

LIBERECKÁ  IS



**MODERNÍ TRENDY  
V DATOVÝCH CEN-  
TRECH  
A V ROZSÁHLÝCH  
DATOVÝCH SÍTÍCH**

**19. KVĚTNA 2010**

**MALÝ SÁL  
KRAJSKÉ VĚDECKÉ  
KNIHOVNY  
V LIBERCI**

**SHRNUTÍ PŘEDNÁŠEK**

---

Liberecká IS, a.s.  
Jablonecká 41  
460 01 Liberec 5  
[lis@libereckais.cz](mailto:lis@libereckais.cz)  
485 243 031

NET-SYSTEM, s.r.o.  
ul. Generála Svobody 50  
460 01 Liberec 13  
[info@netsystem.cz](mailto:info@netsystem.cz)  
482 428 111

## ÚVOD

Informační technologie dnes nejsou v současnosti jen jednou ze součástí moderní civilizované společnosti, nýbrž jí celou prostupují, ovlivňují a mění naše chování, zvyky, postupy.

Dominantní ráz IT současné doby srovnatelný v historii snad jen s vynálezem kola, knihtisku či využití páry má jednu výhodu a zároveň nevýhodu. Vše se strašně rychle mění a bez predikce, odhadu, kam směřuje nejmodernější vývoj, hrozí komukoliv v této branži, že nejen zaostane a začne škodit sám sobě, ale svojí rigiditou negativně ovlivní i chod firmy, efektivní nakládání se svěřenými hodnotami.

Tento workshop není o tom „jak to udělat levněji“ (víme, jak úzce souvisí láce s kvalitou), ale o tom, „jak to udělat kvalitněji a efektivněji“ při stejné ceně.

Cílem je předvést technologie a nástroje, které umožní, aby osoby zodpovědné za chod IT ve firmě mohly pracovat běžnou pracovní dobu dle Zákoníku práce, nenosily si domů starosti a konflikty s uživateli, neměly v zádech pocit permanentního strachu, co by se mohlo stát, kdyby...

Cílem je nabídnout spolupráci v přípravě podkladů pro rozhodnutí managementu o níže uvedených změnách.

Cílem je i přesvědčit Vás, že můžete řídit i to, na co si nemůžete sáhnout. Že si můžete koupit službu a vykoupit se tím ze zodpovědnosti. Že si můžete udělat práci bezstarostnější.

## MODERNÍ TRENDY V INFORMAČNÍCH TECHNOLOGIÍCH

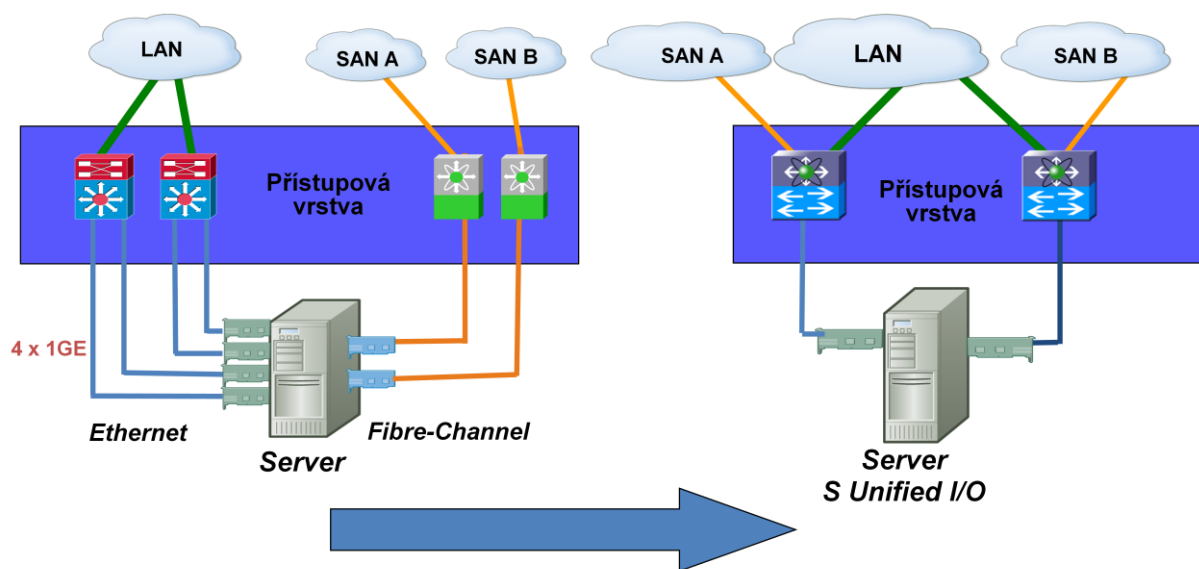
### KONSOLIDACE V DATOVÝCH CENTRECH

Díky výkonu stávajících serverů se virtualizace stává nutností – jinak není možné server využít. Virtualizace ale způsobuje, že je třeba do serveru dostat více dat a důsledkem jsou požadavky na 10GE ethernet.

Praktická zkušenost z datových center ukazuje, že stávající oddělení LAN a SAN je náročné. Vede k budování dvojité infrastruktury LAN přepínačů a SAN přepínačů. To má za důsledek velké množství kabeláže, potřebu napájení a chlazení, velké nároky na administraci.

V současné době je možné konsolidovat LAN i SAN do jedné struktury postavené na DCE a FCoE standardech. Tím lze ušetřit jak v přímých investicích, tak v následném provozu a správě systému. Samozřejmě je možné využít existující řešení a systém postupně rozvíjet.

