INFN-Laboratori
Nazionali di Frascati

COMINTATO UTENTI NOVENBRE 2003

PROGETTO DI UN'INFRASTRUTTURA DI DOMINIO WINDOWS SERVIZI ASSOCIATI

Novembre 2003

AMANZI NUNZIO – http://www.lnf.infn.it/~amanzi – nunzio.amanzi@lnf.infn.it – Phone 2607

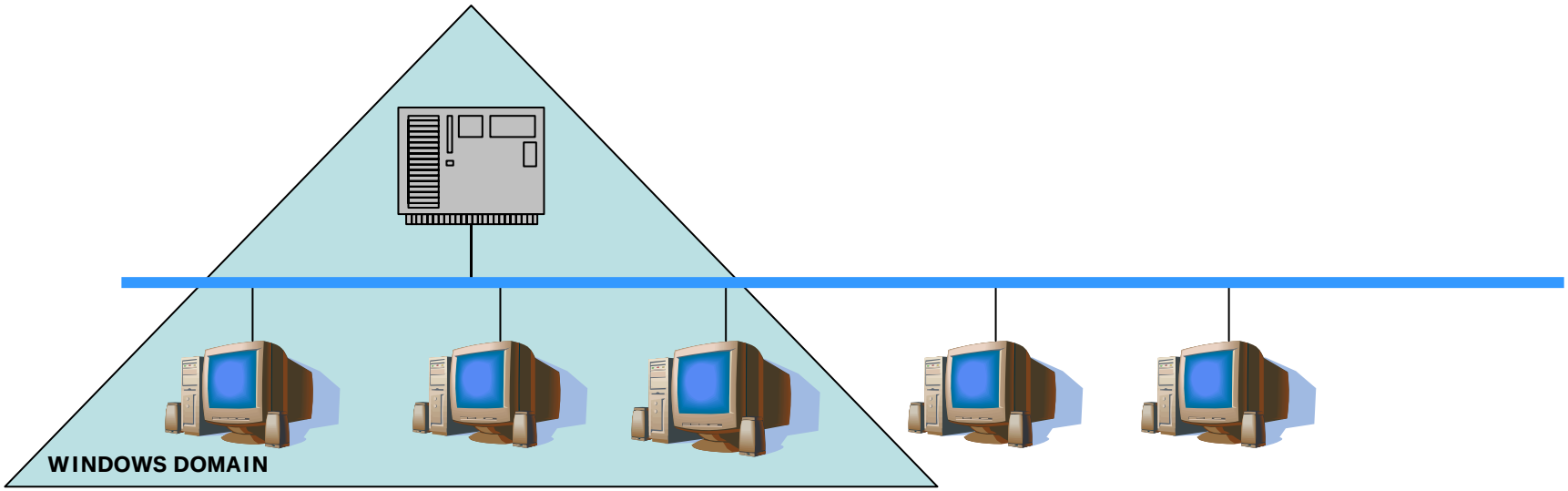
IL DOMINIO WINDOWS – CARATTERISTICHE INTRODUTTIVE

Un Dominio Windows e' un criterio logico di raggruppamento di oggetti, secondo un modello gerarchico, caratterizzato da:

- Un database di oggetti: computer, utenti, gruppi e unita' organizzative, politiche
- Un meccanismo di pubblicazione delle informazioni relativi agli oggetti che compongono il dominio
- Una politica di amministrazione, management e di autorita' delegate
- Un meccanismo di ereditarieta' e gerarchia di definizione e applicazione di regole (politiche di gruppo)

Esso definisce quindi un environment, ovvero un campo di azione

- Centralizzato, poiche' le definizioni e i processi di autenticazione si esplicano nell'ambito di un unico database denominato Active Directory, residente/replicato su uno o piu' servers (controllers)
- Distribuito, poiche' indipendentemente da dove si effettua il login nel dominio, si accede e si e' sottoposti sempre alle stesse politiche



DOMINIO W2K.LNF.INFN.IT

Presso i LNF – INFN risulta definito il dominio windows w2k.lnf.infn.it, attualmente in fase di configurazione e potenziamento i cui punti fondamentali sono:

1. L'implementazione di una infrastruttura di dominio
2. L'implementazione dei servizi
3. La pubblicazione delle informazioni e il supporto all'utenza

I principi in base ai quali l'utente windows puo' accedere, e quindi autenticarsi in un dominio, sono caratterizzati da:

- Aggangiare il proprio pc al dominio
- Avere un account utente di dominio

Essi costituiscono le basi per la definizione dell'infrastruttura, in termini di modello logico, del w2k.lnf.infn.it

INFRASTRUTTURA

Per infrastruttura di dominio windows si intende la definizione e l'implementazione di un modello basato su:

LA TOPOLOGIA OVVERO IL SITO

Essa e' definita dalla struttura di rete propria degli hosts che compongono il dominio, ed in particolare da:

- L'organizzazione della rete in una o piu' sottoreti
- La definizione di servers con funzioni di controllers
- La distribuzione/collocazione ottimale a livello IP degli hosts e in particolare dei controllers nelle sunbnets

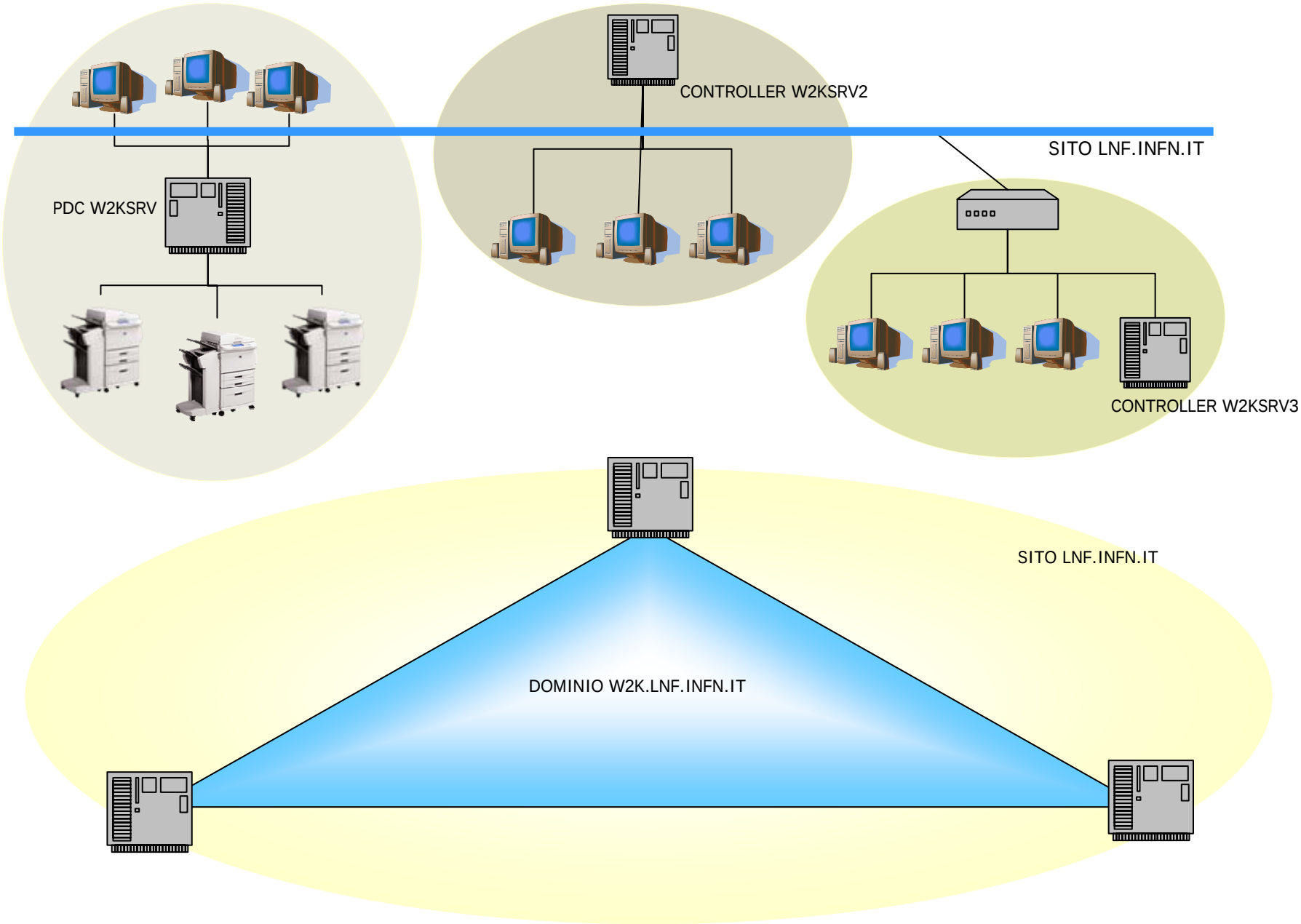
LA LOGICA E LA GERARCHIA DEGLI OGGETTI

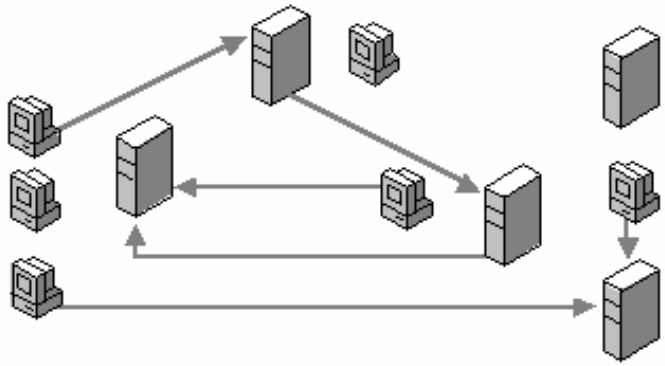
Questi aspetti, propri del dominio,rappresentano un modello di astrazione per il quale occorre:

- Definire gli account computer autorizzati ad essere membri del dominio
- Definire gli account utenti che possono autenticarsi nel dominio
- Definire i gruppi e i criteri di raggruppamento degli utenti per l'accesso alle risorse/servizi e in tal senso:

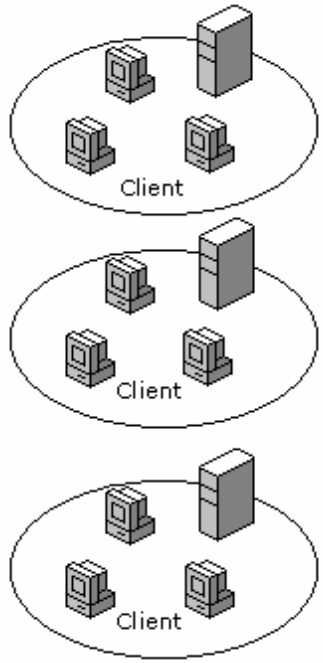
    - creare una struttura di privilegi e permessi (SACL e ACL) per l'accesso discrezionale
    - definire una strategia di applicazione di queste politiche (meccanismo di ereditarieta' e gerarchia)

- Definire le autorita' delegate al controllo e al management e gli strumenti di amministrazione
- Definire un sistema di monitoraggio dei servizi e delle piattaforme mediante logging e/o auditing

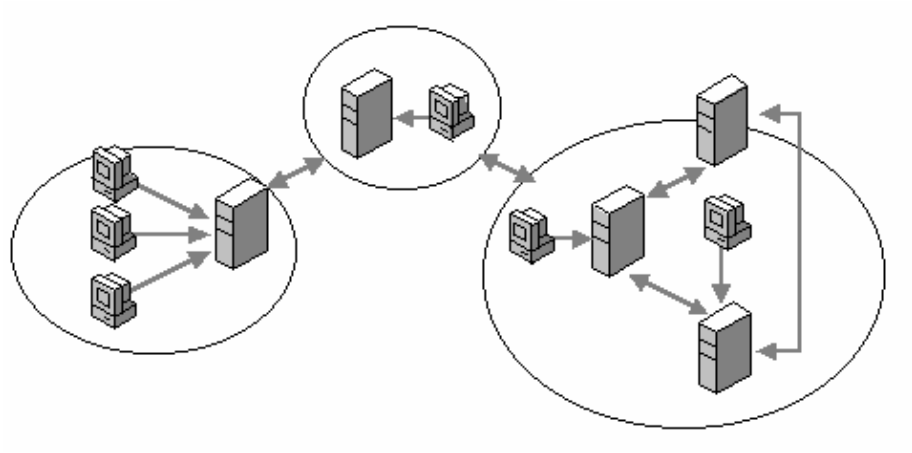

CONTROLLER W2KSRV2
SITO LNF.INFN.IT
PDC W2KSRV
CONTROLLER W2KSRV3
SITO LNF.INFN.IT
DOMINIO W2K.LNF.INFN.IT

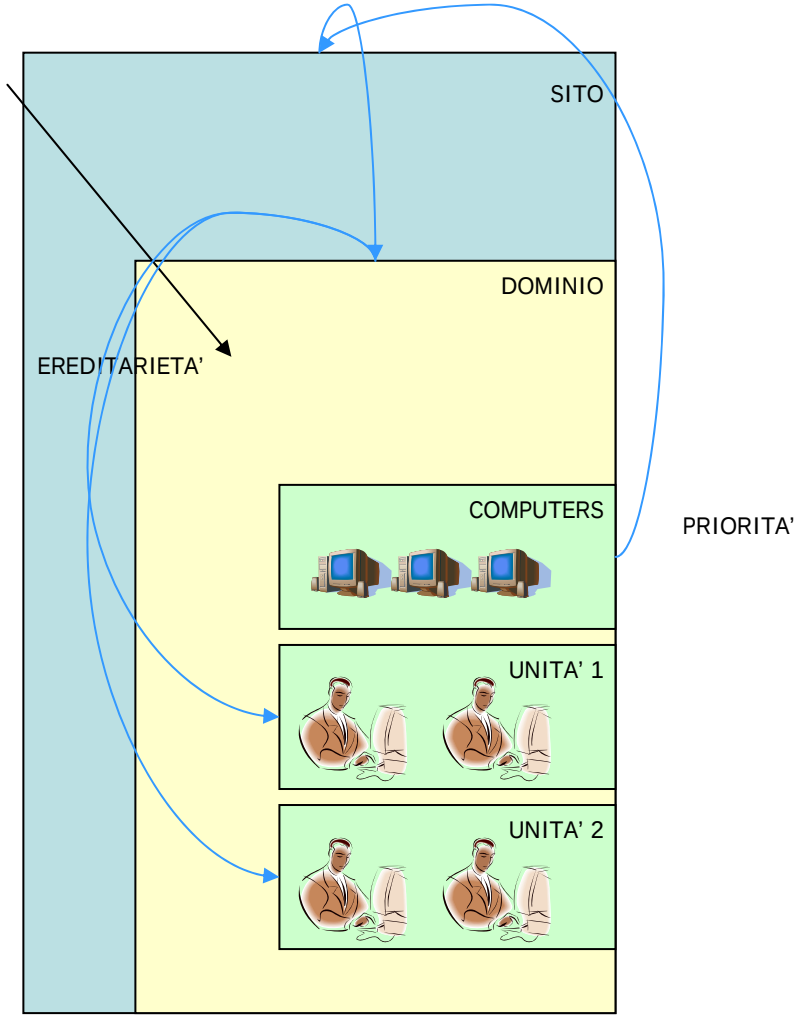


DOMINIO W2K – Situazione attuale: 1 PDC che serve un'unica subnet: lo scambio di informazioni e' caotico



DOMINIO W2K – Situazione futura: 1 PDC e controllers aggiuntivi distribuiti in subnets differenti ben connesse: l'intercambio delle informazioni e' efficiente





Organizzazione logica e gerarchica del dominio w2k.lnf.infn.it. Ogni strato costituisce un campo di azione per il quale sono definiti oggetti e politiche. Ogni oggetto sara' sottoposto ad una risultanza di criteri di impostazione e sicurezza derivanti dai valori che gli essi assumono ai layers superiori.

Alcuni motivi per autenticarsi nel Dominio W2K

- Autenticazione centralizzata, verifica identita' e ottenimento credenziali indipendentemente dai database locali
- Far parte di un environment efficiente e sicuro poiche' le impostazioni per il PC e l'utente sono definite sui servers di dominio e trasmesse ai client/utenti in fase di boot/login
- L'utente non deve eseguire manualmente le configurazioni di interesse generale perche' esse verranno ottenute automaticamente e/o a richiesta: es. la mappatura di una stampante di rete, la configurazione dei mounts points verso AFS, la definizione dei links alle url di rete e ai servizi
- Accedere alle risorse/servizi di dominio senza doversi ogni volta autenticare
- Accedere in netbios al File System Distribuito dello storage Windows
- La possibilita' di accedere al proprio environment Windows (Impostazioni Desktop, link ad AFS, cartella Documenti, bookmarks dovunque e comunque mantenendo le stesse impostazioni
- Un servizio di supporto ed amministrazione piu' snello ed efficiente poiche' basato su un modello centralizzato

SERVIZI E SUPPORTO

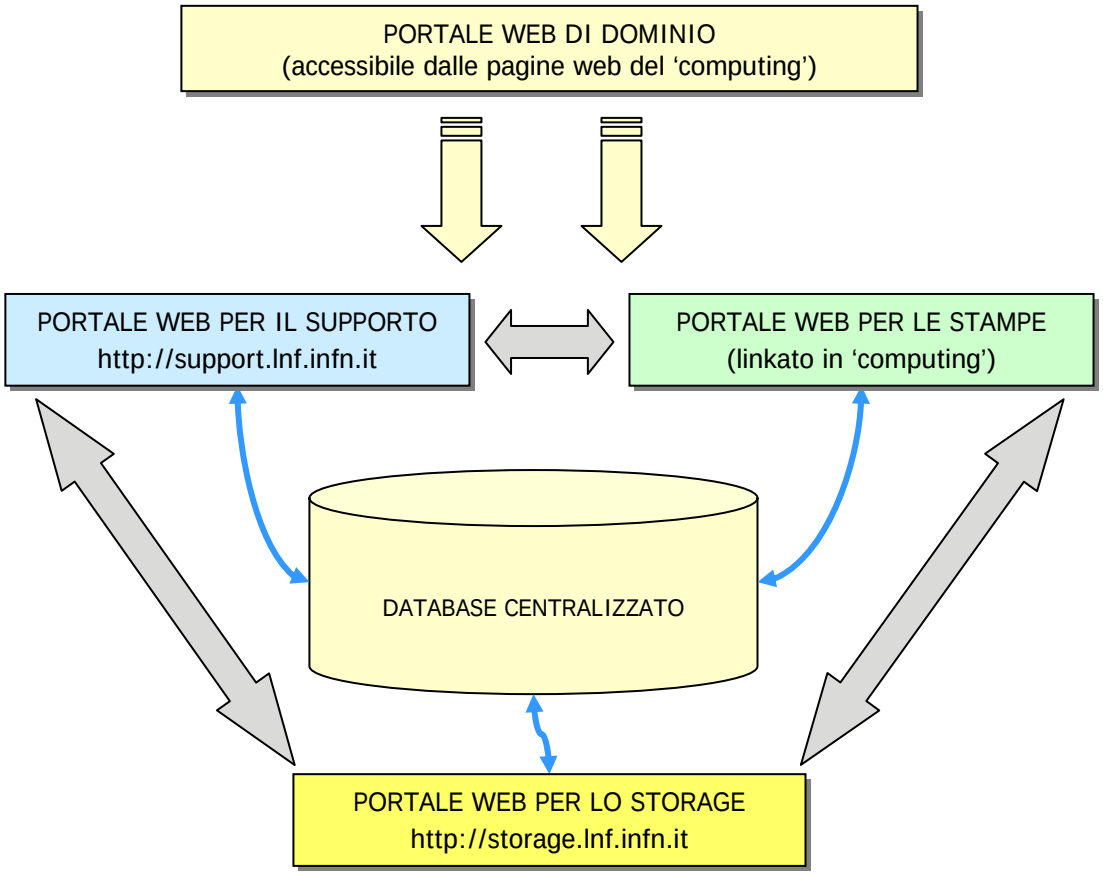
Nell'infrastruttura di Dominio illustrata, intesa sia come struttura fisica che come environment logico, sono previsti i seguenti servizi:

Servizio di login interattivo ad un desktop windows, roaming e puntamento di AFS	**In allestimento**
Servizio di stampa centralizzato	**In potenziamento**
Servizio di storage windows distribuito	**Completo**
Servizio di supporto all'utenza	**Completo**
Servizio generale di informazione e news per il dominio W2k	**In allestimento**

L'approccio alla definizione dei servizi e' caratterizzato da:

- adottare criteri di ridondanza e bilanciamento del carico tra i servers
- eseguire l'implementazione dando particolare rilievo all'informazione e supporto all'utenza

Quest'ultimo obiettivo e' stato perseguito implementando un modello relazionale di servizio globale basato su portali web.

