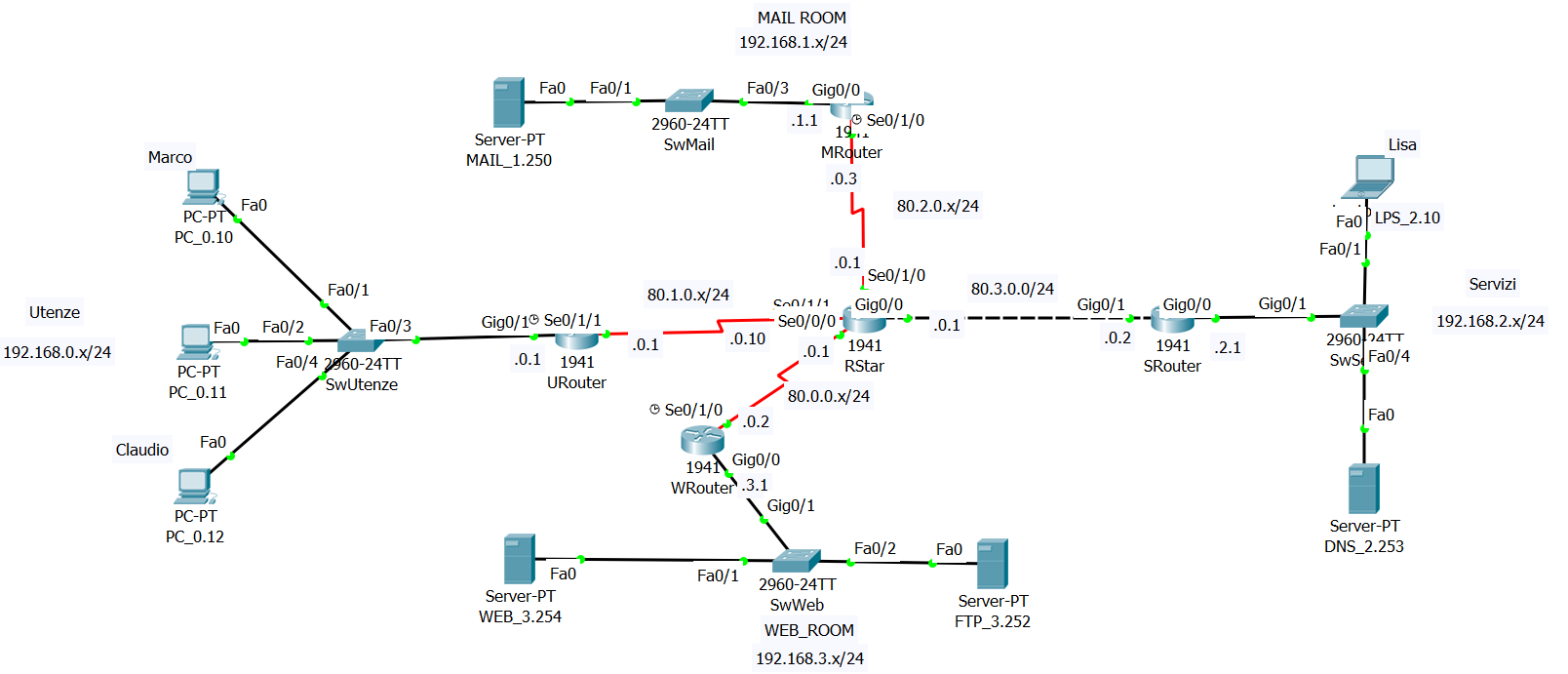
Cognome \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Nome \_\_\_\_\_\_\_\_\_\_\_\_\_ Data\_\_\_\_\_\_ PC# \_\_\_\_\_\_\_

**Verifica Sistemi & Reti**

**“ACL e sicurezza”**

classe 5G – a.s. 2017/2018

Si consideri la seguente infrastruttura di rete (**ZNET**), nella quale viene garantita la connettività di tutti i dispositivi ed il funzionamento di tutti i servizi presenti (file **VerificaAcl\_base.pkt**).



Si proceda con l’applicare le seguenti specifiche addizionali atte ad incrementare il livello di sicurezza degli accessi ai servizi.

**Nota1**: rispettare i criteri “canonici” di applicazione delle ACL; ZNET non prevede né traffico su reti remote né su Internet, di conseguenza la raggiungibilità e configurazione di tutti gli apparati è da ritenersi senza impedimenti di distanza geografica. Le ACL definite di seguito potranno essere applicate alle stesse interfacce in modo cumulativo **definendole tuttavia con un diverso numero di identificazione.** Nei prompt della CLIdeve comparire in modo chiaro la denominazione del router di riferimento e la modalità di configurazione (#/config/config-if ecc.).

**Nota2**: riportare nel documento word, dopo ogni punto, l’elenco dei comandi impostati per soddisfare la richiesta.

1. **Con riferimento alla sola rete Utenze, solo** l’utente **Marco** (PC\_0.10 ) **può** navigare sui siti web gestiti dal **Server** **Web**; nessun’altro host della rete *Utenze* può farlo.

