UNIT 1 – LEZIONE 1 – L'AMBIENTE CLIENT/SERVER

IL MECCANISMO CLIENT/SERVER

L'evoluzione tecnologica ha portato allo sviluppo di un modello di rete **client/server** che comprende l'introduzione di potenti computers "client" in contrasto con i terminali a funzioni fisse utilizzati dai modelli di rete precedenti. Un modello client/server ben progettato unisce le capacità di calcolo di un computer mainframe, alla possibilità di essere personalizzato facilmente. In un ambiente **"mainframe"** un applicazione come ad esempio un database, viene eseguita su un potente computer centralizzato e l'accesso a questa applicazione avviene attraverso i terminali. Quando un terminale invia una richiesta di dati al mainframe, questo trova i dati, li elabora, e li visualizza sul terminale che ha fatto la richiesta. I dati viaggiano in forma di **"pacchetti"** dal mainframe, attraversano la rete, e arrivano al terminale che li ha richiesti. Se i dati sono molti, il loro spostamento prende molto tempo e tiene occupata la rete. In un ambiente di rete centralizzato, tutte le attività di rete vengono eseguite attraverso il **"sistema operativo di rete"** e attraverso i cavi. Non esiste nessun tipo di coordinamento fra il mainframe ed il terminale per quanto riguarda i dati da inviare e ricevere.
Il modello client/server ha un modo di gestire i dati più efficiente, il client ricerca i dati sul server, li elabora, e li visualizza all'utente. La rete client/server memorizza dati contenuti nella RAM sul computer server, visto che il server ha la capacità di memorizzare grosse quantità di dati, questo crea più spazio sul computer client per altre applicazioni. Questo modello di gestione dei dati è utile per tutte le organizzazioni dove molte persone hanno bisogno di un costante accesso a grandi quantità di dati, inoltre è il modo più efficiente per accedere ai database e ad applicazioni come fogli elettronici, contabilità, comunicazioni e gestione documenti, infine è utile nella gestione delle reti e nella memorizzazione di dati centralizzati. In un sistema client/server i dati sono sicuri perché si trovano su un solo server o su un limitato numero di servers, inoltre se i dati si trovano in un'unica postazione possono essere gestiti da una sola persona, semplificando così la procedura di salvataggio dei dati. L'organizzazione dei dati su un server varia in base al tipo di attività che verrà svolta.
In una rete client/server i dati si trovano concentrati su un solo server, o distribuiti su diversi servers in base alla posizione degli utenti e alla natura dei dati. Esistono due varianti della organizzazione dei dati distribuita

- Nel primo tipo di organizzazione i servers che fanno parte di una **WAN**, si collegano periodicamente fra loro per assicurarsi di avere gli stessi dati.
- Nel secondo tipo di organizzazione viene utilizzata una **"Data Warehouse"** per memorizzare una grande quantità di dati. I dati richiesti più urgenti vengono inviati dalla Warehouse ad un sistema intermedio, questa tecnica riduce il carico di elaborazione sul server principale

Il flusso di dati in un sistema client/server avviene fra i due suoi principali componenti che sono le applicazioni chiamate **client o front-end** ed i database sui servers chiamati **server o back-end.** Il computer client invia una richiesta ed il server la elabora. Il software client trasforma la richiesta in

una forma che possa essere interpretata dal corrispondente database. Questa operazione avviene attraverso l'**SQL (S**tandard **Q**uery **L**anguage)
Tutto il meccanismo di richiesta e ricezione dei dati in un sistema client/server si compone di sei passi fondamentali

- Richiesta di dati da parte del client
- Traduzione della richiesta in SQL
- Invio della richiesta dal client al server attraverso la rete
- Ricerca dei dati richiesti eseguita dal server
- Invio del risultato della ricerca dal server al client attraverso la rete
- Visualizzazione dei dati richiesti sul client

FUNZIONI DEL CLIENT

Un client esegue una applicazione per ricevere la richiesta dall'utente, l'applicazione usa una interfaccia funzionale per accettare la richiesta dall'utente. Successivamente l'applicazione prepara la richiesta ricevuta dall'utente e la invia al server. Il server elabora la richiesta, trova le relative informazioni, e le restituisce al client attraverso la rete. Il client trasferisce le informazioni ricevute dal server all'interfaccia che si occupa di visualizzarle all'utente. Il client è in grado di presentare la stessa informazione agli utenti in diversi modi, in base alla richiesta fatta. Per esempio, le informazioni sui clienti e sui prodotti di una azienda costruttrice di computer, sono memorizzate in un database. Un impiegato fa una richiesta di dati dal suo client e le informazioni richieste possono essere trovate ed identificate come "Lista Clienti per l'ufficio marketing dei nuovi prodotti in campagna pubblicitaria"
Il sistema client/server diventa più efficiente con l'aiuto di strumenti di ricerca, applicazioni e programmi di utilità, utilizzati dai client

- QUERY TOOLS sono uno degli strumenti utilizzati dai client. Offrono la possibilità di creare delle richieste predefinite e di definire dei tabulati di riepilogo, per semplificare l'accesso ai dati sul server
- MICROSOFT EXCEL offre l'accesso diretto ai database dei servers
- MICROSOFT ACCESS utilizza il proprio SQL per rendere disponibile una interfaccia con i sistemi di gestione dei principali databases.
- MICROSOFT VISUAL BASIC ed altri programmi simili offrono la possibilità di sviluppare applicazioni per l'accesso ai dati sul server

FUNZIONI DEL SERVER

Il server di solito è un computer più potente dei client ed è in grado di gestire richieste multiple e contemporanee e di eseguire operazioni di gestione della rete. Il server contiene programmi per la gestione dei databases per elaborare le richieste dei client. Questi programmi restituiscono al client solo i risultati della ricerca mentre sulla parte server sono in grado di aggiornare, cancellare, inserire e proteggere i dati. L'elaborazione sul server prevede anche l'ordinamento dei dati, l'estrazione dei

dati richiesti ed il loro invio al client. I servers utilizzano routines per la gestione dei dati brevi e predefinite, chiamate **“stored-procedures”** .Questa tecnica aiuta nella elaborazione e non occupa spazio sul disco dei client. Le stored-procedures possono anche eseguire alcune funzioni normalmente tipiche dei client. Un’unica “stored-procedure” presente su un server può essere utilizzata da diversi client. Queste routines presenti sui server riducono il traffico sulla rete, perché fanno diminuire il numero di chiamate fra clients e servers, un ‘unica chiamata dal client al server può avviare l’esecuzione di una serie di “stored-procedures” sostituendo così le singole chiamate per ogni operazione richiesta. Le store-procedures contengono anche controlli di sicurezza per evitare che utenti non autorizzati le possano utilizzare.

SOLUZIONI CLIENT/SERVER

Una rete spesso utilizza componenti fabbricati da diversi produttori, la compatibilità fra questi componenti prende il nome di **interoperabilità**. Se un componente non è compatibile la rete non funziona correttamente. I problemi che provengono dall’incompatibilità vengono risolti installando soluzioni sul client o sul server. Queste soluzioni possono essere sia hardware che software per raggiungere la compatibilità da entrambe le parti. Esistono **“soluzioni client”** e **“soluzioni server”** e vengono fornite dai principali produttori di reti come Microsoft, Apple e Novell. Molti problemi nascono quando in una rete ci sono diversi sistemi operativi, in questo caso il sistema operativo sul client, e quello sul server devono essere compatibili. La soluzione per questo tipo di problema consiste nella utilizzo di **“programmi di indirizzamento” (redirectors)** multipli che permettono il collegamento con diversi servers alternativi a quello principale. Questo sistema può essere paragonato all’utilizzo di diverse compagnie telefoniche per comunicare con la stessa persona. Ogni redirector può gestire solo dati che utilizzano un protocollo specifico, infatti redirectors differenti operano con protocolli differenti per garantire la compatibilità. Per esempio per abilitare un computer client con il sistema operativo Windows NT ad accedere ad un server con un sistema operativo Novell, l’amministratore della rete caricherà il redirector per l’accesso ai server Novell all’inizio del sistema operativo Windows NT nel computer client. La compatibilità viene raggiunta a volte installando un particolare servizio sul server. Per esempio un computer client Apple Macintosh può essere messo in comunicazione con un server Windows NT collegandosi ad un particolare servizio sul server chiamato **“Servizi per Macintosh”** , questo servizio permette di rendere disponibili i dati presenti sul client Macintosh sia a computer client che server, che utilizzano il sistema operativo Windows NT inoltre permette di trasferire files fra un client Macintosh ed un client Windows NT permettendo così di condividere dati presenti su computers con sistemi operativi diversi.

UNIT 1 – LEZIONE 2 – FUNZIONI DEI SISTEMI OPERATIVI DI RETE

ATTIVITA' DI COORDINAMENTO

Una rete è composta da due o più computers ed ogni computer sulla rete può funzionare sia come computer locale (stand-alone) che come client di una rete. Ogni operazione eseguita da un computer è controllata dal suo sistema operativo. Un sistema operativo di un computer locale, come ad esempio l'MS-DOS, ha bisogno di un particolare software di rete per collegarsi con i servers. Questo speciale software è consciuto come **sistema operativo di rete.** Tale sistema operativo viene eseguito come una applicazione e viene caricato all'inizio del sistema operativo locale.
I sistemi operativi avanzati come Windows NT e Windows 95, hanno la capacità di poter funzionare sia come sistemi operativi locali che come sistemi operativi di rete quando il computer sul quale sono installati, deve funzionare sia come computer locale che come client di una rete. Per esempio un dirigente di una azienda può utilizzare un computer portatile per lavorare mentre viaggia, se però gli servono delle informazioni dall'ufficio il portatile si può collegare all'ufficio e agire come client. Un'altra funzione svolta dal sistema operativo è il coordinamento fra attività hardware e software sul computer. Anche l'utilizzo di risorse hardware come la memoria, il tempo di CPU, lo spazio su disco e le periferiche viene gestito dal sistema operativo, inoltre coordina le operazioni da eseguire fra il computer ed i programmi applicativi.

ESECUZIONE DI PROGRAMMI MULTIPLA (MULTITASKING)

Ci sono diversi sistemi operativi di rete disponibili. La scelta del sistema operativo adatto ad una rete dipende dall'attività della rete e dalle operazioni condivise che si dovranno effettuare. Il **"multitasking"** è una caratteristica di un sistema operativo per eseguire diverse operazioni contemporaneamente. Un sistema operativo con la funzione multitasking può eseguire nello stesso momento un numero di operazioni pari al numero di processori contenuti nel computer. Però ci possono essere condizioni nelle quali il numero di operazioni richieste è maggiore del numero di processori. In questo caso il sistema operativo utilizza la tecnica della **"suddivisione del tempo" (time-slicing)** per portare a termine tutte le operazioni. Utilizzando questa tecnica il sistema operativo dedica una porzione di tempo stabilito alla prima operazione, quindi dedica la stessa porzione di tempo alla seconda operazione, poi passa alla terza e così via. Questo meccanismo si ripete ciclicamente fino a quando tutte le operazioni richieste sono state eseguite e fa sembrare che il sistema operativo esegua tutte le operazioni contemporaneamente. La tecnica multitasking si divide in due classi principali

MULTITASKING PRIORITARIO
MULTITASKING NON PRIORITARIO

Nel multitasking prioritario il sistema operativo calcola la quantità di tempo del processore destinato ad ogni operazione, e quindi sposta l'attività del processore da una operazione all'altra fino a quando tutte le operazioni sono terminate. Questo tipo di multitasking prevede la possibilità

di funzionamento sia come computer locale che come client, questa doppia funzionalità viene gestita dal sistema operativo spostando l'attività del processore da una operazione locale ad una operazione di rete.

Il multitasking non prioritario è conosciuto anche come **multitasking cooperativo.** I programmi scritti per questo tipo di multitasking includono funzioni particolari per fermare il processore. Infatti l'attività del processore può passare alla operazione successiva solo quando l'operazione precedente lascia libero il processore.

