# Realizzazione del gateway privato Pennar-Ekar

**INAF - Osservatorio Astronomico di Padova**

**Danilo Selvestrel**[1]

**06/2020**

**Abstract**

Per motivi logistici la sala di controllo dei telescopi della sede osservativa di Cima Ekar dell'Osservatorio Astronomico di Padova (OAPd-Ekar), già alcuni anni fa, è stata duplicata nella sede in località "*Pennar*" vicino al centro del paese di Asiago. Da tempo le osservazioni ai telescopi si svolgono quasi esclusivamente dall'edificio principale del Dipartimento di Fisica ed Astronomia dell'Università di Padova (DFA). È emersa quindi la necessità di realizzare un network parallelo alla normale rete dati pubblica dedicato esclusivamente alla gestione remota dei telescopi. Questo rapporto tecnico ne descrive l'evoluzione temporale e le scelte tecniche.

**Introduzione**

La soluzione iniziale è stata la costruzione, da parte di personale locale dell'Università, di un ulteriore ponte radio configurando i nuovi apparati in bridging senza intervenire sul routing tra le due reti. Questa scelta si è subito rivelata inadeguata finendo per creare a livello Data Link un'unica LAN di due strutture appartenenti ad istituzioni diverse. Per ovviare al problema è stato inizialmente utilizzato un vecchio PC *dual-homed,* con una distribuzione Linux minimale e regole iptables per separare il traffico tra ponte radio privato e reti pubbliche, che si è rivelato subito di scomoda manutenzione.

**Prima versione del gateway**

La prima evoluzione del gateway era basata su una vecchia versione della distribuzione Linux chiamata "*ZeroShell*", il PC tradizionalmente è sempre stato chiamato con nome logico "*zaphod*". Per comodità è stato mantenuto lo schema con un PC *dual-homed* con la possibilità di duplicare l'interfaccia di amministrazione tra seriale (configurata 9600-8N1) e la console VGA. Tipicamente però la configurazione veniva già eseguita via web. Già alla prima versione è stato possibile mappare tutti i nodi che devono essere accessibili dagli astronomi per le osservazioni ai telescopi (i PC che gestiscono i telescopi, i videoserver per il controllo ambientale dei telescopi e delle cupole, il server che ospita il sistema meteo locale) come singoli *Virtual-IP* della LAN di DFA. In sostanza il gateway aveva una interfaccia di rete sulla LAN di OAPd-EKar e l'altra come *next-hop* in uscita dal ponte radio sempre collocato a Cima Ekar, quindi con un indirizzo appartenente alla LAN di DFA raggiunta direttamente attraverso il nuovo ponte radio. Su questa interfaccia sono stati allocati tanti indirizzi quanti sono i nodi da raggiungere sulla rete di OAPd-Ekar. Ci sono vari modi di definire questa tecnica, il più usato è NAT 1:1. Uno schema logico delle reti di Asiago si può vedere in Figura 1.

**Pregi e difetti di *ZeroShell***

Questa distribution è stata uno dei primi sistemi operativi *free* in grado di trasformare un PC in un router/firewall. Molto flessibile e facile da configurare, si è rivelata una soluzione molto stabile. È stata anche una delle prime ad integrare una comoda interfaccia web che permette di configurare vari servizi in modo intuitivo e veloce. La versione "base" comprende tutti i servizi offerti e non ha bisogno di licenze aggiuntive, funziona molto bene anche con hardware obsoleto ed è facilmente portabile. Poiché gira su qualsiasi PC, una delle caratteristiche più gradite è la facilità con cui è possibile duplicare il gateway per avere offline un PC di backup con configurazione identica per qualsiasi evenienza. Naturalmente questi vantaggi possono essere anche una limitazione: lo sviluppo del sistema operativo è limitato, nuove versioni vengono rilasciate solo se vengono individuati gravi bug nel software di base; inoltre esistono al momento altre soluzioni che val la pena esplorare. Nell'ottica di tenere sotto controllo il consumo energetico usufruire di PC può essere dispendioso a pari prestazioni rispetto a soluzioni alternative.

