meshtastic_meshmonitor

E' il progetto at https://github.com/vinloren/meshtastic_meshmonitor che si prefigge lo scopo di controllare la rete Lora Meshtastic visibile dal nostro punto di osservazione attraverso un nodo Tlora d'interfaccia radio collegato alla porta seriale del computer Linux o Windows che lo ospita.

Per 'controllo' si intende visualizzazione della mappa geografica sulla quale appariranno i riferimenti ai nodi coi quali siamo in contatto, lo scambio di messaggi testuali, la tracciatura dei percorsi fatti dai nodi mobili, la gestione dell'abilitazione dei nodi ad apparire in mappa oltre ad altre funzioni di manutenzione del sistema. Il tutto gira su un server Python Flask locale con al centro un Db Sqlite3 per il salvataggio e il controllo dei dati. Il Db è l'elemento chiave che permette l'interattività all'interno della rete cui si aggiunge questa nuova funzione di ricezione via mail di testi da inviare in rete sul canale primario ch0.

meshtastic_meshcontroller

E' l'applicazione python all'interno del progetto meshtastic_meshmonitor che si occupa di controllare tutti i messaggi di protocollo e testuali ricevuti memorizzandone i contenuti sul Db Sqlite3 per caratterizzare ciascun nodo in vista con data/ora e posizione geografica oltre ad eventuali dettagli di telemetria presenti. Questa applicazione si occupa anche di gestire i messaggi testuali ricevuti fornendo risposte immediate in caso di richiesta qsl?. o anche inviare su ch0 messaggi che attraverso il server Flask abbiamo inserito nella relativa tabella per l'invio ad opera di mesh_controller.

Ricezione Mail

Sfruttando il meccanismo della trasmissione dei messaggi testuali su accennato, diventa possibile fare in modo che un utente non presente presso il proprio sistema meshmonitor sia in grado di inviare messaggi in rete come se fosse davanti alla console. Il meccanismo di trasmissione messaggi è il seguente:

1. ad ogni fine ciclo di scansione di un qualunque messaggio di protocollo da gestire, mesh_controller va a leggere in Db la tabella 'messaggi' per vedere se l'ultimo presente inizia col carattere ^ che è l'identificatore di messaggio da trasmettere.
2. la presenza di un simile messaggio può essere dovuta al fatto di averlo ricevuto da un nodo in rete che ce lo ha trasmesso oppure può essere stato invece inserito da server Flask su sollecitazione dell'operatore.
3. nel primo caso mesh_controller invia il messaggio privato del carattere ^ sul ch0 come risposta tipo pappagallo, nel secondo come messaggio intenzionalmente inviato dall'operatore. In poche parole, indifferentemente da chi ha innescato il processo, la presenza in tabella 'messaggi' di un testo che inizia con ^ provoca la sua trasmissione in rete su ch0.

Stante questa premessa diventa facile capire come si possa ottenere la trasmissione in rete di un messaggio che il sistema ha ricevuto dall'esterno via Email.

Alice_ReadMail.py

E' l'applicazione python che si occupa di ascoltare la propria casella mail ogni 5 minuti. Il provider di mail prescelto per questa applicazione è alice.mail perché è uno di quelli sui quali sono registrato e

sono riuscito a far funzionare. Altro provider su cui posso fare affidamento è gmail ma questo richiede una configurazione su Google di una password specifica (token) per accesso da programma e, sebbene l'abbia provata e fatta funzionare, è una procedura piuttosto complicata da spiegare in un documento: lascio quindi il compito a ciascuno che voglia cimentarsi nell'impresa.

Il problema che si pone è che più o meno ogni provider ha le sue specifiche regole che sono da rispettare per veder garantito accesso al mail, e ciò induce un lavoro di adattamento specifico che per alice.mail è stato eseguito. Credo perciò che la soluzione più pratica per chi volesse introdurre questa funzione in meshtastic_meshmonitor sia quella di registrare un account su alice.mail.

come funziona questa applicazione

una volta lanciata, l'applicazione viene rilanciata automaticamente ogni 5 minuti dal time scheduler incluso. Viene fatto login al mailer leggendo le credenziali dal file '.env' (senza apici) residente nella directory ./source insieme col resto dei programmi python. .env è un file di testo che contiene 2 righe:

1. EMAIL_USER='tuo_username@'alice.it'
2. EMAIL_PASS='tuapassword'

quindi vengono scandite le ultime 5 mail ricevute cercando al loro interno il Subject = /^ che identifica mail contenente testo da inviare in rete su ch0.