UNIT 1 – LEZIONE 3 – COMPONENTI DEL SISTEMA OPERATIVO DI RETE

SOFTWARE DEL CLIENT

Una rete funziona con l'aiuto del software installato sia sul server che sul client. Il software client elabora ed invia le richieste da un computer client verso un computer server, questa procedura è diversa da quella presente in un computer locale. In un computer locale la richiesta fatta da un utente di eseguire una operazione raggiunge la CPU (Central Processing Unit) attraverso il bus locale. La CPU interpreta la richiesta e visualizza i risultati. In un ambiente di rete quando un utente avvia una richiesta per accedere ad una risorsa su un server che è collegato alla rete, la richiesta viene trasferita dal bus locale, attraverso la rete, al server che contiene la risorsa richiesta. Il trasferimento della richiesta dal bus locale al server, viene eseguito da un programma di indirizzamento (redirector). Un redirector è un piccolo programma che si trova nel sistema operativo di rete, la sua funzione è quella di intercettare le richieste fatte dal client verso il server, inoltre stabilisce se la richiesta è indirizzata verso la rete o verso il computer locale. Il redirector si collega ad una risorsa di rete assegnandole una lettera dell'alfabeto per identificarla in questo modo l'utente può effetuare la richiesta verso una risorsa di rete semplicemente utilizzando una lettera come riferimento. Un redirector può anche inviare delle richieste alle periferiche, ad esempio la stampa di un documento può essere indirizzata dalla stampante locale verso una stampante di rete, questa funzione viene eseguita senza coinvolgere l'utente.

SOFTWARE DEL SERVER

Ogni server presente sulla rete ha un software installato per la sua gestione. Il software del server permette agli utenti di una rete di condividere le risorse come archivi, stampanti, scanner, e dischi. L'accesso alle risorse condivise può essere diverso per ogni utente, per esempio l'accesso ad un archivio può essere definito come "sola lettura" o come "lettura e scrittura" , questo tipo di autorizzazione permette ad un utente di accedere all'archivio solo in lettura oppure di modificare l'archivio interessato. Il software del server garantisce anche che due utenti non possano utilizzare la stessa risorsa contemporaneamente. La gestione degli utenti è un'operazione per la quale il software del server offre una serie di funzioni di utilità. Un amministratore di rete può utilizzare il sistema operativo di rete per creare i privilegi come ad esempio l'assegnazione dei codici di accesso. Il sistema operativo di rete fornisce diverse funzioni per concedere o revocare i privilegi agli utenti, anche la cancellazione di utenti non richiesti è un'altra operazione permessa dal sistema operativo di rete. Il software del server facilita anche l'ottimizzazione del funzionamento di una rete infatti offre delle funzioni di utilità per verificare le prestazioni della rete.

UNIT 2 – LEZIONE 1 – FUNZIONAMENTO DEI MODEMS NELLA RETE

INTRODUZIONE AI MODEMS

La crescente popolarità del collegamento in rete ha portato alla installazione di reti in tutto il mondo, queste reti devono essere collegate fra di loro per poter scambiare le informazioni in diversi luoghi del mondo. Il collegamento fra due reti prende il nome di **"internetworking"** .Le reti che si trovano troppo distanti per essere collegate fisicamente con un cavo, si collegano attraverso la linea telefonica. L'apparecchio che permette tale collegamento è il modem, esso offre all'utente la possibilità di comunicare con computers che si trovano in qualunque altra rete al di fuori della propria rete locale. Un computer ed una linea telefonica non possono essere collegati direttamente in quanto ognuno di essi trasmette segnali di tipo diverso, infatti un computer trasmette impulsi elettronici digitali mentre una linea telefonica trasmette solo segnali analogici. Un modem converte i segnali provenienti da un computer in una forma che può essere trasmessa da una linea telefonica. Un modem esegue due funzioni fondamentali che sono conosciute come modulazione e demodulazione infatti la parola **MODEM** deriva dalle iniziali delle parole **MO**dulazione e **DEM**odulazione. La modulazione consiste nel trasformare i segnali digitali provenienti dal computer in segnali analogici. La demodulazione è il processo inverso che trasforma i segnali analogici provenienti dalla linea telefonica in segnali digitali interpretabili dal computer. I modems sono disponibili sia interni che esterni. I modems interni sono installati in uno slot di espansione come qualsiasi altra scheda hardware e si collega alla linea telefonica attraverso un cavo dotato di un connettore di tipo RJ-11C. Il modem esterno è una piccola scatola collegata al computer da un cavo seriale di tipo RS-232 ed anche questo tipo di modem utilizza il connettore di tipo RJ-11C per collegarsi alla linea telefonica.

COMUNICAZIONE FRA MODEMS

Tutte le comunicazioni tramite modem hanno bisogno di un mezzo come un cavo o una linea telefonica, il tipo di mezzo scelto determina i costi e le prestazioni della rete. La maggior parte dei modems trasmette i dati attraverso linee telefoniche che prendono il nome di **"carriers"**. Prima di installare un modem si deve scegliere un tipo di carrier adatta, la scelta di una linea carrier dipende dalla potenza del cavo telefonico, dalla distanza alla quale i dati devono essere inviati, dal costo e dalla riusabilità della linea stessa. Ci sono due tipi di carriers disponibili per le comunicazioni con i modems e sono : **le linee telefoniche pubbliche** e **le linee dedicate**.

Una linea telefonica pubblica, conosciuta anche come linea **"dial-up"** ,richiede che l'utente componga il numero telefonico ogni volta che vuole collegarsi, la necessità di comporre il numero rende questo tipo dil linea lenta e non riutilizzabile. Una linea "dial-up" viene normalmente utilizzata solo per connessioni temporanee fra reti, per un periodo limitato di tempo.

Una linea dedicata non richiede che l'utente componga il numero telefonico ad ogni connessione, al contrario fornisce una connessione dedicata e continua. Essa è più veloce e riutilizzabile dell'altra

ma ha lo svantaggio di essere più costosa. Questo tipo di linea viene di solito utilizzata dalle persone che hanno la necessità di tenere sempre collegate le loro reti. Le linee dedicate utilizzano linee a lunga distanza ed una rete che utilizza questo tipo di linee prende il nome di **V**irtual **P**rivate **N**etwork (**VPN**) .

Una volta scelto il tipo di linea si deve identificare l'ambiente di comunicazione, gli ambienti di comunicazione vengono classificati in due tipi in base al tempo utilizzato dalla comunicazione, e sono

COMUNICAZIONE ASINCRONA
COMUNICAZIONE SINCRONA

La comunicazione asincrona utilizza le linee telefoniche comuni per inviare i dati e i modems che utilizzano questo ambiente si chiamano **modem asincroni** . Una trasmissione asincrona trasmette i dati uno di seguito all'altro (**trasmissione seriale**), ogni carattere si trasforma in un blocchetto di 8 bits, ogni blocchetto di 8 bits (**byte**) contiene il primo bit chiamato "**bit di inizio del carattere**" e l'ultimo bit chiamato "**bit di fine del carattere**" questi due bits vengono utilizzati dal computer che invia e da quello che riceve dati, per sincronizzare la trasmissione. Il computer ricevente usa questi due bits per prepararsi a ricevere il blocchetto di dati successivo. In questo tipo di trasmissione non viene utilizzato nessuno strumento per misurare il tempo, il computer origine invia i dati ed il computer ricevente verifica i dati ricevuti ma non esiste nessun tipo di coordinamento fra i due computers. La comunicazione asincrona usa il **"controllo di parità"** per verificare e correggere gli errori di trasmissione. In questo tipo di controllo vengono confrontati il numero di bits inviati con il numero di bits ricevuti. La comunicazione asincrona è molto conosciuta e poco costosa anche se non è sincronizzata

Per una comunicazione di dati più controllata è preferibile usare la trasmissione sincrona. Questo tipo di trasmissione utilizza i cavi e dipende dal tempo di sincronizzazione fra i computers trasmittente e ricevente, viene utilizzato in tutte le reti a comunicazione digitale ed i modems che utilizzano questo tipo di comunicazione si chiamano "**modems sincroni**". La comunicazione sincrona si basa su uno schema a tempo che divide i dati in blocchetti di bits e li trasmette in modo sincronizzato, questi blocchetti si chiamano "**frames**", la trasmissione si ferma alla fine di ogni frame e inizia con un nuovo frame. Per intercettare e correggere gli errori di trasmissione, l'ambiente sincrono usa uno schema che permette di inviare di nuovo i dati se si verifica un errore. La trasmissione sincrona usa protocolli che svolgono diverse funzioni : preparano i dati in blocchetti, aggiungono informazioni di controllo ai dati, verificano i dati per controllare gli errori.

MODEM/FAX

Un modem/fax condiviso permette agli utenti della rete di utilizzare contemporaneamente le caratteristiche di un fax e l'invio di fax dai loro computers. Un modem tradizionale può trasmettere solo dati, mentre un modem/fax può inviare i dati anche sotto forma di fax. Gli utenti possono anche inviare fax dai loro computers ad un unico computer, a sua volta connesso ad un fax, ma

questo può provocare code di attesa sul computer che ha ricevuto i fax dagli utenti. Per questo motivo i modem/fax sono spesso condivisi sulla rete. Un modem/fax condiviso è collegato da una parte ad un server e dall'altra ad un fax. Il server riceve i fax dai vari computers client, e li memorizza. In un secondo momento li indirizza al modem/fax condiviso e quindi il fax li invia alla loro destinazione.

Quando il documento da inviare arriva al fax, non ha nessuna informazione sull'indirizzo da raggiungere. Questo indirizzamento, cioè l'invio del documento al destinatario finale, può essere realizzato con diversi metodi.

Un metodo di indirizzamento e quello **MANUALE**. Con questo metodo i fax da inviare vengono raccolti in un unico posto, successivamente l'amministratore li indirizza alla loro destinazione manualmente utilizzando un personal computer collegato ad un fax.

Un altro metodo di indirizzamento utilizza software come **OCR** (**O**ptical **C**haracter **R**ecognition) e **ICR** (**I**ntelligent **C**haracter **R**ecognition) entrambi i software sono in grado di interpretare i caratteri sulla copertina del fax in modo da cercare sul computer l'indirizzo del destinatario, una volta trovato il fax ricevuto viene indirizzato al computer di quel destinatario.

Altri metodi di indirizzamento sono il protocollo **T.30** ed il sistema **NEST** (**N**ovell **E**mbedded **S**ystem **T**ecnology). Entrambi i tipi di indirizzamento permettono di indicare l'indirizzo aggiungendo un codice numerico al numero di telefono al momento della chiamata al fax.

Il metodo **TSI** (**T**ransmission **S**tation **I**dentification) utilizza il numero di telefono dell'apparecchio che ha inviato il fax da indirizzare, per stabilire il destinatario del fax. Uno svantaggio di questo metodo è che tutti i fax provenienti dallo stesso apparecchio vanno allo stesso destinatario.

Un altro metodo chiamato **Received Fax Line** utilizza una serie di linee e modems. Tutti i fax ricevuti su una determinata linea, vengono indirizzati ad uno specifico utente o ad un gruppo di utenti.

In alternativa i fax possono essere indirizzati utilizzando il **codice a barre,** questo metodo permette di stampare sulla copertina del fax, un codice a barre che identifica il destinatario finale del fax.

UNIT 2 – LEZIONE 2 – POSTA ELETTRONICA

CARATTERISTICHE DELLA POSTA ELETTRONICA

La posta elettronica è una degli strumenti utilizzati nelle reti che permette agli utenti di comunicare. Gli utenti di posta elettronica comunicano fra loro attraverso l'uso delle **cassette postali (mailbox).**
Una cassetta postale è il luogo dove vengono raccolti tutti messaggi di posta elettronica indirizzati ad un specifico utente. L'amministratore della e-mail crea una cassetta postale per ogni utente della rete. Una e-mail può contenere immagini grafiche e file allegati, oltre al normale testo, inoltre può contenere anche file audio e video. Le e-mail possono essere lette, ignorate, salvate o modificate, possono anche essere reindirizzate ad un altro destinatario o stampate. Ad esempio una e-mail importante come una relazione di lavoro, può essere salvata per un successivo utilizzo, in un secondo momento può essere integrata con i propri commenti e quindi stampata. Una e-mail ricevuta da un utente può essere **reindirizzata** (**reply**) a più utenti, ad esempio una comunicazione dal capoufficio indirizzata a tutti i colleghi. Di solito esiste uno specifico tasto per attivare la funzione di reindirizzamento. Un'altra caratteristica sono gli **allegati (attachments)**. Infatti gli utenti possono allegare al testo della e-mail files di database o di fogli elettronici o di qualsiasi altro tipo.
La funzione di **notifica (notification)** permette di essere avvertiti quando si riceve una nuova e-mail. La notifica avviene attraverso un segnale acustico, un simbolo visivo, o entrambi.
Si può anche attivare una funzione che informa ogni utente se la e-mail inviata e stata ricevuta e letta, questa caratteristica si chiama **ricevuta di ritorno (return receipt)**.
La funzione di **copia carbone (carbon copy)** permette agli utenti di inviare una copia esatta del messaggio a diversi destinatari, nello stesso momento
La funzione di **recupero (undelete)** permette di recuperare i messaggi cancellati per errore.
La funzione **out of office (OOF)** informa gli utenti che il destinatario non è momentaneamente disponibile a ricevere e-mail.

