

Routing & Traffic Analysis for Converged Networks

*Filling the Layer 3 Gap in
VoIP Management*



Packet Design

Executive Summary

Voice over Internet Protocol (VoIP) is transforming corporate and consumer communications today. Service providers have invested in VoIP for years and are starting to see a noticeable ramp in VoIP subscribers, while a significant percentage of enterprises have deployed VoIP in their networks. From the enterprise perspective, organizations are not so much asking *if they should* deploy VoIP, but rather *how to deploy*. Deployments are confirming the business drivers for VoIP—strategic convergence around IP networks for cost economies, and increased productivity based on the flexibility and feature-richness of IP telephony solutions. Yet, while VoIP as an IP application or service is maturing, organizations still face risks in large-scale VoIP deployments, notably due to the gaps in VoIP management best practices and solutions. This paper provides an overview of the state of VoIP deployment and management today, and the need for a comprehensive, multi-faceted VoIP management strategy. It examines why management of the underlying IP network, specifically Layer 3 management, is a critical, missing piece of most VoIP management portfolios. Lastly, the paper describes how integrated IP routing and traffic analysis using route analytics technology can fill this management gap and increase converged IP network reliability and predictability for VoIP deployments. By employing routing and traffic analysis solutions as part of a comprehensive VoIP management strategy, IT and network engineering departments can significantly mitigate risks to their VoIP user experience.

The State of VoIP Deployment and Management

VoIP continues to make significant deployment headway in both enterprise and service provider networks. According to a 2009 survey of global enterprises and service providers¹, 80% of survey participants stated that VoIP would become their primary telephony technology within two years, while 50% stated that VoIP would become primary within one year.

While the deployment of VoIP has risen, so has dissatisfaction with and an urgently felt need for better VoIP management within the network engineering and operations departments tasked with maintaining a positive VoIP user experience. Most notably, survey results show that there is a significant lack of capability to monitor VoIP bandwidth utilization and VoIP-impacting network quality metrics. As a result, while only 10% of those surveyed had yet to deploy third-party management tools to help with their VoIP deployments, 90% stated plans to do so.

This same survey indicated that some of the top management needs for network managers responsible for VoIP deployments are:

- Real-time visibility into performance-affecting issues
- Enhanced ability to see the “big picture” and optimize capacity and other resources

¹ IP Telephony Management, 2009 State of the Market Report, Webtorials Analyst Division

- Better and faster diagnostics to eliminate finger-pointing and unsolved problems

The Need for Comprehensive VoIP Management

VoIP is a complex communication application running over a standard IP network, and it places critical service requirements on the network in order to perform as expected. VoIP equipment, including phones, proxy servers, gateways, gatekeepers, and application servers exercise their own set of session control and other voice-specific functions, but the VoIP application is highly dependent on a predictable, reliable and stable IP network with low latency, jitter and packet loss characteristics. Given this dependency, it is clear that approaching a VoIP deployment without a comprehensive VoIP management strategy that includes network-level monitoring of the IP infrastructure results in a higher degree of risk to the end-user quality of experience.

To be effective, comprehensive VoIP management must have the following characteristics:

- **Multi-Layered:** Management must encompass all IP network infrastructure involved in delivering the VoIP service, including individual network device status, VoIP signaling and call quality monitoring, and visibility into the behavior of the underlying IP network layer, which is the foundation for the VoIP system and all other network services.
- **Continuous:** The VoIP network must be measured continuously, in real-time, and throughout the life cycle of the VoIP application, with accurate event history captured for effective forensic analysis.
- **Deterministic:** Many VoIP solutions provide information on call quality, whether by directly monitoring actual calls or by use of synthetic transactions, but equally important to highlighting sub-optimal performance is the ability to determine the root cause of any problem, enabling immediate corrective action to be taken, while preventing future recurrences.

It's the Network

While justifiable attention has been given to the specialized management requirements of VoIP, including performance monitoring of voice quality, call signaling and the individual VoIP components, by and large, the single biggest factor in quality and reliability of VoIP service is the underlying IP network. A survey conducted on over 300 IT professionals determined that the network was a factor in over 50% of all application degradations.²

IT managers widely recognize the value and need for traditional network management solutions, yet while SNMP-based systems do an admirable job of monitoring status and detecting failures of the individual network devices and interfaces, a significant management gap exists between this physical, Layer 2 oriented approach, and

² The 2009 Handbook of Application Delivery, Dr. Jim Metzler

management of the logical operation of the network at Layer 3. Lacking visibility and management of Layer 3 network issues is a critical liability in deploying and managing VoIP, because logical, Layer 3 problems are the root cause of a significant percentage of IP network problems that affect VoIP quality and reliability.

