Integración de servicios telemáticos en LDAP

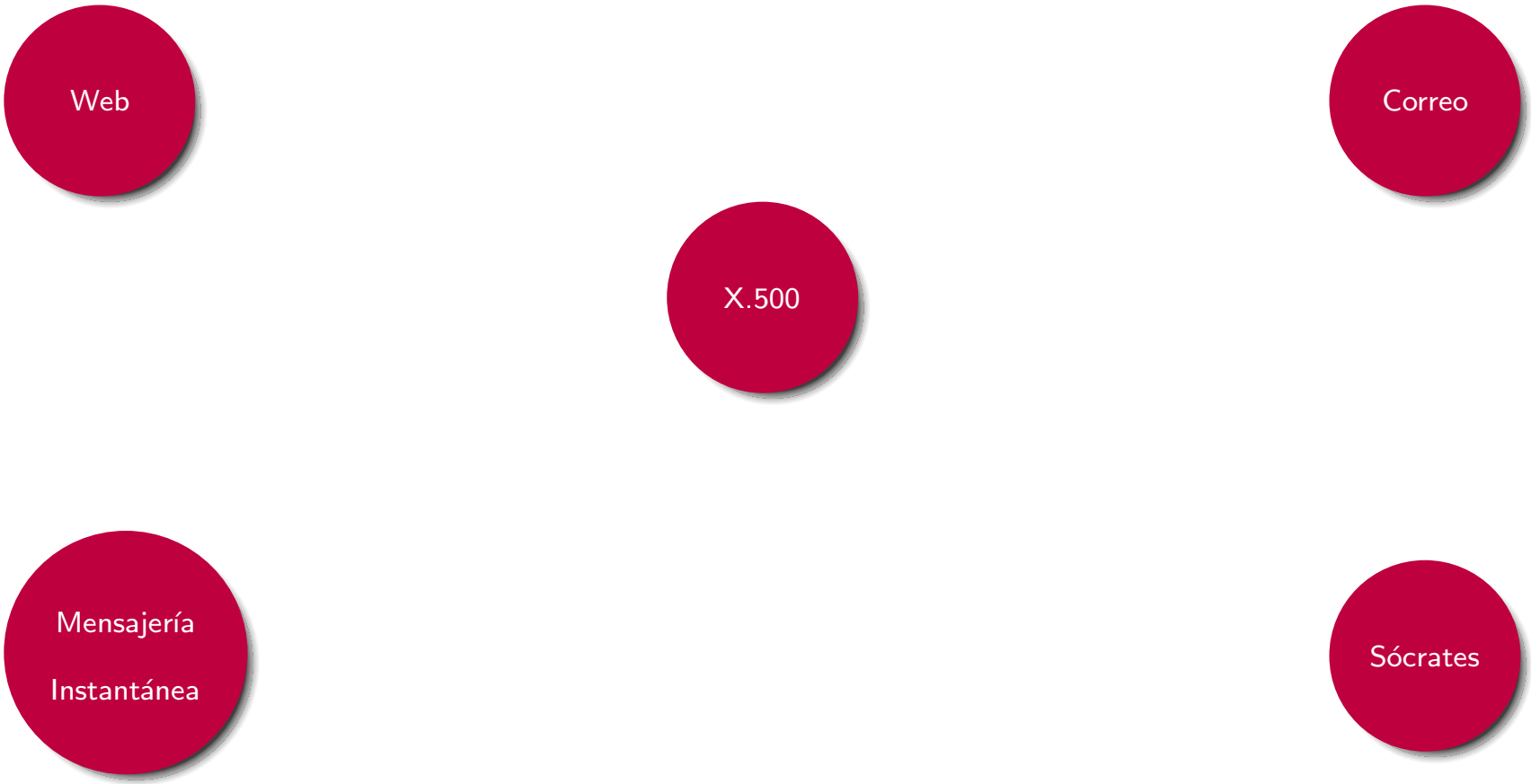
ATICA
UNIVERSIDAD DE MURCIA

Área de Tecnologías de la Información y Comunicaciones Aplicadas

Jornadas Técnicas Rediris 2004
Jueves, 28 de Octubre de 2004

Índice

Islas de servicios (I)



Islas de servicios (II)

- Sin sistema centralizado de cuentas de usuario

Islas de servicios (II)

- Sin sistema centralizado de cuentas de usuario
- Autenticación contenida en cada servidor

Islas de servicios (II)

- Sin sistema centralizado de cuentas de usuario
- Autenticación contenida en cada servidor
- Configuración contenida en cada servidor

Islas de servicios (II)

- Sin sistema centralizado de cuentas de usuario
- Autenticación contenida en cada servidor
- Configuración contenida en cada servidor
- Sólo un servidor por servicio autenticado

Derivados de no centralizar la autenticación

- Un usuario con login/clave distinta para cada servicio o sistema

Derivados de no centralizar la autenticación

- Un usuario con login/clave distinta para cada servicio o sistema
- Administración de cuentas de usuario tediosa y complicada

Derivados de no centralizar la autenticación

- Un usuario con login/clave distinta para cada servicio o sistema
- Administración de cuentas de usuario tediosa y complicada
- Configuración de servicios replicada: problemas de sincronización

Derivados de no centralizar la autenticación

- Un usuario con login/clave distinta para cada servicio o sistema
- Administración de cuentas de usuario tediosa y complicada
- Configuración de servicios replicada: problemas de sincronización
- Dificultad para balancear servicios que requieran autenticación: sin alta disponibilidad

Objetivo: centralizar la autenticación de usuarios

- NIS, NIS+: obsoletos

Objetivo: centralizar la autenticación de usuarios

- NIS, NIS+: obsoletos
- Bases de datos relacionales: PostGres, Oracle, MySQL . . . : no optimizados para lecturas

Objetivo: centralizar la autenticación de usuarios

- NIS, NIS+: obsoletos
- Bases de datos relacionales: PostGres, Oracle, MySQL . . . : no optimizados para lecturas
- Servicios de directorio: nis.schema (RFC 2307)

Objetivo: centralizar la autenticación de usuarios

- NIS, NIS+: obsoletos
- Bases de datos relacionales: PostGres, Oracle, MySQL . . . : no optimizados para lecturas
- Servicios de directorio: nis.schema (RFC 2307)
  - De pago: NDS, AD . . . ¿Por qué pagar . . . ?

Objetivo: centralizar la autenticación de usuarios

- NIS, NIS+: obsoletos
- Bases de datos relacionales: PostGres, Oracle, MySQL . . . : no optimizados para lecturas
- Servicios de directorio: nis.schema (RFC 2307)
  - De pago: NDS, AD . . . ¿Por qué pagar . . . ?
  - Gratuitas: iPlanet=Sun ONE Directory Server, solo gratuito para Solaris (hasta 200.000 DNs)

Objetivo: centralizar la autenticación de usuarios

- NIS, NIS+: obsoletos
- Bases de datos relacionales: PostGres, Oracle, MySQL . . . : no optimizados para lecturas
- Servicios de directorio: nis.schema (RFC 2307)
  - De pago: NDS, AD . . . ¿Por qué pagar . . . ?
  - Gratuitas: iPlanet=Sun ONE Directory Server, solo gratuito para Solaris (hasta 200.000 DNs)
  - GPL: OpenLDAP

OpenLDAP

- Libre. Código fuente disponible.

OpenLDAP

- Libre. Código fuente disponible.
- Amplio uso y amplia documentación (HOWTOs, FAQs, foros,. . .)

OpenLDAP

- Libre. Código fuente disponible.
- Amplio uso y amplia documentación (HOWTOs, FAQs, foros,. . .)
- Abundancia de schemas para distintos servicios: autenticación, DNS, correo, web, samba . . .

OpenLDAP

- Libre. Código fuente disponible.
- Amplio uso y amplia documentación (HOWTOs, FAQs, foros,. . .)
- Abundancia de schemas para distintos servicios: autenticación, DNS, correo, web, samba . . .
- Replicación (alta disponibilidad)

