Monitoraggio e gestione delle reti IP

Michele Bergonzoni - Laboratori Guglielmo Marconi s.p.a.

Abstract: Perché le infrastrutture di rete più avanzate necessitano di gestione e monitoraggio, e quali sono gli obiettivi di tale attività. Gestione in-band ed out of band, i protocolli e le tecniche utilizzate sul campo, SNMP e protocolli generici. Gli strumenti di monitoraggio e gestione. Alcuni problemi di rilevanza pratica: bug, accesso, inventario, mancata instrumentation. Organizzazione di un NOC, teamwork e skill richiesti.

LABORATORI GUGLIELMO MARCONI

Reti IP

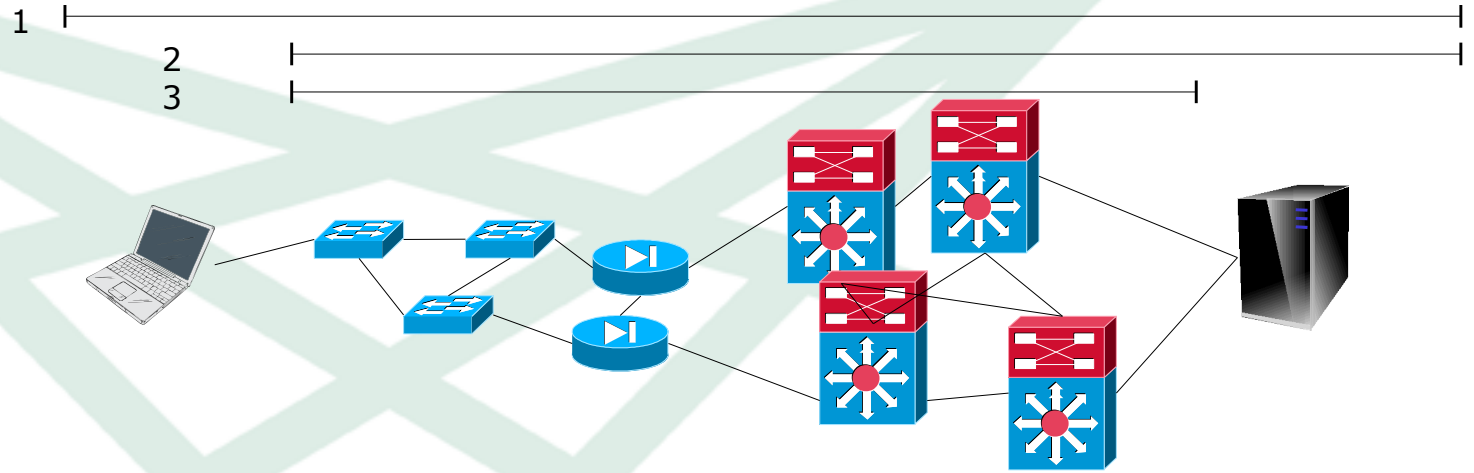
Le reti dati IP sono quelle che compongono Internet, quelle dei carrier o service provider, e anche le reti interne e private di aziende o enti. C'è una ambiguità quando si parla di "reti". La rete è:

1)L'insieme dei PC, dei server, e delle cose per collegarli

2)Tutto ciò che riesco a vedere dal mio PC e che sta fuori da esso

3)Tutto quello che resta quando tolgo i PC ed i server

Normalmente in ambito telecomunicazioni si intende il terzo significato, che è quello che useremo.



LABORATORI GUGLIELMO MARCONI

Bande in gioco

La banda di un collegamento è il numero di bit/s che può trasportare.

- I normali PC hanno un'interfaccia ethernet a 100 Mbit/s o 1 Gbit/s.
- Una ADSL domestica può avere 2 Mbit/s in download e 256 kbit/s in upload. Con ADSL2+ e un po' di fortuna, 20 Mbit/s in download e 1 Mbit/s in upload.
- Le dorsali ottiche di una rete privata in un grosso edificio sono solitamente ad 1 Gbit/s
- I carrier che usano fibre ottiche usano spesso link a 1 Gbit/s o 10 Gbit/s
- Qualche vendor comincia ad avere disponibili interfacce ottiche IP a 100 Gbit/s.

A 1 Gbit/s, un bit è lungo 30 cm. A 10 Gbit/s, 3 cm. Nonostante questi numeri, molte reti aziendali hanno dorsali geografiche di 1 o 2 Mbit/s: la situazione è asimmetrica e squilibrata per problemi di costi e mercato.

Spazi IP

Tradizionalmente, il protocollo IP è usato per Internet. In realtà è usato per tante altre cose, ed è normale che una grossa rete IP trasporti più "internet", più "spazi IP" indipendenti tra loro. Prendono nomi che dipendono dal vendor: VRF (Virtual Routing/Forwarding Instance), Routing instance, Virtual Router, etc.

- Nella rete di un carrier o service provider
  - lo spazio di Internet
  - gli spazi IP privati di ciascun cliente
- In certe reti enterprise (aziende ed enti), diverse zone del firewall

E' buona norma effettuare la gestione in uno "spazio" dedicato. Comune nelle reti carrier, raro nelle reti enterprise.

Quale IP?

- Il protocollo attualmente usato è IPv4. IPv6 è standardizzato da molti anni, ma ancora pochissimo diffuso.
- Il pool centrale di indirizzi IPv4 si è esaurito in novembre 2011, quello europeo in settembre 2012
- IPv6 è usato poco su internet, ed ancor meno nelle reti private. Quasi tutti i vendor, e molti carrier, si stanno attrezzando.
- Nelle reti IPv4/IPv6 (dual stack), la gestione è tuttora quasi esclusivamente IPv4, così come la segnalazione.

Cosa compone una rete IP

Le reti IP sono fatte con apparati di rete, tipicamente switch e router, ma anche apparati di trasmissione, firewall, etc.

Switch e router sono ruoli che oggi si confondono. I costi possono variare da 200 euro a ben più di 100 Keuro per unità. Chiaramente la complicazione varia allo stesso modo.

Vendor: cisco, Juniper, HP/3com/H3G, Extreme Networks, Foundry/Brocade ed altri

Si tratta sostanzialmente di computer dedicati con sistemi operativi proprietari (IOS, JunOS, ExOS...), a volte anche molto sofisticati.

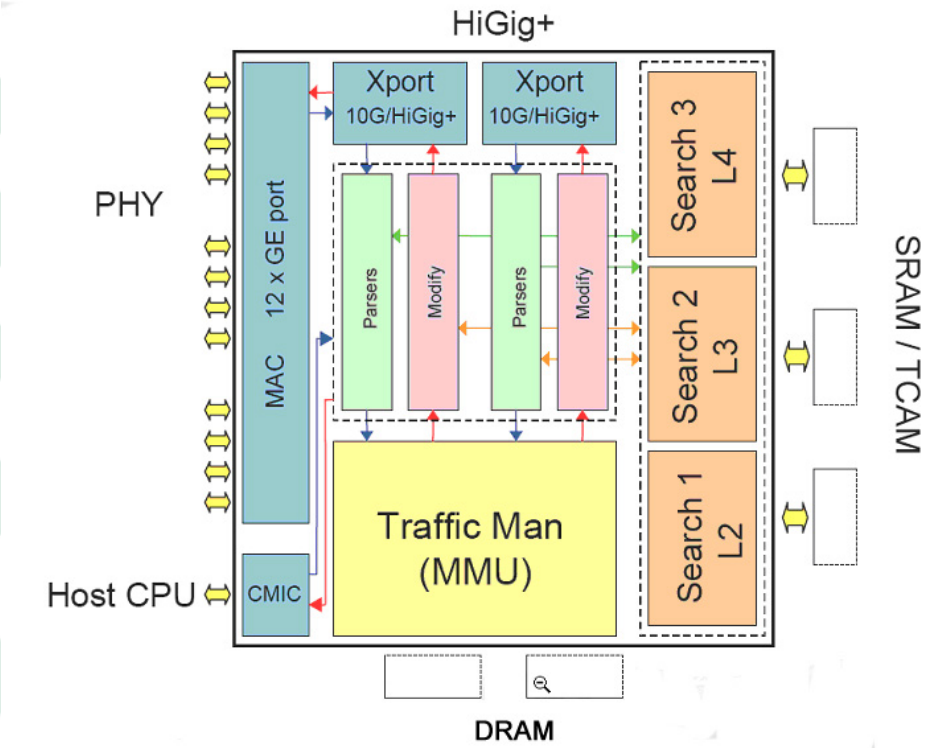
LABORATORI GUGLIELMO MARCONI

Control Plane e Data Plane

Per inoltrare molti Gbit/s non si possono usare le tradizionali CPU

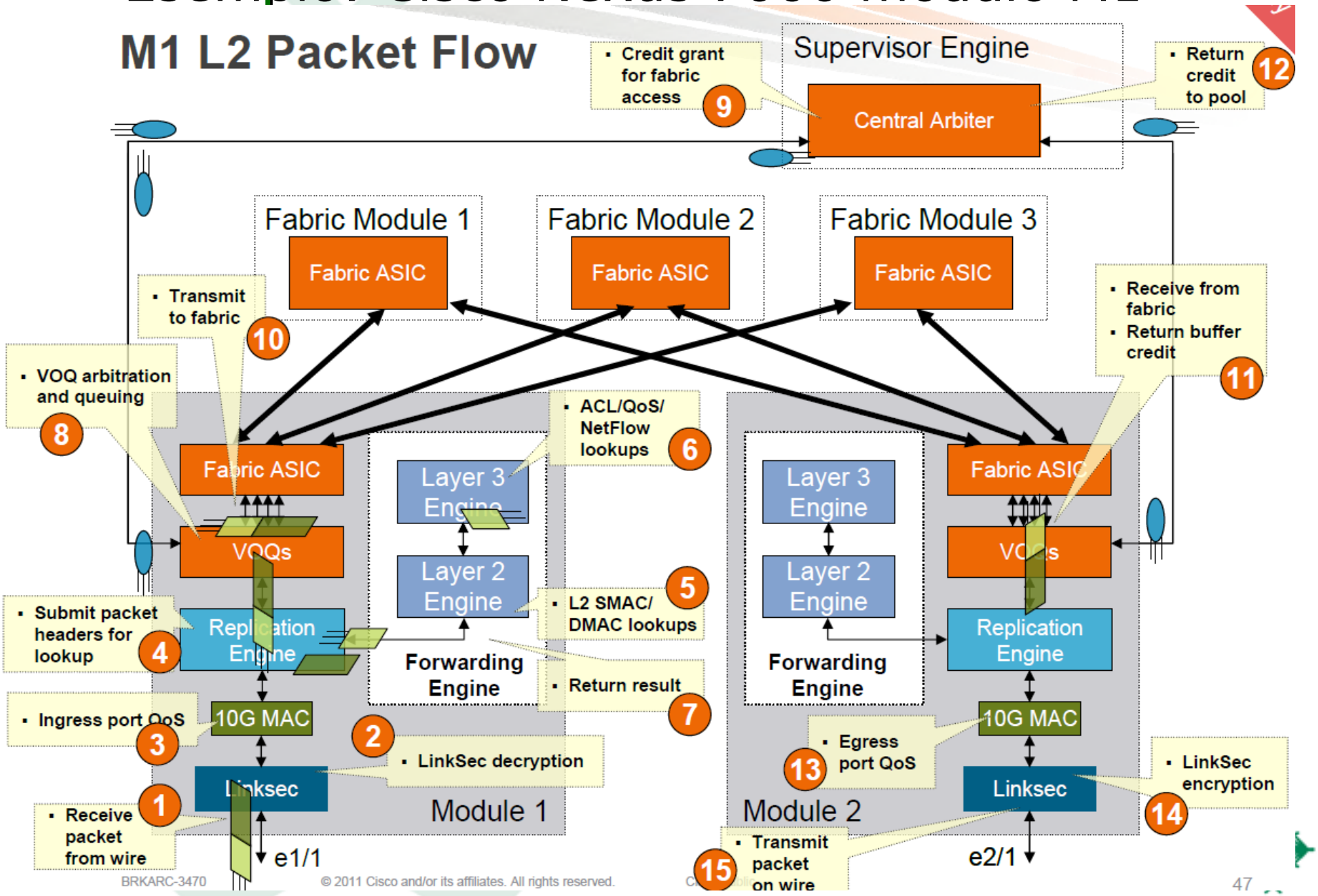
- Data Plane: ASIC o chip specializzati che inoltrano il traffico
- Control Plane: CPU che li gestisce, e implementa i protocolli di routing. Gestione: Management Plane

Es. Broadcom StrataXGS III, chip per forwarding multilayer (da analogzone.com)



LABORATORI GUGLIELMO MARCONI

Esempio: Cisco Nexus 7000 modulo M1



Monitoraggio e gestione

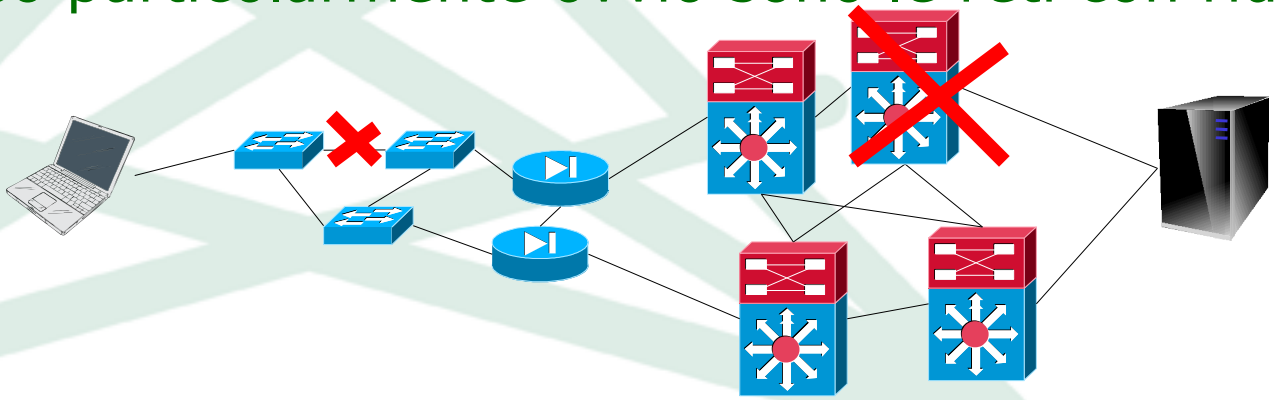
La gestione della rete è genericamente l'insieme di tutte le attività che si svolgono per farla funzionare. Normalmente questo comprende:

- Operazioni fisiche (Maintenance): installazioni, sostituzioni
- Operazioni di configurazione (Administration, Provisioning): programmazione degli apparati per mutate o aumentate esigenze
- Monitoraggio e troubleshooting (Operations): misura e verifica di buon funzionamento, reattiva e proattiva

Monitoraggio

Il monitoraggio serve per accorgersi dei potenziali problemi PRIMA che abbiano effetto: questo è essenziale per avere una rete che funziona "sempre".

