

IP routerek megbízhatósági modellezése

Pándi Zsolt, 2005-08-03

Alapfogalmak

A modellek egyértelmű tárgyalása érdekében az alábbiakban röviden áttekintjük a megbízhatósági modellezésben elterjedt fogalmak általánosan elfogadott definícióit.

MTBF (Mean Time Between Failures)

A meghibásodások közötti időtartam várható értéke. Értékét a gyártó adja meg, ugyanis az üzemeltetési peremfeltételek betartása esetén csak a berendezés szerkezeti tulajdonságaitól függ. Megjegyezzük, hogy az időtartam eloszlásáról önmagában semmit nem árul el.

MTTR (Mean Time To Repair)

A meghibásodástól a hiba teljes javításáig és a rendszer működésének helyreállításáig eltelt időtartam hosszának várható értéke. Nagyrészt az üzemeltetési gyakorlattól függ, de természetesen az esetlegesen szükséges pótalkatrészek elérhetősége is hatással lehet rá. Általánosan elfogadott gyakorlat szerint a berendezések hibáinál 6h, míg a terepen bekövetkező, tipikusan kábelátvágást jelentő hibaesemények esetén 12h a számításokhoz használt közelítő érték. Megjegyezzük, hogy az időtartam eloszlásáról az MTBF-hez hasonlóan nem ad tájékoztatást.

DTR (Down Time Ratio)

A hibás időszakok aránya a teljes megfigyelési időhöz képest. A használhatóság komplementere. A bővebb magyarázatot lásd ott.

Használhatóság (Availability, $A(t)$)

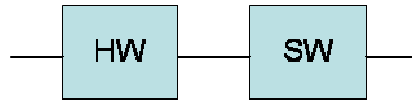
Az üzemképes állapotban töltött idő és az összes megfigyelési idő hányadosa a t időpontig bezárólag. Alternatív definíciója annak a valószínűsége a $[0, t]$ intervallumban, hogy a megfigyelt rendszer üzemképes. Alapértelmezés szerint időfüggő mennyiség, amelynek az idő szerint végtelenben vett határértéke az aszimptotikus használhatóság (A). Ez utóbbi kifejezhető az MTBF és MTTR segítségével is a következőképpen: $A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$. Megjegyezzük, hogy elméletileg tetszőlegesen jó használhatóságú rendszer építhető tetszőlegesen rossz komponensekből ha az MTTR (üzemeltetésfüggő) értékét kellően alacsonyan lehet tartani.

Megbízhatóság (Reliability, $R(t)$)

Annak a valószínűsége, hogy t időpontig bezárólag a rendszerben nem következik be hiba. Nem tökéletes komponensekből álló rendszereknél a végtelenben vett határértéke 0. Megjegyezzük, hogy csak kellően megbízható komponensekből építhető jó megbízhatóságú rendszer.

Routerek hibamodelljei

Az IP routerek megbízhatóságának modellezéséhez a következőkben áttekintünk néhány lehetséges modellezési megközelítést. A modellek többféle részletességgel írják le a berendezéseket, és ebből következően különböző bemeneti paramétereket igényelnek és különböző eredményeket szolgáltatnak. Fontos kérdés ezen kívül a modellek szándékolt felhasználása, amely szintén befolyásolhatja a modellválasztást.



1. ábra: Magas szintű routermodell

A routerek működése alapvetően a hardver és szoftverfunkciók összehangolt és hibamentes üzemelését jelenti. Akár a hardver, akár a szoftver működik hibásan, az a router egésze szempontjából jelent hibás működést. Feltehető továbbá, hogy sem a hardver sem pedig a szoftver hibás működése nem okozza a másik hibáját, azaz egymástól független a két összetevő. A gondolatmenet alapján a routerek magas szintű megbízhatósági modellje legalább két, sorba kapcsolt komponenset tartalmaz: a hardvert és a szoftvert. Természetesen a két komponens modellezése alapvetően eltérő megfontolásokat tesz szükségessé, ezért a következőkben külön tárgyaljuk majd őket.

