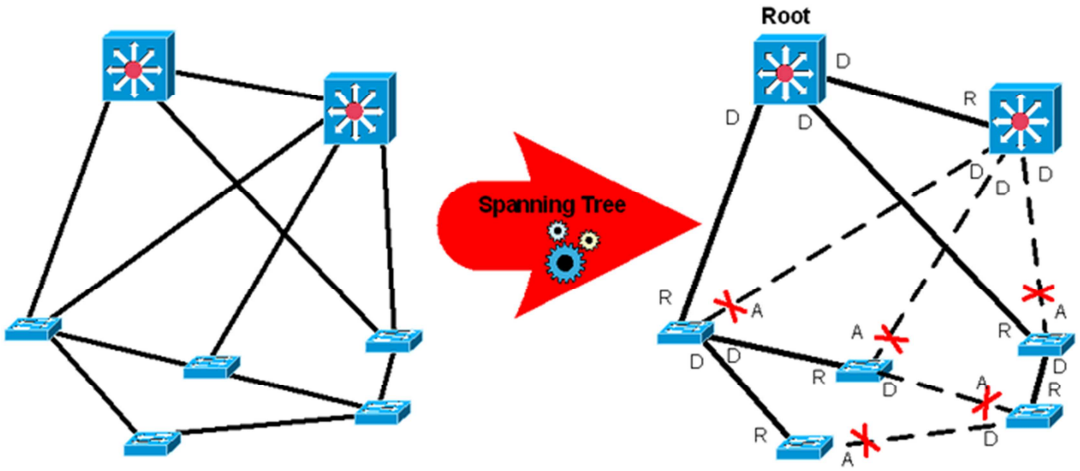
Spanning Tree Protocol

A Spanning Tree Protocol működését javító megoldások

A Spanning Tree Protocol (a továbbiakban STP) célja, hogy a transzparens bridging alapján működő switch hálózatokban a súlyos üzemzavarokat okozó hurkokat biztonsággal észrevegye és kiküszöbölje. Másképpen –pozitívabb attitűddel- fogalmazva a STP lehetővé teszi számunkra redundáns, szükség esetén automatikusan üzembe lépő (hot standby) kapcsolatok fenntartását a campus hálózatunkban, amelyek egyébként fizikailag hurkokként vannak jelen a topgráfiában. A STP tehát hasznos dolog, azonban elég sok szempontból túlhaladott, és így az eredeti formájában részint nem elégíti ki a mai hálózatokkal szemben támasztott kovergencia-sebességi, skálázhatósági és biztonsági elvárásokat. A STP-nek éppen ezért újabb, szabványos és nem szabványos változatait is kifejlesztették (Multiple Spanning Tree, Per VLAN Rapid Spanning Tree), továbbá sok, a konvergenciát és az üzembiztonságot javító technikát fejlesztettek ki. Ezeket a megoldásoka tekintjük át ebben az alfejezetben.

Egy kis STP gyorstalpaló

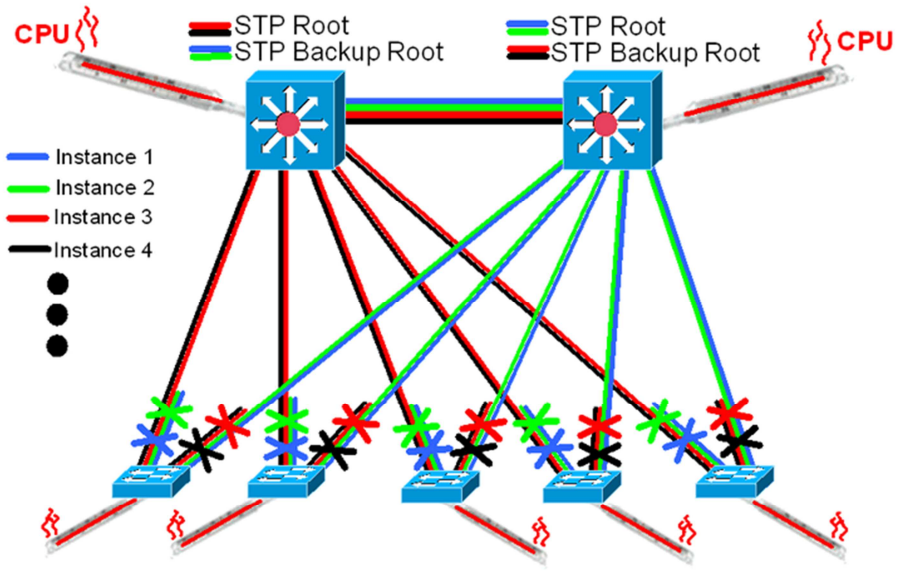
A STP célja tehát a hurokmentes topológia kialakítása, másfelől pedig szakadás esetén a redundáns tartalék kapcsolat mielőbbi felélesztése. A STP domain-ben levő kapcsolók ezért mihamarabb egy hurokmentes fastruktúrát igyekeznek kialakítani megfelelő portjaik blokkolásával, amelynek kiinduló pontjában a Root switch helyezkedik el. A portok adattovábbítási szempontból lehetnek blocking (BLK, nincs adattovábbítás) vagy forwarding (FWD, továbbít kereteket) állapotúak. A portok konvergnes állapotban STP szerepük szerint Root (FWD, a Root felé néző port), Designated (FWD, nem a Root felé néző port), Aternate (BLK) vagy annak speciális változata: a Backup (BLK) port. A portok szerepét mutatja az 1. ábra. Konvergens állapotban a Root switch periodikusan ún. STP BPDU-kat (Bridge Protocol Data Unit) küld, amelyet a többi switch relay-z tovább. A topológiaváltozást a BPDU-k megváltozása jelzi, amelynek hatására aktivizálódik a STP a domainben, és megindul az új topológia kialakítása.



1. ábra: A Spanning Tree Protocol (STP) működése

Per VLAN STP vagy Multiple STP?

A Cisco switch eszközökön jóideje alapértelmezetten a STP VLAN-onként külön példányt futtató PVSTP+ változata működik; az installált rendszerek nagy részében így ezt látjuk. Amikor rengeteg (többszáz) VLAN-unk van, akkor a fizikai topológia és a konvergencia-elvárások ismeretében átgondolandó, hogy szükséges-e ténylegesen minden VLAN-ban külön STP-t futtatni, amely sok VLAN használata mellett CPU igényes feladat. A 2. ábrán látható hálózatban terhelésmegoszást valósítunk meg úgy, hogy a kék és a zöld VLAN STP Root-ja a jobb oldali aggregációs switch, a fekete és a piros VLAN-é pedig a bal oldali. A színes x-ek jelzik az adott access-switch trunkportján az STP blokkoltsági állapotot. Az ábrán rajztechnikai okból csak négy VLAN-t ábrázoltam, és a kérdésfelvetés természetesen sokkal több (százas nagyságrendű) VLAN használata mellett indokolt.