Un caso particolarmente ovvio sono le reti con ridondanza:



Se la rete resiste ad un guasto, dobbiamo continuamente verificare che non ci siano guasti, altrimenti ce ne accorgeremo solo al secondo guasto...

Monitoraggio - cosa si monitora

- Guasti non causanti disservizio
- Guasti causanti disservizio, per saperlo prima degli utenti
- Indicatori di performance sugli apparati
  - CPU, RAM, etc: in fondo comprendono dei computer
- **KPI**: loss, delay (RTT), jitter
- Parametri ambientali
- Flussi di traffico
  - La banda di un collegamento è un suo parametro primario, spesso legato al costo. Occorre monitorarne l'utilizzo
- Indicatori di errore (il TCP resiste agli errori, ma non devono essere troppi)
  - Errori fisici su interfacce
  - Pacchetti scartati per traffico o per altri motivi

Monitoraggio - obiettivi

- Prevenire malfunzionamenti
- Risolvere rapidamente malfunzionamenti che non siamo riusciti a prevenire
- Per le aziende, disservizio = mancata produttività
- Per gli enti, disservizio = disagio ai cittadini
- Per i carrier, disservizio = mancati SLA = penali (talvolta)

Città

Si rompe un cavo e il Santa Maria va in tilt

Tre ore di black out. Impossibile refertare cartelle cliniche e fare terapie

Opzioni avanzate

Guasto sulla rete informatica, all'Asl bloccate le prenotazioni Il problema del Cup ha causato disagi per 2 giorni

il Tirreno — 15 novembre 2001 pagina -1 sezione: CECINA

CECINA. Un guasto alla linea interna dei computer dell'Asl ha bloccato per due giorni l'attività di prenotazione dei Cup. Un disguido che ha creato comprensibili disagi ai cittadini, che non hanno potuto prenotare visite specialistiche. L'intera agenda dell'Asl è infatti informatizzata: avere in rete i dati di tutta l'azienda sanitaria è chiaramente un vantaggio: consente infatti di

NEL SITO NEL WEB VAI

MONDO SOCIETÀ TECNOLOGIA OPINIONI MULTIMEDIA BLOG INTERATTIVI RUBRICHE

SALUTE SPORT COVERSTORY DOSSIER STYLE&DESIGN SPECIALI FOOD&WINE CHIESA

STAMPA INVIA CONDIVIDI

UN GUASTO ALLE LINEE DI FIBRE OTTICHE HA BLOCCATO LA STRUTTURA DI ZELARINO

Blackout, ospedale isolato per 5 ore

Telefoni e computer in tilt, in Radiologia operatori al lavoro al buio. Reparti paralizzati. Sospeso un intervento di Neurochirurgia. Nessun pericolo per i pazienti

Ospedale dell?Angelo isolato per più di cinque ore, nella tarda mattinata di ieri e fino al pomeriggio. Telefoni e computer in tilt. Il centralinista impossibilitato a passare le telefonate. I sanitari nei reparti bloccati, incapaci di stampare un referto o di mettersi in contatto con i colleghi di un altro reparto. Qualcuno, ad esempio in Radiologia, è stato addirittura costretto a lavorare al buio. In un primo momento nella squadra composta da una ventina di ingegneri che subito si è messa al lavoro per cercare di individuare il guasto c?è stato chi ha pensato che si trattasse dell?opera di un hacker. Una verifica puntuale, però, ha permesso di appurare che la rete di protezione non risultava violata. Più «semplicemente» si era verificato un guasto sull?apparato in fibre ottiche che collega l?ospedale ai server. Un guasto tale

LABORATORI GUGLIELMO MARCONI

Complessità

- Le reti sono a volte estremamente complesse e quasi sempre eterogenee
- La gestione è necessariamente complessa, e peggio ancora il troubleshooting
- Il monitoraggio è una specie di **troubleshooting continuo**, automatizzato: ancora più complesso
- Le frontiere amministrative sono i punti più delicati: le reti ne hanno necessariamente tante
- Molti contatti con molti soggetti diversi, "rimpalli" di responsabilità

Protocolli utilizzati

- Gestione
  - telnet, ssh, web: i "soliti" protocolli del TCP/IP
  - nicchie: SNMP, WBEM, NETCONF
- Monitoraggio
  - ping (ICMP), SNMP
  - Netflow
  - telnet, ssh
  - nicchie: WBEM

Sono tutti protocolli basati su TCP/IP - trasportati dalla stessa tecnologia che vogliamo gestire. Un requisito fondamentale è quindi la connettività verso la rete da gestire. La gestione può essere:

- in-band
- out-of-band

Gestione in-band

- I protocolli usati per la gestione viaggiano nello stesso mondo IP della rete che stiamo gestendo

```
bergonz@mason:~$ telnet 192.168.0.2
Trying 192.168.0.2...
Connected to 192.168.0.2 (192.168.0.2).
Escape character is '^]'.


User Access Verification

Password:

chiamalo>sh int fa0
FastEthernet0 is up, line protocol is up
  ...
  Internet address is 192.168.0.2/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
 ...
```


LABORATORI GUGLIELMO MARCONI

Gestione in-band

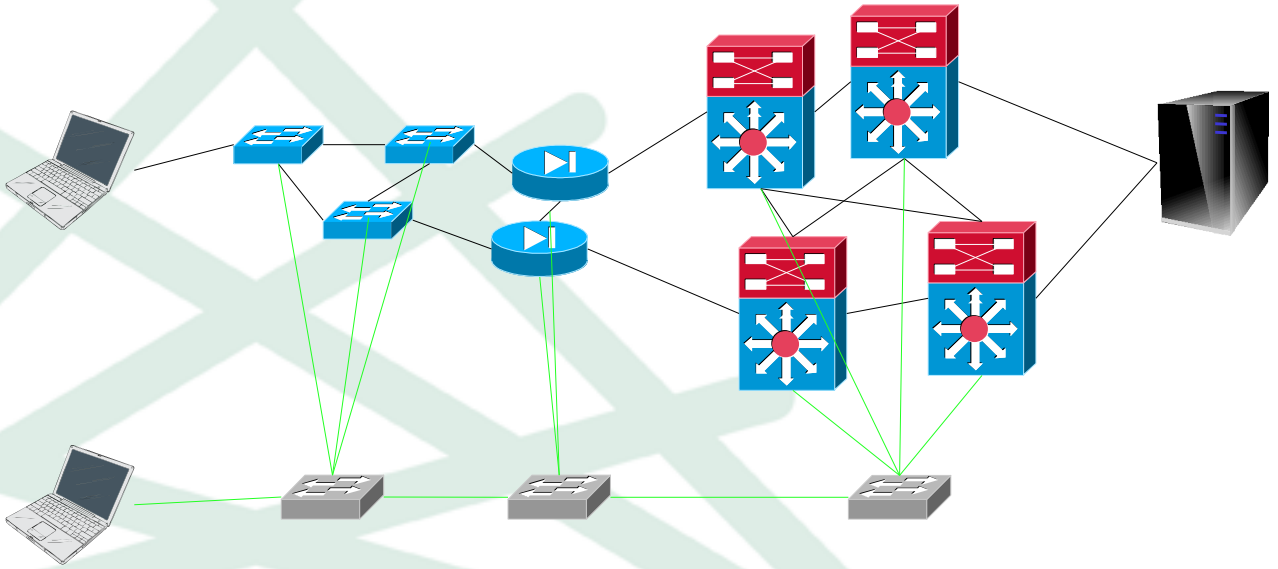
- Si può usare un qualunque PC per la gestione
- Non servono portanti o collegamenti separati
- Tutti gli apparati lo supportano

Ma attenzione:

- Si può usare un qualunque PC? Anche quello dell'utente!
- Tagliarsi fuori dalla gestione se c'è un guasto, se si sbaglia configurazione, etc. E' un problema rilevante.
- Problemi egg/chicken
- In condizioni di degrado o guasto il troubleshooting è più difficile, mentre quando tutto va bene è inutile.

```
chiamalo#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
chiamalo(config)#int fa0
chiamalo(config-if)#shutdown
.....Ehm..
```

Gestione out-of-band (OOB)



- Costruire una rete IP completamente e fisicamente separata, dedicata alla gestione
- Più è separata e meglio è, dato che i guasti alle due reti devono essere il più possibile scorrelati
- E' (era) la norma nelle reti di telecomunicazioni tradizionali (OSS, Operations Support Systems, per la gestione)
- Rispetto alla pila OSI, si può essere in-band a certi livelli ed out-of-band ad altri

Gestione out-of-band (OOB)

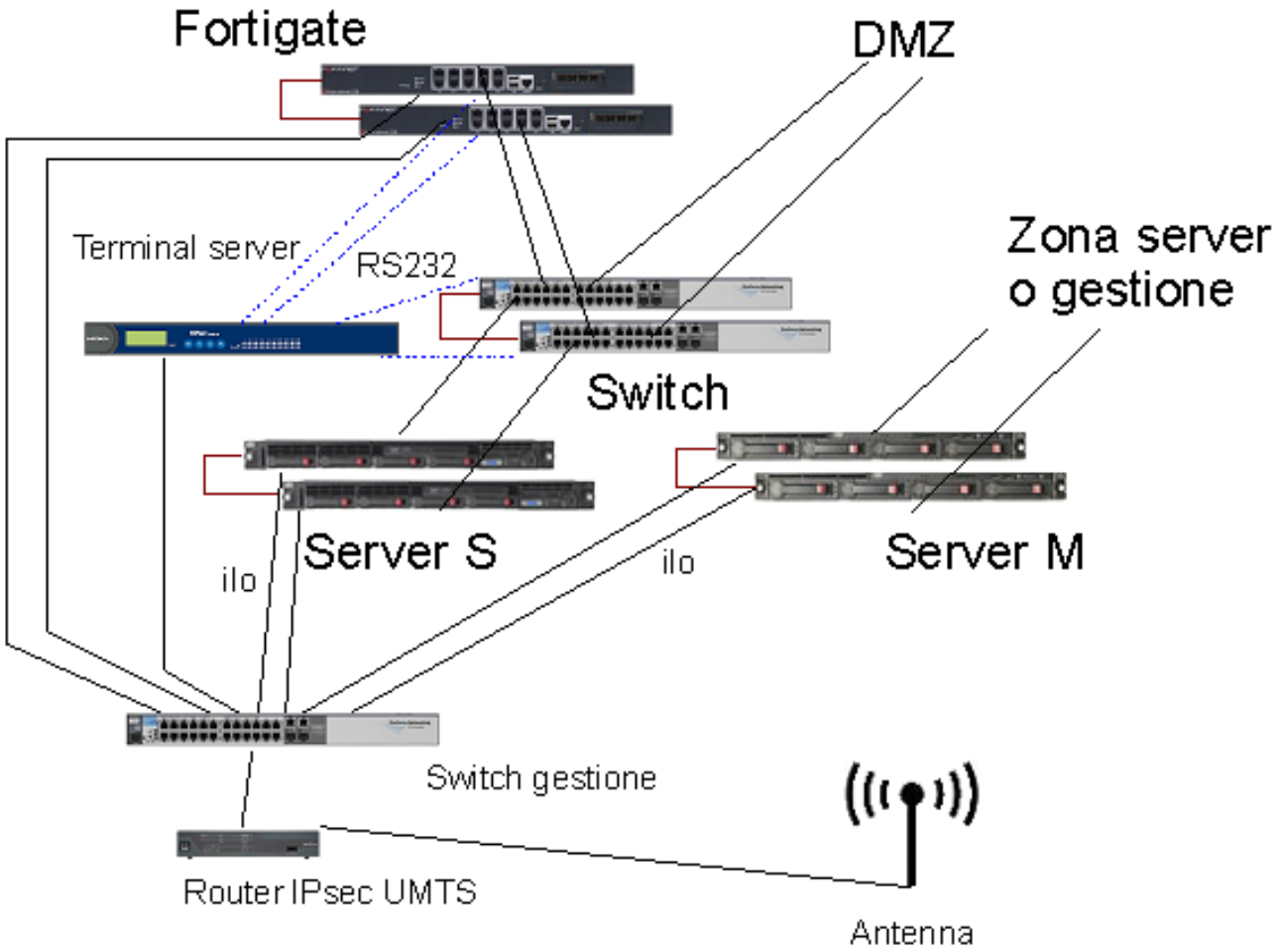
- Più facile impedire accessi non autorizzati
- Più probabile accedere in condizioni di degrado o guasto
- Meno probabile tagliarsi fuori, nessun problema egg/chicken

Ma ovviamente:

- Costi per i circuiti
- Molti apparati non lo supportano -> costi e complicazioni

Non è molto frequente

Gestione out-of-band (OOB)



- Router UMTS 800 euro, TS 8 porte 750 euro, switch 250 euro, licenza ILO advanced per server HP 350 euro

Protocolli per la gestione

Ricordiamo che gli apparati di rete sono in primo luogo dei computer

- CLI (Command Line Interface), via emulazione di terminale
  - Seriale RS 232
  - Telnet, SSH
- File transfer
  - TFTP, FTP, SCP
- Web
- Syslog, Netflow / IPFIX
- NTP
- Protocolli per dati strutturati
  - SNMP
  - altri

LABORATORI GUGLIELMO MARCONI

Accesso alla CLI

Via seriale

Quasi tutti gli apparati richiedono una prima configurazione da console seriale EIA RS232 (V.21/V.24).

