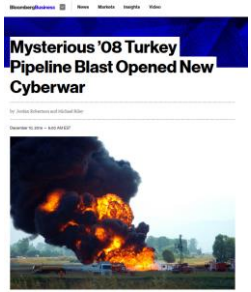
NOKIA

Impregnable network defense for a porous world

Hansen Chan
Product Marketing
IP and Optics Networking

Porous defense leads to fatal and costly incidents



[Turkey pipeline blast report 2014]

[Arizona fiber trunk vandal 2015]

[Ukraine grid down 2015]

[Bangladesh Central Bank cyber bank heist 2016]

NOKIA

Threats to industrial networks accident, error or malice

Deliberate threats

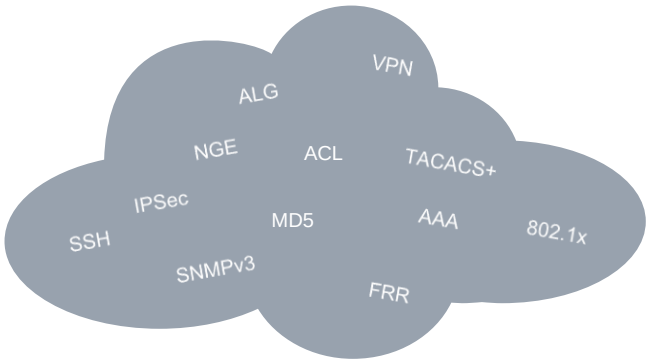
- Disgruntled employees
- Identify theft
- Sabotage
- Espionage
- Vandalism
- Terrorism
- Malware
- Theft
- Denial-of-service

Inadvertent threats

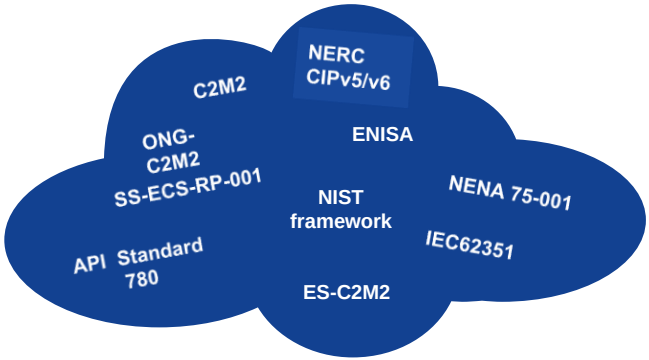
- Safety failures
- Equipment failures
- Carelessness
- Misconfiguration
- Fire
- Natural disasters

