

Adatközpont - Hálózat

State of the Art and Best Practices

-- by Moldován István --

A hatékony adatközpont kiépítése érdekében célszerű a szükséges technológiákat áttekinteni a legalacsonyabb szinttől a legmagasabb szintig.

A következő szinteket különböztetjük meg:

1. Tárolás/Szolgáltatás/virtualizálás
2. Hálózat/hálózat virtualizálás
3. Szolgáltatás menedzsment / Orchestration

1 Szolgáltatások

Szolgáltatások terén szerverekre gondoljunk, melyeken Hypervisor-ok biztosítják a virtuális gépek menedzsmentjét. Elosztott tárolás – új trend az SSD alapú tároló :

<http://www.purestorage.com/products/flash-array-m/> ami sokkal nagyobb sebességű.

A szerver oldali hálózati virtualizálás szintén fontos követelmény, melynek ugyanakkor része a szolgáltatások szeparációjára is (tűzfalak, terhelésmegosztás, VPN és IPSec alapú megoldások, távoli hozzáférés, IPS). Ezeket a feladatokat tipikusan a szerveren futó virtuális switch látja el. Tipikus megvalósítása lehet a s: [VMware virtual switch](#) (standard & distributed), [Cisco Nexus 1000V](#), és az Open vSwitch (OVS).

A vSwitch alapú megoldások általában csak Ethernet/IP konnektivitást igényelnek, de támogatják a VLAN, LACP (link aggregáció) kezelést is.

SAN specifikusan:

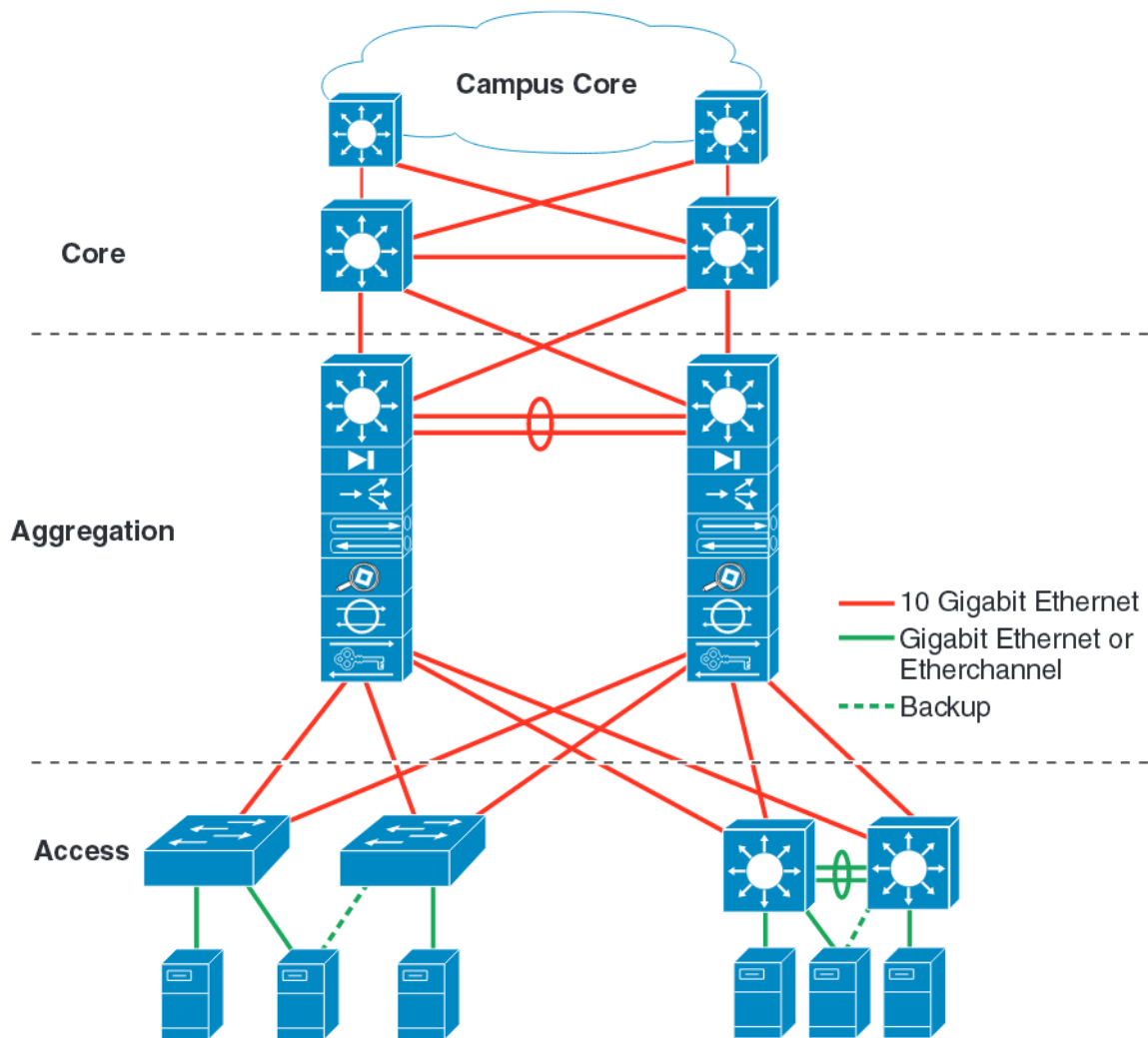
- [ATA over Ethernet \(AoE\)](#), mapping of [ATA](#) over [Ethernet](#)
- [Fibre Channel Protocol](#) (FCP), the most prominent one, is a mapping of SCSI over [Fibre Channel](#)
- [Fibre Channel over Ethernet](#) (FCoE)
- [ESCON](#) over Fibre Channel ([FICON](#)), used by [mainframe computers](#)
- [HyperSCSI](#), mapping of SCSI over Ethernet
- [iFCP^{\[4\]}](#) or [SANoIP^{\[5\]}](#) mapping of FCP over IP
- [iSCSI](#), mapping of SCSI over [TCP/IP](#)
- [iSCSI Extensions for RDMA](#) (iSER), mapping of iSCSI over [InfiniBand](#)

A hálózati réteg követelményeit a szolgáltatások nyújtásához szükséges technológiák határozzák meg, ezért fontos összefoglalni azokat a technológiákat, amelyek használatban vannak/lesznek.

