



1506
UNIVERSITÀ
DEGLI STUDI
DI URBINO
CARLO BO

DISPEA
DIPARTIMENTO DI
SCIENZE PURE E APPLICATE

Progettazione e simulazione di una rete aziendale ipotetica provvista di servizi FTP, HTTP, DNS, Mail.

Progetto d'esame di Reti di Calcolatori A.A. 2021/2022

Relatore:

Matteo Marco Montanari, 299166

Docente:

Prof. Ing. Antonio Della Selva



Specifica di progetto

Si progetti una rete di calcolatori per un'ipotetica azienda che sia dotata dei seguenti servizi, forniti tramite server all'interno dell'azienda stessa. Tali server sono:

1. Un server DNS per la risoluzione degli indirizzi di dominio della rete aziendale.
2. Un server Mail per la gestione della posta elettronica aziendale.
3. Un server con un servizio FTP, per la gestione e il backup di file aziendali, e un servizio HTTP che fornisca una pagina web di presentazione dell'azienda.

Tali server dovranno essere accessibili da ogni dispositivo sulla rete LAN aziendale e anche dall'esterno (tramite internet). Il resto della rete aziendale è composto da una serie di PC, con accesso ad internet, che fanno capo a 3 sottoreti: Amministrazione, Produzione e Vendite. Implementare un meccanismo di sicurezza a scelta per la rete LAN aziendale. Infine, fornire un esempio di simulazione che descriva il funzionamento della rete progettata.



Scelte di progetto

Per la realizzazione del lavoro in questione sono state effettuate le seguenti scelte progettuali:

- La progettazione e simulazione della rete è effettuata tramite il software professionale dedicato Cisco Packet Tracer fornito da Cisco Systems.
- Il meccanismo di sicurezza interna implementato per la rete LAN in questione è lo Switch Port Security. Tale sistema evita l'accesso non autorizzato agli switch della LAN tramite cavo di rete.
- Per simulare la rete internet si utilizzano tre router collegati a formare un triangolo, a rappresentare una backbone di internet, a loro volta collegati a due PC e un server DNS. Gli indirizzi in questione sono tutti IP pubblici.
- L'esempio di simulazione prevede l'accesso tramite Browser, da parte di un PC sulla rete internet, alla pagina web aziendale www.atlas.it ospitata all'interno della rete LAN.



Stato dell'arte

Prima di procedere con la realizzazione della rete, descriviamo brevemente lo *stato dell'arte* relativo quegli aspetti delle reti di calcolatori necessari per il progetto.

Dando per scontato gli elementi base delle reti di calcolatori, introduciamo i seguenti concetti utili alla realizzazione del lavoro.

Architettura Client-Server

Paradigma di realizzazione di reti nella quale più utenti fruitori di servizi, detti Client, si connettono a più macchine Server che erogano vari servizi tramite comunicazioni basate su messaggi di richiesta e risposta.

DNS

Il DNS (Domain Name System) è un sistema di database distribuiti costruito sopra la rete Internet che, tramite dei server DNS organizzati in maniera gerarchica, permette di risolvere i nomi di dominio dei siti web. Risolvere un nome di dominio significa convertire la stringa di caratteri che compone il dominio di un sito web, ad esempio www.google.com, nell'indirizzo IP corrispondente alla macchina sulla quale risiede il servizio che stiamo cercando.



FTP

Il protocollo FTP (File Transfer Protocol) è un protocollo di livello applicazione che permette il trasferimento efficiente di qualsiasi file attraverso una rete (ad esempio Internet). Si basa su una architettura Client-Server e utilizza connessioni basate su TCP (Transfer Control Protocol). Per trasferire dati è necessaria un'autenticazione tramite nome utente e password ma i dati sono trasferiti in chiaro. Per ovviare a questo si utilizza in aggiunta un sottostrato SSL/TLS, in questo caso parliamo di FTP Secure (FTPS).

MAIL

- **POP** (Post Office Protocol) è un protocollo di livello applicativo di tipo Client-Server che permette a un Client autenticato di accedere al proprio account di posta elettronica e scaricare le e-mail presenti su un server remoto. Una volta scaricate nel Client le mail vengono cancellate dal server.
- **SMTP** (Simple Mail Transfer Protocol) è un protocollo di livello applicativo di tipo Client-Server che permette al Client di inviare un messaggio di posta al server mail che gestisce il suo account, il quale si occupa di inviare il messaggio al server di posta del destinatario sempre tramite SMTP. Utilizza TCP.



WWW

Il World Wide Web è un'infrastruttura di calcolo distribuito sopra la rete internet che permette la fruizione di contenuti testuali, multimediali e anche dinamici tramite collegamenti tra pagine (pagine Web) detti link. Solitamente abbreviato in Web, si basa su un'architettura Client-Server ed è accessibile tramite un software chiamato Browser. Tim Berners-Lee fu l'ideatore di questo sistema.

HTTP

HTTP (Hyper Text Transfer Protocol) è un protocollo di livello applicativo basato su testo, che utilizza un'architettura di tipo Client-Server, utilizzato come principale strumento di comunicazione sul World Wide Web. La versione più recente è HTTP 3.0 e utilizza TCP. I messaggi HTTP possono essere di richiesta o di risposta.

Indirizzi IP

Gli indirizzi IP (Internet Protocol) sono necessari per individuare un dispositivo su una rete (scheda di rete). Se un host è connesso a due reti differenti deve avere due indirizzi IP distinti per interfacciarsi con entrambe le reti. Gli indirizzi IP sono gerarchici e sono associati ad una maschera di sottorete che definisce l'indirizzo di quella specifica rete (prima parte dell'IP) e il pool di



indirizzi dedicati agli host di quella rete (seconda parte dell'IP).