PRINCIPALI POSTE ELETTRONICHE

I diversi sistemi operativi di rete usano sistemi differenti di posta elettronica, quindi per poter comunicare fra questi diversi sistemi, indipendentemente dal sistema operativo utilizzato, sono stati sviluppati dei modelli standard di comunicazione.
Uno di questi modelli standard è conosciuto come **X.400** ed è stato progettato per avere un funzionamento indipendente sia dall'hardware che dal software di un computer, esso fornisce regole standard per la codifica delle informazioni, le regole di conversione, la sintassi ed i protocolli di accesso.
Una caratteristica del modello X.400 è la assegnazione della data e dell'ora di creazione di una e-mail. Un'altra particolarità è l'impostazione del livello di priorità, in base all'impostazione di questa priorità una e-mail può essere inviata immediatamente o in un momento successivo. Il modello X.400 può inviare insieme alla e-mail un messaggio di verifica, in questo modo il mittente della e-

mail in oggetto riceve un messaggio di controllo per avere la conferma dell'avvenuta consegna della e-mail.
Si può anche inviare, con questo modello, la stessa e-mail a diversi utenti nella rete.

Un altro modello standard prende il nome di **X.500**. E' un insieme di servizi per aiutare gli utenti a trovare utenti specifici, presenti sulla rete, ai quali inviare posta elettronica. Per questo motivo il modello X.500 offre un elenco di tutti gli utenti di posta elettronica. Il modello X.500 ha bisogno di tre servizi specifici per trovare una risorsa

IL SERVIZIO DEI NOMI	per trovare il nome di un utente sulla rete
LA RUBRICA DEGLI INDIRIZZI DI POSTA	per identificare un particolare indirizzo di posta
IL SERVIZIO CARTELLE	per poter fare una ricerca all'interno della rete

L'**SMTP** (**S**imple **M**ail **T**ransfer **P**rotocol) è stato progettato per trasferire messaggi fra due computer che si trovano in reti separate fra loro e lontane. Utilizza il programma locale di posta elettronica per poter offrire le funzioni sia client che server in modo da poter sia inviare che ricevere e-mail. Questo protocollo offre la gestione dei segnali di controllo della comunicazione fra due computers che consiste nella verifica della connessione, nella trasmissione dei messaggi, nel riconoscimento del mittente, e nella trasmissione dei parametri. L'SMTP permette agli utenti la revisione e la stampa dei messaggi e permette anche ad un utente di inviare una e-mail ad un gruppo di utenti.

Il servizio **MHS** (**M**essage **H**andling **S**ervice) offre un server MHS che traduce i messaggi fra computers che utilizzano sistemi di posta elettronica diversi. Tutti i prodotti che possono comunicare con un server MHS, possono comunicare fra loro attraverso la posta elettronica.

UNIT 2 – LEZIONE 3 – GROUPWARE E AGENDE ELETTRONICHE

GROUPWARE

Il groupware è un insieme di programmi software di utilità nella rete, che racchiude in sé diverse funzioni come il reindirizzamento, la condivisione delle informazioni, e le utilità per la posta elettronica. La sua varietà di funzioni offre possibilità di comunicazione e di coordinamento del lavoro maggiori di un semplice programma di posta elettronica. Il groupware offre l'accesso simultaneo alle informazioni da parte di gruppi di lavoro, tali gruppi possono essere formati da impiegati, aziende in collaborazione, clienti e fornitori. Ci sono molti utilizzi del groupware fra i quali il coordinamento di progetti e lo sviluppo di documenti, inoltre il groupware facilita la gestione di lavori di gruppo e discussioni nel gruppo. Altri utilizzi del groupware sono la traccia delle richieste del cliente e la gestione delle relazioni con il cliente. Esistono programmi di tipo groupware che sono in grado di rendere la comunicazione di gruppo più efficiente. Uno di questi è la **posta elettronica groupware** che permette agli utenti di un gruppo di posta elettronica di comunicare con gli utenti di un altro gruppo di posta elettronica. Un programma **groupware multimediale** offre funzioni di comunicazione avanzate come immagini scannerizzate, invio di fax, comunicazione vocale e sonora, riconoscimento ottico dei caratteri, grafica e video-conferenza.

PRODOTTI GROUPWARE

Il **Microsoft Exchange** ed il **Lotus Notes** sono i due principali prodotti di tipo groupware. La Microsoft ha incorporato le caratteristiche sia della comunicazione di informazioni, che quelle della posta elettronica in un unico prodotto conosciuto come Microsoft Exchange, e progettato per trarre il massimo vantaggio dalla tecnologia client/server. Il Microsoft Exchange lavora con il **MES** (**M**icrosoft **E**xchange **S**erver) che è progettato per dialogare con programmi e reti già esistenti in modo da permettere agli utenti la condivisione di informazioni varie in modo efficiente. Il MES offre funzioni di utilità basate sulla tecnologia client/server. Una di queste utilità è il servizio di messaggistica, questo servizio trasferisce, invia, riceve, indirizza messaggi, offre anche la possibilità di cercare le risorse nella rete. Il Microsoft Exchange permette agli utenti di comunicare attraverso il sistema di posta elettronica presente sul MES, inoltre facilita la condivisione di informazioni nel gruppo, rendendo disponibile un servizio informativo del gruppo (**bulletin board**) ed una libreria di riferimento accessibile agli utenti del gruppo. Il MES ha anche la possibilità di creare maschere personalizzate per la gestione di dati contenuti in database. Una ulteriore possibilità del MES è il progetto delle applicazioni, questo consente ai progettisti di sviluppare applicazioni per automatizzare alcune operazioni all'interno di un gruppo.
Il secondo prodotto groupware maggiormente conosciuto è il Lotus Notes ed è progettato per gestire reti di qualunque misura. I servizi principali di questo prodotto prevedono la sicurezza, la gestione, servizi di elenchi, e servizi di connessione. Questi servizi possono comunicare attraverso diversi ambienti con diversi sistemi operativi come ad esempio Windows NT, Macintosh e Unix, e diversi protocolli di comunicazione come ad esempio TCP/IP. Esistono alcuni programmi che posseggono

già in sé le caratteristiche per la comunicazione fra gruppi, uno di questi è il sistema operativo Microsoft Windows 95.

Il sistema operativo **Microsoft Windows 95** offre un ambiente multitasking con numerose caratteristiche incluso il formato **OLE** (**O**bject **L**inking and **E**mbedding) per creare documenti composti in rete.

Il **Servizio di Messaggeria Intelligente Banyan** permette agli utenti della rete di memorizzare, gestire e indirizzare i loro documenti, inviare e ricevere posta elettronica, e tracciare il flusso delle richieste.

Il **Servizio Teamlinks** è un sistema sviluppato dalla Digital Equipment Corporation per gli uffici. Ha il vantaggio di potersi collegare al sistema operativo di rete della Digital che offre un servizio di posta elettronica standard con protocollo X.400, conversione automatica dei file, video-conferenza, e traccia del flusso delle richieste.

Il **Groupwise Novell** è un software integrato che offre la posta elettronica e funzioni facilitate per la organizzazione delle attività, gestione delle attività e traccia del flusso delle richieste.

PROGRAMMAZIONE DELLE ATTIVITA' (SCHEDULING)

Un programma di agenda elettronica rappresenta la versione informatica della tradizionale agenda cartacea. Permette di pianificare giornalmente, mensilmente e annualmente incontri, appuntamenti ed altre attività varie. La maggior parte delle agende elettroniche mostrano un calendario e visualizzano un messaggio lampeggiante sullo schermo quando un evento si avvicina alla sua scadenza, questa funzione elimina la necessità di dover controllare l'agenda periodicamente. L'agenda elettronica può essere utilizzata per pianificare sia attività individuali che di gruppo. Le pianificazioni individuali aiutano il singolo utente a ottimizzare il proprio tempo. Gli utenti possono memorizzare gli eventi in un file che servirà per ricordare loro ogni evento pianificato. Per inserire un nuovo evento l'agenda elettronica verifica il calendario dell'utente per il periodo richiesto, se il periodo risulta libero il software memorizza il nuovo evento. In un secondo momento se l'utente prova a memorizzare un secondo evento nello stesso periodo, il software avverte della esistenza di un conflitto.
La pianificazione di gruppo risolve i problemi di programmazione delle attività a livello di rete, infatti con questa funzione è possibile pianificare attività che richiedono la partecipazione di diversi utenti della rete, per esempio un membro di un gruppo di lavoro vuole pianificare un periodo nel quale tutti i membri del gruppo saranno liberi per assistere ad una presentazione. Tale utente può vedere i calendari di tutti i membri del gruppo per trovare un periodo nel quale tutti siano liberi, una volta trovato il periodo lo stesso utente può pianificare la presentazione per tutti gli utenti in quel periodo, il software automaticamente inserirà un nuovo impegno in tutti i calendari degli utenti interessati.

UNIT 3 – LEZIONE 1 – GESTIONE DELLE PRESTAZIONI DELLA RETE

ATTIVITA' DI GESTIONE DELLA RETE

Una rete deve soddisfare i bisogni di tutti gli utenti connessi ad essa, quindi per assicurare un corretto funzionamento della rete stessa è essenziale gestirla in maniera efficiente. La persona che si occupa di questa manutenzione è **l'amministratore di rete** che gestisce le cinque maggiori aree della manutenzione di una rete, e ognuna di queste aree contribuisce al corretto funzionamento della rete stessa.
La prima area della gestione di una rete è **l'amministrazione degli utenti** che consiste nella creazione e manutenzione degli utenti e nella impostazione dei permessi di accesso alle risorse di rete da parte degli utenti.
La seconda area è **la gestione delle risorse di rete** che comprende l'installazione e la manutenzione delle risorse hardware e software per la gestione della rete. Per esempio l'amministratore di rete si deve occupare di scegliere il server adatto, di installare il sistema operativo di rete, e di configurare la stampante condivisa in rete.
La terza area è conosciuta come **gestione della configurazione di rete** e consiste nel pianificare la configurazione originale della rete prima ancora della installazione. Le successive espansioni della rete e la documentazione della configurazione di rete sono anche aspetti importanti di quest'area.
La quarta area è **la gestione delle prestazioni della rete** che consiste nel monitorare e tracciare le attività della rete in modo da mantenere e potenziare le prestazioni della rete.
La quinta area riguarda **la manutenzione della rete** che comprende la prevenzione, il riconoscimento e la soluzione di problemi riguardanti la rete

