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

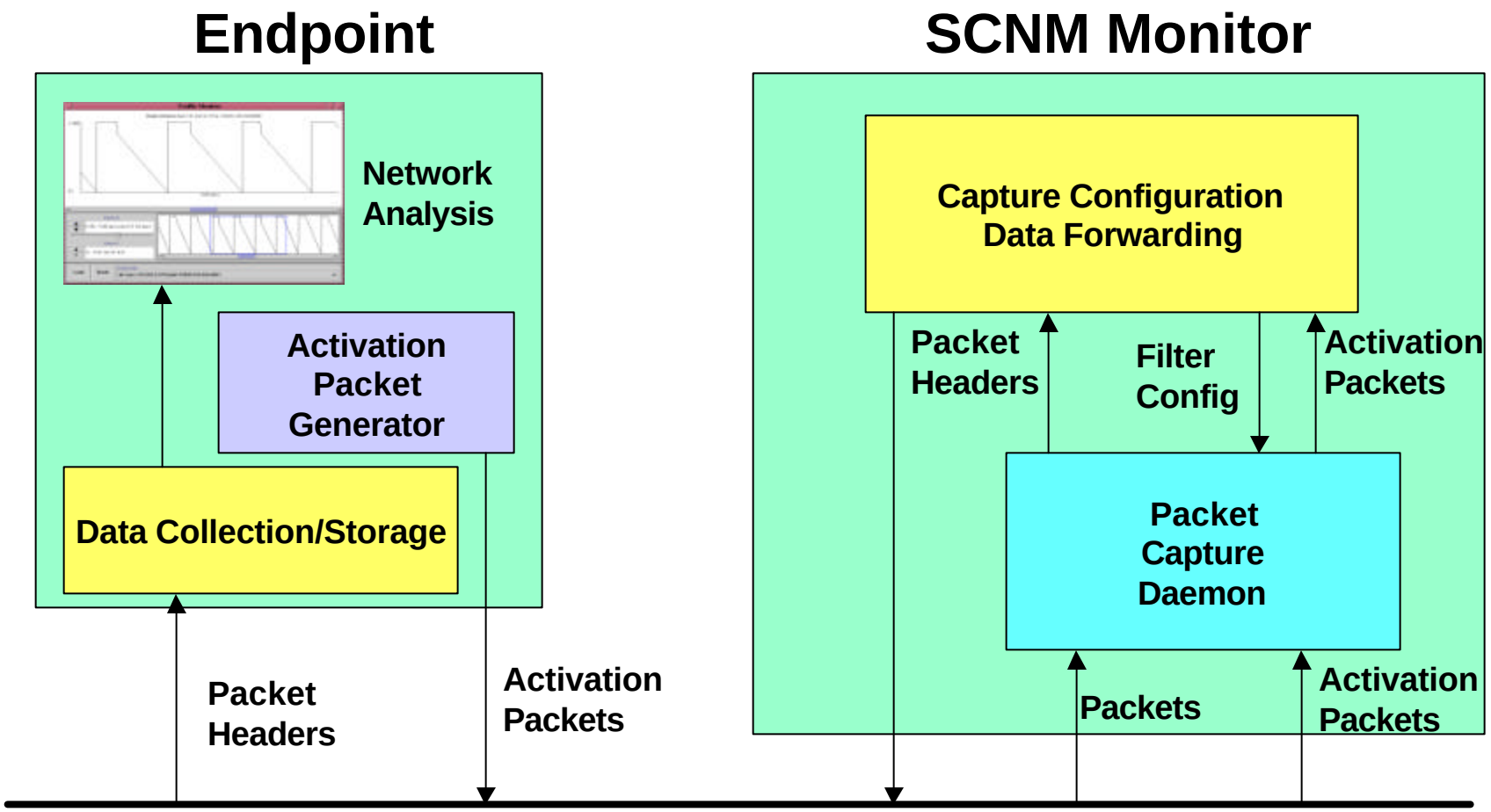
Monitor Host

- 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

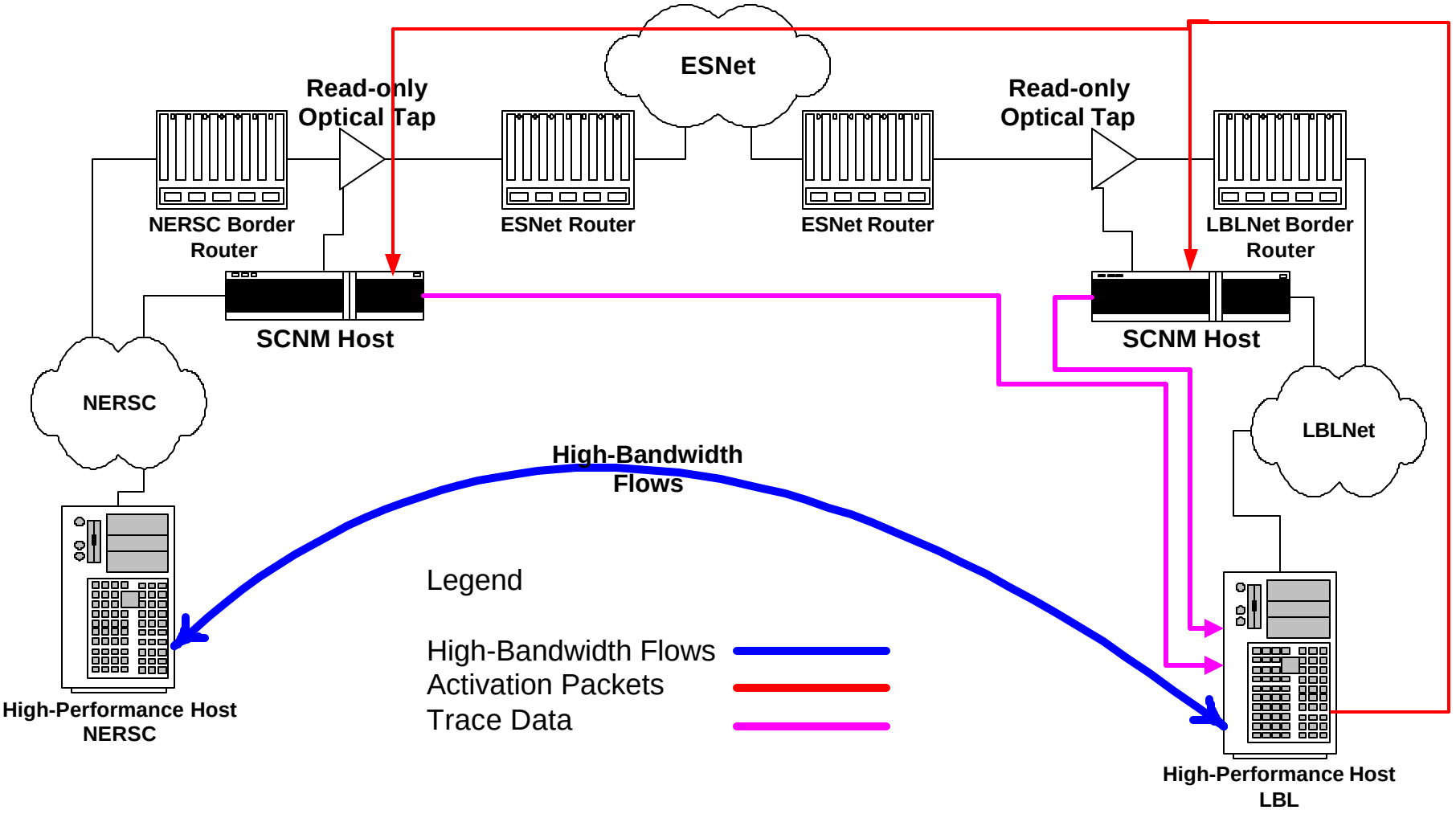
Activation and Configuration

- 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

For More Information

- Self-Configuring Network Monitor
  - Deb Agarwal (DAAgarwal@lbl.gov)
  - Brian Tierney (BLTierney@lbl.gov)
  - www-itg.lbl.gov/Net-Mon/Self-Config.html
- Reliable and Secure Group Communication
  - Deb Agarwal (DAAgarwal@lbl.gov)
  - http://www-itg.lbl.gov/CIF/GroupComm/