Csoportosítási szempontok a modellek komplexitásához kapcsolódóan

Az alkalmazott modell finomsága szerint gyakorlatilag két osztályba sorolhatjuk a lehetséges modelleket. A kétállapotú komponenseket feltételező megközelítés szerint minden önállóan modellezett elem vagy tökéletesen működőképes vagy teljesen működésképtelen állapotban lehet csak. Az önállóan modellezett komponensenként ennél több állapotot leíró modellek lehetővé teszik a különböző minőségi paraméterek fokozatos változásának tetszőleges finomságú követését, a kompozíciós szabályok bonyolultságának számottevő növekedéséért cserébe.

A modellek által szolgáltatott kimenetet tekintve is hasonló kategóriákat állíthatunk fel. A rendszer modelljének kimenete a komponensekre alkalmazott megközelítéstől függetlenül lehet két- vagy többállapotú, a lehetséges kombinációkat az alábbi táblázatban foglaltuk össze.

1. táblázat: Modellek kategorizálása állapotszám szerint

		Modellezett rendszer állapotainak száma	
		kétállapotú	fokozatos
Komponensek állapotainak száma	kétállapotú	a.	c.
	fokozatos	d.	b.

Az későbbiekben az a-val és b-vel jelölt eseteket tárgyaljuk részletesen. A c. és d. esetek elhagyásának oka a következő. A kétállapotú komponensekből felépített, többállapotú kimenetet adó és a többállapotú komponensekből felépített, kétállapotú kimenetet adó modellek esetében a modellezett rendszer struktúrájának szemantikai értelmezésétől függően kell meghatározni a kimeneti paraméterek származtatási szabályait, míg az a. és b. esetekben (ez utóbbiban a rendszer egészét és a komponenseket illetően azonos

állapotszámot feltételezve) egyszerűbb, struktúrafüggetlen, standardnak tekinthető szabályok alkalmazása lehetséges, amelynek bőséges háttérodalma van.

Fontos kérdés a rendszert alkotó komponensek közötti összefüggések tisztázása a hibaesemények szempontjából. Például egy tápegység meghibásodása esetén megnövekedhet az esélye a processzor túlterhelésének és beégésének. Ezen összefüggések szintén a struktúra szemantikai értelmezésétől függenek, bár léteznek módszerek a feltételes hibavalószínűségek kezelésére. A komponensek közötti összefüggések kezelése jelentős komplexitásnövekedéssel jár. A gyakorlatban is sokszor indokolt lehet a független komponenshibák feltételezése, ugyanis a különbségek általában elhanyagolhatók az igényelt többlet-erőfeszítések mértékéhez képest. Az elmondottak miatt a továbbiakban független komponenshibákat feltételezünk.

A többállapotú és az összefüggő komponenshibákat kezelő modellekkel kapcsolatban is általános megjegyzésként hozzáfűzzük, hogy tetszőlegesen bonyolult modellek felállíthatók, de a használhatóság szempontjából kritikus kérdés, hogy a modellek által igényelt bemeneti paraméterek (működési állapotok közötti átmenetek jellemzése, feltételes hibavalószínűségek, stb.) hogyan határozhatók meg úgy, hogy a kimenetként szolgáltatott eredmények jól közelítsék a modellezett valóságos rendszer viselkedését.

Alkalmazható modellek áttekintése a modellezett alrendszerek szerint

I. hardver modellek

I.a. kétállapotú komponensek és berendezések

Ez a modell azon az egyszerűsítő feltételezésen alapul, hogy ha valamely hardverkomponens meghibásodik, akkor az egész berendezés üzemképtelen állapotba kerül. Segítségével a berendezés aszimptotikus rendelkezésre állása határozható meg, azaz annak a valószínűsége, hogy egy adott pillanatban éppen működőképes állapotban van-e. Előállítható komponensszintű megbízhatósági modellezési eszköztárral a redundanciák figyelembe vételével.

Előnyök:

- tömören jellemzi a berendezés rendelkezésre állását,
- könnyen integrálható hálózatszintű modellbe,
- egyszerűen számolható.

Hátrányok:

- a részleges kieséseket nem képes kezelni.

