Operating and Managing GMPLS Multi-Domain Networks

IPOP 2006 - Tokyo, June 2006

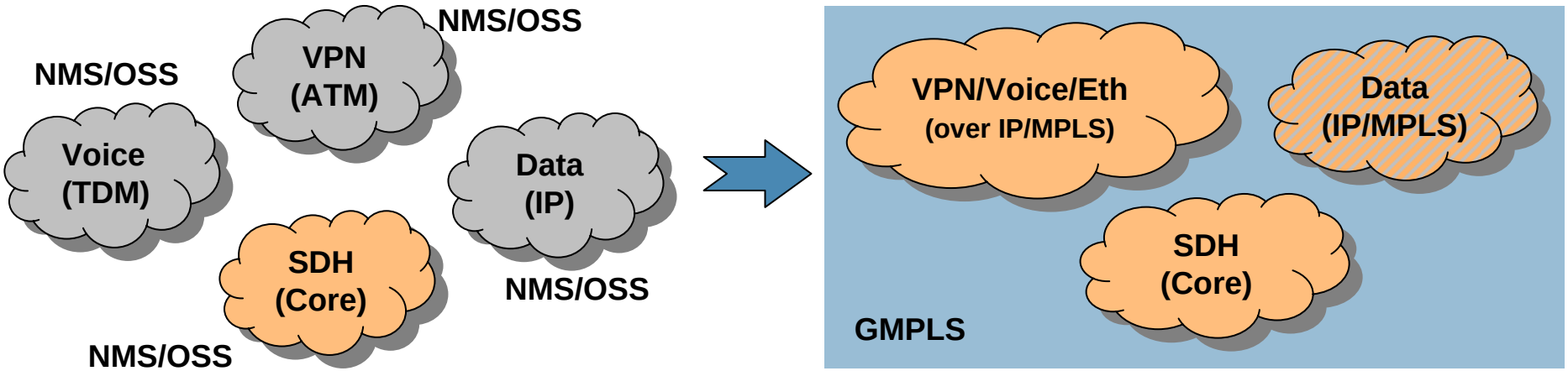
Jan Van Bogaert & Dimitri Papadimitriou
Alcatel Bell
{jan.van_bogaert,dimitri.papadimitrou}@alcatel.be

ALCATEL

Outline

- Multi-domain context
- Network and Service OAM
- Requirements
- Mechanisms and Tools
- Applicability
- Conclusion

The Big Picture



- GMPLS Objectives: increase operational efficiency
  - automating maintenance and control operations using a standard control plane ⇒ OAM
  - unifying maintenance and control operations for different networks (MPLS, SDH, carrier-grade Ethernet, etc.) and service they deliver using a unified control plane ⇒ multi-domain

GMPLS means « Traffic Engineering »

- GMPLS = unification of TE objectives, principles and mechanisms to any switched technology
- TE = adapt traffic routing to network conditions with joint traffic and resource-oriented performance objectives
  - effectively control usage of available network resources (put traffic where unused capacity is)
    - efficiently re-/direct selected traffic flows from IGP shortest path onto an alternative path
    - rapidly redistribute traffic in response to changes in network topology
  - performance objectives (provisioning and recovery)
    - resource-oriented
    - traffic-oriented: packet loss, delay (and variation)
  - approaches
    - proactive (longer-term): anticipating traffic changes
    - reactive/adaptive (shorter-term): responsive to traffic changes

Multi-domain networks and Implications

- Domain ⇒ controlled by a single administrative authority
  - Routing domain → build LSDB/TED
    - group of LSRs that enforces a common routing and forwarding policy
    - boundaries: inter-area, inter-AS (same or different) SP
  - TE domain → compute path (CSPF)
    - group of LSRs that enforces a common TE policy
    - full visibility: end-to-end strict path computation
    - partial visibility: per local domain strict path computation (at boundary); path may be complemented with loose hops or abstract nodes
  - Signaling domain → end-to-end LSP provisioning/re-routing
    - group of LSRs that enforces a common signalling policy
      - contiguous LSP: end-to-end LSP with head-end control
      - stitching (segmented LSP): end-to-end LSP with per-domain control
      - nesting (FA LSP): end-to-end LSP nested into nesting LSP

