표준 iSCSI 솔루션을 설치할 경우에는 상호 운용성을 이루기 위해 공급 업체 제품이 기반으로 하는 초안을 확인해야 합니다.

iSCSI의 기초

이 단원에서는 전체적인 기능을 이해하기 위해 iSCSI의 다양한 레이어와 프로세스에 대해 설명합니다. 따라서 자세한 패킷의 포맷과 구조는 의도적으로 생략되었습니다. 여기서는 주로 iSCSI와 IP를 통한 SCSI 전송에만 중점을 둡니다. 그러나 이 내용을 보다 쉽게 이해할 수 있도록 SCSI 아키텍처에 대해 간단히 설명합니다.

SCSI 아키텍처

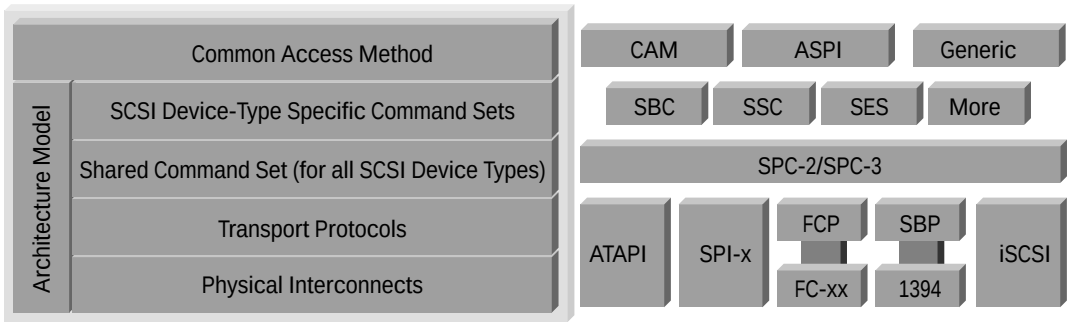
SCSI는 Small Computer Systems Interface를 나타냅니다. 이 용어는 디스크 드라이브 및 컨트롤러 제조업체인 SASI(Shugart Associates System Interface)에서 처음 사용되었습니다. IBM 입/출력(I/O) 채널을 기반으로 한 SASI 인터페이스는 널리 수용되었습니다. 처음 소개된 1979년 당시는 8비트 병렬 인터페이스만 사용할 수 있었습니다. SASI는 기본적으로 독립적인 병렬 장치를 중소형 컴퓨터에 연결하는 데 사용되었습니다.

1982년에 SASI를 기반으로 한 공식적인 SCSI 초안이 개발되었으며, 여기에 기능이 추가되어 1세대 SCSI 표준이 되었습니다. 새 기능에는 피어-투-피어 통신, 논리 장치, 중재 등이 있습니다.

미국 국립 표준기구(ANSI)는 1994년에 SCSI-2를 승인했습니다. SCSI-2는 모든 디스크 드라이버 외에도 많은 주변 장치에 소프트웨어 인터페이스를 제공하는 CCS(Common Command Set)의 확장된 정의를 포함하는 완전한 독립형 문서입니다. SCSI-2는 기본적으로 데이터 처리 성능을 배가하는 차등 인터페이스와 16비트 및 32비트 데이터 버스를 정의하며 SCSI-1과도 호환됩니다.

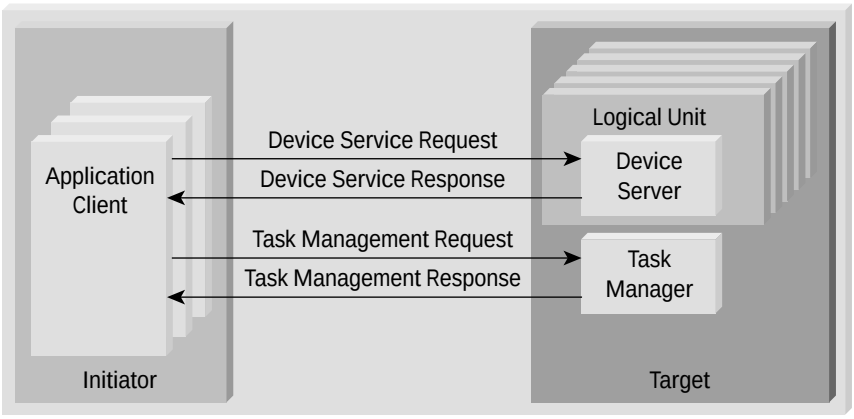
SCSI-3 표준은 현재 개발 중입니다. SCSI-3은 SCSI-2를 SCSI 아키텍처 모듈(SAM)이라는 일반적인 프레임워크에 맞춰 보다 작은 계층 모듈로 분해한 표준 모음입니다(그림 1 참조).

그림 1
SCSI 아키텍처 모델 및 SCSI-3 표준



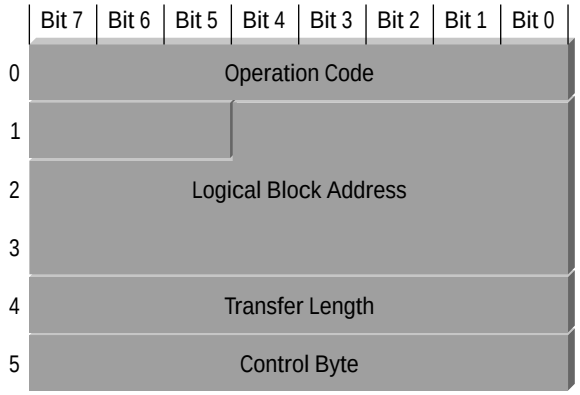
SAM은 SCSI 레이어의 개념, entity 및 상호 작용을 정의하며 클라이언트/서버 모델의 initiator and target entity에 대해 규정합니다. initiator and target entity 간의 상호 작용을 통해 initiator and target entity에 대한 정보를 교환할 수 있습니다(그림 2 참조). 이러한 정보의 예로 논리 장치 번호(LUN)가 있습니다.

