Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Oláh Márk

SZEPARÁLT ESZKÖZMENEDZSMENT HÁLÓZAT FEJLESZTÉSE A RICHTER GEDEON VEGYÉSZETI GYÁR INFORMATIKAI HÁLÓZATÁN

EGYETEMI KONZULENS

Dr. Holczer Tamás

VÁLLALATI KONZULENS

Boór András

BUDAPEST, 2021

SZAKDOLGOZAT FELADAT

Oláh Márk

szigorló üzemmérnök informatikus hallgató részére

Szeparált eszközmenedzsment hálózat fejlesztése a Richter Gedeon Vegyészeti Gyár informatikai hálózatán

Informatikai hálózataink csomópontjaiban álló forgalomirányító és kapcsoló eszközök kulcsfontosságú szerepet játszanak a forgalom helyes és biztonságos továbbításában. Annak érdekében, hogy kritikus hálózati problémák fennállása esetén is képesek legyünk kezelni ezen eszközök beállításait és folyamatosan információt kaphassunk az állapotukról szükség van egy az üzleti forgalomtól szeparált hálózatra, mely fő feladata az előbb felsorolt funkciók biztosítása függetlenül a produktív hálózat állapotától.

A hallgató feladata a vállalatnál már korábban is alkalmazott menedzsment célú hálózat továbbfejlesztése. A feladat részletesen a következő:

- Ismerje meg a vállalat menedzsment eszközeinek topológiáját és konfigurációikat.
- Mérje fel a vállalat menedzsment hálózatát és tegyen javaslatot annak átalakítására.
- Készítsen tervet a javasolt átalakítások elvégzésére.
- Végezze el a tervezett változtatásokat és tesztelje az így kialakított új hálózatrészeket.

Tanszéki témavezető: Dr. Holczer Tamás, adjunktus
Vállalati konzulens: Boór András, Richter Gedeon Nyrt.

Budapest, 2021. március 2.

Dr. Imre Sándor
egyetemi tanár
tanszékvezető

Konzulensi vélemények:

Tanszéki konzulens: ☐ Beadható, ☐ Nem beadható, dátum: aláírás:

Vállalati konzulens: ☐ Beadható, ☐ Nem beadható, dátum: aláírás:

Tartalomjegyzék

HALLGATÓI NYILATKOZAT

Alulírott **Oláh Márk**, szigorló hallgató kijelentem, hogy ezt a szakdolgozatot meg nem engedett segítség nélkül, saját magam készítettem, csak a megadott forrásokat (szakirodalom, eszközök stb.) használtam fel. Minden olyan részt, melyet szó szerint, vagy azonos értelemben, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Hozzájárulok, hogy a jelen munkám alapadatait (szerző(k), cím, angol és magyar nyelvű tartalmi kivonat, készítés éve, konzulens(ek) neve) a BME VIK nyilvánosan hozzáférhető elektronikus formában, a munka teljes szövegét pedig az egyetem belső hálózatán keresztül (vagy hitelesített felhasználók számára) közzétegye. Kijelentem, hogy a benyújtott munka és annak elektronikus verziója megegyezik. Dékáni engedéllyel titkosított diplomatervek esetén a dolgozat szövege csak 3 év eltelte után válik hozzáférhetővé.

Kelt: Budapest, 2021. 05. 23.

...……
Oláh Márk

Összefoglaló

A számítógépes és ipari termelőhálózatok fejlődése nemcsak a végponti vagy a csomóponti eszközök tulajdonságainak javulásában, de a hálózatot alkotó eszközök számának emelkedésében is megnyilvánul. Emellett a nagyobb vállatok, mint amilyen a Richter Gedeon Vegyészeti Gyár is sok esetben rendelkeznek a több telephellyel azokon belül pedig több különálló szerverhelyiséggel. Ez az elosztott struktúra megbízhatóbbá teszi az üzemeltetést, azonban felveti az eszközök kezelésének kérdését. Több lehetséges megoldás is létezik arra vonatkozóan, hogy milyen módon lehet egy hálózat elemeiről adatot gyűjteni vagy távolról hozzáférni a kezelőfelületükhöz. A legkönnyebben kialakítható és a leginkább költséghatékony, ugyanakkor a legkevésbé robosztus megoldás, amikor a hálózat már használatban lévő kapcsolatait használjuk erre a célra és az üzleti forgalom csatornáin keresztül valósítjuk meg a menedzsment funkciókat. A fent említett társaság továbbfejlesztette az előbb ismertetett kialakítási sémát, oly módon, hogy a kulcsfontosságú eszközei mellé külön telepített hálózati kapcsolókat a menedzsment forgalom továbbítására. A feladatom, hogy a meglévő menedzsment hálózatot továbbfejlesszem egy olyan megoldássá, ahol az eszközök elérésével és megfigyelésével kapcsolatos forgalom teljes mértékben elkülönül az üzleti forgalomtól. Ennek létrehozásához felmérem és meghatározom a menedzsment hálózat azon központi eszközeit, amelyeket felhasználva a lehető legkevesebb topológiaváltozással elérhetem a kívánt eredményt. A kivitelezés során telepítek új hálózati eszközöket, létrehozok új kapcsolatokat telephelyek között és ahol szükséges forgalomirányítási protokollok használatát vezetem be közben pedig törekszem a redundancia megvalósítására.

Abstract

The evolvement of the computer and industrial producer networks not only shows in the endpoint or the node devices features improvement but also in the increasing number of devices forming the network. In addition to that larger companies such as Richter Gedeon Chemical Factory has more parks in most cases and inside those has more individual server rooms. This spaced structure makes the operation more reliable, however it also raises the question of managing the devices. There are different possible solutions for collecting data about the elements of the network or accessing remotely their console interface. The most easily built, cost effective and the least robust solution is when we use those connections in the network for this purpose which are already in use and we execute the management functions through production links. The company mentioned above has improved the formation scheme in a way that besides all its key devices it installed network switches in order to transmission the management functions. My task is to further develop the already existing management network so all the access links of the devices and the monitoring links of them will be separated from the production links. In order to achieve that I analyse and specify the management networks central devices and by using those I can accomplish the desired goal with the least possible topology changes. Through the implementation I install new network devices, I make new connections between parks and where it is necessary, I apply routing protocols while I aspire to make redundancy happen.

1 Rövidítések listája

AAA: Authentication, Authorization, Accounting

ACL: Access Control Lists

ARP: Address Resolution Protocol

BDR: Backup Designated Router

BPDU: Bridge Protocol Data Unit

CDP: Cisco Discovery Protocol

Cisco ASA: Cisco Adaptive Security Appliances

Cisco ISE: Cisco Identity Services Engine

Cisco WSA: Web Security Appliance

DR: Designated Router

DWDM: Dense Wavelenght Division Multiplexing

EIGRP: Enhanced Interior Gateway Routing Protocol

FC: Ferrule Connector

GBIC: Gigabit Interface Converter

Gbps: Gigabit per secundum

HSRP: Hot Standby Router Protocol

ICMP: Internet Control Message Protocol

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

IP: Internet Protocol

IPS: Intrusion Prevention System

ISL: Inter Switch Link

LC: Lucent Connector

LED: Light Emitting Diode

LLDP: Link Layer Discovery Protocol

LSA: Link-State Advertisement

MAC: Media Access Control

MIB: Management Information Base

NAS: Network Access Server

NMS: Network Management System

NTP: Network Time Protocol

OOB: Out-of-Band

OSPF: Open Shortest Path First

RADIUS: Remote Authentication Dial-In User Service

RFC: Request For Comments

RX: receiver

SC: Subscriber Connector

SFP: Small Form-factor Pluggable

SMF: Single Mode Fiber

SNMP: Simple Network Management Protocol

SNTP: Simple Network Time Protocol

SSH: Secure Shell Protocol

STA: Spanning-Tree Algorithm

STP: Shielded Twisted-Pair

STP: Spanning Three Protocol

TACACS+: Terminal Access Controller Access Control System Plus

TCP: Transmission Control Protocol

TX: transmitter

UDP: User Datagram Protocol

UPS: Uninterruptible Power Supply

UTC: Universal Time Coordinated

UTP: Unshielded Twisted-Pair

VLAN: Virtual Local Area Network

VPN: Virtual Private Network

2 Bevezetés

Az egyetemi gyakorlatomat a Richter Gedeon Vegyészeti Gyár Network & Security csapatának tagjaként töltöttem. A két féléven át tartó munka során véleményem szerint sokféle feladattal találkoztam, amelyek között akadtak olyanok, melyek jó szervezőképességet, míg mások stabil elméleti vagy gyakorlati tudást igényeltek. Az ott eltöltött gyakorlati idő alatt végzett munkám legjelentősebb részét egy olyan projekt megvalósításával töltöttem, amelynek köszönhetően rengeteg új ismeretet szereztem, a meglévőket pedig elmélyíthettem. Szakdolgozatomban ezen ismeretek széleskörű bemutatásával kívánok kísérletet tenni a *„Szeparált eszközmenedzsment hálózat fejlesztése a Richter Gedeon Vegyészeti Gyár informatikai hálózatán”* téma legalaposabb szakmai megvilágítására.

2.1 Feladat előzményei

A Richter Gedeon Vegyészeti Gyárnak gyógyszeripari vállalat lévén az egyik lefontosabb mozgatórugója az innováció. Az innováció teszi lehetővé, hogy termékei megfeleljenek a folyamatosan változó világ igényeinek. Ebben nyújt segítséget a modern technika, amely szintén megállás nélkül fejlődik, egyre hatékonyabbá és egyre inkább nélkülözhetetlenné válik. Következésképpen a vállalat jelentős méretű informatikai rendszert üzemeltet annak érdekében, hogy a termelési és kutatási munkálatok a lehető legjobb eredményeket érjék el.

Jelentős méretű hálózat alatt, olyan komplex rendszert értek, amely több telephellyel és gyárteleppel, azokban több kialakított szerverhelyiséggel és terepi rendezőszekrénnyel, a szerverhelyiségeken belül pedig számos szerverrel, hálózati eszközzel rendelkezik. Az előbbiekben említett helyiségek és a bennük található eszközök célja a megosztott erőforrások hozzáférhetőségének és az egymás közötti, illetve a vállalaton kívüli kommunikációnak a biztosítása a végfelhasználók számára. Végfelhasználók pedig nem csak alkalmazottak lehetnek, de akár termelőrendszerek is, melyek adatokat mentenek szerverekre. Így belátható, hogy a nagyságrendileg több ezer munkaállomást kiszolgáló hálózat kezeléséhez szükséges a – helyes működés szempontjából nélkülözhetetlen – hálózati eszközökhöz és szerverekhez való távoli hozzáférés, más szóval a menedzselhetőség lehetővé tétele. Erre azért van szükség, mert a hálózaton fellépő hibák esetén, egy fizikailag távollévő például hálózati kapcsoló

(switch) kezelőfelületét vagy naplózott eseményeinek kimutatását a lehető leghamarabb el kell érniük a hálózat karbantartóinak ahhoz, hogy megkezdhessék a hiba okának felderítését, majd megszűntetését. A menedzselhetőség problémájának megoldására több lehetőség is van. Léteznek költséghatékony, de kevésbé megbízható, valamint meglehetősen költséges megoldások, melyek kiépítése sok munkával jár, ugyanakkor megbízható menedzsment hálózatot eredményeznek. Ezen megoldásokat részletesen a felhasznált technológiák In-Band és Out-of-Band menedzsment hálózatok alfejezeténél ismertetem. A RG Vegyészeti Gyár természetesen rendelkezik menedzsment hálózattal, tehát a kritikus eszközök kezelése, folyamatos felügyelete már az érkezésemkor is biztosított volt.

A továbbiakban szeretném bemutatni hogyan épül fel ez a hálózat. A tevékenységem a vállalat budapesti telephelyeire korlátozódik, így más magyarországi vagy külföldi telephelyek menedzsment megoldásait jelen szakdolgozatban nem vizsgálom. A vállalat minden telephelyének szerverhelyiségében és rendezőszekrényében telepítésre került legalább egy darab csak és kizárólag menedzsment forgalom továbbítására használt switch. Ezen eszközök hozzáférési (access) portjai végpontok – például szerverek – menedzsment interfészére csatlakoznak, emellett más menedzsment switchre is kapcsolódhatnak attól függően, hogy mi az adott eszköz szerepe a menedzsment hálózatban amellett, hogy végponti készülékeket kapcsol ahhoz. Minden így kapott menedzsment alhálózat kapcsolódik egy, hozzá logikailag tartozó disztribúciós switchhez. Az OSI modell szerinti adatkapcsolati rétegen értelmezett topológiát a harmadik réteghez tartozó funkciók számára is elérhetővé kell tenni, vagyis az útválasztásban (routing) résztvevő eszközök (ebben az esetben a disztribúciók) számára azonosíthatóvá kell tenni, hogy azok információt szolgáltathassanak a többi résztvevőnek az alhálózat elhelyezkedéséről és a benne található állomásokról. Ennek megoldására mind az állomások menedzsment interfészeit, mind az L2-es menedzsment switchek megfelelő VLAN-hoz tartozó VLAN interfészeit IPv4 címekkel látták el. A különböző lokációkból és ezzel a különböző disztribúciókhoz csatolt menedzsment alhálózatok címei eltérő címtartományokból kerültek kiosztásra. Végül a Routing és az interfész beállítások elvégzése után létrejött a vállalat menedzsment hálózata, amelyen keresztül megvalósul az SSH kapcsolat, a logserver-re való naplózás, az NTP, a TACACS+ és más szolgáltatások használata, melyekről részletes információk a Felhasznált technológiák című fejezet megfelelő alfejezeteiben olvashatók. Az előzőekben ismertetett

menedzsment célú hálózat megbízhatósága abban rejlik, hogy annak forgalmának továbbítása dedikált menedzsment switchek, disztribúciók és a produktív hálózat gerinc eszközein és linkjein keresztül történik. Produktív hálózat alatt azokat a hálózati eszközöket és kapcsolatokat értem, amelyek a tényleges üzleti célú forgalmat továbbítják. Ennek a kialakításnak az az előnye, hogy így a menedzsment hálózat központi elemei ugyanazzal a redundanciával rendelkeznek, mint a produktív hálózat, lévén, hogy ugyanarról a gerincről van szó, továbbá nem volt szükség saját menedzsment gerinc kialakítására. A hátránya pedig az, hogy a produktív hálózat csomópontjain történő kiesés esetén a menedzsment hálózat részei vagy egésze is elérhetetlenné válhat.

2.2 Feladat ismertetése

Az előző alfejezetben rögzített ismertető után véleményem szerint könnyedén belátható, hogy bár a RG Vegyészeti Gyár menedzsment hálózata jelenlegi állapotában is hatékonyan képes üzemelni, mégis szükség lehet ennek fejlesztésére. Ebben az alfejezetben részletesen leírom, mit foglal magába a menedzsment hálózat fejlesztése és milyen célom társul hozzá.

Mint azt már megjegyeztem korábban, a jelenlegi menedzsment hálózat nem teljes mértékben független a produktív hálózattól. Akkor válna azzá, ha a hálózat illetékes üzemeltetői az üzleti hálózattól szeparált menedzsment csomópontokon keresztül is képesek lennének kontrollálni minden, az infrastruktúra működése szempontjából nélkülözhetetlen elemet. A teljes mértékben szeparált menedzsment hálózathoz szükség van különálló gerinchálózatra, melynek van kapcsolata az összes menedzsment alhálózattal, a produktív hálózattal és valamilyen VPN megoldással, amely a hálózaton kívüli irányból is lehetővé teszi a hálózat kezelését. A produktív hálózattal való kapcsolattartás nem merül ki a csomópontok menedzsment elérésében. Olyan eléréseket is biztosítani kell az új menedzsment hálózatnak, ami korábban szinte természetesen adott volt. Gondolok itt TACACS vagy RADIUS szerverek elérésére, amelyek tipikusan egy szerverek számára kialakított alhálózatban helyezkednek el, vagy éppen egy központi logserver elérése is ide tartozik.

A megvalósítás részét képezi a jelenlegi menedzsment alhálózatok kapcsolatainak, függőségeinek felmérése is. A felmérést dokumentálni kell, hogy a tervezési fázisban, minden ismeret könnyen elérhető legyen. Ennek legegyszerűbb módja egy átfogó hálózati rajz készítése, amely tartalmaz minden szükséges információt. A

felmérések elvégzéséről és a tervrajzok megalkotásának folyamatáról a későbbi fejezetekben lesz szó.

A felmérések és az azokból készült tervek után kezdődhet az új menedzsment hálózat központi alappilléreinek felépítése. Ez fizikai eszköztelepítéssel, kábelezéssel és szoftveres beállításokkal is jár. Ha a gerinchálózat már üzemkész, akkor a következő lépés a különböző menedzsment alhálózatok leválasztása a produktív hálózatról és csatolása az új menedzsment hálózathoz. Ez a fázis az alhálózatok részletes feltérképezését igényli és jól átgondolt terv szerint kell végrehajtani, ugyanis az itt felmerülő esetleges hibák egy-egy alhálózat tartós kiesését okozhatják. A művelet sikerességének másik fontos összetevője a tesztelés. Minden menedzsment sziget átállásánál ellenőrizni kell annak helyes működését, annak eddig is működő szolgáltatásainak elérhetőségét. Amennyiben a teljes menedzsment hálózat már a szeparált gerincen keresztül működik, úgy végső feladatként megtervezhető és kivitelezhető a hálózat redundáns összeköttetéseinek létrehozása. Természetesen, ezt a feladatot az alhálózatok csatolásával együtt is el lehet végezni, azonban prioritás szempontjából csak másodlagos lehet.

A menedzsment hálózat fentiekben részletezett fejlesztésének célja, egy olyan menedzsment hálózat létrehozása, amely eszközmenedzsment szempontjából független a produktív hálózattól. Ez maga után vonja azt a tényt, hogy a fejlesztés egy megbízhatóbb topológiát eredményez, amely kritikus meghibásodások esetén kontrollt biztosít a legtöbb hálózati eszköz felett.

3 Felhasznált technológiák

3.1 Cisco switchek

A most következő alfejezetben bemutatom azokat a hálózati eszközöket, amelyeket a munkám során telepítettem és amelyek jellemzően az általam továbbfejlesztett menedzsment hálózatot alkotják. A vállalat által vásárolt és jelenleg is használatban lévő hálózati kapcsolók döntő többsége a Cisco Systems gyártótól származik. Ennek okán én is Cisco gyártmányú eszközökkel dolgoztam. Az új modellek kiválasztásához, figyelembe vettem a kiválasztandó eszköz jövőbeli funkcióját és a gyártó által megadott paramétereit. Azonban nem minden esetben volt szükség új modellek kiválasztására és telepítésére. Sok esetben megfelelő megoldásnak bizonyult a jelenleg is üzemben lévő menedzsment célú eszközök felhasználása. A választás részletesebb leírása a Menedzsment hálózat fejlesztése című fejezetben olvasható.

3.1.1 Cisco SG 300 szériás (small business) switch

A gyártó célja a széria megalkotásával, hogy a kisvállalatok által is megfizethető ár mellett kínáljon mind támogatott szolgáltatások, mind kapacitás terén megfelelő terméket.

3.1.1.1 Szolgáltatások

A Cisco SG 300 sorozatú eszközökben is megtalálható a legtöbb olyan funkció és szolgáltatás, ami egy kisebb hálózat hatékony működtetéséhez szükséges. A sorozat az OSI modell szerinti második, adatkapcsolati réteghez (L2) tartozó funkciók (például STP, VLAN) döntő többségét megvalósítja, viszont a harmadik, hálózati réteghez (L3) tartozó funkciókat nem támogatja. Ugyanakkor van lehetőség VLAN interfészek létrehozására, amelyek így IP címmel elláthatók és statikus útválasztási (routing) bejegyzések is megadhatók. A dinamikus routing protokollok (OSPF, EIGRP) viszont nem alkalmazhatók az eszközökön. A biztonsággal kapcsolatos szolgáltatások közül érdemes kiemelni az SSH protokoll, a TACACS és a RADIUS biztonsági megoldások meglétét (v1.2.7.76 szoftver verziótól), a menedzsment területén pedig az SNMP (1., 2c és 3. verzió) támogatást vagy a keretrendszer frissítésének lehetőségét akár a weben keresztül.

