12. Informatika és távközlés ágazathoz tartozó
5-0612-12-02
Informatikai rendszer- és alkalmazás-üzemeltető technikus
SZAKMÁHOZ

Hálózatok II. tantárgy
helyi tanterve

Összes óraszám: 324/*341* óra

13. évfolyam 324 óra (heti 10,5 óra)

2/14. évfolyam *341 óra (heti 11 óra)*

Témakörök:

	9.		10.		11.		12.		13.		1/13		2/14	
	e	**gy**	**e**	**gy**	**e**	**gy**	**e**	**gy**	**e**	**gy**	**e**	**gy**	**e**	**gy**
Dinamikus forgalomirányítási ismeretek									12	28			11	31
Hálózatbiztonság									12	28			11	31
Hozzáférési listák használata									9	21			9	23
Statikus és dinamikus címfordítás lehető-ségei									9	21			9	23
WAN-technológiák									9	21			9	23
Virtuális magánhálózat (VPN) kialakítása									12	28			11	31
Minőségbiztosítási alapok, hálózatfelü-gyelet megvalósítása									12	28			11	31
Hálózattervezés, hibaelhárítás									6	18			7	18
Hálózatvirtualizáció, hálózatautomatizáció									6	18			7	18
Komplex hálózat tervezése, kialakítása									6	20			8	19
									93	231			93	248

Elmélet: 13. évfolyam 93 óra (heti 3 óra)

2/14. évfolyam *93 óra (heti 3 óra)*

Gyakorlat: 13. évfolyam 231 óra (heti 7,5 óra)

2/14. évfolyam *248 óra (heti 8 óra)*

A tantárgy oktatása során fejlesztendő kompetenciák

Készségek, képességek	Ismeretek	Önállóság és felelősség mértéke	Elvárt viselkedésmódok, attitűdök	Általános és szakmához kötődő digitális kompetenciák
LAN-ban dinamikus forgalomirányítást tervez és valósít meg.	Irányítótábla Dinamikus forgalomirányítás, Távolságvektor-alapú és kapcsolat-állapot-alapú forgalomirányító protokoll OSPF DR BDR Router ID	Teljesen önállóan	Fogékony az információk befogadására és alkalmazására. Érdeklődik az adott téma iránt. Együttműködő és kommunikatív a csoportosan végezhető tevékenységek közben.	Hálózati szimulációs szoftver és valós hálózati eszközök használata Hatékony internetes keresés
Radius hitelesítést alkalmaz.	Biztonsági fenyegetések és a védekezési, megelőzési lehetőségek RADIUS-hitelesítés Szimmetrikus és aszimmetrikus kulcsú titkosítás	Teljesen önállóan		
Érti a forgalomszűrés jelentőségét, forgalomszűrést valósít meg IPv4 környezetben.	Forgalomszűrés Normál hozzáférési lista Kiterjesztett hozzá-férési lista	Teljesen önállóan		
Érti a címfordítás szükségességét, típusait, statikus és dinamikus címfordítást megvalósít meg.	Belső helyi cím Belső globális cím Külső helyi cím Külső globális cím Statikus NAT Dinamikus NAT Túlterheléses NAT Porttovábbítás	Teljesen önállóan		
WAN-szintű kapcsolatokat és forgalomirányítást valósít meg.	WAN-technológiák WAN-összetevők PPP eBGP	Teljesen önállóan		
Site-to-site és remote-access VPN-t konfigurál.	Virtuális magánhálózat IPSec Remote-Access VPN Site-to-Site VPN	Teljesen önállóan		
Hálózatmonitorozást és hálózatfelügyeletet végez.	Alapszintű minőségbiztosítási isme-retek QoS CDP / LLDP NTP	Teljesen önállóan		

	SNMP Syslog NetFlow TFTP			
Hálózatot tervez, hálózati hibaelhárítást végez.	Konvergált hálózat Háromrétegű hierarchikus hálózati modell Hálózati dokumentáció OSI-modell rétegein alapuló hibafelderítési eljárások Viszonyítási alap	Teljesen önállóan		
Értelmezi és meg-nevezi a hálózatvirtualizáció és -automatizáció alapjait és előnyeit.	Cloud computing Virtualizáció API REST	Teljesen önállóan		