The Impact of Layer 3 Problems on VoIP Performance

The genius of the Internet Protocol lies in its distribution of intelligence throughout the network. Routers exchange reachability information with each other using various routing protocols. Based on this information, each router makes its own decision about how to forward individual packets to their destination. Should any link or node fail, the routers detect and propagate that status throughout the network, automatically redirecting traffic to alternate paths around the failed element. The separation of this dynamic router-to-router coordination, or the routing control plane, from the forwarding path that actually transports the data, enables IP networks to be highly resilient while efficiently scaling in a very economical manner

The downside of IP is that its behavior is unpredictable. Paths can change dynamically, causing unexpected traffic shifts that can overwhelm QoS settings and cause packet loss due to congestion. According to a survey of 200 IT professionals, these sorts of logical issues such as sub-optimal routing, intermittent instabilities or slowdowns, and unanticipated network behavior are just as likely to be the root cause for VoIP problems as device failures or other causes that can be traced directly to individual devices.³

Further evidence of the importance of Layer 3 issues in VoIP management is found in the troubleshooting methodologies recommended by VoIP equipment and VoIP test equipment vendors. For example, Cisco recommends a Layer 3 topology path trace as the first step in diagnosing IP telephony problems:

“When you are faced with a lost or distorted audio problem, first try to isolate the path of the audio. Try to identify each network device (switches and routers) in the path of the call audio stream. Keep in mind that the audio may be between two phones, or between a phone and a gateway, or it could have multiple legs (from a phone to a transcoding device and from there to another phone). Try to identify whether the problem occurs only between two sites, only through a certain gateway, on a certain subnet, and so on. This will help narrow the number of devices that you need to look at more carefully.”⁴

Identifying each switch and router along the path of the call audio stream requires a real-time and historical knowledge of routed paths in the entire network—which is not available

³ 2009 Application Delivery Handbook, Metzler

⁴ Troubleshooting Guide for Cisco Call Manager, Release 7.0(1)

from traditional SNMP network management tools or end to end VoIP performance monitoring systems.

Another popular VoIP troubleshooting resource states that route flaps in particular are the most likely cause of a variety of VoIP issues, including high jitter, loss and out of order packet delivery.⁵

While it is clear that logical routing and traffic issues are significant and must be well managed in a converged IP network, network engineering departments today are hard pressed to explain, let alone prevent and resolve these dynamic, Layer 3 problems due to the inadequacy of traditional SNMP-based network management that focus on device issues, and the lack of Layer 3 management tools and solutions.

Route Analytics as Part of a Comprehensive VoIP Management Portfolio

A technology called route analytics that has been adopted by hundreds of enterprises, government agencies and service providers provides the missing Layer 3 routing and traffic management capabilities required to mitigate the risks of VoIP deployment and operation. Route analytics differs fundamentally from traditional SNMP management in that instead of simply managing individual devices or network elements, it provides visibility and automated analysis of the entire network's dynamic routing and traffic behavior.

Route analytics works by listening passively to all routing exchanges on the network and delivering a "router's eye view" of the network's routing topology and all routing and Layer 3 activity in real-time. Network engineers gain previously unavailable intelligence on the real-time, network-wide behavior of an IP network. By addressing the dynamic, logical layer of an IP network, route analysis solutions provide the following routing visibility to enhance VoIP management:

- Real-time, accurate monitoring and notification of issues in the IP network infrastructure that are missed by traditional network management, such as route flaps, missing or invalid routes or other Layer 3 problems that can cause unacceptable levels of latency, jitter, packet loss and unordered packets
- Modeling and validation of routing operations, before, during and after network maintenance, preventing costly configuration errors and service interruptions
- Rewindable history of all routing changes for unmatched forensic analysis and troubleshooting capabilities
- Automated diagnostic and planning tools to help network engineers quickly arrive at root cause determinations of VoIP problems and to proactively and accurately measure the resilience and availability of the network infrastructure under a variety of failure or change scenarios on an "as-running" network model, and without disrupting the production network.

