**2.1.6 VTP**

A Switchek között a **VTP (VLAN Trunking Protocol)** használatával történik a VLAN konfigurációk központi kezelése. A KKK-MLS1 a központi VTP szerver, amely biztosítja, hogy a VLAN információk szinkronban legyenek az összes kapcsolón a központi hálózaton. A VTP használata jelentősen csökkenti a hibalehetőségeket, mivel a VLAN-ok létrehozása és módosítása csak a központi eszközön történik.

A KKK-MLS1 VTP szerverként van konfigurálva, míg a többi eszköz VTP kliensként működik, így azok nem tudják módosítani a VLAN konfigurációkat. A VTP konfigurálása egyszerűsíti a VLAN-ok kezelését, mivel minden módosítás automatikusan továbbítódik az összes érintett eszközhöz. Az eszközök közötti kommunikáció VTP adatcsomagok segítségével történik, amelyeket minden kapcsoló fogad és továbbít.

A VTP domén és verzió megfelelő beállítása elengedhetetlen a hálózatban történő zökkenőmentes VLAN kezeléshez.

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

**2.1.7 STP**

A **STP (Spanning Tree Protocol)** célja, hogy megakadályozza a hurok problémák (looping) kialakulását a hálózatban. A hálózati topológia stabilizálása érdekében az STP egyetlen aktív adatátviteli utat választ a redundáns kapcsolatok közül. Ez a protokoll biztosítja, hogy a hálózaton ne legyenek ciklikus utak, amelyek folyamatos adatforgalmat generálnának, ami a hálózat meghibásodásához vezethetne.

Az STP az **Root Bridge** (gyökérkapcsoló) meghatározásával működik, amely az összes többi eszköz számára alapként szolgál. A Root Bridge-hez kapcsolódó portok lesznek azok, amelyeken keresztül a forgalom irányítható. Ha bármelyik kapcsolat meghibásodik, az STP automatikusan újraépíti az adatútvonalat úgy, hogy elkerülje a hurok kialakulását.

A rendszer folyamatosan figyeli az eszközök közötti kapcsolatokat, és ha szükséges, a portok státuszát (Blocking, Listening, Learning, Forwarding) módosítja, biztosítva a legoptimálisabb adatforgalmat.

**2.1.8 Második rétegbeli redundancia**

A második rétegbeli redundancia célja, hogy biztosítsa a hálózaton belüli folyamatos adatforgalmat akkor is, ha egyes kapcsolatok meghibásodnak. A redundáns eszközök és kapcsolatok alkalmazása lehetővé teszi, hogy a hálózati kommunikáció ne szakadjon meg, ha a fő útvonalak valamelyike elérhetetlenné válik.

**2.1.8.1 LACP**

A **LACP (Link Aggregation Control Protocol)** lehetővé teszi több hálózati kapcsolat kombinálását egyetlen logikai kapcsolattá, amely megnöveli az elérhető sávszélességet és növeli a hálózati redundanciát. Az LACP dinamikusan kezeli az aggregált kapcsolatokat, és automatikusan figyeli azok állapotát. Ha bármelyik link meghibásodik, azonnal eltávolítja azt az aggregált csoportból, és a forgalom továbbra is zavartalanul haladhat a fennmaradó működő linkeken.

A kapcsolatokat az eszközök közötti LACP üzenetek segítségével alakítják ki, és a protokoll folyamatosan ellenőrzi azok állapotát, biztosítva a legnagyobb sávszélesség elérését és a legnagyobb rendelkezésre állást.

A hálózatban a két Multilayer Switch(KKK-MLS1, és KKK-MLS2) között, illetve a két Switch(KKK-SW1, és KKK-SW2) között használtuk.

A képen képernyőkép, szöveg, Betűtípus, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

**2.1.9 Harmadik rétegbeli redundancia**

A harmadik rétegbeli redundancia célja, hogy biztosítsa az IP alapú forgalom folyamatos elérhetőségét és a hálózati útvonalak redundanciáját. A harmadik rétegbeli redundancia különböző technikákkal, például redundáns útvonalakkal és protokollokkal valósítható meg, amelyek automatikusan kezelik a meghibásodásokat, és biztosítják a legjobb elérhetőséget.

**2.1.9.1 Redundáns kapcsolatok**

A redundáns kapcsolatok használata biztosítja, hogy ha az egyik útvonal meghibásodik, akkor a hálózati eszközök automatikusan átváltanak egy másik, elérhető útvonalra. A redundáns kapcsolatok révén a forgalom folyamatosan halad, és nem fordul elő hálózati kiesés.

A rendszer dinamikus útválasztási protokollokat használ, hogy figyelemmel kísérje a hálózati topológia változásait, és ha bármelyik útvonal elérhetetlenné válik, azonnal új útvonalat választ.

**2.1.9.2 HSRP**

A **HSRP (Hot Standby Router Protocol)** lehetővé teszi a hálózat számára, hogy egyetlen virtuális IP címet használjon, miközben két vagy több útválasztó működik együtt. A HSRP biztosítja, hogy ha az aktív útválasztó meghibásodik, a forgalmat automatikusan átirányítja egy standby útválasztóra, ezzel biztosítva a folyamatos elérhetőséget.

A HSRP működése úgy történik, hogy az egyik útválasztó aktív szerepet vállal, míg a többi eszköz standby állapotban marad. Amikor az aktív útválasztó elérhetetlenné válik, a rendszer azonnal átirányítja a forgalmat egy másik eszközre, amely átveszi az aktív szerepet.

A hálózatban a KKK-MLS1 Multilayer Switch tölti be az aktív szerepet, míg a standby szerepet a KKK-MLS2 Multilayer Switch tölti be.

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

**2.1.10 OSPFv2, OSPFv3**

Az **OSPF (Open Shortest Path First)** egy dinamikus útválasztási protokoll, amelyet leginkább nagyobb, IP alapú hálózatokban alkalmaznak. Az OSPF link state alapú, és biztosítja a hálózati eszközök közötti hatékony adatforgalmat és gyors hibaelhárítást.

* **OSPFv2**: Az **OSPFv2** az IPv4 alapú hálózatok számára lett kifejlesztve. Ez a verzió link state protokollként működik, és minden eszköz folyamatosan szinkronizálja az útválasztási adatbázisát, hogy a legoptimálisabb útvonalakat válassza.

A képen szöveg, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

* **OSPFv3**: Az **OSPFv3** az IPv6 alapú hálózatokban való használatra lett kifejlesztve. Az OSPFv3 továbbfejlesztett funkciókkal rendelkezik az IPv6 címek kezelésére, és képes támogatni a szélesebb címzési struktúrákat is.

Mindkét verzió ugyanazzal az alapvető működési elvvel rendelkezik, amely az eszközök közötti kapcsolatokat figyeli, és az adatforgalom számára a legoptimálisabb útvonalat választja. Az OSPF segítségével gyorsan lehet alkalmazkodni a hálózatban történő változásokhoz, biztosítva ezzel a megbízhatóságot és az elérhetőséget.