Archeologia di un ISP: come funzionava davvero un Internet provider nel 1995

Stratigrafia di un'infrastruttura: ricostruire un ISP del 1995 grazie alla digital forensics

di Marco Iannacone ianna@pippo.com – articolo originariamente pubblicato su Codemotion in ottobre 2026

Qualche tempo fa stavo cercando del vecchio materiale per rispondere a una domanda di un amico quando mi sono imbattuto in alcune directory su un NAS che non aprivo da quasi trent'anni. Erano i backup e la documentazione che avevo creato per Internet Force, l'Internet Service Provider di cui ero system e network administrator nel 1995.

Dentro c'erano configurazioni dei router Cisco, zone BIND, file di Sendmail, configurazioni XTACACS, script, mappe SNMP create con tkined, file /etc/hosts e /etc/networks, configurazioni di routing, documentazione operativa e perfino gli inventari di hardware, dischi e filesystem delle macchine Sun. Alcuni backup erano corrotti ed altri file erano mancanti, probabilmente si erano persi nelle numerose migrazioni di computer che li hanno visti coinvolti. Ricordavano un po' le vestigia di una gloriosa civiltà del passato e come per i templi, guardando anche solo le colonne si capiva cosa dovevano essere stati.

Nel rispondere alle domande del mio amico mi sono accorto di due cose. La prima è che quel materiale suscita ancora una curiosità quasi irrazionale in una certa categoria di persone che, per semplicità, chiameremo geek. La seconda è che oggi è sorprendentemente difficile trovare una descrizione completa di **come fosse costruito e funzionasse realmente un piccolo Internet Service Provider commerciale della metà degli anni Novanta**.

Ho cominciato a seguire le tracce dei dati ritrovati. Un indirizzo IP in un file rimandava a un host in un altro; una route spiegava il percorso verso un POP; una regola di FireWall-1 chiariva perché un servizio fosse raggiungibile da una rete ma non da un'altra. Alcuni documenti fotografavano momenti diversi e apparentemente si contraddicevano. A quel punto la somiglianza con un lavoro archeologico ha smesso di essere soltanto una metafora simpatica: dagli artefatti si poteva ricostruire non solo quali macchine esistessero, ma come funzionasse davvero l'organismo nel suo insieme.

Ho quindi deciso di ricostruire quella storia confrontando i materiali originali, la mia memoria e, dove serviva, una assistenza mirata della IA per ricostruire parti mancanti o file corrotti.

Il problema era che non avevo un unico backup coerente, congelato in un preciso giorno del 1995 (o del 96). I backup regolari di un tempo non li avevo conservati. C'erano invece strati diversi: copie sopravvissute a numerose migrazioni di computer, configurazioni aggiornate in momenti successivi (e che mi erano servite negli anni come base per attività varie di consulenza), file incompleti e documenti che fotografavano fasi differenti dell'infrastruttura. A volte due reperti sembravano contraddirsi semplicemente perché appartenevano a mesi diversi.

Ad un certo punto mi è venuto in mente che mi era "rimasta" una copia di un backup su nastro della mia workstation. La cassetta DAT era sopravvissuta per quasi trent'anni in un contenitore in cantina. Il backup originale era stato scritto con un lettore DAT Sun collegato via SCSI a DVLP, una macchina SunOS; per provare a recuperarlo ho invece noleggiato un lettore DAT USB e l'ho collegato a una macchina Linux.

Da lì è iniziata la parte più vicina alla digital forensics vera e propria. Ho usato tar per cercare di estrarre il contenuto e, quando sembrava esserci compressione, gzip per capire cosa fosse ancora leggibile. Il risultato

non era affatto un archivio ordinato: alcuni file uscivano normalmente, altri avevano dimensione zero, altri ancora sembravano archivi .tar.Z ma non si aprivano più. In diversi casi ottenevo semplicemente blob con nomi illeggibili o contenuti parzialmente corrotti.



Immagine dedicata all'articolo ed ispirata ad un famoso gioco uscito nel periodo di cui l'articolo parla

A quel punto il recupero diventava un lavoro per indizi. Guardavo header, stringhe leggibili, dimensioni, nomi vicini nell'archivio e confrontavo ciò che emergeva con configurazioni già recuperate altrove. In alcuni casi ho usato anche DeepSeek tramite OpenCode per provare a interpretare i blob danneggiati e riconoscere strutture plausibili: non per "inventare" il file mancante, ma per capire se dentro quei frammenti fosse ancora riconoscibile una configurazione, uno script o un archivio compresso.

Anche quando un file si apriva correttamente, però, restava da capire quando fotografasse l'infrastruttura. Una configurazione Cisco poteva sembrare quella del lancio e contenere invece rotte verso POP aggiunti soltanto nel 1996. Una mappa tkined poteva rappresentare una fase precedente; un file DNS, una tabella di routing o una policy del firewall permettevano di collocarla meglio nel tempo. La ricostruzione è diventata quindi soprattutto un lavoro di stratigrafia: non chiedersi soltanto "questo file è autentico?", ma "a quale momento della rete appartiene?".

Anche la mia memoria faceva parte delle fonti, ma non era il metro con cui costringere i file a confermare quello che ricordavo. Quando memoria e reperti non coincidevano, cercavo un terzo elemento: una configurazione, una mail, una data, una mappa, un documento operativo. In alcuni casi ho dovuto correggere

ricordi che dopo trent'anni avevano finito per sovrapporre momenti diversi della storia della rete. In altri erano proprio i file a restituire dettagli che avevo completamente dimenticato.

Nel repository ho cercato di conservare anche questa distinzione temporale: quando una configurazione appartiene chiaramente alla fase iniziale, quando è una revisione successiva e quando invece un passaggio è stato ricostruito a posteriori incrociando più fonti. L'articolo può quindi seguire la storia; chi vuole verificare come ci sono arrivato può scendere fino ai singoli reperti.

Da ciò è nato questo articolo e un repository GitHub che ne conserva tutti i dettagli tecnici. Qui su Codemotion non voglio fare un catalogo di configurazioni: voglio raccontare i processi. Cosa accadeva quando un cliente di Milano o di un POP remoto componeva il numero del provider? Come veniva autenticato? Come raggiungeva Internet? Dove finiva la sua posta? Come si costruiva e pubblicava un sito Web? E come lavorava, dietro a tutto questo, un piccolo ufficio pieno di Sun, Cisco, Macintosh, un PC Linux e, a un certo punto, perfino Windows NT con Oracle?

Il repository serve a chi vuole scendere di un livello e vedere i reperti: configurazioni Cisco, file Unix, policy, documentazione e ricostruzioni tecniche. L'articolo prova invece a rimettere quei reperti in movimento.

Il percorso parte dal recupero di quei reperti e dal contesto tecnico in cui erano nati, entra poi nell'architettura di Internet Force e segue una connessione dial-up dal modem fino a Internet; alla fine torneremo ai materiali meno infrastrutturali riemersi dai backup e a ciò che sopravvisse alla società.

La storia seguirà questo percorso:

Recuperare un ISP trent'anni dopo → il contesto di Internet nel 1995 → come nacque l'architettura di Internet Force → sicurezza e servizi → seguire una connessione dal modem a Internet → l'ufficio e il lavoro quotidiano → il repository e gli altri materiali recuperati → cosa accadde dopo la chiusura.

Dal modem alla fibra: cambiano le tecnologie, non le domande

Prima di entrare nei dettagli di Internet Force vale la pena fermarsi un momento su una differenza fondamentale fra allora e oggi. Nel 1995 collegarsi a Internet era un'azione esplicita: il computer chiamava telefonicamente il provider, i due modem negoziavano la connessione e soltanto a quel punto iniziava una sessione di rete. Oggi, con una connessione fissa, diamo invece per scontato che Internet sia sempre presente. Sotto questa differenza enorme, però, il provider deve ancora risolvere problemi sorprendentemente simili. Di seguito una sintesi delle principali differenze

TL;DR:

ISP metà anni '90 = accesso punto-punto su doppino telefonico: modem, terminal server/access server, autenticazione su DB centrale, poi IP.

ISP FTTH oggi = accesso punto-multipunto su fibra passiva: ONT, PON con splitter passivi, OLT, BNG, AAA/RADIUS, backbone, peering/transit.

