Accesso autonomo alla rete cablata

L'accesso autonomo alla rete cablata avviene tramite cavo di rete ethernet del proprio PC solo nelle aree abilitate (vedi http://wireless.units.it/plugnav/) e in gran parte delle aule ad uso del docente (dettaglio su https://r.units.it/cattedre1x). Nelle aree non servite è necessario compilare la richiesta cartacea di registrazione del nodo di rete (indirizzo IP) per accedere alla rete con la vecchia procedura.

Chi si collega alla rete universitaria accetta le norme di utilizzo della stessa.

 È utile portare con sé un cavo di rete di lunghezza adeguata.

Premesse e prerequisiti

Personal computer con una porta ethernet via cavo e con uno dei seguenti sistemi operativi aggiornati:

- Windows 11
- Windows 10 (solo versioni ancora supportate da Microsoft)
- MacOS
- Linux

- ~~Windows 8.1~~ (NON PIÙ SUPPORTATO)
- ~~Windows 8.0~~ (NON PIÙ SUPPORTATO)
- ~~Windows 7~~ (NON PIÙ SUPPORTATO)
- ~~Windows Vista~~ (note) (NON PIÙ SUPPORTATO)
- Windows XP ~~Professional o Home Edition, entrambi con Service Pack 3~~ (note per PC in dominio DS) ~~|~~ (note) (NON PIÙ SUPPORTATO)
- ~~Windows 2000 SP3 e~~ patch 802.1x ~~installata~~ (NON PIÙ SUPPORTATO)

PC personali o di Ateneo ad uso personale

1. Se si ha già la rete eduroam configurata a mano, rimuovere o far dimenticare la rete eduroam.
2. Scaricare ed eseguire il configuratore eduroam dal sito dell'ente eduroam che ha rilasciato le credenziali in vostro possesso (link a quello dell'Università di Trieste)
3. Quando richiesto durante il processo di configurazione, accettare l'installazione per la connessione via cavo.
4. Quando ci si collegherà la prima volta via cavo su una presa di rete abilitata, il sistema operativo potrebbe richiedere l'immissione delle credenziali. Tali credenziali, al primo login con successo, verranno memorizzate dal sistema per le prossime connessioni dello stesso utente locale.

 Disabilitare o spegnere la connessione Wi-Fi prima di collegarsi con il cavo. La maggior parte dei sistemi presenta comportamenti anomali se connesso sia alla rete cablata che a quella Wi-Fi, compresa l'impossibilità di navigare.

Attenzione: su Windows spesso la finestra di immissione delle credenziali compare sotto le finestre già aperte.

Se si modifica la propria password è necessario rimuovere e reinstallare eduroam per aggiornare la password sul dispositivo.

PC in dominio ad uso personale o promiscuo (istruzioni per tecnici informatici)

Connessione alla Rete con Windows 10

È necessario avere connettività di rete sulla schermata di login in modo che il dispositivo contatti il controller di dominio per validare le credenziali degli utenti di dominio.

Fix Me! 20201007: Dalla schermata di login, è possibile accedere ad una rete wireless WPA enterprise come eduroam, tuttavia le credenziali usate restano memorizzate anche dopo il reboot e il certificato server potrebbe non venire validato.

È quindi preferibile che il dispositivo si connetta alla rete cablata con l'utenza di dominio assegnata alla macchina. Questa configurazione non è compatibile con quella impostata dall'installer eduroamCAT. Si dovrà quindi provvedere a disinstallare eduroamCAT e configurare opportunamente delle group policies per effettuare la connessione correttamente. Vedi più sotto.

Connessione alla Rete con Windows 7 con Extended Security Updates

Fix Me! necessaria verifica del funzionamento

Istruzioni per macchine in dominio DS e PC personali fuori dominio

- Premere il tasto Windows + R per far apparire la finestra *Esegui*.
- Nella finestra *Esegui* digitare **services.msc** e cliccare ok.
- Trovare "*Configurazione Automatica Reti Cablate*" e cliccare con il tasto destro sul servizio e poi su "*Proprietà*".
- Nel menù a tendina "*Tipo di avvio*" selezionare "*Automatico*".
- Riavviare il computer.

- Nel menù "*Start*" cliccare su "*Pannello di Controllo*", poi selezionare "*Centro connessioni di rete e condivisione*".
- Cliccare su "*Modifica impostazioni scheda*" sul lato sinistro.
- Cliccare con il tasto destro su "*Connessione alla Rete Locale (LAN)*", poi cliccare "*Proprietà*".
- Sulla scheda Autenticazione selezionare "*Abilita autenticazione IEEE 802.1x*" e nel menù a tendina selezionare "*PEAP (Protected EAP)*".

- Cliccare su "*Impostazioni*".
- Alla voce "*Connetti ai server seguenti*" digitare **raggio.units.it**.
- Alla voce "*Autorità di certificazione radice attendibili*" selezionare "*DigiCert Assured ID Root CA*" e "*USERTrust RSA Certification Authority*".