The security numeric and alphabet soup

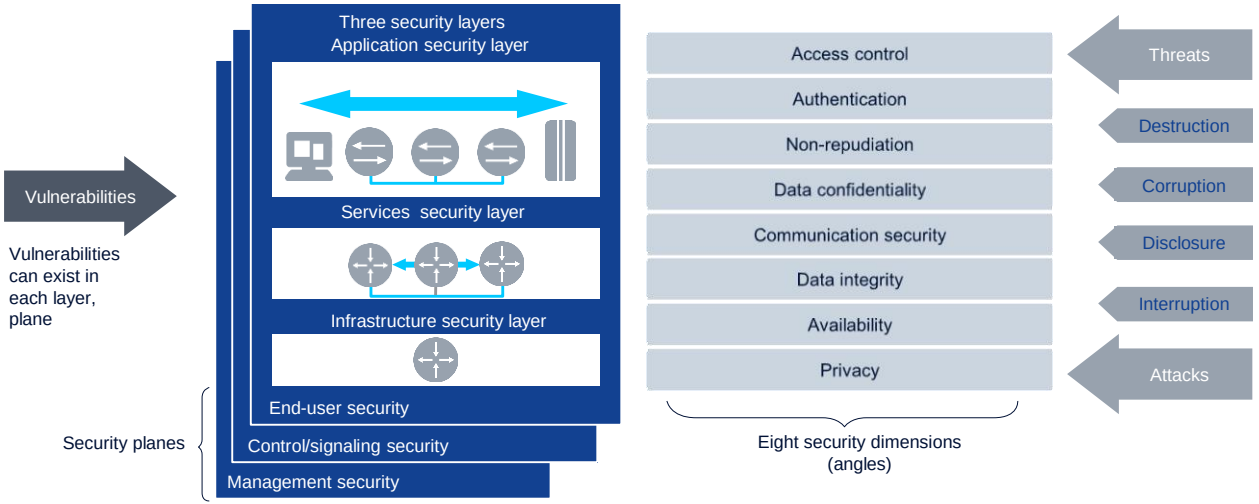
Security toolbox



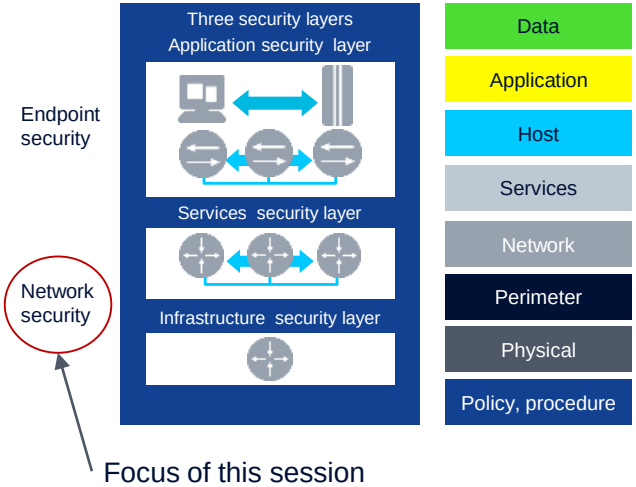
Industry security frameworks/guidelines



ITU-T X.805 communications (network) security framework



An X.805-based In-depth network defence

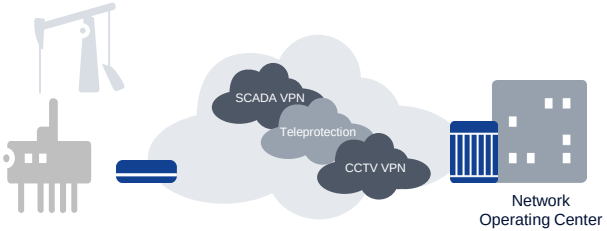


Network defense mechanism highlights

X.805 layer	Defense highlights
Services layer	• Service encryption protects application traffic • Firewall/NAT shields endpoints • Access control list inspects traffic
Infrastructure layer	• Control plane (IP/MPLS/L2) security • Management security • Layer 1 encryption to protect all network data • Network availability, reliability and resilience to withstand network attack and sabotage • Secure node authentication protects against network equipment assault

Inherent strong security of IP/MPLS

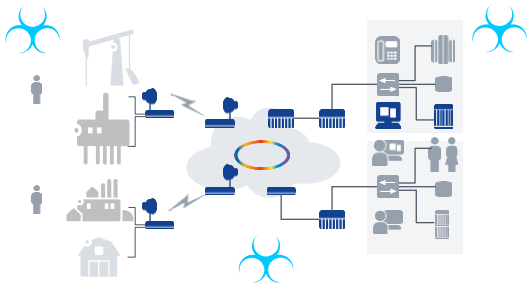
LSP-based transport renders security at par with frame relay/ATM VC



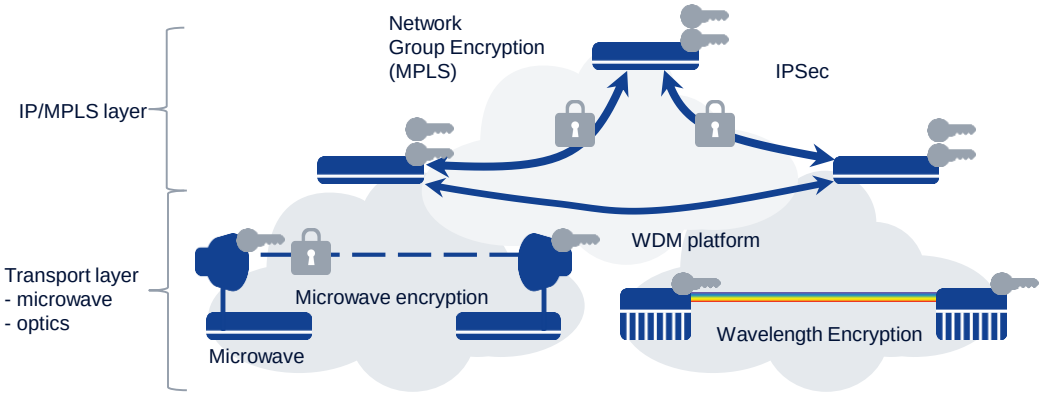
MPLS-based VPNs segregate control and data plane of each application zone

