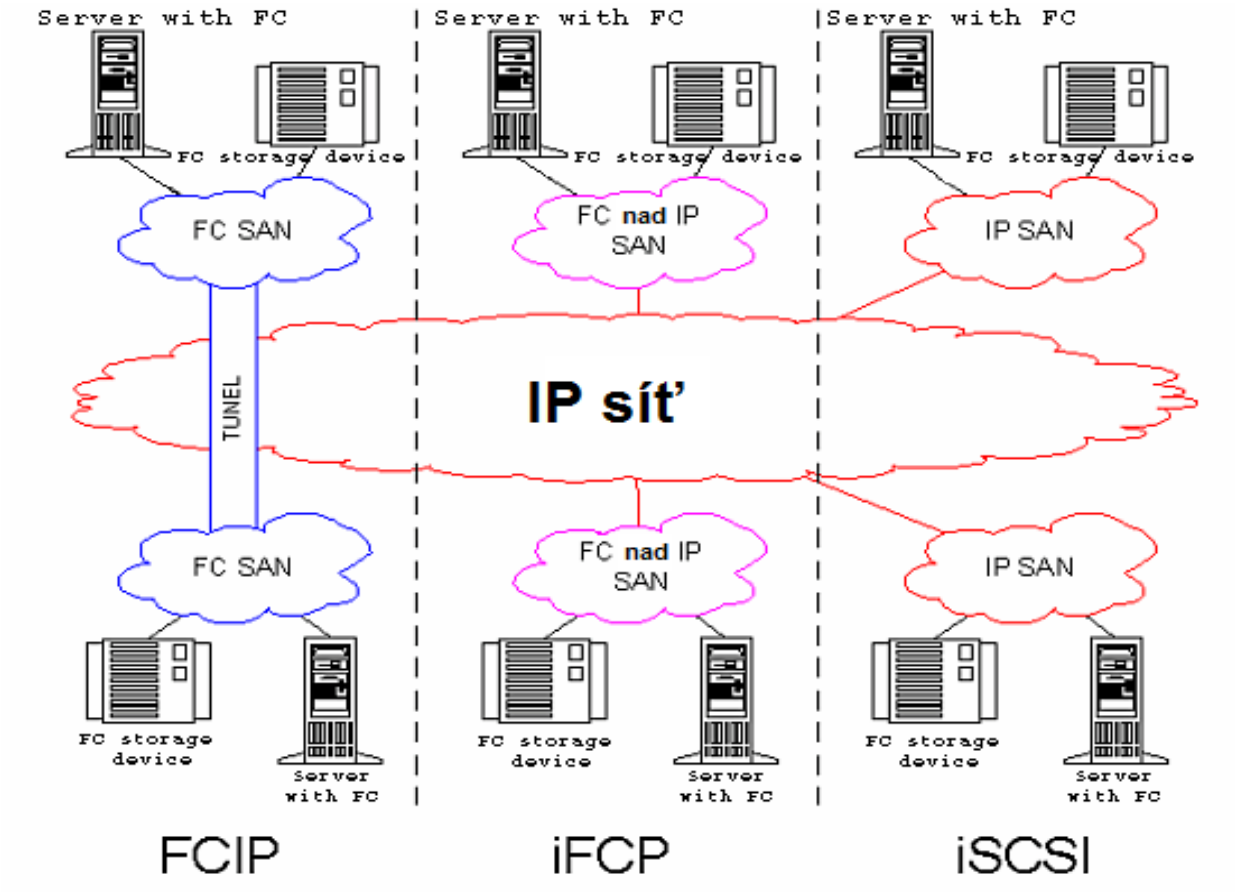
1. Sítě úložišť a protokol IP

Značné úsilí se vynakládá na vývoj protokolů a mechanismů, které by umožnili co nejširší využití počítačových sítí založených na IP protokolech, například i pro přenos dat mezi datovým úložištěm a místem zpracování dat. Sítě úložišť založené na IP mohou do jisté míry nahradit část sítí Fibre Channel, zvláště v případě vzdálených spojů a sítí WAN, menších implementací SAN nebo aplikací bez požadavků na vysoký výkon. Mezi tyto technologie patří:

iSCSI – tento protokol využívá sadu příkazů a formát dat SCSI, které se balí do paketů odesílaných do IP sítě. Protokol IP zde rozšiřuje dosah SCSI na mnohem větší vzdálenosti.

