Laboratorio di introduzione alla matematica computazionale
A.A. 2021/2022
02 - Protocolli di rete

Fabio Durastante <fabio.durastante@unipi.it>
Sergio Steffè <steffe@mail.dm.unipi.it>

5 Ottobre 2021 & 6 Ottobre 2021

Dati e protocolli

- La trasmissione di dati tra calcolatori avviene spesso tramite scambio di pacchetti di dati ("protocolli di trasmissione").
- Al di sopra di questo livello, le applicazioni devono accordarsi su un linguaggio per interpretare i dati scambiati ("protocolli delle applicazioni").
- per trasmettere un flusso apparentemente continuo di dati, come quando si trasmette della musica o un film, il flusso di dati viene spezzato in pacchetti, spedito, e all'arrivo i pacchetti vengono rimessi in ordine, posti in un buffer, che ricostruisce il flusso di dati.
- una caratteristica di questa tecnica digitale - rispetto alla trasmissione analogica - è che si ha un ritardo (time lag) prodotto dal necessario *buffering* dei pacchetti in arrivo.

Dettagli dei pacchetti

- I pacchetti sono formati da una parte contenente i **dati veri e propri** ("payload") e da una **parte** che contiene le informazioni per **trasportare** i pacchetti **a destinazione** e **verificarne l'integrità** ("header" and "trailers")
- Il calcolatore di partenza spedisce il pacchetto ad una interfaccia di rete. Da questa il pacchetto viaggia attraverso diversi tipi di **snodi** che lo **smistano** da una rete all'altra fino ad arrivare al calcolatore di destinazione. Anche questo esamina i dati di *header* e *trailers* per verificare che il **pacchetto** sia giunto **integro**, e per sapere a quale **applicazione** deve **passare i dati**.
- dati complessi sono distribuiti in più pacchetti. *I pacchetti possono arrivare in ordine diverso da quello di spedizione*.
- L'uso dei pacchetti permette di fare *condividere in maniera efficiente* le linee di comunicazione.

MAC Address

- *bluetooth*, *wifi*, *ethernet*, *rete mobile*, comunicano tutti attraverso pacchetti.
- Ad **ogni interfaccia** usata per trasmettere pacchetti viene assegnato - di solito dal costruttore - un identificativo detto MAC Address (**M**edia **A**ccess **C**ontrol Address) che solitamente consiste di **12 cifre esadecimali** (48 bits), di cui la prima parte è il codice del costruttore e la seconda identifica l'interfaccia.

```
f.durastante@mathsgalore:~$ ip --brief link
lo               UNKNOWN        00:00:00:00:00:00 <LOOPBACK,UP,LOWER_UP>
ens160           UP             00:50:56:8f:70:61 <BROADCAST,MULTICAST,UP,LOWER_UP>
```

- Le macchine virtuali hanno interfacce virtuali e anche a queste viene associato un MAC address.
- nello *header* di un pacchetto vengono inseriti i MAC Address del *mittente* e del *destinatario*.

Reti Locali: LAN Local Area Network

- Il **mezzo** attraverso cui i vari calcolatori si scambiano i pacchetti può essere semplicemente **l'etere** – come per il bluetooth e il WIFI, o dei **cavi in rame** o **fibra ottica**.
- le interfacce possono comunicare **direttamente** tra di loro oppure attraverso attrezzature di rete apposite come *hub* e *switches*.
- la distinzione importante dal punto di vista logico è tra **rete mescolante** e **non mescolante**: in una rete mescolante ciascuna interfaccia vede tutto il traffico delle altre interfacce, mentre in una rete non mescolante ad una interfaccia arriva solo il traffico a lei destinato.
- Il primo passo per comunicare con un altro calcolatore della stessa LAN consiste nel procurarsi il suo MAC Address.
- attrezzature di rete, come gli *switches*, vedono arrivare ad una porta **pacchetti con certi MAC Address** nel campo "mittente" e costruiscono per ogni porta una lista dei MAC Address delle interfacce collegate a quella porta. In questo modo quando arriva un pacchetto con destinatario un certo MAC address sanno su quale porta devono mandare il pacchetto.
- le liste sono aggiornate circa ogni 30 secondi.

Internet

- **Internet è essenzialmente una federazione di reti locali (LAN)**. Le LAN sono collegate tra loro da apparecchi dedicati, i *router*.
- per identificare una macchina in Internet viene usato un Indirizzo IP (**I**nternet **P**rotocol). Ci sono attualmente **due standard**, IPv4 e IPv6.

  IPv4 usa indirizzi composti di 4 numeri tra 0 e 255, tipo 131.114.10.97

  IPv6 usa indirizzi composti da 8 gruppi di 4 cifre esadecimali ciascuno, tipo 2001:760:2c0c:202::97 (cioè 2001:0760:2c0c:0202:0000:0000:0000:0097)
- la assegnazione dei numeri viene fatta con un sistema di deleghe a partire dalla IANA (Internet Assigned Numbers Authority)
- **131.114.x.x** sono per esempio i numeri IPv4 assegnati all'Università di Pisa.

```
f.durastante@mathsgalore:~$ nmcli dev show ens160 | grep IP4.ADD*
IP4.ADDRESS[1]:                         131.114.50.240/23
```

- ad una LAN vengono dati numeri vicini.

Maschera di rete e *gateway*

Per collegarsi in internet una macchina deve conoscere il proprio IP. Per mandare pacchetti ad altre macchine su Internet occorrono altre informazioni:

- La **maschera di rete**: se l'IP con cui si vuole comunicare sta sulla stessa LAN allora si possono mandare direttamente i pacchetti sulla LAN. La maschera di rete permette di sapere quali sono gli IP che stanno sulla stessa LAN.

```
f.durastante@mathsgalore:~$ ifconfig ens160 | grep netmask
        inet 131.114.50.240  netmask 255.255.254.0  broadcast 131.114.51.255
```

Maschera di rete e *gateway*

Per collegarsi in internet una macchina deve conoscere il proprio IP. Per mandare pacchetti ad altre macchine su Internet occorrono altre informazioni:

- La **maschera di rete**: se l'IP con cui si vuole comunicare sta sulla stessa LAN allora si possono mandare direttamente i pacchetti sulla LAN. La maschera di rete permette di sapere quali sono gli IP che stanno sulla stessa LAN.
- L'**IP del gateway**. Almeno una interfaccia di rete della LAN deve essere collegata ad un router.

```
f.durastante@mathsgalore:~$ nmcli dev show ens160 | grep IP4.GATEWAY
IP4.GATEWAY:                            131.114.50.1
```

  - Se si usa IPv4 occorre sapere l'IP del router,
  - Se si usa IPv6 il router può venire autoconfigurato, oppure essere configurato a mano. IPV6 prevede di poter avere diversi router sulla LAN e un meccanismo di autoconfigurazione sui computer – Questo è in realtà un **discreto rischio di sicurezza**, perchè un hacker potrebbe inserire in una rete IPv6 un suo router intercettando così il traffico. L'amministratore della rete può però monitorare questi rogue advertisment e bloccarli.

