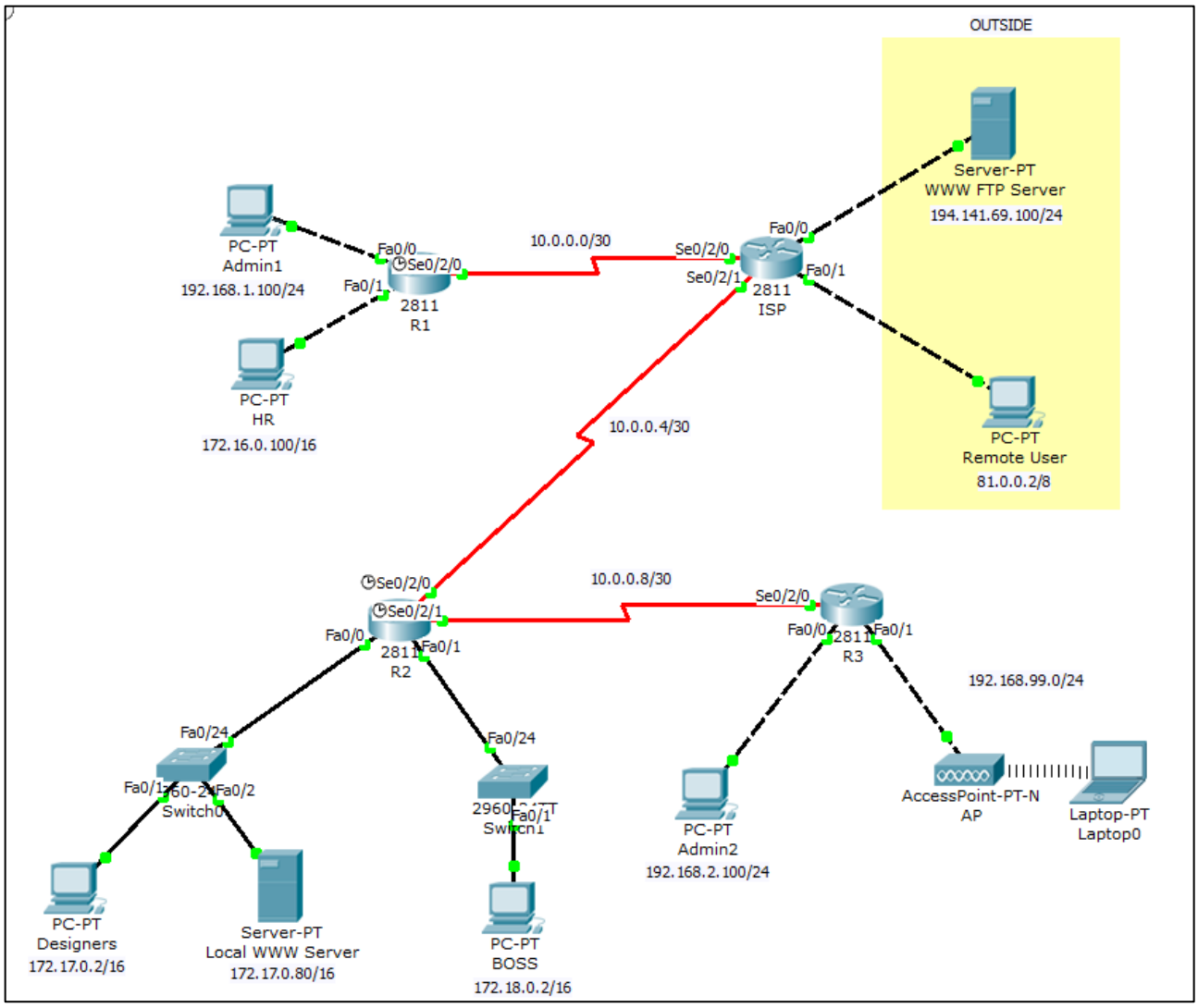
ACL LAB

Примерната топология представлява мрежовата инфраструктура на малка организация. Достъпът до външните мрежи и Internet се осъществява през маршрутизатора ISP. Не се използва DHCP и NAT (PAT). Всички използвани адреси се маршрутизират чрез OSPF в area 0. Всички използвани пароли са *cisco*.



С цел повишаване на сигурността е необходимо да се конфигурират следните правила:

1. Достъп през VTY (login чрез TELNET или SSH) до R1, R2, R3 и ISP да може да се осъществи само от PC Admin1 и PC Admin2.
2. Всички външни устройства (мрежи в зона OUTSIDE) да не могат да достъпват вътрешните устройства. Към вътрешните LAN мрежи да се пропускат единствено ICMP ECHO-REPLY, както и отговори на HTTP, FTP, MS RDC, SMTP и POP3 заявки започващи от устройства, намиращи се във вътрешните мрежи[1]. Към мрежи 10.0.0.0, 10.0.0.4 и 10.0.0.8 да се разреши само ICMP ECHO-REPLY.
3. Достъп до PC Local WWW Server за всички възможни услуги да имат мрежи 172.17.0.0, 172.18.0.0, PC Admin1 и PC Admin2. Освен тези забрани всичкият останал трафик да преминава свободно към другите устройства в мрежа 172.17.0.0.
4. Мрежа 192.168.99.0 да има единствено HTTP, FTP, MS RDC, SMTP и POP3 достъп до OUTSIDE.
5. Устройствата в LAN мрежа 192.168.99.0 да отговарят на ICMP ECHO-REQUEST единствено ако заявката е изпратена от PC Admin1 или PC Admin2. Всичкият останал нефилтриран трафик (точка 4) да преминава.
6. Достъп до мрежа 172.18.0.0 да имат PC HR, PC Admin1 и PC Admin2, както и разрешеният трафик от зона OUTSIDE и от Local WWW Server.
7. *Разрешете всичкия OSPF трафик. (в зависимост от използваните ACL, интерфейси и посока)*

[1] Използвайте extended ACL, не reflexive ACL