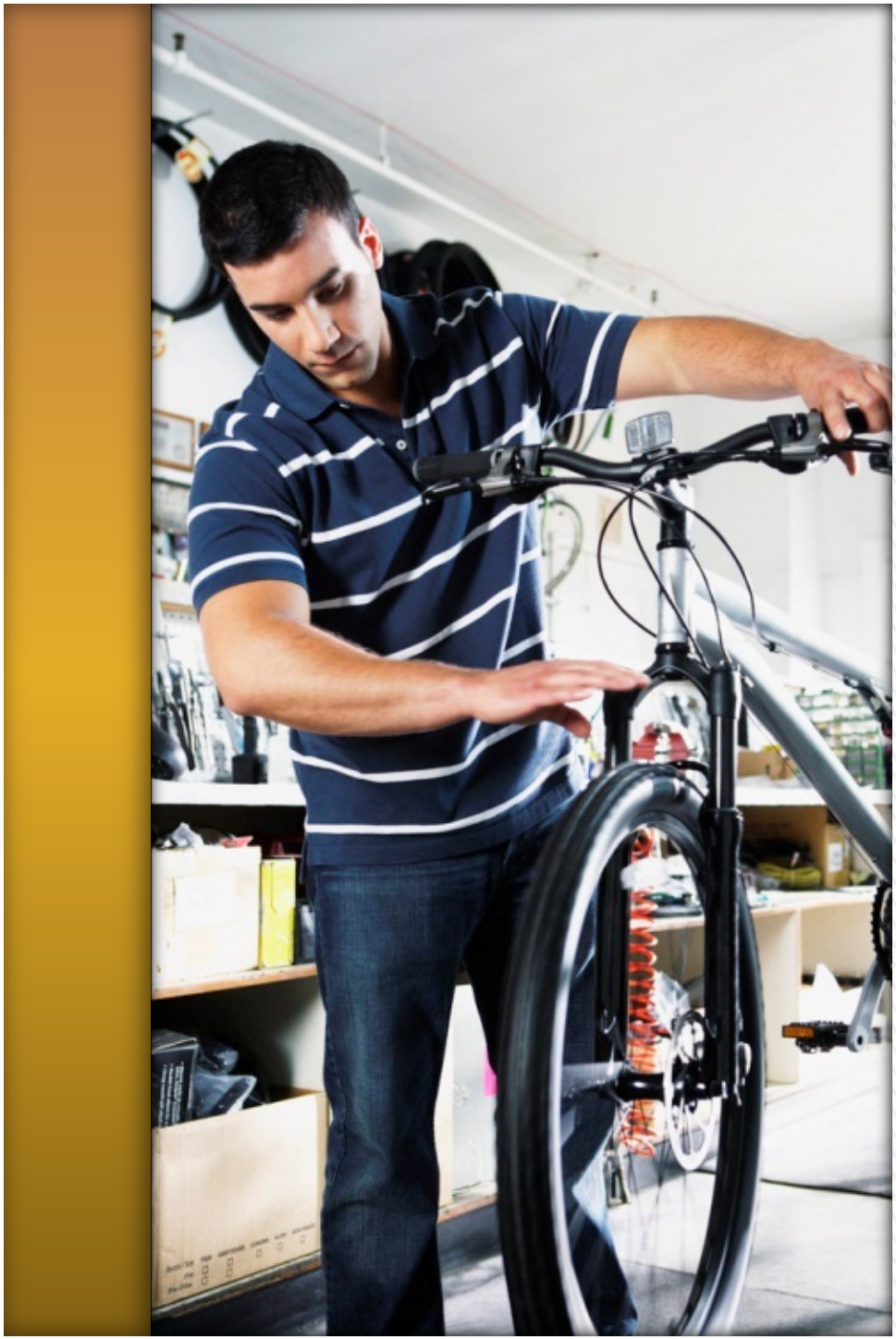


Ricardo de Mingo
Àrea de Tecnologies UB
1/12/2011

Tu red bajo control NACUB

Índice

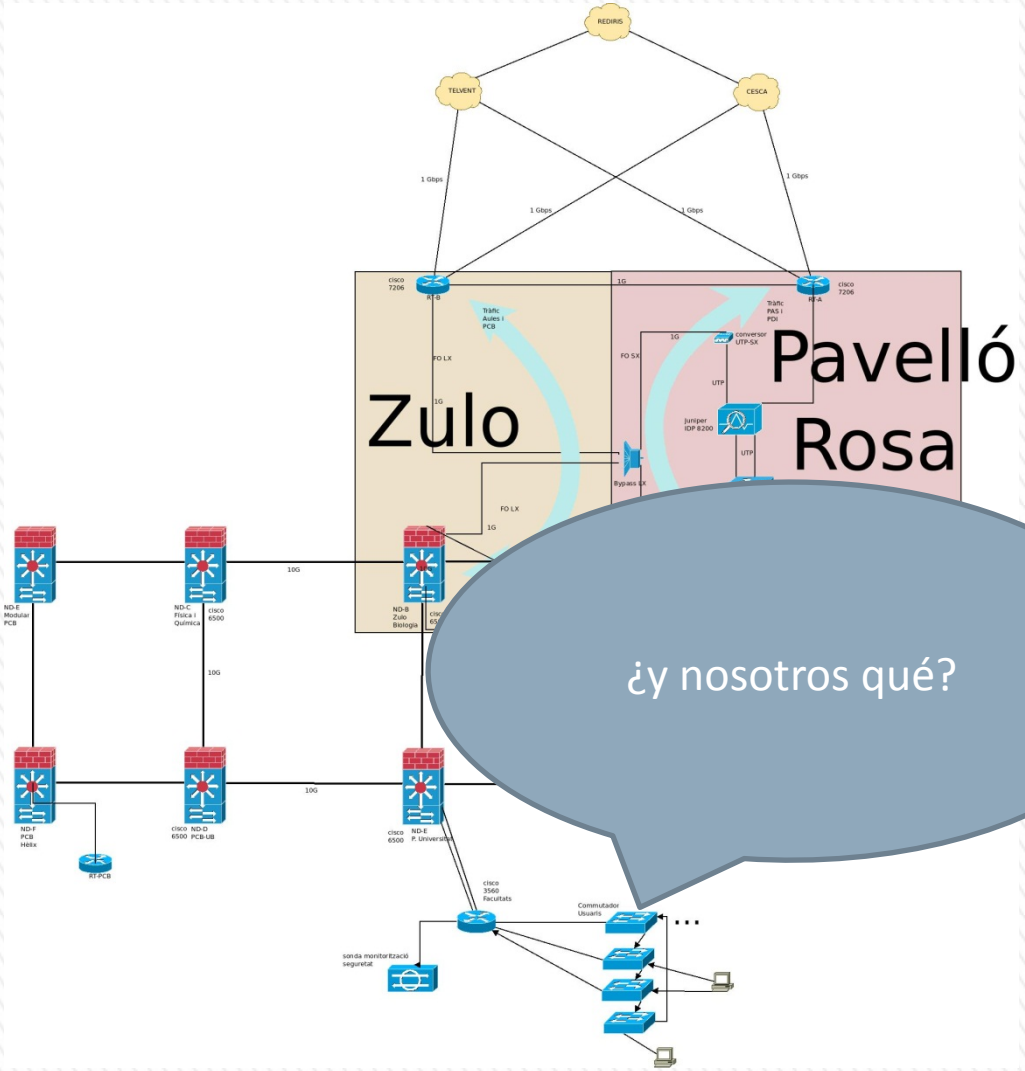

¿Por qué?
Esto ya está visto
Solución técnica
Solución administrativa
Videos

NACUB -> ¿Por qué?

- Más de 12.000 puntos de red “públicos”
- Más de 10.000 cosas con IP, 1200 SW, 800 AP, 40 RT
- Unos 60.000 estudiantes
- 5.000 PDI y 2.000 PAS
- Vlans, ACL, VRFs, MPLS
- Corta fuegos, IPS, Gestor BW, Sonda DDoS, …

- Y los usuarios siguen conectando lo que quieren como quieren

NACUB -> ¿Por qué?



NACUB -> ¿Por qué?

- Usuarios anónimos (una IP no es un usuario)
- Puntos de red “públicos”
- Crecimiento no controlado (AP, hubs, routers,…)
- Mucha información, pero poco cumplimiento
- Cumplir con los controles ISO 27002:2005 de seguridad de acceso a la red:
  - 11.4.1 Política de uso de los servicios de red
  - 11.4.3 Identificación de equipos en la xarxa
  - 11.4.4 Diagnóstico remoto y protección de los puertos de configuración
  - 11.4.6 Control de la conexión a la red

NACUB -> Esto ya está visto

Pues sí:

» JJTT 2006:

Unificación de servicios de red en aulas informáticas
Albert Teixido (UAB), José Antonio Lorenzo (UAB)

» JJTT 2009:

NAC Inverso, un esquema optimizado de acceso a Internet
José Carlos González González, ULL

» JJTT 2009:

Sistema para el control de acceso a red basado en servicios
Jon Matías, EHU

NACUB -> Esto ya está visto

Diferencias y semejanzas

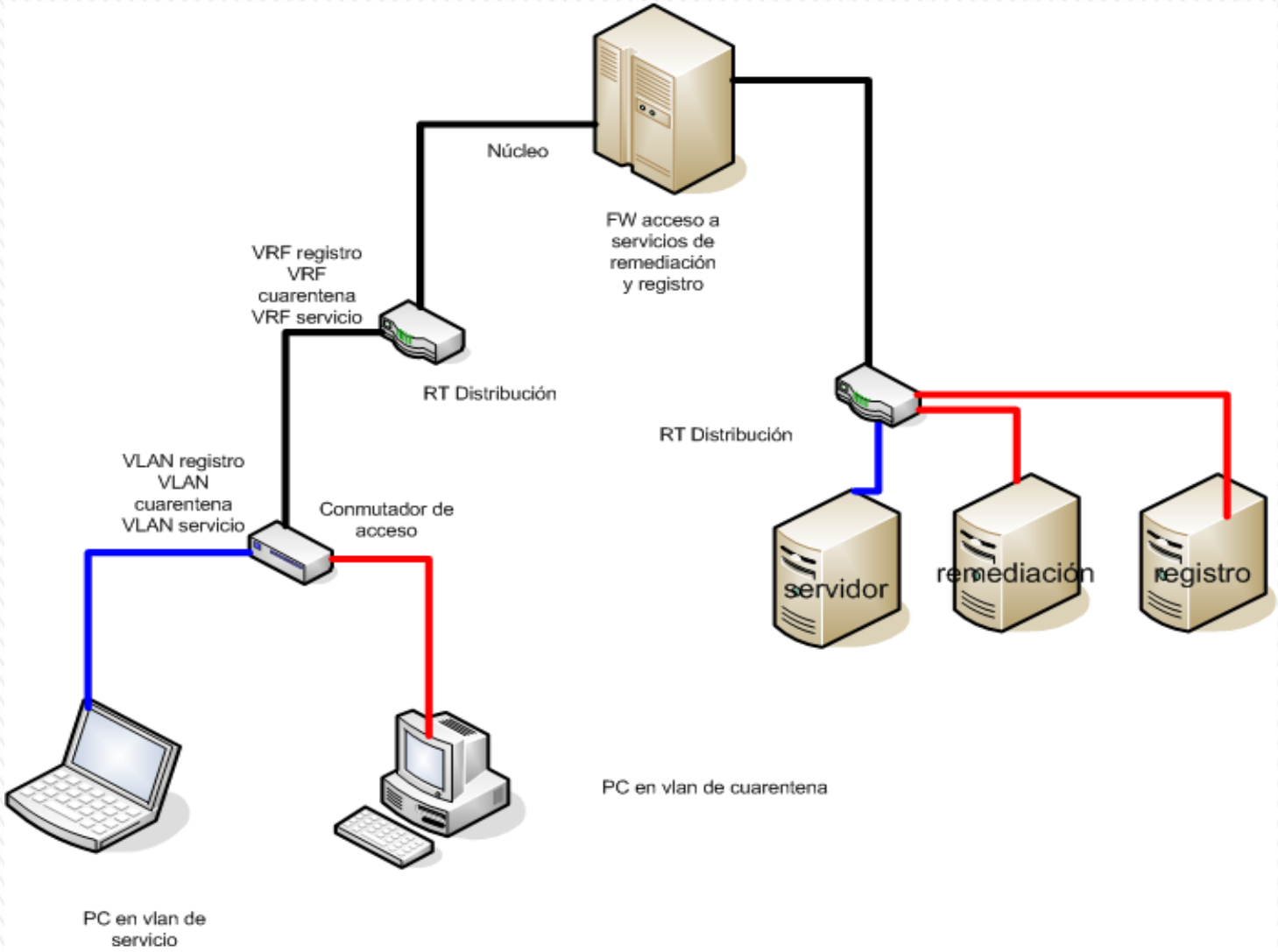
- Universal: funciona para cualquier dispositivo que cumpla con configuración via telnet
- Universal: independiente de S.O. cliente
- Integrable: via webservices
- Funcional entre versiones: adiós SNMP, hola “expect”, NETCONF, openflow.org, …
- Portal de autoregistro y comunicación
- Queremos gestionar servicios, no redes (pero es necesario)
- Voluntad de compartir la solución: www.opennac.org

NACUB -> Solución Técnica

Actores:

- LDAP: directorio de usuarios
- RADIUS: receptor de las peticiones de los SW
- DHCP: ofrece IP para cada vlan
- DNS: contesta con la IP del portal cautivo en la vlan de registro
- Portal web de registro y gestión
- Configuración en la red de las vlans de registro, remediación y servicio

NACUB->Esquema de red



NACUB -> Solución Técnica

Módulos componentes:

- Gestor de políticas y administración
- Netreg: Portal cautivo de autoregistro
- Netconf: configurador de equipos
- Portal de comunicación

Dependencias

- Base de Datos de inventario o CMDB
- De los actores
  - DNS, DHCP, RADIUS, LDAP
  - Configuración de la red

NACUB -> Componentes

Gestor de Políticas y administración

- Reglas estilo quien, cuando, origen, destino, servicio
- Se traducen a instrucciones de diversos dispositivos
- Implementado sólo para dispositivos tipo SW
- Por ejemplo: reglas nivel 2,3 via Radius
- Saber: Fecha-hora-IP-MAC-VLAN-puerto-SW-roseta-usuario
- Enviar a un usuario a la red de remediación manualmente o automático (sondas IDS)