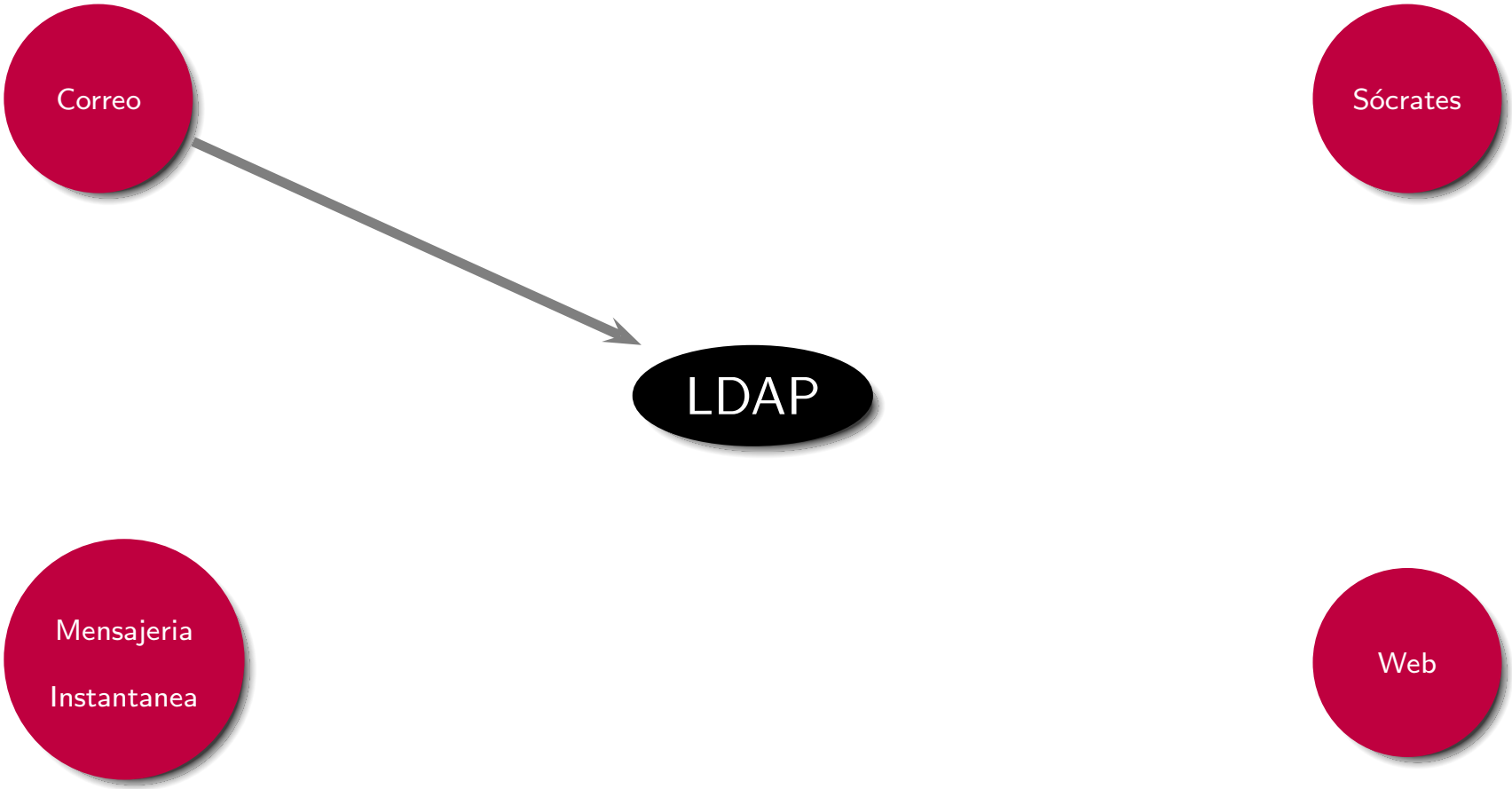
OpenLDAP

- Libre. Código fuente disponible.
- Amplio uso y amplia documentación (HOWTOs, FAQs, foros,. . .)
- Abundancia de schemas para distintos servicios: autenticación, DNS, correo, web, samba . . .
- Replicación (alta disponibilidad)
- Integración con otros servicios de directorio usados en la UMU: AD, NDS