Maschera di rete e *gateway*

Per collegarsi in internet una macchina deve conoscere il proprio IP. Per mandare pacchetti ad altre macchine su Internet occorrono altre informazioni:

- La **maschera di rete**: se l'IP con cui si vuole comunicare sta sulla stessa LAN allora si possono mandare direttamente i pacchetti sulla LAN. La maschera di rete permette di sapere quali sono gli IP che stanno sulla stessa LAN.
- L'**IP del gateway**. Almeno una interfaccia di rete della LAN deve essere collegata ad un router.
- Se dall'**esame dell IP** si vede che il **destinatario** sta sulla **stessa LAN**, si **cerca il MAC Address** del destinatario e si **spedisce** il pacchetto sulla LAN. Altrimenti si cerca il **MAC Address del router** e si **spedisce** il pacchetto **al router**.
- Il router dalle sue tabelle – che vengono *continuamente aggiornate* – sa su quale altra interfaccia deve girare il pacchetto ricevuto per farlo arrivare all'IP di destinazione.

Maschera di rete e *gateway*

Per collegarsi in internet una macchina deve conoscere il proprio IP. Per mandare pacchetti ad altre macchine su Internet occorrono altre informazioni:

- La **maschera di rete**: se l'IP con cui si vuole comunicare sta sulla stessa LAN allora si possono mandare direttamente i pacchetti sulla LAN. La maschera di rete permette di sapere quali sono gli IP che stanno sulla stessa LAN.
- L'**IP del gateway**. Almeno una interfaccia di rete della LAN deve essere collegata ad un router.
- Se dall'**esame dell IP** si vede che il **destinatario** sta sulla **stessa LAN**, si **cerca il MAC Address** del destinatario e si **spedisce** il pacchetto sulla LAN. Altrimenti si cerca il **MAC Address del router** e si **spedisce** il pacchetto **al router**.
- Il router dalle sue tabelle – che vengono *continuamente aggiornate* – sa su quale altra interfaccia deve girare il pacchetto ricevuto per farlo arrivare all'IP di destinazione.
- Per **impostare queste configurazioni** le macchine possono usare un servizio di **D**ynamic **H**ost **C**onfiguration **P**rotocol (DHCP). Questo è un protocollo che permette ai dispositivi della LAN di ricevere automaticamente – ad ogni richiesta di accesso – un IP e la relativa configurazione necessaria.

Numeri e Nomi

La maggior parte delle persone ricorda più facilmente dei nomi piuttosto che dei numeri... Per questo motivo, oltre ai numeri Internet, sono definiti i cosiddetti **domain names** di Internet.

- la **assegnazione** dei nomi viene fatta con un **sistema di deleghe** a partire dalla IANA.
- ordine gerarchico da destra a sinistra: `.it` ← `.unipi.it` ← `.dm.unipi.it` ← `.cs.dm.unipi.it` per esempio.
- a parte quelli istituzionali i domini si possono comperare anno per anno. Per esempio steffe.pisa.it !
- **non c'e' una corrispondenza biettiva tra numeri e nomi**. Sono usati con **principi diversi**. L'**IP** si riferisce ad una **interfaccia di rete** in Internet, il **domain name** può servire per avere dei *sotto-domini*, o per indicare un *dominio di posta*, o per indicare una macchina che può avere più interfacce, o un *sito web* su un server che ospita diversi siti web con nomi diversi...

Numeri e Nomi

La maggior parte delle persone ricorda più facilmente dei nomi piuttosto che dei numeri... Per questo motivo, oltre ai numeri Internet, sono definiti i cosiddetti **domain names** di Internet.

- la **assegnazione** dei nomi viene fatta con un **sistema di deleghe** a partire dalla IANA.
- ordine gerarchico da destra a sinistra: `.it` ← `.unipi.it` ← `.dm.unipi.it` ← `.cs.dm.unipi.it` per esempio.
- a parte quelli istituzionali i domini si possono comperare anno per anno. Per esempio steffe.pisa.it !
- **non c'e' una corrispondenza biettiva tra numeri e nomi**. Sono usati con **principi diversi**. L'**IP** si riferisce ad una **interfaccia di rete** in Internet, il **domain name** può servire per avere dei *sotto-domini*...
- per comunicare con un servizio con un certo domain name **un calcolatore deve comunque risalire a un numero IP**.
- Il sistema dei **Domain Name Server** (DNS) fornisce questo fondamentale servizio di rete, di collegare numeri IP a nomi di domini in maniera appropriata.

Il DNS

Nota: Il loro indirizzo va conosciuto in modo numerico!

```
f.durastante@mathsgalore:~$ nmcli dev show ens160 | grep IP4.DNS*
IP4.DNS[1]:                             131.114.21.25
IP4.DNS[2]:                             131.114.21.15
IP4.DNS[3]:                             8.8.8.8
```

Un server DNS non fornisce solamente traduzioni da nome ad indirizzo, ma anche altre informazioni, ad esempio:

- Records `A`, `AAAA`: indirizzi IPv4 o IPv6.
- Records `MX`: chi gestisce la posta per questo dominio?
- Records `SOA`, `NS`: informazioni sui nameserver del dominio.
- Records `TXT`: ancora altre informazioni varie.

