Experiências com 802.1x

João Marcelo Ceron
Leandro Márcio Bertholdo
Emerson Virti
Liane Tarouco
suporte@pop-rs.rnp.br

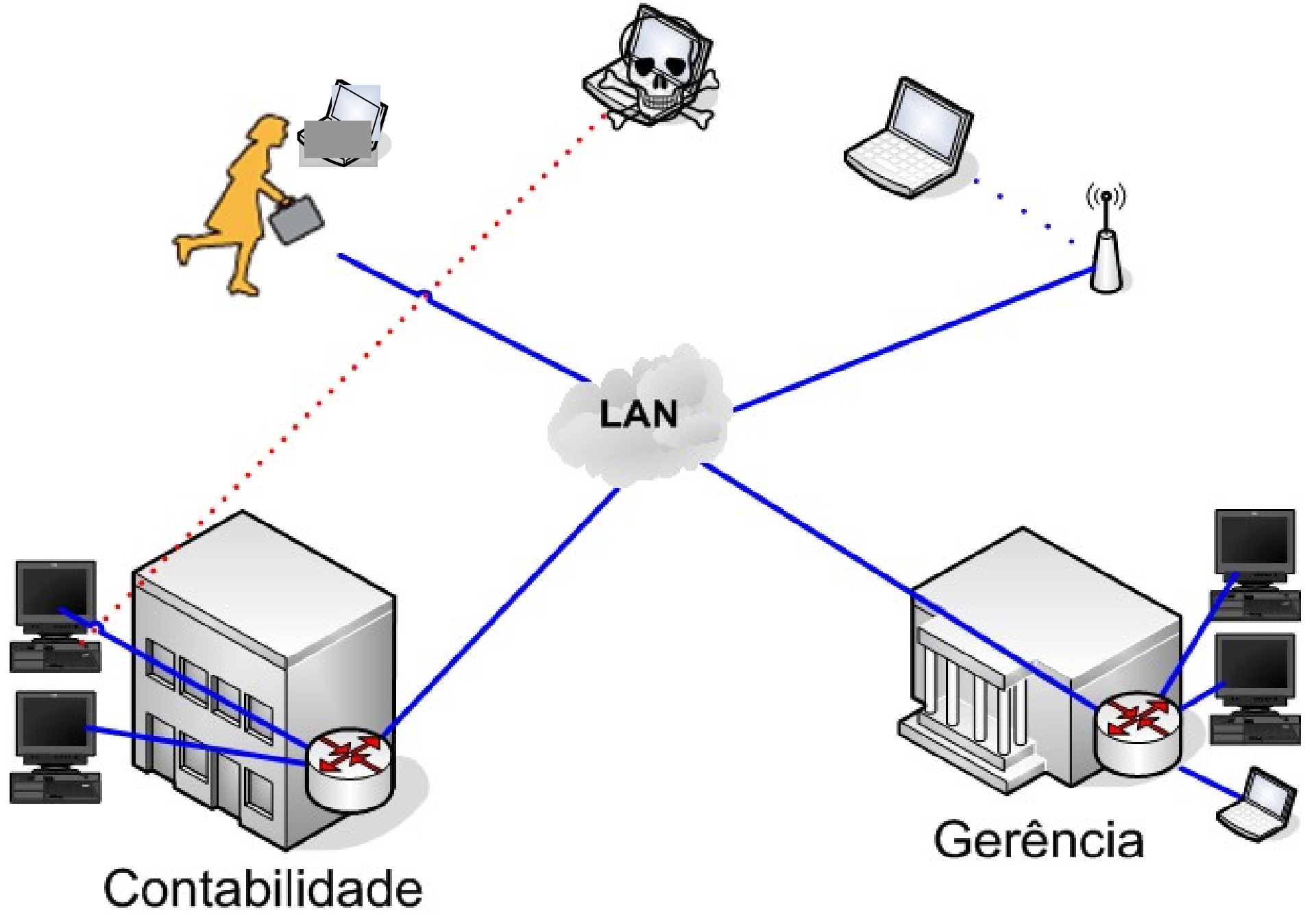
CERT-RS / POP-RS
Centro de Resposta a Incidentes de Segurança da Rede Tchê
Ponto de Presença da Rede Nacional de Ensino e Pesquisa