2 Hálózat

Az adatközpont hálózati tervezés alapja egy bevált többszintű megközelítés, amelyet már a legnagyobb adatközpontokban teszteltek, és sokat fejlesztettek az elmúlt néhány év során. Az adatközpontok tervezésének alapja a réteges megközelítés, amely arra törekszik, hogy javítsa a skálázhatóságot, teljesítményt, rugalmasságot, és megkönnyítse a karbantartást.

Az 1. ábra mutatja be a több rétegű hálózati tervezési modellt.



1. ábra Az alapvető többszintű tervezés

Az adatközpontok tervezésénél a következő rétegeket különböztetjük meg: a központi, aggregációs és hozzáférési réteg. Röviden a következőképpen jellemezhetjük ezeket a rétegeket:

- A Core réteg biztosítja a nagy sebességű csomagkapcsolt backplane-t minden folyamannak, amely ki- és bemegy az adatközpontba. A core réteg összeköttetést teremt az aggregációs modulok között és biztosít egy olyan megbízható harmadik szintű, routolt kapcsolást, amelynek nincs egyedi hibapontja (single point of failure). A core rétegben fut egy interior routing protokoll, mint például OSPF vagy EIGRP, és a terhelésmegosztást végezz a campus core és aggregációs rétegek között a Cisco Express Forwarding alapú hash algoritmusok használatával.
- Az Aggregation rétegbeli modulok fontos funkciókat biztosítanak, mint például a szolgáltatási modul integrálása, Layer 2 domain-meghatározásokat, feszítőfa protokoll (STP) futtatása, és az alapértelmezett átjáró redundancia biztosítása. A Szerverek közötti többlépcsős forgalom átfolyik az aggregációs rétegen és használhat szolgáltatásokat, mint például a tűzfal és szerver terhelés megosztás, hogy optimalizálja és biztonságossá tegye az alkalmazások elérését. A kisebb ikonok az 1. ábra szerinti aggregációs rétegben az integrált szolgáltatási modulokat jelentik. Ezek a modulok szolgáltatásokat nyújtanak, mint például a tűzfal terhelés elosztás, SSL tehermentesítés, behatolás-jelző, hálózati elemzés, stb.

- Access réteg, amelyben a szerver fizikailag kapcsolódik a hálózathoz. A szerver komponensek 1RU szerverekből, beépített kapcsolós blade szerverekből, pass-through kábelezésű blade szerverekből, szerver klaszterekből, OSA adapteres nagygépekből állnak. A hozzáférési réteg hálózati infrastruktúrája moduláris- illetve TOR kapcsolókból, fix konfigurációjú 1 vagy 2RU kapcsolókból és integrált blade szerver kapcsolókból áll. Switchek biztosítják mind a Layer 2 és Layer 3 topológiát, amely megfelel a különböző kiszolgálók broadcast tartomány vagy egyéb adminisztrációs követelményeinek.

2.1 Data Center Design Modellek

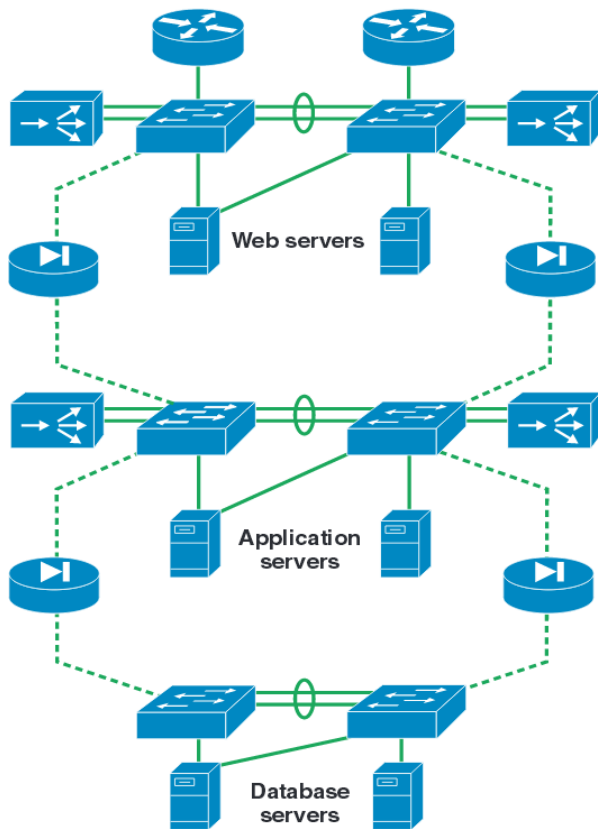
A multi-tier modell a leggyakoribb tervezési módszer. A web, alkalmazás és adatbázis réteget kialakításon alapul, és támogatja a kereskedelmi és a vállalati üzleti ERP és CRM megoldásokat. Ez a fajta kialakítás sokféle webes szolgáltatási architektúrát támogat, mint például a Microsoft .NET vagy Java 2 Enterprise Edition alapúakat. Ezeket a web service alkalmazási környezeteket használják a Siebel és az Oracle által használt ERP és CRM megoldások, hogy csak néhányat említsünk.

A szerver cluster modell az egyetem és a tudományos közösségből nőtt ki és manapság elterjedt a vállalati üzleti szférában, beleértve a pénzügyi, gyártási és szórakoztató ipart. A szerver cluster modellt leggyakrabban nagyteljesítményű számítástechnika (HPC), párhuzamos számítási, és nagy áteresztőképességű számítástechnika (HTC) környezetben használják, de grid / utility számítási feladatokhoz is megfelelő.