그림 2
SCSI initiator and target entity 간의 상호 작용



SAM은 일반적인 요건과 구현 요건에 대해 정의합니다. 서비스 요청에는 SCSI 정보 교환을 위한 기본 빌딩 블록인 CDB(Command Descriptor Block)가 포함되어 있어야 합니다. CDB 포맷은 그림 3과 같습니다.

그림 3
SCSI CDB(Command Descriptor Block)

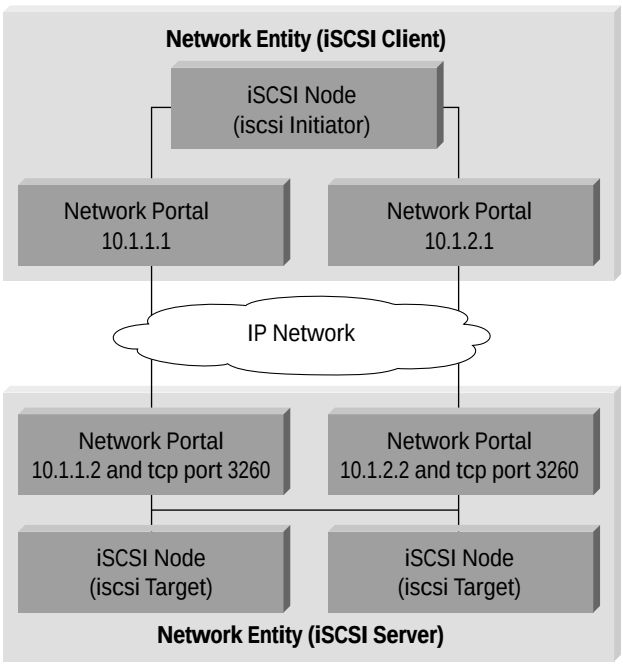


iSCSI 용어

iSCSI 초안에서는 IP 네트워크에 연결된 장치 또는 게이트웨이를 나타내는 "네트워크 entity"라는 개념을 사용합니다. 이 네트워크 entity는 하나 이상의 네트워크 포털을 포함해야 합니다. 네트워크 entity에 포함된 iSCSI 노드는 네트워크 포털을 사용하여 IP 네트워크에 액세스할 수 있습니다. iSCSI 노드는 네트워크 entity 내에서 해당 iSCSI 이름으로 식별되는 iSCSI initiator and target entity입니다. SAM의 정의에 따르면 SCSI 장치란 노드의 iSCSI 이름입니다. 하나의 iSCSI 노드에는 한 개의 SCSI 장치가 있습니다.

네트워크 포털은 기본적으로 TCP/IP 프로토콜 스택을 구현하는 네트워크 entity 내의 컴포넌트입니다. initiator entity에 관한 네트워크 포털은 해당 IP 주소로만 식별됩니다. iSCSI 대상 entity의 경우에는 해당 IP 주소와 TCP 수신 포트로 네트워크 포털을 식별합니다. iSCSI 클라이언트 및 서버의 컴포넌트는 그림 4를 참조하십시오. iSCSI 통신을 위해 initiator 네트워크 포털과 대상 네트워크 포털 간의 연결이 설정됩니다. initiator iSCSI 노드와 대상 iSCSI 노드 간의 TCP 연결 그룹이 iSCSI 세션을 구성합니다. SCSI I_T Nexus와 비슷하지만 똑같지는 않습니다.

그림 4
iSCSI 클라이언트 및 iSCSI 서버의 컴포넌트



표준 초안에서는 포털 그룹에 대해서도 정의합니다. iSCSI는 한 세션 내에서 다중 TCP 연결을 지원하므로 여러 네트워크 포털 간을 연결할 수 있습니다. 따라서 포털 그룹은 다른 네트워크 포털 간의 다중 연결로 구성되는 iSCSI 세션을 지원하는 네트워크 포털 집합입니다.

이름 및 주소 지정

iSCSI 프로토콜에서는 iSCSI initiator entity와 대상 entity의 이름 및 주소를 지정하기 위해 한 가지 방법을 사용합니다. 즉, 모든 iSCSI 노드와 initiator entity 및 대상 entity는 해당 iSCSI 이름으로 식별됩니다. iSCSI 이름은 IP 주소로 분석되는 호스트 유형 이름이나 세계적으로 통용되는 노드 이름이 아닙니다. 따라서 이 이름은 노드 위치와 상관이 없습니다. iSCSI 이름 포맷에는 iqn(iSCSI 한정자 이름) 포맷과 IEEE EUI 포맷 등 두 가지가 있습니다. iqn 포맷의 iSCSI 이름은 iqn.1987-05.com.Cisco.00.9f9ccf185aa2508c7a168967ccf96e0c.target1과 같습니다.

iSCSI 이름은 다음과 같은 기능을 제공한다는 점에서 유용합니다.

- 여러 initiator and target entity가 공통 IP 네트워크 주소를 공유할 수 있는 방법
- 다중 IP 주소를 통해 여러 initiator 또는 대상 entity를 액세스할 수 있는 방법
- 노드의 IP 주소와 방화벽에서의 IP 주소 및 포트 맵핑의 여부에 관계 없이 노드를 인식할 수 있는 방법

iSCSI 프로토콜은 iSCSI 이름에 대해 대소문자 일치 작업 이외의 어떤 처리 작업도 수행하지 않습니다.

iSCSI initiator entity 이름은 전세계적으로 이 initiator entity를 식별하는 고유 이름입니다. 마찬가지로 iSCSI 대상 entity 이름은 전세계적으로 이 대상 entity를 식별하는 고유 이름을 지정합니다. 이러한 이름은 SAM에서 정의한 SCSI I_T Nexus를 식별하는 데에도 도움이 됩니다.

