INSTYTUT BADAŃ SYSTEMOWYCH
POLSKIEJ AKADEMII NAUK

TECHNIKI INFORMACYJNE TEORIA I ZASTOSOWANIA

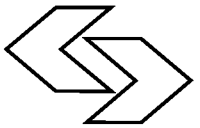
Wybrane problemy
Tom 1(13)

poprzednio

ANALIZA SYSTEMOWA W FINANSACH I ZARZĄDZANIU

Pod redakcją
Jerzego HOŁUBCA

Warszawa 2011



INSTYTUT BADAŃ SYSTEMOWYCH
POLSKIEJ AKADEMII NAUK

TECHNIKI INFORMACYJNE TEORIA I ZASTOSOWANIA

Wybrane problemy
Tom 1(13)

poprzednio

ANALIZA SYSTEMOWA W FINANSACH I ZARZĄDZANIU

Pod redakcją
Jerzego HOŁUBCA

Warszawa 2011

Wykaz opiniodawców artykułów zamieszczonych
w niniejszym tomie:

Dr hab. inż. Przemysław GRZEGORZEWSKI, prof. PAN

Prof. dr hab. inż. Jerzy HOŁUBIEC

Dr inż. Tatiana JAWORSKA

Dr hab. inż. Wiesław KRAJEWSKI, prof. PAN

Dr hab. inż. Maciej KRAWCZAK, prof. PAN

Dr hab. Michał MAJSTEREK

Dr hab. inż. Andrzej MYŚLIŃSKI, prof. PAN

Prof. dr hab. inż. Witold PEDRYCZ

Dr hab. inż. Ryszard SMARZEWSKI, prof. KUL

Prof. dr hab. inż. Andrzej STRASZAK

Dr Dominik ŚLĘZAK

Prof. dr hab. inż. Stanisław WALUKIEWICZ

ISBN 9788389475336

iSCSI ALTERNATYWĄ DLA STANDARDU FC

Adrian Witlib
Studia Doktoranckie IBS PAN

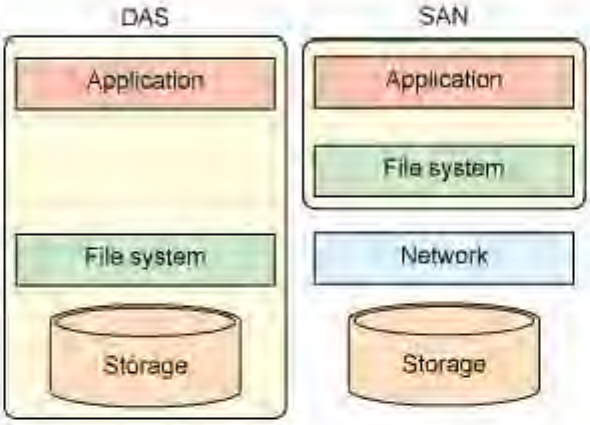
Celem artykułu jest przedstawienie informacji na temat możliwości zastosowania protokołu iSCSI jako alternatywy dla protokołu Fibre Channel w kontekście implementowania sieci typu SAN, jak również opisanie zasad działania samego protokołu. Zawiera informacje ogólne o sieciach SAN w zestawieniu z modelem dostępu DAS. Jednocześnie, pokazuje historię powstawania iSCSI jak również mechanizmy jego działania. Opisuje sposób enkapsulacji w ramce ethernetowej, identyfikatory i adresację urządzeń iSCSI, a także proces zestawiania połączenia pomiędzy inicjatorem i targetem. Artykuł przedstawia również metody wykrywania zasobów dyskowych w sieci i typy adapterów, które pozwalają na logowanie się do zasobów iSCSI.