⁵ <http://www.voiptroubleshooter.com/diagnosis/netsymptoms.html>

- Integration with existing network management platforms and processes through SNMP traps, syslog alerts and automatically delivered reports to help network engineers stay on top of emerging issues

Routing-Aware Class of Service (CoS) Traffic Management

Aside from providing unprecedented routing visibility, route analytics also radically increases the visibility network engineers have into network-wide CoS traffic delivery. By collecting Netflow data from key points in the network and then using knowledge of the precise route that every flow takes at any time through the network, route analytics creates a highly accurate, integrated, and continuously updated routing and traffic map that shows the volume of CoS traffic on every link in the network.

Furthermore, since route analytics understands how every flow gets to every link, it provides the network-wide context for every interface's traffic. For the first time, network engineers can see the big picture – the network as a holistic, dynamic organism – and immediately grasp the impact of routing changes or failures on traffic (even traffic located many hops away from where a change has occurred). Route analytics provides a number of capabilities for CoS traffic management that benefit VoIP management:

- CoS monitoring visibility for all links: Route analytics allows network managers to monitor traffic by specific class of service on every network link. Alerts can be sent when service classes go out of profile. Since VoIP traffic is usually assigned a particular CoS marking, engineers can now easily track VoIP traffic on all links in the network.
- CoS traffic problem localization and root-cause analysis: Since network managers know how service traffic gets to a particular link, it's much easier to discern whether out-of-profile CoS conditions are due to routing changes that shift traffic to or from a link, or due to new traffic coming into the network at the time the problem occurred.
- Replayable routing and CoS traffic history. One of the chief problems in troubleshooting application issues is that when the network is suspect, there is often no history to examine to prove or disprove that suspicion or localize the problem domain within the network. Route analytics continuously records routing and traffic so that network engineers can literally “rewind the network” to look at and even replay past event streams (see Figure 1). This high-fidelity forensic history greatly decreases mean time to repair (MTTR).

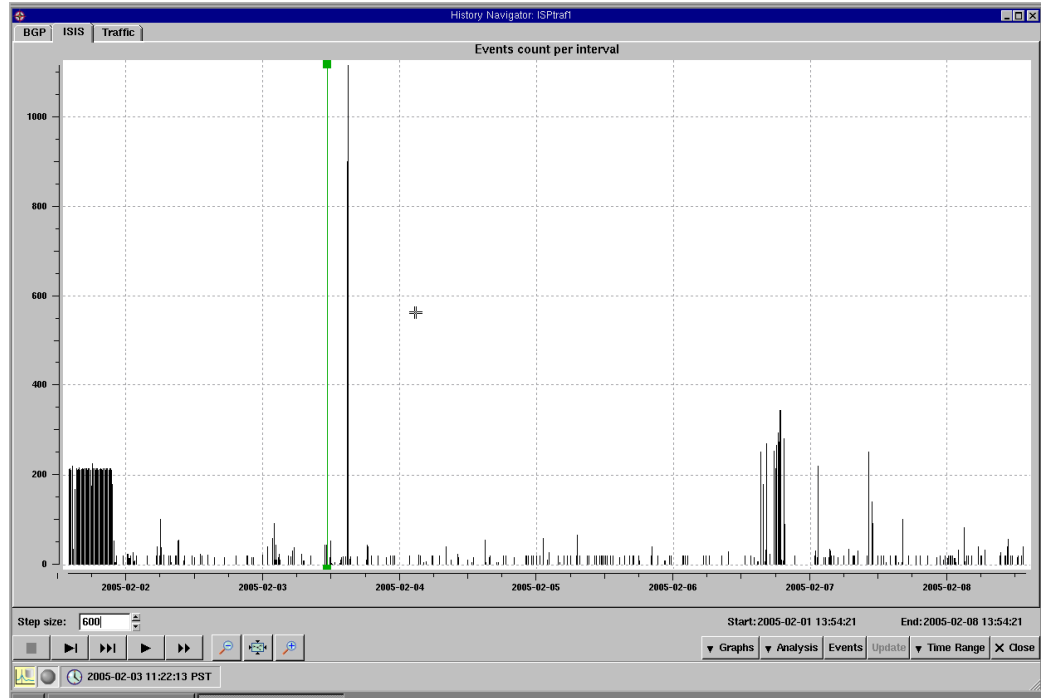


Figure 1: Route analytics' continuously recorded database of all routing and traffic changes can be rewound to look at a particular timeframe when a VoIP problem was occurring, providing an unprecedented forensic and troubleshooting history for network engineers.