*URouter (config)#access-list 100 permit tcp host 192.168.0.10 host 192.168.3.254 eq 80*

*URouter (config)#access-list 100 deny tcp any host 192.168.3.254 eq 80*

*URouter (config)#access-list 100 permit ip any any*

*URouter (config)#interface Gi0/1*

*URouter (config-if)#ip access-group 100 in*

1. **Con riferimento alla sola rete Servizi, impedire** solo a Lisa (LPS\_2.10) di navigare sui siti web gestiti dal **Server** **Web**.

*SRouter (config)#access-list 100 deny tcp host 192.168.2.10 host 192.168.3.254 eq 80*

*SRouter (config)#access-list 100 permit ip any any*

*SRouter (config)#interface Gi0/0*

*SRouter (config-if)#ip access-group 100 in*

1. **Con riferimento alla sola rete Utenze,** la risoluzione dei nomi di **dominio** (accesso al server DNS) deve essere **vietata** solo al PC\_0.11 della rete Utenze.

*URouter (config)#access-list 101 deny udp host 192.168.0.11 host 192.168.2.253 eq domain*

*URouter (config)#access-list 101 permit ip any any*

*URouter (config)#interface Gi0/1*

*URouter (config-if)#ip access-group 101 in*

1. **Con riferimento a tutta la rete ZNET, consentire** solo a Claudio (PC\_0.12 rete Utenze) ed a Lisa (LPS\_2.10 rete Servizi) l’accesso al server **FTP** (rete Web\_Room); a tutti gli altri PC/Server (host) appartenenti anche alle altre reti deve essere impedito l’accesso al server FTP.

*URouter (config)#access-list 102 permit tcp host 192.168.0.12 host 192.168.3.252 eq 20*

*URouter (config)#access-list 102 permit tcp host 192.168.0.12 host 192.168.3.252 eq 21*

*URouter* (config)#access-list 102 deny tcp any any eq 20

*URouter* (config)#access-list 102 deny tcp any any eq 21

*URouter* (config)#access-list 102 permit ip any any

*URouter (config)#interface Gi0/1*

*URouter (config-if)#ip access-group 102 in*

*SRouter (config)#access-list 101 permit tcp host 192.168.2.10 host 192.168.3.252 eq 20*

*SRouter (config)#access-list 101 permit tcp host 192.168.2.10 host 192.168.3.252 eq 21*

*SRouter* (config)#access-list 101 deny tcp any any eq 20

*SRouter* (config)#access-list 101 deny tcp any any eq 21

*SRouter* (config)#access-list 101 permit ip any any

*SRouter (config)#interface Gi0/0*

*SRouter (config-if)#ip access-group 101 in*

*MRouter* (config)#access-list 100 deny tcp any any eq 20

*MRouter* (config)#access-list 100 deny tcp any any eq 21

*MRouter* (config)#access-list 100 permit ip any any

*MRouter (config)#interface Gi0/0*

*MRouter (config-if)#ip access-group 100 in*

1. **Con riferimento a tutta la rete ZNET,** consentire a Claudio (PC\_0.12 rete Utenze) solo l’**inoltro** di **email** ed a Lisa (LPS\_2.10 rete Servizi) solo la **ricezione** di email; Marco (PC\_0.10 rete Utenze) invece potrà inviare e ricevere email. Tutti gli altri PC/server di ZNET non dovranno poter usufruire del servizio email.

*URouter(config)# access-list 103 deny TCP host 192.168.0.12 host 192.168.1.250 eq pop3*

*URouter(config)# access-list 103 permit TCP host 192.168.0.10 host 192.168.1.250 eq pop3*

*URouter(config)# access-list 103 permit TCP host 192.168.0.10 host 192.168.1.250 eq smtp*

*URouter(config)# access-list 103 deny TCP any any eq smtp*

*URouter(config)# access-list 103 deny TCP any any eq pop3*

*URouter* (config)#access-list 103 permit ip any any

*URouter (config)#interface Gi0/1*

*URouter (config-if)#ip access-group 103 in*

*SRouter(config)# access-list 102 deny TCP host 192.168.2.10 host 192.168.1.250 eq smtp*

*SRouter (config)# access-list 102 deny TCP host 192.168.2.253 host 192.168.1.250 eq pop3*

*SRouter (config)# access-list 102 deny TCP host 192.168.2.253 host 192.168.1.250 eq smtp*

SRouter (config)#access-list 102 permit ip any any

*SRouter (config)#interface Gi0/0*

*SRouter (config-if)#ip access-group 102 in*

*WRouter (config)# access-list 100 deny TCP host 192.168.3.254 host 192.168.1.250 eq pop3*

*WRouter (config)# access-list 100 deny TCP host 192.168.3.254 host 192.168.1.250 eq smtp*

*WRouter (config)# access-list 100 deny TCP host 192.168.3.252 host 192.168.1.250 eq pop3*

*WRouter (config)# access-list 100 deny TCP host 192.168.3.252 host 192.168.1.250 eq smtp*

*WRouter* (config)#access-list 100 permit ip any any

*WRouter (config)#interface Gi0/0*

*WRouter (config-if)#ip access-group 100 in*