# Fejezet 3: VLAN-ok

# VLAN-ok

## Bevezetés

A hálózati teljesítmény kulcsfontosságú tényezője egy szervezet termelékenységének. A hálózati teljesítmény javítására használt technológiák egyike a nagyméretű szórási tartományok kisebbekre történő szétválasztása. Tervezésükből fakadóan a forgalomirányítók az interfészeiken blokkolják a szórásos forgalmat. Ugyanakkor a forgalomirányítók általában korlátozott számú LAN interfésszel rendelkeznek. A forgalomirányítók elsődleges feladata, hogy hálózatok között vigyenek át információt, és nem pedig hálózati hozzáférést biztosítani végberendezések számára.

Egy LAN-hoz a hozzáférést biztosítani normál esetben egy hozzáférési rétegbeli kapcsoló feladata. Egy második rétegbeli (Layer 2) kapcsolón virtuális helyi hálózatok (VLAN, Virtual Local Area Network) hozhatók létre a szórási tartományok méretének csökkentésére, harmadik rétegbeli (Layer 3) eszközhöz hasonló funkcióval. A hálózatot rendszerint eleve VLAN-ok használatával tervezik meg, ami megkönnyíti, hogy a hálózat kiszolgálja egy szervezet céljait. Bár a VLAN-okat elsősorban kapcsolt helyi hálózatokon belül alkalmazzák, a modern VLAN megvalósítások lehetővé teszik kiterjesztésüket a MAN és WAN hálózatokra is.

Ez a fejezet a VLAN-ok és a VLAN-trönkök konfigurálását, felügyeletét és hibakeresését tárgyalja. Foglalkozik továbbá a VLAN-okat érintő biztonsági szempontokkal és stratégiákkal, valamint a VLAN-ok tervezésének bevált gyakorlataival.

# VLAN-ok

## Bevezetés

**Nyaralóhely**

**Esetleírás**

Bérbeadási szándékkal vásároltunk egy nyaralóházat a tengerparton. A ház mindhárom szintje ugyanolyan elrendezésű. Minden emeleten található egy digitális televízió, amit a bérlők használhatnak.

A helyi internetszolgáltató szabályai szerint egy televíziós csomagon belül csak három csatorna nyújtható. A mi feladatunk eldönteni, hogy milyen televíziós csomagokat kínálunk a vendégeinknek.

* Osszuk fel az osztályt háromfős csoportokra!
* Válasszunk három különböző csatornát egy előfizetői csomag összeállításához a bérházunk minden emelete számára!
* Töltsük ki a feladathoz tartozó PDF-et!
* Osszuk meg a csoport véleményét tükröző válaszokat az osztállyal!

[Csoportos feladat - Vacation Station Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/3.0.1.2%20Vacation%20Station%20Instructions.pdf)

# VLAN szegmentálás

## VLAN-ok áttekintése

A VLAN-ok szegmentációt és szervezeti rugalmasságot biztosítanak egy kapcsolt hálózaton belül. A VLAN-ok lehetőséget nyújtanak egy LAN-on belül az eszközök csoportosítására. Az eszközök egy VLAN-on belül úgy kommunikálnak egymással, mintha ugyanarra a vezetékre csatlakoznának. A VLAN-ok a fizikai kapcsolatok helyett logikai kapcsolatokra épülnek.

A VLAN-ok lehetővé teszik egy rendszergazda számára, hogy olyan szempontok alapján szegmentálja a hálózatot, mint például a gépek szerepe, egy projektcsapat vagy mondjuk egy alkalmazás, mindezt függetlenül a felhasználó vagy a készülék fizikai elhelyezkedésétől. Egy VLAN-on belül az eszközök úgy viselkednek, mintha a saját független hálózatukon lennének, még akkor is, ha más VLAN-okkal együtt ugyanazt a közös infrastruktúrát használják. Bármely kapcsolóport tartozhat VLAN-hoz, és az egyedi címzéses (unicast), a szórásos (broadcast) és a csoportcímzéses (multicast) csomagok is kizárólag a csomagok forrásához tartozó VLAN-on belüli végberendezésekhez lesznek továbbítva. Valamennyi VLAN egy elkülönített logikai hálózatnak tekintendő, és az adott VLAN-hoz nem tartozó állomásoknak címzett csomagokat olyan eszközön keresztül kell továbbítaniuk, amely a forgalomirányítást (routing) is támogatja.

Egy VLAN akár több fizikai LAN-szegmensre kiterjedő szórási tartományt is alkothat. A VLAN-ok javítják a hálózat teljesítményét, mivel a nagyméretű szórási tartományokat kisebbekre osztják fel. Ha egy eszköz egy VLAN-ban elküld egy szórásos Ethernet keretet, akkor azt a VLAN valamennyi eszköze megkapja, de más VLAN-okon lévő eszközök már nem.

A VLAN-ok lehetővé teszik, hogy a felhasználók adott csoportjaihoz illeszkedő hozzáférési- és biztonsági házirendeket valósítsunk meg. Minden kapcsolóport csak egyetlen VLAN-hoz tartozhat (kivéve egy olyan portot, amely egy IP-telefonhoz vagy egy másik kapcsolóhoz csatlakozik).

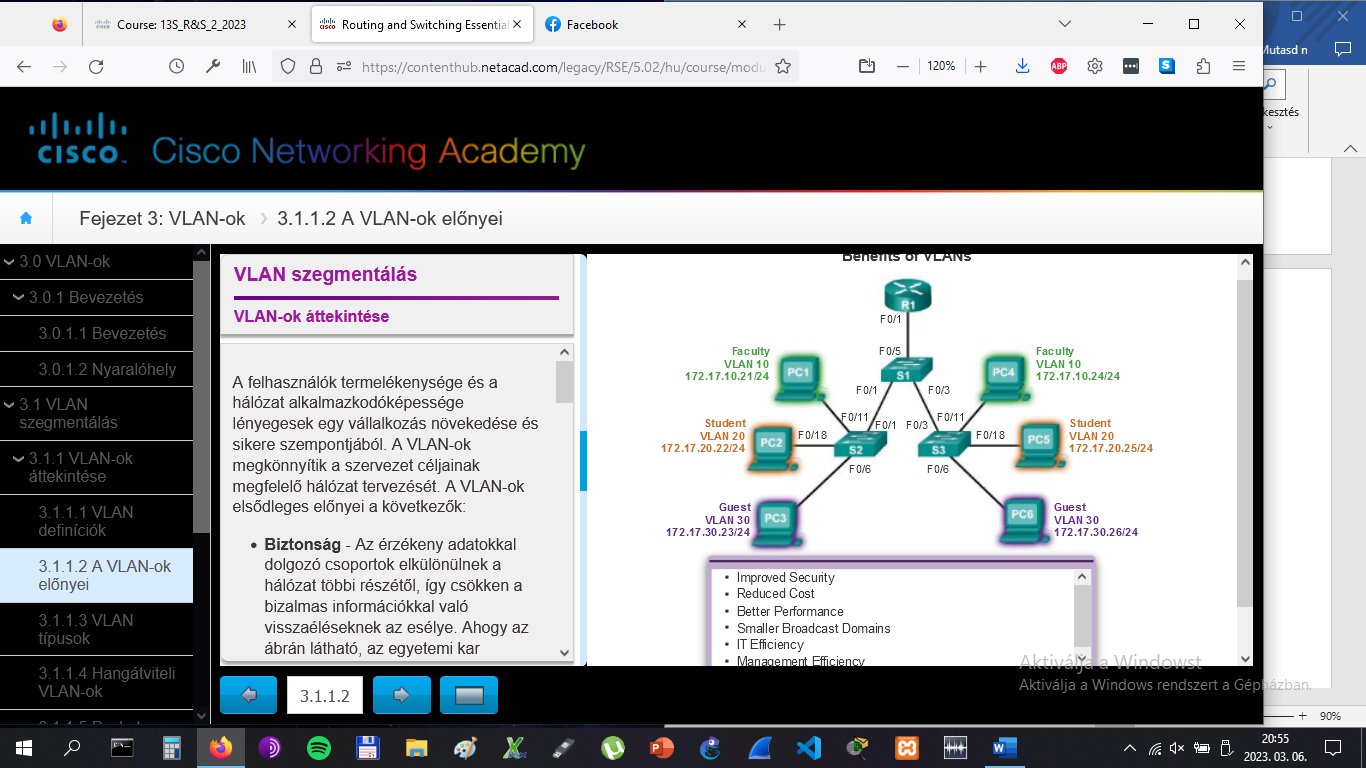
# VLAN szegmentálás

## VLAN-ok áttekintése

A felhasználók termelékenysége és a hálózat alkalmazkodóképessége lényegesek egy vállalkozás növekedése és sikere szempontjából. A VLAN-ok megkönnyítik a szervezet céljainak megfelelő hálózat tervezését. A VLAN-ok elsődleges előnyei a következők:

* **Biztonság** - Az érzékeny adatokkal dolgozó csoportok elkülönülnek a hálózat többi részétől, így csökken a bizalmas információkkal való visszaéléseknek az esélye. Ahogy az ábrán látható, az egyetemi kar (Faculty) számítógépei a 10-es VLAN-ba tartoznak, teljesen elkülönítve a hallgatói (Student) és vendég (Guest) adatforgalomtól.
* **Költségcsökkentés** - A költségek megtakarítása annak az eredménye, hogy csökken a költséges hálózati felújítások szükségessége, valamint sokkal hatékonyabbá válik a meglévő sávszélesség és a gerinckapcsolatok kihasználtsága.
* **Jobb teljesítmény** - Egységes második rétegbeli hálózatok logikai munkacsoportokra (szórási tartományokra) történő felosztása csökkenti a szükségtelen hálózati forgalmat és javítja a teljesítményt.
* **Szórási tartományok méretének csökkentése** - Egy hálózat VLAN-okra történő felosztása csökkenti a szórási tartományban lévő eszközök számát. Az ábrán látható hálózatban hat számítógép van, de három szórási tartomány: a kari (Faculty), a hallgatói (Student) és a vendég (Guest) VLAN-ok.
* **IT személyzet hatékonyságának növekedése** - A VLAN-ok könnyebben felügyelhetővé teszik a hálózatot, mivel a hasonló hálózati igényű felhasználók ugyanazt a VLAN-t használják. Amikor egy új kapcsolóról gondoskodunk, akkor minden az adott VLAN-ra már beállított szabály és eljárás érvényre jut, amint a portokat hozzárendeljük. Az IT személyzetnek is egyszerűbb egy VLAN funkciójának a beazonosítása, ha annak egy megfelelő nevet adnak. Az ábrán a könnyebb azonosíthatóságért a VLAN 10 a "Faculty", a VLAN 20 a "Student", a VLAN 30 pedig a "Guest" nevet kapta.
* **Könnyebb projekt- és alkalmazásmenedzsment** - A VLAN-ok vállalati vagy földrajzi követelmények alapján csoportosítanak felhasználókat és hálózati eszközöket. Az elkülönített funkciók egyszerűbbé teszik egy projekt irányítását, vagy a munkát egy speciális alkalmazással. Egy ilyen alkalmazásra lehet példa egy e-learning fejlesztési platform a kar számára.

