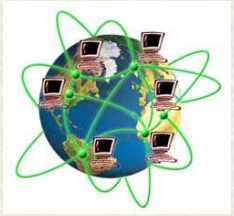
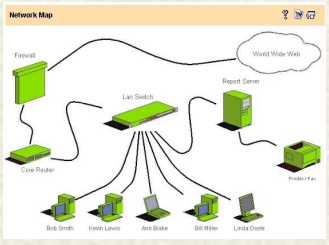
Le reti di calcolatori

Le reti di calcolatori – 1

- Una rete è un complesso insieme di sistemi di elaborazione connessi tra loro tramite collegamenti fisici (linee telefoniche, cavi dedicati, etc.) o con tecnologia ***wireless***, per condividere le *risorse disponibili* e per offrire *servizi di comunicazione*
- Il progetto di una rete copre ampie problematiche, che vanno dalla sua architettura fisica, alla codifica dei dati per facilitarne la trasmissione, fino alla costruzione del software applicativo che mette a disposizione degli utenti i servizi di rete





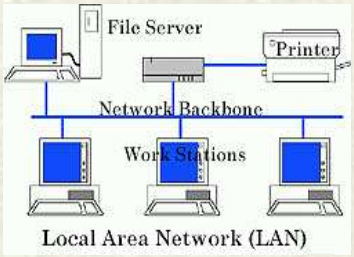
Le reti di calcolatori – 2

- I primi tentativi di trasmissione dati fra due elaboratori risalgono agli anni `40 (collegamento fra elaboratore centrale e terminali remoti)
- Le reti come le concepiamo oggi, ed i servizi ad esse collegati, hanno fatto la loro comparsa negli anni `70, da prima in ambito militare e poi negli ambienti universitari, per lo scambio di informazioni scientifiche
- Solo nell'ultimo decennio, però, grazie alla rapida evoluzione delle tecnologie telematiche, abbiamo assistito all'espandersi frenetico delle reti, sia a livello locale (nelle aziende e negli uffici), sia a livello mondiale (Internet)
- Di pari passo sono aumentati i servizi messi a disposizione dalle reti, che vanno dalla posta elettronica, al trasferimento di file, alla condivisione di risorse fisiche
- L'affermarsi delle reti sta ristrutturando il mondo informatico attraverso un processo, detto ***downsizing***, che spinge le aziende all'eliminazione dei grossi ***mainframe***, con decine di terminali, per sostituirli con reti di personal computer indipendenti, ma fra loro interagenti e cooperanti

Le reti di calcolatori – 3

- I principali servizi offerti da una rete di calcolatori sono:
  - Condivisione delle risorse hardware e software: più utenti possono accedere allo stesso modem, stampante, etc.; i file necessari a molti utenti, quali grosse database, possono essere gestiti su di un unico sistema ed essere resi disponibili attraverso la rete in modo che ciascun utente possa accedervi
  - Comunicazione fra utenti: possibilità di scambio messaggi, tramite la posta elettronica, e di accesso ad Internet, con relativo reperimento di informazione ipertestuale
  - Sicurezza: i dati cruciali possono essere accentrati e resi accessibili ai soli utenti opportunamente autorizzati; più copie degli stessi dati su macchine distinte offrono, grazie alla ridondanza, maggiori garanzie di salvaguardia da guasti

Le reti di calcolatori – 4



Local Area Network (LAN)

- LAN — *Local Area Network* — è una rete limitata ad un'area circoscritta (ad es., tutti i calcolatori di un laboratorio)
- MAN — *Metropolitan Area Network* — è una rete che si estende nell'ambito di medie distanze (fino a 100 Km) ed è costituita da più reti LAN connesse tra loro da ***bridge*** o ***router*** (una MAN connette l'Università di Firenze con quella di Siena)
- WAN — *Wide Area Network* — è una rete che si estende su una vasta area geografica di centinaia o migliaia di chilometri (ad esempio, è una WAN che collega i calcolatori di un'azienda, le cui sedi sono sparse in tutto il mondo)

I virus

I virus – 1

- Un virus informatico è un programma, spesso annidato all'interno di un programma "portatore" dall'apparenza innocua, che esegue azioni dannose: dalla comparsa di scritte sullo schermo, al danneggiamento di file e alla cancellazione di dati, fino alla modifica degli indici del disco rigido
- Il problema dei virus riguarda soprattutto Windows, ma ne esistono anche per Macintosh e Linux
- Oggi, il veicolo di infezione di gran lunga più diffuso è la posta elettronica, ma il problema riguarda in generale qualsiasi trasferimento di file fra computer diversi (attraverso dischi, *FTP* — ***File Transfer Protocol*** — o altro)

I virus – 2

- Installare un buon programma antivirus e tenerlo costantemente aggiornato costituisce sempre la miglior difesa contro i virus; l'aggiornamento è di fondamentale importanza per garantire una protezione veramente efficace
- Infatti, il riconoscimento dei virus avviene attraverso un'*impronta* caratteristica (*signature*), e un programma antivirus non è in grado di riconoscere i nuovi virus finché non ne possiede l'impronta
- Attraverso i signature file (o *definition* file), le case produttrici mettono a disposizione on–line tutte le informazioni sui nuovi "ceppi virali"; è bene effettuare l'aggiornamento dell'antivirus almeno ogni 15–30 giorni
- Tutto questo non mette al riparo dai virus appena creati:
  - Un virus particolarmente efficace (come il famoso *I love you* del maggio 2000) riesce a diffondersi capillarmente in tutto il mondo nel giro di poche ore, assai prima che si riesca ad isolarlo, definirne l'impronta e renderla disponibile on–line per l'aggiornamento
  - Nel momento in cui il virus nasce e viene diffuso, i programmi antivirus non hanno nessuna efficacia contro di esso: i primi giorni di vita sono quelli in cui il virus compie il maggior numero di danni