3.1.1.2 Teljesítmény

A SG 300 széria a forgalomtovábbítás sebessége szempontjából is a kisebb irodák igényeit szem előtt tartva készült, így az elérhető változatok access, vagyis azok a portok, amelyek tipikusan egy kisebb lokális hálózatot kapcsolnak az eszközhöz, maximális sávszélessége 1 Gigabit per szekundum (Gbps). Az Uplink, vagyis azok a portok, amelyek jellemzően egy kisebb lokális hálózatból egy nagyobb hálózat felé biztosítanak kapcsolatot, szintén 1 Gbps maximális átviteli sebességre képesek, de az RJ-45 portok mellett elérhető SFP (Small Form-factor Pluggable) modul csatlakoztatására alkalmas interfész is.

3.1.1.3 Értékelés

A fentebb ismertetett jellemzők alapján, az SG 300 sorozat a kisebb irodák hálózati követelményeinek eleget tesz. Azonban a Richter Gedeon Vegyészeti Gyár hálózatának hatékony működtetéséhez a legtöbb esetben nagyobb átviteli sebesség, redundancia és feladatátvételi (failover) megoldások, multilayer, azaz L2 és L3 funkcionalitásra is képes eszközök szükségesek. Ugyanakkor a vállalat kis számban alkalmaz SG szériás eszközöket a menedzsment alhálózatokban az egyes szerverhelyiségek eszközeinek csatlakoztatására.[1]

3.1.2 Cisco Catalyst 9200 szériás switch

A termékcsalád sokkal több nagyvállalatok számára fontos tulajdonsággal rendelkezik, mint az előzőekben tárgyalt SG széria. Széles funkcionalitásuk a hálózat egyszerűbb üzemeltetését teszik lehetővé, ennek eléréséhez azonban több szakértői tudás szükséges, mint a small business eszközök kezeléséhez.

3.1.2.1 Szolgáltatások

Talán a legfontosabb tulajdonsága ezen modelleknek, hogy képesek multilayer eszközként működni, vagyis támogatják a dinamikus routing protokollok alkalmazását. Emellett természetesen minden olyan funkcióval rendelkeznek, amellyel az SG széria is.

3.1.2.2 Teljesítmény

Modelltől függően az uplink portokon akár 10 vagy 25 Gbps sávszélesség is megvalósítható, illetve egyes modelleknél ezek a portok cserélhető hálózati modulokként vannak jelen, így például az 1 Gbps teljesítményű modul cserélhető tízesre. A

skálázhatóság kérdésének megoldására lehetőséget biztosítanak backplane stacking-re, vagyis két eszköz összekapcsolására oly módon, hogy azok logikailag egy eszközként funkcionáljanak. A stack-ben résztvevő switchek közötti sávszélesség akár 160 Gbps is lehet.

Fontosnak tartom megjegyezni, hogy ezek az eszközök moduláris tápegységgel és ventilátorral rendelkeznek és redundáns tápellátás kialakítására is alkalmasak. Ezen tulajdonságuk miatt is megbízhatóbbak az SG szériánál.

3.1.2.3 Értékelés

A Cisco Catalyst 9200 termékcsalád fejlett hardveres és szoftveres funkciókat foglal magába. Rendelkezik a redundancia, feladatátvétel és a modularitás eszközeivel. Ezen tulajdonságok alkalmassá teszik, hogy nagyvállalati környezetben hozzáférési (access) szerepkör mellett például egy menedzsment alhálózat csomópontja, disztribúciós eszköze legyen. Ezért a vállalat menedzsment hálózatán végzett munkám során a vállalati konzulensemmel, Boór Andrással közös megegyezés alapján Cisco Catalyst 9200L és Catalyst 3850 switcheket használtunk fel a menedzsment hálózat gerincének felépítéséhez. A C3850 sorozatú eszközöket a következőkben nem mutatom be, mivel az szintén a Catalyst termékcsalád tagja. Lényeges különbségként az interfészek kapacitását emelném ki.[2]

3.2 Nem menedzselhető switch

A nem menedzselhető switchek, olyan hálózati eszközök, amelyek konfigurációs beállítások nélkül képesek hálózati kapcsolatot biztosítani több eszköz számára. Ehhez mindössze tápellátásra és a megfelelő hálózati kábelek csatlakoztatására van szükség. A feladatom megvalósítása közben felfedeztem ilyen, a hálózatban aktívan üzemelő eszközt, amelynek néhány jellemzőjét azért ismertetem, hogy az itt felvázolt szempontok megindokolják azt a döntésemet, miszerint a felfedezett eszközt meg kell szüntetnem.

A nem menedzselhető switchek telepítése meglehetősen egyszerű feladat, viszont nem elérhető rajtuk semmilyen funkció, ami egy menedzselhető eszközön igen. Akkor lehet célszerű alkalmazni egy ilyen eszközt, ha a hálózat kapacitásának növelése más módon, például új menedzselhető switch üzembehelyezésével vagy Stack kialakításával nem megoldható. Ennek oka lehet, hogy az imént felsorolt megoldások költsége jelentősen nagyobb a nem menedzselhető switcheknél vagy éppen a bővítés csak

ideiglenes, ilyen esetben egy nem menedzselhető switch telepítése is jó megoldás lehet, később pedig könnyen elbontható. Tehát a nem menedzselhető, vagy mini switchek egyszerű és költséghatékony megoldást kínálnak, azonban mégsem számít jó megoldásnak a használatuk különösen nagyvállalati környezetben.

Ahogy azt már korábban is említettem, nincs lehetőség beállításokat végezni az eszközökön, így nem támogatják a vállalati környezetben nélkülözhetetlen VLAN, STP, SNMP és az NTP protokollokat sem. Ebből következik, hogy nincs lehetőség az eszközök központi felügyeletére sem. CDP és LLDP protokollok támogatásának hiányában az ilyen eszközök detektálása jóformán csak manuálisan készített dokumentáció alapján lehetséges.

Röviden összefoglalva a nem menedzselhető switchek olcsó megoldást kínálnak kisebb irodák vagy otthonok eszközeinek összekapcsolására, de nagyvállalati környezetben, ahol az eszközök felügyelete és beállításainak kezelése elengedhetetlen, ezen megoldás elkerülésére kell törekedni. A felfedezett nem menedzselhető switchet tehát megszüntetem, mert az általa a menedzsment hálózathoz kapcsolt eszközök számára van a közvetlen közelében megfelelő menedzsment eszköz.[3]

3.3 Hálózati kábelek

Ezen alfejezetben kívánom összefoglalni az Ethernet hálózatok kábelezéséhez köthető ismereteimet, amelyek közül is a gyakorlati munkám alatt alkalmazott megoldásokat fejtem ki részletesen.

Az Ethernet hálózat kábelezésének szabványait az IEEE 802.3[17] szabványgyűjtemény rögzíti. Két fő eleme van, az összekötő média és a hálózati csomópontok, melyek közül az összekötő média rész írja le a kábelekre vonatkozó előírásokat, míg a hálózati csomópontok fejezet az útválasztókra (router) és a kapcsolókra tartozó elvárásokat rögzíti.[6]

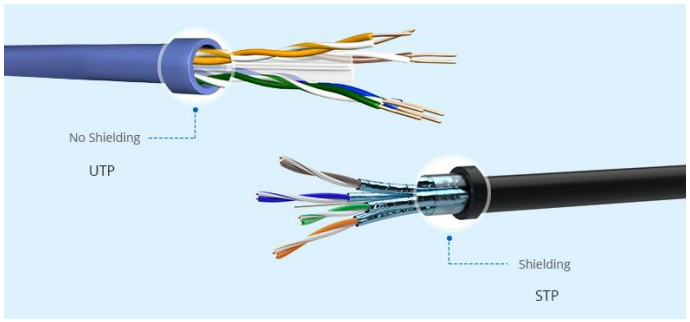
3.3.1 UTP (Unshielded Twisted-Pair) kábel

Magyarul árnyékolatlan csavart érpáras kábel. Ezt a kábeltípust kifejezetten számítógépes hálózatok kialakításához tervezték. A kábel belsőjében nyolc, rézből készült vezeték található, amelyek színes szigetelőanyaggal vannak bevonva annak érdekében, hogy a vezetékek vagy erek azonosíthatók legyenek. Négy különböző színű ér található egy kábelben (kék, barna, zöld, narancssárga) és mindegyik színű érhez

tartozik egy ugyanolyan színű csíkozott ér is, amelyen a csíkozást a fehér szín adja. A színes erek a csíkozott párjukkal összesodorva helyezkednek el a kábelben, innen ered a csavart érpár elnevezés. A különböző érpárok különböző mértékű összesodrásának az interferencia csökkentésében van fontos szerepe. Az összesodrott érpárok egy külső borítással vannak bevonva. Ilyen kábeleket használ a vállalat az állomások menedzsment interfészeinek csatolására a menedzsment hálózathoz.[4]

3.3.2 STP (shielded Twisted-Pair) kábel

Magyarul árnyékolt csavart érpáras kábel. Ezen kábel kialakítása hasonló az előzőéhez, azonban itt az érpárok egy plusz szigetelő fóliába vannak burkolva. Ennek köszönhetően védettebbek az elektromágneses és a rádiófrekvenciás interferenciával szemben, ami magasabb átviteli sebességet tesz lehetővé.[4]



1. ábra: Az UTP és az STP kábel összetétele.[5]

A csavart érpáras kábelek RJ-45 (registered jack) csatlakozókat használnak. A csatlakozóban található pinek bekötésére két alapvető szabvány is vonatkozik, amelyek a T568A és T568B szabványok. A csavart érpáras kábelek a következő kategóriákba sorolhatók frekvenciájuk és jelszint-zaj rátájuk (signal-to-noise ratio) alapján: Cat 3, Cat 4, Cat 5, Cat 5e, Cat 6, Cat 6a, Cat 7, Cat 7a és Cat 8. A Cat egy szabvány, ami az adott kategóriával kapcsolatos elvárásokat írja le. A kategóriák pontos specifikációit a 2. ábrán látható táblázat ismerteti. A táblázatban szereplő Cat szabványok rövidtávú adatátvitelre érvényesek (100 méter).[5]

Category	Typical Construction	Max Bandwidth	Transmission Speeds	Applications
Cat 3	UTP	16 MHz	10Mbps	10BASE-T and 100BASE-T4 Ethernet
Cat 4	UTP	20 MHz	16Mbps	16Mbit/s Token Ring
Cat 5	UTP	100 MHz	10-100Mbps	100BASE-TX & 1000BASE-T Ethernet
Cat 5e	UTP	100 MHz	1000Mbps-1Gbps	100BASE-TX & 1000BASE-T Ethernet
Cat 6	STP	250 MHz	10Gbps (55m)	10GBASE-T Ethernet
Cat 6a	STP	500 MHz	10Gbps (55m)	10GBASE-T Ethernet
Cat 7	STP	600 MHz	100Gbps (15m)	10GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable
Cat 7a	STP	1000 MHz	100Gbps (15m)	10GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable
Cat 7a	STP	2000 MHz	4Gbps (30m)	40GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable

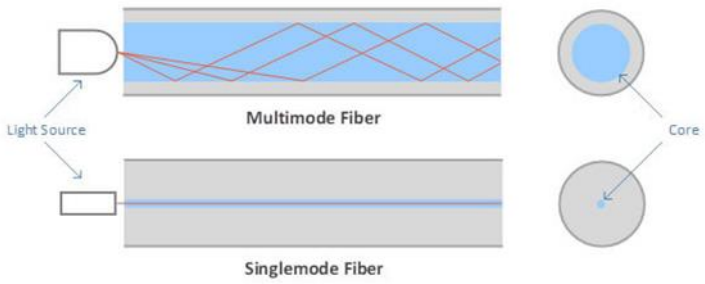
2. ábra: Összefoglaló táblázat az UTP és STP kábelek kategóriáinak jellemzőiről.[5]

3.3.3 Optikai kábel

Az optikai kábel az adatokat fényimpulzusként továbbítja egy rugalmas, optikailag tiszta üvegből vagy műanyagból készült szálon keresztül. Ez a technológia gyorsabb adatátvitelt tesz lehetővé hosszabb távokon is, emellett nem érvényes rá a rézalapú kábeleknél fennálló interferencia probléma.

A fényimpulzusok az optikai kábel magján haladnak keresztül, visszaverődve az oldalakról. A fényforrás kivételével (LED) nincs szükség áramellátásra a jel továbbításához. A fényimpulzusok több kilométeres távolságokon keresztül sem gyengülnek el, vagyis nincs szükség a jel regenerálására.

A mag átmérője meghatározza, hogy mekkora távolságra képes egy kábel megbízhatóan továbbítani az adatokat. A kisebb átmérőjű maggal rendelkező kábelek nagyobb távolságokra képesek továbbítani regenerálás nélkül, mint a nagyobb átmérőjű maggal ellátott médiumok. Az egymodusú kábelek (Single Mode Fiber vagy SMF) kisebb maggal rendelkeznek (8.3 vagy 9µm), ezért képesek akár 100 km távolságba is továbbítani. A multimodusú kábelek magja jellemzően nagyobb átmérőjű (50 és 62.5µm), ami azt jelenti, hogy képesek több adatot vagy akár több adatfolyamot egyidőben továbbítani, de hosszabb távolságok esetén problémák léphetnek fel a jel minőségével kapcsolatban. Így a multimodusú kábeleket általában épületeken belüli kapcsolatokhoz, míg az egymodusú változatot épületek közötti távolságok áthidalásához alkalmazzák. A két mód között nem csak a mag mérete a különbség, a multimodusú kábel több adatfolyam egyidejű továbbítását teszi lehetővé 850 vagy 1310 nm hullámhosszon. Az egymodusú változat egyszerre egy adatfolyam továbbítását végzi, ehhez pedig 1310 és 1550 nm tartományban működő lézerdiódát használ.[7]



3. ábra: Elvi rajz az egymodusú és multimodusú kábelek magjairól és a bennük közlekedő fény útjáról.[7]

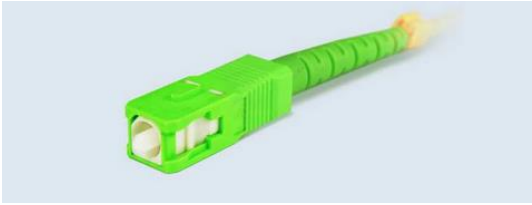
Az optikai kábelek duplexitása lehet simplex vagy duplex. A simplex működés egy optikai szálat használ és azt jelenti, hogy a kábel egyik végén található adó (transmitter vagy TX) küld adatokat a kábel másik végén lévő fogadónak (receiver vagy RX), azonban a visszairányú forgalmazásra nincs lehetőség. Duplex esetben a küldő és a fogadó egyaránt küldhet és fogadhat adatot a médiumon keresztül, amihez ezesetben két optikai szálra van szükség. A duplex kábelek ikercsatlakozói képesek egyidőben küldeni és fogadni is. Ilyen kábeleket gyakran hálózati eszközök összekapcsolására használnak.[7]

A továbbiakban a teljesség igénye nélkül bemutatok néhány optikai kábel csatlakozót, amelyet a munkám során én is használhattam a vállalatnál.

Ferrule Connector (FC) volt az első optikai szálas csatlakozó, amely kerámia hüvelyt használt. Az FC csatlakozókat nagyrészt lecserélték az olcsóbb és könnyebben telepíthető SC és LC csatlakozókra, de a magas rezgésű környezetben továbbra is előnyben részesítik őket a becsavarható reteszük miatt.[7]

4. ábra: A Ferrule Connector (FC).[8]

A **Subscriber Connector (SC)** csatlakozók megbízható, bepattintható reteszelő mechanizmussal rendelkeznek, amely egyszerűbb csatlakoztatást tesz lehetővé, mint az FC csatlakozó. Ez egy olcsó, tartós megoldás, melynek élettartamát 1000 csatlakoztatás körülire becsülik. Az SC csatlakozókat a vállalati hálózatokban többnyire LC csatlakozók váltották fel.[7]



5. ábra: A Subscriber Connector (SC) csatlakozó.[8]

Lucent Connector (LC) csatlakozót úgy tervezték, hogy kiküszöbölje például az SC csatlakozók túlzottan nagy méretét, emellett stabilabb csatlakozást biztosít. Az LC csatlakozók területe körülbelül 50% -kal kisebb, mint az SC csatlakozóké.[7]

6. ábra: A Lucent Connector (LC) csatlakozó.[8]

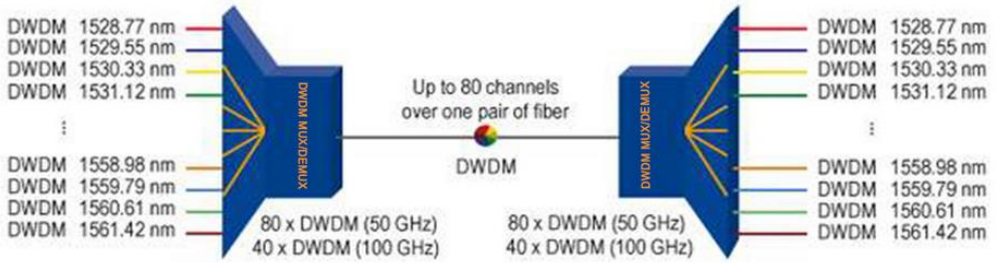
A hálózati kábelek bemutatása után szeretnék az SFP (Small Form-factor Pluggable) modulokról és a DWDM (Dense Wavelenght Division Multiplexing) technológiáról is néhány alapvető információt közölni, mivel fontos szerepet játszanak a menedzsment hálózat kábelezésében.

Az SFP adó-vevő modulok gyorsan illeszthető be- és kimeneti eszközök, amelyek dedikált aljzatokba csatlakoznak. Az adó-vevő összeköti a készülék, például switch elektromos áramkörét a külső optikai vagy réz hálózattal, hogy kiterjessze az útválasztási és kapcsolási funkciókat az egész hálózaton. Az SFP modulok optikai kábelek esetén az LC csatlakozók csatolását teszik lehetővé. Ez meghatározó tényező a kábelezés tervezésénél és megvalósításánál.[9]

7. ábra: Fénykép egy Cisco gyártmányú SFP modulról.[10]

A DWDM technológiák segítségével az optikai összeköttetések adatátviteli kapacitása a többszörösére növelhető, illetve különböző sebességű és protokollokat használó adatfolyamok, például 10GE, Fiber Channel vihetők át egyszerre, egymástól függetlenül ugyanazon az optikai szálon. A technológia alapja, hogy az adatfolyamok

továbbítása eltérő hullámhosszokon történik, amelyeket passzív vagy aktív WDM komponensek fésülnek össze, válogatnak szét és dolgoznak fel.[11]



8. ábra: A DWDM működési elvéről.[12]

Az előbbiekben bemutatott hálózati kábeleket és csatlakozókat aktívan használja a vállalat, ugyanakkor az új hálózatrészek kiépítése során, - mint amilyen az általam fejlesztett menedzsment hálózat is - kizárólag az LC csatlakozóval ellátott mono- vagy multimodusú kábeleket alkalmazzák. Következésképp a tervezési fázisban a vállalati konzulensemmel azt a döntést hoztuk, hogy a menedzsment hálózat fejlesztéséhez kapcsolódó új összeköttetésekre LC csatlakozókban végződtetett egymodusú optikai kábeleket kell alkalmazni. A választáshoz figyelembe vettük, hogy a kapcsolatok megvalósítására használt DWDM hardveregységek 10 Gigabit-es sávszélességet igényelnek, továbbá, hogy az SFP modulok csak az LC csatlakozóval kompatibilisek. Így 10 GigabitEthernet SFP modulokat választottunk és az áthidalni kívánt távolságok alapján egymodusú optikai kábelt.

3.4 Spanning Tree protokoll (STP)

Ebben az alfejezetben szeretném röviden bemutatni a magyarul feszítő faként ismert protokollt, amely fontos szerepet játszik a vállalat menedzsment hálózatának helyes működésében. A feladat megvalósításának tervezési fázisában konkrét példát is mutatok arra, hogy hogyan segíti a protokoll használata az OSI modell második rétegében kialakuló hurkok (a csomagok bent ragadnak a hálózatban és végtelenül keringenek) elkerülését egy redundáns, azaz többszörösen összekötött topológián.