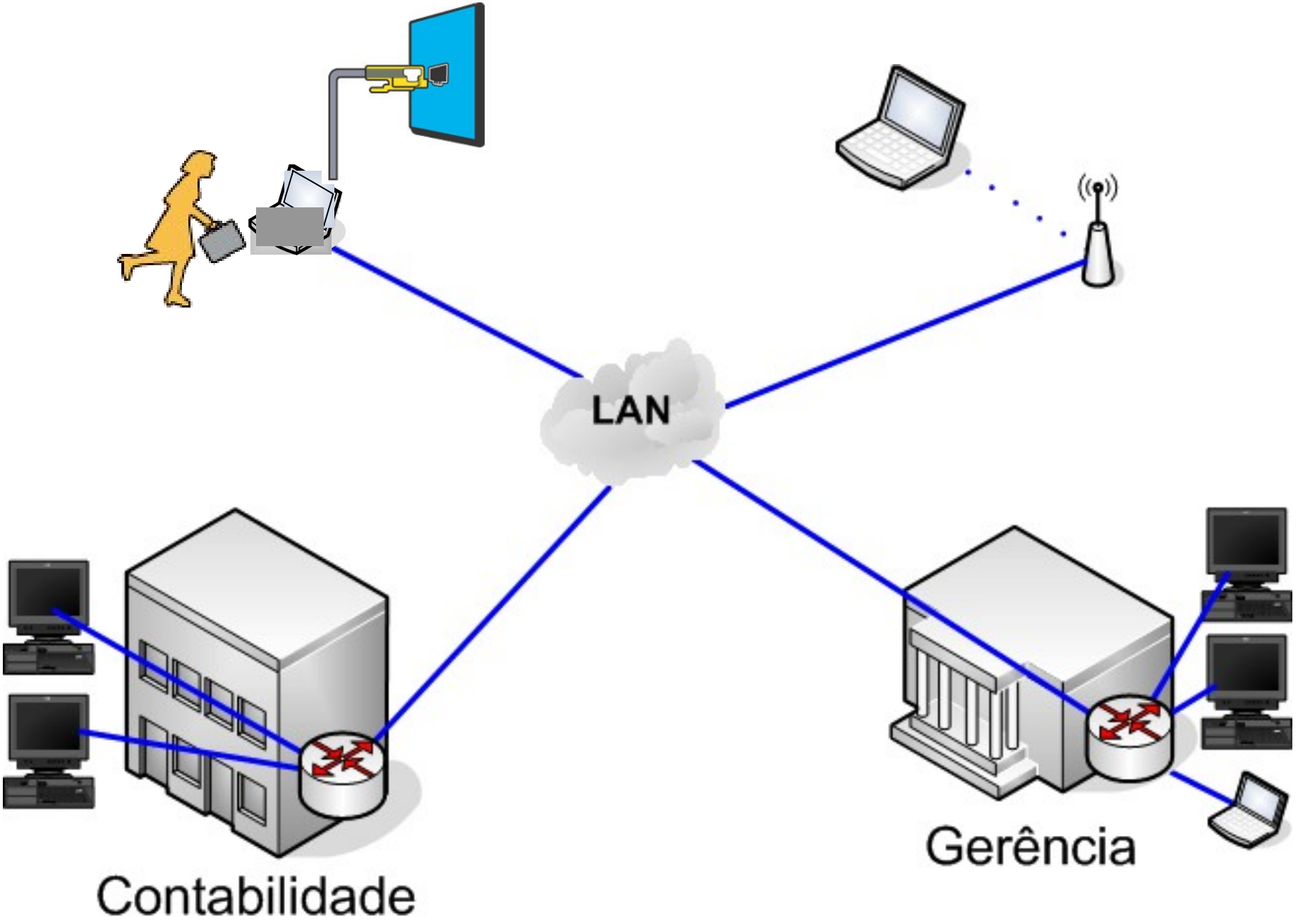
Tópicos

- Motivação
- 802.1X
- Proposta
- Testes realizados
- Lições aprendidas
- Conclusões

Motivação

- Obter controle da LAN


LAN
Contabilidade
Gerência


LAN
Contabilidade
Gerência

802.1X

- Acesso a rede somente a usuários autorizados
- Usuários wire/wireless
- Privilégios baseados em usuários