Confronto di dettaglio

Aspetto	Dial-up anni '90	FTTH oggi
Mezzo fisico	Linea telefonica, modem 28,8 kbit/s, chiamata	Fibra ottica, ONT (Optical Network Terminal, terminale di rete ottica) a casa
Concentrazione	Modem pool → terminal/access server	Splitter passivi → OLT (Optical Line Terminal, terminale di linea ottica)
Sessione/autenticazione	Terminal server interroga DB centrale utenti	BNG (Broadband Network Gateway, gateway di rete a banda larga) + AAA/RADIUS: identifica, autorizza, accounting
IP	Assegnato dopo riconoscimento abbonato	BNG gestisce connettività IP e profili servizio
Uscita Internet	Router provider → Internet	Backbone → peering/IXP o transit
Filosofia	Point-to-point, apparati eterogenei	PON (Passive Optical Network, rete ottica passiva), controllo centralizzato software/policy

Differenza sostanziale: prima il collo di bottiglia era modem + linea telefonica; oggi la parte ottica è passiva e condivisa, mentre intelligenza e controllo stanno in OLT/BNG/AAA.

L'altra differenza evidente è che non si "chiama" più Internet. La connessione è permanente, condivisa e a commutazione di pacchetto fin dalla rete di accesso. Ma l'idea generale rimane la stessa: accesso → identificazione dell'abbonato → assegnazione della connettività IP → aggregazione → backbone → Internet.

È proprio questa continuità funzionale, nascosta sotto tecnologie completamente diverse, a rendere interessante questa archeologia di un ISP.

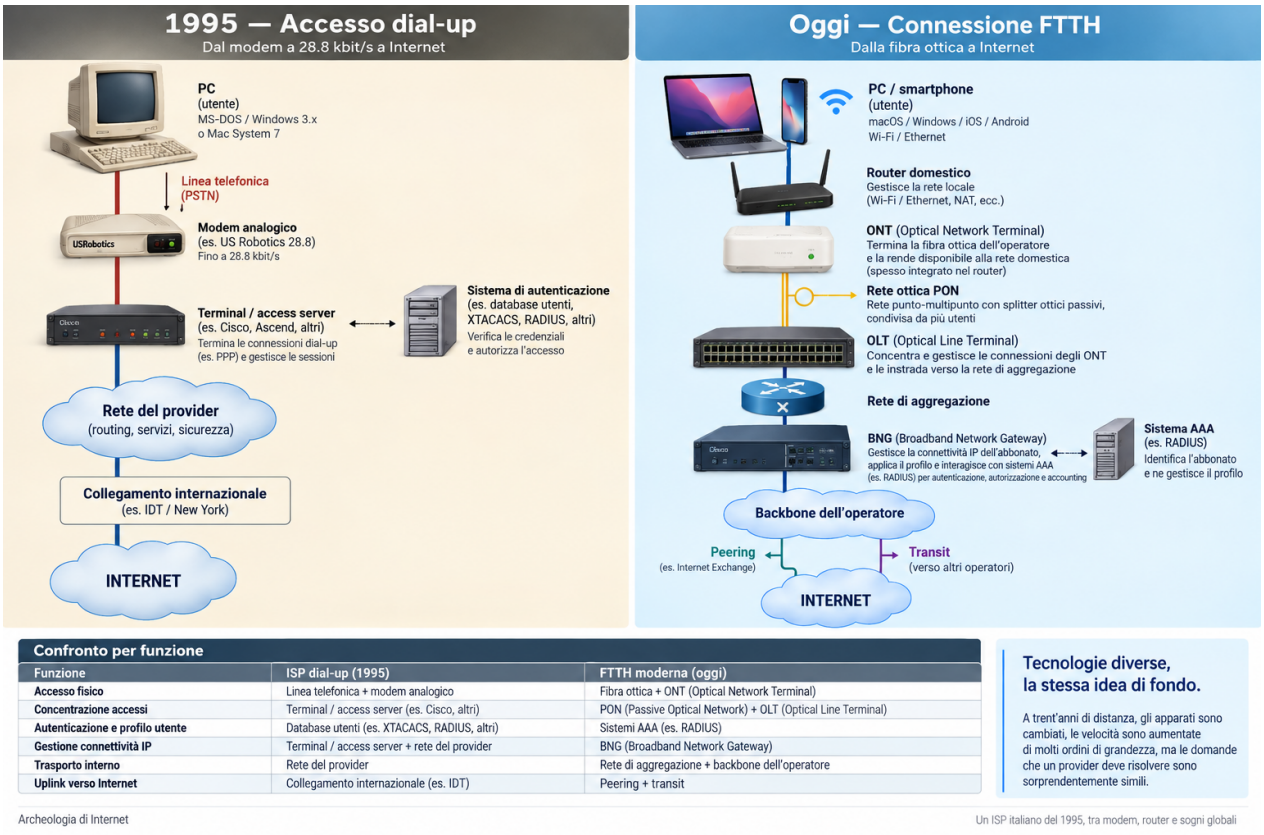


Figura 1 — Due modi di fornire accesso a Internet: dial-up nel 1995 e una tipica architettura FTTH contemporanea. Gli apparati cambiano, le funzioni fondamentali restano riconoscibili.

Un Internet molto più piccolo

Per capire davvero, bisogna prima tornare mentalmente al 1995. Nel 1994 l'ITU stimava circa **20 milioni di utenti Internet nel mondo**, appena lo 0,3% della popolazione. Amazon avrebbe aperto il proprio bookstore sul Web nel luglio 1995; nell'ottobre dello stesso anno annunciava di ricevere già ordini da 45 paesi.

Proprio nell'autunno del 1995 (ho trovato una ricevuta!) anch'io ordinavo da Amazon manuali e testi informatici in inglese, difficili da trovare in Italia, facendomeli spedire in ufficio. La documentazione sul funzionamento dei servizi Internet era così recente ed evolveva così in fretta che la si trovava solo online.

Internet commerciale esisteva, il Web stava accelerando, ma per la maggior parte delle persone in Italia collegarsi significava ancora trasformare una linea telefonica in una connessione dati per qualche ora sottraendola spesso al resto della famiglia.

Usenet: imparare e restituire alla rete

Un'altra grande scuola era Usenet. Nei newsgroup tecnici si potevano incontrare persone estremamente competenti e chiedere aiuto, ma l'etichetta era piuttosto chiara: prima si cercavano le FAQ, si leggeva la documentazione e si provava a capire il problema; poi si faceva una domanda riportando sistema, versione, configurazione, messaggio di errore e tentativi già effettuati.

Da quella cultura nasceva anche il celebre RTFM, "Read The Fucking Manual": una risposta oggi poco diplomatica, ma allora perfettamente comprensibile nel contesto. Non significava semplicemente "arrangiati"; implicava che prima di chiedere aiuto ci si aspettasse almeno il tentativo di leggere il manuale, le FAQ e la documentazione disponibile. La comunità condivideva moltissima conoscenza, ma chiedeva in cambio un minimo di lavoro preliminare.

La presunzione che tutti siano a propria disposizione non rappresentava ancora una conquista dell'umanità.

Usenet non era un sito né apparteneva a una piattaforma. Era un sistema distribuito di gruppi di discussione organizzati per argomento: i messaggi pubblicati in un newsgroup venivano propagati fra i news server che partecipavano alla rete. Per chi lavorava con Unix e Internet era insieme luogo di discussione, supporto tecnico, archivio di esperienza e punto d'incontro con persone che stavano risolvendo gli stessi problemi dall'altra parte del mondo. Usenet esiste ancora tecnicamente, ma quel ruolo centrale nella cultura della rete è in gran parte scomparso.

C'era anche un principio di reciprocità che oggi mi sembra importante ricordare. Per lavoro crescevo continuamente attingendo a documentazione, FAQ, mailing list, sorgenti e discussioni che altri avevano messo a disposizione. Quando potevo, cercavo quindi di restituire alla rete una parte di quella conoscenza. In quegli anni diventai autore della FAQ di it.comp.linux e pubblicai in it.faq documenti sulle emoticon, sul cyberspazio e sul gergo hacker, oltre ad altro materiale tecnico e culturale. Ho ritrovato diversi di quei post originali, completi degli header con cui circolavano su Usenet, e li ho salvati nel repository insieme agli altri reperti.