Multi-domain networks and Implications

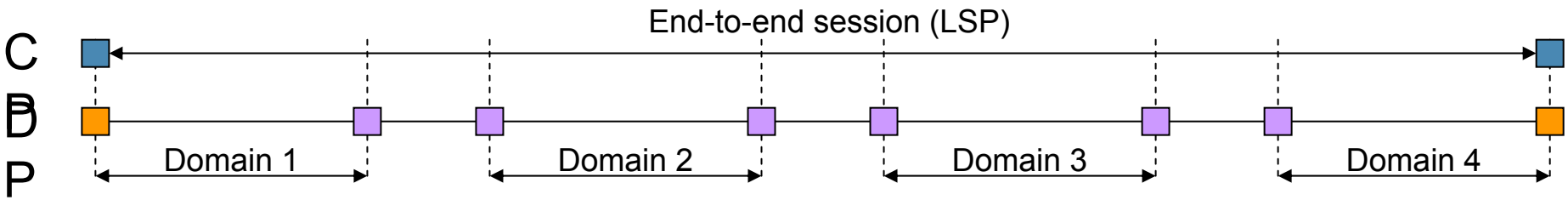
- Network partitioning into domains
  - Administration
  - Topological
  - Scaling
  - Security
- Implications
  - Confidentiality
  - Policy
    - Routing and forwarding
    - Policy-based admission control
    - Differentiated-service Traffic engineering
    - Signaling (filtering, rate limitation, etc.)
  - Scaling (partitioning into separate routing domains)
    - Single area TE information (limited visibility)
    - Multi-domain reachability information
    - … not even multi-domain TE reachability

Packet vs non-packet LSP

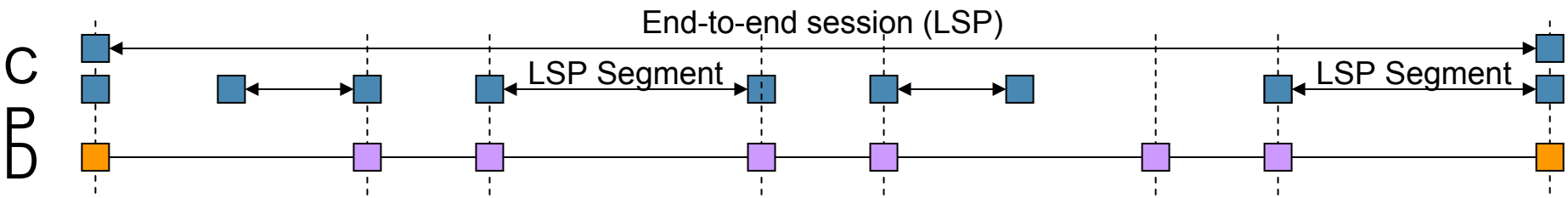
	Packet TE LSP	Non-packet LSP
Directionality	Usually unidirectional	Bi-directional
Provisioning	Intrinsic (RSVP-TE)	GMPLS RSVP-TE
Label	Shim header Frame/Cell header	Logical resource identifier (CP)
Hierarchy	Variable number of label stack entries	Fixed (multiplexing structure)
Connections	P2P, P2MP	P2P, P2MP
Connectivity	P2P, P2MP, MP2P, MP	P2P, P2MP (MP2P, MP)
Load balancing	ECMP, OMP	No (in order delivery)
PHP	Yes	No
OAM	BFD, MPLS Ping	Technology dependent

Multi-domain LSP Signaling

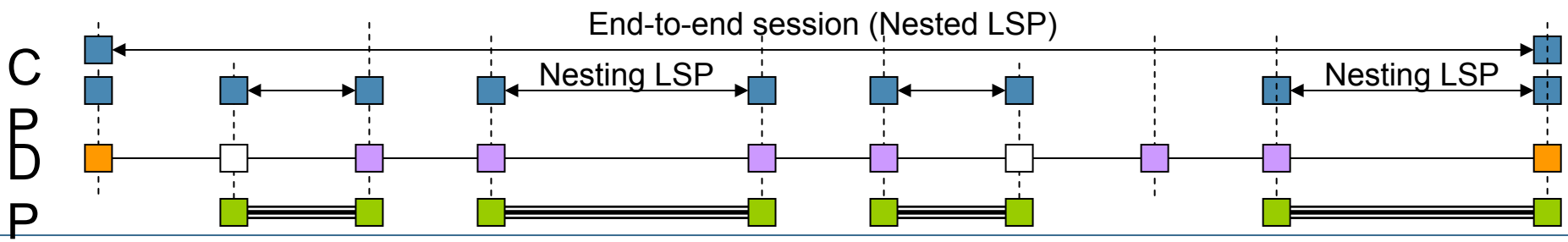
> Contiguous LSP: end-to-end LSP with head-end control