NACUB -> Gestor de políticas

Impressora

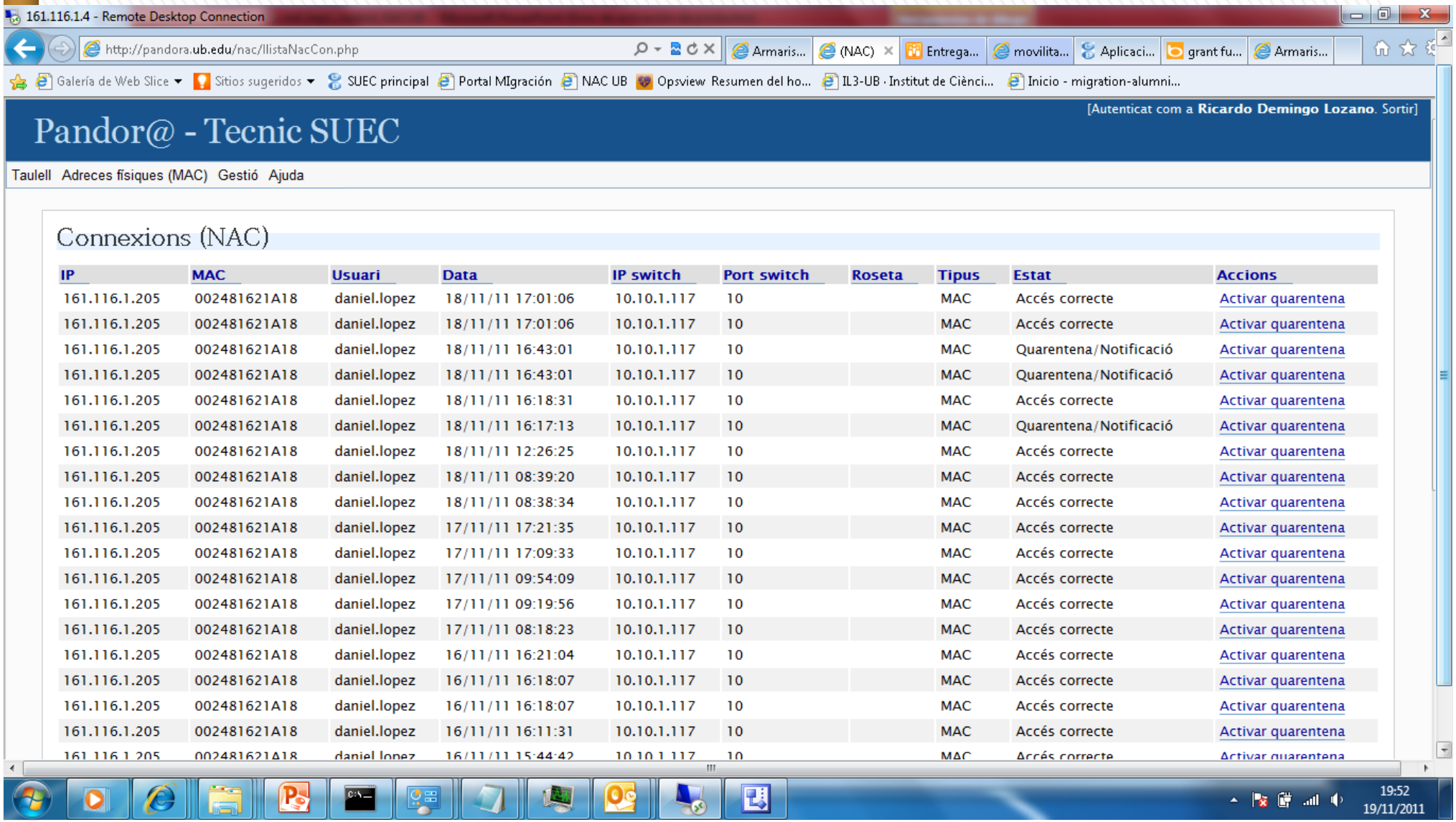
Convidat	Dilluns	Dimarts	Dimecres	Dijous	Divendres	Dissabte	Diumenge
Tots els llocs	Serveis impressora						

Exemples del sistema de polítiques

Exemple de granularitat d'un possible examen

Alumne assignatura XXX	Dilluns	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19
Aula informàtica	Accés a tot. Menys serveis, P2P, CHAT.												
Biblioteca	Accés a tot. Menys serveis, P2P, CHAT.												
Aula informàtica XXX (Examen)	Accés a tot. Menys serveis, P2P, CHAT.								Examen Assignatura XXX	Accés a tot. Menys serv			

