CISCO INFORMATION TECHNOLOGY AT WORK CASE STUDY: CISCO IOS NETFLOW TECHNOLOGY

CISCO INFORMATION TECHNOLOGY

SEPTEMBER 2004

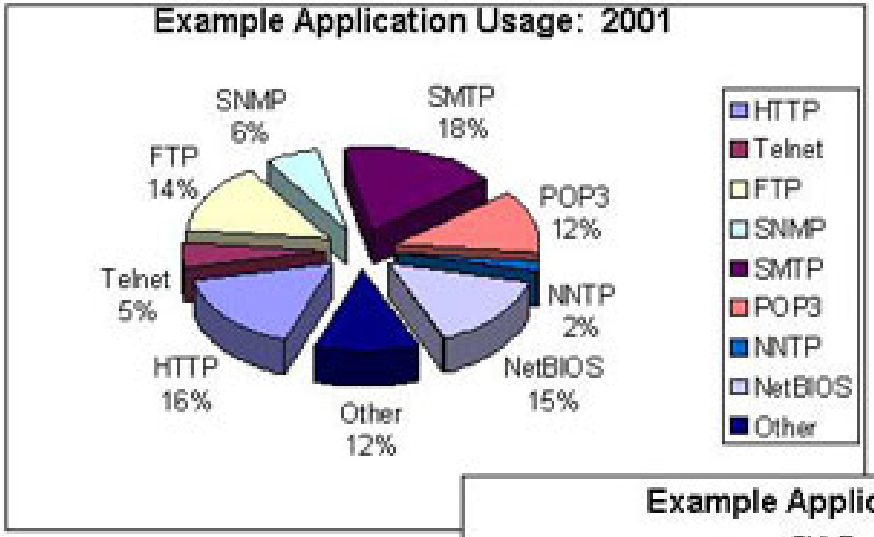
Overview

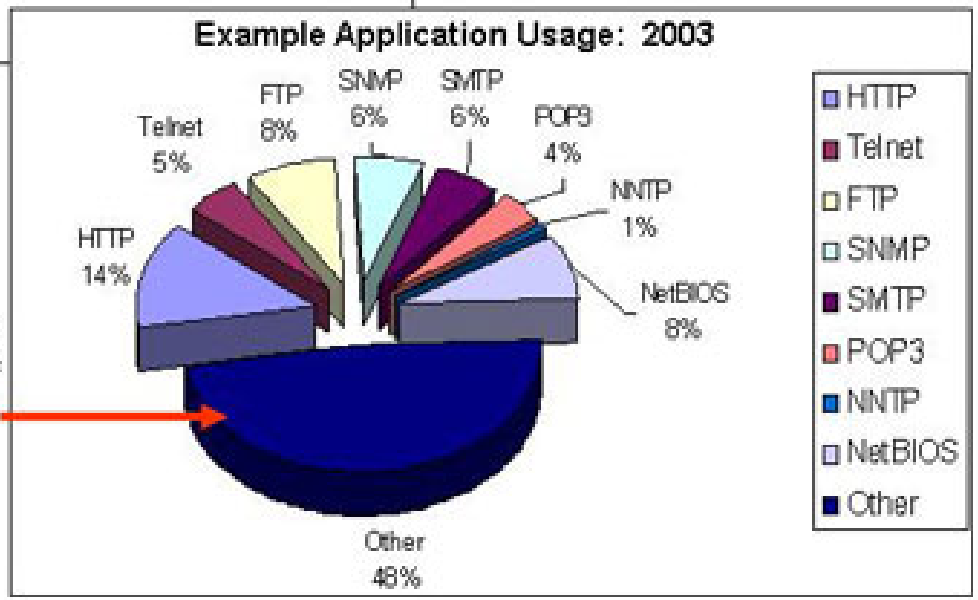
- **Challenge**
  - **To troubleshoot capacity and quality problems and to understand usage, network managers need to see application flows through the network**
  - **Networks provide views of application flows, but don't provide information about them**
  - **Seeing packet flows per port helps, but a growing number of applications use dynamic ports, which complicating traffic characterization**
- **Solution**
  - **Cisco IOS® NetFlow (already part of the network)**
  - **Tools to capture and format the data**
- **Results**
  - **Cisco IOS NetFlow supports capacity planning, network protection against denial of service (DoS) attacks, and other forms of undesirable traffic and provides new information about network use**
- **Next Steps**
  - **Expand the use of the NetFlow technology to other parts of the network**