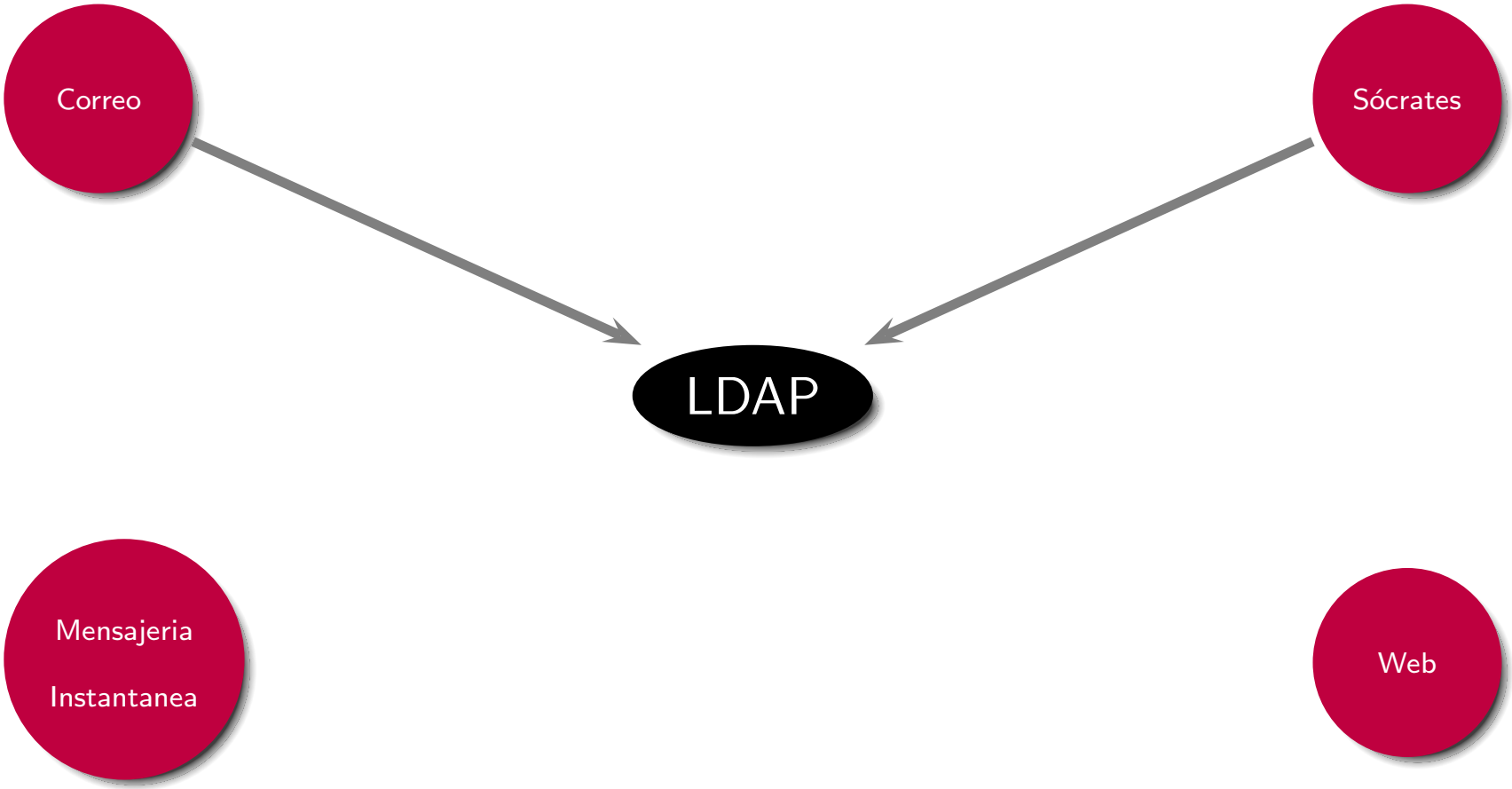
Índice

LDAP en el centro: servicio crítico

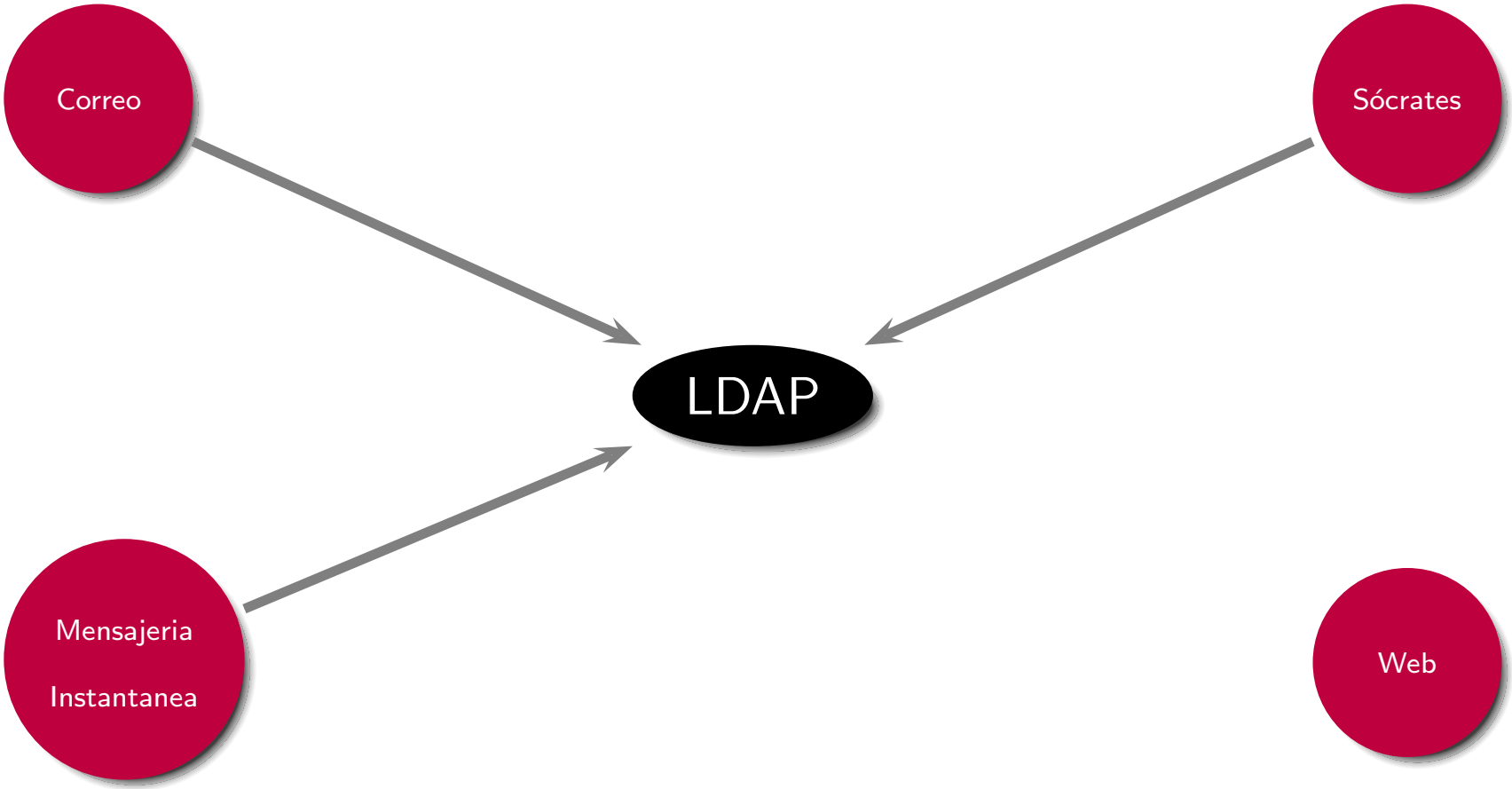
LDAP en el centro: servicio crítico



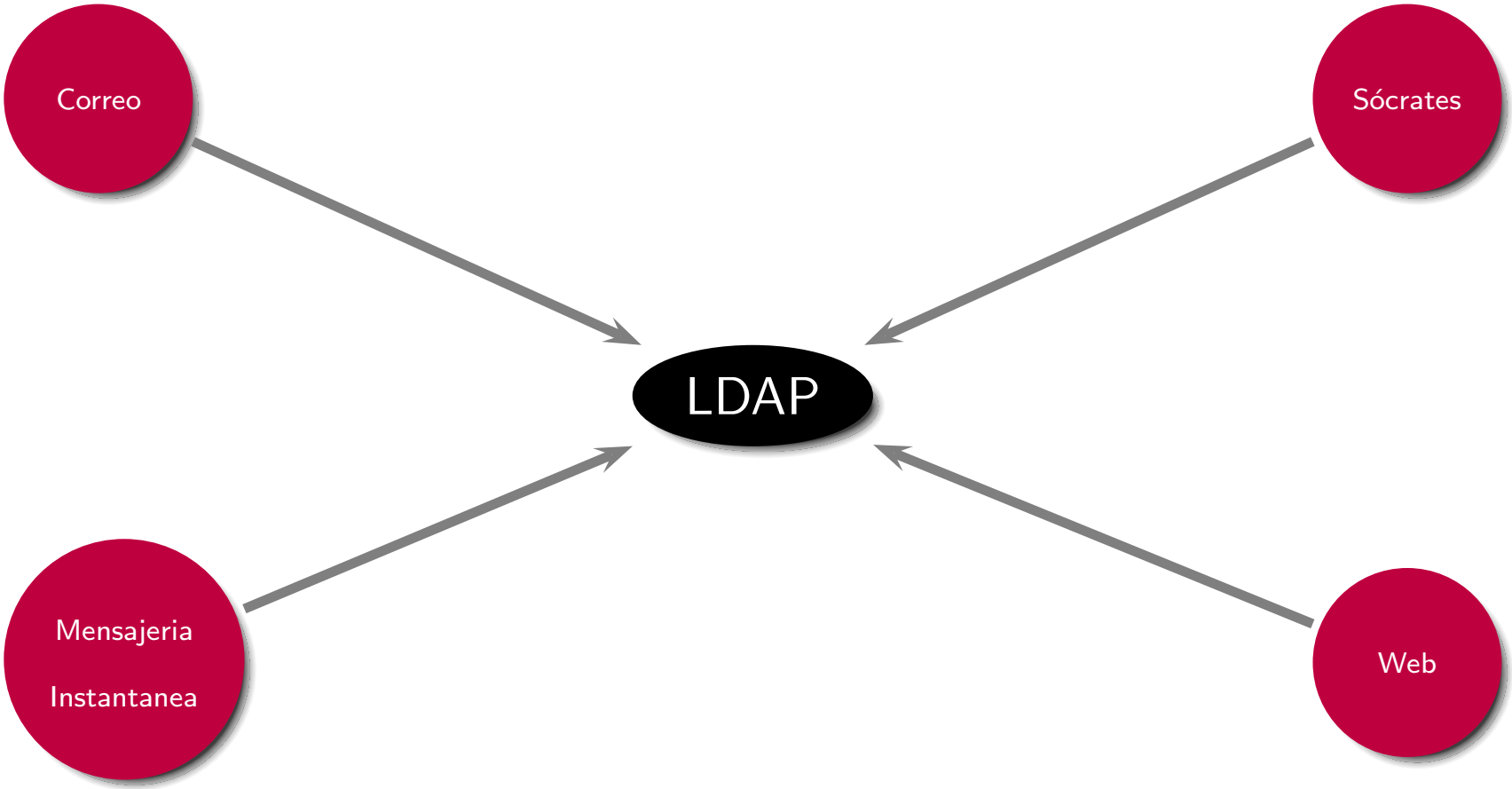
LDAP en el centro: servicio crítico



LDAP en el centro: servicio crítico



LDAP en el centro: servicio crítico



Cluster

- Instalar 2 o más servidores idénticos, con SW de cluster (heartbeat en GNU/Linux, por ejemplo)

Cluster

- Instalar 2 o más servidores idénticos, con SW de cluster (heartbeat en GNU/Linux, por ejemplo)
- Problemas: desperdicio de recursos (dos servidores actuando como uno solo)

Balanceo

- Balanceo de carga

Balanceo

- Balanceo de carga
  - Instalar 2 o más servidores.

Balanceo

- Balanceo de carga
  - Instalar 2 o más servidores.
  - No tienen por qué ser idénticos.

Balanceo

- Balanceo de carga
  - Instalar 2 o más servidores.
  - No tienen por qué ser idénticos.
  - Balanceo de carga mediante DNS Round Robin: barato, poco flexible

Balanceo

- Balanceo de carga
  - Instalar 2 o más servidores.
  - No tienen por qué ser idénticos.
  - Balanceo de carga mediante DNS Round Robin: barato, poco flexible
  - Balanceo de carga mediante dispositivo dedicado: LVS (GNU/Linux), Alteon, ...
    - dirección IP virtual "del servicio"
    - se controlan las posibles caídas de los nodos balanceados
    - flexibilidad a la hora de balancear

Balanceo

- Balanceo de carga
  - Instalar 2 o más servidores.
  - No tienen por qué ser idénticos.
  - Balanceo de carga mediante DNS Round Robin: barato, poco flexible
  - Balanceo de carga mediante dispositivo dedicado: LVS (GNU/Linux), Alteon, ...
    - dirección IP virtual "del servicio"
    - se controlan las posibles caídas de los nodos balanceados
    - flexibilidad a la hora de balancear
  - Problema: mantener todos los directorios sincronizados

Balanceo

- Balanceo de carga
  - Instalar 2 o más servidores.
  - No tienen por qué ser idénticos.
  - Balanceo de carga mediante DNS Round Robin: barato, poco flexible
  - Balanceo de carga mediante dispositivo dedicado: LVS (GNU/Linux), Alteon, ...
    - dirección IP virtual "del servicio"
    - se controlan las posibles caídas de los nodos balanceados
    - flexibilidad a la hora de balancear
  - Problema: mantener todos los directorios sincronizados
  - Solución: replicación automática de actualizaciones

Balanceo + replicación (I)

- Replicación LDAP

Balanceo + replicación (I)

- Replicación LDAP
  - LDAP proporciona mecanismos de replicación

Balanceo + replicación (I)

- Replicación LDAP
  - LDAP proporciona mecanismos de replicación
  - Consigues directorio replicado

Balanceo + replicación (I)

- Replicación LDAP
  - LDAP proporciona mecanismos de replicación
  - Consigues directorio replicado
  - El balanceador proporciona una única dirección IP para el servicio de directorio

Balanceo + replicación (I)

- Replicación LDAP
  - LDAP proporciona mecanismos de replicación
  - Consigues directorio replicado
  - El balanceador proporciona una única dirección IP para el servicio de directorio
  - Las consultas funcionan perfectamente

Balanceo + replicación (I)

- Replicación LDAP
  - LDAP proporciona mecanismos de replicación
  - Consigues directorio replicado
  - El balanceador proporciona una única dirección IP para el servicio de directorio
  - Las consultas funcionan perfectamente
  - Problema: las actualizaciones pueden llegar a cualquier nodo (ciclos en la actualización)

Balanceo + replicación (I)

- Replicación LDAP
  - LDAP proporciona mecanismos de replicación
  - Consigues directorio replicado
  - El balanceador proporciona una única dirección IP para el servicio de directorio
  - Las consultas funcionan perfectamente
  - Problema: las actualizaciones pueden llegar a cualquier nodo (ciclos en la actualización)
  - Solución: hacer modificaciones en uno solo de los nodos

Balanceo + replicación (II)

- Uso de referals

Balanceo + replicación (II)

- Uso de referals
  - Nodo maestro y nodos esclavos

Balanceo + replicación (II)

- Uso de referals
  - Nodo maestro y nodos esclavos
  - Las actualizaciones solo se producen en el maestro

Balanceo + replicación (II)

- Uso de referals
  - Nodo maestro y nodos esclavos
  - Las actualizaciones solo se producen en el maestro
  - El maestro propaga las actualizaciones a los nodos esclavos

Balanceo + replicación (II)

- Uso de referals
  - Nodo maestro y nodos esclavos
  - Las actualizaciones solo se producen en el maestro
  - El maestro propaga las actualizaciones a los nodos esclavos
  - Si llega una petición a un esclavo, éste responde con un referal al cliente

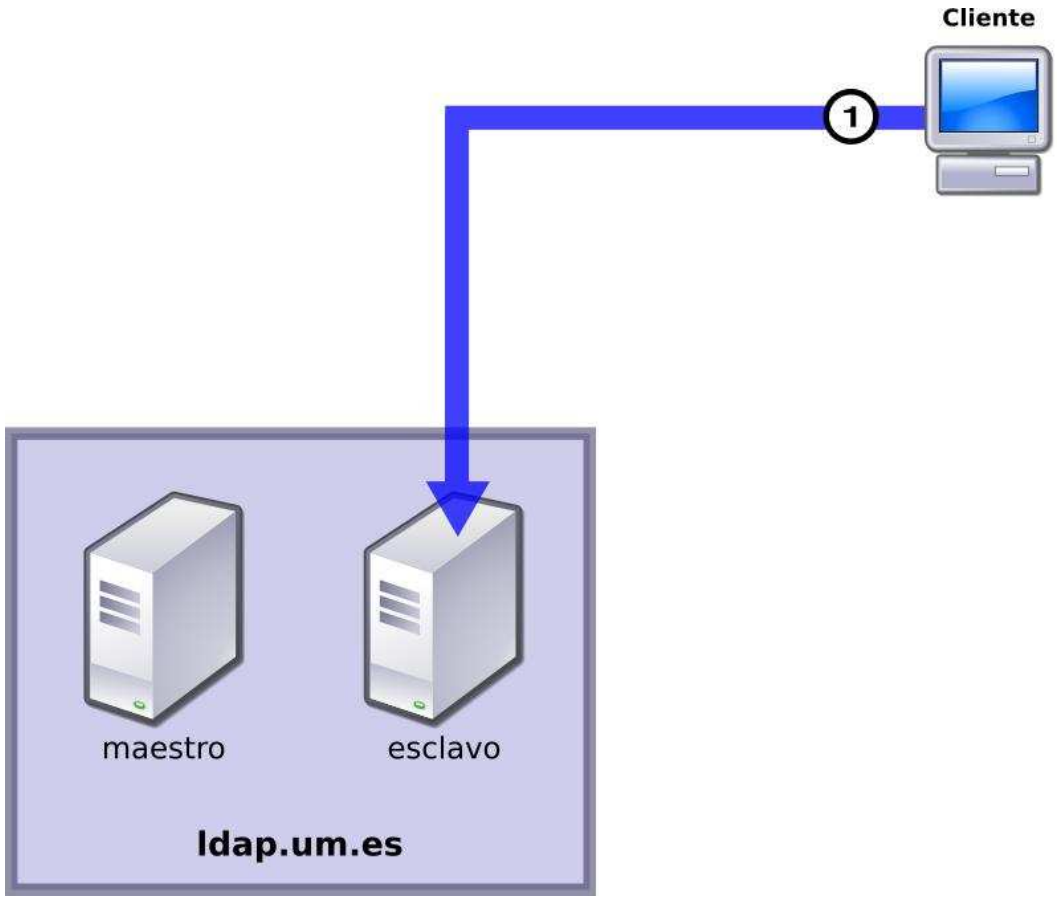
Balanceo + replicación (II)