But attacks are becoming rampant and sophisticated

Stakes are higher than ever



Encrypt critical communications with a best-fit approach



A multi-layer encryption framework

Critical network service encryption requirements

Universal encryption

- Encrypting multi-service (TDM, layer 2 and IP) at MPLS layer
- Service aware, optimizing hardware performance
- Full MPLS advantages (FRR, QoS, OAM, scalability)

Meshed persistent connectivity

- Scale up for large meshed networks
- Persistent connectivity
- Ready the network for future distributed application/IoT intelligence

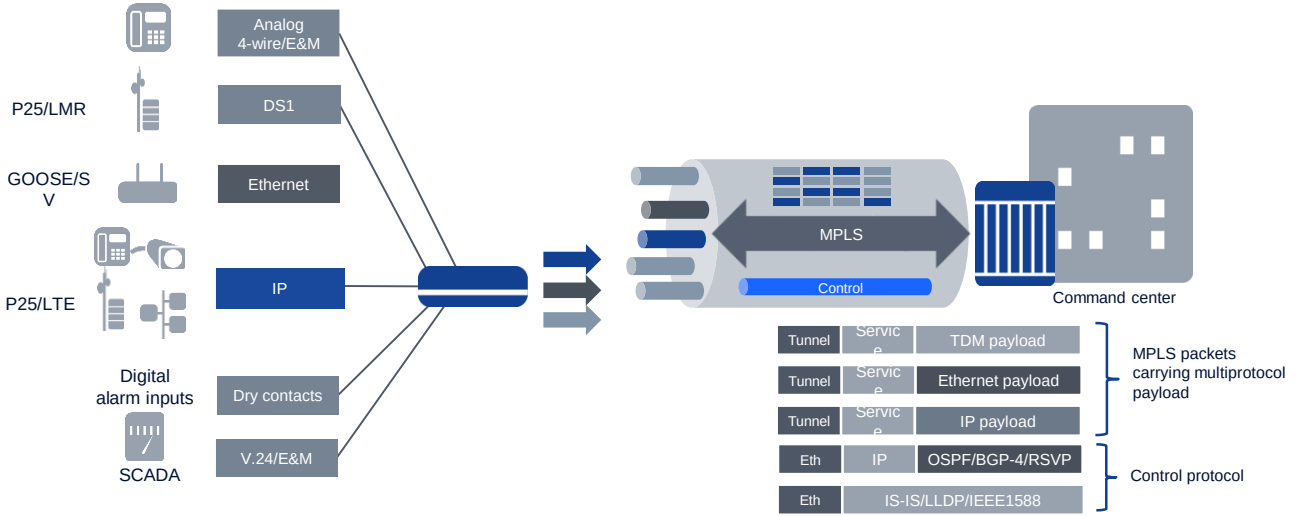
Robust key management

- Elegant service-based hierarchical group key management
- Secure key distribution and hitless re-keying
- No extensive IPsec compute tax

High network efficiency

- Optimal use of hardware resources
- Low packet overhead
- Transparent to core network

Understand traffic in the network - service traffic and control traffic

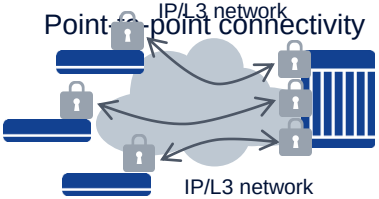


But how to secure multiprotocol traffic?