E' anche usata come accesso di emergenza, quando si è del tutto tagliati fuori.

Molti portatili moderni non hanno più la seriale, ed occorre usare adattatori USB, inoltre il connettore può essere diverso da apparato ad apparato.

Via rete TCP/IP

Il telnet è il protocollo universalmente usato per accedere alla CLI. Normalmente viene protetto da ACL (Access Control List) basate sull'IP sorgente

SSH è teoricamente più sicuro, ma è più delicato.

Autenticazione Autorizzazione Accounting (AAA)

- Normalmente alla CLI ci si autentica con username e password
- La "best practice" è:
  - Backend di AAA ridondato (protocollo RADIUS, Remote Authentication Dial In User Service) ma sopravvive il TACACS+, Terminal Access Controller Access Control System)
  - Chiave RADIUS diversa per ogni apparato
  - Account locale diverso per ogni apparato, utilizzabile se il RADIUS non è raggiungibile
- Questo meccanismo si usa per telnet, ssh, web. Sulla seriale a volte si chiede l'autenticazione, a volte no.
- Si usano tecnologie più forti e sofisticate per accedere allo spazio IP di gestione (VPN, strong authentication).

CLI

- La CLI di una apparato di rete rappresenta solitamente la sua interfaccia di gestione principale:
  - Quella da cui si può fare tutto
  - Quella che insegnano ai corsi
  - Quella sulla quale si formano gli skill del personale
- Origini: Digital Equipment Corp. (DEC)
- Diffusione: cisco IOS (Internetwork Operating System)
- Oggi molti hanno CLI IOS-like, esistono CLI innovative (JunOS)
- In IOS, ma anche in quasi tutti gli apparati, il database di configurazione è rappresentato come una sequenza di comandi CLI. Si può salvare la configurazione, e ripristinarla su un apparato nuovo "incollandola" sull'emulatore di terminale.

CLI

```
chiamalo#conf t
chiamalo(config)#router ospf 1
chiamalo(config-router)#?
Router configuration commands:
  area                    OSPF area parameters
  auto-cost               Calculate OSPF interface cost according to bandwidth
  capability              Enable specific OSPF feature
  compatible              OSPF compatibility list
  default                 Set a command to its defaults
  default-information     Control distribution of default information
  default-metric          Set metric of redistributed routes
  discard-route           Enable or disable discard-route installation
  distance                Define an administrative distance
  distribute-list         Filter networks in routing updates
  domain-id               OSPF domain-id
  domain-tag              OSPF domain-tag
...
```

Trasferimento file

- A volte serve trasferire file da e verso gli apparati
  - Salvataggio configurazione
  - Pezzi di configurazione da inserire
  - Immagini di software per l'upgrade
- Resta molto diffuso il TFTP (Trivial File Transfer Protocol)
  - Inefficiente (UDP senza finestra)
  - Privo di qualsiasi meccanismo di sicurezza
- Se si riesce, si usa SCP, Secure CoPy
- Capita di dover trasferire file su seriale: in tal caso si va a ripescare Xmodem/Ymodem/Zmodem (Hyperterminal di Windows, minicom di linux)

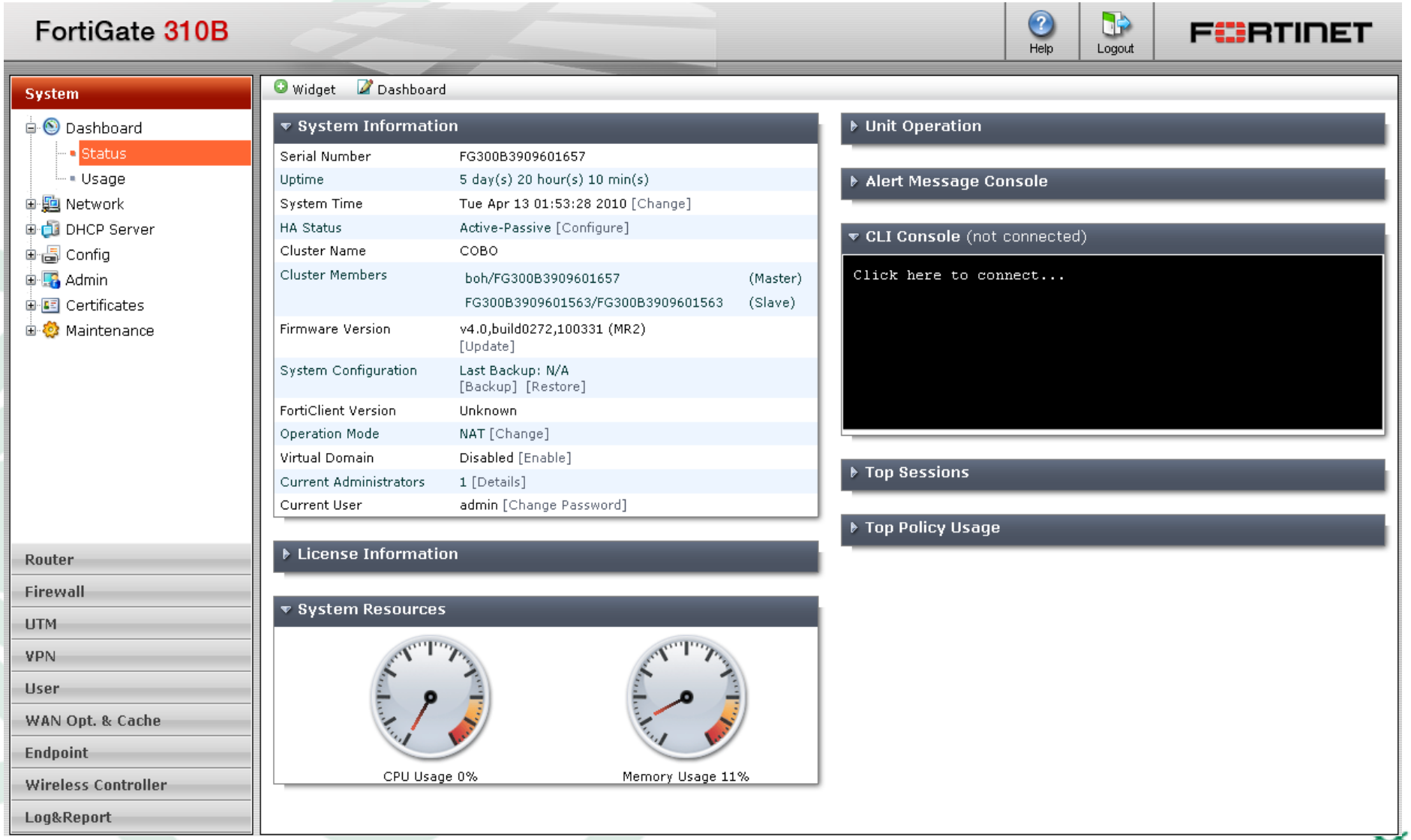
Scripting

- Alcune CLI (non tutte) supportano linguaggi di scripting embedded (JunOS, IOS), per reagire agli eventi
  - Interessanti in reti single vendor, o per lavori specifici su uno o pochissimi apparati
  - A volte sono script di reazione ad eventi, con esito incerto (meglio test periodici)
- Soluzioni per lo scripting di sessioni telnet/SSH
  - RANCID (Really Awesome New Cisco confIg Differ)
  - Basato su Tcl ed expect
  - Raccoglie inventario hw/sw e configurazione
  - Mantiene storia in CVS o SVN e segnala differenze
  - Consente di dare lo stesso comando in sequenza su più apparati

Gestione via web

- Quasi tutti gli apparati di rete offrono un'interfaccia di gestione via web
- Pochi però la usano, e comunque solo per cose semplicissime
- Fanno eccezione i firewall:
  - Sono macchine un po' al confine tra informatica e telecomunicazioni
  - A volte hanno anche appositi software di gestione

Gestione via web



LABORATORI GUGLIELMO MARCONI

Syslog

- Messaggi sostanzialmente di testo, non strutturati, RFC3164
  - Facility, severity, mittente, timestamp, tag, testo
  - Utile all'operatore, difficile da utilizzare da programma
- Viaggia su UDP, senza conferme
  - Quando sarebbe più utile, non arriva
- I firewall tendono a generare volumi enormi
  - E' un uso che sconfina nell'accounting
  - Necessario software di raccolta prestante (syslog-ng)
  - Esistono nicchie con protocolli migliori

```
Apr 13 12:15:36 172.27.129.78 1185874: Apr 13 10:15:35: %SW_MATM-4-
MACFLAP_NOTIF: Host 0022.56cc.0e4c in vlan 3025 is flapping between port Gi0/4
and port Gi0/1
Apr 13 12:15:37 gradenigo-a 816786: Apr 13 12:15:36: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Serial1/0:26, changed state to up
```


LABORATORI GUGLIELMO MARCONI

Netflow / IPFIX

- Protocollo per la trasmissione di dati statistici sull'uso della rete
  - L'apparato (Metering Process) osserva i flussi di traffico in un punto (Observation Point)
  - Il flusso è un insieme di pacchetti che condividono alcune caratteristiche (es. pentupla IP-proto-port)
  - Ogni tanto scarica su un server (Collector) i dati relativi ai flussi osservati
- Oneroso, se si pretende di osservare tutto il traffico (es. billing)
- Semplice, se ci basta un campionamento a fini statistici (sampled Netflow o sFlow)
- Netflow era il nome originale quando l'ha inventato Cisco, IP Flow Information eXport è ora il nome standard. Moltissime le varianti.

NTP Network Time protocol

- Fondamentale per avere diagnostiche significative
- Fortunatamente gli apparati di rete non hanno dimostrato la stessa idiosincrasia per i "leap second" di alcuni server

Da info@hetzner.de

Oggetto **Hetzner Online Client Information: Please check the CPU load of your server!**

A [redacted]

Dear subscribers,

During the night of 30.06.2012 to 01.07.2012 our internal monitoring systems registered an increase in the level of IT power usage by approximately one megawatt.

The reason for this huge surge is the additional switched leap second which can lead to permanent CPU load on Linux servers.

R. [redacted] - was I: errore distribuzione orario Galielo Ferraris 27/03/2013 15:22

s Sistemisti <sistemi [redacted] labs.it> Altre azioni

stemista ha telefonato ad inrim e gli hanno confermato che
uto un crash hardware questa notte.
il sistema era indietro di 30 minuti. Gli ha anche chiesto di pubblicare una news per annunciare il problema (se lo faranno http://www.inrim.it/ntp/news_i.shtml).
Il server proxy [redacted] da noi ha fatto Patching, si è riavviato, ha chiesto aggiornamento e gli è arrivato l'orario sbagliato (probabilmente durante il fail).
A quel punto è stato aggiornato il Domani Controller principale interno, che prende l'ora dai due proxy che escono. Da li si è sparso su host e pc.

Bel casino, che è stato ripristinato alle 7.30...

Protocolli per dati strutturati

- SNMP (Simple Network Management Protocol), inventato nel 1988 (RFC1067), resta lo standard implementato da tutti gli apparati ed ampliamente utilizzato
  - SNMPv1: GET/GETNEXT/SET/TRAP, pochi tipi di dati, autenticazione plaintext con stringa "community"
  - SNMPv2c: GETBULK ed INFORM
  - SNMPv3: autenticazione e privacy con crittografia
- Raramente, alcuni apparati implementano protocolli più moderni, standard oppure no, basati su RPC XML (CIM-XML, WBEM, NETCONF, etc.). Poco diffusi, tool proprietari dei vendor.
- Il protocollo SNMP di solito viene usato nella versione 1 o 2c. La versione 3, pur molto diffusa, non è molto usata in quanto complicata e percepita come "acerba".

SNMP: modello di gestione

- Nel modello SNMP si distinguono agenti (gli apparati), che espongono variabili e generano eventi, e manager (il server dove gira il software) che leggono o scrivono le variabii e raccolgono gli eventi.
- Le variabili sono organizzate ad albero. Primitive:
  - GET: il manager legge una variabile data
  - GETNEXT: il manager legge la variabile successiva ad una variabile data
  - GETBULK (SNMPv2): il manager legge tutte le variabili di un sottoalbero (fino ad un numero massimo)
  - SET: il manager scrive una variabile
  - TRAP: l'agente invia la notifica di un evento al master
  - INFORM (SNMPv2): come il TRAP, ma con acknowledge
- Più tutte le risposte. Incapsulate tipicamente in UDP.

