SOLUZIONI CONVERGENTI PER LA GESTIONE DELLE INTERCETTAZIONI DI FONIA E DATI SU RETI *WIRELESS* E *WIRED*

di Roberto Marega

Quando si parla dell'architettura complessiva di un sistema di intercettazione di servizi telefonici o telematici, non si può prescindere dalle esigenze oggettive che sono rappresentate dalle classi principali di *stakeholder*, che sono gli uffici giudiziari da una parte, gli operatori telefonici dall'altra e, in relazione a entrambi, i fornitori di servizi e tecnologia a supporto delle intercettazioni. **L'obiettivo di fondo e prioritario rimane quello di soddisfare le esigenze delle indagini investigative**. Gli operatori telefonici, del resto, rendono disponibili agli uffici giudiziari i dati relativi alle intercettazioni secondo il principio di obbligatorietà. Sarebbe miope tuttavia affrontare l'aspetto architetturale delle intercettazioni senza tenere conto dell'efficienza del processo di intercettazione nel suo complesso, sia per gli uffici giudiziari, che devono poter svolgere la loro attività nel modo più rapido ed efficiente, sia per gli operatori che, nel garantire i massimi livelli di qualità ed affidabilità del servizio di intercettazione offerto, devono tener conto anche della manutenibilità dell'infrastruttura di intercettazione e dei relativi costi di esercizio.

Questo è il caso che si presenta quando, per soddisfare le esigenze di intercettazione dati, si tende ad eccedere nell'uso delle sonde che vengono inserite presso la sede dell'operatore su richiesta degli uffici giudiziari. Le sonde, così utilizzate, raramente si inseriscono *in passante* (o a T) sul flusso dei dati; molto più frequentemente sfruttano la SPAN *port* (*Switch Port Analyzer*, o porta di *mirroring*) degli *switch* di *core network* per acquisire il traffico indicato. In pratica, in questo caso, lo *switch* invia tutto il traffico indirizzato ad altre porte anche sulla SPAN *port*, rendendolo quindi disponibile alla sonda.

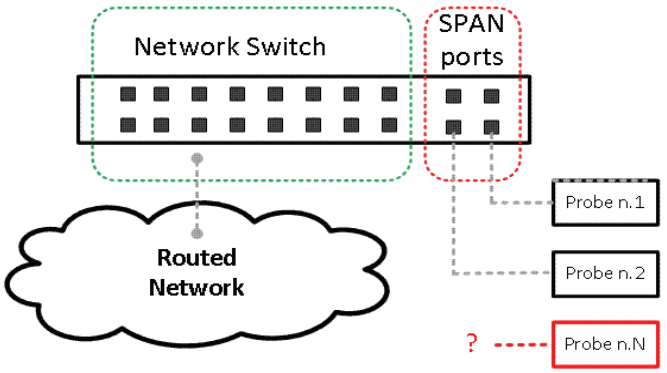

Figura 1 – Sonde e utilizzo delle SPAN *port* come risorsa limitata

L'architettura degli *switch*, tuttavia, pone alcuni limiti nell'utilizzo delle SPAN *port*, in particolare quando ci si relaziona con tecnologia *Gigabit* o 10 *Gigabit* che impegna in maniera significativa la capacità di *processing* degli *switch* e dei *router*. Le SPAN *port* sono innanzitutto disponibili, se disponibili, in un numero limitato. Quando le richieste di intercettazione si sovrappongono, possono non esserci più SPAN *port* disponibili. Inoltre, per come sono congegnati gli *switch*, le SPAN *port* sono quelle che hanno più bassa priorità, e nel caso in cui lo *switch* dovesse essere sovraccarico di lavoro (e l'utilizzo indiscriminato delle SPAN *port* può esserne la causa), **i pacchetti indirizzati verso la SPAN *port* vengono scartati, con conseguente perdita di informazione nella attività di investigazione**. Con l'evolvere della tecnologia e l'aumento del capacità di traffico (anche 40 *Gigabit*) erogata dalle SPAN *port*, le stesse sonde possono avere difficoltà ad offrire il carico computazionale necessario per analizzare e filtrare questa mole di dati.

Un altro fattore critico, è legato alla convergenza dei servizi di telecomunicazioni su reti IP, ed alla sempre più frequente evenienza che le comunicazioni, telefoniche o telematiche, si spostino nel corso della comunicazione stessa attraverso tecnologie diverse. Basti pensare alle comunicazioni di terminali LTE, con la funzionalità "*dual mode*", che possono iniziare una chiamata in modalità LTE per continuare la stessa, in seguito ad un distacco (*fall back*) dal circuito LTE, attraverso una cella GSM/UMTS. Risulta pertanto sempre meno pratico dove "inseguire" il *target* attraverso i suoi spostamenti, sia fisici che tecnologici, utilizzando strumenti di intercettazione distribuiti.

