endace
accelerated

Why sample when you can monitor all network traffic inexpensively?

endace – power to see all

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

Using established commercially available technologies, anomaly detection systems and network intrusion detection systems can now be run losslessly at full line rate on telecommunications networks. Armed with 100% flow monitoring and deep packet inspection capabilities, peering partners' and top-talkers' traffic can be scrutinised in depth, and Network Managers can isolate threats to service performance.

Agenda

- ♣ In pursuit of knowledge
- ♣ Identifying the threats
- ♣ Existing (compromise) solutions
- ♣ Building a scalable monitoring infrastructure
- ♣ The Endace solution
- ♣ Application notes: Protocol Analysis & Lawful Intercept
- ♣ Q&A

In pursuit of knowledge

- You need to know what’s happening on your network
  - To identify information security breaches
  - To ensure application service performance levels
  - To serve national security

- Converged telecommunications networks carry many types of information:
  - Voice (H.323, SIP, Skype)
  - Video (H.263/264, MPEG-2/4)
  - Email
  - IM (instant messaging)
  - FTP
  - P2P (peer to peer)
  - Etc, etc…

- To remain competitive, network operators must control costs and serve users flawlessly. Managing the network to ensure service delivery becomes crucial.
- These networks provide rich intelligence for law enforcement, IF they can be accessed securely, and with high precision.

Identifying the threats

- ♣ Information Security
  - Detect port scans and hack attempts
  - Upon detection, record data to disk for evidence (and potential trace back)
  - Record traffic trace files for forensic analysis in case of failure

- ♣ Service Assurance
  - Measure network load and traffic types
  - Identify network bottlenecks and avoid affecting user experience
  - Ensure application servers are responding appropriately

- ♣ Lawful Intercept
  - Targetting known criminals for ‘probable cause’ or potentially usable evidence
  - Broader intelligence gathering in the interests of national security

Existing (compromise) solutions

endace
accelerated

- Flow records – eg. sFlow
  - Very useful for understanding traffic behaviour at a statistical level
  - But, router-based flow record generators sample traffic (often 1 in 1000 packets)
  - Based on this sample, flow information is inferred from a few packet headers
  - But this misses most of the information (None of the packet payload is inspected!)
  - When routers get heavily loaded they drop non-essential services –

- Router/Switch Based Services
  - Like flow records LI is added on top of the core functionality of the device
  - Limited capabilities to gather data - often just a limited amount of hosts/traffic can be secured
  - When routers get heavily loaded they focus on maintaining the network rather than the LI data

- Portable analysis units
  - Expensive per unit
  - Often provide only Gigabit Ethernet support
  - Time to activate an intercept is often too long as the unit must be physically deployed
  - Not usable for intelligence gathering or network management tasks
  - Security/privacy may be compromised as a single user has access to the hardware and the protocol decode functions.

Building a scalable monitoring infrastructure

- We have 1 underlying network
- We need to be able to see the traffic on it for many reasons – multiple teams focus on service delivery, security, lawful intercept... User/Engineers’ authorisation levels are different.
- In some cases, deep packet inspection and session reassembly is necessary
- Using many independent systems becomes costly
  - Expensive to purchase and depreciate
  - High management, patching, and upgrade costs
- A manageable, network-wide solution is required for full visibility
- It must integrate with our legacy network types near the ‘edge’ while providing a future-proof path as we scale to 10 Gigabit and beyond.