A Spanning tree protocol switchek által használt, az OSI modell szerinti adatkapcsolati réteghez tartozó protokoll. Az STP pontos leírását az IEEE 802.1D[13] szabvány rögzíti. Az elsődleges célja a hurkok kialakulásának megakadályozása. Hurkok például akkor alakulhatnak ki egy hálózatban, amikor a kapcsolatok megbízhatóságát az

eszközök többszörös összekapcsolásával növeljük. Ennek ellenére redundanciára szükség van, ezért STP-t alkalmazunk, ami a redundáns összeköttetések ideiglenes lekapcsolásával segíti a helyes működést.[14]

Ahhoz, hogy az STP felfedezze a redundáns kapcsolatokat (linkeket) egy hálózatban, az STA (spanning-tree algorithm) algoritmust használja, ami először egy adatbázist készít a topológiáról, majd beazonosítja és lekapcsolja a redundáns összeköttetéseket. Ezután már csak az STP által kiválasztott linkek maradnak aktívak. Ha pedig új kapcsolat kerül kiépítésre vagy egy meglévő link megszűnik, akkor a protokoll újra futtattja az STA-t és újra beállítja a kapcsolatokat a változásnak megfelelően. Az STP-ben résztvevő switchek úgynevezett BPDU (Bridge Protocol Data Unit) keretek küldésével terjesztenek információt saját magukról és a kapcsolataikról. Így képesek megtanulni a teljes topológiát. Minden STP topológiában van egy gyökér eszköz (Root Bridge), vagyis egy switch, amelyik a topológia kiinduló pontjául szolgál. A Root Bridge a résztvevő eszközök közül két paraméter alapján kerül kiválasztásra. Ezek a prioritás (bridge prority) és a switch MAC (Media Access Control) címe. A legalacsonyabb prioritással rendelkező switch lesz a gyökér a hálózatban. Egyező prioritás esetén a legalacsonyabb MAC című eszköz tölti be ezt a szerepet. A prioritás alapértelmezett értéke 32768 a Cisco gyártmányú switchek esetében, továbbá van lehetőség a választás befolyásolására oly módon, hogy az alapértelmezett prioritásnál kisebb értékkel felülírjuk a gyári értéket. A gyökér eszköz kivételével minden switch úgynevezett nem gyökér eszköz (Non-Root Bridges) szerepet tölt be. Az ilyen switchek a Root Bridge-től kapott információk alapján frissítik az STP adatbázisukat.

A topológia alakulásának egyik eleme a portköltség (Port Cost), vagyis egy érték, amit az STP a hálózat minden portjához hozzárendel. Az érték segít kiválasztani a legjobb linket, amennyiben két eszköz között több elérhető útvonal is létezik. A kisebb Port Cost-tal rendelkező link lesz az aktív. A Path Cost vagy útvonalköltség a következő összetevője az útvonalak meghatározásának. Értékét a portköltségek összege adja a gyökértől a többi switchig. Mindig a gyökér alapján kalkulálják, tehát az útvonalköltség a gyökérnél nulla. Ezt az információt is BDPU keret továbbítja.

Az STP-ben résztvevő switchek portjainak emellett vannak különleges szerepeik is, amelyek a következők:

- Gyökér (Root) port: Az a port, amelyik közvetlenül csatlakozik a gyökér switchhez.
- Kijelölt (Designated) port: Az a port, amelyen engedélyezett a keretek továbbítása. Ezeket a portokat az adott szegmens portjainak költsége és a gyökérhez való visszatérés költsége alapján választják ki. A gyökér összes portja kijelölt port.
- Nem kijelölt (Non-Designated) port: Azok a portok, amelyek költsége magasabb kijelölt portokénál. Az STP ezeket a portokat blokkoló portoknak jelöli, melyeket a hurkok eltávolítására használ.

Egy STP-t futtató switch összes portja négy állapoton megy keresztül, annak érdekében, hogy részévé váljon a topológiának. Ezek a blokkolás, hallgatás, tanulás és továbbítás (blocking, listening, learning, forwarding states) állapotai. Az állapotok révén a kapcsoló megismeri a topológiát, kiszámítja az útköltséget és kiválasztja a kijelölt és nem kijelölt portokat. Ezen állapotok után a switch már STP konvergens.

A menedzsment hálózat fejlesztésekor, az egyik alhálózat feltérképezésekor szükségesnek láttam az ott kialakított STP topológia értelmezését is. Ennek kulcsa az egyedi portköltségekkel, BPDU filterrel ellátott interfészek meghatározása és a portok szerepeinek (root, designated) átvizsgálása volt. A BDPU filter parancs interfészekre kiadható parancs, amellyel az eszköz nem küld BPDU csomagokat a kiadott interfészen keresztül. A parancs használatának előnyét a tervezési fázisban konkrét példán keresztül szemléltetem.[15]

3.5 Virtuális helyi hálózat (Virtual Local Area Network, VLAN)

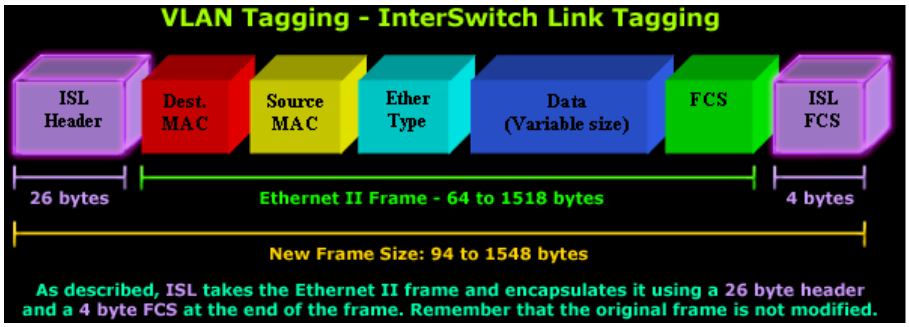
A Spanning tree protokoll mellett a VLAN a másik, OSI modell szerinti második réteghez tartozó konstrukció, amely szervesen kapcsolódik a menedzsment hálózat alhálózatainak összekapcsolásán végzett munkámhoz. Ebből kifolyólag ismertetem a Cisco eszközökben integrált VLAN technológia főbb jellemzőit, amelyeket figyelembe vettem a meglévő VLAN konstrukciók felhasználásakor.

A VLAN-ok alkalmazása a menedzsment hálózaton belül számos előnnyel jár. Különböző VLAN-ok definiálásával az OSI modell szerinti harmadik rétegben létrehozott szeparáció megvalósítható a második réteg szintjén is egy switch portjainak

megfelelő VLAN-okhoz való hozzárendelésével. Más szóval a VLAN-ok használata a switch portjai közötti szeparációt, vagyis külön L2 doménekhez való hozzárendelést tesz lehetővé.

A VLAN terminológiában kétféle interfész működési mód létezik. Ezek az Access és a Trunk módok. Fontos megjegyezni, hogy bármelyik mód használata konfigurált portot igényel. Az Access módra konfigurált port egyetlen VLAN-hoz biztosít hozzáférést, így állomások csatlakoztatására ezt a módot kell választani. Ellenben a Trunk mód egy vagy több VLAN forgalmához biztosít hozzáférést, ezért ezt a módot jellemzően switchek vagy routerek közötti összekapcsolt interfészekre alkalmazzák.

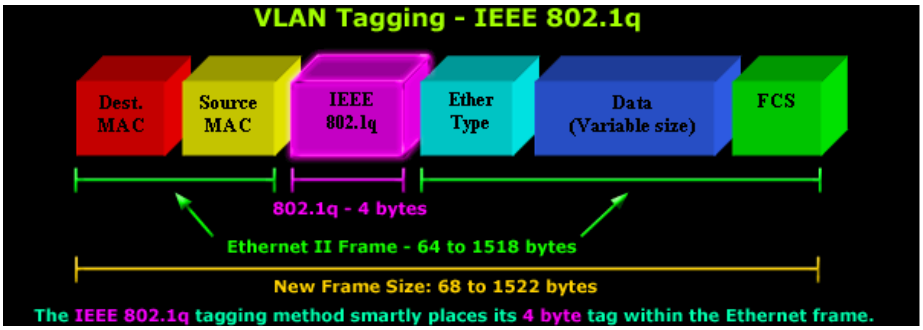
A Trunk mód működéséhez hozzátartozik az úgynevezett VLAN címkézés, más néven Frame Tagging, a Cisco által kifejlesztett ISL (Inter Switch Link) módszer, amely segít a Trunk linkeken keresztül haladó csomagok azonosításában. Ez valójában egy speciális VLAN címke hozzáadását jelenti az Ethernet kerethez, amit a Trunk link végén lévő eszköz eltávolít, majd a megfelelő Access portra küldi.



9. ábra: Az ISL által kiegészített Ethernet keretről.[18]

Az IEEE 802.1Q[16], amelyet gyakran Dot1q néven emlegetnek, az a hálózati szabvány, amely támogatja az IEEE 802.3[17] Ethernet hálózat virtuális LAN-jait. A szabvány meghatározza az Ethernet keretek VLAN címkézési rendszerét, valamint a kapcsolók által az ilyen keretek kezelésénél alkalmazandó kísérő eljárásokat. Hasonló a Cisco megoldásához, de nyílt szabvány lévén sokkal jobb kompatibilitással rendelkezik és több VLAN létrehozását támogatja (1000 helyett 4096), mint a Cisco ISL.

A VLAN címkéknek nem csak a switchek között lehet fontos szerepe, hanem például virtuális állomásokat futtató hardver eszközök bekötése esetén is, ahol a különböző virtuális állomások más-más VLAN-okhoz vannak hozzárendelve.



10. ábra: Az IEEE 802.1Q szabvány szerint kiegészített Ethernet keretről.[18]

Tehát VLAN-ok létrehozása szegmentálja a hálózatot, ezáltal csökkenti a hálózati közvetítéseket és növeli a biztonságot (hozzáférhetőség). Ugyanakkor az így létrehozott VLAN tartományoknak is szüksége lehet alapértelmezett átjáróra. Ehhez szükséges az adott VLAN tartományba tartozó switchen a megfelelő VLAN interfész létrehozása és IP cím beállítása. A tartomány többi eszköze ezt a címet használhatja alapértelmezett átjáróként. A VLAN interfész nem csak arra használható, hogy egy switch alapértelmezett átjáróként működhessen, hanem alkalmazásával menedzsment folyamatok is megvalósíthatók. A vállalat menedzsment hálózatát alkotó switchek is VLAN interfészeket használnak erre a célra.[18]

3.6 Hot Standby Router Protocol (HSRP)

A HSRP a Cisco Systems által kidolgozott redundancia protokoll, amelynek a célja hibatűrő alapértelmezett átjáró létrehozására. A protokoll 1. verzióját az RFC 2281[19] írja le, míg a 2. verziójához nincs RFC. A HSRP tehát biztosítja az IP hálózatok számára, hogy a felhasználói forgalom azonnal helyreálljon az aktív útválasztó meghibásodása után. A RG Vegyészeti Gyár menedzsment hálózatának fejlesztése során használtam a protokollt a menedzsment hálózat két központi (Core) eszközén, ily módon megbízhatóbbá téve a menedzsment hálózat gerincét. Ennek részleteit a munkám leírása során ismertetem, előbb azonban szeretném bemutatni a HSRP alapjait.

A HSRP lehetővé teszi, hogy több, ugyanabban az alhálózatban található útválasztó osztozzon egy virtuális IP és MAC címen, amelyet az állomások alapértelmezett átjáróként használnak. Az azonos HSRP csoportba konfigurált útválasztók csoportjából egy útválasztót választanak aktívnak, egy másikat pedig készenlétinek. Az aktív útválasztó szolgálja ki a virtuális IP-címre küldött kéréseket. Ha az aktív útválasztó nem működik, a készenléti útválasztó átveszi az aktív útválasztó szerepét a hálózatban.

A beállításhoz választani kell egy virtuális címet. A virtuális címet abból az alhálózatból kell kiválasztani, amelyiken a HSRP-t alkalmazzuk. A HSRP-ben résztvevő minden útválasztónak ugyanazt a virtuális címet kell megadni a **standby [csoport száma] ip [virtuális IP cím]** paranccsal. A csoport szám alapértelmezett értéke 0, amennyiben a HSRP-t VLAN Trunk kapcsolatokra szeretnénk alkalmazni, úgy minden VLAN-ra eltérő csoport számot kell választani. A csoportszám befolyásolja a virtuális MAC cím alakulását ezért érdemes ügyelni, az eltérő érték megadására. Az aktív útválasztó kiválasztása a **standby [csoport száma] priority [prioritás]** paranccsal lehetséges. A prioritás alapértelmezett értéke 100 és a legmagasabb prioritással rendelkező útválasztó lesz a HSRP csoport aktív útválasztója. Opcionális beállításként megadható a **standby [csoport száma] preempt delay [minimum | reload | sync]** parancs, amelyet akkor alkalmazunk, ha egy nyomon követett interfész állapotváltozásának bekövetkeztekor szeretnénk, ha egy standby útválasztó venné át az aktív szerepet. Erre jó példa, amikor két útválasztót alkalmazunk, amelyeknek nyomon követjük az uplink interfészeit. Ha az aktív útválasztó uplink státusza lekapcsolt állapotra vált, akkor a készenléti útválasztó átveszi az aktív szerepet. Az előbb ismertetett esetben a **preemt** parancs alkalmazása nélkül nem történt volna feladatátvétel, viszont a forgalomban kiesés történt volna, hiszen az aktív útválasztó uplink interfésze nem működött.[20]

3.7 Open Shortest Path First (OSPF)

Az OSPF egy kapcsolat állapot (link-state) alapú protokoll, amelyet az Internet Engineering Task Force (IETF) fejlesztett ki és az RFC 2328[21] szabvány rögzíti. Használatával egyszerűen megoldható a belső útválasztás és a jövőbeli bővítéseket is könnyű implementálni, emellett átlátható routing-ot eredményez. A vállalat menedzsment hálózatának átalakításához új routing stratégiát kellett kidolgozni, mivel annak útválasztását korábban a produktív hálózat eszközei végezték. Az alhálózatok forgalmának irányítására az OSPF protokollt választottuk többek között a statikus útválasztás helyett. A döntés részleteiről a tervezési fázisban írok részletesebben.

A link-state protokollok működésének két alappillére, hogy a hálózat topológiáját minden résztvevő útválasztó felderíti és az így kapott gráfban megkeresi a legrövidebb útvonalat, majd az ahhoz tartozó első csomópontot, amely felé továbbítani fogja a csomagot. Az algoritmus helyes működésének kulcsa, hogy a csomópontokban tárolt gráf azonos legyen és a különböző útvonalak költségeinek számítási módja is megegyezzen

az összes eszközön. A hálózat topológiáját a link-ek állapotát leíró rekordok (link-state records) egymás közötti terjesztésével ismerik meg az eszközök.

Az OSPF folyamat indulásakor az eszköz HELLO üzeneteket küld a kapcsolódó linkjein keresztül, ha valamelyik szomszédos csomópont válaszol és a HELLO üzenet paraméterei is megegyeznek a két eszköz között, akkor OSPF szomszédosság (Adjacency) alakul ki. Ezután megkezdődik az adatbázisok szinkronizálása a kialakult szomszédok között. Az adatbázis szinkronizálásához azonban az OSPF minden több hozzáférésű szegmensben egy útválasztót kiválaszt kijelölt útválasztónak (Designated Router, DR), és egy másikat tartalék kijelölt útválasztónak (Backup Designated Router, BDR). A BDR-t tartaléknak választják arra az esetre, ha a DR elérhetetlenné válna. A két kiemelt szerep célja, hogy a többi OSPF-ben résztvevő útválasztó, ezekkel végezze az információcserét. Ahelyett, hogy minden útválasztó frissítést cserélne a szegmens minden más útválasztójával, minden útválasztó információt cserél a DR-rel és a BDR-rel. A DR és a BDR továbbítja az információkat mindenkinek.

Az információcserét Link-State Advertisement (LSA) üzenetek küldésével/fogadásával végzik. Ha ez is megtörtént, akkor konvergált állapot áll be az eszközök között, ami azt jelenti, hogy minden eszköz befejezte az adatbázisainak frissítését. A konvergált állapotba való belépést jelzik a Cisco routerek. Egy link meghibásodása esetén a linket bekötő eszközök abba az irányba vezető útvonal költségét végtelenre módosítják, majd értesítik a szomszédos eszközöket, amelyek tovább hirdetik a változást, így a linkhiba után ismét beáll a konvergált állapot.

Az OSPF routing protokoll alkalmazásának néhány előnye például a gyors konvergálás vagy alternatív útvonalak használata a terhelés megosztása érdekében.[22]

3.8 Simple Network Management Protocol (SNMP)

Az SNMP protokoll segítségével a hálózat szegmensei a statisztikai adatokat egy központi felügyeleti eszközre továbbíthatják, így a hálózat üzemeltetői egy centralizált log szerveren ellenőrizhetik a mentett log fájlokat vagy akár egy telepített felügyeleti program segítségével valós idejű megfigyeléseket végezhetnek. A vállalatnál nem csak a produktív hálózati eszközök és szerverek állnak folyamatos felügyelet alatt, hanem a menedzsment hálózatot megvalósító készülékek is. Ezért a továbbiakban röviden összefoglalom az SNMP jellemzőit.

Az SNMP-t az IETF fejlesztette ki és a TCP/IP (Transmission Control Protocol) protokollcsomag része. Egy széles körben elfogadott hálózati protokoll, amely a hálózati elemeket kezeli és felügyeli. A legtöbb professzionális hálózati elemhez mellékelt SNMP ügynök tartozik. Ezeket az ügynököket engedélyezni és konfigurálni kell a hálózatfigyelő eszközökkel vagy a hálózatkezelő rendszerrel (NMS) való kommunikációhoz.

A következőkben bemutatom az SNMP főbb komponenseit, kezdve az SNMP Manager-rel. A Manager vagy a felügyeleti rendszer egy különálló entitás, amely felelős az SNMP ügynök (SNMP agent) által megvalósított hálózati eszközökkel való kommunikációért. Feladatai közé tartozik például az ügynökök lekérdezése, válaszok fogadása az ügynöktől vagy azok változóinak beállítása.

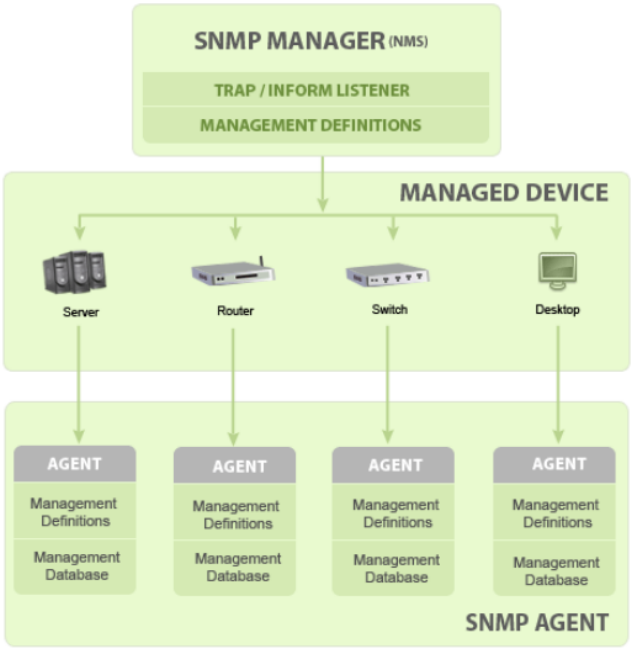
A felügyelt eszköz (managed device) a hálózat olyan része, amely valamilyen megfigyelést és kezelést igényel, például routerek, kapcsolók, szerverek, munkaállomások, nyomtatók, szünetmentes tápegységek (UPS).