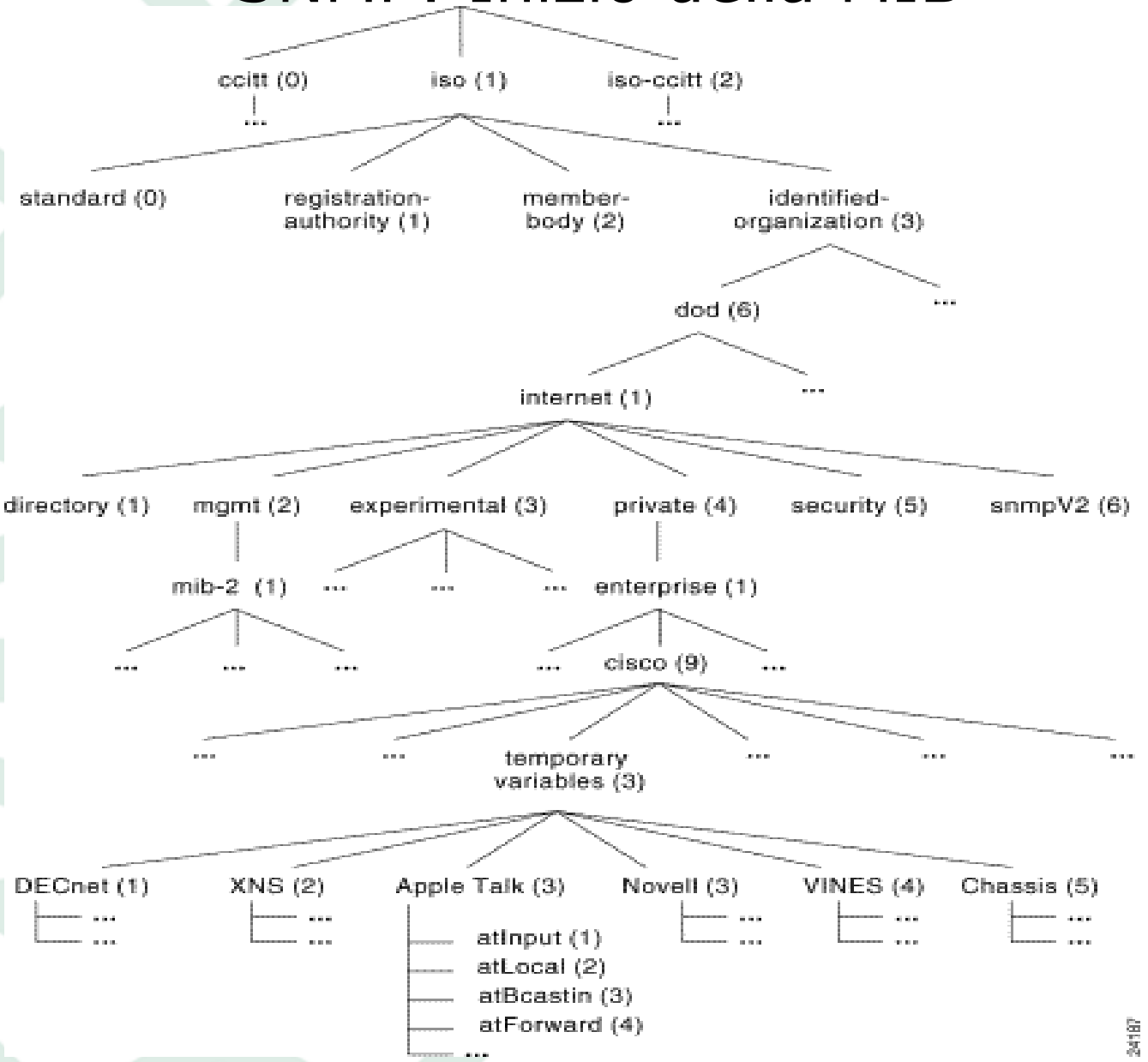
SNMP: MIB

- L'insieme delle variabili gestite tramite SNMP si chiama MIB (Management Information Base)
- Ogni variabile è un'istanza di un oggetto
- Ogni oggetto ha:
  - Nome
  - OID (Object IDentifier) numerico
  - Sintassi e semantica, descritte in ASN.1 (Abstract Syntax Notation - 1)
- Nomi ed OID sono disposti in un albero

Gli organismi di standardizzazione definiscono le parti di MIB (ma normalmente si chiamano semplicemente MIB) relative alle funzionalità standardizzate (es. Spanning tree, OSPF, IP)

Aziende ed altri privati possono disporre di un proprio sottoalbero dove definire le proprie MIB

SNMP: Inizio della MIB



Fonte: pulsewan.com

LABORATORI GUGLIELMO MARCONI

SNMP: OID

- Un oggetto e le sue istanze, si identificano con la sequenza di nomi nell'albero, oppure di numeri, o talvolta anche con una notazione mista. Nelle PDU ovviamente viaggiano i numeri.
- Ad esempio l'oggetto "nome dell'apparato", sysName, è
  - 1.3.6.1.2.1.1.5
  - iso.org.dod.internet.mgmt.mib-2.system.sysName
- Ogni apparato ha un solo nome, perciò c'è una sola istanza, numerata con 0:

```
bergonz@mason:~$ snmpget -Of 192.168.0.2 .1.3.6.1.2.1.1.5.0
.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = STRING: chiamalo
```

A volte si antepone un "." per indicare che si parte dalla radice. Le istanze possono essere più subidentifier.

- E' lo stesso spazio delle OID che si usano in LDAP, X.509 (quello dei certificati SSL), HL7 e DICOM (protocolli per dati medici). "Alto" 128 e "largo" 2^32-1.

SNMP: OID e tabelle

- Le tabelle in SNMP sono nella forma "sequenza di colonne"
- Esempio: la tabella delle interfacce (ifTable) 1.3.6.1.2.1.2.2
  - E' una sequenza di colonne (ifEntry) 1.3.6.1.2.1.2.2.1
  - Ci sono tante colonne, la seconda è ifDescr 1.3.6.1.2.1.2.2.1.2
  - Ha una istanza per interfaccia. Il numero di istanza è sostanzialmente arbitrario. Sono da immaginare un po' come chiavi surrogate.

```
bergonz@mason:~$ snmpget -Of 192.168.0.2 .1.3.6.1.2.1.2.2.1.2.7
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.7 =
STRING: FastEthernet0
```

SNMP: Walk di tabelle

- Se non conosciamo i numeri di istanze di una tabella, usiamo il getnext per scoprirli:

```
bergonz@mason:~$ snmpgetnext -Of 192.168.0.2 .1.3.6.1.2.1.2.2.1.2
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.1 =
STRING: BRI0
bergonz@mason:~$ snmpgetnext -Of 192.168.0.2 .1.3.6.1.2.1.2.2.1.2.1
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.2 =
STRING: BRI0:1
...
```

- Funziona se la tabella non cambia rapidamente
- I tool offrono funzionalità di "walk": dato un sottoalbero, fare getnext finché non si esce dal sottoalbero:

```
bergonz@mason:~$ snmpwalk -Of 192.168.0.2 .1.3.6.1.2.1.2.2.1.2
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.1 =
STRING: BRI0
...
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.7 =
STRING: FastEthernet0
...
...
```

SNMP: Trap

- Le trap, che rappresentano eventi, hanno un OID (dalla v2). Nella PDU c'è poi una sequenza di OID e valori di variabili, che rappresentano cosa è successo. Ad esempio la linkDown 1.3.6.1.6.3.1.1.5.3:

```
linkDown NOTIFICATION-TYPE
    OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }
    STATUS  current
    DESCRIPTION
            "A linkDown trap signifies that the SNMP entity, acting in
            an agent role, has detected that the ifOperStatus object for
            one of its communication links is about to enter the down
            state from some other state (but not from the notPresent
            state).  This other state is indicated by the included value
            of ifOperStatus."
    ::= { snmpTraps 3 }
```

Le trap sono fatte per essere interpretate da programma. Sono diffuse soprattutto nei tool proprietari dei vendor. Per un utilizzo umano, syslog è più immediato.

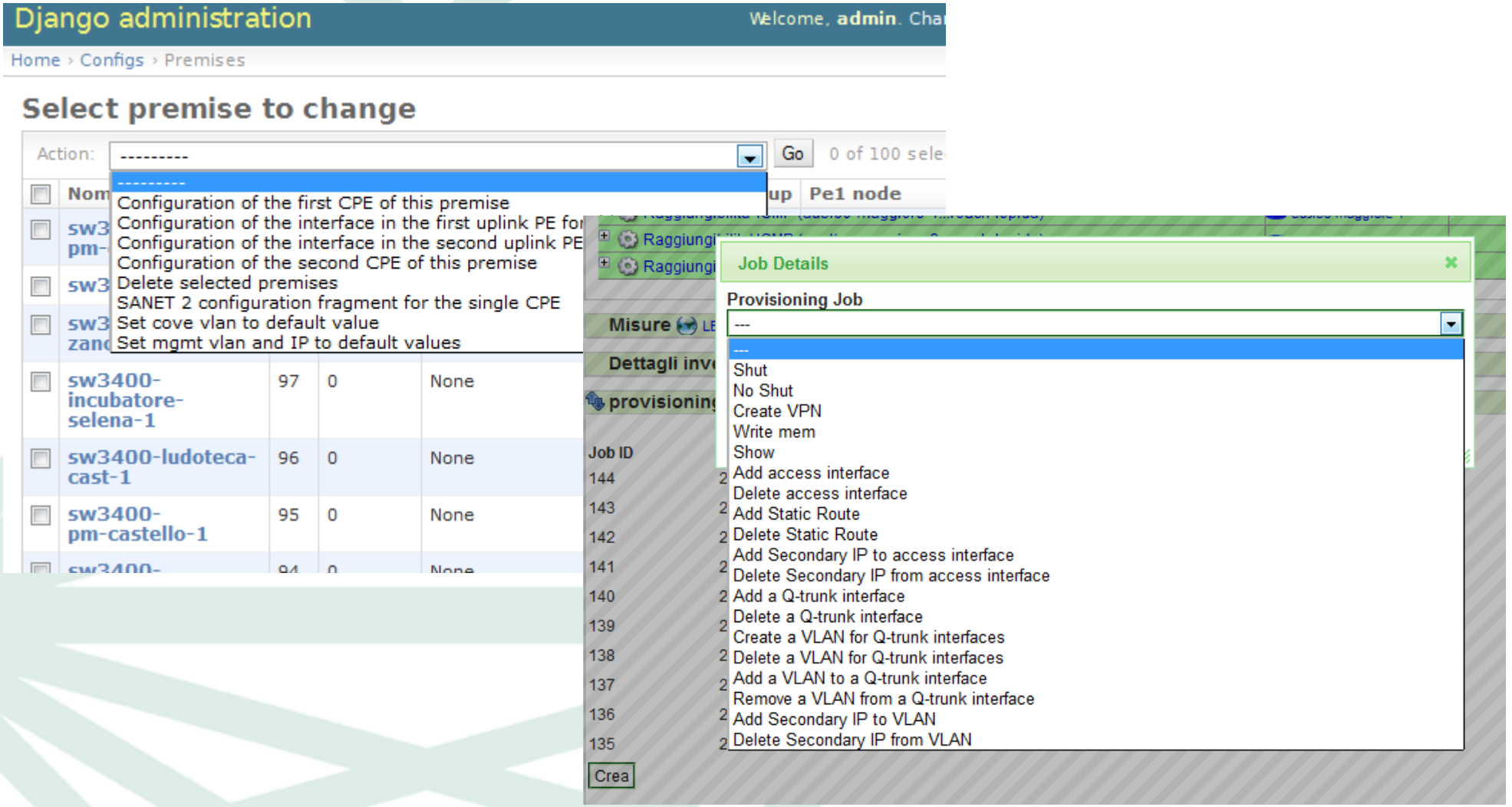
Strumenti gestione e monitoraggio

- Strumenti di basso livello:
  - ping e traceroute in tutti i sistemi operativi
  - ci sono versioni più o meno ricche di opzioni
  - net-snmp, comprende agenti per vari sistemi operativi e tool da linea di comando Unix/Windows
- Strumenti generici di gestione e monitoraggio, multivendor, commerciali
  - Tendono ad essere MOLTO complicati e costosi
  - HP Openview, IBM Tivoli, ...
- Strumenti di gestione e monitoraggio del vendor
  - Tipicamente funzionano ABBASTANZA bene ed hanno costi limitati
  - Ovviamente con gli apparati di altri vendor fanno poco o niente
  - CiscoWorks, HP Procurve Manager, 3com IMC

Automazione del provisioning

- Il provisioning tende ad essere estremamente ripetitivo
  - Abilitare una porta su una certa VLAN
  - Collegare la N-esima sede dello stesso cliente
- Automazione: tradizionale
  - Tool proprietari (es. Cisco)
  - Scripting
  - Soluzioni dedicate
- Automazione: emergenti
  - Tool di configuration management (puppet, etc.)
  - SDN
- Limiti
  - Se la rete non è enorme, non è poi così ripetitivo
  - Se la rete e' enorme, è eterogenea

