endace
accelerated

Where's the money in investing for compliance?

endace – power to see all

endace
accelerated

europe
P +44 1223 370 176
E eu@endace.com

americas
P +1 703 964 3740
E usa@endace.com

asia pacific
P +64 9 262 7260
E asia@endace.com

technology
P +64 7 839 0540
E nz@endace.com

Presenter

Dan delaMare-Lyon

Channel Manager

Endace Europe Ltd

- 10 years experience in telecommunications industry from the grass roots network up to the delivery of complex products across the network.
- Prior to Endace:
  - International Network Engineering/Development - UUNET
  - Product Development and Marketing - MCI/Worldcom

This discussion covers how established commercially available technologies can be integrated to provide secure and separate access to network traffic for LI, while also enabling operators to garner useful information for WAN security and management. Operators can now generate a meaningful ROI on an asset base that would otherwise only serve for regulatory compliance.

Agenda

- The cost of compliance – case study
- Interested parties' concerns
- Vertically integrated systems offer a potential solution
- Building a scalable multi-purpose infrastructure
- Implementation
- Case study wrap-up
- Q&A

The cost of LI compliance

Case study

endace accelerated

- **Network size:** >1200 Cisco 12000 routers
  Transporting traffic from >50 million users
- **Network types:** OC-192, OC-48, OC-12, Gigabit Ethernet
- **Total number of monitoring nodes:** Thousands of links
- **Challenge:** How to record target 'data-in-motion' from anywhere in the network
- **Estimated cost to deploy LI boxes:** Totally unfathomable

"If we deploy all that equipment for LI, will there ever be a return on the investment?"

Interested parties' concerns

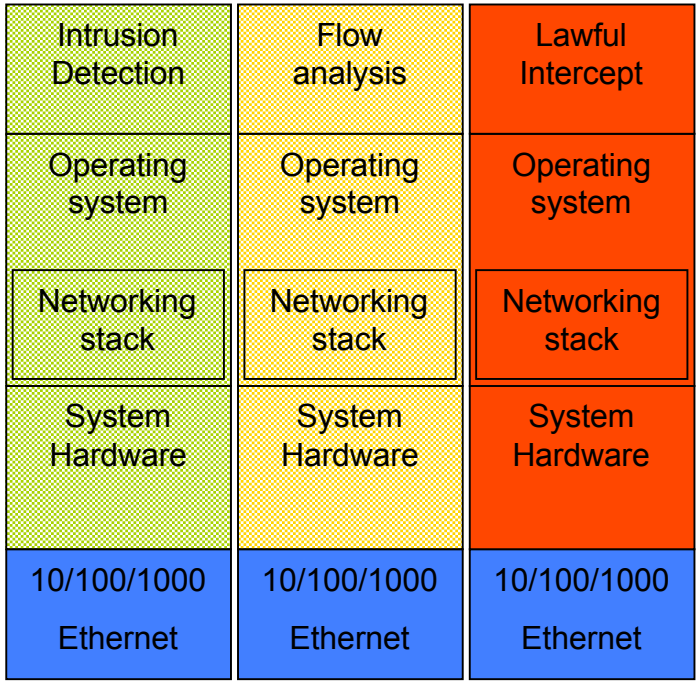
Constituency	End users / Subscribers	Carriers / Service Providers	Government / Law Enforcement
Concerns	♣ Privacy ♣ Service reliability ♣ Service cost/pricing ♣ Information security	♣ CapEx requirement ♣ Cost of deployment ♣ Ongoing OpEx and administration ♣ Interruption of service ♣ Hacks, DDoS, and other threats to service delivery	♣ Authorisation ♣ Security ♣ Effectiveness ♣ Responsiveness