## Konsolidace I/O v přístupové vrstvě



**Méně kabelů, méně zařízení**

**Jedna kabeláž, libovolné I/O  
SAN, NAS, iSCSI**

### RODINA PŘEPÍNAČŮ CISCO NEXUS

Přepínače řady Cisco Nexus slouží ke stavbě Unified Fabric. Unified Fabric umožňuje postavit jednu síť, která spojuje datovou a storage síť.

Přepínače Nexus 5000 umožňují propojit LAN a SAN. Běžně jsou všechny porty 10Gbps Ethernet DCE a lze je spojovat se servery a existující LAN infrastrukturou.

Pro připojení k SAN jsou určeny FiberChannel porty. Pomocí nich může přepínač v SAN vystupovat jako FC switch i FC host.

Pro blade chassi je dostupná řada přepínačů Nexus 4000 – IBM a Dell. Pro HP aktuálně není.

Přepínače Nexus 5000 mají 24 nebo 48 portů, ale přepínací matrice má výkon 520/1040 Gbps. Pro zvýšení počtu portů lze využít Fabric Extender Nexus 2000 (FEX). Poskytuje 24 10GE portů, které agreguje a pomocí několika uplink 10GE portů připojuje do Nexus 5000. Porty FEXu jsou na Nexusu 5000 vidět jednotlivě s plnou funkcionalitou – vytváří se tak virtuální šasi.

Pro virtualizační platformu VMware vSphere 4 je dostupný Nexus 1000v – softwarová implementace Nexus 5000. Vlastnosti shodné s NX 5000, při využití VMotion (přesun VM stroje mezi fyzickými servery) sleduje konfigurace sítě VM stroj.

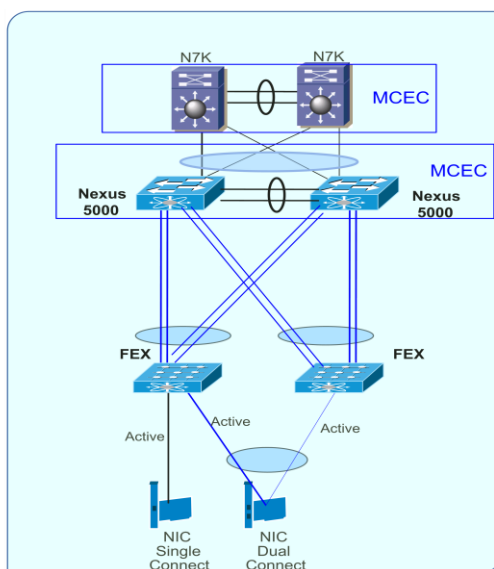
Servery dříve používaly dva typy karet (od každé obvykle dvě a více kvůli redundanci) – datovou pro přístup do datové sítě (obvykle 1 nebo 10Gbps Ethernet) a storage kartu (obvykle FiberChannel o rychlosti 1/2/4/8Gbps).

Nově se používají Converged Network Adapters (CNA), které jsou připojeny 10Gbps Ethernetem s implementací nových standardů Ethernetu – DCE (priorita, bezztrátovost) a FCoE (FiberChannel over Ethernet). Výrobci tyto karty nabízí jak integrované, tak jako rozšiřující karty. Podpora nových standardů je v závislosti na výrobci implementována v driveru nebo přímo v hardware karty, což má vyšší výkon.

Díky CNA je server do sítě připojen jednou (pro redundanci dvěma) linkami a má přístup jak do LAN, tak do SAN. Kapacitu spoje lze využít dle potřeby – někdy více LAN, někdy více SAN. Rozdělení lze garantovat.

Z pohledu serveru se CNA tváří jako dvě karty – LAN a SAN. Není proto třeba měnit nic na úrovni OS a aplikací. CNA obsahují čipy z existujících LAN a SAN karet a není třeba nové drivery.