Scripting e soluzioni dedicate



- Richiedono uniformità della rete, che raramente resta a lungo termine

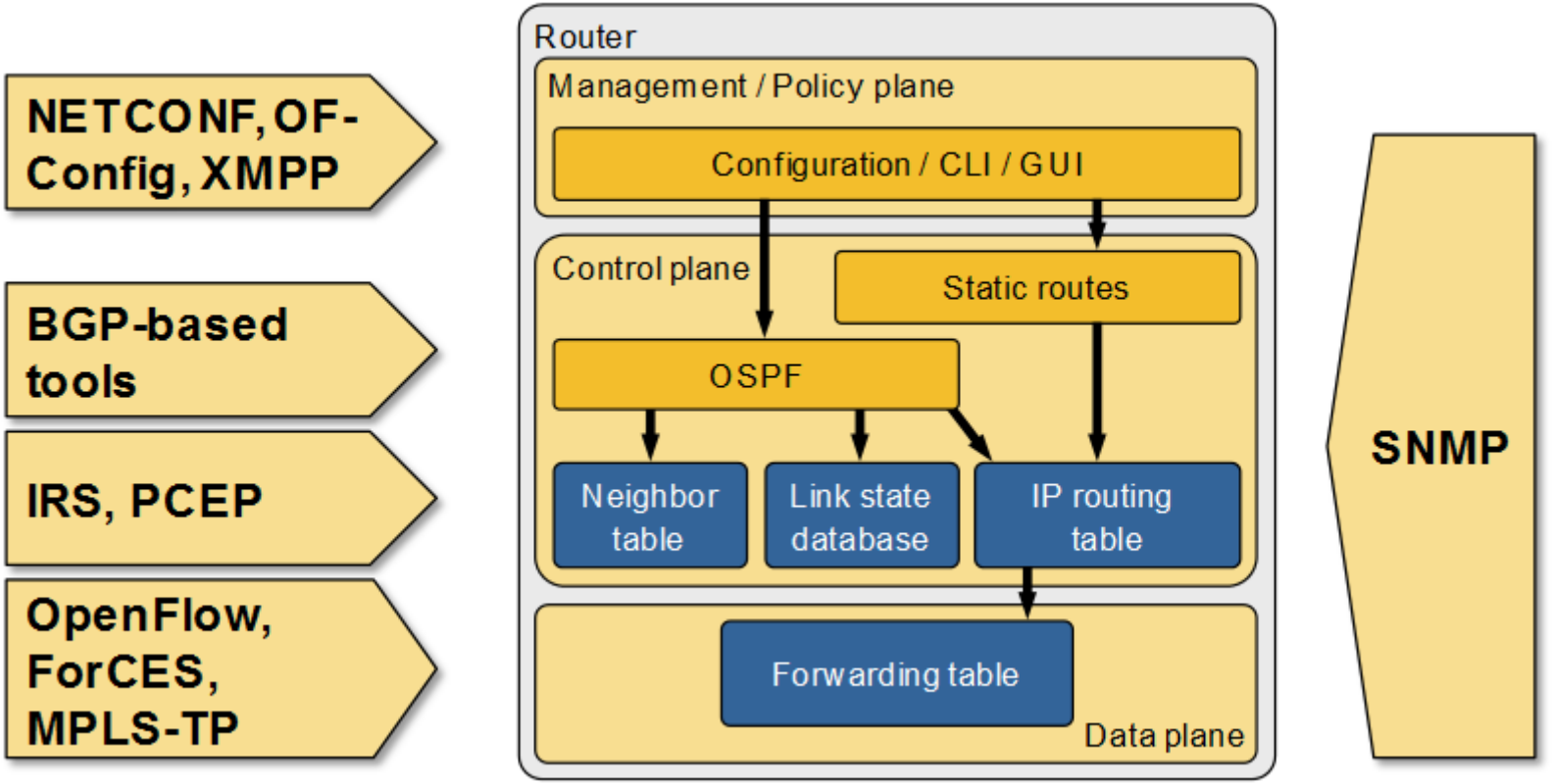
LABORATORI GUGLIELMO MARCONI

Software Defined Networking

Distaccare il control plane dal data plane

- ... e quindi centralizzare il control plane
  - Il controller comanda direttamente i data plane degli apparati, con un protocollo standard come OpenFlow, o proprietario
  - Possiamo sviluppare applicazioni sul controller per specifiche esigenze di networking
- Problema serio: I data plane sono tutti diversi!
  - Scalabilità, tempi di convergenza, OOB
- Si vede qualcosa in alcuni specifici casi
  - Switch virtuali negli host di VM (data plane è in software)
  - Reti di Data Center (piccole, stabili, costose)
  - Google dice di usarlo nel backend. Si costruiscono i loro switch.

SDN: tentativo di centralizzazione



- Gestione e automazione apparati fisici, secondo Ivan Pepelnjak
  - OF-CONFIG: NETCONF + OpenFlow
  - IRS: un tentativo di protocollo di routing centralizzato
  - PCEP: un tentativo di esgnalamento MPLS centralizzato
  - ForCES: un tentativo di standard IETF per SDN
  - MPLS-TP: MPLS sulle reti di trasporto (SDH, DWDM, etc.)

LABORATORI GUGLIELMO MARCONI

Problemi pratici e quotidiani del NOC

- Gli apparati, come i computer:
  - Hanno i bachi ed i guasti hardware, a volte evidenti ma a volte ben poco evidenti
  - Raramente sono identici tra loro (versioni software, generazioni di prodotti, evoluzione del mercato)
  - A volte si "impallano" senza apparente ragione. Inversamente correlato al costo.
- Gli apparati, diversamente dai computer
  - Non consentono l'installazione di software specifico per il troubleshooting (debugger, sniffer, etc.), bisogna fare con quello che è fornito, e non sempre è abbastanza
  - Non consentono di sviluppare software, o quasi
  - La "instrumentation" degli apparati di rete varia in un ampio spettro, in certi casi nulla o troppo

Problemi pratici e quotidiani del NOC

- Standard per la gestione:
  - SNMP è molto usato, ma ha dei limiti intrinseci: niente transazioni, tipi statici, autenticazione inesistente o poco pratica
  - Gli standard nuovi e potenti non sono utilizzati
- Le MIB SNMP in generale funzionano bene, ma ci sono casi in cui:
  - Non contengono quello che serve, difetti di progettazione (non è banale capire qual'è la giusta instrumentation)
  - Vengono superate dalla tecnologia, e restano indietro (es. i diversi "spazi" IP). Generalmente la MIB standard esce quando la tecnologia è in circolazione da un po', ed i vendor inizialmente non hanno MIB, poi usano MIB proprietarie.

Problemi pratici e quotidiani del NOC

- Tecnologie:
  - La stabilità e la robustezza degli apparati sono requisiti fondamentali, ma sono fattori di marketing poco efficaci, e non sono soggetti a specifiche precise.
  - Il mercato è in mano a pochi vendor, ma ogni tanto capitano apparati di vendor "di nicchia" che nessuno conosce bene.

Problemi pratici e quotidiani del NOC

- La gestione delle reti è un lavoro "sporco":
  - Parsing dei messaggi ricevuti con syslog
  - Monitoraggio di contatori che riciclano e talvolta si azzerano, senza primitive atomiche.
  - Le chiavi surrogate a volte cambiano senza motivo apparente (variabilità della ifIndex), non persistono ai reboot, etc.
  - Parsing della CLI: RANCID contiene una quantità di casistiche per inseguire la infinite varianti, ed è sempre indietro rispetto alla realtà

Accesso agli apparati

- A volte è veramente difficile
  - Salti di VPN, telnet, ssh per arrivare fino alla CLI che serve
  - Sicurezza vs. praticità
  - Apparati in luoghi improbabili (es. terminale satellitare del CNR al Monte Cimone)
  - Può volerci di più per trovare tutte le password necessarie che per fare il lavoro stesso (compromesso praticità vs. sicurezza)
  - Può essere impossibile l'accesso fisico al di fuori di certi orari (chiavi, guardie, ...)
  - Reperibilità: restare in zone di copertura UMTS

Problemi organizzativi

- A volte capita di non avere risposta a domande fondamentali:
  - Cosa dobbiamo gestire? Inventario degli apparati
  - Spesso è impossibile fare uno schema decente e completo, mantenere un inventario richiede sforzo, e quasi sempre si ha un'approssimazione
  - A volte si trovano apparati orfani o dimenticati, e si procede con il "password recovery". Quasi tutti gli apparati di rete lo consentono, e se non lo consentono sono da sostituire.
  - Fusioni e cambi di gestione concorrono a questo tipo di problemi

Case study //venice>connected

- Rete //venice>connected (www.veniceconnected.it)
  - Rete del Comune di Venezia - Venis s.p.a. - Fibre di proprietà.
  - Collega sedi comunali, AP WiFi sul canal grande, sedi e pontili ACTV, Casinò
  - 124 sedi su 2+10 POP, rilegamenti 1 Gbit/s, link core 10 Gbit/s. 15 VRF (mondi IP), uno è quello di Internet
- Apparati
  - Core: cisco 7600, POP: cisco ME6524
  - CPE: cisco ME3400 o IE3000
  - Access point tropos
  - Alcuni link Alvarion Breezenet

LABORATORI GUGLIELMO MARCONI

Case study //venice>connected

- Struttura
  - Rete MPLS, 12 PE, VPNv4, EoMPLS PW
  - internet in una VRF, un cliente multi VRF
- Problemi fisici
  - Impianti elettrici, accesso, rumorosità e temperatura in edifici storici
  - Estetica, installazioni in esterno edifici storici
- Accesso agli apparati
  - Management in-band, su GRT o vrf dedicate per varie tipologie di apparati, e limitazioni sul IP di provenienza, che è comunque di rete interna (dietro firewall)
  - RADIUS con account nominativi, utente locale di fallback

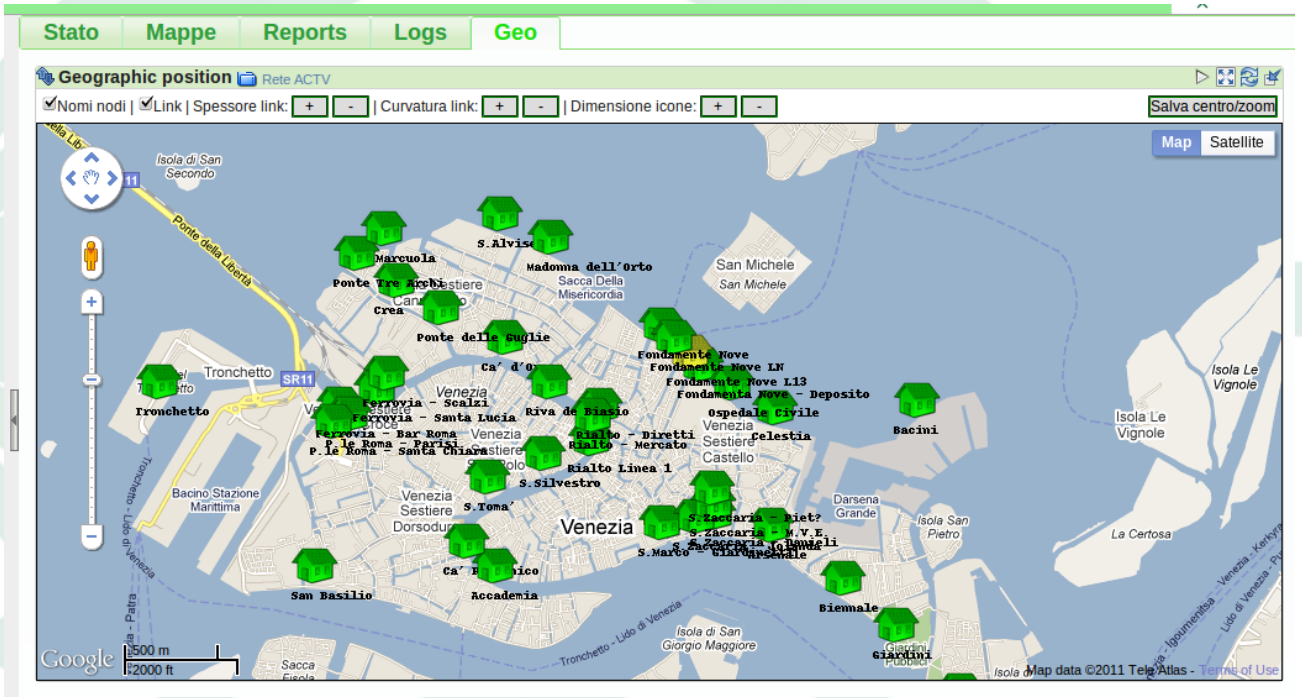
Case study //venice>connected

```
aaa authentication login default group radius local
aaa accounting system default start-stop group radius
username tlc password *********
line vty 0 4
 access-class managers in
 transport input telnet ssh

Tue Mar 22 14:37:48 2011
       Packet-Type = Access-Request
       User-Name = "bergonz"

root@netven2:~# cat /var/log/routerlog | fgrep bergonz
Mar 22 14:38:05 172.27.1.18 519: Mar 22 14:38:04.760 CEST: %SYS-5-CONFIG_I:
Configured from console by bergonz on vty0 (172.22.10.231)

ip vrf actv-mgmt
 ...
ip vrf mgmt
ip vrf mgmt-tropos
ip vrf mgmt-venis

interface GigabitEthernet1/13.503
 ip vrf forwarding internet
 ip address 94.247.8.3 255.255.255.0

bergonz@kickaha:~$ telnet 94.247.8.3
Trying 94.247.8.3...
telnet: Unable to connect to remote host: Connection refused
```