Alkalmazás feltételei:

- komponens szintű hibakarakterisztikák ismerete (megszerzése kérdéses),
- vagy gyártók által közölt aszimptotikus rendelkezésre állási értékek elérhetősége (gépkönyvek tartalmaznak erre vonatkozó adatokat).

I.b. teljesítménydegradáció

Ebben a modellben az I.a-hoz képest az egyes modulok kiesése nem kritikus hiba a rendszer egésze szempontjából (csak a funkciók egy részének elvesztésével jár, pl. egy interface kártya hibája csak az adott linket érinti).

Előnyök:

- finomabb teljesítménykövetést tesz lehetővé.

Hátrányok:

- részletesebb berendezésmo­dellt követel meg,
- az eredményeket nehezebb háló­zatszin­­tű mo­dellbe integrálni, mert a berendezés mo­delljétől is függ azok értelmezése,
- valószínűleg elhanyagolható az eredmények pontosságának növekedése (a linkeken jelentkező hibák valószínűsége mellett) a nagy megbízhatóságú hardverelemek miatt.

Alkalmazás feltételei:

- komponens szintű hibakarakteristikák ismerete (megszerzése kérdéses),
- eredmények háló­zatszin­­tű mo­dellbe való illesztésének kidolgozása.

II. szoftver modellek

II.a. kétállapotú berendezések

Azon a (rendszerint helytálló) egyszerűsítő feltételezésen alapul, hogy minden szoftveres hiba a router lefagyását okozza, amelyet csak újraindítás segítségével lehet orvosolni, és annak, vagy a konfiguráció helyreállításának megtörté­ntéig a router gyakorlatilag üzemképtelen állapotúnak tekinthető. Ugyanúgy aszimptotikus hibavalószínűség ki­menetet szolgáltat, mint az I.a. eset.

Előnyök:

- lásd I.a., kivéve az egyszerű számolhatóságot.

Hátrányok:

- gyakorlatilag lehetetlen pontos modellt adni, sokkal inkább valamilyen hibastatisztika alapú közelítés alapján lehet megbecsülni az aszimptotikus rendelkezésre állást,
- gyártóktól gyakorlatilag lehetetlen erre vonatkozó adatokat szerezni, mert ezek használat- és verziófüggők is.

Alkalmazás feltételei:

- trouble ticket jellegű adatok feldolgozásával nyert információk, vagy a rendelkezésre álló kevés irodalmi adat használata.

II.b. teljesítménydegradáció

II.a kiterjesztése olyan jellegű feltételezésekkel, hogy egyrészt bizonyos jellegű hibák csak bizonyos funkciókat érintenek (pl. keretezést végző kód hibásan működik egy bizonyos típusú interface-en valamilyen paraméterek esetében, ezért egy ilyen típusú interface-en megnövekszik az elvesztett csomagok száma), másrészt ezek lehet, hogy úgy jelentkeznek, hogy a router látszólag helyesen működik (pl. routing protokoll kommunikációt helyesen végzi, de rossz utakat számol), vagy csak bizonyos timeout-ok letelte után ismerhető fel a helytelen működés (pl. tökéletes csomagnyelőként üzemel, és csak az OSPF HELLO-kra adott válaszok hiányából lehet következtetni arra, hogy baj van).

Előnyök:

- a szoftveres/helytelen konfigurációból eredő hibaokok finomabb jellemzését adja, amelyek jelentősége nagyobb, mint a tisztán hardver eredetűeké.

Hátrányok:

- tetszőlegesen bonyolult modell alkotható, a lehetséges hibaokok számossága igen nagy, gyakorlatilag igen nehéz ezek elpfurdulási körülményeit és gyakoriságát jellemezni,

- kérdéses a modell eredményeinek hálózatszintű modellezésben történő alkalmazhatósága (ugyanis a hálózati modellt is jelentősen bonyolítja).