Se c'è un riscontro positivo l'applicazione ne preleva il testo (troncando se necessario a max 188 chars) e lo va a scrivere nel Db in tabella 'messaggi' apponendovi in testa il carattere ^ per informare mesh_controller che questo è un messaggio da inviare in rete su ch0.

L'applicazione si appoggia al log ../logs/alice_readmail.log dove trovare indicazioni sui messaggi trasmessi e su eventuali errori occorsi.

ReadMail_alice.py o ReadMail_gmail.py

Chi avesse un account google gmail può usare l'applicazione alternativa presente in ./source che funziona allo stesso modo di Alice_ReadMail.py. Il problema da superare in questo caso risiede nel fatto che differentemente da Alice mail Google gmail non permette l'uso della stessa password usata sotto Thunderbird o Outlook o Posta etc. ma richiede uno specifico token se l'accesso non è operato da questi. Per ottenere questo token, che sarà la password inserita dall'applicazione python, occorre andare sul proprio account google per generarlo. Questa cosa la feci un anno fa e il token lo sto usando senza problemi ma non ricordo più la procedura per ottenerlo; credo tuttavia che oggi questo non sia più un problema grazie a ChatGpt.

.env da configurare

Come già visto per Alice_ReadMail.py occorre aggiungere le credenziali necessarie all'accesso:

1. GMAIL_USER='iltuouser@gmail.com'
2. GMAIL_PASS='iltoken_ottenuto_su_google'

Questa applicazione funziona in modo simile all'altra ma usa imap_tools in aggiunta a imaps il che rende più snella la programmazione. La peculiarità rispetto a Alice_ReadMail.py sta nel fatto che si possono ricevere le mail non ancora lette invece che le ultime 5 e poi scandendone l'elenco trovare la

presenza o meno di mail con subj = /^. e interrompere la ricerca alla prima trovata. In questo modo potremmo anche, avendo inviato 10 messaggi con subject = /^, trovarli spediti uno alla volta ogni 5 minuti dato che ad ogni passaggio il mail/messaggio precedente non viene più presentato perchè già letto. Questo sistema può essere un sistema per inviare messaggi a ripetizione come avveniva con l'applicazione broadcast_msg_pyqt5.py sotto 'invio messaggi periodici'.

Trasmissione messaggi da ch0 a Mail (Gmail o Alice)

Può risultare utile ricevere sulla propria casella Email e sul repository ho previsto questa opzione per chi ha account gmail e ha la app password per accesso a gmail da app oppure per chi ha account Alice mail. La cosa funziona così:

1. in derectory ./source abbiamo due file: alice_mailout.py e gmail_mailout.py. Dovendo scegliere se usare gmail o alice mail per inviare messaggi di Alert al nostro account di posta, facciamo copia su mailout.py della versione scelta (cp se linux o copy se windows alice_mailout.py (o gmail_mailout.py) mailout.py).
2. ogni volta che mesh_controller intercetta un messaggio testuale contenente la parola Alert allora provvede a inviare il testo ricevuto, arricchito da indicazione del longname di chi lo ha inviato e da rssi/snr, verso il destinatario indicato nel file .env e come mittente il proprio account di posta.
3. a supporto di questa opzione è necessario aggiungere nel file .env che già conteneva le credenziali di lettura mail: MITTENTE='miomailaccount' , DESTINATARIO='miomailaccountl' di destinazione (che può coincidere col mittente), MAILOUT_PASS='password_di_accesso' ovvero token app password se usciamo su gmail.

Con questo sistema, in aggiunta alla pubblicazione su ch0 di messaggi inviati via mail, si può ottenere uno scambio di messaggi fra utenti del mesh anche non essendo presenti davanti alla propria installazione.

Alternativa a Gmail e Alice per trasmissione messaggi Alert

Oltre ad usare un nostro account di posta da Gmail o da Alice esiste un'altra possibilità, per me interessante, costituita da accesso a mailtrap.io che si prenderà cura della trasmissione del messaggio al posto del nostro account di posta personale. Questa soluzione (gratuita) è interessante perché è semplice da usare e non ci mette di fronte alla necessità di generare apposite app password spesso difficili se non impossibili da creare.

