

ISTITUTO : I.P.S.I.A MORETTO-BRESCIA

Busi Stefano, Panza Francesco, Giovanni Buratti

5[^]BZ

Sms Gateway



Anno scolastico 2003/04

Premessa

Per effettuare la nostra tesi d'esame è stato deciso di realizzare un programma che svolge le seguenti funzioni:

1. Connettersi ad un server di posta dove giungono messaggi che devono essere inviati a telefoni cellulari via sms.
2. Controllare rigorosamente il formato delle e-mail.
3. Inoltrare le e-mail che seguono il protocollo predefinito e cancellare le e-mail non valide.

Invio SMS attraverso Internet

L'invio di sms tramite Internet è un procedimento molto semplice da fare. Come prima cosa bisogna scegliere uno dei siti autorizzati per inviare messaggi, poi una volta scelto si deve scrivere il messaggio non superando il numero massimo di caratteri, che variano da sito a sito, in seguito dovrà essere scelto il prefisso del cellulare a cui inviare il messaggio e in fine scrivere il numero del destinatario. Qui sotto abbiamo elencato tutti i prefissi per i cellulari in Italia e la maggior parte di quelli internazionali.

Prefissi cellulari italiani

Prefissi cellulari internazionali Prefissi cellulari internazionali

ITALIA -TIM	333	Albania	35538	Portogallo	351931
ITALIA -TIM	334	Albania	35568	Romania	4074
ITALIA -TIM	335	Albania	35569	Usa	1301
ITALIA -TIM	338	Asia	65974	Usa	1410
ITALIA -TIM	339	Australia	61408	Usa	1703
ITALIA -TIM	337	Australia	61409	Usa	1717
ITALIA -TIM	363	Australia	61411	Spagna	34600
ITALIA -TIM	366	Australia	61417	Spagna	34607
ITALIA -TIM	368	Australia	61418	Spagna	34610
ITALIA -TIM	330	Australia	61419	Spagna	34617
ITALIA -TIM	336	Australia	61425	Spagna	34620
ITALIA -TIM	360	Austria	43676	Spagna	34625
ITALIA - OMMNITEL	340	Austria	43664	Spagna	34626
ITALIA - OMMNITEL	347	Arzebaijan	99450	Spagna	34651
ITALIA - OMMNITEL	348	Repubblica Ceca	420602	Spagna	34666
ITALIA - OMMNITEL	349	Repubblica Ceca	420603	Spagna	34629
ITALIA - OMMNITEL	343	Germania	170	Spagna	34630
ITALIA - WIND	328	Germania	171	Spagna	34636
ITALIA - WIND	329	Germania	172	Spagna	34639
ITALIA - WIND	320	Germania	173	Spagna	34647
ITALIA - WIND	323	Germania	174	Spagna	34649
ITALIA - BLU	380	Germania	177	Spagna	34696
ITALIA - BLU	388	Germania	178	Spagna	34656
ITALIA - BLU	389	Germania	179	Spagna	34670
ITALIA- H3g	390	Mauritsius	23025	Spagna	34606
ITALIA- H3g	391	Olanda	31621	Spagna	34609
ITALIA- H3g	392	Olanda	31625	Spagna	34616
ITALIA- H3g	393	Olanda	31627	Spagna	34619
		Olanda	31630	Spagna	34686
		Olanda	31641	Olanda	31654
		Olanda	31650	Olanda	31655

Cosa è un gateway ?

Il Gateway è un software che ha il compito di fare da tramite fra la rete di telefonia mobile e la rete Internet o Intranet.



Rete Intranet d'Istituto

Nel nostro istituto è presente una rete interna Intranet progettata con la collaborazione di ONION S.p.A. di Brescia e descritta sul documento che di seguito riportiamo.

Questo documento tratta i seguenti aspetti:

- Architettura di rete.
- Requisiti dei principali nodi di rete.
- Architettura applicativa.