Indirizzi IP privati

Gli IP privati sono quegli indirizzi IP che appartengono ad una rete non direttamente collegata con internet, ossia una rete privata. Per convenzione (RFC 3330) vengono utilizzate alcune classi specifiche di IP che non possono essere assegnate ad indirizzi IP pubblici. Queste classi di IP sono (RFC 1597, 1918): classe A, da 10.0.0.0 a 10.255.255.255; classe B, da 172.16.0.0 a 172.31.255.255; classe C, da 192.168.0.0 a 192.168.255.255. L'uso di indirizzi IP appartenenti a queste classi permette di evitare conflitti di indirizzi tra rete pubblica e privata.

Network Address Translation (NAT)

Gli indirizzi IP privati dei dispositivi collegati a una LAN, non possono comunicare direttamente con internet in quanto quest'ultimo non riconosce tali indirizzi. Per poterlo fare, il computer deve inviare una richiesta al router di frontiera che traduce l'indirizzo IP privato in un indirizzo IP pubblico, attraverso un meccanismo chiamato Network Address Translation (NAT).

- **Da LAN ad Internet.** In questo caso il NAT si risolve nel "sovraccarico" degli indirizzi dei pacchetti originati dalla LAN, in modo che l'unico indirizzo ad apparire in Internet sia l'IP pubblico assegnato dall'ISP (Internet Service Provider) al router di frontiera della rete LAN.



- **Da Internet alla LAN.** Tramite il NAT e la tecnica del Port Forwarding (PF) si permette a dispositivi esterni alla LAN di comunicare con alcuni nodi della rete locale. Per fare ciò verrà associata, ai vari dispositivi della rete LAN che devono essere acceduti dall'esterno, una porta specifica per discriminare tale dispositivo all'interno della LAN (PF).

Routing Information Protocol (RIP)

Il RIP è un protocollo di routing dinamico che impiega il numero di hop come metrica. Evita i routing loop adottando un limite massimo di hop dalla sorgente verso la destinazione (15 salti). Come ogni protocollo di routing permette ai router di scambiarsi informazioni tra loro al fine di costruire le tabelle di routing necessarie per instradare correttamente i pacchetti sulla rete.



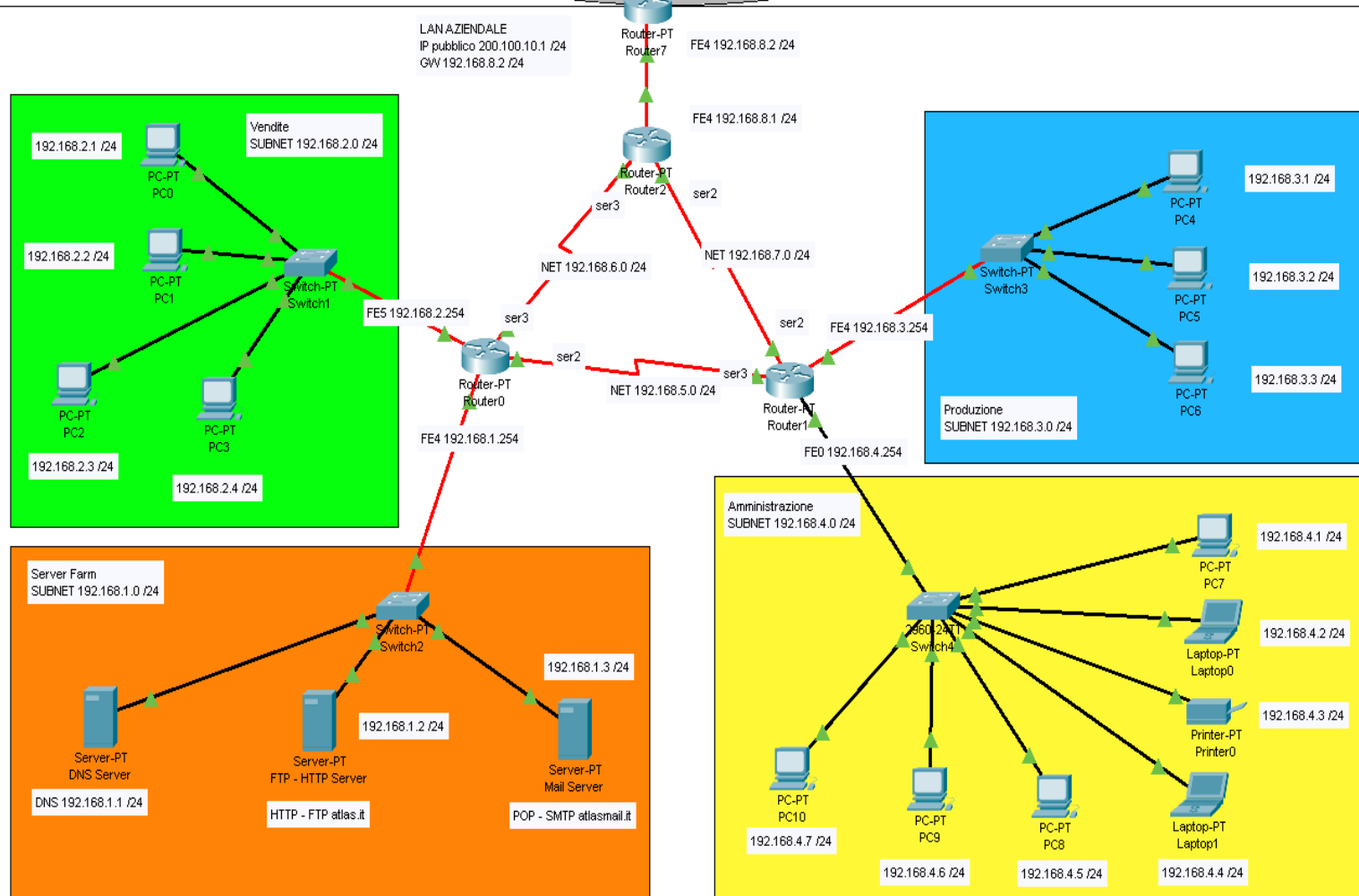
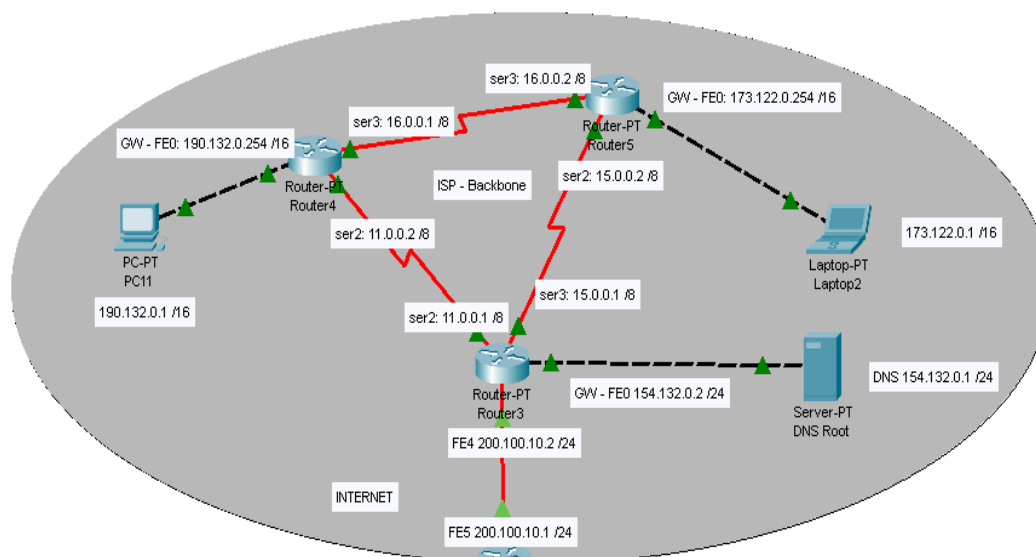
Progettazione della rete