Procedura

1. installare python mailtrap con **pip install mailtrap** nel nostro ambiente virtuale
2. creare un account gratuito su https://mailtrap.io fornendo nostro numero di cellulare e nostro indirizzo di mail che sarà lo user id del login a mailtrap.io
3. l'account gratuito su mailtrap ci consente di inviare fino a 50 mail giornalieri dove il mittente figurerà come nome@demomailtrap.co verso un destinatario a nostra scelta. Per innescare mailtrap per l'invio da noi richiesto occorre ottenere un token per API mail da generare in fase di configurazione del servizio su mailtrap.io. Questo token sarà la chiave nel file .env sotto 'MAILOUT_PASS' mentre MITTENTE= 'nome@demomailtrap.co e destinatario quello che abbiamo scelto. Ad esempio, mettiamo che io mi sia loggato su mailtrap.io col logn iu2rpo@alice.it il MITTENTE che risulterà da mailtrap sarà iu2rpo@demomailtrap.co . Questo

è un vincolo imposto agli account gratuiti ma per noi non è un problema dato che i destinatari siamo noi stessi.

4. attuando questa scelta per invio messaggi Alert occorre nella directory ./source copiare il file send_mailtrap.py su mailout.py ed il gioco è fatto.

Personalmente sono passato alla soluzione mailtrap che mi pare più snella e semplice di quella su gmail o alice, per non parlare di outlook o yahoo dove la generazione della app key è problematica o addirittura non funziona più. Questi fornitori di servizi di mail si stanno ormai orientando verso l'abbandono delle app key a favore di autenticazione OAuth 2.0 per accesso a mail da applicazione python che non è semplicissima da configurare.
.

Soluzione lettura mail in meshmonitor

A parte alice mail, nessun altro fornitore di servizio permette più di accedere al mailer da applicazioni di terze parti se non usando le cosiddette app password da generare appositamente.Purtroppo anche la generazione di queste app password è diventata problematica, se non più praticabile, dato che tutti i fornitori si stanno orientando verso accesso esterno solo via OAuth 2.0.

Il consiglio che posso dare agli utenti di gmail è allora quello di configurare sul proprio account l'accesso alle API google Gmail per accedere alla propria mail da applicazione python via OAth 2.0, (in rete ci sono diversi tutorial per riuscire nell'impresa) e poi usare CallMail_api.py e ReadGmail_api.py presenti nel repository clonato sul proprio PC.

Poi essendo consapevole che tempo e conoscenza tecnica necessaria non sono patrimonio diffuso, mi è venuta in mente una soluzione che possa valere per tutti e che è consistita nella creazione da parte mia di un nuovo account gmail che ho nominato **brianzaticinonet.gmail** confgurandoci dentro l'accesso esterno via google api per gmail con autorizzazione OAuth 2.0.

Tramite il file credentials.json, token.pickle e due files python (CallMail_api.py e ReadGmail_api.py) installati nella directory ./source, chiunque abbia installato meshtastic_meshmonitor ha garantita la possibilità di inviare in rete messaggi tramite ricezione degli stessi in brianzaticinonet@gmail.com e da qui poi passati in rete su ch0. In pratica basterà inviare un messaggio con oggetto /^ alla casella mail su indicata per ottenere il risultato.

Esporre su github i file per l'accesso da api all'account brianzaticinonet@gmail.com mi pare un po' rischioso perché qualche furbastro potrebbe, anche se la password per accesso da web mail la conosco solo io, utilizzare il mio account accedendo con programma via api per finalità illecite.

A fronte di questa osservazione, i files **credentials.json e token.pickle** (chiavi di accesso api) **non li pubblico su github** ma li posso inviare a chi del gruppo Whatsapp cui siamo iscritti me lo chiederà avendo interesse in meshtastic_meshmonitor.

Procedura operativa di configurazione

1. entrati in ambiente virtuale eseguire: pip install --upgrade google-api-python-client google-auth-httplib2 google-auth-oauthlib
2. ora è possibile eseguire il lancio: python CallMail_api.py e con passo di 5 minuti verrà eseguito accesso a gmail dello user brianzaticinonet@gmail.com per vedere se ci sono messaggi da inviare in rete su ch0.