- Uso de referals
  - Nodo maestro y nodos esclavos
  - Las actualizaciones solo se producen en el maestro
  - El maestro propaga las actualizaciones a los nodos esclavos
  - Si llega una petición a un esclavo, éste responde con un referal al cliente
  - El referal incluye la dirección IP real del maestro

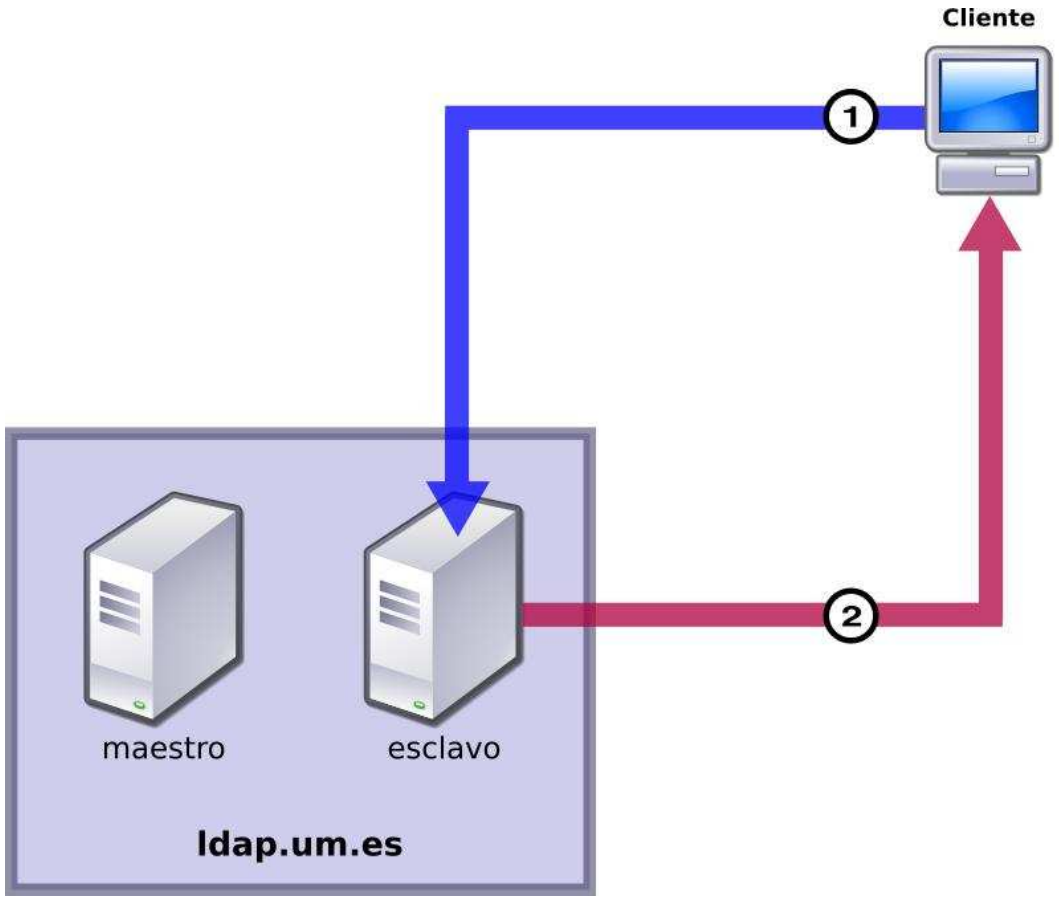
Balanceo + replicación (II)

- Uso de referals
  - Nodo maestro y nodos esclavos
  - Las actualizaciones solo se producen en el maestro
  - El maestro propaga las actualizaciones a los nodos esclavos
  - Si llega una petición a un esclavo, éste responde con un referal al cliente
  - El referal incluye la dirección IP real del maestro
  - El cliente vuelve a solicitar la actualización, pero esta vez al maestro

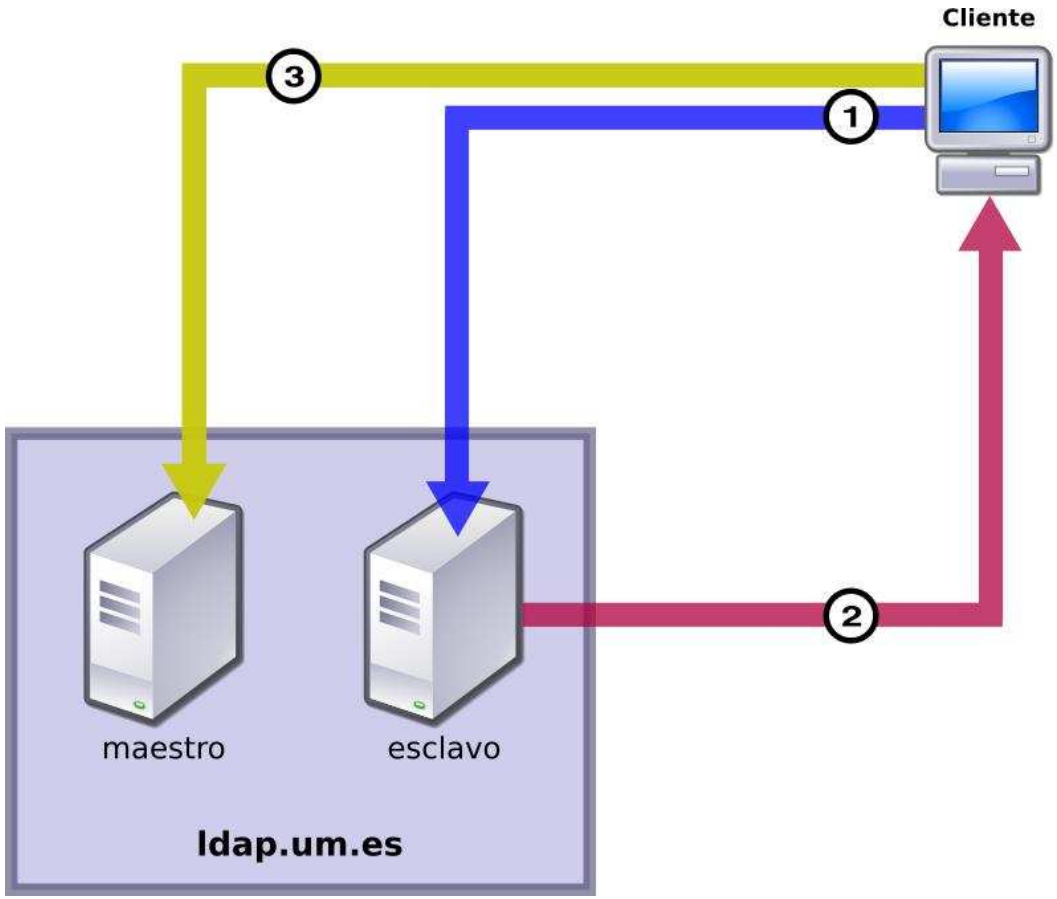
Balanceo + replicación (III)



Balanceo + replicación (III)



Balanceo + replicación (III)



Correo electrónico (I)

- LDAP para autenticar y balancear el acceso a los buzones

Correo electrónico (I)

- LDAP para autenticar y balancear el acceso a los buzones
- LDAP para autenticar el envío de mensajes (SASL)

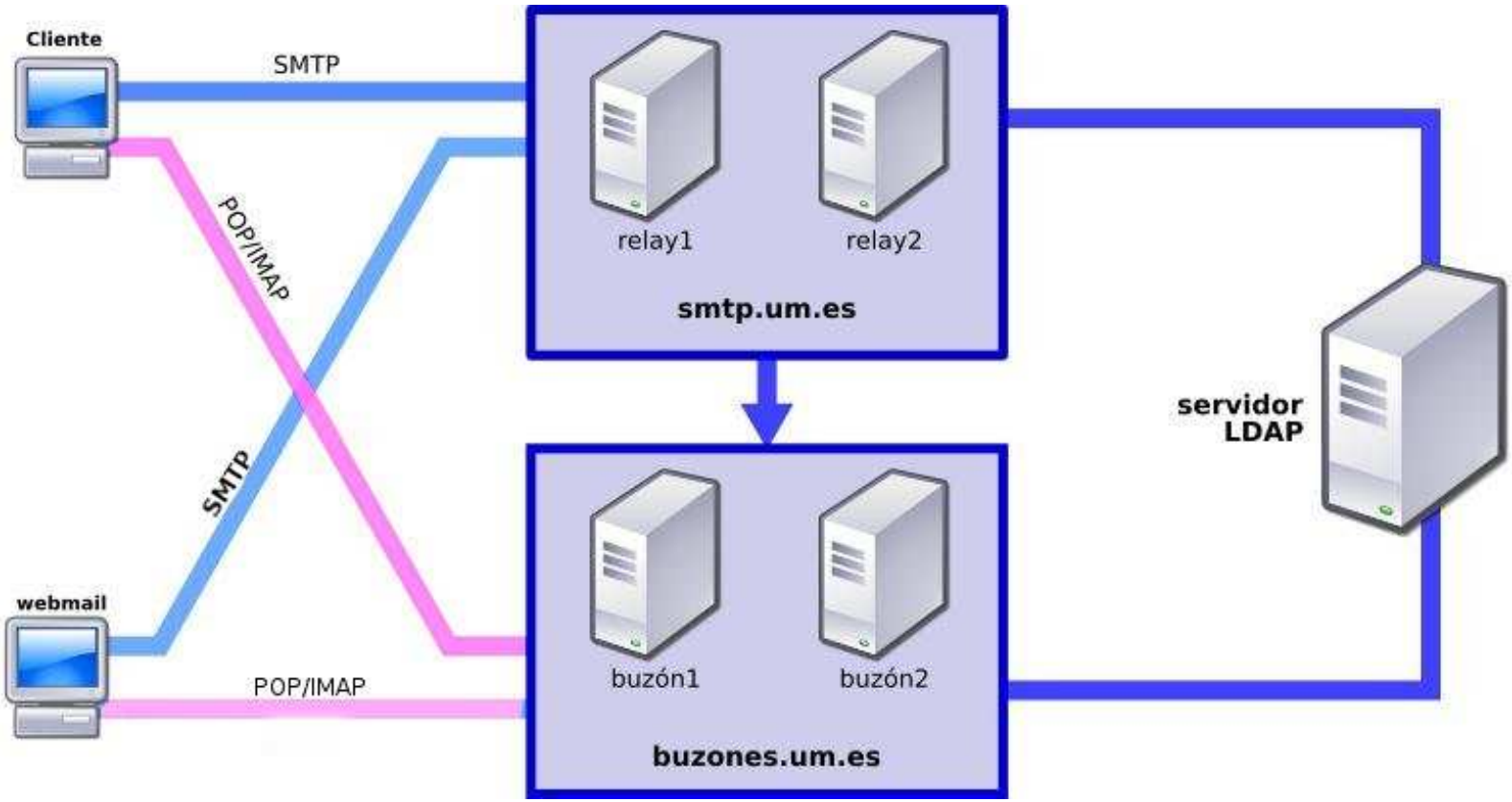
Correo electrónico (I)

- LDAP para autenticar y balancear el acceso a los buzones
- LDAP para autenticar el envío de mensajes (SASL)
- LDAP para guardar configuraciones de las estafetas

Correo electrónico (I)

- LDAP para autenticar y balancear el acceso a los buzones
- LDAP para autenticar el envío de mensajes (SASL)
- LDAP para guardar configuraciones de las estafetas
- LDAP para consultar direcciones de correo (y otra información pública)

Correo electrónico (II)



Descripción

PC's basados en software libre dentro de las aulas de la Universidad de Murcia, de tal forma que el profesorado cuente con la posibilidad de trabajar de forma remota desde cualquier lugar y con su material.

