ITBH Technical White Paper
Italian Black Hats Association - Associazione Italiana Black Hats

I Network X.25: Comprensione della struttura di rete, Tecniche di attacco ed Identificazione delle intrusioni

Versione 1.0

Raoul Chiesa aka Nobody
C.T.O. @ Mediaservice.net Srl, DSD Divisione Sicurezza Dati (http://@mediaservice.net)
Socio Fondatore di Italian Black Hats Association (http://www.blackhats.it)
Socio Fondatore e Membro del Comitato Direttivo CLUSIT, Associazione Italiana Sicurezza Informatica (http://www.clusit.it)
nobody@blackhats.it

Marco Ivaldi aka Raptor
Ricercatore e consulente nel campo della sicurezza informatica, si interessa di networking, telefonia, protocolli di comunicazione e crittografia: fa parte della D.S.D. di @ Mediaservice.net Srl. È socio Fondatore di Antifork Research (http://www.antifork.org) e ITBH (http://www.blackhats.it).
raptor@blackhats.it

INDICE

Disclaimer

Le opinioni e le informazioni espresse nel presente documento appartengono agli autori e non ad aziende: esse non rappresentano in alcun modo idee, politiche aziendali o servizi specifici se non il pensiero e l'esperienza degli autori stessi.

Il disclaimer standard si applica al presente documento, in particolare modo per la non responsabilità degli autori, Raoul Chiesa e Marco Ivaldi, verso qualunque tipo di danni - causati direttamente o indirettamente – conseguenti alla lettura del presente documento e/o all'utilizzo illegale o fraudolento delle informazioni e/o funzionalità ivi contenute.

Gli autori non si assumono alcuna responsabilità per i contenuti di questo documento – così come di eventuali errori od omissioni – o di qualunque documento, prodotto o servizio da esso derivati, indirettamente o meno.

Tutti i servizi menzionati nel presente documento sono di pubblico dominio e reperibili presso gli helpdesk, i servizi informativi X.25 ed i web site dei differenti carrier dati o, in alternativa, sono stati reperiti attraverso la rete Internet nel periodo 2001-2002.

Gli indirizzi X.25 inseriti nel presente documento sono riportati a puro titolo di esempio: qualora non fossero di pura fantasia questi ultimi sono riferiti ad utenze X.25 effettivamente esistite ma non più attive, reperite da documenti pubblici disponibili sulla rete Internet, su BBS o provenienti da archivi file privati.

Il presente documento può essere liberamente distribuito, pubblicato o copiato con ogni mezzo disponibile a patto che lo stesso non venga modificato in alcun modo e previa autorizzazione scritta degli autori.

E' assolutamente vietato "appropriarsi" della proprietà intellettuale dell'opera, ovverosia spacciarsi per gli autori, tradurlo in altre lingue appropriandosene la paternità o estrapolare singoli paragrafi spacciandosi per l'autore degli stessi.

Copyright © 2000-2002 <Raoul Chiesa, Marco Ivaldi> (GNU/FDL License)
This article is under the GNU Free Documentation License,
http://www.gnu.org/copyleft/fdl.html
Verbatim copying and distribution of this entire article is permitted in any medium,
provided this notice is preserved.

ABSTRACT

"X.25 is used in a Packet Switched Network and in 1964 was designed by Paul Baran of the RAND Corporation for use with the Public Data Network (PDN) and unreliable analog telephone services. The idea was to connect a dumb terminal to a packet-switched network. In 1976 X.25 became a standard under the CCITT, now the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T). "

I network X.25, spesso ritenuti erroneamente "reti in via di pensionamento", si stanno rilevando sempre più soggetti ad attacchi di alto livello diretti verso enti bancari, multinazionali, TelCo[1], reti aeronautiche civili e sistemi governativi o militari.

In questo documento verranno illustrate - dopo averne analizzato la storia ed aver fornito una visione generale focalizzata sull'Italia, le principali differenze tra l'hacking su protocolli TCP/IP ed X.25, studiando le diverse tecniche di attacco, indagine e reazione, per concludere fornendo un elenco di regole aggiuntive alle politiche-base di sicurezza: le sezioni principali del documento sono state divise in **Sezione Teorica** e **Sezione Pratica**.

Nella Sezione Teorica viene fornita un'overview sulle reti a commutazione di pacchetto, per proseguire analizzando nel dettaglio il protocollo X.25 definito dall'ITU[2] ed arrivare alle differenti modalità di accesso.

La Sezione Pratica intende invece fornire un'overview sulle varie tipologie di chiamata in uscita da differenti OS e differenti metodologie di NUA scanning, attacco e copertura delle tracce.

Come tutti i Technical Paper dell'Associazione Italiana Black Hats, anche questo documento può essere letto dal punto di vista dell'attaccante o del gestore del sistema stesso: vale in ambo i casi la regola "conosci il tuo nemico prima di"…

Ogni qualvolta se ne presenterà la possibilità il presente documento verrà aggiornato, con le nuove scoperte o gli update rilevati da ITBH: ovviamente invitiamo i lettori a comunicarci eventuali errori, imperfezioni o aggiornamenti dei quali siano a conoscenza.

Buona lettura,

gli autori.

[1] TelCo: Telephone Companies, le compagnie telefoniche
[2] I.T.U. International Telecomunication Union, cfr. pag. 26 (http://www.itu.int)

PRIMA PARTE, SEZIONE TEORICA

I) Introduzione

Le reti X.25 hanno una logica di indirizzamento completamente differente dal TCP/IP e, di conseguenza, le azioni di tracing verso l'attacker sono sostanzialmente diverse. Qualcuno ricorderà le difficoltà di tracciamento vissute da Clifford Stoll e narrate nel libro The Cuckoo's Egg, primo racconto reale di episodi di hacking da parte di europei verso sistemi militari, governativi ed università nordamericane. Hacker celebri come Pengo ed Hagbard del CCC[3] furono utilizzati dal KGB per azioni di hacking e spionaggio militare verso gli Stati Uniti tra il 1984 ed il 1988, con il compito di ottenere tecnologia ed informazioni segrete e portarle fisicamente da Berlino Ovest a Berlino Est. Racconti e storie che rasentano le "spy story" sono realmente accaduti ed hanno avuto come terreno di gioco le dorsali X.25 di vari paesi, europei ed extraeuropei.

Molto probabilmente una buona parte delle tendenze hacking alle quali assisteremo nell'immediato futuro non saranno altro che una ripetizione di quanto è già successo negli anni passati e su altre tipologie di reti, ma saranno però focalizzate su TCP/IP e, sicuramente, IPv6.

Tornando alla logica di funzionamento di una rete X.25, possiamo dire che con la tecnica a commutazione di pacchetto (packet switching) le sequenze dei dati – provenienti dal terminale o dall'elaboratore collegato alla rete X.25, altresì chiamato DTE (Data Terminal Equipment) – sono strutturate in **blocchi**, ovverosia pacchetti. Ognuno di questi pacchetti contiene in un apposito campo di *header* (intestazione) le informazioni sul servizio, quali ad esempio l'indirizzo del destinatario o il numero di sequenza del pacchetto, i quali permettono alla rete X.25 di instradare e di portare a destinazione in modo corretto ogni pacchetto.

Quando i pacchetti raggiungono il DTE remoto, destinatario dei dati, le informazioni di servizio vengono eliminate ed, in questo modo, vengono ricostruite le sequenze dei dati nella forma originaria.

Questa tecnica, denominata prima come multiplexing, permette l'ottimizzazione dell'uso dei mezzi di trasmissione e, soprattutto, rende possibile una diminuzione dei costi per il loro utilizzo, in quanto i pacchetti relativi a comunicazioni differenti possono viaggiare sullo stesso circuito fisico.
Alle reti X.25 possono essere collegati **DTE a pacchetto**, secondo la raccomandazione CCITT X.25 e, quindi, sistemi server, personal computer ed ogni altra apparecchiatura informatica dotata di scheda X.25, oltre a **DTE asincroni** a carattere, quali terminali dumb TTY, terminali video asincroni, personal computer con interfaccia asincrona.

Il compito dell'inoltro dei dati inviati da interfacce asincrone, data la particolarità dell'invio degli stessi sotto forma di singoli caratteri, è svolto dal PAD[4] il quale utilizza una funzione apposita di conversione, assemblando i caratteri in pacchetti e viceversa. I DTE a carattere devono dialogare con il PAD secondo le regole, alquanto precise, stabilite nella raccomandazione X.28 del CCITT.

E' infine possibile collegare alla rete X.25 dei DTE operanti con protocolli di tipo sincrono, quali ad esempio BSC o SDLC, i quali vengono convertiti grazie a dei "convertitori di protocollo" in genere forniti come opzione dal carrier dati X.25.

[3] Chaos Computer Club, gruppo hacker di Amburgo, Germania
[4] PAD Packet Assembler Disassembler

II) Le reti a commutazione di pacchetto X.25

Molti utenti Internet vedono le reti X.25 come un qualcosa di misterioso, arcano e sconosciuto: esse sono quasi interpretate come delle dorsali utilizzate esclusivamente dai fornitori di telecomunicazioni per collegare differenti backbone e rendere possibile la connettività internazionale.

Se è in parte vero che X.25 ha reso possibile la costruzione della prima vera ragnatela mondiale di comunicazioni - anche grazie al fatto di essere stata presente in più di 100 differenti nazioni, prima attraverso le reti delle singole compagnie telefoniche per poi espandersi verso carrier dati privati – è altrettanto vero che gli utenti di questa rete mondiale non rientrano nel solo caso dei carrier di comunicazione ma, anzi, spaziano da multinazionali a realtà governative, centri di ricerca, università, fornitori di servizi a valore aggiunto, centri di controllo remoto, banche, corporate networks, sistemi statali di pubblica utilità, aeroporti, ospedali e così via.

Chi scrive sente di poter dire di avere un'ampia conoscenza dei network X.25, avendoli utilizzati dal 1986 al 1995 in quasi tutti i paesi del mondo; voglio infine evidenziare, prima di iniziare a spiegare nel dettaglio, come in alcune culture e politiche nazionali la "risorsa X.25" sia stata e continui ad essere *La rete* ideale alla quale collegare sistemi e risorse critiche. A titolo di esempio, il Ministry of Health dell'Arabia Saudita è su X.25 e non su altre reti pubbliche, così come il sistema di controllo dell'Aeroporto di Cipro o quello di Dakar: è ovvio che sistemi simili non saranno mai presenti su reti quali Internet o, quantomeno, non per quanto riguarda i server critici di gestione.

***

III) Un po' di storia

La prima WAN[5] esistente al mondo è stata Internet: l'idea e l'obiettivo iniziale nacque alla fine degli anni '50[6] con il progetto Arpanet e, in quella fase, si parlava di una *rete sperimentale*. Essendo sperimentale vi erano molti limiti, tra i quali l'esclusiva praticità effettiva a beneficio di istituzioni (aventi come obiettivo la ricerca) con possibilità di spese elevate, proprio come i militari o le principali università: in quel primo periodo le aziende non si collegarono ad Arpanet, dati i costi esorbitanti e la conseguente mancanza di un buon rapporto necessità-performance-costi.

L'evoluzione tecnologica, la c.d. Information Age, crebbe e le aziende commerciali iniziarono a sentire la necessità di comunicare, in forma digitale ed in maniera economica o, quantomeno, ad un costo accessibile; la necessità di comunicare esplose, in campo commerciale, verso la metà degli anni '70 e le varie TelCos pensarono che, in fondo, disponevano di migliaia di nodi di switch digitali i quali potevano essere multiplexati e quindi ampliati, per poter soddisfare le crescenti esigenze del mercato e poter stendere linee dati dedicate ad un prezzo molto meno esorbitante rispetto agli standard di mercato: i benefici del packet switching furono subito evidenti.

I dati spediti vengono incapsulati in un pacchetto X.25 ed inviati su linee dedicate attraverso il network e, nel contempo, altri dati appartenenti ad altri clienti della rete X.25 li seguono, percorrendo insieme il tragitto deciso sino ai nodi di passaggio nazionali o internazionali. Quello che viene fatto non è altro che multiplexare insieme i segnali, ottimizzando l'utilizzo della dorsale trasmissiva ed incanalando i dati verso i gateway, ovverosia i nodi di passaggio: esistono infatti moltissimi network X.25 e dalla fine degli anni '70 in avanti il loro numero è aumentato considerevolmente.

Per spiegare il funzionamento logico, la struttura ed i pericoli delle reti X.25 prenderemo come esempio l'Italia dove, nel 1984 circa, Telecom Italia – allora SIP – lanciò il servizio ITAPAC. ITA come *Italia* e PAC come *pacchetto*: vedremo più avanti come la fantasia nei nomi delle reti X.25 sia sempre un pò mancata ed il risultato che otteniamo sono reti come TransPac (Francia), Datex-P (Germania), MayPac (Malesya), AustPac (Australia), etc…In realtà una nazione può avere più di una rete X.25 ma, non dimentichiamocelo, la liberalizzazione delle comunicazioni ha riguardato anche – o soprattutto – le trasmissioni dati e sino a pochi anni fa in molti paesi del mondo le TelCos operavano in regime di monopolio: il risultato è che già negli anni '80 gli USA disponevano di almeno 20 reti X.25 differenti mentre l'Italia dispone di 6 reti X.25 solo dall'anno 2000.

Le informazioni sul servizio ITAPAC attualmente non possono più essere reperite sui siti web ufficiali di Telecom Italia (Divisione Reti Dati Itapac), in quanto le URL di riferimento sono state rimosse (gennaio 2001).

[5] Wide Area Network

[6] Il Progetto Arpanet viene approvato (a livello di costituzione e finanziamento) dall'Advanced Research Projects Agency del Department of Defense e dal Congresso USA nel 1958: la prima sede si trovava nell'edificio del Pentagono a Washington. Vedasi l'ottimo documento di Antonella Beccaria aka Shalom, reperibile alla URL http://www.acidlife.com/aciderror/shalom/1_storia_internet.rtf

IV) Gli elementi delle reti X.25

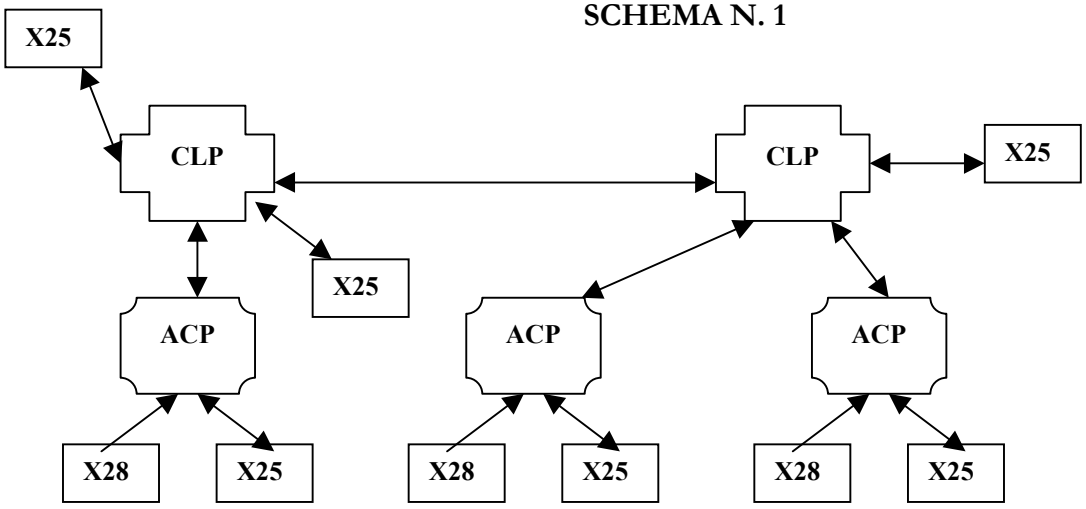
I seguenti elementi costituiscono la maggioranza delle reti X.25 mondiali:

- **Nodi a commutazione di pacchetto (NCP)**, i quali svolgono la sola funzione di transito dei dati;
- **Commutatori locali di pacchetto (CLP)**, i quali hanno funzioni di accessi per i DTE X.25 e di commutazione del traffico dati;
- **Adattatori concentratori di pacchetto (ACP)**, i quali svolgono funzioni di PAD e di accesso per i DTE X.28 (chiamata dialup da linee telefoniche commutate PSTN);
- **Centri di gestione e manutenzione (CGM)**, i quali svolgono compiti di supervisione generale della rete e controllo dei singoli componenti.

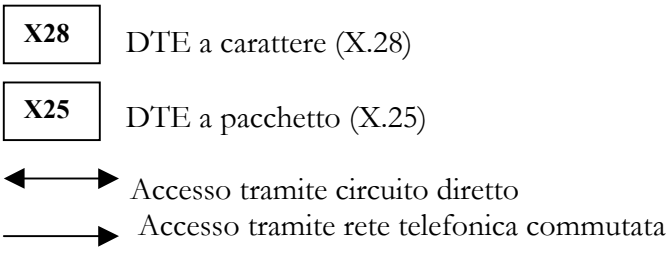
La velocità trasmissiva si differenzia a seconda dell'elemento utilizzato: abbiamo infatti una velocità media standard di 64Kbit/s tra gli NCP e, di conseguenza, tra i CLP collegati agli NCP, mentre gli ACP dialogano con i CLP a 9600 bit/s.

Il seguente schema illustra una tipica struttura di rete X.25.

SCHEMA N. 1



LEGENDA



V) Le modalità di accesso

E' possibile collegarsi alla rete Itapac, così come alla maggior parte delle reti X.25 pubbliche al mondo, in due forme differenti.

La prima modalità consiste nell'utilizzo di una connessione dedicata alla rete: il fornitore del servizio collega una linea dati X.25 dal proprio ACP[7] all'utenza del cliente, il quale paga un canone annuale per la linea ed il noleggio delle apparecchiature (DTE e DCE) al fornitore del servizio, oltre al traffico dati espresso in ottetti.
La seconda modalità di accesso avviene invece utilizzando la linea telefonica commutata (modalità RTG) e viene chiamata X.28. In realtà abbiamo due tipi diversi di accesso X.28: **X.28C** ed **X.28D**.

Con X.28C si intende l'accesso mediante linea telefonica PSTN (accesso commutato), mentre X.28D è l'accesso via ISDN: in quest'ultimo caso viene abilitata la funzione X.28D sulla borchia ISDN del cliente ITAPAC, il quale può però effettuare – come nel caso di accesso X.28C – una sola chiamata contemporanea. Su accesso diretto X.25, invece, è possibile effettuare più chiamate contemporanee, naturalmente in funzione del numero di VC (Virtual Channels) disponibili e sottoscritti a contratto.

Nel caso di chiamata X.28C, dicevamo, sono possibili due modalità:

- **accesso identificato (Accesso identificato via RTG)**
- **accesso Easy Way (Accesso non identificato via RTG)**

L'accesso X.28C viene definito "identificato" quando il chiamante è un abbonato alla rete Itapac e dispone di un proprio NUI[8]. L'utente si collega quindi via modem ad un punto di accesso Itapac e, dopo aver inserito la propria UserID di 6 caratteri alfanumerici e l'indirizzo X.25 (NUA[9]) da chiamare, si collega al DTE remoto. Le spese del traffico dati sono a carico dell'intestatario del NUI.

La sintassi di chiamata è Nxxxxxx-NUA, dove xxxxxx è il NUI del cliente Itapac.. Un esempio di sessione X.28C identificata può essere il seguente:

CONNECT 2400
<CR>
<CR>

ACP:RETE ITAPAC ACP TORINO5 PORTA : 32
^^^^^^^^^ ^^
N.° Nodo N.° porta
*N-26100298

ACP:COM

Notare come i 6 caratteri alfanumerici non vengano visualizzati (noecho) e come, al termine del NUI, si debba inserire il delimitatore "-" seguito dal NUA con il quale ci si vuole collegare.

[7] ACP Access Packet Concentrator, generalmente il punto di accesso locale alla rete X.25
[8] NUI Network User Identification, ovverosia la UserID di accesso alla rete X.25 da dialup
[9] Network User Address

Nel caso di accesso tramite Easy Way, l'utente non sottoscrive un abbonamento ad Itapac ed è quindi sprovvisto di proprio NUI: chiamando il numero 1421 o 1422, con parametri 7E1 alla velocità di 2400 bit/s max., ci si collega al costo di un solo scatto al numero nazionale Itapac Easy Way.

Le modalità di collegamento sono quindi analoghe all'accesso identificato (nel qual caso, però, si chiama un numero di accesso urbano) con l'eccezione della non necessità di inserimento del NUI: il traffico viene infatti addebitato al DTE chiamato e il PAD di accesso Easy Way è stato configurato dal carrier in maniera tale da accettare richieste di chiamate X.28C con una sintassi differente, vale a dire senza l'inserimento del NUI e del delimitatore tra NUI e DTE remoto. Ovviamente il DTE chiamato deve aver sottoscritto l'accettazione di tassazione a carico del ricevente, ovverosia il Reverse Charge.

ATDT1421

CONNECT 2400
<CR>
<CR>

ACP:RETE ITAPAC ACP TORINO LANCIA 7 PORTA : 5
^^^^^^^^^ ^^
N.° Nodo N.° porta
* 26500016 (NUA di Agorà Telematica la quale accetta chiamate Reverse Charge)

ACP:COM

Talvolta un DTE può aver sottoscritto l'opzione di rete X.25 "Reverse Charge", ma può anche aver deciso di utilizzare un "wrapper" per accettare o rifiutare chiamate a carico da alcune zone: come vedremo più avanti, infatti, la rete Itapac così come molte altre reti X.25 utilizzano una struttura logica di indirizzi X.25 (NUA) la quale include il prefisso della città e, quindi, è possibile configurare alcuni OS per accettare chiamate in Reverse Charge dalla zona di Torino ma non dalla zona di Roma.

Tutte le chiamate originate da utenze Easy Way in Reverse Charge hanno come prefisso identificativo del DTE il numero 9: ad esempio 901100064 è un'utenza Reverse Charge (9) di Torino (011).

N.B.: Un'utenza X.28C, sia nel caso di accesso identificato che nel caso di accesso tramite Easy Way, non può ricevere chiamate ma solamente effettuarne verso DTE X.25.

La tabella della pagina successiva (Tabella 1) riassume le velocità medie secondo gli standard tecnici X.25, le raccomandazioni CCITT e la rete fisica di accesso. Alcune reti supportano naturalmente velocità superiori, così come altre (Africa, Zona 6, Centro e Sud America, Zona 7) hanno performance inferiori: si è quindi voluto effettuare una media riassuntiva, la quale non rispecchia forzatamente ogni rete X.25 esistente al mondo.

TABELLA 1

Tipologia DTE	Velocità di trasmissione	Rete fisica di accesso	Raccomandazione CCITT
X.28	300, 1200, 2400 bit/s	Rete telefonica commutata	V.21, V.22, V.22bis
X.28	300 bit/s	Circuito diretto 2 fili analogico	V.21
X.28	9600 bit/s	Rete telefonica commutata	V.22, V.32
X.28	14.400 bit/s	Rete Telefonica Commutata (accesso da 848)	V.32bis
X.28	1200 bit/s	Circuito diretto 2 o 4 fili analogico	V.22, V.23
X.25	2400 bit/s	Circuito diretto 4 fili analogico	V.26 e BB
X.25	2400 bit/s	Circuito diretto 4 fili numerico	X.21 bis
X.25	4800 bit/s	Circuito diretto 4 fili analogico	V.27 bis e BB
X.25	4800 bit/s	Circuito diretto 4 fili numerico	X.21 bis
X.25	9600 bit/s	Circuito diretto 4 fili analogico	V.29 e BB
X.25	9600 bit/s	Circuito diretto 4 fili numerico	X.21 bis
X.25	48000 bit/s	Circuito diretto 4 fili numerico	X.21 bis e X.21
X.25	64000 bit/s	Circuito diretto 4 fili numerico	X.21 bis e X.21

***

VI) X.25: ITAPAC overview

Le reti X.25 consentono lo scambio di informazioni fra elaboratori e/o terminali a pacchetto mediante l'utilizzo di circuiti di tipo "virtuale", così definiti in quanto il collegamento tra i due corrispondenti non comporta l'utilizzo in "uso esclusivo" di circuiti fisici: sullo stesso circuito possono infatti transitare contemporaneamente informazioni relative a più connessioni logiche: l'immediato vantaggio è che un utente X.25 può dialogare contemporaneamente con più DTE remoti, utilizzando una sola sottoscrizione X.25 ed un solo apparato DTE fisico (modem X.25).

Anche il servizio di circuito virtuale deve essere conforme a quanto previsto dalla raccomandazione X.25 del CCITT, la quale definisce il protocollo per lo scambio di infomazioni tra DTE (Data Terminal Equipment) e DCE (Data Circuit Terminating Equipment).

Questa sezione vuole analizzare, prima di passare alla parte più "pratica", le specifiche del protocollo X.25, il quale è articolato su tre livelli (layer) differenti:

1) LIVELLO PACCHETTO
Definisce le procedure per la formazione dei circuiti virtuali e per il corretto trasferimento dei dati all'utente;

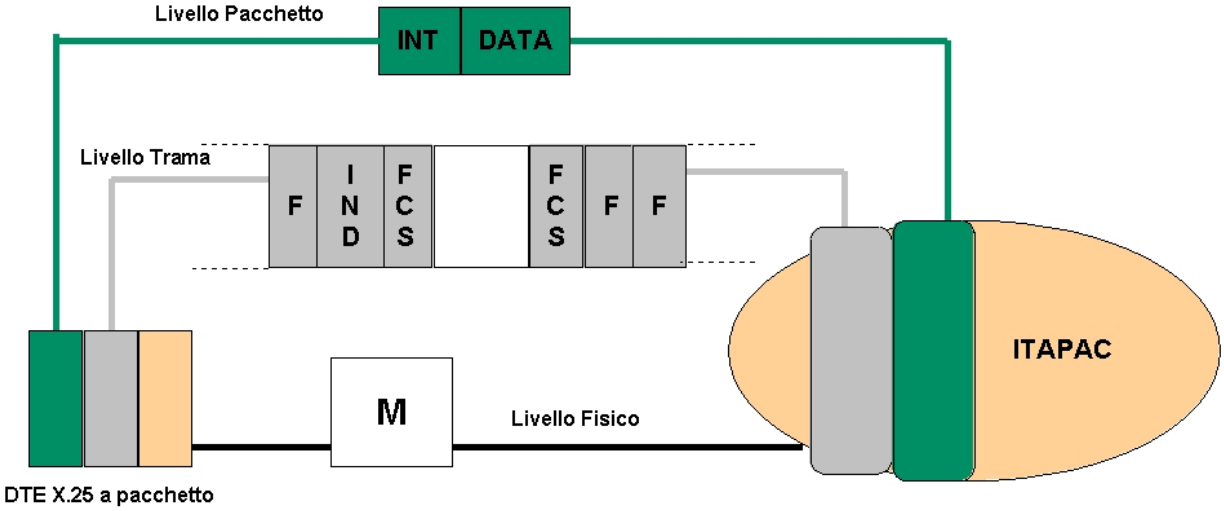
2) LIVELLO TRAMA
Definisce le regole necessarie ad assicurare sia la sincronizzazione della trasmissione, sia la rilevazione – ed il conseguente recupero – di eventuali errori presenti sui dati trasmessi;

3) LIVELLO FISICO
Definisce i criteri di controllo da parte del DTE riguardanti il funzionamento del DCE, ovverosia del modem e della linea fisica di collegamento ad Itapac.