Az ügynök egy olyan program, amely beépítve megtalálható a legtöbb hálózati eszközben. Az ügynök engedélyezése lehetővé teszi a felügyeleti információs adatbázis (Management Information Base, MIB) helyi gyűjtését az eszközről, és elérhetővé teszi az SNMP Manager számára. Ezek az ügynökök lehetnek szabványosak vagy gyártó specifikusak. Az ügynök feladata többek között menedzsment információk gyűjtése a lokális eszközről, a MIB-ben meghatározott kezelési utasítások tárolása és beolvasása, Manager értesítése egy esemény bekövetkezéséről.

Minden SNMP ügynök fenntart egy információs adatbázist (MIB), amely leírja a kezelt eszköz paramétereit. Az SNMP Manager ezt az adatbázist használja arra, hogy az ügynöktől konkrét információkat kérjen. A MIB-ek jellemzően statisztikai és ellenőrzési értékeket tartalmaznak a hálózat hardver eszközeihez. Az SNMP lehetővé teszi ezen standard értékek kiterjesztését privát MIB-ek használatával.

Végül az SNMP csapdák (SNMP Trap) lehetővé teszik egy ügynök számára, hogy kéretlen SNMP üzenettel értesítse az SNMP Managert a jelentős eseményekről. Az SNMP Trap protokollok tartalmazzák az aktuális sysUpTime (utolsó újra indulás óta eltelt idő) értéket, a csapda típusát azonosító OID-t (Object ID, a MIB-eket alkotó objektumok) és opcionális változó kötéseket.

A főbb komponensek áttekintése után az 11. ábrán látható, hogy az egyes elemek elvben hogyan helyezkednek el egymáshoz képest.[23]



11. ábra: Az SNMP komponensei és felépítése.[23]

Az SNMP első verziójára az RFC 1065 - RFC 1067 szabványok vonatkoznak, amelyek közül a protokoll legfontosabb elemeit az RFC 1067[24] írja le. Később ezen szabványokat felülírták az RFC 1155 – RFC 1157 sztenderdek, amelyek közül az RFC 1157[25] tartalmazza a leginkább fontos információkat. A több szempontból is gyenge biztonsági megoldásokkal rendelkező verziót idővel leváltotta az SNMPv2. Ez a verzió azonban nem terjedt el, helyette az SNMPv2c-t alkalmazták széleskörben, amely tartalmazta v2 javításait, de a bonyolult biztonsági eljárások helyett (ezért is nem vált közkedvelté a v2) az egyszerűbb megoldásokat támogatta. Az SNMPv2c verziót az RFC 1901[26], RFC 1905[27] és az RFC 1906 szabványok rögzítik, közülük is az első két sztenderd a legfontosabb. Mára mindkét korábbi verziót elavultnak nyilvánította az IETF. A jelenlegi hivatalos verzió az RFC 3411–RFC 3418 szabványok által definiált SNMPv3. A protokoll legújabb verziójának legfontosabb aspektusai az RFC 3411[28] kerültek rögzítésre, amelynek további kiegészítései az RFC 5343[29] és az RFC 5590[34] sztenderdek.

3.9 Network Time Protocol (NTP)

Az NTP egy internetes protokoll, amely a számítógépek óráinak szinkronizálására szolgál. A protokollnak létezik egy leegyszerűsített változata is, amelyre Simple Network Time Protocol-ként (SNTP) hivatkoznak. Az egyszerűsített megoldás megvalósítását az ösztönözte, hogy az eredeti protokoll teljes implementálása sok szerver számára túl

bonyolult volt. Ennek megfelelően az SNTP-ből kivettek néhány belső algoritmust, amire némely szervereknek nem volt szüksége.

A belső rendszerek időbeli eltérésének számos negatív következménye lehet. Ilyen például az email rendszerekben küldött és fogadott üzenetek időrendi sorrendjének téves megjelenése, de ennél sokkal komolyabb incidensekhez is vezethet a jelenség, például légiforgalom irányítás rendszerében. Nem véltlen, hogy először ezen a területen alkalmaztak NTP-t.

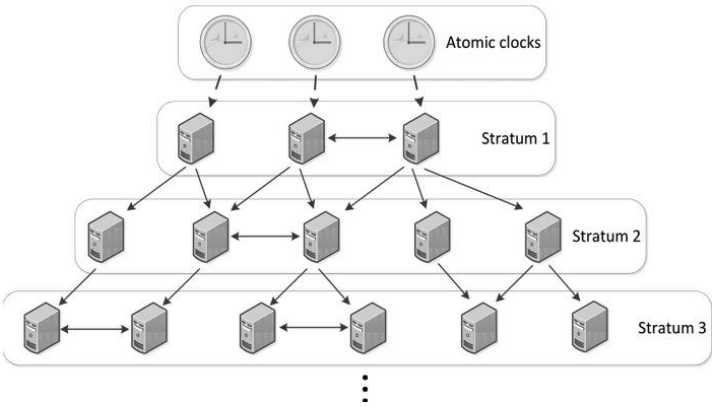
Az egységes idő nem csak a szerverek, alkalmazások és adatbázisok számára nélkülözhetetlen, a hálózati eszközökön bekövetkezett események vizsgálatának is elengedhetetlen feltétele. Így természetesen én is alkalmaztam a protokollt a menedzsment hálózat eszközein.

A működéséhez szükséges valamilyen referenciaóra. Ehhez az NTP az Universal Time Coordinated (UTC), vagyis az aktuális idő hivatalos szabványát használja. Emellett képes több időforrás közül kiválasztani a legmegfelelőbbeket, amelyeket a szinkronizációhoz használ, illetve ignorál általa nem megbízhatónak ítélt forrásokat. A hibatűrő képességét tovább erősíti, hogyha a hálózati kapcsolat ideiglenesen nem érhető el, az NTP a múltbeli mérések alapján megtudja becsülni az aktuális időt és hibát.

Az NTP hierarchikus módon épül fel. A rétegeket stratum-nak nevezzük és nullától kezdődő, növekvő számokkal jelezzük az alsóbb rétegeket. Az aktuális stratum szint meghatározza a távolságot a referencia órától.

- Stratum 0: Itt atomórák találhatók.
- Stratum 1: Ezek a Stratum 0-hoz kapcsolódó eszközök. Alapesetben a Stratum 2 kiszolgálói NTP-n keresztül, más néven idő szerverek.
- Stratum 2: Itt számítógépek vannak, melyek NTP kéréssel fordulnak a Stratum 1 szerverekhez.
- Stratum 3: Ezen a szinten hasonlóan működnek az eszközök, mint az előző szinten, és a Stratum 4 szint kiszolgálói, és így tovább.

A következő ábra az NTP hierarchikus felépítését szemlélteti.



12. ábra: Példa az NTP kommunikáció irányaira.[31]

Az NTP jelenlegi legfrissebb verziója az NTPv4, azonban a hivatalos internetes szabvány továbbra is az NTPv3 (RFC 1305[32]). Az alkalmazni kívánt verzió kiválasztását befolyásolhatja az is, hogy az operációs rendszerek gyártói a saját rendszerükhöz optimalizálják a protokollt, ezzel új verziókat létrehozva. Ez kompatibilitási problémákhoz vezethet, szerencsére a régebbi NTP verziók többsége képes kommunikálni az újabb verziót futtató szerverekkel.[33]

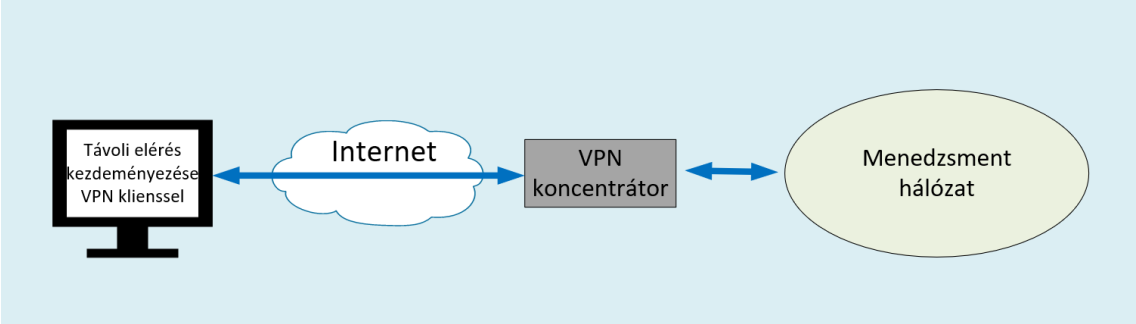
3.10 Virtual Private Network (VPN)

A virtuális magán hálózatok a magán hálózatok kiterjesztései publikus vagy megosztott hálózatokon keresztül. Más szóval a VPN technológia lehetővé teszi a távoli felek számára a privát hálózathoz való csatalakozást az interneten keresztül. A VPN technológiának kulcsfontosságú szerepe van a Richter Gedeon Vegyészeti Gyár továbbfejlesztett menedzsment hálózatának megbízható elérésében. A hálózat üzemeltetői szükség esetén egy dedikált VPN átjárón keresztül elérhetik a menedzsment hálózatot, azzal együtt pedig a hálózat többi elemének kezelőfelületét. Továbbiakban szeretném rövidben bemutatni az előbb leírt funkciót megvalósító megoldást.

A VPN kapcsolatoknak két alapesete van, melyek Remote access VPN és a Site-to-site VPN kapcsolat. Remote access VPN esetén a felhasználók távolról kapcsolódnak egy privát hálózathoz, például egy dolgozó a laptopja segítségével kapcsolódik a vállalat belső hálózatához. A Site-to-site VPN kettő, vagy több telephely, vagy iroda kapcsolatát jelenti.[34]

Ezek alapján az üzemeltetők menedzsment hálózathoz való távoli hozzáférése Remote access VPN kapcsolatot jelent. A megvalósítás pedig Cisco gyártmányú eszközökből és VPN kliensalkalmazásból jön létre.

A hardvereszközök magasszintű integrált biztonsági szolgáltatásokat nyújtanak. A VPN kliens pedig lehetővé teszi, hogy a felhasználók akár mobileszköz segítségével is képesek legyenek igazolni hozzáférésük érvényességét, ezáltal pedig csatlakozzanak a vállalat hálózatához. Az előbbiekben leírt funkciógyűjtemény összeségében ellenőrzött távoli hozzáférést biztosít a vállalat infrastruktúrájához.



13. ábra: Példa a VPN kapcsolaton keresztüli menedzsment elérésre.

A távoli és mobil felhasználók a VPN klienst használják VPN-munkamenetek létrehozására. A Cisco hardveregységek szerepe, hogy ellenőrizzék a felhasználó által generált forgalmat és alkalmazzák a vállalat szabályrendszerét. Az alkalmazott hardverkomponensek és a VPN kapcsolat konkrét beállításait a továbbiakban nem részletezem, ezen konstrukció már korábban élesítésre került a vállalat hálózatán.[35]

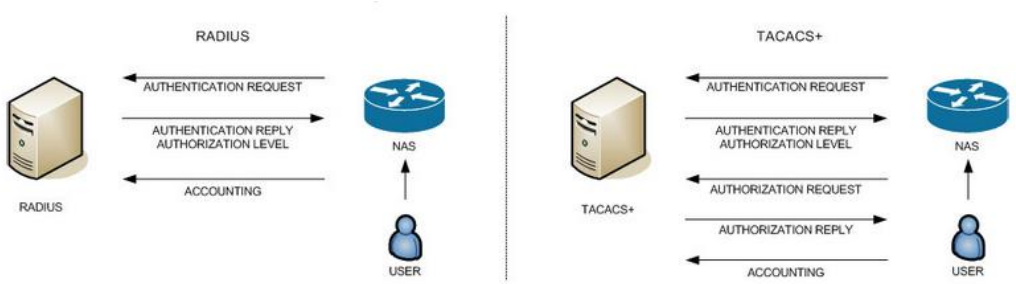
3.11 Authentication, Authorization, Accounting (AAA)

A hálózati hozzáférésének kontrollálására használt két kiemelkedő protokoll a Terminal Access Controller Access Control System Plus (TACACS+) és a Remote Authentication Dial-In User Service, röviden RADIUS. Alkalmazásukkal az AAA házirend (Authentication – kik férhetnek hozzá, Authorization – milyen műveleteket hajthatnak végre, Accounting – milyen tevékenységeket végeztek a bejelentkezésük alatt.) betartatása valósítható meg. A vállalat menedzsment eszközei esetében is alkalmaztam AAA beállításokat, ezért az alábbiakban bemutatom a népszerű protokollokat.

A RADIUS egy közkedvelt biztonsági protokoll, amely authentication, authorization és accounting funkcionalitással bír. Főbb jellemzői az UDP protokoll használat, az authentication és authorization összevont kezelése. A RADIUS protokollt az RFC 2865[36] szabvány írja le. A kommunikáció röviden a következőképp írható le: egy állomás RADIUS szerver által kontrollált hálózathoz való hozzáférés kérelmét egy

Network Access Server (NAS) fogadja, ez általában egy switch vagy egy hozzáférési pont (access point), majd a NAS továbbítja a kérést a RADIUS szerver felé, amely kiértékeli azt. Végül az eredményt válaszként visszaküldi a NAS-nak. Amennyiben az állomás érvényes belépési információkat küldött, úgy a szerver hozzáférés elfogadva (Access-accept) választ ad. Ezután az állomás már hozzáférhet a hálózathoz.

A TACACS egy régebbi biztonsági protokoll, amit eredetileg authentikáció megvalósítására hoztak létre. A Cisco fejlesztette tovább és egészítette ki az authorization és az accounting funkciókkal, melyre TACACS+-ként hivatkoznak. Főbb előnyei, hogy a csomagok küldésekor a teljes csomagot titkosítja, TCP protokollt használ. A TACACS+ protokollt az RFC 8907[37] szabvány írja le. A TACACS+ kommunikáció alapjaiban hasonlít a RADIUS szerveréhez, azonban a külön kezelt szolgáltatások miatt jóval több üzenetváltásra van szükség a felek között.[39]



14. ábra: A RADIUS és a TACACS+ kommunikációjának főbb elemeiről.[38]

3.11.1 TACACS+ és RADIUS rövid összehasonlítása

A következő felsorolásban kiemelek néhány általam fontosnak talált különbséget a két biztonsági protokoll között:

- A TACACS+ a teljes csomagot titkosítja küldéskor, ellenben a RADIUS-al, ami csak a jelszavakat.
- A RADIUS kezdetben User Datagram Protocol -t (UDP) használt, azonban a modern megoldások már a Transmission Control Protocol-t (TCP) is támogatják, amíg a TACACS+ TCP protokollt használ. A skálázhatóság kérdését és a kapcsolatok állapotának ismeretét figyelembe véve a TCP protokoll használata az előnyösebb.
- A RADIUS kombinálja az authentication és authorization funkciókat. Ellenben a TACACS+ szeparáltan valósítja meg az AAA funkcionalitást.

- A TACACS+ képes naplózni az összes kiadott parancsot, míg a RADIUS esetén erre nincs lehetőség.[39]

3.12 In-Band és Out-of-Band menedzsment hálózat

Ebben az alfejezetben a menedzsment hálózatok topológiájához köthető alapvető különbségeket szeretném bemutatni. A gyakorlatom során a vállalat menedzsment hálózatát fejlesztem tovább, hogy az megfeleljen az Out-of-Band menedzsment topológia elveinek.

In-Band menedzsment hálózatnak nevezzük, amikor a menedzsment forgalom az üzleti célú forgalommal azonos linkeken és eszközökön, ezáltal azonos útvonalon kerül továbbításra. Az In-Band kialakítás sokkal költséghatékonyabb, mert a meglévő hálózati erőforrások nagymértékben felhasználhatók erre a célra. Ennek esetén a forgalom szeparációja dedikált menedzsment VLAN alkalmazásával valósítható meg.

Out-of-Band menedzsment hálózat a menedzsment forgalom teljes elkülönítését jelenti az üzleti forgalomtól. A modell megvalósításához dedikált hálózati kapcsolókra és linkekre van szükség. A kialakítás egyik előnye az In-Band topológiával szemben, a fizikai szeparáció nyújtotta megbízhatóság.[40]

4 Menedzsment hálózat fejlesztése

A következő fejezetben bemutatom a gyakorlatom során a vállalat menedzsment hálózatának fejlesztéséhez köthető munkámat és az elért eredményeimet. Ismertetem a tervezési fázis során összegyűjtött információkat és megmutatom az azokból létrehozott tervrajzokat, amelyek különböző nézetekben ábrázolják a hálózatot. A fejlesztések implementálásánál pedig kiemelem az egyes folyamatokban megjelenő újabb ismereteket, amelyek hozzájárultak ahhoz, hogy egyre hatékonyabban végezzem a feladataimat.

4.1 Tervezési folyamat

A tervezés során mind a már rendelkezésre álló, mind az általam végzett felmérések alapján készített dokumentációkat felhasználtam. A munka előrehaladtával folyamatosan frissítettem azokat, így könnyen átlátható volt a munka aktuális állapota, emellett a következő lépések meghatározásában is segítenek a naprakész források.

4.1.1 Kiindulási állapot

A Richter Gedeon Vegyészeti Gyár eszközmenedzsment hálózatának átalakítása a hálózat megismerésével kezdődött. Ehhez először a vállalat által a rendelkezésemre bocsájtott dokumentációkat kezdtem el feldolgozni, emellett pedig sok segítő információt kaptam a Network & Security csapat tagjaitól. A segítségükkel megismertem a vállalat szervertermeit és külső telephelyeit, ahol a menedzsment hálózat komponensei találhatók. A meglévő dokumentációk alapján pedig néhány komponensről több részletet is megismerhettem. Mielőtt folytatnám a felméréssel kapcsolatos munkám ismertetését, előtte tisztázom, hogy mit értek pontosan menedzsment alhálózat alatt.

A vállalatnál a logikailag összetartozó hálózatrészeket, úgynevezett disztribúciós switchek kapcsolják össze. Az alhálózatok szeparációja pedig leginkább szolgáltatás szerint történik. Menedzsment alhálózatokon tehát az egyes disztribúciók által a hálózathoz kapcsolt menedzsment célra létrehozott és használt alhálózatokat értem, amelyek egyedi IP címtartománnyal és disztribúciónként egyedi VLAN ID-val rendelkeznek.

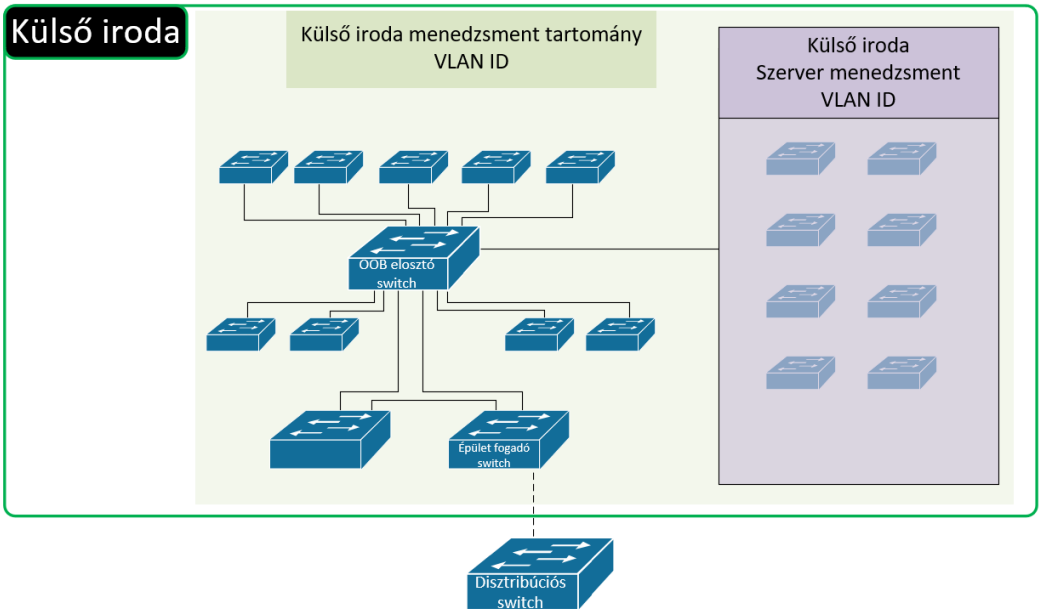
Az előző bekezdésben tárgyalt menedzsment alhálózatok különböző disztribúciókon keresztül kapcsolódnak a hálózat gerincéhez (Core réteg). Mivel a különböző menedzsment alhálózatok különböző IP cím tartományokkal rendelkeznek, ezért kimondható, hogy a vállalat menedzsment hálózata több, szigetszerű hálózatrészből áll. Ezért a továbbiakban ezekre a részekre menedzsment szigetként fogok hivatkozni. Tekintve, hogy nem minden menedzsment szigetről áll rendelkezésemre részletes dokumentáció, Boór András javaslatára készítettem egy átfogó hálózati rajzot a teljes menedzsment hálózat aktuális topológiájának rögzítésére. A tervrajz célja, hogy olyan információkat rögzítsen tömör és egységes formában, amelyek közvetlenül nem állnak rendelkezésre, és amelyek segítik a későbbi fejlesztések megtervezését.