1 danilo.selvestrel@inaf.it

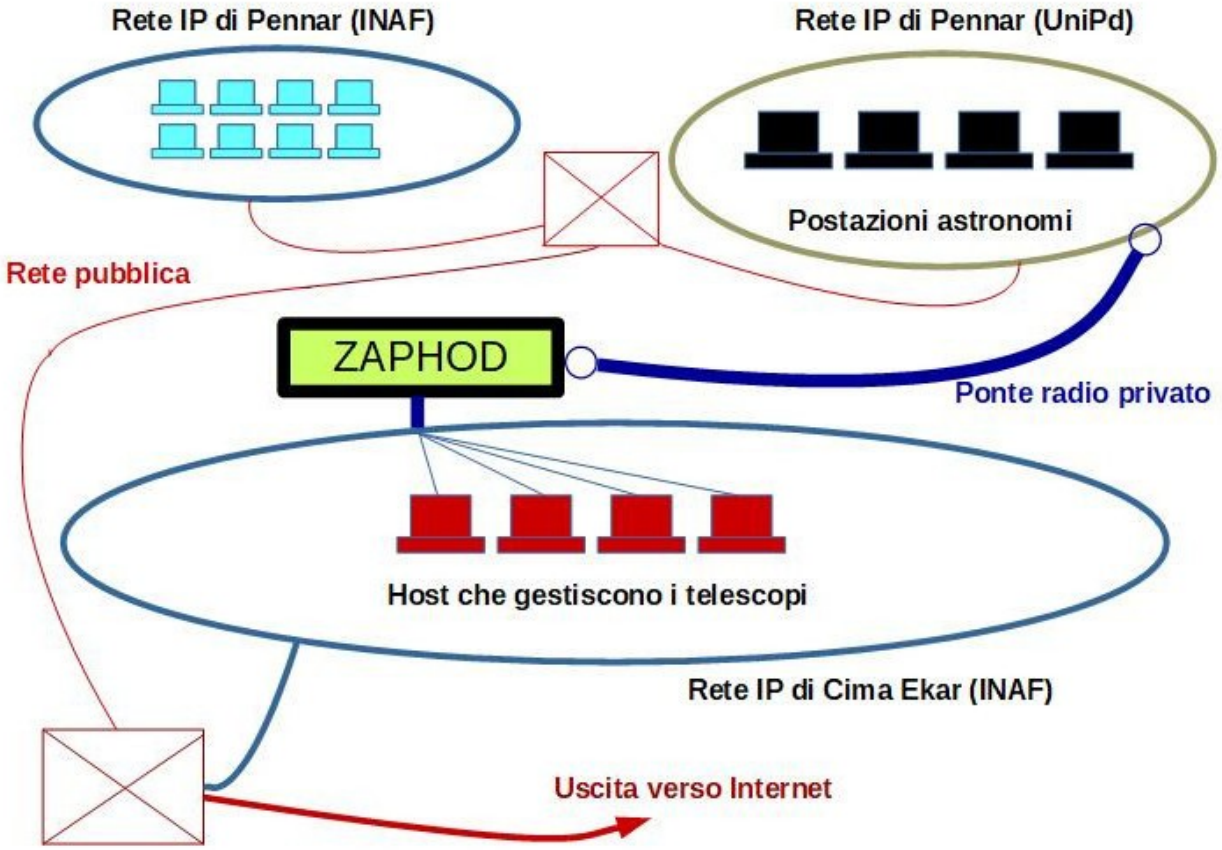


Figura 1 – Schema di base delle reti di Asiago

**Ricerca di soluzioni alternative**

Alternative di qualità senza dubbio non mancano. Rimanendo su piattaforme x86 sono stati testati sia "*pfSense*" che "*OPNsense*", due ottime soluzioni basate su FreeBSD. Entrambi molto completi e continuamente aggiornati, nella maggior parte dei casi si rivelano soluzioni perfino migliori di *ZeroShell*. Con la sola eccezione del nostro caso. Dai test effettuati emerge che entrambi i sistemi si comportano allo stesso modo: prevedono il NAT 1:1 e lo effettuano molto bene se il gateway di cui abbiamo bisogno fosse il defaultrouter per tutta la LAN ma nel nostro caso non è così. Il defaultrouter per tutte le reti coinvolte instrada i pacchetti verso la rete pubblica. Solo i pacchetti destinati ai *VIP* devono essere nattati per transitare lungo il ponte radio privato. Ma quando l'header dei pacchetti viene riscritto dal gateway, viene mantenuto l'indirizzo sorgente del nodo che lo ha generato cambiando correttamente l'indirizzo del destinatario; ma quest'ultimo si trova a rispondere ad un nodo che si raggiunge tramite il defaultrouter, pertanto attraverso la rete pubblica e con indirizzo sorgente non quello del VIP ma il vero indirizzo pubblico. Sostanzialmente questo comportamento è un *IP Spoofing* e quindi il nodo che ha iniziato la connessione rifiuta tutti i pacchetti di ritorno. Sembrerebbe una feature di tutti i sistemi operativi derivati da BSD per una discutibile gestione delle tabelle del NAT. A questo punto sono stati valutati altri due sistemi operativi entrambi derivati da Linux, che hanno l'indubbio vantaggio di essere portati a più architetture supportando hardware parecchio interessante. Si tratta di "*OpenWrt*" e "*DD-WRT*". Entrambi possono esser facilmente testati su un normale PC ma sono portabili a varie altre architetture. Nella loro versione base non includono tutte le *feature* che offre una nuova installazione di *ZeroShell* ma sono comodamente integrabili con una lunga serie di pacchetti aggiuntivi. Pur essendo nati leggermente prima di *ZeroShell* all'apparenza sembrano meno maturi e più ostici da configurare pur se l'interfaccia web è più accattivante. Sono ambedue perfettamente in grado

di fare il lavoro che ci serve, i test eseguiti hanno dato buoni risultati.

