PARMA 24-25 febbraio 2004

Progetto TRIP

2ª parte: 802.1x

Lo standard IEEE 802.1x

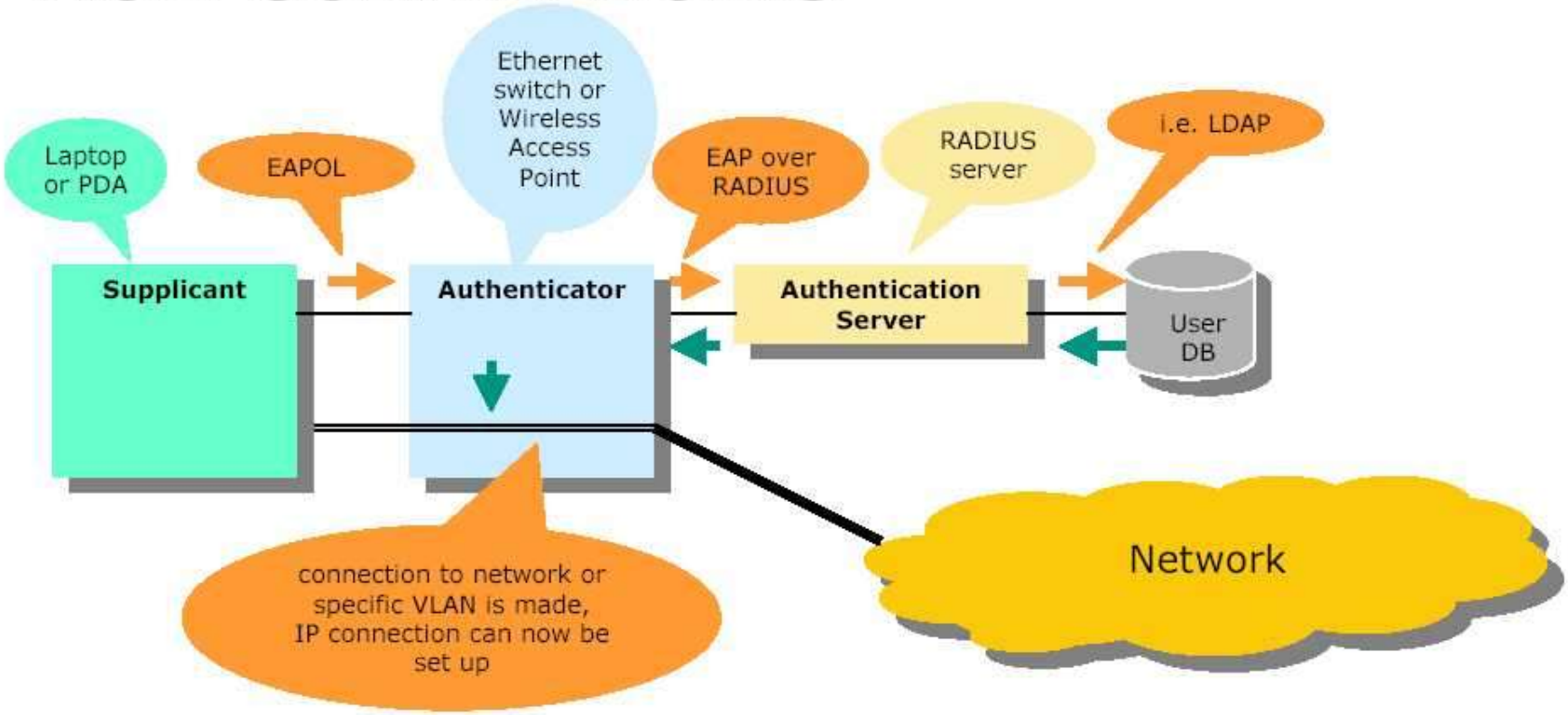
– è stato inizialmente sviluppato per autenticare
– in reti wireless si richiede mutua autenticazione
– in reti wireless serve strong encryption

Tipi di EAP

EAP = Extensible Authentication Protocol

- EAP/MD5 file user/pwd
- EAP/TLS usa certificati client e server
- EAP/TTLS solo cert. server, tunnel
- PEAP tunnel TLS in cui viaggia EAP
- Cisco EAP mutua autenticazione, user/pwd e algoritmo Cisco LEAP