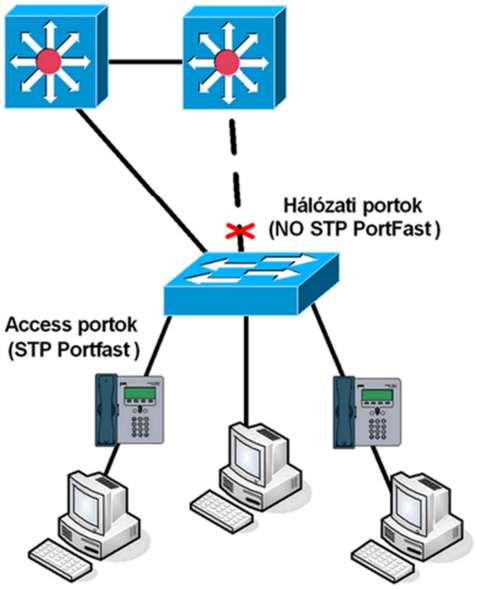


2. ábra:Per VLAN vagy Multiple STP?

Könnyű belátni, hogy még ebben a terhelés-megosztással működő konfigurációban is mindenkor legfeljebb kétféle STP topológia alakulhat ki, így bőven elegendő lehet a Multiple STP használata két STP instance-szal (példánnyal).

Spanning Tree Portfast

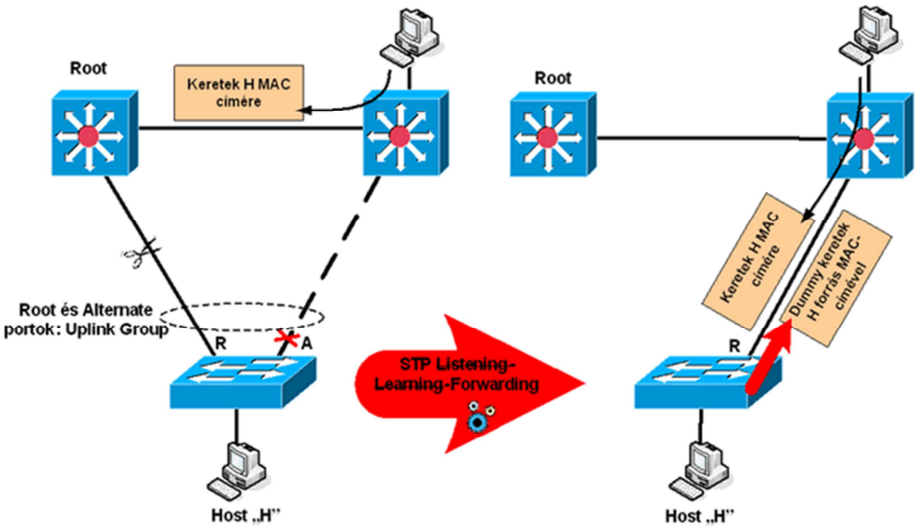
A STP-t futtató switch portok feléledésük (Link Present) után alapértelmezetten a Listening és Learning állapotokon mennek át, mielőtt Forwarding (esetleg Blocking) állapotba jutnának, amely 30-40 másodpercig is eltarthat. A korszerű alkalmazások (és a mai felhasználók) ennél hamarabb várják el a konnektivitást, ezért azokon a portokon, ahol tudjuk, hogy nem az STP domain-ben résztvevő hálózati berendezés, hanem felhasználó fog csatlakozni, alkalmazzuk a STP PortFast működést, amely átugorja a Listening-Learning állapotokat, és azonnal Forwarding működést vesz fel amellett, hogy továbbra is része marad az STP domain-nek. Ha egy így konfigurált porton mégis STP-eszközt csatlakoztat valaki, az komoly üzemzavart okozhat, amelyre a megfelelő védelmi megoldást a későbbiekben ismertetjük (BPDU Guard).



3. ábra: Az STP PortFast használatának helye

STP UplinkFast

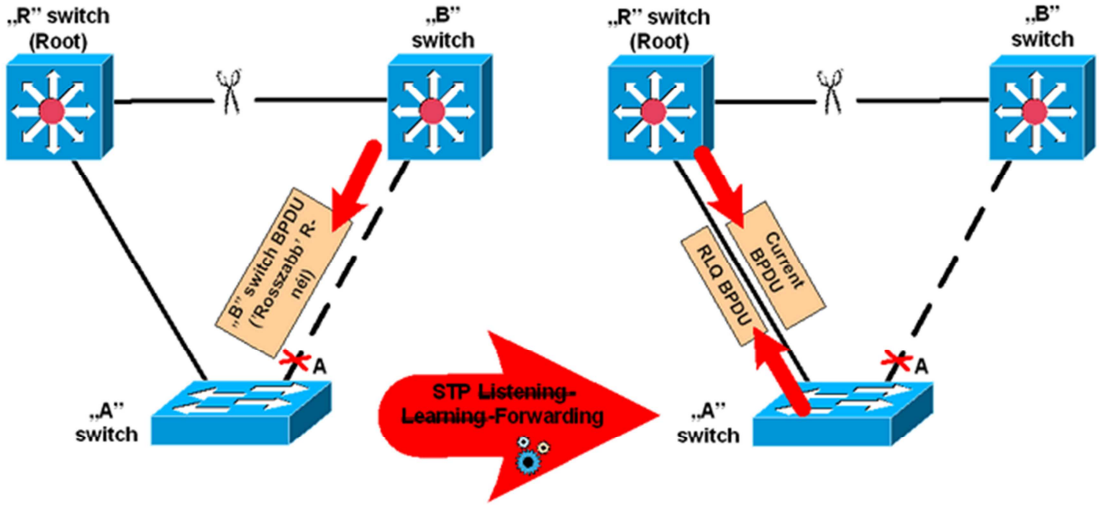
A STP UplinkFast az azt működtető berendezésben a switch-switch kapcsolatokon a közvetlenül csatlakozó link hibájából eredő topológiaváltás konvergenciaidejét gyorsítja. A switch ilyenkor az Alternate portját (ha több van, akkor azok küzül a „legjobbikat") a Listening-Learning állapotok átugrásával azonnal Forwarding állapotba hozza. A STP UplinkFast módon működő switch a szomszédos switchek kapcsolótábláinak megfelelő bejegyzéseit a rá közvetlenül csatlakozó hostok MAC-címével (mint forráscímmel) kiküldött ún. dummy keretek kiküldésével állítják át az új irányra, ahogy ezt a 4. ábra szemlélteti.