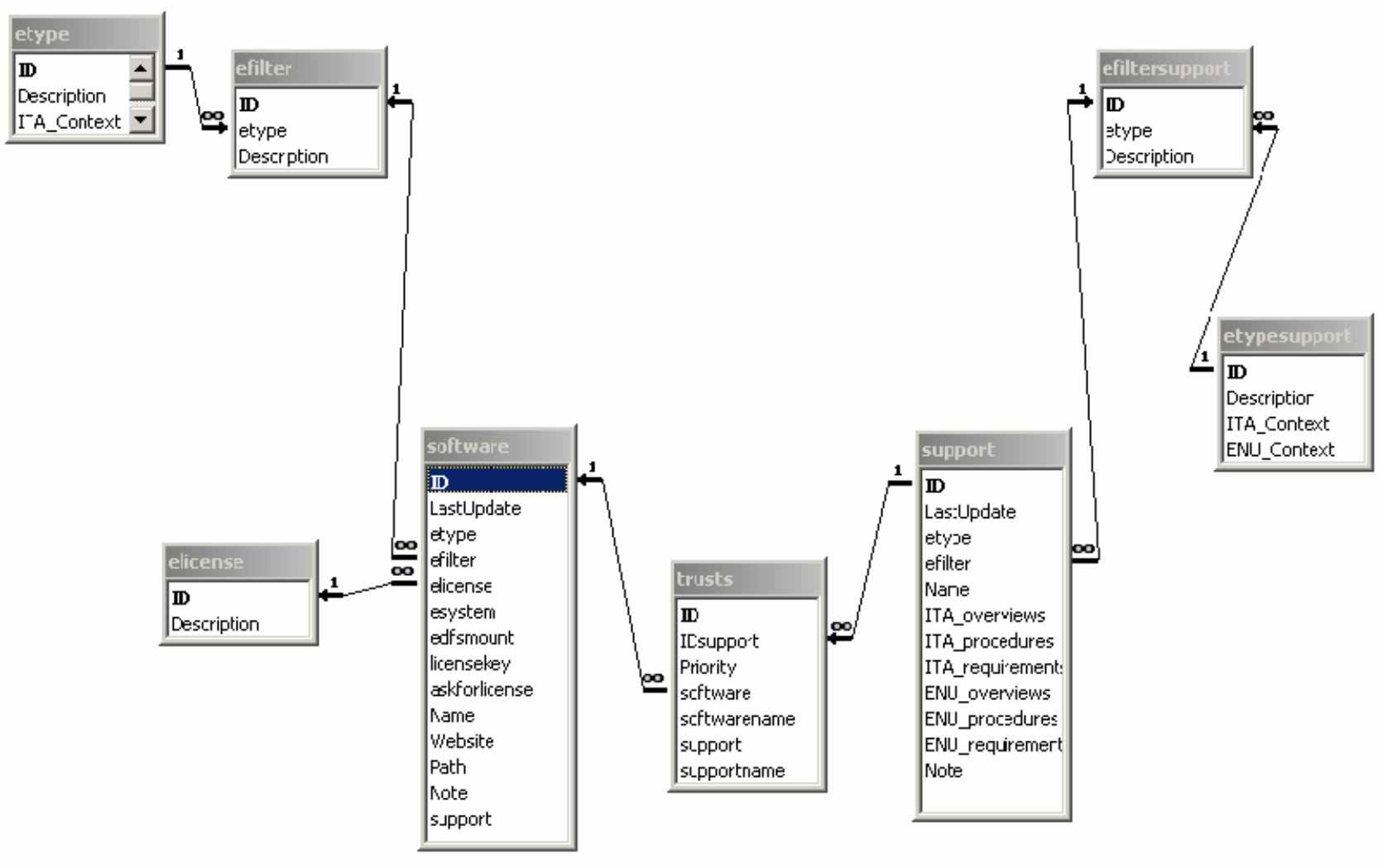


Le pagine web dei portali sono collegate reciprocamente in virtu' delle relazioni definite nel database.

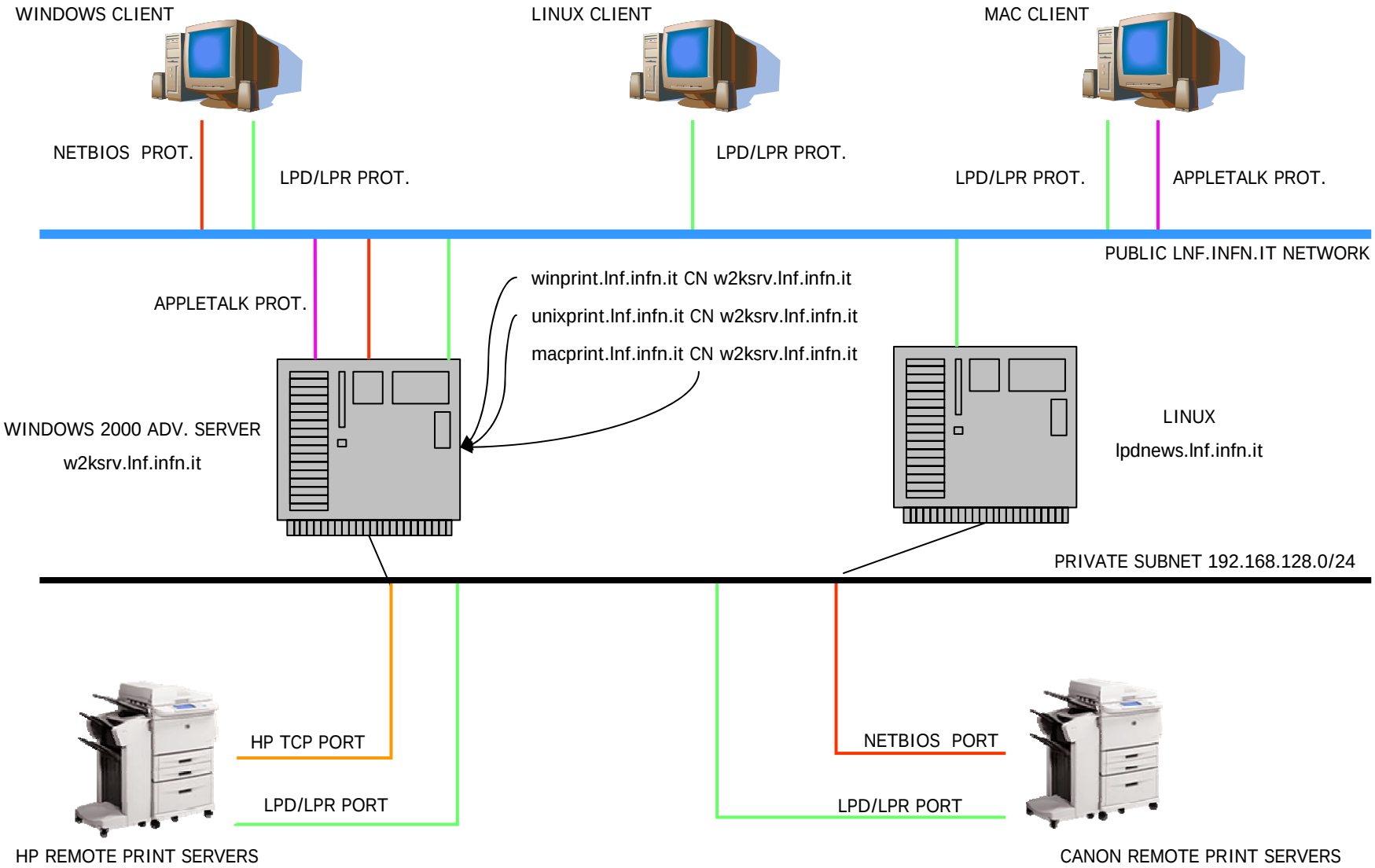
In tal senso:

- Un portale interroga il database e ottiene le informazioni per visualizzare una pagina di contesto.
- Queste informazioni contengono anche i riferimenti ad altri oggetti di database relative ad altri portali e correlate al contesto corrente

Per esempio, l'utente puo' ottenere supporto su un determinato argomento accedendo alle pagine web che distribuiscono il software corrispondente e viceversa.


etype
ID
Description
ITA_Context
efilter
ID
etype
Descr ption
efiltersupport
ID
etype
Description
etypesupport
ID
Description
ITA_Context
ENU_Context
elicense
ID
Description
software
ID
LastUpdate
etype
efilter
elicense
esystem
edfsmount
licensekey
askforlicense
Name
Website
Path
Note
support
trusts
ID
IDsupport
Priority
scftware
scftwarename
support
supportname
support
ID
Las:Update
etype
efilter
Name
ITA_overviews
ITA_procedures
ITA_requirements
ENU_overviews
ENU_procedures
ENU_requirement
Note