How 802.1X works

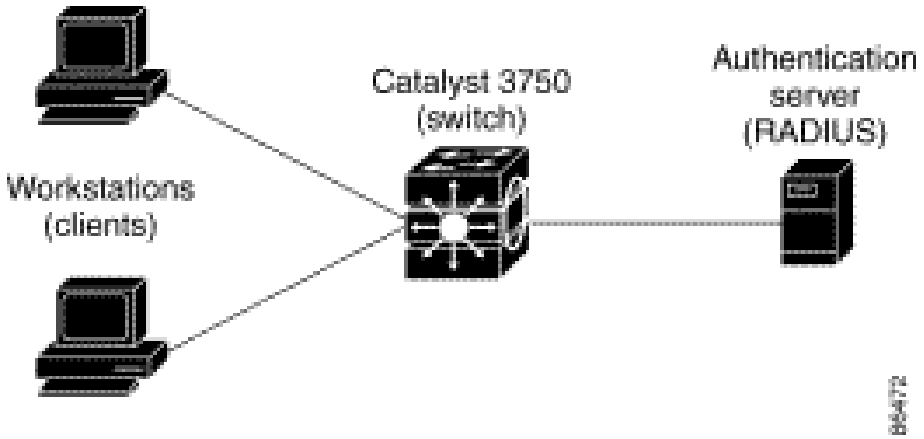


@Surfnet

I test effettuati

- Wired (RV)
  - Server di autenticazione (FreeRADIUS)
  - Autenticatore (Switch Cisco 3750 Cathalyst)
  - Supplicante (Windows XP)
- Wireless (OP)
  - Server di autenticazione (FreeRADIUS)
  - Autenticatore (AP Cisco 350 11.23T)
  - Supplicante (Windows XP SP1)
- Supplicante Linux (*in corso*) (FG)

Test su rete wired



- EAP/MD5 (usando un file locale sul server RADIUS)
- EAP/TLS (certificati e file locale sul server RADIUS)
- EAP/TLS (certificati)

Configurazione Cisco 3750 come authenticator(1/2)

1. Abilitare l'opzione Authentication, Authorization, and Accounting (AAA)

```
aaa new-model
```

4. Definire lo scope dell' autenticazione (opzionale - ad es. utilizza AAA solo per 802.1x)

```
aaa authentication login default none
```

7. Crea una lista di metodi di autenticazione 802.1x, in questo caso radius

```
aaa authentication dot1x default group radius
```

10. Impostare l'autorizzazione per l'assegnazione dinamica delle vlan (opzionale)

```
aaa authorization network default group radius
```

13. Configurare l'interfaccia di rete per il supporto 802.1x

```
interface GigabitEthernet1/0/3
   switchport mode access
   no ip address
   no mdix auto
   dot1x port-control auto
   spanning-tree portfast
```

Configurazione Cisco 3750 come authenticator (2/2)

1. Configurare l'interfaccia di rete di L3 sulla quale si trova il radius server (in questo caso la Vlan di default)

```
interface Vlan1
   ip address 192.84.x.y 255.255.255.0
   no ip route-cache
   no ip mroute-cache
```

6. Configurare i parametri per il radius server

```
radius-server host 192.84.145.22 auth-port 1812 \
    acct-port 1813 timeout 3
radius-server retransmit 3
radius-server key mysecretkey
```

