EduRoam
Istruzioni per l'uso

Lorenzo Puccio – GARR

Giancarlo VIOLA - GARR

Consortium GARR

EduRoam – Istruzioni per l'uso

- Il servizio e la Federazione
  - Cos'e' Eduroam?
  - Come aderire alla Federazione
- Come FUNZIONA
- La ricetta per preparare EduRoam
  - Configurazione del Controller Wireless
  - Configurazione del server Radius
  - Verifica del servizio
  - Servizi da garantire agli utenti di EduRoam
- Cosa fare in caso di incedente

EduRoam – Istruzioni per l'uso

Cos'e' Eduroam?

- **Eduroam**

  (**Edu**cation **Roam**ing)

  è un servizio che offre connettivita' wireless sicura agli utenti che aderiscono alla federazione.

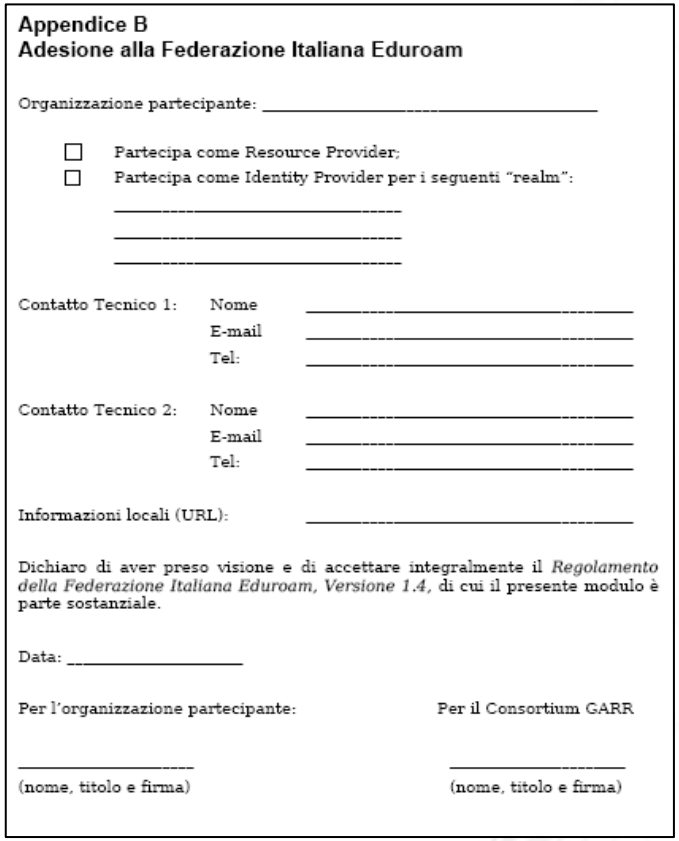
- **Numeri:**
  - **34 Istituti in Italia**
- **Dove e' attivo**
  - **Europa, Canada Australia Cina Giappone Nuova Zelanda USA e sta per essere attivato nella regione Asiatica**

EduRoam – Istruzioni per l'uso

Come aderire alla FEDERAZIONE ITALIANA

Adesione

- **Resurce Provider o Identity Provider?**
- **Far firmare al Rettore/Direttore il modulo di adesione.**
- **Inviare il modulo in duplice copia a mezzo raccomandata al Consorium GARR.**
- **Il modulo verra' quindi controfirmato e reinviato al richiedente.**
- **Ricevuto il modulo controfirmato si potra' procedere al setup del servizio**
  - Con il supporto del gruppo eduroam@garr.it



Appendice B
Adesione alla Federazione Italiana Eduroam

Organizzazione partecipante: _____

☐ Partecipa come Resource Provider;
☐ Partecipa come Identity Provider per i seguenti "realm":
_____
_____
_____

Contatto Tecnico 1: Nome _____
E-mail _____
Tel: _____

Contatto Tecnico 2: Nome _____
E-mail _____
Tel: _____

Informazioni locali (URL): _____

Dichiaro di aver preso visione e di accettare integralmente il *Regolamento della Federazione Italiana Eduroam, Versione 1.4*, di cui il presente modulo è parte sostanziale.