***Abstract**. Main purpose of this article is to present information about usage of iSCSI protocol as an alternative to Fibre Channel Protocol for implementing SAN networks as well as how does it work. It contains general description of SAN and how does it compare do DAS. It also presents history of iSCSI development and the way it works. This article describes iSCSI encapsulation in Ethernet frame, iSCSI identifiers and devices dressing as well as process of establishing initiator-target connection. Storage location protocols and types of iSCSI host bus adapters are also presented.*

1. Wstęp

Typowy komputer, z którym spotykamy się na co dzień, przechowuje dane na podłączonym bezpośrednio, dedykowanym, dysku twardym. Ograniczenia takiego rozwiązania sprawiły jednak, że w przypadku większości dużych środowisk produkcyjnych w firmach i organizacjach, stosowany jest alternatywny, sieciowy, model dostępu do danych, a mianowicie SAN (ang. Storage Area Network). Sieci tego typu, w odróżnieniu od sieci ogólnego przeznaczenia - LAN, wykorzystywane są jedynie w celu uzyskania dostępu do scentralizowanych zasobów dyskowych. Przestrzeń ta zlokalizowana jest najczęściej na macierzach dyskowych, do których dostęp odbywa się na poziomie bloków, za

sprawą czego zasób SAN widziany jest przez serwer jako dysk twardy SCSI. Wariant ten pozwala administratorowi serwera na samodzielne podjęcie decyzje o wyborze systemu plików czy podziale na partycje tak samo jak czyni to w przypadku podłączania fizycznego dysku twardego. Porównanie bezpośredniego (DAS, ang. Direct Attached Storage) oraz sieciowego (SAN) modelu dostępu do danych przedstawia rys. 1.1.



Rys. 1.1. Porównanie DAS i SAN. (źródło: IBM.com)

Przez lata sieci typu SAN realizowane były jedynie w oparciu o powstały i zatwierdzony jako standard ANSI w latach 80'-90' protokół FC (ang. Fibre Channel). Istotną jego wadą jest jednak konieczność zakupienia drogiego, dedykowanego do FC sprzętu wraz z oprogramowaniem zarządzającym i zaimplementowania niezależnej sieci światłowodowej. Sama implementacja i późniejsze zarządzanie środowiskiem FC wymaga zaś administratorów posiadających wiedzę w tym zakresie, których należy dodatkowo zatrudnić lub przeszkolić aktualnie zatrudnionych pracowników. W obu przypadkach są to dodatkowe koszty.

Powody te ograniczały możliwość wejście w świat sieci SAN firm nie dysponującym odpowiednio wysokim budżetem. Sytuacja uległa jednak zmianie dzięki firmie IBM, która w drugiej połowie lat 90' rozpoczęła prace nad analizą możliwościami przesyłu SCSI za pośrednictwem TCP/IP. W 1999 r. IBM zaprezentował swoje rozwiązanie CISCO, w efekcie czego firmy rozpoczęły współpracę i już w lutym 2000 r. roboczą wersję SCSI over TCP/IP pokazano na spotkaniu z największymi firmami w branży IT. Większość z nich wyraziła poparcie dla tej technologii. W tym samym roku uformowała się grupa

mająca na celu eliminację problemów, z którymi borykała się robocza wersja protokołu i późniejsze przedstawienie go do standaryzacji. Działania te zaowocowały ostatecznie powstaniem nowego standardu i pojawieniem się na początku 2001 r. pierwszych produktów wykorzystujących iSCSI. [1].

Wprowadzenie iSCSI umożliwiło realizowanie sieci SAN dużo taniej, ponieważ w oparciu o istniejące już w firmach sieci LAN, z wykorzystaniem istniejącego sprzętu przełączającego i okablowania, a nawet zintegrowanych ze zwykłymi, biurkowymi komputerami, ethernetowych kart sieciowych. Jednocześnie administracja ruchem iSCSI mogła być realizowana przez zatrudnionych już administratorów LAN. Do listy zalet iSCSI należałoby dodać fakt, iż ramkę zawierającą iSCSI traktuje się podczas przesyłania jak zwykłą ramkę Ethernet, więc można wobec niej stosować takie same, istniejące technologie jak QOS czy IPsec. Ramkę zawierającą iSCSI przedstawia rys. 1.2.