Architettura di rete

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

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

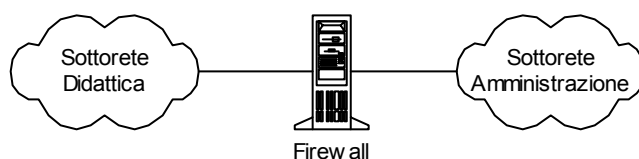
La sotto-rete amministrativa collega tutte le macchine poste negli uffici e non fisicamente accessibili dagli studenti.

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

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

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

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



- Consente di impostare politiche d'accesso differenti tra rete amministrativa e didattica (scelta ISP, velocità, etc.)

- Consente agli studenti più capaci (sempre sotto adeguato controllo) di sperimentare le tecnologie di comunicazione senza porre problemi di sicurezza e affidabilità alla rete amministrativa.
- Aumenta il throuput complessivo della rete, separando il traffico amministrativo da quello degli studenti.
- Gestisce in modo ottimale la capacità della linea ISDN che consente appunto due connessioni contemporanee a 64k.

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

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

Server Intranet

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

- Collega la rete didattica ad Internet
- Gestisce il DNS (Domain name system) principale per entrambe le reti
- Gestisce la posta elettronica degli studenti
- Fa funzionare le applicazioni intranet su interfaccia Web
- Gestisce il database con le informazioni messe a disposizione dall'area amministrativa

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

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

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

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

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

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

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

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

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

I dati sono periodicamente rinfrescati dalle applicazioni nell'area amministrativa

In breve, le applicazioni Intranet avranno le seguenti caratteristiche:

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

Quest'architettura presenta molti vantaggi:

- Il server può accedere solo ad un insieme di dati limitato (quindi sono protetti i dati più sensibili)
- I dati sono presentati alle applicazioni con una logica ad esse ottimizzata. Ne consegue una maggiore semplicità di scrittura delle applicazioni.
- I dati possono essere organizzati in un formato coerente e efficiente indipendentemente dal formato dei dati sorgente.

- Un problema di sicurezza o sistemistico sul server Intranet non pregiudica i livelli minimi di sicurezza e non pregiudica le applicazioni dell'area amministrativa

Esistono ovviamente alcuni svantaggi:

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

Come funziona il gateway all'interno del nostro istituto

Il nostro Gateway interroga a intervalli di tempo predefiniti il server di posta interno mail.ipsiamoretto.it (192.168.146.5) e verifica se la mail box sms@ipsiamoretto.it contiene messaggi. Se la mail box non contiene messaggi il Gateway si sconnette automaticamente, in caso contrario provvede a scaricare uno alla volta i messaggi contenuti, verificandone il protocollo. Se la verifica ha esito positivo, il Gateway salva il messaggio in un file di testo, in caso contrario lo cancella.

Il nome del file è composto nel seguente modo SMS146251200406108.TXT.

Le prime 3 lettere 'SMS' indicano il tipo di servizio che ha generato il messaggio (DID:didattica, SMS:sms Gateway), le 6 cifre che seguono sono quelle che riguardano le cifre più in basso dell'IP (in caso di IP= 192.168.146.251 le cifre estratte sarebbero 146 e 251), le 8 cifre seguenti a queste indicano la data del salvataggio (in caso si salvi il 10/06/2004 nel file troveremo 20040610), l'ultima cifra indica il numero progressivo del messaggio salvato.

Il contenuto del file è strutturato come segue:

SERVIZIO-SMS GATEWAY

DESTINATARIO-3334721582

MITTENTE-192.168.146.251

DATA-10/06/2004

TESTO- L'alunno Guido Lavespa da tempo non frequenta la scuola si prega di contattare la segreteria. Il preside Arturo Montanini

Questo è il protocollo che il Gateway dovrà trovare nei messaggi della mail box per dare esito positivo. Nella prima riga dovrà essere specificato il servizio utilizzato (es. SMS GATEWAY), nella seconda riga dovrà essere indicato il numero del destinatario con prefisso seguito dal numero (es. 3334721582), nella riga seguente dovrà essere indicato il mittente sotto forma di numero IP (es. 192.168.146.251), nella quarta riga dovrà essere indicata la data del messaggio (es. 10/06/2004), nell'ultima riga verrà scritto il messaggio da comunicare.