Challenge—No Application Flow Information

- **Cisco Systems almost exclusively relied on Simple Network Management Protocol (SNMP) to monitor Internet bandwidth**
  - **Although SNMP facilitates capacity planning, it does very little to characterize traffic applications, essential for understanding how well the network supports the business**
- **Cisco needed a more granular understanding of Cisco bandwidth usage**
- **Port flow was monitored, but many newer applications dynamically select new ports for each use**

Challenge—Application Usage





A growing portion of applications use dynamic ports, complicating traffic characterization

Solution—Cisco NetFlow Technology

- **With its NetFlow Technology Cisco gained ability to characterize and analyze network traffic flows**
  - **Cisco IOS NetFlow technology is built into most Cisco switches and routers using a specialized application-specific integrated circuit (ASIC) and some specialized features of Cisco IOS Software and Cisco Catalyst® Operating System Software**
- **Cisco IOS NetFlow has become a primary network accounting technology and anomaly-detection technology in the industry**
- **Cisco IOS NetFlow answers the following questions about network traffic:**
  - **Who, what, when, where, and how ?**
- **Cisco IOS NetFlow Version 9 was chosen for a proposed IETF standard called IP Flow Information Export (IPFIX) in 2003**
  - **IPFIX defines the format by which IP flow information can be transferred from an exporter, such as a Cisco router, to a collector application that analyzes the data**