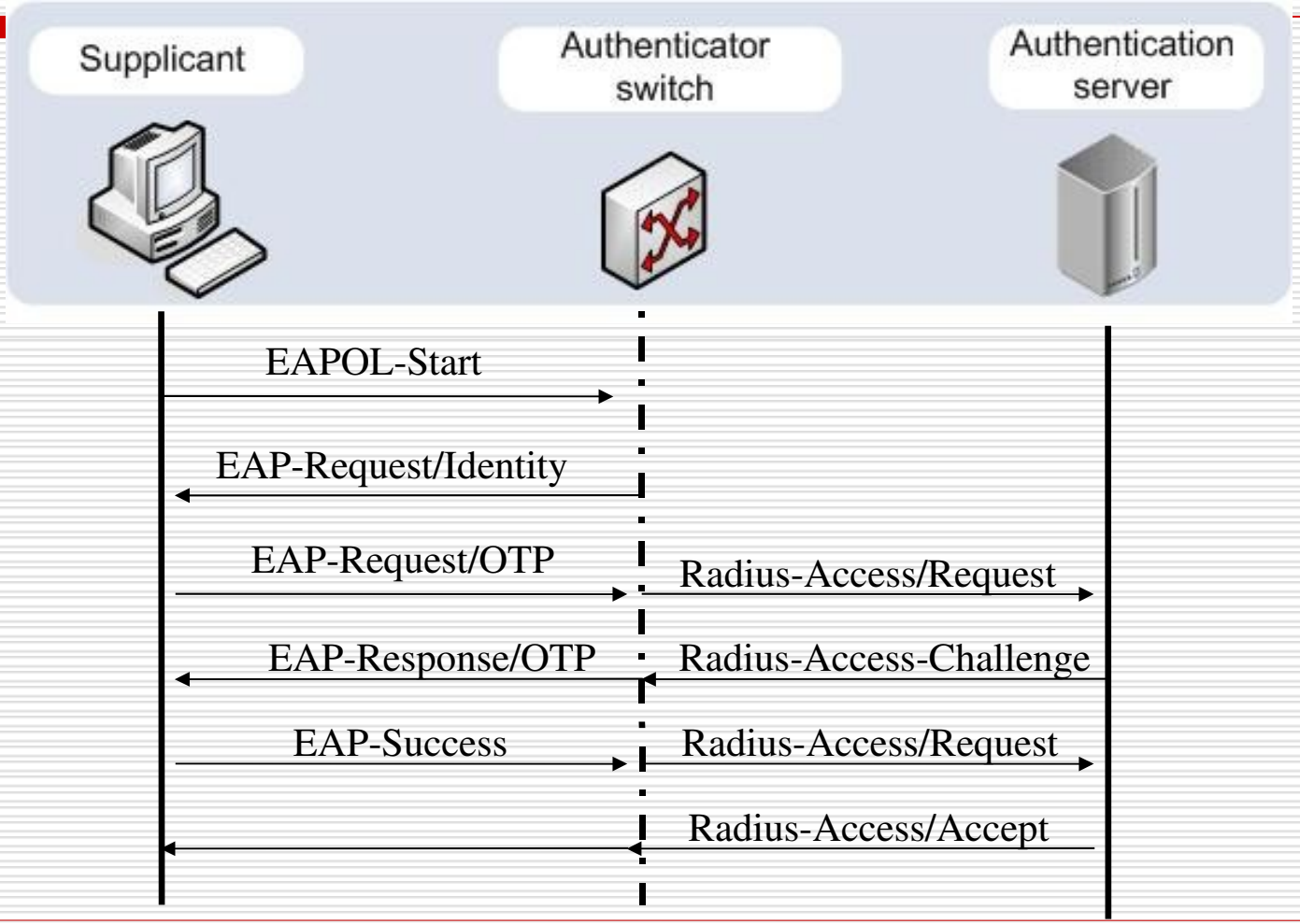
802.1x

- 802.1x – EAP over LAN – EAPOL
- EAP (Extensible Authentication Protocol) RFC 3748
  - Extensão para autenticação
  - Flexibilidade (certificados,tokens)
- PPP (Point to Point Protocol)
  - Autenticação (PAP, CHAP)
  - Pouca flexibilidade