LABORATORI GUGLIELMO MARCONI

Case study //venice>connected

- Monitoraggio
  - SANET, con RANCID per inventario e configurazioni
  - netflow



LABORATORI GUGLIELMO MARCONI

Case study //venice>connected

```
sanet# sh targets node sw3400-farsetti-1
PATH                                                    ID     PRI NODE              IFACE DS STATUS    LASTDONE
------------------------------------------------------- ------ --- ----------------- ----- -- ------ -------------------
sw3400-farsetti-1:::cpe-reach                             2957   1 sw3400-farsetti-1             UP 2011-03-22 15:45:35
sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:iferrs-hc         3071   1 sw3400-farsetti-1 gi0-2       UP 2011-03-22 15:39:13
sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:nucast-target-hc  3072   1 sw3400-farsetti-1 gi0-2       UP 2011-03-22 15:46:05
sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:operstatus        3073   5 sw3400-farsetti-1 gi0-2       UP 2011-03-22 15:46:39
sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:stpnotblocking    3074   1 sw3400-farsetti-1 gi0-2       UP 2011-03-22 15:42:59
sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:stptrans          3075   1 sw3400-farsetti-1 gi0-2       UP 2011-03-22 15:42:56
sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:iferrs-hc         3076   1 sw3400-farsetti-1 gi0-3       UP 2011-03-22 15:38:17
sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:nucast-target-hc  3077   1 sw3400-farsetti-1 gi0-3       UP 2011-03-22 15:44:59
sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:operstatus        3078   5 sw3400-farsetti-1 gi0-3       UP 2011-03-22 15:47:01
sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:stpnotblocking    3079   1 sw3400-farsetti-1 gi0-3       UP 2011-03-22 15:44:25
sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:stptrans          3080   1 sw3400-farsetti-1 gi0-3       UP 2011-03-22 15:41:03
sw3400-farsetti-1:gi0-4:vc-cpe-pe:adjacent-cdp            3022   1 sw3400-farsetti-1 gi0-4       UP 2011-03-22 15:33:38
sw3400-farsetti-1:gi0-4:vc-cpe-pe:iferrs-hc               1094   1 sw3400-farsetti-1 gi0-4       UP 2011-03-22 15:38:40
sw3400-farsetti-1:gi0-4:vc-cpe-pe:operstatus              1095   5 sw3400-farsetti-1 gi0-4       UP 2011-03-22 15:46:47
sw3400-farsetti-1::vc-cpe-3400:cisco-cpu                  1076   1 sw3400-farsetti-1             UP 2011-03-22 15:43:04
sw3400-farsetti-1::vc-cpe-3400:cisco-ioram                1077   1 sw3400-farsetti-1             UP 2011-03-22 15:42:52
sw3400-farsetti-1::vc-cpe-3400:cisco-procram              1078   1 sw3400-farsetti-1             UP 2011-03-22 15:45:37
sw3400-farsetti-1::vc-cpe-3400:reach                      1079   6 sw3400-farsetti-1             UP 2011-03-22 15:46:02
sw3400-farsetti-1::vc-cpe-3400:reboot                     1080   1 sw3400-farsetti-1             UP 2011-03-22 15:36:55

sanet# sh measures node sw3400-farsetti-1
PATH                                        ID     NODE       IFACE DS LASTDONE            VERBSTATUS
------------------------------------------- ------ ---------- ----- -- ------------------- ------------------------
sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:i+   1130 sw3400-fa+ gi0-2    2011-03-22 15:50:21 expr1: 158389350, expr2:+
sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:i+   1131 sw3400-fa+ gi0-2    2011-03-22 15:50:41 expr1: 207682, expr2: 11+
sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:i+   1132 sw3400-fa+ gi0-3    2011-03-22 15:50:19 expr1: 2596914488537, ex+
sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:i+   1133 sw3400-fa+ gi0-3    2011-03-22 15:50:42 expr1: 118886009, expr2:+
sw3400-farsetti-1:gi0-4:vc-cpe-pe:ifgraph+    467 sw3400-fa+ gi0-4    2011-03-22 15:50:07 expr1: 6544386417015, ex+
sw3400-farsetti-1::vc-cpe-3400:cisco-cpug+    459 sw3400-fa+          2011-03-22 15:50:14 expr1: 5
sw3400-farsetti-1::vc-cpe-3400:cisco-iora+    460 sw3400-fa+          2011-03-22 15:50:23 expr1: 7205156, expr2: 5+
sw3400-farsetti-1::vc-cpe-3400:cisco-proc+    461 sw3400-fa+          2011-03-22 15:50:23 expr1: 11023592, expr2: +
```

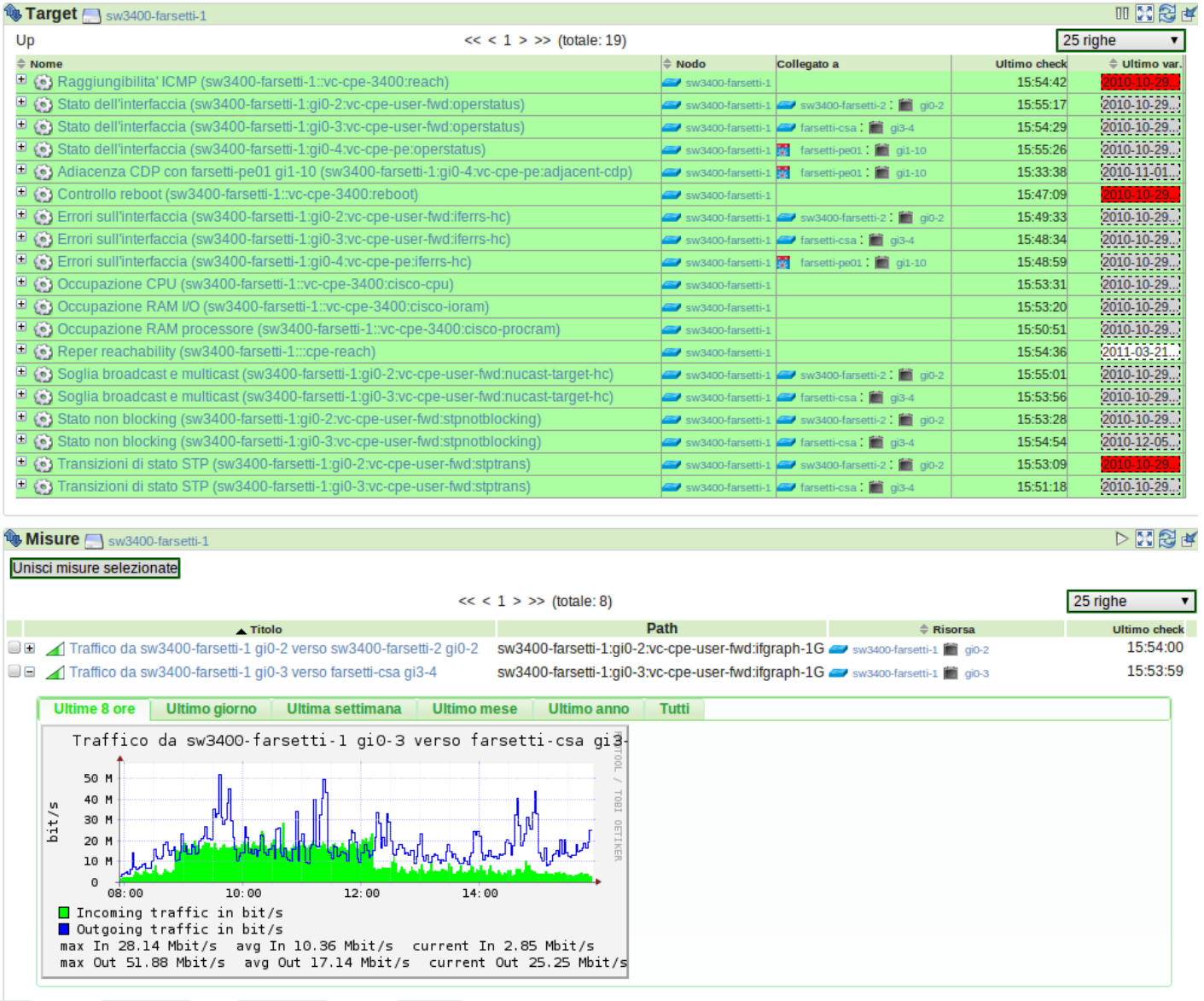

LABORATORI GUGLIELMO MARCONI

Case study //venice>connected

```
sanet# sh tar path sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:stpnotblocking
PATH                          : sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:stpnotblocking
ID                            : 3079
DESCRIPTION                   : STP state not blocking
LASTDONE                      : 2011-03-22 15:49:42 (1300805382)
LASTCONFIG                    : 2010-10-22 15:56:40 (1287755800)
MINPERIOD                     : 300
DELETED                       : False
DEPENDSON                     : Stato dell'interfaccia (sw3400-farsetti-1:gi0-3:vc-cpe-user-
fwd:operstatus) <--> farsetti-csa:gi3-4
TIMES                         : all
SHORTTRIES                    : 3
NODE                          : sw3400-farsetti-1
IFACE                         : gi0-3
CATEGORY                      : stpnotblocking
WHEN_SCHEDULED                : 2011-03-22 15:54:42 (144)
EXPR                          : 1.3.6.1.2.1.17.2.15.1.3.ifIndex2stp($node,$ifindex):vtpCommunity($node,
$community,$ifindex)@$node != $stpifacestate
STATUS                        : UP
TRIES                         : 0
STATUSLAST                    : UU
STATUSLASTCHANGE              : 2010-12-05 04:51:20 (1291521080)
VERBSTATUS                    : up: 1.3.6.1.2.1.17.2.15.1.3.ifIndex2stp($node,
$ifindex):vtpCommunity($node,$community,$ifindex)@$node != $stpifacestate expands to (5 != 2)penalty
0, not dampened
PRIMARY                       : False
DAMPENED                      : False
EMAIL                         : netwarning
PRIORITY                      : 1
STPIFACESTATE                 : 2
```


LABORATORI GUGLIELMO MARCONI

Case study //venice>connected



Target sw3400-farsetti-1

Up — << < 1 > >> (totale: 19) — 25 righe

Nome	Nodo	Collegato a	Ultimo check	Ultimo var.
Raggiungibilita' ICMP (sw3400-farsetti-1::vc-cpe-3400:reach)	sw3400-farsetti-1		15:54:42	2010-10-29..
Stato dell'interfaccia (sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:operstatus)	sw3400-farsetti-1	sw3400-farsetti-2 : gi0-2	15:55:17	2010-10-29..
Stato dell'interfaccia (sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:operstatus)	sw3400-farsetti-1	farsetti-csa : gi3-4	15:54:29	2010-10-29..
Stato dell'interfaccia (sw3400-farsetti-1:gi0-4:vc-cpe-pe:operstatus)	sw3400-farsetti-1	farsetti-pe01 : gi1-10	15:55:26	2010-10-29..
Adiacenza CDP con farsetti-pe01 gi1-10 (sw3400-farsetti-1:gi0-4:vc-cpe-pe:adjacent-cdp)	sw3400-farsetti-1	farsetti-pe01 : gi1-10	15:33:38	2010-11-01..
Controllo reboot (sw3400-farsetti-1::vc-cpe-3400:reboot)	sw3400-farsetti-1		15:47:09	2010-10-29..
Errori sull'interfaccia (sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:iferrs-hc)	sw3400-farsetti-1	sw3400-farsetti-2 : gi0-2	15:49:33	2010-10-29..
Errori sull'interfaccia (sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:iferrs-hc)	sw3400-farsetti-1	farsetti-csa : gi3-4	15:48:34	2010-10-29..
Errori sull'interfaccia (sw3400-farsetti-1:gi0-4:vc-cpe-pe:iferrs-hc)	sw3400-farsetti-1	farsetti-pe01 : gi1-10	15:48:59	2010-10-29..
Occupazione CPU (sw3400-farsetti-1::vc-cpe-3400:cisco-cpu)	sw3400-farsetti-1		15:53:31	2010-10-29..
Occupazione RAM I/O (sw3400-farsetti-1::vc-cpe-3400:cisco-ioram)	sw3400-farsetti-1		15:53:20	2010-10-29..
Occupazione RAM processore (sw3400-farsetti-1::vc-cpe-3400:cisco-procram)	sw3400-farsetti-1		15:50:51	2010-10-29..
Reper reachability (sw3400-farsetti-1:::cpe-reach)	sw3400-farsetti-1		15:54:36	2011-03-21..
Soglia broadcast e multicast (sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:nucast-target-hc)	sw3400-farsetti-1	sw3400-farsetti-2 : gi0-2	15:55:01	2010-10-29..
Soglia broadcast e multicast (sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:nucast-target-hc)	sw3400-farsetti-1	farsetti-csa : gi3-4	15:53:56	2010-10-29..
Stato non blocking (sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:stpnotblocking)	sw3400-farsetti-1	sw3400-farsetti-2 : gi0-2	15:53:28	2010-10-29..
Stato non blocking (sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:stpnotblocking)	sw3400-farsetti-1	farsetti-csa : gi3-4	15:54:54	2010-12-05..
Transizioni di stato STP (sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:stptrans)	sw3400-farsetti-1	sw3400-farsetti-2 : gi0-2	15:53:09	2010-10-29..
Transizioni di stato STP (sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:stptrans)	sw3400-farsetti-1	farsetti-csa : gi3-4	15:51:18	2010-10-29..

