ITS Academy
Adriano
Olivetti

SSH

SSH – Secure Shell (1995)

- E' un protocollo per accedere in modo sicuro a macchine remote
- SSH cifra l'intero traffico, partendo dallo scambio della password, superando i problemi dei protocolli precedenti, quali telnet e rlogin
- Il traffico viene cifrato sulla macchina mittente e decifrato su quella destinataria, rendendo inefficaci gli attacchi di tipo Man In The Middle
- E' un protocollo client-server. Prevede la presenza di un server SSH disponibile ad accettare connessioni e uno o più client che si collegano utilizzando un client SSH
- E' un protocollo con autenticazione reciproca, nel quale il server autentica il client e il client autentica il server

SSH Authentication

L'autenticazione in SSH può avvenire in due modi:

- Tramite username e password
- Tramite scambio di chiavi asimmetriche

Nel primo caso l'autenticazione avviene contestualmente alla connessione, specificando le credenziali.

Il comando per collegarsi è **`ssh nomeutente@ipaddress`** a cui seguirà la richiesta di password.

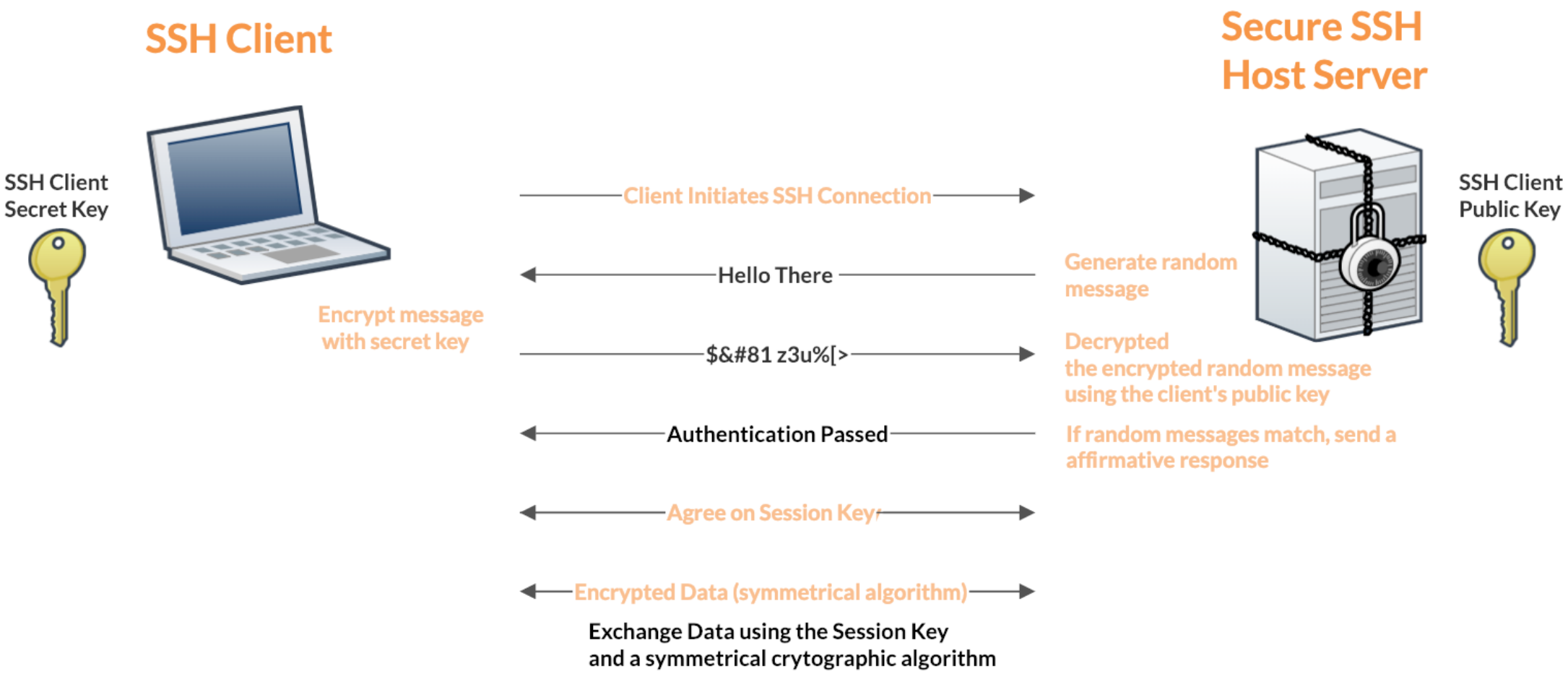
SSH Authentication with Asymmetric Keys

- Il client genera una coppia di chiavi asimmetriche con il comando **`ssh-keygen`** eventualmente specificando l'algoritmo crittografico con il parametro –t (p.e. **`ssh-keygen -t rsa`**)
  - Il comando chiede dove salvare le chiavi e richiede anche una password di protezione della chiave privata (opzionale ma consigliato)
  - Vengono generati due file, uno per la chiave pubblica e uno per la chiave privata
- La chiave pubblica deve essere trasferita sul server
  - Tramite il comando ssh-copy-id o tramite altri metodi di accesso al server. In entrambi i casi le chiavi devono essere associate all'utente che effettuerà il login

SSH Authentication with Asymmetric Keys

- Una volta terminato lo scambio delle chiavi (che va effettuato una volta sola) è possibile collegarsi al server remoto
- Il comando per il collegamento continua ad essere **`ssh nomeutente@ipaddress`** ma non verrà più chiesta la password dell'utente. Verrà invece chiesta l'eventuale password a protezione della chiave privata
- L'autenticazione avviene tramite l'handshake mostrato nella slide successiva