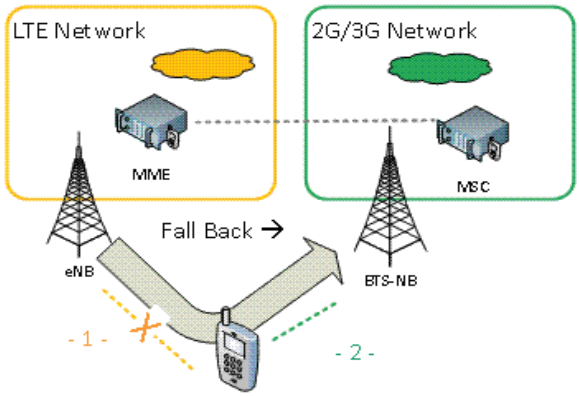

Figura 2 – *Fall Back* da rete LTE a rete 2G/3G

Quanto descritto si applica in termini generali a tutti i servizi di comunicazione che vengono offerti e gestiti dagli operatori telefonici, indipendentemente dal fatto che questi offrano servizi mobili oppure *wired*, indipendentemente dal fatto che si parli di intercettazione telefonica o dati e indipendentemente dalla tecnologia utilizzata (PSTN, ADSL, GSM. GPRS, UMTS, LTE, WiMAX, ecc.) e le rispettive evoluzioni. **È facile da intuire quindi che, a fronte di una evoluzione tecnologica, fisiologica nel settore delle telecomunicazioni, ne derivi l'esigenza, altrettanto fisiologica da parte di tutti gli *stakeholder* nel settore delle**

intercettazioni, di adeguare processi e strumenti nel modo il più possibile rapido ed efficiente, sia in termini funzionali che economici.

I requisiti che l'architettura di intercettazione deve soddisfare sono ben noti. **In riferimento agli uffici giudiziari, ed agli strumenti di ascolto, visualizzazione e analisi delle intercettazioni, i principali requisiti operativi si possono riassumere come segue**: tempestività nell'ottenere risposta alle richieste; supporto di tutte le tecnologie e protocolli adottati dagli operatori telefonici; capacità di ascoltare e visualizzare le comunicazioni effettuate anche con i più recenti strumenti e servizi (e tecnologie) di comunicazione; massima affidabilità del servizio; completezza e integrità delle informazioni, in relazione alle informazioni che la tecnologia di comunicazione può consentire; avere la possibilità di fruire dei dati raccolti nella maniera più possibile uniforme, per facilitare l'utilizzo di strumenti di *intelligence*, in grado di mettere in relazione le informazioni raccolte dai diversi canali; Totale riservatezza sui dati raccolti.
Gli Operatori di telecomunicazioni, da canto loro, hanno esigenze complementari: la soluzione di *lawful interception* (LI) deve rispondere alle normative nazionali vigenti, ma deve anche poter rispondere velocemente alle successive evoluzioni; deve essere garantito il supporto di molteplici *vendor* e tecnologie, anche in un'ottica evolutiva; la soluzione di LI non deve essere da ostacolo al business ed alla creazione di nuovi servizi; la soluzione deve essere interamente scalabile per accompagnare la crescita naturale dei servizi; la *compliance* alla LI deve comportare il minimo onere in termini di amministrazione e monitoraggio del sistema.

La soluzione strutturale al problema è quella già di fatto consolidata per le intercettazioni che riguardano la fonia, e prevede un sistema centralizzato di intercettazione, installato all'interno della rete dell'operatore telefonico, in grado acquisire dati relativi a tutte le tecnologie di interconnessione ed interfacciarsi con tutti i diversi dispositivi di rete utili, come i NAS, che consentono, in maniera più efficace rispetto agli *switch* della *core network*, di filtrare il traffico intercettato in base alle richieste. La convergenza delle reti su IP consente oggi di utilizzare la medesima architettura per tutte le intercettazioni, sia telefoniche che telematiche, su reti *wireless* e *wired*.