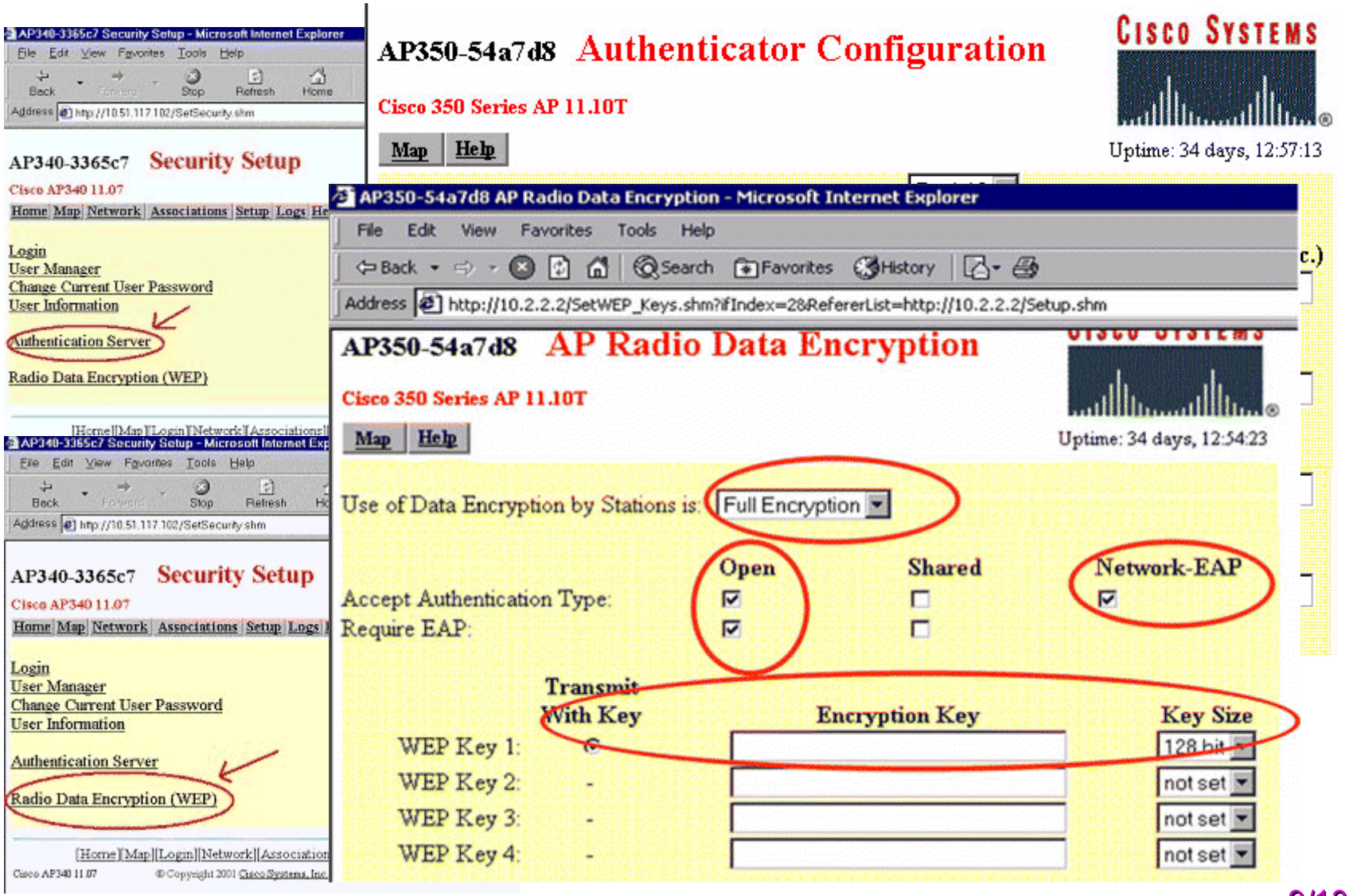
10. Abilita 802.1x

```
dot1x system-auth-control
```

Test su rete wireless

- ~~EAP/MD5~~ (non più disponibile con XP SP1)
- EAP/TLS (certificati e file users)
- EAP/TLS (solo certificati)