Struttura del programma

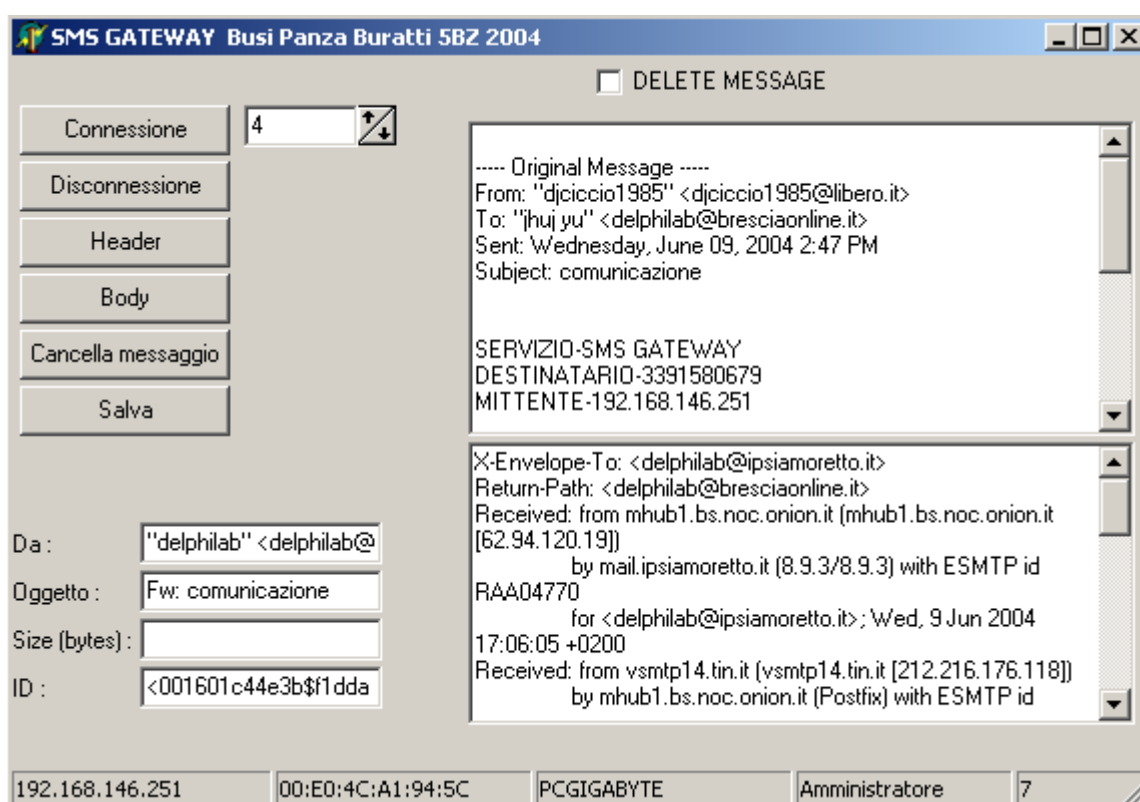
Il programma è stato realizzato con Delphi 5.0. E' composto da sei bottoni con ognuno una funzione diversa (connessione, sconnessione, header, body, cancella, salva):

-CONNESSIONE: è il bottone, che dopo aver controllato nome e password, se proviene da un PC autorizzato, il numero del server. Si connette e fa apparire sullo schermo bianco in alto(memo1) che si è connesso. Con l'automatico e l'uso di un timer(Timer1) dopo tre secondi dalla connessione controlla e dice sempre sullo stesso schermo quanti messaggi validi sono arrivati.