Topologia

La rete LAN progettata è costituita da 4 sottoreti: una contenente i 3 server per ospitare i vari servizi interni all'azienda e le altre 3 sottoreti per gestire le sezioni Amministrazione, Produzione e Vendite. Ogni dispositivo all'interno della stessa sottorete fa capo ad uno switch che ha lo scopo di collegare ciascuna sottorete ai 3 router interni alla LAN, a loro volta collegati reciprocamente tra loro a formare un triangolo. Il router centrale si connette poi al router di frontiera che è a sua volta connesso ad internet. Internet è modellato come una serie di 3 router collegati a formare un triangolo, a rappresentare una backbone, a cui sono collegati due PC e un server DNS. I dispositivi su internet sono distinguibili da quelli della LAN poiché presentano tutti indirizzi IP pubblici, a differenza di quelli nella rete locale che possiedono invece indirizzi privati.



Nell'immagine seguente mostriamo lo schema di progettazione della rete LAN e della rete internet appena descritte.





Assegnazione degli indirizzi IP

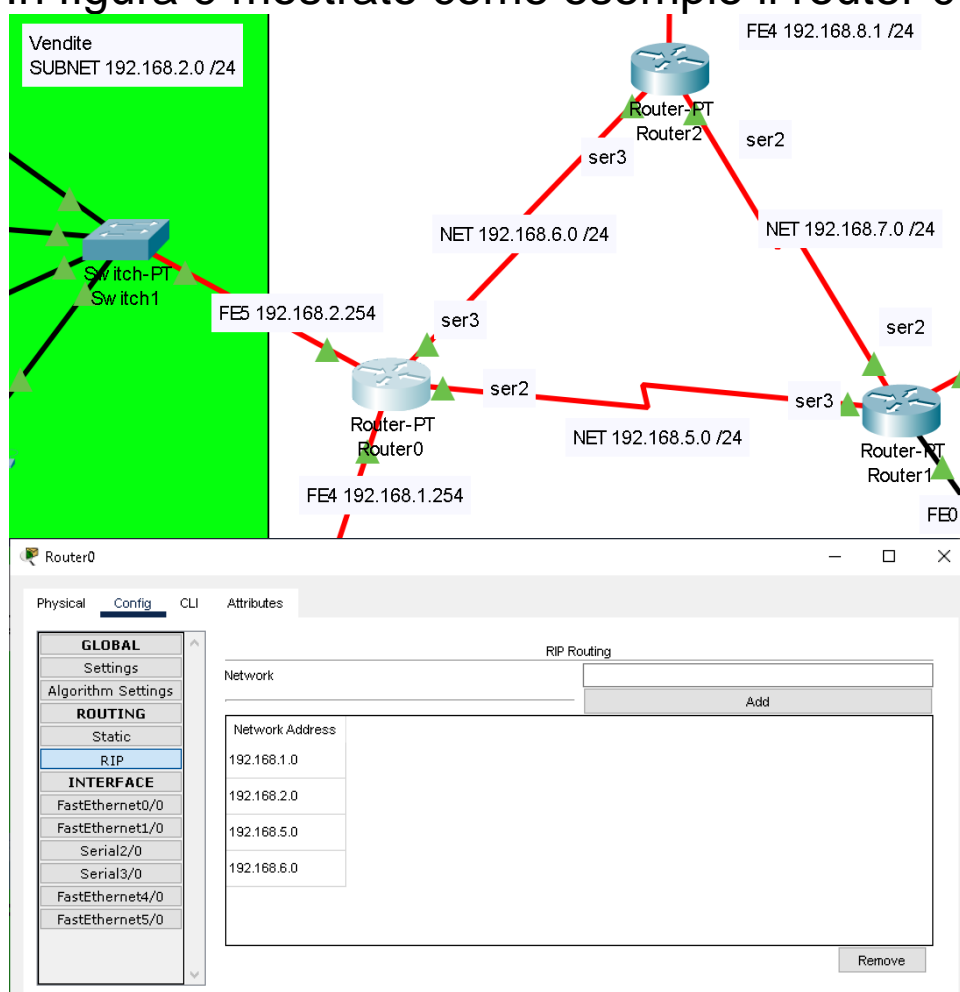
Per quanto riguarda l'indirizzamento tramite protocollo IP, sono stati scelti indirizzi IP privati di classe C per indirizzare i dispositivi della LAN. In particolare i primi due ottetti dell'IP rimangono invariati (192.168) mentre applicando una maschera di sottorete /24 (255.255.255.0) il terzo ottetto determina la sottorete e il quarto l'host all'interno di quella specifica sottorete. La maschera considerata permette di indirizzare fino a $2^8-2 = 254$ sottoreti differenti, ciascuna con $2^8-2=254$ host distinti. Tale configurazione permette