Configurazione Cisco AP 350



Configurazione FreeRADIUS

clients.conf

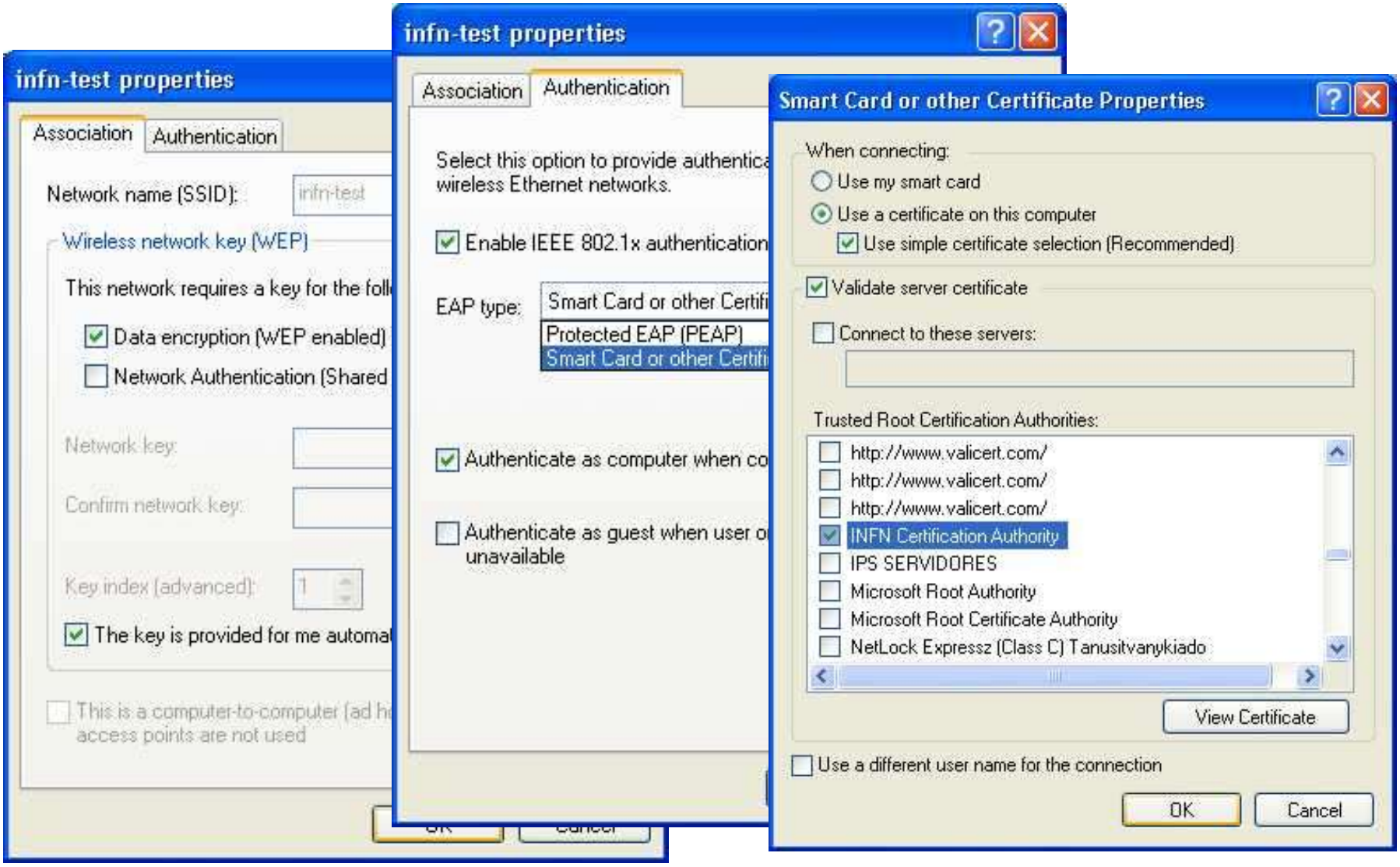
```
client 192.168.253.13 {
        secret          = 1234567890
        shortname       = msm0wl
}
```

users

```
"Ombretta Pinazza" Auth-Type := EAP
"test" Auth-Type := Local,User-Password=="test"
```

```
}
```

Supplicante Windows XP 802.1x



I prossimi test

- test con diversi AP e schede wireless
- test con supplicanti linux
- test con meccanismi multipli di AAA
- test con EAP/TTLS e PEAP
- test con altri server RADIUS

Il fisico viaggiatore

- ha un certificato X.509
  - RADIUS autorizza tutti i supplicanti con certificato
  - RADIUS autorizza i supplicanti con certificato che sono elencati in una lista
- non ha un certificato o deve usare altri meccanismi
  - (controllo dei MAC address)
  - username/password su AP o server RADIUS
  - RADIUS dialoga con altri server (proxy RADIUS)