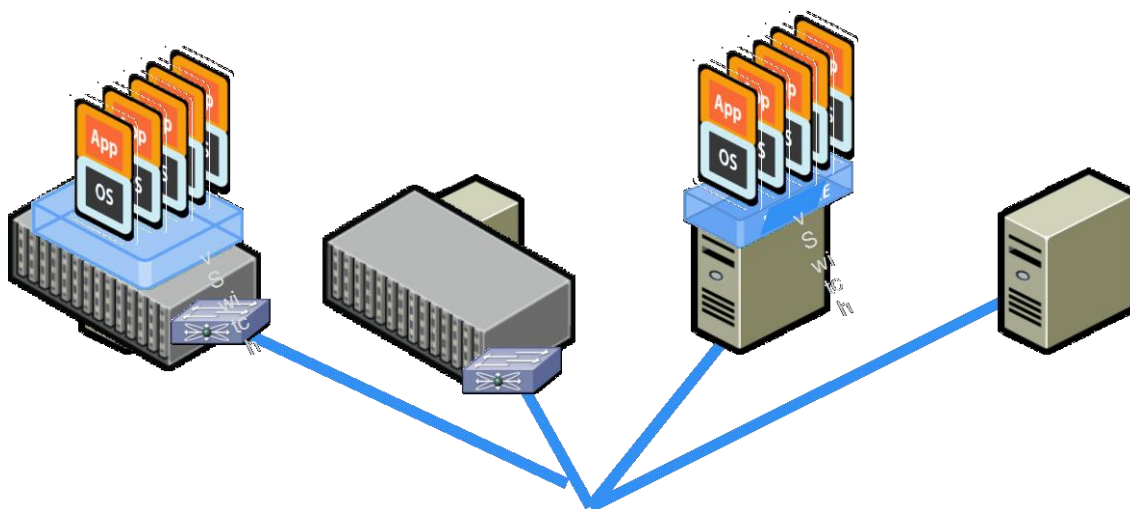
## Topologie s distribuovaným šasi



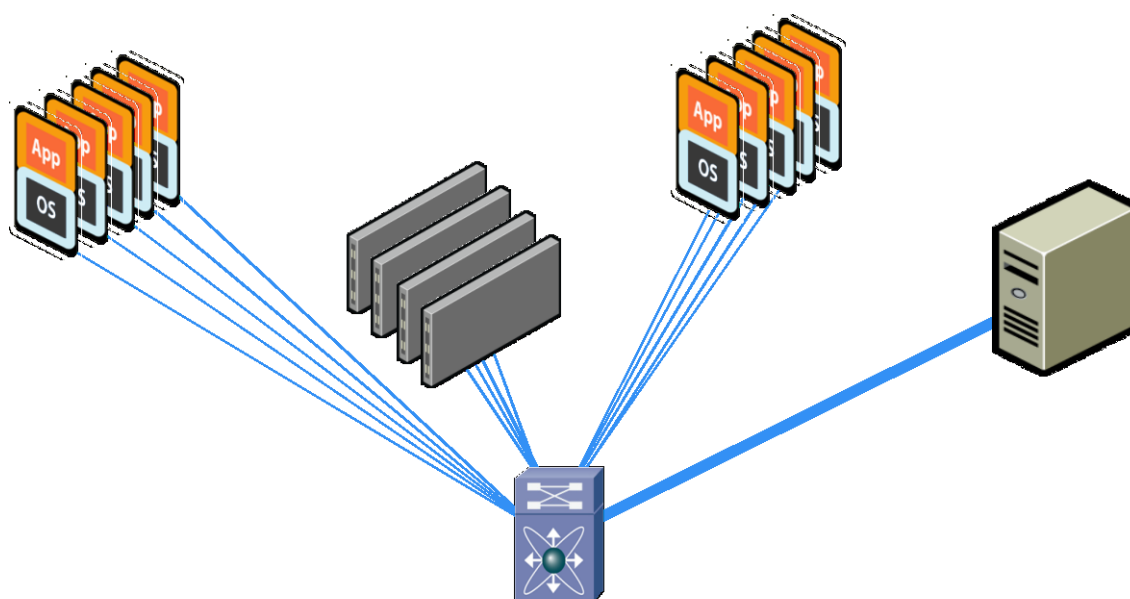
## PODPORA VIRTUALIZACE V SÍTI

Stávající síťové protokoly nechápou, že na jednom fyzickém serveru může pracovat více serverů současně. V důsledku toho síť nedokáže jednotlivé virtuální stroje spolehlivě rozpoznat a oddělit. Problémem je především komunikace mezi dvěma virtuálními stroji v rámci jednoho fyzického serveru.

Se zavedením standardu 802.1Qbh může virtualizační platforma označovat přímo v paketech, který virtuální stroj je zdrojem/cílem paketů. Síť tak vidí jednotlivé síťové adaptéry virtuálních strojů a může na ně aplikovat bezpečnostní politiky.



*Pohled na síť s virtualizovanými servery dříve*



*Pohled na síť s virtualizovanými servery nyní*

## CISCO UNIFIED COMPUTING SYSTEM – CISCO UCS

Řešení vytváří výpočetní pole. Server jako výpočetní výkon je zcela oddělen od datového obsahu a konfigurace – HW je bezstavový. Je zcela jedno, na kterém fyzickém uzlu se server spustí – zjednodušuje správu a zrychluje implementaci nových služeb. Případný výpadek HW způsobí maximálně ztrátu dat v RAM, ale během vteřin lze pokračovat na jiném blade.

Oddělení serveru od obsahu je docíleno důsledným využitím existujících technologií:

- data (OS a aplikační data) jsou uložena SAN
- konfigurace HW (MAC adresy, firmware, ...) jsou programovatelné a ovládá je management
- každý uzel má přístup do LAN i SAN přes CNA rozhraní

Pokud využijeme i virtualizaci (VMWare a další), zmizí zcela i závislost na skutečném HW.

UCS Manager zajišťuje administraci řešení. Díky rolím je možné bezpečně a vynutitelně určit, kdo co smí:

- LAN administrátor definuje VLANy, konfiguraci LAN portů, MAC, zabezpečení, ...
- SAN administrátor definuje VSANy, konfiguraci SAN portů, WWWN, ...
- UCS administrátor definuje profily serverů (DB server, WWW server, ...) a přidělí je skupinám uživatelů
- UCS administrátor definuje počty fyzických uzlů dostupných skupinám uživatelů
- skupinovní administrátoři si mohou v rámci svých oprávnění měnit některé parametry svých serverů (např. paměť, počty LAN/SAN adapterů)
- skupiny uživatelů se nevidí, jejich limity jsou systémem vynuceny