Data: _____

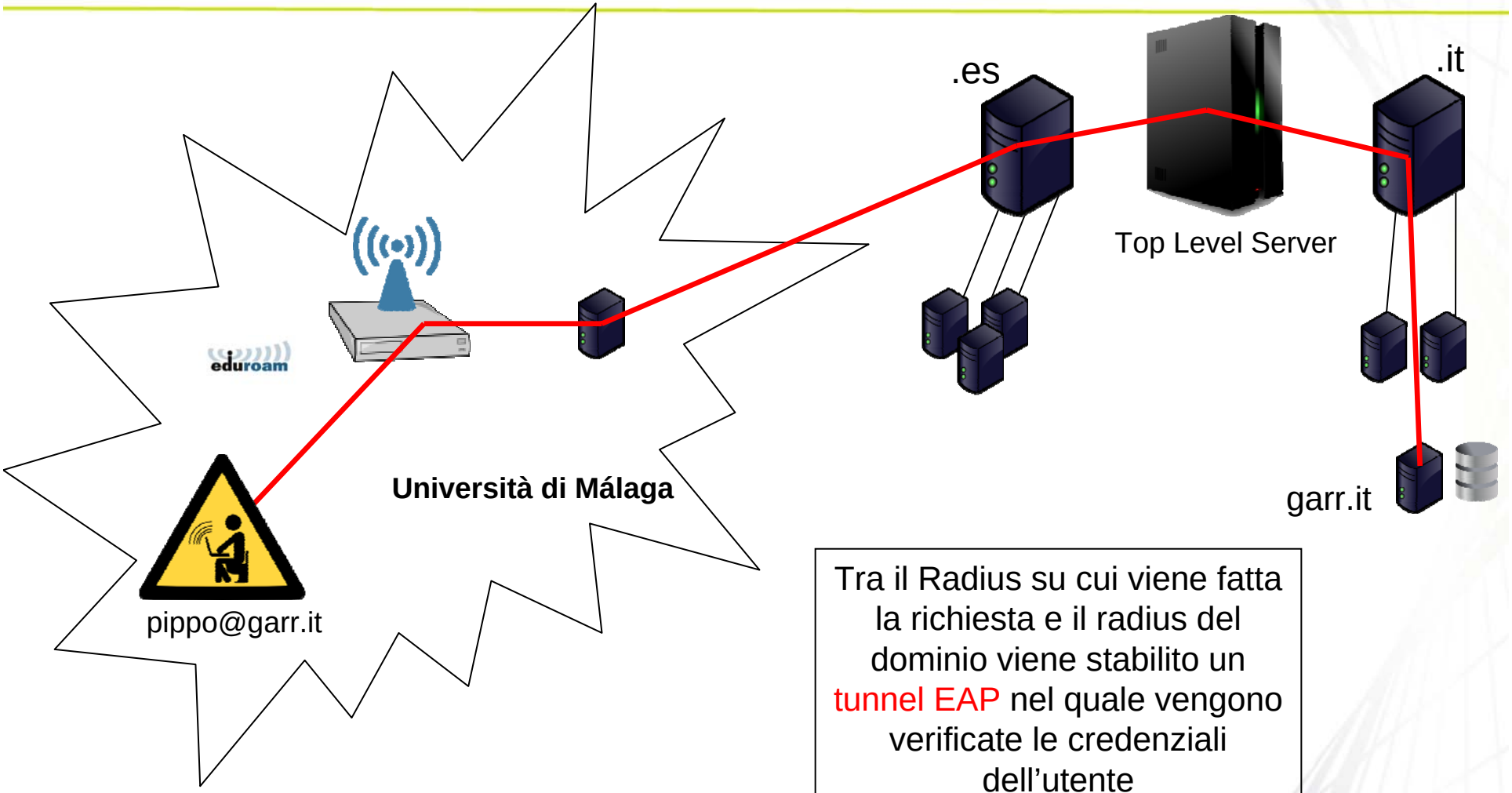
Per l'organizzazione partecipante: Per il Consortium GARR