> Segmented LSP: end-to-end LSP with per-domain control



> Hierarchical LSP (FA)



Multi-domain LSP Signaling

Approach 1

- Single contiguous end-to-end TE LSP spanning multiple domains
  - More control at head-end LSR of inter-domain TE LSP

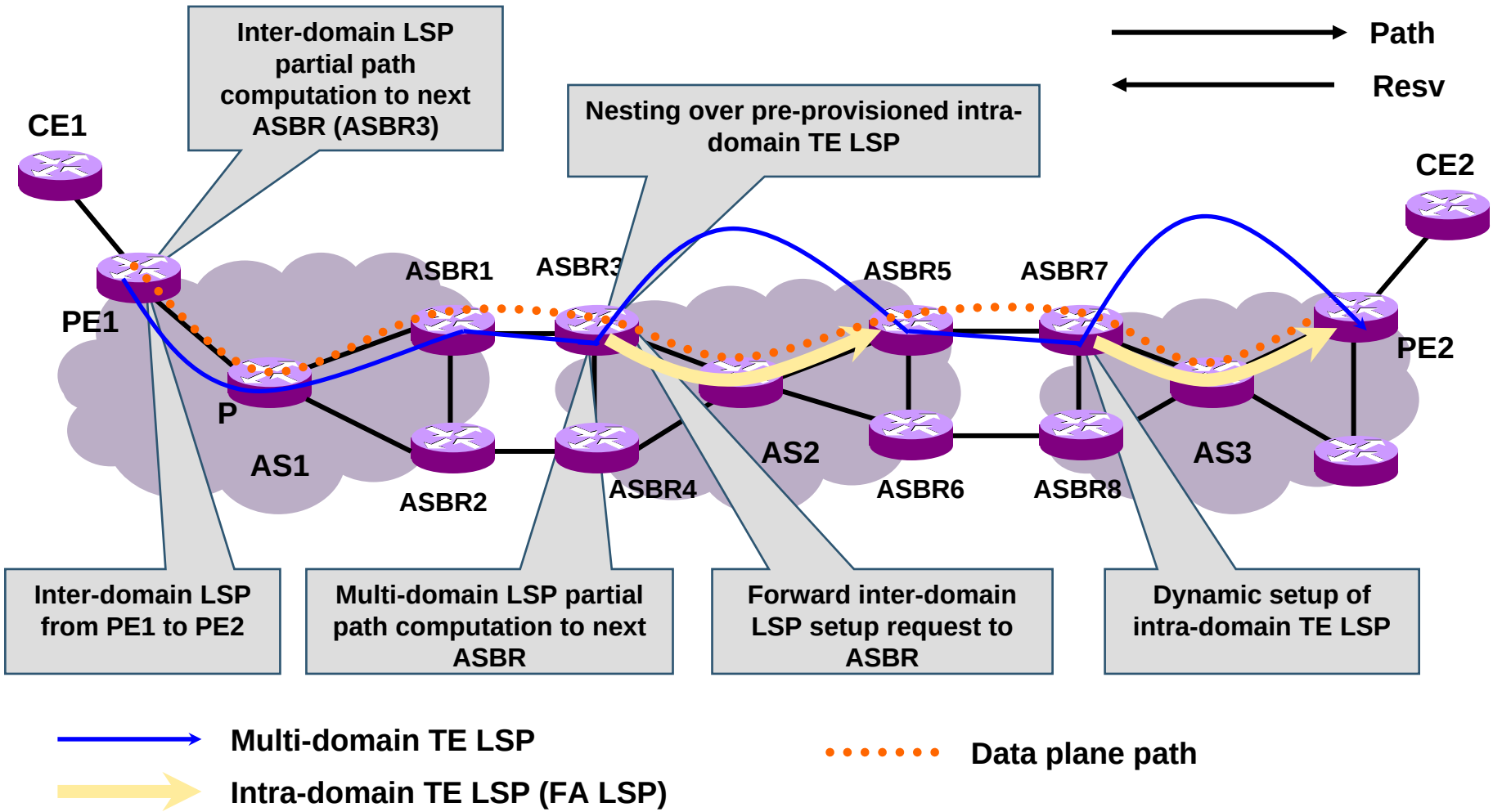
Approach 2

- End-to-end TE LSP spanning multiple domains
