

PROGETTO e REALIZZAZIONE di APPLICAZIONI

PER LA RETE DI ISTITUTO

**"WAKE on LAN"
"REMOTE SHUTDOWN"
"PING LIVE TEST"**

Realizzazione

Parini Marco classe 5BZ

Vitari Cristian classe 5BZ

Corso SISTEMI ed AUTOMAZIONE



Ipsia Moretto Brescia
Anno Scolastico 2003-04

SOMMARIO

PRESENTAZIONE	3
IL PARADIGMA CLIENT SERVER	4
DELPHI	5
PROCEDURA CHE CREA IL TRASFERIMENTO	8
PROCEDURA CHE SVUOTA LA TABELLA	9
WAKE ON LAN (WOL).....	13
PROGRAMMA WAKE ON LAN	16
SHUTDOWN	21
LO SHUTDOWN SCARICATO DA INTERNET	22
PING	22
<i>Ping</i>	24
PROGRAMMA "TEST SULLE MACCHINE ATTIVE":	25
NASCITA DELLA INTRANET ALL'IPSIA MORETTO: 1999 PROGETTO ONION	26
<i>Architettura di rete</i>	26
<i>Requisiti dei principali nodi di rete</i>	28
<i>Requisiti di collegamento delle macchine alla rete</i>	28
<i>Router amministrazione</i>	29
<i>Server Intranet</i>	29
<i>Firewall</i>	30
<i>Vincoli sull'architettura delle applicazioni</i>	30
<i>Sintesi delle attività</i>	31

PRESENTAZIONE

Una volta arrivati al termine (e speriamo sia proprio la fine...) della nostra avventura in questo istituto, ci siamo dovuti porre la domanda tanto aspettata: che argomento tratterà la nostra tesi? Inizialmente non possiamo nascondere di aver avuto un attimo di indecisione, ma poi tutto è venuto spontaneo ,come potrebbero infatti due giovani studenti restare indifferenti ai nuovi metodi che permettono di rendere la vita ancora più facile di quello che è ? Ed è stato a questo punto che si è intromesso il prof. Azzani, la sua proposta, dettata non solo dalla sua continua "voglia di strafare" ma anche dalla necessità di nuovi interventi innovativi da poter mettere a disposizione della scuola, ci è sembrata subito molto interessante e siamo stati molto contenti di poter mettere a disposizione un po' del nostro tempo a beneficio non solo del nostro sapere ma anche di questo istituto. Il nostro progetto è composto da diverse parti, molto collegate però tra loro, esso comprende:

1. la funzione WOL ,che permette l'accensione di uno o più pc a distanza alla data e ora prestabilita tramite un unico computer che potrebbe essere o il server o la postazione del tecnico del laboratorio ;
2. il comando SHUT DOWN, che consente di arrestare o riavviare una o più macchine anch'esso alla data e ora prestabilita tramite un unico calcolatore anche in questo caso il comando potrebbe essere effettuato o dal server o dal tecnico del laboratorio tramite la sua postazione;
3. la verifica oraria dei computer accesi e spenti ogni ora (con eccezione alle ore notturne);
4. l'aggiornamento del database di tutte le macchine installate sulla rete con i rispettivi dati fondamentali.

Noi speriamo che ciò che vi mettiamo a disposizione venga non solo usato nel migliore dei modi ma continuamente perfezionato in modo di tenerlo al passo coi tempi.

.... Accetto di buon grado le vostre battute un pochino goliardiche; le ritengo legate alla necessità di scaricare lo stress accumulato durante l'intero corso di studi quinquennale e giunte al loro culmine in quest'ultimo periodo.

Sono perfettamente consapevole di averVi più volte sollecitato, ad intraprendere un percorso che poteva sembrare buio ma Vi avevo ritenuto capaci anche di una "avventura al di fuori degli schemi tradizionali".

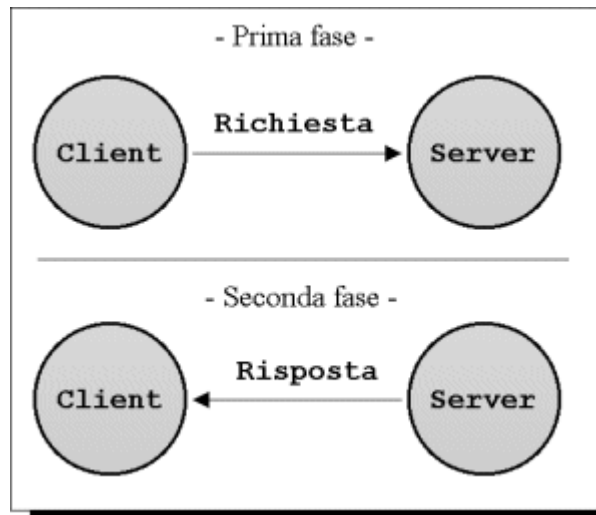
Ho apprezzato la vostra disponibilità e fiducia, ho constatato che giorno dopo giorno "il da farsi" è diventato più chiaro man mano prendevate coscienza di quanto Vi avevo chiesto e voi Vi apprestavate a fare.

Mi auguro che per Voi sia stata una occasione proficua per analizzare e affrontare la soluzione di un problema sicuramente inconsueto ma certamente collocato in un contesto di tecnologie d'avanguardia.

..... Cleto Azzani

IL PARADIGMA CLIENT SERVER

Il server è il computer che per mezzo di uno o più processi attivi, offre dei servizi all'utente tramite applicazioni "client" che vengono fatte eseguire sul PC dell'utente. Possono essere anche molti gli utenti che contemporaneamente accedono tramite il loro client alle



informazioni (risorse) offerte dal server. La comunicazione avviene con la richiesta di un servizio da parte del client e la conseguente realizzazione del compito da parte del server, utilizzando i protocolli necessari per la comunicazione, per esempio quelli dello stack TCP/IP. Per compito si intende l'inserimento dati o la interrogazione di un database, l'elaborazione on-line (server-side, ossia prodotta dal server e successivamente inviata al client), videogames, le pagine web, sistemi di posta elettronica, newsgroup, ecc.

Ad esempio, i giochi Client/Server sono quelli che hanno bisogno di almeno due computer collegati tra loro (quindi in rete) e di due programmi: per esempio se pensiamo ad un gioco di gare automobilistiche, ebbene il programma del computer centrale a cui siete collegati che gestisce coordinate, carburante e condizioni di gara è il server, che oltre a controllare il gioco terrà conto anche delle auto di ciascun utente collegato il quel momento insieme a voi. Il client invece è il vostro computer che ha bisogno di un programma freeware o di rado ottenibile versando una piccola quota (shareware). Questo programma client fornisce l'utente di un'interfaccia che consente di interagire sia con la vostra automobile che con quella degli altri utenti connessi al server.

Il paradigma client/server perciò divide la comunicazione tra due applicazioni, non necessariamente presenti entrambe nello stesso computer, in due distinte categorie,

caratterizzate da chi aspetta una comunicazione o da chi la inizia. Chi inizia la comunicazione è denominato client (cliente), server (servente) chi la aspetta. Normalmente l'applicazione client contatta l'applicazione server e le invia una richiesta, dopo di che si mette nell'attesa della risposta, e quando questa sarà arrivata continuerà nella sua esecuzione. L'applicazione server aspetta l'arrivo di una richiesta da un'applicazione client, esegue le necessarie elaborazioni e invia il risultato al client (vedi figura). Quest'architettura della comunicazione è stata creata per risolvere il problema di sincronizzazione noto con il nome di rendez-vous, decidendo a priori chi "parla" e chi "ascolta" tra le due applicazioni coinvolte. L'architettura descritta e' da considerarsi di base, infatti, alcune applicazioni non ricadono esattamente nella definizione di client o server, ma possono all'occorrenza comportarsi sia in un modo sia nell'altro secondo l'obiettivo prospettato.

DELPHI

Delphi è un ambiente di programmazione visuale ad oggetti per lo sviluppo rapido di applicazioni (RAD / Rapid Application Development) a carattere generale e di applicazioni client/server per Windows 95 e 98 e Windows NT. Con Delphi è possibile creare applicazioni Windows altamente efficienti riducendo al minimo i tempi di programmazione.

Delphi comprende una libreria di componenti riutilizzabili VCL e un insieme di strumenti di progettazione RAD, tra cui i modelli di applicazioni standard e di schede expert di programmazione. Con



questi strumenti e con il compilatore Delphi a 32 bit è possibile creare rapidamente e testare prototipi, trasformandoli in robuste applicazioni perfettamente in linea con le moderne esigenze.

Delphi può essere utilizzato per sviluppare qualsiasi tipo di applicazione, dalle utility di analisi e test dei PC, fino ai più sofisticati strumenti di accesso ai database.

Gli strumenti di gestione dei database e i componenti di gestione dei dati previsti in Delphi permettono di sviluppare strumenti di gestione dati e applicazioni client/server in tempi notevolmente ridotti.

Con i controlli di gestione dei dati di Delphi, i dati vengono visualizzati direttamente durante la creazione dell'applicazione, consentendo una immediata verifica del risultato delle interrogazioni al database e delle modifiche all'interfaccia dell'applicazione.

L'ambiente di sviluppo integrato di Delphi IDE (Integrated, Development, Environment) mantiene sviluppo, verifica e gestione delle applicazioni in un unico ambiente. E' possibile creare o modificare una applicazione compreso schede di inserimento dati, report, menu, finestre di dialogo, database e definizioni di file, moduli dati, componenti, senza uscire da Delphi.

IL DATABASE DEI PC IN RETE

Utilizzando la tecnologia Client/Server, ed altre librerie scaricate da Internet, Andeni e Pitozzi, alunni della 5BZ dello scorso anno scolastico, hanno realizzato un applicativo che raccoglie e registra in un data-base residente sul server, i dati tecnici maggiormente significativi (il nome della macchina, il nome del processore, la frequenza del processore, sistema operativo, utente registrato, la memoria fisica, indirizzo ip, mac, scheda audio ecc...) dei PC connessi in rete.