Misure sw3400-farsetti-1

Unisci misure selezionate

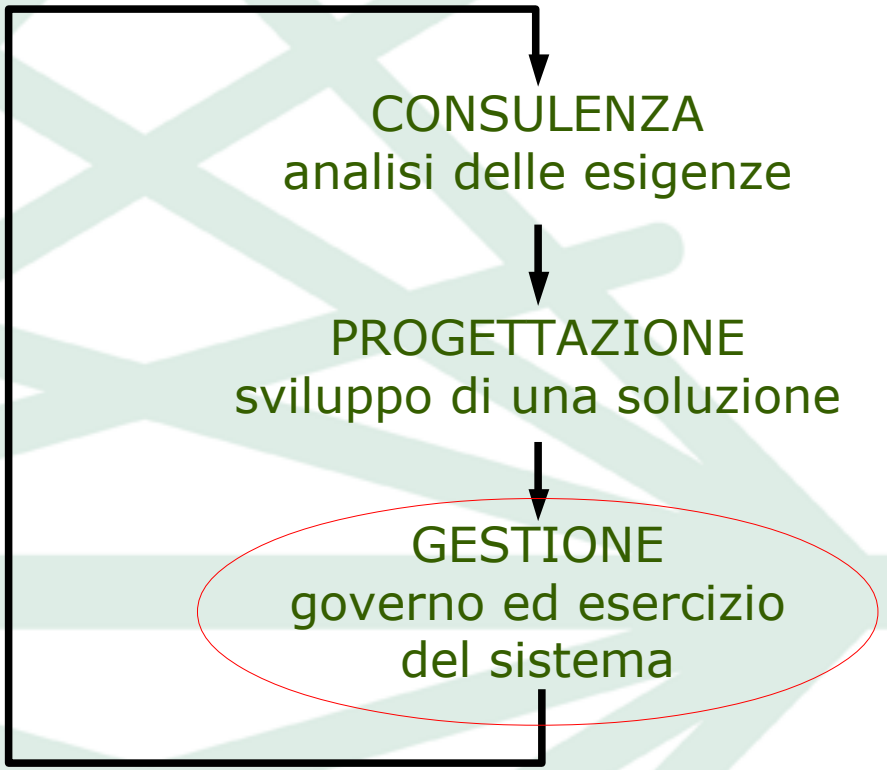
<< < 1 > >> (totale: 8) — 25 righe

Titolo	Path	Risorsa	Ultimo check
Traffico da sw3400-farsetti-1 gi0-2 verso sw3400-farsetti-2 gi0-2	sw3400-farsetti-1:gi0-2:vc-cpe-user-fwd:ifgraph-1G	sw3400-farsetti-1 gi0-2	15:54:00
Traffico da sw3400-farsetti-1 gi0-3 verso farsetti-csa gi3-4	sw3400-farsetti-1:gi0-3:vc-cpe-user-fwd:ifgraph-1G	sw3400-farsetti-1 gi0-3	15:53:59

Ultime 8 ore | Ultimo giorno | Ultima settimana | Ultimo mese | Ultimo anno | Tutti

LABORATORI GUGLIELMO MARCONI

Laboratori Marconi



LABORATORI GUGLIELMO MARCONI

Laboratori Marconi

Network/Security Operations Center (NOC/SOC)

LABORATORI GUGLIELMO MARCONI

NOC Laboratori Marconi

- L'attività del tecnico NOC/SOC comprende:
  - Configurazione apparati di rete e firewall, in ambiente multivendor
  - Troubleshooting su apparati di rete e firewall, in ambiente multivendor
  - Troubleshooting di sistemi comprendenti apparati, firewall, server, PC
  - Configurazione e troubleshooting servizi infrastrutturali, email, antivirus
  - Attività sistemistiche su server (Linux, Windows, Unix)
- Formazione sul campo
- Sessioni periodiche
  - Condivisione novità reti clienti
  - Condivisione esperienze
- Formazione

LABORATORI GUGLIELMO MARCONI

NOC Laboratori Marconi

- Network Operations Center, il luogo delle "Operations"
- Ruoli
  - front-end e back-office
  - presidio periodico e interventi on-site
- Personale
  - sistemisti con competenze di networking, gestione di server, sicurezza
  - minimo 3 anni di esperienza
  - formazione continua
  - conoscenza approfondita delle singole realtà

LABORATORI GUGLIELMO MARCONI

NOC Laboratori Marconi

- Modalità di supporto
  - supporto di primo livello
  - supporto di secondo livello / escalation
  - flessibilità nella ripartizione delle competenze
  - completa condivisione dell'informazione e trasparenza verso il cliente
- SLA
  - reperibilità 24x7, con allerta automatica tramite SMS
  - intervento remoto (> 90% dei casi)
  - intervento on site entro 2 ore

LABORATORI GUGLIELMO MARCONI

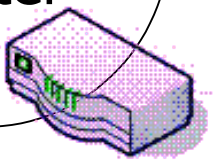
NOC Laboratori Marconi

- Strumenti utilizzati
  - monitoraggio
  - trouble ticketing
  - documentazione
  - checklist
- Reti eterogenee
  - reti multivendor
  - reti multi-tecnologia (fibra, wireless, ecc.)

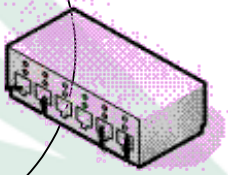
NOC Laboratori Marconi - dimensioni

140.000
postazioni
di lavoro

1.800
router

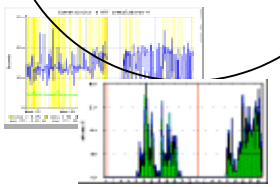


3.200
switch



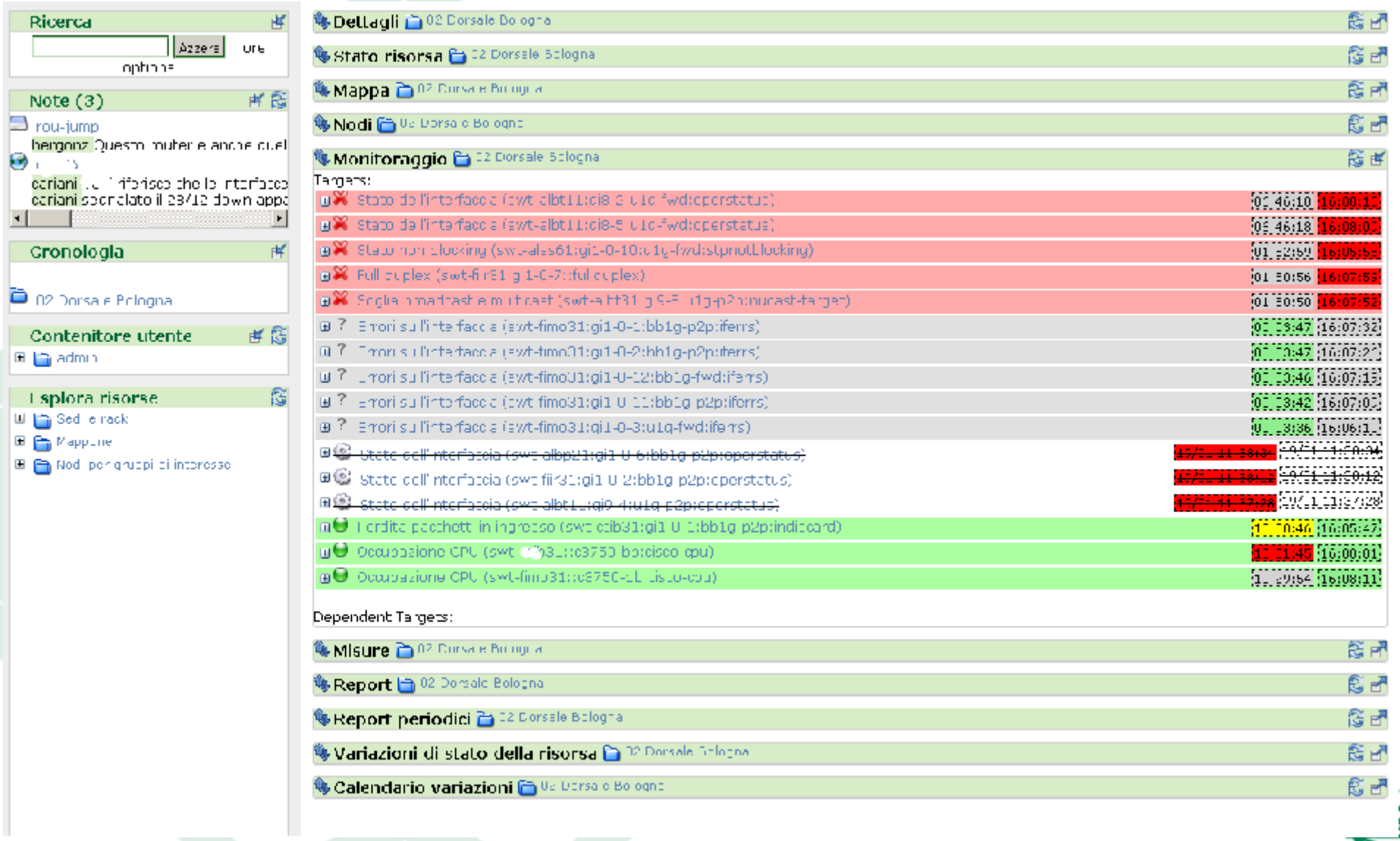
120
firewall

45.000
condizioni
monitorate

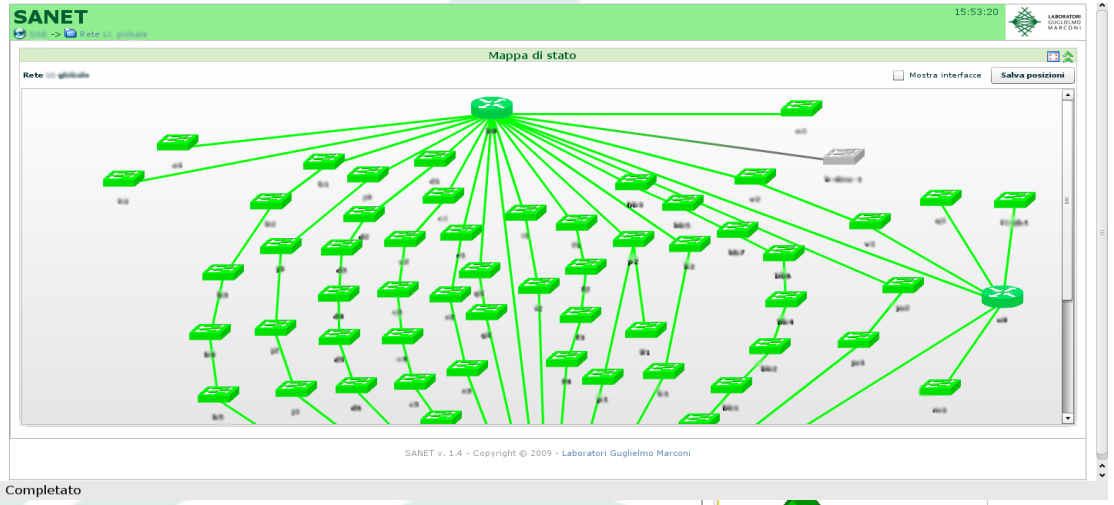


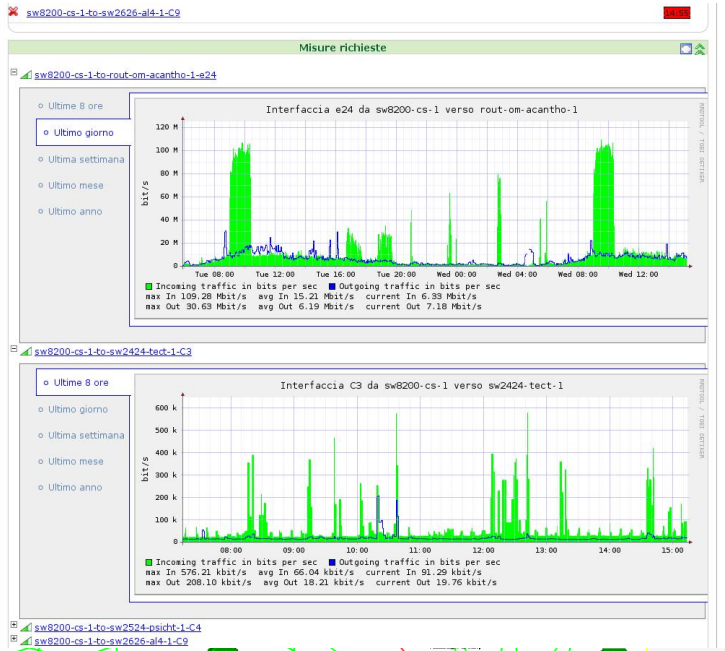
LABORATORI
GUGLIELMO
MARCONI

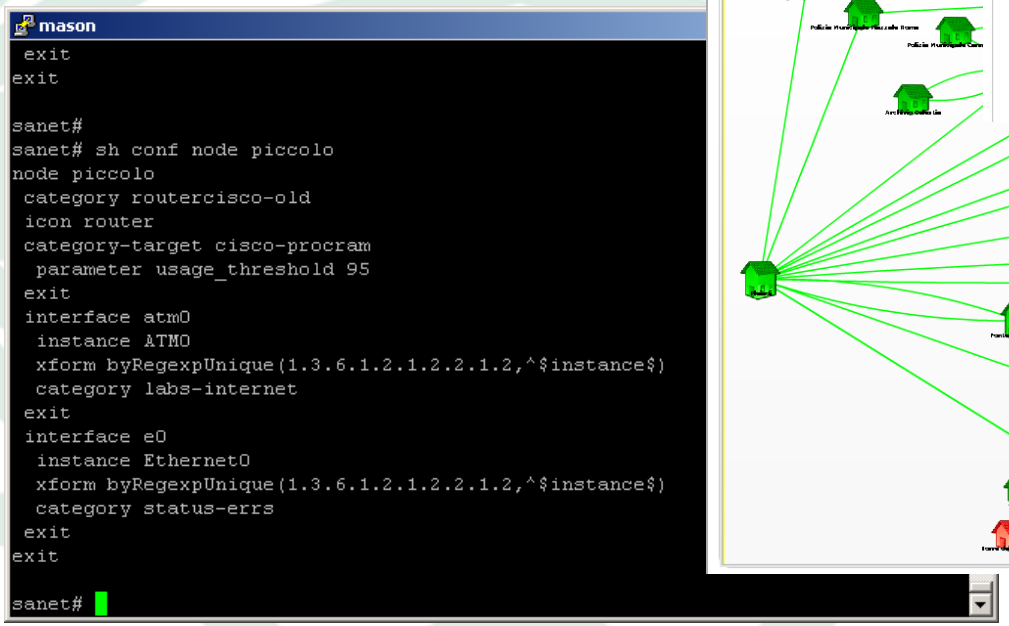
NOC Laboratori Marconi
SANET (monitoraggio)