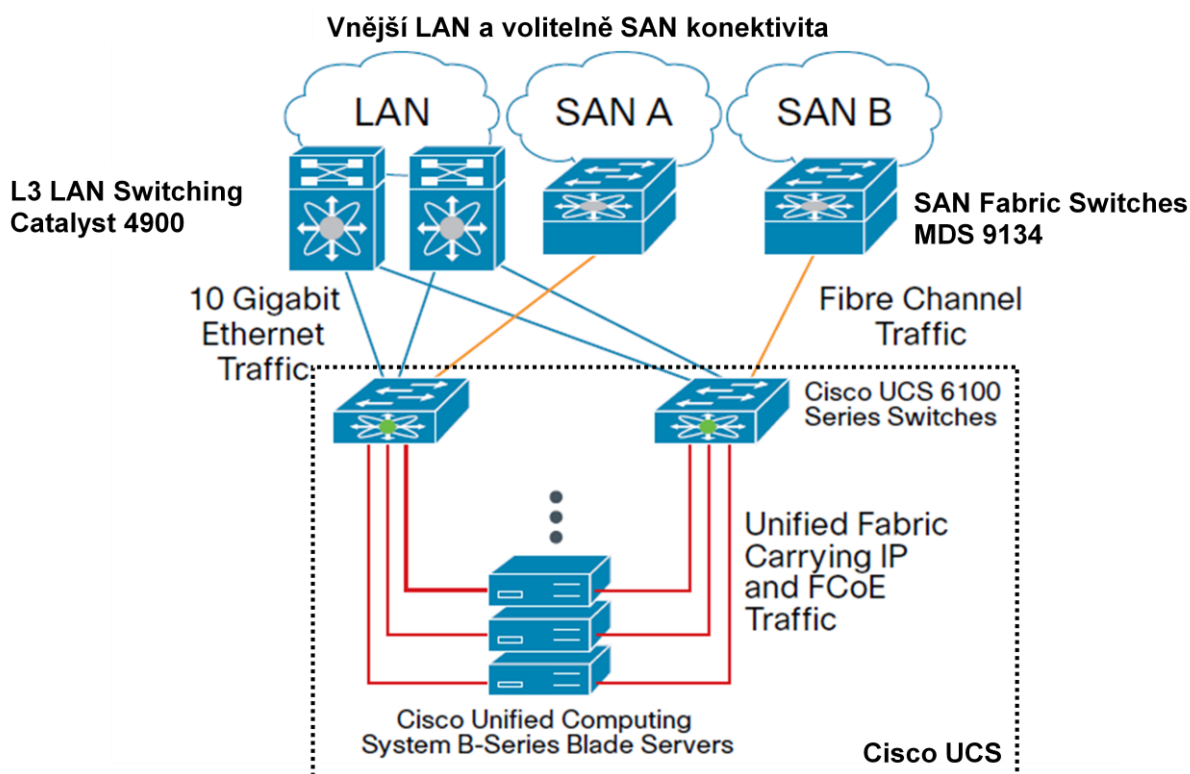
UCS Manager sídlí v šasi UCS a může být redundatní a udržuje konfiguraci jednotlivých serverů a řídí jejich život – vypnutí/zapnutí, monitoring.

UCS Manager má grafické rozhraní (WEB) a dokumentované XML API. Mnoho úloh lze automatizovat, lze svázat s management a dohledovými nástroji třetích stran.

### SKLADBA UCS SYSTÉMU:

- Cisco UCS 61xx Fabric Interconnect – zajišťuje propojení UCS s LAN a SAN, obsahuje UCS Manager
- Cisco UCS 51xx – šasi na blade servery
- Cisco UCS U21xx – propojení mezi šasi a Fabric Interconnectem
- Cisco UCS Bxxx – blade do šasi – CPU a RAM

Diskové pole/SAN a okolní LAN prostředí dle výběru.



#### CISCO UCS BLADE (BXXX)

Šířka: poloviční nebo plná šířka šasí

Paměť: 12/36/48 dimmů – až 96/256/386 GB RAM

CPU: 1-4x XEON 5500, 4-8 jader na CPU

HDD: 2-4 hot swap 2.5" disky HDD nebo SFF, ale neočekává se časté využití

IO: LAN: Intel 10GE, FCoE: QLogic nebo Emulex, LAN/FCoE: Cisco Paolo

#### UNIKÁTNÍ VLASTNOSTI

Pro servery byl Cisco vyvinut speciální memory kontrolér. Umožňuje mít v serveru hodně slotů na paměť – 4x více než běžně, až 48 slotů. Lze tak dosáhnout cenově výhodnější skladbu stejně velké paměti, protože menší paměti jsou levnější.

Např. 96GB RAM z 4GB modulů je o 60% levnější než stejná kapacita z 8GB modulů. Ale pro 4GB moduly je třeba 24 slotů, ale běžný server jich má 12 až 18.

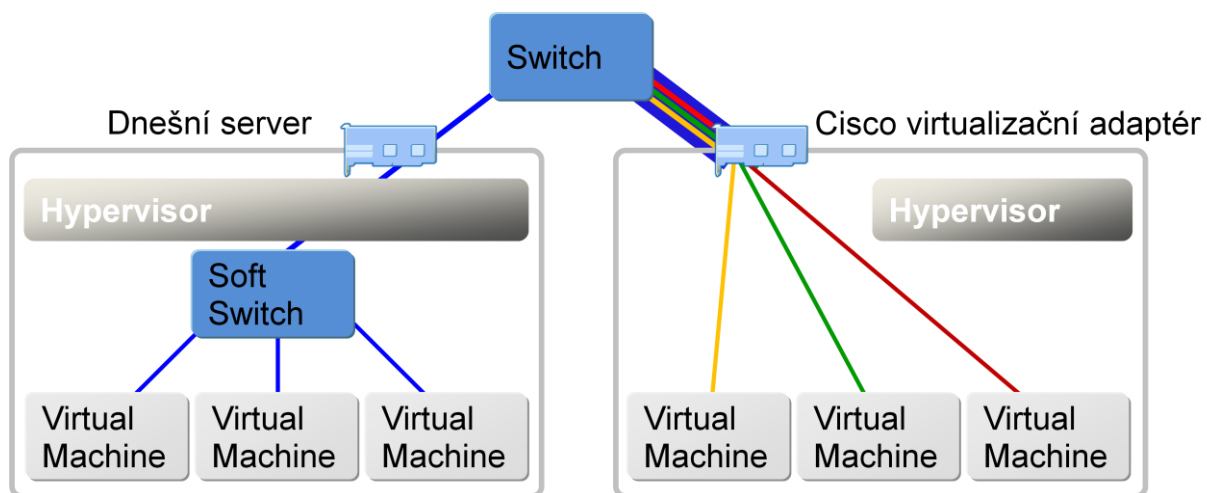
Maximální osaditelná velikost je při 8GB modulech 384GB – to je velikost vhodná pro velké databáze, ale také pro virtualizaci desktopů.