INV: 8084	IP: 192.168.145.109
UBIC: LE7	SOFTW: S3 Refresh
WS: 09	CRTRAM: 0
USER: le7	CRT: SiS 6215
LB: 04/11/03 11.39.36	MHZ: 166
CPU: Pentium MMX	AUDIO: NA
SOP: 4.0.1111	MAC: 00:10:5A:40:E7:CF
UREG: Ipsia Moretto Brescia	RAMT: 31
DUNIT: ACDPQ	HD1S: 1A39-07FA
TUNIT: FHCNN	HD1T: 19530
CRTRES: 800 x 600	HD1F: 17058
NIC: 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)	

Esempio di dati archiviati dal server

Per le applicazioni che ci siamo proposti di realizzare, i dati memorizzati sul server erano sovrabbondanti e disposti in modo disordinato. Abbiamo pertanto scritto un applicativo che ci consentisse di selezionare unicamente i dati necessari e trasferirli in modo ordinato in un'altra tabella, denominata NetMoretto.db (tabella Paradox 7) strutturata in campi secondo il seguente schema :

Tabella : NETMORETTO.DB

ID; Float; 0;
IP; Character; 16;
MAC; Character; 18;
TYPE; Character; 5;
PING; Float; 0;
DEVICE; Character; 15;
LUOGO; Character; 20;
INVENTARIO; Float; 0;
TESTPING; Float; 0;
TESTWOL; Float; 0;
SHUT; Float; 0;
PSHUT; Character; 15;
NOTE; Character; 40;
Numero Complessivo dei Campi : 13

Andiamo a descrivere come avviene questo riordinamento e a cosa servirà.

AGGIORNAMENTO NETMORETTO.DB

TABELLA DEGLI IP ASSEGNATI

NETMORETTO.DB

ID	IP	MAC	T
1	192.168.145.0		S
2	192.168.145.1		F
3	192.168.145.2		F
4	192.168.145.3		F

Buttons: INIT TABELLA, Trasferisco Dati

TABELLA DELLE WS AUTENTICATE

REGISTRO.DB

INV	UBIC	WS	USER
946863	PRESIDENZA	WS146-13	Montanini
8023	LAB. MULTIMEDIA	ws145-251	ät
8023	LAB. MULTIMEDIA	ws145-251	ät
8088	LE7	12	¶†

Search field: 192.168.145.9
Button: Ricerca IP

DB-Registro: 3177 DB-NetMoretto: 512

Un esempio di query con i dati forniti dal server

La tabella "NetMoretto.db" contiene tutti gli IP number delle due sottoreti in cui è articolata la Intranet del nostro Istituto; ogni IP di rete è catalogato in base al tipo (campo TYPE: S se nodo di sistema es.: server o router, A se assegnato ad una Work-Station, F se non ancora assegnato, R se riservato). Ogni IP ha poi associati altri parametri: MAC della scheda di rete

(NIC) cui è abbinato quel determinato IP; PING (contenente o il valore 0 oppure il valore 1: 0 significa che quell'IP non è "pingabile"); DEVICE stringa di 15 caratteri che contiene il nome del dispositivo individuato dall'IP; LUOGO stringa di 20 caratteri che contiene l'ubicazione fisica del Device; INVENTARIO numero che identifica il Device nell'Inventario di Istituto; TESTPING, TESTWOL e SHUT sono tre parametri numerici che indicano la possibilità di eseguire il comando PING su quel determinato IP, la possibilità di eseguire da remoto l'avvio della workstation in quanto configurata per la procedura Wake On Lan e la possibilità di eseguire da remoto la procedura di "Remote Shutdown" utilizzando la password PSHUT. Il primo applicativo realizzato (vedi pag. 7) effettua delle query sul database "registro.db" ed aggiorna nella tabella "netmoretto.db".

PROCEDURA CHE CREA IL TRASFERIMENTO

```

procedure TForm1.Button2Click(Sender: TObject);
  Var st: String;
      k:integer;
begin
  Table1.First;
  For k:=1 to table1.recordcount do
  Begin
  Ipn:= Table1.FieldName('IP').AsString;
  ST := 'SELECT * FROM REGISTRO.DB '+
        'WHERE IP="'+ipn+'";
  Query1.Close;
  Query1.SQL.Clear;
  Query1.SQL.Add(st);
  Query1.Open;

  If Query1.RecordCount <> 0 Then
  Begin
    Mach := Query1.FieldName('MAC').AsString ;
    Inv := Query1.FieldName('INV').AsString ;
    Table1.Edit;
    Table1.FieldName('MAC').AsString := Mach;
    Table1.FieldName('INVENTARIO').AsString := Inv;
    Table1.Post;
  End;
  Table1.next;
  End;
end;

```

Controlla se gli Ip presenti nella query corrispondono con quelli presenti nel database

I dati riportati nella query vengono riportati nel database creato da noi

I due pulsanti al di sotto come "CANCELLA" una volta trasferiti i dati ripulirà i dati nella tabella superiore per rieffettuare un nuovo trasferimento.

PROCEDURA CHE SVUOTA LA TABELLA

```
procedure TForm1.Button3Click(Sender: TObject);
  var k : integer;
begin
  if MessageDlg('Confermi la cancellazione ?',
    mtConfirmation, [mbYes, mbNo], 0) = mrYes then
  begin
    For k :=1 To Table1.RecordCount do
      Begin
        Table1.Edit;

        Table1.FieldName('WS').AsString := "";
        Table1.FieldName('MAC').AsString := "";
        Table1.FieldName('INVENTARIO').AsString := "";
        Table1.Post;
        Table1.Next;
      End;
    Table1.Close;
    Table1.Open;
  End;
end;
```

Tutti i record nel database
vengono modificati con
delle stringhe vuote

Diamo una spiegazione esauriente dei dati memorizzati nella tabella netmoretto.db.

IP

Il nome completo è TCP/IP Internet Protocol Suite, ed è un insieme di protocolli di trasmissione di cui i due principali son appunto il TCP (Transmission Control Protocol) e l'IP (Internet Protocol).

Un protocollo essenzialmente è una serie di regole per comporre dei messaggi e per far sì che le informazioni possano essere scambiate tra due macchine. Un protocollo può contenere regole estremamente dettagliate, come quelle che identificano il significato di ogni singolo bit nella costruzione di un messaggio, oppure fornire uno scenario di alto livello, come per esempio definire come avviene trasferimento di un file da un computer all'altro. Una generica architettura di trasmissione è formata da una torre a più piani, dove ogni piano rappresenta una precisa responsabilità nella trasmissione dei messaggi. Alla base della torre sta la porta di accesso alla rete fisica, che potremmo pensare come una rete di strade. Ogni piano prende il messaggio che arriva dal piano superiore, lo mette in una busta con alcune informazioni aggiuntive, e lo passa come messaggio al piano inferiore. Le regole di comunicazione tra i vari

piani sono dette interfacce. Il messaggio risultante , formato da tante buste una dentro l'altra, viene immesso nella rete dalla porta che si trova alla base della torre. Una volta arrivato al piano terreno infatti , esso viene trasportato alla torre di destinazione e da qui risale un piano dopo l'altro fino all'ultimo piano, detto anche livello applicativo. Ogni piano della torre di destinazione apre solo la busta che gli compete e usa le informazioni aggiuntive per recapitare la busta successiva al piano superiore. Le informazioni aggiuntive rappresentano il protocollo di comunicazione. Ogni piano comunica quindi solo con il piano corrispondente.

L'indirizzo IP su Internet viene assegnato dal NIC mentre su una rete privata Intranet dall'Amministratore di rete.

Ogni host o router ha un indirizzamento IP univoco (a meno di altre soluzioni per gli host) . Le classi sono così suddivise:

- A) (1.0.0.0 - 127.255.255.255) il marcatore di classe è 0, 126 reti con 16 milioni di host ciascuno
- B) (128.0.0.0- 191.255.255.255) il marcatore di classe è 10, 16382 reti con 64000 host ciascuno
- C) (192.0.0.0-223.255.255.255) il marcatore di classe è 110, 2 milioni di reti con 254 host ciascuno
- D) (224.0.0.0- 239.255.255.255)il marcatore di classe è 1110, multicast indica un gruppo di host
- E) (240.0.0.0-247.255.255.255)prossimo utilizzo 00..0 (0) indica questo host o questa rete,11..1 (=1) indica Broadcast in questa rete (es:Lan).

Se la parte NET_ID è tutta 0 allora si vuole indicare un host in questa rete. Se la parte HOST_ID è tutta 1 si vuole indicare un Broadcast del pacchetto in una rete (LAN) remota . Loopbacking 127.xx.yy.zz per testare la rete locale da un sender che non conosce il proprio numero.

Nel nostro istituto di fatti come troveremo nei prossimi test(Wol,Shutdown,Ping) è suddivisa in due sottoreti di "classe C" ,una per la rete didattica: 192.168.145.0; e una per l'Amministrativa: 192.168.146.0

RETE

Come abbiamo detto prima il nostro istituto è suddiviso in due reti per questo abbiamo cercato di raggrupparle in questo campo.

MAC

Il Mac address, è un indirizzo univoco della scheda di rete e serve per realizzare una connessione fisica tra due schede di rete . Esso lavora ai primi due livelli del sistema ISO/OSI.

Questo indirizzo, è strutturato nella seguente maniera:

00:00:00:00:00:00

I primi tre numeri, (24bit) sono stati assegnati dall'I.E.E.E, in base alla casa produttrice , cioè su ogni scheda della "Tricom" troveremo i primi tre numeri uguali . Gli ultimi tre numeri (24bit) vanno in ordine progressivo.

Ovviamente, il numero delle schede non è infinito. Ogni casa produttrice, non può superare un numero pari a 2^{24} di schede prima di 10 anni. Dopo 10 anni ,improbabile ma non impossibile ,è possibile trovare una scheda "clone". Una clone, provocherebbe un conflitto tra i due PC.

Per ricavare il Mac basterebbe aprire il nostro calcolatore e leggere sull'adesivo presente sulla schede di rete oppure lanciando le utility win ip/cfg.

Il mac come l'indirizzo Ip verrà utilizzato nel test wol.

LUOGO

Il campo luogo riporta per ogni ip la ubicazione fisica del calcolatore dentro l'istituto.

NOTE

Se il campo luogo non è predefinito o mancante il record note descrive la funzione che assume quell'indirizzo ip.

