Packet Design

Service Providers Tap Into Layer 3 To Improve MPLS-VPN Services

Alex Henthorn-Iwane
Sr. Director Product Marketing
Packet Design Inc
alex@packetdesign.com

George Wu
Manager, MPLS Backbone Engineering
T-Systems Inc.
George.Wu@t-systems.com

Discover, Resolve and Prevent the Hardest Problems in IP Networks

Packet Design

Packet Design, Inc.

"Harnessing the Intelligence of IP"

- Three years old, founded by Judy Estrin and Van Jacobson
- Pioneer and leader in Route Analytics for IP networks
- OEM supplier to hp/OpenView
- Cisco Technology Developer Partner
- Team of 40 with strong IP heritage based in Palo Alto, CA
- More than 100 production deployments worldwide

eWEEK

Network Magazine PRODUCT OF THE YEAR 2003

ENTERPRISE MANAGEMENT ASSOCIATES IMPACT BRIEF

HP's Strategic Partnership with Packet Design Signals a Landmark in Network Troubleshooting

Cisco Systems Technology Developer Partner

hp invent

Packet Design

The State of MPLS VPN Management

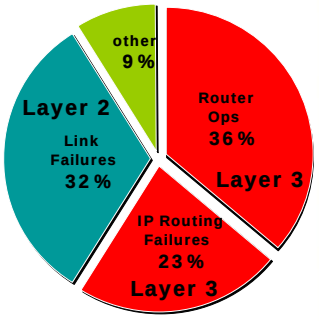
- Most management solutions focused on device and interface configuration and troubleshooting
- SNMP polling is still a primary mechanism
- Device failures are relatively infrequent
- MPLS-enabled networks typically have very robust redundancy
- The virtualized, routing-based nature of Layer 3 MPLS VPN services creates a high degree of service assurance complexity and problems

Packet Design

MPLS VPNs: Challenges Due to Complex, Virtualized Routing

- Design and human error can cause problems during:
  - New service provisioning
  - Changes to customer's service
  - Changes to other services
    - Competing configurations with other services (Internet access)
  - Routine router maintenance or upgrades
  - Due to vendor "soft" failures or bugs

Causes of Downtime in IP Networks



Sources: University of Michigan, Sprint

Packet Design

Provider's Concerns

- Customers can leak extra routes and consume precious resources
  - Full Internet routes could be leaked
    - can take down some provider routers
  - Prefix limits on sessions are difficult to apply globally
    - large per customer variation: 5 - 50,000 routes
    - plus need room for growth
- A routing instability in a customer site can spread to provider's BGP
- Provider needs to monitor the customer's routes and routing activity

Packet Design

Customer's Concerns

- Provider can misconfigure
  - Route Distinguishers: used to distinguish customer routes
  - Route Targets: used to determine intra-VPN routing policy
  - Distributing one customer's routes to another
  - VPN becomes no longer “private”.
- Provider needs to monitor PEs, RDs and RTs associated with each customer and flag any deviation

Packet Design

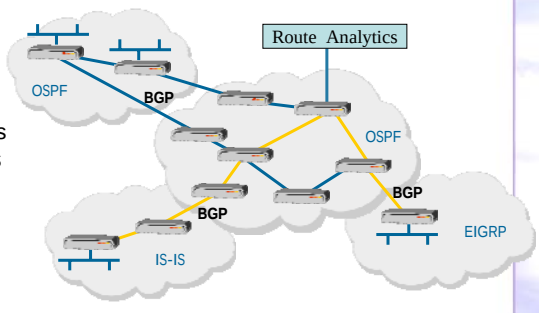
New Layer 3 MPLS VPN Management Metrics Needed

- Per-Customer VPN Reachability
  - "Are all the customer VPN, BGP, IGP (OSPF, IS-IS, EIGRP) routes functioning properly?"
- Per-Customer VPN Privacy
  - Fundamental selling point of MPLS VPNs
  - "Are all customer VPN Route Distinguishers properly configured?"
- Per-Customer VPN Policy
  - "Is the customer's desired routing architecture (Full-mesh, hub and spoke, partial mesh, etc.) working?"

Packet Design

Route Analytics Technology

- Listens passively to routing updates
- Creates a real-time network map
  - As up to date as routers
- Analysis of current paths
  - Paths are computed using the same procedures as routers
- A historical view with breakdown of instability
  - Full routing event history/forensic audit trail
  - Flapping links, prefixes
  - Ability to look at state of routing at any point in recorded history



•Works across protocols (OSPF, IS-IS, BGP, EIGRP, RFC 2547bis)

