Self-Configuring Network Monitor Project: an Infrastructure for Passive Network Monitoring

PIs: Deb Agarwal and Brian Tierney

Distributed Systems Department
Lawrence Berkeley National Laboratory

1/16/2002

Purpose

- Provide the ability to:
  - characterize application data streams as they cross the network
  - assess the impact of application tuning on the network
- Aid in debugging and tuning of distributed applications
- Minimize impact of monitoring on the network infrastructure

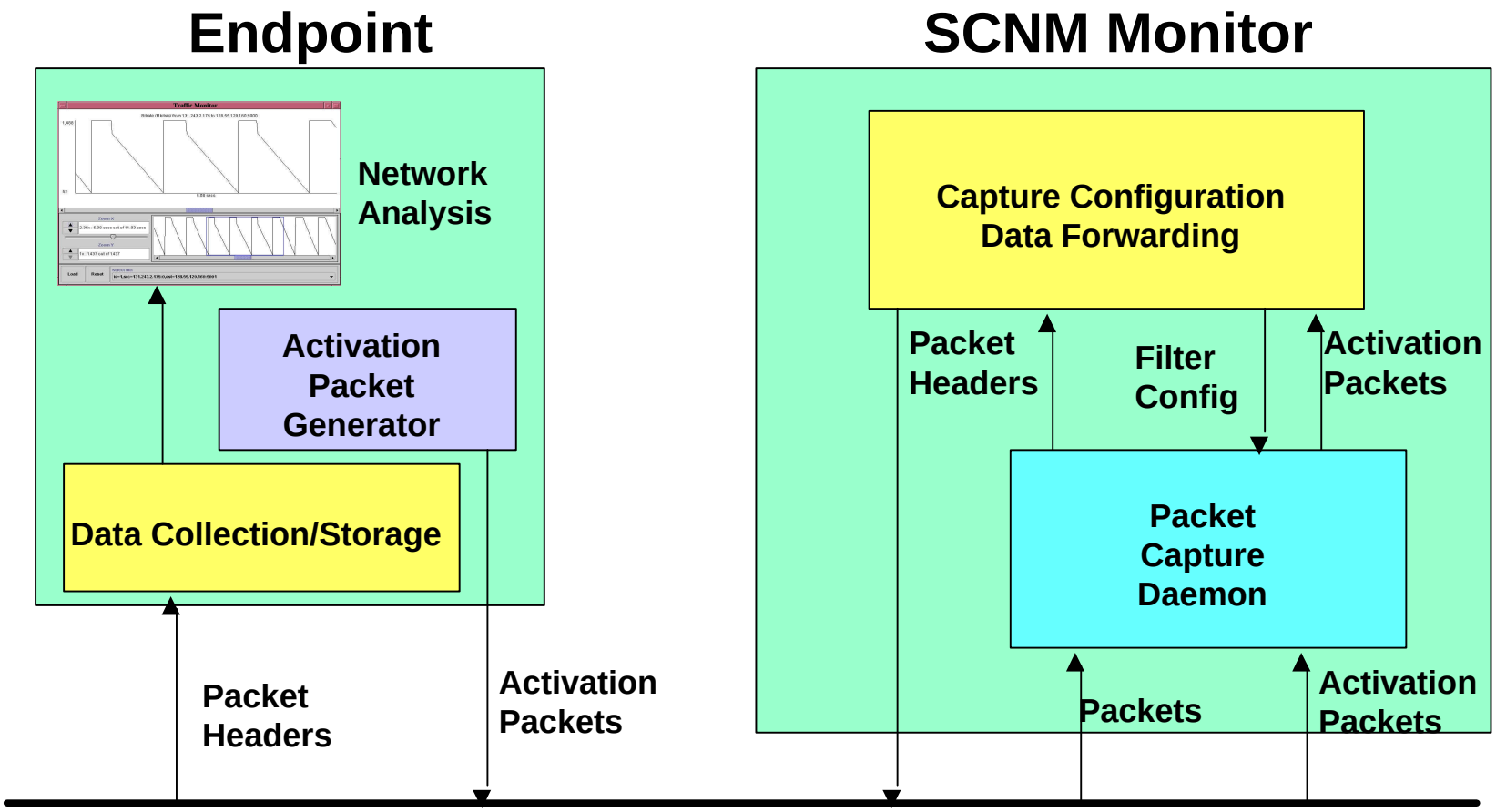
Monitor Host

- Installed at critical points in the network (i.e.: next to key routers)
- Passively captures packet headers of monitored traffic
  - Daemon based on *libpcap* (NIMI and Bro)
- Configured and activated by application end-points
  - Without network administrator involvement
  - Secure from unauthorized access
- Provides application traffic information from the interior of the network