CPU

E' il componente più importante del pc. Questa sigla significa Central (Centrale, perché costituisce il nucleo centrale dell'elaborazione dei dati del computer) Processing (Processo di

elaborazione ,perché si occupa deòll' elaborazione dei dati) Unit (Unità, perché è un microprocessore contenente milioni di transistor); l'espressione dell'acronimo tradotta in italiano è quindi Unità di Elaborazione Centrale.

La CPU è composta da un'unità di controllo, un'unità aritmetico-logica che insieme formano il microprocessore , e dalla memoria d'uso, cioè la Ram e la Rom.

L'unità di controllo deve riconoscere i comandi che l'utente impartisce dalla tastiera ,dalle periferiche e dalle Ram e dalle Rom,dove sono presenti i programmi.

Quindi si può dire che la Control Unit serve da coordinamento e controllo sulla esecuzione dei programmi e sulle periferiche , impartendo i comandi che servono ad ottenere ciò che viene richiesto tramite il software. L'unità aritmetico-logica è il componente della CPU che si occupa dell'elaborazione dei dati che provengono dalla memoria come numeri binari. In pratica la ALU legge la memoria , effettua i calcoli ,le operazioni logiche e di confronto domandate dall'unità di controllo, trasmettendo il risultato ,che viene opportunamente salvato in una determinata cella di memoria.

RAM

La ram è una memoria molto importante:qui vengono stivati i dati ancora in elaborazione e grazie a tempi di accesso molto veloci (anche fino a 10 ns) velocizza l'intero sistema. Molta Ram, per esempio , evita che un sistema operativo molto "pesante" come Windows 9x utilizzi in modo eccessivo il file di swap (che si trova nella directory di Windows, con nome win386.swp dove vengono momentaneamente immagazzinati i dati in transito) , velocizzando l'intero sistema.

FREQUENZA

E' un segnale periodico estremamente regolare ,ottenuto dalle vibrazioni di un cristallo di quarzo sottoposto al passaggio di una corrente elettrica . Questo segnale viene poi normalizzato e stabilizzato elettronicamente da un chip avente quella specifica funzionalità . IL clock in uscita da quest'ultimo viene poi usato effettivamente per sincronizzare tutte le varie parti della macchina.

WS

Cioè la workstation è semplicemente il nome del computer che si sta utilizzando.

TESTWOL,TESTPING,TESTSHUT

Questi tre campi creati da noi possono contenere due valori (0 o 1) i quali determinano specifici procedimenti.

Come andremo a descrivere più avanti se un indirizzo IP presenta il numero ad esempio 1 vuol dire che il test può avvenire al contrario se il numero comporta lo 0 il test richiede dei problemi (impossibilità del calcolatore, pc indispensabile per altre applicazioni) oppure una mancanza di dati nei database (esempio mac, ram ,ws ecc..)

PASSWORD

Contiene la password necessaria per inviare il comando di spegnimento verso il computer remoto, cioè quando avviene la connessione e la password del computer remoto riconosce la decodifica scatta automaticamente la chiusura di Windows.

WAKE ON LAN (WOL)

L'accensione automatica di uno o più pc a distanza (Wake on lan) è una funzione molto richiesta sia dagli utenti classici sia da professionisti o amministratori di rete. Tutti sapete che il Computer si può accendere manualmente semplicemente premendo il tasto Power ma questo è il metodo classico e se vogliamo anche un po' antico. Bisogna imparare ad utilizzare ciò che la tecnologia ci mette a disposizione, in questo modo aumentiamo la nostra produttività e pure quella degli altri riuscendo a fare cose che magari il giorno prima non ci saremmo neanche sognati di realizzare. Questa funzione permette non solo di utilizzare una nuova tecnologia che ci viene messa a disposizione, ma consente anche a chi la utilizza di risparmiare tempo, aumentando così la produttività dell'azienda o del singolo individuo.

Pensiamo solo che se introdotta in un'ampia azienda consentirebbe di far svolgere comodamente a un qualsiasi individuo seduto davanti al proprio pc , operazioni noiose e per la maggior parte inutili.

All'interno del nostro istituto per esempio questo programma permetterebbe a un singolo tecnico tramite il PC docente, di avviare in pochi secondi tutti i calcolatori presenti nel suo laboratorio.

E' forse la modalità più complicata per l'accensione dei calcolatori da remoto da mettere in atto ma anche, a mio avviso, la più potente e la più interessante. Con questa modalità è sufficiente collegare il vostro PC in rete(LAN), dopodichè con un programma che invia dei pacchetti speciali (tipo pacchetti ICMP del Ping detto MAGIC PACKET) alla scheda di rete potrete accendere il Computer.

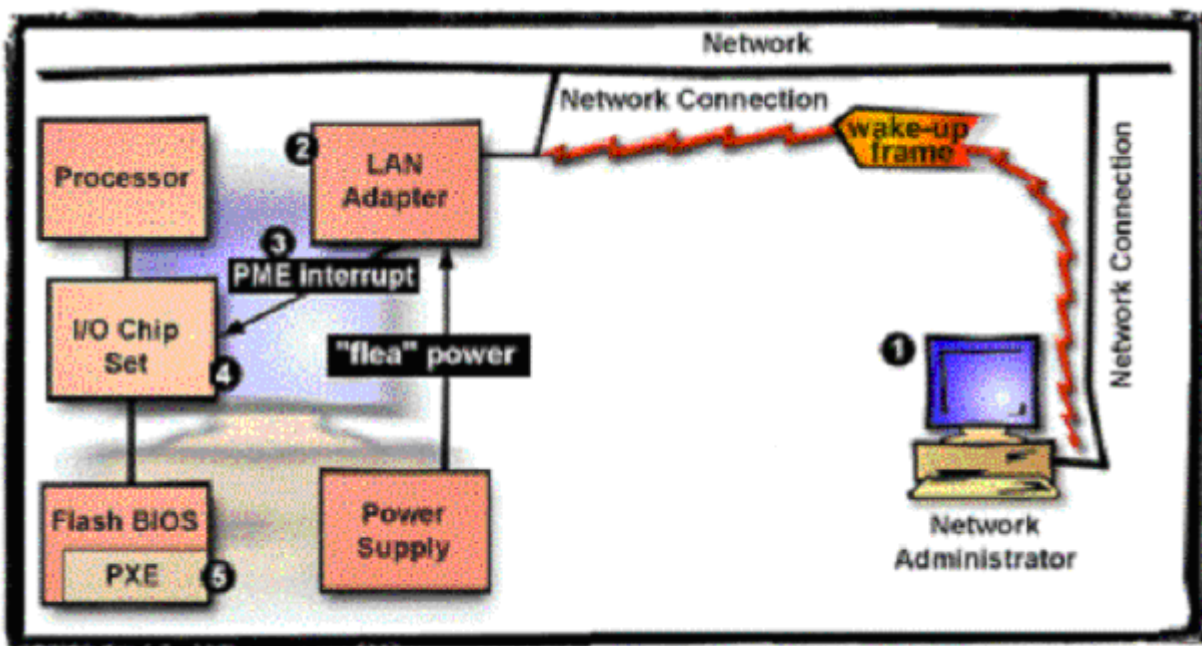


Figure 1. Wakeup On LAN

Vediamo un po' che cosa bisogna fare per utilizzare il Wake on Lan. E' necessario prima di tutto che il BIOS venga impostato per questo tipo di accensione WOL. Molti si chiederanno cos'è il bios e a cosa serve?

Il BIOS è l'acronimo di Basic Input/Output System.

E' una specie di programmino immagazzinato all'interno di un chip di memoria della vostra scheda madre.

```
Power Button Override: Disabled
Resume by LAN       : Disabled
Power On by Ring   : Disabled
Power On by Alarm  : Enabled
- Date(of Month)   : 20
- Time(hh:mm:ss)  : 12:30: 0
```

un menù presente nei bios

Agendo sul BIOS è possibile modificare numerose impostazioni o attivare particolari funzioni :

- Modificare la frequenza della CPU
- Leggere la temperatura di lavoro della CPU, il numero di giri delle ventole di raffreddamento ecc.
- Modificare l'unità di avvio
- Modificare ora e data del sistema (che vengono mantenute da una batteria)
- Attivare le funzioni di Risparmio energetico
- Attivare la funzione Wake on Ring (WOR) che permette di accendere il computer con una telefonata al modem
- Attivare la funzione Wake on Lan (WOL) che permette di accendere il computer via rete ,così il nostro Pc saprà che dovrà rimanere in qualche modo in ascolto di eventuali segnali che arriveranno sull'interfaccia di rete ; infatti la scheda di rete vi segnalerà anche a Computer spento la sua attività, accendendo il led di Link .



una scheda di rete in attesa

Dopo aver impostato il bios in maniera che resti in ascolto anche se spento, ora abbiamo bisogno del **MAC Address** della scheda di rete e l'ip del calcolatore da risvegliare .

A questo punto andando a richiamare un software (Wake on Lan Command Line) che lavora in ambiente Dos inserendo i dati ricavati in questo modo:

wolcmd(che sarebbe il comando esecutivo) [Mac address] [IP] [subnet mask(broadcasting che sarebbe 255.255.255.0)] [porta]

Se ad esempio volessi accendere un computer che ha queste caratteristiche:

Ip 192.168.145.7 ; Mac 00:A3:27:22:FC:97 ;dovrei scrivere la seguente istruzione

Wolcmd 00A32722FC97 192.168.145.7 255.255.255.0 81.

Una volta avviata questa procedura verranno inviati dei pacchetti magici che faranno accendere il computer desiderato.