Packet Design

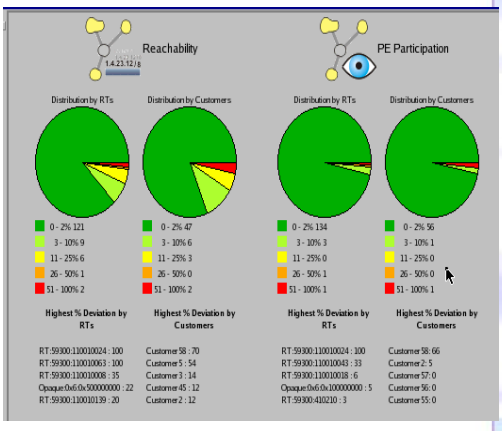
BGP/MPLS IP VPN Analytics

- *Per customer* view of
  - routes
  - BGP messages
  - PEs involved
  - RTs and RDs
- Simple tracking is not sufficient, we need to recognize deviations from a baseline behavior

Packet Design

Baselining Customer VPNs

- For each route, determine how long the route was available over the last week
- If the route was available 80% of the time or longer, then include the route in the baseline
- Similarly for PEs, RDs, RTs
  - i.e. if a PE is announcing at least one route for a customer for 80% of the week, then include that PE in the baseline for that customer



T-Systems

Packet Design

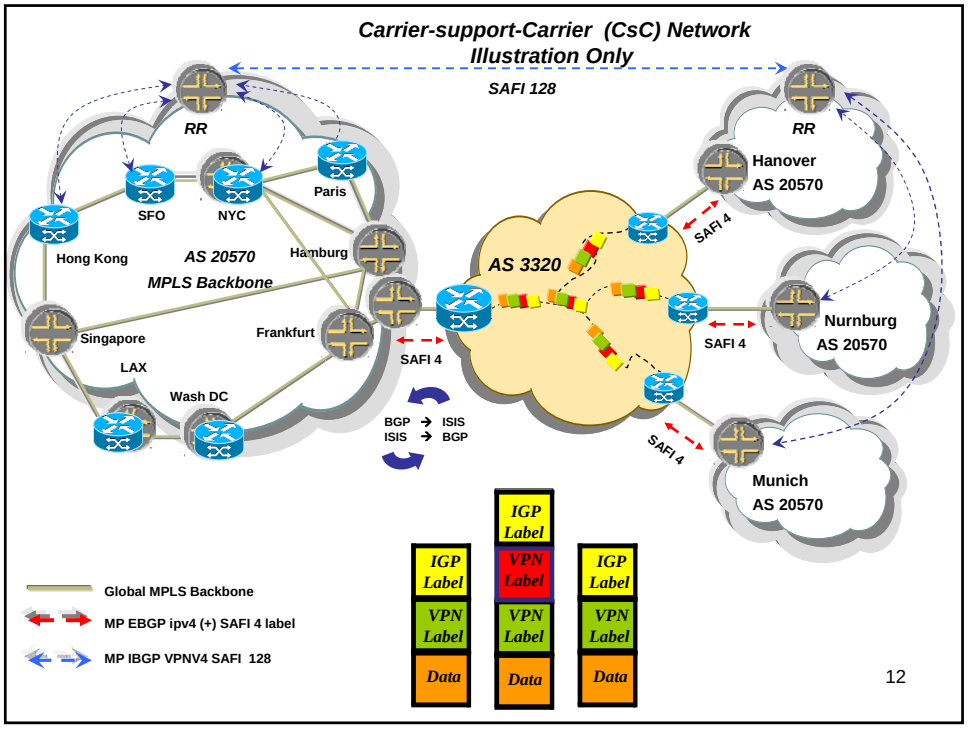
T-Systems

- Deutsch telecom: about 60 billion Euro yearly revenue and quarter millions employees world-wide
- Business divisions:
  - T-COM and T-Online: infrastructure, fixed/broadband network
  - T-Mobile: mobile business
  - T-Systems: communication and IT solutions for business customers
- IPLS backbone is T-Systems business network service platform
  - Offer L3 and L2 VPN services to business customers
  - Offer Internet access to business
  - Offer Value-added services to customers (firewall, VoIP, hosting services etc)
- IPLS is one of largest VPN service providers in Europe
  - POPs in Germany, Europe, North America, Asia, South America and Africa
  - Customers like DHL, Siemens, Daimler-Chrysler, Bosch etc

Packet Design

IPLS backbone

- International backbone with redundant connections
- 100% MPLS end to end connectivity
  - All traffic encapsulated in MPLS once entered into IPLS backbone
- End to end QoS policy with SLA guarantee
- L2/L3 VPN solution with dedicated Route Reflectors for control plane scalability
- Deploy large Carrier-support-Carrier (CsC) network



Packet Design

Route Analytics in T-Systems

- Evaluated and Deployed at T-Systems in Summer 2005
- Immediately became effective tool for engineering and operations
- Deployment scenarios
  - ISIS monitoring for backbone topology
  - BGP monitoring for CsC gateway activities
  - iBGP peering with Route Reflectors
  - BGP VPN explorer for L3-VPN and CsC monitoring and troubleshooting
- Worked closely with Packet Design team to make route analytics technology effective for MPLS L3-VPN management

Packet Design

Typical Usages of Route Analytics

- Backbone monitoring, routing and topology design
- Network key statistics and baseline reporting
- CsC network instability monitoring
- Customer VPN routing monitoring and analysis
- Customer VPN outage troubleshooting
- Primary/backup VPN routing redundancy monitoring