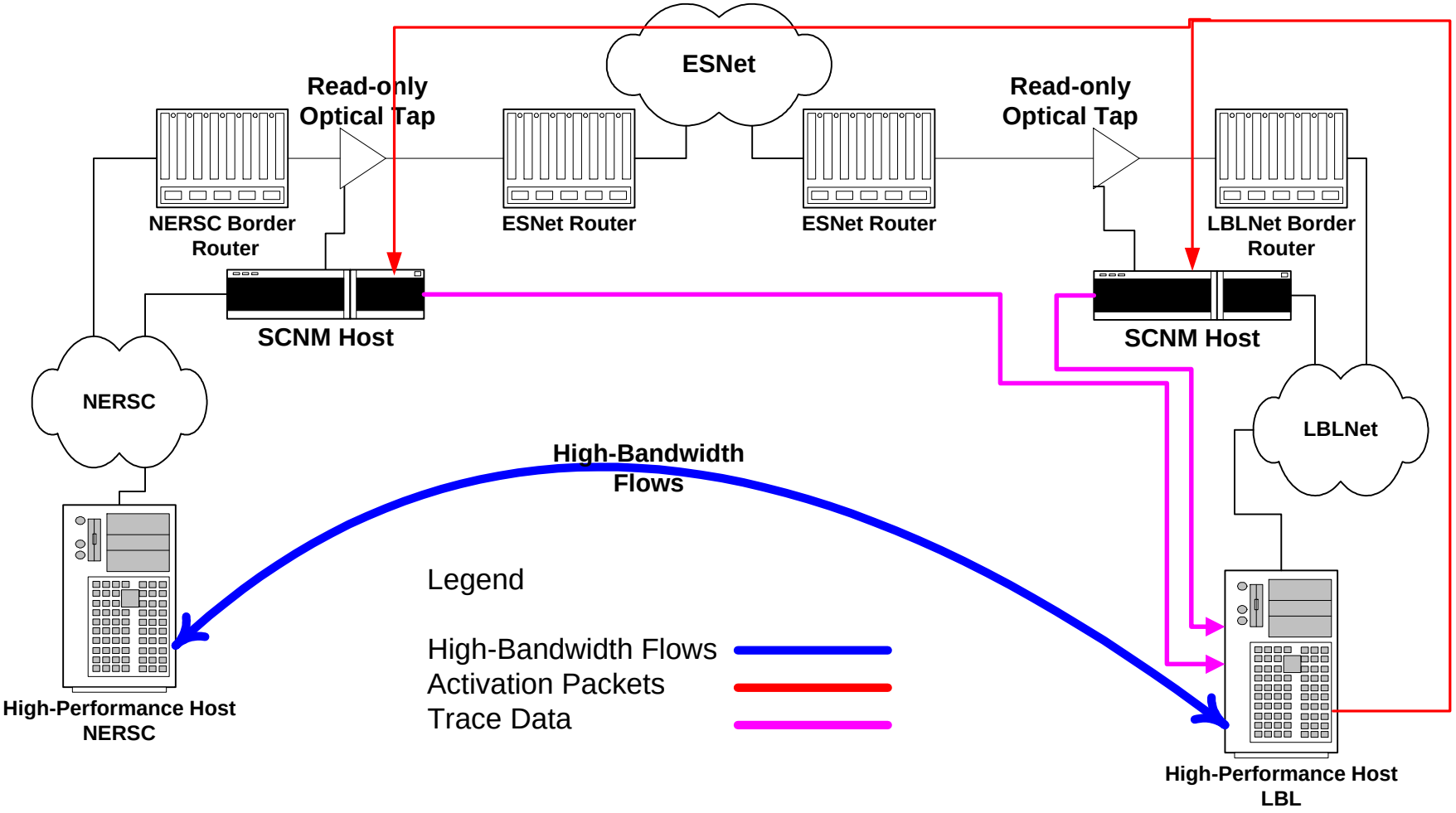
Activation and Configuration

- Activation packets are sent by application endpoints to all monitors along the data path using UDP and a well known port
- Activation packets specify which traffic to monitor
- The monitor configures itself to monitor the traffic
- Activation packets resent periodically to refresh monitor state
- Monitor times out if no activation packets are received