di rendere la topologia di rete scalabile per LAN di qualsiasi dimensione e rende immediata la distinzione tra le varie sottoreti (terzo ottetto) e tra i dispositivi presenti in esse. In particolare le sottoreti di Amministrazione, Produzione e Vendite fanno capo agli indirizzi 192.168.4.0, 192.168.3.0, 192.168.2.0, mentre la Server Farm è la rete 192.168.1.0. L'indirizzo di gateway (per tutti i dispositivi della LAN) è costituito dall'interfaccia interna del router di frontiera, ossia 192.168.8.2 mentre l'interfaccia esterna corrisponde all'IP pubblico dell'azienda, ossia 200.100.10.1. Per la comunicazione tra i router interni alla LAN sono necessari IP di sottoreti differenti, discriminate dal terzo ottetto dell'IP (192.168.5.0, 192.168.6.0, 192.168.7.0, 192.168.8.0). Infine l'indirizzo del server DNS locale (per tutti i dispositivi della LAN) è 192.168.1.1.

Per quanto riguarda la rete che simula il funzionamento di internet, gli indirizzi IP sono assegnati senza un criterio specifico tranne per il fatto che sono tutti IP pubblici.

Configurazione dei router

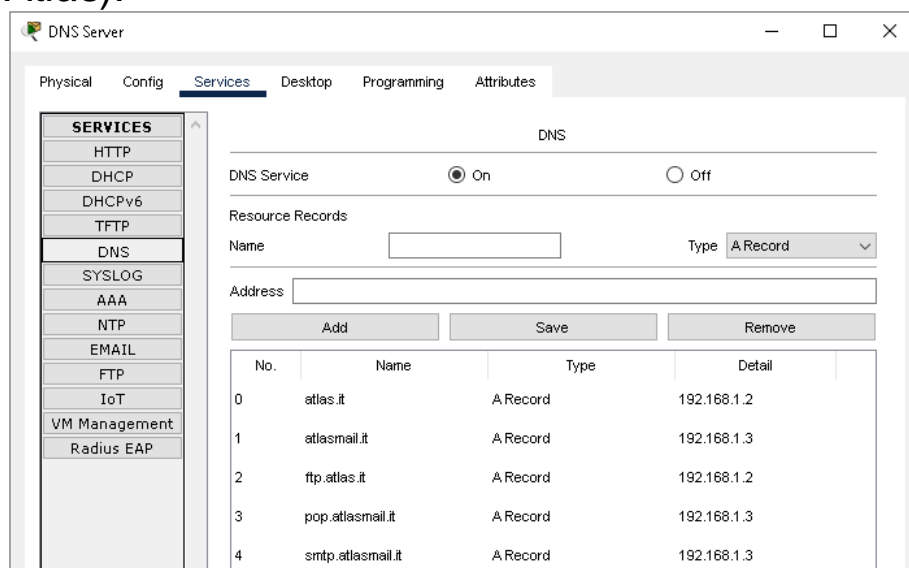
Una volta collegati i router come da topologia, è necessario configurare, per ciascuno di essi, un unico protocollo d'instradamento dei pacchetti di livello rete. Per realizzare un instradamento dinamico utilizziamo il Routing Information Protocol (RIP).

Implementiamo dunque il RIP per ciascun router accedendo alla relativa pagina di configurazione e inserendo per ciascuna interfaccia attiva del router l'indirizzo IP della rete a cui da accesso tale interfaccia. In figura è mostrato come esempio il router 0.