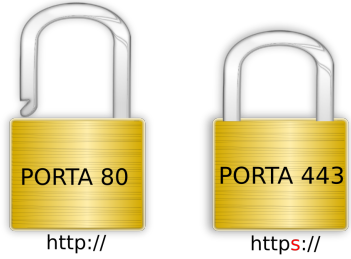
Sotto Linux possiamo usare il comando `host` (oppure anche `dig`, `nslookup`) per interrogare un server DNS.
Esempio: potete provare in una *shell*: `$ host 8.8.8.8`, chi gestisce questo DNS?

Servizi e porte

Normalmente un calcolatore ha in corso allo stesso tempo **scambi di pacchetti** con molti altri calcolatori. Quando arrivano le risposte, come fa a passarle all'**utente** e al **programma giusto**?

- **numero di porta:** serve al calcolatore per sapere a **quale programma** passare il pacchetto arrivato
- servizi standard hanno numeri di porta standard
- i primi 1024 numeri di porta sono riservati a root per servizi standard noti
- gli altri vengono usati dagli utenti se sono liberi.

Per **esempio** per vistare un sito web si mandano pacchetti da una porta utente libera alla porta 80 (*oppure* alla porta 443) del sito da visitare, che risponderà mandando pacchetti dalla porta 80 (*oppure* dalla porta 443) al numero di porta che l'utente ha usato.



Firewall e TCP-Wrappers

- A volte se si vuole **avere un servizio non aperto a tutta la rete** ma solo ad alcune macchine.
- Un *vecchio sistema* usa i TCP Wrappers, che possono impedire l'inizio di una connessione TCP.

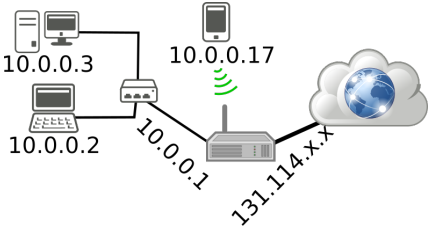
Firewall e TCP-Wrappers

- A volte se si vuole **avere un servizio non aperto a tutta la rete** ma solo ad alcune macchine.
- Un **sistema più recente** e più potente consiste nell'impostare delle regole di Firewall sul calcolatore – le regole sono gestite dal *kernel* e devono essere impostate da root.
- La possibilità di collegarsi a tutte le macchine collegate ad Internet permette a chiunque di *esplorare* (scan) gli altri calcolatori per scoprire se hanno servizi attivi.
- Gli hackers fanno continuamente questi scan e si procurano elenchi di macchine con certe *vulnerabilità*.
- A volte cercano anche di fare *login* sulla macchine, usando **password facilmente indovinabili**.
- programmi come `fail2ban` analizzano in tempo reale i log della macchina, scoprono se un un certo IP fa troppi tentativi falliti di login ed inserisce una regola di firewall che blocca per un certo tempo tutti gli ulteriori accessi alla macchina.

Reti private e NAT

- lo **standard** internet prevede alcune reti **NON** routabili. I numeri di queste reti possono essere usati da chi vuole ed appariranno solo localmente su una LAN
- Un calcolatore con due interfacce può essere collegato a una di queste reti private e ad internet
- Dalla rete privata si comunica con questo calcolatore e da qui si può comunicare con internet.
- Questa procedure può essere automatizzata con il NAT (Network Address Translation).

- la macchina che fa il NAT **prende i pacchetti dalla rete privata** e li **manda** in **internet** col **proprio IP** come fossero propri, e quando da internet arrivano le risposte li smista sulla rete privata. per fare ciò deve manipolare i pacchetti cambiando gli IP e i numeri di porta.
- In molte connessioni domestiche il cosiddetto "*router*" in realtà fa anche il NAT.



802.1x, wifi, eduroam

- 802.1x è il nome di uno standard IEEE che serve a controllare l'autorizzazione a collegarsi in rete.
- Lo switch o il WIFI con lo 802.1x chiede un **username** e **una** password, li **manda criptati** a un *server radius* e se la risposta è "autorizzato" apre il collegamento in rete.
- Viene usato in tutto il mondo per **eduroam**, che è una federazione di enti che mettono in comune l'accesso alle proprie reti WIFI.
- Nell'Università di Pisa anche le prese ethernet in giro per studi e dipartimenti usano l'autenticazione con 802.1x per permettere l'accesso alla rete.

Eduroam

Potete leggere di più sulla storia del servizio Eduroam su:
`https://www.servizi.garr.it/eduroam` e su `https://eduroam.org/`.
Le **istruzioni** per connettervi con i vostri dispositivi a questa rete li trovate su:
`http://ict.unipi.it/rete/wireless/eduroam`.

La Rete GARR

- GARR voleva dire **G**ruppo **A**rmonizzazione delle **R**eti della **R**icerca - è nato nel 1991
- una volta le università avevano 4 diversi protocolli: quello IBM, quello Digital, l'X25 e internet. Il GARR affittò linee usando un multiplexer per instradare tutti e 4 i protocolli di rete... **ora rimane solo internet!**
- Università ed enti di ricerca sono collegati al GARR che poi è collegato al resto del mondo.
- Il GARR è un **consorzio pubblico non a scopo di lucro** ed ha regole un po' più restrittive per l'uso della rete, che tutti gli utenti devono sottoscrivere – per esempio non si può scaricare un film senza un motivo di studio o ricerca...
- Il GARR si accorge (*spesso*) di queste attività non lecite e le segnala all'ente. Agli **studenti è stato bloccato** per un certo tempo **l'account** per infrazioni di questo tipo.

Collegamento ad un computer remoto

- Uno degli utilizzi principali della rete è stato quello di interagire con macchine fisicamente distanti o inacessibili.
- Questo rimane molto importante ancora oggi per chi lavora in ambito scientifico: come possiamo effettuare dei calcoli su un supercomputer come questo?

Telnet

- Verso la fine degli anni '60, i computer si trovavano solo nelle università. Tipicamente erano in stanze inaccessibili.
- Si poteva interagire con dei "terminali", come questo:

- Viene sviluppato il programma `telnet`, che permette di emulare una "telescrivente" da un altro computer connesso in rete.