PROBLEMI DI PRESTAZIONI DELLA RETE

Una volta che la rete è installata e funzionante una delle maggiori responsabilità dell'amministratore di rete è quella di assicurarsi che la rete continui a mantenere le prestazioni iniziali, questo tipo di manutenzione comporta una continua e regolare azione di monitoraggio delle attività di rete, che aiuta a riconoscere le possibili cause dei più comuni problemi di rete. Il monitoraggio fornisce le informazioni fondamentali per riconoscere il problema denominato **"collo di bottiglia" (bottleneck)** che è la causa più frequente di problemi di prestazione. Un collo di bottiglia viene creato da una periferica di rete o da un programma che utilizza più del tempo normale richiesto per l'esecuzione della sua operazione di rete, rallentando così il flusso anche delle altre operazioni. La CPU è una delle periferiche che comunemente tendono a causare il collo di bottiglia, altre periferiche che possono causarlo sono la memoria, le schede di rete, le schede di controllo dei dischi, i dischi di rete ed altre. La presenza di un collo di bottiglia in una rete, causa una prestazione molto bassa nella rete stessa. Anche una periferica che è troppo lenta o che non possiede una memoria locale per gestire le operazioni, può determinare un collo di bottiglia. Comunque i colli di bottiglia non sono le sole cause di rallentamento delle prestazioni in una rete, infatti grossi rallentamenti possono dipendere da gravi errori commessi nella pianificazione e installazione della rete, questi errori possono essere identificati attraverso una lista di controllo

contenente diverse richieste di verifica mirate alla gestione della rete. Le domande presenti nella lista determinano se la rete iniziale è stata pianificata correttamente. Consideriamo una rete che in fase di pianificazione doveva adottare la tipologia “star-ring (token-ring)” e che invece per esigenze degli utenti è stata installata come tipologia “star-bus”, una appropriata domanda nella lista aiuterà ad identificare la discordanza di tipologia fra quanto pianificato e quanto invece realizzato in realtà.
La lista di controllo serve anche ad accertare se qualcosa è cambiato nella rete dal momento della prima installazione, ad esempio si possono aggiungere alla lista l’installazione di un nuovo “router” oppure la creazione di nuovi utenti. La lista inoltre aiuta a capire se un utente sta utilizzando una procedura di rete in modo diverso, come ad esempio l’installazione di un nuovo server senza comunicarlo all’amministratore di rete. Infatti installando un nuovo server, l’utente può aver utilizzato un indirizzo di rete che è identico ad un altro indirizzo già utilizzato, questa situazione crea problemi in rete. Le domande nella lista riguardano anche l’utilizzo di qualsiasi nuovo apparecchio vicino alla rete, per esempio un generatore troppo vicino alla rete può causare disturbi elettrici che possono influenzare le prestazioni della rete.
Assieme alla lista di controllo, l’amministratore di rete utilizza programmi di verifica della rete per tenere sotto controllo le prestazioni della rete, e alcuni di questi programmi di utilità fanno parte del sistema operativo di rete e fanno uso delle statistiche di prestazione per isolare la causa dello scarso rendimento della rete. Le statistiche di prestazione forniscono informazioni sull’andamento di attività come l’utilizzo della CPU da parte di diversi programmi, la parte di memoria utilizzata da un’applicazione ed altre informazioni collegate. I problemi di prestazioni legati invece ad attività della rete come la crescita, le nuove periferiche e la manutenzione, si identificano utilizzando l’archivio storico documentato delle attività sulla rete. Documentare la storia della rete è importante quanto monitorare la sua attività on-line perché costituisce una base di confronto con le informazioni attuali per poter determinare problemi di prestazione. Il documento di registrazione della storia della rete, contiene la data di installazione della rete, i particolari dei componenti della rete e informazioni sui fornitori dei componenti della rete. In questo documento sono registrati la procedura di installazione, la configurazione iniziale della rete e le successive variazioni di configurazione e di risorse, inoltre contiene le copie dei file di sistema come il config.sys e l’autoexec.bat. Il documento registra tutti i problemi di rete e la loro soluzione, ogni cambiamento hardware o software, ed ogni attività che interessa la topologia o la architettura della rete.

UNIT 3 – LEZIONE 2 – GESTIONE DELLA SICUREZZA DELLA RETE

PIANIFICARE LA SICUREZZA

Le attività di rete possono essere intercettate attraverso accessi non autorizzati o da intrusioni elettroniche e furti. Per proteggere le operazioni di rete e rendere sicure le informazioni è necessario pianificare la gestione della sicurezza in rete. L'estensione ed il livello di sicurezza dipendono dal tipo di ambiente dove la rete è installata. Ad esempio la rete di una banca richiede un livello di sicurezza più alto rispetto alla rete di un videonoleggio. La creazione e l'applicazione di una politica di sicurezza ben strutturata è il primo passo per assicurare la riservatezza dei dati. Una politica di sicurezza è un insieme di regole, e norme di comportamento che permettono all'amministratore del sistema ed agli utenti di proteggere la rete. E' importante addestrare gli utenti di rete sulla sicurezza, infatti un utente istruito ha meno probabilità di un utente inesperto di danneggiare accidentalmente le risorse di rete. Un amministratore di rete può creare una guida per la sicurezza per gli utenti della rete, e condurre lezioni di addestramento per i nuovi utenti.

La prima considerazione nella pianificazione della sicurezza di rete, è quella di garantire la sicurezza fisica dei componenti hardware della rete. Ognuno degli utenti di una rete "peer to peer" (piccola rete locale) è responsabile della sicurezza del proprio computer e dei propri dati. In una rete di tipo "peer to peer" non è indispensabile applicare una politica di sicurezza dell'hardware, invece questa attività diventa necessaria in una grande rete centralizzata dove i dati trattati sono importanti e devono essere protetti. In questo caso i servers della rete devono essere fisicamente protetti contro azioni dannose. La soluzione per proteggere fisicamente i servers è quella di chiuderli in una stanza alla quale possa accedere solo l'amministratore di rete, qualunque altro utente che abbia necessità di lavorare sul server dovrà prima essere autorizzato dall'amministratore di rete. Una volta che il server è stato protetto, è importante proteggere i cavi di collegamento della rete, infatti attraverso questi cavi passano le informazioni che possono essere intercettate e prelevate, pertanto i cavi che trasportano informazioni importanti devono essere accessibili solo a persone autorizzate. Si dovrà quindi prevedere, durante la fase di pianificazione, che questo tipo di cavi si trovi all'interno dell'edificio dell'azienda in modo da rendere i cavi inaccessibili a persone non autorizzate.

Una volta completata la protezione fisica dei componenti hardware della rete, è necessario proteggere le risorse di rete contro gli accessi non autorizzati, questo si realizza assegnando agli utenti permessi e diritti di accesso alle risorse di rete. Le risorse di rete possono essere protette attivando modelli di sicurezza come il modello di "**risorse condivise protette da password**" oppure il modello di "**permessi di accesso alle risorse di rete**". Il primo modello presuppone l'assegnazione di una password a tutte le risorse condivise sulla rete.

Alcuni sistemi operativi permettono diversi tipi di accesso per le risorse condivise, per esempio in Windows 95 le cartelle possono essere condivise come **"sola lettura"**, come **"accesso totale"** o come **"accesso dipendente da password"**.

Se una risorsa è condivisa come "sola lettura" gli utenti potranno visualizzare, copiare e stampare i documenti, ,ma non potranno mai cambiare il documento originale.

Se invece una risorsa è condivisa con "accesso totale" gli utenti potranno visualizzare, modificare, aggiungere e cancellare gli archivi contenuti nella cartella condivisa.

L’”accesso dipendente da password” fa in modo che alcuni utenti con determinate password possano utilizzare tutte le funzioni disponibili compresa la modifica e la cancellazione mentre altri utenti con password diverse potranno accedere alle risorse condivise in sola lettura.
Per fornire un livello di controllo maggiore sui diritti di accesso di quello fornito dalla condivisione delle risorse con password è necessario applicare il modello di “permessi di accesso alle risorse di rete”. Con questo modello di protezione ogni utente deve digitare la propria password al momento del collegamento alla rete, e non al momento della connessione con la risorsa condivisa come accade invece con il modello di protezione precedentemente descritto, subito dopo il server convalida la combinazione di nome utente e password e dopo aver verificato l’autenticità dell’utente il server concede o nega l’accesso alle risorse condivise, attraverso la ricerca dei diritti di accesso su un database presente sul server che stabilisce per ogni coppia utente/password quali sono le risorse accessibili.

POTENZIAMENTO DELLA SICUREZZA DELLA RETE

Le reti gestiscono dati molto delicati e riservati come sistemi bancari e militari che richiedono livelli di sicurezza ancora maggiori, in questi casi è importante attivare funzioni di potenziamento della sicurezza. La funzione di “**auditing**” è una di questi meccanismi potenziati che permette di registrare determinati eventi nel registro di sicurezza del server, i records così registrati mostrano i dettagli dell’utilizzo della rete e la traccia delle attività di rete. Per esempio records che mostrino dei tentativi di accesso falliti ripetutamente oppure tentativi di collegamento fatti nelle ore pari del giorno possono indicare che un utente non autorizzato sta cercando di entrare nella rete. Questo sistema si rivela valido anche per quelle società che offrono servizi in rete a pagamento. Per esempio una società come la Compuserve fa pagare agli utenti il servizio di trasferimento di files basandosi sulla durata della connessione alla rete per effettuare il trasferimento
Un altro metodo per rafforzare la sicurezza della rete è l’utilizzo di **computers senza dischi.** Questi computers non hanno né floppy disk né hard disk e ciò rende impossibile per un utente scaricare dati e memorizzarli su disco, questi computers sono utilizzati soprattutto nelle reti militari.
Il terzo metodo per potenziare la sicurezza è quello di **attivare la crittografia dei dati.** Questa è una tecnica che consiste nell’utilizzo di un programma per spezzettare e crittografare i dati prima di inviarli in rete, questo fa in modo che i dati risultino illeggibili per gli utenti non autorizzati che tentino di intercettarli, quando i dati crittografati arrivano al computer di destinazione un altro programma si occupa di ricomporre e decodificare i dati spezzettati.
Quando si attivano le funzioni avanzate di sicurezza della rete è importante per l’amministratore di rete di tenere conto del trattamento dei virus. Un virus è un programma che entra in un computer attraverso la rete e sconvolge il suo normale funzionamento. Un programma di protezione dai virus può prevenire l’attivazione di qualunque virus oppure tenere un virus sotto controllo se viene attivato, può anche riparare gli eventuali danni provocati dal virus

UNIT 3 – LEZIONE 3 – SALVATAGGIO DEI DATI DI RETE

NASTRI DI SALVATAGGIO

Una delle maggiori responsabilità di un amministratore di rete di una compagnia che gestisce le carte di credito, è quella di evitare perdite di dati memorizzati. La perdita di dati può essere causata da motivi sia umani che naturali. La cancellazione o il danneggiamento di dati, il furto, il fuoco, la mancanza di energia elettrica, i guasti del sistema, i disastri naturali come alluvioni e terremoti possono tutti causare la perdita di dati importanti. La manutenzione di una copia di salvataggio dei dati può prevenire la perdita di dati, infatti i salvataggi permettono il recupero dei dati che sono stati danneggiati o persi.
Un mezzo comune per il salvataggio dei dati è il **nastro magnetico** . La scelta di salvare i dati su nastro dipende dal volume di dati da salvare e dalla capacità del nastro, anche la velocità di salvataggio, la qualità del nastro, e la sua compatibilità con il sistema operativo, influiscono sulla scelta di salvare i dati su nastro. Si devono fare salvataggi periodici dei files presenti sul server e conservarli in un luogo diverso dai locali dove si trova il server stesso. Si possono fare salvataggi dell'intero disco, di alcune cartelle o semplicemente di alcuni files.
Il salvataggio completo del disco rende più facile l'eventuale ripristino però richiede una grande quantità di spazio su nastro magnetico
Il salvataggio di alcune cartelle o files, richiede meno spazio ma può darsi che in caso di ripristino si renda necessario un caricamento manuale dei dati dal nastro ed una riconfigurazione del sistema.
La frequenza di esecuzione dei salvataggi dipende dalla criticità dei dati e dalla frequenza con la quale vengono aggiornati. Come regola generale i dati possono essere salvati, giornalmente, settimanalmente, o mensilmente.
Esistono cinque metodi per operare il salvataggio dei dati in base al tipo di files che devono essere salvati. Una valida politica di salvataggio deve utilizzare una combinazione di tutti e cinque i metodi.
Il primo metodo è il **salvataggio completo** che salva e marca come salvati, i files selezionati indipendentemente dal fatto che il file in fase di salvataggio sia cambiato o meno rispetto al salvataggio precedente.
Il secondo metodo è conosciuto come **copia di salvataggio** che semplicemente crea una copia dei file selezionati senza operare nessun tipo di marcatura.
Il terzo metodo si chiama **salvataggio incrementale** e salva i files selezionati, marcandoli come files salvati, solo se sono cambiati rispetto al salvataggio precedente.
Il quarto metodo è la **copia giornaliera** che salva solo quei files che sono stati modificati nel corso della giornata.
Il quinto e ultimo metodo è il **salvataggio differenziale** che salva i files selezionati solo se sono cambiati rispetto al salvataggio precedente, ma non li marca come files salvati.
Parallelamente al salvataggio dei dati è importante avere un **registro dei salvataggi** che risulterà utile in caso di ripristino, tale registro riporterà :

- La data e il tipo di salvataggio
- I files ed il computer dal quale il salvataggio è stato eseguito
- Il luogo dove si trovano i nastri di ripristino

Per installare un sistema di salvataggio, si deve collegare una unità di memorizzazione su nastro direttamente al server oppure ad un client dal quale si eseguiranno i salvataggi. E' preferibile eseguire i salvataggi direttamente dal server in modo che i dati non viaggino troppo lungo la rete, infatti eseguire i salvataggi attraverso la rete aumenta il traffico della rete stessa e riduce la velocità di trasmissione dati sulla rete con un conseguente abbassamento delle prestazioni