Solución

- Servidor
- Cliente

Solución

- Servidor
  - SAMBA-3 + OpenLDAP + smbldap-tools
- Cliente

Solución

- Servidor
  - SAMBA-3 + OpenLDAP + smbldap-tools
  - Software Libre
- Cliente

Solución

- Servidor
  - SAMBA-3 + OpenLDAP + smbldap-tools
  - Software Libre
- Cliente
  - Autenticación via LDAP

Solución

- Servidor
  - SAMBA-3 + OpenLDAP + smbldap-tools
  - Software Libre
- Cliente
  - Autenticación via LDAP
  - Debian GNU/Linux Sarge + Gnome 2.x

Solución

- Servidor
  - SAMBA-3 + OpenLDAP + smbldap-tools
  - Software Libre
- Cliente
  - Autenticación via LDAP
  - Debian GNU/Linux Sarge + Gnome 2.x
  - pam-mount

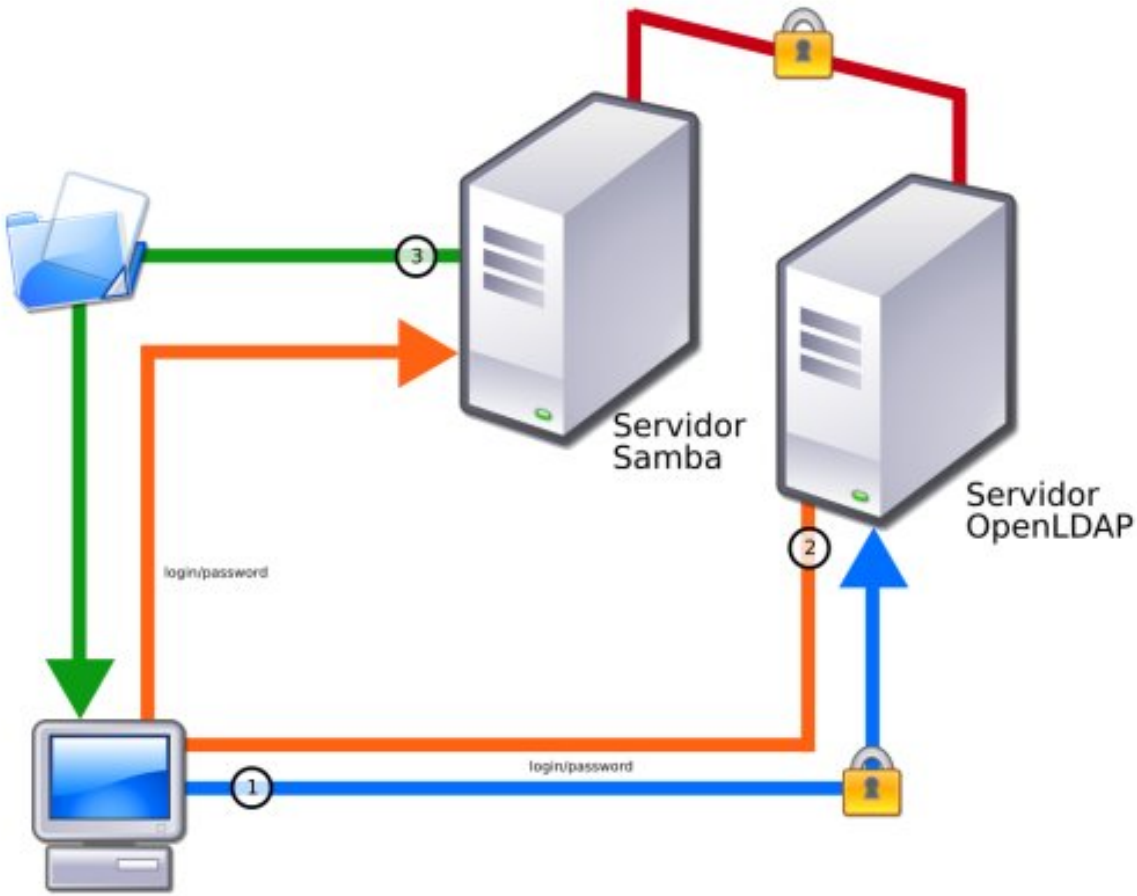
Solución

- Servidor
  - SAMBA-3 + OpenLDAP + smbldap-tools
  - Software Libre
- Cliente
  - Autenticación via LDAP
  - Debian GNU/Linux Sarge + Gnome 2.x
  - pam-mount
  - Transparente al usuario

Solución

- Servidor
  - SAMBA-3 + OpenLDAP + smbldap-tools
  - Software Libre
- Cliente
  - Autenticación via LDAP
  - Debian GNU/Linux Sarge + Gnome 2.x
  - pam-mount
  - Transparente al usuario
  - Integración GNU/Linux, MS Windows, MacOSX

Esquema


3
Servidor
Samba
Servidor
OpenLDAP
2
login/password
1
login/password

Descripción

- Basada en el protocolo Jabber

Descripción

- Basada en el protocolo Jabber
- Protocolo de intercambio de mensajes usando el estándar XML → Habilita la comunicación entre clientes de diferentes lenguajes (Java, C, . . .).

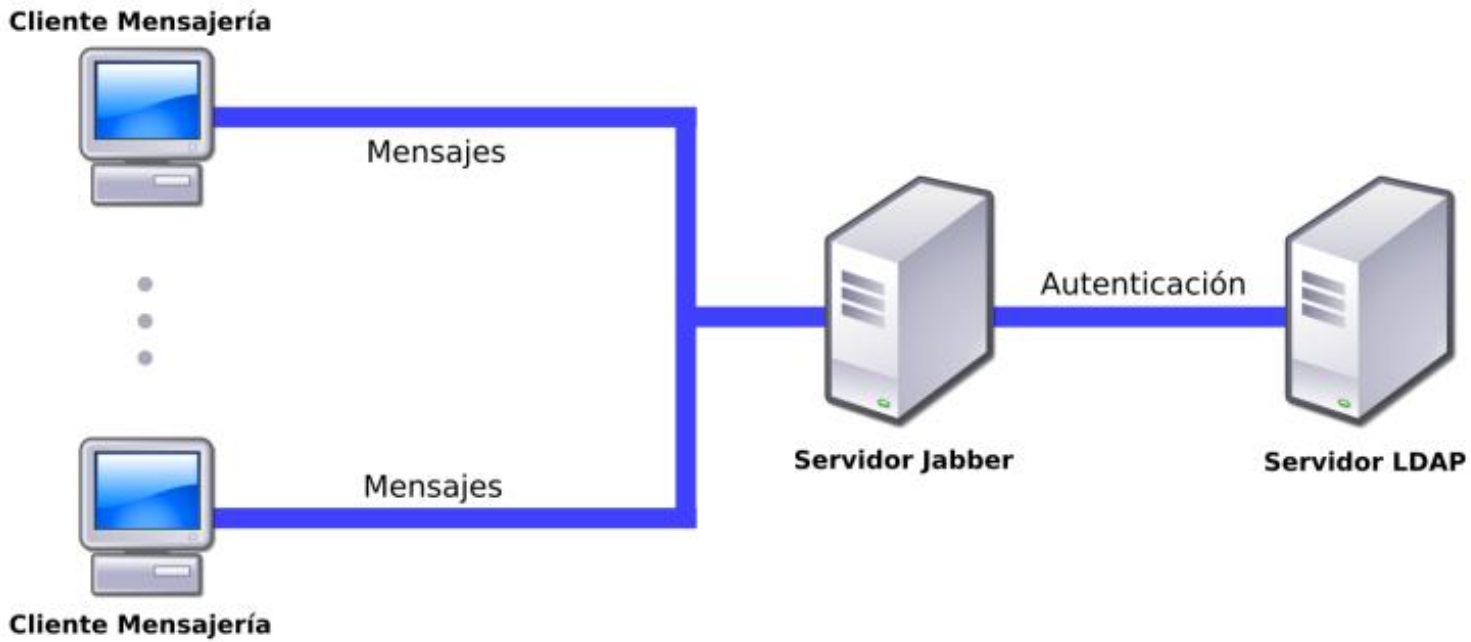
Descripción

- Basada en el protocolo Jabber
- Protocolo de intercambio de mensajes usando el estándar XML → Habilita la comunicación entre clientes de diferentes lenguajes (Java, C, . . .).
- Permite autenticación de usuarios usando LDAP.

Descripción

- Basada en el protocolo Jabber
- Protocolo de intercambio de mensajes usando el estándar XML → Habilita la comunicación entre clientes de diferentes lenguajes (Java, C, . . .).
- Permite autenticación de usuarios usando LDAP.
- Existen implementaciones de servidores y clientes con licencia GPL, facilitando la creación de código abierto.