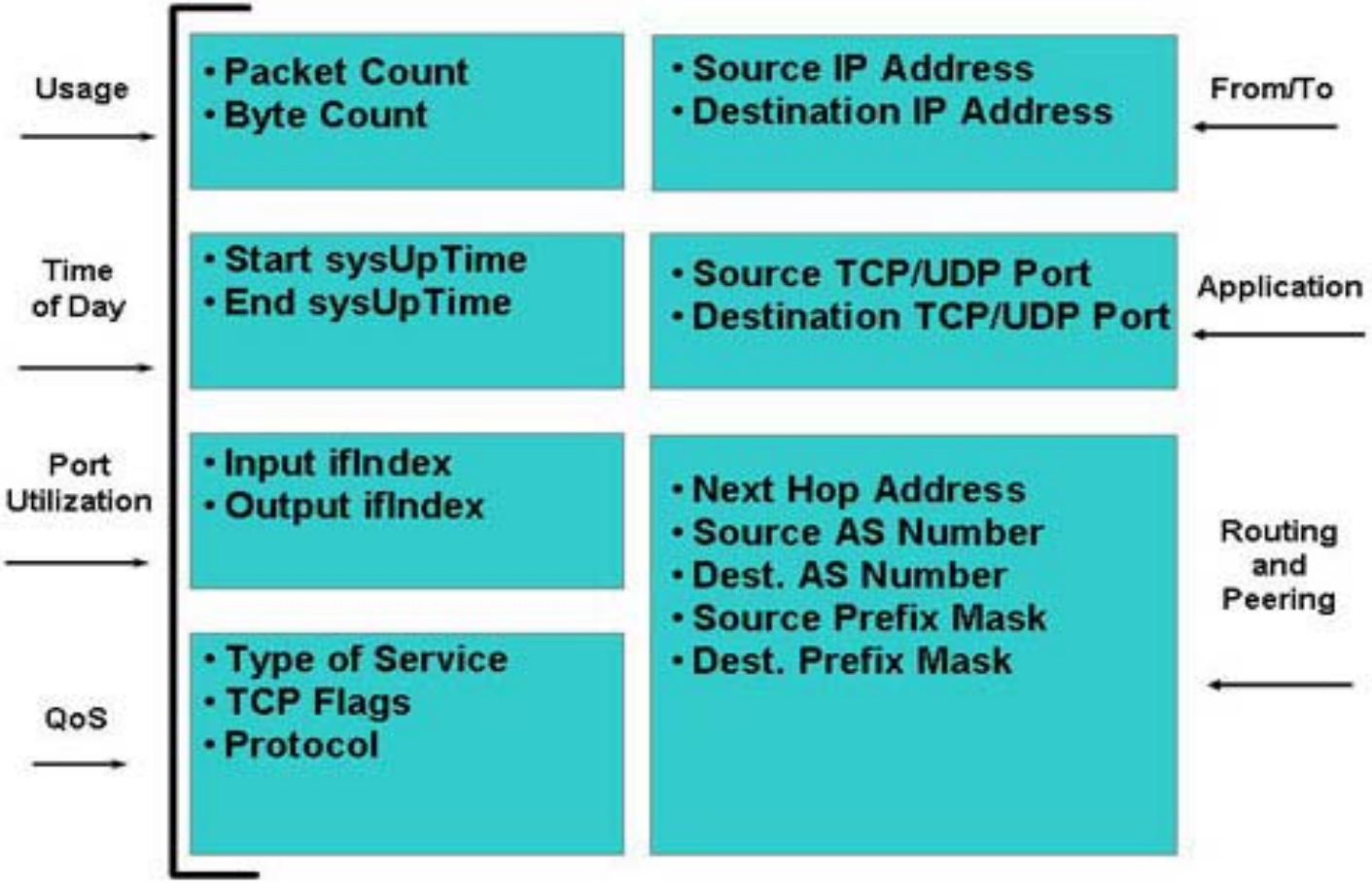
Solution—Cisco NetFlow Technology

- **To export data routers represent each network traffic flow based on:**
  - **Source and destination IP address**
  - **Source and destination port**