  - In each domain, end-to-end LSP may be nested
- Terminology
  - FA-LSP: nesting, N:1

Approach 3

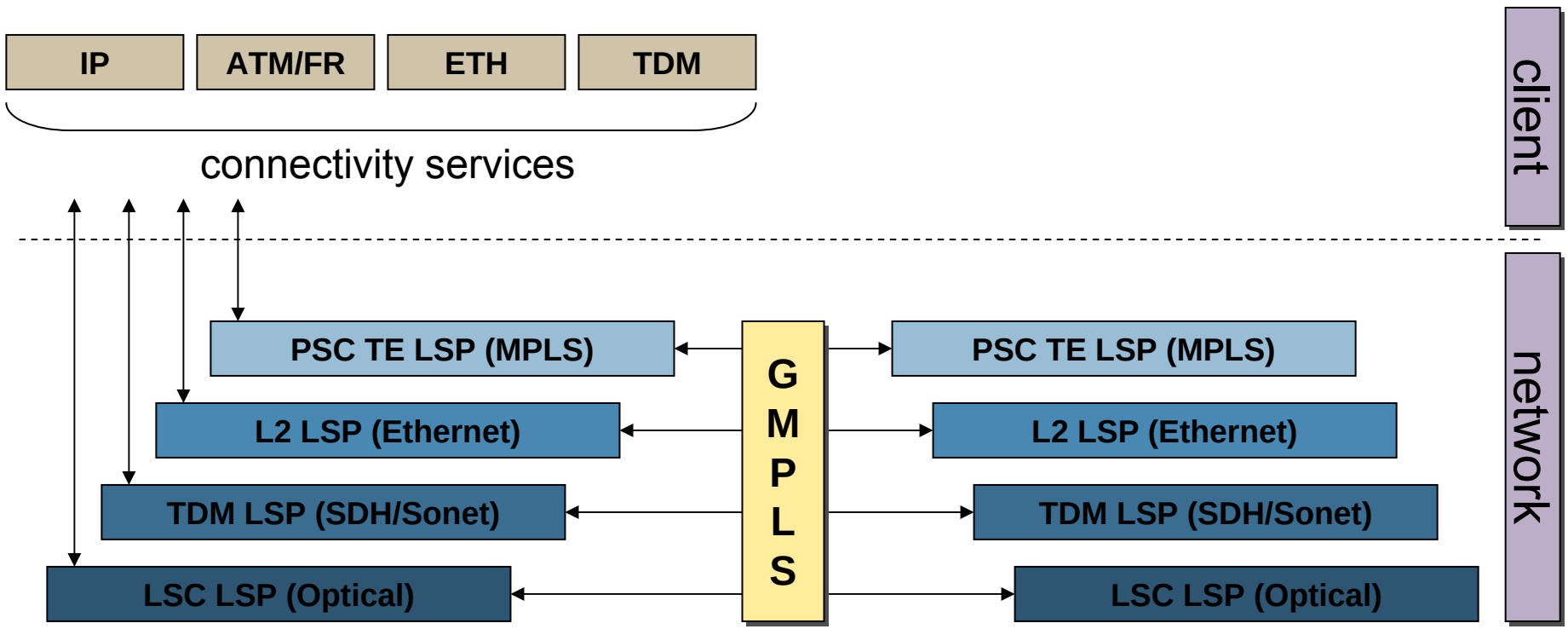
- Multi-domain TE LSP comprising multiple LSP segments
  - That may be *stitched* in each domain to a *different* local TE LSP in that domain
  - Per-domain control
- Terminology
  - LSP segment: stitching, 1:1