Rys. 1.2. Ramka zawierająca iSCSI. (źródło: www.10gea.org)

2. Identyfikatory iSCSI

Standard iSCSI wymaga, aby każdy uczestnik wymiany danych legitymował się identyfikatorem. Identyfikator ten ma być globalnie unikatowy (z pewnymi wyjątkami, dla których dopuszcza się zarządzanie na poziomie lokalnym) i jednocześnie nie być powiązany z fizyczną lokalizacją urządzenia iSCSI.

Zdefiniowane zostały trzy schematy nazewnictwa [1][2]. Pierwszy z nich, najpopularniejszy, czyli IQN zawiera deklarację typu identyfikatora (iqn/eui/naa), datę uzyskania od organu rejestrującego DNS domeny producenta urządzenia oraz samą domenę w odwróconej postaci (np. com.cisco). Ostatnim, opcjonalnym, elementem jest oddzielony dwukropkiem lub kropką ciąg znaków w ramach którego producent nadaje unikalne identyfikatory swoim produktom iSCSI. Pozostałe dwa schematy identyfikatorów – EUI oraz NAA zawierają tylko dwie sekcje: deklarację typu identyfikatora oraz sam unikatowy identyfikator.

Przykładowe identyfikatory:

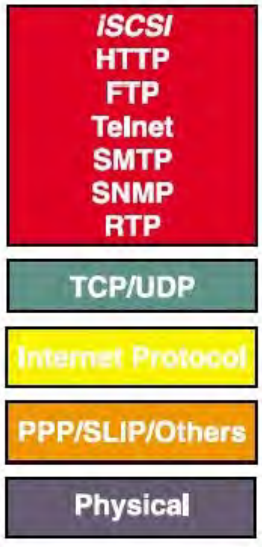
iqn.1987-05.com.cisco:host1 – IQN, wariant z dwukropkiem,

eui.02004567A425678D – EUI,

naa.62004567BA64678D0123456789ABCDEF – NAA, 16bit.

3. Adresacja i zestawianie połączenia iSCSI

Podane wcześniej identyfikatory, jak sama nazwa wskazuje, służą jedynie identyfikacji urządzeń iSCSI. Nie są one translowane na adresy IP, w związku z czym nie mogą być wykorzystywane do routingu w ramach sieci opartych o TCP/IP, na których bazuje iSCSI. Aby uzupełnić ten brak, wprowadzono pojęcie Portalu, który jest de facto adresem IP interfejsu urządzenia pracującego w sieci. W ramach iSCSI adres ten posiada zarówno strona inicjująca operację SCSI (ang. initiator) jak i ta będąca jej celem (ang. target). W przypadku targetu, poza adresem IP, wykorzystywany jest także port TCP, na którym odbywa się nasłuchiwanie nadchodzących żądań ze strony inicjatora. Dzięki takiej dwoistości, zapewniony jest zarówno routing na niższych warstwach OSI (adresy IP) jak i identyfikowanie urządzeń i operowanie w ramach iSCSI ulokowanego w warstwie aplikacji. Umiejscowienie iSCSI w warstwie aplikacji przedstawia rys. 3.1.



Rys. 3.1. Lokalizacja iSCSI w modelu warstwowym. (źródło: www.10gea.org)

W momencie, gdy zachodzi potrzeba rozpoczęcia operacji SCSI, inicjator loguje się do targetu. Po zakończeniu tego procesu, po obu stronach następuje dynamiczne otwarcie portów iSCSI. Porty te są identyfikowane w oparciu o adresy generowane wg następującego schematu:

Po stronie inicjatora: <identyfikator inicjatora>, i, <identyfikator sesji inicjatora (ISID)>

Przykład: **iqn.1987-05.com.cisco:host1,i,0x00023d000002**

Po stronie targetu: <identyfikator targetu>, t, <Tag Grupy Portalowej, do której należy dany target (TPGT)> - TPGT uzyskiwane jest w oparciu o adres IP, na który przyszłą prośba logowania się inicjatora.