Per questo ho deciso di creare nel repository, oltre alle configurazioni delle macchine, una piccola sezione dedicata a Usenet, che raccoglie i documenti che pubblicavo allora mantenendone le date originali; una selezione curata delle mailbox permette invece di conservare qualche frammento della vita quotidiana della rete. Più avanti tornerò su questi materiali e su alcune altre cose riemerse dagli stessi backup, perché raccontano aspetti della cultura tecnica dell'epoca che le sole configurazioni non possono mostrare. I messaggi di terzi sono pubblicati solo quando appropriato e, dove necessario, sanitizzati: l'archeologia digitale non vuole risvegliare miei contatti dormienti da più di trent'anni.

Come si diventa system administrator senza essere ancora un system administrator

C'è un antefatto che vale la pena raccontare, soprattutto perché evita una possibile interpretazione sbagliata di ciò che segue. Quando i soci di Internet Force pubblicarono l'annuncio per cercare il system administrator del provider che stavano costruendo, facevo già consulenze informatiche da qualche anno, assemblavo PC all'occorrenza, programmavo da autodidatta, avevo inoltre lavorato in un centro elaborazione dati della Marina in cui avevo potuto imparare parecchio, avevo iniziato a realizzare pagine Web per piccoli provider milanesi (HTML) e collaboravo con alcune riviste di informatica scrivendo articoli tecnici.

Unix, però, lo avevo approcciato solo da utente ai tempi dell'università.

Mi candidai comunque. Studiai manuali la sera, imparando abbastanza Unix da sostenere il colloquio e riuscii a convincere i soci, che tecnicamente ne sapevano meno di me. In termini meno eleganti: avevo bluffato piuttosto bene.

Il problema arrivò quando entrarono in scena i consulenti israeliani di Xpert UNIX Systems, ai quali era stata affidata la progettazione tecnica dell'ISP. A loro bastarono pochi giorni per capire quale fosse realmente il mio livello. Mesi dopo mi dissero che avevano però apprezzato la determinazione e la velocità con cui imparavo e per questo decisero di formarmi.

In particolare mi affiancarono il mitico Yahel Ben-David, che fecero arrivare appositamente da Israele e che divenne di fatto il mio tutor. Il metodo era molto diverso dal consegnarmi configurazioni già pronte da copiare: mi coinvolgeva nella progettazione, mi chiedeva quale soluzione avrei adottato e perché. Quando sbagliavo, spesso mi lasciava procedere abbastanza da farmi capire dove fosse il problema e poi mi faceva rifare il percorso. Era praticamente un approccio maieutico: trascorrevamo tutto il giorno insieme dalle 8 alle 23 in modo che potessi arrivare alla data del lancio adeguatamente preparato e in grado di gestire il provider. Inutile dire che divenimmo presto amici.

Furono sempre loro a farmi conoscere Linux e convinsero i soci a dotarmi di una workstation 486DX piuttosto potente, con 16 MB di RAM con controller (Adaptec AHA2940) e dischi SCSI (cosa rara ai tempi su PC), perché potessi sperimentare autonomamente. Mentre in Italia aspettavamo l'arrivo di una macchina Sun mancante e l'attivazione del collegamento internazionale, trascorsi circa sei mesi a Tel Aviv continuando quella formazione direttamente alla fonte.

Quando Internet Force iniziò a operare nel 1995, quindi, non stavo semplicemente amministrando una rete progettata da altri: avevo partecipato alla sua stessa costruzione imparando a comprenderne le scelte e a ricostruirla da zero in caso di bisogno.

Un ISP pensato come una rete, non come una BBS evoluta

Nel 1995 la parola provider poteva indicare realtà tecnicamente molto diverse. Molti piccoli operatori italiani provenivano direttamente dal mondo delle BBS e di FidoNet. Li conobbi bene anche negli anni successivi, quando lavorai come consulente alla trasformazione di alcuni ISP milanesi: PC commodity, batterie di modem aggiunte progressivamente, cablaggi e servizi cresciuti intorno ad un paio di PC e, quando andava bene, un collegamento permanente da 64 kbit/s verso un carrier nazionale.



ricostruzione di un piccolo provider/BBS italiano dell'epoca, prima di un mio intervento di refactoring nel '97.

Internet Force era stato concepito in modo diverso fin dall'inizio. I soci si erano rivolti alla statunitense IDT, che li aveva messi in contatto con Xpert UNIX Systems. Il modello era vicino a quello degli ISP statunitensi dell'epoca: sistemi Unix dedicati, router e access server Cisco, POP distribuiti, autenticazione centralizzata, separazione dei ruoli tra le macchine e sicurezza considerata parte dell'architettura.

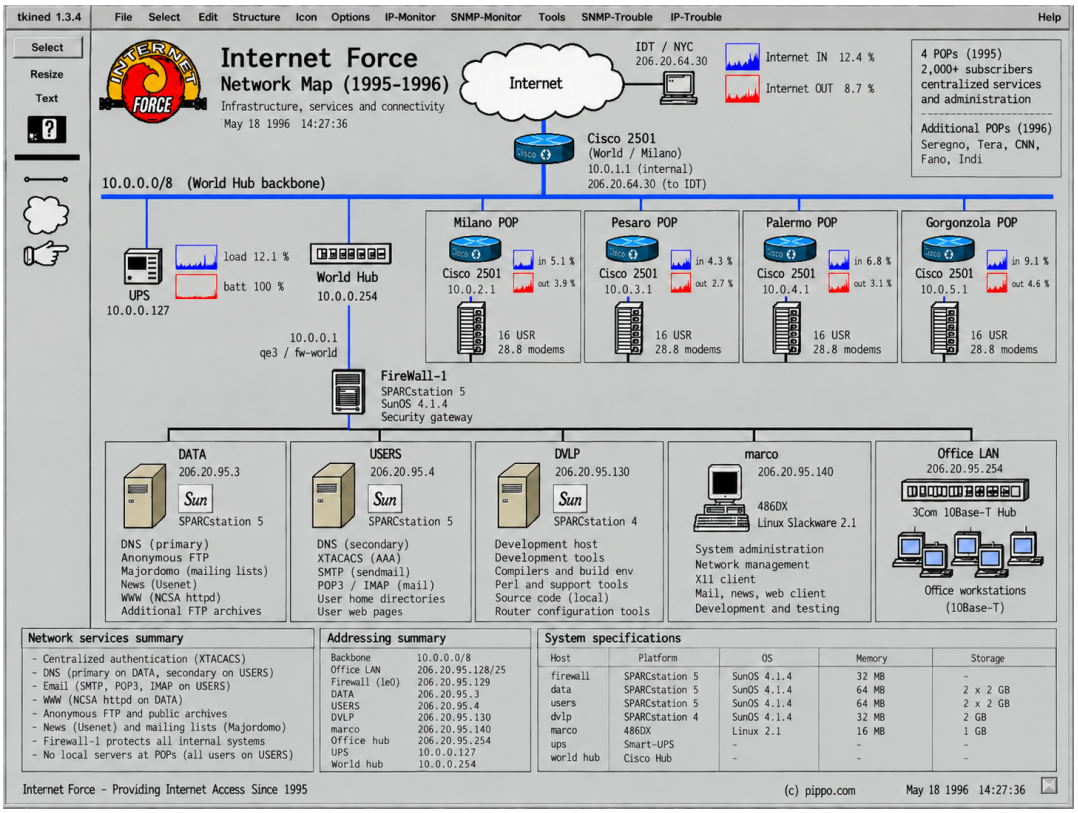
Il collegamento internazionale partì a 128 kbit/s e, dopo circa sei mesi, venne portato a 2 Mbit/s verso IDT negli Stati Uniti.

Anche la scala era ormai significativa. Nella fase di espansione del 1996, considerando i nuovi POP, l'aumento delle linee a Milano e il rapporto fra abbonati e modem utilizzato per dimensionare il servizio, Internet Force aveva raggiunto circa 2.000 abbonati. In un ISP dial-up il numero importante non era soltanto quanti clienti avevi, ma quanti potevano collegarsi contemporaneamente: vendere accesso a migliaia di persone significava dimensionare modem, linee telefoniche e collegamenti geografici sulla probabilità che solo una parte di loro fosse online nello stesso momento.