A tantárgy témakörei

Dinamikus forgalomirányítási ismeretek

A témakör célja, hogy a tanulók megismerjék a dinamikus belső forgalomirányítás lehetőségeit, a forgalomirányító protokollok működését, és megértsék a forgalomirányító protokollok közt lévő különbségeket. Képesek legyenek a hálózat méreteinek megfelelő forgalomirányítás megtervezésére, a protokoll kiválasztására, konfigurálására, hibaelhárítására.

A témakör elvégzését követően a tanuló az alábbi ismeretekkel és gyakorlati készségekkel fog rendelkezni:

– Látja a statikus és dinamikus forgalomirányítás közti különbséget, mindkét esetben tisztában van az előnyökkel és a hátrányokkal.

– Tisztában van a dinamikus belső forgalomirányító protokollok működési elvével. Képes a dinamikus forgalomirányító protokollok csoportosítására osztályosság (osztály nélküli, osztályalapú), a felhasználás helye (külső, belső), működési mód (távolságvektor-alapú, kapcsolatállapot-alapú) szerint.

– Ismer legalább egy távolságvektor-alapú dinamikus forgalomirányító protokollt (pl. RIP, RIPv2, EIGRP), és tisztában van a működésével. Képes az általa ismert távolságvektor-alapú forgalomirányító protokoll konfigurálására, működésének ellenőrzésére, hibaelhárítására.

– Tisztában van a távolságvektor-alapú és a kapcsolatállapot-alapú forgalomirányító protokollok közti különbségekkel. Ismeri a kapcsolatállapot-alapú forgalomirányító protokollok működési elvét.

– Ismeri az OSPFv2 és OSPFv3 forgalomirányító protokollok működését, a forgalomirányítók közötti szomszédság kialakulásának feltételeit és folyamatát.

– Ismeri az OSPF által használt üzenettípusokat (Hello, DBD, LSR, LSU, LSAck) és azok szerepét.

– Tisztában van a hello és a halott időzítők szerepével, és képes azok értékét megváltoztatni.

– Ismeri az OSPF-hálózattípusokat (pont-pont, szórásos többes hozzáférés, nem szórásos többes hozzáférés, pont-többpont, virtuális összeköttetés), és tisztában van a többes hozzáférésű hálózatok kihívásaival (többszörös hozzáférési viszonyok, túlzott LSA-elárasztás).

– Tisztában van a router ID, a DR és a BDR fogalmával és szükségességével a többes hozzáférésű hálózatokban.

– Ismeri a router ID megválasztásának folyamatát, és képes a router ID értékét beállítani, illetve ennek hiányában meghatározni.

– Ismeri a DR/BDR-választás folyamatát, és képes azt befolyásolni interfészprioritás, illetve router ID módosításával.

– Ismeri a passzív interfészek szerepét, és képes megállapítani, hogy egy forgalom-irányító mely interfészét kell passzívként konfigurálni. Képes OSPFv2 és OSPFv3 esetén passzív interfész beállítására.

– Képes alapértelmezett útvonal továbbhirdetésére egyterületű OSPFv2 és OSPFv3 esetén.

– Képes egyterületű OSPFv2 és OSPFv3 konfigurálására, illetve már meglévő OSPFv2- és OSPFv3-terület kiegészítésére.

– Képes hibaelhárítást végezni egyterületű OSPFv2 és OSPFv3 esetén, ismeri a hibaelhárítás során használatos legfontosabb parancsokat.

– Tisztában van az OSPF-területek jelentőségével, a többterületű OSPFv2 és OSPFv3 működésével.

– Képes többterületű OSPFv2 és OSPFv3 konfigurálására, illetve már meglévő konfiguráció kiegészítésére, módosítására.

– Képes alapértelmezett útvonalat behirdetni többterületű OSPFv2 és OSPFv3 hálózatokba.