Vertically integrated systems

From a network stack perspective

endace accelerated

Single-purpose systems



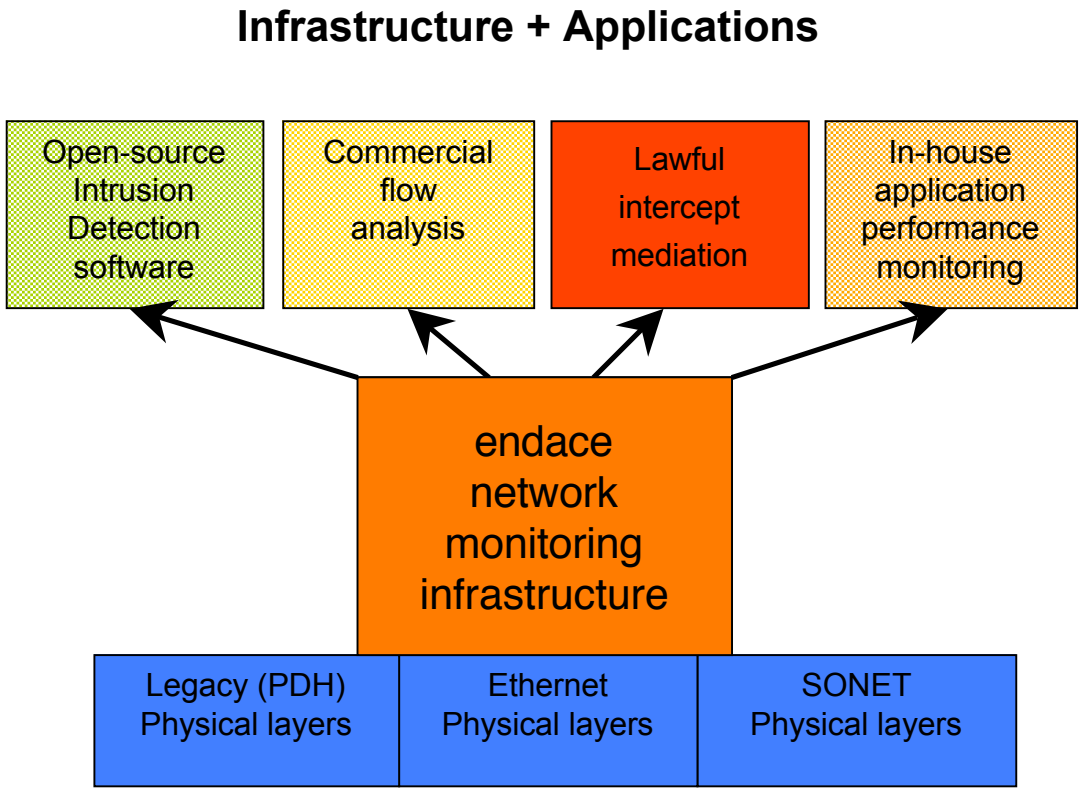
- Independent systems for Lawful Intercept ensure separation/security…
  … but the cost to implement capture equipment for this sole purpose is prohibitive.
- As most vendors focus on Gigabit Ethernet (for the volume market) it is not possible to tap legacy or SDH networks. Networks are rarely single wiretype.
- Vendors of vertically integrated systems will be forced to reengineer their solutions as network speeds scale to 10 Gigabit and beyond.
- Will picking one system vendor limit our ability to integrate with the necessary mediation layer(s) that are mandated by legislation/LEAs?