Once an engineer has selected a timeframe, the precise routed path of the application traffic can be examined for VoIP-affecting conditions such as asymmetric paths, or routing instabilities such as link or prefix flapping, and for out-of-profile CoS conditions, as seen in Figure 2.

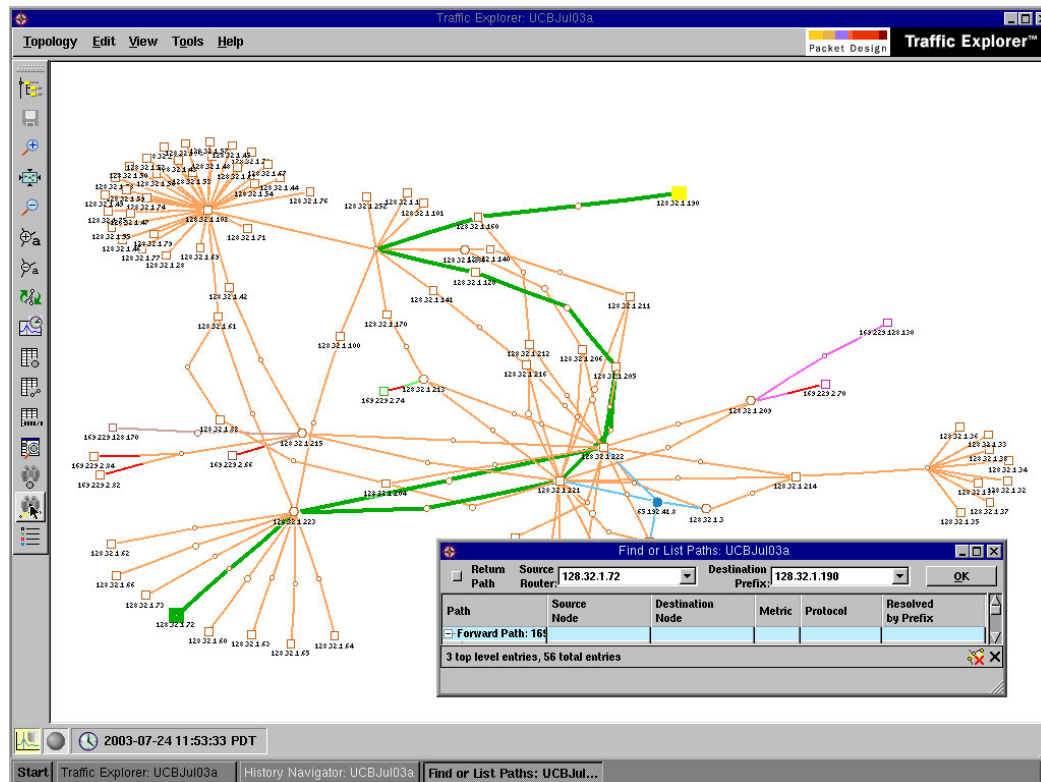


Figure 2: Engineers can select any two endpoint IP addresses and highlight the exact routed path taken by VoIP traffic in question at the time a problem was occurring in order to narrow down the part of the network that needs to be analyzed and see if there were any routing, path or congestion issues that affected the VoIP call(s)

- Modeling the impact of network changes and maintenance: Network engineers planning network changes or even performing routine maintenance can simulate various changes to ensure that CoS traffic will stay in profile based on those changes. Since the modeling is done on the actual state of routing and traffic, engineers can have a high degree of confidence in their planning and maintenance operations. For example, before making changes in the network, engineers can model those changes in the route analytics network model, then view a simulation of how the entire network would behave as a result, including both routing and CoS traffic distribution, as shown in Figure 3:

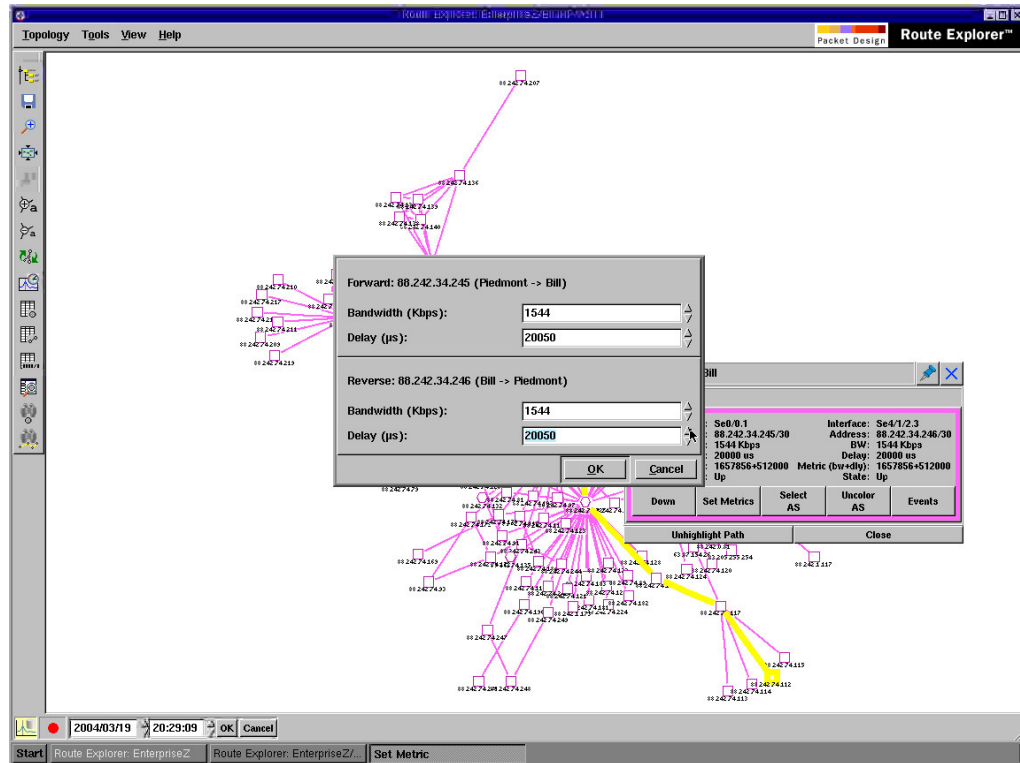


Figure 3: Route analytics can be used to simulate a variety of network changes, such as adding, downing, and moving routers, links and peerings, tuning routing metrics, adding new traffic flows, moving existing traffic flows, or even editing the entire traffic matrix

- Failure analysis and routing audits for service assurance: Route analytics also allows for simulation of failures on key links and components to let network managers analyze their impact on CoS traffic in the network. In addition, network engineers can run a comprehensive routing audit of the network to reveal suboptimal routing for delay-sensitive traffic such as Equal Cost Multi Paths (ECMPs), asymmetric paths, and links where failures could cause large variations in path lengths, as shown in Figure 4.

Destination Node	Reachable by	Paths	Hops	Metric	Show/Hide
128.32.1.200	52	1	3 - 9	100 - 1210	
128.32.1.221	52	1	3 - 7	2 - 1111	
128.32.1.222	52	1	3 - 7	11 - 1111	
128.32.1.3	52	1	3 - 9	100 - 1201	
128.32.1.4	52	1	3 - 9	11 - 1121	
128.32.1.102	46	1	2 - 7	2 - 6511	
128.32.1.252	46	1	3 - 7	110 - 6620	
128.32.1.43	46	1	2 - 8	6477 - 12987	
128.32.1.45	46	1	2 - 8	6477 - 12987	
128.32.1.47	46	1	2 - 8	6477 - 12987	
128.32.1.50	46	1	2 - 8	6477 - 12987	
128.32.1.51	46	1	2 - 8	6496 - 13006	
128.32.1.52	46	1	2 - 8	6477 - 12987	
128.32.1.54	46	1	2 - 8	6477 - 12987	
128.32.1.55	46	1	2 - 8	6477 - 12987	
128.32.1.56	46	1	2 - 8	7476 - 13986	
128.32.1.57	46	1	2 - 8	6496 - 13006	
128.32.1.59	46	1	2 - 8	6477 - 12987	
128.32.1.67	46	1	2 - 8	6477 - 12987	
128.32.1.68	46	1	2 - 8	6496 - 13006	
128.32.1.69	46	1	2 - 8	6477 - 12987	
128.32.1.71	46	1	2 - 8	6477 - 12987	
128.32.1.74	46	1	2 - 8	6477 - 12987	
128.32.1.75	46	1	2 - 8	6477 - 12987	
128.32.1.76	46	1	2 - 8	6477 - 12987	
128.32.1.77	46	1	2 - 8	6477 - 12987	
128.32.1.78	46	1	2 - 8	6477 - 12987	
128.32.1.79	46	1	2 - 8	6477 - 12987	
128.32.1.81	46	1	2 - 8	6477 - 12987	
169.229.0.122	46	1	2 - 8	6477 - 12987	
128.32.1.100	43	1	3 - 5	2 - 6611	
128.32.1.101	39	1	3 - 7	2 - 6611	
128.32.1.223	39	1	3 - 6	2 - 6712	
128.32.1.60	39	1	3 - 8	101 - 6812	
128.32.1.61	39	1	3 - 8	51 - 6762	
128.32.1.62	39	1	3 - 8	101 - 6812	
128.32.1.63	39	1	3 - 8	101 - 6812	
128.32.1.64	39	1	3 - 8	101 - 6812	
128.32.1.65	39	1	3 - 8	101 - 6812	
128.32.1.66	39	1	3 - 8	101 - 6812	
128.32.1.72	39	1	3 - 8	101 - 6812	
128.32.1.120	38	1	3 - 7	2 - 6611	
128.32.1.130	38	1	3 - 7	2 - 6611	
128.32.1.140	38	1	3 - 7	2 - 6611	
128.32.1.160	38	1	3 - 7	2 - 6611	
128.32.1.170	38	1	3 - 7	2 - 6611	
128.32.1.190	38	1	3 - 9	101 - 6711	