GRUPPI DI CONTINUITA'

L'interruzione della corrente elettrica sulla rete può portare alla perdita di dati importanti questa eventualità però può essere prevenuta attraverso l'utilizzo di gruppi di continuità (**UPS** **U**ninterruptible **P**ower **S**upply) . Un gruppo di continuità è una batteria esterna che mantiene funzionanti i computers in una rete quando si verifica una interruzione della corrente elettrica. Molto spesso il gruppo di continuità si trova fra il server e la presa della rete elettrica, quando manca l'erogazione della corrente al server il gruppo di continuità fornisce temporaneamente l'energia per un breve periodo di tempo. Questa energia può essere erogata da una batteria oppure da un generatore di corrente alimentato da un motore a scoppio. Il gruppo di continuità permette anche la gestione sicura dello spegnimento del server proteggendo sia l'hardware che il software da eventuali danni.Un UPS di qualità può avere funzioni aggiuntive, ad esempio può impedire a più utenti di accedere al server nel periodo in cui manca la corrente, inoltre è in grado di mandare un messaggio di allarme all'amministratore di rete sia in caso di mancanza di corrente che in caso di chiusura del sistema. Anche gli utenti della rete vengono avvertiti della mancanza di corrente e vengono invitati a chiudere i loro lavori prima che l'energia manchi completamente. Nello stesso modo gli utenti vengono avvertiti se nel frattempo la corrente elettrica ritorna.
Esistono due tipi di gruppi di continuità
Il primo viene chiamato "**sistema in linea (on-line)**" che si attiva nel momento esatto in cui manca la corrente e fornisce energia attraverso le batterie automaticamente.
Il secondo tipo viene chiamato "**sistema locale (stand-by)**". Esso ha bisogno di essere acceso quando manca la corrente e anche se è meno costoso dell'altro sistema è sicuramente meno affidabile.

SISTEMI DI PREVENZIONE DELL'ERRORE

Per prevenire la perdita di dati importanti gli amministratori di rete utilizzano sistemi di prevenzione dell'errore che proteggono i dati efficacemente.
Esistono varie tipologie di prevenzione dell'errore e si basano sulla duplicazione dei dati su diverse partizioni del disco. Questi sistemi permettono l'accesso ai dati anche se il sistema è parzialmente guasto oppure se il file contenente i dati interessati risulta parzialmente rovinato.
La prima tecnica è conosciuta come "**disk-striping (ripartizione del disco)**" e consiste nel dividere i dati in blocchi da 64 Kilobytes (KB) e duplicare contemporaneamente ognuno di questi blocchi,

con una frequenza regolare su diversi dischi. Per esempio per memorizzare 192 KB di dati su tre dischi il primo blocco di 64 KB verrà memorizzato sul primo disco e altri due blocchi di 64 KB ciascuno, verranno memorizzati sul secondo e sul terzo disco. Questo sistema di memorizzazione dei dati considera diverse aree di disco situate anche su dischi diversi, come un unico disco "logico" e quindi distribuisce i dati indifferentemente su tutti i dischi utilizzabili, inoltre anche lo spazio disco viene ottimizzato utilizzando questo sistema perché grandi unità logiche risultano composte di piccoli pezzi fisici di disco sfruttati al massimo come un mosaico. L'utilizzo di più schede di controllo dei dischi migliora ulteriormente le prestazioni.

La seconda tecnica è invece conosciuta come "**disk mirroring (specchio del disco)**" che duplica una intera partizione del disco origine e la copia su un disco fisso diverso, il risultato è che esistono sempre due copie di tutti i dati separate ognuna su un disco rigido diverso.

La terza tecnica, chiamata "**sector sparing (prevenzione del settore)**" è disponibile solo su sistemi operativi avanzati come Windows NT. Il sistema operativo attiva automaticamente le funzioni di recupero dei settori mentre il computer è in fase di elaborazione. Se il sistema trova un settore rovinato durante le operazioni di lettura/scrittura (I/O) su disco, i dati presenti su quel settore vengono spostati su un settore valido e quel settore viene marcato come inutilizzabile.

Le opzioni di prevenzione dell'errore sono standardizzate e categorizzate in livelli chiamati **R**edundant **A**rrays of **I**nexpensive **D**isks (**RAID**). Questi livelli offrono varie combinazioni di prestazioni, di affidabilità e di costo. La tecnica di "disk-striping" è classificata come livello RAID = 0 mentre la tecnica di "disk-mirroring" è classificata come livello RAID=1.

UNIT 4 – LEZIONE 1 – SOLUZIONE DEI PROBLEMI IN RETE

METODOLOGIA DI SOLUZIONE DEI PROBLEMI

I problemi di rete si possono presentare anche se si è fatto un piano dettagliato, di monitoraggio e di manutenzione della rete. Prendiamo ad esempio una azienda che sviluppa software, l'assistente dell'amministratore di rete ha il compito di risolvere i problemi di rete all'interno dell'azienda, ed è collegato dal suo ufficio a tutte le filiali dell'azienda sul territorio nazionale. Applicare una metodologia di soluzione dei problemi strutturata, piuttosto che una metodologia casuale, permette di risolvere i problemi e di offrire soluzioni in modo efficiente.
L'approccio strutturato comprende cinque passi che portano alla soluzione di un problema di rete.
Il primo passo consiste nell'impostare la **priorità** del problema, ogni utente infatti vorrebbe che il suo problema fosse il primo a essere risolto. Una volta ricevuto un resoconto riguardante il problema che si sta presentando, l'amministratore di rete, valutate le conseguenze che il problema stesso può provocare sulla rete, stabilisce una priorità per quel problema. Per esempio un utente si lamenta che la rete è lenta, mentre tanti altri comunicano che non riescono assolutamente a connettersi al server, siccome il secondo problema è più grave, gli deve essere assegnata una priorità maggiore.
Il secondo passo nell'approccio strutturato consiste nella **raccolta delle informazioni** legate al problema segnalato, questo aiuta ad isolarlo. Si possono raccogliere le informazioni sul problema analizzando la rete e questo può fornire un indizio per la causa e quindi per la soluzione del problema stesso. Esaminando la rete può essere utile rivedere la storia documentata della rete per vedere se il problema in esame è già accaduto in passato e se esiste una soluzione memorizzata.
Un altro metodo per isolare un problema di rete è di chiedere informazioni agli utenti di rete riguardo al problema segnalato, infatti alcune osservazioni degli utenti possono costituire un indizio. Tenendo conto delle segnalazioni iniziali degli utenti, si devono predisporre alcune domande per identificare il problema, può ad esempio essere utile capire se gli utenti interessati sono molti oppure uno solo, se il problema si ripete costantemente e se esisteva prima dell'ultimo aggiornamento. Può essere altrettanto utile sapere se il problema si presenta in tutte le applicazioni o solo in una, se è stata installata una nuova applicazione prima che si presentasse il problema, oppure se recentemente è stato aggiunto qualche nuovo componente della rete.
Se l'esame iniziale della rete e le informazioni raccolte dagli utenti non rivelano il problema, è necessario **dividere l'intera rete in segmenti logici** in questo modo risulta più facile gestire sezioni più piccole della rete alla ricerca dell'errore. Una volta che l'errore è stato circoscritto ad un segmento della rete si deve verificare ogni elemento di quella parte di rete. I componenti di rete da verificare sono i computer client, le schede di rete, i cavi, i connettori, i computer server, la presenza di connessione fra i vari elementi, e i protocolli di trasmissione
Il terzo passo dell'approccio strutturato è **la preparazione di una lista di possibili cause** il ritorno di informazioni dagli utenti e le risposte al questionario preparato in precedenza aiutano a formare questa lista. Una volta creata la lista bisogna cercare di creare una classifica delle possibili cause in modo che la più probabile sia in cima alla lista.

Il quarto passo è quello di **isolare la causa del problema** dalla lista delle possibili cause. Dopo aver selezionato la causa più probabile bisogna verificare se effettivamente si tratta della causa che provoca l'errore. Per esempio se si sospetta che il problema risieda in un connettore difettoso, sostituirlo per verificare che il problema è stato risolto.
L'ultimo passo consiste nell'esaminare i risultati della prova condotta per trovare la soluzione. Se la prova ha identificato il problema con successo, bisogna intervenire e correggere la causa dell'errore, se invece il problema persiste è necessario tornare ai passi precedenti e ricominciare a raccogliere informazioni.

FORMULARE UN PIANO DI PREVENZIONE DEI DISASTRI

Preparare un piano di prevenzione dei disastri è importante per poter recuperare i dati in seguito a qualunque evento, anche catastrofico, che possa accadere alla rete. Gli eventi che si possono catalogare come "**disastri**" sono incendi, alluvioni, terremoti e furti. Immaginiamo di essere l'amministratore di rete di una società di software che non ha ancora sviluppato un piano di prevenzione dei disastri, in questo caso è necessario formularlo per motivi di sicurezza e prevenzione. Un disastro è un evento diverso da un semplice problema che si presenta sulla rete, perché è imprevedibile ed enormemente distruttivo, infatti distrugge sia i dati che le macchine e normalmente la distruzione è così devastante che recuperare i dati e le macchine diventa impossibile. Le situazioni più comuni che possono portare ad un disastro sono guasti del disco sul server, distruzione di macchine costose, o la formattazione accidentale di un disco. La soluzione per prevenire i disastri è pianificarli.
Il primo passo per preparare questo piano è creare un documento che contiene i dettagli di tutti gli aspetti della rete, deve contenere gli schemi di configurazione hardware e software di tutti i clients e servers della rete, deve anche contenere la documentazione riguardanti tutti i cavi utilizzati e le apparecchiature di collegamento della rete, inoltre il piano deve contenere i nomi dei fornitori delle apparecchiature hardware ed il numero di telefono della società locale che fornisce servizi di rete.
Successivamente è necessario pianificare i salvataggi che sono importanti per recuperare i dati dopo un disastro, comunque una calamità naturale può distruggere anche le copie di salvataggio, e quindi pianificare la conservazione delle copie di salvataggio in un luogo diverso è necessario per prevenire anche questa eventualità. Gli indirizzi, i nomi dei contatti ed i codici di autorizzazione per un programma di gestione dei dati di salvataggio situato in un altro luogo devono essere parte integrante del piano. Lo stesso piano deve inoltre contenere gli indirizzi e i numeri di telefono di agenzie specializzate nei servizi di recupero dei dati. Esistono società locali e nazionali che forniscono questo tipo di servizio ed è importante pianificare anche l'attivazione di un contratto con una di queste società. Nel piano deve essere anche specificato se la compagnia responsabile dei servizi di recupero, è in grado di ripristinare i dati su disco in seguito ad eventi disastrosi. Se l'unico componente danneggiato dal disastro è solo il server, spesso è possibile ripristinare i dati danneggiati senza l'aiuto di una società di servizi di recupero professionale. Questo si può fare utilizzando un "kit di emergenza". Questo kit contiene :

- Un dischetto di avvio per ogni tipo di sistema operativo e per ogni scheda di rete
- Una scheda di rete di ricambio

- Un insieme di schede di base come ad esempio la scheda di controllo del disco
- Un dischetto di avvio per ogni tipo di server presente nella rete
- Programmi di utilità per avviare i computers e lavorare su di essi
- Un panno antistatico
- Una bomboletta di aria compressa
- Gli schemi di configurazione per ogni client e server presenti sulla rete
- Può essere incluso anche un programma di elaborazione testi per modificare i files

Per gestire una emergenza è importante creare sul server una cartella che contiene la copia del sistema operativo utilizzato, i files di configurazione originali, e qualunque altra applicazione necessaria per installare un client.
Il piano di prevenzione deve contenere anche gli indirizzi delle aziende che possono sostituire le macchine guaste e riparare i danni sui computers.
La pianificazione della rottura dei dischi o della loro formattazione accidentale, deve includere la presenza di determinati programmi di utilità da installare su tutti i computer client, che tengano traccia dei files che sono stati cancellati. Questa funzione da la possibilità di recuperare i dati in caso di disastro.
Il piano di prevenzione deve necessariamente includere i dettagli della documentazione di rete. E' consigliabile far circolare diverse copie del piano fra gli impiegati, e tenere una copia in un ufficio distante dalla sede della propria azienda o a casa propria.

UNIT 4 – LEZIONE 2 - PROBLEMI DI RETE COMUNI

IDENTIFICARE PROBLEMI DI CAVI

I cavi sono la causa più comune di errori sulla rete, nella ricerca dei problemi i cavi sono uno dei componenti da controllare per primi.