Packet Design

Backbone monitoring, routing and topology design

- Real-time visual display of backbone topology
- Visual display of network faults – link and router failure, maintenance activities
  - Before and after RIB comparison
- Zoom-in and pin-point exact event sequence for backbone outage
- What-if scenarios simulations for link-failure impact
- Routing design simulations for ISIS metric tuning

Packet Design

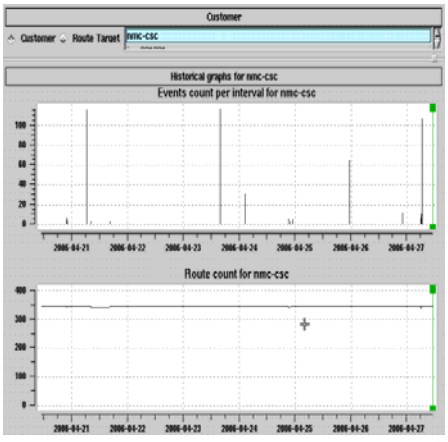
Network statistics and baseline reporting

- Full picture of whole network control plane
  - Network size, availability and instability, trending
- Offers XML API to interface with route analytics data
- Collect network statistics programmatically
  - Network size as router count, link count
  - VPN size as route-target count, total VPN route count
  - Per VPN customer route and routing stability
  - Whole network stability and availability analysis based on monthly backbone ISIS events
    - Least stable links, maintenance impact, overall network availability statistics
- Generate list of top PEs with most VPN routes
- Used as a key component of network statistics reporting

Packet Design

CsC Network Monitoring

- CsC is a challenge for network monitoring
  - No direct IGP adjacency
  - SAFI4 peering with upstream provider (T-COM)
- Employ VPN monitoring to visually display CsC network instability
  - Redistribute all CsC router loopback into special monitoring VPN
- Continue to work with Packet Design for a full solution, including full-mesh connectivity monitoring



Case Study 1 – Customer VPN troubleshooting

Packet Design

- Route-analytics offers real-time customer VPN route monitoring
  - Identify VPN route events and baseline deviation
- In one case, a customer reports outage of VPN sites
- Route analytics shows a injection of new default route into VPN around the outage time
- Default route from VPN suppress the default route origination from CPE router inside customer site
- The root cause of this outage is quickly identified and resolved
- Allows full playbacks of events to pin-point root-cause

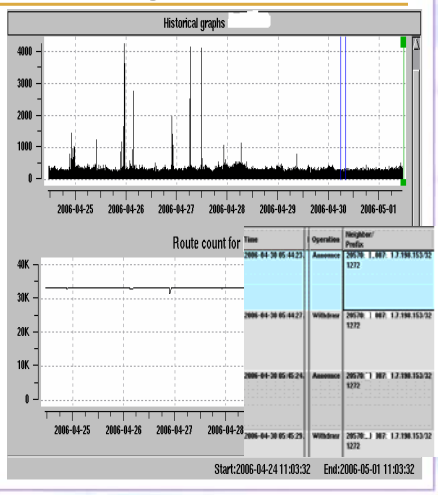
Case Study 2: Customer VPN instability monitoring

Packet Design

- Route analytics provide VPN route monitoring as well as pre-defined customer monitoring
- Use pre-defined customer list for important customers
- Defined alert and trigger for key customers instability events
  - PE participation deviation and route deviation threshold
- VPN routing loop will result in periodic BGP route announce/withdraw for extended time
- Dense background events always indicate route instability or routing loop
- Detailed analysis shows the exact source of instability
- Potential to use this as additional services for VPN customer or competitive edge

Case Study 2: Customer VPN instability monitoring

- Sustained background routing events indicate network flapping or routing loops
- Event graph should be clean with occasional event spikes
- A lot of background noise events always indicate customer VPN network instability
- The graph shows specific customer network with one /32 announcement and withdraw every minute



Case Study 3: Redundant VPN site analysis

- Some VPN customers subscribe to dual-connection design for full-redundancy solution
  - BGP community-based local-pref setting
  - Apply SoS ext-community for loop-prevention
- Audit control plane redundancy besides link redundancy to guarantee failure protection
  - Common mistakes include incorrect SoS, inconsistent BGP route announcement due to CPE mis-configurations
- But Route-reflector blocks back-up routes due to lower local-pref setting of backup routes
- We employs a unique RD per PE solution
  - Decrease route convergence time under failure
  - Provide 100% visibility of backup routes
  - Monitor and guarantee 100% redundancy on control-plane
- Daily report for BGP route redundancy for all redundant service customers

Packet Design

Conclusion

- VPN services are critical to business communications
- ISPs need tool and visibility into VPN to increase competitive edge, to improve customer satisfaction and to expedite troubleshooting
- ISPs need real-time view, historic playback as well as programmatic access to VPN baseline data
- Route-analytics provides a useful tool for ISP L3 VPN monitoring and analysis