Lo schema della pagina seguente riassume graficamente quanto sopra esposto.

SCHEMA N. 2

X.25 e Livello Fisico, Livello Trama, Livello Pacchetto



Legenda

INT	=	Intestazione del pacchetto
F	=	Flag
IND	=	Campo Indirizzo
C	=	Campo Controllo
FCS	=	Frame Check Sequence (sequenza di controllo della trama)
M	=	Modem Utente o DCE se su accesso numerico (CDN)

1 - LIVELLO PACCHETTO

Un circuito virtuale può essere di due tipi:

- **PERMANENTE** (**PVC**, Permanent Virtual Call/Circuit), se la rete X.25 mantiene una connessione fissa tra 2 DTE;
- **COMMUTATO** (**VC**, Virtual Call/Circuit), se la rete procede a stabilire la connessione e la disconnessione in seguito alla richiesta del DTE. Viene altresì identificato come **S**VC.

I circuiti virtuali vengono multiplexati sul circuito fisico di accesso e sono identificati dal Gruppo di Canale Logico (GCL) e dal Numero di Canale Logico (NCL), i quali sono valori presenti nell'header di ogni pacchetto.
N.B.: GCL e NCL corrispondo, nella definizione internazionale, rispettivamente a LGN e LCN.

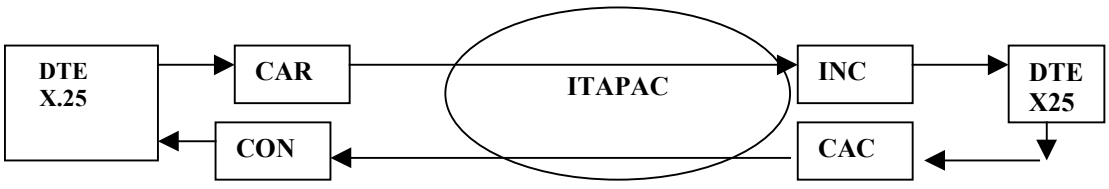
La Raccomandazione CCITT X.25 elenca i seguenti tipi di pacchetti:

TABELLA 2

Descrizione	Denominazione Pacchetto
Richiesta di Chiamata	CAR
Chiamata Entrante	INC
Chiamata Completata	CON
Chiamata Accettata	CAC
Richiesta di Svincolo	CLR
Indicazione di Svincolo	CLI
Conferma di Svincolo	CLC
Dati	D
Interrupt	INT
Conferma di Interrupt	INTC
Pronto a ricevere	RR
Non pronto a ricevere	RNR
Richiesta di Reset	RES
Indicazione di Reset	REI
Conferma di Reset	REC
Richiesta di Restart	RTR
Indicazione di Restart	RTI
Conferma di Restart	RTC

Il seguente flusso illustra il processo di chiamata da un DTE X.25 ad un altro, con le quattro fasi (2 per ogni DTE) di Richiesta di Chiamata (1-CAR), Notifica Chiamata Entrante (2-INC), Accettazione di chiamata (3-CAC) e Chiamata Completata (4-CON). Chi "parla" TCP/IP vedrà in queste fasi una forte analogia con il three-way handshake del TCP.

SCHEMA N. 3



Non sempre, ovviamente, una chiamata X.25 giunge a buon fine: i seguenti codici di errore, riportati per comodità anche in binario, elencano le motivazioni di "chiamata non completata" generalmente presenti sulla rete. Nella sezione pratica vedremo come questi codici di errore vengono presentati dal PAD all'utente X.25/X.28C.

TABELLA 3

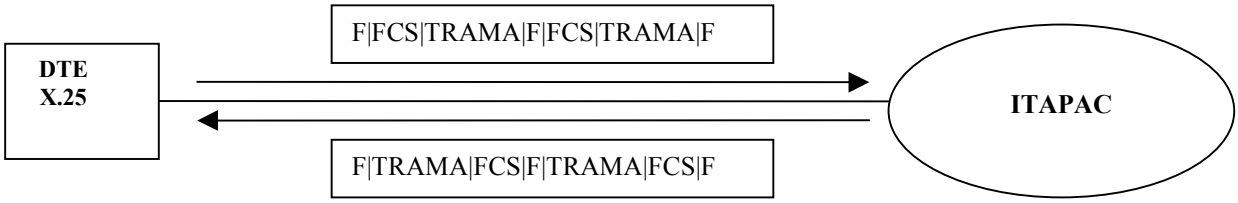
Causa dello Svincolo	Codifica Binaria
Svincolo o Restart del DTE	00000000
DTE chiamato Occupato	00000001
DTE fuori Servizio	00001001
Errore di Procedura del DTE Remoto	00010001
Tassazione al Chiamato non concessa (No Reverse Charge)	00011001
Chiamata non Valida	00000011
Accesso Non Consentito (Barred)	00001011
Errore di Procedura Locale	00010011
Congestione di Rete	00000101
DTE non Raggiungibile	00001101
Destinazione Incompatibile	00100001

2 - LIVELLO TRAMA

Il compito del protocollo a livello trama è quello di fornire un meccanismo per il corretto trasporto dei pacchetti sulla linea d'accesso alla rete X.25. Viene utilizzato il protocollo LAPB, basato su HDLC (ISO): con questa procedura il terminale e la rete possono generare sia comandi che risposte.

La trasmissione dei dati avviene in trame, ognuna contraddistinta da una sequenza di bit di apertura e di chiusura (FLAG). Ogni trama contiene un campo di controllo (FCS) che permette di rivelare eventuali errori di trasmissione.

SCHEMA N. 4



Legenda

F	=	Flag
FCS	=	Frame Check Sequence (sequenza di controllo della trama)

3 - LIVELLO FISICO

I DTE X.25 possono collegarsi alla rete X.25 tramite circuiti diretti analogici o numerici (CDA o CDN), alle velocità di 2400, 4800, 9600, 48000 e 64000 bit/s, come illustrato nella tabella seguente.

TABELLA 4

Velocità DTE X.25	Circuito di Accesso	Standard di Riferimento
2400 bit/s	CDA	V26 o banda base
2400 bit/s	CDN	X21 bis
4800 bit/s	CDA	V27 bis o Banda Base
4800 bit/s	CDN	X21 bis
9600 bit/s	CDA	V29 o Banda Base
9600 bit/s	CDN	X21 bis
48000 bit/s	CDN	X21 bis o X21
64000 bit/s	CDN	X21 bis o X21

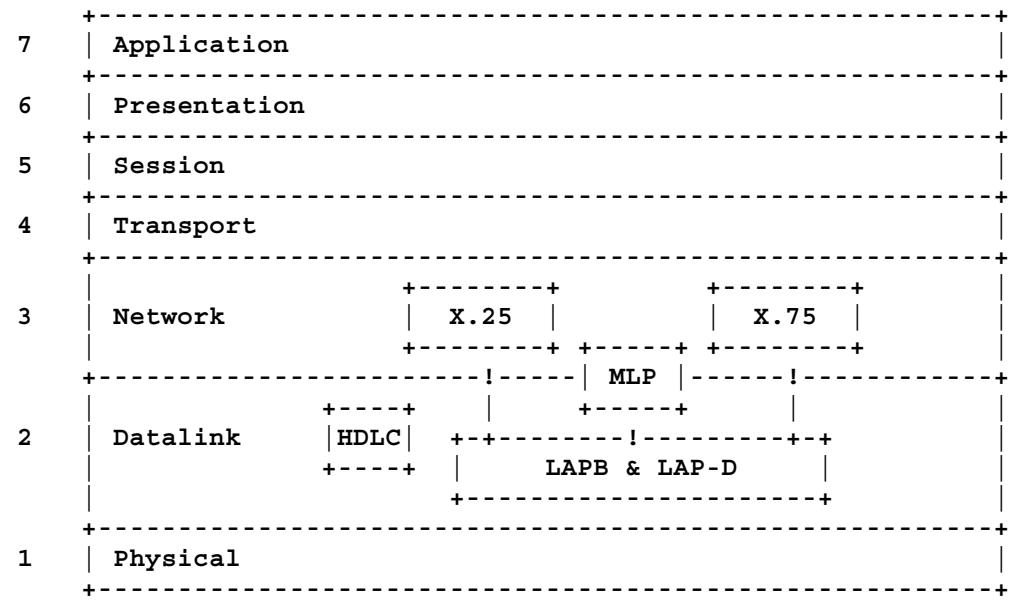
***

VII) X.25: Overview dei protocolli a basso livello

1 - INTRODUZIONE

Cerchiamo di introdurre in breve i protocolli a basso livello che permettono il funzionamento delle reti X.25, estraniandoci per un attimo a livello di visione da ciò che è la rete ITAPAC ed applicando un'analisi generale.
Lo standard X.25 definisce protocolli sia a datalink-layer che a network-layer del modello ISO/OSI, come si vede nello schema seguente:

SCHEMA N. 5



Tralasciando il physical-layer (differenziato in X.25.1, X.21, X.21bis, V.24, V.35) esaminiamo i protocolli a datalink-layer piu' comunemente utilizzati.

In seguito analizzeremo l'X.25 Packet Layer Protocol (PLP), che si posiziona a network-layer.

***

2 – PROTOCOLLI A DATALINK-LAYER (X.25.2)

I protocolli al livello 2 dello stack ISO/OSI permettono la trasmissione di pacchetti X.25 PLP attraverso connessioni LAN e WAN. Quelli piu' comuni, che esamineremo nel dettaglio, sono:

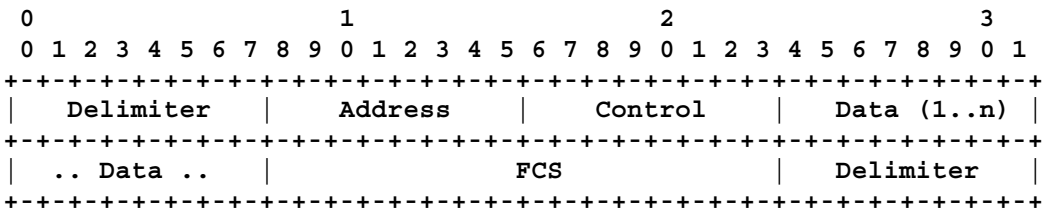
a) LAPB (Link Access Protocol Balanced)
b) LAP-D (Link Access Protocol for D-channel)
c) LAP-M (Link Access Protocol for Modems)
d) MLP (Multi-Link Procedure)
e) LLC (Logical Link Control)

a) LAPB

LAPB e' il protocollo a datalink-layer piu' comunemente utilizzato per X.25.
Si tratta di un protocollo point-to-point derivato da HDLC, come molti dei protocolli attualmente in uso per LAN e WAN full-duplex.

LAPB e' disponibile in diverse varianti; per brevita' ci limitiamo ad analizzare solamente il formato di base del frame LAPB (in modulo 8), che ha la seguente struttura:

SCHEMA N. 6



- I campi Delimiter sono sempre settati alla sequenza di bit 0x7E (01111110 in binario) e sono utilizzati per delimitare l'inizio e la fine di un frame LAPB. Ovviamente per prevenire l'eventualita' che tale sequenza appaia in altri campi del frame la stazione trasmettente utilizza una forma di "escaping": in pratica, viene inserito uno zero in piu' ogni volta che appare una sequenza di 5 bit contigui settati ad 1.
- Il campo Address e' un'eredita' diretta di HDLC, ma poiche' LAPB come si e' detto e' un protocollo point-to-point gli unici valori validi sono 0x01 (che denota i comandi DTE->DCE e le risposte DCE->DTE) e 0x03 (che invece denota i comandi DCE->DTE e le risposte DTE->DCE).
- Il campo Control identifica il tipo di frame.
- I dati incapsulati all'interno di LAPB (campo Data) possono avere lunghezza arbitraria, con un padding di zeri ad un multiplo di 8 bit.
- Il campo FCS (Frame Check Sequence) e' un CRC a 16-bit, calcolato secondo le specifiche ITU-T X.25.

Il formato descritto da' origine alle seguenti classi fondamentali di PDU all'interno di LAPB:

- ***Information***, costituita dai dati stessi incapsulati nel frame (il campo di controllo contiene il numero di sequenza del frame).
- ***Supervisory*** (anche questo tipo di frame contiene i numeri di sequenza).

- RR (Receive Ready): frame di ACK che comunica la disponibilita' a ricevere il prossimo frame.
- REJ (Reject): frame di NAK utilizzato per indicare una condizione di errore nella trasmissione dei dati.
- RNR (Receive Not Ready): si tratta di una forma di controllo del flusso della comunicazione (il peer puo' non essere temporaneamente in grado di ricevere dati).

- ***Unnumbered*** (qui il numero di sequenza non e' presente).
  - DISC (Request Disconnection).
  - DM: risposta a DISC, che indica che la disconnessione sta per avere luogo.
  - FRMR: Frame Reject.
  - UA: frame di ACK.
  - SABM: codice di inizializzazione dell'async balanced mode.
  - SABME: codice di inizializzazione dell'async balanced extended mode, utilizzato in alcune varianti di LAPB come LLC e LAP-D).

Oltre a quelle menzionate, esistono altre tipologie di PDU: esse sono comunque tutte riconducibili alle tre classi Information, Supervisory e Unnumbered gia' individuate.

LAPB e' utilizzato su link X.21 e V.24 (con velocita' massima di 64Kbps).
A causa della sua natura point-to-point esso non puo' essere impiegato con ISDN o Ethernet: e' qua che entrano in gioco LAP-D e LLC.

b) LAP-D
L'unica differenza tra LAP-D e LAPB standard e' nella lunghezza del campo Address. LAP-D utilizza infatti indirizzi a 16-bit (e non a 8 come nel caso di LAPB): 6 bit sono utilizzati per il Service Access Point Identifier (SAPI) e 7 bit sono utilizzati per il Terminal Endpoint Identifier (TEI).
Il protocollo LAP-D specifica il formato di frame utilizzato per la trasmissione dei messaggi su ISDN canale D.

c) LAP-M
Il Link Access Procedure for Modems (LAP-M) e' il protocollo specificato nella recommendation ITU V.42, per implementare la correzione di errore con i modem. Si tratta di un protocollo bit-oriented basato su HDLC, come gli altri della famiglia LAPB.

d) MLP
La Multi-Link Procedure (MLP) e' un'estensione di LAPB che permette l'utilizzo di link fisici multipli, analogamente a quanto accade quando si utilizzano device hardware dedicati per il multiplexing. MLP consente l'aggregazione di piu' link fisici all'interno di un unico link logico, al datalink-layer.

e) LLC
Il Logical Link Control (LLC) e' un protocollo dello standard IEEE Local Area Network (LAN) che consente la trasmissione di pacchetti X.25 attraverso un canale LAN.

***

3 - PROTOCOLLI A NETWORK-LAYER (X.25.3)

Dopo la rapida overview della famiglia di protocolli LAPB, analizziamo finalmente il protocollo X.25 vero e proprio. Consideriamo X.25 in termini di indirizzamento (standard ITU X.121), PDU, sequenza e transizione di stato.

Nell'ordine, affronteremo i seguenti argomenti:

a) PLP (X.25 Packet Layer Protocol)
b) PVC (Permanent Virtual Circuit) e SVC (Switched Virtual Circuit)
c) VCI (Virtual Channel Identifier)
d) Call Setup
e) Indirizzamento X.121 e LCN

a) PLP
PLP ha sostanzialmente 2 ruoli principali:

1) Multiplexing dei circuiti virtuali su rete a commutazione di pacchetto
2) Switching/routing dei circuiti virtuali tra i nodi all'interno della WAN

PLP, come si nota, non specifica protocolli a livello di trasporto o di applicazione.

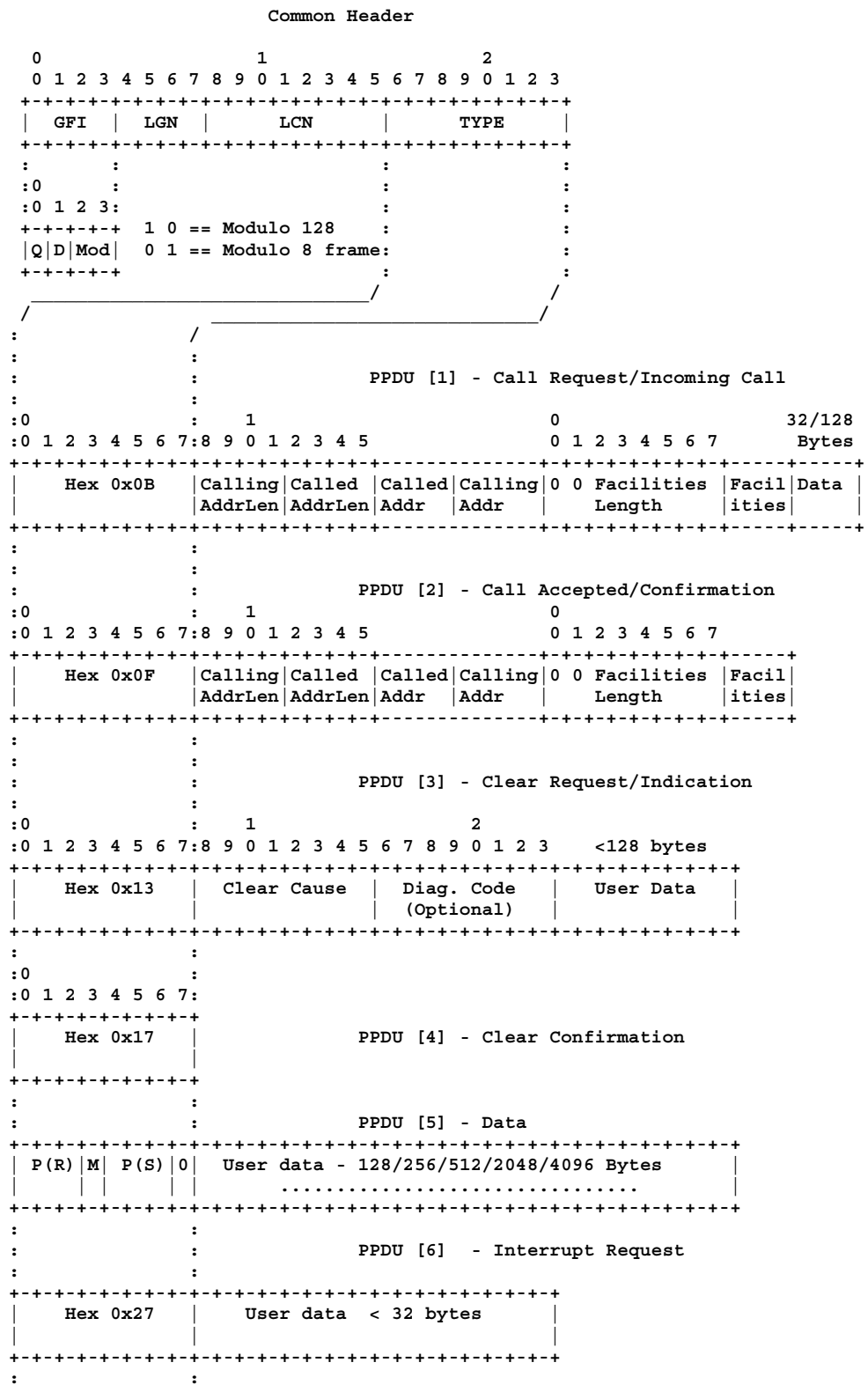
La tabella seguente schematizza le classi di PPDU (PLP PDU):

SCHEMA N. 7

Kind	Direction	
	DTE->DCE	DCE->DTE
Call Setup	1 Call Request	~1 Incoming Call
	2 Call Accepted	~2 Call Confirmation
Call Clearing	3 Clear Request	~3 Clear Indication
	4 DTE Clear Confirmation	~4 DCE Clear Confirmation
Data Transfer	5 DTE Data	~5 DCE Data
	6 Interrupt Request	~6 Interrupt Confirmation
Flow Control	7 DTE Receiver Ready	~7 DCE Receiver Ready
	8 DTE Receiver Not Ready	~8 DCE Receiver Not Ready
	9 DTE Reject	~9 n/a
	A Reset Request	~A Reset Indication
	B DTE Reset Confirmation	~B DCE Reset Confirmation
Resync	C Restart Request	~C Restart Indication
	D DTE Restart Confirmation	~D DCE Restart Confirmation
Network Error Reports	E Diagnostic	~E Diagnostic

Le PPDU appartenenti alle classi descritte nella tabella hanno il formato espresso nello schema seguente:

SCHEMA N. 8



```
+-+-+-+-+-+-+-+-+
|    Hex 0x27   |              PPDU [~6] - Interrupt Confirmation
|               |
+-+-+-+-+-+-+-+-+
:               :
+-+-+-+-+-+-+-+-+
| P(R)|0 0 0 0 1|              PPDU [7] - Receiver Ready
|     |         |
+-+-+-+-+-+-+-+-+
:               :
+-+-+-+-+-+-+-+-+
| P(R)|0 0 1 0 1|              PPDU [8] - Receiver Not Ready
|     |         |
+-+-+-+-+-+-+-+-+
:               :
+-+-+-+-+-+-+-+-+
| P(R)|0 1 0 0 1|              PPDU [9] - Reject
|     |         |
+-+-+-+-+-+-+-+-+
:               :
:               :              PPDU [A] - Reset Request
:0              :    1                   2
:0 1 2 3 4 5 6 7:8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Hex 0x1B   |  Reset Cause  | Diag. Code    |
|               |               | (Optional)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:               :
:0              :
:0 1 2 3 4 5 6 7:
+-+-+-+-+-+-+-+-+
|    Hex 0x1F   |              PPDU [B] - Reset Confirmation
|               |
+-+-+-+-+-+-+-+-+
:               :
:               :              PPDU [C] - Restart Request
:               :
:0              :    1                   2
:0 1 2 3 4 5 6 7:8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Hex 0xFB   |  Reset Cause  | Diag. Code    |
|               |               | (Optional)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:               :
:0              :
:0 1 2 3 4 5 6 7:
+-+-+-+-+-+-+-+-+
|    Hex 0xFF   |              PPDU [D] - Restart Confirmation
|               |
+-+-+-+-+-+-+-+-+
:               :              PPDU [E] - Diagnostic
:               :
:0              :    1                   2
:0 1 2 3 4 5 6 7:8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Hex 0xF1   |  Diagnostic   | Explanation   |
|               |  Code         |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- GFI: Group Format Identifier
- LGN: Logical Group Number
- LCN: Logical Channel Number
- TYPE: Specificato per ogni numbered PDU

b) PVC e SVC

X.25 offre servizi orientati al virtual circuit su di un network layer a commutazione di pacchetto, simile a quello della linea telefonica PSTN.

Per questo motivo e' necessario fornire un meccanismo per il call setup, applicabile unicamente agli Switched Virtual Circuits (SVC).

X.25, inoltre, prevede anche il supporto per Permanent Virtual Circuits (PVC): si tratta di VC a cui e' gia' stato assegnato un VCI (Virtual Channel Identifier) permanente, per cui non si ha la necessita' di una procedura di call setup.

c) VCI

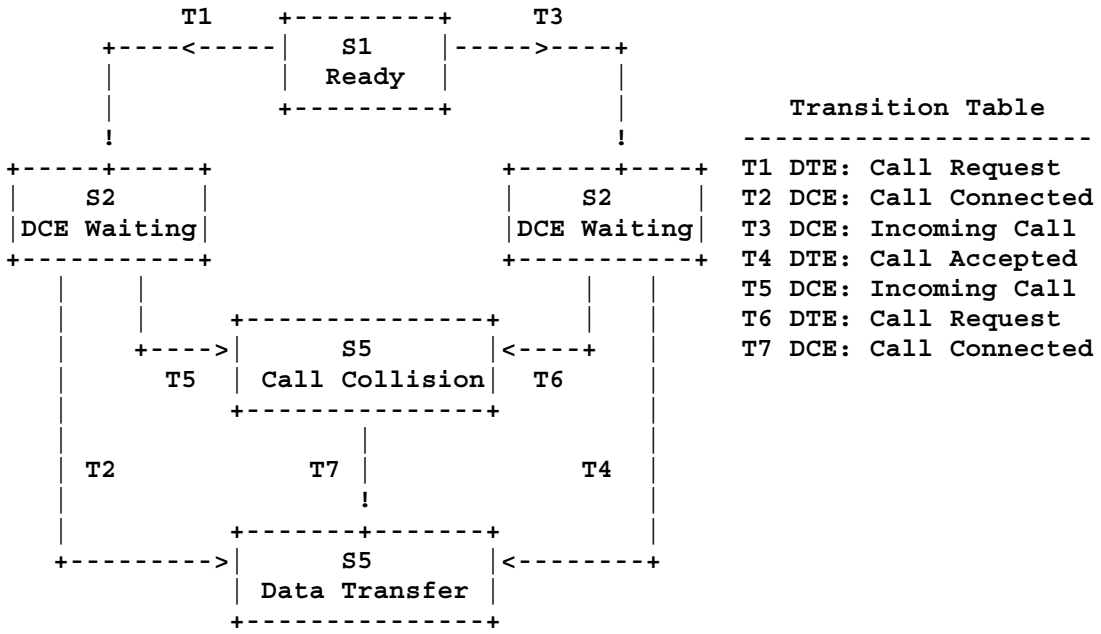
Come abbiamo visto, tutte le PPDU X.25 sono lunghe almeno 3 ottetti. La tupla composta da Logical Channel Number (LCN) e Logical Group Number (LGN) specifica l'SVC o il PVC a cui la particolare PDU si riferisce. L'LGN e' lungo 4-bit, mentre l'LCN misura 8-bit: la dimensione totale della tupla e' pertanto di 12-bit, che si traducono in 4096 possibili valori differenti.

Tale tupla viene comunemente chiamata con il nome di Virtual Channel Identifier (VCI). Sta all'amministratore di rete definire quali valori di VCI fanno riferimento ad un PVC e quali invece si riferiscono ad un SVC.

d) Call Setup

Il diagramma di stato della pagina seguente illustra la procedura di call setup:

SCHEMA N. 9



e) Indirizzamento X.121 e LCN

Le reti X.25 utilizzano l'indirizzamento specificato nella recommendation ITU X.121. A network layer ogni nodo della rete ha un suo indirizzo X.121, conosciuto comunemente con il nome di Network User Address (NUA). Piu' che ad indirizzi IP, i NUA sono accomunabili a numeri telefonici della rete PSTN.
L'LCN (Logical Channel Number), invece, puo' essere considerato come analogo delle porte TCP o UDP al transport-layer dello stack ISO/OSI, nella suite di protocolli TCP/IP.

L'indirizzo X.121 canonico assegnato ad un nodo X.25 DTE/DCE, al quale ITU si riferisce con il termine "International Data Number", e' dato dal DNIC (Data Network Identification Code) insieme con il Network Terminal Number (NTN). Ancora una volta, e' lampante l'analogia con la rete telefonica: non e' necessario comporre il prefisso della nazione se non si sta facendo una chiamata internazionale.

E' interessante osservare come X.25 non soffra del problema di carenza di indirizzi come accade per IPv4 (che ha solo 32-bit a disposizione per l'indirizzamento); le raccomandazioni ITU E.146 e X.121, inoltre, definendo una sorta di gerarchia di indirizzi basata sui country codes permettono un routing delle comunicazioni piu' efficiente. Ovviamente qualcuno potrebbe affermare che uno dei punti di forza del protocollo IP e' proprio la mancanza di uno schema di indirizzamento gerarchico... Non e' questa la sede per le guerre di religione, l'importante e' comprendere le profonde differenze tra le due tipologie di rete.

Prima di passare a parlare del transport-layer e della TPDU, soffermiamoci un momento sugli LCN, a cui abbiamo gia' fatto accenno. Come accade anche per gli indirizzi IP, i NUA costano e pertanto e' perfettamente possibile che una societa' scelga di utilizzare uno stesso NUA per piu' nodi X.25.
Esiste infatti la possibilita' di specificare in questi casi un Logical Channel Number direttamente attraverso il pad: e' qui che la differenza tra DTE e DCE si fa notare in maniera particolare.
Il DCE e' responsabile per il routing della chiamata remota, eseguito tramite il mapping dell'LCN su di un device fisico.

In conclusione, l'LCN e' cio' che rende possibile il subaddressing sulle reti X.25.

Ma come viene codificato un NUA all'interno della PPDU di Call Request?
Si utilizza la vecchia codifica BCD (Binary Coded Decimal), che rappresenta le cifre decimali (0-9) su 4-bit: si tratta di un codice molto semplice da gestire in elettronica, anche se ha il difetto di sprecare i pattern di bit che si riferiscono alle cifre esadecimali A-F. Si noti come nella PPDU gli indirizzi del chiamato e del chiamante siano preceduti da 2 campi che ne specificano la lunghezza, di 4-bit ognuno. Cio' rende possibile la specifica di indirizzi lunghi fino a 15 cifre (anche se in pratica solitamente vengono utilizzate solo 14 cifre per gli indirizzi X.121).

***

4 – PROTOCOLLI A LAYERS SUPERIORI

Storicamente, X.25 e' stata utilizzata con protocolli di trasporto OSI (TP0-TP4). Altri protocolli a livelli superiori sono stati specificati per l'utilizzo su reti X.25: tra di essi ricordiamo T3POS (utilizzato sui sistemi per l'autorizzazione dei pagamenti via bancomat e carta di credito), IODETTE FTP (usato per il trasferimento di informazioni, in maniera particolare dalle industrie di automotive francesi e tedesche, ma presente anche in Italia) e OSI VT (si tratta del servizio di terminale virtuale per la suite di protocolli OSI, quasi analogo al telnet). Stiamo ovviamente parlando di protocolli ad application-layer.

Poiche' X.25 specifica un network-layer point-to-point, affidabile e stream-oriented, molte applicazioni non richiedono un ulteriore protocollo di trasporto (TPDU). Questo e' il caso, ad esempio, di una sempice connessione end-to-end in stile "data pipe", che puo' o non puo' a seconda dei casi utilizzare dei codici di controllo per il terminale compatibili con il DTE utilizzato.

Prima di concludere questa breve panoramica sui protocolli di X.25, accenniamo rapidamente al funzionamento del routing e delle user facilities:

a) X.25 Routing
b) X.25 User Facilities

Le due seguenti sottosezioni trattano separatamente questi due argomenti.

***

a) X.25 Routing

Al contrario di quanto avviene su network-layer IP, i frames X.25 PLP non contengono il NUA chiamato. In altre parole, se su Internet ogni datagramma IP contiene le informazioni relative alla propria sorgente e alla propria destinazione, le PPDU contengono solamente il VCI: il NUA chiamato, infatti, e' presente solamente all'interno delle PPDU preposte al Call Setup.

Cio' significa che esiste la necessita' di mantenere un mapping NUA-VCI per assicurare il routing X.25: e' compito degli stacks X.25 residenti sugli end hosts mantenere queste informazioni. Su alcune piattaforme e' possibile effettuare una query sullo status dei VCI correnti, con un comando analogo a netstat (x25stat su HP-UX).

b) X.25 User Facilities

Nelle recommendations ITU piu' volte citate nel corso del documento e' prevista l'esistenza di "User Facilities", che possono essere disponibili su una rete a commutazione di pacchetto X.25. Su reti differenti potranno esserci User Facilities diverse, con utilizzi e formati specifici.

Alcune di esse sono di particolare interesse dal punto di vista della sicurezza e sono descritte brevemente in seguito:

- ***Network User Identification*** (NUI). Il NUI non e' mai trasmesso al nodo remoto: esso viene tipicamente verificato dagli switch presenti nella rete PSN utilizzata. Il formato di NUI varia generalmente da rete a rete.

- ***ROA Selection***. Opzione che ricorda il loose source routing del mondo IP: grazie alla ROA Selection e' infatti possibile controllare il call routing.
- ***Call Redirection***. Come avviene su IP (anche se probabilmente l'analogia piu' corretta e' ancora una volta quella con la rete PSTN), e' possibile effettuare delle redirezioni di chiamate.
- ***Hunt Group***. Si tratta di una sorta di NAT, che in pratica permette di effettuare il load balancing delle chiamate ricevute su un NUA particolare, mappandole su DTE/DCE appartenenti allo stesso gruppo. Anche l'Hunt Group e' eredita' del mondo telefonico (cfr. Hunt Groups su PBX).
- ***Mnemonic Codes***. Alcune reti X.25 (tipicamente nordamericane: Tymnet, SprintNet, ADP/AutoNet, etc..) forniscono al subscriber la possibilità di specificare dei codici mnemonici alfanumerici, i quali hanno una corrispondenza con indirizzi X.25 (NUA), per facilitare le operazioni di connessione da dialup X.28 o gateway ACP (PAD) X.28 (cfr. 031069 Tymnet-gw).

5 – RIFERIMENTI

- Libnet-X.25: The Preamble, da cui sono stati tratti gli schemi.
- Protocol Vulnerabilities within the X.25 Networking suite.
- X.25 Standards and ITU Recommendations (http://www.itu.int).
- X25US (http://www.x25us.net/).

SECONDA PARTE, SEZIONE PRATICA

I) Sezione Pratica (1 di 5)

1 – SICUREZZA E PERFORMANCE: X.25 VS. TCP/IP

Dopo aver letto la storia ed aver appreso il funzionamento tecnico di una rete X.25, cerchiamo di capire perché le aziende dovrebbero scegliere una rete di comunicazioni dati basata sul protocollo X.25 invece che restarsene su Internet dove, oggigiorno, già si trovano. Ho evidenziato quattro punti che ritengo basilari per un confronto tra le due tecnologie: Sicurezza, Costi, Affidabilità, Varietà di Sistemi Operativi.

Analizziamoli nel dettaglio.

a) SICUREZZA

Piuttosto che definire le reti X.25 *sicure*, direi invece che Internet è *insicura*. Il TCP/IP e Unix portano ad azioni interattive non solo tra un gran numero di server, ma anche e soprattutto tra un gran numero di applicazioni.. questo fa sì che, bene o male, chiunque possa fare hacking sulla rete Internet. X.25 è un protocollo di trasmissione più "povero" ed è stato disegnato per l'interazione con altri sistemi attraverso un Login Server, o comunque attraverso qualcosa di molto simile al protocollo

Telnet nel TCP/IP. Proprio per questo motivo transazioni come quelli dei POS (EFTPOS) avvengono su X.25 e non su Internet.

Generalmente, come detto all'inizio di questo documento, gli hacker dei giorni nostri – così come i programmatori degli ultimi anni – non sanno accedere, utilizzare e fare hacking su X.25, rendendo molto più difficile episodi di intrusione informatica.
Infine una regola non scritta di X.25 è che, al contrario di Internet, non esistono elenchi pubblici con gli indirizzi delle utenze collegate alla rete e, di conseguenza, non è possibile trovare l'azienda XYZ collegata ad Itapac se non effettuando uno scan totale della rete X.25 italiana: ciò comporta un enorme tempo-uomo, una connessione dialup prolungata (la quale può presentare il pericolo di un tracciamento della chiamata ed identificazione dell'attaccante che sta abusando delle risorse di rete o utilizzando una NUI rubata) oppure un accesso ad un sistema collegato ad X.25 come DTE X.25. Anche in quest'ultimo caso accade spesso che, dopo N azioni di scanning sulla rete, il proprietario dell'utenza X.25 (così come nel caso di abuso di NUI X.28) rilevi gli improvvisi ed alti costi e si accorga dell'intrusione avvenuta e delle continue chiamate X.25 ad altri DTE remoti.

Una curiosità: l'unica rete X.25 al mondo dove ho trovato un elenco pubblico di utenze X.25 è RABMN (India), con DNIC 4041.

Quello che segue è un piccolo estratto del servizio informativo, funzionante sino al 1995 e rimosso successivamente, in quanto gli hacker che ne vennero a conoscenza (ben pochi, dato che l'India è un paese molto lento da scannare) violarono sistematicamente tutti i sistemi collegati, avendo l'enorme vantaggio di sapere *chi* stavano "bucando" ed utilizzare quindi una sorta di "social engineering" a monte verso il sistema target.

$ set h /x /fast 0404311002013

PAD-I-COM: Call Connected

Inet DIRECTORY ENQUIRY SERVICE

DIRECTORY ENQUIRY SERVICE ___NMC VER 2 ___ NETWORK : RABMN, INDIA PAGE 0

NETWORK #	NAME / ORGANISATION	LOCATION
404100000162	A C C	WADI
404100010681	A C C	BILASPUR
404100000589	A C C	BOMBAY
404100000381	A C C	CHAIBASA
404100000055	A C C	JAMUL
404100000420	A C C	KYMORE
404100010162	A C C	WADI
404100010589	A C C	BOMBAY
404100010626	A P RAYONS	KAMALAPURA
404100010625	A P RAYONS	HYDERABAD
404100000172	ANAND BAZAR PATRIKA	BOMBAY
404100010882	ANAND BAZAR PATRIKA	CALCUTTA
404100000362	ANAND BAZAR PATRIKA	NEW DELHI
404100010172	ANAND BAZAR PATRIKA	BOMBAY
404100000821	B A R C	BOMBAY
……..	……	……..
……..	……	……..

…….. …… ……..

Da notare anche come, in seguito a questa scoperta, furono violate le sedi indiane di aziende quali Digital, Nestle, Glaxo, etc…

Ritengo molto importante, per chi si occupa professionalmente di sicurezza informatica, sottolineare come, spesso, networks mondiali appartenenti a grandi gruppi privati siano stati violati proprio passando dalle filiali situate in paesi remoti dove, in genere, la concezione di "sicurezza" è estremamente più bassa rispetto alla casa madre. Chi ha letto il libro "Cyberpunk: Outlaws and hackers on the computer frontier", di Kathie Hafner e John Markoff, ricorderà la mitica intrusione alla DEC (Digital Equipment Corporation) di Singapore, dove un hacker tedesco di nickname "Pengo" del CCC copiò un tool interno, riservatissimo, della Digital, chiamato SecurePack e lo vendette al KGB nel 1988, prima della caduta del Muro di Berlino.

b) COSTI

In talune, specifiche occasioni le reti X.25 possono essere più cost-effective rispetto ad Internet: alcuni esempi possono essere le applicazioni EDI[10], query e relative risposte, update di database, transazioni dirette "on the fly" e, sotto certi punti di vista, le comunicazioni via posta elettronica. Le transazioni Business to Business continuano ad essere spesso eseguite su reti X.25 invece che su Internet, sebbene in questo ultimo periodo la tendenza sia di spostare tutto sulla grande Rete. Infine le trasmissioni su reti X.25 sono soggette a minori errori di trasmissione, data l'eccellente qualità del controllo errori.

c) AFFIDABILITA' (RELIABILITY)

Il protocollo X.25, non necessitando di un Layer 4 di trasporto per il controllo della qualità del dato, offre di default comunicazioni affidabili, con una bassissima (ove esistente) percentuale di errore.
Questo si traduce nella possibilità di dialogo tra punti differenti nel globo, evitando soluzioni alternative anche in quei paesi dove la qualità delle comunicazioni raggiunge livelli critici.

d) SISTEMI OPERATIVI DI TUTTI I TIPI [La motivazione dell'hacker ☺]

Su X.25 si trovano i sistemi operativi e le piattaforme hardware più disparate, il che significa la possibilità di imparare (let's "put the hands on") il funzionamento di PAD X.25, XMUX, AS/400, Unix, VMS, VCX, System32/VOS…. Non è raro trovare NUA che rispondono con modem collegati all'utenza X.25, i quali possono essere utilizzati come dialout e mascheramento sicuro della propria chiamata. Nel libro The Cuckoo's Egg, Tracking a Spy through the Maze of Computer Espionage, un membro del CCC chiamava da Datex-P (X.25 tedesca, DNIC 2624) un gateway Tymnet (USA), da lì si collegava sempre via X.25 ai Livermore Berkeley Laboratory (LBL) ed utilizzava i modem per uscire e chiamare via rete telefonica i dialup di sistemi Unix militari americani, reperiti grazie agli Whois sui .MIL.

[10] EDI, Electronic Data Interchange

2 - DNIC, ZONE AREAS, NUA: X.25 NETWORK ADDRESS FORMAT

La prima conoscenza importante da avere per poter comprendere le reti X.25, sia dal lato hacking che da quello security, è la struttura degli indirizzi X.25 (spesso definiti "X.121" nelle configurazione di router X.25 su geografia mondiale) e la logica di indirizzamento geografico.

Il seguente NUA `026245890040004` viene preso come esempio (Altos Computer Chat System):

```
|\ /|\_ _/|
| | | | | |____ 40004: Indirizzo di Rete
| | | |_|_____  58900: AC di Monaco
| | |___________ 4: DATEX-P Network ("l'Itapac" tedesca)
| |_____________ 262: DCC Germania
|_______________ 0: Estero
```

Come primo esempio ho volutamente preso un NUA tedesco e non uno italiano perché ne "leggo" la struttura un po' diversamente rispetto a quelle straniere. I NUA, infatti, non sempre seguono una logica "ad Area Code" ma, anzi, spesso troviamo reti X.25 con logiche completamente differenti. Come vedremo successivamente possiamo comunque individuare alcune tipologie standard di assegnazione NUA da parte dei differenti carrier X.25, ma per ora comprendiamo con attenzione la struttura dei NUA italiani e prendiamo come esempio un NUA italiano storico, il Politecnico di Torino, nodo POL88B (VAX/VMS):