Il "pacchetto magico" o meglio dire "Magic Packet" è una serie di bytes che vengono inviati su un nodo di rete; aventi una struttura di questo genere:

- a) una intestazione o "header" costituita da 6 bytes (6 valori esadecimali 0xFF o \$FF)
- b) il MAC address della scheda destinataria del comando ripetuto 16 volte;

Esempio se il MAC address è 00:A3:27:22:FC:97 (6 bytes), allora il "Magic Packet" avrà la seguente struttura :

FFFFFFFFFFFF

00A32722FC97 00A32722FC97 00A32722FC97 00A32722FC97

00A32722FC97 00A32722FC97 00A32722FC97 00A32722FC97

00A32722FC97 00A32722FC97 00A32722FC97 00A32722FC97

00A32722FC97 00A32722FC97 00A32722FC97 00A32722FC97

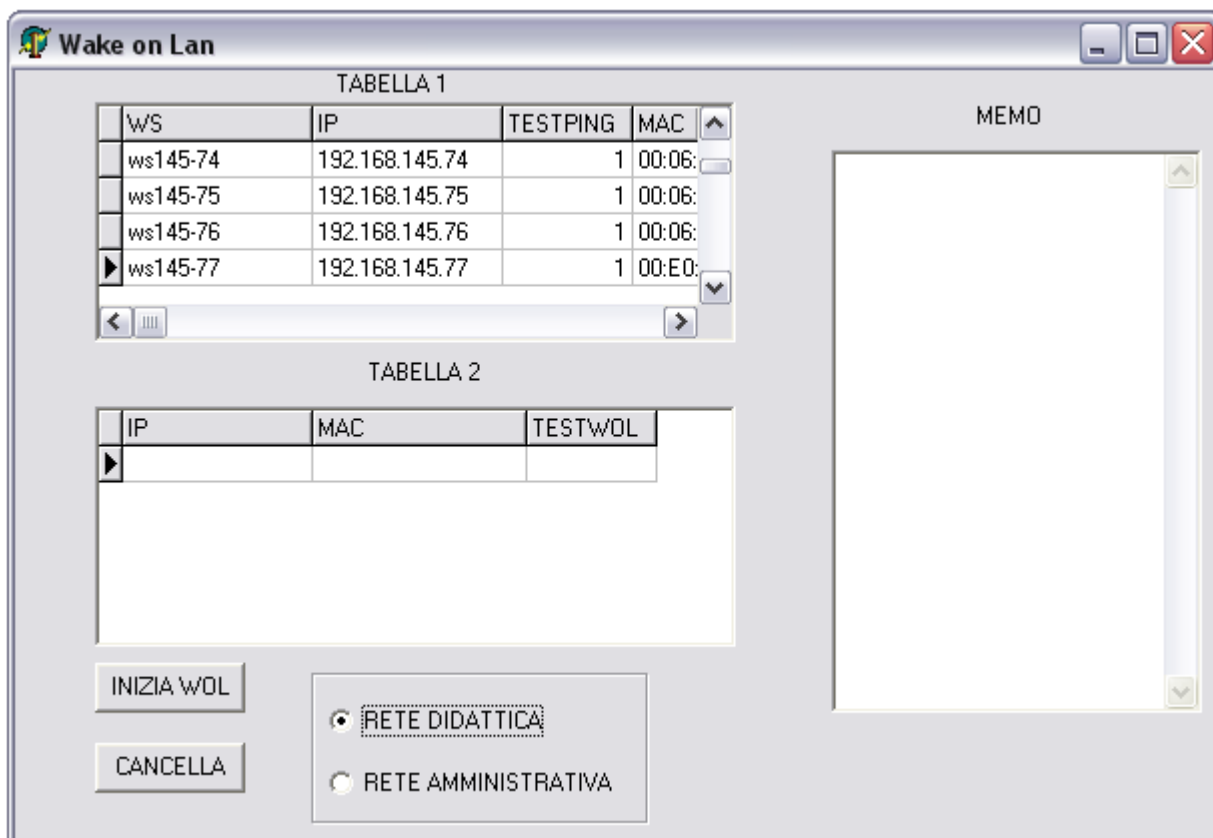
PROGRAMMA WAKE ON LAN

Il nostro progetto siccome la tecnologia moderna richiede molta più produzione in un tempo strettamente ridotto, abbiamo cercato di eliminare o almeno ridurre al minimo operazioni noiose all'interno del nostro istituto come eliminare l'accensione manuale dei calcolatori ,tramite l'aiuto del wol ma con delle opzioni che potrebbero creare vantaggi molto sorprendenti riguardo il campo informatico e aziendale.

Di fatti elaborando il programma che abbiamo descritto prima, ci siamo chiesti ma se noi volessimo accendere circa un centinaio di computer in pochi secondi stando seduti di fronte al nostro computer, come faremmo?

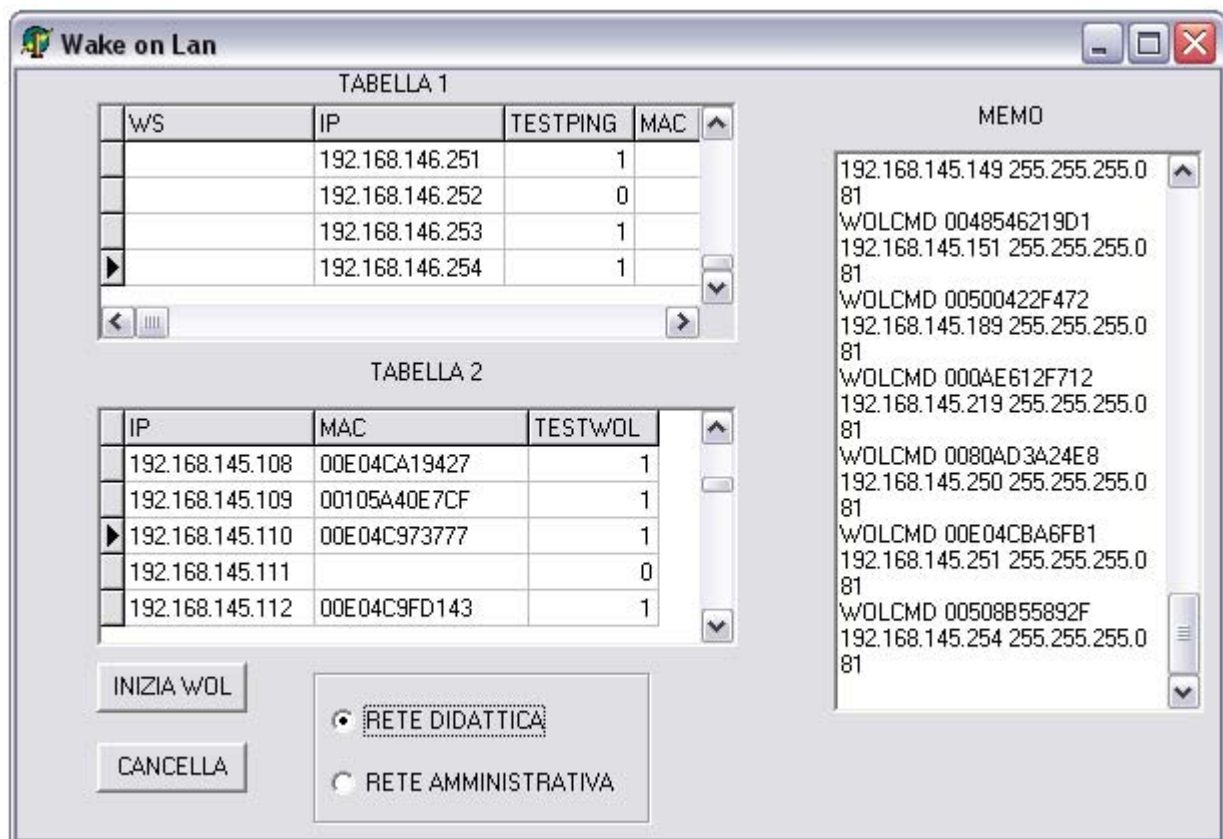
Per accendere un pc il software che gestisce il wake on lan a bisogno di una istruzione per calcolatore e se invece i calcolatori diventassero un centinaio dovremmo perdere una giornata intera a scrivere procedure; per questo abbiamo creato un progetto che ci risolva questi problemi.

Andiamo ad esaminare il programma:



L'immagine superiore raffigura il progetto creato; da come si può notare è presente nel riquadro superiore il nostro database(tabella1) con tutte le descrizioni delle macchine presenti nel nostro istituto riassumendole brevemente troviamo il nome di ogni computer,l'indirizzo ip,il mac,il luogo, distinzione di rete, i vari test possibili da svolgere ecc;al di sotto un altro database(tabella2) per il momento vuoto che dopo andremo a spiegare il perché,una memo anch'essa vuota, due pulsanti di comando e una alternativa distinzione di rete.

Lanciando il programma in esecuzione e premendo il pulsante "INIZIA WOL" verranno eseguite tutte le procedure da noi desiderate.



Prima di tutto la tabella1 provvederà a trasferire tutti gli indirizzi ip ,il mac ,la possibilità del test nella tabella2 .

Una volta riempita, tutti questi dati passeranno in rielaborazione cioè se è stata attivata come si vede in figura ,la rete didattica, tutti gli indirizzi ip aventi queste 9 cifre 192.168.145.xxx con il testwol a 1 (viene messo quando è possibile tentare il wol) verranno riportate nella memo in parte con i rispettivi mac accompagnati inoltre dal comando wolcmd,il broadcasting (che rimarrà uguale per tutti) e numero di porta e scartati se il testwol sarà 0. Stessa cosa capiterà se la rete sarà quella amministrativa solo che verranno presi in considerazione i dati contenenti le cifre 192.168.146.xxx e i rispettivi mac.

Premendo il pulsante "CANCELLA" invece la tabella2 e la memo verranno cancellate .