– Képes többterületű OSPFv2 és OSPFv3 működésének ellenőrzésére, hibaelhárítás-ára.

Hálózatbiztonság

A témakör célja, hogy a tanulók megértsék hálózatbiztonság fontosságát. Tisztában legyenek a támadási technikákkal, és képesek legyenek ezek lehetőség szerinti megelőzésére, kivédésére. A tanulók ismerjék meg a központi hitelesítés szerepét, használatának lehetőségeit, és legyenek képesek RADIUS-hitelesítés megvalósítására. A tanulók ismerjék meg a kriptográfia alapjait.

A témakör elvégzését követően a tanuló az alábbi ismeretekkel és gyakorlati készségekkel fog rendelkezni:

– Tisztában van napjaink hálózati fenyegetéseivel, a CyberSecurity jelenlegi állapotával.

– Ismeri a fenyegetés, sebezhetőség és kockázat fogalmát, a kockázatkezelés módszereit.

– Tisztában van a hacker fogalmával, fajtáival, lehetséges indítékaival.

– Ismeri az etikus hacker fogalmát és az etikus hacker által használt eszközöket (pl. jelszófeltörő programok, hálózatmonitorozó programok, csomagelfogó programok stb.)

– Ismeri a malware fogalmát, fajtáit (vírus, féreg, trójai, spyware, adware, scareware, phishing, rootkits, ransomware). Érti az egyes fajták közti különbségeket.

– Ismeri a hálózati támadások fontosabb típusait (felderítés, jogosultságmegszerzés, social engineering, szolgáltatásmegtagadás).

– Ismeri az IP-, ICMP-, TCP-, UDP-, ARP-, DNS- és DHCP-protkollok sebezhetőségeit.

– Ismeri a webes és levelezési szolgáltatások sebezhetőségeit.

– Ismeri az adatbázisok elleni támadások lehetőségeit (pl. SQL-injection).

– Képes egy kapcsolón a porttükrözés beállítására (SPAN), a hálózati forgalom meg-figyelése céljából.

– Tisztában van a hálózatbiztonsági házirend fontosságával. Tisztában van az egyes támadástípusok esetén használható megelőzési és hatástalanítási technikákkal.

– Ismeri a forgalomirányító védelmének három területét (fizikai biztonság, az operációs rendszer biztonsága, router hardening).

– Ismeri a forgalomirányítón létrehozható felhasználói szinteket, érti ezek működését, és képes forgalomirányítón különböző szintű felhasználókat létrehozni, hozzájuk jogosultságokat rendelni.

– Tisztában van a role-based CLI-hozzáféréssel, a root view, a CLI-view és a superview fogalmával, működésével. Képes forgalomirányítón superview, root view és CLI-view létrehozására, működésének ellenőrzésére.

– Tisztában van a szállítási réteg sebezhetőségével, ismeri a TCP- és UDP-protokoll elleni támadásokat.

– Ismeri az AAA fogalmát, összetevőit.

– Tisztában van a külső központi szerveren történő hitelesítés és hozzáférés-kezelés jelentőségével, fontosságával.

– Tisztában van a RADIUS-protokoll működésével, szerepével.

– Képes forgalomirányítón AAA megvalósítására, használatára. Képes forgalomirányító távoli eléréséhez RADIUS-hitelesítést használni.

– Képes vezeték nélküli hálózatban RADIUS-hitelesítés konfigurálására, használatára.

– Tisztában van a hitelesítés, sértetlenség és megbízhatóság (authentication, integrity, confidentiality) jelentésével, érti a köztük lévő különbségeket.

– Érti a kriptográfia jelentőségét, ismer egyszerűbb titkosítási algoritmusokat (Vigenere-kódolás, Ceasar-kódolás).

– Tisztában van a titkos kulcs és a nyilvános kulcs fogalmával.

– Tisztában van a szimmetrikus kulcsú és az aszimmetrikus kulcsú titkosítás működési elvével. Ismer szimmetrikus kulcsú és aszimmetrikus kulcsú titkosítási eljárásokat (DES, AES, RSA).