4. ábra: A STP UplinkFast működése

STP BackboneFast

Ez szigorúan Cisco proprietary technika, amely csak akkor alkalmazható, ha az STP domain összes tagján működtetjük. A célja hasonló az előbbihez, ám abban az esetben gyorsítja az átállást az Alternate kapcsolatra, amikor nem közvetlenül csatlakozó szegmens hibája (Indirect Link Failure) a topológiaváltás oka. A switch a topológiaváltásról a valamelyik Alternate portján érkező megváltozott BPDU vételéből értesül, amelynek hatására RLQ (Root Link Query) BPDU-kat küld ki a többi non-Designated (Root, Alternate, Backup) portján keresztül, amellyel megkérdezi szomszédjait, hogy ők kit ismernek Root-ként. A válaszokból eldönti, hogy egyáltalán volt-e ténylegesen topológiaváltozás, és aszerint hozza FWD állapotba Alternate portját a Listening-Learning állapotok átugrásával, ahogyan ezt az 5. ábra szemlélteti. Úgy is fogalmazhatunk, hogy itt egy egyszerű Layer2 „routing protokoll” gyorsítja meg az egyébként passzív figyelésen alapuló STP konvergenciáját akár 20 másodperccel.



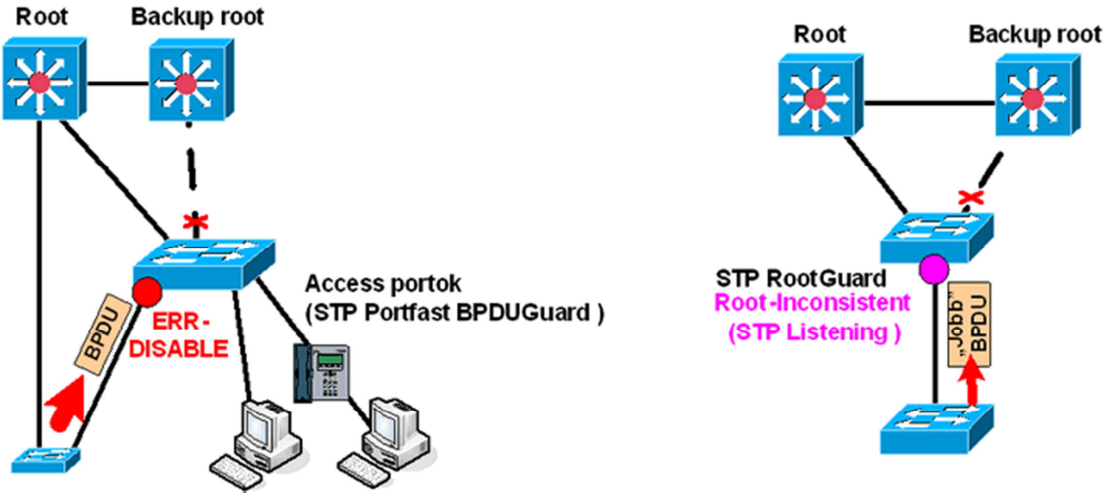
5. ábra: A STP BackboneFast működése

A STP Portfast BPDUGuard és RootGuard

Ezek a funkciók a már említett STP PortFast-ra konfigurált portok sérülékenységét küszöbölik ki.

Amennyiben a BPDUGuard-ra konfigurált porton STP BPDU érkezik, a switch azonnal tiltja a portot (ErrorDisable), amellyel kiküszöböli az STP domain nem kívánt –hibás-topológiaváltását. A port az ErrDisable állapot alatt semmilyen működésben nem vesz részt.

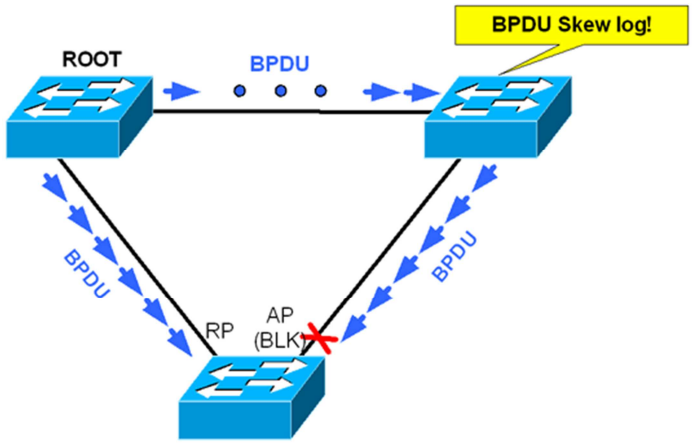
A RootGuard funkciót csak olyan BPDU érkezése váltja ki, amely ténylegesen topológiaváltást okozna, amely eseményre a switch RootInconsistent állapotba helyezi a portot - ez voltaképpen STP Listening állapotnak felel meg. Amennyiben a BPDU-k elmaradnak, a port visszavált Forwarding állapotba (eltérően a BPDUGuard-tól). A két funkció működését szemlélteti a 6. ábra.



6. ábra:Az STP PortFast BPDUGuard és RootGuard működése

Az STP BPDU Skew Detection

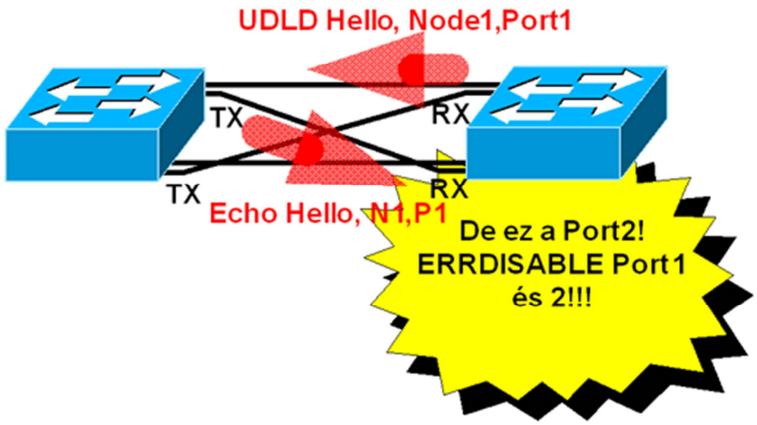
Ez a funkció figyeli a STP BPDU-k érkezési gyakoriságát, és amennyiben rendellenes késleltetést tapasztal, egy syslog üzenetet generál és küld (7. ábra). Egyéb beavatkozást nem tesz, csak informatív jellegű.