Building a scalable monitoring infrastructure

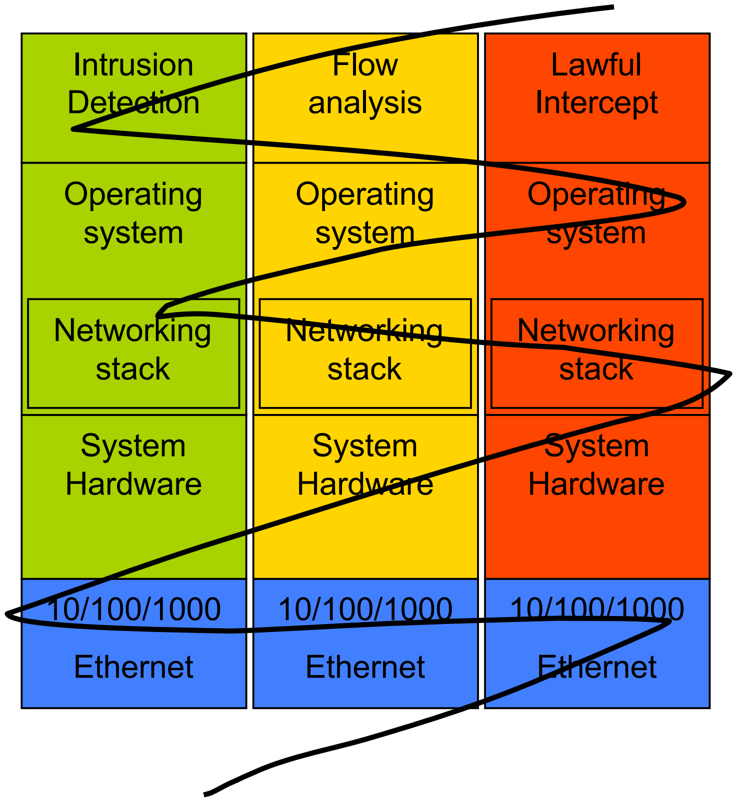
From a network stack perspective

endace accelerated

Speeds are increasing:

… can existing solutions keep pace?

Single-purpose systems



Intrusion Detection | Flow analysis | Lawful Intercept

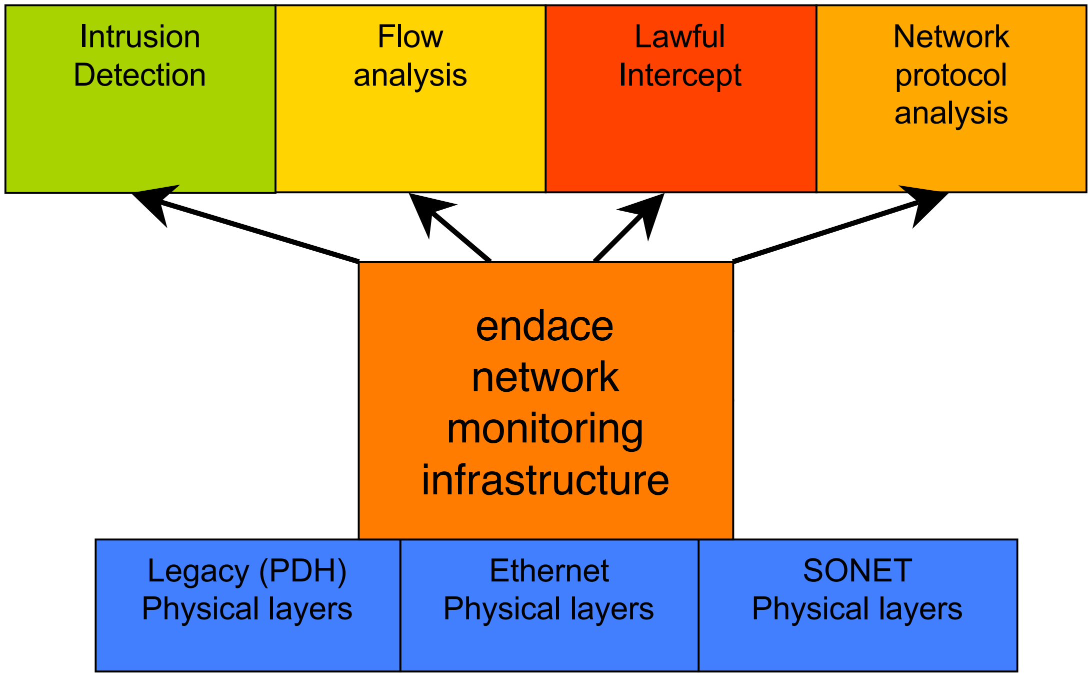
Operating system | Operating system | Operating system

Networking stack | Networking stack | Networking stack

System Hardware | System Hardware | System Hardware

10/100/1000 Ethernet | 10/100/1000 Ethernet | 10/100/1000 Ethernet

Infrastructure + Applications



Intrusion Detection | Flow analysis | Lawful Intercept | Network protocol analysis