  - **Layer 3 protocol type**
  - **Type of service**
  - **Input logical interface**

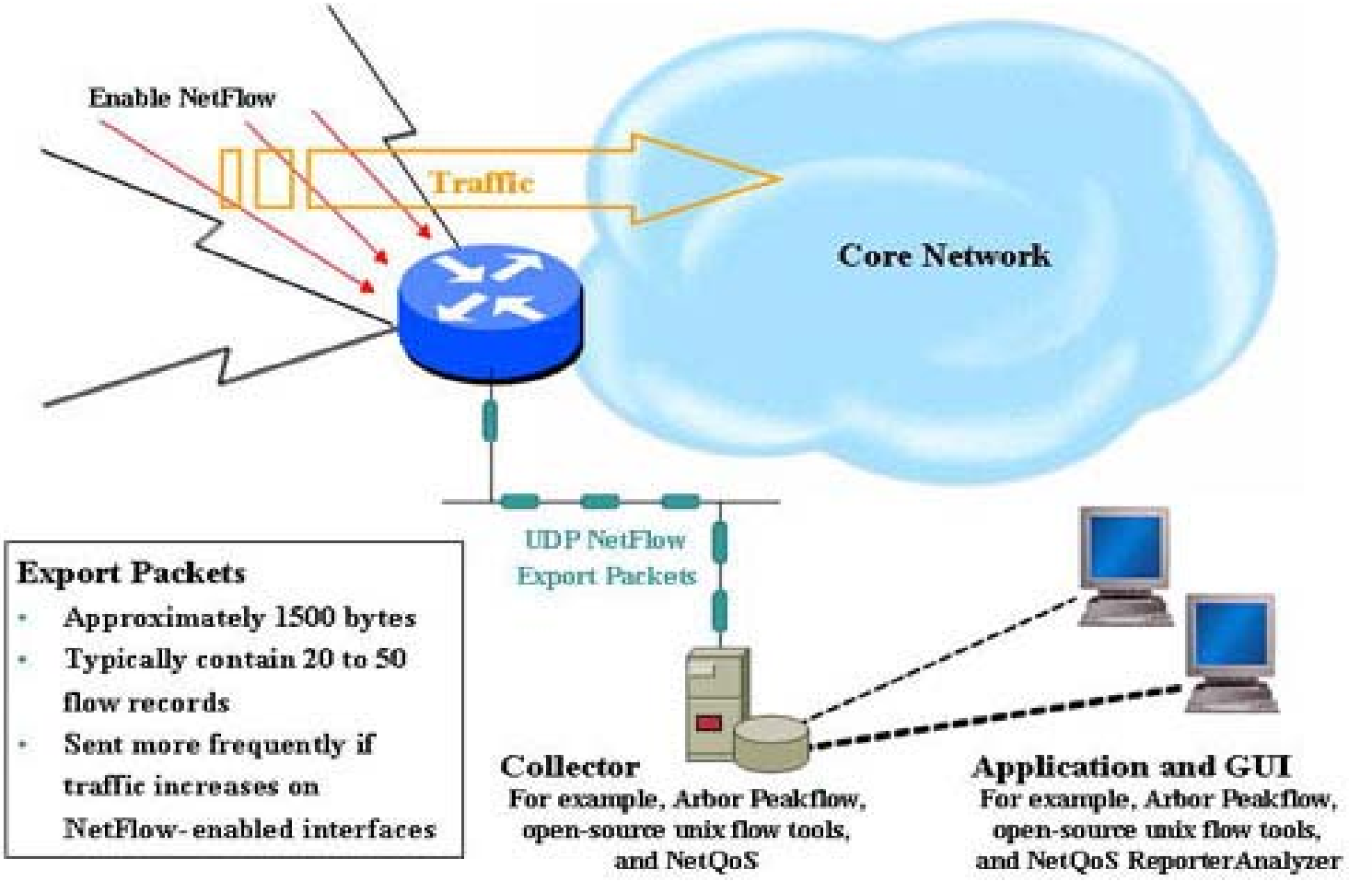
“YOU CAN THINK OF NETFLOW AS A FORM OF TELEMETRY PUSHED FROM ROUTERS AND LAYER 3 SWITCHES, EACH ONE ACTING AS A SENSOR.”