Quel numero diventa più comprensibile guardando il dimensionamento delle linee. Con la regola empirica di 8-16 abbonati per modem, ogni gruppo di sedici modem rappresentava una capacità commerciale nell'ordine di 128-256 clienti. Aggiungendo i nuovi POP del 1996 e l'espansione delle linee su Milano, si arrivava quindi a servire qualche migliaio di abbonati senza dover avere qualche migliaio di modem.

Per dare un ordine di grandezza, nel 1995 Video On Line, allora il maggiore provider nazionale, contava circa 15.000 abbonati, pari a circa il 30% del mercato italiano. Internet Force rimaneva quindi un operatore molto più piccolo, ma duemila abbonati erano già una dimensione tutt'altro che amatoriale.

Due megabit oggi sono meno della banda che una pagina Web moderna riesce a sprecare prima ancora di mostrare il titolo; per un piccolo ISP italiano del 1995 erano invece una capacità importante.



Internet Force Network Map: vista complessiva dell'infrastruttura, ricostruita a partire dalla mappa tkined originale e dagli artefatti conservati.

Internet si assemblava

C'è un aspetto dell'Internet di quegli anni che oggi rischia di essere poco evidente: la rete non era aperta soltanto nei protocolli. Le specifiche erano pubblicate nelle RFC e una parte importante del software necessario a costruire i servizi Internet circolava in sorgente, poteva essere compilata sulle diverse piattaforme Unix e veniva sviluppata da università, gruppi di ricerca e comunità distribuite.

BIND implementava il DNS; Sendmail gestiva SMTP; daemon distinti offrivano FTP, POP e IMAP; altri software gestivano Usenet, mailing list e IRC. Sul Web, nel 1996, NCSA HTTPd avrebbe ceduto il passo al neonato progetto Apache. Non tutto ciò che usavamo corrisponderebbe automaticamente alla definizione moderna di "open source", termine che sarebbe arrivato solo nel 1998, ma la cultura tecnica era fondata su standard pubblici, interoperabilità e una disponibilità del codice che rendeva possibile capire, adattare e integrare i componenti.

Per amministrare un ISP non si acquistava quindi necessariamente una suite che fornisse "Internet". Internet si assemblava. Si prendevano protocolli definiti pubblicamente, implementazioni disponibili in sorgente, daemon differenti, li si compilava sulla propria piattaforma Unix, li si configurava e li si faceva interoperare.

Era esattamente ciò che avevamo fatto in Internet Force. DNS, posta, Web, autenticazione, FTP, News e mailing list erano servizi distinti, costruiti attorno a programmi diversi che il system administrator doveva conoscere abbastanza da poterli integrare. È anche il motivo per cui, trent'anni dopo, pubblicare le configurazioni nel repository mi sembra coerente con la cultura da cui quella rete era nata: il modo migliore per capire un sistema è poterlo ispezionare.

Unix al centro

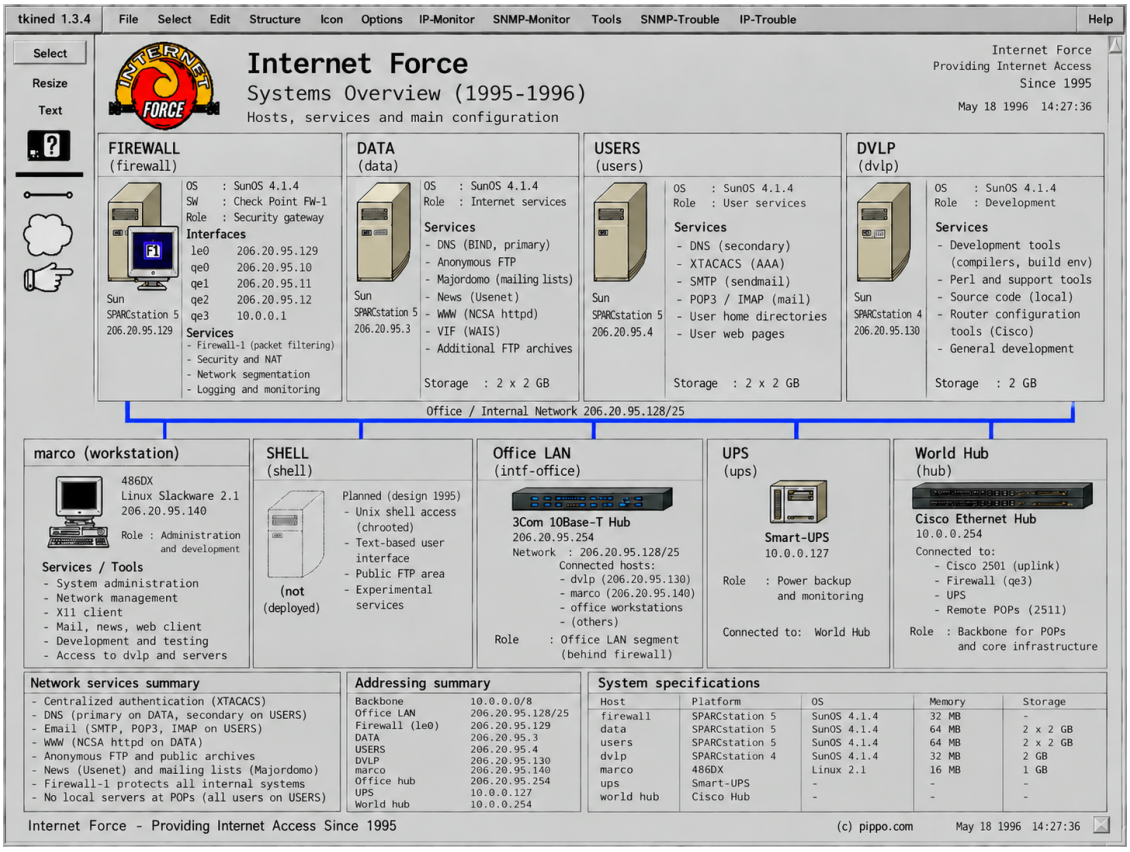
Il cuore dell'ISP era costituito da sistemi Sun con SunOS. La scelta di SunOS invece del più recente Solaris rifletteva la valutazione dei consulenti di Xpert: per un'infrastruttura che doveva essere esposta a Internet preferivano in quel momento una piattaforma che consideravano più matura e conosciuta.

Le macchine avevano ruoli distinti. DATA ospitava il Web pubblico, il DNS primario, FTP anonimo, mailing list e, in diverse fasi, servizi legati a Usenet. USERS concentrava identità e servizi degli utenti: autenticazione XTACACS, posta, home directory, POP3 e IMAP, oltre al DNS secondario. DVLP era la macchina di sviluppo e build. La mia workstation Linux, "marco", era invece il posto da cui amministravo e monitoravo l'infrastruttura.

Anche i nomi delle macchine raccontavano qualcosa dell'azienda, sebbene in questo caso non esattamente quello che avrei voluto raccontassero. Nel mondo Unix era prassi abbastanza consolidata scegliere per gli host nomi appartenenti a uno stesso universo: personaggi mitologici, astronomia, letteratura o fantascienza. La mia prima proposta fu il Signore degli Anelli; come seconda scelta avevo l'Olimpo greco e, in terza posizione, Star Wars.

I soci di Internet Force considerarono l'idea troppo giocosa per un'azienda e optarono per una nomenclatura decisamente più sobria: i server presero il nome della loro funzione, "data", "users", "dvlp", mentre alle workstation vennero assegnati nomi legati ai loro utilizzatori. A trent'anni di distanza, da hacker nell'accezione originaria del Tech Model Railroad Club del MIT, tengo a mettere formalmente agli atti il mio dissenso. Avevamo la possibilità di chiamare un server "gandalf" e scegliemmo "users".

Una piccola rivincita arrivò l'anno successivo. Quando installai il sistema Windows NT destinato agli esperimenti con Oracle, gli assegnai personalmente l'hostname "oracolo". Questa volta, prudentemente, non convocai alcun comitato per la scelta del nome.