Fibre Channel nad IP (FCIP nebo FC/IP) – tento tunelovací protokol zapouzdřuje rámce FC do IP paketů. FCIP je technologie bodových spojení typu P2P. Zdroj balí rámce FC do paketů a cíl je zase z těchto paketů vybaluje.

iFCP – příkazy a data Fibre Channel jsou připojovány do IP paketů a odesílány. Jedná se o nativní metodu transportu přes IP. Tento koncept je podobný iSCSI v tom smyslu, že příkazy iFCP i iSCSI jsou zabaleny do TCP a přenášeny prostřednictvím sítě IP. Naopak FCIP se může používat jen v souvislosti s nějakou existující sítí Fibre Channel. Zatímco pakety iFCP se doručují z jedné brány iFCP na druhou a jsou přitom normálně směrovány, FCIP je pouze mechanismus pro stavbu IP tunelů.



Obr. - schéma fungování protokolů FCIP, iFCP a iSCSI

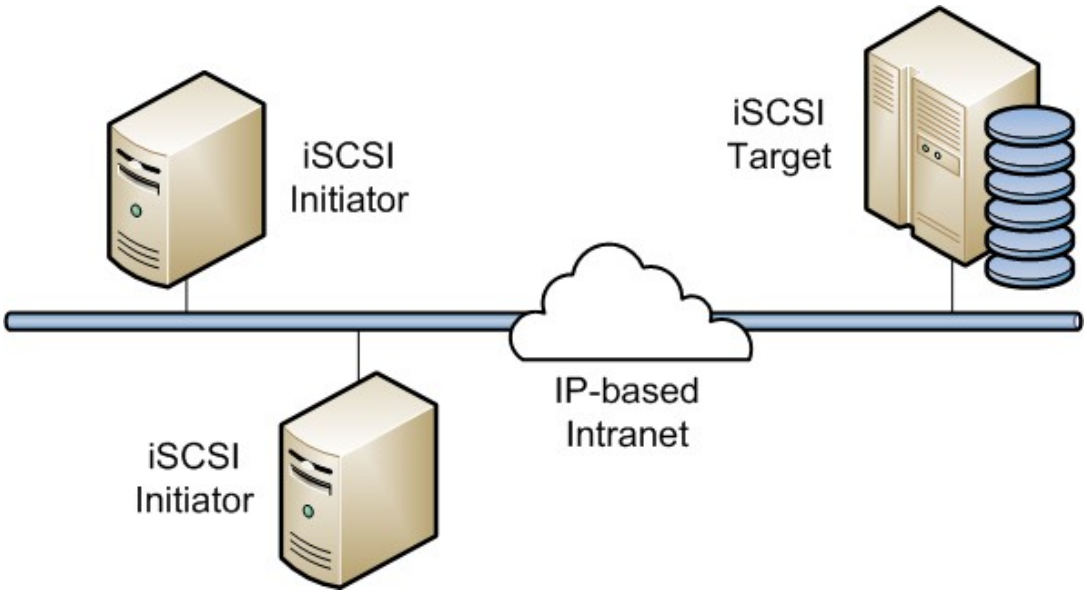
Sítě úložišť a sítě IP byly ale vyvíjeny s úplně jinou sadou výchozích požadavků. Hlavním cílem všech sítí úložišť byla vždy vysoká propustnost a spolehlivé doručování dat. Sítě IP jsou sice tolerantní k chybám, ale nebyly navrženy pro vysoké rychlosti. Tyto rozdíly znamenají pro způsob používání sítí IP za účelem komunikace s úložišti jistá omezení. Aplikace, které jsou na přirozené zpoždění v sítích IP citlivé, nejsou vhodným kandidátem na transport v těchto sítích.

Data, která si vyměňují systémy v sousedních místnostech, možná překonají na cestě jeden směrovač (jeden hop, tedy přeskok). Každý další hop ale znamená v sítích IP narůstající zpoždění. Proto spojení, které překonává jeden směrovač, bude v aplikacích s nároky na vysoký výkon fungovat uspokojivě, pokud má ovšem dostatečnou šířku pásma. Jestliže však spoj překonává celý stát či kontinent, zpoždění jednotlivých přeskoků mezi směrovači se sčítá. Následkem toho nemusí být například FCIP vhodným řešením pro připojení databáze k síťovému úložišti.

Šířku pásma nelze určit bez otestování, a ta je navíc velmi závislá na aktuálních podmínkách v síti. Můžeme si však udělat částečnou představu o zpoždění v sítí pomocí programu traceroute.

2. iSCSI

Protokol iSCSI patří mezi protokoly používané v ethernetové IP SAN síti. Má architekturu typu klient/server, přičemž pro server se používá pojmenování **target** (cíl) a pro klienta se používá **initiator** (iniciátor). Je popsán ve standardu RFC 3720.