JOHN CORNELL, CISCO IT TECHNICAL STAFF

Solution—Flow Information

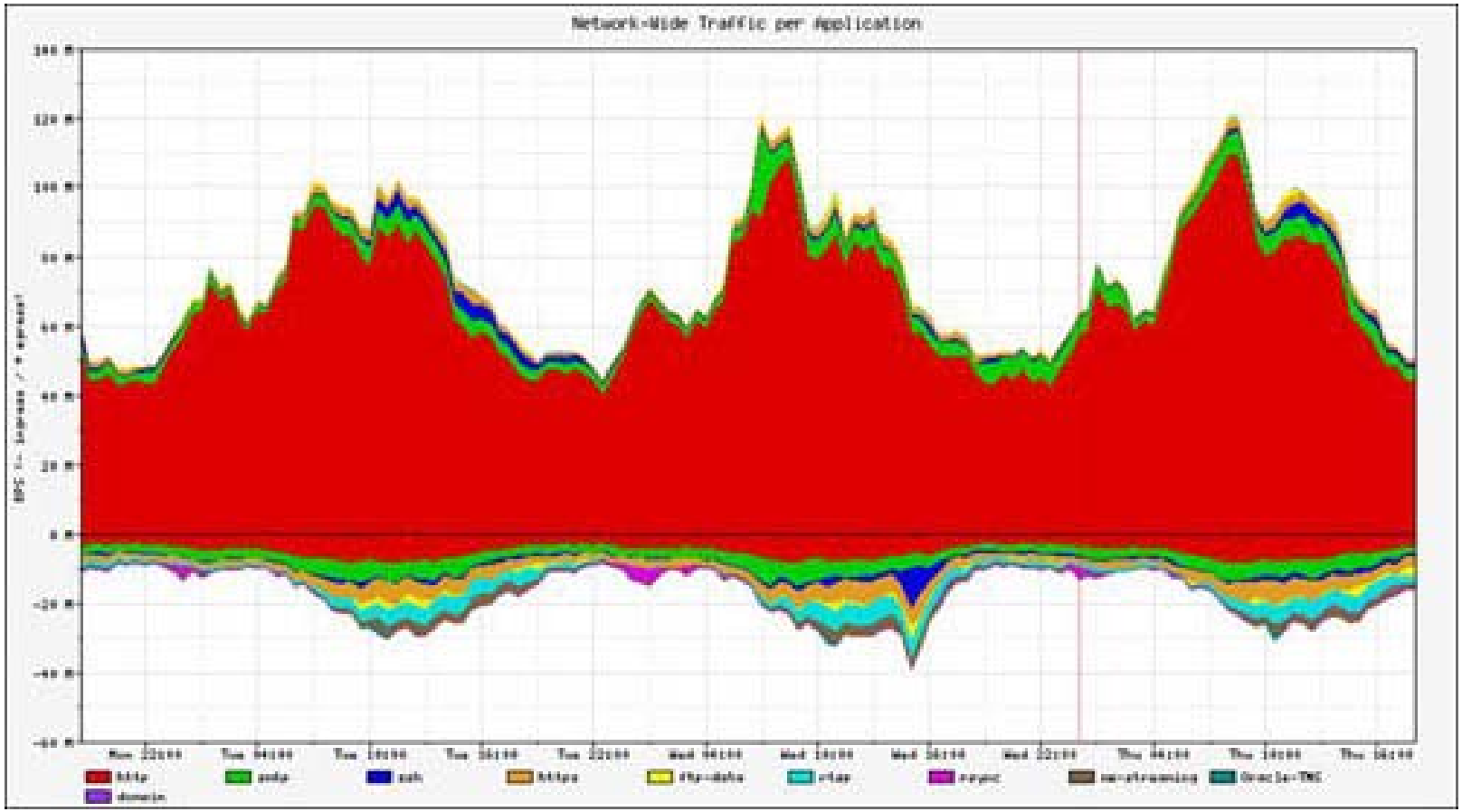


Solution—Export Packets



Results—Characterize Traffic by Application

- **Cisco IOS NetFlow Data by Arbor Networks Peakflow Traffic**



Results—Cost Effective

- **Cisco IOS NetFlow is more cost effective in gathering network traffic information than Remote Monitoring (RMON) probes**
- **Cisco IOS NetFlow feature is enabled in several places on the Cisco network that process incoming and outgoing traffic, for a total of more than 1900 WAN interfaces**
- **Information from each location is useful on its own, as well as in combination with other network–related business intelligence**

  For example, the combination of Cisco IOS NetFlow and Border Gateway Protocol (BGP) routing information provides visibility into the origin and destination of Cisco network traffic, which helps to ensure optimal peering with Internet service providers (ISPs)

Results—Analysis Software (Data Collection)

Network Location	Analysis Software	Purpose
Internet gateway routers that connect to ISP links	Arbor Networks Peakflow Traffic Arbor Networks Peakflow DoS	Network traffic analysis by application Correlation of network traffic with BGP routing information Anomaly detection
Routers at inner edge of public-facing network	Arbor Networks Peakflow DoS	Anomaly detection
WAN core (aggregation layer)	NetQoS ReporterAnalyzer	Network traffic analysis by application for capacity planning
WAN edge	NetQoS ReporterAnalyzer	Network traffic analysis by application for capacity planning
Core routers on public-facing network	OSU flow-tools from splintered.net	Collection of historical data, useful for forensics and diagnostics
Network Address Translation (NAT) gateway	OSU flow-tools from splintered.net	Collection of historical data, useful for forensics and diagnostics Auditing of addresses that have undergone NAT (“NATed” addresses)

