Distributed QoS Monitoring
High Performance Network Assurance

Carter Bullard
FloCon 2005  Pittsburgh, PA
From ITU-T Recommendation E.800 Quality of Service, Network Management and Traffic Engineering
Approach

• Adopt PSTN TMN Usage Strategies
  – Service Oriented Metering
  – Integrated Measurement
  – Establish Comprehensive Transactional Audit
  – Near Real-Time Accessibility

• Extend PSTN Model for Internet Networking
  – Internet Transactional Model
  – Distributed Asymmetric Network Monitoring

10 October 2005
Comprehensive Data Network Accountability

- Ability to account for all/any network use
- At a level of abstraction that is useful
  - Network Service Functional Assurance
    - Was the network service available?
    - Was the service request appropriate?
    - Did the traffic come and go appropriately?
    - Did it get the treatment it was suppose to receive?
    - Did the service initiate and terminate in a normal manner?
  - Network Control Assurance
    - Is network control plane operational?
    - Was the last network shift initiated by the control plane?
    - Has the routing service converged?

10 October 2005
The Global Information Grid
A Diverse Environment

Serving business, warfighting, & intelligence with NCES --
- Collaboration, messaging, & applications
- Storage and mediation
- User assistance
- Information Assurance
- Enterprise Services Management and Operations
10 October 2005

GIG-EF OOO Network
ATDnet & BoSSNET
NRL
NSA
MIT/LL

IPv6/MPLS Instrumented Testbed ...
IS-IS, BGP+
Dual Stack: IPv4/v6 w/ BGP4, OSPF

DREN(HPCMP) Network

Transition IPv4/v6/MPLS
... BGP4, OSPF

Air Force
... as required

Army
... as required

Navy Marines
... as required

GIG-EF OOO Network
ATDnet & BoSSNET

MSPP

DISA

Army
... as required

Air Force
... as required

JITC

NRL

GIG-EF OOO Network
ATDnet & BoSSNET

MIT/LL

NSA
Abstract QoS Control Plane

Figure 1. Reference QoS Control Architecture
Project Methodology

• New Distributed Network Monitoring Strategy
  – Comprehensive Network Usage Measurement (IETF IPFIX WG)
  – User Data Loss Detection (IETF RFC 2680)
  – Generic One-way Delay Monitor (IETF RFC 2679)
  – User Data Jitter Measurements (IETF RFC 3393)
  – Comprehensive Reachability Monitor (IETF RFC 2678)
  – Capacity/Utilization Monitor (IETF RFC 3148)

• Establish Comprehensive Audit (IETF RTFM, ITU TMN)
• Utilize Uniform Data Collection (IETF IPFIX, ITU TMN)
• Perform fundamentally sound statistical analysis
• To Enable Effective Network Optimization

10 October 2005
NTAIS FDO Optimization

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Discover and Identify comprehensive network behavior.</td>
</tr>
<tr>
<td>Analyze</td>
<td>Collect and transform data into optimization metrics. Establish baselines, occurrence probabilities, and prioritize efforts.</td>
</tr>
<tr>
<td>Plan</td>
<td>Establish optimization criteria (both present and future) and implement actions, if needed. This could involve reallocation of network resources, physical modifications, etc.</td>
</tr>
<tr>
<td>Track</td>
<td>Monitor network behavioral indicators to realize an effect.</td>
</tr>
<tr>
<td>Control</td>
<td>Correct for deviations from the criteria.</td>
</tr>
</tbody>
</table>
Gargoyle Probe

• Comprehensive Passive Real-Time Flow Monitor
  – User Plane and Control Plane Transaction Monitoring
  – Reporting on System/Network QoS status with every use
    • Capacity, Reachability, Responsiveness, Loss, Jitter
    • ICMP, ECN, Source Quench, DS Byte, TTL

• Multiple Flow Strategies
  – Layer 2, MPLS, VLAN, IPv4, IPv6, Layer 4 (TCP, IGMP, RTP)

• Small Footprint
  – 200K binary

• Performance
  – OC-192, 10GB Ethernet, OC-48, OC-12, 100/10 MB Ethernet, SLIP
  – POS, ATM, Ethernet, FDDI, SLIP, PPP
  – > 1.2 Mpkts/sec Dual 2GHz G5 MacOS X.
  – > 800Kpkts/sec Dual 2GHz Xeon Linux RH Enterprise

• Supporting Multiple OS’s
  – Linux, Unix, Solaris, IRIX, MacOS X, Windows XP
NTAS Architecture
NTAS Distributed Architecture
Unicast/Multicast QoS Monitor Strategies
Mixed Black-box White-box Approach
So, …, what is a flow?

• Classic 5-Tuple IP flow
• Encrypted VPN IP-Sec Tunnel
• MPLS based Label Switched Path (LSP)
• ATM Virtual Circuit
• PPP Association
• Routing Protocol Peer Adjacency
• Multicast Group Join Request/Reply
• Abstract Object <-> Abstract Object
And what metrics?

• Rate, Load, Bytes, Pkts, Goodput, Max Capacity
• Unidirectional? Bidirectional?
  – Connectivity, Reachability
  – RTT, One-way Delay
• Loss, Packet Size, Jitter, Retransmission Rate
• Protocol specific values (flags, sequence #)
• DS Code points
• TTL, Flow IDs
• Routing Flap Metrics
• Hello Arrival Rates
How Should They Be Transported

• Push/Pull?
• Reliable/Unreliable
• Unicast/Multicast
• Stream/Block/Datagram?
• Encrypted? Authenticated?
Argus

• Argus started 1990 – Georgia Tech
• Redesigned CERT/SEI/CMU – 1993
• Version 1.0 Open Source – 1995
  – Over 1M downloads
    • ~100,000 estimated sites worldwide
    • Unknown sites in production
• Supports 13 Type P and P1/P2 Flows
• 117 Element Attribute Definitions
  – http://qosient.com/argus/Xml/ArgusRecord_xsd/ArgusRecord.htm

10 October 2005
Argus Transport

• Pure Pull Strategy
  – Simplifies Probe Design

• Reliable Stream Transport (TCP)
  – Can support UDP/Multicast Datagram

• Supports TLS “On the Wire” Strong Authentication/Confidentiality
  – Probe Specifies Security Policy
Maybe Incompatible with IPFIX

- Template strategy can’t work with all the combinations of flow types supported.
- Distribution strategies make it even harder.
- Lack of identifiers to support flow objects
- Missing metric types.
- Vendor specific support is minimal
- Resulting in no motivation to adopt.

10 October 2005