Egy kapcsolt hálózatban valamennyi VLAN egy IP-alhálózatnak felel meg, ezért VLAN tervezéskor a hierarchikus hálózatcímzési terv megalkotását is tekintetbe kell venni. A hierarchikus hálózatcímzés annyit jelent, hogy a hálózati szegmensekhez vagy VLAN-okhoz a hálózat egészét szem előtt tartva, rendezett módon, IP-alhálózatokat rendelünk. Ahogy az ábrán is látható, összefüggő hálózati címblokkokat foglalunk le és konfigurálunk be a hálózat egy meghatározott területén lévő eszközök számára.



# VLAN szegmentálás

## VLAN-ok áttekintése

A modern hálózatokban számos különböző típusú VLAN-t hasznának. Egyes VLAN típusok a forgalmi osztályok alapján vannak meghatározva. Más típusú VLAN-ok meghatározása az általuk biztosított funkció alapján történik.

**Adat VLAN**

Az adat VLAN a felhasználók által generált forgalom továbbítására beállított VLAN. Egy hangot vagy felügyeleti forgalmat továbbító VLAN nem lehetne része egy adat VLAN-nak. Általános gyakorlat a hang- és a felügyeleti forgalom elválasztása az adatforgalomtól. Az adat VLAN-t néha felhasználói VLAN-nak is nevezik. Az adat VLAN-okat a hálózat felhasználói- vagy eszközcsoportok alapján történő szétválasztására használjuk.

**Alapértelmezett VLAN**

Egy kapcsoló alapértelmezett konfigurációval történő kezdeti elindítása után minden kapcsolóport az alapértelmezett VLAN részévé válik. Az alapértelmezett VLAN-ba tartozó kapcsolóportok ugyanannak a szórási tartománynak a részei. Ez lehetővé teszi, hogy a kapcsoló egy portjára csatlakozó eszköz képes legyen kommunikálni a kapcsoló más portjaira csatlakoztatott eszközökkel. A Cisco kapcsolók esetében VLAN 1 az alapértelmezett VLAN. Az ábrán a **show vlan brief** utasítás kimenete látható egy alapértelmezett konfigurációt futtató kapcsolón. Figyeljük meg, hogy az alapbeállítások szerint valamennyi port VLAN 1-be lett besorolva!

A VLAN 1 ugyanazokkal a tulajdonságokkal rendelkezik, mint bármely más VLAN, azzal a kivétellel, hogy nem lehet átnevezni vagy törölni. Alapértelmezés szerint minden második rétegbeli vezérlőforgalom is VLAN 1-hez van hozzátársítva.

**Natív VLAN**

A natív VLAN-t egy 802.1Q trönk porthoz van hozzárendelve. A trönk portok azok a kapcsolók közötti linkek, amelyek egynél több VLAN forgalmának a továbbítását is lehetővé teszik. Egy 802.1Q trönk port a különböző VLAN-okból érkező forgalmat (címkézett vagy "tagged" forgalom), valamint a nem VLAN-ból származó forgalmat (címkézetlen vagy "untagged" forgalom) egyaránt továbbítja. A 802.1Q trönk port a címkézetlen forgalmat a natív VLAN-ra helyezi, ami alapértelmezés szerint a VLAN 1.

A natív VLAN-ok az IEEE 802.1Q specifikációjában lettek definiálva, fenntartva visszafelé a kompatibilitást a hagyományos LAN megvalósításokra jellemző címkézetlen forgalommal. A natív VLAN egy közös azonosítóként szolgál a trönk kapcsolat két átellenes végén.

A legjobb módszer a natív VLAN-t egy használatlan, VLAN 1-től és a többi VLAN-tól eltérő VLAN-nak beállítani. Valójában nem szokatlan dolog egy meghatározott VLAN-t rászánni arra, hogy a natív VLAN szerepét töltse be a kapcsolt hálózati tartomány valamennyi trönk portja számára.

**Felügyeleti VLAN**

A felügyeleti VLAN a kapcsoló felügyeleti funkcióinak elérésére beállított VLAN. Alapértelmezés szerint a VLAN 1 a felügyeleti VLAN. A felügyeleti VLAN létrehozásához a VLAN virtuális interfészéhez (Switch Virtual Interface, SVI) kell IP-címet és alhálózati maszkot rendelni, ezzel lehetővé téve a kapcsoló felügyeletét HTTP, Telnet, SSH vagy SNMP használatával. Mivel egy Cisco kapcsoló gyári konfigurációjában a VLAN 1 az alapértelmezett VLAN, ezért nem jó döntés a felügyeleti VLAN-nak VLAN 1-et választani.

Korábban a 2960-as kapcsolók felügyeleti VLAN-ja volt az egyetlen aktív SVI. A Cisco IOS 15.x verziójának használatával a Catalyst 2960 sorozatú kapcsolókon lehetővé vált, hogy egynél több aktív SVI is legyen. A Cisco IOS 15.x használatakor a távoli felügyeletre kijelölt konkrét aktív SVI-t dokumentálni kell. Mivel elméletileg egy kapcsolónak már egynél több felügyeleti VLAN-ja is lehet, ezért a hálózati támadásoknak is több helyen van kitéve.

Az ábrán valamennyi port az alapértelmezett VLAN 1-hez van hozzárendelve. Nincs konkrétan kijelölt natív VLAN és nincsenek egyéb aktív VLAN-ok, következésképpen a hálózat úgy van tervezve, hogy a natív VLAN egyben felügyeleti VLAN is legyen. Ez biztonsági szempontból kockázatot jelent.

# VLAN szegmentálás

## VLAN-ok áttekintése

A VoIP (Voice over IP) adatforgalom továbbítására egy elkülönített VLAN szükséges. A VoIP forgalom az alábbiakat igényli:

* Garantált sávszélesség a hangminőség biztosítására.
* Átviteli prioritás egyéb hálózati forgalommal szemben.
* A hálózaton előforduló torlódásos területek elkerülésének a képessége.
* Kevesebb, mint 150 ms késleltetés a hálózaton keresztül.

Ezeknek a követelményeknek a teljesítéséhez az egész hálózatot úgy kell megtervezni, hogy támogassa a VoIP-t. Egy VoIP-t támogató hálózat konfigurációjának részletei meghaladják ennek a kurzusnak a kereteit, ugyanakkor nem haszontalan röviden összefoglalni, hogy egy hangátviteli VLAN hogyan működik egy kapcsoló, egy Cisco IP-telefon és egy számítógép között.

# Az ábrán a hangforgalom továbbítására a VLAN 150 lett kijelölve. A PC5 hallgatói számítógép egy Cisco IP-telefonhoz van csatlakoztatva, a telefon pedig az S3 kapcsolóhoz. A PC5 a VLAN 20-hoz tartozik, amelyet a hallgatói adatok használnak. VLAN szegmentálás

## VLAN-ok áttekintése

Ebben a feladatban egy 24 portos Catalyst 2960 kapcsolót fogunk teljes mértékben kihasználni. Minden port használatban lesz. Meg fogjuk figyelni a szórásos forgalmat egy VLAN-okat használó hálózatban és válaszolni fogunk néhány felvetődő kérdésre.

[Packet Tracer - Who Hears the Broadcast? Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/3.1.1.5%20Packet%20Tracer%20-%20Who%20Hears%20the%20Broadcast%20Instructions.pdf)

[Packet Tracer - Who Hears the Broadcast? - PKA](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/3.1.1.5%20Packet%20Tracer%20-%20Who%20Hears%20the%20Broadcast.pka)

# VLAN szegmentálás

## VLAN-ok többkapcsolós környezetben

A VLAN trönk vagy egyszerűen csak trönk egy pont-pont kapcsolat két olyan hálózati eszköz között, amelyek egynél több VLAN forgalmát is továbbítják. A VLAN trönk kiterjeszti a VLAN-okat a hálózat egészére. A Cisco az IEEE 802.1Q szabványt támogatja a trönkök összehangolására a Fast Ethernet, a Gigabit Ethernet és a 10-Gigabit Ethernet interfészeken.

A VLAN-ok nem lennének jól használhatóak VLAN trönkök nélkül. A VLAN trönkök lehetővé teszik a VLAN-ok forgalmának kapcsolók közötti továbbítását, így ugyanabba a VLAN-ba tartozó, de különböző kapcsolókhoz csatlakozó eszközök is képesek forgalomirányító közvetítése nélkül is kommunikálni.

Egy VLAN trönk nem tartozik egyetlen meghatározott VLAN-hoz sem, inkább egy csatorna a különböző VLAN-ok számára a kapcsolók és forgalomirányítók között. Trönk egy hálózati eszköz és egy szerver, vagy egy egyéb, 802.1Q kezelésére alkalmas hálózati kártyával felszerelt eszköz között is használható. Alapértelmezés szerint a Cisco Catalyst kapcsolókon egy trönk port valamennyi VLAN forgalmát továbbítja.