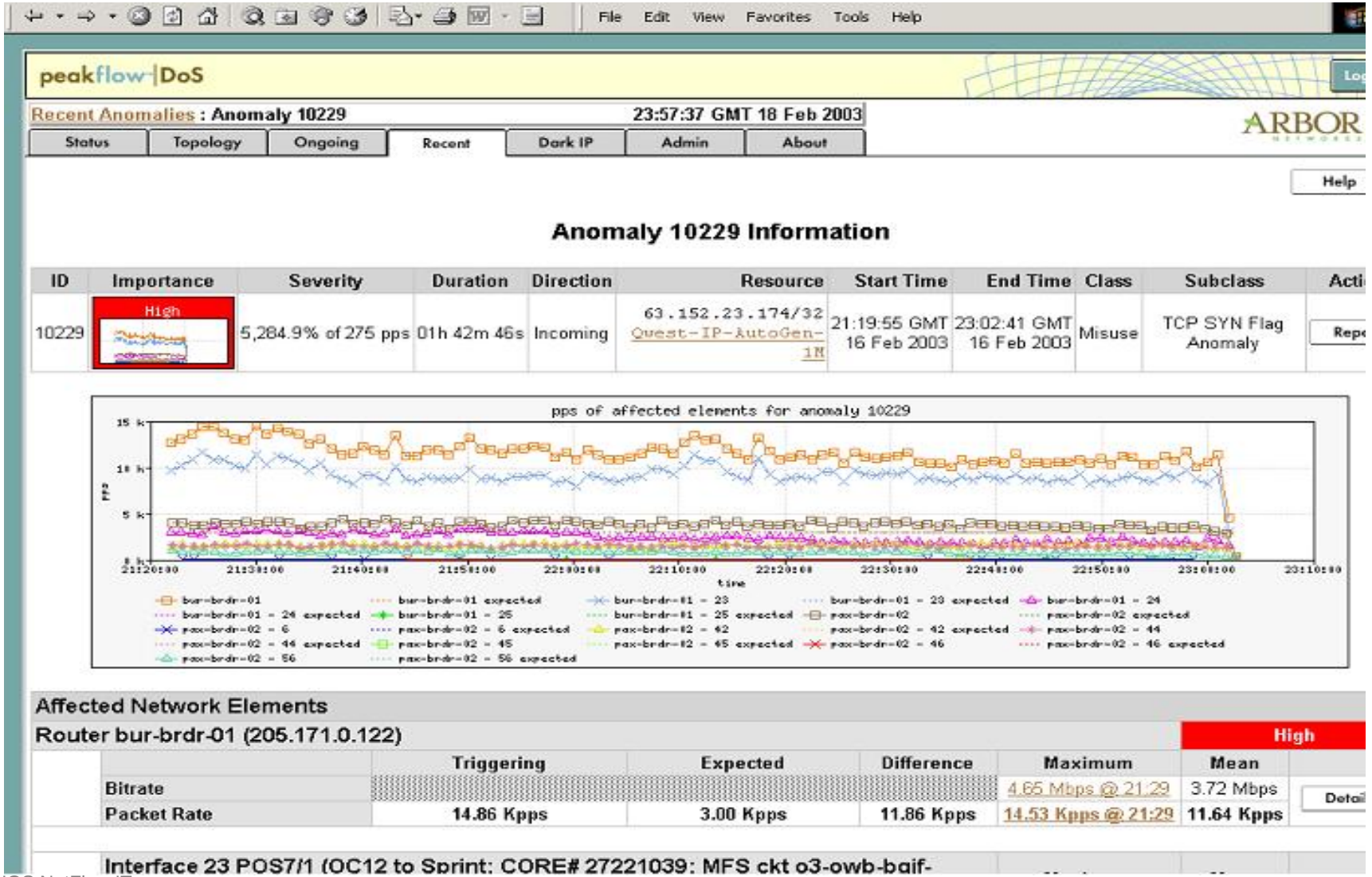
Results—Internet and Security Benefits

- **Avoidance of Structured Query Language (SQL) Slammer Worm**
  - **On January 24, 2003 the SQL Slammer worm, also called Sapphire, propagated worldwide in just eight minutes**
  - **Networks fell worldwide, including entire networks of automated teller machines and leading enterprises**
- **Cisco did not experienced any loss of business continuity from SQL Slammer due to:**
  - **Teamwork**
  - **Established communications plan**
  - **Robust network architecture**
  - **Effective use of Cisco IOS NetFlow technology**

Results—DoS Attacks and Other Undesirable Traffic

- Cisco Information Technology uses NetFlow data to protect the network from viruses and attacks and to understand the effects of current and planned applications on the network
- From time to time, Cisco receives traffic intended to produce a DoS attack
- DoS attacks flood the network with packets, often of an unusual size, from an untrusted source to a single destination
- Cisco detects and prevents DoS attacks by using Cisco IOS NetFlow to collect:
  - Packet source
  - Destination
  - Protocol number
  - Port number
  - Packet size
- Collected information is sent to Arbor Peakflow DoS for anomaly detection

Results—Anomaly Detection Report



Results—WAN Traffic

- **Detection of Unauthorized WAN Traffic**

  Cisco has avoided costly upgrades by identifying the applications causing congestion and, if appropriate, changing the usage policy

- **Reduction in Peak WAN Traffic**

  Cisco Information Technology uses NetFlow statistics to measure WAN traffic improvement from application-policy changes

- **Validation of QoS Parameters**

  By using Cisco IOS NetFlow and NetQoS ReporterAnalyzer IT is able to confirm that appropriate bandwidth has been allocated to each class of service (CoS) and that no CoS is over- or under-subscribed

- **Analysis of VPN Traffic and Teleworker Behavior**

  Cisco Information Technology can easily identify teleworker traffic because it all travels over identifiable tunnels

  This type of traffic analysis facilitates capacity planning for Internet access and understanding of home worker behavior

Results—Total Cost of Ownership Calculation

- To prevent unexpected effects on the WAN, Cisco application development groups first deploy new applications in a test environment
  - Cisco IOS NetFlow is used to measure how much WAN traffic the application is likely to generate when released to a larger population
- Testing applications helps to calculate Total Cost of Ownership (TCO) more accurately
- Benefits of Cisco IOS Netflow for Cisco include:
  - Cost effective deployment of applications
  - Constant availability of services for all employees, customers, and partners worldwide

Next Steps—Summary

- **Cisco Information Technology next steps:**
  - **To benefit from the increasing value of the network data being collected**
  - **To expand the use of NetFlow to other parts of the network**
- **As Cisco continues to collect more NetFlow historical data, capacity planning will become easier**
- **Cisco anticipates extending capacity planning methodologies used for Internet connectivity to internal networks on the Cisco WAN**

Cisco IOS NetFlow Technology

- **As converged networks and IP telephony become more prevalent, the ability to characterize traffic on the network—both for capacity planning and anomaly detection—becomes even more critical**

  NetFlow provides that capability for Cisco