Pro podporu virtualizace byl vyvinut PAOLO CNA adaptér. Na jednom adaptéru umožňuje vytvořit libovolnou kombinaci až 127 LAN/SAN adaptérů v jednom serveru. Adaptéry lze vytvářet a rušit dynamicky.

Pro využití v běžném serveru je počet zbytečný. Ale při nasazení virtualizačního hypervisoru (např. VMware) se naráží na potřebu emulace LAN/SAN pro každý virtuální stroj. Virtualizaci obvykle provádí hypervisor, ale pak nelze zajistit vynucení bezpečnostní politiky mezi jednotlivými virtuálními stroji.

Paolo CNA adaptér vytvoří zvláštní kartu/karty pro každý virtuální stroj a to tak, že jsou viditelné v konfiguraci Fabric Interconnectu – čímž na ně lze aplikovat všechny bezpečnostní politiky. Při přesunu virtuálního stroje na jiný výpočetní uzel ho konfigurace samozřejmě následuje.

Shodnou funkčnost má i Nexus 1000v, ale protože jde o softwarovou implementaci, má nižší výkon.



## SPOLEHLIVÁ A BEZPEČNÁ DATOVÁ SÍŤ

Od současné datové sítě již neočekáváme jen přenos dat, ale i další služby. Síť musí být spolehlivá ve smyslu neztrácet data – chceme po síti telefonovat. Síť musí být spolehlivá ve smyslu odolná vůči výpadkům jednotlivých komponent – bez sítě již nedokážeme efektivně pracovat a komunikovat. A protože jsou na síti organizace stále závislejší a svěřují jí více a více dat, musí být i bezpečná.

Každý očekává, že síť data neztrácí. Ale realita je odlišná – v sítích dochází náhodně k zácpám a často jsou i mimo naši kontrolu. A nelze s tím mnoho dělat, s výjimkou datových center. Ale např. pro přenos hlasu (IP telefonii) a přenos videa potřebujeme, aby síť ztrácela co nejméně a pokud možno jen méně důležitý provoz.

K tomu slouží obecně nástroje implementující kvalitu služby (Quality of Service – QoS). Tyto nástroje musí být ve všech prvcích sítě, jinak se na síť nelze spolehnout.

Dnes jsou na datové síti organizace prakticky závislé. Proto nesmí docházet k zásadním výpadkům sítě. Toho se docílí redundancí – důležité komponenty jsou zdvojeny nebo navrženy tak, aby výpadek jednotlivé komponenty neměl na provoz v síti vliv.

Před několika lety stačila bezpečnost na úrovni přístupu do Internetu. Vznikly tak pojmy jako firewall, demilitarizovaná zóna a další.

Bohužel se ukazuje, že stále většímu množství útoků firewally nezabrání – nepochází totiž z venku, ale zevnitř sítě. A často nejde o útoky v pravém slova smyslu, ale jen o shody náhod, které ale ochromí některou důležitou komponentu sítě – např. někdo omylem aktivuje falešný DHCP server a začne přidělovat nesmyslné IP adresy.

Proti takovým útokům je třeba se bránit v každém prvku sítě a průběžně. Proto je mnoho bezpečnostních mechanismů integrováno v prepínačích či routerech. U prepínačů firmy Cisco jsou obsaženy především tyto bezpečnostní mechanismy:

- obrany proti paketovým bouřím
- obrany proti falešným DHCP serverům
- obrany proti podvržení IP adres

Pokud tedy máte síť postavenou s komponenty Cisco, které obsahují QoS a obsahují potřebné bezpečnostní prvky, proč nastavení neprovést a využít to, za co jste už zaplatili?

## AUTORIZACE PŘÍSTUPU K SÍTI

Bohužel se čím dál častěji stává, že firma investuje do obrany sítě, do obrany svých PC a dalších svých prvků. Pak ale „někdo“ přinese vlastní notebook a veškerá obrana přijde vniče. Podobně „někdo“ může připojit hub/switch, který nesplňuje firemní standardy.

Tomu lze efektivně bránit využitím protokolu 802.1x, který od každého připojeného zařízení vyžaduje ověření. Ověřením může být jméno/heslo uživatele u obsluhovaných zařízení, nebo např. číslo síťové karty u neobsluhovaných zařízení. Pokud se zařízení neověří, není do sítě připojeno.

S nadstavbovými aplikacemi může administrátor také vyžadovat, aby se na zařízení provedly další kontroly (aktuální antivir, instalované patche, povolený SW). Pokud zařízení kontrolou neprojde, není do sítě vůbec připojeno.