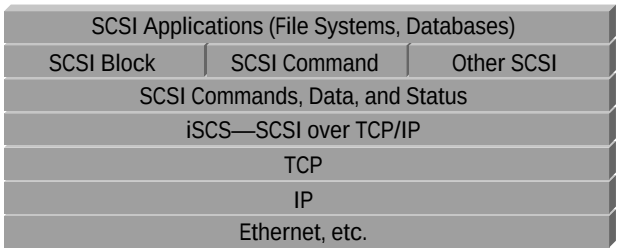
iSCSI 노드에 대한 주소 지정은 〈domain-name〉[:port]라는 표준 기반 IP 주소 지정 체계를 따릅니다. 〈domain-name〉은 도트 십진수 표기법인 IPv4 주소, 콜론으로 구분된 16진수 표기법인 IPv6 주소 또는 완벽한 도메인 이름 중 하나의 포맷을 사용합니다.

iSCSI 대상 entity의 경우 주소와 함께 포트 번호도 지정할 수 있습니다. 포트를 지정하지 않으면 IANA(Internet Assigned Numbers Authority)에서 할당한 기본 포트 3260이 사용됩니다.

iSCSI 프로토콜

iSCSI 프로토콜은 SCSI 원격 프로시저 호출(기준 SAM) 모델을 TCP/IP 프로토콜로 맵핑합니다. iSCSI 프로토콜은 전송하는 SCSI CDB 정보와 상관 없이 자체 개념 레이어를 제공합니다. 이러한 방식으로 SCSI 명령은 iSCSI 요청에 의해 전송되고 SCSI 응답 및 상태는 iSCSI 응답에 의해 처리됩니다. iSCSI 프로토콜 작업도 이와 같은 iSCSI 요청 및 응답 메커니즘에 의해 수행됩니다(그림5 참조).

그림 5
iSCSI 프로토콜 스택



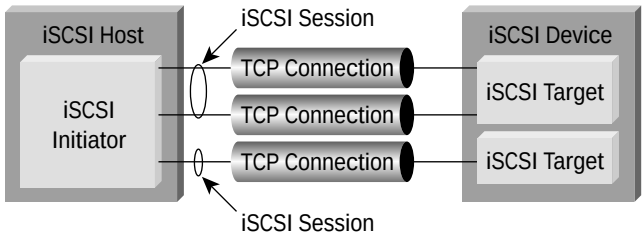
SCSI 프로토콜에서와 같이 iSCSI는 "initiator entity", "대상 entity" 및 프로토콜 데이터 단위(PDU)라는 통신 메시지의 개념을 사용합니다. 마찬가지로 iSCSI 전송 방향은 initiator entity를 기준으로 정의됩니다. 성능을 개선하기 위해 iSCSI는 "단계 축소"를 사용하여 명령 또는 응답과 관련 데이터를 단일 iSCSI PDU로 보낼 수 있습니다.

iSCSI 세션

iSCSI 통신 경로에서 가장 높은 수준은 iSCSI initiator entity와 iSCSI 대상 entity 사이에 형성되는 세션입니다. iSCSI에서는 두 종류의 세션이 정의됩니다. 하나는 정상 작동 세션이고 다른 하나는 initiator entity가 사용할 수 있는 대상 entity를 검색하기 위해 사용하는 검색 세션입니다.

세션은 initiator entity(ISID) 및 대상 entity(TSID) 컴포넌트로 구성된 세션 ID(SSID)로 식별됩니다. 세션 내에 TCP 연결을 추가하고 제거할 수 있지만 모든 연결은 동일한 initiator entity 및 대상 entity iSCSI 노드 간에 설정됩니다. 세션 내의 각 연결은 고유한 연결 ID(CID)를 가집니다. SSID, ISID, TSID 및 CID의 구성에 대해서는 이 문서의 뒤에서 보다 자세하게 설명합니다(그림 6 참조).

그림 6
연결이 한 개 이상 설정된 iSCSI 세션



iSCSI 세션은 iSCSI 로그인 프로세스를 통해 설정됩니다. 이 세션을 사용하여 특정 SCSI I_T Nexus와 연관된 모든 TCP 연결을 식별합니다. 한 세션 내에 한 개 이상의 TCP 연결이 있을 수 있습니다.

initiator entity가 알려진 포트나 지정된 대상 포트를 통해 원하는 대상에 대한 TCP 연결을 설정하면 로그인 프로세스가 initiator됩니다. initiator and target entity는 서로에 대한 인증을 수행하고 프로토콜에 대해 협상할 수 있습니다. 로그인 단계 중에 iSCSI initiator and target entity는 많은 속성에 대해 협상합니다.

로그인 단계를 성공적으로 마치면 세션은 "완전 기능 단계"에 들어갑니다. 로그인과 보안에 대해서는 뒤에서 추가로 설명합니다.

iSCSI 시퀀싱

iSCSI 프로토콜은 명령, 상태 및 데이터의 순서 및 시퀀싱을 유지 관리하기 위해 여러 가지 레지스터를 설치합니다. 각각의 레지스터는 부호 없는 32비트 정수 카운터입니다. 명령, 상태 및 데이터를 교환하는 동안 이 숫자들은 initiator entity와 대상 entity 간에 적절한 iSCSI PDU 필드로 통신됩니다. 또한 initiator entity나 대상 entity는 NOP-OUT/IN PDU를 이용하여 시퀀싱 및 번호 지정 레지스터를 동기화할 수 있습니다.

명령 번호 지정

iSCSI 세션 내에서 모든 명령(initiator entity-투-대상 entity PDU)에는 명령 시퀀스 번호(CmdSN)로 번호가 지정됩니다. CmdSN을 사용하면 한 세션에서 해당 명령을 전달하는 TCP 연결이 무엇이든 관계 없이 모든 명령이 전송된 순서대로 전달됩니다.