Configurazione dei servizi DNS, FTP, HTTP e Mail

I servizi DNS, FTP, HTTP e Mail interni alla LAN, sono ospitati sui 3 server della sottorete 192.168.1.0. Il servizio DNS locale è raggiungibile all'IP 192.168.1.1 ed è configurabile andando a popolare il relativo database DNS come nella figura seguente (per una ipotetica azienda che ospita tali servizi denominata *Atlas*).



DNS

DNS Service ☒ On ☐ Off

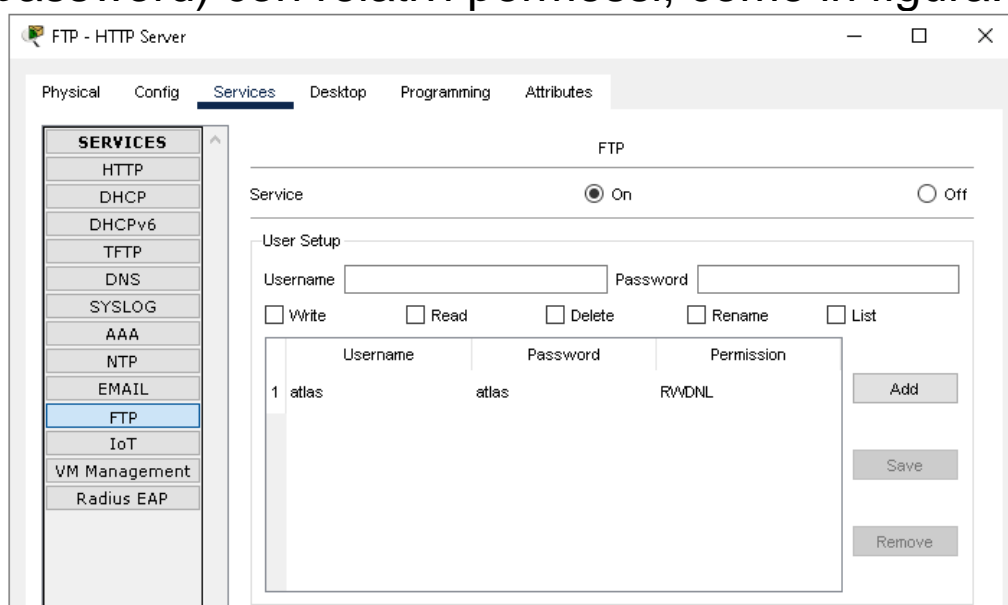
Resource Records

Name Type

Address

No.	Name	Type	Detail
0	atlas.it	A Record	192.168.1.2
1	atlasmail.it	A Record	192.168.1.3
2	ftp.atlas.it	A Record	192.168.1.2
3	pop.atlasmail.it	A Record	192.168.1.3
4	smtp.atlasmail.it	A Record	192.168.1.3

Il servizio FTP è raggiungibile all'IP 192.168.1.2 ed è configurabile andando ad attivare il servizio e aggiungendo le credenziali di accesso (nome utente e password) con relativi permessi, come in figura.