7. ábra:A STP BPDU Skew Detection

UniDirectional Link Detection (UDLD)

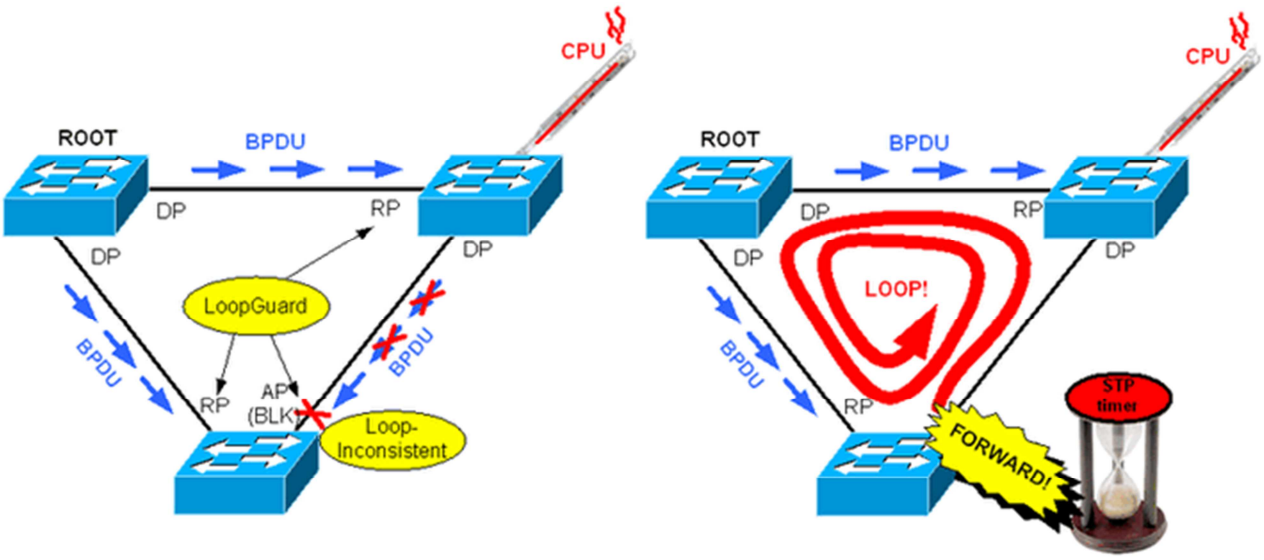
Az UDLD leginkább a fizikai félrekábelezések következtében fellépő STP problémák ellen véd, tipikusan optikai portokon alkalmazzuk. Az UDLD biztosítja, hogy a switch a portot kizárólag abban az esetben használja, ha az adási és vételi ág is a megfelelő fizikai csatlakozón végződik. Az UDLD Hello üzenetekben benne vannak az eszköz- és portazonosítók, így a vissza echo-zott Hello üzenetünk azonnal feltárja a hibát, amelyre a port tiltásával (ErrDisable állapotba helyezés) reagál a switch. Ezt mutatja a 8. ábra.



8. ábra: Az UDLD működése

STP LoopGuard

Ha egy switch valamely portján a szomszédos switchtől egyszer csak nem kap STP BPDU-kat, akkor azt topológiaváltozásként kezeli, és a port Forwarding állapotba kerülhet, és ezzel nem kívánt hurkot képezhet abban az esetben, ha a BPDU-k elmaradását valójában nem valódi topológiaváltozás, hanem egyéb, pl. a szomszédos switch szoftverhibája, vagy magas CPU terheltsége okozza. A LoopGuard-ot switchek közötti Alternate vagy Root állapotú pont-pont kapcsolatokon célszerű bekapcsolni (ahol pontosan tudjuk, hogy egyetlen switch lesz a szomszéd és senki más). Hatása az, hogy mindössze attól az eseménytől, hogy elmaradnak a BPDU-k azon a kapcsolaton (és pl. a port nem veszti el link-jét, vagy más jele nincs az esetleges topológiaváltásnak) nem hozza Forwarding állapotba a portot, hanem az LoopInconsistent állapotot vesz fel, amelyből a BPDU-k újabb megjelenése automatikusan kimozdítja a portot. A LoopGuard funkciót csakis a topológia teljeskörű ismeretében, körültekintéssel alkalmazzuk! Működését szemlélteti a 9. ábra bal oldala, a jobb oldal pedig azt mutatja be, mi történne, ha nem működne.



9. ábra:Az STP LoopGuard

Az UDLD és a LoopGuard együttes használata

A két funkció első olvasatra hasonló szolgáltatásokat kínál, ezért joggal tesszük fel a kérdést: érdemes-e UDLD-t és LoopGuard-ot egyidejűleg alkalmazni egy porton? A válasz igen, és az indoklást 1. Táblázat - leginkább az utolsó két sora - adja meg. A legfőbb különbség, hogy míg az UDLD a fizikai kábelezés hibái ellen véd, addig a LoopGuard a szoftver jellegű STP hibák okozta hamis topológiaváltásokat előzi meg. Másképpen fogalmazva van olyan hiba, amit az UDLD nem vesz észre, a LoopGuard viszont kiküszöböl és viszont.

Funkcionalitás	LoopGuard	UDLD
Konfigurálás helye	Porton	Porton
Hatása hol érvényesül	VLAN-onként	Porton
Beavatkozás nélkül rendbejön-e	Igen, ha általánosan alkalmazzuk	Igen, ha általánosan alkalmazzuk
Véd-e a BPDU elmaradás okozta STP hibák ellen	Igen	Nem
Véd-e a félrekábelezés ellen	Nem	Igen

1. Táblázat :A STP LoopGuard és az UDLD összehasonlítása

VLAN Trunking Protocol (VTP) meggondolások

A VTP a VLAN-ok adminisztrációját könnyíti meg kiterjedt, sok switchből álló hálózatban azzal, hogy a VLAN információkat leíró VLAN Database-t replikálja a switchek között. Ezzel egy új VLAN felvételekor vagy törlésekor nem kell az összes switchben külön-külön konfigurálni a változást; elegendő azt a VTP szerveren megtenni, és a változás tovaterjed.