명령 시퀀싱은 첫 번째 로그인 명령에서 시작하여 이후의 각 명령에 대해 1씩 증가합니다. 명령을 해당 CmdSN 순서에 따라 SCSI 레이어에 전달하는 작업은 iSCSI target 레이어에서 담당합니다. 단, 즉시 전달하도록 표시된 명령은 제외됩니다. 이런 경우에는 CmdSN이 증가되지 않으며 iSCSI target entity가 명령을 탐지하는 즉시 바로 SCSI 레이어로 전달합니다.

initiator and target entity는 CmdSN 외에도 예상 명령 레지스터(ExpCmdSN)와 최대 명령 레지스터(MaxCmdSN)를 유지 관리합니다. target entity는 SCSI 레이어에 전달할 수 있는 가장 높은 번호이며 즉시 실행되지 않는 명령인 CmdSN에 1을 더한 값을 ExpCmdSN으로 설정합니다. initiator entity는 이 번호를 통해 대상이 수신한 마지막 시퀀스 명령을 확인합니다. 여러 TCP 연결을 통해 명령을 보낼 수 있기 때문에 target entity의 대기열에 CmdSN이 ExpCmdSN보다 높은 명령이 있을 수 있습니다. 시퀀스에 맞지 않는 명령이 SCSI 레이어에 전달되지 않도록 이러한 명령은 순서대로 보관됩니다. MaxCmdSN은 initiator entity가 target entity에 추가 명령을 보낼 대기열 공간이 있는지 확인하는 데 사용됩니다. 대기열 용량은 MaxCmdSN – ExpCmdSN + 1로 구할 수 있습니다.

상태 번호 지정

명령 번호 지정과 비슷하게 상태 응답에도 상태 시퀀스 번호(StatSN)가 순서대로 지정됩니다. 마찬가지로 initiator entity는 예상 상태 시퀀스 번호(ExpStatSN) 레지스터를 사용하여 target entity에서 수신한 상태 PDU를 확인합니다. StatSN과 ExpStatSN의 차이가 미리 설정된 값을 초과하면 initiator entity는 복구 작업을 시작합니다.

데이터 시퀀싱

데이터 및 요청-투-전송(R2T) PDU는 각각 DataSN과 R2TSN을 사용하여 순서가 지정됩니다. 데이터 시퀀싱은 같은 명령 내에서 데이터를 순서대로 전달하기 위해 사용됩니다.

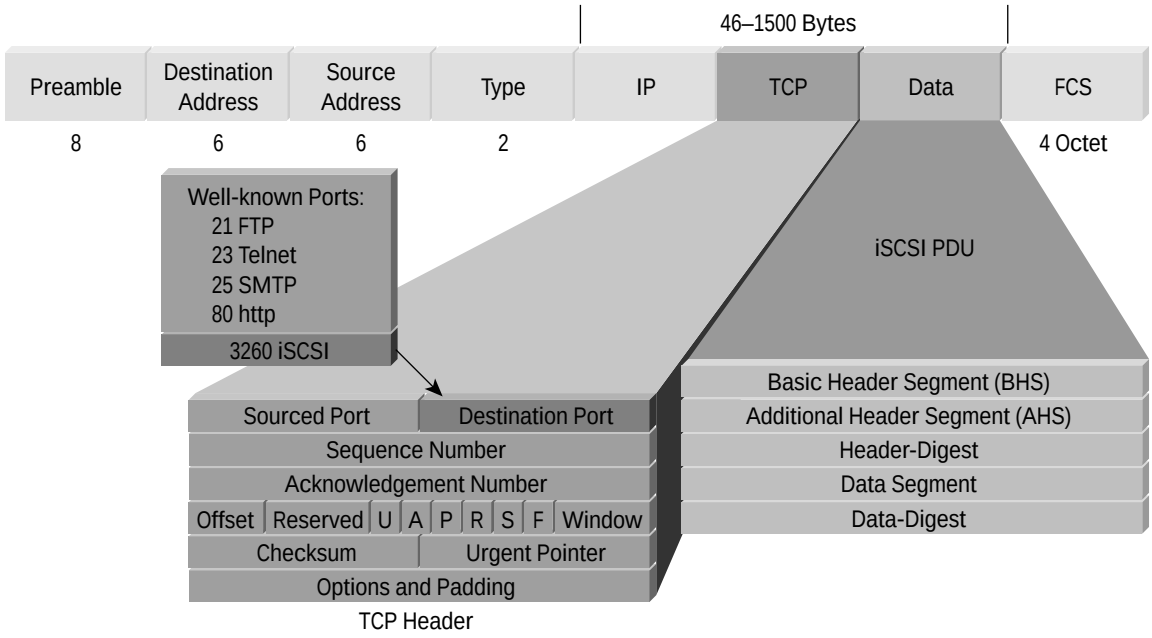
읽기 작업의 경우 DataSN은 0부터 시작하고 해당 명령 시퀀스에서 이후의 각 데이터 PDU에 대해 1씩 증가합니다. 쓰기 작업인 경우 R2T에 대한 응답인 첫 번째 임의 데이터 PDU 또는 첫 번째 데이터 PDU는 DataSN 0부터 시작하고 이후의 각 데이터 PDU에 대해 1씩 증가합니다. R2TSN은 명령을 시작할 때 0으로 설정되고, target entity가 해당 명령에 대해 보낸 이후의 각 R2T에 대해 1씩 증가합니다.

iSCSI PDU

iSCSI 패킷의 TCP 페이로드는 iSCSI PDU를 포함합니다. 모든 iSCSI PDU는 하나 이상의 헤더 세그먼트로 시작하며 다음에 0개 또는 한 개의 데이터 세그먼트가 옵니다.