Az ábrán lévő S1 és S2, valamint az S1 és S3 kapcsolók közötti linkek a 10-es, 20-as, 30-as és 99-es VLAN-okból eredő forgalom hálózaton keresztüli továbbítására vannak konfigurálva. Ez a hálózat nem működhetne VLAN trönkök nélkül.

# VLAN szegmentálás

## VLAN-ok többkapcsolós környezetben

**VLAN-ok nélküli hálózat**

Egy kapcsoló normál működése során amikor az egyik portján szórásos keretet fogad, akkor azt valamennyi portján továbbítja, kivéve azt, amelyen a szórás beérkezett. Az 1. ábra animációján az egész hálózat ugyanabba az alhálózatba (172.17.40.0/24) tartozik és nincsenek VLAN-ok konfigurálva. Ennek eredményeként amikor a kari számítógép (PC1) elküld egy szórásos keretet, akkor azt az S2 kapcsoló valamennyi portján kiküldi. Végül az egész hálózat megkapja a szórást, mivel a hálózat egyetlen szórási tartomány.

**VLAN-okat használó hálózat**

Ahogy a 2. ábra animációján látható, a hálózat két VLAN felhasználásával szegmentálva lett: a kari (Faculty) eszközök a VLAN 10-be, a hallgatói (Student) eszközök VLAN 20-ba lettek besorolva. Amikor a kari PC1 számítógép szórásos keretet küld az S2 kapcsolónak, akkor a kacsoló ezt a szórásos keretet kizárólag azokhoz a kapcsolóportjaihoz fogja továbbítani, amelyek a VLAN 10 használatára lettek beállítva.

Az S2 és S1 kapcsolók közötti linkhez tartozó F0/1 port, valamint az S1 és S3 közötti linkhez tartozó F0/3 port trönkök, így úgy lettek konfigurálva, hogy a hálózat valamennyi VLAN-ját továbbítsák.

Amikor S1 az F0/1 porton fogadja a szórásos keretet, akkor az egyetlen VLAN 10-et támogató másik portján, az F0/3-on továbbítja azt. Amikor S3 az F0/3 porton megkapja a szórásos keretet, akkor ő is a VLAN 10-et támogató egyetlen másik portján, az F0/11-en továbbítja azt. Ezek után a szórásos keret megérkezik a PC4 kari számítógéphez, amely az egyetlen másik VLAN 10-re konfigurált számítógép a hálózatban.

Amikor egy kapcsolón VLAN-okat használunk, akkor egy meghatározott VLAN-ba tartozó állomás egyedi- és csoportos címzésű, valamint szórásos forgalmának a továbbítása kizárólag azokra az eszközökre fog korlátozódni, amelyek ugyanabba a VLAN-ba tartoznak.

# VLAN szegmentálás

## VLAN-ok többkapcsolós környezetben

A Catalyst 2960 sorozatú kapcsolók második rétegbeli (Layer 2) eszközök. A csomagok továbbításához az Ethernet keretek fejlécének információit használják. Irányítótábláik nincsenek. A szabványos Ethernet keretfejléc nem tartalmaz információt arról a VLAN-ról amelyhez a keret tartozik, ezért amikor az Ethernet kereteket egy trönkre helyezik, el kell látni azokat a hozzájuk tartozó VLAN-okra vonatkozó információval. Ez a címkézésnek (tagging) nevezett folyamat az IEEE 802.1Q szabványban meghatározott IEEE 802.1Q fejléc használatával történik. A 802.1Q fejléc egy az eredeti Ethernet keret fejlécébe illesztett 4 bájtos címkét tartalmaz, amely beazonosítja azt a VLAN-t, amelyhez a keret tartozik.

Amikor a kacsoló egy VLAN-hoz hozzárendelt hozzáférési módú porton keretet fogad, akkor a keretfejlécbe egy VLAN-címkét szúr be, majd újraszámítja a keretellenőrző összeget (FCS), és a címkézett keretet egy trönk porton továbbküldi.

**A VLAN-címke mező felépítése**

A VLAN-címke mező egy típus (Type) mezőből és egy címkevezérlési információkat tartalmazó (Tag Control) mezőből áll:

* **Típus (Type)** - Egy 2 bites érték, amit a címke protokollazonosító értékének (Tag Protocol ID, TPID) neveznek. Ethernet esetén az értéke hexadecimális 0x8100.
* **Felhasználói prioritás (User Priority)** - Egy 3 bites érték, amely a szolgáltatási szintek (QoS) megvalósítását támogatja.
* **Kanonikus formátumazonosító (Canonical Format Identifier, CFI)** - Egy 1 bites VLAN azonosító, amely Token Ring keretek továbbítást teszi lehetővé Ethernet linkeken.
* **VLAN ID (VID)** - Egy 12 bites VLAN azonosító, amely így maximálisan 4096 VLAN ID-t támogat.

Miután a kapcsoló beillesztette a típus és címkevezérlési információ mezőket, újraszámolja az FCS értéket és elhelyezi azt a keret FCS mezőjében.

# VLAN szegmentálás

## VLAN-ok többkapcsolós környezetben

**Címkézett keretek a natív VLAN-on**

A trönkölést támogató egyes eszközök VLAN-címkét adnak a natív VLAN forgalomhoz. A natív VLAN-on küldött vezérlési forgalmat nem kell címkézni. Ha egy 802.1Q trönk port egy a natív VLAN ID-val megcímkézett keretet fogad, akkor eldobja azt. Következésképpen mikor kapcsolóportot konfigurálunk egy Cisco kapcsolón, akkor úgy kell az eszközöket konfigurálnunk, hogy azok ne küldjenek címkézett kereteket a natív VLAN-on. Egyéb gyártók natív VLAN-címkézést támogató eszközei közé tartoznak az IP-telefonok, a szerverek, a forgalomirányítók és a nem Cisco kapcsolók.

**Címkézetlen keretek a natív VLAN-on**

Amikor egy Cisco kapcsoló trönk portja címkézetlen kereteket fogad (ami egyébként szokatlan egy jól tervezett hálózatban), akkor azokat a natív VLAN-ba továbbítja. Ha nincsenek a natív VLAN-hoz társított eszközök (ami viszont nem szokatlan) és más trönk portok sincsenek (ami szintén nem szokatlan), akkor a keret eldobásra kerül. Alapértelmezés szerint VLAN 1 a natív VLAN. Egy 802.1Q trönk port konfigurálásakor a natív VLAN ID értéke az alapértelmezett port VLAN ID (PVID) lesz. Minden 802.1Q portra beérkező, vagy arról kimenő címkézetlen forgalom a PVDI érték alapján kerül továbbításra. Ha például natív VLAN-nak a VLAN 99 lett beállítva, akkor a PVID értéke 99 és minden címkézetlen forgalom a VLAN 99-be lesz továbbítva. Ha a natív VLAN nem lett újrakonfigurálva, akkor a PVID értéke a VLAN 1 lesz.

Az ábrán PC1 egy hub-on keresztül csatlakozik egy 802.1Q trönk kapcsolathoz. PC1 címkézetlen forgalmat küld, amit a kapcsolók a trönk portokon konfigurált natív VLAN-hoz társítanak, és annak megfelelően továbbítanak. A trönkről érkező címkézett forgalmat PC1 eldobja. Ez a felállás több szempontból is gyenge hálózattervezést tükröz: hub-ot használ, állomást csatlakoztat egy trönk kapcsolathoz, és ez maga után vonja, hogy a kapcsolóknak vannak hozzáférési portjai a natív VLAN-hoz rendelve. Jól szemlélteti azonban az IEEE 802.1Q specifikáció azon szándékát, hogy a natív VLAN-ok segítségével kezeljék a hagyományos hálózati megvalósításokat.

# VLAN szegmentálás

## VLAN-ok többkapcsolós környezetben

Ahogy az 1. ábra mutatja, az S3 kapcsoló F0/18 portja hangátviteli módra van konfigurálva, ezáltal a hangot tartalmazó keretek VLAN 150 címkét kapnak. A Cisco IP-telefonon keresztül a PC5 felől érkező adatkeretek címkézetlenek maradnak. A PC5-nek szánt, az F0/18 portról ékező adatkeretek a telefonoz vezető úton VLAN 20-al címkézettek. A telefon eltávolítja a VLAN-címkét mielőtt az adatokat PC5-nek továbbítaná.

A Cisco IP-telefon egy beépített három portos 10/100-as kapcsolót tartalmaz. A portok meghatározott célú kapcsolatokat biztosítanak az eszközöknek:

* Az 1-es port a kapcsolóhoz vagy egy másik VoIP eszközhöz csatlakozik.
* A 2-es port egy belső 10/100 interfész, amely az IP-telefon forgalmát továbbítja.
* A 3-as port (hozzáférési port) PC-hez vagy valamely más eszközhöz csatlakozik.

Amikor a kapcsolóporton hangátviteli VLAN (voice VLAN) van konfigurálva, akkor a kapcsoló és az IP-telefon közötti link trönkként szolgál, mind a címkézett hangforgalom, mind pedig a címkézetlen adatforgalom továbbítására. A kapcsoló és az IP-telefon közötti kommunikációt a CDP protokoll (Cisco Discovery Protocol) segíti elő.

**Példakonfiguráció**

A 2. ábra egy parancskimenetet mutat. Bár a Cisco IOS VoIP utasításainak tárgyalása túlmutat ennek a kurzusnak a keretein, a kimeneti példában lévő kiemelt részek így is jól mutatják, hogy az F0/18 interfész egy az adatok számára beállított VLAN-nal (VLAN 20) és egy a hang számára beállított VLAN-nal (VLAN 150) lett konfigurálva.