```
022221122878
|\ /|\_ _/|
| | | | | |____ 22878: Indirizzo di Rete (Trama + Indirizzo Utente)
| | | |_|_____  11: AC di Torino
| | |___________ 2: ITAPAC Network (la rete X.25 ufficiale italiana)
| |_____________ 222: DCC Italia
```

Leggendola in un altro modo abbiamo:

0 222 2 11 22 878 dall'estero;

21122878 dall'Italia.

Lo **0** identifica se la nostra chiamata deve "uscire" dalla rete nazionale e, quindi, chiamare un sistema X.25 estero. E' importante notare come lo 0 sia spesso necessario (ma non in tutti i casi) per chiamare sistemi X.25 situati nello stesso paese ma su reti X.25 differenti: un esempio è ITAPAC, DNIC 2222, verso la rete X.25 di Italcable, DNIC 2227. In questo caso la nostra chiamata da una utenza X.25 ITAPAC sarà infatti 02227NUA.

Non è però sempre lo 0 ad identificare l'uscita internazionale: in alcuni paesi si utilizza il 9 (Portogallo/Telepac, DNIC 2680), in altri il 6 (ex-Yugoslavia/Yugopac, DNIC 2201, Slovenia DNIC 2931…), in altre reti ancora non è richiesto lo zero (USA/Infonet, DNIC 3137, USA/TymNet, DNIC 3106…).

2222 e' il DNIC completo dell'Italia per la rete ITAPAC ed è formato dal DCC (Data Country Code) + l'identificativo della rete X.25 di quel paese, quindi 222 + 2. Ogni stato può infatti avere più di una rete X.25, in paesi come gli USA ne esistono addirittura una trentina e, come vedremo, non è raro trovare lo stesso carrier X.25 presente in più paesi con la **stessa** rete e lo stesso NUA, ma contattabile su DNIC differenti.

11 identifica la zona di Torino. Da notare come, nel caso di NUA X.28 ad accesso commutato (via dialup), l'AC sia preceduto da uno zero, risultando quindi del tipo 201124010. Gli AC in Italia possono essere ad una, due o tre cifre: nel primo caso rientrano Milano (2) e Roma (6), nel secondo città come Genova (10), Bologna (51) e così via mentre nel terzo caso i distretti a tre cifre (generalmente centri più piccoli) quali 961, 422, eccetera.

22 878: l'usanza comune è definire 22878 come indirizzo utente finale, ma chi scrive ha sempre utilizzato un'altra logica, ovverosia vedere **22** come la Trama di Zona ed **878** come l'effettivo indirizzo finale dell'utenza X.25. Questo ragionamento semplifica di molto gli scanning, grazie ad accorgimenti particolari per l'individuazione delle "trame attive".
Se infatti prendiamo un NUA italiano vediamo come segua una prima, importante policy: il NUA è sempre lungo 8 cifre. Una seconda regola è che la grandezza della Trama cambia in funzione della grandezza dell'A.C.: in altre parole, 26100298 ha 6 come A.C. e 100 come Trama, 21122878 ha 11 come A.C. e 22 come Trama mentre 29840111 ha 984 come A.C. e solo 0 come Trama
L'avere una sola cifra come Trama significa che il numero massimo di Trame Attive sarà pari a dieci (da 0 a 9), per un totale di 9.999 possibili NUA: questo semplifica già la scrittura di un NUA Scanner o l'esecuzione fisica di scan automatizzati ma con intervento manuale.
Seguendo questo calcolo i NUA assegnabili sulla zona di Torino saranno 99.999 (99*999) mentre Milano, di controparte, essendo indubbiamente più grande di Torino sia come dimensione che come numero di aziende con necessità di telecomunicazioni (possibile parco utenti per il carrier X.25) potrà assegnare un massimo di 999.999 NUA, quasi un milione di utenze X.25.

In realtà non tutte le Trame sono utilizzate e c'è un modo – su ITAPAC come su altre reti X.25 – di "individuare" le Trame Attive.

Molti carrier X.25 utilizzano infatti dei NUA di servizio, i quali hanno funzioni di test ed erogano in genere i seguenti servizi:

a) **Echo**: invia l'echo di ogni carattere digitato dal DTE remoto;
b) **Drop**: disconnette dopo aver risposto alla connessione;

c) **Traffic Generator**: invia in continuo una frase di test, quale
"*The quick brown fox jumped over the lazy dog 01234567890*"
oppure (secondo standard riscontrato)
"*Traffic Generator (città) (Trama) (Nome rete X.25) pacchetto 1*"
"*Traffic Generator (città) (Trama) (Nome rete X.25) pacchetto 2*"
…….

Nel momento in cui troviamo, effettuando scanning "a caso" o essendo a conoscenza dell'indirizzo, un NUA di test come quelli sopra elencati, possiamo dire di essere ad un buon punto per la comprensione della struttura di indirizzamento della rete X.25 oggetto dei nostri test.
In Italia tali NUA sono posizionati nella Numerazione Finale Utente 997, 998 e 999: ovviamente se la Trama non è attiva non avviene l'attivazione dei NUA di test e servizio. Per far meglio comprendere applichiamo un NUA di servizio alla Trama sulla quale era collegato il Politecnico di Torino.

21122878->21122997.

Sintassi: **211xx997**
Chiamando a mano o modificando un NUA scanner affinchè diventi un "Active Area Scanner" possiamo chiamare tutte le possibili Trame Attive su Torino, lasciando 997 come valore fisso: qualora la rete ci rispondesse con un ACP:COM (connessione avvenuta), un CLR DTE (chiamata rifiutata) o CLR DER (sistema chiamato spento o non collegato) capiremo che la Trama testata in quel momento è attiva, ovverosia possiamo trovare delle utenze X.25 attive.
Individuate delle Trame Attive cambieremo la nostra sintassi, scannando yyy da 000 a 999 per trovare sistemi collegati, dove xx corrisponde ad una della Trame Attive trovate: **211xxyyy**

Ora che abbiamo compreso la struttura dei NUA italiani (quantomeno sulla rete ITAPAC) cerchiamo di capire le Zone Areas e, successivamente, le differenti tipologie di indirizzamento mondiali.

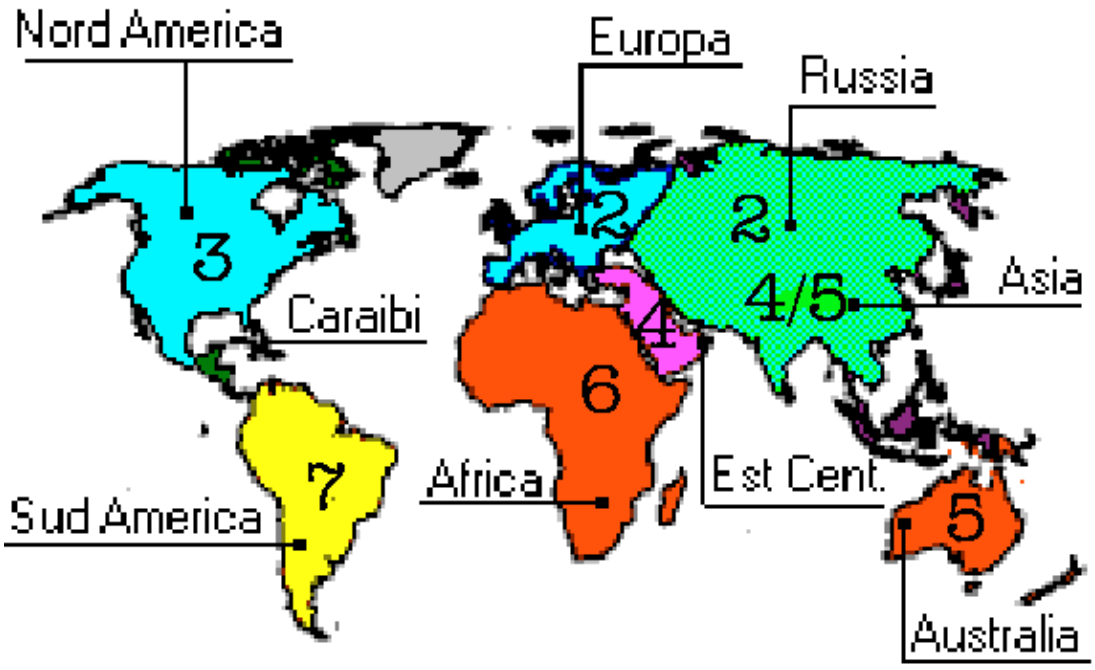
***

3 - ZONE AREAS

Anche se non lo si percepisce immediatamente dopo aver visto alcuni NUA esteri, il mondo è stato diviso a "zone" e comprendendone la suddivisione risulta più facile individuare a prima vista la posizione geografica di un sistema, anche senza consultare elenchi di DNIC.

L'immagine seguente rappresenta visivamente tale suddivisione.

SCHEMA N. 10



La seguente tabella riassume invece le World Zones assegnate.

TABELLA 5

Zona	Continente/Area
1	Connessione Satellitari InmarSAT Voice/Dati(Oceano Atlantico, Pacifico ed Indiano)
2	Europa, Ex URSS
3	Nord America, Centro America, alcune Aree Caraibiche
4	Asia
5	Oceania
6	Africa
7	Parte del Centro America, Caraibi e Sud America

4 – ASSEGNAZIONE DI RETI X.25

Ma chi è a decidere questi Data Country Code ? L'organismo si chiama I.T.U., International Telecommunication Union e ad occuparsene è la Divisione "Telecommunication Standardization Sector" (ITU-T).

Quello che segue è il modulo di richiesta per attivare una rete X.25.

This Notification form should be returned to:

International Telecommunication Union
Telecommunication Standardization Bureau (TSB)
Place des Nations
CH - 1211 Genève 20
Suisse

Telefax:+41 22 730 5853

Our ref: TSB/ARTS

Notification for the assignment of Data Network Identification Codes (DNIC) by the Administrations	
Name and address of Administration :	
DNIC No.:	
Name of network to which a DNIC is allocated :	
Locality of the Network (Country or Geographical Area) :	
Date of application :	
Postal address of the service provider and from which additional information may be requested : Tf: Tlx: Fax:	_____ _____ _____ _____ _____
Your reference :	
Date :	
Signature :	

* Further details, if any, concerning the network for which this DNIC has been assigned may be attached to this form.

5 – ELENCO DEI DCC MONDIALI, SUDDIVISI PER ZONA

ZONA 1

Code	**Country or Geographical Area**
111	Ocean Areas (InmarSAT)

ZONA 2

Code	**Country or Geographical Area**

202	Greece
204	Netherlands (Kingdom of the)
205	Netherlands (Kingdom of the)
206	Belgium
208	France
209	France
210	France
211	France
212	Monaco (Principality of)
213	Andorra (Principality of)
214	Spain
215	Spain
216	Hungary (Republic of)
218	Bosnia and Herzegovina (Republic of)
219	Croatia (Republic of)
220	Yugoslavia (Federal Republic of)
222	Italy
223	Italy
224	Italy
225	Vatican City State
226	Romania
228	Switzerland (Confederation of)
229	Switzerland (Confederation of)
230	Czech Republic
231	Slovak Republic
232	Austria
234	United Kingdom of Great Britain and Northern Ireland
235	United Kingdom of Great Britain and Northern Ireland
236	United Kingdom of Great Britain and Northern Ireland
237	United Kingdom of Great Britain and Northern Ireland
238	Denmark
239	Denmark
240	Sweden
242	Norway
243	Norway
244	Finland
246	Lithuania (Republic of)
247	Latvia (Republic of)
248	Estonia (Republic of)
250	Russian Federation
251	Russian Federation
255	Ukraine
257	Belarus (Republic of)
259	Moldova (Republic of)
260	Poland (Republic of)
262	Germany (Federal Republic of)
263	Germany (Federal Republic of)
264	Germany (Federal Republic of)
265	Germany (Federal Republic of)
266	Gibraltar
268	Portugal
269	Portugal
270	Luxembourg
272	Ireland
274	Iceland
276	Albania (Republic of)
278	Malta
280	Cyprus (Republic of)
282	Georgia (Republic of)
283	Armenia (Republic of)
284	Bulgaria (Republic of)
286	Turkey
288	Faroe Islands
290	Greenland
292	San Marino (Republic of)

293	Slovenia (Republic of)
294	The Former Yugoslav Republic of Macedonia
295	Liechtenstein (Principality of)

ZONA 3

Code	Country or Geographical Area
302	Canada
303	Canada
308	Saint Pierre and Miquelon (Collectivité territoriale de la République française)
310	United States of America
311	United States of America
312	United States of America
313	United States of America
314	United States of America
315	United States of America
316	United States of America
330	Puerto Rico
332	United States Virgin Islands
334	Mexico
335	Mexico
338	Jamaica
340	Guadeloupe (French Department of) and Martinique (French Department of)
342	Barbados
344	Antigua and Barbuda
346	Cayman Islands
348	British Virgin Islands
350	Bermuda
352	Grenada
354	Montserrat
356	Saint Kitts and Nevis
358	Saint Lucia
360	Saint Vincent and the Grenadines
362	Netherlands Antilles
363	Aruba
364	Bahamas (Commonwealth of the)
365	Anguilla
366	Dominica (Commonwealth of)
368	Cuba
370	Dominican Republic
372	Haiti (Republic of)
374	Trinidad and Tobago
376	Turks and Caicos Islands

ZONA 4

Code	Country or Geographical Area
400	Azerbaijani Republic
401	Kazakstan (Republic of)
404	India (Republic of)
410	Pakistan (Islamic Republic of)
411	Pakistan (Islamic Republic of)
412	Afghanistan (Islamic State of)
413	Sri Lanka (Democratic Socialist Republic of)
414	Myanmar (Union of)

415	Lebanon
416	Jordan (Hashemite Kingdom of)
417	Syrian Arab Republic
418	Iraq (Republic of)
419	Kuwait (State of)
420	Saudi Arabia (Kingdom of)
421	Yemen (Republic of)
422	Oman (Sultanate of)
423	Yemen (Republic of)
424	United Arab Emirates
425	Israel (State of)
426	Bahrain (State of)
427	Qatar (State of)
428	Mongolia
429	Nepal
430	United Arab Emirates (Abu Dhabi)
431	United Arab Emirates (Dubai)
432	Iran (Islamic Republic of)
434	Uzbekistan (Republic of)
436	Tajikistan (Republic of)
437	Kyrgyz Republic
438	Turkmenistan
440	Japan
441	Japan
442	Japan
443	Japan
450	Korea (Republic of)
452	Viet Nam (Socialist Republic of)
453	Hongkong
454	Hongkong
455	Macau
456	Cambodia (Kingdom of)
457	Lao People's Democratic Republic
460	China (People's Republic of)
466	Taiwan, China
467	Democratic People's Republic of Korea
470	Bangladesh (People's Republic of)
472	Maldives (Republic of)
480	Korea (Republic of)
481	Korea (Republic of)

ZONA 5

Code	Country or Geographical Area
502	Malaysia
505	Australia
510	Indonesia (Republic of)
515	Philippines (Republic of the)
520	Thailand
525	Singapore (Republic of)
528	Brunei Darussalam
530	New Zealand

534	Northern Mariana Islands (Commonwealth of the)
535	Guam
536	Nauru (Republic of)
537	Papua New Guinea
539	Tonga (Kingdom of)
540	Solomon Islands
541	Vanuatu (Republic of)
542	Fiji (Republic of)
543	Wallis and Futuna (French Overseas Territory)
544	American Samoa
545	Kiribati (Republic of)
546	New Caledonia (French Overseas Territory)
547	French Polynesia (French Overseas Territory)
548	Cook Islands
549	Western Samoa (Independent State of)
550	Micronesia (Federated States of)

ZONA 6

Code	Country or Geographical Area
602	Egypt (Arab Republic of)
603	Algeria (People's Democratic Republic of)
604	Morocco (Kingdom of)
605	Tunisia
606	Libya (Socialist People's Libyan Arab Jamahiriya)
607	Gambia (Republic of the)
608	Senegal (Republic of)
609	Mauritania (Islamic Republic of)

610	Mali (Republic of)
611	Guinea (Republic of)
612	Côte d'Ivoire (Republic of)
613	Burkina Faso
614	Niger (Republic of the)
615	Togolese Republic
616	Benin (Republic of)
617	Mauritius (Republic of)
618	Liberia (Republic of)
619	Sierra Leone
620	Ghana
621	Nigeria (Federal Republic of)
622	Chad (Republic of)
623	Central African Republic
624	Cameroon (Republic of)
625	Cape Verde (Republic of)
626	Sao Tome and Principe (Democratic Republic of)
627	Equatorial Guinea (Republic of)
628	Gabonese Republic
629	Congo (Republic of the)
630	Zaire (Republic of)
631	Angola (Republic of)
632	Guinea-Bissau (Republic of)
633	Seychelles (Republic of)
634	Sudan (Republic of the)
635	Rwandese Republic
636	Ethiopia (Federal Democratic Republic of)
637	Somali Democratic Republic
638	Djibouti (Republic of)
639	Kenya (Republic of)
640	Tanzania (United Republic of)
641	Uganda (Republic of)
642	Burundi (Republic of)
643	Mozambique (Republic of)
645	Zambia (Republic of)
646	Madagascar (Republic of)
647	Reunion (French Department of)
648	Zimbabwe (Republic of)
649	Namibia (Republic of)
650	Malawi
651	Lesotho (Kingdom of)
652	Botswana (Republic of)
653	Swaziland (Kingdom of)
654	Comoros (Islamic Federal Republic of the)
655	South Africa (Republic of)

ZONA 7

Code	Country or Geographical Area
702	Belize
704	Guatemala (Republic of)
706	El Salvador (Republic of)
708	Honduras (Republic of)
710	Nicaragua
712	Costa Rica
714	Panama (Republic of)

716	Peru
722	Argentine Republic
724	Brazil (Federative Republic of)
725	Brazil (Federative Republic of)
730	Chile
732	Colombia (Republic of)
734	Venezuela (Republic of)
736	Bolivia (Republic of)
738	Guyana
740	Ecuador
742	Guiana (French Department of)
744	Paraguay (Republic of)
746	Suriname (Republic of)
748	Uruguay (Eastern Republic of)

6 – COMPRENDERE LA STRUTTURA DI UN NUA

A questo punto, comprese le suddivisioni delle zone mondiali e rimandandovi all'"**Allegato A**" per l'elenco completo dei DNIC mondiali (inclusivi quindi della specifica inerente le differenti reti X.25 di ogni paese) cerchiamo di comprendere le differenti strutture di numerazione mondiali.

In linea di massima possiamo dividere le strutture in:

1) **Area Code Style**
2) **Unknown**

Nel primo caso riscontriamo l'utilizzo degli A.C. all'interno del NUA X.25, mentre nel secondo caso i NUA X.25 sono apparentemente assegnati "a caso" o mediante assegnazione di numerazione progressiva.

Nel primo caso rientrano la maggioranza delle reti X.25, mentre nel secondo network quali TymNet o, molto più spesso, di piccoli paesi (Burundi, Principato del Brunei, etc..).
Una seconda suddivisione che ci è possibile fare riguarda la prima casistica: troviamo reti "**SprintNet like**" e reti "**Itapac like**".

SprintNet (conosciuta anche con il nome di TeleNet) è una rete X.25 statunitense, di proprietà della Sprint Corporation: la esamineremo con attenzione successivamente, quando analizzeremo i c.d. "carrier multi-country", ovverosia quelle reti X.25 dove il DNIC è unico ma le utenze X.25 allacciate appartengono a differenti paesi (utilizzo di sottonumerazione)
Sebbene se le reti SprintNet like ed Itapac like utilizzino un concetto uguale (DNIC + AC + TRAMA + INDIRIZZO FINALE UTENTE) è molto importante differenziarle e capirne le strutture, simili ma non identiche.

SprintNet like: 03110 212 00 xxx
Itapac like: 02222 11 22 xxx

Una prima differenza riguarda l'AC: negli USA gli Area Code sono sempre a tre cifre e, quindi, l'AC del NUA è di conseguenza a 3 cifre; una seconda differenza riguarda invece la Trama, la quale è sempre di due cifre. Come abbiamo visto ITAPAC funziona in un altro modo, variando la dimensione della Trama Attiva, mentre SprintNet ha una lunghezza fissa.

Non è un caso il mio prendere SprintNet come riferimento: essendo uno dei network X.25 più grandi e tra i primi a nascere, le Telecom di altri paesi hanno spesso preso la struttura SprintNet come riferimento per la progettazione della propria sintassi di assegnazione NUA: reti X.25 come quella del Pakistan (4100) – a puro titolo di esempio – utilizzano una struttura identica a SprintNet.

0 4100 111 00 xxx
0 4100 111 14 xxx

"111" è l'A.C. di Islamabad, la capitale, mentre "00" e "14" sono due Trame Attive.
Prendendo invece l'Arabia Saudita come esempio, otteniamo:

0 4201 402 00 002 echo station
0 4201 402 00 003 drop station

Anche l'indirizzamento di Itapac va con i prefissi telefonici in cui l'host si trova, ad esempio 26500153 si trova a Roma, mentre 28181421 è un NUA di Napoli: capiamo quindi come tutti i NUA di Itapac inizino per **2.**

Roma 26**xxx**yyy
Napoli 281**xx**yyy
Ivrea 2125**x**yyy

Le trame possono essere suddivise in aree di 999 indirizzi possibili, per cui Roma avrà 999 trame da 999 indirizzi l'una, Napoli invece avendo un prefisso più lungo avrà un numero di trame minore, 99 trame da 999 indirizzi ed infine Ivrea avrà 9 trame da 999 indirizzi.

Un riassunto definitivo delle differenti tipologie "SprintNet & Itapac like" potrebbe essere:

TABELLA 6

Tipo	Struttura	Nua di Esempio	Stile
A	0 DNIC AC 000 yyy	0 4251 30 000 yyy	Israel like (AC=2/000/yyy)
B	0 DNIC AC xx yyy	0 4100 111 14 yyy	Sprint like (AC=3/xx/yyy)
C.1	0 DNIC AC (xx) yyy	0 2222 11 22 yyy	Itapac style (AC e Trama a lunghezza variabile)
C.2	0 DNIC AC (xxx) yyy	0 2222 6 504 yyy	Itapac style (AC e Trama a lunghezza variabile)
C.3	0 DNIC AC (x) yyy	0 2222 984 x yyy	Itapac style (AC e Trama a lunghezza variabile)

Quando cerchiamo di capire la struttura/sintassi di un network X.25, quindi, è bene effettuare alcune prove utilizzando queste tre logiche principali e ponendo xxx (indirizzo finale utente) come 000, 001, 999, etc..

7 – CODICI DI ERRORE E DI STATO

E' molto importante conoscere i codici di errore più comuni quando si effettuano chiamate X.25, sia per capire il perché della mancata connessione sia per capire – specie durante azioni di scanning – se si sta andando nella direzione giusta o meno. Per inciso, questa sezione si riallaccia all'ultimo schema del LIVELLO PACCHETTO illustrato nella sezione Teorica di questo documento.

Al fine di rendere più utile questo documento di riferimento, ho deciso di elencare due differenti tipologie di risposte e codici di errore: la prima che riassume i codici più tipici, vale a dire i messaggi che effettivamente riscontriamo durante azioni di probing e security attiva, ed una seconda più dettagliata.

La prima casistica può dunque essere un buon riferimento quando si lavora su sistemi operativi connessi direttamente ad X.25 mediante un software PAD montato sulla macchina (PSIPAD su VMS, PADEM su HP/UX, etc..), mentre nel secondo caso sono stati presi di riferimento i messaggi tipicamente riscontrati su PAD X.3/X.28, vale a dire connessioni dialup. In quest'ultimo caso si è preso come riferimento la rete ITAPAC, ma bene o male i PAD X.3 sono abbastanza standard e quindi questi dati si possono applicare anche a PAD di altre reti X.25.

A – Codici di risposta ed errore BASE

COM	Call Connected	Chiamata connessa
NP	NUA Not Present	Indirizzo X.25 chiamato non esistente
DER	Out of Order	Il DTE remoto è spento (ma fisicamente collegato)
OCC	Busy	L'utenza X.25 chiamata non ha VC (Virtual Channel) X.25 liberi
DTE	Dropped by Remote DTE	Chiamata abbattuta dal DTE Remoto. Può voler dire che il DTE richiede subaddress aggiuntivi (da 1 a 2 cifre, 0->9 / 00->99) o che delle ACL[11] ci impediscono di stabilire la sessione col DTE remoto.
RPE	Remote Procedure Error	Il DTE chiamato aspetta informazioni aggiuntive (le c.d. "informazioni opzionali") nel pacchetto X.25. Queste informazioni possono essere subaddress aggiuntivi in forma numerica (generalmente di 3 cifre, ma di regola da 1 a 3) oppure caratteri alfabetici, preceduti in alcuni PAD dalla lettera D o P (25110373DSAM ad esempio, un vecchio chat system italiano). Con la D prima del campo dati i caratteri che seguono vengono visualizzati, con la P avviene un "no echo"
RNA	Reverse not Allowed	Il DTE chiamato non accetta la chiamata a carico (Reverse Charge)

[11] ACL Access Control List, dove vengono definite i NUA per il quale il sistema è autorizzato ad accettare la chiamata X.25.

NA	Access Barred	Il DTE chiamato non accetta la chiamata dal DTE chiamante, ma solo da DTE autorizzati. In questo caso è però il carrier X.25 ad abilitare il servizio ed i singoli DTE autorizzati.

B- Codici di risposta PAD X.3/X.28

La rete può trasmettere un certo numero di segnali, i quali sono suddivisibili in :
a) in risposta ad un comando (modifica dei parametri al PAD X.3, lettura dei parametri, etc..)
b) di propria iniziativa
c) in seguito ad un'azione del DTE remoto.

Abbiamo quindi di conseguenza:
1) Segnali di errore
2) Segnali di disconnessione
3) Segnali di indicazione di reset
4) Segnali del pad per l'Editing (non commentati in questo documento).

***

1) Segnali di Errore

ERR CNA	il comando è sintatticamente corretto ma non è ammesso in questo stato
ERR ILL	il comando non è sintatticamente corretto oppure non è riconosciuto
ERR EXP	la temporizzazione è scaduta e il comando non è stato completato
ERR PNA	il profilo del PAD X.3 non è stato assegnato

2) Segnali di Disconnessione

CLR OCC	il NUA chiamato è occupato in altre chiamate (o non ha VC disponibili)
CLR NC	le condizioni di congestione o di guasto temporaneo all'interno della rete impediscono lo stabilirsi di nuove chiamate virtuali
CLR INV	prestazione richiesta non valida
CLR NA	il DTE chiamante non può ottenere la connessione con il DTE Chiamato (CUG, Closed User Gruppo non compatibile)
CLR ERR	la chiamata è abbattuta a causa di un errore di procedura locale
CLR RPE	la chiamata è abbattuta a causa di un errore di procedura locale del DTE remoto
CLR NP	il NUA chiamato non è assegnato
CLR DER	il NUA chiamato è fuori servizio (spento)
CLR PAD	il PAD ha abbattuto la chiamata in seguito alla ricezione di un invito al "clear" da parte del DTE a pacchetto

CLR DTE	il DTE remoto ha abbattuto la chiamata
CLR RNA	il DTE remoto non accetta chiamate a carico (Reverse Charge)
CLR ID	la modalità di applicazione del protocollo X.29 fra il PAD della rete ITAPAC e il DTE X.25 remoto non è corretta

3) Segnali di Indicazione di Reset

RESET DTE	il DTE remoto ha posto in reset la chiamata virtuale (VC)
RESET RPE	la chiamata è posta in reset per un errore di procedura del DTE remoto
RESET ERR	la chiamata è posta in reset per un errore di procedura locale
RESET NC	la chiamata è posta in reset per congestione all'interno della rete
RESET DER	la chiamata è posta in reset per fuori servizio del DTE remoto
RESET NOP	la chiamata è posta in reset in quanto la rete riprende servizio
RESET DOP	la chiamata è posta in reset in quanto il DTE remoto riprende servizio

8 – RETI X.25 A DNIC UNICO SU PAESI ESTERI & INTL. REVERSE CHARGE

Come accennavo prima SprintNet è una delle reti X.25 più complesse e diffuse al mondo in quanto, oltre ad offrire connettività negli USA diventando quasi una sorta di Virtual POP e di gateway per diverse aziende, fornisce connettività internazionale in altri paesi.
Il modo in cui lo fa è però un po' complicato, dato che utilizza indifferentemente il DNIC ufficiale di SprintNet o il DNIC del carrier X.25 con il quale SprintNet ha effettuato gli accordi.

Per rendere meglio l'idea prendiamo un sistema collegato a USA/SprintNet e lo stesso sistema con l'abilitazione a questo strano "roaming" su Australia/OTC[12]:

SprintNet/USA 03110 998 10 224
Australia/OTC 05057 998 10 224

In ambo i casi otterremo un COM, ovverosia una connessione allo stesso sistema.

La stranezza maggiore di questi accordi tra carrier è la possibilità, chiamando un dialup SprintNet (presenti in tutto il mondo sia su numeri urbani che su numeri verdi) di effettuare chiamate X.25 in Reverse Charge anche su altri paesi oltre agli USA, aggirando quindi eventuali ACL, restrizioni di rete, network congestion e, comunque, ottimizzando le velocità di trasferimento dati.

La seguente tabella elenca gli A.C. da me conosciuti per la rete extra-USA SprintNet.

Country	X.121 Address	Country	X.121 Address
Austria	3110 774	New Zealand	3110 998
Australia	3110 968	Norway	3110 767
Canada	3110 568	Puerto Rico	3110 810
Denmark	3110 787	Russia	3110 772
Finland	3110 775	Scotland (U.K.)	3110 778
France	3110 762	Singapore	3110 964
Germany	3110 763	Spain	3110 768
Hong Kong	3110 960	Sweden	3110 787
Ireland	3110 773	Switzerland	3110 770
Italy	3110 764	Taiwan	3110 965
Japan	3110 967	U.K. (England)	3110 771
Kuwait	3110 786	Ukraine	3110 772
Latvia	3110 772		
Netherlands	3110 766		

II) Sezione Pratica: Attacco (2 di 5)

1 – COME ACCEDERE A X.25

Vi sono molteplici modi per accedere a X.25, vediamone qualcuno.

[12] OTC in realtà non è proprietaria dell'intero range sul DNIC 5057, il quale è "sharato" da più carrier. Vedasi l'Allegato B per una descrizione completa della suddivisione.

A) Tramite il dial up di un carrier X.25, ad esempio Itapac (NUI Access)

I dial up di Itapac si chiamano ACP o PAD (Packet Assembler Disassembler) e sono presenti in ogni città italiana.
Per connettersi ad un ACP bisogna usare un programma di emulazione di terminale (Telix, Hyperterminal), settare il modem a 2400 baud 7 bit di dati, nessuno di parità 1 di stop (2400 7N1).
Esempio:

atdt0651558934
Connected 2400/MPN5

ACP Roma Colombo 28
*

Il prompt di Itapac è un asterisco.
Si deve digitare la lettera N (maiuscola) la quale indica che si sta per introdurre il NUI (Network User Identifier), vale a dire la password personale di ogni abbonato Itapac; finito di introdurre il NUI si mette il segno meno "-" e si introduce il NUA: se tutto funziona si ha una risposta di questo tipo:

ACP Roma Colombo 28
*N-0208057040540

ACP:COM

La risposta ACP:COM indica che tutto è andato a buon fine e che il collegamento è stato stabilito; il nostro costo è quello della chiamata urbana verso l'ACP, mentre il traffico x.25 viene invece addebitato al proprietario del NUI.

Come si può vedere il NUI non viene mostrato e l'echo dei caratteri riprende dopo la digitazione del tasto "-" meno.

N.B.: spesso i carrier X.25 particolarmente grandi dispongono di dialup in svariati stati e forniscono il servizio ad utenze internazionali: molti ISP si appoggiano a questa tipologia di servizio per proporre connessioni a 0 scatti (MC-LINK su Itapac, altri su Tymnet/British Telecom, etc..). Può quindi essere utile verificare da web i dialup di vari ISP ed effettuare una verifica incrociata per capire se sono dialup di un carrier X.25.

B) I NUI Itapac

I NUI di Itapac sono lunghi 6 caratteri alfanumerici, cioè numeri e lettere, le lettere sono per forza maiuscole[13].
Sebbene gli ACP sconnettano dopo l'immissione di tre NUI errati è tecnicamente possibile scannare per trovare NUI ma la cosa è tristemente lenta…

[13] In realtà un NUI riportava una lettera minuscola, ma è il solo caso conosciuto. Il NUI in questione era N5GFVdD, valido su tutto il territorio nazionale via accesso Easy Way 1421 e durata quasi due anni.

Bisogna infatti provare due NUI, introdurne uno valido al terzo tentativo per connettersi da qualche parte, risconnettersi premendo CTRL P e poi digitando CLR, per poi riprovare altri due NUI a caso.
CTRL P è il carattere di escape di Itapac, serve a riprendere il controllo del pad per potergli inviare dei comandi, nel nostro caso abbiamo inviato CLR che indica il comando di CLEAR, cioè chiusura del collegamento.

C) EASY WAY ITAPAC
E' un servizio che offerto dalla SIP/Telecom, permette di collegarsi al costo di un solo scatto e di addebitare il traffico telefonico e quello Itapac al NUA che viene chiamato; questa modalità si chiama **Reverse Charge**.

Non c'è bisogno di NUI per utilizzare Easy Way Itapac, basta digitare il NUA da chiamare.
Non tutti gli host su Itapac permettono il Reverse Charge ma, anzi, le utenze con questo servizio abilitato sono veramente poche: infatti un'azienda deve fare esplicita richiesta alla Telecom per attivare il servizio di R.C.. Una curiosità: su altre reti X.25 il R.C. è configurato di default dal carrier e viene eliminato solamente su esplicita richiesta del Cliente (USA/SprintNet).
Per un hacker Easy Way è uno dei tanti modi per non pagare il servizio utilizzato e la tecnica più usata è quella di hackerare un host che accetta il Reverse Charge e usarlo come ponte per fare le chiamate x.25 desiderate verso NUA non R.C.

D) Tramite un PAD su NUMERO VERDE
Scannare i numeri verdi può riservare molte sorprese, come ad esempio un PAD x.25: il problema però sta nel capire che quello che si è trovato è un pad ed in più bisogna capire come funziona.
Una volta impostati i parametri della connessione (parita, bit di dati etc…) per avere una risposta coerente del modem basta studiare i messaggi di errore che si ricevono e capire se si tratta di un pad o meno.

Il difficile sta nel riuscire a farlo chiamare; intanto procuriamoci un NUA che sappiamo per certo essere funzionante (QSD in Francia può andar bene, 0208057040540[14]) e proviamo a digitarla per osservare la risposta. Si possono anche provare i comandi **help, ? call, c, pad** e tutto quello che può venire in mente.
Bisogna infine considerare anche il fatto che potrebbe non trattarsi di un pad Itapac, per cui potrebbe essere necessario togliere lo zero iniziale o addirittura sostituirlo con qualcos'altro.

E) Tramite un PAD su INTERNET
Valgono le stesse basi dei PAD su numero verde, bisogna capire come funziona e in che rete si trova. I PAD più diffusi sono i VCX, i PAD di tipo X.3 standard ("*" come prompt), i CDC, i GS/1 ed infine quelli da me definiti "anonimi", i quali usualmente hanno sintassi "C 0nua".

E) Tramite un CISCO su INTERNET
Digitando il comando show interface su un router Cisco si può capire se ad una delle interfacce seriali è assegnato un NUA e quindi se si può utilizzare il cisco per "paddare" fuori, tramite il comando **pad.**
Altri comandi utili sui sistemi Cisco sono **show x25 map**, il quale elenca le mappature

[14] QSD è "morta" ufficialmente il 4 settembre 2001. Vedasi l'allegato C per una videata commemorativa.

X.25 <-> TCP/IP (generalmente su reti private ma a volta anche su IP pubblici) e **sh x25 route**, per visualizzare i routing X.25 effettuati dal Cisco (dati, voice, etc..).
Se si ha la password di enable si può vedere l'intera configurazione del router compresa la parte X.25 (inclusiva del NUA assegnato al royter) digitando **show run** o **sh conf.**

F) Tramite un VAX su INTERNET
Se si dispone di un Vax che abbia sia il collegamento Internet che x.25 si può utilizzare il comando **set host/x29** nua per chiamare. Sui sistemi inferiori a OpenVMS 6.0 e su tutti i VMS dall'utility di NCP è possibile visualizzare il NUA del sistema con il comando **SHOW KNOWN DTE**, mentre i comandi **SHOW KNOWN CIRCUIT** e **SHOW KNOWN LINE** ci forniscono informazioni sulla configurazione delle linee dati.

G) Tramite SPRINTNET
Come illustrato nell'apposita sezione di questo documento la rete Sprintnet è presente in tutto il mondo: esistono quindi anche i dialup per raggiungerla e gli stessi sono facilmente reperibili sia su Internet, sia collegandosi ad un nodo SprintNet ed inserendo al prompt "@" l'utenza MAIL. A questo punto inserire UserID *phones* e Password *phones* alla richiesta di login; più difficile è invece trovare i toll free, ovverosia i numeri verdi per l'accesso a Sprintnet, presenti in diversi paesi del mondo.
Caratteristica peculiare di Sprintnet è che di default **gli host accettano il reverse charge**: vedasi a questo proposito la sezione relativa alla rete Sprintnet in questo documento.

H) Tramite uno UNIX su INTERNET
A seconda della distribuzione Unix (e comunque del software X.25 PAD installato) il comando per chiamare un NUA cambia, vediamone qualcuno:

- **DG/UX (Data General Aviion)**: il comando è "**pad**" e l'utilizzo è *pad nua* ; se invece lanciamo il solo comando di pad, al prompt "PAD:" la sintassi è "C nua" oppure "C A.nua" I file relativi alla configurazione X.25 del sistema sono in /usr/opt/x25/ mentre in /usr/opt/x25/etc/x3defaults troviamo i parametri di default per il pad, in caso si riscontrassero problemi di ricezione per settaggi del pad X.25 su sistemi con configurazione propria.

- **IBM AIX** Il comando di pad si chiama **xu**, utilizzo *xu nua*.

- **Sco UNIX SYSTEM V** Il comando è **xpad –d** nua; se non si specifica il "-d" non vi è alcuna possibilità di uscire.

- **SUN OS/ SUN SOLARIS** se è installato il software SunLink c'e' il comando **pad**, la sintassi è *pad –t 0 nua.*
  /opt/SUNWconn/bin/pad
  /opt/SUNWconn/x25/bin/pad

- **Unix BULL PAD** Come si intuisce dal nome della distribuzione, operante su Server DPS e DPX, il comando è come per i DG/UX, *pad A.nua* oppure *pad* ed al prompt *C A.nua.* Sulle prime release software il comando era invece **tpad**.

- **HP-UX** C'è il comando **padem,** una volta eseguito basta inserire il NUA (prompt di "*" come su dialup X.28).

- **DIGITAL ULTRIX : x29login**

Utile può essere il comando ***find / -name "*pad*" –print*** per trovare le possibili variabili (tpad, lpad, cpad, padem, pademu)

N.B. Per una visione completa delle modalità di accesso, NUA logging, tipici account di default, tips & tricks, etc.. su un elevato numero di OS, rimandiamo al prossimo ITBH White Paper, "**Systems Catalogue**", la cui uscita è prevista per ottobre 2002.

2 - SCANNING

Non esistendo motori di ricerca sulle reti X.25 né tantomeno elenchi pubblici di NUA, il solo modo per reperire indirizzi di sistemi collegati a reti X.25 è quello di trovarseli da soli ☺.
I modi per trovare NUA "on your own" sono comunque molti, partendo da dei semplici search sulla rete Internet (file di scan, e-zines di gruppi hacker, siti informativi di compagnie telefoniche e carrier dati, pagine di help per la connessione di Fornitori di Servizi presenti su X.25….). Naturalmente se cerchiamo NUA su vecchi file, le stesse saranno state chiamate da migliaia di persone, i sistemi

avranno subito breaking, brute force attacks e, in generale, hacking sino alla nausea, gli audit saranno alzati e, per farla breve, non conviene tentare ulteriori intrusioni su detti sistemi.

Il migliore modo per trovare NUA è quindi quello di "scannare", ovverosia effettuare scanning di NUA X.25.

Scanning non vuole dire altro che chiamare un NUA dopo l'altro, incrementando di una cifra il NUA stesso, uno dopo l'altro. Per capirci, se scanniamo Torino nella solita Trama Attiva "22" e decidiamo di partire dall'Utenza 800, chiamaremo:

21122800
21122801
21122802
……
……

Naturalmente l'esperienza, il background e gli "archivi personali" aiutano a cercare NUA nei posti giusti, vale a dire su reti X.25 ed in città con un'alto numero di possibili clienti e quindi un'alta proliferazione di sistemi informatici collegati alla rete. Bisogna anche dire che effettuare scanning "a mano" può essere divertente, permette di verificare con attenzione i singoli messaggi di errore (se riceviamo NP 067 da un PAD X.3 vorrà dire che il NUA non è assegnato, mentre NP 000 significa che oltre a non essere assegnato la Trama non è attiva) e di comprendere la struttura dell'assegnazione utenze decisa dal carrier dati, ma di controparte risulta estremamente lenta e – a lungo andare – noiosa.

Nulla vieta dunque di scriverci il nostro scanner personalizzato, il quale scannerà gli indirizzi X.25 per noi, magari apportando opzioni di logging avanzato, scan automatico dei DTE per i subaddress o funzioni di Test Nua Finding, ovverosia individuazione delle Trame Attive utilizzando dei test address reperiti da siti ufficiali.

A) Reverse Charge Scanning

E' possibile scannare da accessi pubblici X.28 (dialup) anche se non si dispone di un NUI: le connessioni X.28 sono sì tipicamente intese a carico del chiamante (e quindi utilizzando un NUI dai dialup urbani presenti nelle maggiori città), ma moltissime reti X.25 dispongono di dialup su numeri verdi o numeri speciali – comunque a zero scatti o a tariffazione speciale, ovverosia un solo scatto alla risposta – dai quali è possibile effettuare chiamate verso NUA X.25 in modalità Reverse Charge.
In Italia questo tipo di servizio, sulla rete ITAPAC, viene chiamato Easy Way e permette la connessione da parte di utenti non abbonati alla rete ITAPAC ma abbonati ad un Fornitore di Servizi il quale è invece collegato direttamente mediante utenza X.25 alla rete.

Ci sono naturalmente dei pro e dei contro: le chiamate vengono effettuate direttamente dal PAD della rete X.25, il quale dopo un certo numero di chiamate non a buon fine fa cadere la nostra connessione modem. ITAPAC utilizza un contatore il quale scollega dopo la decima chiamata non andata a buon fine: una soluzione è quella di chiamare un NUA di appoggio – la quale accetta la chiamata in Reverse Charge - al nono tentativo, facendo così azzerare il contatore del PAD e proseguire per altri nove NUA. E' facile dedurre come questo primo accorgimento inserito dal carrier dati rallenti di molto il nostro scanning.

Un secondo "difetto" del Reverse Scanning consiste nel logging: se possiamo chiamare solo NUA che accettano il Reverse Charge non potremo mai sapere quali sistemi sono collegati alle utenze attive ma non Reverse Charge, in quanto non accetteranno la nostra chiamata (CLR RNA da PAD X.28 o "Reverse Charge is not Allowed" da PAD su OS collegati direttamente a rete X.25); a questo punto dovremo segnarci i NUA "RNA" e contattarli in un secondo tempo utilizzando un NUI o un'utenza X.25 diretta.

B) Direct X.25 Scanning & Scanner Automatici

La fase di scanning su X.25 può essere di due tipi, manuale o automatizzata, ma sono in genere entrambe utilizzate. L'impiego di uno scanner automatico implica però una ulteriore suddivisione, ben più importante ai fini delle funzionalità e performance: scanner che operano in locale (sul nostro personal) e scanner che operano da sistemi informatici fisicamente remoti e collegati con connessioni dirette alla rete X.25.

Sulla Rete esistono diversi script o programmi per scannare da dialup X.28 (quindi dal proprio PC) mentre poco e nulla esiste a livello pubblico per i vari sistemi operativi generalmente collegati via X.25. Nel primo caso le reti maggiormente prese come riferimento sono USA/SprintNet e Canada/Datapac e si tratta di script più o meno recenti per programmi di comunicazione quali Telix, Procomm Plus, Minicom o Hyper Terminal: esistono tuttavia anche alcune release di programmi italiani scritti per la rete ITAPAC.

Un consiglio che posso dare è di dialogare direttamente con la porta seriale e gestire completamente il dialogo con il modem, come per un wardialer, integrando un terminale "intelligente" che registri il tutto e scremi i dati secondo rules predefinite: con questa logica si può adattare senza problemi l'applicazione ai diversi linguaggi di programmazione e, soprattutto, sistemi operativi.

Nel secondo caso invece, anche se di difficile reperibilità, rimane famoso il DEFCON Scanner per i Prime Computer scritto in PRIMOS da The Force, lo SCAN.COM scritto in DCL per sistemi Digital VAX/VMS da un hacker italiano, Zibri, ed il sottoscritto, una versione shell per SunOS scritta da un serbo di nome Sentinel (con operatività anche in background, al contrario di altri).
La leggenda racconta poi di scanner compilati in Macro assembler su VMS 4.x dal Chaos Computer Club, i cui componenti negli anni '80 violarono effettivamente la Digital Equipment Corporation[15] riuscirono a trioianizzare[16] la procedura di login con una *magic password* dopo averne ottenuto il codice sorgente.
Riteniamo doveroso ed utile segnalare un ottimo NUA scanner altamente adattabile alle proprie esigenze, reperibile alla URL http://www.0xdeadbeef.EU.org/code/vudu.
Per meglio far comprendere l'output di uno scanner riporto due log di esempio, uno italiano (dall'Italia su Cipro/CytaPac) e l'altro canadese (su Canada/DataPac). Il primo è automatico lanciato da un VAX/VMS mentre il secondo è uno scanning manuale.

LOG 1: CYTAPAC