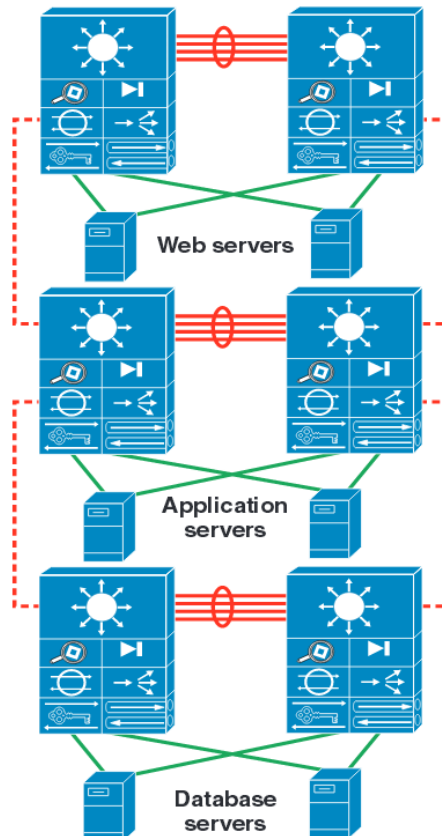
2.1.1 A Multi-tier Modell

A multi-tier adatközponti modellt jellemzően a HTTP-alapú alkalmazások esetén használják. A multi-tier adatközponti modell web, alkalmazás és adatbázis szerver rétegeket tartalmaz. Manapság a legtöbb web-alapú alkalmazás többrétegű alkalmazásként épül fel. A sokszintű modellben olyan szoftver fut, amely különálló processzekből áll, amelyek ugyanazon a gépen futnak inter-processz kommunikációt használva (IPC), vagy különböző gépeken futnak és ez esetben a kommunikáció a hálózaton keresztül történik. Jellemzően, a következő három lépcsője használjuk:

- Web – szerver
- Alkalmazás
- Adatbázis

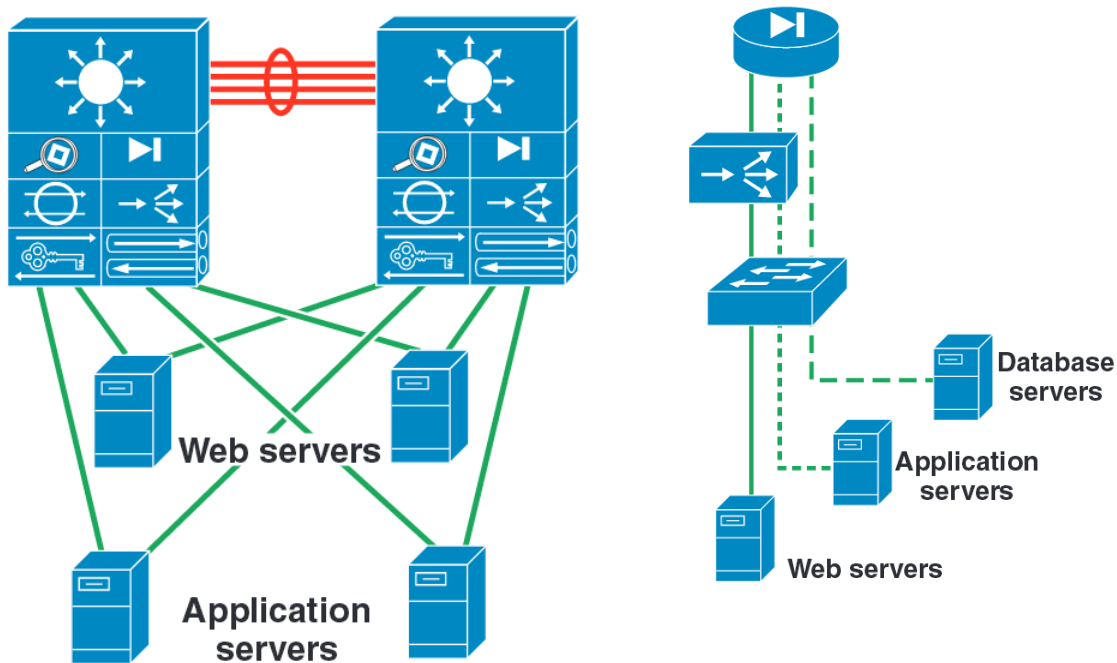


2. ábra Fizikailag szétválasztott infrastruktúra (A)



(B)

A Multi-tier szervert farmok amelyek különböző gépeken futtatják a processzeket általában nagyobb rendelkezésre állást és jobb biztonságot nyújtanak. A megbízhatóság azért javul, mert egy szervert kiesése esetén más szervert veheti át ugyanazt a funkcionalitást. A biztonság javul, mert a támadók behatolhatnak a web szervertre anélkül, hogy hozzáférjenek az alkalmazás vagy adatbázis-kiszolgálókhoz. A Web és alkalmazás szervert futtatnak fizikailag közös szerverten; az adatbázis jellemzően továbbra is külön szerverten fut.