# VLAN-ok megvalósítása

## VLAN-ok hozzárendelése

Különböző Cisco Catalyst kapcsolók eltérő számú VLAN-t támogatnak. A támogatott VLAN-ok száma elegendően nagy a legtöbb szervezet igényeinek kielégítésére. A Catalyst 2960 és 3560 sorozatú kapcsolók például több mint 4,000 VLAN-t kezelnek. A normál tartományú VLAN-ok ezeken a kapcsolókon 1-től 1,005-ig számozottak, a kiterjesztett tartományú VLAN-ok pedig 1,006 és 4,094 között. Az ábra egy Cisco IOS Release 15.x-et futtató Catalyst 2960 kapcsolón rendelkezésre álló VLAN-okat szemlélteti.

**Normál tartományú VLAN-ok**

* Kis- és közepes méretű vállalkozásokban és vállalati hálózatokban használtak.
* 1 és 1500 közötti VLAN ID-val vannak azonosítva.
* Az 1002 és 1005 közötti ID-k a Token Ring és az FDDI VLAN-ok számára vannak lefoglalva.
* Az 1, valamint az 1002 és 1005 közötti ID-k automatikusan jönnek létre és nem lehet őket törölni sem.
* A konfigurációk a vlan.dat nevű VLAN adatbázisfájlban vannak tárolva. A vlan.dat fájl a kapcsoló flash memóriájában található.
* A VTP (VLAN Trunking Protocol), amely a kapcsolók közötti VLAN konfigurációt segíti, kizárólag normál tartományú VLAN-okat képes megtanulni és tárolni.

**Kiterjesztett tartományú VLAN-ok**

* Lehetővé teszik a szolgáltatóknak, hogy nagyobb számú előfizetőre terjeszthessék ki az infrastruktúrájukat. Egyes globális vállalatok lehetnek annyira nagyméretűek, hogy kiterjesztett tartományú VLAN ID-kra legyen szükségük.
* 1006 és 4094 közötti VLAN ID-val vannak azonosítva.
* A konfigurációk nem íródnak bele a vlan.dat fájlba.
* A normál tartományú VLAN-oknál kevesebb VLAN funkciót támogatnak.
* Alapértelmezés szerint a futó konfigurációs fájlban tárolódnak.
* A VTP nem tanulja meg a kiterjesztett tartományú VLAN-okat.

**MEGJEGYZÉS**: Mivel az IEEE 802.1Q keretfejléc VLAN ID mezője 12 bites, ezért a Catalyst kapcsolókon 4096 az igénybe vehető VLAN-ok számának felső határa.

# VLAN-ok megvalósítása

## VLAN-ok hozzárendelése

Amikor normál tartományú VLAN-okat konfigurálunk, akkor a konfigurációs részletek a kapcsoló flash memóriájában egy vlan.dat nevű fájlban tárolódnak. A flash memória tartalma megmarad, és nem igényli a **copy running-config startup-config** utasítás kiadását sem. Ugyanakkor, mivel egy Cisco kapcsolón a VLAN-ok létrehozásával párhuzamosan gyakran más részletek is beállításra kerülnek, jól bevált gyakorlat az aktuális konfigurációt az indulási konfigurációba is elmenteni.

Az 1. ábra egy VLAN-nak a kapcsolón történő létrehozásához és névadásához használt Cisco IOS utasítások szintaktikáját mutatja. Kapcsolók konfigurációjakor bevált gyakorlatnak számít valamennyi VLAN-nak nevet adni.

A 2. ábra azt szemlélteti, hogy hogyan kell az S1 kapcsolón a hallgatói VLAN-t (VLAN 20) bekonfigurálni. A példa topológiájában a hallgatói számítógép (PC1) még nem lett VLAN-hoz rendelve, de már van IP-címe, a 172.17.20.22.

Használjuk a 3. ábrán lévő parancsszimulátort egy VLAN létrehozásához és használjuk a **show vlan brief** utasítást a vlan.dat fájl tartalmának megjelenítéséhez!

Egyetlen VLAN ID bevitelén felül VLAN ID-k vesszővel elválasztott sorozatát, vagy kötőjellel elválasztott tartományát is megadhatjuk a **vlan** *vlan-azonosító* utasítás segítségével. Használhatjuk például az alábbi utasítást a 100, 102, 105, 106 és 107 VLAN-ok létrehozásához:

S1(config)# **vlan 100,102,105-107**

# VLAN-ok megvalósítása

## VLAN-ok hozzárendelése

Egy VLAN létrehozása után a következő lépés a portoknak a VLAN-hoz rendelése. Egy hozzáférési port egyszerre csak egy VLAN-hoz tartozhat, egyetlen kivétel ez alól a szabály alól, amikor a porthoz IP-telefonhoz csatlakozik. Ebben az esetben két VLAN van a porthoz társítva: egy a hang, egy pedig az adatok számára.

Az 1. ábra egy port hozzáférési portként történő definiálásának és egy VLAN-hoz történő hozzárendelésének a szintaktikáját mutatja. A **switchport mode access** utasítás ugyan opcionális, de mint biztonsági gyakorlat erősen ajánlott. Ezzel a paranccsal az interfész állandó hozzáférési módra vált.

**MEGJEGYZÉS**: Használjuk az **interface range** utasítást több interfész párhuzamos konfigurációjához.

A 2. ábra példájában S1 kapcsolón az F0/18 interfészhez a VLAN 20 van hozzárendelve, ezért a hallgatói számítógép (PC2) a VLAN 20-ba tartozik. Más kapcsolókon a VLAN 20 konfigurációjakor a hálózati rendszergazda tudja, hogy az egyéb hallgatói számítógépeket a PC2-vel egy alhálózaton (172.17.20.0/24) lévőnek kell beállítani.

Használjuk a 3. ábrán lévő parancsszimulátort egy VLAN hozzárendeléséhez és használjuk a **show vlan brief** utasítást a vlan.dat fájl tartalmának megjelenítéséhez.

A **switchport access vlan** parancs kikényszeríti egy VLAN létrehozását, amennyiben az még nem léteik a kapcsolón. A VLAN 30 például nem jelenik meg a **show vlan brief** kimenetében. Ha előzetes konfiguráció nélkül bármelyik interfészen kiadjuk a **switchport access vlan 30** utasítást, a kapcsoló a következőt jelzi ki:

% Access VLAN does not exist. Creating vlan 30

# VLAN-ok megvalósítása

## VLAN-ok hozzárendelése

Egy port VLAN tagságának a megváltoztatására többféle módszer létezik. Az 1. ábra egy kapcsolóport VLAN 1 tagságra történő visszaváltoztatásának szintaktikáját mutatja a **no switchport access vlan** interfész konfigurációs paranccsal.

Az F0/18 interfész előzőleg a VLAN 20-hoz volt hozzárendelve. A **no switchport access vlan** utasítás ki lett adva az F0/18 interfészen. Vizsgáljuk meg a **show vlan brief** parancs kimenetét a 2. ábrán. A **show vlan brief** utasítás megjeleníti a kapcsolóportok VLAN hozzárendelését és tagságának a típusát. A **show vlan brief** utasítás soronként egy VLAN-t jelenít meg. A kimenet minden VLAN esetében tartalmazza a VLAN nevét, állapotát és a kapcsolóportokat.

A VLAN 20 továbbra is aktív annak ellenére, hogy nincs hozzá port rendelve. A 3. ábrán a **show interfaces f0/18 switchport** utasítás kimenetén leellenőrizhetjük, hogy az F0/18 interfész VLAN hozzáférése valóban vissza lett-e állítva VLAN 1-re.

Egy port VLAN tagsága könnyen megváltoztatható. A port VLAN tagságának a megváltoztatásához nem szükséges először azt a VLAN-ból eltávolítani. Amikor egy hozzáférési port VLAN tagságát egy másik létező VLAN-ra változtatjuk meg, akkor az új VLAN tagság egyszerűen felváltja az előzőt. A 4. ábra az F0/11 port VLAN 20-hoz rendelését mutatja.

Használjuk az 5. ábrán lévő parancsszimulátort egy port VLAN tagságának a megváltoztatására!

# VLAN-ok megvalósítása

## VLAN-ok hozzárendelése

Az ábrán a **no vlan** *vlan-azonosító* globális konfigurációs utasítás lett kiadva a VLAN 20 kapcsolóról történő eltávolítására. Az S1 kapcsoló egy minimális konfigurációval rendelkezett, valamennyi portja VLAN 1-hez tartozott, és volt egy használatlan VLAN 20 az adatbázisában. A **show vlan brief** utasítás azt ellenőrzi, hogy a **no vlan 20** utasítás kiadása után VLAN 20 a továbbiakban már valóban nincs benne a vlan.dat fájlban.

**FIGYELEM**: VLAN törlése előtt először győződjünk meg arról, hogy minden hozzá tartozó port át lett helyezve egy másik VLAN-ba. Bármely port, amely nem lett egy aktív VLAN-ba áthelyezve, a VLAN törlése után egészen addig nem lesz képes más állomásokkal kommunikálni, amíg a hozzárendelése egy aktív VLAN-hoz meg nem történik.

Egy másik lehetőség az egész vlan.dat fájl törlése a **delete flash:vlan.dat** privilegizál EXEC módbeli paranccsal. Használható a parancs rövidített változata is (**delete vlan.dat**), amennyiben a vlan.dat fájl nem lett áthelyezve az alapértelmezett helyéről. Ennek a parancsnak kiadása, valamint a kapcsoló újraindítása után a korábban konfigurált VLAN-ok többé már nem lesznek elérhetők. Ez a VLAN konfiguráció tekintetében tulajdonképpen a kapcsolót annak gyári alapértelmezett állapotba állítja vissza.

**MEGJEGYZÉS**: Egy Catalyst kapcsoló esetében a gyári alapértelmezett állapot visszaállítására irányuló újraindítás előtt az **erase startup-config** utasítás mellett ki kell adni a **delete vlan.dat** utasítást is.

# VLAN-ok megvalósítása

## VLAN-ok hozzárendelése

Egy VLAN bekonfigurálása után a VLAN beállítások a Cisco IOS **show** parancsaival ellenőrizhetők.