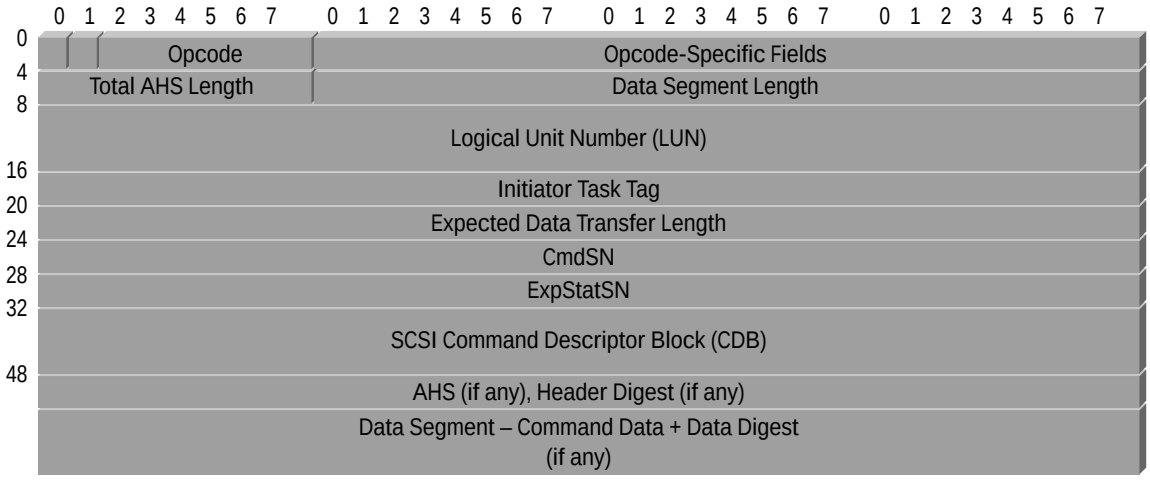
첫 번째 세그먼트는 고정 길이 48바이트의 기본 헤더 세그먼트(BHS)입니다. BHS 다음에 추가 헤더 세그먼트(AHS)가 올 수 있습니다. 그림 7에서는 iSCSI PDU의 포맷과 내용을 보여 줍니다. BHS를 제외한 모든 헤더는 옵션입니다. 이 그림은 TCP 페이로드에 iSCSI PDU가 포함된 iSCSI 패킷에 대해 설명합니다.

그림 7
iSCSI 패킷 포맷



iSCSI PDU의 종류에는 iSCSI 요청 및 응답, 텍스트 요청 및 응답, 로그인 요청 및 응답 등이 있습니다. 그림 8에서는 iSCSI 요청 명령 중 하나의 헤더 포맷에 대한 예를 보여 줍니다.

그림 8
iSCSI PDU 명령



iSCSI 오류 처리

오류 복구는 기본적으로 잘못된 프로세스를 복구하기 위해 충분한 상태 및 데이터를 유지 관리하는 것입니다. iSCSI의 경우 initiator entity는 해결되지 않은 PDU를 다시 작성하기 위해 필요한 명령과 데이터 정보를 보유해야 합니다. 이와 마찬가지로 target entity는 상태 응답 정보와 함께 확인되지 않은 데이터 출력을 유지 관리해야 합니다.

iSCSI에서 오류 처리를 위해 사용하는 두 가지 메커니즘은 재시도와 재할당입니다. initiator entity는 같은 명령 또는 데이터 PDU를 target entity에 다시 보내서 누락된 CmdSN을 "연결(plug)"하려고 할 수 있습니다. 재할당은 initiator entity와 target entity 간의 TCP 연결이 끊어진 경우에 사용됩니다. 이 경우 initiator entity는 새로운 연결을 통해 "작업 재할당" 작업 관리 PDU를 전송함으로써 target entity에게 해결되지 않은 명령을 새로운 CID에서 계속하도록 명령합니다. target entity에서 이 기능을 지원할 필요는 없으며 로그인할 때 지원 여부를 협상합니다.

iSCSI 프로세스

이 단원에서는 전체적인 iSCSI 연결 설정, 교환 및 종료에 대해 설명합니다. 실제 iSCSI 구현에서는 인증, 암호화, 다양한 파라미터 설정, 기타 SCSI 작업 등과 같은 여러 가지 다른 작업을 수행할 수 있습니다. 이 단원의 목적은 iSCSI 단계 및 프로세스 흐름에 대한 기본적인 이해를 제공하기 위한 것입니다.

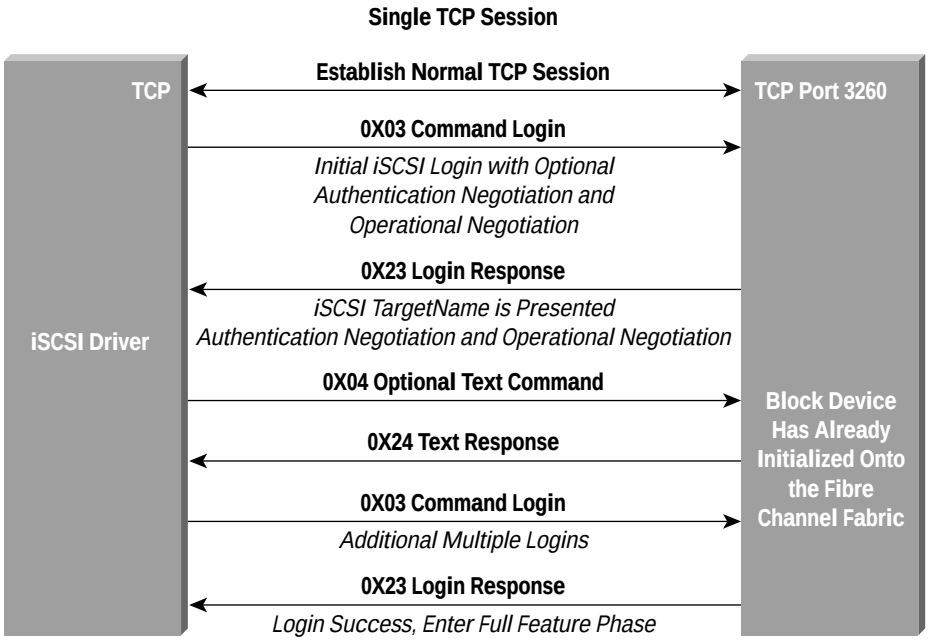
로그인 프로세스는 로그인 initiator 요청으로 시작되고 이후에 initiator entity가 추가 로그인 요청으로 응답하는 로그인 부분 응답(옵션)이 수행되는 로그인 단계의 측면에서 설명됩니다. 추가 파라미터 설정이 필요할 때마다 로그인 부분 응답과 추가 로그인 요청을 반복할 수 있습니다. 이 단계 이후에는 target entity로부터 로그인 최종 응답이 수행되어 "로그인 허용"이나 "로그인 거부"를 나타내야 합니다.

