



IPv6 Deployment in NATO

presented at the

French IPv6 Worldwide Summit

Tuesday 14th November 2006

Rob Goode

NATO Consultation, Command and Control Agency

+31 (0)70 374 3481, Rob.Goode@nc3a.nato.int



Deployment drivers for IPv6

- **Maintain and improve interoperability**
 - National IPv6 transition (Alliance and Partners)
 - NATO Network Enabled Capability (NNEC)
- **Take advantage of IPv6 capabilities**
 - Address space
 - Mobility
 - Auto-configuration
- **Stay in line with commercial developments**
 - Use standards-based COTS products with low cost of ownership and good upgrade path

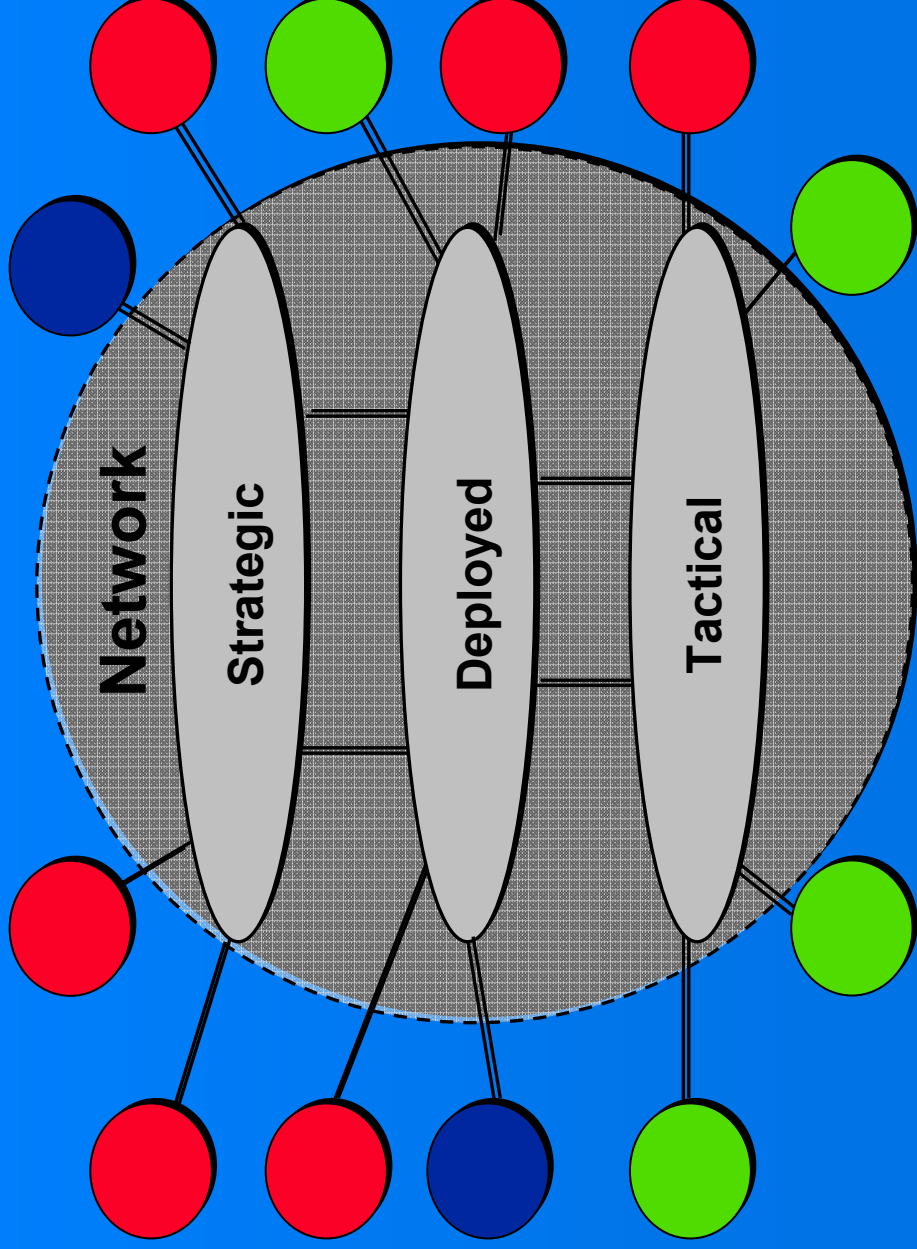


NATO network enabled capability

- **Improve operational effectiveness through the federation of capabilities**
 - **Synergy of contributed forces**
- **Service-oriented architecture over ubiquitous unclassified IP network**
 - **Seamless connectivity**
 - **Everything over IP**
 - **Information discovery**
 - **Scalability**



Multiple Domains over Seamless IP Backbone





IPv6 Deployment Requirements

- **Operational infrastructure requires:**
 - **Unbroken availability and interoperability during transition**
 - **Fully functional and pre-tested IPv6 systems**
 - **Transition mechanisms that “just work” for networked applications**
 - **Provider-independent globally de-conflicted addresses**
- **System-wide security assessment and guidance**
 - **Network complexity and network management**
 - **Security devices – gateways/guards/crypto/IDS**
- **IPv6 Conformance**
 - **Require NATO standard definition**
 - **Support NATO procurements**



Deployment: transition

- **Maintain IPv4 during transition**
- **Evolutionary approach: first tunnels then dual stack**
- **No network translation. Might require application-level gateways**
- **Network services required before applications can deploy (DNS, network management, firewalls, etc.)**
- **Each application has own deployment timeline**



Deployment: security

- **New code means possible new weaknesses**
- **Dual stack may allow cross-stack attack**
- **Require IPv6 versions of network security devices (firewalls, encryption, etc.)**
- **New features mean new threats (auto configuration; mobility; anycast; etc.)**



Deployment: network management

- **Network management system requirements:**
 - IPv6 version of management suite
 - Automated address space management
 - Manage IPv6 transition mechanisms, gateways, applications
- **Manage multiple inter-dependent networks**
 - IPv4 and IPv6 networks
 - RED virtual private networks over BLACK WAN
- **Challenge**
 - Holistic network management



Deployment: applications

- **Core area services**
 - Electronic mail; web; directory
 - Cannot have “flag day”; need incremental update
- **Functional are services**
 - Command and Control; Logistics; Intel; etc.
 - Transition on case-by-case basis
- **Challenge**
 - Avoid service interruptions



Deployment: timeline

- **Requirements**
 - IPv6 policy
 - Network transition plan
 - IPv6 network management
 - IPv6 security devices
 - Core area services transition plan
 - Transition plan for each functional area service
- **Drivers**
 - National transition timelines
 - Commercial support for IPv6 (and IPv4)
- **Challenge**
 - Not too early, not too late



Thank you for listening!

Questions?



CONTACTING NC3A

NC3A Brussels

Visiting address:

Bâtiment Z
Avenue du Bourget 140
B-1110 Brussels
Telephone +32 (0)2 7074111
Fax +32 (0)2 7078770

Postal address:

NATO C3 Agency
Boulevard Leopold III
B-1110 Brussels - Belgium

NC3A The Hague

Visiting address:

Oude Waalsdorperweg 61
2597 AK The Hague
Telephone +31 (0)70 3743000
Fax +31 (0)70 3743239

Postal address:

NATO C3 Agency
P.O. Box 174
2501 CD The Hague
The Netherlands