endace network monitoring infrastructure

Legacy (PDH) Physical layers | Ethernet Physical layers | SONET Physical layers

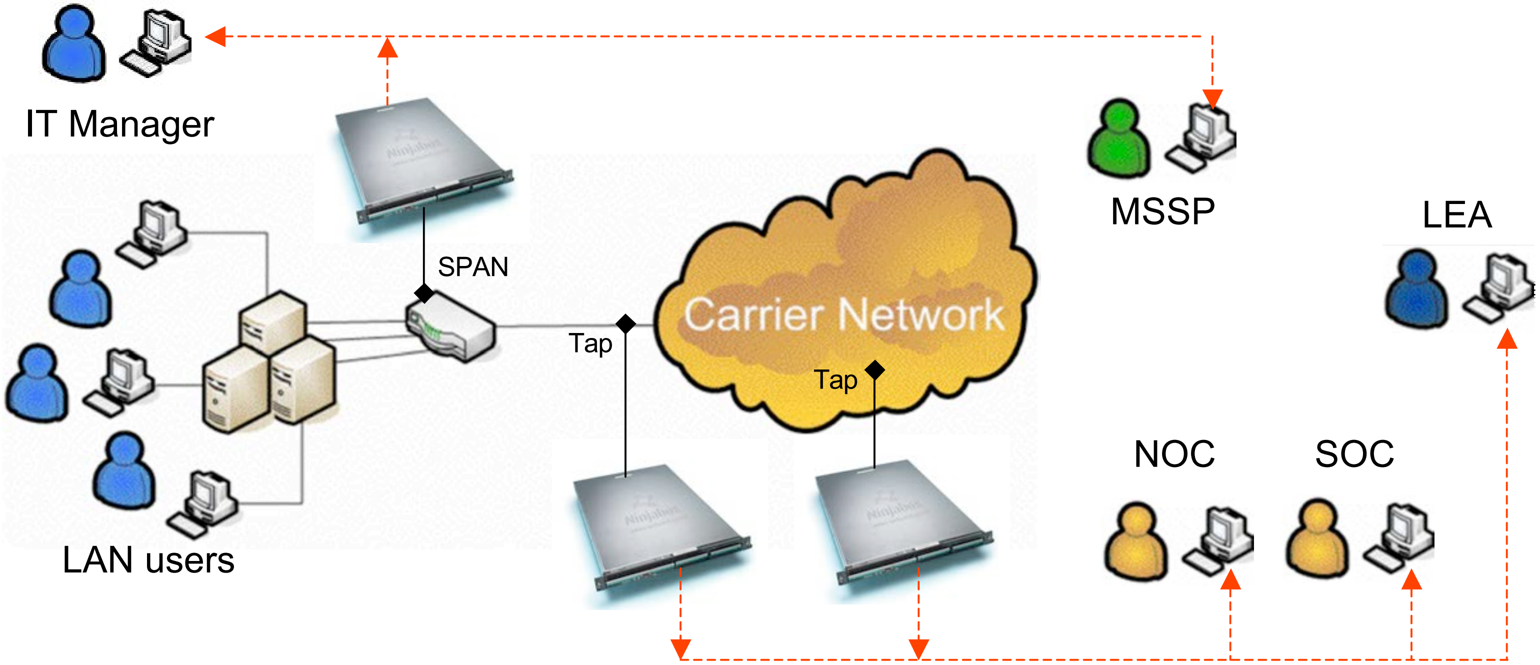
The Endace solution

- 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)
- Multiple applications can run on top of the common monitoring infrastructure.
  - Designed for distributed deployment: manageability and upgradeability
  - Secure multi-user access
  - Lowest total cost of ownership
- Standards-based application interfaces enable usage of existing analysis tools, whether commercial or open-source.
- The solution enables much deeper levels of traffic inspection:
  - Generate flow records based on every single packet (integrating immediately with existing analysis and reporting tools)
  - Record full packet payload to disk for archiving and evidence
  - Filter traffic at full line rate for targetted traffic capture (eg. Lawful Intercept)
  - Run deep packet inspection software (eg. Intrusion Detection) at full line rate in many areas of the network (edge, core, peering points)

The Endace solution

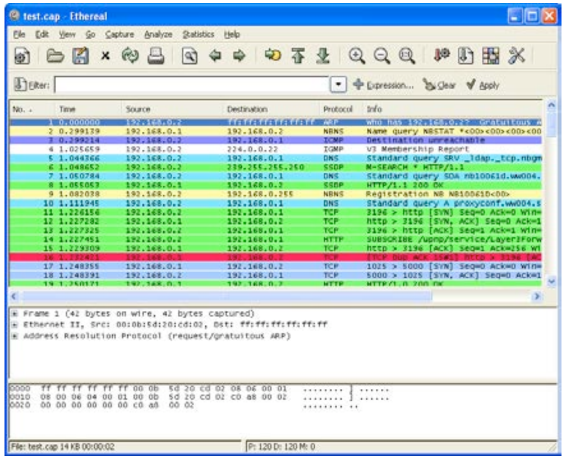
Endace Ninja appliances deliver a scalable monitoring infrastructure for a wide array of real-time and historical analysis applications.