Az 1. ábra a **show vlan** és a **show interfaces** utasítások gyakoribb opcióit mutatja.

A 2. ábra példáján látható **show vlan name student** utasítás egy nehezebben értelmezhető kimenetet ad. Szerencsésebb inkább a **show vlan brief** utasítás használata. A **show vlan summary** parancs a konfigurált VLAN-ok számát adja vissza. A 2. ábrán látható parancs kimenete hét VLAN-t mutat.

A **show interfaces vlan** *vlan-azonosító* utasítás olyan részleteket is kijelez, amelyek meghaladják ennek a kurzusnak a kereteit. A lényeges információ a 3. ábrán a második sorban jelenik meg, amely jelzi, hogy a VLAN 20 működik.

Használjuk az 4. ábrán lévő parancsszimulátort a kapcsoló portinformációinak megjelenítéséhez a **show interfaces** *interfész-azonosító* **switchport** utasítást használva. Az utasítás a VLAN hozzárendelések és a port mód ellenőrzésére használható.

# VLAN-ok megvalósítása

## VLAN trönkök

A VLAN trönk egy OSI második rétegbeli link két kapcsoló között, amely valamennyi VLAN forgalmát továbbítja (hacsak az engedélyezett VLAN-ok listája manuálisan vagy dinamikusan nem korlátozott). VLAN trönk kapcsolatok engedélyezéséhez a fizikai kapcsolat két végén lévő portokat azonos parancsokkal konfiguráljuk.

Egy trönk kapcsolat egyik végén lévő kapcsolóport konfigurálásához a **switchport mode trunk** utasítást használjuk. Az utasítás hatására az interfész egy állandósult trönk módra vált. A port egy dinamikus trönkprotokoll (Dynamic Trunking Protocol, DTP) egyeztetésbe kezd, hogy a kapcsolatot trönk kapcsolattá alakítsa még akkor is, ha a hozzá csatlakozó interfész nem járult hozzá a változtatáshoz. A DTP részletezését a következő témakör tárgyalja. Ebben a kurzusban kizárólag csak a **switchport mode trunk** utasítást használjuk trönkök konfigurációjához.

A natív VLAN (VLAN 1-től eltérő) megadásának Cisco IOS utasításszintaktikáját az 1. ábra mutatja. Példánkban VLAN 99 lett natív VLAN-nak beállítva a **switchport trunk native vlan 99** utasítással.

A **switchport trunk allowed vlan** *vlan-lista* Cisco IOS utasítást használhatjuk egy trönk kapcsolaton az engedélyezett VLAN-ok listájának megadására.

A 2. ábrán a VLAN 10, 20 és 30 lettek a kari (Faculty), a hallgatói (Student) és a vendég (Guest) számítógépek (PC1, PC2 és PC3) számára kialakítva. Az S1 kapcsoló F0/1 portja trönknek lett konfigurálva és a 10-es, 20-as és 30-as VLAN-ok forgalmát továbbítja. Natív VLAN-nak a VLAN 99 lett beállítva.

A 3. ábra S1 kapcsoló F0/1 portjának trönk konfigurációját mutatja. A natív VLAN le lett cserélve VLAN 99-re, és a trönkön engedélyezett VLAN-ok listája pedig le lett korlátozva 10, 20 és 30-ra.

Ha a natív VLAN nincs a trönk kapcsolaton engedélyezve, akkor a trönk semmilyen adatforgalmat nem engedélyez a natív VLAN számára.

**MEGJEGYZÉS**: A konfiguráció Cisco Catalyst 2960 kapcsolók használatát feltételezi a 802.1Q beágyazás automatikus alkalmazásával a trönk kapcsolatokon. Más típusú kapcsolók igényelhetik a beágyazás manuális beállítását. Egy trönk kapcsolat mindkét végét ugyanazzal a natív VLAN-al konfiguráljuk. Ha a 802.1Q trönk konfiguráció nem ugyanaz a két végen, akkor a Cisco IOS szoftver hibát jelez.

# VLAN-ok megvalósítása

## VLAN trönkök

Az 1. ábra az engedélyezett VLAN-ok eltávolítására és a trönk natív VLAN-jának visszaállítására szolgáló parancsokat mutatja. Az alapértelmezett állapot visszaállítása után a trönk valamennyi VLAN-t engedélyezi és VLAN 1-et használja natív VLAN-nak.

A parancs, amely egy kapcsolóportot hozzáférési porttá alakít vissza és ennek eredményeként megszünteti a trönk portot, szintén bemutatásra kerül.

A 2. ábra egy trönk interfész trönkölési alapbeállításainak a visszaállítására szolgáló parancsokat mutatja. A **show interfaces f0/1 switchport** utasítás igazolja, hogy a trönk valóban visszaállt az alapértelmezett állapotra.

A 3. ábrán látható példa az S1 kapcsoló F0/1 portjáról a trönk tulajdonság eltávolítására szolgáló utasításokat mutatja. A **show interfaces f0/1 switchport** utasítás igazolja, hogy az F0/1 interfész most már valóban statikus hozzáférési módban van.

# VLAN-ok megvalósítása

## VLAN trönkök

Az 1. ábra az kapcsoló F0/1 portjának beállításait mutatja. A konfiguráció a **show interfaces** *interfész-azonosító* **switchport** utasítással lett ellenőrizve.

A felső kiemelt rész mutatja, hogy az F0/1 port adminisztrációs módjának (Administrative Mode) beállítása **trunk**. A port tehát trönk módban van. A következő kiemelt terület igazolja, hogy a VLAN 99 a natív VLAN. A parancskimenetben lejjebb látható kiemelt rész jelzi, hogy a trönkön valamennyi VLAN engedélyezve van.

Használjuk az 2. ábrán lévő parancsszimulátort az F0/1 interfészen egy az összes VLAN-t támogató trönk konfigurálásához 99-es natív VLAN-al. Ellenőrizzük a trönk konfigurációját a **show interfaces f0/1 switchport** utasítással.

# VLAN-ok megvalósítása

## VLAN trönkök

A VLAN információk kapcsolók közötti átviteléhez trönkök szükségesek. Egy kapcsolóport lehet hozzáférési port vagy trönk port. A hozzáférési portok a hozzájuk rendelt, meghatározott VLAN forgalmát továbbítják. Egy trönk port alapértelmezésben minden VLAN-nak tagja, ezért valamennyi VLAN forgalmát továbbítja. Ez a feladat a trönk portok létrehozására, és azok az alapértelmezettől eltérő natív VLAN-hoz rendelésére fókuszál.

[Packet Tracer - Configuring Trunks Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/3.2.2.4%20Packet%20Tracer%20-%20Configuring%20Trunks%20Instructions.pdf)

[Packet Tracer - Configuring Trunks - PKA](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/3.2.2.4%20Packet%20Tracer%20-%20Configuring%20Trunks.pka)

# VLAN-ok megvalósítása

## Dinamikus trönkprotokoll (Dynamic Trunking Protocol)

Az Ethernet trönk interfészek különböző trönkölési módokat támogatnak. Egy interfész trönk (trunking) vagy nem trönk (nontrunking) módúra konfigurálható, illetve megadható az is, hogy a trönkölést egyeztesse a hozzá csatlakozó szomszédos interfésszel. A hálózati eszközök között a trönk egyeztetését a pont-pont alapon működő dinamikus trönkprotokoll (Dynamic Trunking Protocol, DTP) végzi.

A DTP a Cisco szabadalmaztatott protokollja, amely a Catalyst 2960 és Catalyst 3560 sorozatú kapcsolókon automatikusan engedélyezve van. Más gyártók kapcsolói nem támogatják a DTP-t. A DTP a trönk egyeztetését csak akkor hajtja végre, ha a szomszédos kapcsolón lévő port is olyan trönk módra van beállítva, amely támogatja a DTP-t.

**FIGYELEM**: Egyes hálózati eszközök helytelenül továbbíthatják a DTP kereteket, amely hibás konfigurációt eredményezhet. Ennek megelőzésére kapcsoljuk ki DTP-t egy Cisco kapcsoló azon interfészein, amelyek a DTP-t nem támogató eszközökhöz csatlakoznak.

A Cisco Catalyst 2960 és 3560 kapcsolók alapértelmezett DTP-konfigurációja az "automata dinamikus" (dynamic auto) mód, ahogy az az 1. ábra S1 és S3 kapcsolóinak F0/3 interfészein látható.

Egy Cisco kapcsoló és egy a DTP-t nem támogató eszköz között a trönkölés engedélyezéséhez használjuk a **switchport mode trunk** és a **switchport nonegotiate** interfész konfigurációs parancsokat. Ennek eredményeként az interfész trönk lesz, ugyanakkor nem generál DTP kereteket.

A 2. ábrán az S1 és S2 kapcsolók közötti link trönk lesz, mivel a kapcsolókon az F0/1 portok úgy lettek konfigurálva, hogy hagyjanak figyelmen kívül minden DTP-hirdetést, ugyanakkor váltsanak trönk módra és maradjanak is abban. Az S1 és S3 kapcsolók F0/3 portjai automata dinamikus módra lettek beállítva, így az egyeztetés eredménye a hozzáférési mód (Access Mode) lesz. Ez egy inaktív trönk kapcsolatot eredményez. Amikor egy portot trönknek konfigurálunk, akkor nem kétséges, hogy a trönk milyen állapotban van: mindig be van kapcsolva. Ezzel a konfigurációval egyszerűbb megjegyezni, hogy a trönk portok milyen állapotban vannak. Ha a portnak trönknek kell lenni, akkor a mód beállítása is legyen trönk.