SCHEMA DEL SERVIZIO DI STAMPA CENTRALIZZATO

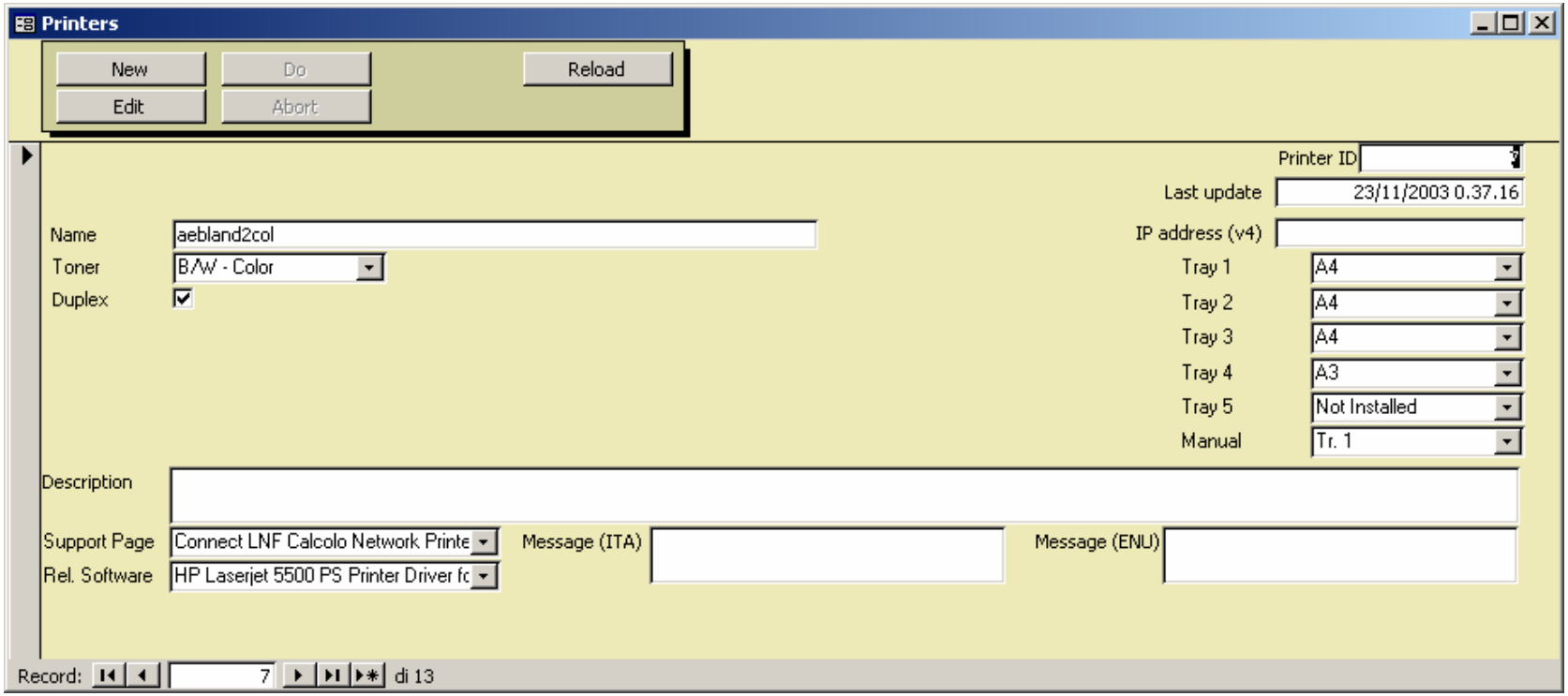


Ogni stampante esporta code in *LPD/LPR* ed in *NETBIOS*: in particolare le stampanti HP utilizzano il protocollo proprietario *HP TCP Standard Port* al posto del *NETBIOS*.
Le stampanti quindi vengono montate dal print server in *NETBIOS* o in *HP TCP Standard Port* e riesportate in *NETBIOS*, *LPD/LPR* e *APLLE TALK.* Questa impostazioni consente ai clients windows che importano code in *NETBIOS* di ottenere localmente il feedback delle stampe.

IL PORTALE DEL SERVIZIO DI STAMPA

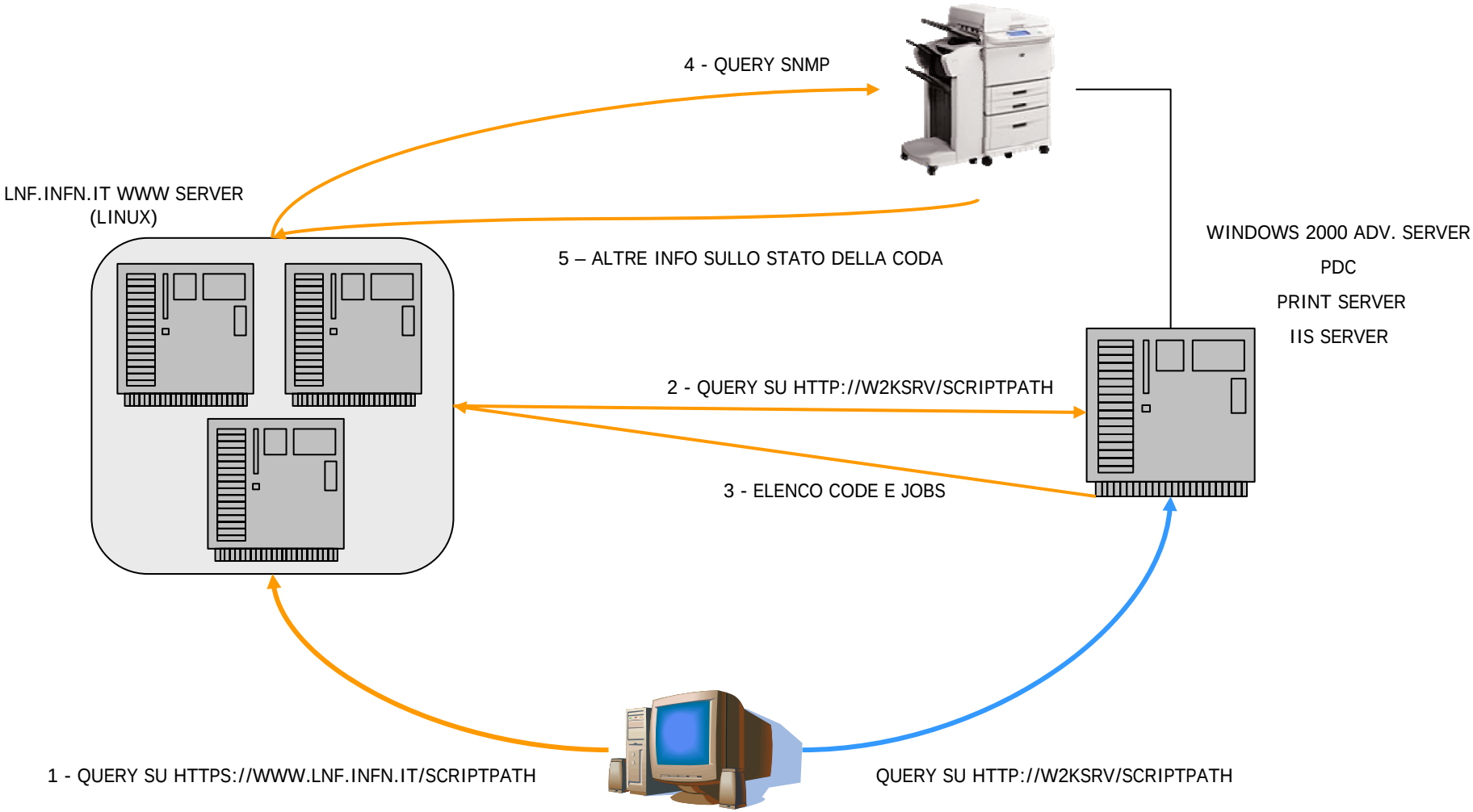
Il portale web destinato al servizio di stampa e' concepito con lo scopo di:

- monitorare in tempo reale dello stato del print server, dei processi in attesa e dello stato delle code
- visualizzare un report dei seguenti eventi: *stampa*, *spostamento in coda*, *eliminazione*, *coda inesistente*, *parametri errati*, *errore di stampa*
- fornire un elenco **dinamico** delle stampanti corredato da informazioni di supporto alla configurazione, da procedure di connessione e dal software driver di gestione



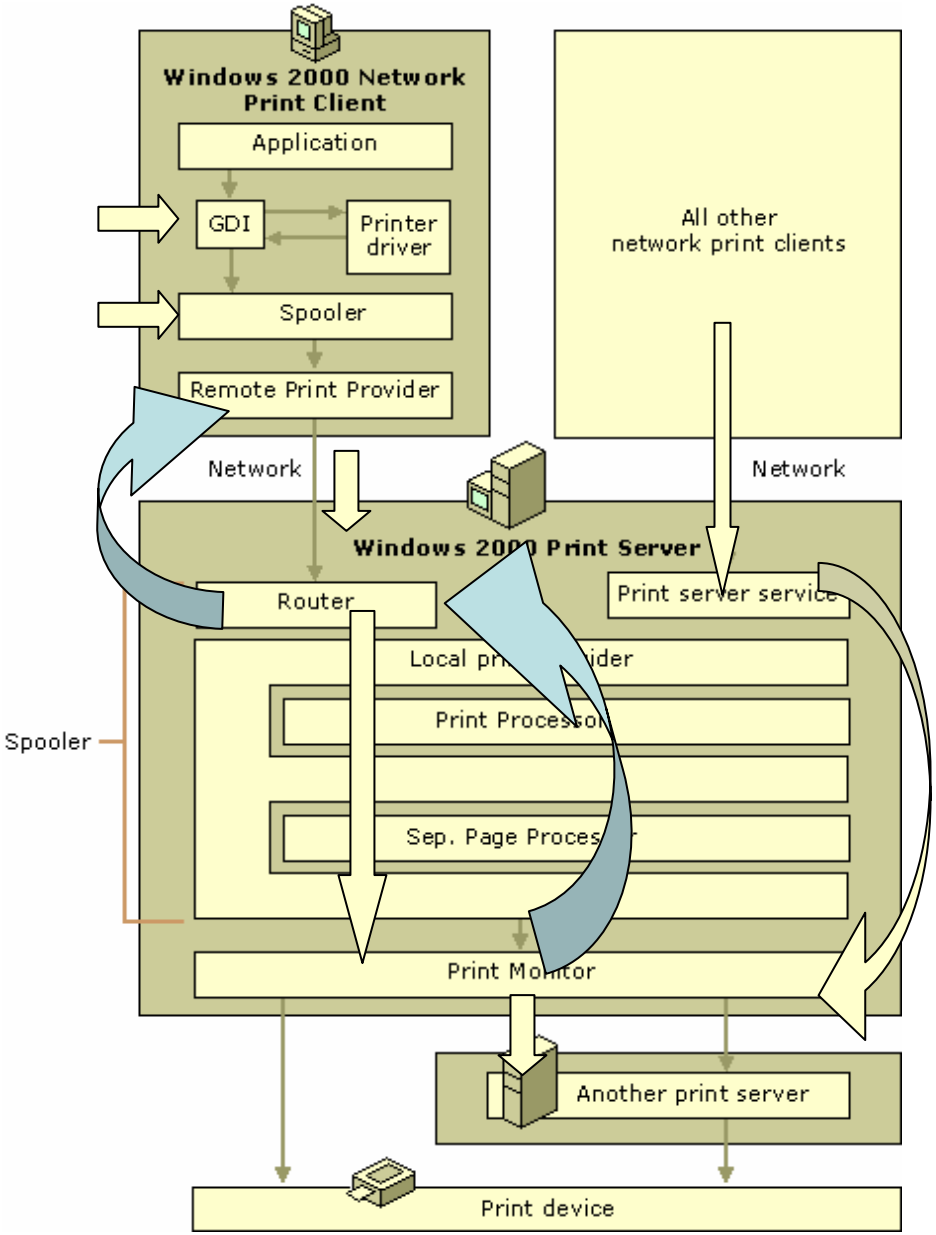
Form relativo alle stampanti: tutte le informazioni di configurazione e di supporto sono memorizzate in un database e disponibili on the fly tramite il portale web

SERVIZIO DI STAMPA - MECCANICA DI MONITORAGGIO DELLE CODE



Accesso al Portale

Seguire il link opportuno definito nelle pagine del computing (http://www.lnf.infn.it/computing/)



1 - L'applicazione genera il job di stampa mediante la chiamata a funzioni API di GDI e quindi al driver della stampante.