Przykład: **iqn.1987-05.com.cisco:array1,t,0x4097** [2]

Pomiędzy parą identyfikatorów portów iSCSI może być zestawiona jedynie jedna sesja, ale możliwe jest utrzymywanie wielu równoległych sesji przy wykorzystaniu innych identyfikatorów portów iSCSI (o odmiennych od już wykorzystywanych kombinacji ISID i TPGT). [2]

Sama procedura logowania składa się z dwóch faz, a mianowicie z negocjacji parametrów związanych z bezpieczeństwem oraz negocjacji parametrów związanych z pracą.

Pierwsza z faz jest opcjonalna, jednak jeśli występuje, musi odbyć się przed negocjacją parametrów pracy. Według standardu, druga faza również nie musi być implementowana, ponieważ parametry po stronie inicjatora i targetu mogą zostać prekonfigurowane, jednak w praktyce zawsze stosuje się autonegocjację, ponieważ oferuje ona większą elastyczność.

Po zakończeniu procedury logowania następuje tzw. faza full feature, podczas której inicjator i target dokonują właściwych operacji SCSI w oparciu o zestawione sesje iSCSI. Faza ta przewiduje również możliwość renegocjacji parametrów ustalonych podczas fazy logowania. Na koniec, inicjator może wylogować się z targetu. [2]

4. Uwierzytelnianie urządzeń

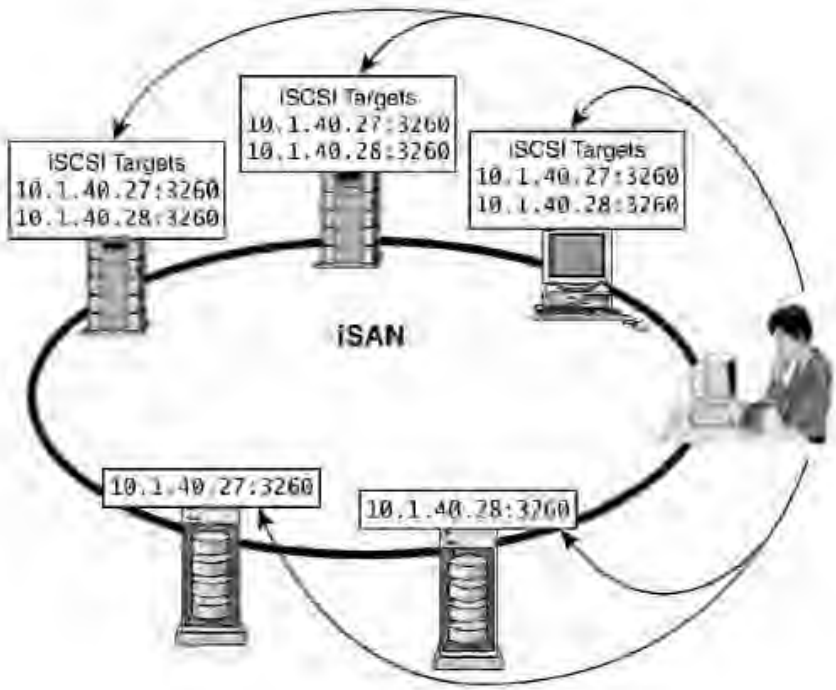
W ramach iSCSI dostępne są dwie metody uwierzytelniania. Pierwsza, tzw. podstawowa, wykorzystuje jedynie identyfikator iSCSI inicjatora. W tej metodzie, administrator określa na targecie, że do danego zasobu dyskowego dostęp ma jedynie posiadacz określonego identyfikatora iSCSI (np. iqn.1987-05.com.cisco:host1). W momencie logowania się następuje sprawdzenie identy-

fikatora inicjatora i jeśli nie występuje on na liście dopuszczonych do korzystania z określonego zasobu, prośba jest odrzucana. Druga metoda, rozszerzona, wykorzystuje dodatkowe algorytmy. Są to: CHAP, SRP, Kerberos v.5, SPKM-1 i SPKM-2, jednak jedynie pierwszy musi być obowiązkowo implementowany przez producentów. Pozostałe są opcjonalne.[1]