```
Scanning from NUA: 0280221000 started on 15-OCT-1994 15:29:30.75
0280221091  %COM        DROP STATION
0280221092  %COM        ECHO STATION
0280221093  %COM        TRAFFIC GENERATOR
```

[15] Come Kevin Mitnick pochi anni dopo, il cui sogno era proprio quello di ottenere il codice sorgente del VMS per poter comprenderne a fondo la struttura e riuscire ad individuare falle di sicurezza
[16] Troianizzare: inserire un troiano (trojan), ovverosia modificare il programma per eseguire altri comandi ed operazioni

```
0280221101  %CLR_OCC
0280221102  %CLR_DTE
0280221106  %CLR_DTE
0280221107  %COM
0280221108  %CLR_DTE
0280221117  %CLR_OCC
0280221118  %CLR_DTE
0280221121  %COM         MINISTRY OF HEALT, VAX/VMS
0280221122  %COM         IBM AIX UNIX
0280221125  %CLR_DTE
0280221147  %CLR_RPE SUBADDRESS 48 CYTA Pager via x.25
0280221199  %COM         CISCO
0280221206  %COM        LOGON: ??
0280221225  %COM         CISCO
0280221229  %COM        CISCO BYBLOS BANK S.A.L. - LIMASSOL/CYPRUS ACS-CYPRUS LINE 6
0280221248  %COM         COM/DTE
0280221273  %CLR_DTE
0280221274  %CLR_OCC
0280221276  %CLR
Scanning ended with NUA: 0280221396 on 15-OCT-2000 15:46:36.32
```

LOG 2: DATAPAC

```
- 202 - ONTARIO  - Up to 700
20200115          VAX/VMS
20200116          VAX/VMS
20200156          Diand Information System
20200214          $ UNIX      (gtagmhs2)
20200230          METS Dial-In Server  Enter your login:
2020024098        Control Port on Node Ottawa 6505 PAD
20200286          $ VAX/VMS
2020032099        MPX.25102: PASSWORD
20200321          SunOS     Rel 4.1.3 (X25)
20200322          SunOS         ""
20200330          INETCO    Magicbank
20200342          ::
20200497          VAX/VMS
202005421         $ VAX/VMS
20200548          SunOS     Rel 4.1.3 (TMS470)
20200582          $ VAX/VMS   Production System
```

Come si può notare a fianco del NUA chiamato troviamo un campo di commento, dove vengono inserite le informazioni relative al sistema individuato.

3 - X.25 HACKING

L'hacking su reti X.25 rappresenta sicuramente al meglio lo stile di "old style hacking", un modo di fare hacking (attacchi di tipo brute force, conoscenze di metodologie ed exploit su particolari sistemi operativi, trucchi e "chicche" vari) che non è mai realmente passato di moda. Potrei invece affermare che questo stile è stato semplicemente oscurato dalle tecniche hacking ai servizi di rete (network services hacking) utilizzate su Internet: alla fin fine anche gli attacchi ad applicazioni e servizi di rete

altro non sono che il provare un exploit dopo l'altro ed il tutto si riassume con il concetto di brute force attack…

In questa sezione esamineremo i punti essenziali dell'hacking su X.25, divisi in quattro "eventi" standard.

A) Richieste di "LOGIN"

Con "Richieste di LOGIN" mi riferisco a tutte le connessioni X.25 dove, al COM, ci viene richiesto un identificativo. Il nostro terminale è generalmente in emulazione standard o abbiamo impostato un'emulazione particolare (IBM 3270, etc..) ma comunemente reperibile.

Possiamo dividere le potenziali vulnerabilità di un login server nelle seguenti categorie:

1) **Falle nella verifica dell'input** (Input Validation Flaw). Esistono alcuni casi, abbastanza rari, dove il costruttore dell'OS abilita una stringa particolare nell'input validation, per la propria autenticazione. Per esempio sulle versioni di PRIME precedenti alla 18 è sufficiente dare due "^C" (Control-C) per avere accesso al sistema operativo, mentre è famoso il validation flaw di IRIX spiegato nello stesso System Catalogue. Per quanto riguarda i buffer overflow sui login server, che io sappia, non ne esistono su nessun sistema operativo.

2) **Account di default**. Sono gli account pre-configurati dal sistema operativo "vergine". La categoria dei "lazy sysadmins", alquanto folta, lascia spesso questi account così come sono. Non dimentichiamoci che le realtà presenti su reti X.25 sono spesso enormi gruppi industriali con un parco macchine estremamente elevato: in questi ambienti l'abitudine diffusa è quella di installare il server e "lasciarlo lì", mettendoci le mani solo quando gli utenti lamentano disservizi o problematiche tecniche.

4) **Default di Amministrazione**. Esistono default account impostati dai sysadmin per semplificarsi la vita. E' facile trovare shell script di vari tipi dove la procedura utilizza un account specifico senza password, o altre procedure che impostano la stessa password per tutti gli account di sistema relativi ad operazioni specifiche. Questi username e password semplificano l'intrusione, essendo in realtà account non utilizzati da utenti del sistema e non essendo quindi soggetti a cambi di password non previsti.

5) **Application Backdoor Account**. Il sysadmin installa un'applicazione sul suo box come root e l'applicazione scrive nel file delle password, creando un'account: spesso il sysadmin non si cura di ciò, essendo il suo compito esclusivamente quello di installare e testare l'applicazione e poi lasciarla agli utenti del sistema. Un esempio tipico è il DB

Ingres in ambiente UNIX: dopo l'installazione è sufficiente loggarsi con user ingres e password ingres.

6) **Weak Password**. A causa dell'ignoranza e non curanza degli utenti, i quali non capiscono come rendere difficili le password e le vedono invece come una noia, non è raro trovare password quali "password" oppure il login con l'aggiunta di cifre quali "99", "00", etc..

7) **Pre-Login Procedures Bugs/Backdoor**. In alcuni sistemi operativi (cito, tra gli altri, VOS/32, HP3000, PICK Systems, Prime Computers..) esistono sequenze le quali, se inserite durante la richiesta di logon, by-passano la procedura di login stessa. Queste tipologie di OS, spesso,

permettono la consultazione dell'help di sistema anche se non si è ancora proceduto all'identificazione tramite procedura di login.

Le vulnerabilità numero 5 e 6 possono essere esplose mediante attacchi di tipo Brute Force, con altissime probabilità di accesso nel sistema target.

B) X.25 Network Services

Chi legge avrà probabilmente ben chiaro il concetto dei network services e del TCP/IP, ma deve essere chiara la differenza nell'averli su reti TCP/IP o su reti X.25. Il concetto di "porte" su X.25 è diverso: differenti utenti che chiamano lo stesso NUA si collegheranno al server corrispondente all'indirizzo X.25 ed avranno assegnato un channel number, cosicchè diverse connessioni su differenti canali possano raggiungere un server nello stesso momento.

Una connessione verso un NUA non può includere un'assegnazione di porta TCP/IP per collegarsi ad un servizio differente mentre si utilizza il protocollo X.25 (per farlo normalmente si utilizza il subaddressing, facendolo gestire a monte da un router X.25). E' naturalmente possibile incapsulare il TCP/IP nel protocollo X.25, ma ciò dipende dai sistemi posti ai due estremi della connessione e non dal protocollo X.25. Le porte su X.25 sono vere e proprie connessioni separate e per conto loro, e spesso hanno network services attivi.

L'hacking su X.25 è più stimolante di quello su TCP/IP proprio per la mancanza di centralizzazione dei network services, non essendoci così tanti servizi di rete come tipicamente avviene sulla reti TCP/IP.

Esistono ad ogni modo network services su X.25 che possono essere di estrema utilità per avere informazioni o esplorare certi sistemi e reti. A prima vista sembra che il solo modo per entrare in un sistema su rete X.25 sia effettuando attacchi di tipo brute force sul Login Server, ma ciò non è sempre vero. Il grazioso mix di "culture" nelle aziende, dove rimane la vecchia scuola del Frame Relay ma il TCP/IP ha invaso ogni tipo di connessione, rende possibile trovare router X.25 gestiti via SNMP, dove è quindi necessario solamente "parlare" quel tipo di network service per poter accedere o ottenere informazioni utili all'attacco.

In definitiva sulle reti X.25 troveremo i servizi di rete più arcani, nei quali spesso non ci si è mai imbattuti, ma troveremo anche sistemi bene o male conosciuti, partendo dai Gandalf XMUX, passando per i Digital Access Server per arrivare ai Cisco router, agli HP Data Communications o ai Terminal Controller..ce n'è per tutti i gusti, basta aver voglia di imparare…

Ricordiamoci infine come, non essendoci davvero confronti con la logica del mondo TCP/IP, potrà capitare di trovare sistemi che ci collegano immediatamente con un menù interno, così come access router senza password o con policy estremamente "rilassate".

C) Identificazione dei Sistemi

Se sapete qualcosina del sistema che vi trovate di fronte avrete la possibilità di provare password di default o backdoor conosciute su quell'OS; in più avrete un'idea chiara del formato di login.
Non esistendo altre informazioni se non il semplice messaggio di testo che appare dopo la connessione al NUA, per identificare il sistema operativo prestate molta attenzione ad eventuali system banner, prompt di sistema o quant'altro: una buona conoscenza di queste tipologie di messaggi aiuta sicuramente a capire con cosa si ha a che fare, specialmente quando il sysadmin decide di cambiare i prompt di default alla richiesta di login.

Direi che i seguenti punti possano riassumere le "cose a cui fare attenzione" quando si chiama un sistema.

1) **Lettere Maiuscole/Minuscole al prompt di login**. Non fate attenzione solo alle parole utilizzate nel prompt, ma anche a quale lettera è maiuscola (o non lo è): tutto ciò in modo particolare per le primissime lettere del prompt.
   Prendiamo ad esempio il prompt UNIX:
   login:
   Notate le minuscole. Se invece fosse stato qualcosa del tipo:
   Login:
   sarebbe stato probabilmente un System75 (la prima lettera è maiuscola).

2) **L'importanza del messaggio di errore (login incorretto)**. Otteniamo questo messaggio di errore quando inseriamo un'autenticazione non valida. Innanzitutto possiamo identificare i sistemi dal fatto che diano o meno il messaggio di errore, o che aspettino sia il login che la password prima di risponderci con il messaggio di errore stesso. Il secondo luogo possiamo identificare il sistema operativo esaminando quello che ci dice proprio nel messaggio di errore. Prendiamo ad esempio il prompt:
   `Username:`

Se continua con:

```
Password:
User authorization failure
```

è a tutti gli effetti un VAX/VMS (o un Alpha/OpenVMS)

Ma se invece continuasse così:

```
Password:
Invalid username - password pair
```

..lo potremmo identificare come un AOS/VS.

Per essere sempre sicuri di arrivare al messaggio di login error, possiamo inserire lettere a caso alla richiesta di autenticazione o, nei casi di sistemi "muti", lunghe sequenze di caratteri o caratteri di controllo quali ^H, ^C, ^Z, ^Q, etc..

3) **L'importanza dell'errore Login Format Incorrect**. Con "login format incorrect" generalizzo tutti quei sistemi per i quali è necessaria una stringa di comandi particolare prima dell'inserimento di UserID e Password. Prendiamo come esempio gli HP3000:

```
EXPECTED A: HELLO COMMAND (CIERR 6057)
```

...il che significa solamente che l'autenticazione va preceduta dal comando "HELLO". Nei casi in cui ci si imbatta in uno dei tanti sistemi di questa macrocategoria, consiglio di provare con [ENTER] senza che sia preceduto da altri caratteri, oppure varie combinazioni di Control (come nel punto 3) o vari delimitatori quali ',' o '.' L'esempio dei Gandalf XMUX chiarisce abbastanza la convenienza di queste combinazioni incrociate: se diamo [ENTER], senza caratteri che lo precedano, alla connessione X.25 con uno XMUX, il sistema risponderà con

