JSP 602 Instruction	1021	**Applicability**	Infrastructure, Network/Communications
Configuration Identity	Version: 01.01 Reviewed: 2006-06-22	**Epoch Applicability**	2005 - 2009

JSP 602: 1021 - MOD LAN/ WAN to External WAN

Outline

Description: This policy leaflet covers the sub-network standards (including physical and logical (Link and Network) layers) that shall be implemented by all WANs within the GII in order to connect to external WANs. Where the purpose of the WAN-to-WAN connection is to connect end-systems using IP, the reader is referred to the networking standards as define within JSP602: 1013 - Internetworking. Systems are able to offer IP services over all of the sub-networks described in this section.

This policy also identifies the principal provider of external WAN connectivity, who should be contacted when such services are required.

Reasons for Implementation: This interconnection policy supports MoD by (i) maximising the ability for MOD networks to interconnect to commercial and third-party WANs for the purposes of extending MoD networks (e.g. IP tunneling across a commercial bearer); (ii) allowing MoD to exchange data by connecting to similar sub-networks (e.g. ATM); (iii) when combined with internetworking policy provides the basis for MoD WANs to exchange IP data with external parties such as allies, coalition partners, industry partners and other government departments (via the GSI) and the Internet (via the IGS).

Issues: The choice of which sub-networks to implement is generally left to the IPT or other procuring authority depending on the specific system requirements. However, there are some sub-network types that are mandated in order to produce a common baseline. Where a system implements a particular sub-network (below the IP layer) it must ensure that it does so to those standards mandated for that sub-network. The sub-networks described in this leaflet are both packet switched and circuit switched.

Guidance: Connections to external WANs are subject to CESG security policy. Since it may be necessary to include crypto devices within the interconnection (which may not conform to JSP602 standards), the choice of physical and logical link layers is generally best decided by the IPT based upon which cryptos are envisaged being used when connecting to external WANs. The exception is where there is an overriding benefit to interoperability, in which case the standards have been mandated. Where no crypto device is required, policy is as for MoD WAN-MoD WAN. The e-GIF does not address policy at this level. This policy is consistent with the NC3TA; however the NC3TA does not address the Physical connection policy.

It is highly recommended that the guidance laid down in the GCN Architecture (see Relevant Links section) is followed.

DCSA DFTS IPT is the mandatory provider of External WAN connectivity services within the Strategic, Deployed and Remote domains.

Policy

Strategic

1021.01: General Interconnection Policy

1021.01.01 Where the purpose of the WAN-to-WAN connection is to connect end-systems using IP the only mandated subnetwork technology is defined under Local Area Network Access (below). (Note this does not mean that IP cannot be offered over other subnetwork interfaces in addition).

1021.02: Local Area Network Access

1021.02.01 All Systems and/or projects providing LAN/WAN to external WAN connections shall implement the following standards:

> **1021.02.01.01** ISO/IEC 8802-3:2000 (IEEE Std. 802.3, 2000 Edition), Information technology,Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: CSMA/CD access method and physical layer specifications, Clauses 21-30 for 100BaseT and Clause 14 for 10BaseT.
>
> *While security accreditation may place restrictions upon its use (e.g. TEMPEST) this standard is mandated because its widespread commercial adoption gives the greatest opportunity for external connection.*
>
> *Comment:* Commonly referred to as Fast Ethernet. This standard refers to auto-negotiation 10 baseT /100 base TX. 100Base FX with an SC type connector. Note no physical layer medium is mandated. This is to enable data rates to be tailored to the project.

1021.02.02 All Systems and/or projects providing LAN/WAN to external WAN connections shall implement the following standards:

> **1021.02.02.01** IETF Standard 41/RFC 894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984.
>
> **1021.02.02.02** IETF Standard 37/RFC 826, An Ethernet Address Resolution Protocol, November 1982.

1021.02.03 All Systems and/or projects providing LAN/WAN to external WAN connections shall implement the following standards for Routing services on the boundary routing device:

> **1021.02.03.01** OSPFv2 (RFC 2328:1998) - mandated where connected networks exist within a common geographical area or are both nationally controlled.
>
> **1021.02.03.02** BGP-4 (RFC 1771:1995) - mandated where long haul bearers are used to connect between geographical areas or when connecting to a network infrastructure that is not nationally controlled.

These are the de facto industry standards. OSPF is particularly appropriate for its auto-discovery and fail-over resilience. BGP gives national control over reachability and routability.

1021.02.04 Where Multicast services are required within a network the following standards are mandated on the boundary routing device:

> **1021.02.04.01** PIM-SM (RFC 2362:1998)

Strategic (continued)

1021.02.04.02 PIM-DM (RFC 3973:2005)

PIM SM and DM standards are still formally experimental RFCs, however they are widely implemented by router manufacturers.

1021.03: ATM

1021.03.01 Where ATM technology is used, the following standards are mandated:

1021.03.01.01 ATM Forum PNNI Version 1.0.

1021.03.01.02 ATM Forum UNI Version 4.0.

These standards give national control over reachability and routability.

1021.03.02 If the MoD WAN provides or consumes LAN Emulation Services in external systems it must do so in accordance with the following.