-SCONNESSIONE: è il bottone usato alla fine per uscire, dalla connessione, in modo regolare. Con l'automatico anche questa funzione viene fatta in automatico dopo che sono stati effettuato tutti i necessari del programma.

-HEADER: è il bottone che viene usato solo manualmente per visualizzare il messaggio completo selezionato e appare nella memo1.

-BODY: è il bottone che ha il compito di suddividere in due parti il messaggio che viene selezionato. Nella memo1 appare il messaggio essenziale dove è presente il nome del servizio, mittente, destinatario, data/ora e il testo. Es.



Nella parte bianca sotto la memo1 cioè memo2 viene visualizzata tutta la parte superflua del messaggio che a noi non interesserà quasi per niente.

-CANCELLA: è il bottone usato per cancellare il messaggio che non si vuole più visualizzare o usare. In automatico cancella tutti i messaggi dopo che vengono controllati e selezionati in validi e non validi.

-SALVA: è il bottone usato per il salvataggio del messaggio che si effettua solo dopo essere stato controllato rigorosamente e risulta valido. Viene usato anche in automatico, ha il comando di controllare e salvare messaggio per messaggio tutti quelli validi e scrivere nella cartella .log tutti i messaggi che ha salvato e invece quelli non salvati doveva dirne il motivo.

Sotto questi bottoni sono state messe **quattro edit** con il compito di segnalare, nel caso venga scelto body, da dove arriva il messaggio, il nome del servizio, la grandezza in bytes del messaggio e la ID.

Un'altra **edit** e uno **scorritore** (avanti indietro) è stata messa per far apparire il messaggio che si vuole leggere e potendolo scegliere facendo scorrere lo scorritore avanti o indietro fino al massimo dei messaggi che sono arrivati.

Le **due memo** citate precedentemente sopra hanno lo scopo di far visualizzare le parti del messaggio come spiegato prima e, in fine, in basso allo schermo c'è 1 barra di stato divisa in 5 blocchi denominati nel seguente modo:

Nella primo blocco c'è l'IP che è l'indirizzo del computer, poi c'è il MAC che è la scheda di rete del computer, il terzo blocco contiene il nome del PC, nel blocco seguente troviamo il nome dell'utente collegato in quel momento e nell'ultimo il numero dei messaggi salvati nel file .ini.

Ricezione della posta

Il server destinato alla ricezione della posta viene generalmente denominato POP3 e per comunicare con esso ci si deve collegare alla porta 110. Se per esempio il nostro server destinato alla ricezione della posta fosse mail.ipsiamoretto.it dovremmo digitare quanto segue:

mail.ipsiamoretto.it 110.

Il gateway si connette al server di posta; bisognerà essere sicuri, però, che oltre alla porta e all'indirizzo siano corretti anche la password e l'userID. Il gateway tutte queste informazioni le troverà scritte nel file .ini della quale un esempio è riportato qui di seguito:

IPZ=192.168.146.251,192.168.146.132

PM=7

HOST=192.168.146.5

USERID=delphilab

PASSWORD=mailtest

TIMEOUT=23.59.00

Nel file .ini di questo programma può essere configurata la porta sulla quale deve essere connesso (host), decisi gli indirizzi IP delle macchine che possono connettersi al server, in modo tale da restringere notevolmente gli accessi indesiderati (IPZ), ed inoltre la possibilità di decidere quando il programma deve spegnersi automaticamente.

Conclusioni finali

Il programma è stato realizzato in poco tempo ma è stato di difficile comprensione all'inizio. Sono dovuti essere affrontati difficili problemi in tutte le fasi della progettazione (all'inizio, durante e alla fine). All'inizio il problema era trovare esempi che facessero vedere bene come doveva essere e funzionare il nostro programma, durante la creazione il problema era trovare i giusti spunti e idee per poter andare avanti ma il problema più grande si è verificato alla fine del programma perché non è stato risolto il problema di come cancellare, senza neanche controllare se erano validi, tutti i messaggi con allegati e probabili portatori di virus. Inoltre c'è la mancanza di un client di posta dedicato alla spedizione di sms.