FTP

Service ☒ On ☐ Off

User Setup

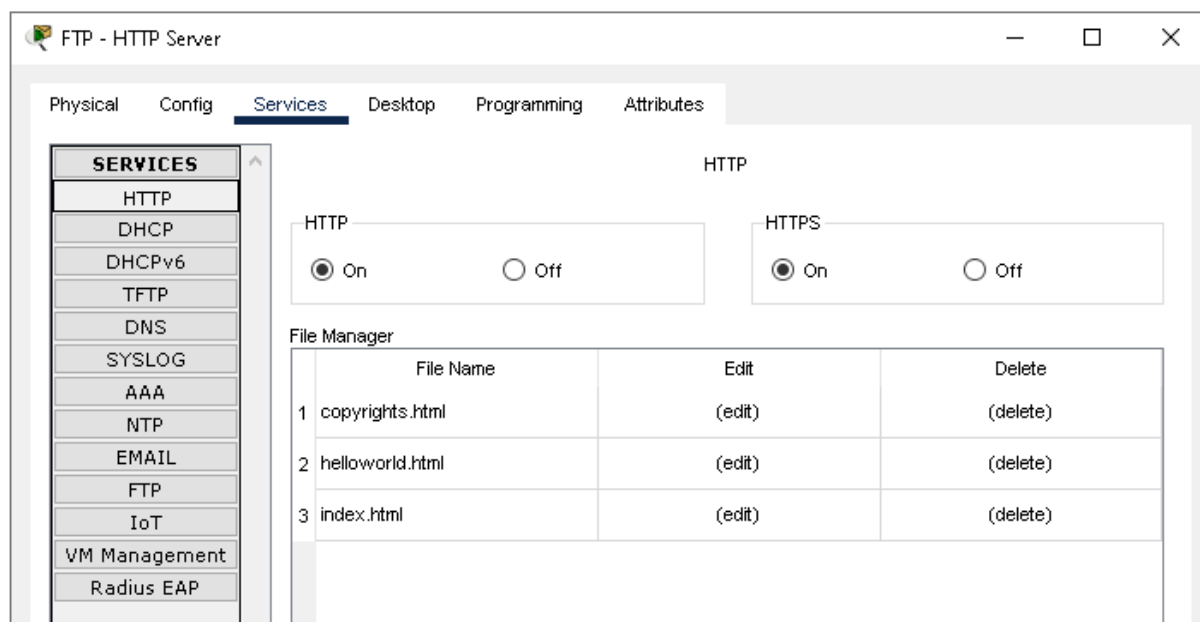
Username Password

☐ Write ☐ Read ☐ Delete ☐ Rename ☐ List

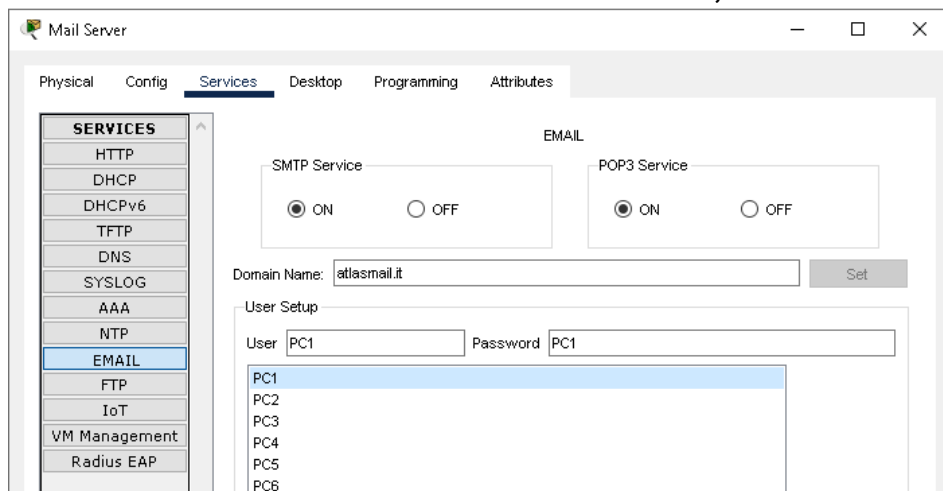
	Username	Password	Permission
1	atlas	atlas	RWDNL



Il servizio HTTP è raggiungibile all'IP 192.168.1.2 ed è realizzabile inserendo i file relativi al sito web (HTML, CSS, JS) nella apposita finestra di configurazione, come nella figura seguente.



Il servizio di e-Mail aziendale è raggiungibile all'IP 192.168.1.3 ed è realizzabile inserendo nel database del mail server le credenziali di accesso di tutti i fruitori del servizio di posta (nome utente e password) ed abilitando i servizi POP3 e SMTP, come in figura sotto.





Collegamento della LAN ad Internet

NAT e Port Forwarding (PF)

Gli indirizzi IP privati sono riutilizzabili e servono per limitare l'utilizzo degli IP pubblici, per cui, quando un Host di una LAN, che utilizza un IP privato, intende collegarsi a Internet (dove è richiesto un IP pubblico univoco) si ricorre al Network Address Translation (NAT) per far corrispondere i due indirizzi (altrimenti la connessione non può avvenire). Simmetricamente un indirizzo IP privato non è visibile dall'esterno (internet) ed è necessaria la traduzione degli indirizzi tramite NAT e PF.

Il router di frontiera (Router 7), su cui sarà abilitato il NAT, avrà due interfacce: una che si affaccia sulla rete locale, a cui sarà associato un IP privato (192.168.8.2); e una che si affaccia sulla rete Internet, a cui sarà associato un IP pubblico (200.100.10.1).

Per abilitare il NAT sul router di frontiera della LAN occorre digitare i seguenti comandi nella CLI del router.

```
<invio>  
> enable  
# configure terminal  
# ip nat inside source static <ip privato> <ip  
pubblico>  
  
# interface <interfaccia esterna>  
# ip nat outside  
  
# interface <interfaccia interna>  
# ip nat inside
```



Mentre per abilitare il Port Forwarding sui vari server della LAN, occorre digitare (nella CLI del router):

```
# ip nat inside source static [tcp | udp] <ip statico  
server> <porta ascolto server> <ip pubblico rete>  
<porta ascolto router frontiera>
```

Tramite il comando `ip nat inside source static <ip privato> <ip pubblico>` abilitiamo un NAT statico che mappa gli indirizzi privati della LAN nell'unico IP pubblico sul gateway di frontiera. Con i comandi `ip nat outside` e `ip nat inside` configuriamo rispettivamente il NAT per l'interfaccia esterna e interna del router di frontiera. Infine, con il comando `ip nat inside source static [tcp | udp] <ip statico server> <porta ascolto server> <ip pubblico rete> <porta ascolto router frontiera>` abilitiamo il Port Forwarding per poter accedere ai vari servizi dalla rete internet.

In particolare, per la rete LAN progettata, i comandi specifici sono i seguenti (Router 7).

Per il NAT:

```
<invio>  
> enable  
# configure terminal  
# ip nat inside source static 192.168.8.2 200.100.10.1  
  
# interface fastEthernet5/0  
# ip nat outside  
  
# interface fastEthernet4/0  
# ip nat inside
```




Per il Port Forwarding:

- HTTP: # ip nat inside source static tcp
192.168.1.2 80 200.100.10.1 80
- HTTPS: # ip nat inside source static tcp
192.168.1.2 443 200.100.10.1 443
- DNS: # ip nat inside source static udp
192.168.1.1 53 200.100.10.1 53
- FTP data: # ip nat inside source static tcp
192.168.1.2 20 200.100.10.1 20
- FTP control: # ip nat inside source static tcp
192.168.1.2 21 200.100.10.1 21
- POP3: # ip nat inside source static tcp
192.168.1.3 995 200.100.10.1 995
- SMTP: # ip nat inside source static tcp
192.168.1.3 25 200.100.10.1 25