Example



Two dimensional problem space

- Network management (Network-to-Network) OAM
- Service management (Client-to-network) OAM



OAM → FCAPS

- *Fault* management: LSP/link fault
  - detection/isolation
  - notification/(alarm) suppression
  - correction (re-routing, protection switching)
  - location, correlation and diagnosis
- *Configuration* management
  - LSP/link provisioning operation monitoring and verification (LSP/link status pro-active monitoring)
  - Network element/system configuration monitoring and verification
- *Accounting* management (RFC 2975)
  - Accounting: collect resource consumption/utilisation data
  - Objectives:
    - Trend analysis and capacity planning
    - Billing/charging
    - Auditing

OAM → FCAPS

- *Performance* management
  - Performance metrics and alert conditions (thresholds)
  - Performance data collection
    - measurement: loss, delay, jitter, etc.
    - statistics/counters: MIBs
  - Performance data processing wrt metrics
    - Resource-oriented objectives
    - Traffic-oriented objectives
- *Security* management
  - Data plane mis-connection/leaks from/to sensitive resource areas
  - Control and monitor access to network elements/resources
  - Prevent accessibility to sensible information without AAA

Operational Concerns in GMPLS operations

- Effectiveness and performance of conducted provisioning/re-routing operations
  - resource selection and allocation, mis-connection, etc.
- Troubleshooting (verification/diagnosis) in case of data plane performance degradation
- Coordination and synchronization between (data plane) resource status/ usage and control plane “view”
  - Key for effective unified traffic-engineering
- Ensure efficient OAM operations in multi-domain / multi-service environment
- Unify (and simplify) maintenance and control operations in multi-layer networks

Inter-domain Interface requirements

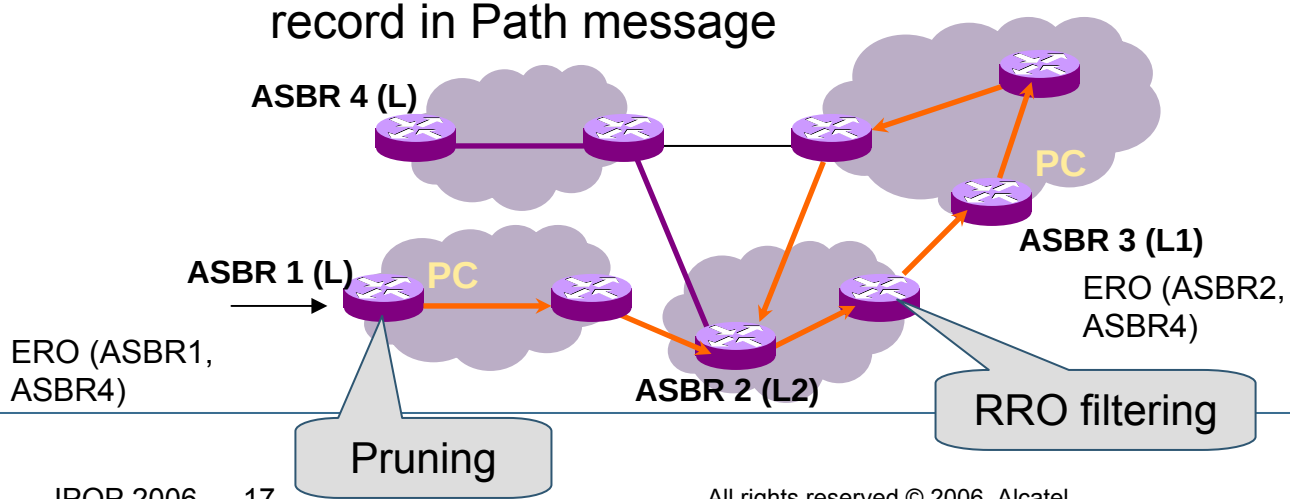
- OAM functions: part of requirement set for establishing GMPLS inter-connects
  - Fault management
    - Connectivity verification
    - Alarms communication and handling
    - Loopback tests
    - Fault diagnosis (e.g. traceroute)
  - Performance management
    - Performance measurement
- Inter-domain boundary specifics
  - Confidentiality: control what is returned in traceroute, route record, etc.
  - Policy: filter/modify control plane error/alarm propagation
  - Scaling: block performance OAM packets