2 - Il job viene messo in coda nello spooler in attesa di essere inviato al server.

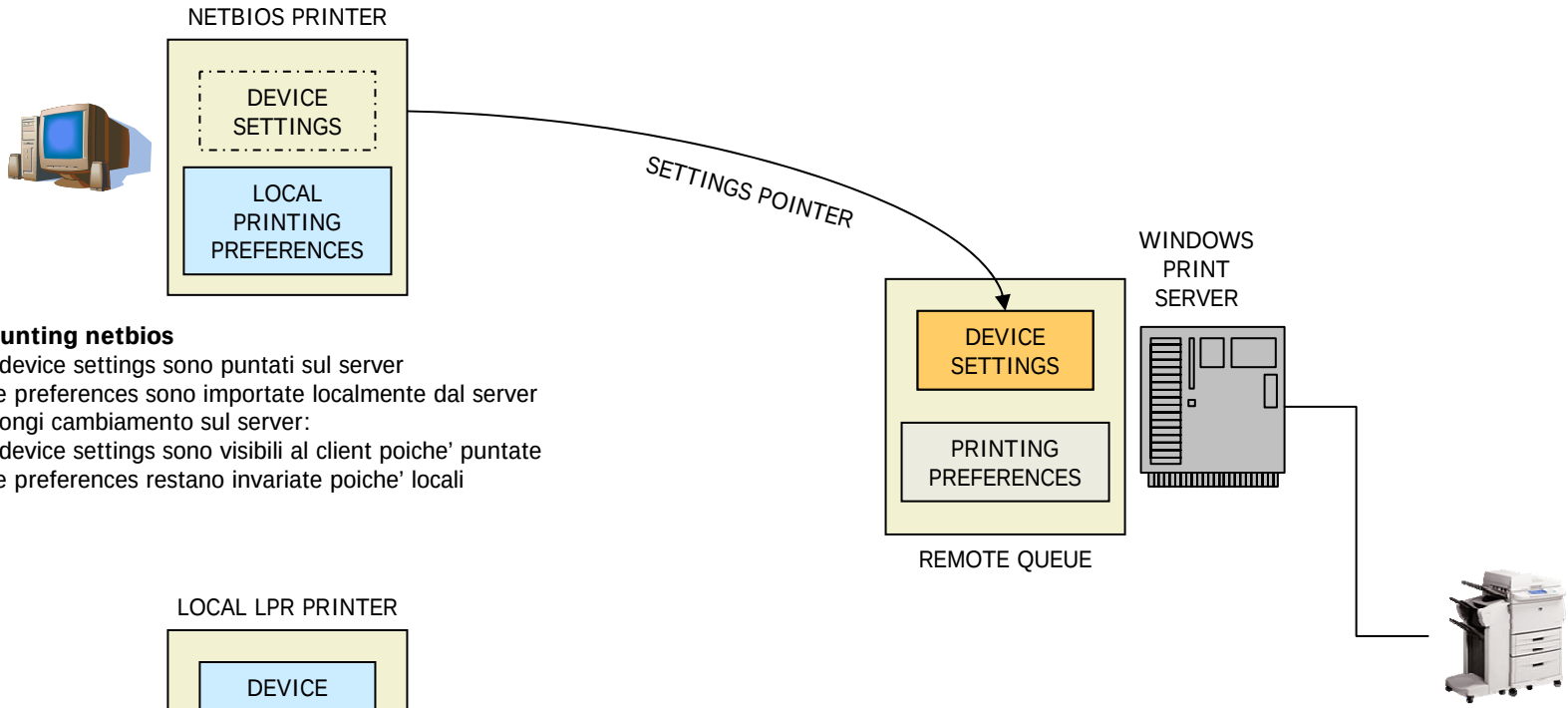
3 – Il **Remote Print Provider** contatta costantemente il server (modulo **Router**) per inviare le richieste di stampa

4 – Il **Router** instrada il job remoto verso il processo di spooling sul server che lo rielabora e lo assegna alla coda di stampa richiesta

5 – Il **Print Monitor** invia definitivamente il job alla stampante

6 – Nelle connessioni **Netbios** il **Router** restituisce il feedback del processo al client che puo' quindi monitorare lo stato del job nella finestra dello spooler

7 – Nelle connessioni LPR/LPD il **Remote Print Provider** non ottiene risposta dal Router poiche' esso questo non e' convolto nel processo: le richieste di stampa verso una coda inestistente o errata vengono attuate continuamente ogni 4 secondi generando un tracciato di errore sul server



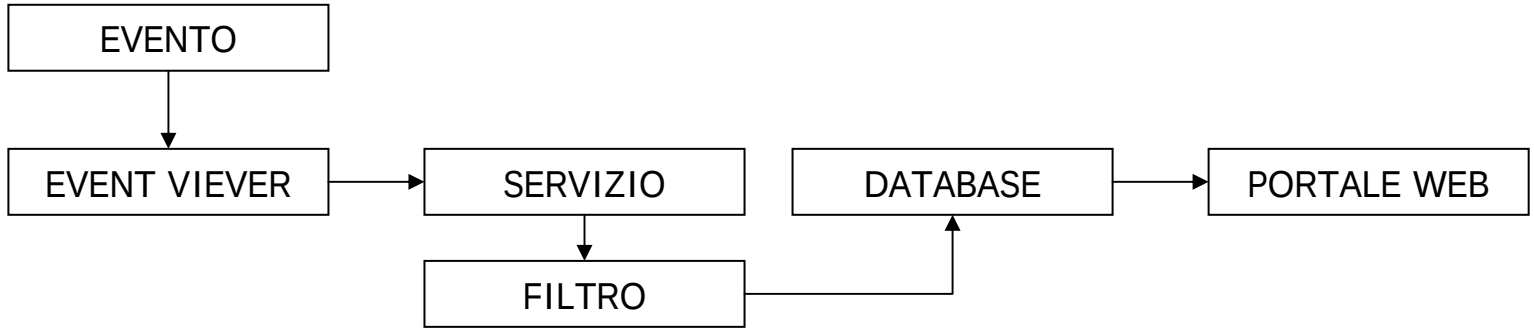
Mounting netbios
- I device settings sono puntati sul server
- Le preferences sono importate localmente dal server

Ad ongi cambiamento sul server:
- I device settings sono visibili al client poiche' puntate
- Le preferences restano invariate poiche' locali

Mounting locale (LPR)
- I device settings devono essere impostati localmente
- Le preferences devono essere impostate localmente

Ad ogni cambiamento sul server:
- I device settings non vengono trasmessi poiche' locali
- Le preferences restano invariate poiche' locali

Nell'ambito del monitoraggio delle code di stampa si e' implementato sul print server un servizio windows di logging, basato sull'intercettazione degli eventi di sistema e su database.



Per ogni evento il servizio di monitoraggio fornisce informazioni su:

- la data e l'ora
- il tipo e la descrizione: *stampa*, *spostamento in coda*, *eliminazione*, *coda inesistente*, *parametri errati*, *errore di stampa*
- il titolo del job
- l'utente e l'IP del client di invio
- il nome della coda

A completo regime operativo sarà possibile:

- notificare l'evento direttamente al client windows mediante un sistema si messaggistica
- intraprendere azioni di risposta ad eventi di errore
- fornire una base di dati per valutazioni statistiche e di distribuzione inerenti al servizio di stampa

SERVIZIO DI STORAGE DISTRIBUITO

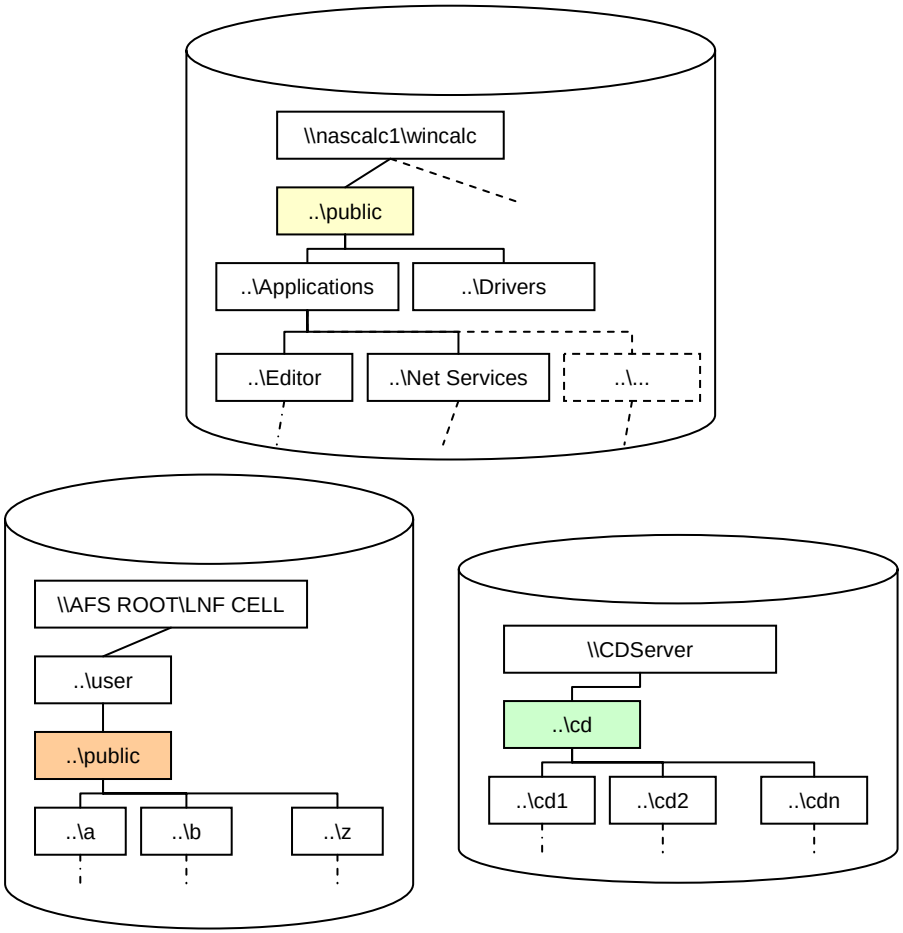
- E’ un servizio mediante il quale gli utenti possono effettuare il download del software necessario sia alla configurazione del proprio PC, in base ad opportuni criteri di efficienza e sicurezza, sia all'accesso e utilizzo delle risorse disponibili presso i LNF - INFN.