_____ _____
(nome, titolo e firma) (nome, titolo e firma)

http://www.servizi.garr.it/index.php/it/eduroam/documenti/doc_download/18-regolamento-della-federazione-italiana-eduroam-

EduRoam – Istruzioni per l'uso

Come FUNZIONA



Tra il Radius su cui viene fatta la richiesta e il radius del dominio viene stabilito un tunnel EAP nel quale vengono verificate le credenziali dell'utente

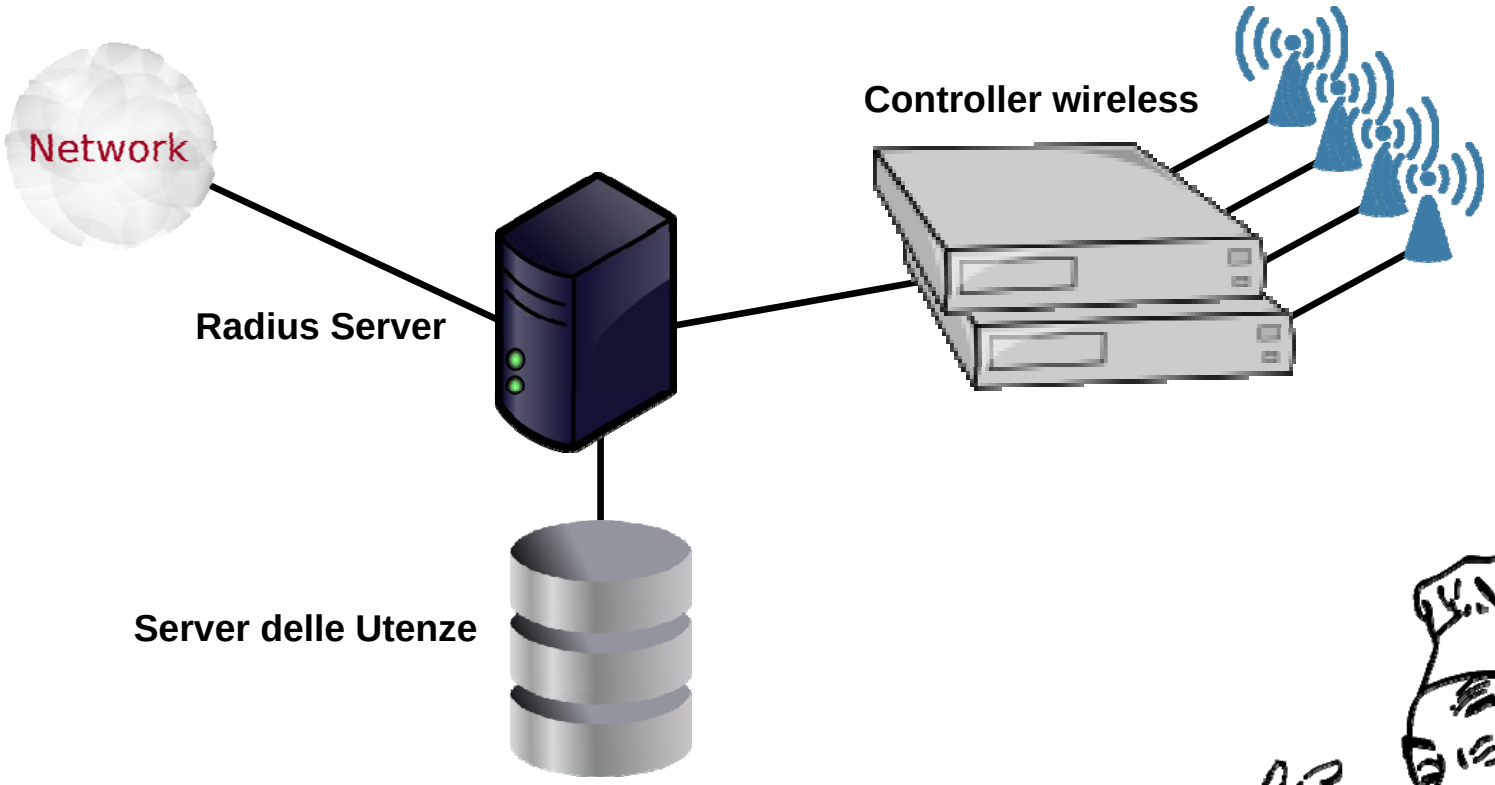
EduRoam – Istruzioni per l'uso

La ricetta per la preparare di EduRoam - INGREDIENTI

- Rete Wireless di Campus
  - Controller Wireless
- Sistema centralizzato delle utenze locali (LDAP–MySqL-…)
- Server Radius con certificato
  - Si puo' richiedere un certificato per il server a ca.garr.it
- Indirizzi IP pubblici

EduRoam – Istruzioni per l'uso

La ricetta per la preparare di EduRoam - INGREDIENTI



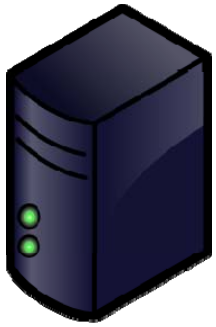
EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del Controller Wireless

- SSID: eduroam
- Network Authentication: WPA e WPA2 (Enterprise)
- Encryption: TKIP e AES
- Abilitare il protocollo 802.1X
- Indirizzo IP del server RADIUS per l'autenticazione
- Indirizzo del server RADIUS per l'accountig

EduRoam – Istruzioni per l'uso

Preparazione … Server Radius



FreeRadius

http://freeradius.org/

Radiator

http://www.open.com.au/radiator/

EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del server FreeRADIUS - Radiator
definizione dei Client

FreeRADIUS

/etc/radiusdir/clients.conf

```
client Controller_Wireless {
        ipaddr = 1.2.3.4
        netmask = 32
        secret                  = secret1234