System Design



Typical Usage



Security

- Monitor host system installed and maintained by network administrators
- User mode:
  - Activation packet must be traveling between source and destination of monitored traffic to configure a monitor
  - Packet headers only sent to the source or destination
- Network Admin mode:
  - to activate monitoring from a host that is not one of the endpoints requires signed and authorized activation packet
- Logs all traffic monitoring requests

Deployment

- Install at critical points in the network
  - DMZ's
  - Critical end site routers
- Installed by network administrators
- Initial installations
  - SC 2001
  - NERSC DMZ
  - LBNL DMZ
  - ORNL

Project Milestones

- Year 1
  - Design and implement base monitor activation protocol
  - Design and implement base monitoring capability (tcpdump)
  - Deploy to a limited number of sites
- Year 2
  - Expand activation mechanisms: security and options
  - Deploy to additional sites
  - Improvements to the Berkeley Packet Filter
  - Integration of archiving mechanisms
- Year 3
  - Expansion of monitor and activation capabilities

For More Information

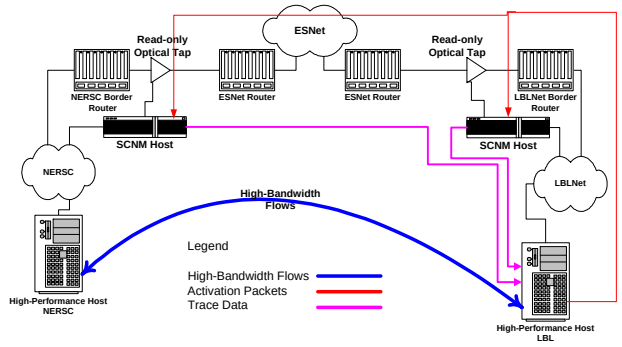
- Contact
  - Deb Agarwal (DAAgarwal@lbl.gov)
  - Brian Tierney (BLTierney@lbl.gov)

Self-Configuring Network Monitor (SCNM)

PIs: Deb Agarwal and Brian Tierney, LBNL

High-Performance Network Research- SciDAC/Base

SCNM: Developing a distributed passive network monitoring system



Novel Ideas

- A secure monitoring infrastructure that applications can use to monitor their own data streams as they cross the network
- Passive – introduce traffic only in the form of monitoring data and requests for monitoring

Tasks Involved

- Develop a monitor activation mechanism
- Develop monitor software and hardware
- Develop data collection and display capabilities
- Deploy monitors
- Work with applications

Impact and Connections

? IMPACT:
  ? Build a monitoring infrastructure that will aid in debugging of distributed application communication and support both active and passive monitoring
  ? Allow the analysis of network streams from the interior of the network
? CONNECTIONS:
  ? Net 100, DOE Science Grid, Astrophysics, Bandwidth Estimation, PPDG, EU DataGrid, INCITE, DataTag
? URL:
  ? *http://www-itg.lbl.gov/Net-Mon/Self-Config.html*

Milestones/Dates/Status

	Year
• Monitor Daemon	
- Design base passive monitor daemon	1
- Activation mechanism integration	1
- Improvements to network drivers	1
- Improvements and enhancements to capture mechanism	2 & 3
? Activation Mechanisms	
- Design basic activation mechanism	1
- Develop and deploy full activation capabilities	2 & 3
• Results Handling Infrastructure	
- TCP dump viewing capabilities	1
- Develop improved data viewing capabilities	2 & 3
• Deployment of Monitors	
- Deployment to initial ESnet sites (gig-E)	1 – 3
- Work with applications	2 & 3
- Additional ESnet sites	2 & 3