Entidades do 802.1X

- Supplicant: software que reside no cliente
- Authenticator: equipamento de rede, que atua como intermediário
- Authenticator Server: radius

Elementos


Supplicant
Authenticator switch
Authentication server
EAPOL-Start
EAP-Request/Identity
EAP-Request/OTP
Radius-Access/Request
EAP-Response/OTP
Radius-Access-Challenge
EAP-Success
Radius-Access/Request
Radius-Access/Accept

Solução Proposta

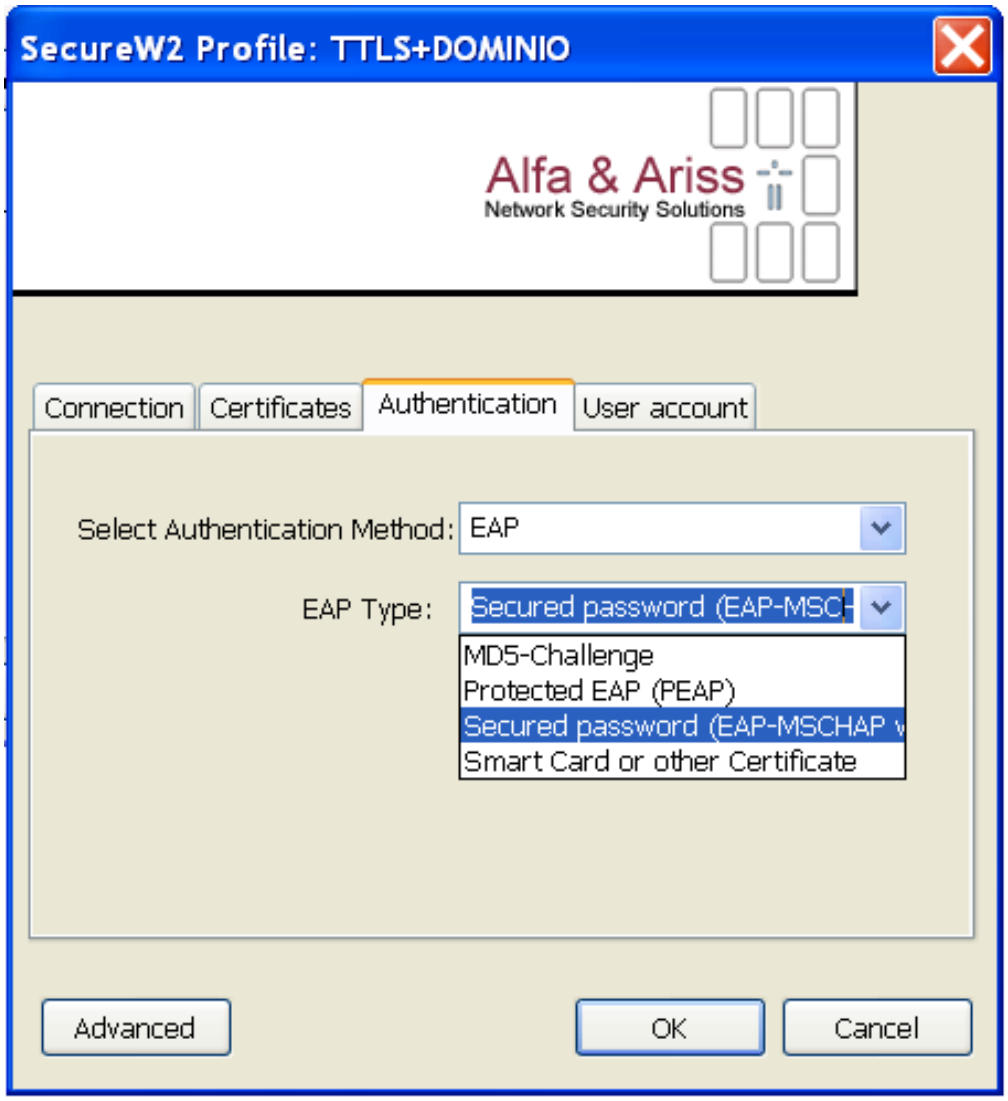
- Usuários não autorizados com acesso à rede
- Solução escalável e flexivel
  - Mobilidade (wireless/wired)
  - Interoperabilidade (freebsd, linux, windows XP, cisco, extreme)
  - Custos