- Esso viene esportato in rete principalmente attraverso un **portale web** che nasce con la prerogativa di offrire all'utente da una parte gli efficienti strumenti e le procedure di accesso al software, secondo le specifiche condizioni di licenza, dall'altra un adeguato **supporto tecnico e documentazione** on line per l'installazione e la configurazione di particolari distribuzioni.

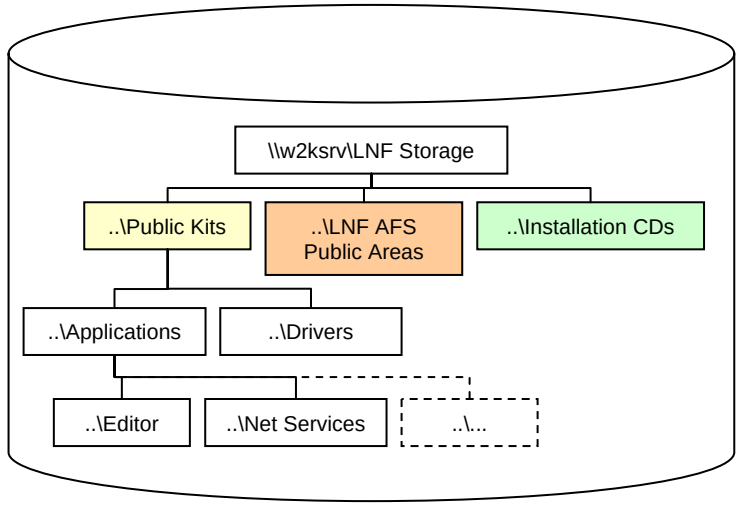
- Il servizio e’ basato su un **database relazionale** e su un **file system distribuito**

Quest’ultimo e’ un tipo di file system caratterizzato da piu' servers che cooperano esportando volumi di files collocati e delocalizzati nell'ambito di un unico file system.
In un file system distribuito ogni risorsa di share e' montata, in forma trasparente per l'utente, all'interno di un'unica struttura logica di file, e coopera appunto alla costituzione dei suoi nodi. I vantaggi evidenti, tra l'altro, sono i seguenti:

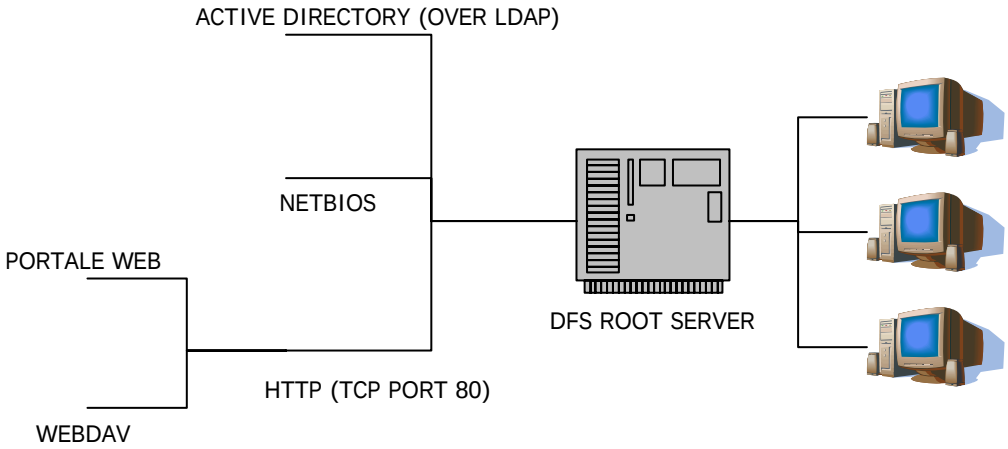
- si elimina la necessita' per gli utenti di accedere a differenti locazioni nella rete per cercare le informazioni di cui essi hanno bisogno;
- i files distribuiti attraverso i molteplici servers appaiono agli utenti come se fossero residenti in un unico posto nella rete: essi devono quindi conoscere solo un indirizzo di accesso, ovvero il percorso di rete relativo alla radice di questo struttura virtuale



Modello tradizionale di export.
Ogni risorsa ha un indirizzo di rete distinto: l'utente accede conoscendo la URL fisica di ogni condivisione.



File system distribuito.
L'utente accede a tutto lo storage mediante un unico indirizzo che prescinde dalla collocazione fisica dei contenuti. I folders colorati evidenziano i mount points dei singoli file systems all'interno di quello virtuale.



Implementazione.

Il ROOT SERVER monta le risorse di share in netbios e le riesporta su protocolli differenti.
Il client che accede ad un percorso DFS attraverso la root, **\\w2ksrv\LNF Storage** viene reindirizzato al corrispondente percorso fisico definito nel server.

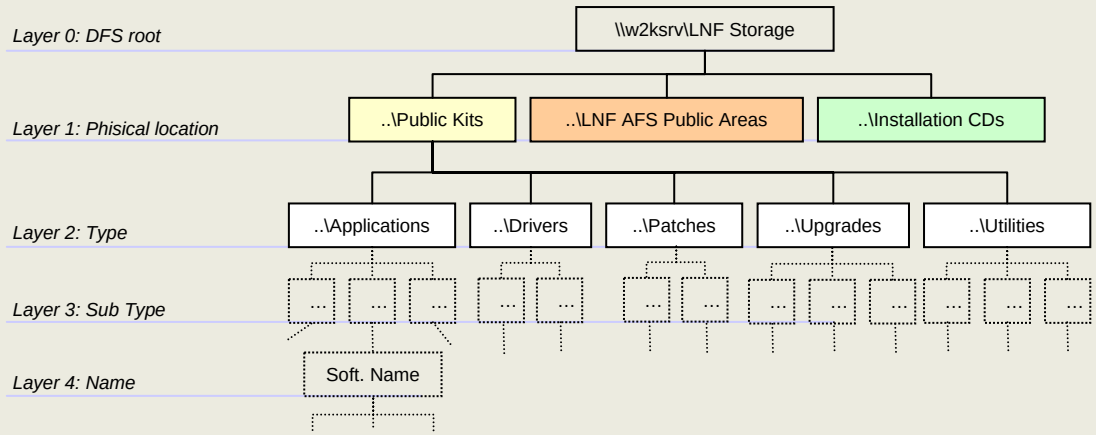
MODALITA' DI CONNESSIONE DISPONIBILI IN BASE AL SISTEMA OPERATIVO E AL TIPO DI AUTENTICAZIONE DI RETE

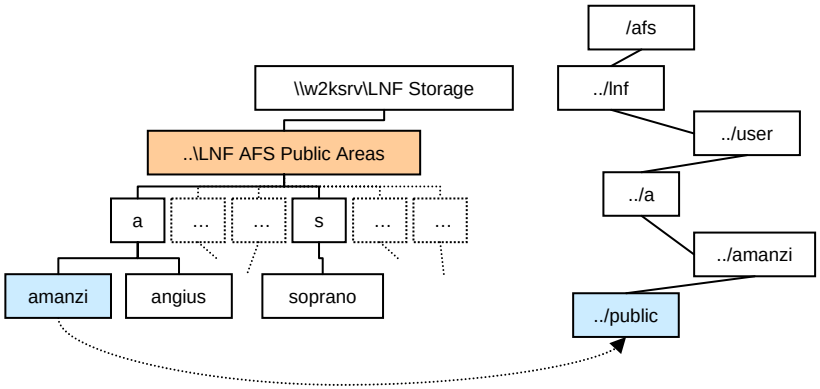
	PC WINDOWS MEMBRO DEL DOMINIO W2K		PC WINDOWS MEMBRO DI UN WORKGROUP	PIATTAFORME NON WINDOWS
	LOGIN NEL DOMINIO	LOGIN LOCALE		
PORTALE WEB Netbios nel portale Webdav nel portale	SI SI, con IE SI, Win 2K o sup. e IE	SI SI, con autenticazione e IE SI, Win 2K o sup. e IE	SI SI, con autenticazione e IE SI, Win 2K o sup. e IE	SI - -
NETBIOS	SI	SI, con autenticazione	-	-
WEBFOLDER	SI, Win 2K o sup.	SI, Win 2K o sup.	SI, Win 2K o sup.	-
BROWSE ACTIVE DIR.	SI, Win 2K o sup.	-	-	-

URLS FONDAMETALI

PORTALE WEB: http://storage.lnf.infn.it
NETBIOS: \\w2ksrv\LNF Storage
WEBDAV: http://w2ksrv.lnf.infn.it/services/storage/dfs_root

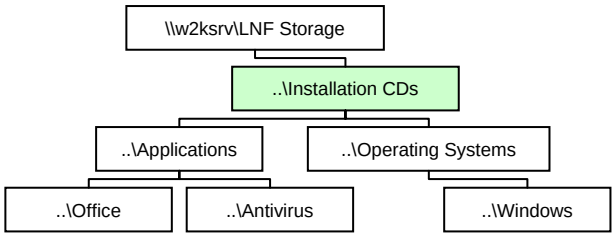
Poiche' il servizio di storage si basa su un datase relazionale, la pubblicazione del software si articola nelle due fasi:

CATALOGAZIONE	Ogni pacchetto software viene schedulato in un record di database mediante i campi: • Denominazione • Tipo e codice di licenza, termini per la richiesta • Categoria e Sub-Categoria • Sistemi operativi richiesti • Area fisica di storage • Path fisico di memorizzazzione • Path del pacchetto nell'ambito del file system distribuito • URL web dell'Autore e/o del pacchetto software • Link alla pagina web di supporto • Descrizione e note
MEMORIZZAZIONE	Ogni pacchetto software viene collocato in un folder di storage distinto ed univoco. Il database mediante il quale e' organizzato il software esporta definizioni in base alle quali si organizza la struttura del file system distribuito. In altri termini, la localizzazione di un pacchetto software all'intrerno del file system e' correlata ai valori dei campi del record di definizione associato. 



