TopoNA – a simple Topological Network Analyzer

Luca Carbone <luca.carbone@mib.infn.it>

INFN – Sezione di Milano/Bicocca

Problema: data una rete composta di apparati di livello 2, e' possibile dedurne **automaticamente** la topologia facendo uso di strumenti standard e non proprietari?

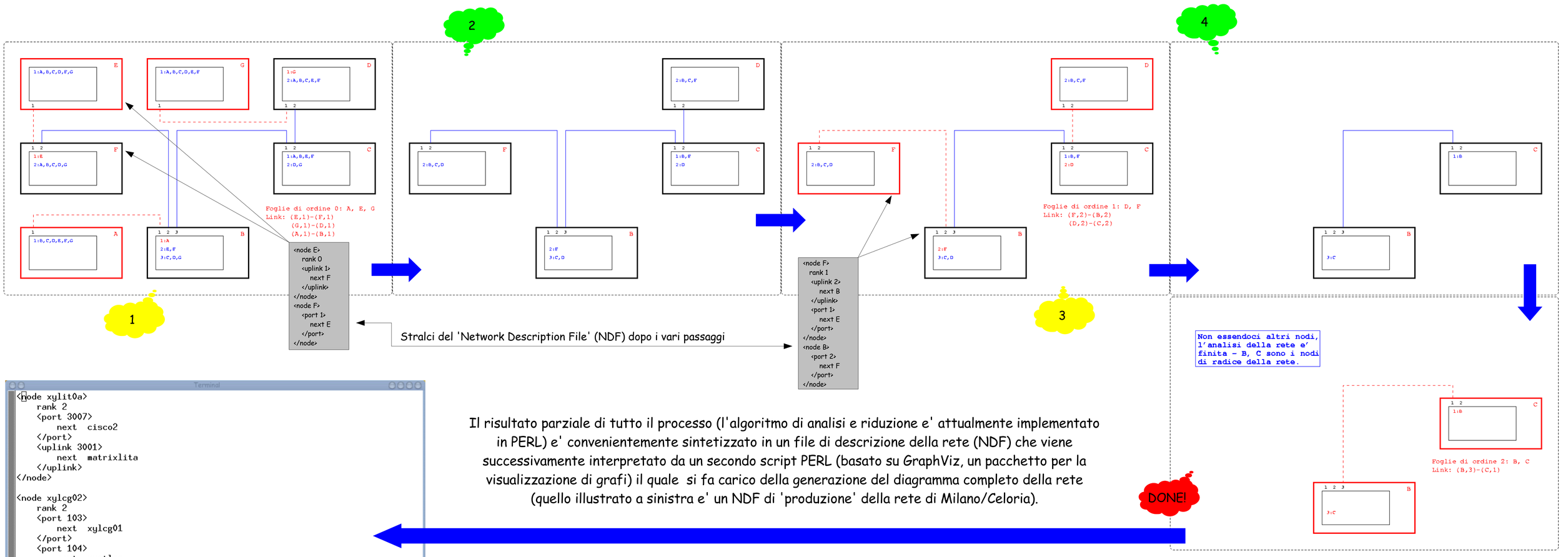
FWT (**forwarding table**) di *C*:

port 1: *A,B,E,F,...*
port 2: *D,G,...*
...
port n: ...

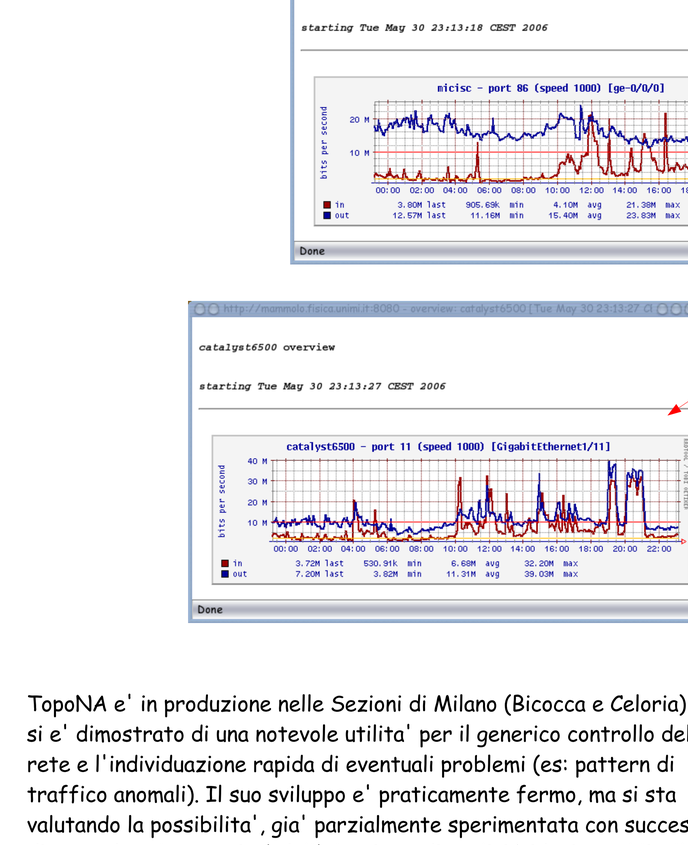
FWT di B:

port 1: *A,...*
port 2: *E,F,...*
port 3: *C,D,G,...*
...