Systems Overview: DATA, USERS, DVLP, firewall, workstation di amministrazione e Office LAN.

La filosofia di base per sistemi pubblicamente esposti era ridurre il più possibile ciò che esisteva sui sistemi di produzione. Compilatori, strumenti di sviluppo e software non necessario al ruolo del server stavano solo su DVLP; i server esposti venivano installati e sottoposti a hardening lasciando solo ciò che serviva. Si compilava su DVLP e si trasferivano gli eseguibili sulle macchine operative. Nel 1995 usavamo anche FTP interno per questi trasferimenti; non molto dopo il modo di lavorare evolse con l'introduzione di strumenti più sicuri (ssh e scp).

La sicurezza come architettura

Un'altra scelta significativa era Check Point FireWall-1, installato su una Sun SPARCstation 5 con SunOS 4.1.4.

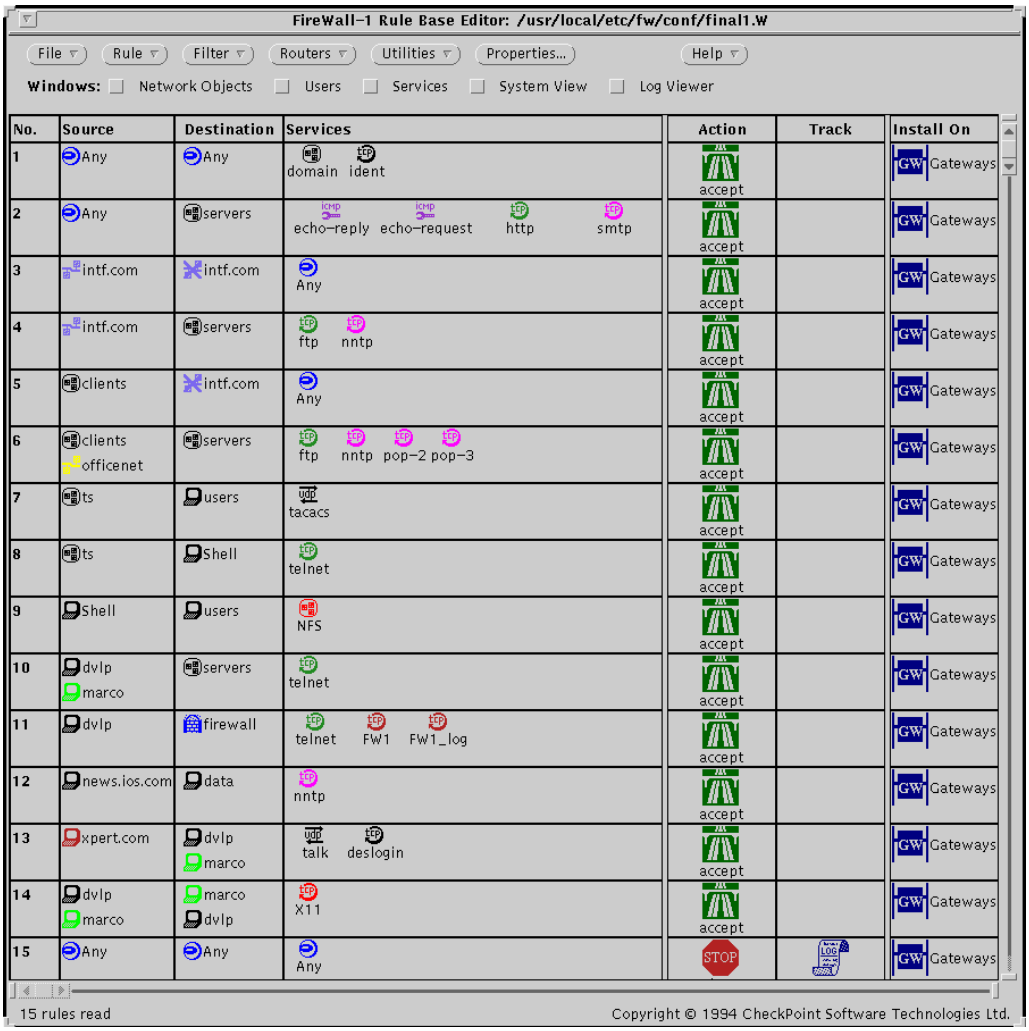
FireWall-1 era stato commercializzato da pochissimo e portava un'idea allora molto avanzata: la Stateful Inspection, insieme a una GUI X11 (quindi in ambiente grafico) che permetteva di esprimere le policy usando oggetti che rappresentavano host, reti e servizi.

La cosa interessante non era soltanto avere un firewall, ma il modo in cui era inserito nella rete. DATA e USERS disponevano di collegamenti Ethernet separati verso il firewall; l'Office LAN costituiva un altro segmento. Non era una singola LAN piatta con un filtro davanti. Le policy descrivevano esplicitamente chi potesse raggiungere quale sistema e attraverso quali protocolli.

Tra i materiali recuperati c'è anche un GIF originale della rule base di FireWall-1. È uno dei reperti che preferisco perché non mostra soltanto che avevamo un firewall: racconta concretamente come funzionava la rete. La regola 7, ts → users, tacacs, è il ramo laterale dell' autenticazione: i terminal server potevano interrogare USERS senza che il traffico Internet degli abbonati dovesse attraversare il server. La regola 12, news.ios.com → data, nntp, mostra invece il feed Usenet proveniente dall' esterno. La 13 autorizzava xpert.com verso DVLP e la mia workstation "marco" per talk e deslogin: accesso remoto del fornitore israeliano, con un meccanismo di login cifrato, prima che SSH diventasse il modo normale di fare la stessa cosa.

In una sola schermata compaiono quindi autenticazione centralizzata, feed Usenet e accesso remoto di un fornitore esterno: problemi che oggi chiameremmo identity, service exposure e third-party access. E in fondo alla policy c'era la regola che dava senso a tutte le altre: Any → Any → Any: STOP. Tutto ciò che doveva passare doveva essere autorizzato esplicitamente prima.

C'è però una distinzione importante: i clienti dial-up non erano "dietro" FireWall-1. Il firewall proteggeva i server centrali e l'ufficio. Il traffico ordinario dei clienti verso Internet rimaneva sul lato world della rete; attraversava il firewall solo quando doveva raggiungere un servizio protetto, per esempio l'autenticazione su USERS o i servizi centrali consentiti dalle policy.



Screenshot originale della rule base Check Point FireWall-1 su X11, 1995.

Seguire una connessione: da Milano a Internet

Il modo più semplice per spiegare il resto dell'architettura è seguire un utente. Nel 1995 non si apriva un'app: si faceva una telefonata.

Prima che potesse fare quella telefonata, però, il cliente doveva essere stato attivato. L'area commerciale lasciava in segreteria un modulo cartaceo con i dati del cliente e il contratto firmato; dalla workstation chiamata "anna" quei dati venivano inseriti nel gestionale e poi inviati via email a me, perché creassi l'account sui sistemi del provider e ne abilitassi l'accesso. Dalla stessa macchina arrivavano anche le richieste di assistenza via email: i problemi più comuni venivano gestiti facendo riferimento alle FAQ che avevo preparato, mentre le questioni più tecniche mi venivano inoltrate. Fra i materiali recuperati sono sopravvissuti anche alcuni di questi scambi, ed è attraverso quegli scambi che ho ricostruito il passaggio quotidiano fra commerciale, amministrazione, customer care e infrastruttura tecnica.

Il cliente di Milano componeva il numero di accesso. La rete telefonica usava un gruppo di ricerca per inoltrare la chiamata su una linea libera, collegata a uno dei modem. All'inizio il POP disponeva di sedici modem: sedici linee significavano sedici utenti contemporanei, perché ogni sessione occupava fisicamente un modem e una linea telefonica per tutta la durata del collegamento.

Il modem negoziava la connessione con quello del cliente e consegnava la linea seriale a un Cisco 2511. Sul 2511 le interfacce asincrone erano configurate per PPP. Era l'access server a ricevere username e password, ma non era lui a possedere il database degli utenti.