NACUB -> Componentes



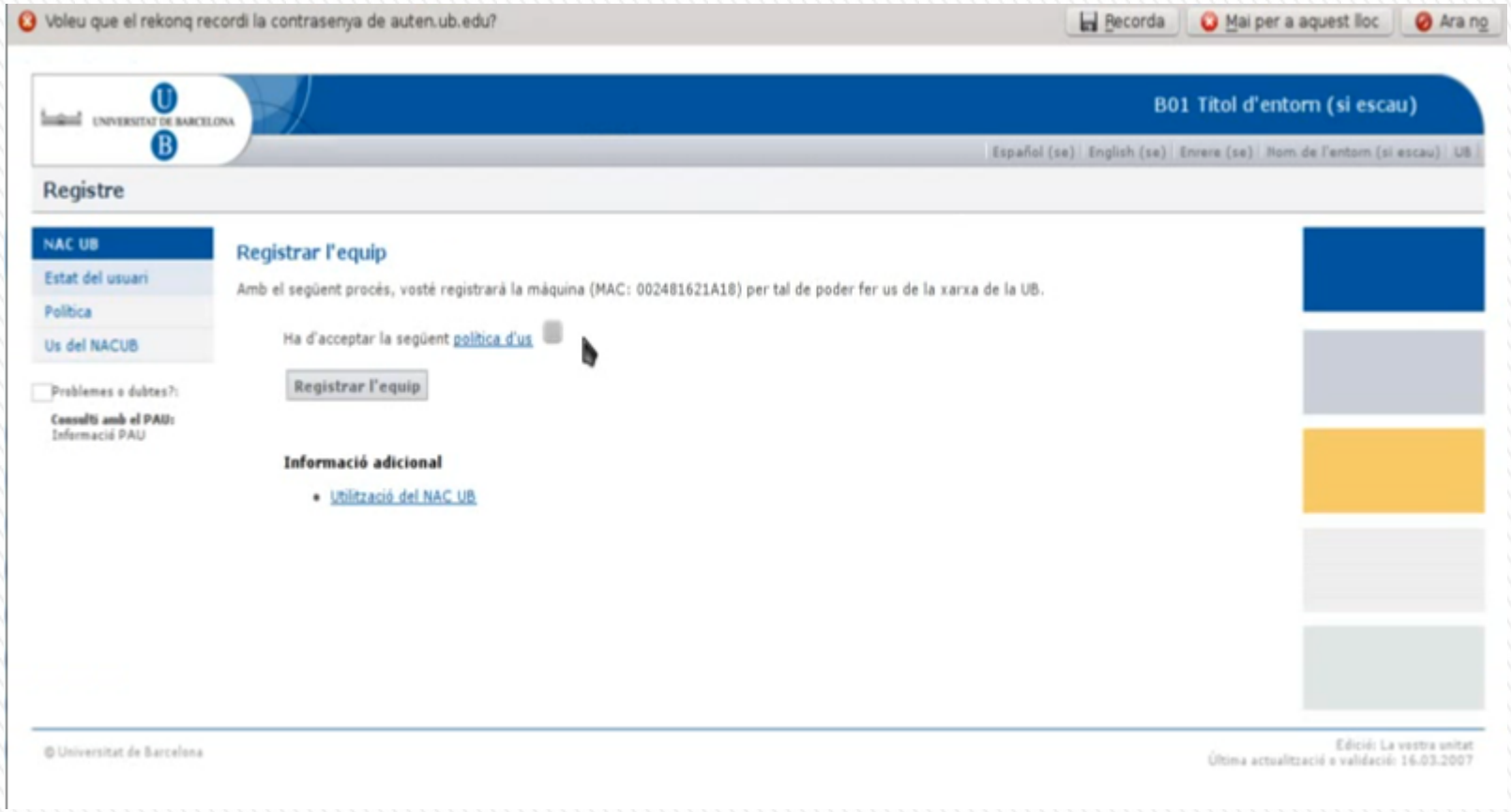
IP	MAC	Usuari	Data	IP switch	Port switch	Roseta	Tipus	Estat	Accions
161.116.1.205	002481621A18	daniel.lopez	18/11/11 17:01:06	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	18/11/11 17:01:06	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	18/11/11 16:43:01	10.10.1.117	10		MAC	Quarentena/Notificació	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	18/11/11 16:43:01	10.10.1.117	10		MAC	Quarentena/Notificació	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	18/11/11 16:18:31	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	18/11/11 16:17:13	10.10.1.117	10		MAC	Quarentena/Notificació	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	18/11/11 12:26:25	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	18/11/11 08:39:20	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	18/11/11 08:38:34	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	17/11/11 17:21:35	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	17/11/11 17:09:33	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	17/11/11 09:54:09	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	17/11/11 09:19:56	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	17/11/11 08:18:23	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	16/11/11 16:21:04	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	16/11/11 16:18:07	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	16/11/11 16:18:07	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	16/11/11 16:11:31	10.10.1.117	10		MAC	Accés correcte	Activar quarentena
161.116.1.205	002481621A18	daniel.lopez	16/11/11 15:44:42	10.10.1.117	10		MAC	Accés correcte	Activar quarentena

NACUB -> Componentes

Netreg: Portal de autoregistro y autenticación

- Permite asociar puerto, MAC, IP a usuario
- Asignación automática de IP fija (dhcp) o pool (dhcp)
- Encargado de asociar al usuario a la ***vlan de servicio (a mejorar)***
- Sirve como portal de invitados.
- Eduroam? Fácil.