Universal encryption approach with service encryption

Traditional IPSec

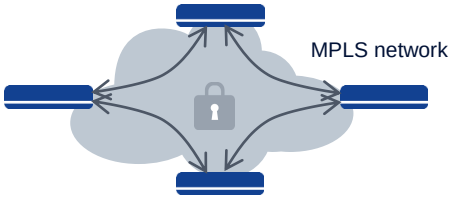
Point-to-point connectivity



- Tunnel based approach designed primarily for IP/L3 services
- PE-PE configuration considerations needed
- Multiple keys managed by IKEv2
- Some added overhead (GRE, IPSec headers and IKE control plane)

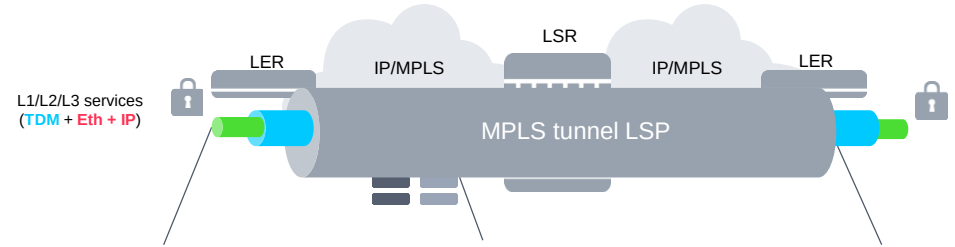
Service Encryption

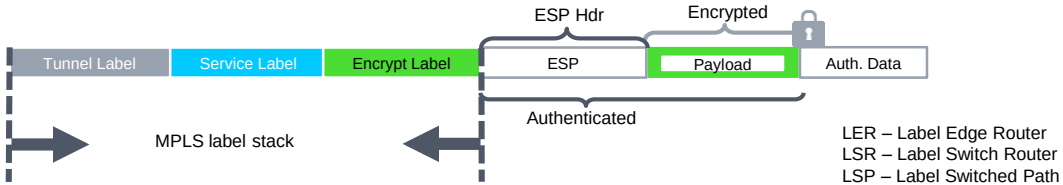
Persistent meshed connectivity



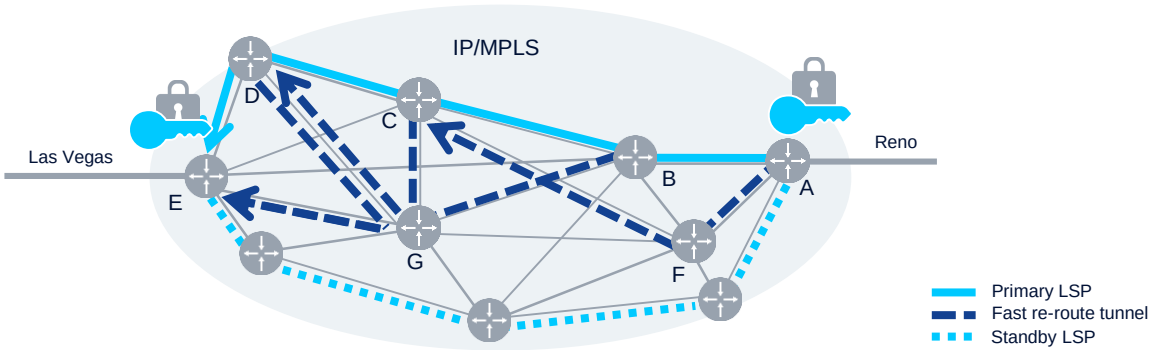
- MPLS-based/service aware group encryption
- Supports all service types over MPLS:
  - P2P and multi-point TDM, Ethernet and IP VPNs
- Leverage seamless MPLS and high availability
- Lower overhead and less complex

Service encryption added to MPLS seamlessly





Service encryption with MPLS resiliency



Standard LSP failover

- Failure signaled at Ingress LSR
- Calculate and signal new LSP
- Reroute traffic to new LSP