```
Invalid Name
```

```
Names must consist of 1 to 8 alphanumeric characters
```

Il che, essendo inusuale come login format error, ci permette di identificare l'OS alle spalle del NUA chiamato.

4) **Le modalità di sconnessione**. E' in genere "quel qualcosa" che accade mentre premiamo caratteri di escape a caso e ci sconnette. Se non abbiamo trovato lo shortkey per la sconnessione dal PAD X.25 dal quale abbiamo chiamato il sistema target, allora abbiamo un indizio per capire davanti a quale sistema ci troviamo. Nel VMS il ^Z ci scollegherà dalla richiesta di login (a volte PAD X.25 mal configurati non permettono di visualizzare la richiesta di login del sistema remoto, ma il classico "beep" della connessione ad un sistema VMS si sente), così come il ^D per i sistemi UNIX.

Questi quattro punti riassumono i metodi che si possono utilizzare per identificare il sistema operativo obiettivo del nostro attacco. Gli esempi inclusi sono "tipici" e non elencano assolutamente la totalità degli OS reperibili sulle reti X.25, né tantomeno illustrano nel dettaglio le vulnerabilità più conosciute. A questo scopo ho inserito nella sezione Systems Catalogue le caratteristiche di tutti gli OS di cui sono venuto a conoscenza negli anni.

D) Quando si è dentro il sistema (cosa fare ?)

Il "cosa fare" dopo che si è entrati in un sistema remoto è argomento base di moltissimi articoli e documenti – peraltro spesso molto ben scritti e dettagliati – reperibili su Internet, anche se il subject è spesso circoscritto ai soli sistemi *NIX: per reperire informazioni utili su sistemi differenti è necessario ricercare i vecchi numeri di e-mag storici quali Phrack, 2600 Magazine, LOD Technical Journal e così via. Ad ogni modo gli accorgimenti ed i tool da utilizzare su sistemi X.25 sono bene o male gli stessi dei sistemi su Internet e preferisco quindi fornire alcuni consigli specifici per X.25.

a) troianizzare il PAD (inteso come sistema remoto) con backdoor, far sì che ci si possa ricollegare utilizzando account "jolly" utilizzati esclusivamente per le attività di chiamate X.25 in uscita;

b) troianizzare il PAD per registrare le utenze e le password su sistemi remoti o, nel caso di demoni di login X.25 (IBM AIX), l'applicativo del login stesso;

c) cercare di trovare NUI X.28 sul PAD stesso. Non è raro su sistemi quali Gandalf, Xenix 386 o Solstice PAD trovare script per chiamate con addebiti differenziati o chiamate a CUG specifici, per le quali il NUI è abilitato. Non essendo semplice reperire NUI in altri modi questa tecnica risulta spesso estremamente proficua;

d) leggere i log del PAD o del sistema gaetway ("last" su Unix, "sys$sysmanager:psiaccounting.com su VMS ed OpenVMS, etc..) per ottenere altri NUA validi (spesso appartenenti alla stessa azienda e quindi con default account simili a quelli utilizzati);

e) allo stesso scopo del punto precedente, reperire file di host x.25 predefiniti con valori mnemonici. Su sistemi pad tipo VCX è necessario andare "a caso", fornendo nomi di città o nomi di sezioni e filiali dell'azienda. Sui sistemi *NIX arrivati al PAD ci si porta in modalità prompt e si richiede l'elenco degli host, mentre su VMS l'utility NCP fornisce molte informazioni su circuiti logici permanenti (PVC) verso altri DTE;

f) la backdoor migliore: prendere ogni tipo di file minimamente importante presente sul sistema. Liste di nomi, file di password (/etc/passwd e shadow vari su *NIX, sysuaf.dat su VMS) ed in genere tutto ciò che potrebbe essere utile per rientrare in un secondo momento. Su X.25 questo

accorgimento vale molto di più che su Internet, essendo i sistemi stessi designati per scopi specifici e spesso ad uso esclusivamente interno, portando ad una strana logica di "uso interno" su reti geografiche di tipo mondiale. LA sezione Systems Catalogue riporta i file più importanti dei sistemi operativi di cui sono a conoscenza.

III) Sezione Pratica: Attacco (3 di 5)

1 – PERFEZIONARE IL BRUTE FORCE HACKING

Gli attacchi di tipo Brute Force sono probabilmente i soli che possiamo definire come "nostri", una tipologia di hacking alla quale ci si affeziona particolarmente: alla fin fine il concetto è quello di provare combinazioni di username e password una dopo l'altra o, in alternativa, tirare su un programma automatizzato che svolga il lavoro per noi.

Al contrario di quanto si dice ritengo che ci sia assolutamente *un'arte* negli attacchi di questo tipo: in particolar modo su X.25 l'accoppiata user/pass può essere facilmente indovinata, seguendo alcuni principi generali di seguito esposti in questa sezione.

In linea di massima il brute forcing funziona al meglio se si passa molto tempo su ogni sistema oppure, in alternativa, se si passa poco tempo su ognuno di essi, ma se ne prova un gran numero. Con la stessa logica abbiamo la possibilità di provare poche password su un gran numero di usernames, oppure tanti tipi di password per ogni singolo username. Diciamo che la "regola d'oro" del brute forcing dice che un approccio metodologico è quello che porta i risultati, escludendo la fortuna ma non escludendo però i "casi rari".

Questa metodologia si applica anche con successo al "dialup server hacker" e non credereste a quanti target sulla rete Internet o sui dialup 800 (numeri verdi) siano vulnerabili ad attacchi sistematici di questo genere. Si possono utilizzare i concetti di seguito esposti anche per creare un veloce dizionario per il cracking dell'/etc/passwd.

A) Login Names

1) testare utenze "default login" anche dopo che la password di default non ha funzionato;

2) combinazioni "last name/first name", ad esempio Mario Rossi = *mrossi* oppure *rossim* . In genere viene utilizzata la regola di 5 lettere per il cognome ed una lettera per il nome;

3) progetti dell'azienda target, nomi e marchi aziendali, prodotti, divisioni, abbreviazioni sugli stessi;

4) la serie "welcome", ovverosia quegli utenti della nostra userlist che oltre ad avere password nulla [NULL] hanno scopi generici di "visita" o open support (guest, ospite, temp, info, help, helpdesk, supporto, support, aiuto, intro, aid, test, demo, visitor…)

***

B) Utenza non valida

I sistemi operativi come UNIX e VMS non ci diranno se abbiamo inserito un login e password non corretti, ma continueranno tutta la sequenza di logon prima di dirci se ci siamo riusciti o meno. Esistono però alcuni sistemi operativi che ci diranno se è stata inserita una username non valida, ad esempio gli HP3000 ci dicono esattamente cosa c'è di sbagliato nell'autenticazione: insistete su sistemi operativi di questo tipo per creare o verificare una users list ad hoc sui singoli OS.
Lo stesso dicasi per alcune configurazioni su router Cisco IOS.

***

C) Passwords

1) Utilizzare i default e le backdoor conosciute. Si può anche iniziare a creare una propria lista di default in maniera empirica, annotando gli account più comuni (nomi e cognomi di un certo paese, default di una società o rete specifica, etc..) che si vedono quando si è dentro un sistema (cat /etc/passwd ed /etc/hosts, SHOW USERS/FULL e MC NCP SH KN NODES, etc..).

2) Analizzare, isolare ed utilizzare tutto ciò che è nel banner, con variazioni e combinazioni.

3) Account name=password: la classica accoppiata. L'esempio tipico è Login: mario Password: mario. Se il target è un grande sistema con centinaia di utenti, come minimo uno di questi utenti c'è. Nel VMS così come su alcuni altri sistemi è estremamente semplice e parecchio utilizzata la definizione della password iniziale uguale allo username.

4) Account name al contrario (backwards). Effettuate variazioni sull'account name o incrociatelo con le informazioni del banner, il nome del nodo, etc..

5) "i classici": [x25, x29, c, qwerty, asdfgh, hello, computer, secret, password, whatever, open, access, vaffanculo, account, please, work, lavoro]. Si può anche provare con "sesso" e "amore" già che ci siamo ☺ Ad ogni modo si deve cercare di pensare come la persona che utilizza l'account su quel sistema.

6) I "nomi base": *tantissime* persone utilizzano il nome della moglie, del figlio, della ragazza, del proprio animale, etc.., come password personale. Penso che alcune tipologie di utenti si sentirebbero "in colpa" se non scegliessero password di questo tipo: ritengo che la motivazione psicologica risieda nell'associare un segreto (la password) a qualcuno di cui ci fidiamo.

7) Le scelte comuni: i nomi di animali a livello base (cane, gatto, tigre, leone, etc..), le squadre di calcio, i nomi dei giocatori, gruppi musicali e cantanti, automobili, star e VIP di vario tipo.

8) Locazione geografica: il nome della città o della regione dove il sistema risiede e simili associazioni applicate alla geografia.

9) Pensare a cose che c'entrino con quello che pensiamo il sistema target sia o svolga: per che cosa è utilizzato ? Che procedure vi operano ? Quale tipologia di utenza può avere accesso e da dove ?

10) Nome della rete X.25 del paese ove il sistema risiede, con varianti.

11) Progetti dell'azienda conosciuti, prodotti, nomi di tipologie di servizi.

12) Abbreviazioni e varianti sul company name.

13) Lettere singole: a, b, c, etc…. ce ne sono 26 !

14) L'associazione delle combinazioni "default password" + "utenti con password unica". Sono molti gli utenti che utilizzano la stessa password su più sistemi: analizzate i log e le sessioni di intercettazione (x25 trace o TCP/IP sniffing) alla ricerca di password ricorsive o accoppiate di login/password ed usate spesso, anche se non su tutti i sistemi, magari su network vicini e con funzionalità specifiche di gestione amministrativa: il worm WANK funzionò esattamente così.

15) SNMP community names: [public, private, secret, world, network, community, read, write, all private, admin, dafault, password, monitor, manager, security].

Ricordatevi sempre di provare password nulle [NULL] con ogni username: alcuni sistemi fanno entrare se la password è nulla, ma altri (la maggior parte) richiedono ugualmente la password.

Un ultimo commento: il tipo di password. Solo se la password è nota ad un'unica persona può essere identificata in un qualcosa di "personale" (o che ha a che fare con gusti personali); se è utilizzata da

un gruppo di persone sarà invece più tecnica, o magari qualcosa di comune e/o noto a tutti i membri del gruppo.
E' bene ricordarsene se si ha accesso ad informazioni a priori o se si prova ad accedere su un particolare account.

***

2 – AUTOMATIZZARE GLI ATTACCHI BRUTE FORCE

Le stesse tecniche di scripting per gli scanner automatici possono essere applicate nell'automatizzare il brute force password cracking. In primo luogo prendiamo la nostra lista di default account, poi l'elenco di password comuni.

Ci si deve assicurare che il nostro brute forcer si sposi bene con il formato di login del sistema target.

Alla fin fine si devono avere due elenchi principali: un listato di password comuni (oppure la serie dei nomi propri, delle città, dei cognomi, etc..) ed una serie di listati di defaults per i singoli sistemi.

Ordinate i file in maniera tale che i più comuni siano i primi ad essere provati.

Secondo me è divertente farsi da soli il proprio brute forcer ad "intelligenza artificiale" ☺

***

3 – SICUREZZA PERSONALE

Se un sysadmin vede 1000 tentativi di login falliti, esiste una sola spiegazione possibile.

Se siete rimasti ore ed ore a provare ed avete fallito, lui saprà che qualcuno sta tentando di entrare; se siete riusciti ad entrare, pulite i log immediatamente affinchè non ci sia traccia della vostra attività.

Cercate anche di utilizzare metodi che rendano difficile un tracing della chiamata quando si adotta un brute forcing attack "pesante" e prolungato.

IV) Sezione Pratica: Attacco (4 di 5)

1 - ALTRE METODOLOGIE DI HACKING SU X.25: SOCIAL ENGINEERING

Non ritengo l'ingegneria sociale una "tecnica di basso livello", in quanto un attaccante utilizza qualunque metodo possibile per raggiungere il proprio obiettivo. Uno degli assetti primari del Social Engineering è il pensare "out of the box": può comunque essere utile venire a conoscenza di alcune informazioni dall'interno della rete target per poi utilizzarle come contorno alla "figura" che ci si è

costruiti per l'occasione. Le informazioni interne possono anche servire per accedere in maniera "meno convenzionale" al target finale.

Il Social Engineering può essere effettuato via E-mail o attraverso telefonate, nazionali o internazionali che siano: è forse la sola tecnica di information gathering o di attacco applicabile quando il sistema non è locale (il trashing in questo caso diverrebbe problematico) e non si hanno altre tipologie di contatto con il target se non il numero telefonico.

L'idea è quella di portare l'interlocutore a fare o dire qualcosa che ci garantirà accesso. In genere è sempre meglio chiedere di cambiare la password di un account piuttosto che chiedere di comunicarcela: il concetto è quello di "aggirare" la richiesta diretta, operando trasversalmente ed ottenendo mano a mano la fiducia dell'interlocutore (o la paura delle conseguenze nel non rispettare un ordine arrivato "dall'alto"). Questo metodo è molto meno sospettoso e veloce, ma ricordiamoci anche come spesso i target siano il diretto proprietario dell'account o il sistemista responsabile il quale, però, nel 95% dei casi non è a conoscenza della password e può solo decriptarla o sostituirla.

Un secondo "stile" è quello di chiedere al target un accesso "legittimo", presentandosi e comportandosi come uno studente o un ricercatore. Nel momento in cui si ha un account sul sistema target il passo da compiere per avere privilegi di Sysadmin prima che qualcuno se ne accorga è in genere molto breve. Seguendo questa logica si può anche arrivare ad acquistare un account, se ne vale veramente la pena ed il target ci interessa in maniera particolare.

Vorrei dilungarmi oltre in questa sezione ma preferisco dedicare l'attenzione dovuta a questa tema in un white paper a parte sul Social Engineering.

***

2 – ALTRE METODOLOGIE DI HACKING SU X.25: ATTACCARE I SISTEMI COLLEGATI

Se avete problemi con un sistema target, cercate di entrare in un "related system": le informazioni che acquisirete potrebbero portarvi al sistema finale di vostro interesse, senza troppe difficoltà e perdite di tempo.

Molto spesso si trovano durante lo scanning due o più sistemi "gemelli", della stessa società e divisione operativa, ma con nomi di nodo differenti (roma1 e roma2, torino, milano e roma, etc..): entrati in uno di questi non è raro scoprire che tutti gli hosts sono trustati l'uno con l'altro, oppure trovare nel passwd degli account "jolly" utilizzati da un utente sui diversi nodi.

Quanto sopra è poi particolarmente veritiero se il sistema target è su una sottoporta (subaddress) di un NUA o, ancora, lo si chiama da un indirizzo mnemonico da dialup X.28 (o X.25 gateway stile Tymnet).

***

3 – ALTRE METODOLOGIE DI HACKING SU X.25: ATTACCARE IL ROUTER DI SERVIZIO (O SNODO)

In genere è molto semplice entrarci: sono router lasciati collegati ad una dorsale X.25 per la gestione in outsourcing dell'infrastruttura aziendale, per remote management o per necessità proprie dell'azienda.
Se il sistema target utilizza un'autenticazione "a due fattori", ad esempio, il modo migliore di affrontare il problema è quello di entrare sul router e da lì attivarsi verso il target, il quale potrebbe essere stato configurato per verificare sia l'accoppiata username/password che il DTE (NUA) di provenienza.

Come sapete i Cisco router si trovano comunemente sulle reti X.25 e queste tecniche possono essere utilizzate per addentrarsi maggiormente nella rete target, o per sferrare attacchi brute force su macchine interne, acquisire default accounts per quella rete (sempre analizzando i sistemi interni, ad esempio quelli visualizzabili dopo uno *show arp, show x25 map, show x25 route, show ip route, show cdp neig*) o, ancora, utilizzare informazioni "alternative" quali configurazioni di linee ISDN (utilissime per rientrare nel sistema target da un'altra strada, oppure da impostare come callback su receiving numbers "sicuri": *show dial map, show isdn history*) e così via.

Il seguente elenco riassume i principali punti ottenibili dai border routers:

- Intercettare il traffico di rete (ad esempio le password).
- Redirigere il traffico di rete ed installare un "fake login screen" per ottenere i dettagli della procedura di autenticazione. Si può anche impiegare un tipico attacco da "man in the middle" utilizzando questa tecnica e leggendo il challenge tra l'effettivo login screen e la vittima, leggere le risposte corrette senza creare alcun sospetto nell'utenza.
- E' anche possibile effettuare un attacco di "session hijacking", molto simile a quelli effettuati sui routers TCP/IP: programmi come Juggernaut ed Hunt trattano il tema e, anche se nulla del genere è mai stato ufficialmente sviluppato su X.25, la mia opinione è che sarebbe addirittura più facile su X.25 piuttosto che su TCP/IP, ed il risultato sarebbe *molto compromettente* dal punto di vista della sicurezza.
- Infine, è possibile effettuare attacchi simili su Gandalf XMUX o altri servizi di rete.

4 – ALTRE METODOLOGIE DI HACKING SU X.25: MAIL VIA X.25

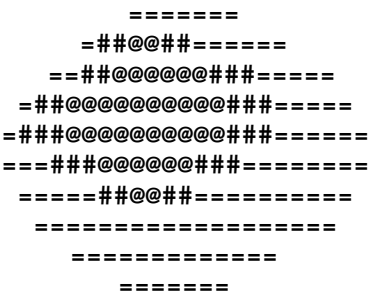
Su X.25 esistono molti hosts che forniscono servizi di mailing. In genere l'utente si logga sul sistema per prendere la propria posta, oppure il loro sistema si connette periodicamente e scarica la mail, o ancora il sistema ha un account sul quale il mail server si logga per uploadare la new mail a cadenze fisse. Se si ottiene accesso a questi sistemi, si può provare ad avere accesso alle mail di varie persone: la posta elettronica è notoriamente uno strumento molto diffuso per la comunicazione di password (Ciao Paolo, vado in vacanza per 2 settimane, puoi controllare tu se ricevo mail urgenti ? la mia password e'……..”), cambiamenti nelle regole di firewalling, abilitazioni di IP o comunicazioni di impostazioni SNMP. Questa tipologia di mail server possono essere un sistema pubblico utilizzato sulla rete X.25 pubblica (nazionale o mondiale) oppure un sistema corporate, che fornisce il servizio solamente a pochi sistemi anch'essi su rete X.25.

Esistono ad ogni modo diversi protocolli utilizzati per mail via X.25: il più comune sui sistemi *NIX è UUCP, ma in ambiente VMS abbiamo la PSI (Packet Switched Interface) Mail, utile tra parentesi ad effettuare il corrispettivo di un vrfy sulla 25 nel TCP/IP, per la verifica degli account esistenti.
Il bello di UUCP è che richiede un account sul sistema ricevente per poter funzionare: il primo sistema (System_1) si logga con l'account UUCP o NUUCP sul sistema remoto (System_2) e trasferisce i file, come la mail. Dare un'occhiata un po' attenta agli script nella directory di UUCP può a volte risultare estremanente utile: vi si trovano infatti gli indirizzi X.25 (e spesso i numeri di modem) degli hosts remoti, con la user e la pass utilizzati.
Molto spesso l'account UUCP *ha shell* e lavorando sui file di configurazione si aprono tantissime porte verso altri target.

Ricordo infine come siano generalmente le Telco ad utilizzare UUCP per lo scambio di log files verso le macchine NCC (Network Control Center) e come tutta la rete At&t fosse impostata in questo modo per la comunicazione tra le filiali remote e la casa madre, attraverso la rete Accunet X.25 in USA e le singole reti dei carrier X.25 negli altri paesi: vedasi a questo proposito il seguente quote dal vecchio passwd della At&t:

```
lcluucp:qbcbBVX3v0Rns:10:10:Uucp local to AT&t Egypt:/usr/spool/uucppublic:/usr/lib/uucp/uucico
```

A titolo di ricordo posto di seguito il logo del banner di attmail, lo Unix At&t 3.2B che gestiva la mail interna worldwide per la compagnia telefonica.