NACUB-> Componentes

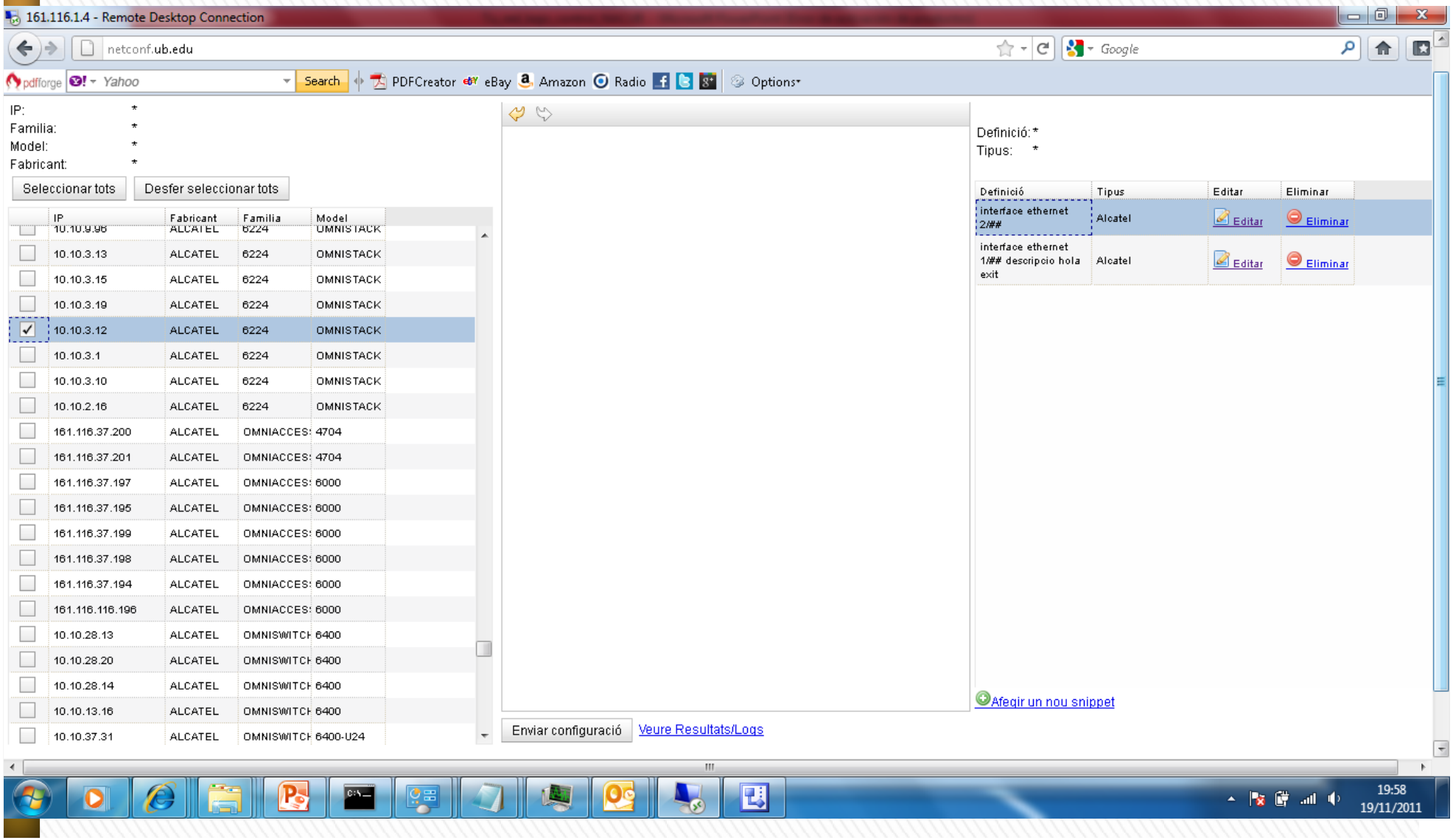


NACUB -> Componentes

Netconf: Configurador de equipos

- Basado en expect via ssh
- Gestor de colas escalable en base a productores y consumidores
- Acceso via CLI, GUI o webservices
- Administración de snippets de configuraciones con macros
- Por ejemplo: cambiar contraseña en 1000 equipos
- Equipos soportados: Alcatel 6224, Cisco 2950 y 3COM4400

NACUB -> Componentes



NACUB -> Componentes

Portal de Comunicación

- Informa y aplica los procesos de acceso a red al usuario según marque la política
- Altamente configurable

NACUB -> Solución Administrativa

- Herramienta de comunicación con el usuario
- Herramienta de aplicación de políticas
- Red de invitados, registro y remediación

NACUB -> Proceso de autenticación -Videos-

- Autenticación via MAC – no hay video -
- Autenticación via 802.1x

» (registre_li): registrar una máquina linux nueva.