로그인 시작

iSCSI 로그인은 iSCSI initiator entity와 iSCSI target entity 간의 iSCSI 세션을 설정하는 데 사용됩니다. TCP 연결은 iSCSI 세션에 속해 있어야 하고 iSCSI initiator entity와 iSCSI target entity는 보안 인증 및 기타 운영 파라미터를 교환하고 합의합니다.

이 프로세스는 initiator entity가 target TCP 수신 포트에서 target entity에 대한 TCP 연결을 열고 CID를 할당하면서 시작됩니다. 그런 다음 initiator entity는 자신이 지원하는 프로토콜 버전, SSID, CID 및 시작하려는 설정 단계 등이 포함된 로그인 요청을 보냅니다. 선택 사항으로 초기 요청에 보안 파라미터나 iSCSI 운영 파라미터를 포함시킬 수도 있습니다. 그림 9에서는 iSCSI 로그인 프로세스를 보여 줍니다.

그림 9
iSCSI 로그인 패킷 흐름



앞에서 설명한 대로 SSID는 ISID와 TSID로 구성됩니다. ISID는 SSID의 처음 6바이트로 1바이트의 유형, 3바이트의 이름 지정 기관 및 2바이트의 한정자 필드로 구성됩니다(표 1 참조). 유형 바이트는 이름 지정 기관의 포맷을 나타냅니다(표 2 참조). ISID의 이름 지정 기관(Naming Authority) 필드는 이 iSCSI initiator entity의 공급업체 또는 조직입니다. 마지막으로 한정자는 부호 없는 16비트 정수로 특정 initiator entity와 target 포털 그룹 조합에 대해 고유해야 합니다.

TSID는 target entity의 iSCSI 노드에 따라 결정되는 16비트 값입니다. initiator entity가 target entity와의 새 세션을 설정하면 초기 로그인 요청의 TSID는 0으로 설정됩니다. 이 값은 새 세션이 요청되었음을 target entity에게 알립니다. target entity는 TSID를 생성하여 로그인 응답으로 반환합니다. initiator entity가 기존 세션에서 추가 TCP 연결을 설정하려는 경우에는 세션이 생성되었을 때 이전에 성공한 로그인 시도에서 알게 된 TSID를 사용합니다. 값이 0이 아니므로 target entity는 initiator entity가 이미 설정된 세션에 연결을 추가하려고 한다는 것을 알 수 있습니다. initiator entity가 초기 로그인 응답에서 TSID를 수신하면 SSID가 완성되며 이 SSID는 이후의 모든 로그인 PDU에서 세션을 식별하는 데 사용됩니다.

표 1: 세션 ID 필드

SSID	바이트 0	바이트 1	바이트 2	바이트 3
단어 0	유형	이름 지정 기관		
단어 1	한정자		TSID	

initiator entity 부분: ISID

target entity 부분: TSID

표 2: 유형 바이트 정의

유형	이름 지정 기관
0x00	IEEE OUI
0x01	IANA 기업 번호
0x02	"임의"
0x03-0xFF	예약됨

인증 및 파라미터 설정

initiator and target entity를 인증해야 하는 경우에는 운영 파라미터를 교환하기 전에 인증을 설정해야 합니다. 인증에는 다양한 방법을 사용할 수 있으며 이에 대해서는 뒤에서 설명합니다. 파라미터 협상은 initiator entity가 보낸 초기 로그인 요청으로 시작됩니다. 초기 entity는 인증이 성공적으로 완료된 후에(필요한 경우) 파라미터 협상을 진행할 수 있습니다. 일부 운영 파라미터는 텍스트 포맷으로 전달됩니다. 이러한 교환에서 사용하는 포맷은 다음과 같습니다.

발신 포맷: <key>=<value>

응답 포맷: <key>=<value>|None|Reject|NotUnderstood|Irrelevent|

〈value〉 인수는 숫자, 리터럴, 부울(예 또는 아니오) 또는 쉼표로 구분한 리터럴 값의 목록이 될 수 있습니다. 발신자가 〈values〉 목록을 제공하면 응답자는 지원되는 첫 번째 값으로 응답하거나, 지원되지 않는 경우 "거부(Reject)"해야 합니다. 리터럴 목록의 경우 "없음(None)" 응답은 "없음(None)"이 사용 가능한 값 중 하나로 제공된 경우에만 허용됩니다. 공급업체가 키 앞에 X를 첨부하고 뒤에 해당 도메인 이름을 역으로 붙여 새로운 〈key〉를 추가할 수도 있습니다.

연결

initiator entity가 target entity로부터 로그인 최종 응답을 수신하면 로그인 프로세스가 종결됩니다. "로그인 거부"라는 응답을 받으면 로그인에 실패한 것이며 initiator entity는 CID로 식별되는 해당 TCP 연결을 닫아야 합니다. "로그인 허용" 응답을 수신하면 세션은 완전한 기능 단계로 들어갑니다(초기 로그인 시도인 경우). 완전한 기능 단계에 도달한 경우에만 initiator entity가 iSCSI PDU에 포함된 SCSI 명령과 데이터 정보를 보낼 수 있습니다.