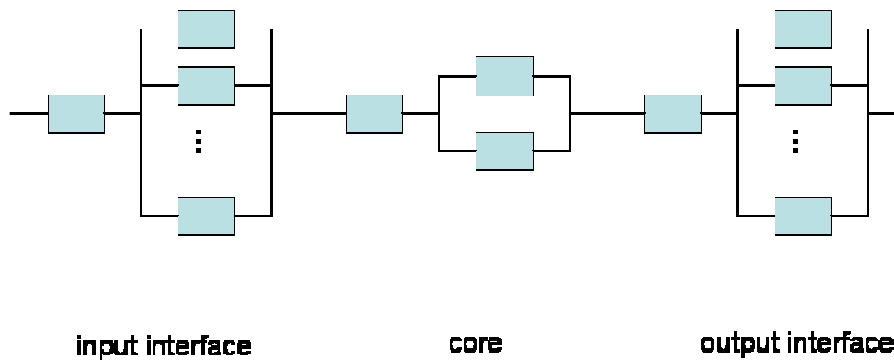
Alkalmazás feltételei:

- megfelelő hibastatisztikák (trouble ticket) rendelkezésre állása, azok elemzése,
- szoftverek belső architektúrájának ismerete (erősen kérdéses).

Csoportosítás a modellek felhasználásának szempontjából

A fentiekben tárgyalt modellek alkalmazása alatt a teljes megbízhatósági modellezési folyamat által vizsgált megbízhatósági jellemzők előállítását értjük, pontosabban a routermodellek illesztését a magasabb szintű hálózati megbízhatósági modellbe.

A keresett paraméterek jellege alapvetően visszahat a routermodellek célszerű struktúrájára, ahogy az következőkből is kiderül majd.

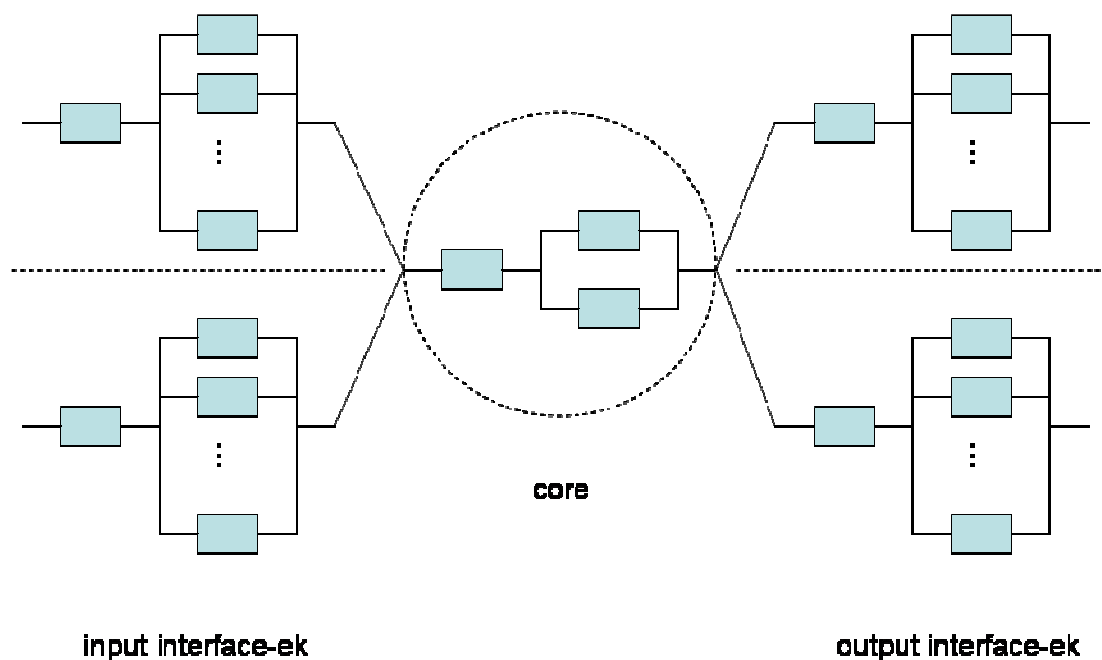


2. ábra: Routermodell pont-pont kapcsolat esetén

Pont-pont kapcsolat megbízhatóságának modellezése esetén a célszerű router modellt a 2. ábra mutatja. Ennek alapvetően lineáris szerkezete a csomópontba belépő és onnan kilépő kapcsolat által használt komponenseket fűzi fel egy láncra a megfelelő redundanciák figyelembe vételével (az ábra csak illusztráció). Alapvetően három szakaszt lehet elkülöníteni: a be- és kimeneti interfészekhez rendelt komponenseket leíró, valamint a routerben (esetlegesen) igénybevett központi funkciókat megvalósító komponenseket leíró szakaszokat.