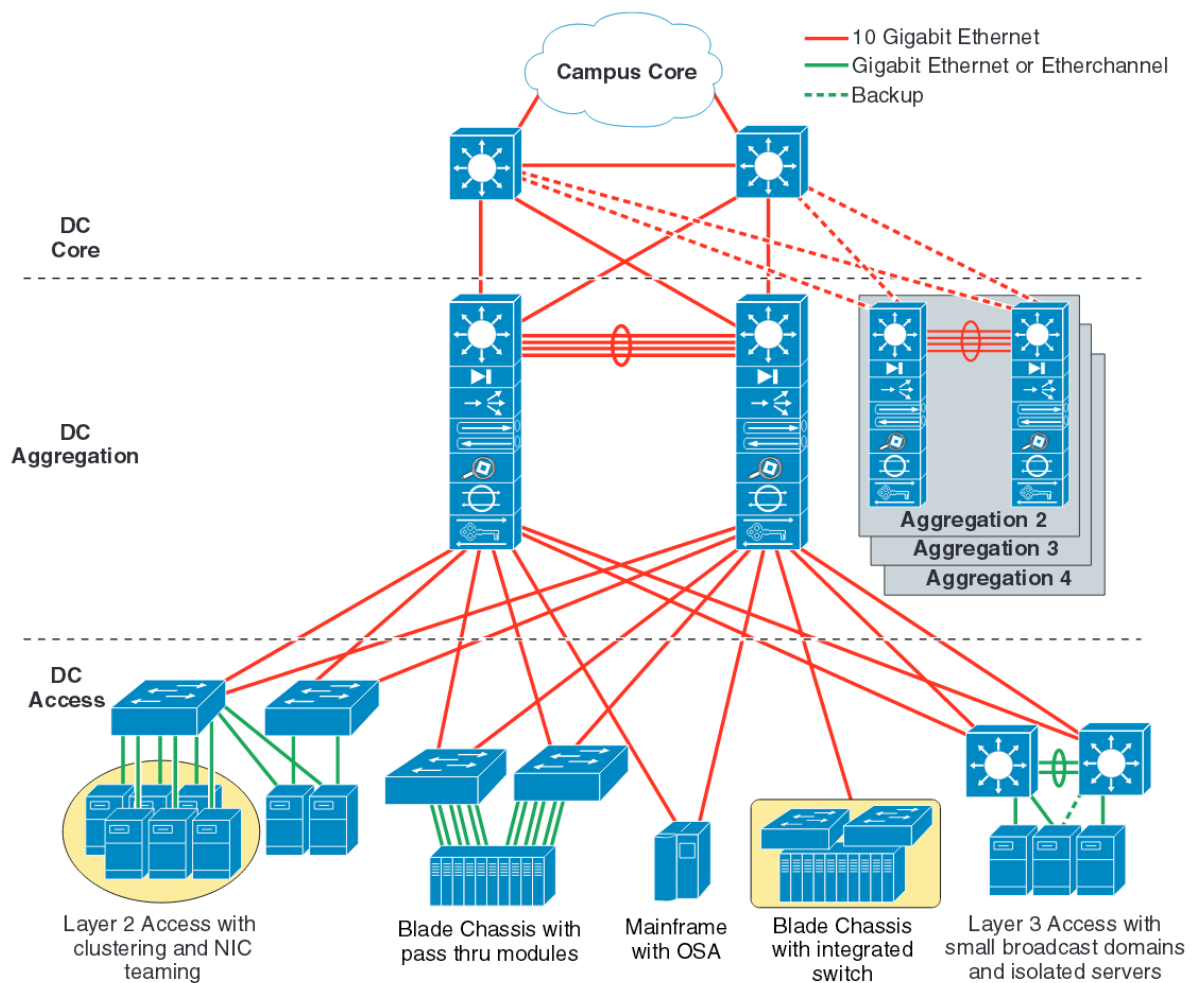
3. ábra VLAN alapú elválasztás – fizikai topológia (A)

és logikai topológia (B)

A 3. ábra egy olyan megoldást mutat be, ahol VLAN-okat használunk a szerver farmok elkülönítésére. A bal oldali ábra (A) mutatja a fizikai topológiát, míg a jobb oldali (B) mutatja a VLAN-ok at a különböző szolgáltatási modulok, tűzfal, terheléselosztó és kapcsolók között. A tűzfal és terheléselosztó, amelyek VLAN-képes, biztosítja a szerver farmok között a VLAN alapú szegregációt. Megfigyelhető, hogy nem minden a VLAN-ra szükséges a terhelés megosztás. Például az adatbázis a példában forgalmat küld közvetlenül a tűzfalnak.

A fizikai szegregáció javítja a teljesítményt, mert a lánc minden szintjén a szerverek dedikált hardverhez csatlakoznak. A VLAN-okkal megvalósított szegregáció előnye, hogy segítségével egyszerűsödik a szerver farm. A fizikai elkülönítés vagy logikai szegregáció közötti választás függ a konkrét hálózati teljesítmény követelményektől és a forgalomtól.

Tipikusan a nagyságrendileg max. 40 szerver egy rack-ből csatlakozik a Top of the Rack (TOR) kapcsolóhoz. A TOR kapcsolók, amelyek az egyes rack-eken belül kötik össze a szervereket jelentik az első hálózati réteget a hierarchiában, az úgynevezett access réteget. Az egyes access kapcsolók több aggregációs kapcsolóhoz csatlakoznak. Ezek alkotják a második réteget. Egyetlen hozzáférési réteg kapcsolónak csatlakoznia kell minden aggregációs rétegbeli kapcsolóhoz. Az felső kategóriás enetrprise szintű core kapcsolók alkotják a legfelső szintét a három rétegű topológiának. A rack-en belüli forgalmat az access rétegbeli kapcsolók kezelik le. A rack-ek közötti forgalom esetében, ha a TOR kapcsolók ugyanahhoz az aggregációs kapcsolóhoz csatlakoznak, a forgalom az aggregációs rétegbeli kapcsolókon halad keresztül. Ha a TOR kapcsolók nem ugyanahhoz az aggregációs kapcsolóhoz csatlakoznak, a forgalom áthalad a core rétegbeli kapcsolókon. A hierarchia felsőbb rétegei magasabb túlméretezési tényező (oversubscription ratio) rendelkeznek. A túlméretezési tényező a legrosszabb a végpontokra jutó rendelkezésre álló sávszélesség és az őt kiszolgáló teljes hálózati topológia sávszélességének arányai közül.