Standby LSP

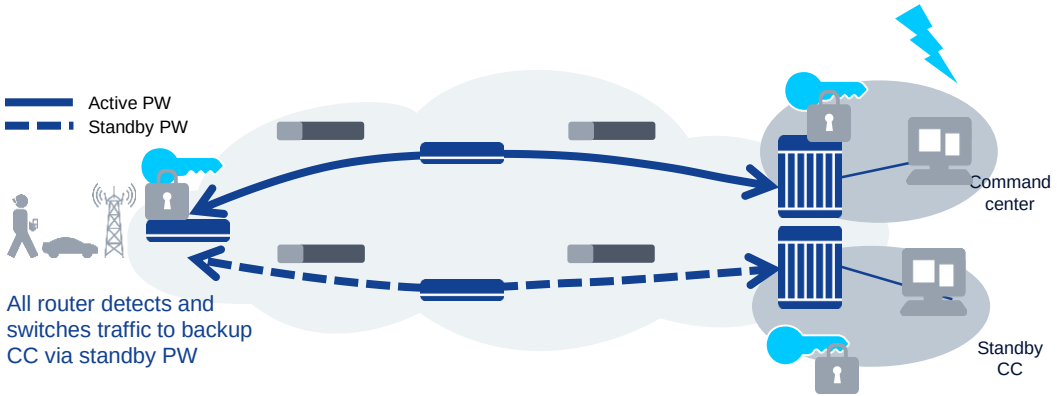
- Pre-established LSP
- Sub-second switchover

Fast Re-Route (FRR)

- Signaled during LSP setup as topology requires
- Each LSR computes a detour path
- Supports failover in < 50 ms after detection

Same key regardless of which protecting LSPs are in use

Service encryption with geo-redundancy



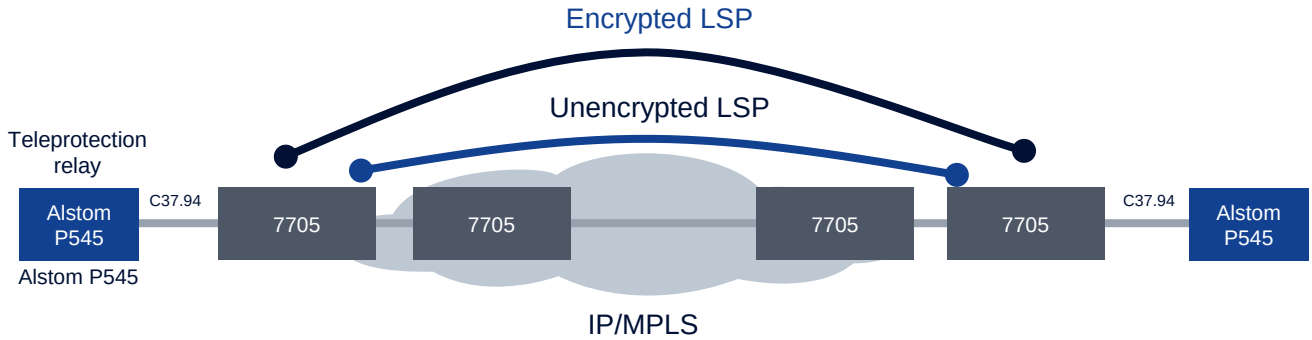
All traffic is lost due to site disaster

A pair of geo-redundant command centers

- Pseudowire redundancy protects end-to-end connections
  - Protection against end-point failure at control center (router, control center building etc.)
  - All remote routers switches automatically without manual intervention
  - Multi-Chassis Synch (MCS) maintains flow/group/link state information across routers

Control center site protection against disaster with same key

Independent service encryption delay measurement



A. E2E delay without encryption = 1.68 ms
B. E2E delay with service encryption = 1.70 ms

Incurred end-to-end delay is only 20 US

Mitigating management security risk

Role-based user profiles

Based on each user's role in network operations, only

- grant visibility of the relevant network span (span of control), and
- empower germane network command capability (scope of command)