Az interfészekhez rendelt szakaszok leírhatják az interfészek csatlakozóinak és az interfész kártyáknak a megbízhatósági paramétereit a hozzáférhető adatoktól függő részletességgel. A központi szakasz egyrészt a router egészének működéséhez szükséges funkciókat írja le (tápegység, hűtés, backplane busz, központi memória), másrészt az esetlegesen szükséges egyedi, pontosabban központosítottan implementált funkciókat (routing processzor).

Ez a modell nyilvánvalóan nem szükségszerűen teljes abban az értelemben, hogy kizárólag a routeren áthaladó kapcsolat által használt komponenseket tartalmazza. Ha a be- és kimeneti interfész megegyezik, akkor a két interfész szakasz közül csak az egyiket kell szerepeltetni.



3. ábra: Router modell teljes hálózat modellezése esetén

Integrált hálózati modell esetében ezzel szemben a 3. ábrán vázolthoz hasonló, csillagszerű struktúra alkalmazása lehet célszerű, amelyben a hálózati modellekben gyakran előforduló útkeresési feladatok könnyebben értelmezhetőek. Amennyiben További megfontolások is szükségesek azonban abban az esetben, ha a bemenő és kimenő interfész megegyezése megengedett, de ezzel jelen tanulmány keretei között nem foglalkozunk.

Illusztratív numerikus eredmények

A következőkben a hozzáférhető adatok alapján egy pont-pont kapcsolat modellezéséhez felhasználható lineáris routermodell segítségével illusztráljuk a várható eredményeket egy Cisco 12008 típusú router modellezése esetén. A vizsgálatnál a 6 órás, standard MTTR időt feltételezzük ($MTTR_s$), ha ezt másképpen nem jelezzük.

[1], továbbá a rendelkezésünkre álló MTBF táblázatok és egyéb Cisco leírások alapján a router következő főbb komponenseit modellezhetjük:

- ház (chassis): $MTBF=398788h$,
- route processzor (GRP): duplázott redundáns elem, $MTBF=188768h$ processzoronként, amelyből [2] alapján a route processzor pára $MTBF \approx 283152$ (exponenciális viselkedést feltételezve), valamint $MTTR=3s$, ha feltételezzük, hogy a meghibásodást követő $MTTR_s$ időn belül nem következik be újabb hiba (ennek valószínűsége elhanyagolható), és a rendszer automatikusan átkapcsol a rendelkezésre álló tartalék processzorra,
- tápegység (PS): duplázott, redundáns elem, $MTBF=414931h$,
- clock scheduler kártya (CSC): a kapcsolómátrix komponense, duplázott, redundáns elem, $MTBF=256470h$,

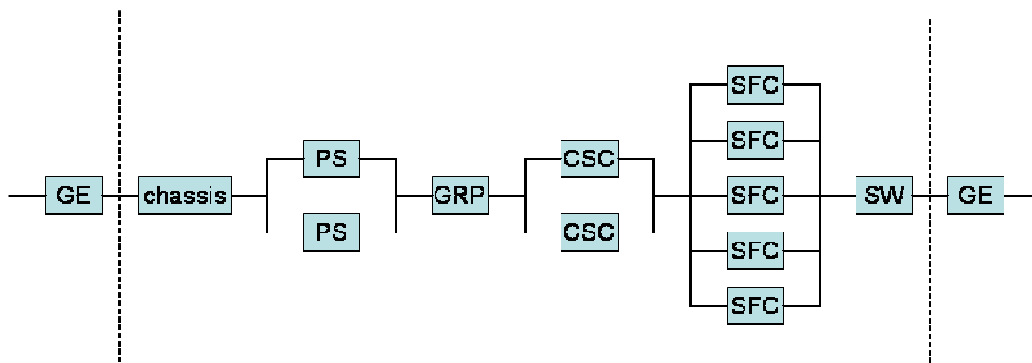
- switch fabric kártya (SFC): a kapcsolómátrix komponense, ötszörözött, redundáns elem, MTBF=492917h,
- GE modul (GE): interfész kártya, nem redundáns, MTBF=147248h,
- operációs rendszer (SW): [3] alapján az MTBF=100000h becslés adható meg.