주어진 iSCSI 세션에 대해 여러 개의 TCP 연결이 설정되어 있으면(다중 로그인) 이후의 데이터 및 응답 PDU는 관련 명령을 보냈던 TCP 연결(CID)을 통해 보내야 합니다. 이런 개념을 "연결 고수(connection allegiance)"라고 합니다. 발신 CID가 실패한 경우 앞에서 설명한 오류 복구 절차로 인해 연결 고수가 다시 설정될 수 있습니다. 반대로 SCSI 작업과 관련된 여러 개의 명령을 다른 TCP 연결을 통해 보낼 수도 있습니다. 또한 관련 없는 SCSI 명령, 데이터 및 상태를 iSCSI 세션에 끼워넣을 수 있습니다. 그러나 각각의 해당 데이터와 응답은 연결 고수 규칙을 따라야 합니다.

협상되는 운영 파라미터 중 하나는 target entity가 발신 데이터 전송(SCSI Write)을 위해 유도(R2T) 모드 또는 임의 모드로 작동하는지를 나타냅니다. 임의 모드인 경우 initiator entity가 "즉시 데이터"를 명령과 같은 PDU로 보내거나(단계 축소) 별도의 PDU로 보낼 수 있습니다. 각각의 경우에 대해 initiator entity가 보낼 수 있는 데이터의 최대량은 로그인 시 설정할 수 있습니다. 초기 즉시 데이터를 보낸 이후의 모든 데이터 PDU는 R2T 응답에 대한 회신으로 보내야 합니다(유도 모드).

initiator and target entity는 명령, 데이터 및 응답 교환의 순서를 유지 관리하기 위해 앞에서 설명한 시퀀스 번호 지정 체계를 사용합니다. initiator entity는 비동기적 조건을 확인하면 SNACK 요청을 보낼 수 있습니다. 단일 SNACK은 시퀀스 번호 레지스터에 따라 누락된 연속 데이터 집합을 처리합니다.

로그아웃 및 종료

로그아웃 프로세스는 iSCSI 연결 또는 세션을 닫기 위한 적절한 종료 메커니즘입니다. 로그아웃 절차를 시작하는 것은 initiator entity이지만 내부 오류 조건을 나타내는 비동기 iSCSI 메시지를 보내 이 절차를 수행하는 것은 target entity입니다. 어떤 경우든 initiator entity가 로그아웃 요청을 보낸 후에는 다른 요청을 보낼 수 없습니다. target entity에서 로그아웃 응답을 보내면 정리가 완료되었고 이 연결에서 다른 응답을 보낼 수 없다는 것을 나타냅니다. 또한 로그아웃 응답에는 target entity에서 보낸 복구 정보도 포함되어 있습니다. 이런 복구 정보에는 target entity가 복구를 위해 명령 정보를 보류하면서 대기하는 시간 길이(Time2Retain)와 initiator entity가 연결을 다시 설정할 수 있기까지 기다려야 하는 시간 길이(Time2Wait) 등이 있습니다. 마지막으로 TCP FIN을 보내 연결을 종료합니다.

보안 고려 사항

과거에는 스토리지 장치 및 스토리지 네트워크와 관련된 보안은 주요 고려 사항이 아니었습니다. 스토리지 장치는 호스트에 직접 연결되거나 사용자가 액세스할 수 있는 네트워크와는 별도의 SAN을 통해 연결되었습니다.

iSCSI의 경우 다른 IP 기반 SAN 프로토콜과 마찬가지로 스토리지 정보를 개방형 IP 네트워크를 통해 전송하기 때문에 보안 위험이 있습니다. 이런 점을 알고 있기 때문에 IP Storage 작업 그룹에서는 IP 기반 스토리지 통신을 보안하기 위한 초안을 개발했습니다. 이 작업은 "Securing Block Storage Protocols over IP" 초안에 포함되어 있습니다. iSCSI 프로토콜 초안에서는 보안, 인증 및 패킷 보호와 관련하여 두 가지 요소를 지정합니다.

인증

iSCSI에서는 로그인 프로세스 중에 target entity가 initiator entity를 인증할 수도 있고 initiator entity가 target entity를 인증할 수도 있습니다. 이러한 인증은 파라미터 설정이나 로그인 허용 전에 수행됩니다. 인증을 이용하는 경우 iSCSI 세션 내의 각 연결이 인증되어야 합니다. iSCSI 초안에는 다음 인증 방법이 정의되어 있으며 로그인 단계에서 "AuthMethod" 키를 통해 설정됩니다.

- KRB5 커버로스 V5
- SPKM1 단순한 공개 키 일반 보안 서비스(GSS) 애플리케이션 프로그래밍 인터페이스(API) 메커니즘
- SPKM2 단순한 공개 키 GSS API 메커니즘
- SRP 보안 원격 암호
- CHAP 챌린지 핸드셰이크(Challenge Handshake) 인증 프로토콜
- 없음 인증 없음

이 메커니즘은 target 장치에 권한 없이 연결하는 것을 방지할 수 있지만 연결한 이후의 PDU 교환에 대해 보호하지는 못합니다.

패킷 보호

패킷 보호는 iSCSI 노드 간 통신에서의 무결성, 인증 및 기밀 유지를 보장합니다. iSCSI 연결의 경우 IP 레이어에서 개인 정보를 안전하게 교환하기 위해 IP Security(IPSec)를 사용합니다. 초안을 준수하려면 iSCSI 네트워크 요소는 재생 방지 기능을 비롯하여 ESP(Encapsulating Security Protocol)의 IPSec 터널 모드를 구현해야 합니다. iSCSI 구현의 빠른 속도로 인해 IPSec 시퀀스 번호 확장은 속도에 따라 구현될 수 있고 또 구현되어야 합니다.