Při vybavení vhodným HW je aktuálně možné komunikaci již na úrovni všech síťových karet a dalších komponent šifrovat, takže se účinně brání útokům odposlechem síťové komunikace.

Cisco prvky obsahují v základní verzi podporu 802.1x, využijte ji. S dalšími nadstavbovými aplikacemi pak poskytují podporu vyšším úrovním bezpečnosti.

## BORDERLESS SÍŤ

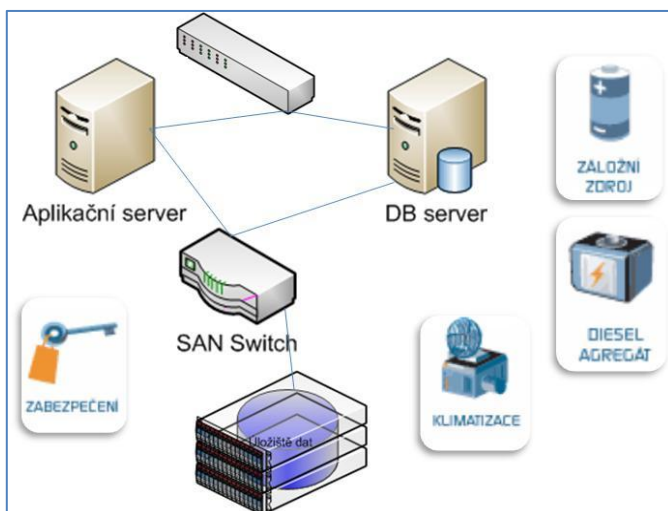
Pro mnoho pracovníků a firem je síť jádrem jejich práce. A velmi jim záleží na tom, aby byla přístupná odkudkoliv a kdykoliv. Proto síť musí umožňovat přístup takovým způsobem, aby uživatel nemusel zkoumat, kde je – zda v síti nebo na cestách.

Kdykoliv má uživatel přístup k Internetu (kavárna, Wifi Hotspot, GSM 3G, ...), komponenty sítě zajistí snadné navázání konektivity do firemní sítě, bezpečnost připojení a přístup k firemním zdrojům. Přičemž firemními zdroji jsou chápány jak servery a sdílená data, tak virtualizované desktopy, telefonní služby či videokonferenční systémy.

## PRAKTICKÉ UKÁZKY UŽITÍ

## UCS (UNIFIED COMPUTING SYSTEMS) – DATOVÁ CENTRA

Na virtuálním příkladu aplikace pro Odbavovací systém MHD je prezentováno řešení hostování aplikace pro zákazníka.



Jelikož se jedná o kritickou aplikaci s vysokými nároky na dostupnost a stabilitu, čeká v konzervativním řešení zákazníka masivní investice do výpočetního systému - musí pořídit nejen všechny HW komponenty, k nim příslušný systémový software, ale vzhledem k požadavkům na dostupnost i dostatečně dimenzovaný záložní zdroj, klimatizaci serverovny a pravděpodobně i záložní diesel agregát, který pokryje masivní výpadek dodávek elektrické energie.

1.rok

2.rok

3.rok

4.rok

5.rok

Zákazník uvažující v rámci moderních trendů v IT se soustředí na samotné poskytování služby aplikace, její administraci a správu. Výpočetní výkon si nakupuje jako službu od společnosti, která jí je schopna nabídnout. Tato varianta mu dává několik nesporných výhod:

- rozložení nákladů rovnoměrně v čase
- požadavky na výpočetní výkon stupňuje v souvislosti s požadavky aplikace (začíná na 1000 klientech, po roce jich má 50 000)
- HW zákazníkovi nestárne (žádný nemá, nakupuje jen výkon) a nemusí řešit reinvestici a jeho obnovu
- dostupnost, stabilita a bezpečnost, kterou není schopen dosáhnout vlastním konzervativním řešením
- v následném provozu se může soustředit na kvalitní administraci aplikace a uživatelskou podporu pro svého interního zákazníka



Virtuální servery / UCS

1.rok

2.rok

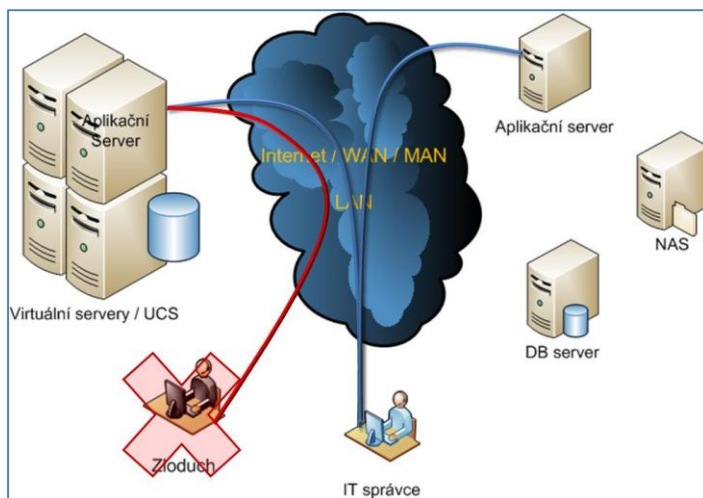
3.rok

4.rok

5.rok

## ZABEZPEČENÍ DAT V UCS A V SÍTI LIS

Tak, jak se stávají informační technologie nejdůležitějším nástrojem pro řídicí procesy firem i organizací veřejné správy, je bezpečnost dat čím dál více noční můrou nejen šéfů a managementu společností, ale i vedoucích oddělení IT a administrátorů. Ztráta dat či jejich únik nejen dokáže položit nejen prosperující firmu, ale i například v nezničitelné veřejné správě může následný mediální útok vyvolat zemětřesení, které „nepřežije“ ani jindy nezničitelné IT oddělení.