Prima di tutto si deve verificare se il cavo è rotto, poi bisogna considerare che l'interruzione su un cavo può essere provocata dall'aggiunta di un nuovo computer alla rete ma collegato male, oppure se c'è un nuovo cavo nella rete, il problema può provenire da un corto circuito al suo interno. Un'altra verifica consiste nel controllare che il cavo non sia arrotolato o annodato troppo forte. Altri problemi collegati ai cavi sono determinati dai "terminali" che sono i connettori posti alle estremità dei cavi di collegamento, questi terminali possono mancare in seguito ad un errore o a un distacco accidentale, per cui è importante verificare che tutti i cavi abbiano i loro terminali.

La successiva verifica riguarda la compatibilità del cavo con la scheda di rete, infatti ogni scheda di rete richiede uno specifico tipo di cavo e utilizzando un tipo di cavo non compatibile con la rete si crea sicuramente un problema. Un problema di cablaggio può anche essere generato dalla vicinanza al cavo di una sorgente di interferenze come un condizionatore, un trasformatore o un grande motore elettrico. Un ulteriore problema si genera quando la lunghezza totale dei cavi supera la lunghezza massima consentita dalla rete, ciò può accadere quando si aggiunge un nuovo computer alla rete.

PROBLEMI COLLEGATI ALLE SCHEDE DI RETE

Un problema relativo alla scheda di rete può generarsi quando l'impostazione della scheda non corrisponde alla impostazione richiesta dal software di rete, infatti l'impostazione della porta di I/O, l'indirizzo di partenza della memoria, e l'impostazione dell'interrupt (IRQ) sulla scheda di rete devono essere gli stessi di quelli specificati nel software di gestione della rete. Bisogna assicurarsi che l'indirizzo I/O della scheda di rete non sia lo stesso di nessun'altra scheda installata sul computer, infatti gli indirizzi I/O sono unici e assegnare lo stesso indirizzo a due schede diverse può generare conflitti di memoria. Normalmente per installare una scheda di rete si utilizza l'IRQ 3 oppure l'IRQ 5.

Un altro tipo di problema può provenire dalla scheda di rete, quando la velocità di trasmissione impostata sulla scheda non corrisponde a quella richiesta dalla rete.

Bisogna anche verificare che il tipo di scheda utilizzato sia compatibile con il tipo di rete installato. Ad esempio una scheda di rete "token-ring" installata su una rete di tipo "ethernet" creerà sicuramente problemi.

Il computer e la rete diventano incompatibili anche se l'architettura della scheda di rete non corrisponde con l'architettura interna del computer, ad esempio una scheda con architettura EISA è compatibile con un computer Hewlett Packard ma non con un computer Macintosh

Successivamente è importante verificare che si stia utilizzando il tipo giusto di connettore per quel tipo di scheda. Per esempio una connessione alla rete di tipo “thicknet” deve utilizzare un connettore AUI a 15 pin per effettuare fisicamente il collegamento fra il cavo e la presa a 15 pin situata sulla scheda di rete.

SOLUZIONI PER I PROBLEMI COMUNI RELATIVI AI CAVI

Molti errori della rete provengono da problemi legati ai cavi, quindi è importante identificare il problema ed offrire la soluzione appropriata.

Un primo problema nasce quando si aggiungono nuovi computers alla rete, in questo caso può succedere che alcuni utenti non riescano più a collegarsi al server. Per risolvere il problema bisogna affrontarlo per piccoli passi successivi.
Se il cavo è interrotto si deve trovare il punto di interruzione con l’aiuto di strumenti di verifica dei cavi e ripararlo. Gli strumenti più utilizzati per trovare queste interruzioni sono i **voltmetri digitali (Digital Volt Meters o DVMs) , i Time Domain Reflectors o TDRs e gli oscilloscopi.**

Il voltmetro digitale è uno strumento elettronico capace di misurare il voltaggio che passa attraverso una resistenza, in questo modo il DVM è in grado di verificare se il cavo e intero è può trasportare dati, oppure se è interrotto e causa un problema alla rete, inoltre può aiutare a capire se c’è un corto circuito sul cavo ma sarà necessario anche un “tester” per trovare il punto esatto del corto circuito

Il TDR è un altro strumento di verifica dei cavi che invia impulsi “sonar” lungo il cavo. Questi impulsi, tornando indietro al TDR, sono in grado di identificare le interruzioni o i corto circuiti presenti sul cavo, infatti quando gli impulsi raggiungono la fonte del problema e tornano al TDR, questo li analizza e visualizza i risultati, ciò permette di trovare un difetto del cavo nel raggio di pochi metri.

Anche un oscilloscopio è in grado di identificare questo tipo di problemi. Un oscilloscopio è uno strumento che misura la quantità di segnale in un arco di tempo definito e visualizza il risultato su un monitor. Per esempio la diminuzione del segnale su una rete, può essere anch’essa un problema, utilizzando un oscilloscopio in combinazione con un TDR, si otterranno informazioni sul voltaggio presente in intervalli di tempo definiti, segnalando così l’eventuale diminuzione del segnale sulla rete.

Un altro tipo di problema si verifica quando un nuovo cavo aggiunto alla rete non è compatibile. La soluzione è di sostituirlo con un cavo adatto. Ad esempio in una rete Ethernet di tipo 10base2 sono richiesti cavi coassiali di tipo RG-58 se invece vengono utilizzati cavi di tipo thicknet STP, i problemi sulla rete saranno inevitabili. La soluzione è quella di utilizzare tutti cavi RG-58.

Aggiungendo nuovi computers nella rete si può raggiungere la lunghezza massima consentita, in questo caso si può risolvere il problema aggiungendo un “**ripetitore**” nella rete che dividerà la rete in due segmenti entrambi minori dei limiti richiesti. Per esempio in una rete Ethernet di tipo

10base2 la lunghezza massima di un segmento può essere 185 metri. Per collegare un computer che si trova ad una distanza di 900 metri si dovranno utilizzare 4 ripetitori per ottenere 5 segmenti da 185 metri ciascuno (185 x 5 = 925 metri – lunghezza massima raggiungibile con 5 ripetitori)

Quando in un segmento di una rete "thinnet" si scollega un terminale, tutto il segmento diventa irraggiungibile. Si deve verificare se questa è la causa dell'interruzione e quindi bisogna utilizzare uno strumento come un TDR oppure un analizzatore di rete per fare una traccia del segmento guasto. Per trovare il segmento guasto bisogna scollegare un computer che si trova circa a metà della rete e verificare quale delle due metà continua a evidenziare il problema, quindi si può continuare a dividere la rete a metà fino a localizzare il cavo che causa l'errore.

SOLUZIONI PER I PROBLEMI RELATIVI ALLE SCHEDE DI RETE

Immaginiamo che in una rete Ethernet di tipo 10base2 sia stato rilevato un errore su una scheda di rete di un computer IBM. Dopo essersi assicurati di avere il driver necessario per configurare la scheda di rete che provoca l'errore, si devono verificare i parametri fondamentali della scheda per identificare il problema.
Prima di tutto si deve utilizzare un programma diagnostico di sistema per scoprire quale IRQ risulta libero sul computer interessato e quindi bisogna impostare l'IRQ giusto sulla scheda di rete, se il problema persiste si deve verificare se l'impostazione della porta di I/O è giusta, per esempio l'impostazione giusta per l'IRQ potrebbe essere fra l'indirizzo 300 F e 30 F.
Se dopo questi interventi il problema non si risolve, bisogna assicurarsi che la scheda sia compatibile con l'architettura dei bus di sistema, ad esempio l'architettura dei bus ISA presente sul computer IBM che sta presentando il problema, richiede una scheda con architettura ISA a 16 bit.
Bisogna assicurarsi anche che siano utilizzati i connettori adatti. Per esempio la scheda per la rete Ethernet di tipo 10base2 richiede dei connettori di tipo BNC T, qualunque altro tipo di connettore genera sicuramente un problema in questo tipo di rete.
Se la scheda di rete ha la possibilità di utilizzare sia il circuito ricevente presente sulla scheda stessa, che un circuito ricevente esterno alla scheda, si deve scegliere quale dei due circuiti utilizzare. Questo si realizza impostando un "**jumper**" sulla scheda, un jumper è un piccolo connettore presente sulla scheda che unisce insieme due pins attivando in questo modo un circuito alternativo ad un altro.

SITUAZIONI CHE DETERMINANO PROBLEMI DI SOVRACCARICO SULLA RETE

I problemi di sovraccarico sulla rete si determinano quando il numero di messaggi generali (**broadcast messages**) inviati supera i limiti imposti dalla larghezza di banda della rete. Un messaggio generale (broadcast) è un messaggio inviato contemporaneamente a tanti destinatari. In una rete un messaggio “broadcast” viene inviato a tutti i computers che ne fanno parte. Questo può essere paragonato ad un messaggio comunicato con un megafono in una stanza piena di ascoltatori. Se un ascoltatore nella stanza continuamente fa domande alla persona che sta comunicando il messaggio nessun altro ascoltatore avrà la possibilità di parlargli, nello stesso modo se un computer trasmette messaggi incessantemente questo provoca un sovraccarico nella rete (**broadcast storm**). Durante un “broadcast storm” un computer comincia ad inviare una quantità enorme di messaggi, questo provoca che il traffico sulla rete raggiunge il punto di saturazione, a questo punto la rete non è più in grado di inviare messaggi a nessun computer, infine la conseguenza finale è lo scollegamento della rete.
Un'altra causa di sovraccarico della rete può provenire dalla configurazione errata di un computer che fa parte della rete stessa e può essere risolto riconfigurando il computer in questione.
Anche una rete molto estesa composta di un solo segmento può generare un sovraccarico. Si può evitare questo inconveniente dividendo la rete in segmenti più piccoli utilizzando i “routers”. I “routers” agiscono anche come barriera di sicurezza fra un segmento e l’altro, infatti si possono mettere i messaggi in attesa sul “router” per passare al prossimo segmento solo quando il traffico della rete non risulta sovraccaricato.

UNIT 5 – LEZIONE 1 – TECNOLOGIE DI TRASMISSIONE WAN

TRASMISSIONE ANALOGICA

I computers che fanno parte di una **WAN** (**W**ide **A**rea **N**etwork) comunicano fra loro utilizzando la tecnologia di trasmissione analogica, l'identificazione dei differenti tipi di linee analogiche disponibili e le condizioni in cui possono essere usate aiutano nella pianificazione della installazione di una rete WAN. Esistono due tipi di linee analogiche utilizzabili per le reti WAN e sono le **linee telefoniche comuni** e le **linee dedicate.**

Le linee telefoniche comuni sono fornite in America dal **P**ublic **S**witched **T**elephone **N**etwork (**PSTN**) e consistono di una rete di circuiti commutati utilizzati principalmente per la trasmissione della voce, le reti WAN possono usare questa rete di linee telefoniche con l'aiuto dei modems. In questo tipo di linee ogni connessione utilizzata per una singola comunicazione è riutilizzabile, ciò significa che ogni nuova comunicazione stabilisce sempre una nuova connessione. Bisogna notare che le operazioni su questo tipo di linee sono lente perché le connessioni non sono di ottima qualità.

Un altro tipo di linea analogica è la linea dedicata o linea in "affitto". Contrariamente alla linea comune, questa linea offre un collegamento a tempo pieno senza dover effettuare una connessione manuale per ogni comunicazione, quindi queste linee sono utili per quelle aziende che hanno la necessità di comunicare costantemente con le loro filiali o con i loro clienti. Le linee dedicate sono più veloci e affidabili delle linee analogiche comuni ma sono anche più costose.

La scelta di una linea comune o di una linea dedicata dipende da diversi fattori come il tempo che verrà utilizzato per la connessione, il costo del servizio, e la velocità ed affidabilità richiesta nella trasmissione dei dati. Se la linea analogica è richiesta per trasmissioni poco frequenti è sicuramente più adatta una linea comune per una rete WAN, questo tipo di linea è da preferirsi anche quando il costo delle comunicazioni piuttosto che la affidabilità costituisce il fattore decisivo.
Invece se si richiede una linea per trasmissioni molto frequenti o addirittura 24 ore su 24 la linea dedicata è sicuramente la migliore per una rete WAN, è anche da consigliare nel caso in cui sia richiesta affidabilità indipendentemente dal costo della trasmissione.