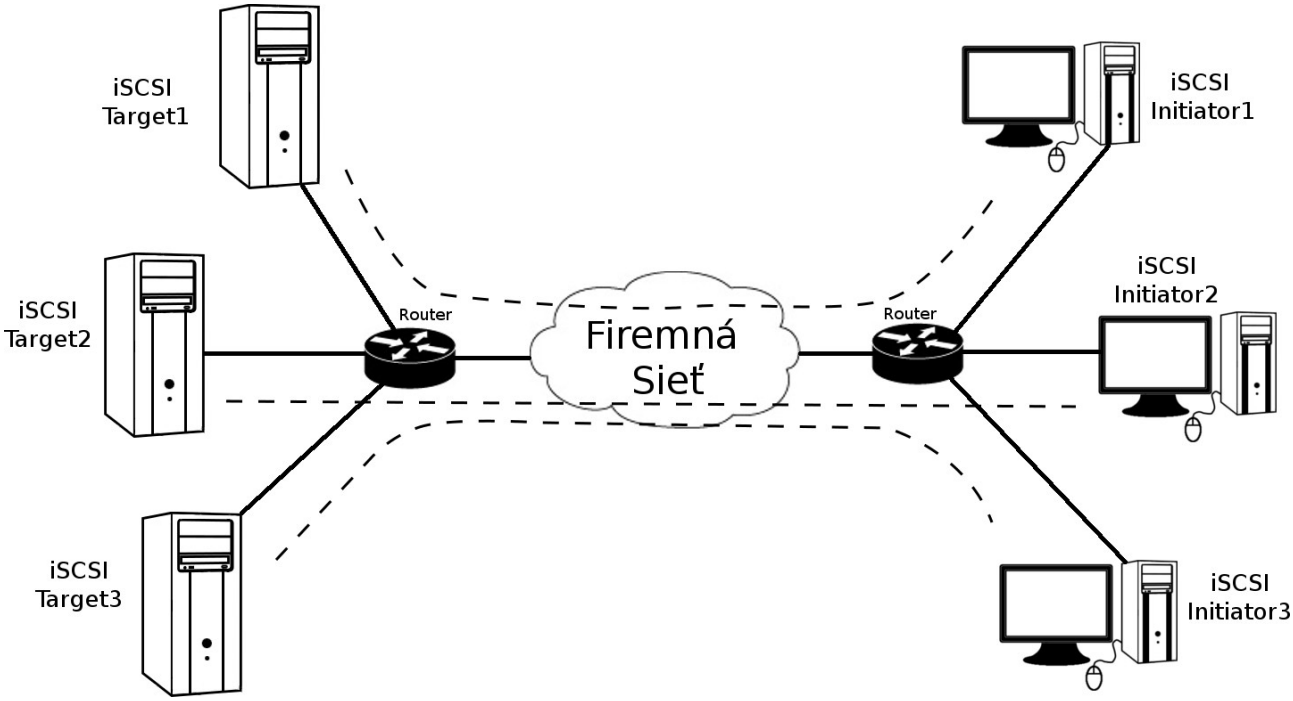
Obr. - architektura iSCSI

Initiator představuje klientskou část iSCSI spojení, která má za úkol iniciovat komunikaci. Posílá SCSI příkazy přes IP síť. Může být v provedení jako: softwarový iniciátor (implementovaný v systému ve formě kódu) nebo hardwarový iniciátor (používá pro generování SCSI příkazů vlastní zařízení).

Target zase představuje serverovou část spojení. Neslouží k iniciování spojení, ale pouze čeká na požadavek od iniciátora, a následně poskytne požadované vstupně/výstupní data. Jeho úkolem je poskytovat úložné zařízení klientům.

Komunikace mezi iSCSI zařízeními začíná tak, že iniciátor vygeneruje SCSI příkaz pro cíl. Následně vytvoří IP paket, do kterého vloží vygenerovaný SCSI příkaz. Pak ho už může vyslat do lokální sítě nebo do internetu, které fungují na bázi IP protokolu. Po doručení paketu se IP obal odstraní a cíl obdrží původní SCSI příkaz.

Tím, že iSCSI využívá konektivitu prostřednictvím ethernetových IP sítí, mohou se iniciátor a cíl spojit přes několik sítí nebo přes internet. Jednotlivé cílové servery mohou být umístěny v jedné firemní síti a pomocí routeru připojeny do ostatních firemních sítí. Aby mohl iniciátor navázat spojení s cílem, musí mít k dané síti přístup.