User action non-repudiation

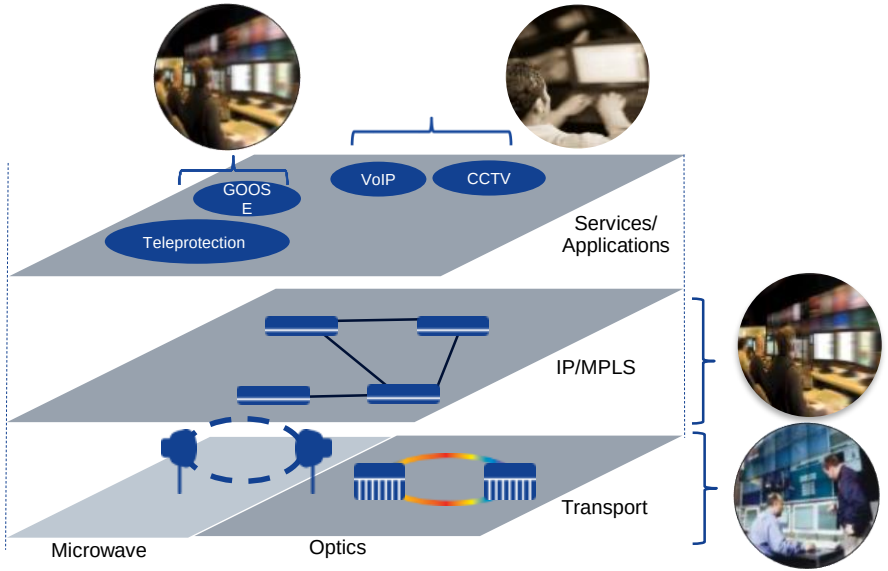
- Through logging, each user's every action is recorded
- Archive for future analysis and audit

Workflow checkpoint

- When creating, deleting and modifying services, insert checkpoints to verify validity

NOKIA

Role-based user profiles – minimize security exposure

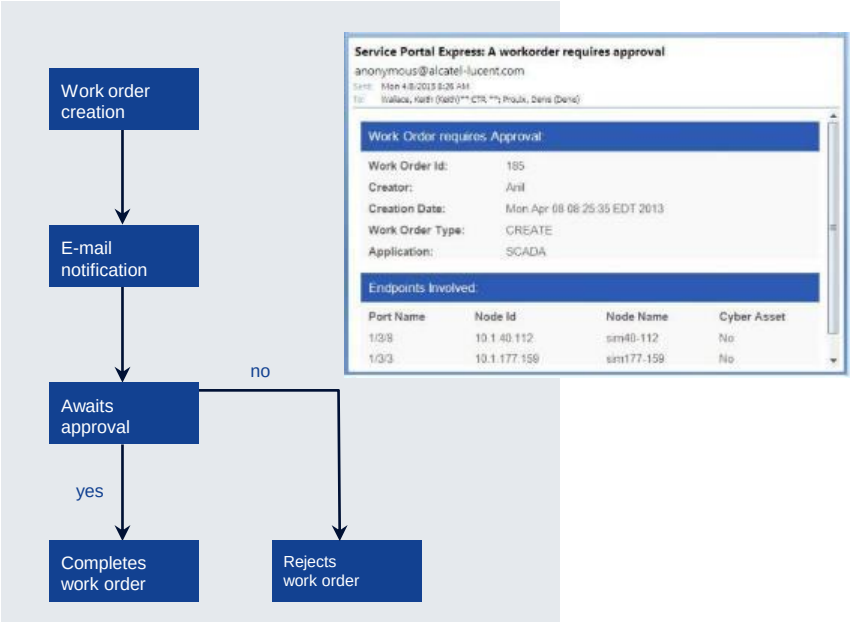


Span of control/scope of command

- Give staff only necessary control according to their jobs
- Reduce risk of operation error

Workflow checkpoint

- Email notification to supervisor for approval
- Work Order States:
- Pending Approval,
- Approved,
- Rejected,
- Withdrawn,
- Completed,
- Failed



Deploy network security with no performance compromise

Centralized policy creation and update

Security processing in forwarding hardware

MPLS QoS and performance preserved

Negligible latency incurred

NOKIA

Nokia network security resources

Whitepapers

- Impregnable defense for mission-critical networks (download here)
- Encryption for mission-critical networks (download here)
- Network Group Encryption (download here)
- 7705 SAR security overview for mission-critical industries (download here)

Article

- Mission possible with Network Group Encryption (NGE)

NOKIA

NOKIA