Multi-domain Fault Management

- Some elements may be intentionally confined within a domain
- Fault management tools (MPLS data plane)
  - ensure capability support by intermediate end-points
  - connectivity check/verification: BFD-MPLS, LSP Ping
  - alarms handling
  - loopback tests: BFD-MPLS (echo), LSP Ping
  - fault location/diagnosis: LSP Traceroute (= incremental connectivity check)
- Fault and configuration management tools (control plane)
  - administration: *admin_status* (notify/path/resv message)
  - alarm handling: *alarm_spec*
  - fault notification: error_spec in notify/error message
  - fault location/diagnosis: error_spec, *route recording* (label)
  - path verification

Multi-domain Route Recording

- Signaling mechanism providing for diagnostic information about the path of an established LSP
- Route record processing at inter-domain boundaries
  - boundary node may remove, filter or aggregate some of the recorded information for trust/confidentiality/policy reasons
    - route record may not be available on a Path message
  - in case of per domain boundaries path computation
    - computed path may loop back
    - loop avoidance: pruning during path computation using the route record in Path message



Alarm communication and handling

- Communicate alarm information on a per LSP basis in both upstream and downstream direction

  ⇒ information available at every node along the LSP for display, diagnostic, monitoring and re-routing purposes

- Data plane problems typically filtered based on elapsed time and local policy

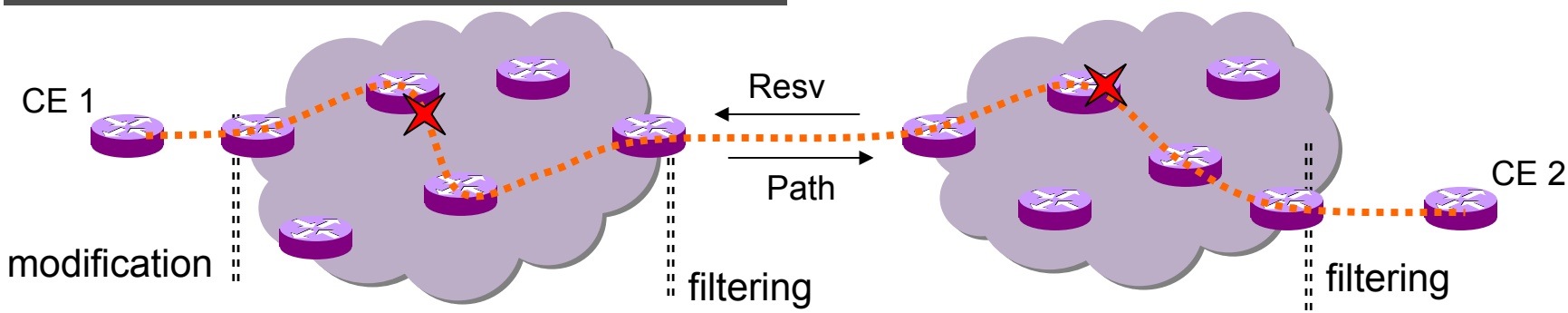
```
- Node 172.16.25.6, IP Interface 1.1.3.2
  Severity: Major, Error: LOL
  Time: 21:11:09 - Date: JAN 01 2006
- Node 172.16.25.12, IP Interface 1.1.2.1
  Severity: Critical, Error: LOS
  Time: 20:52:15 - Data: JAN 01 2006
```

cess normally raised as alarms

ms cause the LSP to be re-routed

us and communicate relevant alarm

ne status is under complete failure



Why a new object ?