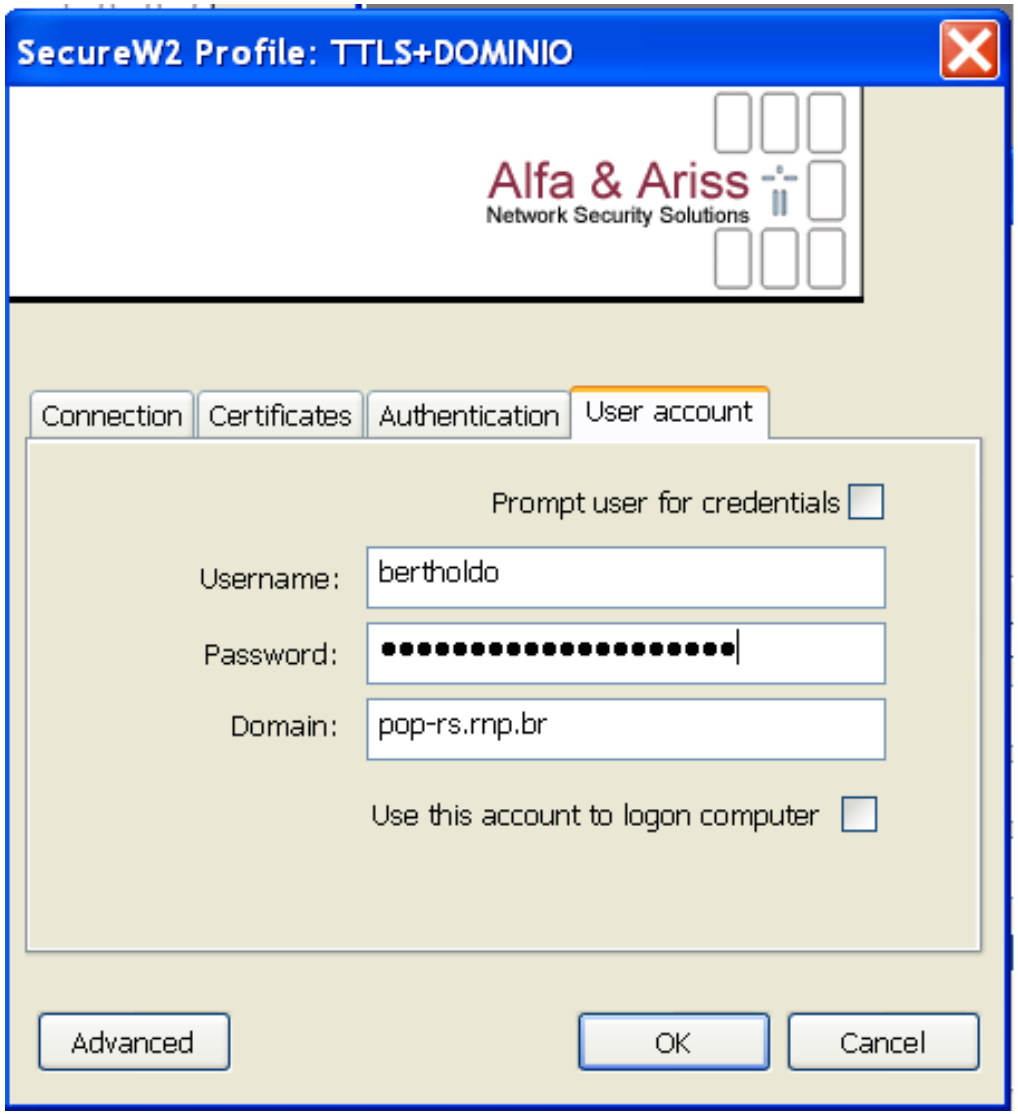
Supplicantes

Clientes	98/ ME	XP/ 2K	OS X	Li nux	Pckt PC	TLS	PEAP	TTLS	Licença
Win Nativo	✘	✓	✘	✘	✘	✓	CHAP v2	✘	Nativo
OSX Nativo	✘	✘	✓	✘	✘	✓	✓	✓	Nativo
SecureW2	✘	✓	✘	✘	✓	✘	✘	✓	Free
Odyssey	✓	✓	✘	✘	✓	✓	✓	✓	$$
AEGIS	✓	✓	✓	✓	✓	✓	✓	✓	$$
wpa_supp	✓	✓	✘	✓	✘	✓	✓	✓	Free
Xsupplicant	✘	✘	✘	✓	✘	✓	✓	✓	Free