Una volta che la memo avrà terminato di copiare i dati dalla tabella2 verrà creato un file esecutivo che prenderà il nome wol.bat e a questo punto partirà automaticamente il software in dos (Wake on Lan Command Line) il quale invierà i cosiddetti pacchetti magici verso i nodi di rete da noi selezionati.

```

C:\WINNT\System32\cmd.exe
D:\Wake On Lan\Command Line>wolcmd
Wake On Lan Command Line...

Usage: wolcmd [mac address] [ipaddress] [subnet mask] [port number]
i.e. wolcmd 009027a322fc 195.188.159.20 255.255.255.0 8900
Copyright Depicus <Brian Slack> 1966-2002

D:\Wake On Lan\Command Line>wolcmd 009027a322fc 195.188.159.20 255.255.255.0 8900
0

Wake On Lan signal sent to Mac Address 009027a322fc
via Broadcast Address 195.188.159.255 on port 8900

D:\Wake On Lan\Command Line>

```

esecuzione del programma(Wake on Lan Command Line in ambiente dos) guidato dalle nostre procedure con i dati desiderati

Programma Wake on Lan (linguaggio Delphi)

```

procedure TForm1.FormActivate(Sender: TObject);
var k:integre;
begin
  for k:=1 to table2.recordcount do
    table2.delete;
    memo1.clear;
end;

```

Quando il programma va in esecuzione la tabella 2 e la memo vengono cancellate

```

procedure TForm1.Button1Click(Sender: TObject);
var Ipl,macl,SUB,st:string;
    k,tw:integer;
begin
  Table1.First TABELLA2
  If table2.recordcount = 0 Then
    Begin
      logf.LogToFile(TimeToStr(Now)+' CREAZIONE TABELLA TESTWOL');
      for k:=1 to table1.recordcount do
        begin
          IPL := Table1.FieldName('IP').AsString;
          MACL :=Table1.FieldName('MAC').AsString;
          MACL := Copy(MACL,1,2)+ Copy(MACL,4,2)+
            Copy(MACL,7,2)+ Copy(MACL,10,2)+
            Copy(MACL,13,2)+ Copy(MACL,16,2);
          TW :=Table1.FieldName('TESTWOL').AsInteger;
          Table2.Append;
          Table2.FieldName('IP').AsString:=IPL;
          Table2.FieldName('MAC').AsString:=MACL;
          Table2.FieldName('TESTWOL').AsInteger:=TW;
          Table2.Post;
          Table1.Next;
        end;
      end;
      If Rg1.ItemIndex = 0

```

Inizio trasferimento dati dalla tabella1 alla tabella 2

```

Then logf.LogToFile(TimeToStr(Now)+' WOL SU RETE DIDATTICA')
Else logf.LogToFile(TimeToStr(Now)+' WOL SU RETE AMMINISTRATIVA') ;
Table2.First;
for k:=1 to table2.recordcount do
begin
  IPL:= Table2.FieldByName('IP').AsString;           Rielaborazione dati tabella2
  SUB:= copy(IPL,9,3);
  MACL:=Table2.FieldByName('Mac').AsString;
  TW :=Table2.FieldByName('TESTWOL').AsInteger;
  if (macl<>'') AND (tw<>0)                          Verifico se il testwol è a 1
  THEN
    Begin
      if (SUB='145') AND (RG1.ItemIndex=0)           Se il testwol è a 1 controllo la rete
      OR (SUB='146') AND (RG1.ItemIndex=1)         selezionata e la invio alla memo
      Then                                          con i rispettivi comandi
        Memo1.Lines.Add('WOLCMD '+MACL+' '+IPL+' 255.255.255.0 81');
    end
  Table2.next
End;
Memo1.Lines.SaveToFile('wol.bat');                  Creo il file wol.bat
if ShellExecute(Application.Handle,Pchar('open'),Pchar('wol.bat'),
  Pchar(''),Nil,SW_NORMAL) <=32                    Esecuzione file wol.bat e inizio invio
Then                                              magic packet
  logf.LogToFile(TimeToStr(Now)+' IMPOSSIBILE ESEGUIRE WOL.BAT')
Else logf.LogToFile(TimeToStr(Now)+' ESEGUITO WOL.BAT ');
End;

procedure TForm1.Button2Click(Sender: TObject);
var k:integre                                     Cancellazione tabella2 e memo
begin
  for k:=1 to table2.recordcount do
  table2.delete;
  memo1.Clear;
  logf.LogToFile(TimeToStr(Now)+' CANCELLAZIONE TABELLA TESTWOL ');
end;

procedure TForm1.FormCreate(Sender: TObject);
begin
  logf.LogToFile(TimeToStr(Now)+' APERTURA PROGRAMMA WOL ');
end;

procedure TForm1.FormClose(Sender: TObject; var Action: TCloseAction);
begin
  logf.LogToFile(TimeToStr(Now)+' CHIUSURA PROGRAMMA WOL ');
end;

end.

```

Inoltre nel sorgente, in alcune righe, si può leggere "logf.LogToFile..." .Questo non è altro che un componente Delphi ,che ci "relaziona" durante l'esecuzione del programma ,gli eventi più importanti e li salva in un file di testo . Con questo,riusciamo a risalire ad eventuali problemi, o solamente ad avere un resoconto del lavoro svolto.

Ad esempio:

```
Open "wol.log" : 02/06/2004
02/06/2004-1.34.54 APERTURA PROGRAMMA WOL
02/06/2004-1.34.57 CREAZIONE TABELLA TESTWOL
02/06/2004-1.34.57 WOL SU RETE DIDATTICA
02/06/2004-1.34.58 ESEGUITO WOL.BAT
02/06/2004-1.35.02 CANCELLAZIONE TABELLA TESTWOL
02/06/2004-1.35.05 CREAZIONE TABELLA TESTWOL
02/06/2004-1.35.05 WOL SU RETE AMMINISTRATIVA
02/06/2004-1.35.06 ESEGUITO WOL.BAT
02/06/2004-1.35.12 CHIUSURA PROGRAMMA WOL
```

SHUTDOWN

Come abbiamo visto che esiste un metodo per accendere vari pc stando seduti comodamente sulla propria poltrona abbiamo cercato anche di ripetere la stessa operazione però cercando di farli spegnerli .

Potrà sembrare anche un'operazione inutile ma se stiamo a guarda può portare elevati vantaggi (riferito al nostro istituto):

- 1) Una diminuzione di un uso sprecato di corrente elettrica (molte volte capita che gli alunni alla fine delle ore di lezione lascino il computer acceso);
- 2) I tecnici non devono più girare per i laboratori in cerca di pc accesi;
- 3) I processori dei calcolatori smetteranno di stare in attesa per lunghe ore;

A differenza del wol ,lo shutdown richiede semplicemente tre caratteristiche fondamentali:

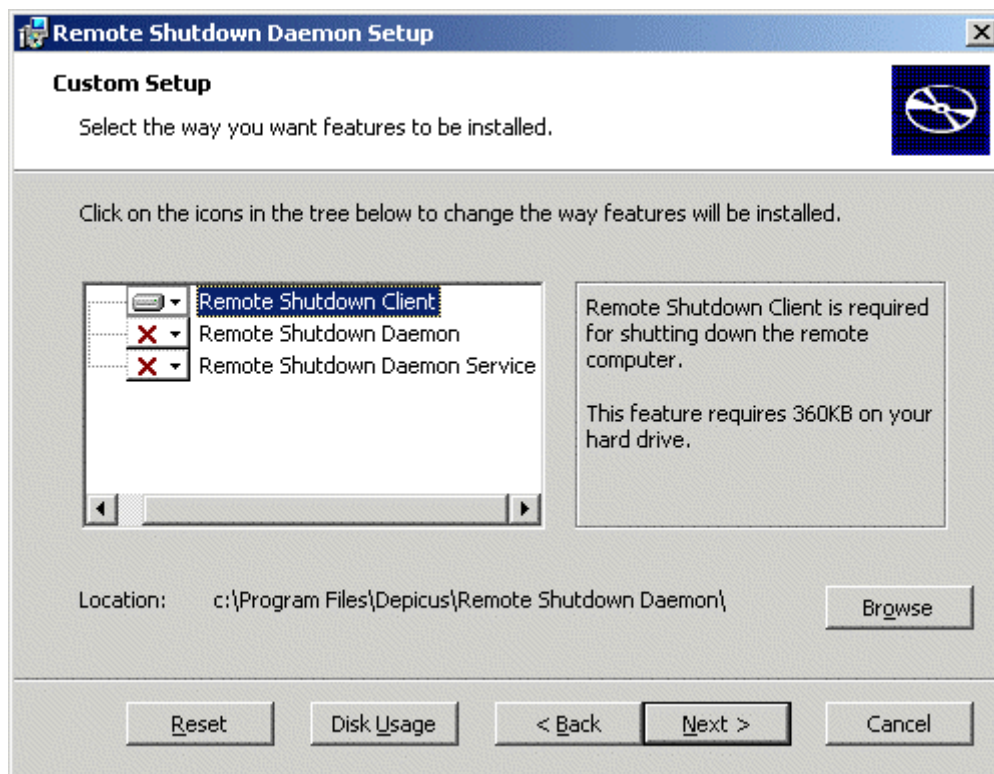
- 1) Lo spegnimento, come per l'accensione da remoto,avviene sempre se i pc son presenti sulla rete (basandoci al nostro progetto su una rete LAN);
- 2) Bisogna essere a conoscenza dell'indirizzo IP del computer da spegnere;
- 3) Su entrambi i pc bisogna installare il software che richiama lo spegnimento (il software che verrà installato sul pc da spegnere si comporterà come il client , mentre quello che invierà la richiesta si comporterà come un server)

Lo shutdwon da noi utilizzato fa riferimento a un software già presente, che però come andremo a vedere richiede molte operazioni per essere eseguito rispetto a delle variazioni che abbiamo creato noi nell'ambiente Delphi.

LO SHUTDOWN SCARICATO DA INTERNET

Prima di tutto dopo aver scaricato (www.depicus.com) oppure acquistato il software, avviene la parte più importante da svolgere per tutti i programmi :l'installazione .

Come abbiamo detto l'installazione richiede una particolare attenzione perché il software può comportarsi o da client o da server.



PING

Ping, acronimo di Packet InterNet Groper (ricercatore di pacchetto Internet), è un programma che serve per verificare la raggiungibilità di un host e i tempi di risposta. L'host potrà essere un computer collegato all'interno di una piccola rete LAN oppure una macchina connessa a Internet.

Il suo funzionamento è molto semplice. Il programma Ping invia un certo numero di pacchetti di dati al computer destinatario; se quest'ultimo è acceso e correttamente funzionante, una volta ricevuti i pacchetti, li rinvia istantaneamente al computer mittente. Il computer mittente conta il numero di pacchetti restituiti e il tempo impiegato e fornisce un report di statistiche sull'operazione avvenuta.

Questo, una volta ultimate le operazioni di cablaggio della rete e configurati i sistemi operativi, consentirà di verificare se tutti i computer sono collegati correttamente e se si

"vedono" tra loro. In altre parole, permetterà di capire se le macchine sono in grado di scambiare dati tra loro e di condividere risorse.