L'autenticazione era il primo passaggio

Il Cisco 2511 interrogava via XTACACS il server USERS. Questo passaggio è importante da visualizzare correttamente: USERS non era "in mezzo" al traffico Internet del cliente. Il 2511 chiedeva a USERS se quelle credenziali fossero valide; ottenuta la risposta, la sessione PPP poteva proseguire sulla rete. Un unico sistema di autenticazione serviva quindi tutti i POP.

Su molti PC Windows l'accesso TCP/IP richiedeva ancora software dedicato. Tra i materiali conservati c'è, per esempio, la distribuzione di Trumpet Winsock 3.0 insieme alla documentazione di configurazione fornita agli utenti.

Il Welcome Kit di Internet Force, che ho recuperato integralmente (e di cui ho deciso di pubblicare anche i sorgenti), lo avevo realizzato per i clienti del provider: forniva software (tra cui le versioni di Netscape ed Eudora di allora) e istruzioni per configurare il collegamento e iniziare a navigare. È un reperto interessante perché mostra l'altra estremità dell'infrastruttura: da una parte Cisco, Sun, DNS e autenticazione; dall'altra un utente con Windows, un modem e nessuna ragione per sapere cosa fosse PPP.

Poi arrivavano DNS e routing

Una volta autenticato, il cliente era davvero sulla rete. Se apriva Netscape e digitava il nome di un sito, prima ancora di scaricare una pagina il resolver doveva ottenere dal DNS l'indirizzo IP corrispondente. Internet Force gestiva direttamente i propri name server, primario e secondario, sui sistemi centrali.

Ottenuto l'indirizzo, i pacchetti del cliente milanese passavano dal 2511 alla backbone "world" e raggiungevano il Cisco 2501 centrale, che instradava il traffico sul collegamento Frame Relay verso IDT e da lì su Internet. Il firewall non era sul percorso ordinario di quella sessione.

Anche l'indirizzo IP della sessione veniva assegnato dinamicamente: il pool era gestito dal servizio DHCP fornito dagli stessi access point. Il routing della rete, invece, rimase statico. Il progetto discusso con Xpert prevedeva di introdurre IGRP quando la crescita dell'infrastruttura lo avesse reso utile; con l'aggiunta di un secondo collegamento verso un carrier italiano Internet Force avrebbe inoltre dovuto evolvere verso un proprio Autonomous System. La società chiuse prima che quel passaggio diventasse necessario.

La stessa telefonata da Pesaro, Palermo o Gorgonzola

I POP remoti aggiungevano un passaggio, ma non duplicavano i servizi centrali. Pesaro, Palermo e Gorgonzola avevano ciascuno una coppia di apparati Cisco: un 2511 per le linee asincrone e l'accesso dial-up, e un 2501 che collegava il POP alla backbone del provider. I due router erano collegati localmente; da lì il POP raggiungeva Milano attraverso un circuito dedicato CDA/CDN da 64 kbit/s.

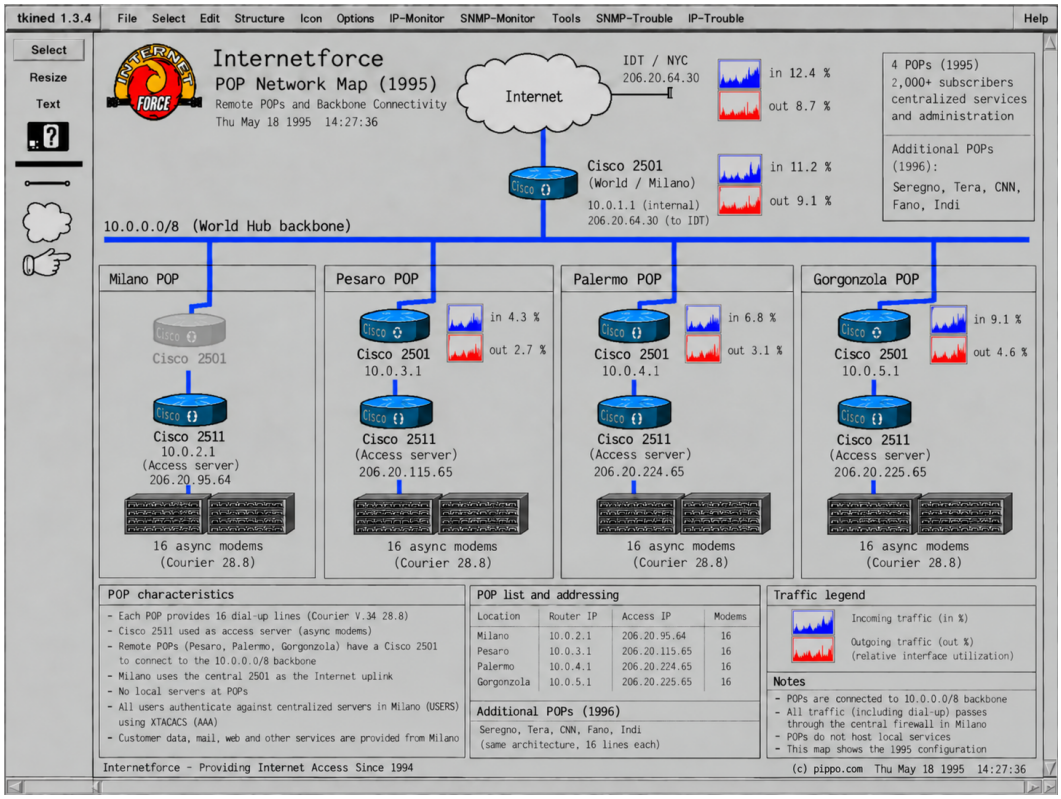
Il cliente di Pesaro, per esempio, faceva un percorso concettualmente semplice: telefono → modem → Cisco 2511 → Cisco 2501 del POP → backbone → Cisco 2501 centrale → IDT → Internet. Quando serviva autenticarsi, il 2511 apriva invece il ramo XTACACS verso USERS a Milano.

Questa scelta permetteva di mantenere i POP relativamente semplici. Non c'erano server utenti, mail server o DNS completi da amministrare in ogni città: il bordo della rete raccoglieva le connessioni, mentre identità e servizi rimanevano centralizzati.

Xpert mi aveva insegnato anche una regola empirica per dimensionare queste reti. Il numero magico era 8, non 42. Per la banda, prendevamo la capacità del collegamento geografico e la moltiplicavamo per otto, confrontandola con la banda nominale complessiva dei modem. In un POP con 16 modem da 28,8 kbit/s il

carico teorico massimo era circa 461 kbit/s; 64 kbit/s di CDN moltiplicati per otto davano invece 512 kbit/s. Finché il secondo valore rimaneva superiore al primo, il dimensionamento era considerato adeguato. Era naturalmente una regola statistica: si assumeva che non tutti gli utenti trasferissero dati contemporaneamente alla massima velocità.

Una logica analoga valeva per il numero di linee. I tecnici di Xpert mi indicavano come riferimento per un provider di buona qualità fra gli 8 e i 16 abbonati per modem: abbastanza pochi da mantenere ragionevole la probabilità di trovare una linea libera nelle ore di punta. Un POP con 16 modem poteva quindi servire indicativamente fra 128 e 256 abbonati senza che fosse necessario avere una linea telefonica dedicata a ciascuno.



Dettaglio dei POP: Milano e i tre POP remoti iniziali, con la successiva espansione del 1996.

Essere online significava usare i servizi del provider

Raggiungere Internet era solo una parte dell'esperienza. Un ISP doveva offrire e amministrare direttamente una quantità di servizi che oggi tendiamo a dare per scontati o a delegare a piattaforme esterne.

Posta elettronica

La posta arrivava via SMTP e veniva conservata sui sistemi del provider. Il client dell'utente la recuperava tramite POP3 o IMAP. USERS ospitava quindi non soltanto l'identità necessaria per collegarsi, ma anche una parte importante della vita digitale quotidiana dell'abbonato.

Web, FTP, News e mailing list

DATA ospitava il Web pubblico e l'FTP anonimo, oltre a servizi e contenuti che cambiarono nel tempo. Le mailing list erano gestite con Majordomo. Usenet faceva ancora parte dell'esperienza normale di Internet. Il

feed esterno arrivava da news.ios.com via NNTP: è lo stesso flusso che compare nella regola 12 della policy FireWall-1.