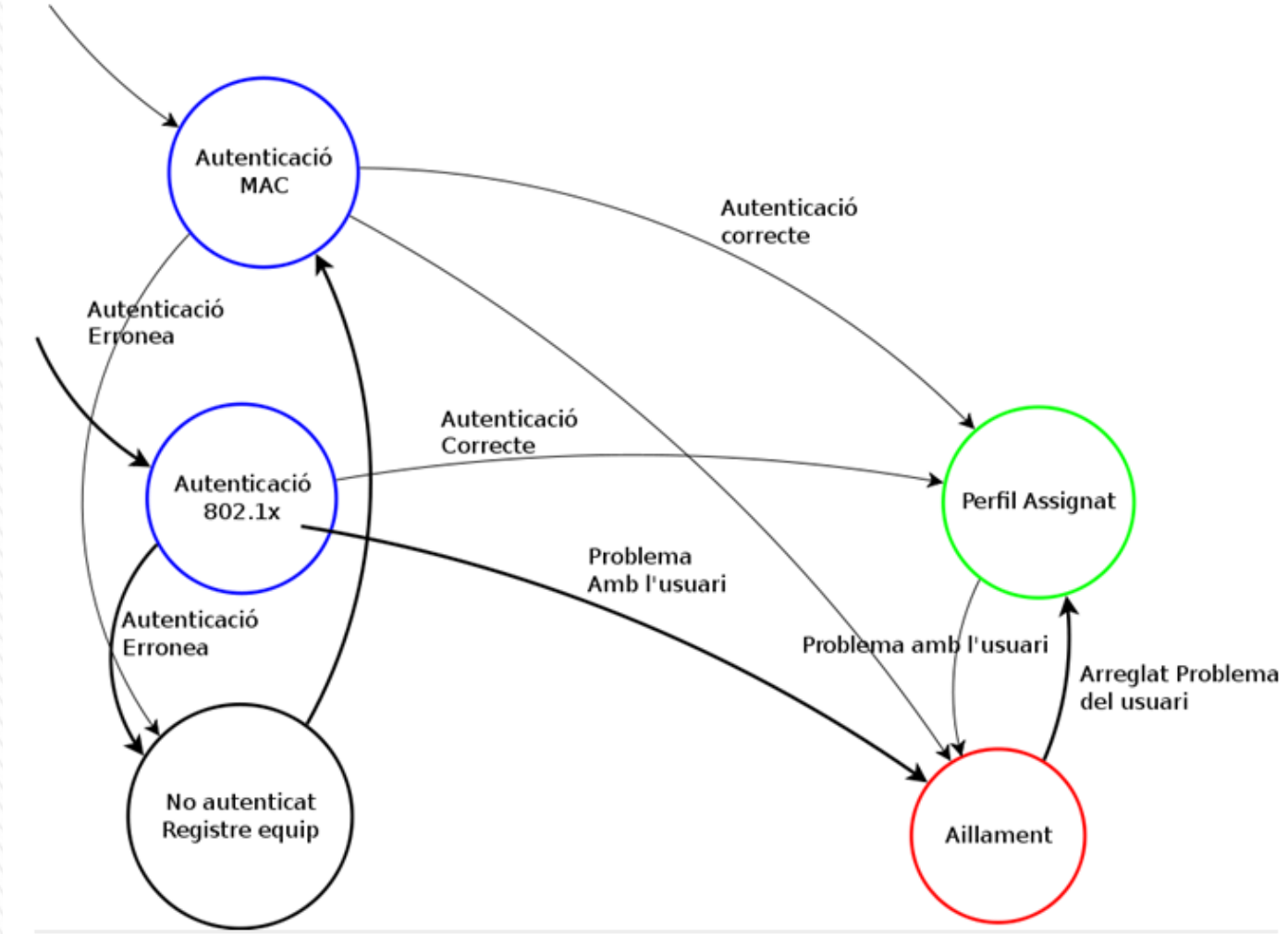
» (Auten1) : suplicante windows con usuario. Pide las credenciales tarde (2 minutos)

» (auten auto2): Las credenciales estan en cache. Autenticación transparente.