Secondo le impostazioni predefinite, il programma invia 4 pacchetti contenenti l'indirizzo IP della macchina dalla quale sono partiti ed una serie di dati di controllo (pacchetti di ECHO ICMP) che la macchina destinataria dovrà rispedire (pacchetti di ECHO). Ogni pacchetto è composto da 32 byte di dati, costituiti da una sequenza periodica di caratteri alfabetici

```
Prompt dei comandi
Microsoft Windows 2000 [Versione 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 192.168.0.2

Esecuzione di Ping 192.168.0.2 con 32 byte di dati:

Risposta da 192.168.0.2: byte=32 durata<10ms TTL=128
Risposta da 192.168.0.2: byte=32 durata<10ms TTL=128
Risposta da 192.168.0.2: byte=32 durata<10ms TTL=128
Risposta da 192.168.0.2: byte=32 durata<10ms TTL=128

Statistiche Ping per 192.168.0.2:
  Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
  Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\>
```

```
Prompt dei comandi

C:\>ping hdt-c4

Esecuzione di Ping hdt-c4 [192.168.0.2] con 32 byte di dati:

Risposta da 192.168.0.2: byte=32 durata<10ms TTL=128
Risposta da 192.168.0.2: byte=32 durata<10ms TTL=128
Risposta da 192.168.0.2: byte=32 durata<10ms TTL=128
Risposta da 192.168.0.2: byte=32 durata<10ms TTL=128

Statistiche Ping per 192.168.0.2:
  Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
  Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\>_
```

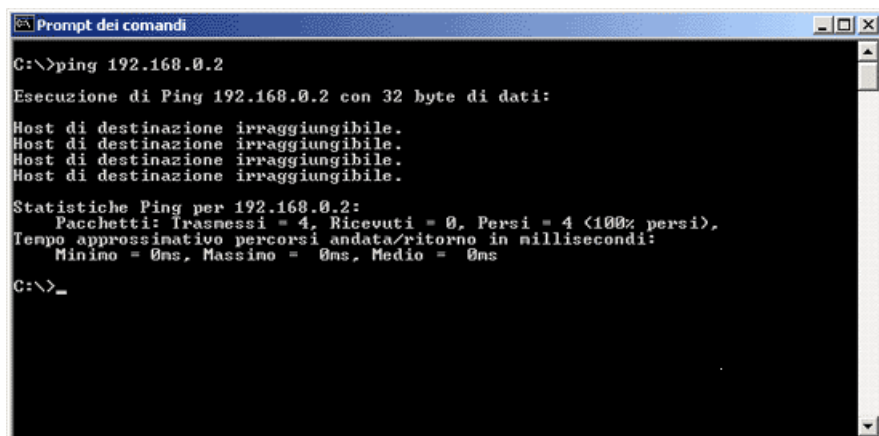
maiuscoli.

Entrambe le schermate sopra riportate mostrano chiaramente che la macchina pingata è perfettamente raggiungibile. Infatti, i 4 pacchetti da 32 byte inviati alla macchina 192.168.0.2 sono stati tutti rispediti alla macchina da cui è stato generato il ping. Dato inconfutabile, anche in virtù delle statistiche riportate nella parte inferiore delle schermate, che indica la percentuale dei pacchetti persi (zero) e i tempi di andata e ritorno degli stessi (nel nostro caso equivalgono a zero, poichè la macchina pingata è vicinissima). Un altro valore indicato nella schermata è il TTL (Time To Live), cioè il tempo massimo entro cui il pacchetto è considerato perso.

Ping

Vediamo ora il risultato del ping simulando un guasto hardware. Per realizzare questo test, abbiamo scollegiamo di proposito il cavo di rete della macchina da pingare.

La schermata sottostante mostra chiaramente che l'host in questione non è raggiungibile.



```
Prompt dei comandi
C:\>ping 192.168.0.2
Esecuzione di Ping 192.168.0.2 con 32 byte di dati:
Host di destinazione irraggiungibile.
Host di destinazione irraggiungibile.
Host di destinazione irraggiungibile.
Host di destinazione irraggiungibile.

Statistiche Ping per 192.168.0.2:
    Pacchetti: Trasmessi = 4, Ricevuti = 0, Persi = 4 (100% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\>_
```

Nel nostro progetto il ping è stato utilizzato per mettere a disposizione della scuola una funzione che permette di sapere in breve tempo, stando comodi davanti ad un solo PC, quanti computer sono accesi e quanti sono spenti, all'interno del nostro istituto.

Per far ciò abbiamo innanzitutto creato un database dove vengono riportati tutti gli indirizzi IP e i rispettivi MAC di ogni singolo computer, inserendo in esso anche altri due campi, denominati "test ping", e "orari". In quest'ultimo campo, abbiamo inserito 18 lettere N, che rappresentano i vari orari in cui è stato deciso di effettuare questo test, ossia dalle 6 alle 23. Ogni volta che il programma farà pingare i PC, ovvero una volta ogni ora, inserirà al posto delle N degli 1 o degli 0, l'uno significa che la macchina è accesa, mentre lo zero indica che quel computer o è spento o non è collegato in rete.

Il campo "test ping" è stato inserito per prevedere una possibile necessità, infatti solo con l'opzione descritta sopra è possibile pingare solo tutte le macchine, ma se volessimo o dovessimo rendere immune a questa operazione una o più macchine? Grazie a questo programma è possibile. Se nel campo test ping si inserisce un 1 la macchina verrà pingata, mentre se viene messo uno 0 non verrà interrogata dal nostro test. Successivamente è venuto spontaneo inserire un altro comando, stavolta sotto forma di check box, con il quale, a seconda se esso è attivo o no, trascura il comando inserito nel "test ping", sottoponendo

dunque tutte le macchine al nostro test. Il programma ping inoltre crea un report ogni ora dove vengono riportati i risultati del test.

Esempio:

Check box = attivo

Test ping = 1

Orari = 0001010NNNNNNNNNN

In questo caso il check box non disattiva il comando del test ping, quindi esso avendo il valore uguale a 1 fa procedere il test su quella macchina, infatti dalla casella orari si capisce che il programma è giustamente partito. Si può quindi dire che questo PC era spento o scollegato dalla rete alle 6, alle 7, alle 8, alle 10, e alle 12, mentre era acceso alle 9 e alle 11. Da questo esempio siamo in grado di dedurre che ci troviamo in un orario compreso tra mezzogiorno e le tredici, perché dalle tredici in poi non è stato effettuato alcun test, infatti sono presenti ancora le N.

PROGRAMMA “TEST SULLE MACCHINE ATTIVE”:

Questo programma è in grado di farci visualizzare i PC accesi sulla rete amministrativa e su quella didattica, di far selezionare la data e l'ora a cui si vuol vedere il risultato del test ping, e riportare all'interno di un memo l'indirizzo IP, il MAC, l'ora, la data, il numero di inventario, e il luogo delle macchine che erano accese quando sono state interrogate dal nostro test. Esso è dotato di due comandi che sono in grado di far selezionare la data e l'ora della ricerca, una tabella con riportati al suo interno tutti gli IP, un pulsante che avvia la ricerca, e un altro pulsante denominato "copia interping", con il quale si possono visualizzare gli IP fino all'ora e la data attuale.

Nascita della Intranet all'IPSIA Moretto: 1999 progetto ONION

Author's Signature:

Your signature verifies that to the best of your knowledge this document complies with all the ONION company policies and procedures, any applicable regulatory requirements, and that it completely and accurately describes the content of the study.

Name	Area	Date	Signature
E. Fagnoni	R&D	31 Marzo 1999	

Reviewer's Signature:

Your signature indicates that, as a content expert, you have reviewed this document and agree with its contents.

Name	Area	Date	Signature
M.Piotti	Communications/Technologies	31 Marzo 1999	

Approvers' Signatures:

Your signature affirms that the reviewers listed above are qualified to have addressed the content of this document, and that you agree with the intent and purpose of this document.

Name	Area	Date	Signature
E.Fagnoni	R&D	1 Aprile 1999	

Introduzione

Questo documento raccoglie alcune proposte e idee riguardanti l'architettura di rete e l'architettura di applicazioni intranet all'istituto Moretto.

Le proposte nascono dall'analisi delle specifiche della rete definite nel documento "La rete di Istituto : riunione del 5.XII.98 (Preside, Modiano, Prandelli, Azzani)" e dalla successiva riunione del 24.3.99 presso l'istituto Moretto.

Questo documento tratta i seguenti aspetti:

- architettura di rete: soluzioni tecniche per garantire la sicurezza tra la area didattica e area amministrativa;
- requisiti dei principali nodi di rete: una proposta per i requisiti HW e SW per le principali macchine coinvolte nell'architettura di rete;
- architettura applicativa: proposta per l'architettura ad alto livello delle applicazioni Intranet

Architettura di rete

Per soddisfare i requisiti di sicurezza richiesti occorre sezionare elettricamente in due parti (sottoreti) la rete dell'istituto: la sotto-rete della didattica e la sotto-rete amministrativa.

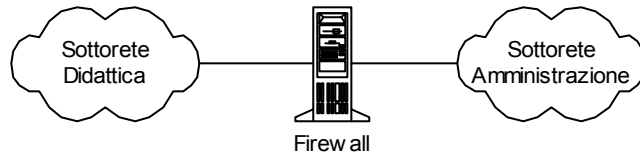
La sotto-rete didattica collega tutte le macchine dei laboratori ed in generale le macchine accessibili fisicamente agli studenti (ovvero macchine poste in aule, locali pubblici etc.)

La sotto-rete amministrativa collega tutte le macchine poste negli uffici e non fisicamente accessibili dagli studenti.

Ogni sotto-rete realizza propri metodi sicurezza (es. accessi e password) ma, indipendentemente dalle regole di sicurezza impostate sulle singole reti valgono i seguenti principi:

- Nessuna macchina attestata sulla rete didattica ha accesso alla rete amministrativa.
- Le macchine attestate sulla rete amministrativa possono (se autorizzate) accedere alle macchine poste sulla rete didattica.

In sostanza si prevede il collegamento delle due sottoreti attraverso una speciale macchina chiamata “firewall” che, essendo collegata ad entrambe le reti tramite due schede, di governare l’interscambio di dati tra le due aree.