Protocolos para autenticação

- EAP-MD5
- EAP-TLS
- LEAP, EAP-FAST – CISCO
- EAP-PEAP Microsoft
- EAP-TTLS


SecureW2 Profile: TTLS+DOMINIO
Alfa & Ariss
Network Security Solutions
Connection
Certificates
Authentication
User account
Select Authentication Method:
EAP
EAP Type:
Secured password (EAP-MSC
MD5-Challenge
Protected EAP (PEAP)
Secured password (EAP-MSCHAP v
Smart Card or other Certificate
Advanced
OK
Cancel


SecureW2 Profile: TTLS+DOMINIO
Alfa & Ariss
Network Security Solutions
Connection
Certificates
Authentication
User account
Prompt user for credentials
Username:
bertholdo
Password:
Domain:
pop-rs.rnp.br
Use this account to logon computer
Advanced
OK
Cancel

Authenticator

Radius configuration

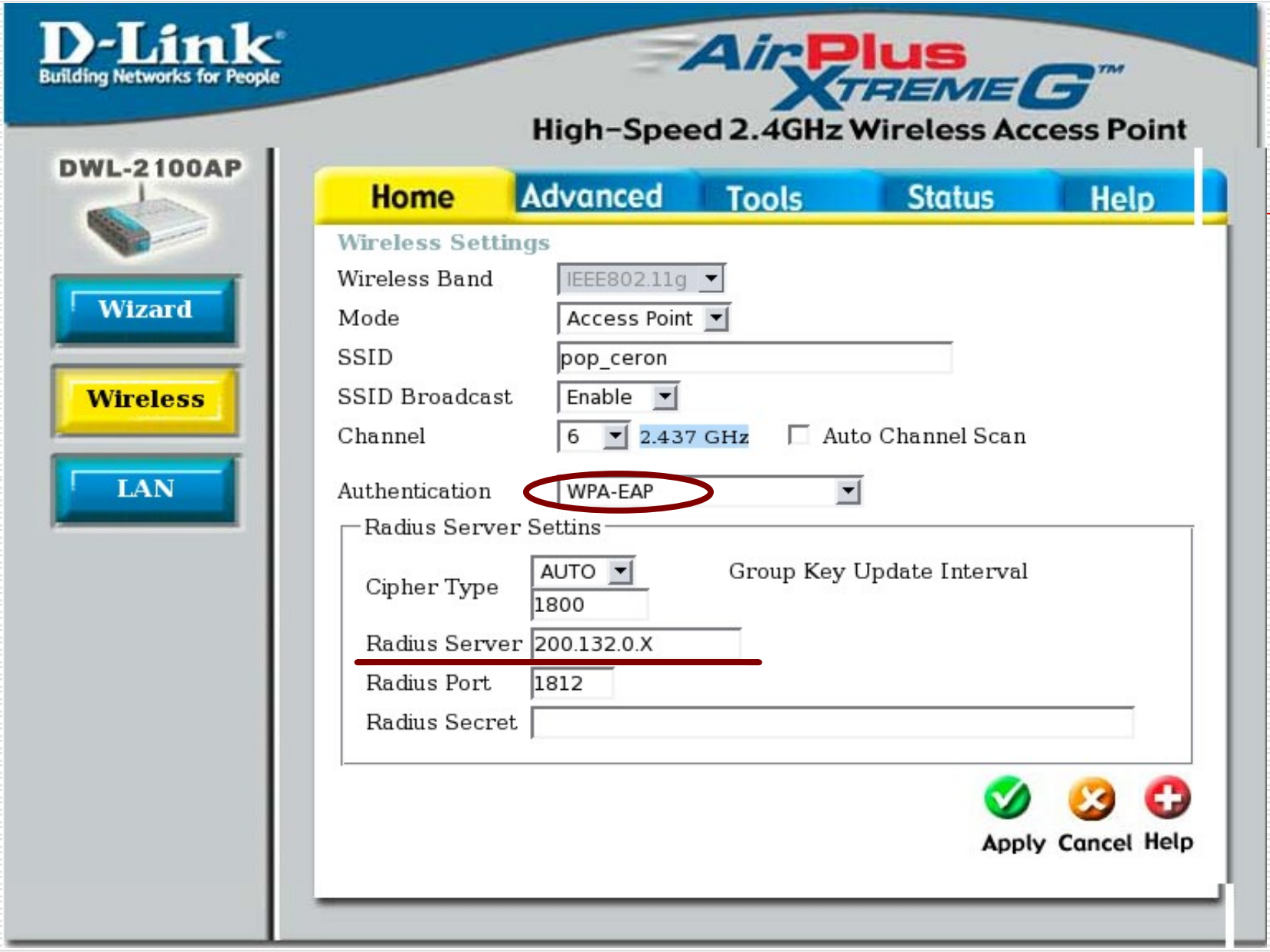
enable radius

configure radius primary shared-secret encrypted
"abc1#$2130fdf"

configure radius primary server 200.132.X.X 1812
client-ip 200.132.X.X

Network Login Configuration

enable netlogin dot1x


D-Link
Building Networks for People
AirPlus XTREME G™
High-Speed 2.4GHz Wireless Access Point
DWL-2100AP
Wizard
Wireless
LAN
Home
Advanced
Tools
Status
Help
Wireless Settings
Wireless Band
IEEE802.11g
Mode
Access Point
SSID
pop_ceron
SSID Broadcast
Enable
Channel
6
2.437 GHz
Auto Channel Scan
Authentication
WPA-EAP
Radius Server Settins
Cipher Type
AUTO
Group Key Update Interval
1800
Radius Server
200.132.0.X
Radius Port
1812
Radius Secret
Apply
Cancel
Help

Authenticator Server

- freeRadius
  - Suporte EAP
  - Suporte LDAP

- Problemas encontrados
  - Desenvolvido um patch para FreeRadius
  - Não é um BUG, é uma diferença na interpretação da RFC 3579

```
                }
                vp->next = request->packet->vps;