Telnet

- Verso la fine degli anni '60, i computer si trovavano solo nelle università. Tipicamente erano in stanze inaccessibili.
- Si poteva interagire con dei "terminali", come questo:
- Viene sviluppato il programma `telnet`, che permette di emulare una "telescrivente" da un altro computer connesso in rete.
- Negli anni '70, la rete era un lusso per pochi.
- Di conseguenza, la sicurezza del `telnet` era inesistente. Come una telescrivente, tutto quello che era scritto o stampato veniva inviato e ricevuto senza nessun filtro o crittografia.

SSH

Al giorno d'oggi, `telnet` non viene più utilizzato.

- Chiunque potrebbe ascoltare la "conversazione", rubando ad esempio la nostra password.
- Non c'è nessun modo di garantire che il computer a cui ci stiamo collegando sia "autentico", qualcuno potrebbe aver dirottato la connessione.

SSH

Al giorno d'oggi, `telnet` non viene più utilizzato.

- Chiunque potrebbe ascoltare la "conversazione", rubando ad esempio la nostra password.
- Non c'è nessun modo di garantire che il computer a cui ci stiamo collegando sia "autentico", qualcuno potrebbe aver dirottato la connessione.

Questi problemi e limitazioni sono risolti dal programma che lo ha sostituito, ovvero `ssh`. Vediamo un esempio.

```
$ ssh f.durastante@mathsgalore.unipi.it
The authenticity of host 'mathsgalore (x.y.z.w)' can't be established.
ECDSA key fingerprint is SHA256:xcn6kDnHQzfKjijUuhpgeGyYN5naeAD7r24SX9IwCCI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'mathsgalore' (ECDSA) to the list of known hosts.
f.durastante@mathsgalore's password:

f.durastante@mathsgalore:~$
```

Struttura del comando SSH

$$\texttt{ssh}\ \underbrace{\texttt{f.durastante}}_{\texttt{username}}\texttt{@}\underbrace{\texttt{mathsgalore.unipi.it}}_{\texttt{nome del server}}$$

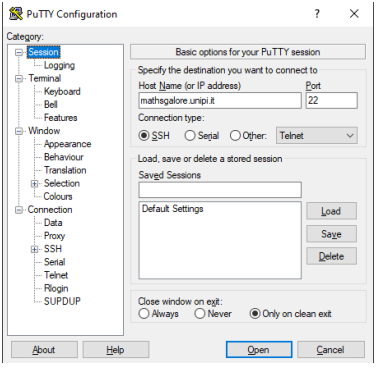
- Se lo *username* è lo **stesso sui due PC**, può essere omesso.
- Questo comando ci permette di aprire una sessione non grafica sul computer remoto.
- Sarà lo step preliminare di tutti gli esercizi in laboratorio.

Se utilizzate Linux o MAC OS X, avete già il comando ssh a disposizione. Su Windows, è possibile utilizzare il software Putty, che potete scaricare da:

`https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html`

Configurare Putty (solo per utenti Windows)

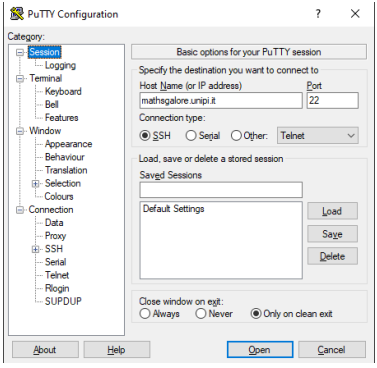
Per il momento utilizzeremo connessioni da remoto **senza interfaccia grafica**, quindi possiamo accontentarci di una configurazione basilare di Putty.



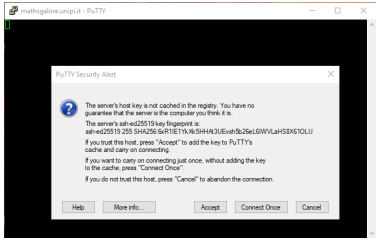
1. Installare e avviare Putty
2. Nell'interfaccia qui illustrata inserire il nome (o l'**indirizzo IP**) della macchina a cui ci si vuole connettere.
3. Fare click su open

Configurare Putty (solo per utenti Windows)

Per il momento utilizzeremo connessioni da remoto **senza interfaccia grafica**, quindi possiamo accontentarci di una configurazione basilare di Putty.



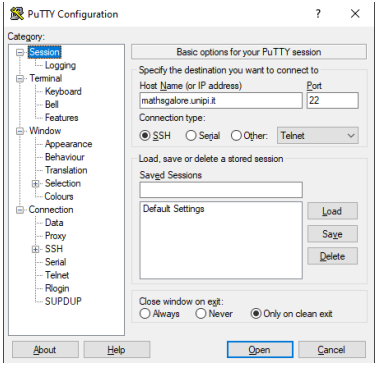
1. Installare e avviare Putty
2. Nell'interfaccia qui illustrata inserire il nome (o l'**indirizzo IP**) della macchina a cui ci si vuole connettere.
3. Fare click su open



- Ci viene richiesto di accettare il certificato crittografico della macchina a cui vogliamo connetterci, se è quella voluta si prema "Accept",

Configurare Putty (solo per utenti Windows)

Per il momento utilizzeremo connessioni da remoto **senza interfaccia grafica**, quindi possiamo accontentarci di una configurazione basilare di Putty.

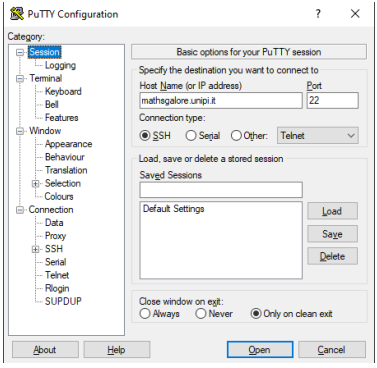


1. Installare e avviare Putty
2. Nell'interfaccia qui illustrata inserire il nome (o l'**indirizzo IP**) della macchina a cui ci si vuole connettere.
3. Fare click su open

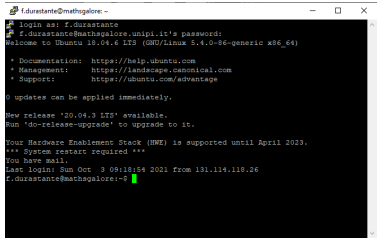
- Ci viene richiesto di accettare il certificato crittografico della macchina a cui vogliamo connetterci, se è quella voluta si prema "Accept",
- Inserire il proprio **nome utente** e **password**.