A fentieknek megfelelően a tervrajz készítésénél figyelembe vettem a földrajzi elhelyezkedést, az egyes szigeteket alkotó switchek kapcsolatait, azok IP címeit és az eszközök típusát. A sziget jellemzői közül az IP tartományt és a hozzá tartozó VLAN ID-t jelenítem meg, továbbá a tartomány csatlakozását biztosító disztribúciós eszközt. Ezen információk jelentős részét fizikai felmérésekkel és az eszközök konfigurációinak áttekintésével gyűjtöttem össze.

4.1.1.1 Menedzsment szigetek

A következőkben röviden bemutatom milyen komponensekből tevődik össze a vállalat menedzsment hálózata, közben kiemelem az egyes komponensek jellegzetességeit, amelyeket figyelembe vettem a tervezési fázis későbbi szakaszaiban.

Az első általam felmért menedzsment szigetről készült tervrajz részlet a következő ábrán látható. Az eredeti tervrajz tartalmaz IP címeket, konkrét eszköz típusokat és egyéb szenzitív információkat, amelyeket a megjelenített ábrákon nem szerepeltetek.



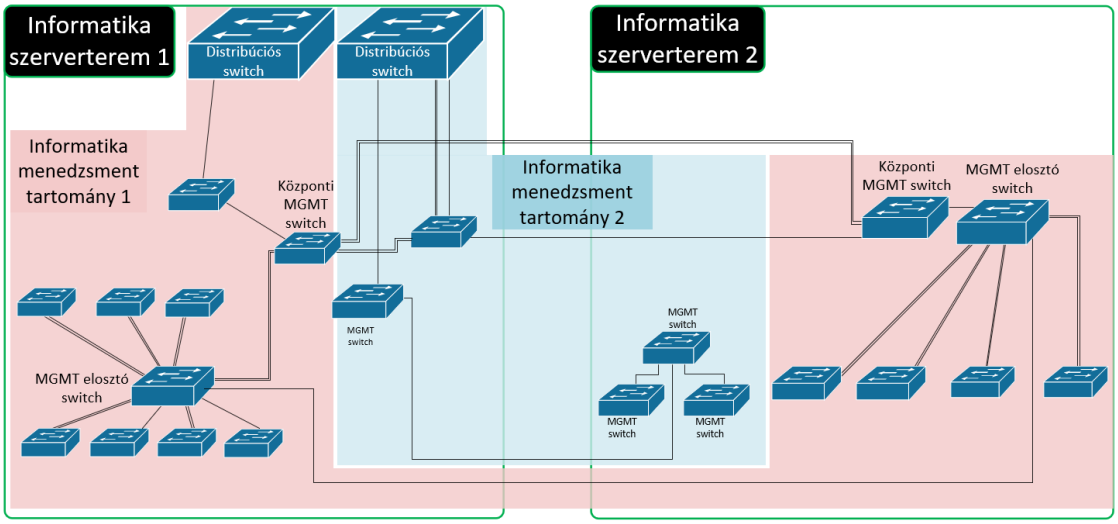
15. ábra: Tervrajz részlet a külső iroda menedzsment hálózatáról.

A 15. ábrán a vállalat egyik külső irodájának menedzsment hálózata látható. Az ábrán a fehér alapú, zöld körvonallal ellátott téglalap az épületet jelzi, azon belül a zöld és lila téglalapok a menedzsment IP címek különbözőségét jelölik. Ebben az esetben a menedzsment hálózatot két alhálózat alkotja, a zöld tartomány, amelynek címei a hálózati eszközök számára vannak fenntartva, míg a lila tartomány a szerverek menedzsment interfészeihez kerültek hozzárendelésre. A tartományokkal és a hozzájuk tartozó VLAN-okkal kapcsolatos információk összegyűjtéséhez a vállalat IP cím nyilvántartó rendszerét használtam, amelyet szükség esetén én is frissítettem menedzsment IP címek bejegyzésével. Fontos megjegyezni, hogy az előbb kiemelt szeparáció nem jelenti a tartományok fizikai elkülönítését, vagyis a szerverek számára fenntartott alhálózat forgalmát is a zöld téglalapban látható switchek továbbítják. Végül jelöltem a rajzon a menedzsment szigetet a hálózathoz kapcsoló eszközt is. Itt a kapcsolat jelölésére szaggatott vonalat használtam, ezzel jelezve, hogy valójában az az eszköz fizikailag más helyszínen található.

Az előbbiekben bemutatott menedzsment sziget topológiája véleményem szerint könnyen átlátható, így a későbbiekben könnyű volt meghatározni az ezzel kapcsolatos változtatásokat. Azonban egyes menedzsment szigetek esetében az eszközök összeköttetései kevésbé egyértelmű topológiát eredményeztek.

A következő ábrán egy másik menedzsment sziget felépítése látható. Az ábrán két fontos szerepet betöltő szerverhelyiség menedzsment hálózata látható, melyekre a

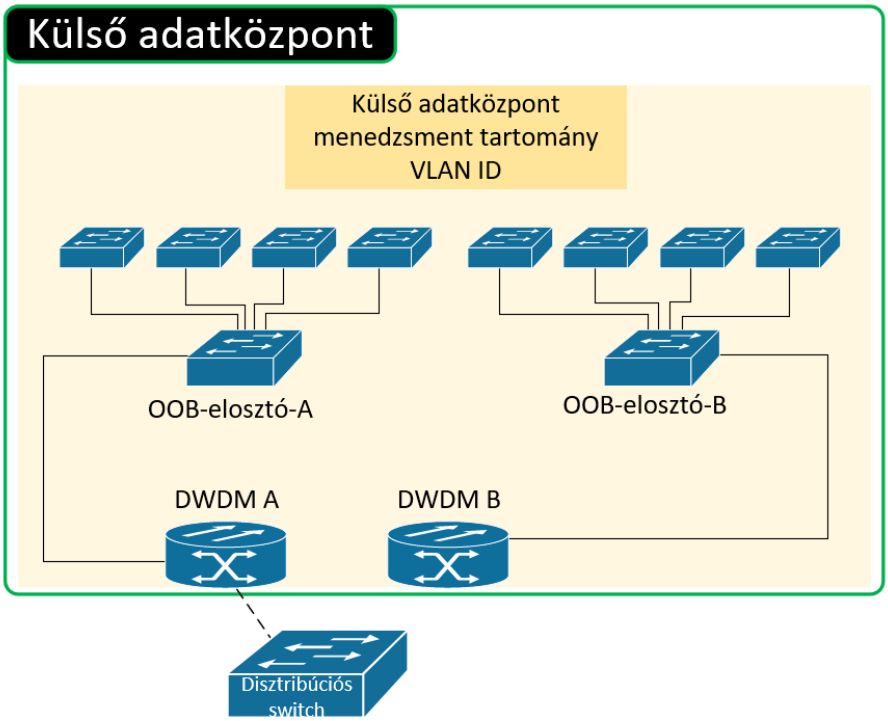
továbbiakban az egyszerűség kedvéért az informatika épület szervertermeiként fogok hivatkozni. Bár fizikailag különálló épületekben található eszközök alkotják, az egymással való kapcsolataik miatt mégis akár egynek is tekinthetők.



16. ábra: Tervrajz részlet az informatika épület menedzsment hálózatáról.

Ha csak az összeköttetéseket veszem figyelembe valóban egy menedzsment hálózatnak tekinthető. Ugyanakkor, ha az eszközöknek kiosztott IP címeket és a használatban lévő VLAN-okat is számításba veszem, akkor értelmet nyernek az ábrán szerepeltetett kék és piros területek, amelyek itt is a különböző IP tartományokat jelölik. Az elsőként bemutatott külső iroda hálózatához képest a különbség az, hogy ebben az esetben a két különálló tartománynak nem ugyanaz a fizikai eszköz biztosítja a csatlakozási pontját. A felmérés eredményeként kapott topológia nem fedi fel a tartományok állomások szerinti megoszlását, így akár előfordulhat, hogy az egyik tartományt nem indokolt a későbbi OOB hálózathoz kapcsolni. Az állítás igazolása a fejlesztés későbbi fázisában válik igazán fontossá, így azt részletesen 4.2.5 alfejezetben vizsgálom.

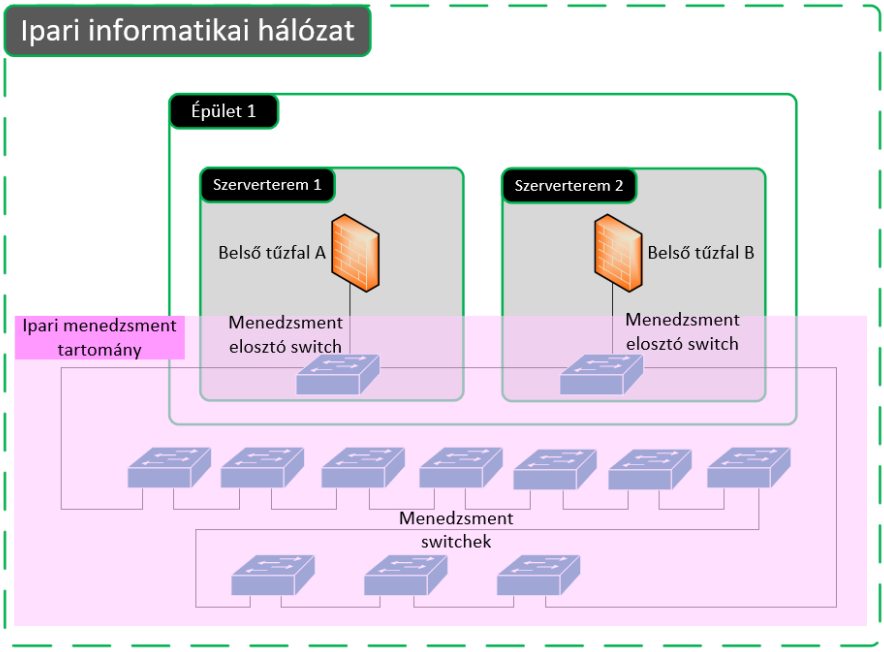
A következő rajzomon szerepeltett menedzsment hálózat egy újonnan kiépített hálózatrész, pontosabban egy külső lokáción található adatközpont menedzsment hálózatának felépítését írja le. Az adatközpont menedzsment hálózata a 17. ábrán látható.



17. ábra: Tervrajz részlet a külső adatközpont menedzsment hálózatáról.

Ez a menedzsment sziget talán a legkönnyebben csatolható egy egységes menedzsment hálózathoz. Ezen állításomat támasztja alá, hogy az ábrán szemléltetett topológia egyetlen menedzsment tartományt szolgál ki, továbbá a switchek kapcsolatai alapján könnyen meghatározhatók a sziget későbbi csatolási pontjai. A csatolási pontokkal kapcsolatosan szeretnék rávilágítani az ábra alján látható DWDM hardveregységekre, amelyek a sziget csatolásában kulcsfontosságú szerepet töltenek be. Az új hálózatrészről emellett részletes és naprakész dokumentáció állt rendelkezésemre, amelynek a feladatomhoz kapcsolódó elemeit emeltem át a saját tervrajzomba.

Az utolsó menedzsment szigetet, amelyet bemutatok, az ipari informatikai hálózat menedzsment eszközei alkotják. Ezen sziget hasonlóan több épület és helyiség eszközeit foglalja magában csakúgy, mint az informatika épület szervertermei. A rajz ipari szeparáció menedzsment hálózatát leíró részlete az 18. ábrán látható.



18. ábra: Tervrajz részlet az ipari informatikai hálózat menedzsment hálózatáról.

Alapvető különbség azonban, hogy az előbbi szigeteknél a csatlakozáshoz alkalmazott switch helyett, ennek a menedzsment alhálózatnak a csatolását egy belső tűzfal végzi. A tűzfal alkalmazása az ipari rendszerek fokozott védelme érdekében történik, de fontosnak tartom megjegyezni, hogy a rajzon látható tűzfalak elsősorban nem a menedzsment hálózat védelmére szolgálnak. Ez az információ indokolja a későbbi tervezés során a kapcsolat megszűntetését a tűzfallal. Az ipari informatikai hálózat esetében megfelelő mennyiségű és aktualitású dokumentáció állt rendelkezésemre, így itt is más dokumentációk elemei alapján készítettem el a menedzsment sziget vázlatát. A tartományok és a VLAN-ok feltérképezésénél több különböző menedzsment funkciókhoz köthető tartományt is azonosítottam. Ezek igazolására olyan kollégák segítségét kértem, akiknek több információjuk van az ipari hálózatról.

Az egyeztetés során fényderült rá, hogy az általam azonosított tartományok valóban menedzsment funkciókhoz tartoznak, azonban azok közül csak egy tartomány az, amely ténylegesen a hálózati eszközök számára van fenntartva. A többi alhálózat más funkcióhoz került hozzárendelésre, például mérőeszközök felügyeletéhez és ez a felismerés egy új szempontot vezetett be a tervezési fázisba. Ez számomra azt jelentette, hogy az új menedzsment hálózatra olyan eszközök kerülhetnek, amelyek ténylegesen a hálózat elemeinek menedzsmentjében vesznek részt. Ezt az elvet szem előtt tartva folytattam a tervezést.

4.1.1.2 A felmérések összegzése

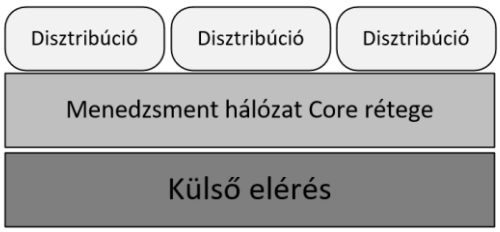
A felmérés elvégzése és az így összegyűjtött információk felhasználásával elkészült átfogó hálózati rajz alapján a legtöbb menedzsment sziget esetén már egyértelműen meghatározhatóvá vált az a csatolási pont, amelyet leválasztva a produktív hálózatról és csatlakoztatva egy szeparált menedzsment gerinchálózathoz az adott menedzsment sziget teljes egészében az új gerinchálózaton keresztül válik elérhetővé az eddigi produktív irányok helyett. Az átalakítások megtervezéséhez néhány esetben szükség lesz további felmérésekre, amelyek akkor végezhetők el, ha már a gerinchálózat felépítése tisztázott. Ennek megfelelően a jelenlegi állapot ismeretében megkezdődhet az átalakítások megtervezése, amelyben fontos szerepet játszik majd az adatközpont hálózatának bemutatásánál említett DWDM technológia is.

4.1.2 Out-of-Band menedzsment hálózat tervezése

A vállalat menedzsment hálózatának megismerése után a következő lépés annak a konstrukciónak a megtervezése, amely ezt a jelenleg félig In-Band, félig Out-Of-Band menedzsment hálózatot teljes egészében az OOB elveknek megfelelő hálózattá alakítja. A következőkben ismertetem az általam és a vállalati konzulensem által választott megoldásokat, közben pedig bemutatom az ezen megoldásokat indokló tervezési szempontokat is.

4.1.2.1 Gerinchálózat tervezése

A fejlesztés legfontosabb célja, hogy a már meglévő menedzsment szigetek függetlenné váljanak a produktív hálózattól. Ehhez szükség van egy gyökér vagy gerinc eszközre, ami minden menedzsment szigettel kapcsolatban áll egy disztribúciós eszközön keresztül és a megfelelő hálózatrészek felé irányítja a forgalmat.

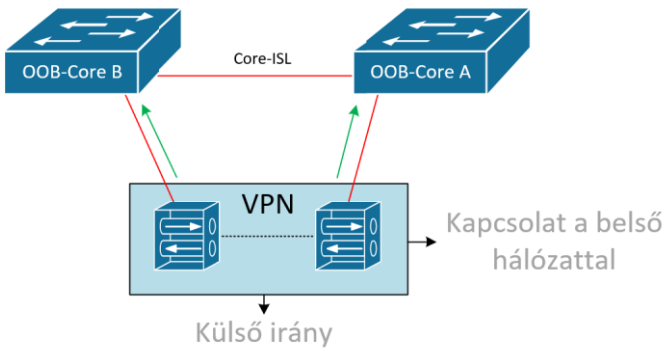


19. ábra: Vázlat az új OOB hálózat felépítéséről.

Az új menedzsment hálózat Core rétege pedig emellett kapcsolatban áll majd a külső irányokkal.

Ez az eszköz azonban kritikusnak számít a leendő OOB hálózat működésének szempontjából, így annak elkerülése érdekében, hogy egyetlen eszköz meghibásodása miatt a teljes hálózat elérhetetlenné váljon (Single point of failure), két OOB gerinc vagy Core eszköz telepítését tűztem ki célul. Ennek megfelelően mindkét Core switchnek lesz kapcsolata minden menedzsment szigettel, így az egyik meghibásodása esetén a másik eszköz továbbra is kapcsolatot biztosít majd.

Tehát két eszköz fogja alkotni az OOB hálózat gerincét. A következő lépcsőfok ezen eszközök elérhetőségének és velük együtt az egész menedzsment hálózat elérhetőségének meghatározása. Egyrészt biztosítani kell, hogy a belső, produktív hálózatból elérhető legyen például az üzemeltetők vagy a hálózati felügyeleti rendszerek számára. Másrészt pedig kell egy olyan biztonságos elérési lehetőség is, amely nem a belsős hálózaton keresztül valósul meg, hiszen ennek megléte nélkül aligha nevezhetnénk OOB hálózatnak. Ezen elvárásoknak megfelelően a vállalati konzulensem azt javasolta, hogy használjuk a vállalat által üzemeltetett egyik VPN koncentrátor klasztert. A klaszter is a leendő OOB hálózat magjához hasonlóan két eszközből áll, így a single point of failure lehetősége itt sem áll fenn. Továbbá a VPN megoldásnak van kapcsolata a belsős hálózattal, ezáltal a produktív irányból elérhetővé lehet majd tenni a menedzsment hálózatot. Ha az OOB hálózat gerincével is közvetlen kapcsolata lesz, úgy a belső hálózat használata nélküli menedzsment elérés is megoldható. Ehhez a VPN technológia alkalmazása szükséges.



20. ábra: Tervrajz részlet az OOB hálózat gerincének felépítéséről.

A hálózat gerincének és a megfelelő elhelyezkedés meghatározása után már könnyebben eldönthető, hogy pontosan milyen hardverkomponensekre lesz szükség. Itt az első szempont a kábelezés megvalósítása volt, amihez az eszközök lokációi is szorosan kapcsolódnak. Idetartozó információ, hogy az adatközpontban, majd később a külső iroda

szerverhelyiségében is telepítésre kerültek DWDM eszközök, amelyek kapcsolatot biztosítanak az informatika épület szervertermeihez. Tehát ezen szigetek csatlakoztatására érdemes ezt a technológiát felhasználni. A technológia használatának feltétele az optikai kapcsolatok alkalmazása, így mindenképpen olyan Core switcheket kell választani, amelyek rendelkeznek elegendő SFP kompatibilis interfésszel. Az OOB hálózat Core rétegét tekintve a két eszköz terv szerint külön csomóponti helyiségbe kerül, ezzel növelve a működés megbízhatóságát. Ebből következik, hogy ezen eszközök összekötése is optikai kábellel lehetséges. Továbbá a VPN koncentrátor klaszter elemeit is össze kell kapcsolni az egyes Core switchekkel. Itt van lehetőségünk RJ-45 csatlakozóval kompatibilis SFP modult és UTP Cat 6 kábelt is használni, mivel ezek az eszközök páronként ugyanabban a helyiségben találhatók. Azonban az egységes kialakítás érdekében ezen kapcsolatok is optikai kábelekkel kerülnek megvalósításra.