# VLAN-ok megvalósítása

## Dinamikus trönkprotokoll (Dynamic Trunking Protocol)

A Catalyst 2960 és 3650 sorozatú kapcsolók Ethernet portjai a DTP segítségével különböző trönkölési módokat támogatnak:

* **switchport mode access** - Az interfészt (hozzáférési portot) állandósult nem trönk (nontrunking) módba helyezi, és egyeztetésbe kezd a kapcsolat "nem trönkké" alakítására. Az interfész "nem trönk" (nontrunk) interfész lesz, függetlenül attól, hogy a szomszédos interfész egy trönk vagy egy hozzáférési port.
* **switchport mode dynamic auto** - Képessé teszi az interfészt, hogy a kapcsolatot trönk kapcsolattá alakítsa. Az interfész trönk interfésszé válik, ha a szomszédos interfész trönk (trunk) vagy kezdeményező (desirable) módra van beállítva. Minden Ethernet interfészen az **automata dinamikus** az alapértelmezett kapcsolóport mód.
* **switchport mode dynamic desirable** - Az interfész megpróbálja a kapcsolatot aktívan trönk kapcsolattá alakítani. Az interfész trönk interfésszé válik, ha a szomszédos interfész trönk (trunk), kezdeményező (desirable) vagy automata (auto) módra van beállítva. Ez az alapértelmezett kapcsolóport mód olyan régebbi kapcsolók esetében, mint például a Catalyst 2950 és 3550 sorozatú kapcsolók.
* **switchport mode trunk** - Az interfészt állandósult trönk módba helyezi, és egyeztetésbe kezd a kapcsolat trönkké alakítására. Az interfész trönk interfésszé válik, függetlenül attól, hogy a szomszédos interfész esetleg nem trönk interfész.
* **switchport nonegotiate** - Megakadályozza, hogy az interfész DTP-s kereteket generáljon. Ez az utasítás csak akkor alkalmazható, ha a kapcsolóport **access** vagy **trunk** módban van. Trönk kapcsolat kiépítéséhez a szomszédos interfészt manuálisan kell trönk interfésznek beállítani.

Az 1. ábra a DTP konfiguráció lehetséges kimeneteit mutatja egy Catalyst 2960 kapcsolóportokhoz csatlakozó trönk kapcsolat átellenes végeinek a függvényében.

Amikor csak lehetséges, a trönk kapcsolatokat statikusan állítsuk be. Az alapértelmezett DTP-mód függ a Cisco IOS szoftver verziójától és a platformtól. A DTP-mód megtekintéséhez adjuk ki a **show dtp interface** utasítást (lásd 2. ábra).

Használjuk az 3. ábrán lévő parancsszimulátort az F0/1 interfész DTP-módjának meghatározására.

**MEGJEGYZÉS**: Általánosan bevált gyakorlat az interfészt **trunk** és **nonegotiate** módra beállítani, amikor trönk kapcsolatra van szükség. Azokon az interfészeken, amelyeken nem akarunk trönkölni, a DTP-t ki kell kapcsolni.

# VLAN-ok megvalósítása

## VLAN-ok és trönkök hibakeresése

Minden VLAN-hoz egyedi IP-alhálózatot kell rendelni. Ha ugyanazon a VLAN-on belül két eszköznek különböző alhálózatokhoz tartozó címeik vannak, akkor nem képesek egymással kommunikálni. Ez gyakori probléma, amelyet azonban a hibás konfiguráció beazonosításával és az alhálózati cím megfelelőre cserélésével könnyű kijavítani.

Az 1. ábrán PC1 nem tud csatlakozni a Web/TFTP-szerverhez.

PC1 IP-beállításainak az ellenőrzése (lásd 2. ábra) rámutat a VLAN-ok konfigurálásának leggyakoribb hibájára: egy hibásan konfigurált IP-címre. PC1 a 172.172.10.21 IP-címmel lett konfigurálva, pedig a 172.17.10.21-et kellett volna rajta beállítani.

A PC1 FastEthernet párbeszédablaka mutatja a kijavított 172.17.10.21 IP-címet. A 3. ábra alján látható kimenet igazolja, hogy PC1 kapcsolata a 172.17.10.30 IP-címen található Web/TFTP-szerverrel helyreállt.

# VLAN-ok megvalósítása

## VLAN-ok és trönkök hibakeresése

Ha az egy VLAN-ban tartozó eszközök között nincs kapcsolat, ugyanakkor az IP-címzési hibákat már kizártuk, akkor a hibakeresés során kövessük az 1. ábrán látható folyamatábrát.

**1. lépés:** Használjuk a **show vlan** utasítást annak ellenőrzésére, hogy a port a megfelelő VLAN-hoz tartozik-e. Ha a port hibás VLAN-hoz lett hozzárendelve, akkor használjuk a **switchport access vlan** utasítást a VLAN tagság korrigálásához. Használjuk a **show mac address-table** utasítást annak ellenőrzésére, hogy egy adott porton mely címek lettek megtanulva és a port melyik VLAN-hoz tartozik.

**2. lépés:** Ha egy porthoz már hozzárendelt VLAN-t törlünk, akkor a port inaktívvá válik. Használjuk a **show vlan** vagy a **show interfaces switchport** parancsot.

A MAC-cím tábla megjelentéséhez használjuk a **show mac-address-table** parancsot. A 2. ábra példája az F0/1 interfészen megtanult MAC-címeket mutatja. Látható rajta, hogy a 000c.296a.a21c MAC-cím a 10-es VLAN-ba tartozó F0/1 interfészen lett megtanulva. Ha ez a szám nem a megfelelő VLAN azonosító, akkor a **switchport access vlan** utasítással változtassuk meg a port VLAN tagságát.

Egy kapcsoló minden portjának tartoznia kell valamelyik VLAN-hoz. Ha a porthoz tartozó VLAN-t töröljük, akkor a port inaktívvá válik. Törölt VLAN-hoz tartozó portok nem képesek kommunikálni a hálózat többi részével. Használjuk a **show interface f0/1 switchport** utasítást annak eldöntésére, hogy a port inaktív-e. Ha a port inaktív, akkor egészen addig nem működik, amíg a hiányzó VLAN-t létre nem hozzuk a **vlan** *vlan-azonosító* utasítással.

# VLAN-ok megvalósítása

## VLAN-ok és trönkök hibakeresése

A hálózati rendszergazda megszokott feladata egy trönk kapcsolat kiépülésének vagy a hibásan működő trönk kapcsolatoknak a hibaelhárítása. Egy kapcsolóport néha akkor is viselkedhet trönk portként, ha nem annak lett konfigurálva. Például egy hozzáférési port elfogadhat a saját VLAN-jától eltérő VLAN-okból származó kereteket is. Ezt VLAN szivárgásnak nevezzük.

Az 1. ábra egy trönk hibakeresés általános lépéseinek folyamatábráját szemlélteti.

Az alábbiak szerint járjuk el azon problémák hibakeresése során, amikor nem épül fel egy trönk, vagy amikor VLAN szivárgás következik be:

**1. lépés** : Használjuk a **show interfaces trunk** utasítást annak ellenőrzésére, hogy a helyi és a szomszédos natív VLAN megegyezik-e. Ha a natív VLAN a két oldalon eltér, akkor VLAN szivárgás következik be.

**2. lépés** Használjuk szintén a **show interfaces trunk** utasítást annak ellenőrzésére, hogy a trönk kiépült-e a kapcsolók között. Amikor csak lehetséges, a trönk kapcsolatokat statikusan állítsuk be. A Cisco Catalyst kapcsolóportok alapértelmezésben DTP-t használnak és megpróbálnak egy trönk kapcsolatot leegyeztetni.

A trönk állapotának, a trönk kapcsolaton használt natív VLAN-nak, és a trönk kiépülésének ellenőrzésére használjuk a **show interfaces trunk** utasítást. 2. ábra példája mutatja, hogy a natív VLAN a trönk kapcsolat egyik oldalán meg lett változtatva VLAN 2-re. Ha trönk kapcsolat egyik oldalán VLAN 99 a beállított natív VLAN, a másik oldalán pedig VLAN 2, akkor az egyik oldalon egy a VLAN 99-ből elküldött keretet a másik oldalon a VLAN 2 fogad. A VLAN 99 átszivárog a VLAN 2 szegmensébe.

Egy trönk kapcsolaton a hibás natív VLAN párosításról a CDP egy figyelmeztetést jelenít meg az alábbi üzenettel:

\*Mar 1 06:45:26.232: %CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).

Hibás natív VLAN párosítás esetén a hálózatban kapcsolódási problémák lépnek fel. A beállított két natív VLAN-tól eltérő VALN-ok adatforgalma sikeresen továbbítódik a kapcsolaton keresztül, de ugyanakkor a natív VLAN-ok egyikéhez társuló adatok továbbítása már sikertelen lesz.

**MEGJEGYZÉS**: A 2. ábrán látható kimenet ugyanakkor azt is mutatja, hogy a natív VLAN keveredése ellenére a trönk aktív. A működés kijavításához a natív VLAN-t a kapcsolat mindkét végén ugyanarra a VLAN-ra kell beállítani.

# VLAN-ok megvalósítása

## VLAN-ok és trönkök hibakeresése

A trönkölési hibákat általában a nem megfelelő konfiguráció eredményezi. Egy kapcsolt infrastruktúrában VLAN-ok és trönkök konfigurációjakor az alábbi típusú konfigurációs hibák a leggyakoribbak:

* **Natív VLAN keveredés** - A trönk portok különböző natív VLAN-okkal vannak konfigurálva. Ez a konfigurációs hiba a konzolon egy figyelmeztetést generál, valamint a vezérlő- és felügyeleti forgalom téves irányítását eredményezi. Ez biztonsági kockázatot jelent.
* **Trönk mód keveredés** - Az egyik trönk porton be van kapcsolva a trönk mód, a másikon pedig ki van kapcsolva. Ez a konfigurációs hiba a trönk kapcsolat működésképtelenségét okozza.
* **A trönkökön engedélyezett VLAN-ok** - A trönkön engedélyezett VLAN-ok listája nem lett az éppen aktuális trönkölési igényeknek megfelelően frissítve. Ebben az esetben nem várt forgalom, vagy éppen semmilyen forgalom nem lesz a trönkön keresztül továbbítva.