Configurare Putty (solo per utenti Windows)

Per il momento utilizzeremo connessioni da remoto **senza interfaccia grafica**, quindi possiamo accontentarci di una configurazione basilare di Putty.



1. Installare e avviare Putty
2. Nell'interfaccia qui illustrata inserire il nome (o l'**indirizzo IP**) della macchina a cui ci si vuole connettere.
3. Fare click su open



- Ci viene richiesto di accettare il certificato crittografico della macchina a cui vogliamo connetterci, se è quella voluta si prema "Accept",
- Inserire il proprio **nome utente** e **password**.
- Si è completato il *login* e si ha una *shell* attiva sulla macchina remota.

Come connettersi alle macchine del centro di calcolo

Per una **questione di sicurezza** per connettersi alle macchine del centro di calcolo d'ateneo è necessario connettersi da un IP della rete di ateneo

Come connettersi alle macchine del centro di calcolo

Per una **questione di sicurezza** per connettersi alle macchine del centro di calcolo d'ateneo è necessario connettersi da un IP della rete di ateneo... ma noi siamo a casa, come dobbiamo fare?

Come connettersi alle macchine del centro di calcolo

Per una **questione di sicurezza** per connettersi alle macchine del centro di calcolo d'ateneo è necessario connettersi da un IP della rete di ateneo... ma noi siamo a casa, come dobbiamo fare?

Dobbiamo usare una **r**ete **v**irtuale **p**rivata, *Virtual Private Network*, **VPN**.

- Una VPN è un servizio di rete che può essere utilizzato per **criptare il traffico Internet** e proteggere la propria identità online.
- Una VPN può essere paragonata ad una **estensione geografica della rete LAN**: possiamo collegare tra loro, in maniera sicura, i vostri computer come se fossero agganciati alla rete di ateneo.
- Sfruttiamo l'**instradamento dei pacchetti tramite il protocollo IP**: cioè realizziamo una LAN "virtuale" e "privata" ma funzionalmente equivalente ad un'infrastruttura fisica di rete dedicata.

Come connettersi alle macchine del centro di calcolo

Per una **questione di sicurezza** per connettersi alle macchine del centro di calcolo d'ateneo è necessario connettersi da un IP della rete di ateneo... ma noi siamo a casa, come dobbiamo fare?

Dobbiamo usare una **r**ete **v**irtuale **p**rivata, *Virtual Private Network*, **VPN**.

- Una VPN è un servizio di rete che può essere utilizzato per **criptare il traffico Internet** e proteggere la propria identità online.
- Una VPN può essere paragonata ad una **estensione geografica della rete LAN**: possiamo collegare tra loro, in maniera sicura, i vostri computer come se fossero agganciati alla rete di ateneo.
- Sfruttiamo l'**instradamento dei pacchetti tramite il protocollo IP**: cioè realizziamo una LAN "virtuale" e "privata" ma funzionalmente equivalente ad un'infrastruttura fisica di rete dedicata.

VPN e Sicurezza

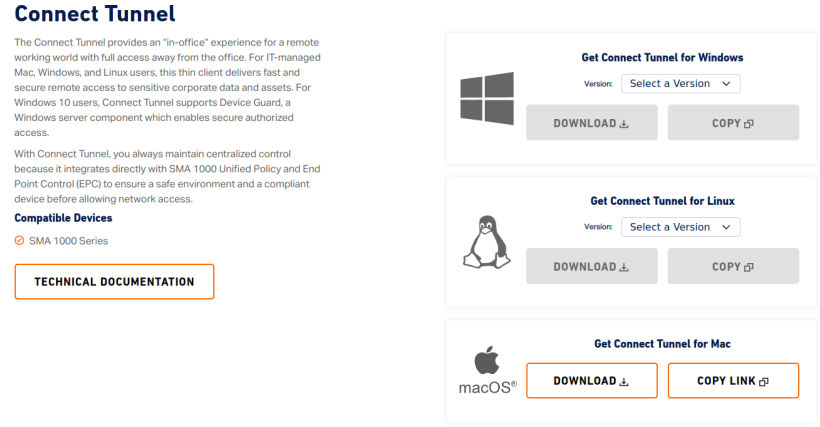
Le VPN sono molto allettanti per gli hacker; se possono entrare in una rete tramite una connessione VPN, hanno accesso a tutto quello che è sulla rete come se ne facessero parte! *Storie dell'orrore:* `https://thehackernews.com/2021/07/ransomware-attacks-targeting-unpatched.html`

Connect Tunnel: Installazione

Per connettersi alla VPN di Ateneo[1] abbiamo bisogno di utilizzare il programma Connect Tunnel dal sito:

`https://www.sonicwall.com/products/remote-access/vpn-clients/`

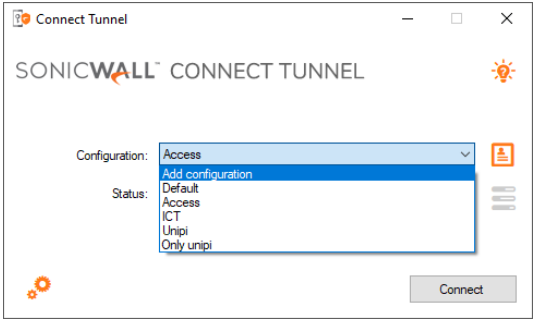
per il vostro sistema operativo:



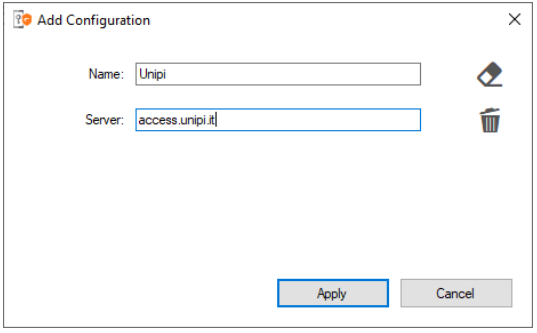
[1] Le istruzioni complete si trovano presso `https://start.unipi.it/help-ict/vpn/`.