Az interfészekkel szemben támasztott elvárások mellett a következő fontos szempont, hogy az OOB hálózat gerincét alkotó eszközök támogassák a dinamikus routing protokollok alkalmazását. Bár jelen tervezési fázisban, még nem eldöntött, hogy milyen módon valósul majd meg a routing az OOB hálózatban, azonban valószínűsíthető, hogy dinamikus routing protokollt alkalmazok majd.

A fentiekben felsorakoztatott konkrét kritériumok mellett, azt is figyelembe kellett vennem, hogy milyen eszközök állnak aktuálisan rendelkezésre a vállalat eszköztárában. A választás végül két darab Cisco Catalyst 3850-24XS switchre esett. Ezek az eszközök 24 darab 10 Gbps maximális sávszélességű, SFP modul kompatibilis access porttal rendelkeznek, továbbá támogatják az OSI modell szerinti harmadik réteghez tartozó funkciókat, így a dinamikus routing protokollok használatát is.

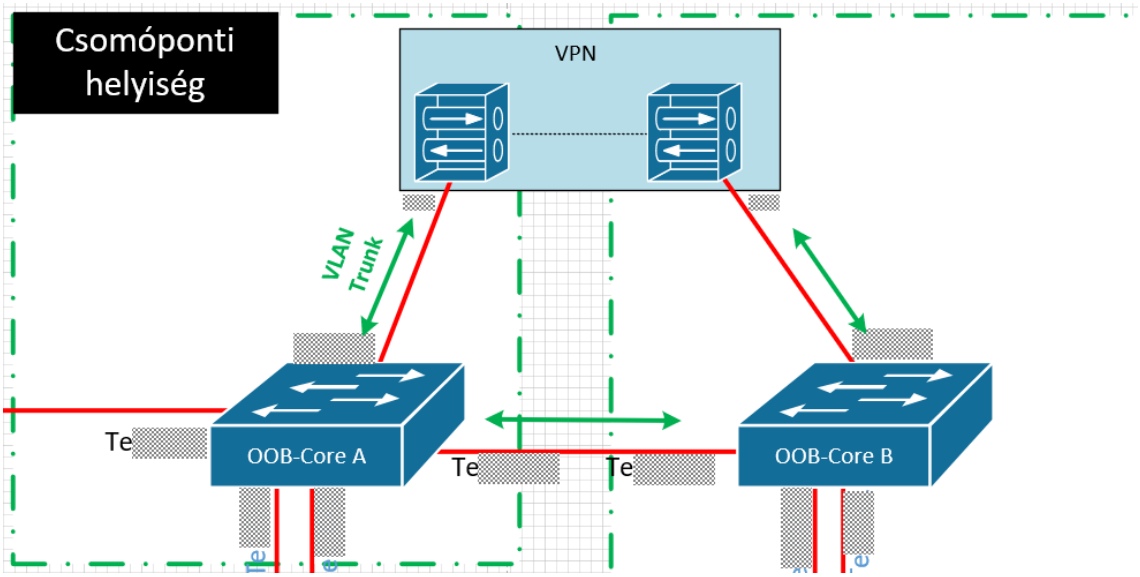
A tervezés ezen szakaszában tehát meghatároztam az OOB hálózat gerincének összetételét, illetve a konzulensem javaslata alapján eldöntöttük, hogy a meglévő VPN koncentrátor segítségével biztosítjuk majd a szükséges kapcsolatokat, valamint kiválasztottam az OOB hálózat Core rétegét alkotó két switchet.

4.1.2.2 OOB hálózat kapcsolatainak megtervezése

Már a fentiekben bemutatott hálózatrész megtervezésénél is nagyon sok tényezőt számításba kellett venni és a jövőbeli követelményeket is szem előtt tartani. Ezek után számomra is világossá vált, hogy az OOB hálózat hatékony fejlesztéséhez szükséges egy

átfogó tervrajz, ami a jelen állapotot leíró rajznál jobban kiemeli azokat a tényezőket, amelyekre a változtatások során fókuszálni fogok.

Ennek nyomán késztettem el a kiépíteni kívánt OOB hálózat kapcsolati rajzát, aminek célja, hogy egyetlen rajzon szerepeltesse a fő komponenseket, vagyis a VPN koncentrátort, a Core switcheket, a DWDM egységeket és az összes sziget esetében kijelölt vagy kiépíteni kívánt OOB disztribúciós switchet. További célja jelölni a kapcsolatokat a komponensek között, az azokhoz rendelt interfészeket és a switchek között alkalmazott VLAN-okat. A következő ábrán bemutatom az így elkészült rajz egy részletét, amely az OOB hálózat Core eszközei és a VPN koncentrátor klaszter kapcsolatát írja le.

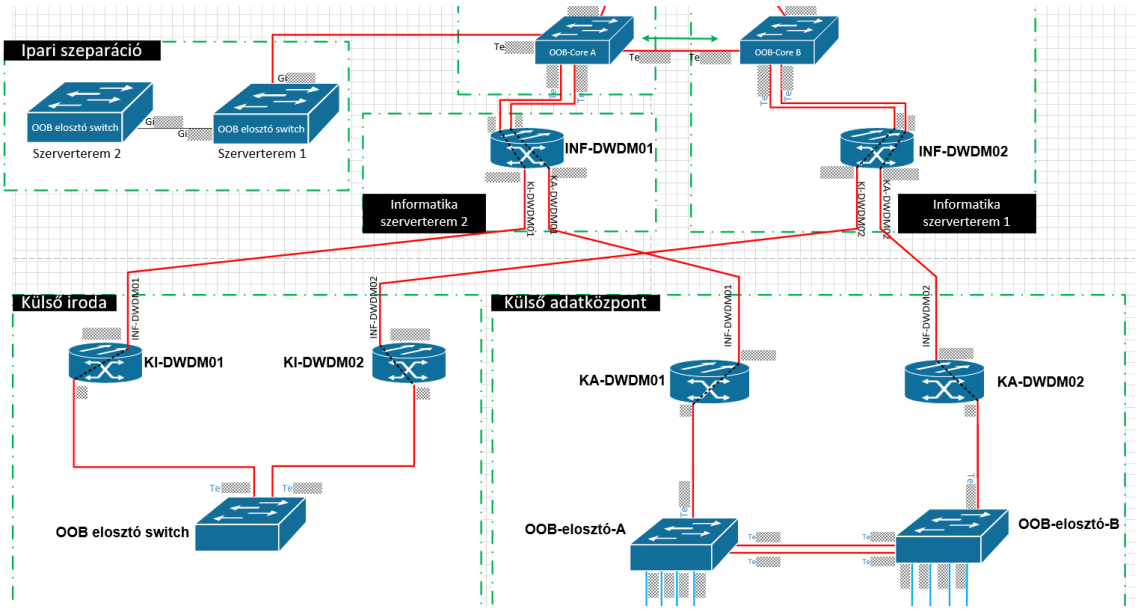


21. ábra: A kapcsolati tervrajzból kiragadott részleten az OOB hálózat gerincének fizikai összeköttetései láthatók és az azokhoz felhasznált interfészek.

Az 21. ábrán fehér alapon, zöld szaggatott körvonallal jelöltem az épületeket, piros vonallal pedig a fizikai kapcsolatokat. A két irányú zöld nyilak jelzik, hogy az adott kapcsolat VLAN Trunk módban fog működni. Ennek okát később az útválasztás megtervezésénél részletesen kifejtem. Mivel ezen OOB Core eszközöket én választhattam és telepíthettem, így ezek esetében nem jelentett akadályt a szabad interfészek száma, az SFP modullal való kompatibilitása vagy más korlátozó tényezők, melyek fennállhatnak például a menedzsment szigetek esetében.

A következő ábrán szintén az OOB hálózati kapcsolati rajzának egy részlete látható, amelyen most a menedzsment szigetek disztribúciós eszközeit jelenítem meg.

Ezen megjelenítési mód segít az interfészek felhasználásának konkrét megtervezésében és a követelmények ellenőrzésében.



22. ábra: Részlet a kapcsolati tervrajzból.

A tervrajz ezen részének elkészítésénél nagy mértékben támaszkodtam a korábban készített tervrajzomra, amely elsősorban abban volt segítségemre, hogy meghatározhassam mely menedzsment szigetek esetében áll rendelkezésre a sziget csatolásához felhasználható központi switch. A központi switch egyik ideális esete a 15. ábrán bemutatott külső iroda menedzsment hálózatában található eszköz, amely a csillag topológia közepén áll. Ennek a switchnek az OOB Core eszközökhöz való csatolása elégséges ahhoz, hogy a sziget teljes menedzsment hálózatát elérhetővé tegyük az OOB hálózaton keresztül. Ennek ellenére a kapcsolati rajz készítésekor nyilvánvalóvá vált, hogy a csillagtopológia központi eleme nem felel meg a követelményeknek. Ez az eszköz egy Cisco SG 300 szériás switch, amely a 3.1.1 fejezetben közölt információk alapján nem támogatja a routing protokollok használatát. Bár valójában a routing funkcionalitás hiánya nem tartozik a kapcsolati rajz fókuszába, a problémát mégis az eszköz teljesítményének és szabad kapacitásának ellenőrzése közben azonosítottam, amelyek a már a rajzhoz kapcsolódó információk. A probléma feloldására a legegyszerűbb mód, ha kicserélem a központi SG 300 switchet egy minden kritériumnak eleget tevő eszközre.

A külső adatközpontban és az ipari szeparációban hasonló menedzsment hálózat került kialakítása, így azok topológiájának központi szerepét két-két Cisco 9200 szériás switch tölti be. Ezek közül kezdetben szigetenként egyet tervezek közvetlenül az OOB

hálózathoz csatlakoztatni, a másik pedig később redundáns kapcsolat kiépítésére alkalmazható. Ezen szigetek esetében nincs szükség sem cserére, sem bővítésre. A kapcsolati rajzon jelölt interfészek szabadon rendelkezésre állnak.

Végül az Informatika épületet, mint menedzsment szigetet is szerepeltettem a tervrajzon. Látható, hogy ennek két szervertermében találhatók a DWDM egységek, amelyeken keresztül megvalósul a majd a külső iroda és a külső adatközpont szigetek csatlakoztatása az OOB hálózathoz, továbbá itt található a VPN koncentrátor klaszter egyik résztvevője és az egyik OOB Core eszköz is. Visszatekintve a 16. ábrára, amelyen ezen szervertermek menedzsment hálózata látható, azt a következtetést vontam le, hogy mindenképp szükség lesz disztribúciós eszközök telepítésére. A döntést két érvvel támasztom alá, amelyek közül az első az, hogy az itt található menedzsment eszközök kivétel nélkül SG 300 szériás Cisco switchek, tehát ezek egyike sem alkalmas a menedzsment hálózat csatolására. A másik érvem pedig, hogy a kapcsolati tervrajzon meghatározott új és meglévő OOB disztribúciós switchek mind Cisco 9200 szériás switchek, így az informatika épület szervertermeiben is ilyen eszközöket lenne célszerű OOB disztribúcióként alkalmazni.

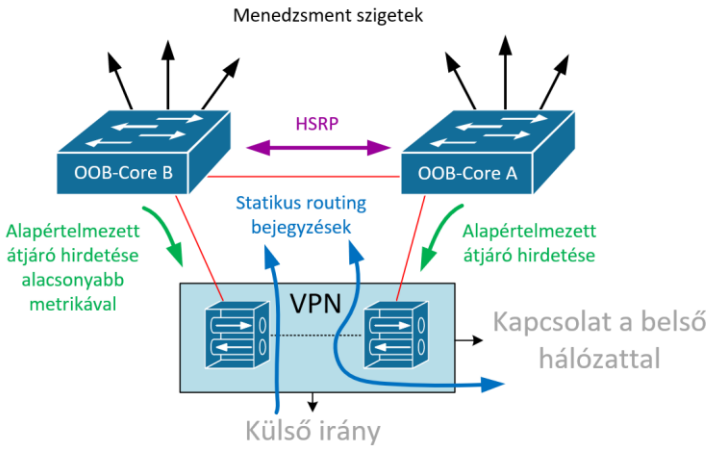
4.1.2.3 Routing

A kapcsolatok részletes megtervezése után már pontos képet kaptam az OOB hálózat jövőbeli kinézetéről. Egyetlen fontos részlet hiányzik ahhoz, hogy megkezdődhessen a kivitelezés folyamata. Ez a részlet a routing eljárás kidolgozása. Routingra szükség van, hisz az OOB hálózatra a VPN koncentrátor felől érkező forgalomról az OOB Core switcheknek valamilyen módon továbbítaniuk kell a csomagokat a megfelelő menedzsment sziget felé. A továbbiakban ismertetem az OOB hálózaton alkalmazott routing eljárást.

Az OOB hálózat belső útválasztásának bemutatása előtt azonban ismertetem, hogy hogyan jut majd el a célforgalom az új OOB hálózat Core eszközeihez. A gerinchálózat tervezéséről szóló szakaszban már említettem, hogy a VPN koncentrátor biztosít majd kapcsolatot belső hálózattal, illetve segítségével külső irányból is elérhető lesz majd a hálózat. Ennek feltétele, hogy a belső vállalati hálózatból, illetve a külső VPN irányból indított csomagok az OOB Core switchek felé kerüljenek továbbításra, amennyiben a csomagok célja valamelyik menedzsment sziget tartományában található. Ennek feloldására kezdetben felmerült az ötlet, hogy dinamikus routing protokollt,

például OSPF protokollt alkalmazzunk a VPN koncentrátoron, ami hirdeti a menedzsment tartományok irányát. Ezt az ötletet azonban a vállalati konzulensemmel egyeztetve elvetettük, azzal az indokkal, hogy viszonylag kevés (kevesebb mint 10) menedzsment tartomány forgalomirányítására egyszerűbb megoldás statikus routing bejegyzésekkel megadni a következő ugrás címét vagy a kimenő interfészt. Emellett a VPN koncentrátor jelenleg is továbbít más forgalmakat, amelyek szintén statikus routing bejegyzések alapján történnek, így nem találtuk indokoltnak megtörni ezt a konvenciót. Tehát a belső és külső irányból érkező és a menedzsment tartományoknak címzett forgalom statikus routing alapján érkezik majd meg az OOB Core switchekre.

A konkrét megvalósítás szemléltetésére készítettem a következő ábrát:



23. ábra: Elvi rajz az útválasztás működéséről.

Látható, hogy a VPN koncentrátor és a Core switchek között VLAN trunk módban működő interfészek kerültek beállításra. Ennek megfelelően a Core eszközökön a VLAN ID-val megegyező VLAN interfészeket is definiáltam, amelyeken a 3.6 fejezet alapján HSRP-t állítottam be. A VPN koncentrátor tehát a HSRP-ben lévő eszközök virtuális IP címére továbbítja a forgalmat.

A létrehozott VLAN interfészek címzésével felmerülhet a kérdés, hogy pontosan milyen címtartományból kerüljenek a címek kiválasztásra, illetve milyen VLAN ID alkalmazható. Az OOB hálózat esetében a vállalati konzulensem javaslatára külön HSRP alhálózatot definiáltam és új VLAN ID-t vezettem be. Nem csak a Core és VPN eszközök közötti kapcsolatokra, hanem a Core és az egyes menedzsment szigetek disztribúciói számára is létrehoztam úgynevezett transzfer alhálózatokat, amelyek alapján osztottam ki az IPv4 címeket a kapcsolódó interfészek között. A dedikált transzfer alhálózatok

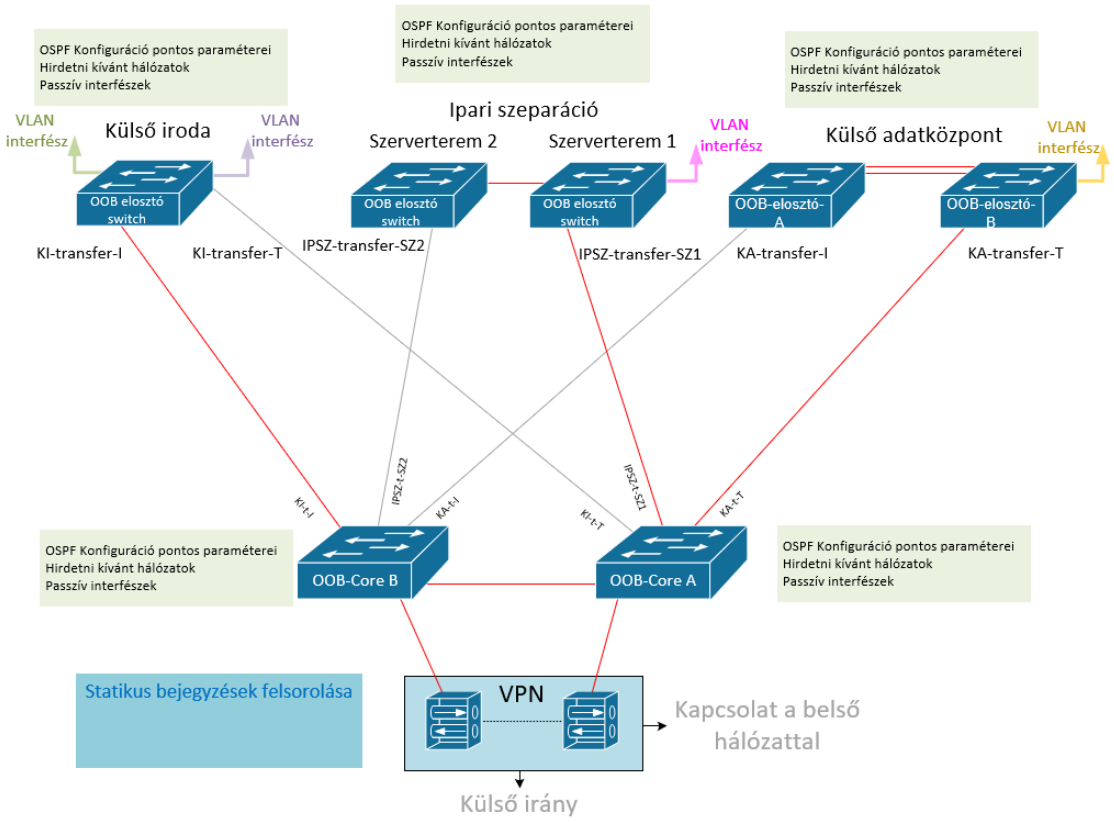
alkalmazása lehetővé teszi, hogy olyan címeket oszthassak ki ezeken az interfészeken, amelyek a hálózaton sehol máshol nincsenek használatban, így nem okoz törést a korábban definiált alhálózatok használatának konvenciójában. Természetesen ezen alhálózatok használatának első lépéseként ellenőriztem a vállalat IP nyilvántartó rendszerét és az ott látottak alapján választottam ki azokat.

Jelen állapot szerint az ismertetett routing beállítások után a menedzsment tartományoknak címzett csomagok már megérkeznek a HSRP-ben aktív szerepet betöltő Core switchre. Már csak az a kérdés maradt tisztázatlan, hogy milyen routing eljárással kerüljenek útválasztásra a menedzsment szigetek.

Ezen kérdés kapcsán is felmerült a statikus útválasztás lehetősége. Azonban hosszútávon a cél, hogy minden menedzsment sziget mind a két Core switchcsel kapcsolatban álljon. Az ilyenfajta redundancia helyes kialakítása meglehetősen bonyolult lenne statikus útválasztás alkalmazásával. Továbbá a statikus bejegyzések egy bizonyos komplexitású hálózatnál nehezen átláthatóvá tehetik az útválasztás folyamatát.