Questa è forse la differenza più evidente rispetto a molti servizi Internet contemporanei: il provider non vendeva soltanto un "tubo". Doveva costruire e mantenere un piccolo ecosistema di servizi interoperabili. Per l'utente erano icone separate sul desktop: Netscape, Eudora, un client FTP, un newsreader, Telnet. Dietro ciascuna icona c'era un protocollo, e dietro quel protocollo un daemon che qualcuno doveva configurare e tenere in vita.

Dietro la rete c'era un ufficio

Le configurazioni raccontano bene i pacchetti, ma meno bene le persone. Eppure anche l'Office LAN ha lasciato una specie di organigramma fossile: i nomi delle macchine. Alcuni erano funzionali, come "dvlp" e "html"; altri coincidevano con i nomi con cui in ufficio identificavamo le workstation. Rivederli oggi è probabilmente il modo più rapido perché un ex collega riconosca il proprio posto di lavoro senza che io debba trasformare questo articolo nell'elenco telefonico del 1995.

L'ambiente era molto eterogeneo. La mia workstation "marco" era un 486DX con Linux Slackware; DVLP era una Sun SPARCstation; "maxi", usata da uno dei commerciali, era un PowerBook; diverse workstation dell'ufficio erano Macintosh con System 7.5.x. "Laura" e "Alice", in particolare, erano Power Macintosh 9500 della redazione. Nel 1996 comparve anche "oracolo", un sistema Windows NT con Oracle. Tutto conviveva sulla stessa infrastruttura Ethernet dell'ufficio, collegata tramite un hub 3Com.

La redazione: Web e carta

Internet Force aveva una redazione giornalistica che produceva contenuti per il Web ma anche una rivista cartacea. laura e alice erano workstation Power Macintosh 9500 equipaggiate con una suite completa di desktop publishing e trattamento delle immagini: QuarkXPress, Adobe PageMaker, Adobe Photoshop e Adobe Type Manager.

La direzione artistica lavorava invece sulla macchina "salvatore", preparando anche le immagini finite destinate ai siti. La macchina "HTML" aveva un compito molto meno ambiguo del suo nome: lì le pagine venivano scritte a mano in HTML. Nel 1995, se si voleva controllare davvero il risultato, era una pratica perfettamente normale.

Dal file HTML al server pubblico

Il passaggio dalla redazione alla produzione era già separato. Avevo predisposto su DVLP un'area FTP a uso interno. salvatore forniva a HTML gli asset grafici; HTML costruiva le pagine e, quando il sito era completo, l'intero artefatto veniva depositato in una cartella dedicata ai siti sull'FTP interno.

A quel punto intervenivo io. Prelevavo il sito, verificavo che fosse completo e funzionasse come previsto e lo caricavo su DATA. La redazione, quindi, non pubblicava direttamente sul Web server di produzione. C'erano authoring, un'area di scambio che oggi chiameremmo staging, una verifica tecnica e infine il deployment. Non lo chiamavamo CI/CD, e forse è meglio così: funzionava anche senza una dashboard con dodici badge verdi.

Quando serviva interattività sviluppavo personalmente dei CGI. Nel marzo 1996 installai PHP/FI (una delle primissime versioni di PHP da compilare come cgi); successivamente arrivò anche Postgres95 su DATA, database che in futuro sarebbe divenuto noto come PostgreSQL. Non ricordo ancora la data esatta dell'installazione del database, e l'archeologia serve anche a questo: lasciare aperta una data finché non salta fuori il reperto che la chiude.

In pochi mesi quella pipeline racconta una trasformazione più ampia del Web: pagine statiche scritte a mano, CGI, scripting server-side e infine dati persistenti gestiti da un database.

Un server Oracle perché il mestiere cambiava continuamente

“oracolo”, documentato nell’archivio nel 1996, era un esperimento Windows NT con Oracle. Non faceva parte del cuore Unix dell’ISP: i soci volevano costruire competenze su quella piattaforma per poter proporre anche consulenza ai clienti. Il dettaglio divertente è che io Oracle e Windows NT non li conoscevo.

Li studiai da autodidatta in circa sette-dieci giorni e realizzai il progetto. È un episodio che descrive abbastanza bene cosa significasse essere il responsabile tecnico di una piccola società Internet in quegli anni: non esisteva un team Unix, uno database, uno security, uno networking e uno Web. Il perimetro del ruolo si spostava insieme al problema.

Una rete che potevi vedere

L’intero sistema veniva monitorato dalla mia workstation Linux attraverso Scotty/Tkined, un ambiente Tcl/Tk per la gestione delle reti. La mappa non era soltanto un disegno: tramite SNMP potevo osservare il traffico sulle interfacce, l’utilizzo delle linee asincrone dei Cisco, lo stato dei nodi e altri indicatori operativi.

È proprio da una mappa tkined originale conservata nei backup che è partita una parte importante della ricostruzione del 2026. Confrontandola con configurazioni Cisco, file di routing, DNS, documenti hardware e policy del firewall è stato possibile distinguere ciò che ricordavo correttamente, ciò che apparteneva a momenti diversi e qualche dettaglio che trent’anni avevano inevitabilmente mescolato.

Guardata oggi, l’infrastruttura sembra minuscola: poche Sun, alcuni Cisco, rack di modem, due hub Ethernet e un collegamento internazionale che prima misurava 128 kilobit e poi due megabit. Ma dentro quella mappa c’erano già quasi tutti i problemi fondamentali di un provider: accesso, routing, AAA, DNS, posta, Web, sicurezza, monitoring, provisioning e pubblicazione dei contenuti.

Il repository: il livello sotto la storia

Questo articolo segue volutamente i processi e non i file. Il repository GitHub fa il contrario: permette di aprire il cofano e scendere dentro l’infrastruttura. Le configurazioni Cisco e Unix, le zone DNS, la policy del firewall, le mappe di rete, i documenti operativi e i reperti recuperati sono organizzati in modo da poter essere letti nel loro contesto, distinguendo i materiali originali dalle ricostruzioni.

Ho cercato però di non trasformarlo in una semplice collezione di vecchi file. Le mappe interattive permettono di esplorare i POP, la rete centrale e i singoli sistemi, arrivando dalle macchine alle configurazioni che sono sopravvissute. Chi preferisce seguire un percorso tecnico può invece partire da “Build an Internet Force POP”, una guida che prova a rispondere a una domanda molto concreta: se nel 1995 aveste dovuto costruire un Internet provider, da dove avreste cominciato?

Il percorso parte dalla preparazione di una macchina Unix e attraversa routing, modem e access server, autenticazione, DNS, posta, Web, sicurezza, monitoring e gestione operativa. In pratica segue dall’interno molti degli stessi processi raccontati in questo articolo, ma permettendo di aprire i file e vedere come erano realmente configurati.

Tra le cose che l’archivio ha permesso di ricostruire ci sono anche procedure quotidiane ormai completamente scomparse. Registrare un dominio, per esempio, era molto più complesso di oggi; per i .it esistevano inoltre vincoli amministrativi e tecnici particolarmente rigidi. Nel repository è ricostruita l’intera procedura, passo per passo, insieme ad alcuni esempi reali di registrazioni che ho effettuato ai tempi come Internet Force.

Nel repository sono finiti anche reperti meno infrastrutturali: il Welcome Kit destinato ai clienti, documenti e post Usenet, materiali recuperati dalle mailbox, i sorgenti della Guida ad Internet e alla realtà virtuale e altri frammenti della cultura tecnica di quegli anni. Non perché tutto ciò facesse parte dello stesso “sistema”, ma

perché un ISP non era soltanto router e daemon: era anche il modo in cui quelle tecnologie venivano imparate, spiegate e utilizzate.

Altri strati dell'archivio

Nei backup della mia workstation Linux di allora sono riemerse anche alcune cartelle di posta originali. Dentro ci sono messaggi tecnici e mailing list, i ringraziamenti di persone che avevano scaricato la mia Guida ad Internet e alla realtà virtuale, scambi personali e inevitabili barzellette nerd.