```
Welcome to At&T node attmail Unix System V/386 Release 3.2B

attmail login:
```

5 - ALTRE METODOLOGIE DI HACKING SU X.25: TRUCCHI, TRUCCHETTI E TROJANI

In questa sezione voglio porre alcuni cenni su altri metodi, non convenzionali, che di base "exploitano" l'elemento umano facendo guadagnare tempo e risorse:

- E-mailate un trojano. Ricordiamoci i vari "file_zippato.exe" o "i love you" della primavera '99 e 2000, applicati però – con le giuste modifiche – ai nostri obiettivi. Sebbene non si utilizzi X.25 come partenza o rete implicata, questi "attacchi" hanno dimostrato in passato come anche il sistema più sicuro possa avere un security hole proprio per la leggerezza degli utenti interni.

- Fate sì che gli utenti si registrino su un altro sistema con uno Username ed una Password di loro scelta: potrebbero usare un'accoppiata uguale a quelli scelti per il "vostro" sistema anche sul sistema target. In caso di policy account specifiche, "forzate" sul vostro sistema-esca la stessa policy (prima iniziale del nome + cognome, etc..).

- Se possibile inviate mail agli utenti iscritti e con questionari "stupidi" reperite informazioni aggiuntive sulle loro password preferite, oppure obbligateli nella prima settimana di iscrizione a cambare password 3 o 4 quattro volte, per forzare l'utilizzo della password utilizzata sul sistema target.

***

6 – ALTRE METODOLOGIE DI HACKING SU X.25: PRIOR KNOWLEDGE

Come ho illustrato nella Sezione Pratica di questo documento, in genere si inizia l'attacco verso il sistema target senza conoscere informazioni utili sullo stesso; è però stato anche accennato il concetto di "Prior Knowledge", molto molto importante.

Se siamo già stati precedentemente nel sistema target (o in uno dei suoi nodi), o se abbiamo comunque informazioni utili quali ad esempio gli utenti ed i default di sistema utilizzati, una intera nuova serie di tecniche si rende disponibile come per magia..

Il conoscere ad esempio i numeri telefonici (esterni o interni) di alcuni utenti, così come i dipartimenti di appartenenza, apre la strada al social engineering; la conoscenza dei prodotti porta ad opzioni importanti nel password guessing, e così via.

Ecco il motivo per cui è estremamente importante prendere il maggior numero di informazioni dai sistemi in cui si entra e dai sistemi in cui si è intenzionati a rimanere.

V) Sezione Pratica: Attacco (5 di 5): Sicurezza personale

1 – LA CHIAMATA

Possiamo dire che è da qui che inizia tutto. Se temete tracciamenti dal vostro PAD o dal dialup di accesso, il vostro rifugio ideale è il vecchio Sistema Telefonico Nazionale: quelle che seguono sono alcune tecniche ed idee base.

1) **La linea telefonica di qualcun altro**. Si può applicare utilizzando un diverter o semplicemente utilizzando la linea telefonica del vostro vicino. Vi sono comunque alcune implicazioni etiche ed, inoltre, rimane il pericolo di essere scoperti a causa delle anomalie nella linea o nella bolletta telefonica di qualcun altro. Il buon Hydra, nel lontano 1988, era solito – abitando in un piccolo condominio di 6 appartamenti più due negozi – utilizzare le linee delle utenze commerciali (la pellicciaia sotto casa) per chiamate internazionali o interurbane di breve durata, mentre utilizzava "a rotazione" le linee telefoniche dei vicini (privati) per chiamate lunghe ed urbane, nelle ore notturne.

   Ad ogni modo è buona norma utilizzare dialup su numeri verdi (800) in alternativa alle brevi chiamate, ma si possono anche utilizzare le linee telefoniche di telefoni a pagamento, linee affari o ancora utenze telefoniche in zone "vip", dove chiunque può permettersi una bolletta leggermente più alta senza insospettirsi troppo.

2) **Non iniziate una sessione di hacking da un dialup server se state chiamando da casa**. Potete cancellare i log del vostro sistema operativo, modem e così via ma, in questo caso, l'attaccato verificherà i dial-in ricevuti e cercheranno numeri "non riconosciuti" o fuori standard (tante chiamate consecutive, chiamate alle 4 di mattina, etc…): i log della compagnia telefonica non si cancellano con troppa facilità.

3) **Utilizzate il cellulare quando possibile.** Chiamando da un cellulare clonato (TACS) o da un GSM con il device SIM non direttamente intestato a voi; le convenienze logistiche e pratiche sono ovvie: il solo modo per tracciarvi è "direzionalmente", trovando la fonte del segnale mentre siete on-line.

4) **Criptate i vostri dati**. Questo può essere fatto installando un programma di cifratura sulla vostra workstation, una partizione cifrata, o ancora installando il server sul Launchpad system remoto ed il Client sulla vostra workstation (in questo caso parlo di cifratura dei dati in transito, del flusso insomma, e non dell'off-line). In questo modo tutte le comunicazioni tra il vostro computer ed il Launchpad saranno criptate e qualunque apparato di intercettazione dati installato sulla vostra utenza telefonica registrerà il classico "garbage".

***

2 – PULIZIA DEI LOG

Quando si entra in un sistema il NUA originale di chiamata viene registrato da qualche parte. Al fine di evitare il tracciamento all'indietro sino a quel NUA (e magari da quello ai NUA precedenti di bounce) si devono alterare i log affinchè non mostrino più da dove siete arrivati.

Il "Log Doctoring" serve anche per un secondo scopo: evita che nel sistema target capiscano (in qualunque modo, per controllo a scadenza fissa, per caso, etc..) che c'è un intruso ed applichino le procedure di tracing.

***

3 - LAUNCHPAD (BOUNCE)

Un Launchpad System, o sistema di "Bounce", è quel sistema che si utilizza per essere ruotati su altri sistemi ed altri reti X.25, ma si usa sempre come base di partenza. E' un sistema dove ci sentiamo a nostro agio, dove siamo presenti da diverso tempo e del quale conosciamo alla perfezione orari, policy, abitudini, budget. In questo sistema modifichiamo sempre i log delle chiamate in ingresso ed in uscita in modo tale da evitare azioni di tracing o data collect su di noi, nel caso in cui non sia possibile alterare i log sui sistemi seguenti (quelli chiamati dal Launchpad).

Un buon sistema di partenza ha in genere un basso livello di sicurezza, con sysadmin pigri o non aggiornati: è il sistema dove i log sono facilmente alterabili ed i processi possono essere tenuti sotto controllo con facilità (tipicamente la descrizione di una UNIX Box ☺

Non si deve ovviamente utilizzare esclusivamente il Launchpad, più sono i sistemi di bounce utilizzati e minori sono le possibilità di tracing: se poi su ogni bounce si alterano i log diciamo che la strada è sufficientemente sicura. Come ultimo consiglio ricordo che utilizzando bounce "oltreoceano", del tipo dall'Europa all'Asia, dall'Asia agli USA, rende molto difficile il dialogo tra i carrier in caso di richiesta di log dalle autorità: se poi usiamo il cervello e seguiamo un minimo la politica, appare ovvio come le autorità di Cuba difficilmente fornirebbero i loro log all'FBI per attacchi verso reti X.25 americane.

***

4 – HACKING CON CLASSE (INVISIBLE HACKING)

Come ultimo consiglio, quello più importante: se non ci si fa scoprire non ci si fa tracciare. Quindi, fare del proprio meglio per evitare di fare notare la nostra presenza al Sysadmin: in molti hacking files noterete come le voci "etica" e "sicurezza" capitino sempre sotto la stessa voce. Questo perché fare cose che danneggiano il sistema, l'azienda target o gli utenti portano forzatamente alla scoperta dell'intrusione.

Un buon metodo è anche quello di sorvegliare le mail degli Admin del sistema Launchpad e degli hop immediatamente successivi, per vedere se sono state inviate mail di alert o di richiesta (richieste di log in quanto non presenti sul sistema chiamante, etc..), così come vedere se sull'OS vi sono comunque attività strane di verifica o processi "strani".

ALLEGATO A

Country/Area DNIC
No.
Name of network to which a DNIC is allocated

ALGERIA
603 0 DZ PAC (Réseau public de données à commutation par paquet)
GERMANIA
262 1 ISDN/X.25
262 2 Circuit Switched Data Service (DATEX-L)
262 4 Packet Switched Data Service (DATEX-P)
262 5 Satellite Services
262 7 Teletex
262 9 D2-Mannesmann
263 1 CoNetP
263 3 DPS
263 6 EPS
264 0 DETECON
264 1 SCN
264 2 INFO AG NWS
264 3 ALCANET
264 4 IDNS
264 5 INAS-net
264 6 EuroDATA
264 7 MEGANET
264 8 SNSPac
264 9 MMONET
265 0 BB-DATA-NET
265 1 WestLB X.25 Net
265 2 PSN/FSINFOSYSBW
265 3 PAKNET DB
265 4 TNET
265 5 ISIS_DUS
265 6 RWE TELPAC
265 7 DTN/AutoFüFmNLw
265 8 DRENET
ANGOLA
631 5 ANGOPAC
ANDORRA
213 5 ANDORPAC
ANTIGUA-ET-BARBUDA
344 3 Antigua Packet Switched Service
ANTILLE OLANDESI
362 0 TELEMATIC NETWORK
362 1 DATANET CURACAO
ARABIA SAUDITA
420 1 ALWASEET - Public Packet Switched Data Network
ARGENTINA
722 1 Nodo Internacional de Datos - TELINTAR
722 2 ARPAC (ENTEL)
722 3 EASYGATE (ATT)
ARMENIA
283 0 ArmPac
AUSTRALIA
505 2 Telstra Corporation Ltd. - AUSTPAC packet switching network
505 3 Telstra Corporation Ltd. - AUSTPAC International
505 7 Australian Private Networks
AUTRIA
232 2 Dataswitch (DATAKOM)
232 9 Radausdata (DATAKOM)
AZERBAIDJAN
400 1 AZPAK (Azerbaijan Public Packet Switched Data Network)
400 2 “AzEuroTel” Joint Venture
BAHREIN
426 0 Batelco GSM Service
426 2 Bahrain Managed Data Network (MADAN)
426 3 Batelco Packet Switched Node
BARBADOS
342 2 CARIBNET

342 3 International Data Base Access Service (IDAS)
BELARUS
257 0 BELPAK
BELGIO
206 2 Réseau de transmission de données à commutation par paquets (DCS)
206 4 CODENET
206 5 (le code est utilisé au niveau national pour le réseau DCS)
206 6 Unisource Belgium X.25 Service
206 7 MOBISTAR
206 8 Accès au réseau DCS via le réseau télex commuté national
206 9 Accès au réseau DCS via le réseau téléphonique commuté national.
BERMUDA
350 2 Cable and Wireless Data Communications Node
350 3 Cable and Wireless Packet Switched Node
BOSNIA ERZEGOVINA
218 0 BIHPAK
BRASILE
724 0 International Packet Switching Data Communication Service (INTERDATA)
724 1 National Packet Switching Data Communication Service (RENPAC)
724 2 RIOPAC
724 3 MINASPAC
724 4 TRANSPAC
724 5 Fac Simile Service (DATA FAX)
724 6 BRAZILIAN PRIVATE NETWORKS
724 7 DATASAT BI
725 1 S.PPAC
725 2 TELEST PUBLIC PACKET DATA NETWORK
725 3 TELEMIG Public Switched Packet Data Network
725 4 PACPAR
725 5 CRT/CTMR
725 6 Western and Midwestern Public Switched Packet Data Network
725 7 TELEBAHIA and TELERGIPE Public Switched Packet Data Network
725 8 Northeastern Public Switched Packet Data Network
725 9 Northern Public Switched Packet Data Network
BURKINA FASO
613 2 FASOPAC
CAMEROON
624 2 CAMPAC
CANADA
302 0 Telecom Canada Datapak Network
302 1 Telecom Canada PSTN Access
302 2 Stentor Private Packet Switched Data Network Gateway
302 3 Stentor ISDN Identification
302 4 Teleglobe Canada - Globedat-C Circuit Switched Data Transmission
302 5 Teleglobe Canada - Globedat-P Packed Switched Data Transmission
302 6 AT&T Canada Long Distance Services – FasPac
302 8 AT&T Canada Long Distance Services – Packet Switched Public Data Network (PSPDN)
303 5 North American Gateway – International Carrier ATM/Frame Relay Network
303 6 Sprint Canada Frame Relay Service - Packet-Switched Network
303 7 TMI Communications, Limited Partnership — Mobile Data Service (MDS) X.25 public switched data network
303 8 Canada Post — POSTpac — X.25 Packet Switched Data Network
303 9 Telesat Canada — Anikom 200
CAPO VERDE
625 5 CVDATA
CAYMAN (ISOLE)
346 3 Cable and Wireless Packet Switching Node
CHILE
730 2 Red nacional de transmisión de datos
730 3
730 5 Vtr/TomNET
CINA
460 0 reserved for international service
460 1 Teletex and low speed data network
460 2 CHINAPAC 1 (Public Packet Switched Data Network)
460 3 CHINAPAC
460 4 reserved for public mobile data service
460 5 Public data network
460 6 Dedicated network
460 7 Dedicated network
460 8 Dedicated network
460 9 Public data network
CIPRO
280 2 CYTAPAC - PSDN, subscribers with direct access

280 8 CYTAPAC - PSDN, subscribers with access via telex
280 9 CYTAPAC - PSDN, subscribers with access via PSTN - X.28, X.32
COLOMBIA
732 2 COLDAPAQ
732 1 RED DE ALTA VELOCIDAD
COREA (REP. DI)
450 0 HiNET-P (KOREA TELECOM)
(REP. OF) 450 1 DACOM-NET
(REP. DE) 450 2 CSDN (attribué seulement au télétex/only assigned to Teletex/ atribuido solamente al teletex)
COSTA RICA
712 0 RACSADATOS
712 2
COSTA D'AVORIO
612 2 SYTRANPAC
CROAZIA
219 1 CROAPAK (Croatian Packet Switching Data Network)
CUBA 368 0 Servicios de información por conmutación de paquetes del IDICT
DANIMARCA
238 0 Tele Danmark A/S
238 1 DATEX (Circuit Switched Network)
238 2 DATAPAK (Packet Switched Network)
238 3 DATAPAK (Packet Switched Network)
238 4 Transpac
238 5 SONOFON GSM
DOMINICAINE (REP.)
370 6 All America Cables and Radio Inc.
EGITTO
602 6 EGYPTNET
EMIRATI ARABI UNITI
424 1 EMDAN Teletex Network
424 3 EMDAN X.25 and X.28 Terminals
SPAGNA
214 0 Administración Pública
214 1 Nodo internacional de datos
214 2 RETEVISIÓN
214 5 Red IBERPAC
214 7 France Telecom Redes y Servicios
214 9 MegaRed
ESTONIA
248 0 ESTPAK
USA
310 1 PTN-1 Western Union Packet Switching Network
310 2 MCI Public Data Network (ResponseNet)
310 3 ITT UDTS Network
310 4 MCI Public Data Network (International Gateway)
310 5 WUI Leased Channel Network
310 6 MCI Public Data Network (XStream)
310 7 ITT Datel Network
310 8 ITT Short Term Voice/Data Transmission Network
310 9 RCAG DATEL II
311 0 Telenet Communications Corporation
311 1 RCAG DATEL I (Switched Alternate Voice-Data Service)
311 2 Western Union Teletex Service
311 3 RCAG Remote Global Computer Access Service (Low Speed)
311 4 Western Union Infomaster
311 5 Graphnet Interactive Network
311 6 Graphnet Store and Forward Network
311 7 WUI Telex Network
311 8 Graphnet Data Network
311 9 TRT Packet Switching Network (IPSS)
312 0 ITT Low Speed Network
312 1 FTCC Circuit Switched Network
312 2 FTCC Telex
312 3 FTCC Domestic Packet Switched Transmission (PST) Service
312 4 FTCC International PST Service
312 5 UNINET
312 6 ADP Autonet
312 7 GTE Telenet Communications Corporation
312 8 TRT Mail/Telex Network
312 9 TRT Circuit Switch Data (ICSS)
313 0 TRT Digital Data Network
313 1 RCAG Telex Network
313 2 Compuserve Network Services

313 3 RCAG XNET Service
313 4 AT+T/ACCUNET Packet Switched Capability
313 5 ALASCOM/ALASKANET Service
313 6 Geisco Data Network
313 7 International Information Network Services - INFONET Service
313 8 Fedex International Transmission Corporation - International Document Transmission Service
313 9 KDD America, Inc. – Public Data Network
314 0 Southern New England Telephone Company - Public Packet Network
314 1 Bell Atlantic Telephone Companies - Advance Service
314 2 Bellsouth Corporation - Pulselink Servie
314 3 Ameritech Operating Companies - Public Packet Data Networks
314 4 Nynex Telephone Companies - Nyex Infopath Service
314 5 Pacific Telesis Public Packet Switching Service
314 6 Southwestern Bell Telephone Co. - Microlink II Public Packet Switching Service
314 7 U.S. West, Inc. - Public Packet Switching Service
314 8 United States Telephone Association - to be shared by local exchange telephone companies
314 9 Cable & Wireless Communications, Inc. - Public Data Network
315 0 Globenet, Inc. - Globenet Network Packet Switching Service
315 1 Data America Corporation - Data America Network
315 2 GTE Hawaiian Telephone Company, Inc. - Public Data Network
315 3 JAIS USA-NET Public Packet Switching Service
315 4 Nomura Computer Systems America, Inc. - NCC-A VAN public packet switching service
315 5 Aeronautical Radio, Inc. - GLOBALINK
315 6 American Airlines, Inc. - AANET
315 7 COMSAT Mobile Communications - C-LINK
315 8 Schlumberger Information Network (SINET)
315 9 Westinghouse Communications - Westinghouse Packet Network
316 0 Network Users Group, Ltd. - WDI NET packet
316 1 United States Department of State, Diplomatic Telecommunications Service Black Packet Switched Data Network
316 2 Transaction Network Services, Inc. -- TNS Public Packet-switched Network
316 6 U.S. Department of Treasury Wide Area Data Network

FAROE (ISOLE)
288 1 FAROEPAC

FIJI
542 0 FIJPAK
542 1 FIJINET

FINLANDIA
FINLANDE 244 2 Datapak
FINLAND 244 3 Finpak (Packet Switched Data Network PSDN) of Helsinki Telephone Company Ltd.
FINLANDIA 244 4 Telia Finland Ltd.

FRANCIA
FRANCE 208 0 Réseau de transmission de données à commutation par paquets TRANSPAC
FRANCE 208 1 Noeud de transit international
FRANCIA 208 2 Grands services publics
208 3 Administrations
208 4 Air France
208 5 SIRIS
208 6 BT France
208 9 Interconnexion entre le réseau public de transmission de données Transpac et
d'autres réseaux publics français, pour des services offerts en mode synchrone

GABON
GABON 628 0 GABONPAC (Réseau de transmission de données à commutation par paquets)
GABON 628 2 GABONPAC2

GAMBIA
GAMBIE 607 0 GAMNET

GEORGIA
GEORGIE 282 1 IBERIAPAC

GHANA
GHANA 620 2 DATATEL

GRECIA
GRECE 202 3 Packet Switched Public Data Network (HELLASPAC)
GREECE 202 7 LAN-NET
GRECIA.Annex to ITU OB 714-E – 10 – 15.04.2000

GRENADA
GRENADE 352 2 CARIBNET

GROENLANDIA
GROENLAND 290 1 DATAPAK (Packet Switched Network)

GUAM
GUAM 535 1 The Pacific Connection, Inc. - Pacnet Public Packet Switching Service

GUYANA FRANCESE
GUYANA 738 0 GT&T PAC

HONDURAS
HONDURAS 708 0 HONDUPAQ

HONG KONG
HONGKONG 454 0 Public Switched Document Transfer Service
HONGKONG 454 1 Hutchison Communications Limited
HONGKONG 454 2 INTELPAK
454 3 New T&T
454 5 DATAPAK
454 6 AT&T EasyLink Services, Asia/Pacific Limited (AT&T EasyLink services)
454 7 New World Telephone Limited
454 8 KDD Telecomet Hong Kong Ltd.
UNGHERIA
HONGRIE 216 0 Circuit Switched Data Service
HUNGARY 216 1 Packet Switched Data Service
HUNGRIA 216 4 GTSNet
216 5 Packet Switched Private Data Networks (DNIC shared by a number of private networks)
216 6 Packet Switched Public Data Networks (DNIC shared by a number of public networks)
INDIA
INDE 404 1 RABMN
INDIA 404 2 International Gateway Packet Switching System (GPSS)
INDIA 404 3 INET (Packet Switched Public Data Network)
INDONESIE 510 1 SKDP Packet Switched Service (Sambungan Komunikasi Data Paket)
INDONESIA
INDONESIA.Annex to ITU OB 714-E – 11 – 15.04.2000
INMARSAT (OCEANI)
INMARSAT 111 1 Atlantic Ocean-East
111 2 Pacific Ocean
111 3 Indian Ocean
111 4 Atlantic Ocean-West
IRAN
IRAN (REPUBLIQUE ISLAMIQUE D') 432 1 IranPac
IRAN (ISLAMIC REPUBLIC OF)
IRAN (REPUBLICA ISLAMICA DEL)
IRLANDA
IRLANDE 272 1 International Packet Switched Service
IRELAND 272 3 EURONET
IRLANDA 272 4 EIRPAC (Packet Switched Data Networks)
272 8 PostNET (PostGEM Packet Switched Data Network)
ISLANDA/ICELAND
ISLANDE 274 0 ISPAK/ICEPAC
ISRAELE
ISRAEL 425 1 ISRANET
ITALIA
ITALIE 222 1 Rete Telex-Dati (Amministrazione P.T. / national)
ITALY 222 2 ITAPAC X.25
ITALIA 222 3 PAN (Packet Network)
222 6 ITAPAC - X.32 PSTN, X.28, D channel
222 7 ITAPAC International
223 3 ALBADATA X.25
223 4 Trasmissione dati a commutazione di pacchetto X.25 (UNISOURCE ITALIA S.p.A.)
223 5 Trasmissione dati a commutazione di pacchetto X.25 (INFOSTRADA S.p.A.)
223 6 Trasmissione dati a commutazione di pacchetto X.25 (WIND Telecomunicazioni S.p.A.)
JAPAN/GIAPPONE
JAPON 440 0 GLOBALNET (Network of the Global VAN Japan Incorporation)
JAPAN 440 1 DDX-P (NTT Communications Corporation)
JAPON 440 2 NEC-NET (NEC Corporation)
440 3 JENSNET (JENS Corporation)
440 4 JAIS-NET (Japan Research Institute Ltd.)
440 5 NCC-VAN (NRI Co., Ltd.)
440 6 TYMNET-JAPAN (JAPAN TELECOM COMMUNICATIONS SERVICES CO., LTD.)
440 7 International High Speed Switched Data Transmission Network (KDD)
440 8 International Packet Switched Data Transmission Network (KDD)
441 2 Sprintnet (Global One Communications, INC.)
441 3 KYODO NET (UNITED NET Corp)
441 5 FENICS (FUJITSU LIMITED)
441 6 HINET (HITACHI Information Network, Ltd.)
441 7 TIS-Net (TOYO Information Systems Co., Ltd.)
441 8 TG-VAN (TOSHIBA Corporation)
JAPON 442 0 Pana-Net (MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD.)
JAPAN 442 1 DDX-P (NTT Communications Corporation)
JAPON 442 2 CTC-P (CHUBU TELECOMMUNICATIONS CO., INC.)
442 3 JENSNET (JENS Corporation)
442 4 SITA NETWORK
442 5 GLOBAL MANAGED DATA SERVICE (Cable & Wireless IDC-Si)
442 6 ECHO-NET (HITAHC INFORMATION SYSTEMS LTD.)

442 7 U-net (NIHON UNYSYS INFORMATION SYSTEMS LTD.)
KAZAKISTAN
KAZAKSTAN 401 0 KazNet X.25
KAZAKSTAN 401 1 BankNet X.25
KENYA
KENYA 639 0 KENPAC - Telkom Kenya Ltd.
LETTONIA
LETTONIE 247 1 Latvia Public Packed Switched Data Network
LATVIA
LETONIA
L'EX-REPUBLIQUE
YOUGOSLAVE DE MACEDOINE
MACEDONIA
294 0 MAKPAK
THE FORMER YUGOSLAV
REPUBLIC OF MACEDONIA
LA EX REPUBLICA
YUGOSLAVA DE MACEDONIA
LIBANO
LIBAN 415 5 Réseau public de transmission de données par paquets
LEBANON
LIBANO
LITUANIA
LITUANIE 246 2 Vilnius DATAPAK
LITHUANIA 246 3 LITCOM
LITUANIA
LUSSEMBURGO
LUXEMBOURG 270 2 CODENET
LUXEMBOURG 270 3 RAPNET (Regional ATS Packet Switched Network)
LUXEMBURGO 270 4 LUXPAC (réseau de transmission de données à commutation par paquets)
270 5 LUXNET (interconnection entre le réseau public de transmission de données
et d'autres réseaux publics luxembourgeois)
270 9 LUXPAC (accès X.28 et X.32 au réseau téléphonique commuté).Annex to ITU OB 714-E – 13 – 15.04.2000
MACAO
MACAU 455 0 MACAUPAC
MACAU
MACAU
MADAGASCAR
MADAGASCAR 646 0 INFOPAC
MADAGASCAR
MADAGASCAR
MALESIA
MALAISIE 502 1 Malaysian Public Packet Switched Public Data Network (MAYPAC)
MALAYSIA 502 3 Corporate Information Networks
MALASIA 502 4 ACASIA-ASEAN Managed Overlay Network
502 6 Mutiara Frame Relay Network
502 7 Mobile Public Data Network (WAVENET)
502 8 Global Management Data Services (GMDS)
MALDIVE
MALDIVES 472 0 DATANET (Maldives Packet Switching Service)
MALDIVES
MALDIVAS
MALTA
MALTE 278 2 MALTAPAC (Packet Switching Service)
MALTA
MALTA
MAROCCO
MAROC 604 1 MAGHRIPAC
MOROCCO 604 2 MAGHRIPAC X.32
MARRUECOS 604 9 MAGHRIPAC RTC PAD
MESSICO
MEXIQUE 334 0 TELEPAC
MEXICO 334 1 UNITET
MEXICO 334 2 IUSANET
334 3 TEI
334 4 OPTEL
334 5 TELNORPAC
334 6 TYMPAQ
334 7 SINFRARED
334 8 INTERVAN
334 9 INTELCOMNET
335 0 AVANTEL, S.A.
335 1 ALESTRA, S. DE R.L. DE C.V.

MICRONESIA
MICRONESIE 550 1 FSMTC Packet Switched Network
MICRONESIA
MICRONESIA.Annex to ITU OB 714-E – 14 – 15.04.2000
MOZAMBICO
MOZAMBIQUE 643 5 COMPAC (Packet Switching Public Data Network)
MOZAMBIQUE
MOZAMBIQUE
MYANMAR
MYANMAR 414 1 MYANMARP
MYANMAR
MYANMAR
NAMIBIA
NAMIBIA 649 0 SWANET (Public Packet Switched Network)
NAMIBIA
NAMIBIA
NEPAL
NÉPAL 429 0 NEPPAK (Nepal Packet Switched Public Data Network)
NEPAL
NEPAL
NICARAGUA
NICARAGUA 710 0 NicaPac
NICARAGUA
NICARAGUA
NORVEGIA
NORVEGE 242 1 DATEX (Circuit Switched Network, CSDN)
NORWAY 242 2 DATAPAK (Packet Switched Network, PSDN)
NORUEGA 242 9 Shared by private data networks, for PNIC allocation
NOUVELLE-CALEDONIE 546 0 Transpac - Nouvelle Calédonie et opérateur public local
NUOVA CALEDONIA
NEW CALEDONIA
NUEVA CALEDONIA
NUOVA ZELANDA
NOUVELLE-ZELANDE 530 1 PACNET Packet Switching Network
NEW ZEALAND
NUEVA ZELANDIA
UZBEKISTAN
OUZBEKISTAN 434 1 UzPAK
UZBEKISTAN
UZBEKISTAN
PAKISTAN
PAKISTAN 410 1 TRANSLINK
PAKISTAN
PAKISTAN
PANAMA
PANAMA 714 1 Red de transmisión de datos con conmutación de paquetes (INTELPAQ)
PANAMA 714 4 CWP DATA NETWORK
PANAMA.Annex to ITU OB 714-E – 15 – 15.04.2000
PARAGUAY
PARAGUAY 744 0 PARABAN
PARAGUAY 744 7 ANTELPAC
PARAGUAY 744 8 PARAPAQ
PAESI BASSI (OLANDA)
PAYS-BAS 204 1 Datanet 1 X.25 access
NETHERLANDS 204 4 Unisource / Unidata
PAISES BAJOS 204 6 Unisource / VPNS
205 2 NV CasTel
205 3 Global One Communications BV
205 5 Rabofacet BV
205 7 Trionet v.o.f.
PERU
PEROU 716 0 MEGANET (PERUNET)
PERU 716 1 MEGANET
PERU
PHILIPPINES/FILIPPINE
PHILIPPINES 515 1 CWI DATANET - Capitol Wireless, Inc. (CAPWIRE)
PHILIPPINES 515 2 Philippine Global Communications, Inc. (PHILCOM)
FILIPINAS 515 4 Globe-Mackay Cable and Radio Corp. (GMCR)
515 6 Eastern Telecommunications Philippines, Inc. (ETPI)
515 7 DATAPAC
POLONIA
POLOGNE 260 1 POLPAK
POLAND 260 2 NASK

POLONIA 260 3 TELBANK
260 4 POLPAK -T
260 5 PKONET
260 6 Shared by a number of data networks
260 7 CUPAK
POLINESIA FRANCESE
POLYNESIE FRANCAISE 547 0 Transpac - Polynésie et opérateur public local
FRENCH POLYNESIA
POLINESIA FRANCESA
PORTOGALLO
PORTUGAL 268 0 TELEPAC
PORTUGAL 268 1 COMNEXO, Redes de Comunicações, S.A.
PORTUGAL 268 2 CPRM-Marconi
268 3 Eastécnica, Electrónica e Técnica, S.A.
268 4 SIBS, Sociedade Interbancária de Serviços, S.A.
268 5 Global One – Comunicações, S.A.
268 6 HLC, Telecomunicações & Multimédia, S.A.
PORTO RICO
PUERTO RICO 330 2 ATM Broadband Network
PUERTO RICO
PUERTO RICO.Annex to ITU OB 714-E – 16 – 15.04.2000
QATAR
QATAR 427 1 DOHPAK
QATAR
QATAR
REPUBBLICA CECOSLOVACCA
REP. TCHEQUE 230 1 NEXTEL
CZECH REP. 230 2 Aliatel
REP. CHECA
ROMANIA
ROUMANIE 226 0 ROMPAC
ROMANIA
RUMANIA
ROYAUME-UNI 234 0 BT
UK REGNO UNITO
UNITED KINGDOM 234 1 International Packet Switching Service (IPSS)
REINO UNIDO 234 2 Packet Switched Service (PSS)
234 3 BT Concert Packet Network
234 4 BT Concert Packet Network
234 7 BT
234 8 BT
234 9 Barclays Technology Services
235 0 C&W X.25 Service, International Packet Gateway
235 1 C & W X.25 Service
235 2 Kingston Communications (Hull) PLC.
235 3 Vodaphone, Packet Network Service
235 4 Nomura Computer Systems Europe Ltd. (NCC-E)
235 5 JAIS Europe Ltd.
235 7 FEDEX UK
235 8 Reuters
235 9 BT
236 0 AT&T ISTEL
237 0 GlobalOne (France Telecom)
237 8 Racal Telecom
RUSSIA
RUSSIE 250 0 ROSPACK
RUSSIA 250 1 SPRINT Networks
RUSIA 250 2 IASNET
250 3 MMTEL
250 4 INFOTEL
250 6 ROSNET
250 7 ISTOK-K
250 8 TRANSINFORM
250 9 LENFINCOM
251 0 SOVAMNET
251 1 EDITRANS
251 2 TECOS
251 3 PTTNET
251 4 BCLNET
251 5 SPTNET.Annex to ITU OB 714-E – 17 – 15.04.2000
SAN MARINO
SAINT–MARIN 292 2 X-Net SMR
SAN MARINO

SAN MARINO
SALOMONE (ISOLE)
SALOMON 540 0 DATANET
SOLOMON
SALOMON
SENEGAL
SENEGAL 608 1 SENPAC
SENEGAL
SENEGAL
SINGAPORE
SINGAPOUR 525 2 TELEPAC (Public Packet Switching Data Network)
SINGAPORE 525 7 ISDN packet switching service
SINGAPUR
SLOVACCHIA
SLOVAQUIE 231 1 EuroTel
SLOVAKIA
ESLOVAQUIA
SLOVÉNIE 293 1 SIPAX.25
SLOVENIA 293 2 SIPAX.25 access through ISDN
ESLOVENIA
SRI LANKA
SRI LANKA 413 3 M/S Electroteks Private Ltd.
SRI LANKA
SRI LANKA
SUD AFRICA
SUDAFRICAINE (REP.) 655 0 Saponet – P
SOUTH AFRICA
SUDAFRICANA (REP.)
SVEZIA
SUEDE 240 1 Datex (Public Circuit Switched Data Network)
SWEDEN 240 2 WM-data Infrastructur
SUECIA 240 3 Datapak (Public Packet Switched Data Network)
240 6 Flex25 (Public Packet Switched Data Network)
240 7 Private X.25 Networks (DNIC shared by a number of private networks)
240 8 TRANSPAC Scandinavia AB
SVIZZERA
SUISSE 228 0 ISDNPac
SWITZERLAND 228 2 Transpac-CH
SUIZA 228 4 Telepac
228 5 Telepac (accès de réseaux privés)
228 6 DataRail.Annex to ITU OB 714-E – 18 – 15.04.2000
CHAD
TCHAD 622 2 TCHADPAC
CHAD
CHAD
TAILANDIA
THAILANDE 520 1 THAIPAK 1 - Public Packet Switched Data Network
THAILAND 520 2 THAIPAK 2 - Value Added Public Packet Switched Data Network
TAILANDIA 520 3 CAT Store and Forward Fax Network
520 9 TOT ISDN
TONGA
TONGA 539 0 TONGAPAK
TONGA
TONGA
TRINIDAD E TOBAGO
TRINITE-ET-TOBAGO 374 0 TEXDAT
TRINIDAD AND TOBAGO 374 5 DATANETT
TRINIDAD Y TABAGO
TURQUES E CAICOS
TURQUES ET CAIQUES (ILES) 376 3 Cable and Wireless Packet Switched Node
TURKS AND CAICOS ISLANDS
TURQUESAS Y CAICOS (ISLAS)
TURCHIA
TURQUIE 286 0 TELETEX
TURKEY 286 1 DATEX-L
TURQUIA 286 3 Turkish Packet Switched Data Network (TURPAK)
286 4 TURPAK
UCRAINA
UKRAINE 255 0 UkrPack
UKRAINE 255 1 bkcNET
UCRANIA
URUGUAY
URUGUAY 748 2 URUPAC - Servicio público de transmisión de datos con conmutación de paquetes

URUGUAY 748 8 URUPAC - Interfuncionamiento con la red télex
URUGUAY 748 9 URUPAC - Interfuncionamiento con la red telefónica
VANUATU
VANUATU 541 0 VIAPAC (Vanuatu International Access for Packets)
VANUATU
VANUATU
VATICANO (STATO DEL)
VATICAN 225 0 Packet Switching Data Network (PSDN) of Vatican City State
VATICAN
VATICANO
YUGOSLAVIA
YOUGOSLAVIE 220 1 YUPAC (Yugoslav Packet Switched Public Data Network)
YUGOSLAVIA
YUGOSLAVIA.Annex to ITU OB 714-E – 19 – 15.04.2000
ZAMBIA
ZAMBIE 645 1 ZAMPAK
ZAMBIA
ZAMBIA
ZIMBAWE
ZIMBABWE 648 4 ZIMNET
ZIMBABWE
ZIMBABWE

ALLEGATO B

Australian Network Identifiers:

Prefix	Allocation Date	Organisation
5052	30 June 1991	Telstra Corporation Ltd
5053	30 June 1991	Telstra Corporation Ltd
50541	6 September 1994	AAPT Ltd
50542	6 September 1994	AAPT Ltd
50543	6 September 1994	AAPT Ltd
50560	16 February 1994	SingCom (Australia) Pty Ltd
50568	16 February 1994	SingCom (Australia) Pty Ltd
50569	16 February 1994	SingCom (Australia) Pty Ltd
50573000	30 June 1991	Fujitsu Australia Ltd
50573500	19 February 1992	Department Of Defence
505790	17 November 1993	Department Of Defence
505791	17 November 1993	Department Of Defence
505799	23 February 1995	Telstra Corporation Ltd

5052 = Austpac
5053 = Austpac International (formerly Midas / OTC Data Access)
5054 = Australian Teletex Network
5057 = Australian Private Networks

NB The allocation dates are official allocation dates, not necessarily actual dates. Austpac existed long before 1991.

ALLEGATO C

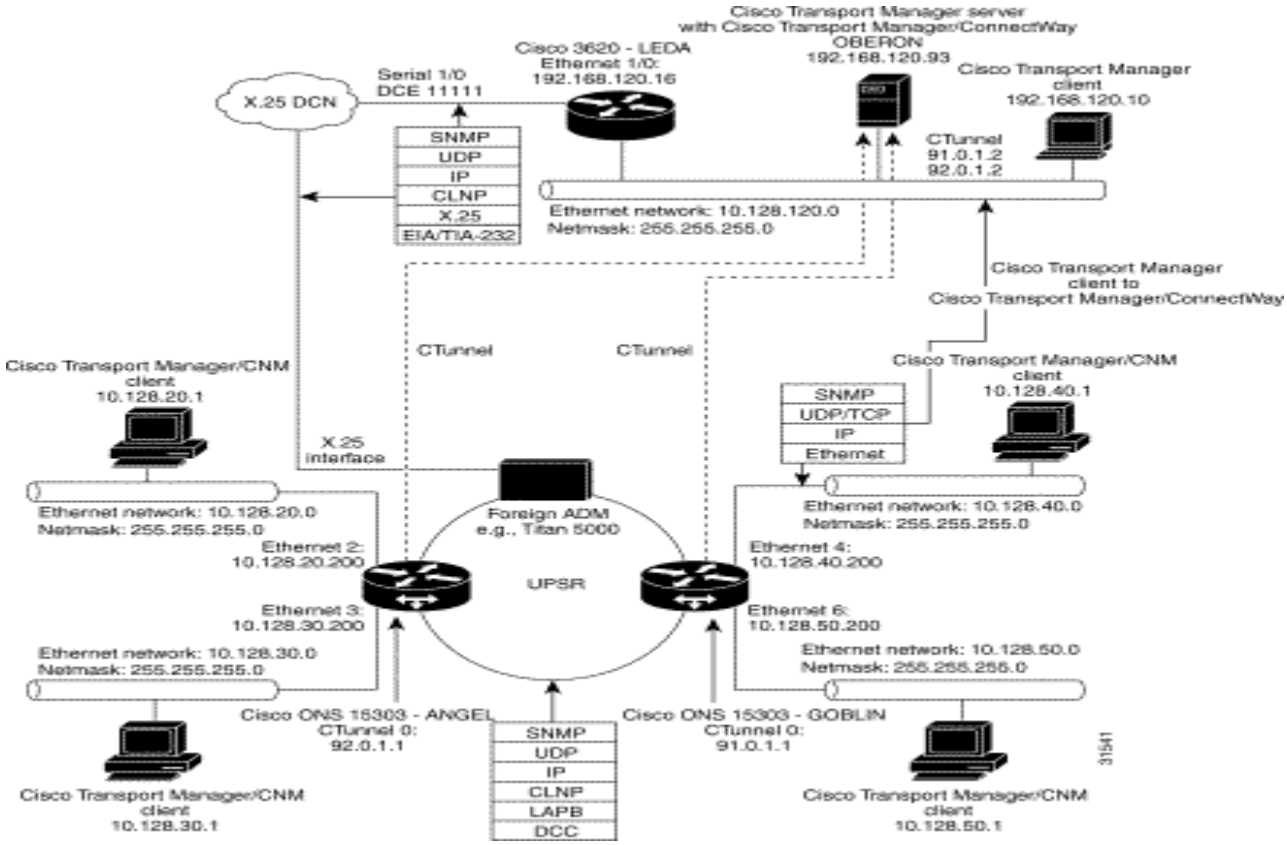
Subject: qsd...
Date: Tue, 04 Sep 2001 16:59:52 +0200
From: xxxxxx <xxxxx@xxxxxxx-xxxxxxx.com>
Organization: xxxxxxx-xxxxxxx
To: Raoul Chiesa <raoul@mediaservice.net>

qsd is definitely down... NP.
:-(

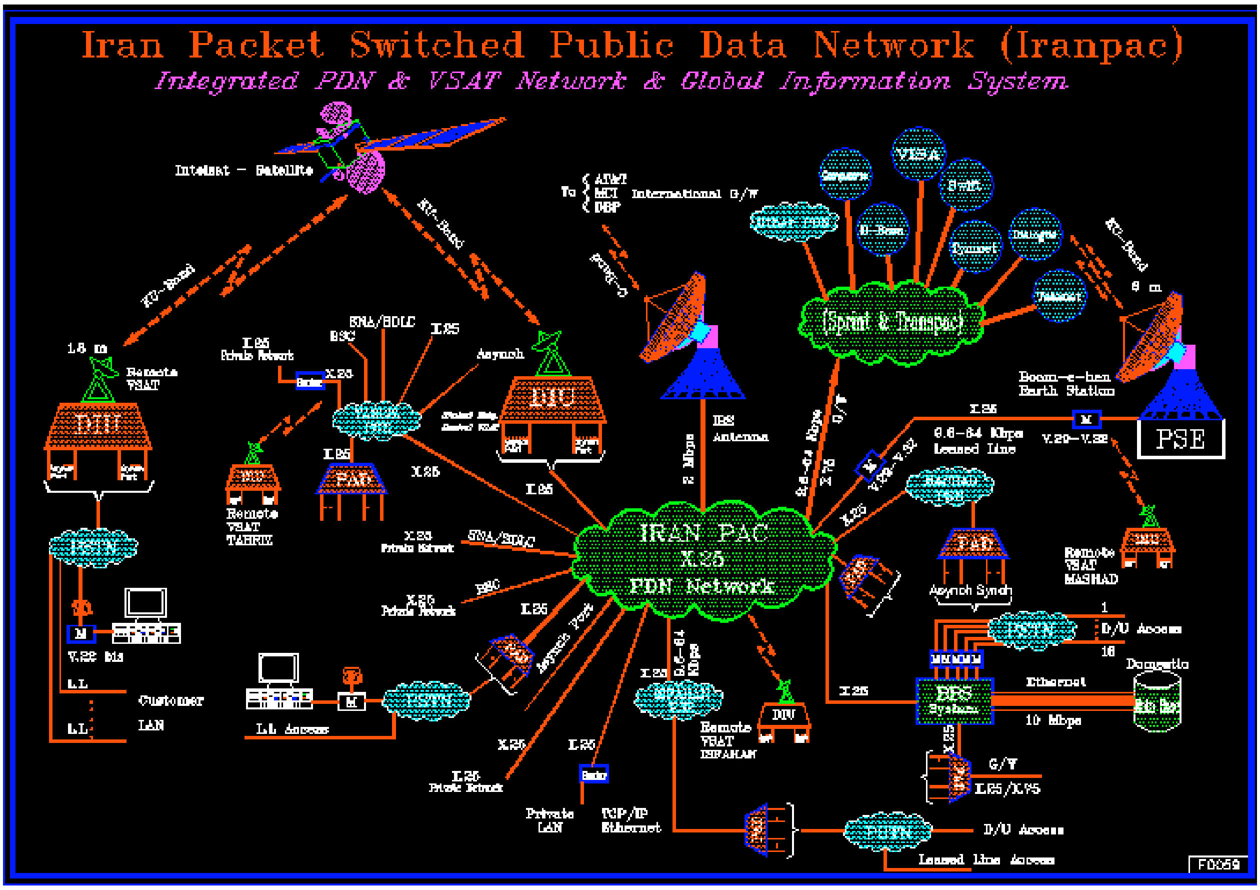
```
 ####    #####  #####                Software SICOMM France
##  ##  ##      ##  ##
##  ##   ####   ##  ##              You Are on QSD (France)
##  #       ##  ##  ##           International Chat System
 #####  #####   #####                    Free Access
 /// // /////   /////
//  //      //  //  //
//   //  ////   //  //                 For fun and friends !
//   // //      //  //           No pirating nor hacking Please !
/////   /////  /////
```

- QSD, International Chat System: 15 anni di hacking -
Videata Commemorativa

ALLEGATO D


Cisco Transport Manager server
with Cisco Transport Manager/ConnectWay
OBERON
192.168.120.93
Cisco 3620 - LEDA
Ethernet 1/0:
192.168.120.16
Serial 1/0
DCE 11111
X.25 DCN
Cisco Transport Manager
client
192.168.120.10
CTunnel
91.0.1.2
92.0.1.2
SNMP
UDP
IP
CLNP
X.25
EIA/TIA-232
Ethernet network: 10.128.120.0
Netmask: 255.255.255.0
Cisco Transport Manager
client to
Cisco Transport Manager/ConnectWay
CTunnel
CTunnel
Cisco Transport Manager/CNM
client
10.128.20.1
Cisco Transport Manager/CNM
client
10.128.40.1
SNMP
UDP/TCP
IP
Ethernet
X.25
interface
Foreign ADM
e.g., Titan 5000
Ethernet network: 10.128.20.0
Netmask: 255.255.255.0
Ethernet 2:
10.128.20.200
Ethernet network: 10.128.40.0
Netmask: 255.255.255.0
Ethernet 4:
10.128.40.200
UPSR
Ethernet 3:
10.128.30.200
Ethernet 6:
10.128.50.200
Ethernet network: 10.128.30.0
Netmask: 255.255.255.0
Ethernet network: 10.128.50.0
Netmask: 255.255.255.0
Cisco ONS 15303 - ANGEL
CTunnel 0:
92.0.1.1
Cisco ONS 15303 - GOBLIN
CTunnel 0:
91.0.1.1
SNMP
UDP
IP
CLNP
LAPB
DCC
Cisco Transport Manager/CNM
client
10.128.30.1
Cisco Transport Manager/CNM
client
10.128.50.1
31541

ALLEGATO E



Iran Packet Switched Public Data Network (Iranpac)
Integrated PDN & VSAT Network & Global Information System
Intelsat - Satellite
International G/W
VISA
Sprint & Transpac
Boom-e-hen Earth Station
PSE
IRAN PAC
X.25
PDN Network
PSTN
PAD
Remote VSAT TABRIZ
Remote VSAT MASHAD
Remote VSAT ISFAHAN
Customer LAN
Asynch Synch
Ethernet
10 Mbps
D/U Access
Leased Line Access
Private LAN
TCP/IP Ethernet
F0069

ALLEGATO F: Glossario Tecnico

E.146 Raccomandazione ITU-T E.146
Piano di numerazione dei servizi telefonici internazionali.

X.3 Raccomandazione ITU-T X.3
Servizio di Packet Assembly/Disassembly (PAD) su reti dati pubbliche.

X.21 Raccomandazione ITU-T X.21
Interfaccia tra DTE e DCE per operazioni sincrone su reti dati pubbliche.

X.21bis Raccomandazione ITU-T X.21bis
Uso dei DTE progettati per interfacciarsi ai modem di serie V su reti dati pubbliche.

X.25 Raccomandazione ITU-T X.25
Interfaccia tra DTE e DCE per operazioni terminale in modalita' pacchetto e connessi sulle reti dati pubbliche tramite circuiti dedicati.

X.28 Raccomandazione ITU-T X.28
Interfaccia DTE/DCE per l'accesso non permanente al servizio PAD su una rete dati pubblica situata nello stesso paese.

X.29 Raccomandazione ITU-T X.29
Procedure per lo scambio di informazioni di controllo e dati tra servizio PAD e DTE a pacchetto o altro PAD.

X.75 Raccomandazione ITU-T X.75
Sistema di segnalazione su reti a commutazione di pacchetto tra reti pubbliche che offrono servizi di trasmissione dati.

X.121 Raccomandazione ITU-T X.121
Piano di numerazione internazionale per le reti dati pubbliche.

V.24 Raccomandazione ITU-T V.24
Lista di definizione per circuiti di interscambio tra DTE e DCE.

V.26 Raccomandazione ITU-T V.26
Modem 2400 bps standardizzato per l'uso tramite circuiti telefonici a 4 coppie.

V.27bis Raccomandazione ITU-T V.27bis
Modem 4800/2400 bps con equalizzazione automatica standardizzato per l'uso tramite circuiti telefonici.

V.29 Raccomandazione ITU-T V.29
Modem 9600 bps standardizzato per l'uso punto-punto tramite circuiti telefonici a 4 coppie.

V.35 Raccomandazione ITU-T V.35
Trasmissione dati a 48 Kbps per circuiti operanti su frequenze di 60-108KHz.

V.42 Raccomandazione ITU-T V.42
Procedure per la correzione d'errore per DCE utilizzanti la conversione asincrona-sincrona.

==========

Molti dei termini qui presenti fanno implicitamente riferimento al funzionamento di X.25.

AC Area Code.
Prefisso del numero da raggiungere, come per il telefono. Segue il DNIC e puo' essere di lunghezza variabile.
Cfr. DNIC, NTN.

ACP Adattatori concetratori di pacchetto.
Servono per assemblare e disassemblare pacchetti, in modo tale che i dispositivi che utilizzano la trasmissione a carattere, preceduta dal bit di start e seguita da quello di stop, possono essere assemblati in pacchetti e disassemblati.
Cfr. CGM, NCP, PAD.

ADCCP Advanced Data Communication Control Procedure.
Un altro protocollo livello data-link derivato da SDLC e reso standard ANSI.
Cfr. HDLC, LAPB, LAP-D, LAP-F, LAP-M, LLC, QLLC, SDLC.

BBS Bulletin Board System.
Sistema di scambio messaggistica e file molto in voga prima dell'avvento massiccio di Internet.

BCD Binary Coded Decimal.
Una rappresentazione numerica dove un numero e' espresso come una sequenza di cifre decimali, codificate in un numero binario di 4-bit, detto anche nibble.

BSC Binary Synchronous Communication.
Un protocollo di comunicazione a livello data-link character-oriented.
Questo protocollo e' ormai reso obsoleto da tecnologie bit-oriented quali SDLC, HDLC e altre.
Cfr. SDLC, HDLC.

CCC Chaos Computer Club.

CCITT Comite Consultatif International de Telegraphique et Telephonique.
Il nome originale della ITU.
Cfr. ITU.

CDA Circuito Diretto Analogico.
Circuito dedicato analogico per la connessione punto-punto.
Cfr. CDN.

CDN Circuito Diretto Numerico.
Circuito dedicato digitale per la connessione punto-punto.
Cfr. CDA.

CGM Centri di gestione e manutenzione.
Hanno il compito di controllare tutti i dispositivi del nodo a cui appartengono, e di rilevare il traffico sulla rete per effettuarne la tariffazione.
Cfr. ACP, CLP, NCP.

CLP Commutatori locali di pacchetto.
Permettono funzioni di accesso per i DTE X.25 e di commutazione del traffico.
Cfr. ACP, CGM, NCP.

CLI Command Line Interface.
Interfaccia a linea di comando.
Cfr. DCL.

CISC Complex Instruction Set Computer.
Cfr. RISC.

CRC Cyclic Redundancy Check.
Un numero derivato da, e depositato o trasmesso con, un blocco di dati in ordine di identificare corruzioni.
Il CRC e' `redundant' poiche' non aggiunge informazioni. L'algoritmo tratta i blocchi di bits in input come un set di coefficenti polinominali.

CUG Closed User Group.
In X.25, in un gruppo chiuso, se il DTE chiamante non appartiene al gruppo, la chiamata viene rifiutata.
Esistono pero' anche gruppi chiusi dove l'accesso puo' essere concesso tramite autenticazione.

DCC Data Country Code.
Identificativo, in un DNIC, del codice paese.
Cfr. AC, DNIC, NC, NTN.

DCE Data Circuit-terminating Equipment.
Dispositivo che collega il circuito di comunicazioni tra l'origine e la destinazione (il DTE).
Un esempio comune di DCE sono i modem.
Cfr. DTE.

DCL DEC Command Language.
Linguaggio utilizzato dalla CLI di VMS/OpenVMS.
Cfr. DEC, VMS.

DCS Digital Communication System.
Cfr. GSM.

DEC Digital Equipment Corporation.
Produttore di computer, quali VAX e Alpha, e del sistema operativo VMS/OpenVMS.
Acquisita nel 1998 da Compaq Computer Corporation, adesso HP.
Cfr. VAX, VMS.

DNIC Data Network Identification Code.
Dalla raccomandazione ITU-T X.121, le prime 4 cifre di un numero dati internazionale.
Il DNIC e' divisi un due parti, il DCC di tre cifre ed una quarta cifra detta NC.
Cfr. AC, DCC, NC, NTN.

DTE Data Terminal Equipment.
Dispositivo che agisce come origine o destinazione, in grado di controllare il canale di comunicazione.
Cfr. DCE.

EDI Electronic Data Interchange.
E' un insieme di protocolli per effettuare scambi altamente strutturati di interorganizzazione, come acquisti e richieste di prestito.
Cft. EFTPOS, T3POS.

EFTPOS Electronic Funds Transfer Point-Of-Sale.
Insieme di informazioni essenziali che consentono il trasferimento di contanti tra cliente e venditore mediante POS, come avviene per le carte di credito.
Cfr. EDI, T3POS.

FCS Frame Check Sequence.
Informazione presente per l'identificazione e correzione d'errore.

GCL Gruppo di Canale Logico.
Identifica il gruppo di canale logico di un circuito virtuale, con un numero compreso tra 0 e 15, che esso sia permanente o meno.
Cfr. NCL, LGN, VC, PVC, SVC, VCI.

GFI Group Format Identifier.
Detto anche General Format Identifier.
Sono i primi 4 bit dell'header di un pacchetto X.25, contengono il Qualifier bit, che identifica il tipo di informazione destinata al PAD, il Delivery bit che trasporta l'acknowledgment punto-punto ed il Sequence Number che descrive se la generazione dei numeri di sequenza e' modulo 8 o modulo 128.

GSM Global System for Mobile communication.
Originariamente "Groupe de travail Speciale pour le services Mobiles".
Standard 2G per le comunicazioni telefoniche cellulari utilizzato in molti paesi.
Le frequenze utilizzate dallo standard GSM sono 900-1800MHz, in alcuni paesi, come gli USA, 1900MHz.
Cfr. TACS, SIM.

HDLC High-Level Data Link Control.
Protocollo livello data-link utilizzato fondamentalmente su connessioni WAN.
E' attualmente uno standard ISO, derivato dall'SDLC.
Cfr. LAPB, LAP-D, LAP-F, LLC, SDLC.

IEEE Institute of Electrical and Electronics Engineers.

Istituto che si occupa di regolamentare gli standard di elettrotecnologia.

ISDN Integrated Services (on) Digital Network.
ISDN e' una rete che dispone di una gamma di servizi, ISDN e' documentata nelle racomandazioni ITU-T serie I, per quanto riguarda l'utenza nella serie Q e per quanto la compressione pcm utilizzata nella serie G.
Esistono diverse implementazioni e molte volte cambiano da paese a paese, l'europa utilizza, nella maggioranza della comunita', lo standard ETS 300 102-1, definito dall'ETSI.
Esistono fondamentalmente due tipologie di ISDN, BRI e PRI.
BRI e' la Basic Rate Interface e dispone di due canali B per i dati a 64Kbps, ed un canale D a 9.6Kbps per controllo e, eventualmente il trasporto per reti a commutazione di pacchetto.
PRI e' la Primary Rate Interface e dispone di 30 canali B a 64Kbps ed un canale D a 64Kbps.
I piani per reti ISDN a larga banda (B-ISDN) definiscono velocita' di tasmissione dati piu' elevate, dai 32Mbps in su.
Cfr. PSTN, PSN.

ISO International Standard Organization.
Organizzazione internazionale che si occupa di regolamentare gli standard.
Cfr. OSI, TP0-TP4.

ITU International Telecomunication Union.
Unione internazionale che si occupa di regolamentare gli standard per le telecomunicazioni.
Cfr. CCITT.

KESU Kernel, Executive, Supervisor, User.
Modello di protezione a 4 livelli implementato nel VAX ed utilizzato da VMS.
Cfr. VAX, VMS.

LAN Local Area Network.
Rete ad estensione locale.
Cfr. WAN.

LAPB Link Access Protocol Balanced.
Come per l'HDLC, anche LAPB e' derivato dall'SDLC, e viene utilizzato per accedere alle reti X.25.
Cfr. ADCCP, HDLC, LAP-D, LAP-F, LAP-M, LLC, MLP.

LAP-D Link Access Protocol for D-channel.
Come LAPB, ma implementato per il corretto funzionamento tramite canale D su ISDN.
Cfr. ISDN, HDLC, LAPB, LAP-F, LAP-M, LLC.

LAP-F Link Access Protocol for Frame Realy.
Come LAPB, ma implementato per il corretto funzionamento tramite Frame Relay.
Cfr. ADCCP, HDLC, LAPB, LAP-D, LAP-M, LLC, SDLC.

LAP-M Link Access Protocol for Modems.
Come LAPB, ma implementato per il corretto funzionamento tramite Modem.
Cfr. ADCCP, HDLC, LAPB, LAP-D, LAP-F, LLC, SDLC.

LCN Logical Channel Number.
Cfr. NCL.

LGN Logical Group Number.
Cfr. GCL.

LLC Logical Link Control.
E' il protocollo livello data-link utilizzato su Ethernet.
Generalmente viene utilizzato LLC 802.2.
Cfr. HDLC, LAPB, LAP-D, LAP-F, LAP-M, MLP, SDLC.

MLP Multi-Link Procedure.
Un'estensione a LAPB che permette l'utilizzo di piu' collegamenti fisici contemporaneamente.
Cfr. LAPB.

NAT Network Address Translation.
Tecnica utilizzata per la traduzione degli indirizzi tra una rete privata ed una pubblica.

NC Network code.
Identificativo, in un DNIC, della rete da chiamare all'interno di un paese.
Cfr. AC, DCC, DNIC, NTN.

NCC Network Control Center.
Centro di controllo rete.

NCL Numero di Canale Logico.
Identifica il numero di canale logico di un circuito virtuale, compreso tra 0 e 255, che esso sia permanente o meno.
Cfr. GCL, LCN, VC, PVC, SVC, VCI.

NCP Nodi a commutazione di pacchetto.
Hanno la funzione di impostare il circuito virtuale tra i due dispositivi che devono colloquiare.
Ad ogni NCP sono collegati piu' ACP ed un CGM.
Cfr. ACP, CGM.

NTN Network Terminal Number.
Nello standard ITU-T X.121, l'insieme di cifre che comprende l'indirizzo completo del punto terminale.
Se l'NTN non fa parte della numerazione nazionale, l'NTN e' composto da 10 cifre dell'indirizzo a 14 cifre X.25 che segue il DNIC.
Quanto e' parte della numerazione nazionale, l'NTN e' composto da 11 cifre dell'indirizzo a 14 cifre X.25 che segue il DNIC.
Cfr. AC, DNIC.

NUA Network User Address.
Indirizzo, che segue le raccomandazioni ITU-T X.121 ed E.164, sulla rete X.25.
Cfr. NUI.

NUI Network User Identification.
Identificativo, sulla rete X25, di un utente.
Comunemente, puo' essere vista in una sorta di password.
Cfr. NUA.

OSI Open System Interconnection.
Solitamente riferito al modello di riferimento a 7-livelli standard ISO.
Cfr. ISO, TP0-TP4.

PAD Packet Assembly/Disassembly.
Cfr. ITU-T X.3, ACP.

PBX Private Branch Exchange.
Un centralino telefonico privato.

PDN Packet Data Network.
Cfr. PSN.

PDU Protocol Data Unit.
Un pacchetto di dati che attraversa la rete.
Il termine implica un livello specifico del modello di riferimento OSI e un protocollo specifico.
Cfr. PPDU, TPDU.

PLP Protocol Layer Protocol.
Il PLP e' il protocollo a livello tre di X.25. Permette la presenza fino a 4095 canali virtuali su di una singola interfaccia.

PPDU Presentation Protocol Data Unit.
Sesto livello del modello di riferimento OSI della relativa PDU.
Cfr. PDU, TPDU.

POSIX Portable Operating System Interface for uniX
Standard IEEE 1003 che definisce le interfaccie che un sistema operativo deve avere per essere POSIX compliant.

PSI Packet Switched Interface.
In referimento a VMS, l'interfaccia che permette di colloquiare con X.25.
Cfr. DEC, VMS.

PSN Packet Switched Network.
Rete a commutazione di pacchetto, come ITAPAC.
Cfr. PSTN, ISDN.

PSDN Public Switched Data Network.
Cfr. PSN.

PSTN Public Switched Telephone Network.
La comune rete telefonica.

Cfr. RTG, ISDN, PSN.

PVC Permanent Virtual Circuit.
Un circuito virtuale permanente.
In X.25, i DTE tra i due punti si scambiano solo dati.
Cfr. VC, SVC, VCI.

QLLC Qualified Logical Link Control
Protocollo livello data-link che permette il trasporto di reti SNA su X.25.
Cfr. ADCCP, HDLC, LAPB, LAP-D, LAP-F, LAP-M, LLC, SDLC.

RISC Reduced Instruction Set Computer.
Cfr. CISC.

RTG Rete Telefonica Generale.
Cfr. PSTN, ISDN.

SDLC Synchronous Data Link Communication.
Protocollo livello data-link sincrono, utilizzato e pensato da IBM nell'implentazione delle reti SNA.
Questo protocollo non e' piu' usato, se non tra link WAN SNA, ed e' stato in seguito modificato e reso standard come HDLC da parte di ISO, come ADCCP dall'ANSI, LAP da parte di ITU e LLC da parte di IEEE.
Cfr. ADCCP, HDLC, LAPB, LAP-D, LAP-F, LAP-M, LLC, QLLC.

SIM Subscriber Identification Module.
Smartcard contente i dati identificativi dell'utente per l'accesso al servizio di comunicazione GSM o DCS.
Cfr. GSM.

SNMP Simple Network Management Protocol.
Protocollo definito dallo standard RFC 1157 per il management dei nodi su una rete IP.

SVC Switched Virtual Circuit.
Il termine `Switched Virtual Circuit' fu' coniato inutilmente per distinguere un circuit virtuale "ordinario" da un circuito virtuale permanente (PVC).
Da non essere confuso con la Switched Virtual Connection presente nel protocollo ATM.
Cfr. GCL, NCL, VC, PVC, VCI.

T3POSTransaction Processing Protocol for Point-Of-Sale.
E' un protocollo characted-oriented per effettuare transazioni da POS su reti a commutazione di pacchetto X.25. T3POS consente l'invio dei dati sul canale D ISDN.
Cfr. EDI, EFTPOS.

TACS Total Access Communication System.
Sistema analogico di comunicazione telefonica mobile, superato dal GSM ma ancora presente.
Cfr. GSM.

TPDU Transport Protocol Data Unit.
Quarto livello del modello di riferimento OSI della relativa PDU.
Cfr. PDU, PPDU.

TP0-TP4 Transport Protocol Class 0-4. (ISO/OSI Protocols)
Protocolli appartenenti allo standard ISO/OSI.
Seguendo la storia, se non ci fosse stato TCP/IP, probabilmente oggigiorno utilizzeremmo OSI/TP4.
Cfr. ISO, OSI.

UUCP Unix-to-Unix Copy.
Un software e, anche protocollo, che permette l'invio di file mediante link seriale, diretto o via modem.

VAX Virtual Address eXtension.
E' stato il piu' grande successo per la DEC dopo il PDP-11. Era un vero CISC, a 32bit con 4 livelli
di protezione (modello KESU) e, come dice il nome, possibilita' di avere indirizzamento virtuale.
Cfr. CISC, DEC, VMS, KESU.

VC Virtual Circuit.
Un circuito virtuale connection-oriented, implementato su una rete a commutazione di pacchetto o, a sua volta, su una rete connection-oriented.
Avviene in tre fasi: istaurazione del collegamento, trasferimento dati, abbattimento del collegamento.
In X.25, i DTE si scambiano pacchetti dati e pacchetti di segnalazione.
Ad ogni VC viene assegnato un numero di gruppo di canale logico (GCL) ed un numero di canale logico (GCN).
Cfr. GCL, NCL, SVC, PVC, VCI.

VCI Virtual Circuit Identifier.
Un identificatore utiilizzato per il routing di un circuito virtuale, che esso sia permanente o meno.
Cfr. GCL, NCL, VC, SVC, PVC.

VMS Virtual Memory System.
Sistema operativo proprietario di DEC, originariamente scritto per i propri minicomputer VAX.
Ora chiamato OpenVMS poiche' l'X/Open Consortium ha certificato l'alta compatibilita' con gli standard POSIX. Lo sviluppo di VMS e' ancora molto attivo, attualmente e' in grado di girare su piattaforme VAX, Alpha e a breve Itanium.
Cfr. DCL, DEC, KESU, VAX.

WAN Wide Area Network.
Rete ad estensione geografica.
Cfr. LAN.

BIBLIOGRAFIA

Quelli che seguono sono alcuni file o libri dei quali consiglio la lettura qualora si desiderassero maggiori informazioni sull'argomento trattato nel presente documento. Alcuni di essi trattano hacking su reti X.25, altri spiegano come coprire le proprie tracce ed altri ancora cosa fare quando si è dentro un sistema informatico collegato ad una dorsale X.25; i libri narrano invece episodi realmente accaduti durante i quali si sono verificate delle vere e proprie "cacce all'uomo" on-line in seguito ad episodi di hacking provenienti da reti dati X.25.

X.25 Hacking e storia

- The Cuckoo's Egg, Clifford Stoll, Pocket Books, ENG, 1989, LIBRO
- Cyberpunks: Outlaws and hackers on the Computer Frontier, Katie Hafner & John Markoff, Touchstone Books, 1991, LIBRO
- Out Of The Inner Circle - By Bill Landreth LIBRO
- Underground - By Suelette Dreyfuss LIBRO
- McGraw Hill Internetworking Handbook LIBRO
- Accessing Telecom Australia's AUSTPAC service - By Softbeard
- A Novice's Guide To Hacking - By The Mentor
- The Beginner's Guide To Hacking On Datapac - By The Lost Avenger and UPI
- The Force Files - By The Force
- NEOPHYTE'S GUIDE TO HACKING (1993 Edition) - By Deicide
- Infosurge Ezine #1 : Social Engineering - By The Czar
- Austpac.notes - by Vorper VII
- Globetrotter Ezine - By The Force
- An Introduction To Packet Switched Networks Parts I and II
- Telecom Security Bulletin File - Written By Blade Runner
- The Alt.2600 Hack FAQ - By Simple Nomad

Sistemi Specifici

- Hacking UNIX Tutorial - By Sir Hackalot
- RIM Remote System - Neurocactus Ezine
- Advanced Hacking VAX's VMS - By Lex Luthor
- Guide to Gandalf XMUXs - By Deicide
- B4B0 Ezine #7 : Hacking The Shiva LAN-Rover - By Hybrid
- The Complete Hewlett Packard 3000 Hacker's Guide - By AXIS
- X.25 And LAPB Commands For Cisco Routers

Sicurezza

- Pitting - Neurocactus Ezine
- SS7 Based Diverter - Phrack 50 File 9 Of 16
- Insider Ezine #1 : Safer Boxing Using The RJ31X jack - By VX0MEG
- Infosurge Ezine #1 : Defeating ANI - By phase5
- Wiretap Detection Techniques - By Theodore N Swift (Book)

RFCs

RFC 874 - A Critique Of X.25
RFC 877 - Standard For Transmission Of IP Datagrams Over Public Data Networks
RFC 1356 - Multiprotocol Interconnect On X.25 And ISDN In The Packet Mode
RFC 1090 - SMTP On X.25
RFC 1381 - SNMP MIB Extension For X.25 LAPB
RFC 1382 - SNMP MIB Extension For The X.25 Packet Layer
RFC 1461 - SNMP MIB Extensions For Multiprotocol Interconnect Over X.25

Links

- http://www.x25us.net (vecchio http://qwerty.nanko.ru/x25/)

Un ottimo archivio di files su X.25: molti dei file sopra menzionati possono essere reperiti qui.

- http://www.microtronix.com

Produttori del router X-Span X.25 e del MicroNODE: dispongono di alcuni tutorial e di un glossario X.25

- http://www.internos.it/archivio/otto.pdf

La storia di Otto Sync e White Knight: leggiamo il racconto reale di un hacker X.25 e di come sia riuscito ad evitare il processo per intrusioni in sistemi informatici.

Documentazione utilizzata

- X25 Trace: X.25 network tracing for Internet users, by Dennis Jackson, JANET-CERT Coordinator, U.K.
- A novice Guide to X.25 Hacking, by Anonymous
- Desktop Guide to X.25 Hacking in Australia, by Epic Target

X.25 TRACE