Az OSPF protokoll a 3.7 alfejezetben ismertetett tulajdonságai alapján több szempontból is jobb megoldást jelenthet. Az OSPF protokollal a statikus megoldásnál sokkal könnyebben kialakítható a redundáns topológia. Emellett az útválasztás folyamata is átláthatóbb lesz. Továbbá új szigetek csatolása is egyszerűen megoldható és a redundáns linkekre történő sikeres átálláshoz kevesebb tervezésre van szükség, bővebben kifejtve az OSPF protokollnál nem szükséges útvonal költségeket (metrikákat) megadni, míg statikus bejegyzések esetében igen. Ez alól kivétel az OOB Core eszközök OSPF konfigurációja, amely minkét eszköz esetében alapértelmezett átjárót hirdet a VPN koncentrátorok felé. Az erre vonatkozó két bejegyzéshez olyan metrikák kerültek beállításra, hogy a forgalom a VPN koncentrátor klaszter aktív elemével kapcsolatban álló Core switchen keresztül kerüljön továbbításra.

Az eddig ismertetett döntések és információk alapján, amelyben a konzulensem meglátásai is tükröződnek, elkészült a routing pontos paramétereit leíró harmadik tervrajzom. Ez az elvi rajz már csak a folyamatban résztvevő hálózati komponenseket szerepelteti, a komponensek mellett pedig a szükséges konfigurációs beállításokat, amelyekkel a helyes útválasztás biztosítható.



24. ábra: Tervrajz részlet az útválasztás folyamatát leíró tervrajzból.

A routing eljárást leíró tervrajz tetején láthatók az egyes menedzsment szigetek disztribúciós eszközei, középen az OOB hálózat Core switchei találhatók és alul pedig a VPN koncentrátor. Pirossal jelöltem azokat a kapcsolatokat, amelyek elsőként élesítésre kerülnek és szürkével azokat, amelyekkel a redundancia megvalósítható lesz később. A zöld téglalapokból a pontos OSPF konfigurációk olvashatók ki az eredeti rajzon. Továbbá jelöltem VPN koncentrátor két logikai irányát is.

4.1.3 Tervezési fázis összegzése

A vállalat menedzsment hálózatának feltérképezése és egy átfogó tervrajzon való megjelenítése nagyban segítette a fejlesztéseket leíró tervek készítését. Elkészítése közben nemcsak a topológiával kapcsolatban, hanem az egyes menedzsment eszközök kezelésében is tapasztalatot szereztem.

Ezen tapasztalataimat a kapcsolati rajz készítésénél kamatoztathattam, ugyanis fény derült rá, hogy egyes switchek nem rendelkeznek a szükséges funkciókkal, így azok cseréjét már a tervezés korai szakaszában, a munkafolyamatok közé tudtam sorolni. A kapcsolati rajzzal párhuzamosan végzett felmérések garantálják, hogy a kábelezés során minden összeköttetés számára rendelkezésre áll megfelelő mennyiségű szabad interfész

az eszközökön. Továbbá az OOB hálózat ezen nézete segít meghatározni, hogy mely épületek között lesz szükség szabad optikai szálpárokra, illetve segít meghatározni a patch kábelek és az SFP modulok számát is.

Az OOB hálózat útválasztását összefoglaló tervrajz gyors áttekintést biztosít a routing megértéséhez, amiben szintén segítséget nyújtanak a pontos konfigurációkat tartalmazó szövegdobozok, amelyek tartalma közvetlenül felhasználható a változtatások alkalmazásakor. Az eredeti tervrajzban található IP címek alapján könnyű megérteni az ezekre vonatkozó konvenciókat, így a tervrajz hasznos lehet a későbbi bővítések eszközölésekor.

4.2 Tervezett fejlesztések implementálása

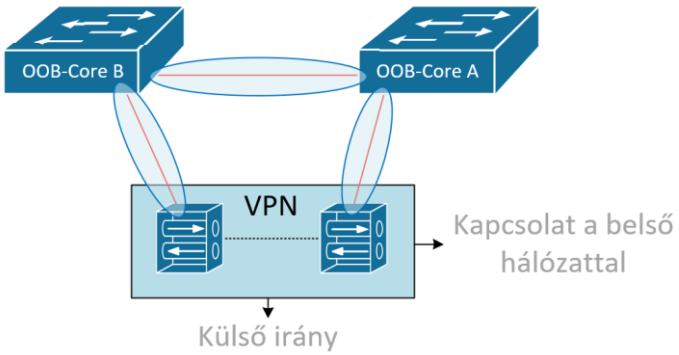
A tervezés során elkészített dokumentumok segítségével kezdetét veheti az Out-of-Band menedzsment hálózat kiépítése. Az alábbiakban bemutatom a fejlesztésekhez kapcsolódó munkám főbb lépcsőfokait.

4.2.1 Gerinchálózat kiépítése

Az OOB gerincének kiépítése a két darab Cisco Catalyst 3850 szériás switch konfigurációjával kezdődött. Az alapbeállításokkal kezdtem, amelyek közül a jelentősebbeket a 3. fejezetben részletesebben is bemutattam. Ezek a teljesség igénye nélkül az NTP szerver, az AAA beállításai, az SNMP, a logszerver és az SSH elérést foglalják magukban. A következő lépés az interfészek előkonfigurációja volt. A VPN koncentrátorral és a két Core egymással összekötött interfészein a terveknek megfelelően VLAN Trunk módot konfiguráltam, továbbá létrehoztam a megfelelő VLAN interfészeket és beállítottam a HSRP-t a VPN koncentrátor irányába. A címzéshez a vállalat IP cím nyilvántartó rendszerében bejegyeztem egy még nem használt C osztályos hálózatot (supernetwork), amelyet kisebb alhálózatokra (subnet) bontva hoztam létre a 4.1.2.3 alfejezetben említett transzfer hálózatokat. A disztribúciókat bekötő interfészeket L3 interfész módba kapcsoltam és a megfelelő transzfer hálózatok IP címeit osztottam ki rájuk. Miután minden szükséges beállítást elvégeztem, beszereltem egy kollégám segítségével az OOB hálózat Core switcheit a tervezési fázisban meghatározott szerverhelyiségekbe. Végül a 3.3 alfejezetben leírt kábelezési szempontokat és irányelveket figyelembevéve kialakítottam az eszközök közötti fizikai összeköttetéseket.

Az interfészek engedélyezése után ellenőriztem azok státuszát, majd ICMP (Internet Control Message Protocol) üzenetekkel ellenőriztem a linkek megfelelő működését.

A megvalósított fejlesztések szemléltetésére a továbbiakban az útválasztás leírására készített rajzot használom alapként, amelyen minden fázis végén kiemelem a változtatás eredményeképp létrejött új állapotokat.



25. ábra: Tervrajz részlet az útválasztást leíró rajzból. A kék oválisok jelölik az új kapcsolatokat.

4.2.2 Külső adatközpont csatolása az OOB hálózathoz

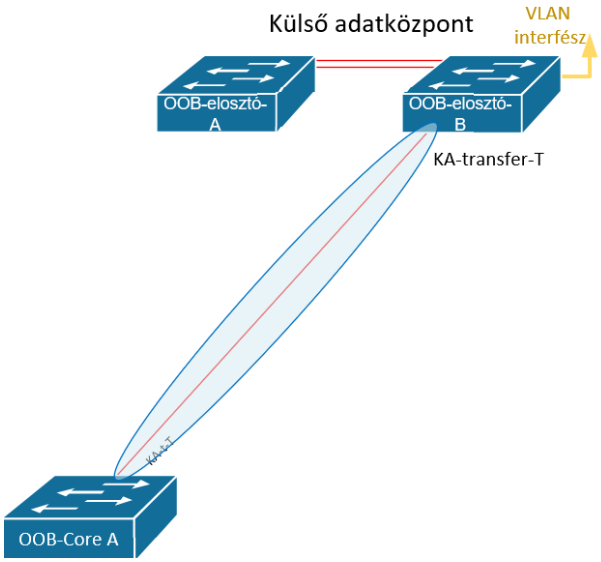
Ahogy a 4.1.1.1 alfejezetben is említettem ezen menedzsment sziget csatolása valósítható meg a legkönnyebben. Ehhez nagyban hozzájárul, hogy ott található hálózatrész a munkám ideje alatt még a fejlesztési stádiumában tartott, vagyis az ott található eszközök még csak teszt üzemmódban működtek, így nem volt szükség előre egyeztetett karbantartási időt kérnem ahhoz, hogy változtatásokat végezhessek a hálózaton.

Annak érdekében, hogy a külső adatközpont menedzsment hálózata az OOB Core eszközökön keresztül váljon elérhetővé fizikai összeköttetésre volt szükség az egyik Core switch és a sziget egyik disztribúciós eszköze között. Ezt a DWDM technológia tette lehetővé. A DWDM hardverkomponensek portjait a kollégáim által tervezett tervrajzok alapján választottam ki, hogy biztosan olyan portot használjak fel, amelyre nem vonatkozik semmilyen jövőbeli egyéb felhasználási cél. A kapcsolatok kialakítása után következett a linkek felkapcsolása és a helyes működés ellenőrzése. A folyamat sikere után egy kollégám támogatásával elvégeztem az OSPF beállításokat, mind a Core, mind a disztribúció oldalán. Az OSPF beállítások teszteléséhez ellenőriztük a szomszédosság kialakulását az eszközökön. Miután minden eddig elvégzett módosítást megfelelőnek találtunk, már csak az volt hátra, hogy a menedzsment forgalom eddigi irányát megszüntessük és létrehozzuk az új, OOB hálózaton keresztül vezető irányt. Ennek

elvégzése előtt egyeztettünk a szerverüzemeltető kollégákkal, hogy biztosan ne okozzunk nekik váratlan kiesést az általuk felügyelt rendszerek elérésében. A forgalom áttereléséhez néhány produktív eszközön létrehozott statikus routing bejegyzést kellett módosítani, jobban mondva újra definiálni ahhoz, hogy a külső adatközpont menedzsment alhálózata az eddig alkalmazott produktív disztribúció iránya helyett a VPN koncentrátorra kerüljön továbbításra. A VPN koncentrátoron egy statikus bejegyzés írja le, hogy ezen tartományhoz az OOB hálózat Core eszközén keresztül vezet az út. Az oda megérkező forgalom pedig az OSPF protokoll segítségével jut el a célállomásokhoz.

A routing beállítások mellett, további fontos lépés volt még a forgalom engedélyezése az új útvonalon található tűzfalon és a régi kapcsolatot biztosító disztribúció megfelelő interfészének lekapcsolása.

Az átállás sikerességének bizonyításához meggyőződtünk arról, hogy a forgalom valóban a tervezett útvonalon keresztül éri el az adott menedzsment tartományt. A tesztet a köztes eszközök IP címeinek és a traceroute parancs eredményeinek összevetésével kiviteleztük. Végül a hálózat felügyeleti rendszerének felületén megbizonyosodtunk arról, hogy minden a tartományhoz tartozó állomás és szolgáltatás megfelelően működik.



26. ábra: Tervrajz részlet az útválasztást leíró rajzból. A menedzsment sziget már a jelölt linken keresztül érhető el.

4.2.3 Ipari szeparáció menedzsment hálózatának csatolása

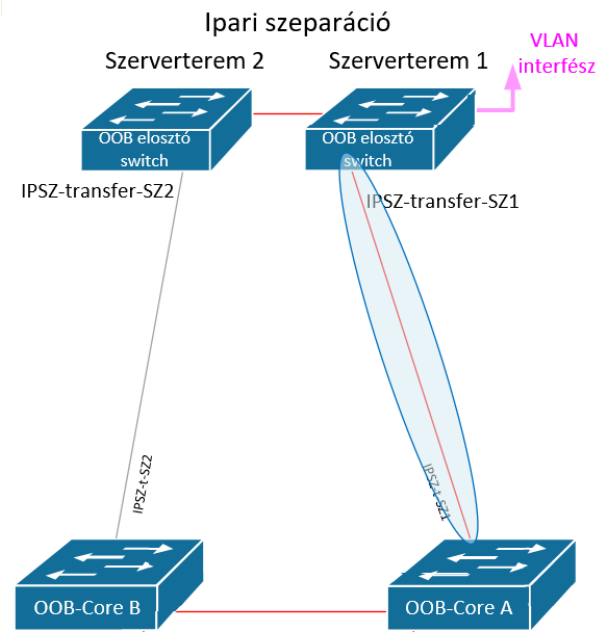
Ez a menedzsment sziget annyiban tér el a többitől, hogy disztribúciós switch helyett egy az ipari rendszereket védő tűzfal biztosítja a kapcsolatát a belső hálózattal. Tehát az átállásnál ezt a kapcsolatot kell majd megszűntetni, annak érdekében, hogy csak

az OOB hálózaton keresztül vezető útvonalon legyenek elérhetőek az itt található állomások.

Az ipari hálózatnak kiemelt szerepe van a vállalat működésében, ezért az azon végrehajtandó módosítások kizárólag előre meghirdetett karbantartási időben végezhetők el. Ennek megfelelően engedélyt kértem egy előre meghatározott időpontban a változtatások végrehajtásához. Az engedély igénylésénél konkrétan meg kell adni a változtatás célját, lépéseit, az érintett eszközök azonosítóját, egy tesztelési és visszaállási tervet. Ezen szükséges információk gondos összegyűjtésének eredményéül nem csak engedélyt kaptam a tervezett időpontban a munkára, de én is tisztábban láttam a sziget átállításának folyamatát.

Az átállással kapcsolatos előkészületek ebben az esetben is a fizikai összeköttetések létrehozásával kezdődtek. Ehhez a saját tervrajzaimon túl más dokumentációkat is felhasználtam, annak érdekében, hogy az épületek közötti optikai átkötések pontos paramétereit meghatározhassam. A kapott időablakban elvégeztem a kábelezési munkákat, majd a korábbiakhoz hasonló módon teszteltem a linkeket. Ezután következett az OSPF beállítások elvégzése az OOB Core switchen és a menedzsment sziget korábban kijelölt disztribúciós eszközén, majd a szomszédosság tesztelése. A következőkben a konzulensem és egy kollégám segítségével megszakítottuk a menedzsment tartomány kapcsolatát a fentiekben említett tűzfallal, majd elvégeztük az új irányban található tűzfalon a szükséges beállításokat például hálózat felügyeleti rendszer eléréséhez, továbbá a produktív hálózat routing bejegyzéseit módosítottuk, hogy ezen menedzsment tartomány a régi irány helyett az OOB hálózaton keresztül legyen elérhető csakúgy, mint a külső adatközpont esetében.

Végül az átállás ellenőrzéseként eszközök elérését teszteltük SSH kapcsolatok kezdeményezésével és meggyőződtünk róla, hogy a hálózati felügyeleti rendszerben nem találhatók a munkákhoz köthető riasztások. Fontosnak tartom kiemelni, hogy a menedzsment sziget korábbi betáplálását biztosító kapcsolatot nem bontottuk el véglegesen, így indokolt esetben akár visszaállítható a fejlesztés előtti állapot.



27. ábra: Tervrajz részlet az útválasztást leíró rajzból. A menedzsment sziget már a jelölt linken keresztül érhető el.

4.2.4 Külső iroda menedzsment átállása az OOB hálózatra

Két menedzsment sziget sikeres átállása után folytattam a fejlesztéseket méghozzá a külső iroda menedzsment hálózatának előkészítésével. A tervezési fázisban már említettem, hogy az ott található menedzsment switchek csillag topológiát alkotnak, így annak központi eszközét lenne érdemes a sziget disztribúciójaként alkalmazni. Azonban hamar nyilvánvalóvá vált, hogy az a központi switch nem felel meg a szükséges követelményeknek. Ha meg akarom őrizni az eredeti topológiát, ahhoz egy megfelelő eszközzel kell helyettesítenem a jelenlegit.

Az eszköz pótlására Cisco Catalyst 9200 szériás switchet választottam, mivel az előző két menedzsment szigetnél is ilyen switchek töltik be a menedzsment hálózat disztribúciójának szerepét.

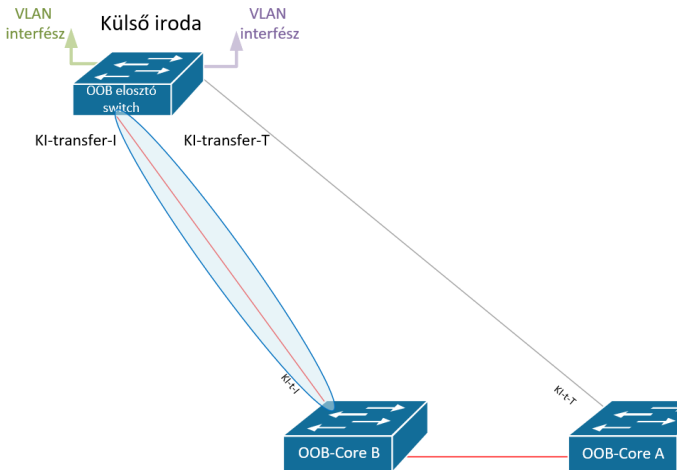
Mivel a külső iroda hálózata is produktív hálózat, így itt csak engedéllyel és előre egyeztett időpontban végezhetek átalakításokat. Ilyenkor törekedni kell arra, hogy az átalakítás a lehető legkevesebb kiesést okozza, ezzel együtt pedig a lehető legkisebb időablak alatt elvégezhető legyen. A lehető leggyorsabb átálláshoz megpróbálok minden olyan lépést, ami nem engedélyköteles már az engedélyezett időkeret előtt elvégezni.

Ennek nyomán a kiválasztott eszköz konfigurálásával kezdtem. Elvégeztem az alapbeállításokat, majd a jelenleg üzemben lévő központi switch konfigurációs

beállításainak mintájára elvégeztem többek között az interfészek, a VLAN interfészek és a VLAN-ok beállítását. Azzal, hogy az interfészek konfigurációt a régi eszköz interfész számozásának megfelelően végeztem az új eszközön is, elértem, hogy az access portok régi switchről való átkötésénél az újra, csak a számozás követésére kelljen ügyelni. Ezzel is gyorsul majd a folyamat. A konfiguráció végeztével kiszállíttattam az új switchet a külső irodába, majd beszereltem a jelenlegi központi switchhez legközelebb eső szabad pozícióba. Ezután pedig tápellátást biztosítottam az eszköznek, továbbá kialakítottam az egyik fizikai kapcsolatát a szintén a szerverhelyiségben található DWDM hardveregységgel. Következő lépésként DWDM kapcsolat másik oldalán található egységet kapcsoltam a megfelelő interfészen keresztül az egyik OOB Core switchre. Az így létrehozott kapcsolat lehetővé tette, hogy az új központi switchet még az átállás előtt teszteljem például OSPF beállítások szempontjából.

Ezen lépések véghezvitelére azért volt lehetőségem, mert elvégzésük semmilyen kihatással nem járt a produktív hálózatra nézve. Ugyanakkor a menedzsment sziget tényleges átállásakor már nem kell majd a fizikai beszereléssel, illetve a Core kapcsolatának kiépítésével foglalkozni.

Minden lehetséges előkészítési munkálat elvégzése után már csak a tényleges átállás megvalósítása volt hátra. Ezt az engedélyezett időablakban végeztem, a feladatok elvégzéséhez pedig most is kaptam segítséget. A munka első fázisában elvégeztem a régi eszköz access portjaira csatlakoztatott kábelek átkötését az új eszközre. A továbbiakban az eddigiekhez hasonló feladatokat és tesztelési lépéseket végeztük el. Röviden összefoglalva lekapcsoltuk az eddig használt produktív disztribúció megfelelő interfészét, annak IP címét használtuk az új disztribúció VLAN interfészéhez, mivel ez a cím van beállítva a többi menedzsment switchen alapértelmezett átjáróként. Ezután routing bejegyzések módosítása következett a produktív hálózat és az OOB érintett eszközein. Végül pedig az új routing útvonalán található tűzfalon létrehoztuk az engedélyező szabályokat, majd teszteltük a helyes működést. A tesztelésben a szerverüzemeltető kollégák is részt vettek, mivel általuk felügyelt eszközök menedzsment elérése is megváltozott. A monitoring rendszer, az ICMP üzenetek, SSH kapcsolatok pozitív visszajelzései alapján az átállást sikerrel zártuk.



28. ábra: Tervrajz részlet az útválasztást leíró rajzból. A menedzsment sziget már a jelölt linken keresztül érhető el.