- Full line rate flow analysis – eg. NarusInsight
- Security monitoring with TCP/UDP session reassembly – eg. Snort® IDS
- Protocol decode and analysis – eg. Wireshark (Ethereal)
- Lawful Intercept – Filtered capture, interfacing with mediation layer – eg. Verint



Application note: Protocol Analysis

- Wireshark (Ethereal) is open source software.
- It is a tool used widely by those managing or deploying networks.
- It has leading-edge protocol support – often in advance of commercial tools.
- The Endace value-add for Wireshark:
  - Capture performance: Wireshark has limited capture performance – Endace monitoring infrastructure ensures that the application has 100% of the relevant traffic to analyse.
  - Pre-filtering: Different filters can be set to capture only required data, reducing the complexity and time of analysis e.g. communications between specific hosts on a network or the Internet.
  - Historical analysis: Endace monitoring infrastructure can store days of traffic data allowing forensic analysis of past events.
  - Interface options: Most current Wireshark users employ commodity Ethernet NICs. The Endace solution guarantees lossless operation and adds support for SONET network types so that Wireshark can be used for carrier networks also.



```
No. .   Time      Source        Destination        Protocol Info
   1 0.000000  192.168.0.2   ff:ff:ff:ff:ff:ff  ARP      Who has 192.168.0.2?  Gratuitous A
   2 0.299139  192.168.0.1   192.168.0.2        NBNS     Name query NBSTAT *<00><00><00><00
   3 0.299214  192.168.0.2   192.168.0.1        ICMP     Destination unreachable
   4 1.025659  192.168.0.2   224.0.0.22         IGMP     V3 Membership Report
   5 1.044366  192.168.0.2   192.168.0.1        DNS      Standard query SRV _ldap._tcp.nbgm
   6 1.048652  192.168.0.2   239.255.255.250    SSDP     M-SEARCH * HTTP/1.1
   7 1.050784  192.168.0.2   192.168.0.1        DNS      Standard query SOA nb10061d.ww004.
   8 1.055053  192.168.0.1   192.168.0.2        SSDP     HTTP/1.1 200 OK
   9 1.082038  192.168.0.2   192.168.0.255      NBNS     Registration NB NB10061D<00>
  10 1.111945  192.168.0.2   192.168.0.1        DNS      Standard query A proxyconf.ww004.s
  11 1.226156  192.168.0.2   192.168.0.1        TCP      3196 > http [SYN] Seq=0 Ack=0 Win=
  12 1.227282  192.168.0.1   192.168.0.2        TCP      http > 3196 [SYN, ACK] Seq=0 Ack=1
  13 1.227325  192.168.0.2   192.168.0.1        TCP      3196 > http [ACK] Seq=1 Ack=1 Win=
  14 1.227451  192.168.0.2   192.168.0.1        HTTP     SUBSCRIBE /upnp/service/Layer3Forw
  15 1.229309  192.168.0.1   192.168.0.2        TCP      http > 3196 [ACK] Seq=1 Ack=256 Wi
  16 1.232421  192.168.0.1   192.168.0.2        TCP      [TCP Dup ACK 15#1] http > 3196 [AC
  17 1.248355  192.168.0.1   192.168.0.2        TCP      1025 > 5000 [SYN] Seq=0 Ack=0 Win=
  18 1.248391  192.168.0.2   192.168.0.1        TCP      5000 > 1025 [SYN, ACK] Seq=0 Ack=1
  19 1.250171  192.168.0.1   192.168.0.2        HTTP     HTTP/1.0 200 OK
```

```
⊞ Frame 1 (42 bytes on wire, 42 bytes captured)
⊞ Ethernet II, Src: 00:0b:5d:20:cd:02, Dst: ff:ff:ff:ff:ff:ff
⊞ Address Resolution Protocol (request/gratuitous ARP)
```

```
0000  ff ff ff ff ff ff 00 0b  5d 20 cd 02 08 06 00 01   ........ ] ......
0010  08 00 06 04 00 01 00 0b  5d 20 cd 02 c0 a8 00 02   ........ ] ......
0020  00 00 00 00 00 00 c0 a8  00 02                     ........ ..
```

File: test.cap 14 KB 00:00:02 | P: 120 D: 120 M: 0

Application note: Lawful intercept

endace
accelerated

- ♣ With a network-wide infrastructure for network monitoring, LI functions can be layered on top, along with the carriers' network management applications.
- ♣ Requests for traffic intercepts are authorised and controlled by the mediation layer, which sends a secured SNMP request to the monitoring appliances. These return captured traffic by a secure IP tunnel.
- ♣ The Endace value-add:
  - Fast and secure: Upon authorisation, implementation of an intercept is immediate and costless, plus delivery of the data secure.
  - Lossless operation: Full line rate performance guarantees that nothing is missed.
  - Lowest TCO: The same infrastructure is leveraged for Lawful Intercept, while being separated from the carrier's internal network monitoring applications. Being vendor agnostic means the system is also shielded from reliance on vendor provided solutions – grow the network without having to replace the complete monitoring system.
  - Privacy via operational separation: Individuals that install the hardware are separated from those that can configure a traffic intercept.
  - **Benefits the carrier:** Detailed information about threats

Q&A time