Per verificare la presenza del NAT e PF basta digitare `show ip nat translations` nella CLI del router di frontiera (Router 7), come nella figura seguente.

```
Router>enable
Router#show ip nat trans
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  ---
udp  200.100.10.1:53      192.168.1.1:53    ---                ---
    200.100.10.1      192.168.8.2       ---                ---
tcp  200.100.10.1:1030    192.168.8.2:1030  173.122.0.1:1029   173.122.0.1:1029
tcp  200.100.10.1:110    192.168.8.2:110   173.122.0.1:1030   173.122.0.1:1030
tcp  200.100.10.1:20     192.168.1.2:20    ---                ---
tcp  200.100.10.1:21     192.168.1.2:21    ---                ---
tcp  200.100.10.1:25     192.168.1.3:25    ---                ---
tcp  200.100.10.1:443    192.168.1.2:443   ---                ---
tcp  200.100.10.1:80     192.168.1.2:80    ---                ---
tcp  200.100.10.1:80     192.168.1.2:80    173.122.0.1:1025   173.122.0.1:1025
tcp  200.100.10.1:80     192.168.1.2:80    173.122.0.1:1026   173.122.0.1:1026
tcp  200.100.10.1:80     192.168.1.2:80    173.122.0.1:1027   173.122.0.1:1027
tcp  200.100.10.1:80     192.168.1.2:80    173.122.0.1:1031   173.122.0.1:1031
tcp  200.100.10.1:80     192.168.1.2:80    173.122.0.1:1032   173.122.0.1:1032
tcp  200.100.10.1:80     192.168.1.2:80    173.122.0.1:1033   173.122.0.1:1033
tcp  200.100.10.1:995    192.168.1.3:995   ---                ---
```

Router#



Sicurezza della rete LAN

Switch Port Security (SPS)

Per quanto riguarda la sicurezza interna all'azienda si è deciso di implementare un meccanismo per limitare l'accesso a determinate interfacce dei vari switch di rete, in modo che solo i dispositivi autorizzati possano accedere alla rete LAN. Tale funzionalità è detta Switch Port Security e permette di associare indirizzi MAC di determinati dispositivi (ad esempio PC aziendali) a specifiche interfacce di uno switch.

Per implementare lo Switch Port Security sui 4 switch presenti sulla rete LAN (Switch 1,2,3,4) occorre configurare opportunamente ogni switch tramite Command Line Interface (CLI).

Una volta acceduto alla CLI dello switch scelto occorre digitare i seguenti comandi per abilitare tale funzionalità di sicurezza.

Accedo al terminale per configurare lo switch:

```
<invio>  
> enable  
# configure terminal
```

Seleziono le interfacce su cui operare:

```
# interface <interfacce in cui implementare SPS>
```



Applico lo SPS ed esco dalla configurazione:

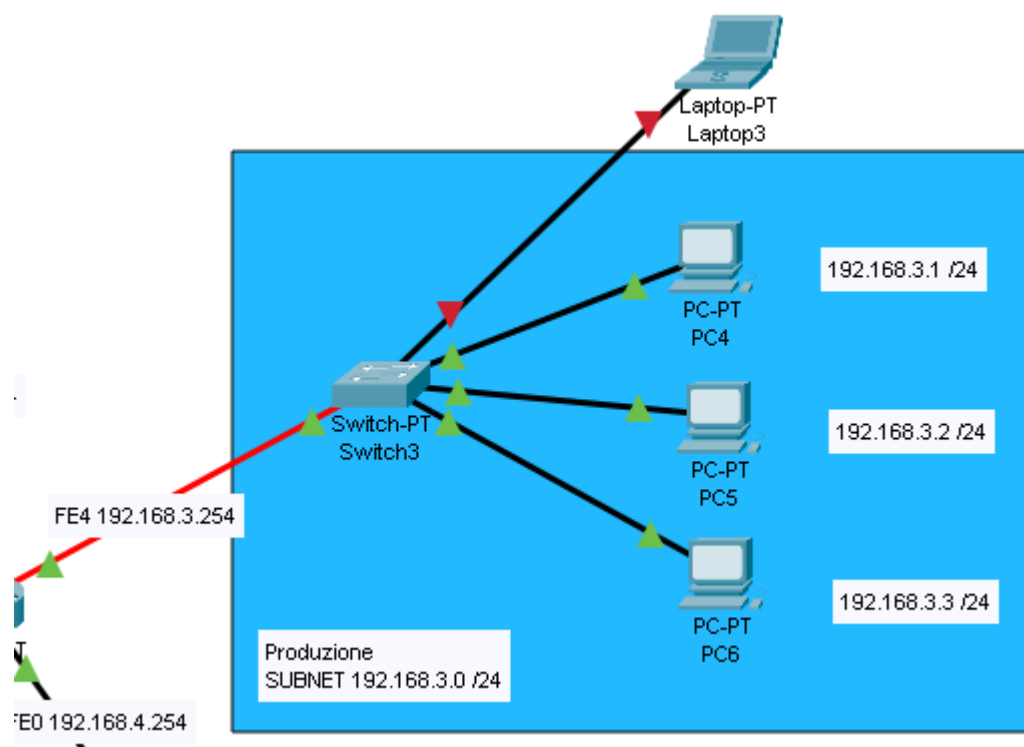
```
# switchport mode access
# switchport port-security
# switchport port-security maximum 1
# switchport port-security mac-address sticky
# switchport port-security violation restrict
# exit
```

Per disabilitare le porte non utilizzate occorre digitare:

```
# interface <interfacce da disabilitare>
# shutdown
```

Tramite questi comandi configuriamo tutte le interfacce lecite dei vari switch (come stabilito da progetto) abilitando tale sicurezza su ciascuna porta e associando gli indirizzi MAC dei dispositivi aziendali alle interfacce corrispondenti in modo automatico tramite il comando `switchport port-security mac-address sticky`. Con il comando `shutdown` le restanti interfacce vengono disabilite in modo da impedire connessioni tramite cavo non autorizzate dall'amministratore di rete. Tramite il comando `switchport port-security violation restrict` i pacchetti inviati alla rete da un dispositivo non autorizzato sono ignorati. Il comando `switchport port-security maximum 1` definisce il numero massimo di indirizzi MAC che possono essere associati alla stessa porta dello switch. I comandi `switchport mode access` e `switchport port-security` permettono rispettivamente di configurare la porta come porta di accesso e abilitare SPS.