5. Wykrywanie i resolving identyfikatorów targetów iSCSI

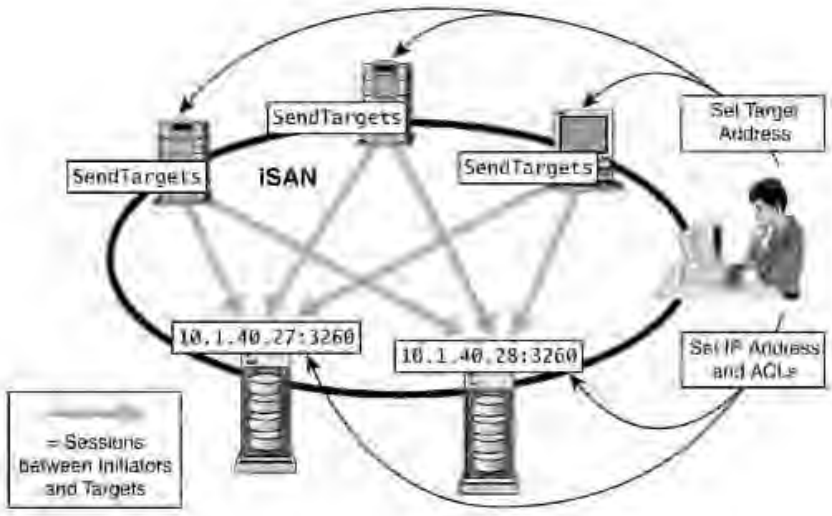
Występują trzy możliwości odnajdowania w sieci targetów iSCSI:

- manualna – inicjator ma z góry podane identyfikatory i gniazda iSCSI targetów, do których może się logować. Resolving realizowany jest po stronie inicjatora bez udziału jakichkolwiek dodatkowych usług sieciowych. Wariant takiego typu wykrywania przedstawiony jest na rys. 5.1.



Rys. 5.1. Manualne wykrywanie targetów iSCSI. (źródło: [1])

- pół-automatyczna – inicjator dysponuje jedynie gniazdami, do których wysyła polecenie Sendtargets. W odpowiedzi, inicjator otrzymuje Tag Grupy Portalowej TPGT, która odebrała to polecenie oraz listę identyfikatorów iSCSI targetów dostępnych poprzez ten Portal lub grupę Portali. [2] Możliwe jest wykrywanie poprzez broadcast, lub skonfigurowany wcześniej zakres adresów lub pojedynczy adres IP. [1] Wariant takiego typu wykrywania przedstawiony jest na rys. 5.2.

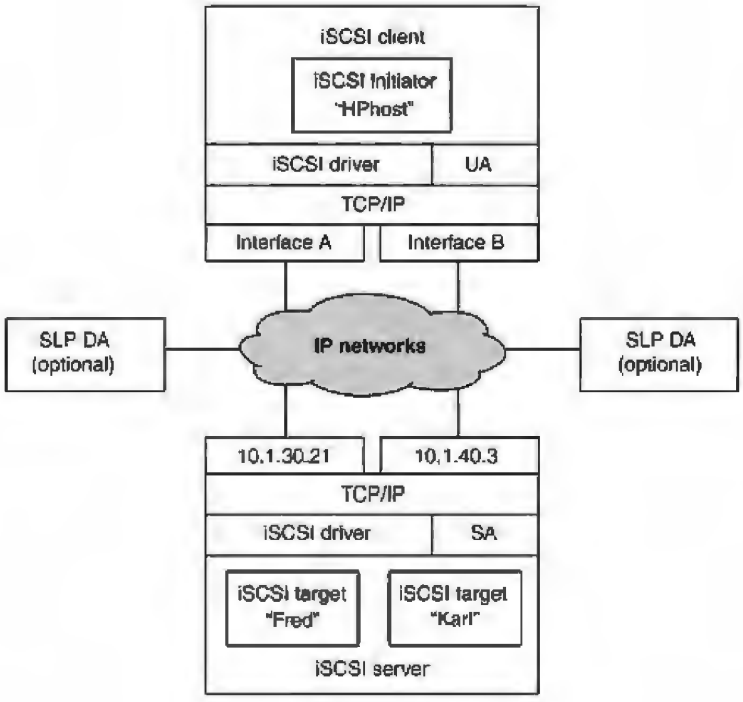


Rys. 5.2. Pół-automatyczne wykrywanie targetów iSCSI. (źródło: [1])

- automatyczna – korzysta z dodatkowych usług i występuje w dwóch odmianach.