        require_message_authenticator = no
        shortname  = Controller_Wireless
        virtual_server          = default
}
client radius.garr.net {
        ipaddr                  = 192.84.145.15
        netmask                 = 32
        secret                  = secretxserver
        require_message_authenticator     = no
        shortname  = radius.garr.net
        nastype                 = other
        virtual_server          = default
}
```

Radiator

etc/radiusdir/radius.conf

```
<Client 123.123.123.123>
        Secret   passwordradius
</Client>

<ClientListSQL>
        DBSource dbi:mysql:radius
        DBUsername <Username>
        DBAuth <Password>

</Client>
```

E' consigliato definire un client anche per i test locali.

EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del server RADIUS
configurazione del proxy server

FreeRADIUS

/etc/radiusdir/proxy.conf

```
proxy server {
        default_fallback = yes
}
home_server radius.garr.net {
….
        type = auth+acct
        ipaddr = 192.84.145.15
        port = 1812
        secret = questae'lapasswordradius
….
}
realm DEFAULT {
        pool                    = EDUROAM-IT
        nostrip
        type                    = radius
}
```

Radiator

/etc/radiusdir/radius.conf

```
<Handler NAS-Port-Type=Wireless-IEEE-802-11>
        <AuthBy RADIUS>
                Host 192.84.145.15
                Secret passorwdradius
                AuthPort 1812
                AcctPort 1813
                Retries 3
        </AuthBy>


</Handler>
```

EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del server RADIUS
configurazione del proxy server