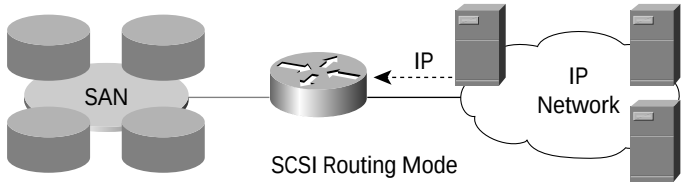
기밀 유지를 위해 3DES(Triple Digital Encryption Standard)를 사용하여 CBC(Cipher Block Chaining) 모드로 IPSec 터널을 암호화합니다. iSCSI 노드는 인증, 보안 연관 협상 및 키 관리를 제공하기 위해 IKE(Internet Key Exchange)를 지원해야 합니다. 별도의 IKE Phase 2 Security Association은 iSCSI 세션 내의 각 TCP 연결을 보호합니다.

iSCSI 구현

Cisco SN 5420 및 5428 스토리지 라우터는 iSCSI 초안 8을 지원합니다. 이들 라우터는 iSCSI를 블록 수준 스토리지 액세스를 위한 전송 수단으로 사용합니다. 일반적인 파이버 채널 SAN에서 스토리지 장치/LUN은 IP 네트워크 호스트에 마치 직접 연결되어 있는 것처럼 표시됩니다. iSCSI 작업을 지원하려면 IP 호스트에 iSCSI 드라이버나 iSCSI 네트워크 인터페이스 카드를 설치해야 합니다.

Cisco SN 5420 스토리지 라우터는 iSCSI target entity로 작동하는 반면 IP 호스트는 iSCSI initiator entity 기능을 합니다. IP 호스트는 Cisco SN 5420 스토리지 라우터에 접속하여 정의된 iSCSI target 주소와 포트를 통해 iSCSI 로그인을 수행합니다. 스토리지 라우터는 교환되는 정보와 설정된 파라미터에 따라 로그인(또는 다중 로그인)을 허용하거나 거부합니다. Cisco SN 5420은 iSCSI target/LUN을 실제의 물리적 target/LUN에 맵핑합니다. iSCSI 로그인에 성공하면 작동이 완전한 기능 단계로 돌입하고 데이터 전송을 할 수 있게 됩니다. 따라서 IP 네트워크에 있는 iSCSI initiator entity가 물리적 스토리지 target/LUN을 사용할 수 있게 됩니다. 그림 10에서는 Cisco SN 5420 구현의 iSCSI target 모드 또는 SCSI 라우터 모드를 보여 줍니다.

그림 10
iSCSI 구현 예



Cisco SN 5420은 iSCSI target 모드 외에도 투명 모드와 iSCSI 다중 initiator entity 모드를 지원합니다. Cisco SN 5420은 주로 분산 환경에서의 스토리지 통합/중앙 집중화 및 원격 백업에 사용됩니다.

Cisco SN 5420 스토리지 라우터에 대한 자세한 내용은 아래의 Cisco 웹 페이지를 참조하십시오.
http://www.cisco.com/warp/public/cc/pd/rt/5420/

요약

iSCSI의 표준화는 스토리지 업계에서 혁신적인 기술이 될 것입니다. iSCSI는 기존 스토리지 네트워크의 물리적 제약을 제거하므로 가까운 장래에 워크그룹 및 엔터프라이즈 네트워크에 상당한 영향을 끼치는 기술이 될 것이 확실합니다. 표준 기반의 장치가 많이 출시되고 있기 때문에 네트워크 기술자들은 iSCSI 프로토콜 및 이와 관련된 구현 요건에 대해 이해할 필요가 있습니다. 이 문서는 특히 iSCSI 프로토콜에 중점을 두고 있으며 구현 시의 고려 사항에 대해서는 다루지 않습니다. 하지만 성능, 보안, 애플리케이션 요건 등 구현과 관련된 일부 주제는 여기서 설명합니다. 구현 시의 고려 사항으로는 장치 기능, 네트워크 기능, QoS 파라미터, 애플리케이션별 요건 등이 있습니다. 이러한 영역에 대한 정보는 백서, 설계 안내서, 제품 인증서 및 애플리케이션 정보와 같은 추가 자료를 참조하십시오.

추가 자료는 다음과 같은 웹 사이트에서 살펴볼 수 있습니다.

http://www.cisco.com

http://www.ietf.org/html.charters/ips-charter.html

http://www.snia.org/

참조 문서

IETF IPS 작업 그룹, 문서: draft-ietf-ips-iscsi-14
IETF IPS 작업 그룹, 문서: draft-ietf-ips-security-11
SCSI-3 아키텍처 모드, 문서 번호: X3.270-1996

CISCO SYSTEMS

www.cisco.com/kr

2003-03-05

■ Gold 파트너	•㈜데이콤아이엔	02-6250-4700	•한국아이비엠㈜	02-3781-7800	•쌍용정보통신㈜	02-2262-8114
	•㈜데이타크레프트코리아	02-6256-7000	•㈜콤텍시스템	02-3289-0114	•에스넷시스템㈜	02-3469-2400
	•㈜인네트	02-3451-5300	•㈜인성정보	02-3400-7000	•현대정보기술	02-2129-4111
	•㈜링네트	02-6675-1216	•한국후지쯔㈜	02-3787-6000	•케이디씨정보통신㈜	02-3459-0500
	•한국휴렛팩커드㈜	02-2199-0114				
■ Silver 파트너	•대우정보시스템	02-3708-8642	•㈜시스폴	02-6009-6009	•한국NCR	02-3279-4423
	•한국유니시스㈜	02-768-1114,1432				
■ Local SI 파트너	•㈜LG씨엔에스	02-6276-2821	•포스데이타주식회사	031-779-2114	•이스텔시스템즈㈜	031-467-7079
	•SK씨앤씨㈜	02-2196-7114/8114				
■ Global 파트너	•이퀀트코리아	02-3782-2600				
■ Local 디스트리뷰터	•㈜소프트뱅크코리아	02-2187-0114	•㈜인큐브테크	02-3497-9303	•㈜아이넷뱅크	02-3400-7486
■ IPT 파트너	•청호정보통신	02-3498-3114	•LG기공	02-2630-5156		
■ WLAN 전문 파트너	•㈜에어키	02-541-1557	•(주)텔레트론INC	02-2105-2300		
■ Security 전문 파트너	•코코넛	02-6007-0133	•TISS	051-743-5940		
■ NMS 전문 파트너	•㈜넷브레인	02-573-7799				