Megjegyezzük, hogy a route processzor esetében azért kezeljük speciálisan a struktúrát, mert speciális failover mechanizmust biztosít a gyártó amely néhány részletének ismeretében némileg pontosabb modell adható.

A fenti értékekből az I.a. és II.a. modellek szerint származtatott aszimptotikus rendelkezésre állási értékeket a 2. táblázat tartalmazza.

2. táblázat: Cisco 12008 router komponenseinek származtatott megbízhatósági jellemzői

komponens	1-A
chassis	$1.5 * 10^{-5}$
GRP	$2.9 * 10^{-9}$
PS	$1.4 * 10^{-5}$
CSC	$2.3 * 10^{-5}$
SFC	$1.2 * 10^{-5}$
GE	$4.1 * 10^{-5}$
SW	$6.0 * 10^{-5}$



4. ábra: Cisco 12008 router lehetséges megbízhatósági modellje

A bemutatott komponensekből felépített modell a 4. ábrán látható. A soros és párhuzamos struktúrákból felépített modellben a router rendelkezésre állása dekompozícióval számítható és $1-A_{\text{router}} \approx 1.57 * 10^{-4}$ adódik.

Az eredmény értelmezéséhez meg kell említenünk, hogy a GE, chassis és SW komponensek megbízhatósági paramétereinek van kritikus hatása a becslés végeredményére nézve. Egy példával érzékeltetve a paraméterek fontosságát: ha a szoftverkomponens rendelkezésre állására adott becslésben MTBF=100000h helyett MTBF=200000h értéket alkalmazunk, a modell végeredménye $1-A_{\text{router}} \approx 1.27 * 10^{-4}$ -re változik, míg a szoftverkomponens elhagyásával (azaz hibátlannak való feltételezésével már $1-A_{\text{router}} \approx 9.7 * 10^{-5}$ lesz a végeredmény.

Konklúzió

Az IP routerek gyártói a nagy megbízhatóságú komponenseket eredményező gyártási technológiával és a kritikus hardverelemek redundáns struktúrákba szervezésének segítségével napjainkra már 10^{-5} nagyságrendjébe szorították a nagy teljesítményű berendezések aszimptotikus rendelkezésre állását. A szoftverhibákról igen nehéz információkat beszerezni, csak valós hibastatisztikákon alapuló elemzés adhat használható adatokat. Bonyolultabb modellek felállítása is csak a modellparaméterek meghatározhatóságának garantálásakor lehet célravezető.

A magyarországi transzportálózatban előforduló link meghibásodási valószínűségek statisztikai adatok alapján a $2.5...7.5 * 10^{-4}$ nagyságrendbe esnek. Ha az IP routerek megbízhatósági modellezésével nyerhető adatok stabilan egy nagyságrenddel kisebb értékeket eredményeznek, akkor a megbízhatósági elemzés során elkövetett hiba a kapcsolatok hopszámának függvényében 3...20%-ra tehető, ami megbízhatósági paraméterek esetében nem mondható jelentősnek.

Referenciák

- [1] http://www.cisco.com/en/US/products/hw/routers/ps167/products_data_sheet09186a00800920b9.html
- [2] Jereb L.: *Hibatűrő architektúrák és modellezésük*, Egyetemi jegyzet
- [3] C. R. Johnson, Y. Kogan, Y. Levy, F. Saheban, P. Tarapore, *VoIP Reliability: A Service Provider's Perspective*, IEEE Communications Magazine, July 2004, pp. 48-54