TRASMISSIONE DIGITALE

Quando il traffico sulla rete è molto elevato, la trasmissione di dati su una rete WAN attraverso le linee analogiche, diventa inefficiente e costosa. Per superare questo problema si possono usare le **linee digitali** come metodo alternativo per la trasmissione dei dati. La comunicazione attraverso le linee digitali non richiede l'uso di modems e quindi questo tipo di comunicazione è più veloce di quello analogico, inoltre le linee digitali sono più sicure in quanto utilizzano linee dedicate molto affidabili, un utente che utilizza questo tipo di connessione può contare sul 99% di trasmissione dei dati senza errori perché i computers sono connessi direttamente fra di loro attraverso circuiti digitali "punto a punto".

Esistono quattro tipi di linee digitali :

La prima è la linea di tipo **D**igital **D**ata **S**ervice (**DDS**) che offre una comunicazione simultanea fra il punto di invio dei dati e quello di ricezione dei dati a velocità di 2,4 / 4,8 / 9,6 fino a 56 Kilobits per secondo (Kbps). Quando viene utilizzata una linea di tipo DDS i dati vengono inviati sulla rete da un BRIDGE o da un ROUTER verso un apparecchio che prende il nome di **C**hannel **S**ervice **U**nit / **D**ata **S**ervice **U**nit (**CSU/DSU**). Questo apparecchio converte i segnali digitali provenienti da un computer in segnali digitali bipolari che costituiscono una parte fondamentale della comunicazione sincrona cioè la comunicazione di dati sincronizzata fra il computer che invia i dati e quello che li riceve.

Il secondo tipo di linea digitale è conosciuto come linea **T1** e viene utilizzata soprattutto per trasmettere segnali audio e video alla velocità di 1544 Megabits per secondo (Mbps). Una linea T1 utilizza una tecnologia di trasmissione che utilizza due coppie di cavi di rame per inviare e ricevere i dati simultaneamente. Questo tipo di linea comunque è molto costosa e per ridurre il costo di questo tipo di connessione gli utenti possono attivare una "sottolinea" di tipo T1 chiamata **Fractional T1 (FT-1)** . Una linea FT-1 è composta di diversi canali da 64 Kbps e ogni utente può scegliere il numero di canali che vuole utilizzare.

Il terzo tipo di linea digitale è la **linea T3.** E' una linea dedicata per la trasmissione di dati e voce ad una velocità fra 6 e 45 Mbps e può utilizzare sia cavi a microonde che in fibra ottica. Una sola linea di tipo T3 sostituisce diverse linee di tipo T1. Anche per questa linea gli utenti possono attivare una linea **Fractional T-3 (FT-3)** per ridurre i costi

Il quarto tipo è la linea **Switched 56** che è gestita da compagnie telefoniche locali e di lunga distanza, e consiste in un servizio da rete LAN a rete LAN che trasmette i dati alla velocità di 56 Kbps. Utilizzando questo tipo di rete vengono inviate grandi quantità di dati da un punto fisso della rete ad un altro attraverso un apparecchio CSU/DSU che può a sua volta collegarsi con un altro nodo Switched 56, dato che la linea viene utilizzata solo su richiesta di una connessione non esiste il costo che invece è legato alle linee dedicate

TECNOLOGIA DI SCAMBIO DEI PACCHETTI

La tecnologia di scambio dei pacchetti è una tecnica molto popolare nella comunicazione sulle reti WAN. E' una tecnica veloce e affidabile di trasmissione dei dati, nella quale i dati vengono trasmessi in forma di "pacchetti". La trasmissione dei dati in "pacchetti" avviene attraverso circuiti virtuali o connessioni logiche fra i computer che inviano e quelli che ricevono dati.
Ci sono due tipi di circuiti virtuali, i **circuiti virtuali commutati** ed i **circuiti virtuali permanenti**

I circuiti virtuali commutati sono circuiti temporanei perché la connessione fra il computer che invia e quello che riceve i dati termina quando la comunicazione si conclude. Questa comunicazione avviene attraverso un canale specifico sulla rete.

I circuiti virtuali permanenti invece sono simili alle linee dedicate, gli utenti che chiedono di attivare questo tipo di linea pagano per il tempo utilizzato dai computers per inviare e ricevere i dati

Prima ancora di avviare la connessione logica fra due computers, in una rete con scambio di "pacchetti", gli stessi computers si scambiano informazioni riguardanti i parametri di comunicazione. Questi parametri includono la misura dei pacchetti e i canali utilizzati dai dati per raggiungere il computer di destinazione. Una volta che i computers di origine e di destinazione hanno stabilito i parametri di comunicazione i pacchetti di dati originali vengono divisi in pacchetti più piccoli prima di dare inizio alla trasmissione vera e propria. Ognuno di questi piccoli pacchetti contiene l'indirizzo del computer destinazione e i dati da trasportare ciò permette ad ogni pacchetto di poter viaggiare individualmente sulla rete, ogni pacchetto può prendere diverse strade per raggiungere il computer ricevente, ogni volta la strada scelta è quella più veloce disponibile in quel momento sulla rete, di conseguenza i piccoli pacchetti che compongono il pacchetto originale arrivano al computer ricevente in tempi diversi e senza nessun ordine, comunque il computer ricevente è in grado di ricomporre sempre il pacchetto originale. I piccoli pacchetti vengono ricomposti nel pacchetto originale solo se la trasmissione dei dati non ha presentato errori, nel caso in cui si verifichi un errore, il pacchetto che lo ha generato viene trasmesso di nuovo.

PROTOCOLLI DI COMUNICAZIONE TELEFONICA

Le varie funzioni delle linee telefoniche dipendono dai protocolli utilizzati dalla rete telefonica per la trasmissione.Il protocollo **IP** (**I**nternet **P**rotocol) è comunemente usato dalle reti telefoniche comuni per realizzare le comunicazioni fra computers. Ogni connessione che si stabilisce fra il computer che invia e quello che riceve i dati, prende il nome di **IP Account** . Esistono due tipi di connessione IP Account :

Serial **L**ine **I**nternet **P**rotocol (**SLIP**)
Point to **P**oint **P**rotocol (**PPP**)

Le connessioni SLIP e PPP sono state progettate per per gestione collegamenti in rete attraverso le linee telefoniche. Questi protocolli regolano la connessione fisica fra i componenti della rete, ad esempio per collegare due computers attraverso un modem possono essere usati sia il protocollo SLIP che il PPP.

Il protocollo SLIP definisce le sequenze di caratteri che compongono i pacchetti su una linea seriale che può essere sia telefonica che dedicata. La velocità di trasmissione lungo questa linea seriale varia da 1200 Bps a 19,2 Kbps e dato che questo protocollo supporta una così ampia varietà di velocità di trasmissione, il protocollo SLIP può essere utilizzato per collegare due computers, un computer con un router, oppure due routers. I pacchetti trasmessi con il protocollo SLIP non hanno una lunghezza massima prestabilita, comunque di solito la lunghezza massima viene impostata a 1006 bytes, infatti questa è la massima lunghezza per i **pacchetti di dati Berkeley UNIX** dato che il protocollo SLIP viene utilizzato dalla maggior parte delle macchine con sistema operativo Berkeley UNIX. Il protocollo SLIP non supporta protocolli multipli, ciò significa che se due

computers che utilizzano diversi protocolli vogliono comunicare fra loro utilizzando il protocollo SLIP devono avere la possibilità di convertirsi al protocollo SLIP stesso. Gli errori di trasmissione dovuti ai disturbi presenti sulle linee telefoniche non sono rilevati né corretti dal protocollo SLIP, inoltre le connessioni SLIP non sono standard e quindi due installazioni del protocollo SLIP su due reti diverse possono essere incompatibili, questo protocollo e consigliabile per le aziende che vogliono trasmettere pacchetti di dati di dimensioni differenti alla velocità di 1000/2000 Bps.

Per superare i limiti imposti dal protocollo SLIP è stato sviluppato un altro protocollo conosciuto come PPP. Questo protocollo attiva, configura e verifica la connessione fra due computers con l'aiuto del **L**ink **C**ontrol **P**rotocol (**LCP**) che fa parte dello stesso protocollo PPP. Un altro componente di questo protocollo, conosciuto come **N**etwork **C**ontrol **P**rotocol (**NCP**), aiuta il protocollo PPP a collegarsi e configurarsi per il collegamento con diversi altri protocolli di rete come IP, IPX e Apple Talk, inoltre il protocollo PPP supporta la gestione di protocolli multipli sulla stessa connessione, e supporta anche la lunghezza variabile dei pacchetti nelle connessioni fra i vari componenti della rete. Questo protocollo è progettato in modo da poter collegare diversi tipi di componenti hardware ad apparecchi per la connessione come "bridges" o "routers", inoltre gli errori di trasmissione dei dati vengono rilevati e le connessioni errate vengono concluse. Il protocollo PPP è consigliabile per quelle aziende che vogliono espandere la loro rete collegando un server ad un router per la trasmissione di pacchetti di dati con lunghezza variabile e utilizzando diversi protocolli.

UNIT 5 – LEZIONE 2 – TECNOLOGIE DI TRASMISSIONE WAN AVANZATE

X.25

Una rete X.25 è una rete con scambio di pacchetti che utilizza l'insieme dei protocolli X.25. Un'azienda che voglia inviare le informazioni sulle vendite annuali da una filiale alla sede principale, in un ambiente protetto, può utilizzare una rete X.25. Nelle prime versioni della rete X.25 la trasmissione dei dati avveniva attraverso le linee telefoniche, che però erano inaffidabili e provocavano errori nella comunicazione dei dati. Per superare questi problemi la rete X.25 è stata potenziata includendo il controllo degli errori e la ritrasmissione dei dati errati.
L'insieme di protocolli X.25 attuale è una interfaccia fra una periferica ed una rete pubblica attraverso una linea dedicata. Questa interfaccia prende il nome di **D**ata **T**erminal **E**quipment/**D**ata **C**ommunication **E**quipment (**DTE/DCE**). Una DTE può essere un computer con una interfaccia X.25 o può essere anche un "gateway" fra una rete pubblica ed una LAN o WAN, oppure un assemblatore/disassemblatore di pacchetti (**PAD**).
Una DTE, quando funziona come assemblatore, riceve i caratteri in forma asincrona da un terminale a bassa velocità e compone i "pacchetti" con i caratteri ricevuti, quindi i pacchetti vengono trasmessi sulla rete.
Quando invece funziona come disassemblatore scompone i pacchetti ricevuti dalla rete e quindi invia i caratteri in essi contenuti verso i terminali.
L'elemento DCE di una interfaccia DTE/DCE si riferisce alle reti pubbliche.
L'utilizzo dell'insieme di protocolli X.25 in una rete pubblica permette la condivisione delle linee di comunicazione che riduce i costi di connessione, inoltre la trasmissione dei dati su una rete X.25 è affidabile grazie ad un meccanismo di autocorrezione.
In una rete X.25 non è mai definito il percorso che i pacchetti devono seguire per raggiungere la loro destinazione, essi possono essere trasmessi da qualunque dei circuiti di smistamento multipli, e questi circuiti possono essere scelti liberamente dai pacchetti, questo meccanismo aumenta molto la velocità della rete.
Ogni pacchetto è numerato, catalogato e controllato dalla rete X.25, se un pacchetto non raggiunge la propria destinazione la rete genera un segnale che provoca una nuova trasmissione dello stesso pacchetto, inoltre la rete X.25 garantisce una grande compatibilità per il trasferimento dei files, la condivisione delle risorse e l'invio di posta elettronica.

FRAME RELAY

I progressi fatti nella tecnologia digitale e nei cavi in fibra ottica hanno portato ad un grande cambiamento nella comunicazione sulle reti, facendole diventare tecnologie di avanguardia, infatti esse richiedono un minor controllo dell'errore rispetto alle precedenti tecnologie analogiche.
La tecnologia **"Frame Relay"** è una tecnologia di comunicazione attraverso pacchetti digitali e le reti che la utilizzano sono conosciute come **"reti frame relay"** ed utilizzano un circuito virtuale permanente per effettuare la trasmissione dei dati.