Connect Tunnel: Configurazione

Il server per la connessione VPN si chiama **access.unipi.it** e può essere configurato nel programma Connect Tunnel con pochi semplici passaggi.



1. Aggiungere una nuova configurazione.



2. Dare un nome e indicare l'indirizzo del server e salvare la configurazione (Apply).

3. Selezionare la connessione appena configurata e premere **Connect**. Il sistema presenterà i termini d'uso del servizio e **al primo accesso chiederà di selezionare il profilo di connessione**, selezionare **Internet attraverso UNIPI**. L'accesso richiede le *credenziali di ateneo*.

Connect Tunnel: Cosa abbiamo ottenuto

L'opzione **Internet attraverso UNIPI** ci permette di accedere alle risorse digitali Internet utilizzando un indirizzo IP dell'Ateneo (131.114.x.x), in particolare ci permette di essere accettati dal firewall delle macchine a cui ci vogliamo connettere via SSH.

Una volta abilitata la VPN, il **comando SSH** per l'utente `n.cognome12@unipi.it` utilizzare, via terminale su Linux o MAC, via *Putty* sarà dunque:

- `ssh n.cognome12@nome-della-macchina`
- La **password** sarà la stessa delle *credenziali di ateneo*.
- Gli IP delle macchine sono:
  0. mathsgalore.unipi.it
  1. mathsgalore2.unipi.it
  2. mathsgalore3.unipi.it
  3. mathsgalore4.unipi.it

  il vostro account risiede sulla macchina r per: n°matricola $\equiv r \pmod 4$[2].

[2] Si dice che un intero a m a è equivalente a $m \equiv r \pmod n$ se e solo se la differenza $m - r$ è un multiplo relativo di n. La vostra macchina è quindi quella con IP all'elenco $r = 0, 1, 2, 3$, ovvero alla classe di resto r rappresenta, oltre a r stesso, tutti i numeri interi della forma $m = k \times 4 + r$ per qualche intero k.

Esempio di determinazione della macchina

Supponiamo di essere lo studente `d.lampa` con **numero di matricola** 583447.

- Per scoprire su che macchina dobbiamo connetterci dobbiamo calcolare:

$$583447 \equiv r \,(\mathrm{mod}\, 4)$$

- Se cercassimo due numeri interi qualsiasi k, r per cui:

$$583447 = k \times 4 + r,$$

  ne troveremmo tanti, ad esempio $k = 100$ e $r = 583047$,
- Cerchiamo il **più grande intero** k per cui possiamo scrivere la precedente.
- Calcoliamo in $\mathbb{R}$ la divisione $583447/4$ otteniamo: $145861,75$, allora possiamo scegliere $k = 145861$ con cui troviamo:

$$583447 = 145861 \times 4 + 3 \;\Rightarrow\; r = 3,$$

- Il nostro comando di connessione è quindi:

```
ssh d.lampa@mathsgalore4.unipi.it
```

Email e protocolli

Lo scambio di email viene gestito in maniera simile, con diversi protocolli:

- SMTP: “Simple Mail Transfer Protocol”, gestisce la spedizione delle e-mail. Questo è il vero protagonista dello smistamento delle e-mail.
- IMAP, POP3, sono invece protocolli che permettono agli utenti di consultare la propria casella e-mail.
- Una mail, nella forma più semplice, è sostanzialmente un file di testo con un'intestazione.
- L'intestazione (header) contiene i metadati del messaggio: data e ora, oggetto, mittente, destinatario, ecc.

Come viene spedita una email?

Supponiamo che Alice voglia scrivere a Bob.

Come viene spedita una email?

Supponiamo che Alice voglia scrivere a Bob.

1. Alice digita il messaggio sul suo calcolatore.
2. Tramite un software, Alice affida il messaggio ad un server SMTP (il relay), che lo prende in carico.
3. Tramite uno o più passaggi, il server consegna il messaggio al server in carico di gestire le mail di Bob (ricordate `host -t MX bob.com`?)
4. Bob accede alla sua casella (con il suo software preferito, o una webmail), e legge il messaggio di Alice.

Come viene spedita una email?

Supponiamo che Alice voglia scrivere a Bob.

1. Alice digita il messaggio sul suo calcolatore.
2. Tramite un software, Alice affida il messaggio ad un server SMTP (il relay), che lo prende in carico.
3. Tramite uno o più passaggi, il server consegna il messaggio al server in carico di gestire le mail di Bob (ricordate `host -t MX bob.com`?)
4. Bob accede alla sua casella (con il suo software preferito, o una webmail), e legge il messaggio di Alice.

La trasmissione dei messaggi avviene tramite il **protocollo SMTP**.

Server di posta

- Normalmente, noi affidiamo le nostre e-mail ad un server di posta (SMTP) che gira su qualche server (`smtp.unipi.it`, ad esempio).
- Su sistemi Linux è però (abbastanza) comune avere un server su ogni macchina.
- Questo permette di spedire e-mail utilizzando comandi appositi: `sendmail`, `mail`, ...
- In realtà, questi server redirigono semplicemente tutte le e-mail ad un altro mail server del dipartimento (si veda la catena di Receive del messaggio decomposto).

SPAM

- La spedizione di e-mail è libera: chiunque può mandarmi un messaggio.
- Questo causa un'abbondanza di messaggi di spam nelle nostre caselle, in particolare se il nostro indirizzo viene pubblicato online.
- La maggior parte dei mailserver utilizza dei filtri di vario tipo per cercare di limitare queste dinamiche.
- Due tipo di filtri principali: blocking list e filtri statistici / Bayesiani.

Blocking list

- Idea molto semplice: mantenere una lista di PC che sono noti per spedire mail di spam (e.g., PC infetti, o server tipicamente utilizzati da spammer).
- La lista viene continuamente aggiornata, se il vostro PC è infetto ci potete facilmente finire per sbaglio!
- Esiste una procedura di removal per chiedere di essere rimossi dalla lista.

Filtri Bayesiani

Consideriamo $\mathcal{E}$ l'insieme di tutte le e-mail, partizionato come

$$\mathcal{E} = \mathcal{S} \cup \mathcal{M}, \qquad \mathcal{S} \cap \mathcal{M} = \emptyset,$$

e dove $\mathcal{S}$ sono le e-mail di spam, e $\mathcal{M}$ quelle "regolari".