1021.03.02.01 ATM Forum: LAN Emulation over ATM v 2.0 - LUNI specification (af-lane-0084.000, af-lane-0112.000)

De-facto standards for provision of IP services over ATM.

Comment: WANs implementing ATM are not mandated to offer LANE services externally since this will depend on the security policy.

1021.04: X.25

1021.04.01 X.25 is not recommended for new projects unless there are specific requirements to use this service for interoperability with legacy systems.

1021.05: Point-to-point

1021.05.01 There are no mandated standards in this area.

1021.06: ISDN

1021.06.01 Systems and/or projects providing connections to external networks using ISDN shall do so using the following standards:

1021.06.01.01 Basic user-network interface - Layer 1 specification, ITU-T I.430:1995

1021.06.01.02 Primary rate User-network interface - Layer 1 specification, ITU-T I.431:1993, AMD1:1997

1021.06.01.03 ETSI Basic interface specification, ITU-T ETS 300 011:1991, A2:1996

1021.06.01.04 ETSI Primary interface specification, ITU-T ETS 300 012:1992, A2:1996

1021.06.01.05 DSS1 ISDN User interface network Data Link layer, ITU-T Q.930:1993 - formerly ITU-T I.440

1021.06.01.06 ISDN User interface network Data Link layer specification LAPD, ITU-T Q.931:1998 - formerly ITU-T I.441

1021.06.01.07 Numbering standard for ISDN era, ITU-T E.164:1997

Strategic (continued)

1021.06.01.08 ISDN-PCI, ETSI ISDN API, ITU-T

1021.06.01.09 CAPI v2, CAPI CAPI v2:2001

Deployed

1021.07: General Interconnection Policy

1021.07.01 Where the purpose of the LAN/WAN-to-WAN connection is to connect end-systems using IP the following the only mandated subnetwork technology is defined under Local Area Network Access (below). (Note this does not mean that IP cannot be offered over other subnetwork interfaces in addition).

1021.07.02 Where the purpose of the LAN/WAN-to-WAN connection is to connect end-systems using circuit switched voice the only mandated subnetwork technology is defined under Local Area Network Access (below).

1021.08: Local Area Network Access

1021.08.01 As defined for the Strategic domain with the following exceptions:

1021.08.01.01 If copper-based connections are used the mandation of ISO/IEC 8802-3:2002 (IEEE Std. 802.3, 2002 Edition), for 10BaseT and 100BaseTXs is exempt from the physical form (but not electrical properties) of the connector as stated in the standard.

1021.08.01.02 If optical fibre Ethernet connections are used ISO/IEC 8802-3:2002 (IEEE Std. 802.3, 2002 Edition), for 100BaseFX , does not have to have a MDI conforming to any of those in section 26.4.1 of the standard.

1021.09: ATM

As for Strategic domain.

1021.10: X.25

As for Strategic domain.

1021.11: Point-to-point

As for Strategic domain.

1021.12: ISDN

As for Strategic domain.

Tactical

1021.13: Physical Connectors

As for Strategic domain.

Comment: For the tactical domain it is important that the physical form factor of connectors are not mandated for environmental reasons. Systems should use those standards in the strategic section if they cannot show an environmental need. So long as the electrical properties of the standard are not altered a cable with different connector types will provide interoperability.

Tactical (continued)

1021.14: General Interconnection Policy

1021.14.01 Where the purpose of the WAN-to-WAN connection is to connect end-systems using IP the following the only mandated subnetwork technology is defined under Local Area Network Access (below). (Note this does not mean that IP cannot be offered over other subnetwork interfaces in addition).

1021.15: Local Area Network Access

As for Deployed domain.

1021.16: ATM

As for Strategic domain.

1021.17: X.25

As for Strategic domain.

1021.18: Point-to-point

As for Strategic domain.

1021.19: ISDN

As for Strategic domain.

Remote

1021.20: Remote WAN Connections

1021.20.01 Remote users/systems connect to a LAN; relevant policy is covered in JSP602: 1019 - MOD LAN to MOD LAN.

Comment: Remote users/systems in practice connect to a LAN infrastructure. Protocols such as V.90, DSL, ISDN and GSM operate over wide area or long haul bearers but are used to connect LANs together or to connect a remote user to a LAN. Similarly protocols such as PPP operate over WANs but are used to connect LANs together or to connect a remote user to a LAN. These protocols are covered in JSP602: 1019 MOD LAN - MOD LAN.

Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all MOD projects (and their suppliers) that provide connections with external Wide Area Networks from the GII.

Procedure

The principal provider of WAN connectivity data services in the Strategic, Deployed and Remote domains is the DCSA DFTS IPT. Projects in these domains requiring connectivity with external

networks shall contact the DFN IPT.

Relevant Links

JSP602: 1019 - MOD LAN to MOD LAN

DFN IPT can be contacted here. (`http://www.mod.uk/dcsa/organisations/dfn/index.htm`)

AMS guidance on GCN Architecture can be found here (not yet available). (`http://www.ams.mod.uk/ams/default.htm`)

The RFC site can be found here. (`http://www.rfc-editor.org/`)

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
Initial Gate/DP1	MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s).
Main Gate/DP2	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.
Release Authority/DP5	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.