**Estensione delle necessità tecniche**

Il trasferimento della gestione dei telescopi alla controlroom nella sede del "*Pennar*" ha dato vita all'opportunità di utilizzare i telescopi anche all'esterno delle sedi canoniche di Asiago, rispondendo all'esigenza di osservare dalle sedi di Padova e, più in generale, da qualsiasi posizione disponga di capacità banda sufficiente (si pensi a dimostrazioni per il pubblico). Per far accedere gli astronomi in sicurezza ai nodi che controllano i telescopi da fuori delle strutture canoniche è stata attivata la VPN di *ZeroShell* del tipo Host-to-LAN. L'implementazione della VPN è la classica OpenVPN il cui client è liberamente disponibile per Linux, Windows, e MacOSX. Dopo i normali test del caso è stato possibile autenticare gli utenti sia su DB locale (per le persone non di staff dell'Osservatorio), sia sul Domain Controller di struttura (per l'utenza interna INAF-OAPd). L'integrazione di questo servizio ha interrotto la ricerca di soluzioni alternative dato l'alto grado di affidabilità raggiunto dal sistema, rivelandosi *ZeroShell* la migliore scelta possibile. Sono stati condotti alcuni test sulla configurazione di una VPN LAN-to-LAN con ottimi risultati.

**Dettagli della configurazione finale**

La configurazione attuale di *zaphod* è un datato PC dual-core con a bordo *ZeroShell* versione 3.9.3 con due schede di rete Gb, 4GB RAM e disco SSD da 120GB. L'hardware si è rivelato più che sufficiente a sostenere il modesto carico di lavoro di cui il servizio necessita. L'interfaccia marcata ETH00 è collegata direttamente con un indirizzo pubblico alla LAN OAPd-Ekar, l'interfaccia ETH01 è un bridge cui sono assegnati tutti gli indirizzi nattati dei Virtual-IP (pubblici, della rete di DFA) collegata a valle dell'apparato del ponte radio privato installato sul ballatorio del telescopio Copernico. Qui sotto viene riportata la tabella degli indirizzi attualmente tradotti dal gateway.

| **Nome logico del nodo** | **Funzione** |
|---|---|
| strumenti-sch | PC gestore della strumentazione telescopio Schmidt |
| puntamento-sch | PC gestore del puntamento telescopio Schmidt |
| puntamento-t182 | Ex-PC gestore della puntamento telescopio Copernico (inutilizzato) |
| kvm-ekar | Console per botom1 e botom2 |
| meteo-ekar | (stug) alias servizio meteo MTX e database server |
| hactar | Collettore dati/immagini e mirror locale IA2-AAO |
| vs-schmidt | Videoserver per telecamere interne cupola Schmidt |
| vs-copernico | Videoserver per telecamere interne cupola Copernico |
| vs-sud | Videoserver per telecamere interne cupola Schmidt che vede Copernico |
| vs-nord | Videoserver per telecamere interne cupola Copernico che vede Schmidt |
| copernico | Attuale PC di controllo del telescopio Copernico |
| schmidt | Nuovo PC di controllo del telescopio Schmidt |
| halfrunt | Nodo dedicato esclusivamente ai backup |

Per il collegamento punto-punto il secondo apparato è situato vicino alla cupola del telescopio Galileo nella sede DFA del "*Pennar*". Entrambi sono di proprietà di DFA e appartengono alla rete DFA, di recente sono stati sostituiti con apparati nuovi Mikrotik RouterBOARD DynaDish G-5HacD r3

garantendo alla rete prestazioni nettamente superiori. Esiste una interfaccia virtuale che pilota la VPN il cui software assegna indirizzi IP privati nattati, se l'autenticazione dell'utente va a buon fine, dalla stessa interfaccia. Un utente collegato alla VPN acquisisce alcune *route* statiche per la rete di DFA, per la rete al "*Pennar*" dell'Osservatorio e per la rete di OAPd-Ekar in modo da poter raggiungere direttamente tutti i nodi che controllano i telescopi delle due sedi. Nella nostra configurazione non vi è alcuna necessità di utilizzare le altre caratteristiche di *ZeroShell* quali il Captive Portal, l'HTTP Proxy (che fra l'altro non supporta HTTPS) e il Net-Balancer. Una particolarità rilevante è la possibilità di tenere varie versioni della configurazione la cui gestione è molto pratica.

**Conclusioni**

Pur basandosi su una architettura obsoleta e su un sistema operativo scarsamente aggiornato la scelta di rimanere su base *Zeroshell* si è rivelata opportuna in rapporto al servizio che doveva essere garantito in una sede scomoda e senza supporto informatico. La limitatezza di aggiornamenti software viene compensata dalla semplicità di gestione e dall'affidabilità della soluzione attuata. Il confronto con altre soluzioni è sempre stato fatto tenendo ben presente la peculiarità del servizio richiesto rispetto ad altre sistemi quali *ClearOS* o *Untangle*, anche queste distribuzioni Linux ma più adatte a servire piccoli uffici piuttosto che a gestire sostanzialmente una linea punto-punto.