SSH Authentication with Asymmetric Keys

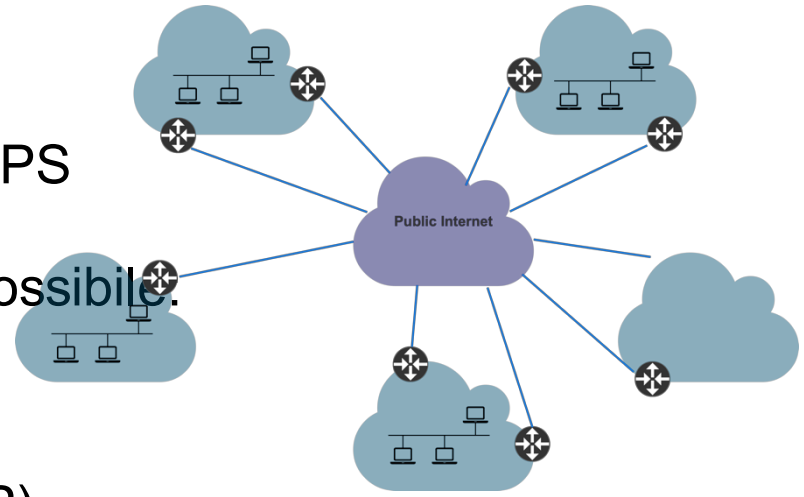


ITS Academy
Adriano
Olivetti

IPSec

Roadwarrior problem

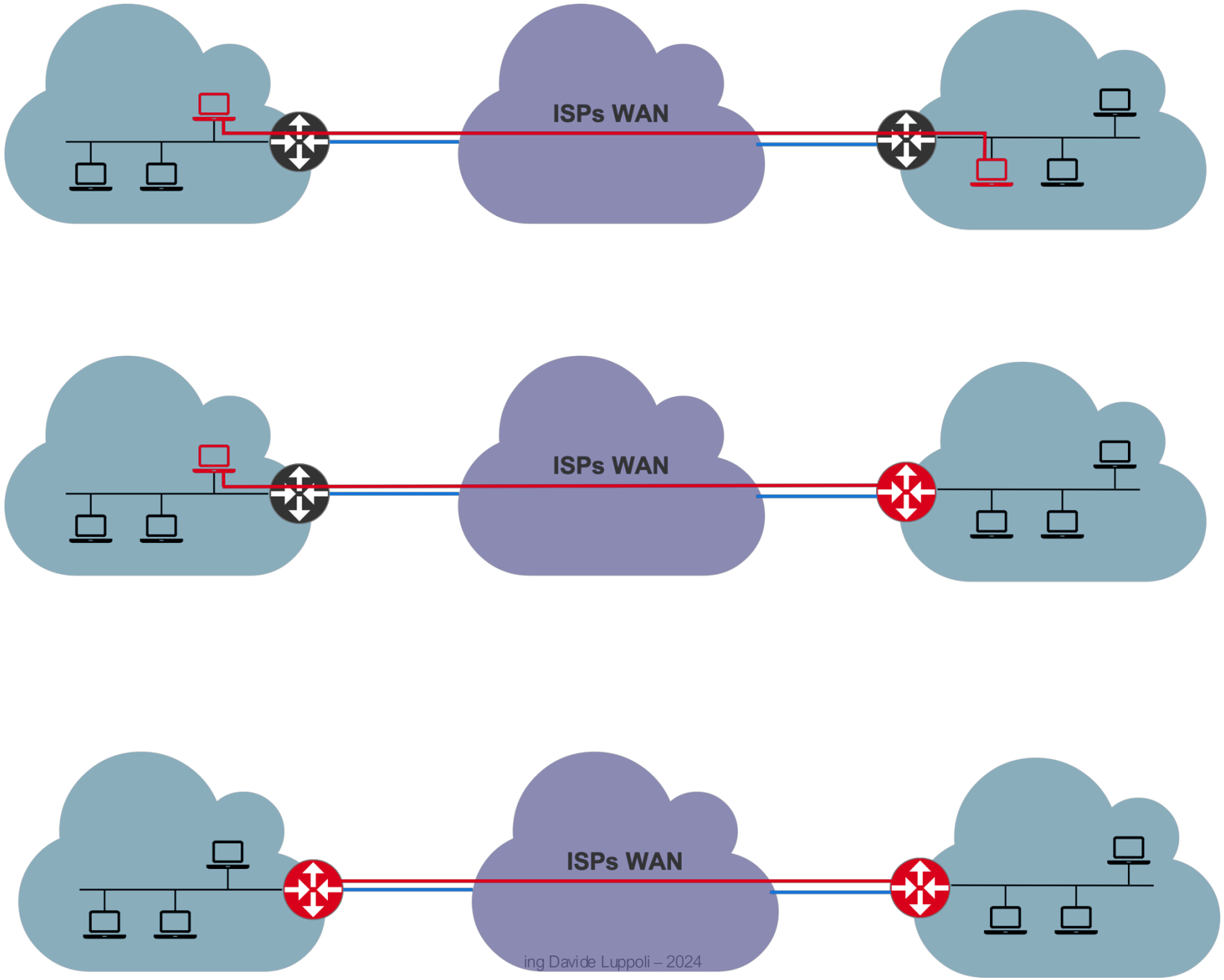
- La comunicazione tra due reti distinte, passando per internet pubblica, comporta problemi di riservatezza dei dati trasmessi. → Chiunque intercetta i dati riesce a leggerli e/o modificarli.
- L'unica soluzione consiste nel cifrare la comunicazione.
- E' possibile lavorare a livello applicativo, per esempio con HTTPS
- Ci sono casi però in cui la cifratura a livello applicativo non è possibile.
  - Per applicazioni "vecchie" che non si possono modificare
  - Quando è necessario usare protocolli non cifrati (p.e. ICMP)
  - Quando è necessario creare delle reti locali tra host



IPSec

- IpSec è un set di protocolli che introduce la crittografia a livello di rete (a livello di IP)
- Usando IP sec le comunicazioni saranno cifrate indipendentemente dai protocolli utilizzati a livello di trasporto e a livello applicativo
- IPSec è un protocollo connection-oriented, sebbene lavori a livello di rete.
- Il canale di comunicazione sicuro è cioè realizzato tra due end-point che, in base al caso possono essere: Due host, un host e un gateway, due gateway
- IPSec gestisce anche l'autenticazione dei datagrammi, ovvero la possibilità di verificare l'integrità dei dati
- E' possibile utilizzare tutti i protocolli di cifratura moderni