Nei backup sono riemersi anche i sorgenti della Guida ad Internet e alla realtà virtuale stessa, insieme ad altro materiale legato agli esperimenti che facevamo allora con il Web e con VRML. Nel 1995-96 la realtà virtuale sul Web sembrava una delle possibili direzioni in cui Internet avrebbe potuto evolvere: mondi tridimensionali descritti in VRML, navigabili dal browser con gli strumenti dell'epoca. Rivedere oggi quei sorgenti è interessante proprio perché conserva non soltanto ciò che Internet era, ma anche alcune delle idee su ciò che pensavamo potesse diventare.

Nello stesso backup è riemerso anche il materiale di un articolo che scrissi nel 1997, dopo aver partecipato al DEFCON V di Las Vegas, una delle prime edizioni della convention hacker. È successivo alla chiusura di Internet Force e quindi non appartiene alla storia dell'ISP, ma il fatto che sia rimasto nello stesso backup DAT racconta bene un'altra caratteristica dell'archeologia digitale: gli archivi personali non rispettano i confini delle aziende o dei progetti, continuano semplicemente ad accumulare strati.

Rileggerle fa emergere un'altra differenza apparentemente minuscola: le signature delle email. Ai tempi spesso non erano noiosi blocchi aziendali standardizzati, ma piccole dichiarazioni di identità fatte di citazioni, motti, ASCII art o battute. Anche da quattro righe in fondo a un messaggio traspariva la personalità di chi scriveva.

Il repository è pubblico qui: https://github.com/pippocom/internetforce-1995. Se questo articolo racconta cosa accadeva quando un cliente si collegava, lì si può seguire il percorso fino ai file di configurazione e, volendo, provare a capire come si costruiva davvero un ISP nel 1995. Il repository comprende anche la guida Build an Internet Force POP, che attraversa passo per passo la costruzione dell'infrastruttura; le mappe interattive permettono invece di esplorare la rete complessiva, la struttura dei POP e i dettagli dei server centrali.

C'è anche un motivo più personale per averlo pubblicato. Gran parte di ciò che avevamo imparato allora proveniva da RFC pubbliche, sorgenti leggibili, FAQ, mailing list e discussioni tecniche aperte. Trent'anni dopo, rendere nuovamente ispezionabile quell'infrastruttura mi sembra un modo abbastanza naturale di restituire alla rete una parte di ciò che la rete aveva dato a me.

Che fine fece Internet Force?

La storia della società fu molto più breve di quella di alcune parti della sua rete. Internet Force terminò prematuramente la propria attività alla fine del 1996: i suoi soci pensavano che non fosse un business così redditizio come avevano pensato e decisero di chiuderla proprio alla vigilia degli anni in cui Internet avrebbe iniziato a crescere molto più rapidamente anche in Italia.

Ma la fine della società non significò che tutto ciò che era stato costruito venisse semplicemente spento. Mi piace pensare che, nel suo piccolo, Internet Force avesse gettato dei semi nelle aree in cui aveva aperto i propri POP. Portare un punto di accesso locale significava installare infrastruttura e competenze, ma anche stimolare un bisogno in persone e aziende che fino a poco prima non lo avevano avuto a portata di telefonata.

Quando Internet Force chiuse, alcuni di quei nodi continuarono quindi una vita autonoma. Il POP di Gorgonzola proseguì come Pointest, che ritroviamo successivamente citata anche in una delle edizioni italiane della Guida a Internet della Electronic Frontier Foundation. A Pesaro, Pesaro Point continuò invece a crescere fino a diventare un ISP regionale: pochi anni dopo il suo sito presentava una rete articolata su nove POP nelle Marche.

Sono soltanto due esempi, ma rendono meno netta la data in cui questa storia dovrebbe finire. Internet Force come società scomparve prima di poter partecipare al boom che stava arrivando; alcuni dei POP che aveva contribuito a mettere in rete continuarono invece a crescere proprio dentro quel boom. La società non raccolse quei frutti, ma qualche seme aveva germogliato.

Cosa può insegnare un provider del 1995 a chi sviluppa software oggi

A trent'anni di distanza, le tecnologie utilizzate da Internet Force possono sembrare rudimentali. Eppure, osservando l'architettura e le scelte operative, emerge qualcosa di interessante: molti dei problemi che oggi affrontiamo con piattaforme cloud, strumenti DevOps e infrastrutture automatizzate erano già presenti allora.

Le tecnologie cambiano molto più rapidamente dei problemi che devono risolvere.

L'accesso alla rete richiedeva di autenticare gli utenti, gestire autorizzazioni e coordinare sistemi differenti. Oggi parliamo di Identity and Access Management, federazione delle identità e Zero Trust. Sono architetture e modelli di sicurezza molto più evoluti, ma rispondono anche a esigenze che un provider degli anni Novanta conosceva bene: sapere chi sta accedendo, a quali risorse e con quali privilegi.

Anche la separazione degli ambienti non nasce con i container. Compilare software su una macchina e distribuirlo su un'altra, limitare i servizi esposti, distinguere gli ambienti di lavoro da quelli operativi erano scelte tecniche che potevano essere adottate ben prima dell'esistenza delle moderne pipeline CI/CD. L'automazione è cambiata radicalmente; la necessità di controllare ciò che viene messo in produzione, molto meno.

Un'altra lezione riguarda la rete. Oggi l'osservabilità si concentra spesso su applicazioni, container e metriche dei servizi. Ma per un Internet Service Provider la rete non era uno strato trasparente: era parte integrante del sistema da comprendere, configurare e diagnosticare. È un promemoria ancora attuale: monitorare un'applicazione senza comprenderne le dipendenze di rete significa osservarne soltanto una parte.

C'è poi il ruolo degli standard aperti e del software ispezionabile. Internet è cresciuta grazie a protocolli interoperabili e a un ecosistema nel quale era possibile studiare, modificare e integrare componenti software. Non tutto era open source, naturalmente, ma la possibilità di comprendere il funzionamento dei sistemi, anziché trattarli esclusivamente come scatole nere, era una risorsa tecnica fondamentale. Lo è ancora oggi, soprattutto quando valutiamo dipendenze tecnologiche, sicurezza e rischio di vendor lock-in.

Infine, questi archivi ricordano una cosa che rischiamo di sottovalutare: la documentazione tecnica è parte dell'infrastruttura, anche quando l'infrastruttura non esiste più.

Configurazioni, sorgenti, script, procedure operative e persino errori raccontano non soltanto come funzionava un sistema, ma perché erano state prese determinate decisioni. Conservarli permette di ricostruire vincoli, compromessi e soluzioni che altrimenti andrebbero perduti.

Conclusione: prima che Internet semplicemente “ci fosse”

La cosa che mi ha colpito di più durante questa ricostruzione non è quanto fossero primitive le tecnologie del 1995. È il contrario: molti dei problemi erano già sorprendentemente familiari. Separare sviluppo e produzione, ridurre la superficie di attacco, centralizzare l’identità, distribuire l’accesso, monitorare la rete, definire policy esplicite, evitare che chi produce contenuti pubblichi direttamente sui sistemi operativi. Sono

problemi che continuiamo a risolvere con strumenti molto più potenti e, occasionalmente, con diagrammi molto più belli.

La differenza è che allora i confini erano visibili. Una connessione occupava un modem. Un POP era una coppia di router e un rack di linee telefoniche. La posta era un processo su una macchina che potevi indicare con il dito. Se il DNS non funzionava, sapevi quale daemon andare a guardare. E se volevi capire Internet, prima o poi finivi per leggere una RFC o un file di configurazione.

È per questo che considero questi backup una piccola forma di archeologia digitale. Presi singolarmente sono resti: una route, una zone file, una policy, una directory FTP, il nome di un Macintosh. Rimessi nel loro contesto raccontano invece una comunità di utenti, un ufficio, una redazione e una rete che ogni giorno trasformava telefonate analogiche in accesso a Internet.

Rimettere online tracce di un'Internet in cui l'infrastruttura tecnica e la comunità che la costruiva erano molto più visibilmente intrecciate, significa restituire ancora oggi alla rete un po' della conoscenza che la rete aveva dato a me.

Prima che Internet diventasse qualcosa che semplicemente "c'è", qualcuno doveva costruirlo. Un modem, un daemon e una regola di routing alla volta.