Pierwsza z nich, to SLP (Service Locator Protocol). Wariant ten jest prostszy w implementacji przez producentów, jednak nie oferujący rozbudowanych usług z zakresu separacji ruchu i bezpieczeństwa, jak również , z uwagi na kiepską skalowalność, nie mający zastosowania w dużych środowiskach. SLP składa się z User Agentów (UA), service agentów (SA), oraz Directory Agentów (DA). User Agent zlokalizowany jest po stronie inicjatora i odpowiada za skomunikowanie się z SA lub DA w celu uzyskania informacji o targetach. Service Agent działa z ramienia targetów i przechowuje informacje na ich temat. Informacja ta dystrybuowana jest w formie listy zawierającej takie infor-

macje jak IP:port pod którym dostępny jest target, jak również jego identyfikator i TPGT. Na tym poziomie istnieje możliwość określenia jacy inicjatorzy mają dostęp do jakich targetów. Directory Agent, o ile został zastosowany w danym środowisku, jest miejscem, w którym rejestrowane są informacje rozgłaszane przez SA. Użycie Directory Agenta redukuje ruch sieciowy, ponieważ może centralizować informacje z wielu Service Agentów. [1][2][3]. Service Agent może podjąć decyzję czy udostępnia informacje o targetach Directory Agentowi czy też User Agenci mają komunikować się z nim bezpośrednio. W drugim przypadku (lub w sytuacji, gdy Directory Agent nie został zaimplementowany), User Agent używa multicastu, aby odnaleźć Service Agentów. Możliwe jest również prekonfigurowanie tej informacji po stronie inicjatora. Analogiczne możliwości odnajdywania występują w przypadku Directory Agentów. Dodatkowo, istnieje możliwość uzyskania tej informacji z DHCP [1] Architekturę SLP przedstawia rys. 5.3.



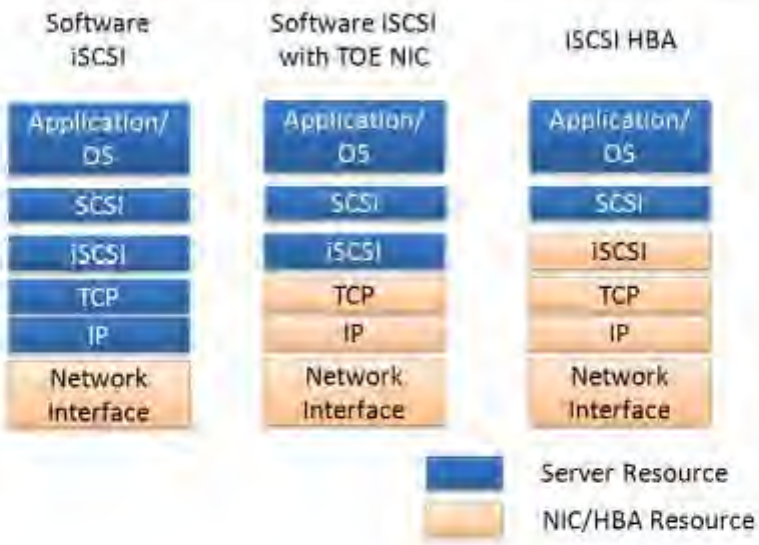
Rys. 5.3. Architektura SLP. (źródło: [3])

Wykrywanie targetów realizowane jest poprzez odpytanie Service Agenta przez inicjatora w momencie, kiedy ten włącza się do sieci. W przypadku wariantu stosującego Directory Agenta, to właśnie on jest odpytywany i umożliwia selektywne zwracanie informacji na temat targetów Incjatorowi w zależności od tego do jakich targetów dostęp mu nadano.