Le interfacce non utilizzate per scopi aziendali vengono disabilitate in modo da impedire connessioni tramite cavo non autorizzate dall'amministratore di rete.



Per verificare la presenza di SPS basta digitare `show port-security` nella CLI dello switch, come nella figura seguente.

```
Switch>enable
Switch#show port-se
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/1      1              1              0          Restrict
Fa1/1      1              1              0          Restrict
Fa2/1      1              1              0          Restrict
Fa4/1      1              1              0          Restrict
-----
Switch#
```

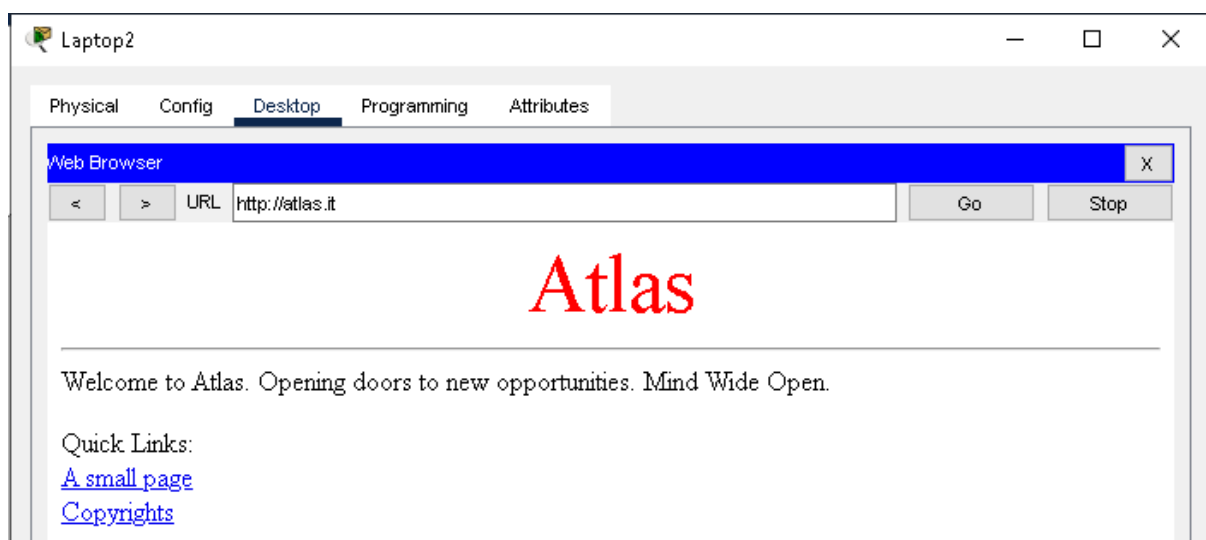


Simulazione di funzionamento della rete

Per simulare il corretto funzionamento della rete progettata, tentiamo di accedere alla pagina web dell'azienda (www.atlas.it) da un PC posto sulla rete internet. L'IP pubblico della rete LAN verrà fornito da un DNS Root posto su internet all'indirizzo 154.132.0.1.

Dunque il Laptop2 (173.122.0.1) richiederà tramite Browser di accedere alla pagina www.atlas.it e tramite il DNS Root (154.132.0.1) verrà reindirizzato sul router di frontiera della LAN dell'azienda (200.100.10.1), poi, tramite NAT e PF si collegherà al servizio HTTP posto sulla macchina all'indirizzo locale 192.168.1.2 alla porta 80.

Pagina Web del sito aziendale all'indirizzo www.atlas.it:





Traccia di simulazione della richiesta HTTP descritta:

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop2	DNS
	0.001	Laptop2	Router5	DNS
	0.002	Router5	Router3	DNS
	0.003	Router3	DNS Root	DNS
	0.004	DNS Root	Router3	DNS
	0.005	Router3	Router5	DNS
	0.006	Router5	Laptop2	DNS
	0.006	--	Laptop2	TCP
	0.007	Laptop2	Router5	TCP
	0.008	Router5	Router3	TCP
	0.009	Router3	Router7	TCP
	0.010	Router7	Router2	TCP
	0.011	Router2	Router0	TCP
	0.012	Router0	Switch2	TCP
	0.013	Switch2	FTP - HTTP Server	TCP
	0.014	FTP - HTTP Server	Switch2	TCP
	0.015	Switch2	Router0	TCP
	0.016	Router0	Router2	TCP
	0.017	Router2	Router7	TCP
	0.018	Router7	Router3	TCP
	0.019	Router3	Router5	TCP
	0.020	Router5	Laptop2	TCP

In questa simulazione il Laptop2 effettua una richiesta DNS al DNS Root (pubblico) per ottenere l'IP pubblico associato al dominio `www.atlas.it` (200.100.10.1), successivamente, accede alla pagina HTTP stabilendo una connessione TCP con l'FTP – HTTP Server aziendale all'interno della rete LAN.