Zákazník, který si objedná výpočetní výkon v UCS, neřeší bezpečnostní politiku na centrální úrovni zpracování – toto řeší poskytovatel služby výpočetního výkonu. Ať se již jedná o ochranu před vnějšími nebo naopak před vnitřními útoky. Každá aplikace či každý zákazník může mít vytvořenou svoji virtuální privátní síť, která se, ač postavená na logické vrstvě, vůči okolí chová jako fyzicky oddělená. K dispozici je velké množství preventivních opatření i

analytických nástrojů pro analýzu incidentů a důvodu jejich vzniku.

Úroveň bezpečnosti je nastavena po dohodě se zákazníkem a lze ji opět nastavit v mnoha úrovních, které umožní jak vzdálený přístup dodavatele aplikace k řešení problémů na aplikaci, tak i uživatelů z prostředí domova mimo podnikovou počítačovou síť.

Není zapotřebí mít obavy o bezpečnost „své“ sítě v případě poskytování výpočetního výkonu na virtuálních serverech v síti Liberecké IS,a.s. Tato podporuje plné oddělení zákaznických sítí na všech úrovních:

- přístup do Internetu – každý má vlastní pravidla, adresy, DMZ atd.
- kontrolovaný přístup mezi zákazníky – obě strany musí otevřít svůj firewall
- celá LAN/WAN vidí zákazníky odděleně – existuje tak N sítí na jedné infrastruktuře
- příslušnost do sítě zákazníka na úrovni portu přepínače
- příslušnost do sítě zákazníka na úrovni VNtagu u virtualizovaných platform
- vzdálený přístup do zákaznických sítí

Celá páteř sítě LIS je přiměřeně redundantní - přístup do Internetu je redundantní, páteřní prvky jsou redundantní a redundance se postupně rozšiřuje. Topologie sítě je zokruhovaná. Síť je aktivně monitorovaná a podporovaná v režimu 24/7.

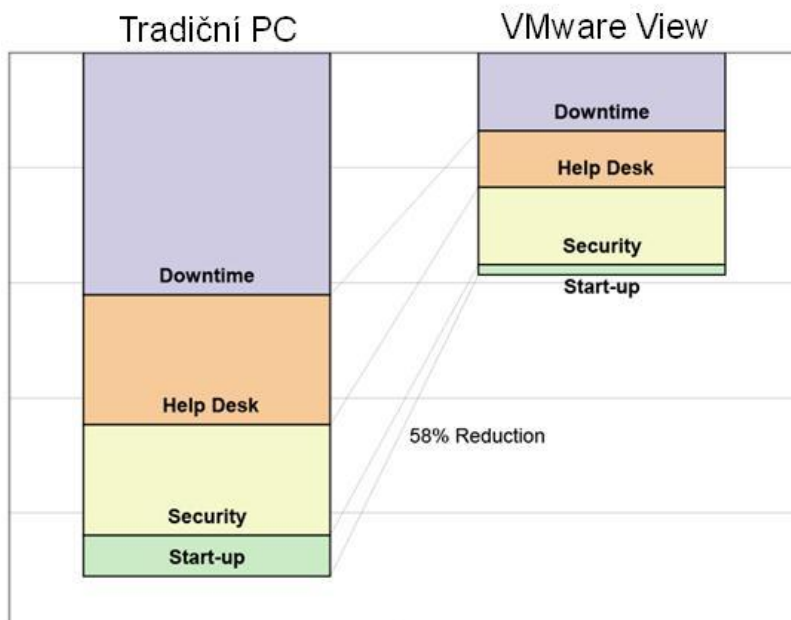
## VIRTUALIZACE PC

Asi největším lákadlem všech IT zaměstnanců je virtualizace koncových stanic – PC. Tento trend není novinkou (viz např. CITRIX), ale v souvislosti s novými trendy řeší některé původně negativní vlastnosti, pro které se „terminálové“ systémy nerozšířily.

Ačkoliv nejnovější typy koncových stanic velikosti malé krabičky o úhlopříčce tužky jsou lákavé, samotná vizualizace koncových stanic nemusí být provedena pouze jednorázovým hromadným nákupem těchto desktopů, ale postupnou obměnou, při níž jsou vyměňována morálně i fyzicky odepsaná PC za nová koncová zařízení. Je nutné si uvědomit, že fyzicky zastaralá PC, která by nezvládla virtualizaci, snad již ve firmách a v úřadech nejsou.

Výhody pro administrátora a helpdesk jsou zjevné – významné úspory času i nervů při řešení běžných incidentů na koncových stanicích. Zvyšuje se i komfort koncového uživatele – při pádu PC zůstává vše na serveru, pracuje z libovolné stanice, kde se přihlásí a neztrácí svoje data.

V literatuře se uvádí až 58% úspora času jak uživatele, tak i IT odborníka pro řešení incidentů.



jednotlivými uživateli na svá PC a z toho vyplývajících možných problémů pro IT oddělení i management, je zřejmé.

