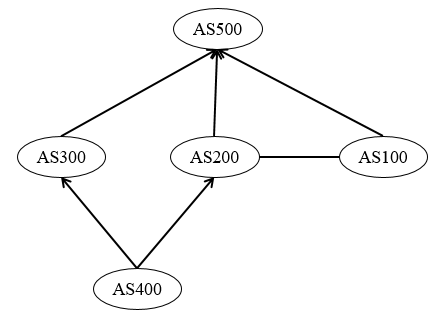
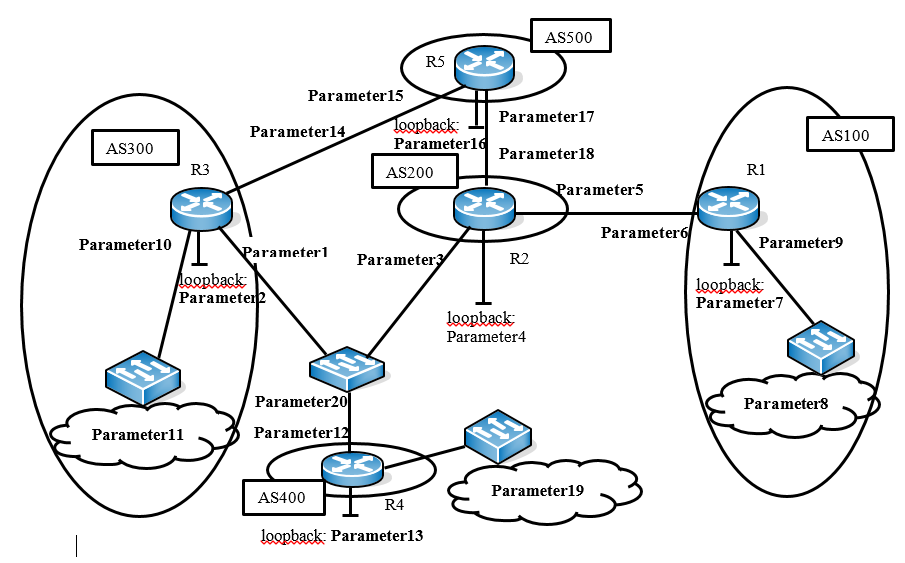
6. gyakorlat (Határidő: április 17.) Név: Neptun kód:

1. Indítsa el a GNS3-ban az előző házi eredményeként kiépített hálózatot és rajta az alábbi AS szintű hierarchiát! Módosítsa úgy, hogy az AS400 is hirdessen meg a szokásos módon egy prefixet, ahogy azt az ábra is mutatja. Gondoskodjon róla, hogy a hálózatban csak valley-free útvonalak terjedhessenek!



**Backup routing & prefer customer**

1. Legyen AS400 elsődleges szolgáltatója AS300 és másodlagos (backup) szolgáltatója AS200.
   1. Oldja meg, hogy AS400 másodlagos szolgáltatója felé hirdetett útvonalai „sokkal hosszabbnak” tűnjenek, mint az elsődleges szolgáltató felé hirdetett utak (tipp: AS path prepending: illesszük be mondjuk 4x a AS400-at a hirdetésekbe!)
   2. Vizsgálja meg, milyen útvonalakat ismer R5 a **Parameter19** prefixre! Melyik ezek közül a preferált út? (tipp: a két előfizetői út közül az AS300-on keresztüli rövidebb)
   3. Milyen útvonalat választ R2 ugyanerre a prefixre? Miért? (tipp: ha nem konfiguráltunk még prefer-customer pollicy-t, akor a 4x-es AS path prepending miatt az AS500 szolgáltatón keresztüli út rövidebb lett)
   4. Konfigurálja az összes routert úgy, hogy az előfizetői utakat mindig preferálják a szolgáltatói és peer útvonalak fölött! Jegyezze le R2 útvonalait a konfiguráció után! Ellenőrizze az utakat traceroute segítségével!

**Prefix hijacking & Man in the Middle**

1. Legyen AS100 most egy rosszindulatú támadó, amely megkísérli eltéríteni az AS400 „áldozat AS” által legitim meghirdetett **Parameter19** prefix forgalmát.
   1. Hirdesse meg a **Parameter19** prefixet R1-en is)! Jegyezze fel, hogy az egyes BGP routerek milyen útvonalat választanak a prefixre!
   2. Hirdesse meg R5 saját hálózatát (tehát a **Parameter17**-hez tartozó hálózatot), majd ellenőrizze a csomagszintű kapcsolatot R5-ről az eltérített **Parameter19** prefix felé a ping paranccsal! R2-ről válaszol a ping a **Parameter19** felé? Miért? (tipp: igen válaszol, pedig R5-ről nem válaszolt)
   3. Oldja meg, hogy a ping csomagok célhoz érjenek és válasz is érkezzen! (tipp: adjon hozzá egy megfelelő statikus route-ot R1 FIB-jéhez R2 felé)
   4. Hárítsa el a prefix hijacking támadást és igazolja a BGP RIB-ek vizsgálatával, hogy a lépései helyesek voltak! (tipp: megoldható vagy az R4-en a **Parameter19** prefix deaggregálásával, vagy R5-n az AS100 hirdetéseinek BGP prefix-szűrésével!

Minden eredményt dokumentáljon: a beállítások eredményét bizonyító lekérdezéseket screenshotokkal prezentálja!