Drugim wariantem jest natomiast iSNS (Internet Storage Name Server), który w swoim podstawowym działaniu jest podobny do SLP. Inicjatorzy i targety muszą zarejestrować się na serwerze iSNS zanim będą mogli odczytać informacje, które przechowuje. Target rejestruje w nim takie same informacje jak w przypadku SLP czyli identyfikatory targetów, informacje o Portalu: IP:port oraz TPGT. Inicjator z kolei odczytuje te informacje, jednakże są mu one udzielane jedynie na temat targetów, do których umożliwiono mu dostęp. Podstawowa zaleta iSNS w stosunku do SLP, to mechanizm powiadomień o zmianach w środowisku. W przypadku SLP, gdy jakiś target znikał z powodu np. awarii interfejsu sieciowego, inicjator nie otrzymuje żadnej informacji na ten temat, w związku z tym musi stale odpytywać Agenta czy target jest wciąż dostępny lub dowiedzieć się o tym nie wprost w momencie próby zalogowania się niego. W iSNS, każda zmiana w dostępności urządzenia pociąga ze sobą automatyczne powiadomienie (RSCN) zainteresowanych stron. Dodatkową zaletą jest możliwość podziału na strefy, w ramach których urządzenia mogą się ze sobą komunikować (Discovery Domains i Domain Sety). [2][3]

6. Adaptery w sieciach iSCSI SAN

Jak wspomniano we wstępie, SAN oparty o protokół iSCSI może wykorzystywać najtańsze nawet karty Ethernetowe. Karty te jednak realizują sprzętowo jedynie niezbędne minimum, natomiast cała reszta przetwarzania realizowana jest przez mikroprocesor serwera, w którym umieszczona jest karta. Według niektórych testów, obciążenie to może sięgać nawet 80% w związku z czym w środowiskach stawiających na wysoką wydajność, stosowane są dwa inne typy kart. Pierwszy z nich, to karty TOE (ang. TCP Offload Engine), które realizują sprzętowo cały stos TCP/IP. Są to karty w znacznym stopniu odciążające mikroprocesor, a jednocześnie zachowujące uniwersalność (korzystanie z sieci LAN i z iSCSI). Drugi typ, to karty iSCSI. Karty te cechują się najniższym obciążeniem mikroprocesora, ponieważ sprzętowo realizują nie tylko TCP/IP, ale również operacje związane z samym iSCSI. Karty tego typu są dedykowane iSCSI.



Rys. 6.1. Lokalizacja iSCSI w modelu warstwowym. (źródło: www.windowsitpro.com)

Podsumowanie

Ilość informacji, do których firmy muszą mieć stały dostęp ciągle rośnie i tendencja ta raczej nie ulegnie zmianie. Taki stan rzeczy sprzyja rozwojowi istniejących i tworzeniu nowych sieci SAN, jednakże wiele projektów nie doczekałoby się realizacji, gdyby na rynku panowała jedynie, wymagająca pod względem finansowym, technologia FC. Na szczęście dla firm dysponujących ograniczonym budżetem, iSCSI stanowi doskonałą alternatywę, dzięki której wdrożenie sieci SAN staje się tańsza niż kiedykolwiek. Największe korporacje prawdopodobnie wciąż będą wybierały FC, jednakże pozostałe środowiska stawiać będą raczej na tańsze i prostsze w administrowaniu iSCSI, na którym coraz większą uwagę skupiają zarówno producenci sprzętu i oprogramowania jak i ich klienci.

Literatura

[1] J.L. Hufferd (2002): iSCSI: The Universal Storage Connection, Addison Wesley

[2] J.Long (2006): Storage Networking Protocol Fundamentals, Cisco Press

[3] T. Clark (2003): Designing Storage Area Networks: A Practical Reference for Implementing Fibre Channel and IP SANs, Addison Wesley

ISBN 9788389475336

J. Hołubiec, red. – TECHNIKI INFORMACYJNE-TEORIA I ZASTOSOWANIA, tom 1 (13)