Esquema


Cliente Mensajería
Mensajes
Mensajes
Cliente Mensajería
Servidor Jabber
Autenticación
Servidor LDAP

Autenticación LDAP en Apache

- The auth_ldap Module for Apache
  http://www.rudedog.org/auth_ldap/

Autenticación LDAP en Apache

- The auth_ldap Module for Apache
  http://www.rudedog.org/auth_ldap/
- Plataformas Unix y Windows NT

Autenticación LDAP en Apache

- The auth_ldap Module for Apache
  http://www.rudedog.org/auth_ldap/
- Plataformas Unix y Windows NT
- Características
  - Se puede especificar en: .htaccess, httpd.conf, ...
  - Permite políticas de autorización muy flexibles mediante filtros LDAP
  - Cachea las operaciones para incrementar rendimiento
  - Permite el uso de LDAP sobre SSL para evitar que no viaje en claro la clave hasta el ldap

Funcionamiento(I) – Autenticación

El módulo verifica que las credenciales presentadas son válidas. Los pasos son:

1. Se genera filtro combinando el "login" provisto por el usuario y la directiva AuthLDAPURL
2. Se busca en el directorio si devuelve una única entrada
3. Con la información anterior, procede a realizar la autenticación, bind, con la clave del usuario

Funcionamiento(II) – Autorización

Una vez autenticado el usuario, verifica que tiene permisos sobre el recurso permitiendonos las siguientes condiciones:

- Usuario válido:

```
AuthLDAPURL ldap://ldap1.um.es:389/ou=Usuarios,dc=um,dc=es?uid?sub?(objectClass=*)
require valid-user
```

- O que tenga determinado atributo (ejemplo Nivel Seguridad = TopSecret):

```
AuthLDAPURL ldap://ldap1.um.es/ou=Usuarios,dc=um,dc=es?uid?sub?(secLeve=TopSecret)
require valid-user
```

- O que perteneza a un grupo:

```
AuthLDAPURL ldap://ldap1.um.es/ou=Usuarios,dc=um,dc=es?uid?sub?(objectClass=*)
require group group cn=pings,ou=Groups,dc=um,dc=es
```

- ...

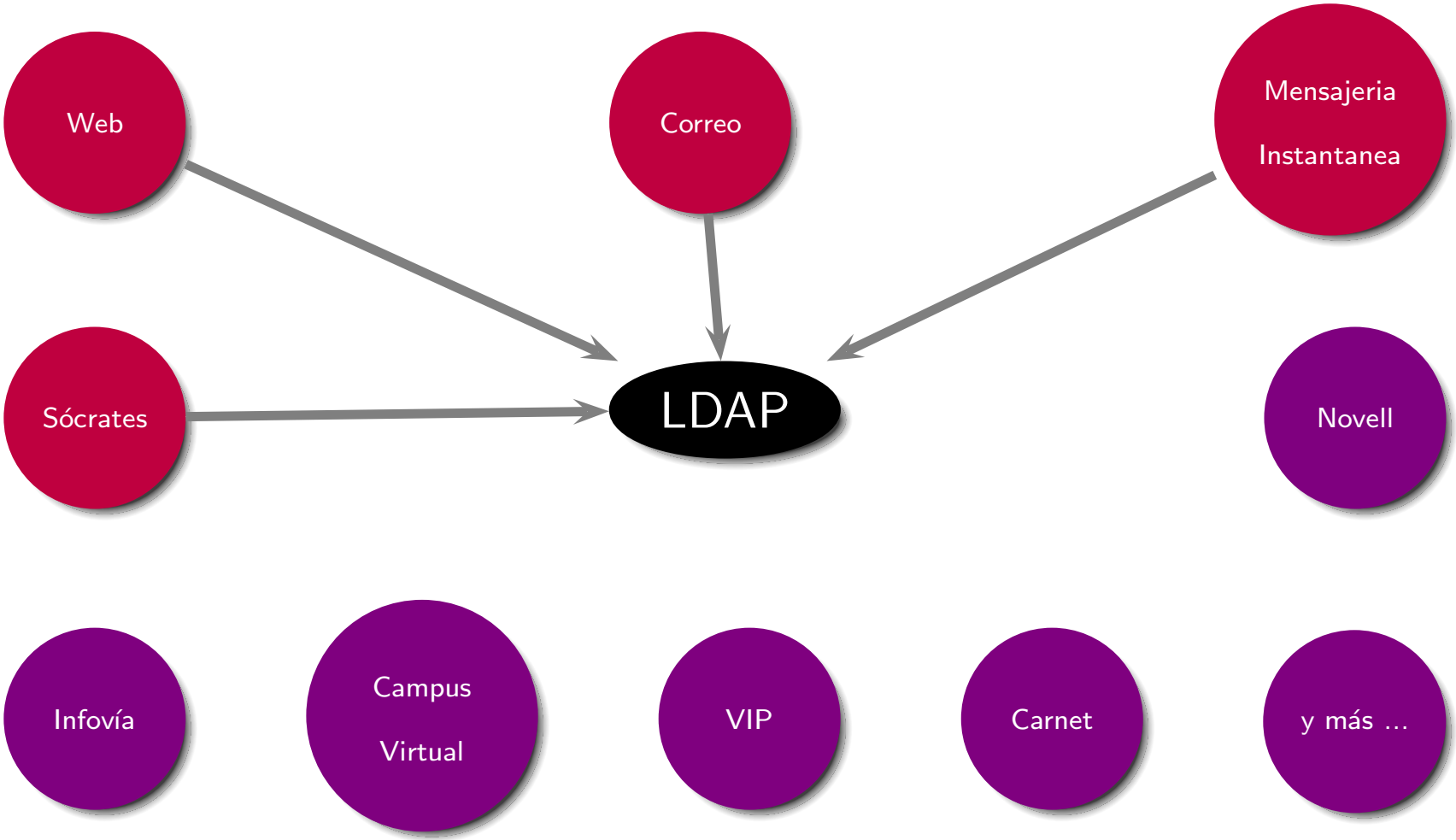
Ejemplo

Ejemplo

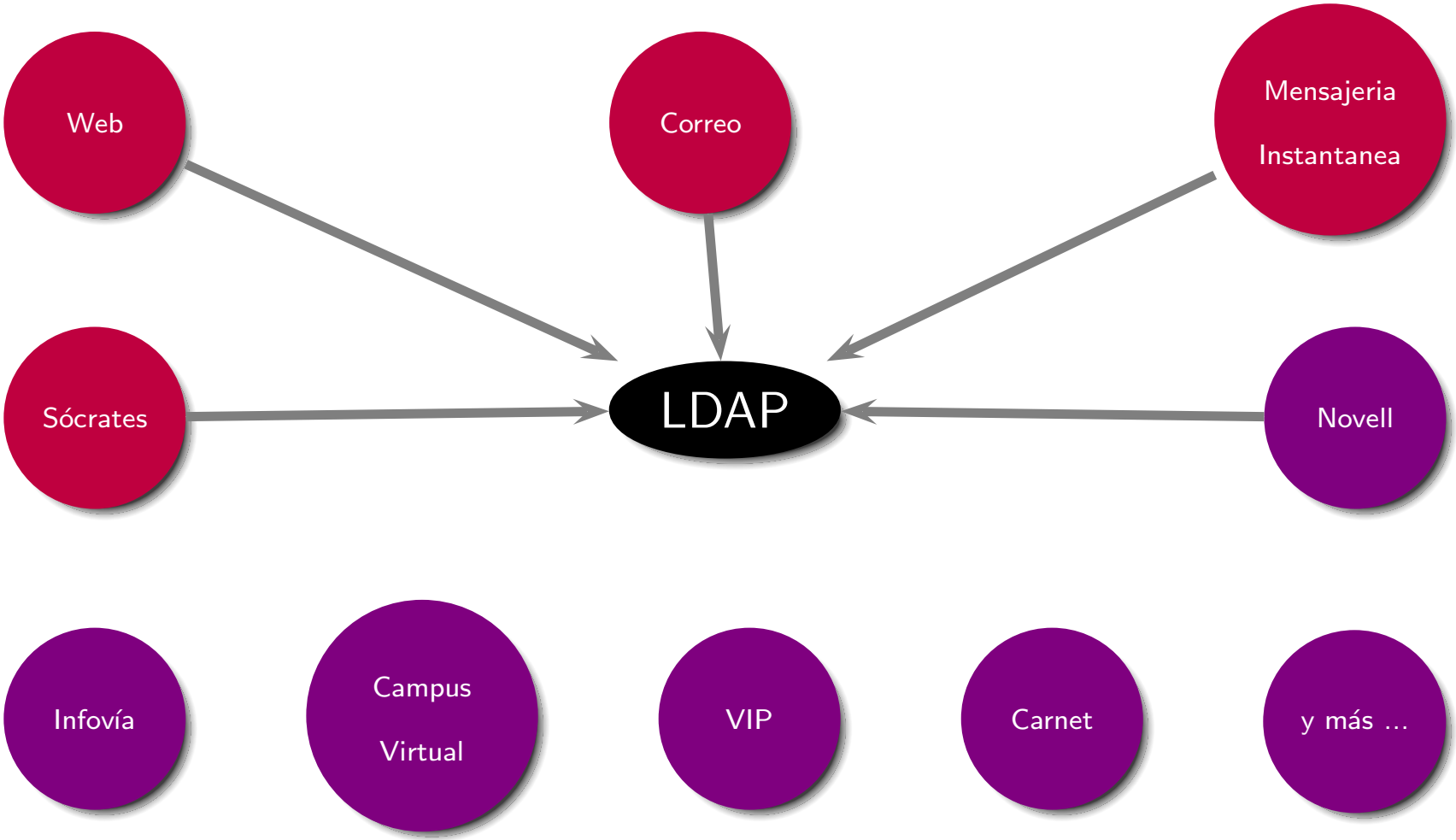
```
# Protección del acceso a las páginas de pings
<Directory /opt/scripts/pings>
        AllowOverride    AuthConfig
        Order            Allow,Deny
        Allow From       All
        AuthName         "Acceso a la página de pruebas"
        AuthType         Basic
        AuthLDAPURL      ldap://ldap1.um.es:389/ou=Usuarios,dc=um, \
        dc=es?uid?sub?(objectClass=*)
        AuthLDAPGroupAttributeIsDN       off
        AuthLDAPGroupAttribute  memberUid
        require group cn=pings,ou=Groups,dc=um,dc=es
</Directory>
```