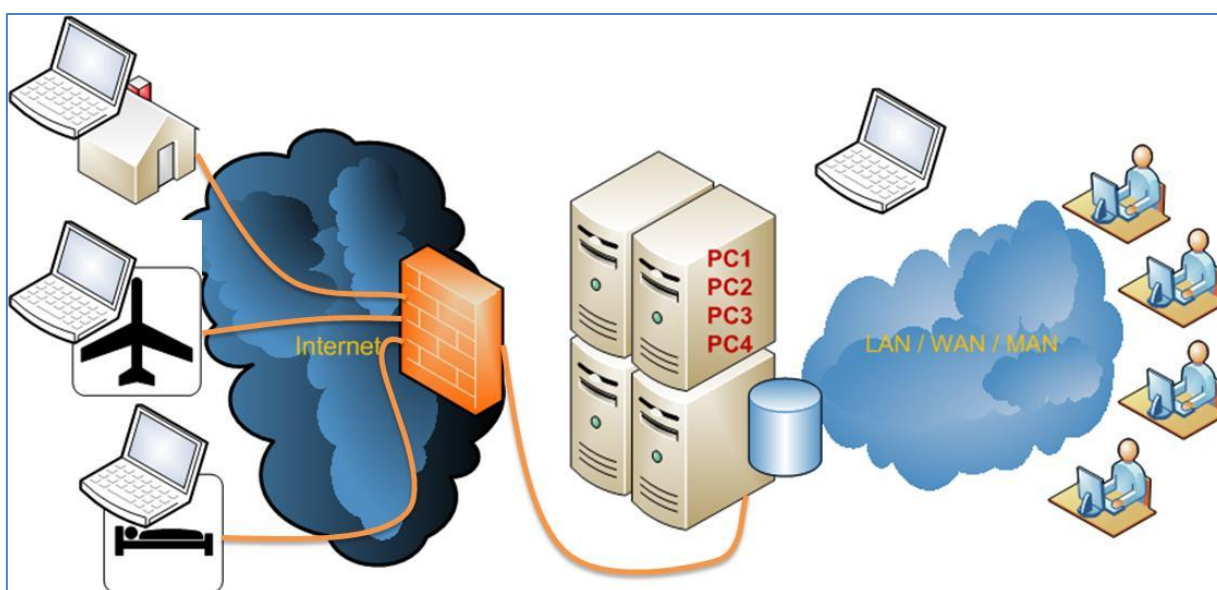
Virtualizace PC nevyklučuje, že se v síti připojují stanice s klasickým operačním systémem, vše je vyřešeno na úrovni systémového SW.

Pro úplnost je nutné dodat, že vizualizace PC nesnižuje požadavky na licence operačního systému a aplikačního SW, na druhou stranu však umožňuje optimalizovat jejich počet v organizaci. Že se tím eliminuje jakákoliv možnost instalování nelegálního SW

## BORDERLESS NETWORK

Borderless network je výraz, při kterém pracovníku IT musí vstávat vlasy hrůzou na hlavě. Všechny výše uvedené nástroje však dokážou takto provozovanou síť zajistit pro své uživatele opravdu „bez hranic“.

Míní se tím práce uživatele ze svého PC, smartphone, notebooku odkudkoliv, kde je konektivita, ve své privátní síti. Nezáleží na tom, zdali se jedná o zaměstnance, který má povoleno pracovat z domova, obchodního zástupce pendlujícího mezi zákazníky a neustále zasahujícího do firemního objednávkového systému nebo ředitele společnosti, který často cestuje do zahraničí a potřebuje být neustále se svými firemními daty. Stačí mít pouze konektivitu, a je jedno, jestli je to v rámci GSM, WiFi hotspotu či na návštěvě u kamaráda s domácí sítí.



A lahůdka na závěr – pokud je ve firmě implementován VoIP, lze odkudkoliv, kde je konektivita, volat téměř zdarma jakoby ze svého stolního telefonu, a je jedno, jestli se jedná o volání z hotspotu v pražské kavárně, nebo z herny v Las Vegas.

## PROFILY PREZENTUJÍCÍCH FIREM

## LIBERECKÁ IS

Liberecká IS, a.s. je společností založenou v roce 2002 Statutárním městem Liberec pro správu a rozvoj svého informačního systému. Postupně zakládá a rozvíjí další městské projekty, jako je Metropolitní síť, Liberecká městská karta a Technologické centrum SML. Je držitelem prověrky NBÚ na stupeň vyhrazené a certifikátu ISO 9001:2000.



NET-SYSTEM s.r.o. je liberecká firma založená v roce 1993. Stěžejní oblastí je návrh a konfigurace LAN/WAN sítí zahrnujících datové, hlasové i další služby. Firma je držitelem mnoha bezpečnostních prověrek, znalostních certifikací a certifikátu ISO 9001:2000.

## PROFILY PREZENTUJÍCÍCH

**Ing. Jiří Novák, NET-SYSTEM, s.r.o., technický ředitel**

Věnuje se návrhu LAN/WAN datových a hlasových sítí a virtualizaci.

**Martin Zapadlo, NET-SYSTEM, s.r.o., vedoucí úseku služeb**

Věnuje se návrhu LAN/WAN datových sítí a bezpečnostní problematice v nich.

**Petr Solnař, Liberecká IS, a.s., manažer úseku projektů**

Zpracovává design IT řešení pro LIS a zákazníky společnosti, řídí strategické IT projekty společnosti.

**Ing. Jiří Hruboň, Liberecká IS, a.s., manažer úseku obchodu a marketingu**

Řídí projekty aplikovaného IT (kartové systémy, rezervační a platební systémy), marketing a obchod společnosti.