In questo tipo di rete i pacchetti, che possono avere lunghezza variabile e che sono chiamati **“frames”** , vengono trasmessi da un nodo all’altro ad una velocità che varia da 56 Kbps a 1.544 Mbps. L’utilizzo di un circuito virtuale permanente rende le comunicazioni molto rapide e rende possibile conoscere l’intero percorso seguito da ogni pacchetto nella rete, inoltre non è necessario comporre e scomporre i pacchetti come invece avviene in altre reti. Un’altra caratteristica è che questa rete trasmette i dati in modo molto veloce perché non deve correggere gli errori, infatti in caso di errore o di sovraccarico, la rete ferma temporaneamente i pacchetti in viaggio, saranno poi i computers trasmittente e ricevente ad occuparsi della correzione degli errori.
Per gestire il traffico su una rete “frame relay” è necessario un “router” oppure un “bridge” compatibili con questo tipo di rete per garantire una trasmissione dei dati affidabile.

ISDN

La rete **ISDN** (**I**ntegrated **S**ervices **D**igital **N**etwork) viene utilizzata per trasmettere voce, dati ed immagini su una rete telefonica digitale, questa rete integra in sé la trasmissione sia analogica che digitale e quindi permette la trasmissione di dati anche su vecchi cavi telefonici già esistenti.
Gli utenti possono accedere alla rete ISDN attraverso canali di comunicazione digitale chiamati **“bit pipes”** . Un “bit pipe” è un collegamento virtuale e temporaneo, creato fra l’utente e la linea telefonica attraverso il quale i bits di dati scorrono in entrambe le direzioni. I “bit pipes” sono utilizzati per le connessioni con scambio di pacchetti ed ogni “pipe” può supportare canali di trasmissione multipli.

Ci sono due tipi fondamentali di canali di trasmissione in una rete ISDN

CANALE ISDN DI BASE
CANALE ISDN PRIMARIO

Il canale ISDN di base ha un sottocanale chiamato **“canale B”** con velocità di 64 Kbps per la trasmissione dei dati, e un altro sottocanale chiamato **“canale D”** con velocità di 16 Kbps per i segnali di controllo, questi canali trasmettono voce, dati e immagini.
Due “canali B” possono essere utilizzati contemporaneamente in modo da trasmettere insieme dati e immagini alla velocita di 128 Kbps

Il canale ISDN primario usa l’intera larghezza di banda di un collegamento T1, questo permette l’utilizzo di 23 canali B a 64 Kbps e 1 canale D anch’esso a 64 Kbps.

ATM

Il metodo **ATM (Asynchronous Transfer Mode)** rappresenta un modello avanzato di rete con scambio di pacchetti caratterizzato da una altissima velocità. Il metodo ATM trasmette pacchetti di dimensioni fisse, ogni pacchetto infatti contiene 53 bytes e viene chiamato **"cell"** , in realtà in ogni pacchetto ci sono 48 bytes di dati e 5 bytes che contengono dati identificativi del pacchetto. Al contrario dei pacchetti a lunghezza variabile, questi pacchetti utilizzano i buffers in maniera efficiente e riducono il tempo necessario per elaborare i dati in arrivo, le celle vengono trasmesse ad una velocità molto alta che varia da 100 a 1000 Mbps. Una rete che utilizza il metodo ATM non è in grado di correggere gli errori durante la trasmissione quando ciò accade la rete ferma temporaneamente il pacchetto in viaggio. Il metodo ATM utilizza **"larghezze di banda dedicate".**
Una larghezza di banda è costituita dall'insieme di tutte le frequenze comprese fra la frequenza più bassa della banda e quella più alta, con una rete che utilizza la larghezza di banda si possono inviare dati, suoni, e immagini contemporaneamente. L'hardware utilizzato deve essere compatibile alla trasmissione di tipo ATM, se non è così sarà necessario sostituire alcuni componenti della rete per renderla compatibile. I cavi da utilizzare per le reti di tipo ATM devono essere cavi coassiali oppure cavi in fibra ottica. In una rete ATM esistono dispositivi chiamati **"switches"** che possono agire sia come **"hub"** che come **"router"**

Quando agiscono come "hub" hanno il compito di trasferire i dati da un computer a quello successivo sulla stessa rete.
Quando invece agiscono come "router" hanno il compito di trasferire i dati, ad alta velocità, verso altre reti remote.

La tecnologia ATM permette connessioni logiche multiple utilizzando una singola interfaccia fisica, per le reti WAN e LAN.

SMDS

Il servizio SMDS (**S**witched **M**ultimegabit **D**ata **S**ervice) è un altro servizio che utilizza la tecnologia di trasmissione di celle a lunghezza fissa per l'invio di dati. La trasmissione dei dati avviene ad una velocità che può variare da 1 Mbps a 34Mbps attraverso connessioni di tipo **"molti verso molti (many to many)"** , in questo tipo di connessione una sola linea SMDS permette di collegarsi a diversi computers. Le reti di tipo SMDS utilizzano uno schema **"dual-bus"** per collegare fra di loro i computers. In pratica tutti i computer della rete sono collegati ad un anello costituito da due canali (bus) che trasportano i dati, uno in senso orario e l'altro nel senso inverso.

FDDI

L'aumento delle comunicazioni legate al commercio, richiede metodi di trasmissione dei dati veloci, efficienti e sicuri. La rete **FDDI** (**F**iber **D**istributed **D**ata **I**nterface) è un tipo di rete ad anello ad alta velocità che utilizza cavi di fibra ottica per raggiungere queste caratteristiche.
La rete FDDI è stata progettata per computers che richiedono una larghezza di banda maggiore di quella fornita da una rete TOKEN RING a 4 Mbps oppure da una rete ETHERNET a 10 Mbps. Una

rete FDDI può arrivare a trasmettere dati alla velocità di 100 Mbps attraverso cavi in fibra ottica che permettono connessioni ad alta velocità a vari tipi di reti. Per esempio una rete FDDI può essere adatta per creare una **M**etropolitan **A**rea **N**etwork (**MAN**) collegando fra loro diverse reti nella stessa città invece, dato che la rete FDDI è limitata ad una distanza massima di 62 miglia (100 chilometri), non è consigliabile per creare reti WAN. La rete FDDI utilizza il metodo di trasmissione a **"doppio anello".** I due anelli vengono utilizzati per inviare i dati che viaggiano in direzioni opposte a seconda che siano dati in andata oppure in ritorno.
I due anelli vengono chiamati **"anello primario"** e **"anello secondario"** il primo viene utilizzato per il traffico normale della rete, mentre il secondo viene utilizzato quando si verifica un errore sul primo. Il sistema FDDI utilizza un metodo chiamato **"beaconing"** per isolare gli errori presenti su un anello. Il computer che rileva l'errore manda un segnale specifico sulla rete, che prende il nome di **"beacon".**
Ogni rete FDDI può gestire al massimo 500 computers e la lunghezza totale dei cavi di collegamento può essere al massimo 100 chilometri, sfruttando però l'esistenza dell'anello secondario si può anche arrivare a gestire 1000 computers ed una lunghezza totale dei cavi di 200 chilometri, comunque il cavo di collegamento ha bisogno di un **"ripetitore (repeater)"** ogni 2 chilometri per poter rigenerare il segnale. In questo tipo di rete i computers possono essere collegati ad entrambi gli anelli **(Stazioni di classe A)** oppure ad uno solo degli anelli **(Stazioni di classe B)** .

SONET

Un'altra tecnologia emergente che utilizza la trasmissione dei dati su cavi in fibra ottica è **SONET** (**S**ynchronous **O**ptical **Net**work) , una rete che utilizza questo tipo di tecnologia può inviare dati, suoni e immagini ad una velocità di 1 Gigabit per secondo (Gbps). La velocità di una rete SONET è definita dal livello dell' **"Optical Carrier (OC)"** e dall'equivalente segnale elettrico del **"Segnale di Trasporto Sincrono (STS)"** . L'STS-1 è la velocità minima di trasmissione di questo tipo di rete e corrisponde a 51.84 Mbps. Utilizzando multipli di STS-1 si ottengono maggiori velocità di trasmissione, ad esempio una connessione STS-3 è tre volte più veloce della STS-1 e corrisponde a 155.52 Mbps. La rete SONET permette una maggiore flessibilità di trasmissione perché utilizza la connessione BISDN e le celle ATM parallelamente.

UNIT 5 – LEZIONE 3 – FORNITORI DI ACCESSO AI SERVIZI

INTERNET

Internet è un insieme di reti, gateways, servers e computers che contiene una enorme quantità di dati. Gli utenti possono accedere alle informazioni attraverso i servizi offerti da internet stessa, e ciò ha portato ad una immensa crescita dei tipi di servizi offerti e del loro utilizzo da parte degli utenti.

Il primo tipo di servizio offerto da internet è un servizio multimediale chiamato **W**orld **W**ide **W**eb (**WWW**) esso è composto da documenti ipertestuali scritti in **HTML** (**H**yper**T**ext **M**arkup **L**anguage). Il metodo ipertesto collega fra loro testi, immagini, suoni e video in maniera libera e permette all'utente di consultarli in qualunque ordine.
Il secondo tipo di servizio offerto da internet è conosciuto come **F**ile **T**ransfer **P**rotocol (**FTP**) . L'FTP è un protocollo di trasferimento dei dati utilizzato negli ambienti TCP/IP, supporta il collegamento con reti remote e permette il trasferimento di archivi da servers di tipo FTP che gestiscono una incredibile quantità di informazioni. Gli utenti possono accedere a queste informazioni scaricando un intero archivio dal server FTP al server locale e possono essere sia archivi di testo che archivi binari.
Il terzo tipo di servizio internet è conosciuto come **GOPHER** . E' un protocollo di trasferimento dei dati simile all'FTP che ha il vantaggio di poter gestire archivi che si trovano sparsi su diversi computers. Il servizio gopher è uno strumento, con gestione da menù, che permette agli utenti di fare ricerche su liste di risorse disponibili e ricevere dati da queste risorse.
Il quarto tipo di servizio offerto da internet è conosciuto come **N**etwork **N**ews **T**ransfer **P**rotocol (**NNTP**) o **News** . Questo protocollo viene utilizzato per distribuire velocemente richieste, risultati e novità gestite dal servizio Network News **(USENET)**, questo servizio mette a disposizione resoconti **(bulletin board)** e stanze virtuali per discussioni **(chat rooms)** che offrono una fonte di informazioni su argomenti che vanno dalle novità tecnologiche agli hobbies personali, inoltre offre la possibilità di partecipare a videoconferenze chiamate **newsgroups.** Gli utenti possono aderire a queste newsgroups e comunicare attraverso un sistema di messaggi simile alla posta elettronica. Le comunicazioni nelle newsgroup avvengono in un forum pubblico. Esiste anche una opzione per vedere i dialoghi in corso senza partecipare.
Il quinto tipo di servizio offerto da internet si chiama **TELNET.** Questo è un protocollo internet che permette di collegarsi ad un server internet come terminale remoto. Utilizzando il protocollo TELNET si possono eseguire programmi che risiedono su un computer che si trova all'altro capo del mondo proprio come se ci si trovasse seduti di fronte a quel computer. Il protocollo TELNET fa parte del protocollo TCP/IP nei computers che hanno il sistema operativo Windows 95 e Windows NT.
L'ultimo tipo di servizio offerto da internet è la **posta elettronica**. E' il servizio più popolare di internet per inviare e ricevere messaggi in forma elettronica. Questa forma di comunicazione è meno costosa di una comunicazione telefonica specie se a lunga distanza. Un altro vantaggio della posta elettronica consiste nella possibilità da parte degli utenti di consultare i loro messaggi i

qualunque momento, e di poter inviare lo stesso messaggio a tanti utenti contemporaneamente con la semplice pressione di un tasto.

MSN

Il **M**icro**s**oft **N**etwork è uno dei più grandi fornitori di servizi su internet. E' un servizio in linea che fornisce informazioni dalla Microsoft, dall'**ICP** (**I**ndependent **C**ontent **P**roviders) e da Internet, fra di questi sia la Microsoft che l'ICP creano contenuti specifici per l'MSN. Il servizio di posta elettronica offerto dal MSN permette ai suoi membri di gestire tutti i loro messaggi e fax in un solo luogo anche se provenienti da diversi gestori di posta.
Le funzioni di gestione della posta elettronica sono accessibili dagli utenti attraverso il programma **Microsoft Exchange** che viene fornito da MSN, questo programma supporta il **Rich Text Format** che permette di mescolare nei messaggi caratteri, dimensioni, stili e colori insieme anche a immagini grafiche. E' possibile anche includere nei messaggi oggetti come documenti, immagini ed altri archivi come allegati.
I membri del MSN possono navigare più facilmente utilizzando il programma Internet Explorer perché utilizza la stessa interfaccia di Microsoft Windows 95.