Network Flow Monitoring

Luca Deri <deri@ntop.org>

Flow Monitoring: Requirements

- Custom Flow Definition (à la NetFlow V9)
- (Really) Open Flow Specification
- Ability to provide (initial) payload access (useful for protocol decoding)
- Flow Compression (save space dramatically)
- Non Repudiation of Flows (via MD5 digest)
- MPLS/VLAN/IPv6 Information in Flows

Flow Monitoring: Optional Features

- Application/Network Performance (use flows also for performance measurement).
- Support for connection oriented/connectionless transport.
- Flow Encryption (a secure channel as SSH/SSL should provide this).
- Ability to access hardware addresses (e.g. MAC addresses) on flows

Flow Monitoring: What to Avoid

- No Flow Templates (make Collector's Life Hard)
- Definition of a Protocol Collector -> Probe for instrumentation

A New Flow Protocol: nFlow

nFlow (http://www.nflow.org)

- Open Specification
- Free Probe/Collector Available
- Based on NetFlow V9
- Security (non repudiation)
- Flow compression (gzip)
- MPLS/VLAN/IPv6 information
- Payload information
- Application/network performance.