- Alla voce "*Selezionare metodo di Autenticazione*" assicurarsi di aver selezionati "*EAP-MSCHAP v2*".
- Cliccare su "*Configura*".
- Assicurarsi che il checkbox "*Utilizza automaticamente il nome utente, la password e se disponibile il dominio di accesso a Windows*" sia DESELEZIONATO.
- Click su "*Ok*".
- Click su "*Ok*" sulla finestra proprietà PEAP.
- Deselezionare "*Fallback ad accesso di rete non autorizzato*" se il PC è registrato nel dominio DS.
- Cliccare su "*Impostazioni Aggiuntive*".
- Assicurarsi che "*Specificare la modalità di autenticazione*" sia impostato su "*Autenticazione Computer*" se il PC è registrato nel dominio DS e su "*Autenticazione Utente*" se si sta usando un PC non in dominio DS.

Applicare il seguente script che modificherà le seguenti voci nel registry:

```
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\dot3svc\BlockTime valore 2 tipo
DWORD
```

Questo permetterà di ritentare l'autenticazione dopo 2 minuti anziché 20. Riavviare il PC per rendere effettive le modifche.

- Collegare il cavo ethernet e inserire le proprie credenziali nel formato corretto quando richiesto.

Estratto Group Policy per macchine in dominio DS

Per una opportuna resilienza in un ambiente enterprise è necessario modificare retry e timeout della connessione 802.1x. La seguente configurazione o analoghe sono utilizzate in produzione su molti PC.

```
<ExtensionData>
    <Extension xsi:type="q5:Dot3SvcSettings">
        <q5:Dot3SvcSetting>
            <LanPolicies>
                <name>dotXRadiologia</name>
                 <description>802.1X U.C.O. Radiologia</description>
                 <globalFlags>
                     <enableAutoConfig>true</enableAutoConfig>
                     <enableExplicitCreds>true</enableExplicitCreds>
                 </globalFlags>
                 <profileList>
                     <LANProfile>
                        <MSM>
                            <security>
                                <OneXEnforced>false</OneXEnforced>
                                <OneXEnabled>true</OneXEnabled>
                                <OneX>
```

```
                                    <heldPeriod>3</heldPeriod>
                                    <authPeriod>18</authPeriod>
                                    <startPeriod>5</startPeriod>
                                    <maxStart>5</maxStart>
                                    <maxAuthFailures>5</maxAuthFailures>
<supplicantMode>compliant</supplicantMode>
                                    <authMode>machine</authMode>
                                    <EAPConfig>
                                        <EapHostConfig>
                                            <EapMethod>
                                                <Type>25</Type>
                                                <VendorId>0</VendorId>
                                                <VendorType>0</VendorType>
                                                <AuthorId>0</AuthorId>
                                            </EapMethod>
                                            <Config>
                                                <Eap>
                                                    <Type>25</Type>
                                                    <EapType>
                                                        <ServerValidation>
<DisableUserPromptForServerValidation>false</DisableUserPromptForServerValid
ation>
<ServerNames>raggio.units.it</ServerNames>
<TrustedRootCA>aa bb cc dd ee ff 1a 1b 1c 1d 1e 1f 2a 2b 2c 2d 2e 2f
</TrustedRootCA>
<TrustedRootCA>33 bb cc dd ee ff 1a 1b 1c 1d 1e 1f 2a 2b 2c 2d 2e 2f
</TrustedRootCA>
                                                        </ServerValidation>
<FastReconnect>true</FastReconnect>
<InnerEapOptional>false</InnerEapOptional>
                                                        <Eap>
                                                            <Type>26</Type>
                                                            <EapType>
<UseWinLogonCredentials>false</UseWinLogonCredentials>
                                                            </EapType>
                                                        </Eap>
<EnableQuarantineChecks>false</EnableQuarantineChecks>
<RequireCryptoBinding>false</RequireCryptoBinding>
                                                        <PeapExtensions>
<PerformServerValidation>true</PerformServerValidation>
<AcceptServerName>true</AcceptServerName>
                                                        </PeapExtensions>
                                                    </EapType>
                                                </Eap>
                                            </Config>
                                        </EapHostConfig>
                                    </EAPConfig>
                                </OneX>
                            </security>
                        </MSM>
                    </LANProfile>
```

```
                </profileList>
            </LanPolicies>
        </q5:Dot3SvcSetting>
    </Extension>
    <Name>LanSvc Networks</Name>
</ExtensionData>
```

<TrustedRootCA>aa bb cc dd ee ff 1a 1b 1c 1d 1e 1f 2a 2b 2c 2d 2e 2f </TrustedRootCA> corrisponde al thumbprint/fingerpring SHA1 del certificato CA Root correntemente in uso o con la coppia di CA root vecchia e nuova per agevolare la transizione asincrona da una CA root all'altra.

Sostituire i seral number con quello delle CA correntemente in uso.

Per evitare problemi di sincronizzazione del trust store, si suggerisce di inserire anche le Sub CA in uso.

I certificati CA referenziati nella GPO devono essere presenti nel sistema.

Reference: OneX Schema Elements