Figure 4: Comprehensive path reports allow network engineers to examine the health of their routing operations for potential trouble such as asymmetric paths or vulnerability, such as where there is only a single path to important destinations.

- Network-wide capacity planning. Since route analytics captures a complete history of both routing and traffic changes across the entire network as a baseline, and is able to model changes, it can generate highly accurate capacity planning trending projections for link and CoS traffic.

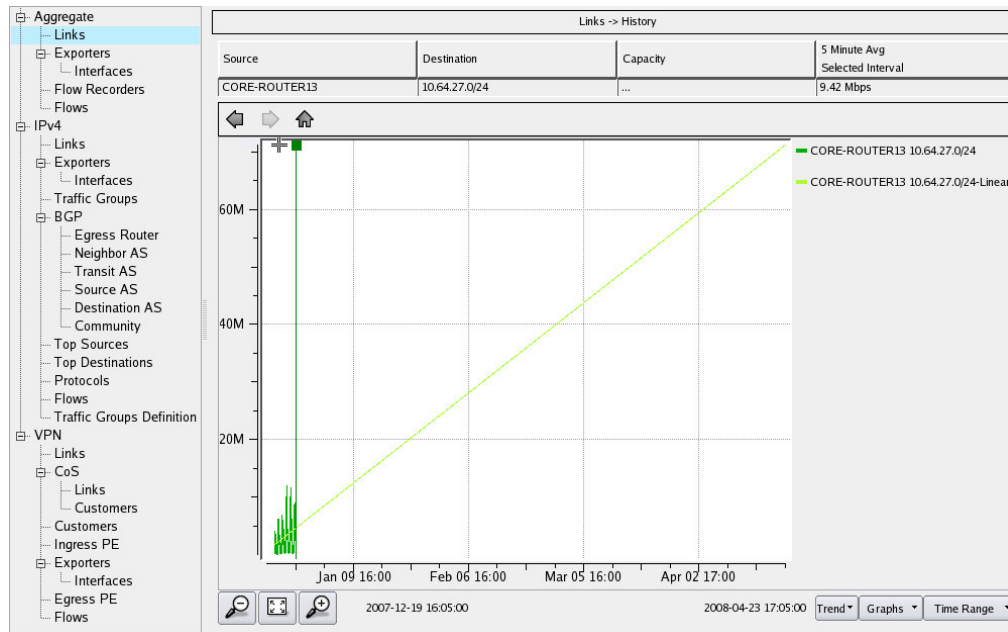


Figure 5: Route analytics can utilize its collected routing and traffic history as the baseline from which to project traffic trends on any and all links in the network in aggregate, by CoS or application.

Conclusion

VoIP deployments are becoming more strategic to both enterprises and service providers, requiring a more comprehensive approach to managing the end-user’s experience. Route analytics fills a critical gap in network management tools and practices that helps IT and network managers ensure more reliable and predictable network behavior, localize and resolve problems faster, prevent outages from mistakes made in routine maintenance changes or unanticipated failure conditions, and properly plan network capacity by CoS. To learn more about Packet Design’s industry-leading route analytics solutions, please:

- Email us at info@packetdesign.com
- Visit Packet Design’s web site at <http://www.packetdesign.com>
- Call us at 408-490-1000