4. ábra Multi-tier topológia

Az **adatközpont core** réteg egy nagy sebességű csomagkapcsolt kapcsolatot biztosít több aggregációs modul között. Ez a réteg szolgál átjáróként a campus core felé, ahol más modulok csatlakoznak, beleértve például az extranetet, WAN-t és az internet edge routereket. Minden útvonalat az adatközpont core-nál Layer 3 szinten végződtetnek, és jellemzően 10 GigE vagy annál nagyobb sebességű interfészeket támogatnak a nagy átviteli sebesség, teljesítmény garantálására és hogy megfeleljen a túlméretezési tényezőknek.

Az **aggregációs réteg**, melyhez nagy számú access rétegből jövő uplink kapcsolódik, elsődleges feladata a nagyszámú kapcsolat kezelése, amelyek bejönnek illetve elhagyják az adatközpontot. Az aggregációs kapcsolóknak képesnek kell lenniük támogatni sok 10 GigE és GigE interfészeket miközben egy nagy sebességű kapcsolómezővel kell rendelkezniük. Az aggregációs réteg nyújt érték-növelt szolgáltatásokat is, mint például a szerver terhelés megosztás, tűzfal, és az SSL terhelésmentesítést a hozzáférési réteg kapcsolói által kiszolgált szerverek számára. Az aggregációs réteg kapcsolói végzik a feszítőfa (spanning tree) protokollok futtatását és az alapértelmezett átjáró redundancia protokoll kezelését. Az aggregációs réteg lehet a legkritikusabb réteg az adatközpontban, mert portsűrűség, túlméretezési tényező szintje, CPU, a szolgáltatási modulok egyedi követelményeket támasztanak. Az aggregációs réteg kialakítása kritikus a teljes adatközpont stabilitása és a skálázhatósága szempontjából. Minden forgalom az adatközpontban nem csak áthalad az aggregáción, hanem támaszkodik a szolgáltatásaira, az útvonal kiválasztásra, és az aggregációs réteg redundáns

architektúrára. Az aggregációs réteg kialakításánál nagy hangsúlyt kell fektetni a következő négy területre:

- Layer 2 fault domain méret
- Spanning tree skálázhatóság
- 10 GigE denszítás
- Default gateway redundancia skálázhatósága (HSRP)

Az **access réteg** biztosítja a fizikai szintű kapcsolatot a szerver erőforrások között, Layer 2 vagy Layer 3 szintű hozzáférést biztosítva. A mód kritikus szerepet játszik különböző szerver követelmények esetén, mint pl. a NIC teaming, klaszterezés, és broadcast domain elszigetelés. A hozzáférési réteg az első túlméretezési pont az adatközpontban, mert aggregálja a szerverek forgalmát 10 GigE / 10 Gigabit EtherChannel uplinkekre. A feszítőfa protokollok vagy a Layer 3 routing protokollok kiterjednek az aggregációs rétegből az access rétegbe attól függően, hogy milyen módú aggregációt használunk.

Javasolt az access rétegbeli kapcsolókat redundáns módon párokba rendezni.

2.1.2 Server Cluster Model

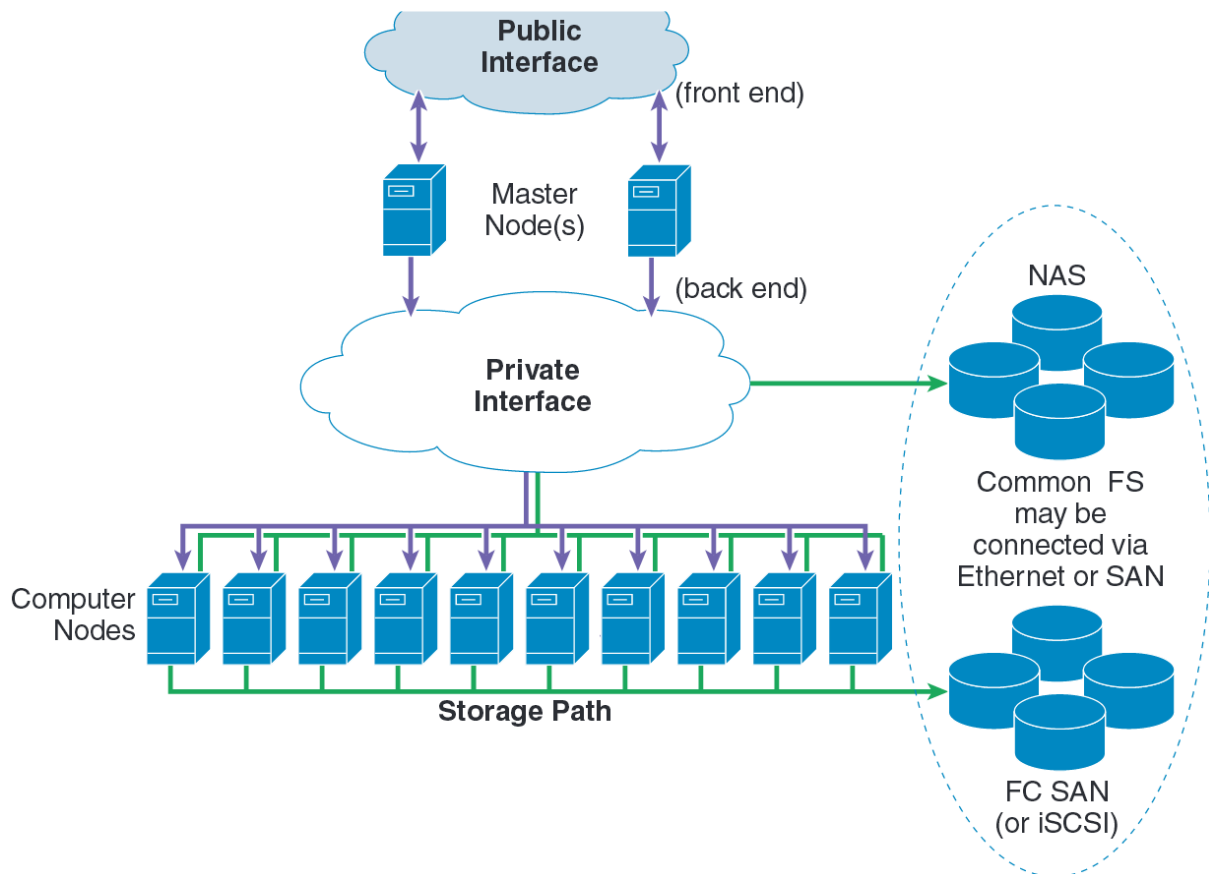
A modern adatközpont környezetben szerver klasztereket használnak sokféle célra, beleértve a magas rendelkezésre állást, terheléelosztást, és a megnövekedett számítási teljesítményt. Minden klaszter közös célja egyesíteni több CPU-t, hogy úgy jelenjen meg, mint egy egységes, nagy teljesítményű rendszer. Ezt speciális szoftverrel és nagy sebességű hálózati összeköttetésekkel valósítja meg. A szerver klasztereket korábban egyetemi kutatással, a tudományos laboratóriumokban való munkával, és a katonai kutatásokkal kapcsolatban használták, illetve különleges alkalmazásokhoz, mint például a következők:

- Meteorológia
- Szeizmológia
- Katonai kutatás
- Applikációs szerverek
- Web szerverek
- Adatbázis szerverek

A szerver klaszterek most a vállalati szférában is megjelentek, mert a klaszterezési technológia ma már szélesebb körben alkalmazható. Az alábbi alkalmazások igénylik ezt a technológiát:

- Pénzügyi Trendanalízis - Real-time kötvény árelemzés és trendkezelések
- A film animáció – A művészek gigabájtos fájlokat renderelnek
- Gyártás - Automotive tervezés, modellezés és aerodinamika
- A keresőmotorok - gyors párhuzamos keresés és tartalombeszúrás

A vállalati szférában egyre nagyobb az igény a nagy sávszélesség és alacsonyabb késleltetés felé, amelynek szerver klaszterezéssel lehet eleget tenni.



5. ábra Szerver klaszter topológia

A szerver klaszter komponensek a következők:

- **Front end** - Ezeken az interfészekon nyújt külső hozzáférést a klaszterhez, amely elérhető az alkalmazás szerverek, vagy a felhasználók, amelyek benyújtása munkahely vagy visszakeresése munkát eredmények a klaszter. Ilyen például egy művész, aki benyújtja a fájlt a renderelésre, vagy visszaolvas egy már renderelt eredményt. Itt tipikusan egy Ethernet IP interfész csatlakozik a hozzáférési rétegből a meglévő szerver farm infrastruktúrájához.
- **Master node**-ok (más néven head node) -A mester csomópontok menedzselik a klaszterben a számítási csomópontokat és felelősek a klaszter és optimális működéséért. Általában mester csomópont az egyetlen csomópont, amely kommunikál a külvilággal. Klaszterező middleware fut a mester csomóponton, amely biztosítja azokat az erőforrás menedzsmentet, a munka ütemezését, és a számításokat végző node-ok monitorozását. A Mester csomópontokat jellemzően redundáns módon telepítik és általában a nagyobb teljesítményű szerverek, mint a számítási node-ok.
- **Back-end** nagysebességű kapcsolómező-Ez a nagy sebességű kapcsoló az elsődleges közeg amely biztosítja a master node és számítási csomópontok közötti kommunikációt. Tipikus követelmények közé tartozik az alacsony késleltetés, magas sávszélesség de a követelmények kiterjedhetnek a jumbo frame és 10 GigE támogatásra is. Ethernet a legnépszerűbb technológiavde más technológiák is ígéretesnek mutatkoznak, különösen az Infiniband.
- **Compute node** – A számítási csomóponton fut egy optimalizált OS kernel, és felelős a CPU-intenzív tevékenységek elvégzéséért.
- **Storage path**-jellemzően az Ethernet vagy Fibre Channel interfész. A back-end és a storage path lehet egy közös médium, például olyankor amikor az IP over Ethernet-et használunk a tároló eléréséhez. Tipikusan ha az NFS vagy iSCSI protokollt használunk a NAS vagy SAN-átjáró elérésére.

•**Közös fájlrendszer** -A szerver cluster közös párhuzamos fájlrendszert használ, amely lehetővé teszi a nagy teljesítményű hozzáférést az összes számítási node-hoz. A fájlrendszer típusok az alkalmazott operációs rendszertől függenek (például PVFS vagy Lustre)

2.2 Új trendek

2.2.1 Converged Enhanced Ethernet

Az adatközpontban többféle transzport technológiát [3] használnak, melyek között egyre nagyobb szerepet kap az Ethernet. Ennek fő oka a nagy elérhető sávszélesség és az alacsony ár. Azonban az Ethernet sok korlátozással és hiányossággal bír amelyeket folyamatos szabványosítással orvosolnak.

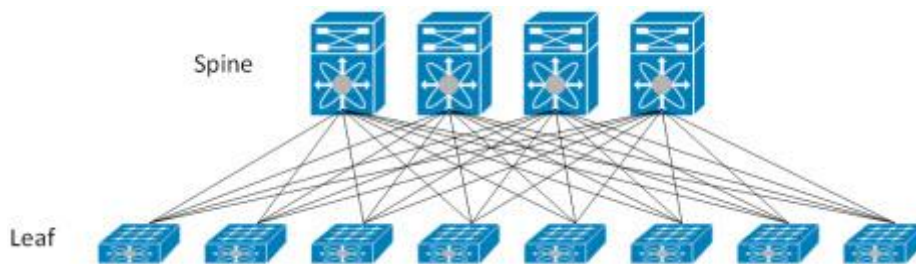
A Converged Enhanced Ethernet (CEE) egy továbbfejlesztett Ethernet technológia, amelyet az adatközpontokban használt különböző alkalmazások egységes hálózaton való kiszolgálására fejlesztettek ki. A CEE elsődleges célja, hogy csökkentse a szerverek kapcsolódásához szükséges kábelek és adapterek számát. A Convergence Enhanced Ethernet olyan fejlesztéseket (pl. csomag prioritizálás), tartalmaz, amelyek révén a nagy adatközpontok egyetlen Ethernet-hálózaton konszolidálhatják a különféle (pl. Infiniband, Myrinet, FC, SCSI) fűtözési, tárolási és adatkapcsolataikat. A CEE a következő fontosabb kiegészítéseket tartalmazza:

- Priority Flow Control: egy szabványos a különböző forgalmi osztályok prioritásos kezelésére. A cél a nulla csomag veszteség biztosítása leterhelt adatközpont esetén is.
- Data Center Bridging exchange: elsősorban a szabványos adatközponti kapcsolódási mechanizmus, amely az interoperabilitást biztosítja
- Priority-Based Packet Scheduling: egy szabványos mechanizmus különböző forgalmi osztályok proiritási sorokba való rendezésére.

A CEE egy új szabvány, amelyet sok gyártó - beleértve a legnagyobbakat - támogat. Heterogén rendszer kialakítása esetén feltétlenül érdemes olyan eszközöket választani, amelyek támogatják ezt a szabványt.

2.2.2 Architektúra és vezérlés

Az adatközpont nagy teljesítményű, kezelhetőbb hálózatot igényel, amely képes biztosítani a nem-blokkoló közötti összeköttetést a rack-ek között az adatközpontban. Ezeket a követelményeket a nagyobb teljesítményt nyújtó Top-of-Rack (TOR) kapcsolókkal és sík, egyrétegű hálózati topológiával érhetjük el. Először is, költség-hatékony 1U TOR kapcsolókat vezettek be, hogy egy teljes rack szerverek vagy a tároló csomópont kiszolgálását biztosítsa 10 GbE sebességgel, 40 GbE uplinkekkel a gerinc hálózat felé. Másodsor, az adatközpontok üzemeltetői új hálózati topológiát alkalmaznak, hogy megfeleljen a skáláhatósági és a teljesítményre vonatkozó követelményeknek. A hagyományos három vagy négy szintű hálózati modell (hozzáférés-aggregációs-gerinc-core) egy túljegyzett (oversubscribed) fat-tree topológia. A nyilvános felhő szolgáltatók most hogy inkább a költséghatékony kevesebb szintet használó alapján Clos hálózati topológia irányába mozdulnak el.



6. ábra CLOS hálózati topológia

Clos hálózatokra vannak példák számos adatközpont összekötési közeg (fabric) architektúrában a különböző kapcsoló gyártónál. A *Transparent Interconnect of Lots of Links* (TRILL) egy 2. rétegbeli adatközpont protokoll, amely az STP protokoll lecserélését célozza, „flat” topológiát hozva létre harmadik szintű protokollok segítségével. A TRILL lehetővé teszi alternatív útvonalak használatát redundáns Clos hálózati architektúrában és feleslegessé teszi a feszítőfa protokollt, amely blokkolná az alternatív kapcsolatokat. Sok gyártó implementálta a TRILL egy saját változatát:

A Cisco megoldása a FabricPath, ami a TRILL szabvány egy kiterjesztése. Cisco adatközponti kapcsolók, mint a Nexus 7000 switchek kapcsolódnak egy Clos hálózatban Nexus 5000 és / vagy Nexus 2000 kapcsolókhoz és FabricPath futtat ezen az adatközponton belül és csatlakozhat más adatközpontokhoz is.

A Juniper QFabric rendszer valójában nem TRILL-alapú, hanem egy belső anyag Juniper által kifejlesztett protokoll „fabric” protokollt használ, amely az IEEE RFC1142 (más néven az IS-IS) routing protokollra épül. A QFabric csomópontok összeköttetése alkot egy olyan adatközpont „fabric”-ot, amely, több redundáns uplink-et képes használni így nyújtva nagyobb teljesítményt és megbízhatóságot.

A Brocade Virtual Cluster Switching (VCS) „fabric” a Brocade TRILL szabvány implementációja, amely lehetővé teszi a Clos hálózati topológián az redundáns linkek használatát.

Az Arista Spline architektúrája a levél (leaf) és a gerinc (spine) terminológiát egy új szóban egyesíti, amely egy egyszintű, lapos hálózati architektúrát takar.

OpenFlow közvetlen hozzáférést tesz lehetővé, és lehetővé teszi a hálózati eszközökben, például a fizikai és a virtuális (hypervisor-alapú) kapcsolók és útválasztók csomagtovábbítási síkjának manipulációját. A nyílt szabványt nagy érdeklődés övezi, segítségével (és egy központosított vezérlő segítségével) kézben tarthatók az útvonalak az adatközpontban. Az Openflow támogatottságával kapcsolatos jó hír, hogy az elmúlt néhány hónapban, szinte minden nagyobb adatközpont Ethernet kapcsoló gyártó (Arista, a Cisco, a Dell Force 10, a HP és a Juniper) piacra dobott általános elérhetőségű (GA) dokumentált OpenFlow változatot az egyes adatközpont kapcsolóira. Ugyanakkor a rossz hír az, hogy két gyártó implementációja még távolról sem bír hasonlítható funkcionalitással... Összegezve, az elérhető Openflow implementációkkal csak nagyon alapvető L2 vagy L3 célállomás alapú kapcsolást lehet megvalósítani az interoperabilitást is figyelembe véve.

2.3 Forgalom szétválasztás

Míg a VLAN-okat már régóta használjuk kisebb és kevésbé komplex hálózatokban forgalom elválasztásra, az IEEE 802.1Q VLAN szabvány csak 12 bites VLAN azonosító mezőt támogat.