Obr. - Propojení iSCSI targetu a initiatoru

Směry komunikace jsou určovány s ohledem na iniciátor. Odchozí spojení jsou definovány jako spojení od iniciátoru směrem k cíli. Naopak příchozí spojení jsou spojení odchozí od cíle k iniciátoru.

Protokol iSCSI má oproti Fibre Channel protokolu výhodu v tom, že je cenově méně náročný, poskytuje neomezené limity vzdálenosti a koncové stanice nepotřebují při připojování do sítě žádné speciální vybavení. Většina firem při zavádění SAN sítě již má zavedenou svoji lokální síť (LAN) fungující na ethernetovém IP protokolu, a tím že použijí jako protokol iSCSI, nemusí investovat do tvorby nové sítě, ale mohou využít stávající. Tím se dá ušetřit na správě, protože je vše implementované v jedné síti, nepotřebujeme dalších správců a stávající správci nemusí studovat nové technologie potřebné pro provoz.

Protokol iSCSI můžeme používat na ethernetové síti o různých rychlostech. Celkový výkon námi vytvořené SAN sítě bude závislý na tom, jakou verzi ethernet protokolu použijeme resp., na jakou rychlost navrhneme jednotlivé propojovací prvky. Většina firemních sítí je tvořena UTP kabely kategorie 5e a 6 o ethernetovém standardu 100Base-T či 1000Base-T. Taková síť nám dovolí komunikovat maximální rychlostí 100 megabitů za sekundu (1 Gb/s). To nám ale pro naše potřeby nemusí vždy stačit. V takovém případě můžeme použít vyšší standardy ethernet protokolu. Nejvíce používaná verze u IP SAN sítí v současnosti je 1 nebo 10 Gbit/s (10GBase-T). Při využití těchto standardů dokážeme dosáhnout rychlosti až 10 gigabitů za sekundu.

1.1. LUN - Logical Unit Number

Hlavním úkolem iSCSI cíle je poskytování úložného prostoru pro iSCSI iniciátor. Úložný prostor je identifikován zkratkou **LUN** (**Logical Unit Number**), což v překladu znamená logická jednotka.
Logická jednotka (LUN) může představovat buď jeden fyzický pevný disk, popř. jen jeho oddíl.

1.2. adresování

Aby zařízení spolu mohli v síti komunikovat, potřebují mít jednoznačně určené adresy. Při použití iSCSI protokolu musí mít koncové body komunikace (iniciátor a cíl) nastavené **iQN**, **EUI** nebo **NAA** jméno. Tato jména slouží jako adresa, pomocí které dokážou iniciátor a cíl navázat spojení.

iQN - iSCSI qualified name
V iSCSI protokolu můžeme jako adresy použít iQN jména. Tato jména mají svou strukturu a jsou konstruovány tak, aby byly v rámci celého světa jedinečné.
Příklad iqn jména: iqn.2016-11.cz.vspj.kts.server:nazev.disku.
Slovo iqn na začátku nám indikuje, že se jedná o iqn jméno. Čísla 2016-11 nám představují datum spuštění daného serveru, kde 2016 představuje rok a 11 je měsíc, ve kterém byl spuštěn. Dále následuje DNS jméno, které však musí být v obráceném pořadí. Nakonec následuje iSCSI unikátní řetězec znaků, který jasně identifikuje konkrétní zařízení v síti. Doménové jméno a unikátní řetězec jsou odděleny znakem ":".

EUI - enterprise unique identifier
EUI představuje (podobně jako iQN) adresu (jméno) zařízení využívajícího iSCSI protokol. Oproti iQN se liší strukturou, podle které je konstruováno, ale stále platí, že musí být v rámci světa jedinečné.
Příklad EUI jména: eui.0123456789abcdef
EUI používá EUI-64 formát, který se skládá z 64 bitů. EUI jméno je složen z "eui." slova, za kterým následuje 16 hexadecimálních čísel (64 bitů). Těchto 64 bitů můžeme složit ze dvou částí. Prvních 24 bitů obsahuje identifikační číslo (ID) instituce, která provozuje daný server. Identifikační čísla přiděluje organizace IEEE, která zajišťuje jedinečnost

přidělovaných EUI. Zbývajících 40 bitů doplní provozovatel serveru podle vlastního uvážení. Celkově dostaneme 64 bitové číslo zapsané v hexadecimálním tvaru.