A VTP-nek jelenleg három változata van.

Az első kettő között nincsenek jelentős funkcionális különbségek, a legfőbb talán a Token Ring támogatottság megjelenése volt, így önmagában a VTP v1-ről v2-re áttérés nemigen hoz fejlődést, nem érdemes meglépni. Érdemes viszont megvizsgálni switcheink VTP állapotát, hiszen sokszor tapasztaljuk, hogy vannak itt-ott VTP transzparens berendezések a hálózatokban, vagy mindenki VTP szerver, de láttunk már eltérő VTP domain névvel konfigurált eszközöket is - azaz ahol a VTP domain nem volt folytonos. Célszerű ezeket a hibákat kifésülni, átgondolni, hogy mely switchek legyenek VTP szerverek és általánosan rendbe tenni a VTP domainünket.

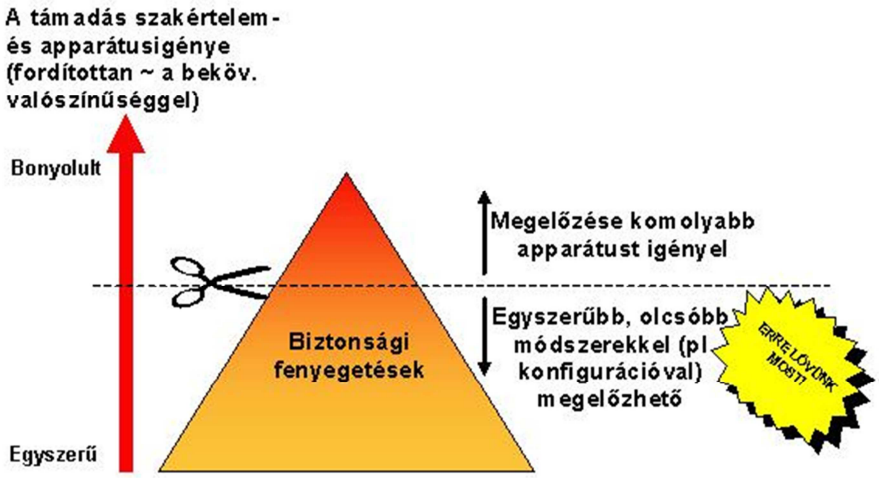
A VTP v3 jelentős újdonságokat hozott, így bizonyos esetekben érdemes elgondolkodni a bevezetéséről. Ilyen eset lehet például az, amikor Multiple Spanning Tree protocol-t használunk, ugyanis a VTP v3 a VLAN adatbázis mellett az MSTP adatbázist is képes replikálni. (MSTP adatbázis az, amelyben a VLAN-ok és a STP instance-ok összerendelése definiált.) A VTP v3 további lényeges tulajdonságai:

- Centralizált, redundáns VTP adabázis-kezelés
- Hidden/secret VTP passwords
- Extended VLAN range propagation (1000 feletti VLAN ID)
- Primary/Secondary Servers (PS/SS): A PS runtime állapot, bármelyik SS lehet PS
- Alapértelmezetten minden switch SS
- VTP-vel bármilyen adatbázist propagálhatunk (Pl. MST database)

Campus LAN biztonsági fejlesztések

A LAN hálózatokban előforduló biztonsági jellegű incidensek meglehetősen sokfélék. Azt biztosan kijelenthetjük, hogy a bonyolult, jelentős szakértelmet vagy apparátust igénylő incidensből sokkal kevesebb fordul elő, mint azokból, amelyek egyszerűen kivitelezhetők. Hozzáteszem még, hogy a biztonsági incidensek nagy része nem is szándékos, előre eltervezett, rosszindulatú cselekmény, hanem véletlen, nem szándékos változtatás következménye (pl félrekonfigurált számítógép). Ilyen eset volt, amikor egy ügyfél rendszergazdája egy virtuális gép TCP/IP beállításait rosszul konfigurálta, és az egy, a szerverek számára fenntartott címtartomány öles részét a magáénak tekintette. Ennek a következménye az lett, hogy rengeteg, üzleti szempontból fontos szolgáltatás szerverének címére küldött forgalom hozzá került az igazi szerverek helyett, és ezek a szolgáltatások a hiba behatárolásáig és elhárításáig (mintegy egy óra időtartamig) nem működtek, amely jelentős presztizs- és anyagi kárt okozott a vállalatnak. Ez a hiba például abba a csoportba sorolható, amelynek előidézéséhez sem különösebb szakértelemre, sem komolyabb apparátusra nincs szükség, bekövetkezési valószínűsége viszonylag magas (hiszen véletlenül is előfordult), ám a következőkben meglátjuk, hogy az ellene való védekezés konfigurálással megoldható, és a kiküszöbölés lehetősége valószínűleg benne van a birtokolt Cisco switchekben.

Az alábbi ábra reprezentálja a biztonsági jellegű hibák megoszlását, az előfordulási valószínűséget a háromszög adott bonyolultsági szintbeli szélessége szimbolizálja. Meghúztunk egy szimbolikus szaggatott vonalat, amely alatt levő fenyegetések elleni védekezést a meglevő Cisco switcheink megfelelő konfigurációjával meg tudunk valósítani. Tapasztalatunk szerint – amelyet az ábra is sugall – a fenyegetettség nagy része megelőzhető így, ráadásul az a része, amelynek előfordulási esélye a legnagyobb. Összegzésképpen azt mondhatjuk tehát, hogy Campus hálózatunkban mindössze az eszközök meglevő képességeinek kihasználásával jelentős biztonsági szint emelkedést érhetünk el. A következőkben ezeket a technikai megoldásokat taglaljuk.