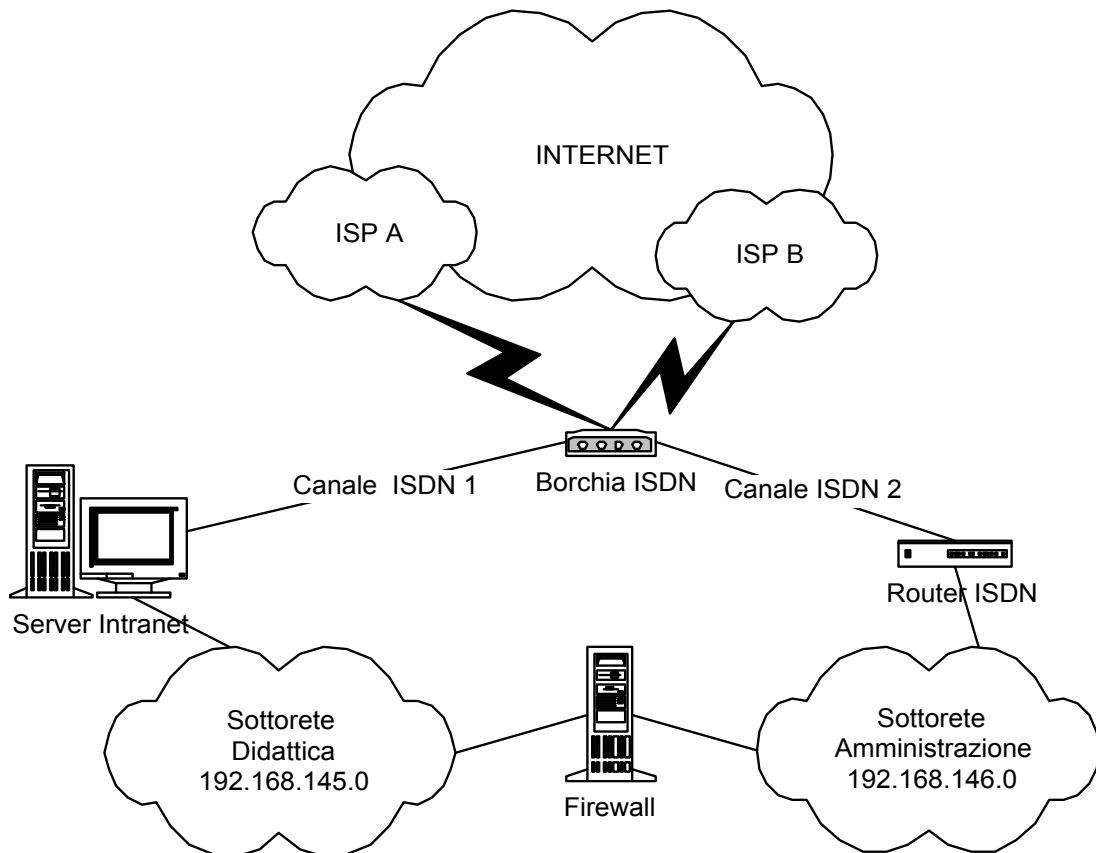


Per consentire l’accesso a Internet da entrambe le sottoreti si consiglia di impostare due accessi separati via ISDN. La soluzione proposta presenta i seguenti vantaggi:

- consente di impostare politiche di accesso differenti tra rete amministrativa e didattica (scelta ISP, velocità, etc.)
- consente agli studenti più capaci (sempre sotto adeguato controllo) di sperimentare le tecnologie di comunicazione senza porre problemi di sicurezza e affidabilità alla rete amministrativa.
- aumenta il throughput complessivo della rete, separando il traffico amministrativo da quello degli studenti.
- Gestisce in modo ottimale la capacità della linea ISDN che consente appunto due connessioni contemporanee a 64k.

Lo svantaggio di questa soluzione è dato dalla necessaria duplicazione degli apparati di collegamento (schede o router) e la duplicazione del contratto con ISP. Si sottolinea che una singola connessione ISDN (BRI) supporta due canali dati indipendenti a 64Kbps ed è quindi sufficiente per supportare due accessi ISDN Internet distinti in completa sicurezza.

In sostanza l’architettura di rete è schematizzata dalla seguente figura:



I principali componenti della architettura sono:

Server Intranet	Server primario della rete didattica con funzioni di: <ul style="list-style-type: none">- accesso alla rete Internet e funzioni di NAT (Network Address Translation)- server Web intranet- data-warehouse per le applicazioni intranet- mail server della rete didattica (studenti)- DNS primario di rete
Router amministrazione	Router per accesso Internet da parte della sotto-rete amministrativa con funzioni di NAT
Firewall	Punto di contatto tra la sotto-rete didattica e la sotto-rete amministrativa con le seguenti funzioni: <ul style="list-style-type: none">- firewall- mail server rete amministrativa- default gateway- DNS secondario di rete
Borchia ISDN	Accesso BRI ISDN dedicato che consente l'attivazione di due connessioni a 64Bbps verso due ISP

Requisiti dei principali nodi di rete

Questo capitolo raccoglie i requisiti HW, SW e di servizio dei principali nodi di rete definiti nella architettura descritta nel capitolo precedente.

Requisiti di collegamento delle macchine alla rete

Per garantire l'isolamento delle due sottoreti e- necessario il rispetto delle seguenti regole:

1. nessuno switch o hub attestato sulla rete Moretto può contenere sia macchine della sotto-rete amministrativa che macchine della sotto-rete.
2. le macchine della sotto-rete didattica e le macchine della sotto-rete amministrativa devono avere indirizzi tratti da due classi di indirizzi IP distinte. Si consiglia di utilizzare un indirizzamento statico (gestito tramite DNS) in cui le macchine della rete didattica abbiano indirizzi appartenenti alla rete 192.168.145.0 mentre le macchine della rete amministrativa abbiano un indirizzo della rete 192.168.146.0.

Operativamente:

- tutte le macchine della rete didattica devono avere assegnato un IP univoco scelto nel range 192.168.145.3 – 192.168.145.254 (l'indirizzo 1 viene riservato per il firewall, il 2 al server intranet)
- tutte le macchine della rete amministrativa devono avere assegnato un IP univoco scelto nel range 192.168.146.2 – 192.168.146.254 (l'indirizzo 1 viene riservato per il firewall)
- agli indirizzi va assegnato un nome mnemonico da registre tramite DNS sul server intranet (di entrambe le reti)
- nessun hub o nessuno switch può avere collegato contemporaneamente macchine con indirizzi 192.168.145.x e macchine 192.168.146.x

Le macchine nella sotto-rete didattica avranno quindi la seguente configurazione di rete:

Host name:	<nome univoco>
IP address:	192.168.145. x (x= numero univoco tra 3 e 254)
Netmask:	255.255.255.0
Default gateway:	192.168.145.1 (il firewall)
DNS primario:	192.168.146.2 (server intranet)
Domain:	rd.moretto.edu

Le macchine nella sotto-rete amministrativa avranno la seguente configurazione di rete:

Host name:	<nome univoco>
IP address:	192.168.146. x (x= numero univoco tra 3 e 254)
Netmask:	255.255.255.0
Default gateway:	192.168.146.1 (il firewall)
DNS primario:	192.168.145.1 (firewall intranet)
Domain:	ra.moretto.edu

Router amministrazione

Il router dell'amministrazione ha la funzione di collegare ad Internet la sotto-rete dell'amministrazione. E' necessario che sia programmato per:

- gestire la chiamata al provider quando necessario (dial-on-demand)
- mascherare gli indirizzi interni con l'indirizzo assegnato dal provider (NAT)

Operativamente si può mantenere l'attuale router con lievi modifiche alla configurazione oggi in uso.

Server Intranet

Il server intranet è una macchina centrale nella architettura di rete proposta. Si trova nella sotto-rete didattica e svolge i seguenti importanti compiti:

- collega la rete didattica a Internet
- gestisce il DNS (Domain name system) principale per entrambe le reti
- gestisce la posta elettronica degli studenti
- fa funzionare le applicazioni intranet su interfaccia Web
- gestisce il database con le informazioni messe a disposizione dalla area amministrativa

Pur gestendo importanti servizi, un malfunzionamento sul server intranet non pregiudica in alcun modo l'operatività e la sicurezza della rete amministrativa.

Ciò detto è comunque indispensabile che il server intranet sia amministrato con attenzione e utilizzando tutte le tecniche di controllo e prevenzione accessi non autorizzati. Il server intranet dovrebbe essere posto in un locale non accessibile agli studenti, possibilmente non nello stesso locale del firewall.

Si consiglia la seguente configurazione HW:

- PC intel Pentium II (anche un compatibile va bene)
- Minimo 128Mbyte di RAM (256 consigliati)
- 8GB hd
- Scheda ISDN
- Scheda rete Ethernet

Si consiglia inoltre la seguente configurazione per il SW di base:

- NT Server (4.0 o Windows 2000 server quando disponibile)
- IIS 4.0
- MS Proxy server
- MS SQL Server 7.0
- MS Exchange

Il software può essere acquistato da Microsoft usufruendo delle particolari condizioni riservate agli istituti didattici. Probabilmente esistono agevolazioni specifiche a livello di provveditorato.

Firewall

Il firewall è un nodo di rete particolarmente delicato, il suo compito principale è di mettere in comunicazione le due sottoreti governandone il traffico in modo controllato tramite regole (policy).

Fisicamente la macchina ha due schede ethernet di cui una ha un indirizzo nella sotto-rete didattica (192.168.145.1) e l'altra ha un indirizzo della sotto-rete amministrativa (192.168.146.1).

La configurazione della macchina è delicata e soggetta a poche modifiche. La gestione di tale macchina è quindi complicata anche se relativamente poco onerosa (sono richiesti interventi solo a fronte di guasti).

Esistono in commercio molti tipi di firewall, alcuni esclusivamente HW altri basati su HW e SW. In generale si sconsiglia l'utilizzo di macchine NT come base per sistemi Firewall.

ONION S.p.A. sarebbe onorata di poter sponsorizzare il progetto di networking del Moretto con la fornitura e la configurazione di un proprio INTERPRISE ONION SERVER. Uno dei più sofisticati firewall disponibili sul mercato.