Ez a 12-bites mező, vagy durván 4000 VLAN, úgy tűnt, elegendő az 1990-es években, amikor a szabványt eredetileg kidolgozták, azonban a nagy multi-tier felhők sokkal több VLAN tunnelt igényelnek. Ahhoz, hogy megoldjuk ezt a problémát az adatközponti környezetben, a gyártók három megoldást javasoltak: VXLAN, NVGRE és Stateless Transport Tunneling (STT). Mindhárom megoldás beágyazást használ, ahol az adatcsomagok egy új fejléccel kapnak, nem kompatibilisek egymással. VXLAN és NVGRE fejlécek mind tartalmaznak egy 24-bites azonosító mezőt. Az STT egy 64 bites azonosító mezőt használ. Egyik megoldás sem igényel hardver cserét vagy módosítást, bár az egyes gyártók hardveres gyorsítást is használnak a hatékonyság növelésére.

Most egy új hálózati virtualizációs szabvány jelenik meg - a Generic Network Virtualization Encapsulation (GENEVE) [4] amely az eddigi megoldások hátrányait javítja ki, míg az VXLAN, NVGRE és STT összes tulajdonságát örökli. Előre láthatóan az új szabvány teljes egészében le fogja váltani elődeit, azonban jelenleg még nincs széles körben elterjedve.

3 Szolgáltatás menedzsment

Az **OpenStack** egy infrastruktúra szolgáltatás projekt, egy szabad szoftver, ami több alprojektből áll, amelyek irányítják a tárhely, a számítási kapacitás és a hálózat felhasználását egy adatközpontban. Mindehhez egy web felületet biztosít, amelyen a felhasználók virtuális gépeiket hozhatják létre, illetve a rendszergazdák felügyelhetik a rendszer erőforrásait.

A **CloudStack** egy nyílt forráskódú felhő alapú számításokat vezérlő szoftver, amellyel az Oracle VM, a KVM, a vSphere és a XenServer hypervisorokkal tud együttműködni. Saját API-ja mellett az Amazon EC2 és S3 felületeket is biztosítja.

A **vmWare NSX** névre keresztelt új megoldással triviálissá egyszerűsíthető a fizikai hálózat, a komplex feladatokat pedig kizárólag a szoftveres hálózati eszközök végzik. A vállalat reményei szerint az NSX-szel kiegészülve a portfóliója már versenyképes alternatívát nyújt a divatos OpenStack ellenében és sikerül felugrani a "software defined data center" vonatjára. Az NSX központi elemét a logikai switchek és routerek jelentik, amelyekkel hálózatba rendezhetőek a virtuális gépek. A logikai hálózati eszközök teljesen elválnak a hardveres, fizikai hálózattól, ezzel ez utóbbi gyakorlatilag minden hozzáadott értékét elveszti, csupán a fizikai gépek fizikai összekapcsolására szolgál. A fejlettebb hálózati funkciókat a virtuális hálózati eszközök végzik, ezek közé tartozik logikai tűzfal, terheléelosztó, QoS, biztonság, felügyelet és VPN is, amelyek API-kon keresztül a VMware saját rendszerfelügyeleti eszközeivel egységesen programozhatóak és automatizálhatóak. [1]

A **Cisco ACI** kontroller-alapú infrastruktúra, amely a hálózati eszközök és a vezérlő közötti hatékony és mély együttműködésre épít a nyílt szabványokon alapuló OpenFlow-val és a hálózatvirtualizációval szemben. Az Application Centric Infrastructure felépítését tekintve nagyon hasonló az OpenFlow modellhez, a switchek beállításait egy célgép, az APIC (Application Policy Infrastructure Controller) vezérli, ennek megfelelő programozásával a teljes hálózat automatizáltan irányítható. A megközelítés előnye, hogy új adatközponti alkalmazás telepítésekor vagy a meglévő alkalmazások módosításakor a hálózat könnyedén adaptálható, nincs szükség időigényes és hibaforrásként jelentkező manuális beállításokra. További fontos szempont, hogy a vezérlő egységes programozási felületet kínálhat, amely a hálózatot, szervereket és tárolókat egyben kezelő megoldások számára könnyű belépési pontot jelent a hálózat irányába - ezzel pedig elhárul a "felhő", vagyis a magas szinten automatizált adatközpont létrehozása útjából az akadály. A vezérlő és a switchek közötti kommunikáció a Cisco

architektúrájában nem szabványos, az OpenFlowtól eltérően igen korlátozott a nyitottságról az ACI rendszerén belül - mondták el a gyártó képviselői a HWSW kérdésére. Ez azt jelenti, hogy az APIC nem képes más gyártók kapcsolóit vezérelni, és más cégek sem készíthetnek a Cisco switcheihez ilyen vezérlőt. [8]

A Nuage Networks Virtual Services Platform - összhangban az SDN elvekkel, a Nuage Networks VSP tartalmaz egy Cloud Service Management síkot, egy Datacenter vezérlési síkot, és a Datacenter adatsíkot. Ezek segítségével egy komplex menedzsment megoldást nyújt, melyen keresztül vezérelhető mindhárom sík. További előnye a megoldásnak, hogy szabványos és nyílt forrású megoldásokra épít, együtt képes működni a leggyakrabban használt megoldásokkal.

Referenciák

- [1] <http://www.networkcomputing.com/networking/your-networks-next-step-cisco-aci-or-vmware-nsx/a/d-id/1318600>
- [2] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/HA_Clusters/HA_Clusters/HAtrans_2.html
- [3] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/HA_Clusters/HA_Clusters/HAtrans_2.html
- [4] <http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-733127.pdf>
- [5] <http://www.accton.com/NewsPage.asp?sno=79>
- [6] <http://www.networkworld.com/article/2226122/cisco-subnet/clos-networks--what-s-old-is-new-again.html>
- [7] <http://www8.hp.com/us/en/networking/sdn/infrastructure-technologies.html>
- [8] <http://www.hwsz.hu/hirek/51252/cisco-aci-insieme-nexus-switch-sdn.html>