Building a scalable monitoring infrastructure

From a network stack perspective

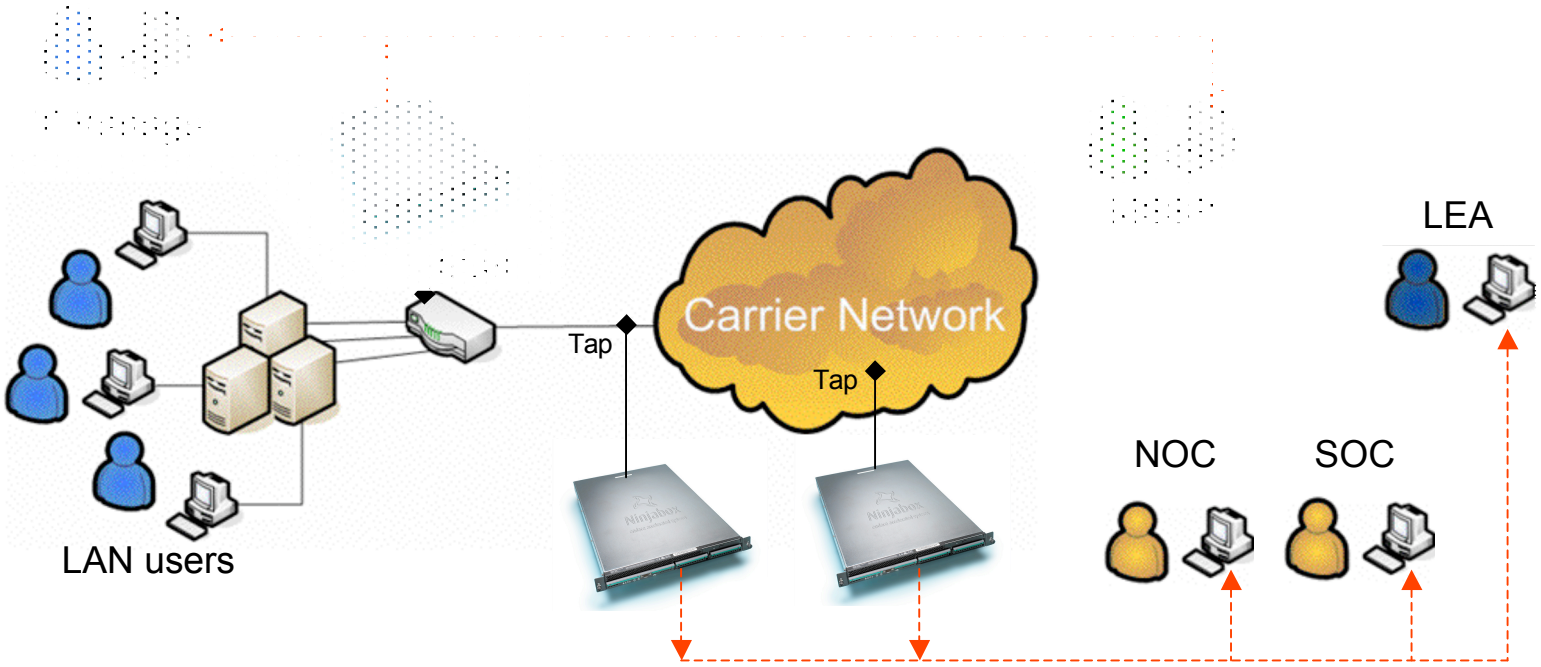
endace accelerated

- Internal network operations to intercept and record traffic are separated from the mediation layer(s). (ie. See ETSI model)
- The infrastructure is application-agnostic (any traffic analysis applications and LI mediation systems can be layered on top)
- Each analysis/intercept application is securely separated from the others.
- The infrastructure asset can be leveraged for the service provider's benefit also:
  - Manage service delivery
  - Offer revenue-generating security monitoring services



Building a scalable monitoring infrastructure

Deployment



- Provides support for a wide range of network types for network-wide coverage:
  - PDH: T1/E1, DS3/E3
  - Ethernet: 10/100/1000, 10 Gigabit
  - SONET/SDH: OC-3 to OC-192 (STM-1 to STM-64), and now OC-768/STM-256 (40G)

Implementation

endace
accelerated

Performed by Endace infrastructure	Performed by the applications
♣ Consistent full-line rate traffic recording ♣ Hardware-based traffic filtering ensures nothing is missed ♣ Precise timestamping (15 nanoseconds, synchronised by GPS to ~100ns) ♣ Interface with multiple applications concurrently, each with it's own separate traffic stream. ♣ Secure delivery of captured data to the mediation layer (and/or analysis applications) ♣ Provides an API for configuring the capture infrastructure from within the mediation/analysis software.	♣ User authorisation & warrant management. ♣ Provides 'front-end' user interface to the lawful intercept team. ♣ Send requests for intercepts to the infrastructure ♣ Store intercepted data and deliver it to the LEA.

Interested parties benefit

Constituency	End users / Subscribers	Carriers / Service Providers	Government / Law Enforcement
Concerns	♣ Privacy ♣ Service reliability ♣ Service cost/pricing ♣ Information security	♣ CapEx requirement ♣ Cost of deployment ♣ Ongoing OpEx and administration ♣ Interruption of service ♣ Hacks, DDoS, and other threats to service delivery	♣ Authorisation ♣ Security ♣ Effectiveness ♣ Responsiveness
Benefits	♣ Improved service price/performance ♣ Option of managed security services	♣ Monitoring is invisible to the network and its users ♣ Low cost to provide Lawful Intercept on top ♣ Leverage asset for multiple purposes/teams ♣ Offer managed security services generating new revenues	♣ Reliable intercepts with full packet data ♣ Once authorised, taps are activated very quickly

The cost of LI compliance

Case study

- **Network size:** >1200 Cisco 12000 routers
  Transporting traffic from >50 million users
- **Network types:** OC-192, OC-48, OC-12, Gigabit Ethernet
- **Total number of monitoring nodes:** Thousands of links
- **Challenge:** How to record target 'data-in-motion' from anywhere in the network
- **Estimated cost to deploy LI boxes:** Totally unfathomable

- **Solution:** Using Endace network monitoring infrastructure, lossless traffic capture is guaranteed at full line rate across a range of network types, network-wide.
- **Augmented solution for LI:** Adding the mediation layer from a leading LI vendor, the Endace monitoring probes are configured to record and securely deliver targeted traffic streams.

- **This is not the sole purpose!** The monitoring infrastructure is also leveraged by the in-house service performance monitoring team, and the Security Operations Centre.
- **Total cost:** Justifiable (US$ millions)
- **This project is presently being rolled out.**

Q&A

endace
accelerated