                request->packet->vps = vp;

        } else {
                /*
                 *      A little more paranoia.  If the NAS
                 *      *did* set the User-Name, and it doesn't
                 *      match the identity, (i.e. If they
                 *      change their User-Name part way through
                 *      the EAP transaction), then reject the
                 *      request as the NAS is doing something
                 *      funny.
                 */


                //  Changed by <Leandro Bertholdo/Joao Marcelo Ceron>
                 if (strncmp(handler->identity, vp->strvalue,
                      MAX_STRING_LEN) != 0) {
                      radlog(L_ERR, "rlm_eap: Identity does not match User-Name.  Authentication failed

                      free(*eap_packet_p);
                      *eap_packet_p = NULL;
                       return NULL;
                 }

        }
    } else {                /* packet was EAP identity */
          handler = eap_handler_alloc();
ork/freeradius-1.1.2/src/modules/rlm_eap/eap.patch.c: 1134 lines, 31655 characters.
```

Logs do freeRadius

rlm_eap: **EAP/ttls**

rlm_eap_ttls: Authenticate

rlm_eap_tls: processing TLS

TLS_accept: SSLv3 write server done A

EAP-Message =
0x0107040a15c0000007501603010 04a02000046030142c28d123a055e37de2ecce3e9fe2c19ae0a8b373bfbbb685c9d652a938d476b204103f23ab40c6797a5481059ccac9882f90a0d95a67c362b75276ea199991e36000a0016030106f30b0006ef0006ec0002c5308

Going to the next request

modcall[authorize]: module "chap" returns noop for request 0

modcall[authorize]: **module "mschap"**

rad_recv: Access-Request packet from host 200.132.X.X:1028, id=2, length=111

User-Name = "**bertholdo**"