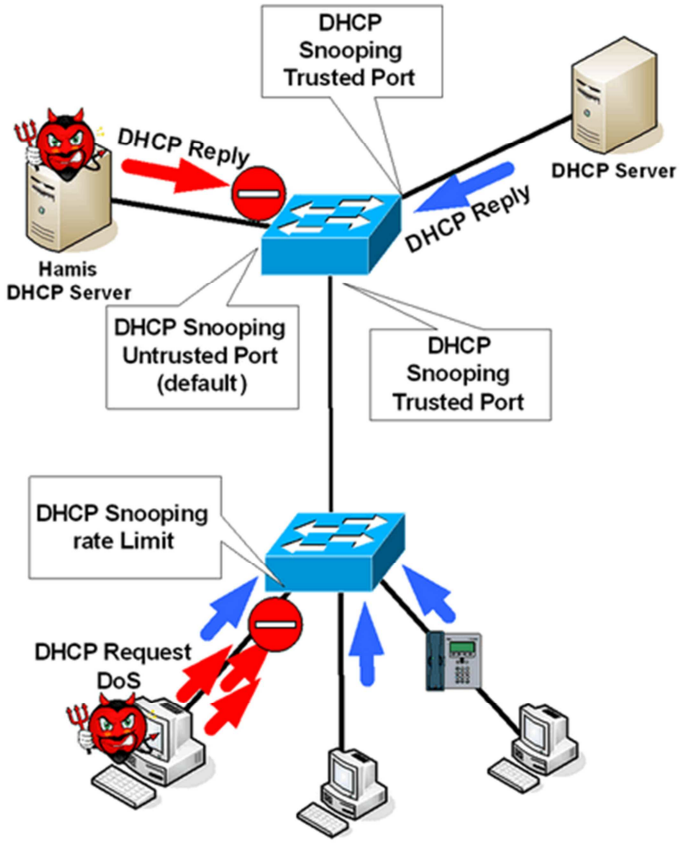


10. ábra: A biztonsági fenyegetettségek megoszlása

Az IP DHCP Snooping

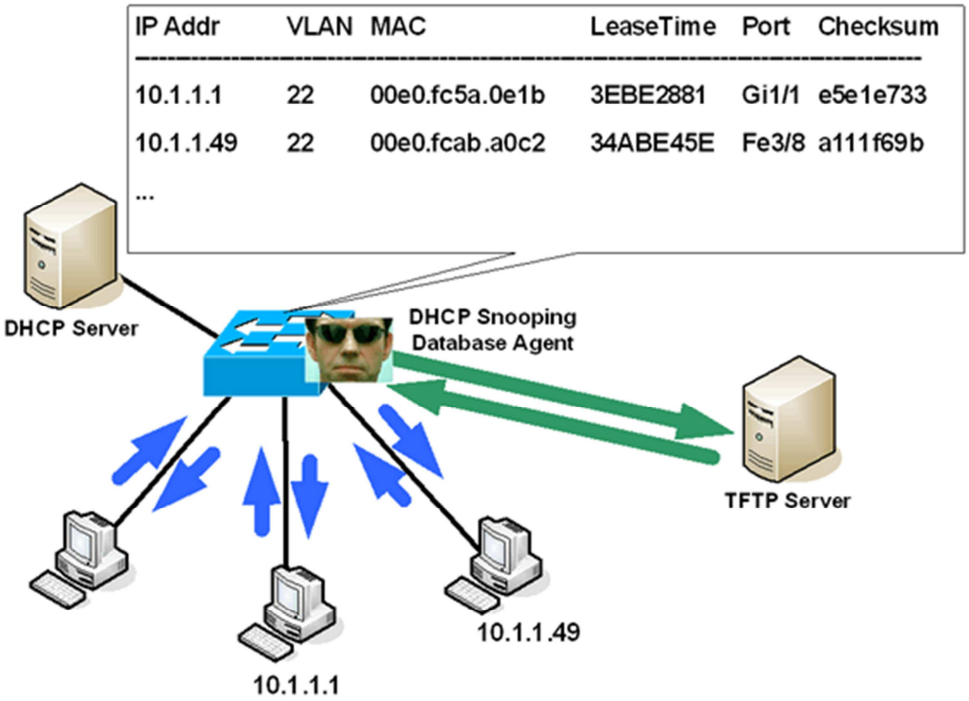
A vállalatok ma már központi TCP/IP menedzsmentet használnak, vagyis DHCP (Dynamic Host Configuration Protocol) protokollon osztják ki az IP-címeket és az egyéb TCP/IP beállításokat (maszk, default gateway IP címe, DNS név, DNS szerver IP címe, stb.). Egy tipikus, viszonylag egyszerű MIM (Man In the Middle) támadás az, amikor a támadó hamis DHCP válasszal default gateway címet ad a kliens gépnek, és magára irányítja a klienstől a lokális hálózatból kifelé irányuló forgalmat. Ezt azzal szokták kombinálni, hogy míg a valódi DHCP szervert rengeteg DHCP kérés küldésével megbénítják (DoS), azalatt a hamis DHCP szerverrel kiszolgálják a kliens gépet. Látjuk tehát, milyen fontos a DHCP kommunikáció megfelelő szintű ellenőrzése a hálózatban.

A DHCP Snooping (Snooping = kémkedés, szaglászás) funkció bekapcsolásával a Layer2 eszköz (switch) a keretekben utazó DHCP kommunikációt felismeri és értelmezi. DHCP Snooping szempontból léteznek bizalmat élvező (Trusted) és azt nem élvező (Untrusted) portok; alapértelmezetten minden port Untrusted. Az eszköz egyrészt csak a megbízhatóként konfigurált portok felől enged DHCP választ a kliensek felé, másrészt a DHCP kommunikáció elemzése alapján felépít egy adatbázist, amelyben nyilvántartja többek között azt, hogy a portokon csatlakozó kliensek milyen IP címmel, milyen MAC címmel rendelkeznek, mennyi időre kapták az IP címet, harmadrészt pedig korlátozni tudjuk a portokon beérkező DHCP kérések mennyiségét a DoS támadások megelőzése érdekében. Ezt mutatja be a 11. ábra.



11. ábra: Az IP DHCP Snooping működése

A már említett, dinamikusan épülő adatbázist DHCP Snooping Binding Database-nek (DHCPSBDB) nevezzük, és a switch memóriájában van. Ha a switch újraindul, akkor elvész, ezért konfigurálhatunk egy ún. DHCPSBD Agent-et, amely minden változtatás esetén TFTP szerverre menti az adatbázist, újraindításkor pedig feltölti azt a switch memóriájába (12. ábra).