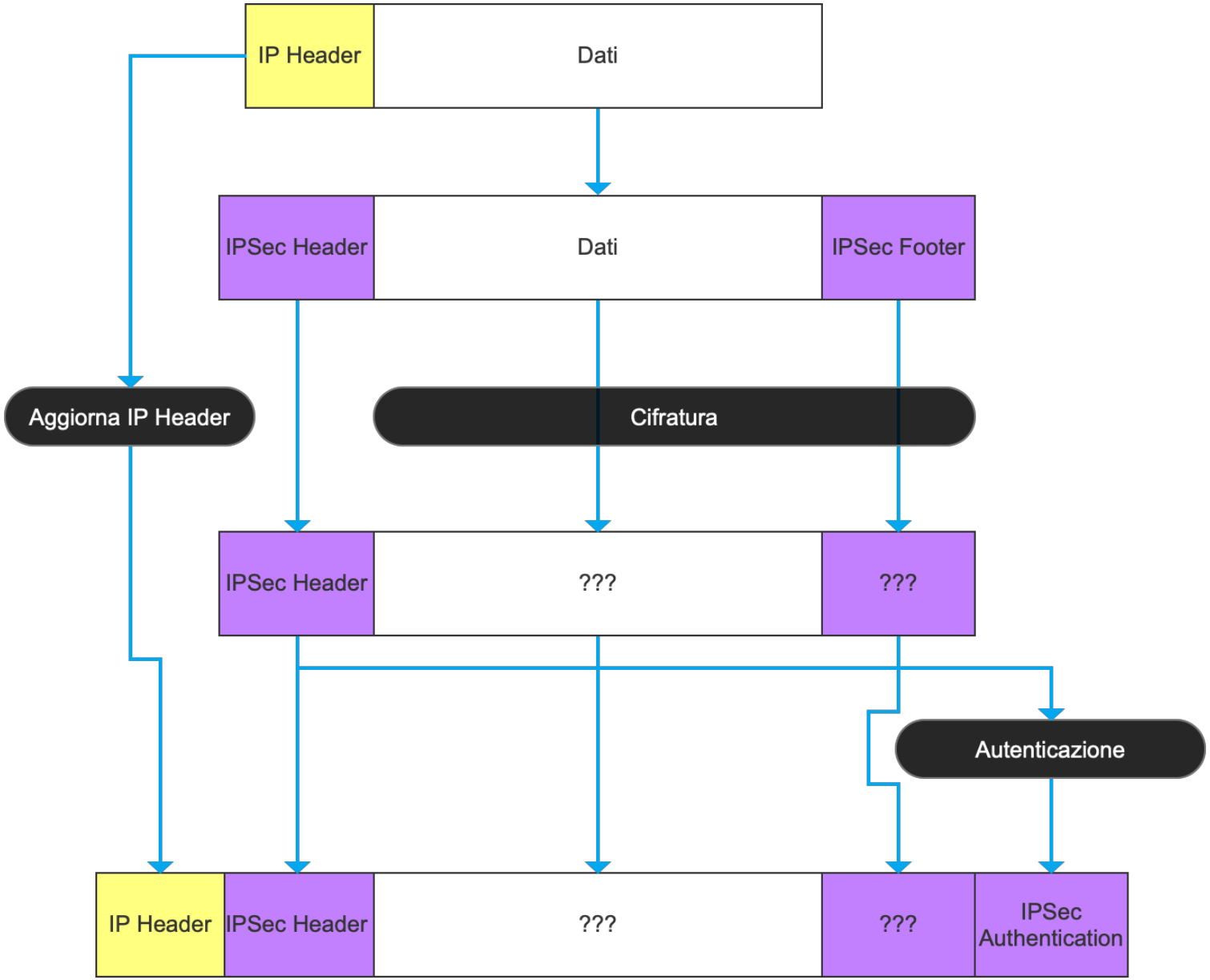
IPSec



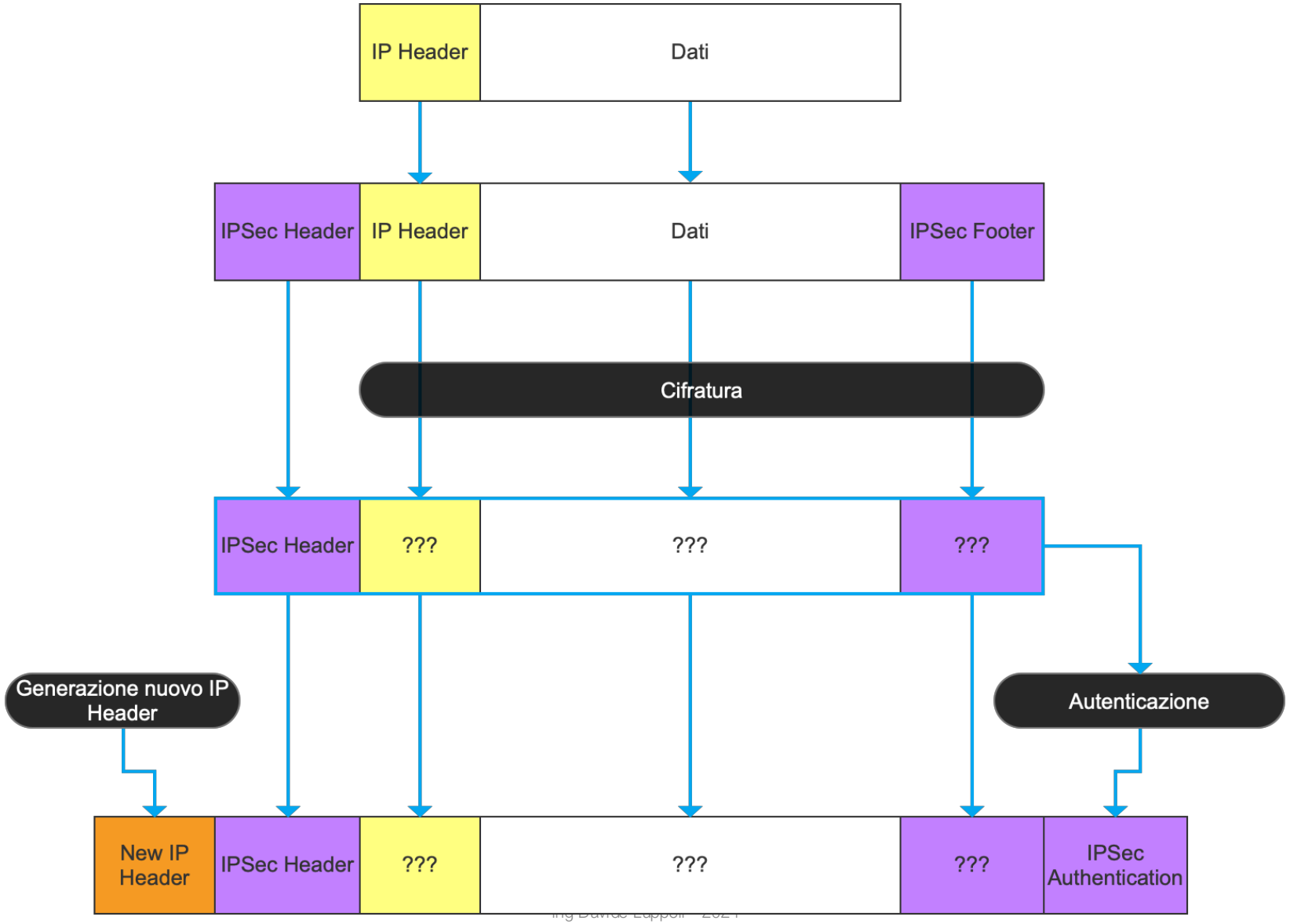
IPSec

- IPSec Aggiunge degli header al datagramma IP per gestire:
  - La connessione tra i due endpoint (detta Security Association – SA)
  - Gli errori
  - Lo scambio delle chiavi di cifratura
- IPSec può lavorare in due modi:
  - **Transport Mode:** Gli header IPSec vengono aggiunti al normale header IP, che viene solamente aggiornato per segnalare la presenza degli header aggiuntivi.
  - **Tunnel Mode:** L'intero datagramma viene cifrato ed inserito in un nuovo datagramma IP. E' la modalità spesso utilizzata quando la connessione IPSec termina presso un gateway.