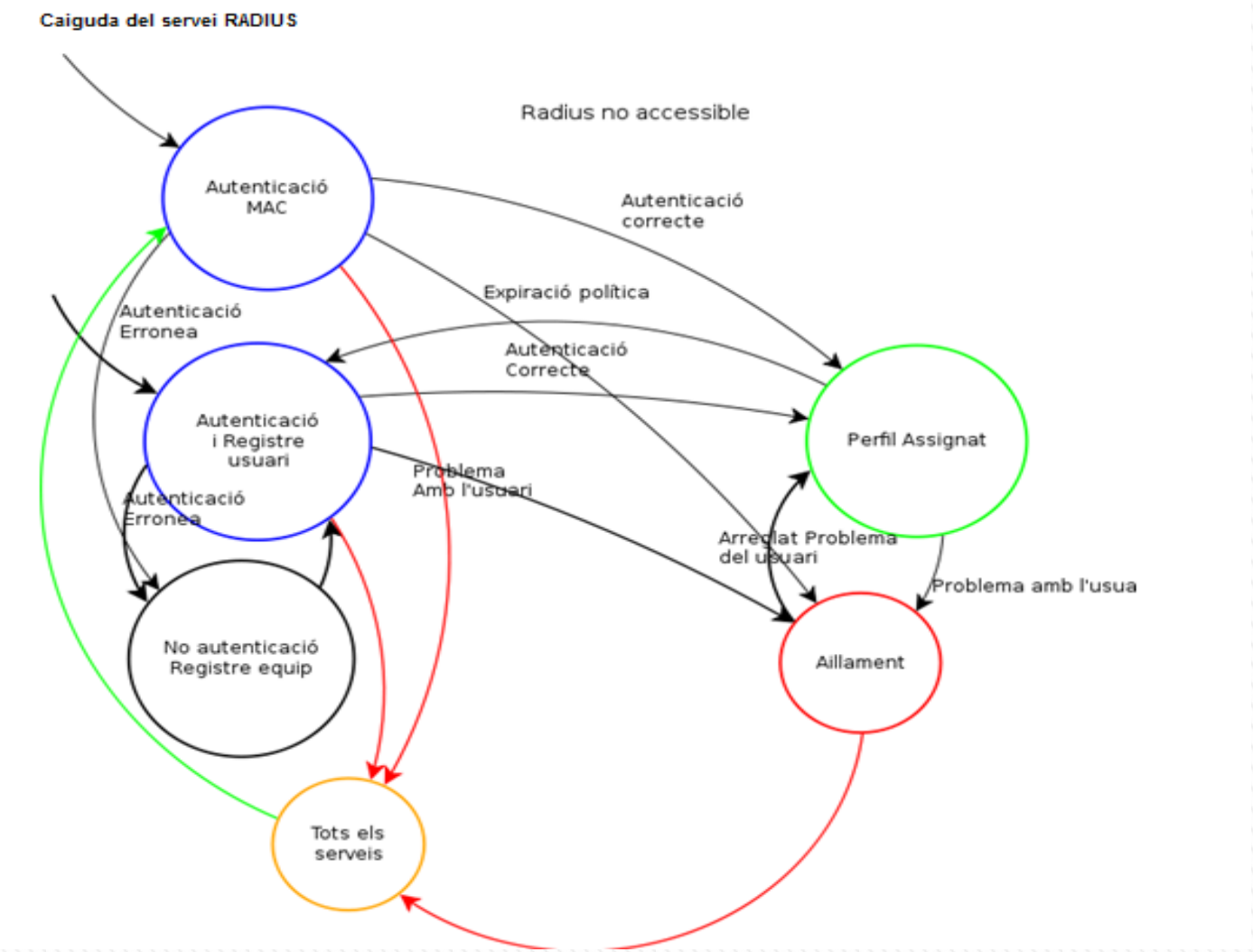
» (movilitat_vlan66-800): un usuario se cambia de ubicación y entra en cuarentena automáticamente

» (Cuarentena): ponemos a un usuario en cuarentena a través del portal de administración

NACUB -> flujo de autenticación



NACUB-> Radius caído



NACUB -> Usos

Netconf

- Leer MACs, IPs
- Asignar MAC<->IP

P. Comunicación

- Cambio de passwd LOPD
- Evitar movilidad

P. Comunicación

- Motivo de cuarentena
- Instalar Software

P. Administración

Saber en tiempo real la asociación:

Fecha-hora-IP-MAC-VLAN-puerto-SW-roseta-usuario

Y poder sacarlo de la red manual o automáticamente

NACUB->Usos

- Registrar MAC o red de invitados
- Evitar movilidad de equipos “no móviles” (impresoras, servidores, equipos de sobremesa)
- Retirar servicios (cuarentena o remediación) a equipos que no cumplan la política de uso
- Comunicar al usuario una noticia personalizada
- Aumento de la seguridad en la red: dhcp snooping + arp inspection + 802.1x
- Autenticación via MAC o usuario

NACUB -> problemas

- Hay que hacer shut/no shut del puerto para que el usuario obtenga una nueva IP por DHCP o forzar DHCP FORCERENEW (RFC 3203) (Windows no lo soporta).
- Las máquinas virtuales no entran en NAC (no podemos tirar el puerto) en modo bridge
- Desactivar NAC para IP fijas: el control se consigue añadiendo entrada en dhcp snooping + port security via netconf.exe
- VMs, APs y RT funcionan con NAC en modo NAT
- Los PC conectados a Hubs y SW necesitan registrarse pero no los podemos poner en remediación individualmente: control con port security y número de MACs permitidas.

NACUB futuro?

OPEN NAC .org

demingo@ub.edu

GRACIAS