Avendo semplicemente accesso alle forwarding table degli switch che compongono la rete (BRIDGE-MIB::dot1dTpFdb), e conoscendo i MAC address degli switch, e' possibile individuare le foglie (cioe' gli switch periferici); tramite un algoritmo ricorsivo di riduzione e' quindi possibile eliminarle per semplificare la rete e risalire via via sino agli switch di centro stella (che possono essere uno o due – paritetici – a seconda del numero di nodi totali e della topologia della rete in esame), mantenendo inoltre traccia delle connessioni 'risolte' durante il processo:

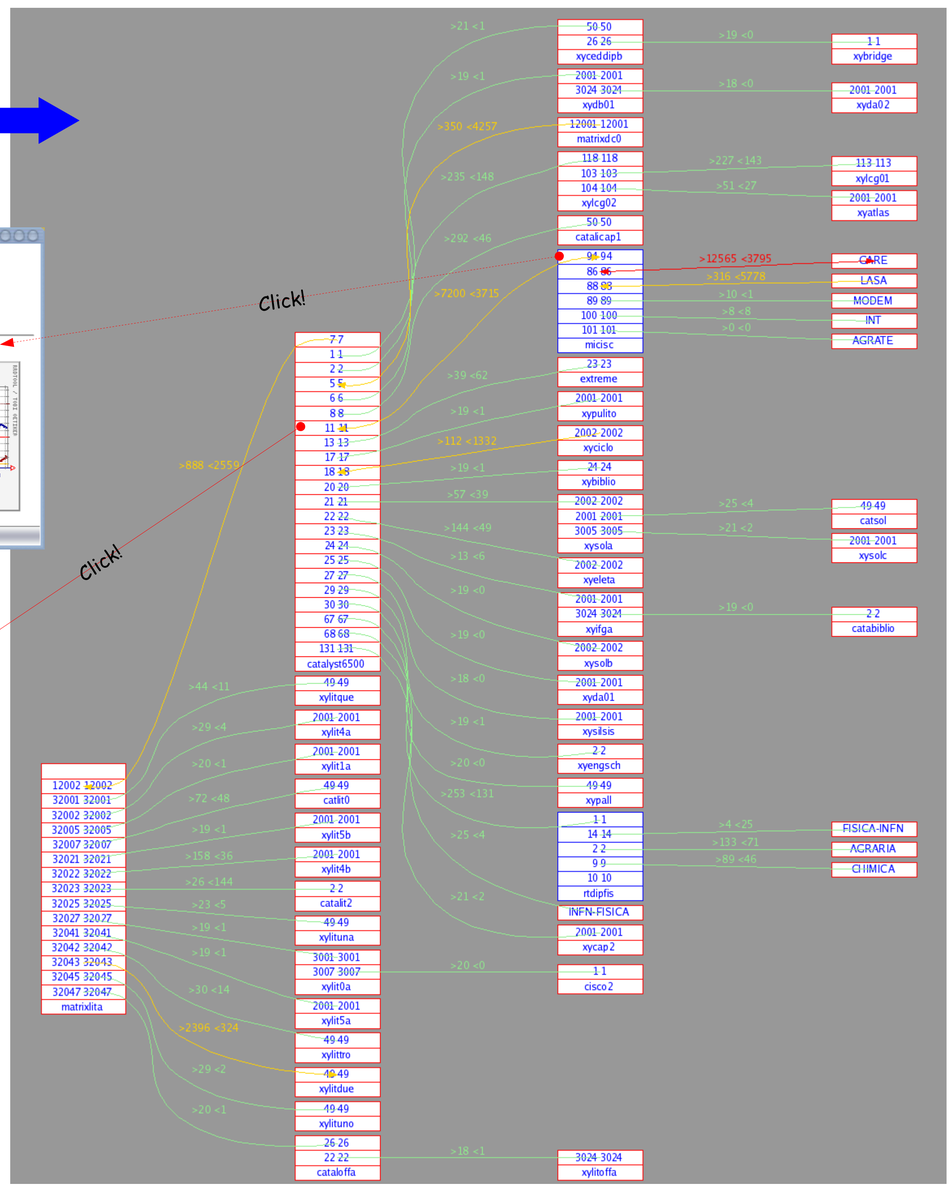


Stralci del 'Network Description File' (NDF) dopo i vari passaggi

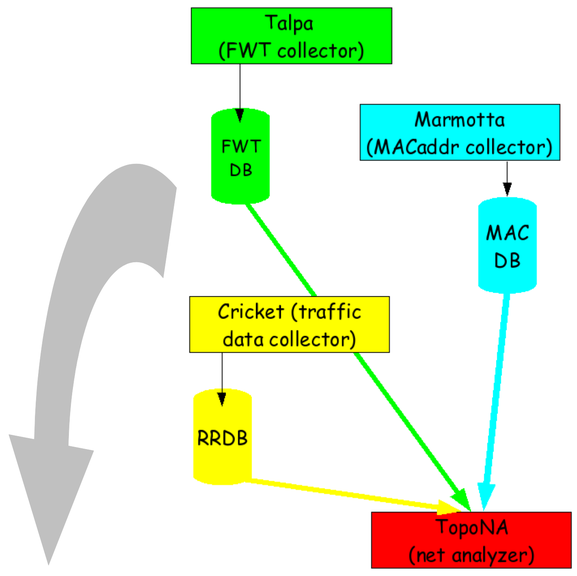


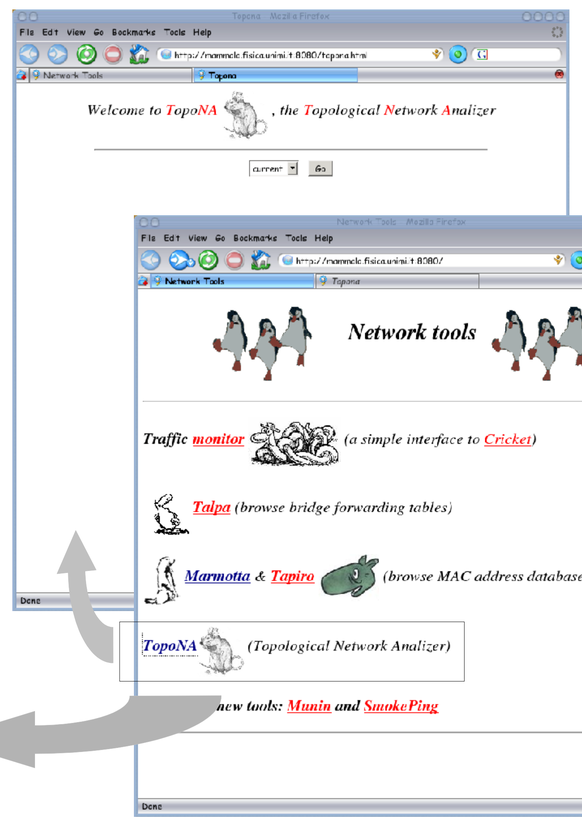
Il risultato parziale di tutto il processo (l'algoritmo di analisi e riduzione e' attualmente implementato in PERL) e' convenientemente sintetizzato in un file di descrizione della rete (NDF) che viene successivamente interpretato da un secondo script PERL (basato su GraphViz, un pacchetto per la visualizzazione di grafi) il quale si fa carico della generazione del diagramma completo della rete (quello illustrato a sinistra e' un NDF di 'produzione' della rete di Milano/Celoria).

TopoNA e' stato integrato (in via sperimentale) in un sistema completo di network management creato da zero ed interamente basato su SNMP e tool Open Source, composto dal Data Collector Cricket/RRD, da un FWT collector/browser (Talpa), da un MAC Address collector/browser (Marmotta) basato su pcap/MySQL. La visualizzazione dei dati raccolti avviene via Web; il sistema di analisi dinamica della rete si avvale di tali dati per produrre vere e proprie weather-map (clickabili) on-demand della rete; tali mappe sono comprensive della visualizzazione del traffico sui vari link e consentono di richiamare i dati di traffico delle singole porte di ogni switch componente la rete:



Weather-map della rete di Milano/Celoria





TopoNA e' in produzione nelle Sezioni di Milano (Bicocca e Celoria) e' si e' dimostrato di una notevole utilita' per il generico controllo della rete e l'individuazione rapida di eventuali problemi (es: pattern di traffico anomali). Il suo sviluppo e' praticamente fermo, ma si sta valutando la possibilita', gia' parzialmente sperimentata con successo, di estendere le capacita' dell'algoritmo di analisi/riduzione al livello 3 della pila OSI (ipNetToMediaTable) e quindi alle reti composte da router (o switch/router) oltre che da soli switch/bridge.