Il firewall basato su ONION Interprise è in grado di svolgere le seguenti funzioni:

- controllo del traffico tra le varie sottoreti e tra le singole macchine di reti diverse;
- routing tra le sottoreti;
- DNS secondario;
- Mail server per area amministrativa;

Vincoli sull'architettura delle applicazioni

La realizzazione della infrastruttura descritta nei capitoli precedenti non è sufficiente per garantire la realizzazione delle specifiche richieste.

E' infatti necessario organizzare le applicazioni di rete su un modello che si potrebbe definire di data-warehouse.

In questo modello, la macchina che realizza i servizi disponibili in Intranet, non accede direttamente alla sorgente dei dati ma interroga un proprio database che contiene una copia dei dati reali, riorganizzata sia per logica che per tecnologia di accesso.

I dati vengono periodicamente rinfrescati dalle applicazioni nell'area amministrativa

In breve, le applicazioni Intranet avranno le seguenti caratteristiche:

- funzioneranno tutte sul server Intranet (ad esempio potrebbero essere delle applicazioni scritte con la tecnologia ASP)
- le applicazioni intranet accederanno ai dati posti su un database (es. MS SQL server 7.0 o Access) posto sul server intranet stesso.
- Il database conterrà solo i dati strettamente necessari alla realizzazione delle applicazioni. Non conterrà le informazioni sensibili che risiedono esclusivamente nella rete amministrativa e quindi tali dati non potranno essere acceduti dalle applicazioni Intranet.
- L'accesso al database ed alle applicazioni sarà soggetto alle regole di sicurezza impostate sul server Intranet tramite le funzionalità di NT server.
- Gli applicativi nella sotto-rete amministrativa dovranno, ad intervalli di tempo schedulati (es. tutte le notti), inviare in un formato standard (ASCII o Access) porzioni dei propri archivi sulla macchina Intranet. In caso di archivi molto grossi, (oltre 10M) l'invio potrebbe riguardare solo i record modificati. Nel caso gli applicativi dell'area amministrativa non prevedano una funzione di export parziale dei dati occorrerà approntare dei piccoli programmi specifici.
- Periodicamente (es. ogni notte) il database sul server Intranet processerà i nuovi dati ricevuti inserendoli nella propria struttura. In pratica l'intero database sul server Intranet potrebbe essere completamente ricostruito ogni notte.
- Occorre sottolineare che, grazie all'impostazione del firewall, gli applicativi dell'area amministrativa potranno senza problemi accedere a tutti i dati presenti sul server Intranet. Un'altra possibilità di comunicazione tra applicativi Intranet e l'area amministrativa è data dall'e-mail.

Questa architettura presenta molti vantaggi:

- il server può accedere solo ad un insieme di dati limitato (quindi sono protetti i dati più sensibili)
- i dati sono presentati alle applicazioni con una logica ad esse ottimizzata. Ne consegue una maggiore semplicità di scrittura delle applicazioni.

- i dati possono essere organizzati in un formato coerente e efficiente indipendentemente dal formato dei dati sorgente.
- un problema di sicurezza o sistemistico sul server Intranet non pregiudica i livelli minimi di sicurezza e non pregiudica le applicazioni dell'area amministrativa

Esistono ovviamente alcuni svantaggi:

- i dati importati sono in read-only e non possono essere modificati dagli applicativi Intranet
- i dati non sono aggiornati in real-time ma il loro aggiornamento dipende dalla frequenza di rinfresco (tipicamente una volta al giorno)
- i dati più sensibili non sono trasmessi dalla amministrazione al server intranet e quindi non sarà possibile per le applicazioni intranet accedervi.

Sintesi delle attività

In sintesi ed ad alto livello ecco le attività che si consigliano di realizzare:

1. Separare le macchine della didattica dalle macchine dell'amministrazione utilizzando hub e switch differenti.
2. Attuare le diverse politiche di indirizzamento IP sulle varie macchine
3. Assicurarsi l'utilizzo dedicato di una linea ISDN (borchia) scollegata dal centralino
4. Impostare il server intranet con particolare attenzione ai componenti di accesso a Internet (RAS e Proxy)
5. Attivare un nuovo accesso Internet per la didattica
6. Riconfigurare il router amministrazione
7. Installare e configurare il firewall
8. Richiedere dominio Internet (es. moretto.edu o moretto.it) e impostare il DNS
9. Impostare e configurare la posta elettronica per la parte amministrativa su firewall
10. Impostare e configurare la posta elettronica sul server Intranet (Exchange)
11. Realizzare su server intranet la struttura in HTML del sito intranet
12. Configurare tutte le macchine
13. Definire le politiche di sicurezza e di uso della rete
14. Eseguire i corsi per diffondere l'uso della posta elettronica e intranet e le policy di sicurezza
15. Pianificare e progettare le applicazioni Intranet
16. Installare e definire la struttura del database sul server Intranet
17. Pianificare e realizzare l'export dei dati sulle applicazioni amministrative
18. Pianificare e realizzare l'import dei dati su server intranet
19. Scrivere le applicazioni Intranet

IP version 4 (IPv4) addresses are 32 bits long, as [Figure A](#) shows. IPv4 addresses typically occur as a sequence of four numbers that represent the decimal value of each of the address bytes. Because periods separate the values in IPv4 addresses, the IPv4 address notation is called dotted decimal.

IP addresses are hierarchical for routing purposes (as are the addresses of all Open Systems Interconnection—OSI—network layer protocols) and divided into two subfields. The Network Identifier (NET_ID) subfield identifies the IP subnetwork and facilitates high-level routing between networks in much the same way country codes, city codes, and area codes facilitate routing in telephone networks. The Host Identifier (HOST_ID) subfield identifies the specific host within a subnetwork.

To accommodate different-size networks, IP defines several classful addresses. Classes A, B, and C apply to host addressing; the only difference between the three classes is the length of the NET_ID subfield.

Class A addresses have a 7-bit NET_ID and a 24-bit HOST_ID. Class A addresses apply to very large networks and can address up to 16,777,216 (2²⁴) hosts per network. The first segment of a Class A address is a number between 1 and 126; however, very few networks are this large. IBM's network has a Class A address.

Class B addresses have a 14-bit NET_ID and a 16-bit HOST_ID. Class B addresses apply to moderate-size networks and can address up to 65,536 (2¹⁶) hosts per network. The first segment of a Class B address is a number between 128 and 191. The Class B address space has been under threat of depletion for some time, and getting a new Class B address is difficult. (To learn more about the IP address-depletion problem and the coming change in IP addressing from IPv4 to IPv6, see Tao Zhou, "The Next Generation IP in Action," June 1998.) America Online's (AOL's) network has a Class B address.

Class C addresses have a 21-bit NET_ID and an 8-bit HOST_ID. These addresses apply to small networks and can address only up to 256 (2⁸) hosts per network. The first segment of a Class C address is a number between 192 and 223. Currently, most networks receive Class C (or sub-Class C) address assignments; one example includes Saint Michael's College in Colchester, Vermont.

The remaining two address classes apply to special functions only. Class D addresses, which begin with a value between 224 and 239, are for IP multicasting (i.e., broadcasting one packet to multiple hosts). Class E addresses begin with a value between 240 and 255 and are for experimental use.

Several NET_ID and HOST_ID values either are reserved or have special meaning. A HOST_ID of 0 is a dummy value reserved as a placeholder when referring to an entire subnetwork; the address 192.168.99.0 refers to a Class C address with a NET_ID of 192.168.99. A HOST_ID consisting solely of ones (usually written 255 but also sometimes depicted as -1) is the broadcast address and refers to all hosts on a network. The NET_ID value 127 is for loopback testing, and the address 127.0.0.1 refers to the localhost.

Request for Comments (RFC) 1918 reserves several NET_IDs for private network addresses, and routers won't pass packets over the Internet to these network addresses. The reserved NET_IDs are the Class A address 10.0.0.0 (formerly assigned to ARPANet), the 16 Class B addresses from 172.16.0.0 to 172.31.0.0, and the 256 Class C addresses from 192.168.0.0 to 192.168.255.0. Organizations with private network addresses frequently use the addresses on a network sitting behind a firewall or router that performs

Network Address Translation (NAT). NAT converts a host's private address to a public IP address for Internet use. One advantage to using NAT is that an organization need not change host addresses if the organization changes service providers and receives another public IP address.

An additional addressing tool is the subnet mask. The subnet mask indicates the portion of the address that identifies the network (or subnetwork) for routing purposes. The subnet mask appears in dotted decimal, and the total number of ones that a subnet mask contains identifies the significant NET_ID bits (for fans of Boolean logic, the subnet mask and the entire 32-bit IP address are ANDed together to obtain the relevant NET_ID bits). [Table A](#) shows the subnet mask and number of significant address bits for the NET_ID in classful IP addresses. Depending on the context and literature, subnet masks appear in dotted decimal form or simply as a number representing the number of significant address bits for the NET_ID. Thus, 192.168.99.17 255.255.255.0 and 192.168.99.17/24 both refer to a Class C NET_ID of 192.168.99.

Subnet masks can also subdivide a large address space or combine multiple small address spaces. A network might subdivide its address space to define multiple logical networks by segmenting the HOST_ID subfield into a Subnetwork Identifier (SUBNET_ID) and (smaller) HOST_ID. For example, an organization with an assigned Class B address space of 191.160.0.0 might segment the address into a 16-bit NET_ID, 4-bit SUBNET_ID, and 12-bit HOST_ID. The subnet mask for routing to the NET_ID on the Internet would be 255.255.0.0 (or 16 bits), and the mask for routing to individual subnets within the larger Class B address space would be 255.255.240.0 (or 20 bits). Alternatively, an organization with the assigned four Class C addresses of 223.168.128.0, 223.168.129.0, 223.168.130.0, and 223.168.131.0 might use the subnet mask 255.255.252.0 (or 22 bits) for routing to this domain. Using subnet masks in routing tables to consolidate addresses using NET_IDs that aren't one, two, or three bytes in length is termed Classless Inter-Domain Routing (CIDR).

TABLE A: Classful Address Subnet Masks and NET_ID Address Bits

Class	Subnet Mask	Number of Bits	Binary Representation
A	255.0.0.0	8	11111111 00000000 00000000 00000000
B	255.255.0.0	16	11111111 11111111 00000000 00000000
C	255.255.255.0	24	11111111 11111111 11111111 00000000