Índice

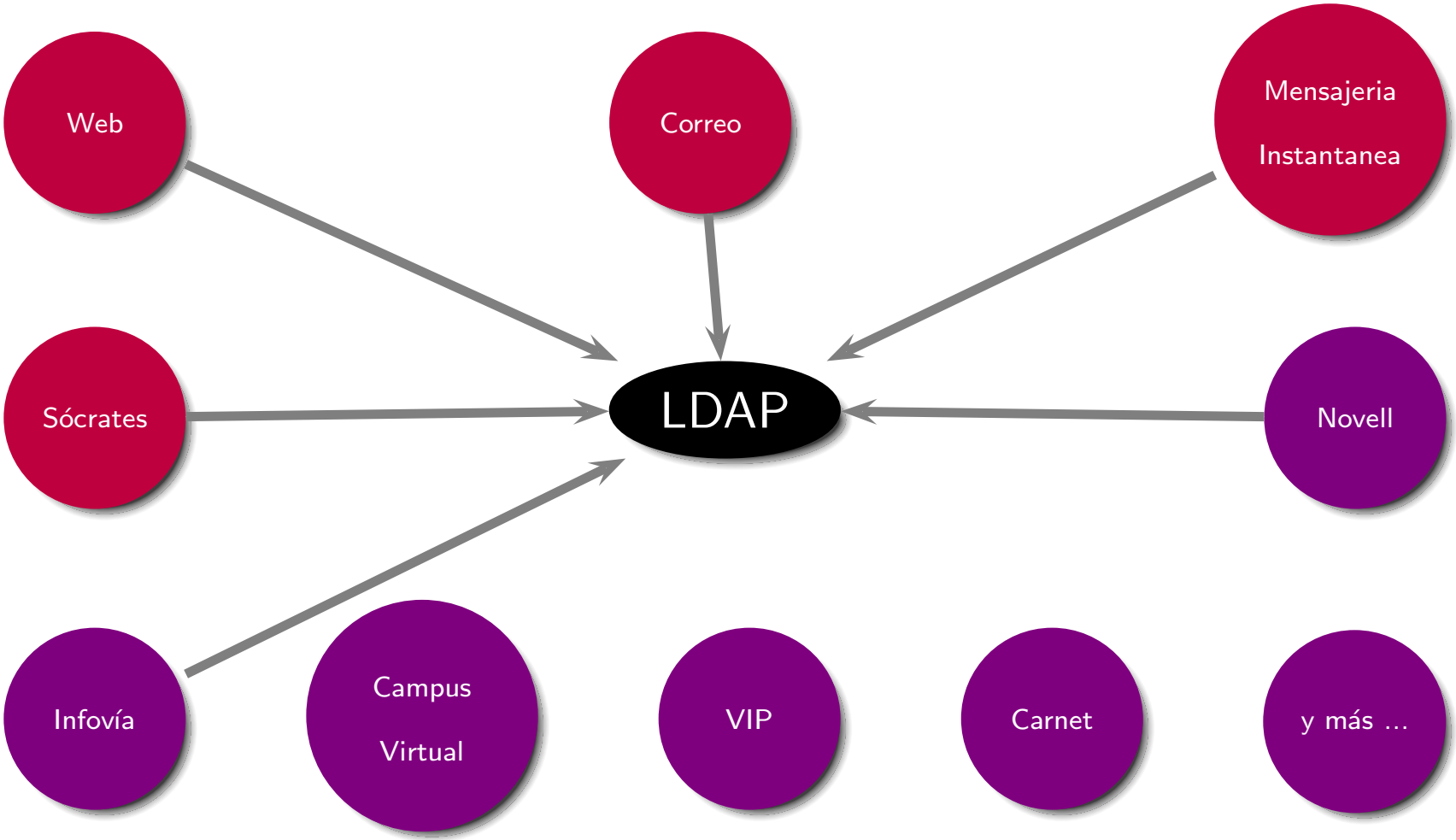
Seguiremos integrando servicios (I)



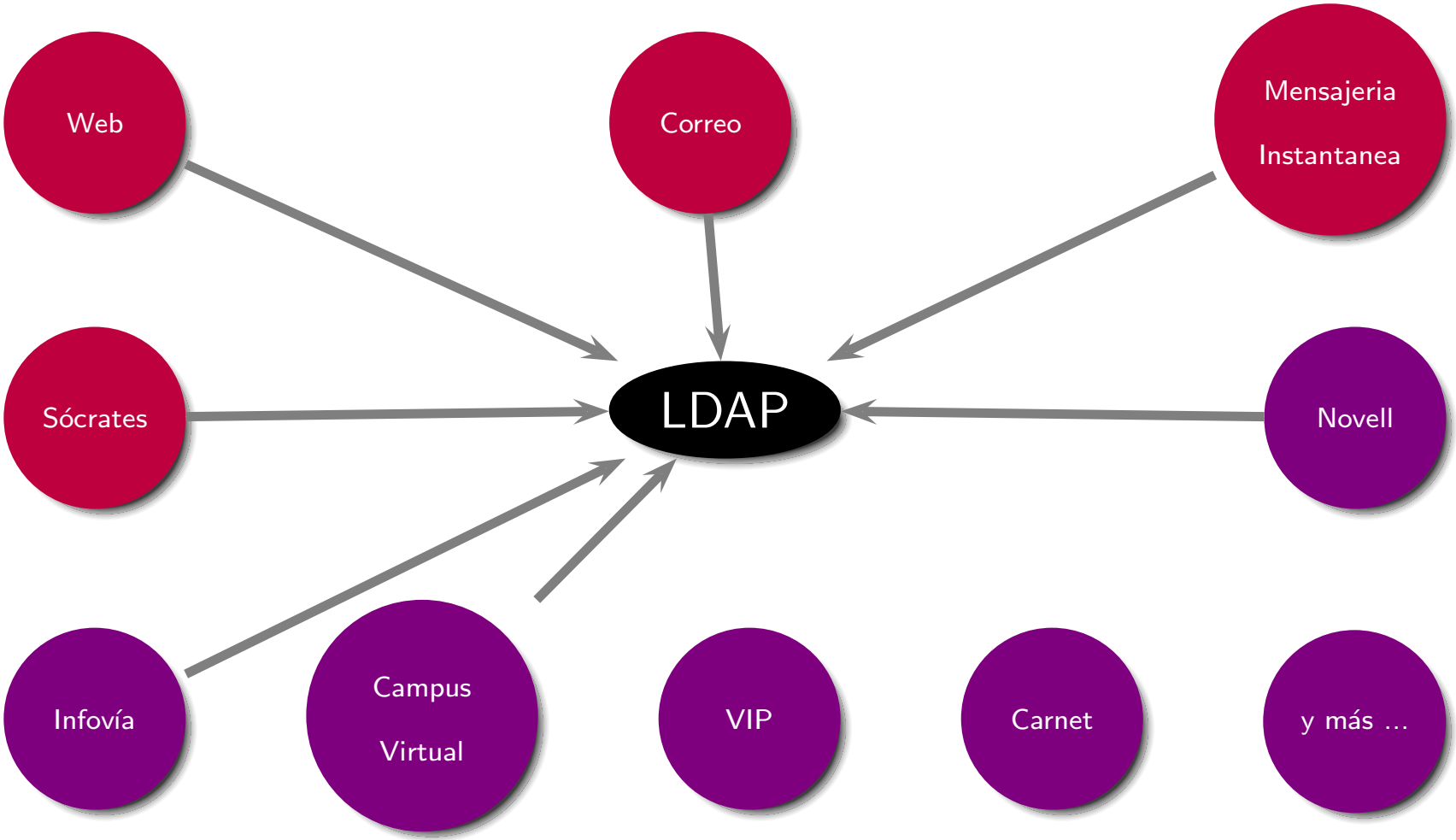
Seguiremos integrando servicios (I)



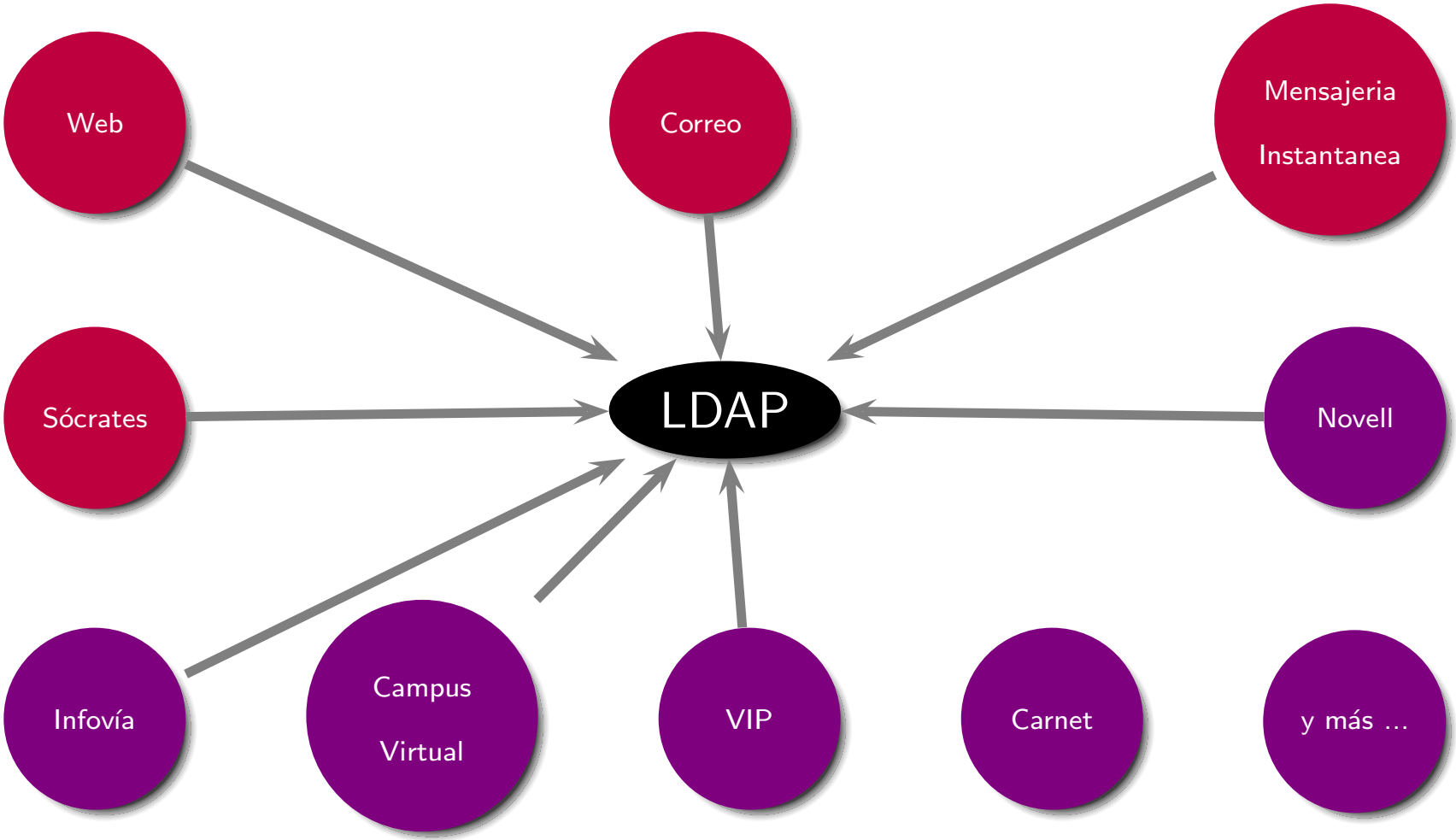
Seguiremos integrando servicios (I)