FreeRADIUS

/etc/radiusdir/attrs.pre-proxy

DEFAULT
User-Name =* ANY,
User-Password =* ANY,
CHAP-Password =* ANY,
CHAP-Challenge =* ANY,
MS-CHAP-Challenge =* ANY,
MS-CHAP-Response =* ANY,
EAP-Message =* ANY,
Message-Authenticator =* ANY,
State =* ANY,
NAS-IP-Address =* ANY,
NAS-Identifier =* ANY,
NAS-Port-Type =* ANY,
Proxy-State =* ANY

Radiator

Passa automaticamente al radius di gerarchia superiore tutte le informazioni provenienti dal Controller Wireless

EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del server FreeRADIUS
Autenticazione - Autorizzazione

FreeRADIUS

/etc/radiusdir/eap.conf

```
        eap {
....
                tls {
                        certdir = ${confdir}/certs
                        cadir = ${confdir}/certs
                        private_key_password = passwordcertificato
                        private_key_file = ${certdir}/certificato.key
                        certificate_file = ${certdir}/certificato.pem
...
                }
                ttls {
                        default_eap_type = mschapv2
                        copy_request_to_tunnel = yes
                        use_tunneled_reply = yes
                        virtual_server = "inner-tunnel"
                }
                peap {
                        ……..
                }
        }
```

EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del server Radiator
Autenticazione - Autorizzazione

Radiator

/etc/radiusdir/radius.conf

```
<Handler Realm=garr.it>
                .......
</AuthBy LDAP>
                .......
 EAPType TTLS,PEAP,TLS
      EAPTLS_CAFile %D/certificates/GARRCA/CAcert.pem
      EAPTLS_CertificateFile %D/certificates/GARRCA/radpub-serv.pem
      EAPTLS_CertificateType PEM
      EAPTLS_PrivateKeyFile %D/certificates/GARRCA/radcert.pem
      EAPTLS_PrivateKeyPassword passwordcartificato
      EAPTLS_MaxFragmentSize 1000
      AutoMPPEKeys
  </AuthBy>
</Handler>
```

FreeRADIUS

/etc/radiusdir/radius.conf

```
modules {
$INCLUDE eap.conf
        ldap {
                server = "ipserverldap"
                identity = "cn=admin,dc=….."
                password = PasswordserverLDAP
                basedn = "ou=people,dc=……."
                filter = "(uid=%{Stripped-User-Name:-%{User-
Name}})"
                base_filter = "(objectclass=radiusprofile)"
…….
                net_timeout = 1
                tls {
                        start_tls = no
                }
                dictionary_mapping = ${confdir}/ldap.attrmap
                password_attribute = userPassword
                edir_account_policy_check = no
                set_auth_type = no
        }
```

EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del server Radiator
Autenticazione - Autorizzazione

Radiator

/etc/radiusdir/radius.conf

```
<Handler Realm=garr.it>
 <AuthBy LDAP2>
            Host (Server Ldap)
             Port 636
             UseSSL
             SSLCAPath /etc/pki/tls/certs
             SSLCAFile /etc/pki/tls/certs/cacert.pem
             SSLVerify none
             AuthDN cn=admin, dc……,dc=it
             AuthPassword passwordserverldap
             BaseDN  dc=……..,dc=it
             Scope sub
             UsernameAttr cn
             CheckAttr x-WirelessEduroam

……
</Handler>
```

EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del server FreeRADIUS
Autenticazione - Autorizzazione

/etc/radiusdir/site-available/inner-tunnel

```
server inner-tunnel {
authorize {
        preprocess
        suffix
        update control {
            Proxy-To-Realm := LOCAL
        }
        eap {
                ok = return
        }
        ldap
}
authenticate {
        Auth-Type MS-CHAP {
                mschap
        }
        Auth-Type LDAP {
                ldap
        }
        eap
```

EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del server FreeRADIUS
Autenticazione - Autorizzazione