4.2.5 Az informatika épület menedzsment hálózata

A munkám ismertetése során többször kihangsúlyoztam, hogy az informatika épület különálló szervertermeiben kialakított menedzsment hálózat működése felvet néhány olyan kérdést, amelyeknek tisztázása nélkül a sziget átállítása az OOB hálózatra nem várt mellékhatásokkal járhat. A következő alfejezetben bemutatom ez imént említett menedzsment sziget csatolásával kapcsolatos munkámat.

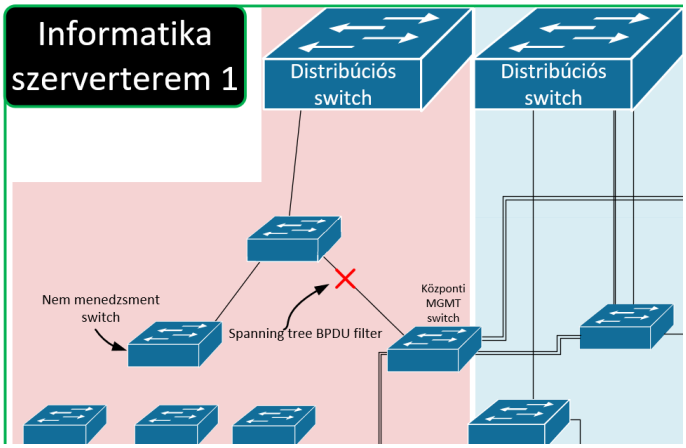
Az előzetes felmérések azt mutatták, hogy két menedzsment célú alhálózat, ezekhez pedig külön VLAN ID-k vannak jelen a két szerverterem menedzsment eszközein. A két eltérő tartomány két eltérő disztribúcióhoz tartozik. Ez idáig nem jelent gondot, hiszen ebben az esetben akár külön menedzsment szigetnek is tekinthetnénk a két tartományt és csatolásukat az OOB hálózathoz külön is megvalósíthatnánk. Azonban nem vagyunk biztosak abban, hogy mindkét tartomány csatolása indokolt. A cél nem csak az, hogy az itt található menedzsment tartományokat elérhetővé tegyem az OOB hálózaton keresztül, hanem ezzel párhuzamosan felmérjem a tartományokban található eszközöket és azok funkciója alapján döntsem el, hogy az adott tartomány csatolása indokolt vagy sem.

Az egyes tartományokba tartozó IP címeket birtokló állomások felmérése választ adhat a kérdésre. Ez persze nem jelenti azt, hogy minden használatban lévő címet ellenőriztem a szóban forgó alhálózatokból. Helyette készítettem egy táblázatot, amiben rögzítettem a két szerverhelyiségben található összes menedzsment switch (16 darab) összes portjával kapcsolatos információt. Ilyen információ volt például a port konfigurációja, vagyis, hogy access vagy Trunk móban van és attól függően, hogy melyik

módba van konfigurálva, milyen VLAN vagy VLAN-ok elérését vagy továbbítását engedélyezi. Emellett rögzítettem a CDP parancs eredményét is az adott interfészeknél.

Az adatok összegyűjtése és egy egyszerű struktúrába való beillesztése rengeteg felesleges munkát spórolt meg, ugyanis az eredmények egyértelműen azt mutatták, hogy a switchek döntő többségében csakis az egyik menedzsment tartományhoz tartozó VLAN ID van használatban az access portokon, míg a másik tartományból csupán magának a switchnek a menedzsment IP címe származott. Egy esetben találtam olyan, nem is biztos, hogy menedzsment célra telepített switchet, melynek az access portjai a másik tartományhoz tartozó VLAN elérését tették lehetővé. Tapasztaltabb kollégáim erről a switchről azt nyilatkozták, hogy valóban nem menedzsment szerepet tölt be a hálózatban, csupán ismeretlen okból szoros kapcsolatban áll a menedzsment hálózattal.

Ez egyrészt azt jelenti, hogy amennyiben a menedzsment switchek címét megváltoztatom abból a tartományból való címre, amit amúgy is kiszolgálnak, akkor azzal a másik tartomány csatolására nincs szükség. Másrészt pedig azt jelenti, hogy fel kell mérnem a menedzsment hálózaton felfedezett, de nem menedzsment szerepet betöltő switch több aktív kapcsolata közül azt, melyiket használja a disztribúció elérésére. Erre azért van szükség, mert ha olyan kapcsolaton keresztül éri el a disztribúciót, amely menedzsment eszközökön keresztül vezet, abban az esetben, új, a menedzsment hálózattól független kapcsolatot kell számára létrehozni a disztribúcióhoz. A használt irány felderítéséhez az egyes irányokban alkalmazott, a 3.4 fejezetben is ismertetett STP beállításokat elemeztem. A beállítások alapján egyértelműen igazolható, hogy ez a különálló switch nem a menedzsment hálózaton keresztül éri el a disztribúciót.



29. ábra: Kiegészített tervrajz részlet az informatika épület menedzsment hálózatáról. Az STP beállítás bizonyítja, hogy a forgalom nem a menedzsment hálózaton keresztül jut el a disztribúcióig.

Ezzel minden akadály elhárult az átállás megvalósítása elől. Ezért az előkészületek kezdő lépéseként telepítettem mindkét szerverhelyiségbe egy-egy Cisco Catalyst 9200 switchet, amelyek HSRP-t alkalmazva töltik majd be az OOB disztribúció szerepét. Két eszköz alkalmazására azért van szükség, mert így a helyiségek közötti átkötésre egyetlen optikai szálpárra van szükség a két disztribúció összekötéséhez. Amennyiben csak egy eszközt telepítek, úgy az egyik szerverhelyiség minden menedzsment switchének uplink kapcsolatát optikai szálpárokon keresztül kellene továbbítani a másik szerverhelyiségbe, ahol az OOB disztribúció található. A HSRP- re pedig megbízhatóbb működés mellett azért is szükség van, mert így a két disztribúció ellenére használhatok majd egyetlen alapértelmezett átjáró címet, melyet virtuális címként állítok majd be, és amelyet jelenleg is használnak a menedzsment switchek.

Jelenleg a disztribúciós switchek már telepítésre kerültek és a kapcsolataik is aktívak az OOB Core eszközökkel. Emellett megterveztem az átállás folyamatát. A közeljövőben kijelölésre kerül az átállás időpontja is. A sikeres megvalósítás után kimondható, hogy a Richter Gedeon Vegyészeti Gyár budapesti telephelyének menedzsment hálózata immár az OOB elveinek megfelelően működik.

5 Értékelés

Összefoglalva elmondható, hogy a munkám jelentős részét a tervek előkészítése töltötte ki, amelybe beletartozik a hálózat feltérképezése is. A tervezési feladatok által nem csak a menedzsment hálózatról szereztem hasznos információkat, hanem a tervkészítéséről, mint feladatkörről is. A folyamat során véleményem szerint egyre inkább sikerült a ténylegesen szükséges információkat rögzítenem és azokat olyan módon megjeleníteni, ami talán más kollégák számára is könnyen értelmezhető. A tervrajzok hasznosságának talán hiteles bizonyítéka lehet, hogy a menedzsment hálózaton végzett változtatások során sokszor támaszkodtam a bennük összegzett információkra.

A megtervezett átalakítások sikerességének kulcsa a precíz, alapos felkészülés volt. A tervezéshez hasonlóan ezen a területen is minél többet tapasztaltam annál inkább képessé váltam elsőre látni a következő lépéseket és figyelmet fordítani az azokhoz tartozó részletekre is. Egy-egy változtatás végrehajtása ugyanakkor rendkívül komplex feladat volt, amelyhez nem csak a menedzsment hálózat ismeretére volt szükség. Ezen feladatok elvégzéséhez, mindig kaptam kellő segítséget és ennek köszönhetően sokat fejlődtem a produktív eszközök kezelésében is.

A feladat teljesítése érdekében felmértem és tervrajzon részleteiben ábrázoltam a vállalat menedzsment hálózatát. Ennek alapján megterveztem a kialakítandó OOB hálózat szerkezetét és fizikai kapcsolatait, valamint meghatároztam az útválasztáshoz szükséges beállításokat, amelyeket egy harmadik nézetben ábrázolt tervrajzon rögzítettem. Az elkészült dokumentumok alapján a legkevesebb kockázattal járó menedzsment sziget OOB hálózatra való átállításán kezdtem dolgozni. Ezt követte az ipari informatikai hálózat menedzsment eszközeinek csatolása, amely a meglévő elrendezésnek köszönhetően kevés változtatással is sikeresen átállítható volt. A külső iroda menedzsment hálózatán eredményesen végeztem el módosításokat, amelynek köszönhetően ezen sziget csatolása is megvalósulhatott. Végül pedig az informatika épület szervertermein végzett munkámat szeretnék kiemelni, amelynél véleményem szerint sikerült egyszerű módszerekkel igazolnom a feltételezéseimet. Továbbá elvégeztem az átálláshoz szükséges előkészületeket.

Az új OOB hálózat jelenleg a 23. ábrán piros vonallal jelölt linkeken keresztül működik. Szürke vonallal jelöltem azokat az összeköttetéseket, melyek jelenleg még nem

aktívak, azonban van lehetőség a jövőben kialakítani ezeket a kapcsolatokat, ezzel biztosítva a szigetek redundáns bekötését. A legtöbb menedzsment switch esetében – amely állomások menedzsment interfészeinek kapcsolatát biztosítja – elérhető új szoftver verzió, amely telepítésének számos előnye közül a TACACS támogatást emelném ki. Az eszközök számát tekintve a frissítések elvégzése történhet akár szakaszokban is, vagy elvégezhető több kollégát bevonva egy leállás keretén belül akár egyidőben is. Én mindenképpen fontos feladatnak tartom a jövőben, hogy az OOB hálózat eszközei is naprakész verziójú szoftvert futtassanak.

A projekt jelen állapotát és az ehhez vezető döntéseket végig gondolva vétettem egy hibát. Az OOB hálózat Core eszközeinek telepítésekor felmerült az egyik eszköz esetében, hogy egy másik szerverhelyiségben kellene elhelyezni, mivel a vállalat hosszútávú terveit tekintve annak a helyiségnek biztosabb a fennmaradása. Én ennek ellenére az általam választott helyiségbe telepítettem az eszközt, mert így a tervezett kapcsolatait egyszerűbb volt kiépíteni. Időközben biztossá vált, hogy a jövőben az eszközt át kell majd helyezni, jóllehet nem a közeljövőben, de az áthelyezés munkálatai megspórolhatók lettek volna, ha kérdést jobban megvizsgálom, felmérem mennyivel több munkát jelentett volna a kapcsolatok kialakítása a másik helyiségben és úgy döntök, hogy oda telepítem az OOB hálózat egyik központi eszközét.

Összegezve eredményeimet és tapasztalataimat, úgy gondolom sikerült értéket adnom a vállalatnak azzal, hogy növeltem a menedzsment hálózat megbízhatóságát. Emellett számos visszajelzést kaptam a kollégáktól az elkészített dokumentációkkal kapcsolatban, így már azt is külön előnynek tekintem, hogy naprakész információk állnak rendelkezésre erről a hálózatrészről is. A munkám során nem csak a célt tartottam szem előtt, hanem azt is, hogy a jövőben más szakemberek által a menedzsment hálózaton végzett munkák is könnyen tervezhetők és implementálhatók legyenek. Ugyanakkor vannak fejlesztési lehetőségek, amelyek egy részét én magam tervezem elvégezni és vannak olyanok, amelyek elvégzéséről csapat szinten kell döntést hozni.

6 Köszönetnyilvánítások

Köszönöm Dr. Holczer témavezetőmnek, hogy a szakdolgozat során ötleteivel és tanácsaival elengedhetetlen iránymutatást adott. Hálával tartozom Boór András vállalati konzulensemnek, aki a feladat kivitelezése során nyújtott szakmai tudásával, segítőkészségével és eszközökkel hozzájárult az elért eredményeimhez.

Tisztaszívvel köszönöm a Richter Gedeon Vegyészeti Gyár Network & Security csapatának a sok támogatást, ami végigkísért a munkám során.

Irodalomjegyzék

[1] Cisco.com: *Cisco 300 Series Managed Switches Data Sheet*, https://www.cisco.com/c/en/us/products/collateral/switches/small-business-smart-switches/data_sheet_c78-610061.html (2021. máj.11, 14:10)

[2] Cisco.com: *Cisco Catalyst 9200 Series Switches Data Sheet*, https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html (2021. máj.11, 14:11)

[3] TechTarget network: *Managed vs. unmanaged switches: What are the differences?* https://searchnetworking.techtarget.com/answer/What-is-the-difference-between-a-managed-and-unmanaged-switch (2021. máj.11, 17:57)

[4] ComputerNetworkingNotes: *Network Cable Types and Specifications*, https://www.computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html (2021. máj.11, 18:04)

[5] FS Community: *Network & Communication Cables That Power Your Internet*, https://community.fs.com/blog/network-communication-cables-that-power-your-internet.html (2021. máj.11, 18:07)

[6] electronicsnotes: *What is Ethernet IEEE 802.3* https://www.electronics-notes.com/articles/connectivity/ethernet-ieee-802-3/basics-tutorial.php (2021. máj.11, 18:12)

[7] Tripp Lite: *Fiber Optic Cable Buying Guide*, https://www.tripplite.com/products/fiber-optic-cable-buying-guide (2021. máj.11, 18:19)

[8] PROMAX: *Optical fiber connector types: An easy guide*, https://www.promaxelectronics.com/ing/news/578/optical-fiber-connector-types-an-easy-guide/ (2021.máj.11, 18:24)

[9] Cisco.com: *Cisco Business Switches: SFP Modules*, https://www.cisco.com/c/en/us/support/docs/smb/switches/Cisco-Business-Switching/kmgmt-1524-SFP-Modules-CBS.html (2021. máj.11, 18:27)

[10] Cisco.com: *Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet*, https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/datasheet-c78-366584.html (2021. máj.11, 18:31)

[11] SinusNetworks: *CWDM/DWDM*, http://www.sinusnet.hu/2016/01/07/cwdmdwdm/ (2021.máj.11, 18:33)

[12] SPLAYMARK TECH CO.*: xWDM for Simplex Bidirectional Fiber Transmission*, http://www.splaymark.com/xwdm (2021. máj.11, 18:36)

[13] ieee802.org: Mick Seaman, *802.1D MAC Bridges*, 2004, 802.1D-2004, IEEE, https://www.ieee802.org/1/pages/802.1D-2003.html (2021. máj. 19, 10:57)

[14] Cisco.com: *Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches*, https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html (2021. máj.19, 10:49)

[15] ComputerNetworkingNotes: *STP - Spanning Tree Protocol Explained With Examples*, https://www.computernetworkingnotes.com/ccna-study-guide/stp-spanning-tree-protocol-explained-with-examples.html (2021. máj.19, 11:07)

[16] ieee802.org: Tony Jeffree, *802.1Q-2014 - Bridges and Bridged Networks*, 2004, 802.1Q-2014, IEEE, https://www.ieee802.org/1/pages/802.1Q-2014.html (2021. máj.19, 11:14)

[17] ieee802.org: Adam Healey, *IEEE 802.3 ETHERNET WORKING GROUP*, 2021, IEEE, https://www.ieee802.org/3/ (2021. máj.19, 11:26)

[18] Firewall.cx: Chris Partsenidis, *VLAN Networks*, http://www.firewall.cx/networking-topics/vlan-networks/226-vlan-security.html (2021. máj.19, 11:33)

[19] ietf.org: T. Li, B. Cole, P. Morton, D. Li, *Cisco Hot Standby Router Protocol (HSRP)*, 1998, 2281, IETF, https://datatracker.ietf.org/doc/html/rfc2281 (2021. máj.19, 11:42)

[20] Cisco.com: *HSRP Overview And Basic Configuration*, 2019, https://community.cisco.com/t5/networking-documents/hsrp-overview-and-basic-configuration/ta-p/3131590 (2021.máj.19, 11:46)

[21] ietf.org: J. Moy, *OSPF Version 2*, 1998, RFC 2328, IETF, https://datatracker.ietf.org/doc/html/rfc2328 (2021. máj.19, 11:53)

[22] Cisco.com: Cisco Systems, *IP Routing: OSPF Configuration Guide, Cisco IOS Release 15M&T*, 2012-2014, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/iro-15-mt-book.pdf (2021. máj.19, 11:56)

[23] ManageEngine.com: *SNMP tutorial*, https://www.manageengine.com/network-monitoring/what-is-snmp.html (2021. máj.19, 13:32)

[24] ietf.org: J. Case, M. Fedor, M. Schoffstall, J. Davin, *A Simple Network Management Protocol*, 1988, RFC 1067, IETF, https://datatracker.ietf.org/doc/html/rfc1067 (2021. máj.19, 15:13)

[25] ietf.org: J. Case, M. Fedor, M. Schoffstall, J. Davin, *A Simple Network Management Protocol (SNMP)*, 1990, RFC 1157, IETF, https://datatracker.ietf.org/doc/html/rfc1157 (2021. máj.19, 15:13)

[26] ietf.org: J. Case, K. McCloghrie, M. Rose, S. Waldbusser, *Introduction to Community-based SNMPv2*, 1996, RFC 1901, IETF, https://datatracker.ietf.org/doc/html/rfc1901 (2021. máj.19, 16:13)

[27] ietf.org: J. Case, K. McCloghrie, M. Rose, S. Waldbusser, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*, 1996, RFC 1905, IETF, https://datatracker.ietf.org/doc/html/rfc1905 (2021. máj.19, 16:17)

[28] ietf.org: D. Harrington, R. Presuhn, B. Wijnen, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*, 2002, RFC 3411, IETF, https://datatracker.ietf.org/doc/html/rfc3411 (2021. máj.19, 16:33)

[29] ietf.org: J. Schoenwaelder, *Simple Network Management Protocol (SNMP) Context EngineID Discovery*, 2008, RFC 5343, IETF, https://datatracker.ietf.org/doc/html/rfc5343 (2021. máj.19, 16:44)

[30] ietf.org: D. Harrington, J. Schoenwaelder, *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, 2009, RFC 5590, IETF, https://datatracker.ietf.org/doc/html/rfc5590 (2021. máj.19, 16:44)

[31] ResearchGate: Marcin Bajer, *Topology of NTP server structure*, 2013, https://www.researchgate.net/figure/Topology-of-NTP-server-structure_fig4_259267101 (2021. máj.19, 16:54)

[32] ietf.org: David L. Mills, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*, 1992, RFC 1305, IETF, https://datatracker.ietf.org/doc/html/rfc1305 (2021. máj.19, 17:00)

[33] ntp.org: Ulrich Windl, David Dalton, *The NTP FAQ and HOWTO*, 2006, http://www.ntp.org/ntpfaq/NTP-a-faq.htm#AU-NM (2021. máj.19, 17:06)

[34] Cisco.com: Cisco Systems, *What Is a VPN? - Virtual Private Network*, https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html (2021. máj.19, 17:23)

[35] wikipedia.org: Wikipedia, *Virtual private network*, 2021, https://en.wikipedia.org/wiki/Virtual_private_network (2021. máj.21, 20:07)

[36] ietf.org: C. Rigney, S. Willens, A. Rubens, *Remote Authentication Dial In User Service (RADIUS)*, 2000, RFC 2865, IETF, https://datatracker.ietf.org/doc/html/rfc2865 (2021. máj.19, 17:20)

[37] ietf.org: T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, L. Grant, *The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol*, 2020, RFC 8907, IETF, https://datatracker.ietf.org/doc/html/rfc8907 (2021. máj.19, 17:50)

[38] 51sec.org: *Basic Cisco Tacacs+ Configuration With Free Tacacs+ Software for Windows – Part 1*, 2015, https://www.51sec.org/2015/02/08/basic-cisco-tacacs-configuration-with-free-tacacs-software-for-windows-part-1/ (2021. máj.19, 17:53)

[39] Cisco.com: Cisco Systems, *TACACS+ and RADIUS Comparison*, 2008, https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html (2021. máj.19, 17:57)

[40] Cisco.com: Martin Pueblas, *Cisco SAFE Reference Guide*, https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap9.html (2021. máj.19, 18:13)