– Tisztában van a hash algoritmusok feladatával, ismeri a leginkább használt hashképző algoritmusokat (MD5, SHA).

Hozzáférési listák használata

A témakör célja, hogy a tanulók megértsék a forgalomszűrés jelentőségét, és legyenek képesek forgalomszűrést megvalósítani IPv4-környezetben.

A témakör elvégzését követően a tanuló az alábbi ismeretekkel és gyakorlati készségekkel fog rendelkezni:

– Tisztában van a forgalomszűrés szükségességével, és meg is tudja azt valósítani hozzáférési listák alkalmazásával.

– Érti a hozzáférési listák használatának célját és működését.

– Tisztában van a helyettesítő maszk szerepével a hozzáférési listák vonatkozásában, és képes a helyes helyettesítő maszk meghatározására.

– Ismeri a normál hozzáférési lista nyújtotta forgalomszűrési lehetőségeket.

– Képes meghatározni a normál hozzáférési lista alkalmazásának legmegfelelőbb helyét.

– Képes számozott és nevesített normál hozzáférési listát készíteni IPv4-környezetben.

– Képes nevesített normál hozzáférési lista szerkesztésére, módosítására.

– Képes ellenőrizni a normál hozzáférési lista működését, az átengedett és eldobott csomagok számát.

– Képes normál hozzáférési listákon hibakeresést és hibaelhárítást végezni.

– Ismeri a kiterjesztett hozzáférési lista nyújtotta forgalomszűrési lehetőségeket.

– Képes meghatározni a kiterjesztett hozzáférési lista alkalmazásának legmegfelelőbb helyét.

– Képes számozott és nevesített kiterjesztett hozzáférési listát készíteni IPv4 környezetben.

– Képes nevesített kiterjesztett hozzáférési lista szerkesztésére, módosítására.

– Képes ellenőrizni a kiterjesztett hozzáférési lista működését, az átengedett és eldobott csomagok számát.

– Képes kiterjesztett hozzáférési listákon hibakeresést és hibaelhárítást végezni.

– Tisztában van a távoli elérést biztosító VTY-vonalak védelmének jelentőségével.

– Képes normál és kiterjesztett hozzáférési lista segítségével a VTY-vonalak védelmére.

– Képes a VTY-vonalakra alkalmazott normál, illetve kiterjesztett hozzáférési lista működésének ellenőrzésére és hibaelhárítására.

Statikus és dinamikus címfordítás lehetőségei

A témakör célja, hogy a tanulók megértsék a címfordítás szükségességét, típusait, és legyenek képesek statikus és dinamikus címfordítás megvalósítására.

A témakör elvégzését követően a tanuló az alábbi ismeretekkel és gyakorlati készségekkel fog rendelkezni:

– Tisztában van az IPv4-címfordítás (NAT) szükségességével. Ismeri a címfordítás előnyeit és hátrányait.

– Ismeri a címfordítás nyújtotta lehetőségeket, és ismeri a címfordítás fajtáit (statikus címfordítás, dinamikus címfordítás, portcímfordítás, porttovábbítás).

– Tisztában van a címfordítás fajtái közötti különbségekkel.

– Tisztában van a címfordításhoz kapcsolódó címek négy típusával (belső helyi cím, belső globális cím, külső helyi cím, külső globális cím).

– Képes a megfelelő címfordítási típus kiválasztására.

– Képes a belső és külső hálózat határának megállapítására.

– Képes annak megállapítására, hogy melyik eszközön szükséges címfordítás kialakítása.

– Képes statikus címfordítás konfigurálására, ellenőrzésére és hibaelhárítására.

– Képes dinamikus címfordítás konfigurálására, ellenőrzésére és hibaelhárítására.

– Képes túlterheléses dinamikus címfordítás vagy portcímfordítás (PAT) konfigurá-lására, ellenőrzésére és hibaelhárítására.

– Képes port továbbítás konfigurálására, ellenőrzésére és hibaelhárítására.

– Képes a címfordítási tábla (NAT-tábla) megjelenítésére, ellenőrzésére, kiürítésére. Érti a NAT-táblában szereplő bejegyzéseket.