/etc/radiusdir/site-available/default

```
authenticate {
        Auth-Type MS-CHAP {
                mschap
        }
        Auth-Type LDAP {
                ldap
        }
        eap
}
```

EduRoam – Istruzioni per l'uso

Preparazione … Configurazione del server FreeRADIUS Accounting

/etc/radiusdir/site-available/default

```
accounting {
        detail
        radutmp
        attr_filter.accounting_response
}
```

/etc/radiusdir/site-available/default

```
attr_filter attr_filter.accounting_response {
                key = %{User-Name}
                attrsfile = ${confdir}/attrs.accounting_response
        }
```

Archiviare sia I dati dell'**ACCOUNTING**, ma principalmente il log dell'**AUTENTICAZIONE**

EduRoam – Istruzioni per l'uso

Verifica del SERVIZIO

Per verificare il processo di proxy, abilitare il radius in debug mode:

radiusserver# freeradius -X

Su un'altra shell digitare:

radiusserver# radtest testedu@garr.it xxxxx 127.0.0.1 1812 passwordfileclien

```
Sending Access-Request of id 132 to 127.0.0.1 port 1812
        User-Name = "testedu@garr.it"
        User-Password = "xxxxxx"
        NAS-IP-Address = 123.123.123.123
        NAS-Port = 1812
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=132, length=36
        Reply-Message = "Request Denied"
```

Verificare se dal debug risulta il forward della richiesta al radius proxy di gerarchia superiore

E' possibile chiedere un account di test con scadenza al gruppo eduroam@garr.it per verificare se effettivamente le richieste vanno a buon fine.

Monitoring del roaming Europeo su **http://monitor.eduroam.org**

EduRoam – Istruzioni per l'uso

Servizi da garantire agli utenti di EduRoam

- IPSec VPN: protocolli IP 50 (ESP) e 51 (AH) in entrata e in uscita e UDP/500 IKE
- OpenVPN: UDP/1194
- IPv6 Tunnel Broker service: protocollo IP 41 in entrata e in uscita
- IPsec NAT-Traversal: UDP/4500
- Cisco IPSec VPN over TCP: TCP/10000 in uscita
- PPTP VPN: protocollo IP 47 (GRE) in entrata e in uscita e TCP/1723 in uscita
- SSH: TCP/22 in uscita
- HTTP e HTTPS: TCP/80 e TCP/443 in uscita
- IMAP4 e IMAPS: TCP/143 e TCP/993 in uscita
- IMAP3: TCP/220 in uscita
- POP3 e POP3S: TCP/110 e TCP/995 in uscita
- (S)FTP passivo: TCP/21 in uscita
- SMTPS: TCP/465 in uscita
- SMTP submission via STARTTLS: TCP/587 in uscita
- RDP: TCP/3389 in uscita

EduRoam – Istruzioni per l'uso

Cosa fare in caso di INCIDENTE ….

- Contattare tramite email il servizio eduroam@garr.it riportando gli estremi dell'incidente ed eventualmente parte del log di accounting.

- Al resto penseremo noi e vi terremmo informati tramite email.

EduRoam – Istruzioni per l'uso

Cosa fare in caso di INCIDENTE ….

Esempio:

Riscontrato un problema in fase di accounting sul dominio tu-berlin.de all'Universita' di Perugia

Desc: Un utente del dominio tuberlin.de in fase di accounting perdeva il realm nell'identita'.

Tempi di ripristino:

- Problema identificato in 24 ore
- Problema risolto in una settimana con una patch su Freeradius:

Patch:

```
post-auth {
...
   if ("%{reply:User-Name}" !~ /.*@.*/) {   # returning User-Name does not contain an @ sign
      if ("%{request:User-Name}" =~ /(.*)@(.*)/) {# always true, but realm portion lands in subexp %{2}
         update reply {
            User-Name := "%{reply:User-Name}@%{2}"
                        }
                  }
            }
...
      }
```

Domande

Grazie e a presto in e-Learning ….