- Idea: l'occorrenza di varie parole è diversa in $\mathcal{S}$ ed in $\mathcal{M}$;
- Dato un sample di emails in $\mathcal{M}$ ed $\mathcal{S}$, possiamo studiare le probabilità che una nuova email e stia in $\mathcal{S}$:

$$\mathbb{P}(e \in \mathcal{S} \mid e \in W) = \frac{\mathbb{P}(e \in W \mid e \in \mathcal{S}) \cdot \mathbb{P}(e \in \mathcal{S})}{\mathbb{P}(e \in W)}$$

dove W è un'insieme di e-mail contenente certe parole (e la parte a destra è fatta di cose note o "facilmente stimabili").

Ma da dove viene il termine SPAM?

Ma da dove viene il termine SPAM?

https://www.youtube.com/watch?v=Gxtsa-OvQLA

Client di posta & Mailing lists

Ci sono svariati **client di posta**:

- Webmail (GMail, Roundcube (email di ateneo), ...)
- Client desktop (Outlook, Apple Mail, Thunderbird, ...)
- Client per smartphone

Mailing lists

- Spesso, si vuole comunicare con un insieme di persone (o discutere di qualcosa).
- Per questo, sono state inventate le mailing-list.
- Quando si spedisce ad una mailing list, tutti ricevono il messaggio; rispondendo alla mailing list si continua la discussione.
- Voi siete già iscritti a varie mailing list: Studenti, Galois, ...

Conclusioni e riassunto

- Abbiamo un'**idea di massima** del funzionamento di una rete locale e di internet,
- Possiamo collegarci alle macchine da remoto su cui svolgere il resto del corso!

Conclusioni e riassunto

- Abbiamo un'**idea di massima** del funzionamento di una rete locale e di internet,
- Possiamo collegarci alle macchine da remoto su cui svolgere il resto del corso!

Se **abbiamo ancora tempo** in laboratorio, altrimenti come primo esercizio per testare le connessioni alle macchine remote, possiamo indagare ulteriormente il funzionamento della mail...

Il protocollo SMTP

Assumiamo di voler scrivere a `fabio.durastante@unipi.it`.

```
f.durastante@mathsgalore:~$ host -t MX unipi.it
unipi.it mail is handled by 50 emailsecurity.unipi.it.
```

Ora abbiamo determinato chi gestisce la posta per `@unipi.it`. Colleghiamoci con `telnet`.

Il protocollo SMTP (continua)

```
f.durastante@mathsgalore:~$ telnet emailsecurity.unipi.it 25
Trying 131.114.142.148...
Connected to emailsecurity.unipi.it.
Escape character is '^]'.
220 esra3.unipi.it ESMTP SonicWall (10.0.10.6287)
```

Il protocollo SMTP (continua)

```
f.durastante@mathsgalore:~$ telnet emailsecurity.unipi.it 25
Trying 131.114.142.148...
Connected to emailsecurity.unipi.it.
Escape character is '^]'.
220 esra3.unipi.it ESMTP SonicWall (10.0.10.6287)

helo mathsgalore
250 esra2.unipi.it
```

Il protocollo SMTP (continua)

```
f.durastante@mathsgalore:~$ telnet emailsecurity.unipi.it 25
Trying 131.114.142.148...
Connected to emailsecurity.unipi.it.
Escape character is '^]'.
220 esra3.unipi.it ESMTP SonicWall (10.0.10.6287)

helo mathsgalore
250 esra2.unipi.it

mail from: <f.durastante@mathsgalore.unipi.it>
250 2.1.0 MAIL ok
```

Il protocollo SMTP (continua)

```
f.durastante@mathsgalore:~$ telnet emailsecurity.unipi.it 25
Trying 131.114.142.148...
Connected to emailsecurity.unipi.it.
Escape character is '^]'.
220 esra3.unipi.it ESMTP SonicWall (10.0.10.6287)

helo mathsgalore
250 esra2.unipi.it

mail from: <f.durastante@mathsgalore.unipi.it>
250 2.1.0 MAIL ok

rcpt to: <fabio.durastante@unipi.it>
250 2.1.5 <fabio.durastante@unipi.it> ok
```

Il protocollo SMTP (continua)

```
data
354 3.0.0 End Data with <CR><LF>.<CR><LF>
Date: 21 September 2021
Subject: Email di prova
From: f.durastante@mathsgalore.unipi.it
To: f.durastante@unipi.it
Questo e' un messaggio di prova
-- Fabio via Telnet
.
250 2.6.0 message received
```

Il protocollo SMTP (continua)

```
data
354 3.0.0 End Data with <CR><LF>.<CR><LF>
Date: 21 September 2021
Subject: Email di prova
From: f.durastante@mathsgalore.unipi.it
To: f.durastante@unipi.it
Questo e' un messaggio di prova
-- Fabio via Telnet
.
250 2.6.0 message received

quit
221 2.0.0 esra2.unipi.it says goodbye; [...]
Connection closed by foreign host.
```

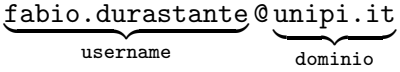
Il protocollo SMTP (continua)

```
data
354 3.0.0 End Data with <CR><LF>.<CR><LF>
Date: 21 September 2021
Subject: Email di prova
From: f.durastante@mathsgalore.unipi.it
To: f.durastante@unipi.it
Questo e' un messaggio di prova
-- Fabio via Telnet
.
250 2.6.0 message received

quit
221 2.0.0 esra2.unipi.it says goodbye; [...]
Connection closed by foreign host.
```

- Per una serie di ragioni, questo messaggio sarà *probabilmente* finito nello SPAM.
- Il protollo SMTP è leggermente più complesso al giorno d'oggi: firme crittografiche permettono di controllare (in parte) che la catena di trasmissione sia corretta – noi abbiamo ignorato tutto questo.

Struttura di un indirizzo email



username è la parte dell'indirizzo che (solitamente) descrive l'utente locale.

dominio invece determina dove dev'essere recapitata l'email (ancora, utilizzando `host -t MX unipi.it`).