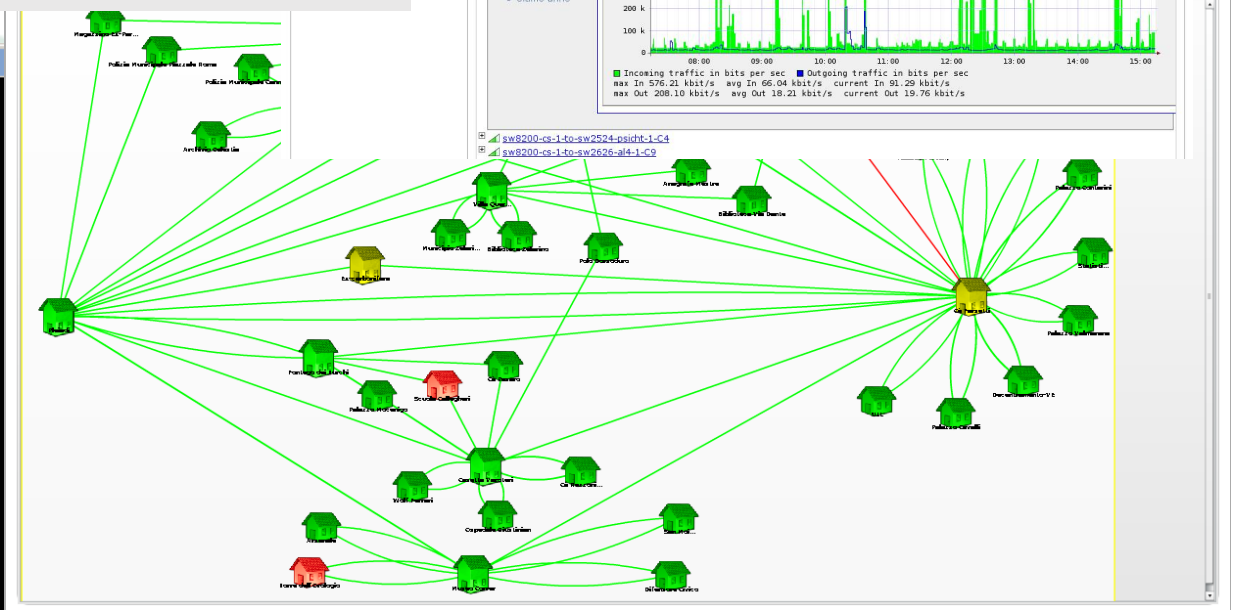


NOC Laboratori Marconi
SANET (monitoraggio)



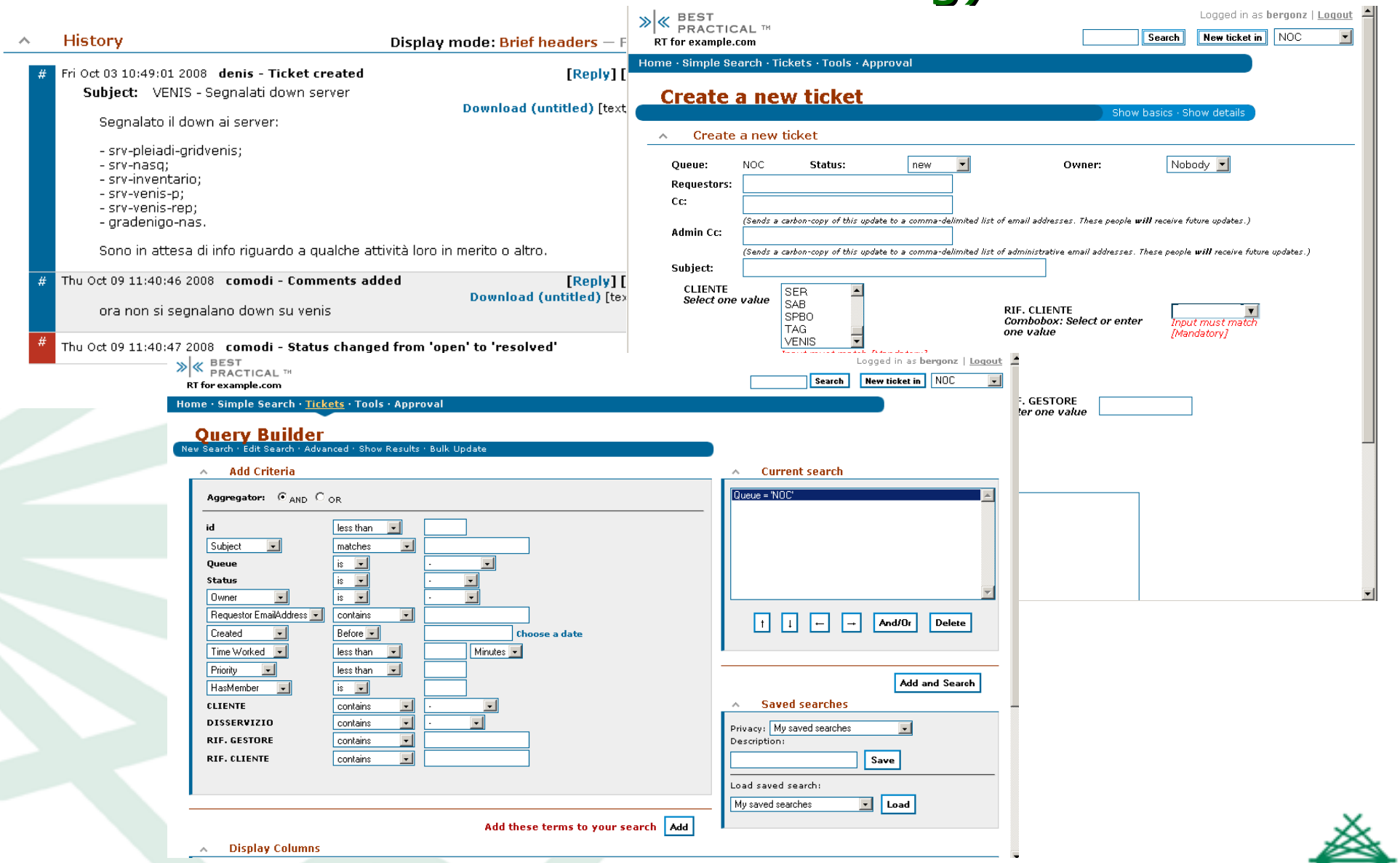






LABORATORI GUGLIELMO MARCONI

NOC Laboratori Marconi
RT (trouble ticketing)



NOC Laboratori Marconi
Mediawiki (documentazione)

- Per noi è fondamentale
- **Condivisa** con il cliente e modificabile
- Assicura teamwork
- Assicura un buon servizio
- Richiede impegno e controllo
- Difficile dare organizzazione, ma ci proviamo

Per l'accesso da remoto utilizziamo una vpn ipsec attestata su phink0 (lato LABS) e su pix-venis (194.243.104.186).

Gli host raggiungibili dalla rete LABS sono NETVEN1 (172.22.10.22) e NETVEN2 (172.22.10.231).

Wireless [modifica]

Come substrato per permettere connettivita' tra gli apparati wireless viene utilizzata la tecnologia **pseudowire**.

Nelle In reti informatiche e delle telecomunicazioni, un Pseudowire (o pseudo-wire) e' un emulazione di uno strato di un servizio point-to-point a livello 2 sviluppato a monte di una rete a commutazione di pacchetto (PSN).

Grazie a questa implementazione e' possibile mettere in comuncazione gli switch periferici sui quali sono attestati gli Access Point Wireless Tropos con lo switch core al quale e' connesso il Controller.

Essendo una rete L2 point-to-point la configurazione dev'essere implementata sulle interfacce interessate in entrambi i nodi. Nello specifico, questa configurazione mette in comuncazione pleaidi-pe01 e slorenzo-pe01.

```
pleiadi-pe01# sh run int GigabitEthernet1/17
interface GigabitEthernet1/17
 description pseudowire tropos slorenzo-pe01 gi1/24
 mtu 1504
 no ip address
 storm-control broadcast level 1.00
 storm-control multicast level 1.00
 xconnect 172.27.0.9 1 encapsulation mpls
!
```

```
slorenzo-pe01# sh run int GigabitEthernet1/17
interface GigabitEthernet1/24
 description pseudowire tropos pleiadi-pe01 gi1/17
 mtu 1504
 no ip address
 ip flow ingress
```


LABORATORI GUGLIELMO MARCONI

NOC Laboratori Marconi
Competenze e formazione

We push the buttons and pull the levers until things appear to work, which is a poor substitute for actually understanding what we are doing.

--Wayne Conrad

- Dobbiamo svolgere professionalmente un lavoro complicato, con una solida base di conoscenza
- Prodotti, che usano e implementano tecnologie
  - Da quale lato arrivarci, prodotti o tecnologie?
- Per noi è importante capire PRIMA le tecnologie, POI i prodotti.
  - Conoscere gli standard ed i protocolli di comunicazione
  - Conoscerli nei loro dettagli, nei loro difetti, nelle "manopole" e nei "bottoni" che offrono: **capirli**
  - Quindi vedere come sono implementati nei vari prodotti.
  - Nel settore spesso l'approccio è quello inverso

NOC Laboratori Marconi
Competenze di riferimento richieste

Networking in area locale (modello OSI 1-4, reti ethernet, protocollo spanning tree [802.1d], RSTP [802.1w], MSTP, VLAN [802.1q], tecniche di aggregazione [LACP 802.3ad])

Networking in area geografica [CDN, reti L2 frame relay/ATM/ADSL, accessi SDH 34 e 155 Mbit/s, reti MPLS (dal punto di vista dell'utente)]

WiFi: 802.11a/b/g/h/n, sicurezza [WEP, WPA, PEAP, LEAP, EAP-FAST, EAP-TLS, con associate problematiche sui server RADIUS di backend], tecniche di visibilità [SSID, MSSID]

Protocollo TCP/IP [pacchetti, indirizzi, netmask], metodi di incapsulamento [ethernet, 802.2, SNAP, VCMUX, PPP, HDLC, etc.], protocolli di routing [OSPF, BGP], protocolli di ridondanza del next hop [HSRP, VRRP], meccanismi di windowing, protocolli applicativi [telnet, FTP (attivo e passivo), POP, SMTP, IMAP, DNS, BOOTP e DHCP, NetBIOS su IP, HTTP, SSH, NTP], protocollo IPsec

Sicurezza negli apparati di rete e configurazione sicura, sicurezza nei sistemi operativi e loro vulnerabilità, vulnerabilità applicative, tecniche ed algoritmi di crittografia, simmetrica ed asimmetrica, tecniche di impronta (hash), tecniche e framework di autenticazione, protocollo RADIUS per l'autenticazione, autorizzazione ed accounting relativamente all'accesso alle risorse, tecniche per la selezione ed il filtraggio del traffico in ambiente multivendor [access list sui router (stateless), policy dei firewall (stateful)]

Informatica: sistemi operativi delle famiglie Unix e Microsoft, interfacciamento con la rete, tecniche di troubleshooting per il file sharing tramite protocollo SMB (dischi di rete), domini Windows, AD, group policy, servizi DNS, DHCP e IAS, troubleshooting dei server, programmazione in linguaggio C e Python

LABORATORI GUGLIELMO MARCONI

NOC Laboratori Marconi
Competenze e formazione

- Solida formazione di base, scolastica ed accademica
- Formazione "frontale" continua, settimanale
  - Si ruota tra gli argomenti di interesse
- Condivisione delle novità tecnologiche e delle evoluzioni dei clienti
- Discussioni e consultazioni che coinvolgono tutto il team di lavoro

LABORATORI GUGLIELMO MARCONI

Monitoraggio e gestione delle reti IP

- Riassunto:
  - Le reti sono fatte di tanti pezzi
  - Spesso diversi
  - Simili a dei computer, ma non proprio
  - Proprietari e talvolta poco instrumentati
  - Sparsi per il mondo
  - Non è la stessa cosa di una server farm
- Domande e risposte
- Saluti