- Error information reported in Error/Notify messages but indicate problem in signaling state and only report one problem at a time

  $\Rightarrow$ correlation of problems associated with a single LSP becomes complex + requires to examine LSP status by listing all problems

- Alarm communication via
  - new *alarm_spec* object
  - new error/alarm information TLVs
  - new Administrative Status bit (to inhibit alarm communication)

  To
  - operator/software component to obtain a list of current alarms associated with the resources supporting an LSP
  - ensure that this list is kept up-to-date and synchronized with the actual network alarm status
  - make this list available at every node traversed by an LSP

Alarm_Spec definition

- Alarm_spec object use same format as error_spec object
  - new Error Code value assigned to support "Alarms”
  - Error Values from Alarm MIB [RFC 3877]
- Alarm_spec TLVs

TLV Type	Length	Short Description
REFERENCE_COUNT	8	The number of times this alarm has been repeated.
IMPACT-SEVERITY	8	Indicates the impact/severity of the indicated alarm
GLOBAL_TIMESTAMP	8	The number of seconds since 0000 UT on 1 January 1970, according to the clock on the node that originates the alarm(s).
LOCAL_TIMESTAMP	8	Number of seconds reported by the local system clock at the time the associated alarm was detected on the node that originates the alarm(s).
ERROR_STRING	variable	A string of characters, representing the type of error/alarm. Multiple strings may be included.

- Impact-Severity TLV:
  - Impact: unspecified, non-/service affecting
  - Severity: critical, major, minor, warning, undetermined

Alarm Processing at Boundaries

- Client-to-network interface:
  - Ingress/egress edge-node can
    - ***filter*** alarms to protect network information, or to indicate that the network is performing or has completed recovery actions for the LSP
    - ***modify*** alarms sent to client to facilitate understanding of the failure impact and take corrective actions in a more-appropriate manner
  - Egress edge-node can decide to not request alarm reporting
- Network-to-network interface:
  - Ingress/egress edge-node can
    - ***filter*** alarms to protect network information, or to indicate that the network is performing or has completed recovery actions for this LSP
    - ***modify*** alarms to facilitate peer egress/ingress-node understanding of failure impact, and take corrective actions in a more-appropriate manner or prolong generated alarms upstream/ downstream as appropriated
  - Egress/ingress edge node can decide to not request alarm reporting

Admin Status

- Per LSP administrative status information carried in admin_status object
- Main usage
  - when carried in the Path/Resv message: indicate the administrative state of a particular LSP
    - A bit: actions corresponding to admin state down must be taken
    - T bit: LSP in "testing" mode
    - D bit: LSP deletion in progress
    - I bit: inhibit alarm communication
  - when carried in a Notify message: request that the ingress node change the administrative state of a particular LSP
    - the administrative status info acts as a request to the ingress node to set an LSP's administrative state
    - Ingress node acts on the request

Conclusion

- GMPLS provides for a set of tools that
  - unifies administration, and maintenance network operations
  - suites for both single and multi-domain networks
- Fault management tools provides for
  - fault notification
  - fault location/diagnosis
  - path verification
  - admin status communication
  - alarm communication and processing
    - part of GMPLS set of tools for controlling the health of a network (in particular, data paths)
    - simplifies the operator tasks in correlating data plane alarms (list kept up-to-date and synchronized with the real alarm status in the network)

References

- RFC 2975, *Introduction to Accounting Management*, October 2000.
- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*, January 2003.
- RFC 3877, *Alarm Management Information Base (MIB*), September 2004.
- RFC 3945, *Generalized Multi-Protocol Label Switching (GMPLS) Architecture*, October 2004.
- RFC 4204, *Link Management Protocol (LMP*), October 2005.
- draft-ietf-ccamp-inter-domain-framework-04.txt, *A Framework for Inter-Domain MPLS Traffic Engineering*, July 2005.
- draft-ietf-ccamp-inter-domain-rsvp-te-03.txt, *Inter domain GMPLS Traffic Engineering - RSVP-TE extensions*, March 2006.
- draft-ietf-ccamp-lsp-stitching-03.txt, *Label Switched Path Stitching with Generalized MPLS Traffic Engineering*, March 2006.
- draft-ietf-ccamp-gmpls-alarm-spec-03.txt, *GMPLS - Communication of Alarm Information*, September 2005.
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*, January 2006.
- draft-ietf-bfd-mpls-02.txt, *BFD for MPLS LSPs*, July 2005.
- draft-ietf-bfd-base-04.txt, *Bidirectional Forwarding Detection*, October 2005.

www.alcatel.com