SPAZIO PUBBLICO AFS

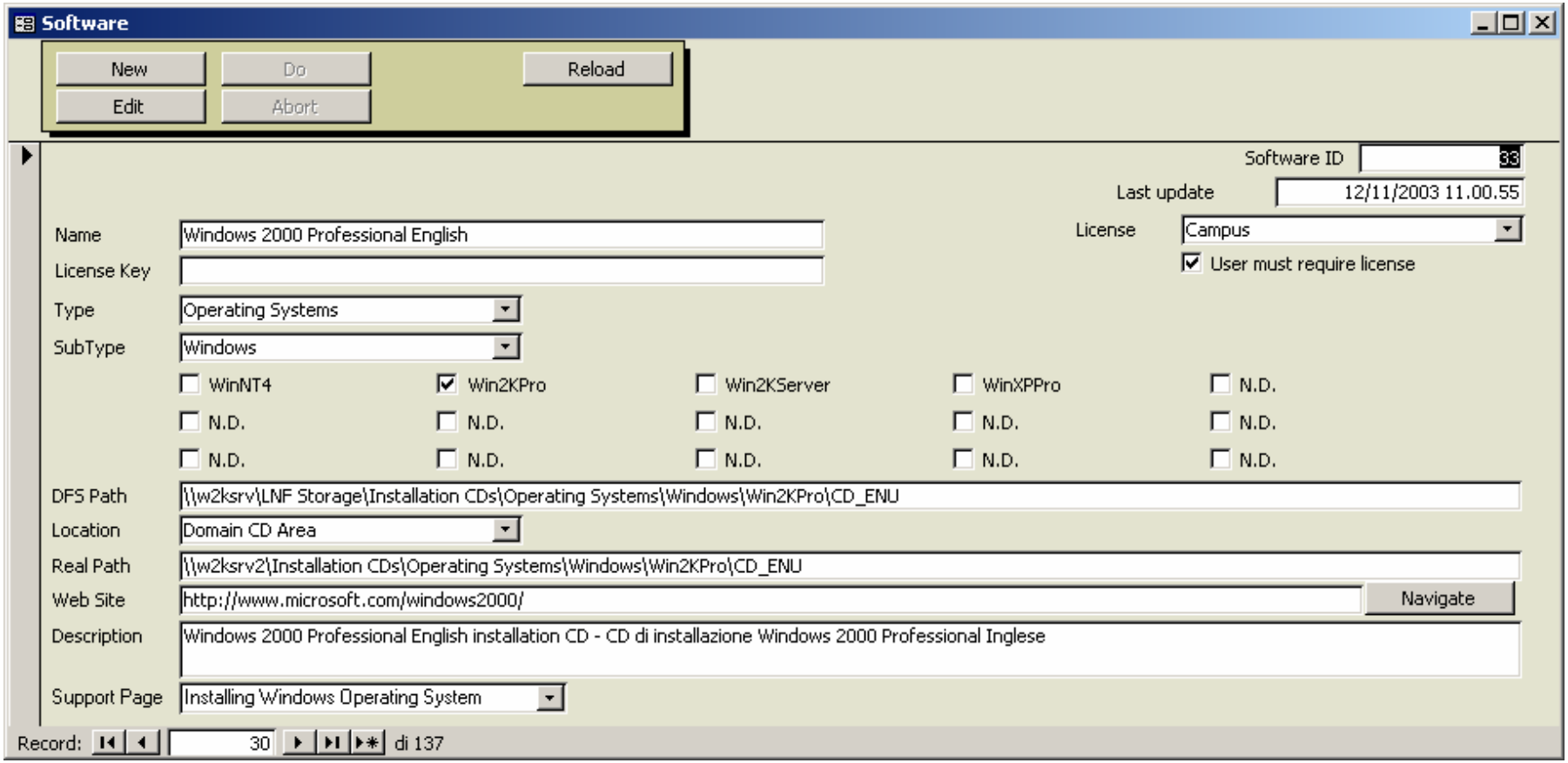
Mediante portale web e' possibile accedere alle aree pubbliche di AFS nell'ambito della cella lnf.infn.it.
In questo caso e' possibile la condivisione delle informazioni **senza client e token afs**

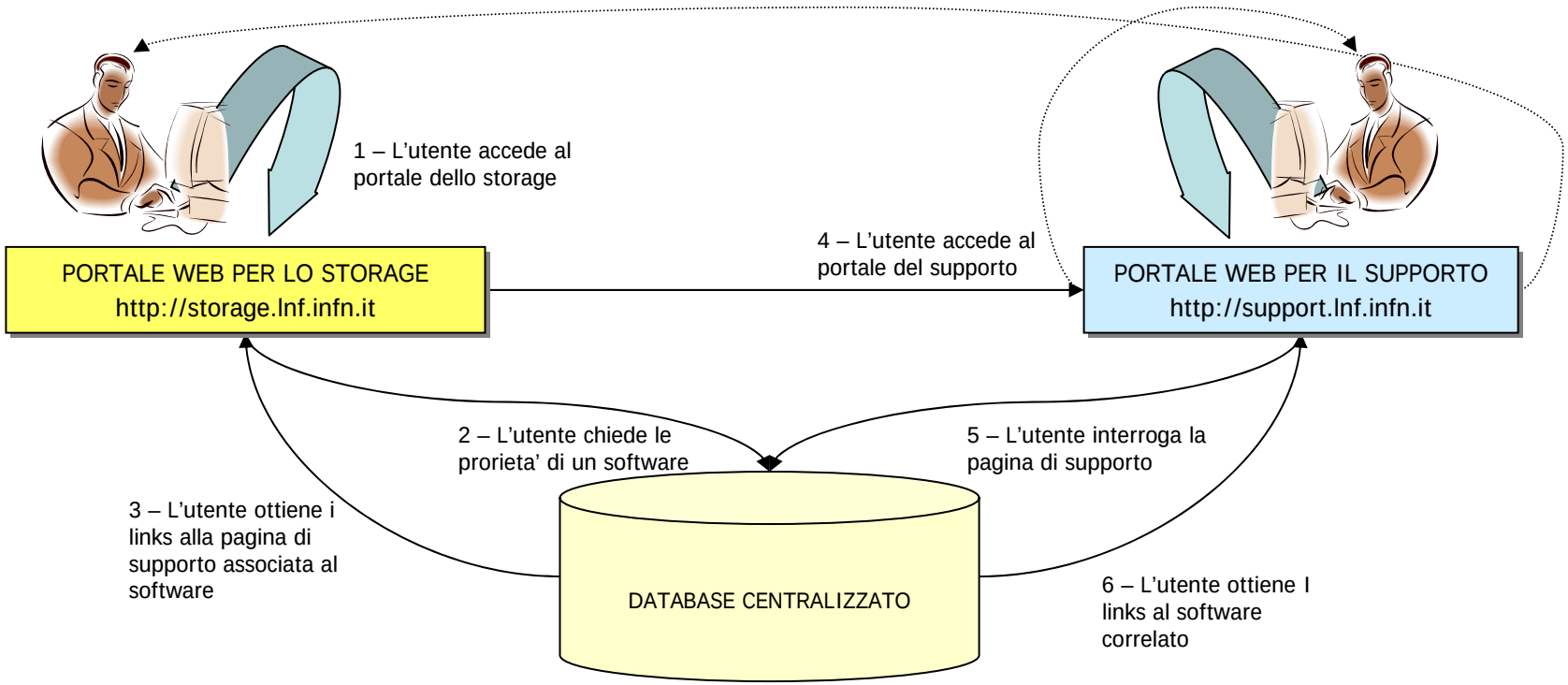


CD DI INSTALLAZIONE

L'area *Installation CDs* esporta in forma integrale i CD di installazione del software a disposizione dei LNF - INFN ed, in particolare:

- Sistemi operativi
- Office automation
- Linguaggi e strumenti di programmazione


Software
New
Do
Reload
Edit
Abort
Software ID
33
Last update
12/11/2003 11.00.55
Name
Windows 2000 Professional English
License
Campus
License Key
User must require license
Type
Operating Systems
SubType
Windows
WinNT4
Win2KPro
Win2KServer
WinXPPro
N.D.
DFS Path
\\w2ksrv\LNF Storage\Installation CDs\Operating Systems\Windows\Win2KPro\CD_ENU
Location
Domain CD Area
Real Path
\\w2ksrv2\Installation CDs\Operating Systems\Windows\Win2KPro\CD_ENU
Web Site
http://www.microsoft.com/windows2000/
Navigate
Description
Windows 2000 Professional English installation CD - CD di installazione Windows 2000 Professional Inglese
Support Page
Installing Windows Operating System
Record:
30
di 137


1 – L'utente accede al portale dello storage
PORTALE WEB PER LO STORAGE
http://storage.lnf.infn.it
4 – L'utente accede al portale del supporto
PORTALE WEB PER IL SUPPORTO
http://support.lnf.infn.it
2 – L'utente chiede le prorieta' di un software
5 – L'utente interroga la pagina di supporto
3 – L'utente ottiene i links alla pagina di supporto associata al software
DATABASE CENTRALIZZATO
6 – L'utente ottiene I links al software correlato

SERVIZIO DI SUPPORTO

E’ un servizio basato su portale web mediante il quale gli utenti dei LNF – INFN possono accedere a pagine dinamiche relative ad articoli tecnici e di informazioni su:

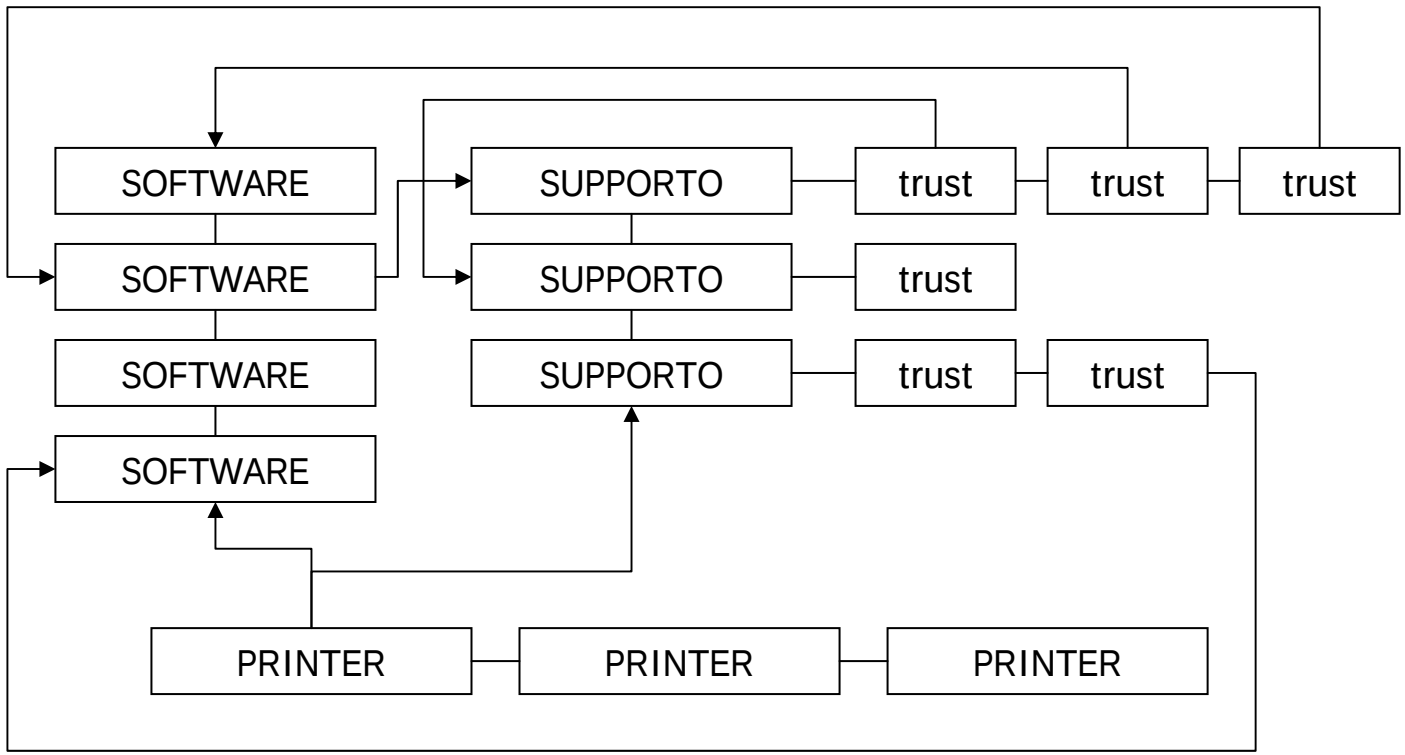
- la configurazione ottimale e sicura del PC
- le istruzioni per l' aggiornamento e la protezione delle piattaforme
- le procedure da seguire per richiede assistenza

Le informazioni pubblicate sono residenti si database e organizzate in categorie e sottocategorie.
Le categorie individuano aree tematiche e sono le seguenti:

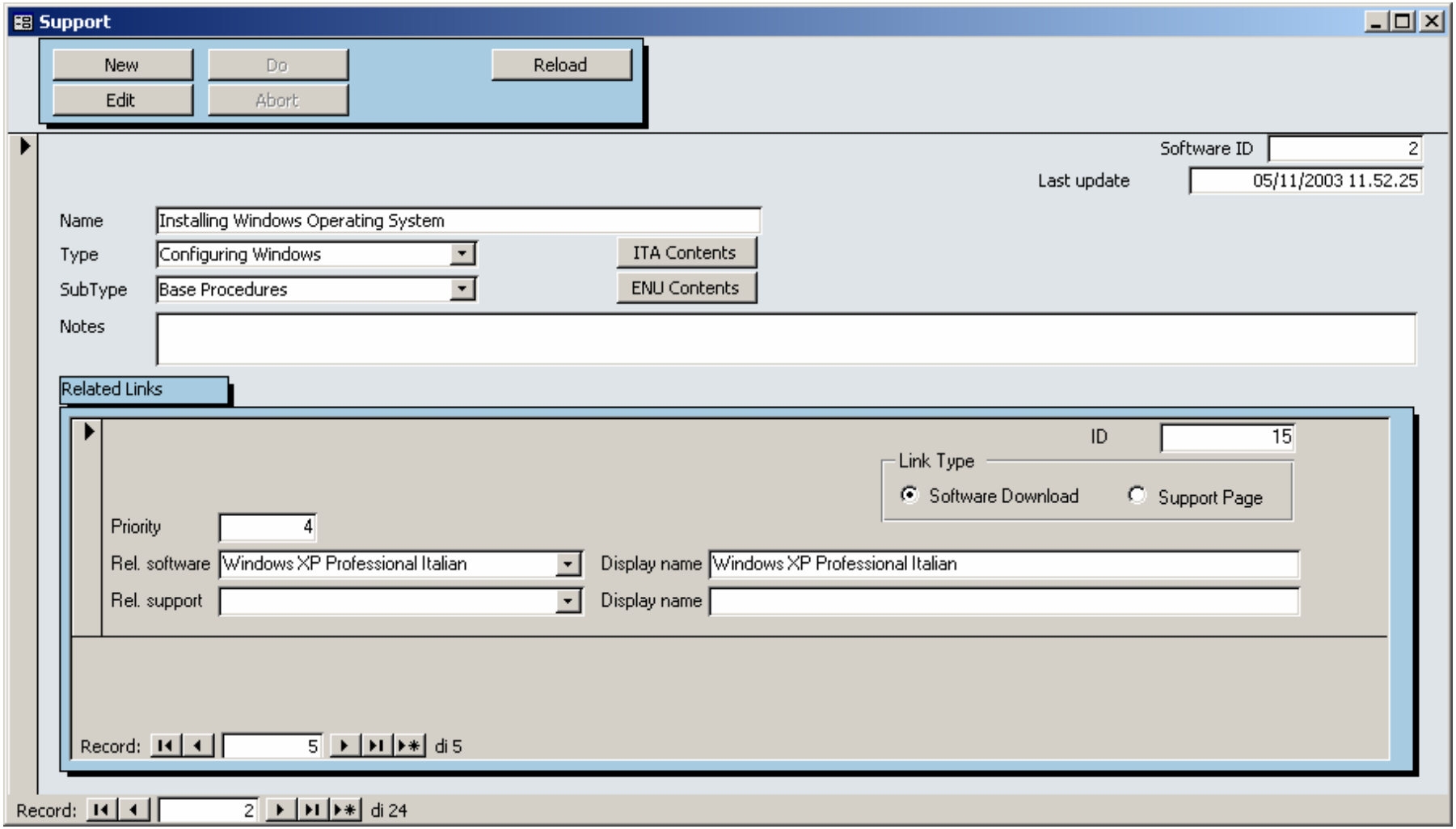
Configuring Windows	Contiene spiegazioni e consigli sulla configurazione di una piattaforma Windows, dall'installazione del Sistema Operativo all'installazione del software consigliato ai LNF.
Installing Devices	Relativa all'installazione e configurazione di dispositivi di I/O in una piattaforma Windows: l'utente puo' trovare in questa sezione, per esempio, le procedure per configurare le stampanti di rete servite dal Calcolo
Setting Applications	Consigli e procedure per configurare le applicazioni utilizzate ai LNF
Upgrading and Patching	Questa sezione contiene la guida sulle procedure di aggiornamento delle piattaforme soprattutto in termini di protezione e sicurezza

Ogni pagina di supporto e’ suddivisa in tre sezioni: **Overviews**, **Procedures** e **Requirements**, rispettivamente relative alla descrizione del problema, le procedure da eseguire, i requisiti hardware/software che la piattaforma deve possedere.

Poiche' il servizio si basa su database relazionale, ogni argomento di supporto puo' essere associato sia ai pacchetti software sia ad altri argomenti di supporto correlati mediante una corrispondenza di tipo uno a molti.
Il portale web esprime questa corrispondenza mediante links visualizzati nelle due sezioni **Available Downloads** e **Related Topics** presenti in ogni pagina di supporto.



Esempio di collegamenti relazionali implementati mediante un modello di liste e puntatori


Support
New
Do
Reload
Edit
Abort
Software ID
2
Last update
05/11/2003 11.52.25
Name
Installing Windows Operating System
Type
Configuring Windows
ITA Contents
SubType
Base Procedures
ENU Contents
Notes
Related Links
ID
15
Link Type
Software Download
Support Page
Priority
4
Rel. software
Windows XP Professional Italian
Display name
Windows XP Professional Italian
Rel. support
Display name
Record:
5
di 5
Record:
2
di 24

INFORMAZIONE

I portali web hanno la prerogativa di veicolare e diffondere l'informazione agli utenti.
L'obiettivo e' raggiunto mediante il duplice approccio costituito da:

- il portale di domino, che fornisce notizie a carattere generale sulla infrastruttura, sui servizi, sui link di maggior interesse e sugli argomenti dell'ultima ora

- i portali specifici dove le informazioni sono trattate via via sempre piu' nello specifico. Per esempio il portale dello storage implementa i tre livelli di informazione:
  - generale, diffusa nella home page e relativa alle notizie sul portale, sul software disponibile, sulle procedure esecutive
  - contestuale, relativa a ciascuna categoria di software
  - specifica, relativa al singolo pacchetto software

Il database su cui si basano i portali offre campi opportunamente destinati alle notizie da divulgare nei portali dei servizi.
Cio' rende per esempio semplice diffondere le notizie relative allo stato di riparazione e/o disponibilità delle stampanti o la necessità di installare aggiornamenti software.