I virus – 3

- I programmi antivirus si possono scaricare attraverso Internet, dai siti delle case produttrici
- Installare l'antivirus quando la macchina è già stata attaccata è quasi sempre inutile…
  - …Molti virus, quando hanno preso il controllo della macchina, non si lasciano cancellare dall'antivirus e vanno rimossi manualmente
  - …Se l'antivirus riesce ad andare in esecuzione, si può sapere il nome del virus e quali sono i file che ha infettato, dopodiché, usando un altro computer non infetto, si possono cercare su Internet informazioni su come rimuovere il virus dalla macchina
  - Un sito molto interessante è la Virus Encyclopedia della *Symantec* (la casa che produce il Norton Antivirus), in cui vengono spiegati gli effetti di ogni virus e quali sono le procedure per la sua rimozione manuale

I tipi di virus – 1

- Programmi eseguibili: dall'apparenza innocua, caratterizzati (in genere) dall'estensione .exe; possono arrivare come allegati a messaggi di posta elettronica; il virus non si attiva se il programma non viene lanciato
  - Esistono virus che si appropriano della rubrica inviando una copia di se stessi a tutti gli indirizzi in essa contenuti, oppure virus che si allegano di nascosto a tutti i messaggi in partenza dalla macchina che hanno infettato
  - Può accadere di ricevere un messaggio, apparentemente inviato da un amico o conoscente, che contiene il virus come allegato

I tipi di virus – 2

- Per proteggersi: evitare di aprire i file allegati ai messaggi se non si è assolutamente certi della loro provenienza; più precisamente…
  - Non aprire un allegato che arriva da uno sconosciuto, specialmente se accompagnato da un messaggio amichevole o rassicurante
  - Se il messaggio arriva da un conoscente, ma il testo è assente o ha un'aria impersonale o è diverso dallo stile del mittente, potrebbe trattarsi di un falso messaggio generato dal virus (*I love you* funzionava così)
  - Un allegato con doppia estensione, es. "message_for_you.txt.vbs", è quasi certamente un virus: la prima è una falsa estensione, per far credere che l'allegato sia un innocuo file di testo (.txt) o un'immagine (.gif, .jpg), la seconda è la vera estensione del file (.vbs: visual basic script; .pif: program information file; .exe: executable)
  - Se il messaggio arriva da un conoscente che però non parla mai dell'allegato, il file potrebbe essere stato introdotto di nascosto dal virus nel momento in cui il messaggio veniva spedito
- La stessa prudenza riguarda tutti i file eseguibili che ci si procura per altra via; occorre evitare di scaricare software da siti sospetti o sconosciuti; nei siti pirata si rischia l'incontro con i Trojan, virus che di solito non procurano danni diretti, ma predispongono la macchina per essere presa sotto controllo dai pirati informatici ed essere usata per le loro incursioni nella rete

I tipi di virus – 3

- Macrovirus: sono ottenuti sfruttando le funzioni delle macro in documenti Word o Excel
  - Le macro sono istruzioni eseguibili inglobate all'interno dei documenti (pensate per automatizzare operazioni di uso frequente) e si attivano non appena il documento viene aperto: in una macchina infettata da macrovirus l'infezione si trasmette a tutti i documenti
  - Ogni file di Word, Excel, Access, etc., è potenzialmente in grado di contenere un macrovirus nascosto (e non basta essere certi della provenienza del file, perché chi lo ha inviato può averlo fatto senza accorgersi dell'infezione)
  - L'unica difesa è la disattivazione di tutte le macro prima di aprire i documenti (le versioni recenti di programmi come Word o Excel avvisano sempre l'utente dell'eventuale presenza di una macro prima di renderla attiva)

I tipi di virus – 4

- Script: i virus più insidiosi fra quelli diffusi attraverso la posta elettronica, perché non si presentano come allegato, ma sfruttano la possibilità, offerta da diversi mailer, di scrivere messaggi di posta elettronica in HTML, in modo da migliorare l'aspetto grafico del testo
  - Dato che una pagina HTML può contenere istruzioni attive (dette script), il messaggio può essere costruito in modo da svolgere azioni potenzialmente pericolose sul computer del destinatario
  - I virus realizzati con gli script si attivano da soli non appena il messaggio viene aperto per la lettura
  - Particolarmente esposti sono MS Outlook e Outlook Express, che accettano e lanciano in automatico i **Visual Basic Script** (VBS)
  - Per difendersi…
    - Usare un mailer basato sul testo semplice, o impostare l'opzione che disabilita l'esecuzione automatica degli script

I tipi di virus – 5

- Hoax: burle, non si tratta di virus, ma di falsi allarmi diffusi soprattutto attraverso catene di posta elettronica che mettono in guardia contro presunti virus dagli effetti devastanti (sono esempi *California* e *Sulfnbk*)

- Joke: scherzi, programmi creati per gioco che non provocano nessun danno al sistema (o almeno niente che non si possa risolvere riavviando la macchina); non essendo virus, i joke non si propagano da soli, ma possono venir scaricati dalla rete

Il virus EICAR

- EICAR è la sigla di un virus fittizio creato dall'***European Institute of Computer Antivirus Research*** per testare il funzionamento dei programmi antivirus: si tratta di un piccolo file assolutamente inerte ed innocuo che tutti i software, per un reciproco accordo fra i produttori, riconoscono come se fosse un vero virus
- Il file può essere creato ricopiando in un editor di testo la seguente linea, senza nessuna modifica o aggiunta:

  X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

  salvando il file come eicar.com; facendo doppio click sul file, dovrebbe comparire la finestra di allarme virus, e lo stesso accade lanciando la ricerca di virus su tutti i file del disco