Ha fény derül egy trönkölési hibára, amelynek nem ismerjük az okát, akkor a hibakeresés első lépéseként a natív VLAN keveredése szempontjából vizsgáljuk meg a trönköket. Ha nem ez okozza a hibát, akkor ellenőrizzük a trönk mód keveredését, és végül pedig a trönkön engedélyezett VLAN-ok listáját. A következő két oldal azt vizsgálja, hogy hogyan lehet a tipikus trönk hibákat kijavítani.

# VLAN-ok megvalósítása

## VLAN-ok és trönkök hibakeresése

Normál körülmények között a trönk kapcsolatokat statikusan, a **switchport mode trunk** utasítással konfiguráljuk. A Cisco Catalyst trönk kapcsolóportok DTP-t használnak a kapcsolat állapotának egyeztetéséhez. Amikor a trönk kapcsolat egyik portja a szomszédos porttal inkompatibilis trönk módra van konfigurálva, akkor a két kapcsoló között a trönk nem épül ki.

Az 1. ábrán illusztrált esetleírásban PC4 nem tud csatlakozni a belső webszerverhez. A topológia egy valós konfigurációt vázol fel. Mi okozhatja a problémát?

Ellenőrizzük le az S1 kapcsolón a trönk portok állapotát a **show interfaces trunk** utasítással. A 2. ábrán látható kimenet jelzi, hogy az S3 kapcsolón az F0/3 interfész pillanatnyilag nem egy trönk kapcsolat. Megvizsgálva az F0/3 interfészt azt láthatjuk, hogy a kapcsolóport jelenleg automata dinamikus (dynamic auto) módban van. Az S3 kapcsolón a trönkök vizsgálata azt mutatja, hogy nincsenek aktív trönk portok. A további ellenőrzés pedig azt mutatja, hogy az F0/3 interfész szintén automata dinamikus módban (dynamic auto) van. Ez megmagyarázza, hogy a trönk miért nem működik.

A probléma megoldásához újra kell konfigurálni az F0/3 portokat az S1 és S3 kapcsolókon, ahogy azt a 3. ábra mutatja. A konfiguráció megváltoztatása után a **show interfaces** utasítás kimenete jelzi, hogy a port az S1 kapcsolón már trönk módban van. A PC4-ről származó kimenet pedig megmutatja, hogy a kapcsolat a 172.17.10.30 IP-címen található Web/TFTP-szerverrel helyreállt.

# VLAN-ok megvalósítása

## VLAN-ok és trönkök hibakeresése

Egy VLAN forgalmának áthaladását egy trönkön engedélyezni kell. Ehhez használjuk a **switchport trunk allowed vlan** *vlan-azonosító* utasítást.

Az 1. ábrán VLAN 20 és PC5 hozzá lett adva a hálózathoz. A hálózat dokumentációja frissítve lett annak jelzésére, hogy a trönkön a 10-es, 20-as és 99-es VLAN-ok vannak engedélyezve. Ebben az esetleírásban most PC5 nem tud csatlakozni a hallgatói levelezőszerverhez.

Ellenőrizzük az S1 kapcsolón a trönk portokat a **show interfaces trunk** utasítással, ahogy a 2. ábrán látható. Az utasítás mutatja, hogy az S3 kapcsolón az F0/3 interfész megfelelően lett konfigurálva a 10-es, 20-as és 99-es VLAN-ok engedélyezésére. Az S1 kapcsoló F0/3 interfészének vizsgálata azonban feltárja, hogy az F0/1 és F0/3 interfészek csak a 10-es és 99-es VLAN-okat engedélyezik. Valaki frissítette a dokumentációt, de elfelejtette a portokat az S1 kapcsolón újrakonfigurálni.

Az S1 kapcsoló F0/1 és F0/3 portjainak újrakonfigurálásához használjuk a **switchport trunk allowed vlan 10,20,99** utasítást a 3. ábrán látható módon. A kimenet megmutatja, hogy a 10-es, 20-as és 99-es VLAN-ok már az S1 kapcsolón is hozzá lettek adva az F0/1 és az F0/3 interfészekhez. A **show interfaces trunk** utasítás egy kiváló eszköz a gyakori trönkölési problémák felderítésére. PC5 visszanyerte a csatlakozást a 172.17.20.10 IP-címen található hallgatói levelezőszerverhez.

# VLAN biztonság és tervezés

## VLAN-ok elleni támadások

A modern kapcsolt hálózatokban számos különböző, a VLAN-ok ellen irányuló támadástípus létezik. A VLAN architektúra leegyszerűsíti a hálózat karbantartását és javítja a teljesítményét, ugyanakkor visszaélésekre is lehetőséget ad. Fontos hogy megértsük a támadások általános módszertanát, valamint megelőzésüknek elsődleges megközelítéseit.

A VLAN ugrás lehetővé teszi, hogy egy VLAN forgalmát egy másik VLAN is láthassa. A kapcsoló hamisítás a VLAN ugrási támadásnak egy típusa, amely egy nem megfelelően konfigurált trönk portot használ ki. Alapértelmezés szerint a trönk portok valamennyi VLAN forgalmához hozzáférnek és több VLAN forgalmát továbbítják ugyanazon a fizikai kapcsolaton keresztül, általában kapcsolók között.

Kattintsunk a Lejátszás! gombra a kapcsoló hamisítási támadás animációjának megtekintéséhez.

Egy alapszintű kapcsoló hamisítási támadásban a támadó azt a tényt használja ki, hogy egy kapcsolóport alapértelmezett konfigurációja "automata dinamikus". A hálózati támadó úgy konfigurál egy rendszert, hogy az kapcsolónak álcázza magát. Ez a hamisítási típus azt igényli, hogy a hálózati támadó képes legyen a 802.1Q és a DTP-üzeneteket utánozni. Ezzel a trükkel a kapcsoló azt hiszi, hogy egy másik kapcsoló próbál vele trönköt kiépíteni, a támadó pedig hozzáférést szerez a trönk porton engedélyezett valamennyi VLAN-hoz.

Egy általános kapcsoló hamisítási támadás megelőzésének legjobb módja a trönkölés kikapcsolása minden olyan porton, amelyeken az kifejezetten nem szükséges. Azokon a portokon, amelyeken a trönkölés szükséges, tiltsuk le a DTP-t és manuálisan engedélyezzük a trönkölést.

# VLAN biztonság és tervezés

## VLAN-ok elleni támadások

A VLAN-ok támadásának egy másik típusa a kettős címkézéssel (vagy kettős beágyazással) végrehajtott VLAN ugrásos támadás. Ez a támadástípus azt a módot használja ki, ahogyan a legtöbb kapcsoló hardvere működik. A kapcsolók többsége a 802.1Q beágyazásnak csak egyszintű visszafejtését hajtja végre, ami lehetővé teszi, hogy a támadó egy rejtett 802.1Q címkét ágyazzon be a keret belsejébe. Ez a címke lehetővé teszi a keretnek egy olyan VLAN-ba történő továbbítását, amely az eredeti 802.1Q címkében nem volt megadva. A kettős beágyazásos VLAN ugrásos támadás egy fontos tulajdonsága, hogy akkor is működik, ha a trönk portok le vannak tiltva, mivel egy állomás jellemzően nem trönk kapcsolaton küld el egy keretet.

A kettős címkézéses VLAN ugrásos támadás az alábbi három lépésből áll:

1. A támadó egy duplán megcímkézett 802.1Q keretet küld a kapcsolónak. A külső fejléc a támadó a VLAN-címkéjét tartalmazza, amely megegyezik a trönk port natív VLAN-jával. A feltételezés az, hogy a kapcsoló feldolgozza a támadótól kapott keretet, mintha az egy trönk porton vagy egy hangátviteli VLAN-hoz tartozó porton érkezett volna (egy kapcsolónak nem szabadna egy hozzáférési porton címkézett Ethernet keretet kapnia). A példa kedvéért feltételezzük, hogy VLAN 10 a natív VLAN. A belső címke pedig a megtámadott VLAN, amely ebben az estben VLAN 20.

2. A keret megérkezik a kapcsolóba, amely megnézi az első 4 bájtot, a 802.1Q címkét. A kapcsoló látja, hogy a keretet a 10-es natív VLAN-hoz tartozik. A kapcsoló a csomagot a VLAN 10-es címke eltávolítása után valamennyi VLAN 10-be tartozó portján továbbküldi. A trönk porton a VLAN 10-es címke eltávolításra kerül, és a keret nem is lesz újracímkézve, mivel a natív VLAN-hoz tartozik. Ezen a ponton a VLAN 20-as címke még érintetlen, az első kapcsoló nem foglalkozott vele.

3. A második kapcsoló csak a belső, a támadó által küldött 802.1Q címkét nézi meg, és azt látja, hogy a keret céljaként a VLAN 20 van feltüntetve. A második kapcsoló a keretet kiküldi a megtámadott porton, vagy valamennyi portját elárasztja vele attól függően, hogy a megtámadott állomásnak van-e bejegyzése a MAC-cím táblában.

Ez a támadástípus egyirányú, és csak abban az esetben működik, amikor a támadó a trönk port natív VLAN-jához tartozó portra csatlakozik. Ezt a támadástípust nem olyan könnyű megakadályozni, mint az egyszerű VLAN ugrásos támadásokat.

A kettős címkézéses támadások megelőzésének legjobb módja annak biztosítása, hogy a trönk portok natív VLAN-ja különbözzön valamennyi felhasználói port VLAN-jától. A 802.1Q trönkök natív VLAN-jának egy rögzített, a kapcsolt hálózaton belül a felhasználói VLAN-októl eltérő VLAN-t használni tulajdonképpen a biztonság egy bevált gyakorlatának tekinthető.