– Szimulációs szoftver segítségével végig tudja kísérni egy címfordítást használó adatcsomag harmadik rétegbeli fejlécének változását.

WAN-technológiák

A témakör célja, hogy a tanulók ismerjék a WAN-hálózatokra fókuszálva a technológiák, a hálózatokban szükséges eszközök és alkalmazások telepítésének, üzemeltetésének elméleti alapjait és gyakorlati megvalósításait. A tanulók ismerjék meg a WAN-ok esetén használt második rétegbeli protokollokat, és ismerjék meg a WAN-okban használt forgalomirányítás alapjait és gyakorlati megvalósítását.

A témakör elvégzését követően a tanuló az alábbi ismeretekkel és gyakorlati készségekkel fog rendelkezni:

– Tisztában van a WAN- és az OSI-modell kapcsolatával. Érti a WAN fogalmát, használatának célját.

– Ismeri a WAN-összetevőket és -eszközöket.

– Érti a WAN működését, üzemeltetését.

– Képes megállapítani a LAN és a WAN határát.

– Ismeri a publikus és privát WAN-technológiákat, képes azok összehasonlítására és adott szempontok szerint a legmegfelelőbb technológia kiválasztására.

– Tisztában van a soros pont-pont kapcsolat kommunikációs szabványaival.

– Ismeri a PPP-protokoll működését, lehetőségeit.

– Adatforgalom elfogására alkalmas szoftverrel képes PPP-keret elfogására, és ismeri a keret fejlécének részéit.

– Képes forgalomirányítók között PPP-kapcsolat kialakítására, ellenőrzésére, hibaelhárítására.

– Képes PPP-kapcsolaton hitelesítés (PAP, CHAP) használatára. Érti a hitelesítési módok működését, és tisztában van a két hitelesítési mód közötti különbségekkel.

– Képes PPP-kapcsolaton konfigurált hitelesítés működésének ellenőrzésére, hibaelhárítására.

– Tisztában van az eBGP forgalomirányító protokoll szerepével, fontosabb tulajdonságaival, működésével.

– Képes az eBGP-protokoll alapszintű konfigurálására.

Virtuális magánhálózat (VPN) kialakítása

A témakör célja, hogy a tanulók megismerjék a virtuális magánhálózat (VPN) működését, használatának előnyeit és fajtáit. A tanulók legyenek képesek Site-to-site és Remote-access VPN konfigurálására.

A témakör elvégzését követően a tanuló az alábbi ismeretekkel és gyakorlati készségekkel fog rendelkezni:

– Tisztában van a virtuális magánhálózat szükségességével, szerepével, alapvető funkcióival.

– Érti a virtuális magánhálózat nyújtotta lehetőségeket, előnyeit és hátrányait.

– Ismeri a legelterjedtebb VPN-technológiákat (Remote-Access VPN, Site-to-Site VPN).

– Ismeri az IPSec-technológiát, érti az IPSec-keretrendszer működését, összetevőit.

– Tisztában van a Remote-Access VPN nyújtotta lehetőségekkel, alkalmazási területeivel.

– Ismeri a Remote-Access VPN összetevőit.

– Képes Remote-Access VPN-konfigurálásra forgalomirányítón.

– Képes Remote-Access VPN-kapcsolat kialakítására végberendezésen.

– Ismeri a Remote-Access VPN-kapcsolat ellenőrzéséhez ajánlott parancsokat, és képes azok megfelelő használatával a Remote-Access VPN-kapcsolat működésének ellenőrzésére.

– Tisztában van a Site-to-Site VPN nyújtotta lehetőségekkel, alkalmazási területeivel.

– Ismeri a Site-to-Site VPN összetevőit.

– Képes Site-to-Site VPN-konfigurálásra forgalomirányítón.

– Képes Site-to-Site VPN-kapcsolat kialakítására forgalomirányítók között.

– Ismeri a Site-to-Site VPN-kapcsolat ellenőrzéséhez ajánlott parancsokat, és képes azok megfelelő használatával a Site-to-Site VPN-kapcsolat működésének ellenőrzésére.