EAP-Message = 0x020700061500

modcall: entering group authorize for request 2

modcall[authorize]: module "chap" returns noop for request 2

modcall[authorize]: module "mschap" returns noop for request 2

rlm_ldap: - authorize

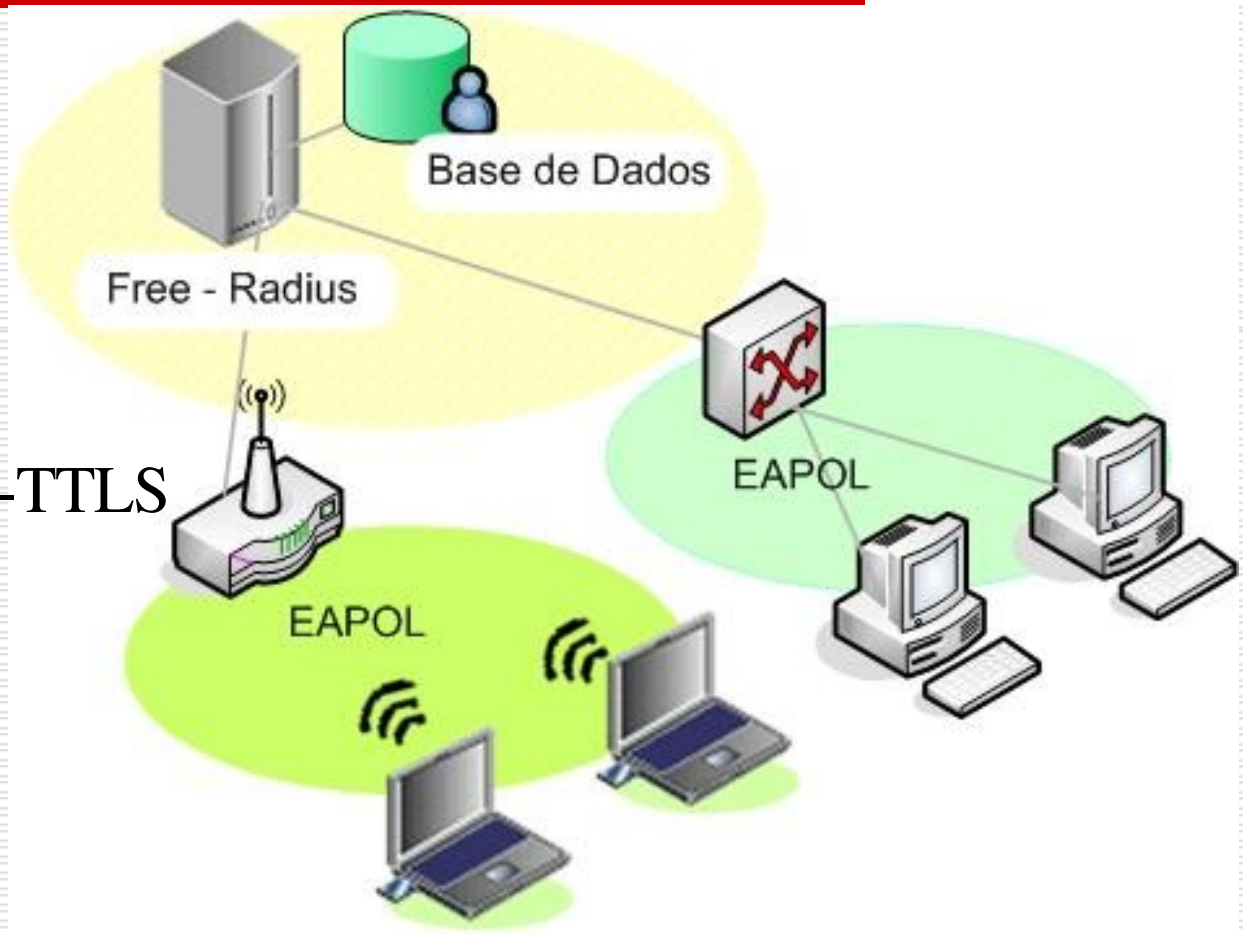
rlm_ldap: performing user authorization for leandro

radius_xlat: '(**uid= bertholdo**)'

radius_xlat: 'ou=People,ou=adsl,dc=pop-rs.rnp,dc=br'

802.1x - Estrutura

EAP-TTLS



Desvantagens do 802.1x

- Necessita de uma infra-estrutura
- Suporte nativo a clientes
- TLS envolve uma PKI (Public Key Infrastructure)

Conclusões

- Solução flexível e robusta
- Fácil implementação
- Switchs com suporte 802.1x
- Segurança => $$

- A 802.11i incorpora 802.1x

Agradecimentos

- Obrigado!
- Contato:

ceron@pop-rs.rnp.br
berthold@pop-rs.rnp.br

Dúvidas e questionamentos...

- POP-RS/CERT-RS
- suporte@pop-rs.rnp.br