T11 Network Address Authority - (NAA)
Formát je podobný jako EUI s rozdílem možností dvou délek identifikátorů 64bit a 128 bit.
Příklad NAA: naa.{NAA 64 or 128 bit identifier} (e.g. naa.52004567BA64678D)

3. Bezpečnost protokolu iSCSI

Při každé komunikaci, která probíhá přes síť, nám vzniká potenciální bezpečnostní riziko. Pokud se jedná o komunikaci přes internet, musíme být zvlášť opatrní, jelikož nevíme přes kolik sítí náš paket prochází. I při použití iSCSI protokolu musíme dbát na bezpečnost dat, které přenášíme. Existuje několik způsobů, jak může útočník odposlouchávat naši komunikaci a následně zneužít získaná data. Proti všemu je ale možné se bránit, pokud máme dostačující znalosti.

3.1. CHAP Autentifikace

CHAP (Challenge Handshake Authentication Protocol) autentifikaci používáme v případě, že chceme, aby se nejprve iniciátor a cíl autentifikovali a až potom zahájili komunikaci. Používá se při spojení typu bod-bod, to znamená mezi dvěma koncovými zařízeními sítě. Touto metodou zabráníme útočníkovi použít útok nazývaný "Snoofing", při kterém se útočník vydává za zařízení, se kterým komunikujeme. Ověřování pomocí CHAP protokolu probíhá ve 3 fázích.

V první fázi vyšle autentifikátor (koncové zařízení, které vyžaduje ověření a specifikuje ověřovací protokol) zprávu, kterou vyzve peera (zařízení na druhém konci spojení, které má být ověřeno autentifikátorem), aby se identifikoval. Peer odpoví zprávou, ve které pošle číselnou hodnotu vypočtenou pomocí určitého hash algoritmu. Autentifikátor po přijetí zprávy danou hodnotu porovná se svým výpočtem a pokud se shodují, tak daného peera potvrdí. CHAP autentizace je popsána v doporučení RFC 1994. CHAP autentizace může být dvojí:

- Jednoduchá autentifikace (**One-way CHAP authentication**) slouží k ověření Iniciátoru cílem. Tím že nastavíme autentizaci (jméno a heslo) omezíme přístup pouze na initiciátor, který zná dané údaje. Tajný klíč je nastaven pouze pro cíl a všechny iniciátory, které chtějí získat přístup k příslušnému cíli, musí použít stejný tajný klíč, aby bylo možné zahájit relaci přihlášení s cílem.

- Oboustranná autentifikace (**Mutual CHAP authentication**) slouží k vzájemné ověření iniciátoru a cíle. Iniciátor musí znát údaje potřebné pro autentizaci u cíle a naopak cíl musí znát údaje pro autentizaci u iniciátoru.

  Podle RFC 3720 musí být heslo použito při CHAP autentizaci větší než 96 bitů. Námi zadávané heslo sestávající se z písmen, čísel nebo znaků je pomocí ASCII tabulky převedeno na bity. 96 bitů představuje 12 znaků, takže při nastavování hesla musíme zadat minimálně 12-místný řetězec. V případě, že chceme použít heslo kratší než je 96 bitů (12 znaků) musíme použít IP Security protokol (IPsec).

3.2. IPsec

IPsec je protokol, který slouží k zajištění komunikace na IP vrstvě pomocí ověřování a šifrování paketů. Šifrování paketů je vhodné proto, aby nikdo, kdo se nachází mezi koncovými zařízeními našeho bod-bod spojení nemohl odposlouchávat tuto komunikaci. Tímto zajištěním vyřadíme útočníka, který chce použít útok nazývaný "man-in-the-middle", kde útočník odposlouchává komunikaci mezi koncovými body. Útočník sice data odchytí, ale protože jsou zašifrovány, není schopen přečíst jejich obsah. Ověřování pravosti paketů je vhodné použít, abychom si byli jisti, zda paket, který jsme přijali, je opravdu od odesílatele, se kterým komunikujeme.

3.3. iSNS - Internet Storage Name Service

Další metodu, kterou můžeme použít pro zvýšení bezpečnosti iSCSI protokolu je použití iSNS serveru. Používáním iSNS serveru můžeme seskupit jednotlivé cíle a iniciátory do skupin, a tím zabezpečit, aby iniciátor mohl komunikovat jen s cílem, který je pro něj určený. Jednotliví iniciátoři i cíle se zaregistrují u iSNS serveru, který zabezpečí jejich úvodní komunikaci. iSNS server se může nacházet buď přímo v síti s ostatními zařízeními, nebo v jiné IP síti, ke které se mohu zařízení připojit.

Nevýhodou použití iSNS serveru je fakt, že při výpadku iSNS serveru se nemohou iniciátoři spojit se svými cíli.