# VLAN biztonság és tervezés

## VLAN-ok elleni támadások

Egyes alkalmazások megkívánják, hogy a második rétegben ne legyen forgalom továbbítva egyazon kapcsoló különböző portjai között, így az egyik szomszéd ne láthassa a másik által generált forgalmat. Egy ilyen környezetben a privát VLAN (PVLAN) Edge (más néven védett portok) funkció használata biztosítja, hogy a kapcsoló ezek között a portjai között se egyedi címzésű, se szórásos, se pedig csoportcímzéses forgalom ne cserélődhessen (lásd 1. ábra).

A PVLAN Edge funkció tulajdonságai a következők:

* A védett portok semmilyen forgalmat (egyedi címzésű, csoportcímzésű vagy szórásos) nem továbbítanak más védett portok felé, kivéve a vezérlő forgalmat. Második rétegben a védett portok között nem lehet adatot továbbítani.
* A védett és a nem védett portok közötti továbbítás a szokásos módon történik.
* Védett portokat manuálisan kell beállítani.

A PVLAN Edge funkció konfigurálásához adjuk ki a **switchport protected** interfész konfigurációs utasítást (lásd 2. ábra). Egy védett port kikapcsolásához a **no switchport protected** interfész konfigurációs utasítást használjuk. A PVLAN Edge funkció konfigurációjának ellenőrzésére használjuk a **show interfaces** *interfész-azonosító* **switchport** utasítást.

A 3. ábrán lévő parancsszimulátorral gyakoroljuk a PVLAN Edge funkció beállítását a G0/1 interfészen, valamint a konfiguráció ellenőrzését.

# VLAN biztonság és tervezés

## VLAN-ok tervezésének bevált gyakorlatai

A Cisco kapcsolók olyan gyári konfigurációval rendelkeznek, amelyben az alapértelmezett VLAN-ok a különböző közeg- és protokolltípusok támogatására előre konfigurálva vannak. A VLAN 1 az alapértelmezett Ethernet VLAN. Bevált biztonsági gyakorlat a kapcsolókon az összes portot úgy konfigurálni, hogy azok VLAN 1-től eltérő VLAN-hoz legyenek társítva. Ez általában úgy történik, hogy az összes nem használt portot úgy konfiguráljuk, hogy egy a hálózaton másra nem használt, "fekete lyuk" VLAN-hoz tartozzon. Minden használatban lévő port pedig VLAN 1-től és a "fekete lyuk" VLAN-tól eltérő VLAN-hoz legyen társítva. Szintén egy bevett gyakorlat a használaton kívüli portok letiltása a jogosulatlan hozzáférés megelőzésére.

Hasznos biztonsági eljárás még a felügyeleti és a felhasználói adatforgalom szétválasztása. A felügyeleti VLAN-t, amely alapértelmezésben a VLAN 1, meg kell változtatni egy független, különálló VLAN-ra. Egy Cisco kapcsoló távoli felügyelhetőségéhez a kapcsolónak egy a felügyeleti VLAN-hoz tartozó konfigurált IP-címmel kell rendelkezni. A biztonság egy kiegészítő rétegét alkotva nem szabad, hogy más VLAN-okon lévő felhasználók távoli hozzáférési párbeszédeket tudjanak kialakítani a kapcsolóval, hacsak azok be nincsenek irányítva a felügyeleti VLAN-ba. Ezen felül a kapcsolót is úgy kell konfigurálni, hogy a távoli felügyelethez kizárólag titkosított SSH párbeszédeket fogadjon el.

Minden vezérlőforgalom a VLAN 1-en van elküldve. Ezért amikor a natív VLAN megváltozik VLAN 1-ről valami másra, akkor minden vezérlőforgalom az IEEE 802.1Q trönkökön címkézve lesz (VLAN ID 1 címkével). Ajánlott biztonsági eljárás a natív VLAN lecserélése egy VLAN 1-től eltérő VLAN-ra. A natív VLAN-nak is különböznie kell minden felhasználói VLAN-tól. Figyeljünk rá, hogy a natív VLAN egy 802.1Q trönk kapcsolat mindkét végén ugyanaz legyen!

A DTP négy kapcsolóport módon biztosít: hozzáférési (access), trönk (trunk), automata dinamikus (dynamic automatic) és kezdeményező dinamikus (dynamic desirable). Általános irányelv az automatikus egyeztetés (autonegotiation) letiltása. A portbiztonság bevett gyakorlataként, ne használjuk az automata dinamikus és a kezdeményező dinamikus kapcsolóport módokat.

Végül pedig, a hangforgalomnak szigorú QoS követelményei vannak. Ha a felhasználói PC-k és az IP-telefonok ugyanazon a VLAN-on vannak, akkor mindegyik megpróbálja kihasználni a rendelkezésre álló sávszélességet anélkül, hogy a másik eszközt figyelembe venné. Ezen konfliktus elkerülésére jól bevált módszer külön VLAN-t használni az IP-telefónia és az adatforgalom számára.

# Összefoglalás

## Összefoglalás

**VLAN terv**

**Esetleírás**

Egy VLAN-kapcsolt hálózatot tervezünk a kis-közepes méretű vállalkozásunk számára.

A vállalkozásunk egy toronyház két szintjét birtokolja. A VLAN tervezés és a hozzáférés szempontjából az alábbi szervezeti egységeket kell figyelembe venni:

* igazgatás
* pénzügy
* értékesítés
* munkaügy
* hálózati rendszergazda
* általános látogatók a vállalkozás telephelyén

Két Cisco 3560-24PS kapcsolónk van.

Használjunk szövegszerkesztő programot a VLAN-kapcsolt hálózatunk tervezetének elkészítéséhez.

A tervük első részének tartalmaznia kell a részlegeink pontos nevét, a javasolt VLAN neveket és azonosítókat, és hogy mely kapcsolóportokat szeretnénk az egyes VLAN-okhoz hozzárendelni.

A tervünk második részének fel kell sorolnia, hogy hogyan lenne megtervezhető ennek a kapcsolt hálózatnak a biztonsága.

A VLAN tervünknek elkészülte után válaszoljunk a feladat PDF-jének kérdéseire!

Mentsük el a munkánkat! Legyünk készek elmagyarázni és megbeszélni a VLAN tervünket más csoporttal vagy az osztállyal!

[Csoportos feladat - VLAN Plan Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/3.4.1.1%20VLAN%20Plan%20Instructions.pdf)

# Összefoglalás

## Összefoglalás

Ez a fejezet a VLAN-okat mutatta be. A VLAN-ok a fizikai kapcsolatok helyett logikai kapcsolatokra épülnek. A VLAN-ok olyan mechanizmusok, amelyek lehetővé teszik a hálózati rendszergazdáknak, hogy egy vagy akár több kapcsolóra is kiterjedő logikai szórási tartományokat hozzanak létre, függetlenül a fizikai közelségtől. Ez a funkció jól használható a szórási tartományok méretének csökkentésére, illetve lehetővé teszi a csoportok és felhasználók logikai csoportosítását anélkül, hogy fizikailag ugyanazon a helyen kellene lenniük.

A VLAN-oknak számos különböző típusa létezik:

* alapértelmezett VLAN
* felügyeleti VLAN
* natív VLAN
* felhasználói vagy adat VLAN
* fekete lyuk VLAN
* hangátviteli VLAN

Egy Cisco kapcsolón VLAN 1 az alapértelmezett Ethernet VLAN, és egyben az alapértelmezett felügyeleti VLAN is. A biztonság növelése érdekében bevált gyakorlat a natív és a felügyeleti VLAN-okat egy elkülönített VLAN-ba helyezni, illetve a nem használt kapcsolóportokat egy "fekete lyuk" (black hole) VLAN-ba átcsoportosítani.

A **switchport access vlan** utasítást használjuk egy kapcsolón egy VLAN létrehozására. Egy VLAN létrehozása után a következő lépés a portoknak a VLAN-hoz rendelése. A **show vlan brief** utasítás jeleníti meg a kapcsolóportok VLAN hozzárendelését és tagságának a típusát. Minden VLAN-nak egyedi IP-alhálózattal kell rendelkezni.

Használjuk a **show vlan** utasítást annak ellenőrzésére, hogy egy port a megfelelő VLAN-hoz tartozik-e. Ha a port hibás VLAN-hoz lett hozzárendelve, akkor használjuk a **switchport access vlan** utasítást a VLAN tagság korrigálásához. Használjuk a **show mac address-table** utasítást annak ellenőrzésére, hogy egy konkrét porton mely címek lettek megtanulva és a port melyik VLAN-hoz tartozik.

Egy kapcsolóport lehet hozzáférési port vagy trönk port. A hozzáférési portok a hozzájuk rendelt, meghatározott VLAN forgalmát továbbítják. Egy trönk port alapértelmezésben minden VLAN-nak tagja, ezért valamennyi VLAN forgalmát továbbítja.

A VLAN trönkök azáltal könnyítik meg a kapcsolók közötti kommunikációt, hogy több VLAN forgalmát is továbbítják. A közös trönk kapcsolatokon történő áthaladáskor az egyes VLAN-okhoz hozzárendelt Ethernet kereteket az IEEE 802.1Q keretcímkézés különbözteti meg. A trönk kapcsolatok engedélyezéséhez a **switchport mode trunk** utasítást használjuk. Használjuk a **show interfaces trunk** utasítást annak ellenőrzésére, hogy a trönk kiépült-e a kapcsolók között.

A hálózati eszközök között a trönk egyeztetését a pont-pont alapon működő dinamikus trönkprotokoll (Dynamic Trunking Protocol, DTP) végzi. A DTP a Cisco szabadalmaztatott protokollja, amely a Catalyst 2960 és Catalyst 3560 sorozatú kapcsolókon automatikusan engedélyezve van.

Egy kapcsoló gyári alapértelmezett állapotának és az 1-es alapértelmezett VLAN visszaállításához a következő parancsokat használhatjuk: delete **flash:vlan.dat és**

**erase startup-config.**

A fejezet foglalkozott még a VLAN-ok konfigurációjával, ellenőrzésével és hibakeresésével a Cisco IOS CLI-t használva, valamint a VLAN-ok szempontjából vizsgálta az alapvető biztonsági és tervezési irányelveket.