Minőségbiztosítási alapok, hálózatfelügyelet megvalósítása

A témakör célja, hogy a tanulók alapszintű ismereteket szerezzenek a minőségbiztosítás területén, elsajátítsák a hálózatmonitorozás és a hálózatfelügyelet elméleti alapjait és gyakorlati megvalósításait.

A témakör elvégzését követően a tanuló az alábbi ismeretekkel és gyakorlati készségekkel fog rendelkezni:

– Érti, hogy a hálózati forgalom milyen hatással van az átvitel minőségére.

– Képes meghatározni a különböző típusú forgalom (hang, adat, videó) számára szükséges minimális hálózati követelményeket.

– Ismeri a hálózati eszközök által használt, sorba rendező algoritmusokat.

– Ismeri a különböző szolgáltatásminőségi (QoS) modelleket.

– Tisztában van azzal, hogy a QoS által használt mechanizmusok hogyan biztosítják az átvitel megfelelő minőségét.

– Képes alapszintű QoS konfigurálására forgalomirányítón.

– Ismer legalább egy második rétegbeli protokollt, mely képes a szomszédos eszközök felfedezésére (CDP, LLDP).

– Tisztában van a hálózatfelderítő protokollok működésével, használatuk előnyeivel, hátrányaival.

– Képes az általa ismert hálózatfelderítő protokoll konfigurálására és használatára.

– Képes az általa ismert hálózatfelderítő protokoll használatával a hálózat feltérképezésére.

– Ismeri a Network Time Protocol (NTP) működését, szerepét. Tisztában van az NTP használatának szükségességével.

– Képes forgalomirányítót NTP-szerverként és NTP-kliensként konfigurálni.

– Képes két eszköz között NTP-kliens és NTP-szerver-kapcsolatot kialakítani.

– Képes hitelesítést alkalmazni az NTP-protokoll használata során.

– Képes megjeleníteni az NTP működésének állapotát forgalomirányítón.

– Képes NTP esetén hibaelhárítást végezni.

– Ismeri a Simple Network Management Protocol (SNMP) működését, szerepét, használatának lehetőségeit.

– Tisztában van az SNMP esetén előforduló fogalmak jelentésével (SNMP manager, SNMP agent, MIB, trap).

– Ismeri az SNMP-verziókat, tisztában van a köztük lévő főbb különbségekkel.

– Képes forgalomirányítón SNMP alapszintű konfigurálására. Képes az SNMP használatára, segítségével konfigurációs adatok lekérdezésére, módosítására.

– Ismeri a Syslog-protokoll működését, szerepét. Tisztában van a Syslog-protokoll által használt üzenetformátummal. Ismeri a súlyossági szinteket, és tudja azok jelentését.

– Képes forgalomirányítón Syslog konfigurálására. Képes Syslog-szerverként funkcionáló eszközön nyomon követni a forgalomirányító által küldött naplóüzeneteket. Képes ezekben az üzenetekben szűrést, keresést, rendezést végrehajtani.

– Ismeri a NetFlow-protokoll működését, szerepét, verzióit. Tisztában van a NetFlow által használt adatfolyam jelentésével.

– Képes forgalomirányítón NetFlow konfigurálására, ellenőrzésére, forgalmi statisz-tika megjelenítésére.

– Ismeri a kapcsolók és forgalomirányítók által használt konfigurációk fajtáit (kezdeti konfiguráció, futó konfiguráció). Tisztában van ezek szerepével, tárolási helyével.

– Ismeri a TFTP-protokoll működését, képes annak használatára.

– Képes forgalomirányító és kapcsoló futó, illetve kezdeti konfigurációjának mentésére, külső szerverre történő mentésére TFTP-protokoll használatával.

– Képes forgalomirányító és kapcsoló futó, illetve kezdeti konfigurációjának helyre-állítására, visszaállítására TFTP-protokoll használatával.

– Ismeri az IOS fogalmát, szerepét, tárolási helyét, működés közbeni tárolási helyét.