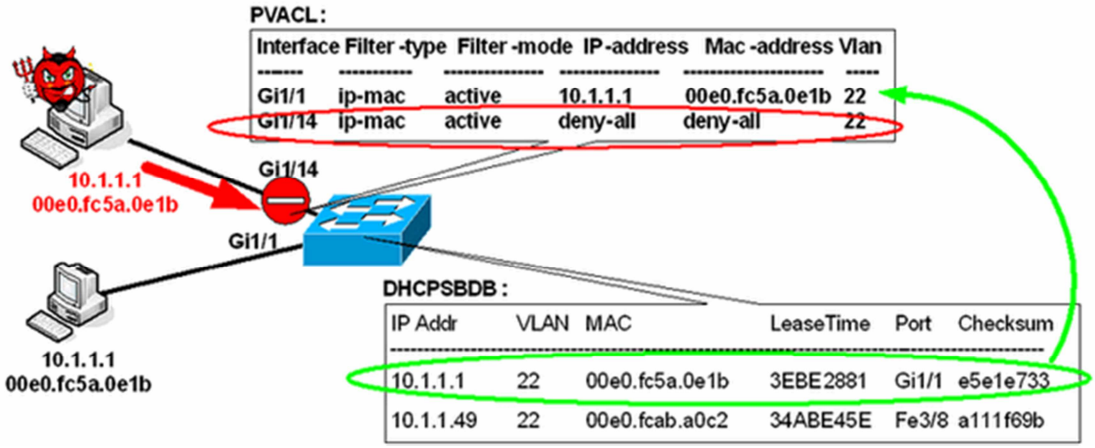


12. ábra: A DHCPSBDB agent

Az adatbázis – ahogy a következőkben látni fogjuk – alapja lesz további értékes biztonsági funkciók alkalmazásának.

Az IP Source Guard (IPSG)

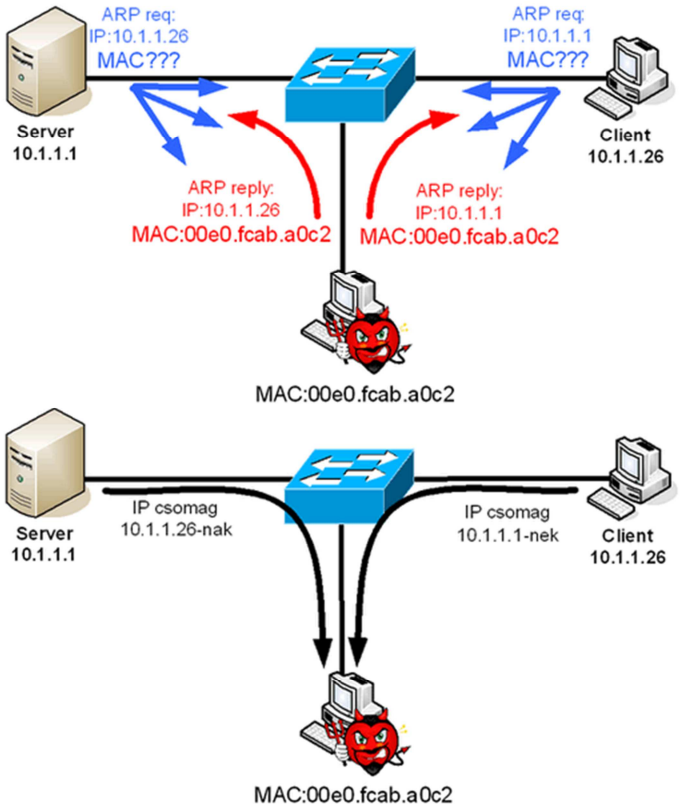
Ez a funkció a DHCP Snoopingra épül, untrusted portokon működtethető. Hatására a portokon kizárólag a DHCPSBDB-nek megfelelő IP- és MAC-forráscímmel feladott csomagokat enged be. Amikor a port feléled, és nincs mögötte érvényes TCP/IP stack-kel rendelkező host, akkor csak a DHCP forgalmat engedi, majd a bizalmat élvező DHCP szervertől kapott paraméterekkel feltölti az adatbázis. Ekkor a portokra ún. Per VLAN Access List-bejegyzések (PVACL) kerülnek, de lehet adminisztratív úton statikus bejegyzéseket is konfigurálni. Az IPSG használatánál –különösen ha sok host csatlakozik – a PVACL-ek miatt érdemes odafigyelni a switch RAM használatára (pl. TCAM). Az IPSG működését szemlélteti a 13. ábra.



13. ábra: Az IP Source Guard működése

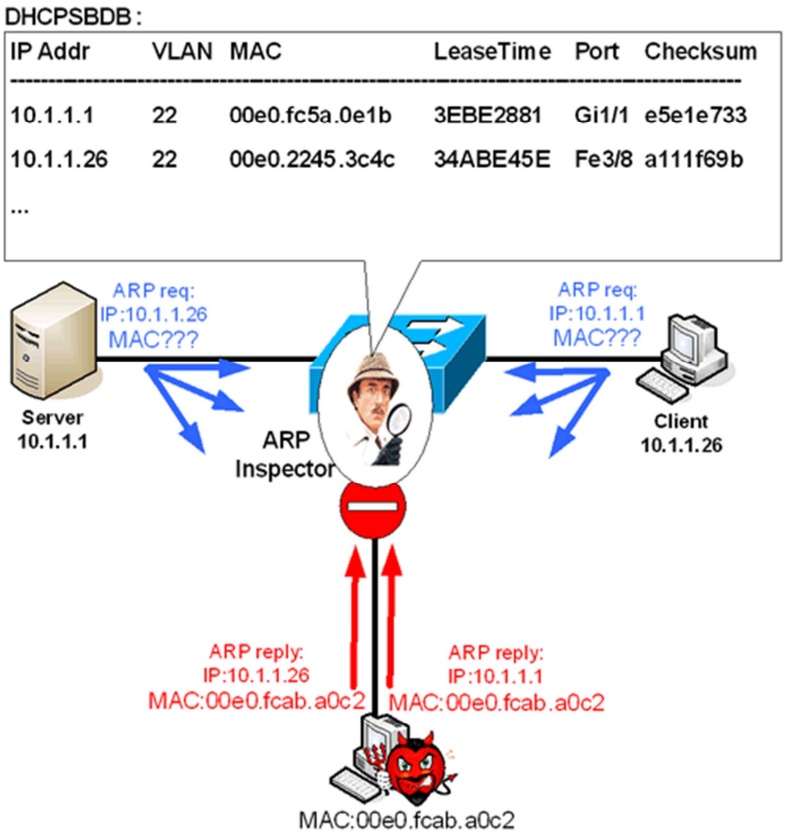
A Dynamic ARP Inspection (DAI)

A DAI működéséhez előbb ismerjük meg az egyik legegyszerűbb MIM támadási formát, az ARP Poisoning-ot! A támadó két fél közötti kommunikációt saját magán akarja átfolyatni, ehhez mindkét félnek a másik MAC-címét tudakoló ARP-kérésére olyan választ ad, amelyben a saját MAC-címe van. A két fél ezután Layer2 szinten a támadó MAC-címére küldi a kereteket, és már kész is a MIM/ARP Poisoning támadás (14. ábra).