Struttura di un indirizzo email

$$\underbrace{\texttt{fabio.durastante}}_{\text{username}}\texttt{@}\underbrace{\texttt{unipi.it}}_{\text{dominio}}$$

username è la parte dell'indirizzo che (solitamente) descrive l'utente locale.

dominio invece determina dove dev'essere recapitata l'email (ancora, utilizzando `host -t MX unipi.it`).

Esistono molte varianti di questa sintassi, in particolare per lo username – sono perlopiù in disuso. Una che può tornare utile è:

`fabio.durastante+keyword@unipi.it`

- Alcuni caratteri non sono ammessi.
- Ultimamente, è stato esteso il set di caratteri utilizzabile anche per i domini (UTF8).

Struttura di un messaggio

Un'email è sostanzialmente un file di testo, con questa struttura:

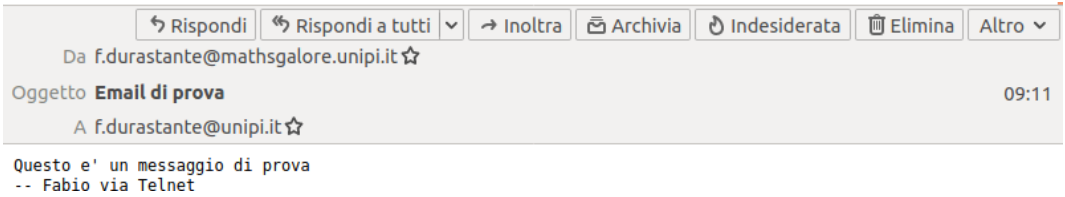
```
Subject: Messaggio
From: Signor Mittente <signor.mittente@beldominio.it>
To: Dottoressa Ricevente <dottoressa.ricevente@importanteluogo.it>

Contenuto del messaggio qui
```

- La prima parte si chiama header, e contiene linee del tipo `Chiave: valore`.
- La seconda è il corpo del messaggio (body).
- Sono separate da una linea vuota.

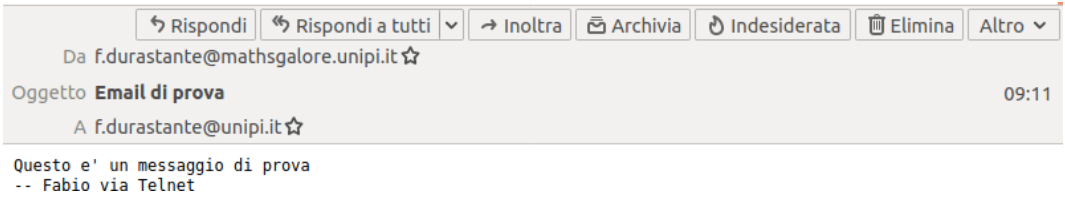
Dissezione di un header

Consideriamo questa e-mail che mi sono auto-mandato:



Dissezione di un header

Consideriamo questa e-mail che mi sono auto-mandato:



Dal programma di posta è possibile aprire il sorgente della e-mail, ed ispezionarne il contenuto.

Dissezione di un header

```
Received: from EX16-05.ad.unipi.it (131.114.73.245) by EX16-01.ad.unipi.it
(131.114.73.241) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2308.14 via Mailbox
Transport; Tue, 21 Sep 2021 09:23:45 +0200
Received: from EX16-02.ad.unipi.it (131.114.73.242) by EX16-05.ad.unipi.it
(131.114.73.245) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2308.14; Tue, 21 Sep
2021 09:23:45 +0200
Received: from mx3.unipi.it (131.114.72.205) by EX16-02.ad.unipi.it
(131.114.73.242) with Microsoft SMTP Server id 15.1.2308.14 via Frontend
Transport; Tue, 21 Sep 2021 09:23:45 +0200
Received: from localhost (localhost [127.0.0.1])
by mx3.unipi.it (Postfix) with ESMTP id 0FE184140F
for <fabio.durastante@unipi.it>; Tue, 21 Sep 2021 09:23:45 +0200 (CEST)
Received: from esra1.unipi.it (esra1.unipi.it [131.114.142.95])
by mx3.unipi.it (Postfix) with ESMTP id F224F413EC
for <fabio.durastante@unipi.it>; Tue, 21 Sep 2021 09:23:44 +0200 (CEST)
Received: from esra1.unipi.it (127.0.0.1) id h964800171s9 for <fabio.durastante@unipi.it>;
Tue, 21 Sep 2021 09:23:44 +0200 (envelope-from <f.durastante@mathsgalore.unipi.it>)
Authentication-Results: esra1.unipi.it;
spf=temperror smtp.mailfrom=f.durastante@mathsgalore.unipi.it;
Received: from mathsgalore ([131.114.50.237])
by esra1.unipi.it ([192.168.50.95]) (SonicWall 10.0.10.6287)
with SMTP id i20210921072118015431O-1; Tue, 21 Sep 2021 09:22:45 +0200
```

Dissezione di un header (parte 2)

```
Date: Tue, 21 Sep 2021 00:00:00 +0000
Subject: Email di Prova
From: <f.durastante@mathsgalore.unipi.it>
To: <f.durastante@unipi.it>
[...]
Message-ID: <20210921072345.0FE184140F@mx3.unipi.it>
Return-Path: f.durastante@mathsgalore.unipi.it
[...]
Content-Type: text/plain
MIME-Version: 1.0
```

Dissezione di un header (parte 2)

```
Date: Tue, 21 Sep 2021 00:00:00 +0000
Subject: Email di Prova
From: <f.durastante@mathsgalore.unipi.it>
To: <f.durastante@unipi.it>
[...]
Message-ID: <20210921072345.0FE184140F@mx3.unipi.it>
Return-Path: f.durastante@mathsgalore.unipi.it
[...]
Content-Type: text/plain
MIME-Version: 1.0


Questo e' un messaggio di prova
-- Fabio via Telnet
```

MIME

- In realtà, raramente i messaggi hanno un corpo così semplice e leggibile;
- Molti software utilizzando un formato più complesso per avere un documento con più parti nel testo (ad esempio, testo formattato, poi uno o più allegati, ...).
- A volte il contenuto viene codificato in modo particolare (base64) – rendendolo di fatto illeggibile ad un essere umano.