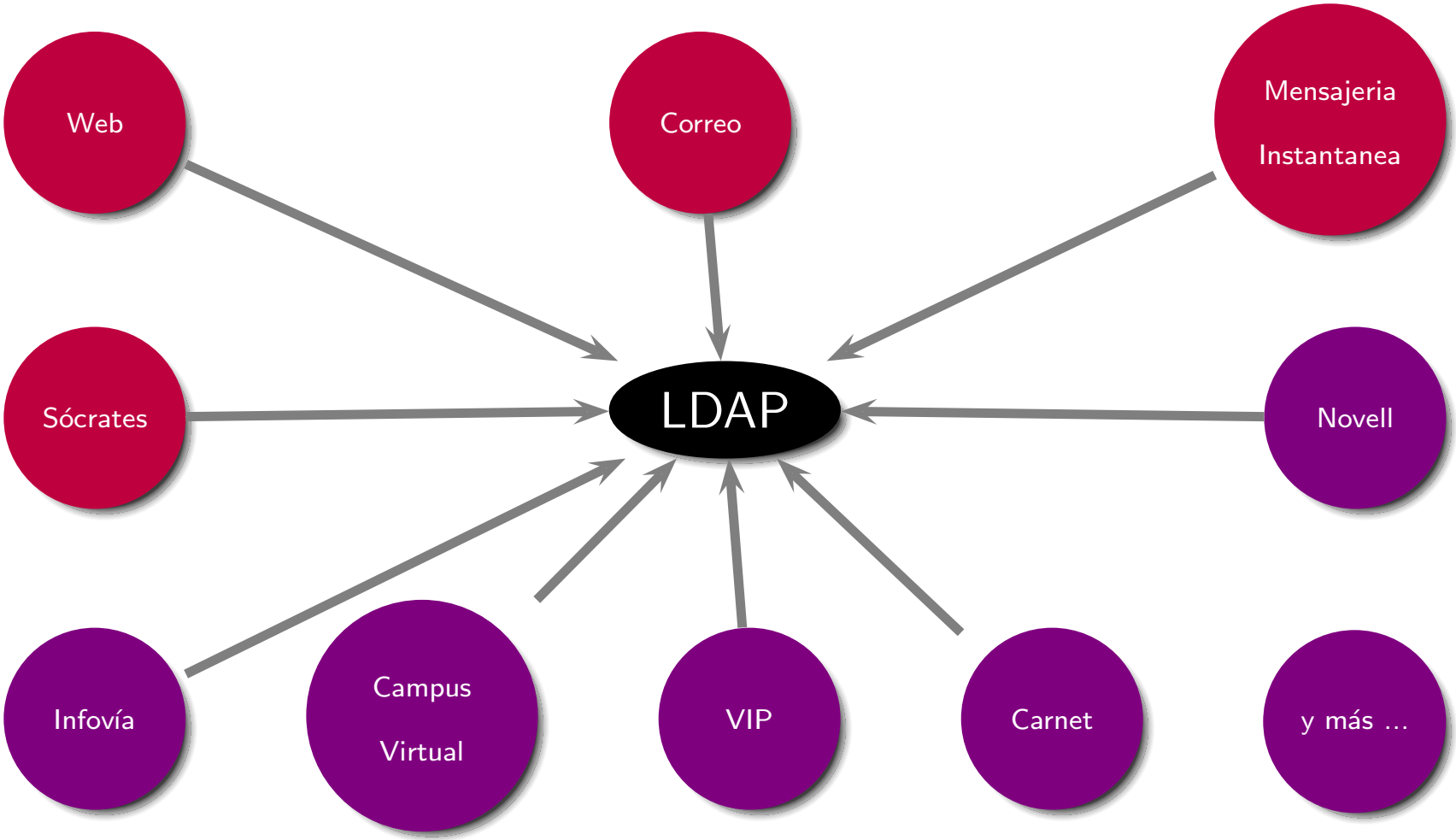
Seguiremos integrando servicios (I)



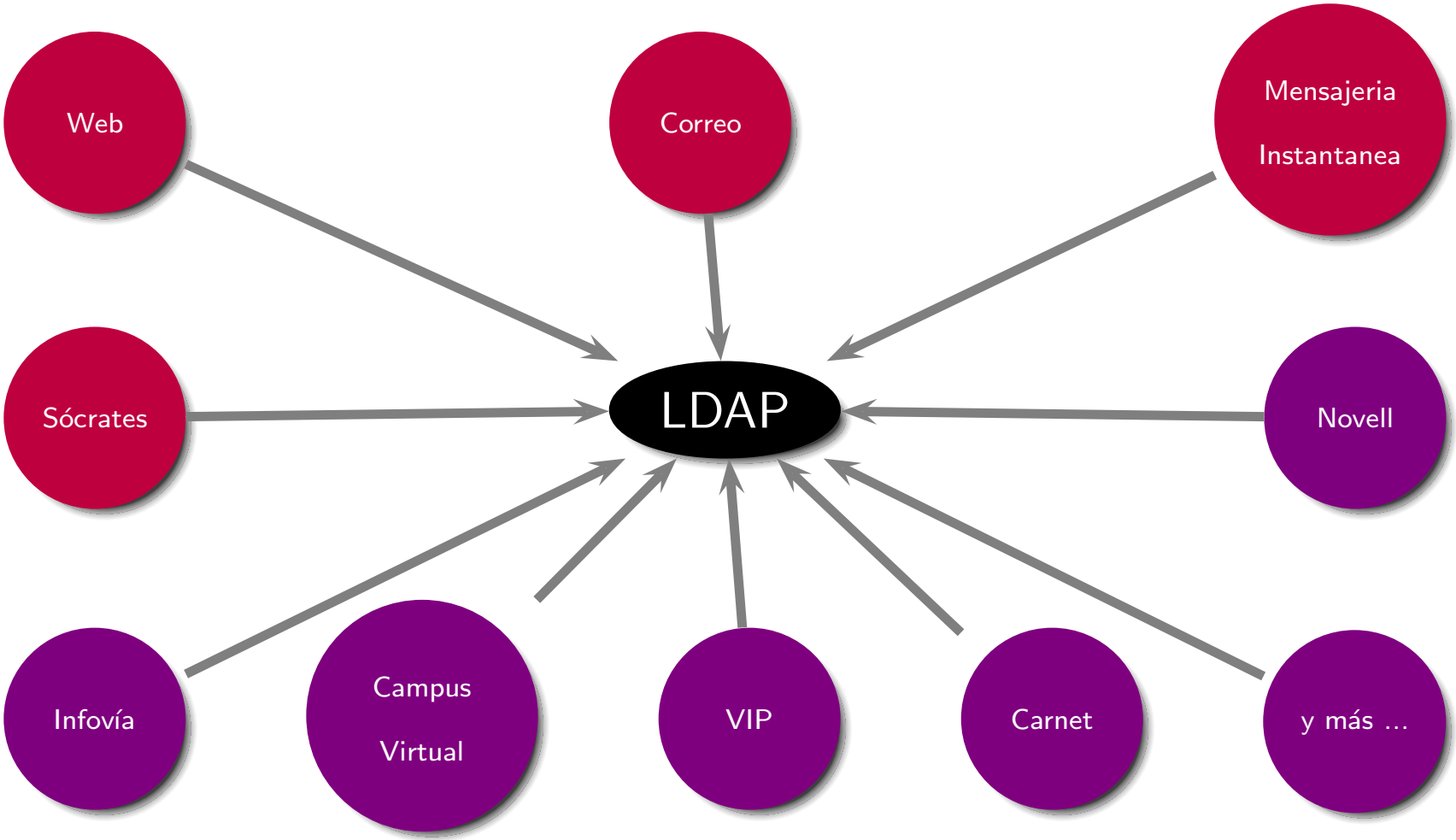
Seguiremos integrando servicios (I)



Seguiremos integrando servicios (I)



Seguiremos integrando servicios (I)



Seguiremos integrando servicios (II)

- Campus Virtual

Seguiremos integrando servicios (II)

- Campus Virtual
- Carnet inteligente

Seguiremos integrando servicios (II)

- Campus Virtual
- Carnet inteligente
- NDS de Novell

Seguiremos integrando servicios (II)

- Campus Virtual
- Carnet inteligente
- NDS de Novell
- VPN

Seguiremos integrando servicios (II)

- Campus Virtual
- Carnet inteligente
- NDS de Novell
- VPN
- DNS

Seguiremos integrando servicios (II)

- Campus Virtual
- Carnet inteligente
- NDS de Novell
- VPN
- DNS
- TIP (Telefonía IP)

¿Nuevos servicios y aplicaciones?

- Aplicación de gestión integral de usuarios de los servicios telemáticos

¿Nuevos servicios y aplicaciones?

- Aplicación de gestión integral de usuarios de los servicios telemáticos
- Sistemas de gestión de red (gestores de ancho de banda, . . .)

¿Nuevos servicios y aplicaciones?

- Aplicación de gestión integral de usuarios de los servicios telemáticos
- Sistemas de gestión de red (gestores de ancho de banda, . . .)
- Autenticar usuarios del resto de secciones de ATICA

¿Nuevos servicios y aplicaciones?

- Aplicación de gestión integral de usuarios de los servicios telemáticos
- Sistemas de gestión de red (gestores de ancho de banda, . . .)
- Autenticar usuarios del resto de secciones de ATICA
- VIP (Videovigilancia IP)

Índice

Conclusiones

- El directorio se constituye en un servicio horizontal básico para el acceso a los servicios

Conclusiones

- El directorio se constituye en un servicio horizontal básico para el acceso a los servicios
- También permite centralizar las configuraciones y dotar a los servicios de alta disponibilidad

Conclusiones

- El directorio se constituye en un servicio horizontal básico para el acceso a los servicios
- También permite centralizar las configuraciones y dotar a los servicios de alta disponibilidad
- Cohesiona a las distintas secciones y unidades de ATICA

Créditos

- Miguel A. García
  glax@um.es
- Francisco Javier García Ros
  jgarcia@um.es
- M. Antonia Martínez
  amart@um.es
- Angel L. Mateo
  amateo@um.es
- Javier Tavira
  jtavira@um.es
- Juan José Vidal
  juanjova@um.es
- Francisco Yepes
  pacoy@um.es