– Tisztában van a különböző IOS-verziókkal, és ismeri az aktuális IOS-verzió jellemzőit, sajátosságait.

– Képes forgalomirányítón és kapcsolón IOS-frissítés végrehajtására.

– Ismeri a jelszóhelyreállítás lépéseit forgalomirányítón és kapcsolón.

– Képes jelszóhelyreállítást végezni forgalomirányítón és kapcsolón. A témakör részletes kifejtése

Hálózattervezés, hibaelhárítás

A témakör célja, hogy a tanulók elsajátítsák a hálózattervezés és a hálózati hibaelhárítás elméleti alapjait és gyakorlati megvalósításait.

A témakör elvégzését követően a tanuló az alábbi ismeretekkel és gyakorlati készségekkel fog rendelkezni:

– Tisztában van a konvergált hálózat fogalmával, jelentőségével.

– Ismeri a háromrétegű hierarchikus hálózati modellt (hozzáférési réteg, elosztási réteg, központi réteg), és tisztában van az egyes rétegek feladatával, ajánlott eszközeivel.

– A háromrétegű modell használatával képes kis- és közepes méretű kapcsolt hálózat tervezésére.

– Tisztában van a kapcsoló hardverjellemzőivel, a kapcsolók fajtáival (moduláris, fix kiépítésű, stackelhető), és képes a hálózat követelményeit figyelembe véve a meg-felelő kapcsoló kiválasztására.

– Tisztában van a forgalomirányító hardverjellemzőivel, és képes a hálózat követelményeit figyelembe véve a megfelelő kapcsoló kiválasztására.

– Tisztában van a hálózati dokumentáció tartalmával, jelentőségével. Képes hálózati dokumentáció készítésére. Tudja, hogyan érdemes a hálózati dokumentációt fel-használni a hibakeresés során.

– Tisztában van a hibaelhárítás folyamatával.

– Ismeri az OSI-modell rétegein alapuló hibafelderítési eljárásokat (fentről lefelé, lentről felfelé, oszd-meg-és-uralkodj), és képes ezek alapján hibafelderítést végez-ni.

– Ismeri a hibafelderítéshez használható hardveres és szoftveres eszközöket, és képes ezek használatára.

– Képes a hálózati hibák tüneteinek, következményeinek és a hiba által érintett területnek a meghatározására.

– Képes a hálózati hibák megfelelő dokumentálására.

– Tisztában van a viszonyítási alap jelentőségével, tudja, hogyan és mikor érdemes viszonyítási alapot készíteni.

Hálózatvirtualizáció, hálózatautomatizáció

A témakör célja, hogy a tanulók megismerjék a hálózatvirtualizáció és -automatizáció alapjait, előnyeit.

A témakör elvégzését követően a tanuló az alábbi ismeretekkel és gyakorlati készségekkel fog rendelkezni:

– Tisztában van a cloud computing és a virtualizáció fontosságával, jelentőségével.

– Ismeri a hálózati eszközök és a hálózat virtualizálásának lehetőségeit.

– Ismeri a szoftveralapú hálózati megoldásokat.

– Ismeri a hálózatautomatizáció alapjait.

– Ismeri a használható adatformátumokat (JSON, YAML, XML), és képes ezek összszehasonlítására.

– Tisztában van az API- és a REST-szoftverarchitektúra működésével.

– Ismeri a különböző konfigurációs menedzsmenteszközöket (Puppet, Chef, Ansible, SaltStack).

Komplex hálózat tervezése, kialakítása

A témakör tanításának célja, hogy a tanulók képesek legyenek egy nagyobb és összetettebb hálózatot tervezni, megvalósítani és konfigurálni úgy, hogy a hálózatban egy eszköz vagy kapcsolat meghibásodása a legkisebb kiesést okozza. A tanulók eddigi ismereteik alapján végezzék el egy komplex hálózat tervezését, dokumentálását, majd szimulációs szoftver-ben a hálózat működésének tesztelését. A tanulók végül fizikai eszközök használatával valósítsák meg a tervezett hálózatot. A témakör tanítása során csoportos projektmunka javasolt.