```
================================================================================

10:15:16:56    10  A   outgoing       RcvR     3 octets    8       136
          LGN=0   LCN=10   LCI=10    P(R)=4
10 0a 81

Command line:  x25decode
Trace protocol: /dev/x25
Trace date: Tue Apr  7 10:14:54 BST 1998

Timestamp      VC  Snid  Direction   Pkt Type      Size     Mod  PacketId
================================================================================

10:15:16:98    10  A   outgoing       Data   126 octets    8       137
      D=0  LGN=0   LCN=10   LCI=10    P(S)=3    P(R)=4    M=0  Q=0
10 0a 86 56 2e 0d 56 48    48 47 2e 57 41 2f 45 31    * ...V..VHHG.WA/E1 *
42 54 55 4b 2f 49 31 31    47 49 41 2f 50 a0 25 d9    * BTUK/I11GIA/P.%. *
0d 56 47 59 41 0d 55 4e    42 2b 49 41 54 41 3a 31    * .VGYA.UNB+IATA:1 *
2b 31 47 2b 46 53 2b 39    38 30 34 30 37 3a 31 30    * +1G+FS+980407:10 *
31 35 2b 54 32 27 55 4e    48 2b 31 2b 48 53 46 52    * 15+T2'UNH+1+HSFR *
45 51 3a 39 34 3a 31 3a    49 41 27 4f 52 47 2b 46    * EQ:94:1:IA'ORG+F *
53 3a 4c 4f 4e 27 4c 54    53 2b 2a 52 27 55 4e 54    * S:LON'LTS+*R'UNT *
2b 34 2b 31 27 55 4e 5a    2b 31 2b 54 32 27          * +4+1'UNZ+1+T2'   *

================================================================================
```