14. ábra: Az ARP Poisoning

A DAI éppen az ilyen ARP-tábla hamisításon alapuló támadásokat (amelybe a fejezet elején leírt nem szándékosan előidézett incidens is sorolható) küszöböli ki; alapja a DHCP Snooping adatbázis. Lényege az, hogy az ARP-válaszokat a DHCPSBDB alapján értékeli, és amennyiben az alapján érvénytelen IP-MAC összerendelést lát egy ARP-válaszban, azt eldobja (15. ábra). Mivel mindenhol vannak statikus IP címekkel konfigurált hostok, ezért lehetőség van statikus ARP ACL-ek (Access List) felvételére, amelyben ezeket fel tudjuk sorolni. Fontos tudni, hogy a DAI (pontosabban az ARP feldolgozás) nem hardver, hanem CPU erőforrást köt le, így célszerű ezzel együtt az ARP forgalmat is korlátozni egyéb beállításokkal DoS támadások megelőzése céljából.



15. ábra: A Dynamic Arp Inspection működése

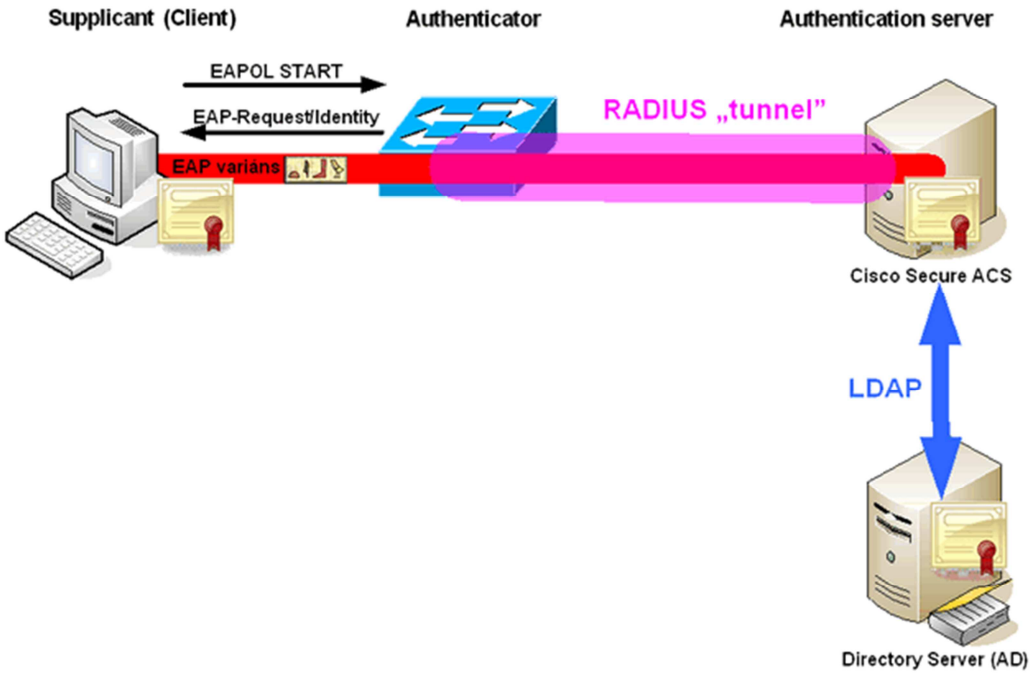
Az IEEE 802.1x (dot1x) azonosítási keretrendszer

A keretrendszer célja, hogy a hálózati és informatikai erőforrásokhoz való hozzáférést közvetlenül a hozzáférési ponton szabályozza – vagyis a switch porton.

Az architektúra elemei a Supplicant („Kérvényező”, vagyis a dot1x kliens, amely a felhasználó gépén fut), az Authenticator (a switch), és az Authentication Server (az azonosításhoz szükséges információkat szolgáltató AAA szerver).

Az AAA szerver legtöbbször RADIUS protokollon kommunikál az Authenticatorral, és nem mindig ő tárolja a felhasználói adatbázis, gyakran kérdez tovább LDAP protokollon a vállalati címtárból (Microsoft Active Directory vagy egyéb).

A felhasználó gépén futó Supplicant először a switchnek küld egy EAPOL-START (Extensible Authentication Protocol Over LAN) csomagot, amire az – szintén EAP-ban – az azonosítását kéri. A továbbiakban a switch közvetítő szerepet játszik az AAA szerver és a kliens között; az end-to-end EAP azonosítás már köztük folyik, és a switch csak RADIUS üzenetekbe csomagolja, „tunnelezi” az EAP variánson folytatott kliens-szerver kommunikációt. Ez a kommunikáció jellemzően titkosított, gyakran tanúsítványokkal PKI alapon védett, amely függ az alkalmazott EAP-variánstól. Sikeres azonosítás esetén az AAA szerver egy RADIUS ACCESS-ACCEPT üzenetben értesíti a switchet arról, hogy a megfelelő VLAN-hoz való hozzáférést megnyithatja a portján. Az architektúrát és a működést szemlélteti a 16. ábra.



16. ábra: A dot1x keretrendszer működése

Az előadás elején vázolt projekt anyagi kereteibe egy egyszerűbb, külső eszközöket (pl RSA tokeneket vagy Generic Token Card-ot) nem igénylő dot1x bevezetés beleférhet, amellyel valóban jelentősen megnövelhetjük a vállalati informatika biztonsági szintjét. A későbbi, forrásokban gazdagabb időkben a pl. directoryból történő (domain alapú) azonosítást migrálhatjuk vagy kiegészíthetjük robusztusabb és drágább eszközökkel, vagy a dot1x-re épülő Cisco NAC (Network Admission Control) megoldással.

Összefoglalás

A cikk olyan, kisösszegű beruházást igénylő fejlesztési lehetőségeket mutat be, amelyek a vállalati hálózat egy specifikus részén: a Campus hálózatban hajthatók végre. Hatékonyság-, biztonság- és rendelkezésre-állás növelő hatásuk a vállalat alaptevékenységére is számszerűsíthető előnyöket eredményez. A bemutatott megoldásokban a meglevő erőforrásokból a szakértelem dolgoztatásával igyekszünk kihozni a legtöbbet, ezzel megtámogatva és serkentve a cég valódi üzleti tevékenységét. Cégünk a vázolt fejlesztéseken kívül a hálózat más részein is felméri a meglevő eszközpark lehetőségeit, az értelmesen bevezethető funkciókat mérlegeli, és implementálja is azokat.