Avendo come riferimento una architettura convergente *full IP*, tutti i dati di intercettazione possono convergere, indipendentemente dalla tecnologia, su un unico sistema, chiamato di *mediation*, per la formattazione (secondo gli *standard*) ed il *delivery* verso gli uffici giudiziari. L'interfaccia a circuito (CS) su rete telefonica, ancora in essere con gli uffici giudiziari, può essere gestita utilizzando opportuni apparati di conversione (chiamati *gateway*) che consentono appunto di interfacciare il mondo IP con quello a circuito (incluso il circuito telefonico tradizionale).
È chiaro che ad ogni evoluzione tecnologica dovrà corrispondere un adeguamento del sistema centralizzato di intercettazione. Ciononostante **la presenza strutturale del sistema di intercettazione, consente agli operatori telefonici di pianificare l'evoluzione della rete insieme a quella del sistema di intercettazione**, migliorando l'efficienza del processo e riducendo drasticamente i rischi che possono essere connessi ad una possibile risposta a richieste di intercettazione con soluzioni estemporanee e non adeguatamente collaudate. Utilizzando un sistema centralizzato, inoltre, è sicuramente più agevole ottenere alta affidabilità del servizio, massima disponibilità e gestire situazioni anomale in caso di guasto sugli apparati di rete, anche attraverso soluzioni architetturali di ridondanza geografica. La soluzione centralizzata può inoltre essere adeguatamente scalabile, ovvero crescere in termini hardware al crescere del volume di traffico intercettato. **Questo consente di mantenere i costi del servizio di intercettazione al minimo necessario e ridurre comunque la probabilità di guasto con i relativi costi**.
Il vantaggio che è evidente per gli operatori telefonici, può non essere subito evidente per gli uffici giudiziari, ma lo diventa se si tiene conto della maggiore velocità di risposta che questi riescono ad ottenere, la maggiore affidabilità del servizio e la riduzione dei rischi, sempre insiti nell'instaurazione di nuove interfacce con i sistemi di ascolto e con gli apparati di rete, pur avendo come riferimento protocolli standard e/o consolidati.

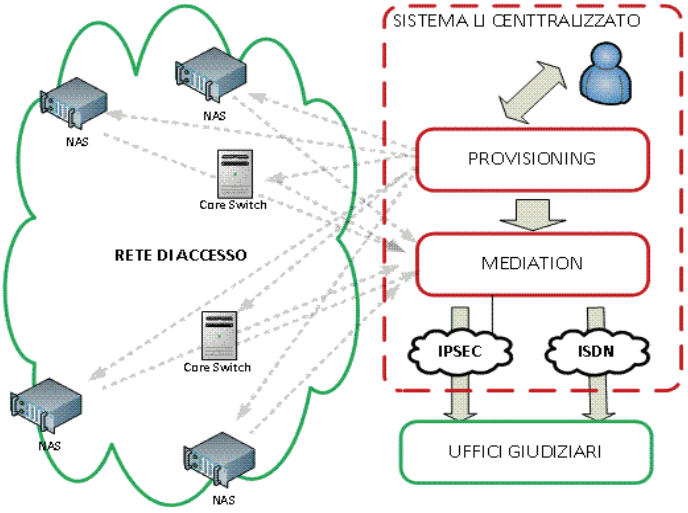

Figura 3 – Schema concettuale
del sistema di intercettazione centralizzato

Un altro aspetto non trascurabile riguarda la riservatezza nelle operazioni e sui dati raccolti. Risulta piuttosto evidente che l'implementazione di un sistema di amministrazione centralizzato consente di adottare opportuni strumenti e processi tesi a massimizzare la riservatezza e consentire all'operatore telefonico di soddisfare le richieste degli uffici giudiziari senza entrare nel merito dell'indagine stessa e dei dai raccolti. L'utilizzo di strumenti decentralizzati, che richiedono la configuazione di sonde da parte dei tecnici coinvolti nelle operazioni, espone inevitabilmente a maggior rischio la riservatezza dell'operazione stessa e la segretezza dell'operazione giudiziaria.

L'approccio basato su una architettura centralizzata risulta pertanto preferibile per i molteplici vantaggi evidenziati e per il benefici diretti ed indiretti che a livello di "sistema" porta a tutti gli attori coinvolti. Su questo sistema possono confluire la gestione ed il *delivery* di tutte le richieste di intercettazione, indipendentemente dall'area geografica e dalla tecnologia da tenere sotto intercettazione. Anche nel caso, pur raro, in cui dovesse risultare funzionale l'utilizzo di sonde sulle Span *port* della *core network*, l'approccio centralizzato può sempre essere adottato per governare il loro utilizzo razionalizzandone l'impiego. ©