Realizzato da:

Panza Francesco
Busi Stefano
Buratti Giovanni

5 ^ BZ

Con la partecipazione di Ing. Cleto Azzani

Anno scolastico 2003/04

I.P.S.I.A. MORETTO BRESCIA

Il protocollo SMTP

(Allegato)

Per valutare il significato dei vari messaggi più o meno contraffatti che si possono ricevere per posta elettronica, occorre comprenderne il meccanismo di trasmissione. La trasmissione dei messaggi e-mail avviene usando un semplice protocollo (SMTP) che funziona come segue:

Lo scambio avviene fra un mittente (**M**) ed un server destinatario (**D**) attraverso una connessione di rete.

Normalmente l'invio del messaggio avviene in due passi:

1. Il programma di posta elettronica usato dall'utente invia il messaggio al proprio server usando il protocollo SMTP.
2. Il server trasferisce il messaggio al server del destinatario utilizzando lo stesso protocollo.

È possibile però che il programma di posta elettronica usato dall'utente effettui direttamente il collegamento con il server del destinatario senza utilizzare il proprio server (linea rossa nella figura).

In entrambi i casi la procedura per il trasferimento del messaggio, considerata dal punto di vista del server destinatario **D**, è la seguente:

1. **M**, sulla base dell'indirizzo e-mail del destinatario, identifica il server **D** ed apre una connessione.
2. **D** identifica il nodo di rete da cui proviene la connessione (cioè il suo indirizzo IP) ed accetta la connessione. Inoltre memorizza tale identificazione come parte iniziale del messaggio da ricevere.
3. **M** comunica lo *username* del destinatario.
4. **D** verifica la validità dell'indirizzo ed autorizza la trasmissione del messaggio.
5. **M** invia il messaggio e chiude la trasmissione.
6. **D** memorizza il messaggio in attesa che il reale destinatario si colleghi e ritiri il messaggio utilizzando un apposito protocollo (solitamente POP3 o IMAP).

È importante sottolineare alcuni aspetti:

- Tutto il contenuto del messaggio memorizzato, esclusa la prima parte generata da **D** (punto 2), è una semplice copia di quanto inviato da **M**. Questo include, ad esempio, tutti i campi in testa al messaggio (*From:*, *To:*, *Date:*, *Subject:*, ecc.)
- Gli unici elementi che non possono essere arbitrari (e quindi contraffatti) sono: l'indirizzo IP di **M** e lo *username* del destinatario usato al punto 3 sopra. Quest'ultimo però è quello dell'utente che effettivamente riceve il messaggio mentre l'indicazione *To: xx@yyy.zzz* contenuta nel testo è quella trasmessa da **M** e quindi può essere totalmente arbitraria.
- Il server destinatario non ha modo di sapere se il messaggio proviene da un server ben configurato e correttamente gestito, oppure da un generico PC magari controllato da un programma installato da un virus.

Per comprendere meglio il significato dei vari elementi è utile usare un'analogia con la posta ordinaria:

Posta ordinaria	Posta elettronica
Timbro dell'Ufficio Postale	Dati di identificazione di M (indirizzo IP)
Indirizzo del destinatario sulla busta	Lo <i>username</i> comunicato da M a D come parte del protocollo di comunicazione (punto 3).
Indirizzo del mittente sulla busta	Campo <i>From:</i>
Intestazione della lettera	Campo <i>To:</i>
Data	Campo <i>Date:</i>

È evidente che sia per la posta ordinaria che per quella elettronica gli unici dati affidabili sono quelle delle due prime righe della tabella, tutti gli altri possono essere del tutto arbitrari. Niente vieta, ad esempio, che il reale mittente scriva sulla busta un mittente fittizio, oppure che il destinatario citato nell'intestazione della lettera contenuta in una busta sia diverso da quello dell'indirizzo sulla busta stessa.