IPSec – Transport Mode



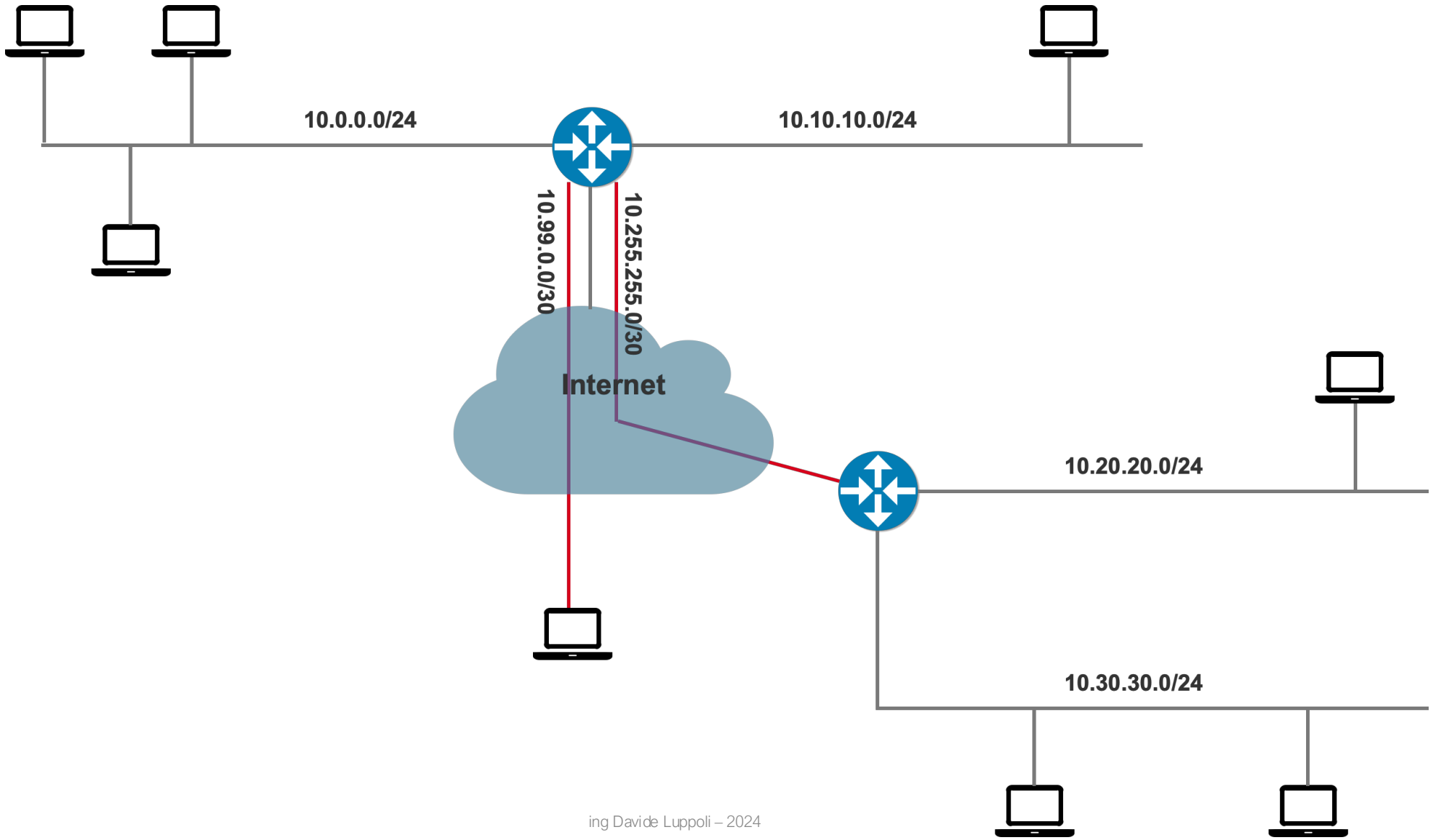
IPSec – Tunnel Mode



VPN

- Tramite IPSec è possibile realizzare VPN (Virtual Private Network), ovvero reti private costruite su infrastrutture pubbliche quali Internet.
- Il termine virtuale è legato al fatto che la rete risulta privata solamente perché il traffico è cifrato
- L'architettura più diffusa è quella di implementare i server VPN sui gateway, lasciando che i client si colleghino ad essi.
    - I client possono essere sia host che altri gateway
- La connessione VPN genera negli host una nuova scheda di rete (virtuale) e relative regole di routing per instradare adeguatamente il traffico

VPN


10.0.0.0/24
10.10.10.0/24
10.99.0.0/30
10.255.255.0/30
Internet
10.20.20.0/24
10.30.30.0/24