

<b>JSP 602 Instruction</b>	1023	<b>Applicability</b>	Applications, Infrastructure, Network/Communications
<b>Configuration Identity</b>	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-16	<b>Epoch Applicability</b>	2005 - 2009

## **JSP 602: 1023 - Domain Naming and IP Addressing**

### **Outline**

*Description:* Domain Naming and IP Addressing policy covers the protocols, standards and rules for the provision of IP address allocation and name resolution services across the GII. It also covers the common infrastructure service identification schema that is used for resource location.

*Reasons for Implementation:* Modern computer systems and networks identify resources (such as devices, people and services) using logical names, which are mapped to physical addresses. Setting a coherent policy on naming and addressing is critical to the delivery of all infrastructure services throughout the GII.

*Issues:* None.

*Guidance:* This policy is consistent with the e-GIF and the NC3TA.

All projects should follow the guidance provided in JSP 457 The Defence Manual of Interoperable Network and Enabling Services, Volume 1 Common Network Services.

## Policy

### Strategic

#### **1023.01: Network Name Services**

**1023.01.01** Systems and/or projects that provide network domain name services shall implement the standards defined within JSP 457 - The Defence Manual of Interoperable Network and Enabling Services, as follows:

**1023.01.01.01** DNS(IETF STD 3, 13:1987)

**1023.01.01.02** Additionally the implementation shall be in accordance with the Internet Systems Consortium's BIND v9.2.x or later ([www.isc.org](http://www.isc.org)).

*Comment:* If implementations cannot upgrade to BINDv9.2.x then at a minimum the DNS should provide a standard or capability equivalent to BINDv8.2.2 fully patched - this allows for multi-mastering and both zone delegation and forwarding. If the DNS is implemented as an embedded capability within the OS it must be presented as a BIND compliant service at the boundary of this system.

*These are ubiquitous internet standard protocols for providing, sharing and federating name services within networks.*

#### **1023.02: Supernetting and Subnetting**

**1023.02.01** All Systems and/or projects providing local, metropolitan or wide area networking services shall implement the standards defined within JSP 457 - The Defence Manual of Interoperable Network and Enabling Services, as follows:

**1023.02.01.01** CIDR(RFC 1519:1993)/VLSM

*Necessary to support super-netting/sub-netting.*

#### **1023.03: IP Address Allocation**

**1023.03.01** All IP address ranges used within networks and systems shall be allocated by DINSA.

*DINSA are the MOD authority for domain naming and IP address allocation.*

*Comment:* Whereas DINSA will allocate address ranges to systems, the allocation of IP addresses within system boundaries should typically be performed using a DHCP service.

#### **1023.04: Common Infrastructure Service Identifiers**

**1023.04.01** All systems and/or projects shall implement the service naming and addressing rules as defined in JSP 457 - The Defence Manual of Interoperable Network and Enabling Services.

*JSP 457 provides the naming and addressing principles and rules to be used throughout MOD infrastructure. It also provides implementation guidance for naming and addressing services.*

### Deployed

As for Strategic domain.

## **Tactical**

### **1023.05: Network Name Services**

As for Strategic domain.

### **1023.06: Supernetting and Subnetting**

1023.06.01 Nothing is mandated in this area.

*Comment:* Where networks are likely to be mobile it is not practical to mandate policy for super-netting and sub-netting. Whereas it is preferable to make the IP addressing structure fit the network topology, as subnets move it is more practical in the short term to manage mobility by accepting the additional routing overheads that ensue. In the long term, however, mobility will increase the routing overheads to unacceptable levels, hence it may be preferable to re-address all network elements thus making the IP address structure once again match the network topology. It is impractical, therefore, to mandate these network management decision points as they will largely be governed by the nature and state of the operations being undertaken.

### **1023.07: IP Address Allocation**

**1023.07.01** All IP address ranges used within networks and systems shall be allocation by DINSAs.

*DINSAs are the MOD authority for all IP address allocation.*

**1023.07.02** Private address ranges shall not be used unless specifically authorised by DINSAs.

*Systems that cannot use the MOD class A address (25.x.y.z) must use private addresses (e.g. 10.x.y.z) internally and translate between its internal IP addresses and the IP addressing scheme used within the wider MOD infrastructure.*

*Comment:* No Private IP addresses (e.g. 10.x.y.z) must ever be routed over public networks (i.e. networks outside of MOD's control) if such addresses are exposed to MOD's routing network. Neither should Private IP addresses be advertised as service points or routes.

### **1023.08: Common Infrastructure Service Identifiers**

**1023.08.01** All systems and/or projects shall implement the service naming and addressing rules as defined in JSP 457 - The Defence Manual Of Interoperable Network and Enabling Services.

*JSP 457 provides the naming and addressing principles and rules to be used throughout MOD infrastructure. It also provides implementation guidance for naming and addressing services.*

## **Remote**

As for Strategic domain.

## **Responsibility for Implementing the Policy**

Implementation of this policy shall be the responsibility of all MOD projects (and their suppliers) that provide and/or use domain naming and IP addressing services within the GII.

## Procedure

Naming, Addressing and Registration Guidance can be obtained through the DCSSA DINSA Helpdesk: DCSA DINSA-Helpdesk(DII/C), [dcsadinsa-helpdesk@mod.uk](mailto:dcsadinsa-helpdesk@mod.uk) (Internet) ([dcsadinsahelpdesk@mod.uk](mailto:dcsadinsahelpdesk@mod.uk) )

## Relevant Links

JSP602 1013 – Internetworking

JSP457 The Defence Manual Of Interoperable Network and Enabling Services can be found here (not yet available). (<http://www.ams.mod.uk/>)

The DINSA web site can be found here (RLI only). (<http://www.dinsa.r.mil.uk/>)

Details of RFCs listed can be found here. (<http://www.rfc-editor.org/rfcsearch.html>)

Details of IETF standards listed can be found here. (<http://www.apps.ietf.org/rfc/stdlist.html>)

A glossary of terms and abbreviations used within this document is available here.

Instructions on how to read a JSP602 leaflet are available here.

## Compliance

Stage	Compliance Requirements
<b>Initial Gate/DP1</b>	MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s).
<b>Main Gate/DP2</b>	MOD Projects shall reference in their SRD (and MODAF technical views) the specific policy elements contained within this leaflet that are applicable to the system, equipment or application they are procuring or updating.
<b>Release Authority/DP5</b>	MOD Projects (supported by their equipment suppliers) shall provide evidence of their compliance with the elements of this policy defined within the SRD (and MODAF technical views). Evidence of conformance with standards shall be presented; sources of evidence may include: conformance/compliance certificates provided by equipment suppliers (e.g. under type approval or other assessment regimes), demonstrations, inspection, analysis, tests carried out by suppliers (e.g. Factory Acceptance Tests) and tests carried out at Defence Test and Reference Facilities.