No. 1(3)/2004-EGD

Guidelines

On

Standards, Inter-operability, Inter-connect & Security

For

State Wide Area Networks (SWANs)

May, 2005
Department of Information Technology,
Govt. of India, Electronics Niketan,
New Delhi – 110 003.

Standard, Interoperability, Interconnect & Security for SWANs

1. Introduction

The Internet, which is a loosely organized international collaboration of autonomous, interconnected networks, supports host-to-host communication through voluntary adherence to open protocols and procedures defined by Internet Standards. There are also many isolated interconnected networks, which are not connected to the global Internet but use the Internet Standards.

The State Wide Area Network (SWAN), which will be specifically and independently built for a particular State with heterogeneous applications and Devices in the network should have common Network Standards & Security Policy to be followed by each of the independent SWAN Network.

The SWANs should be interoperable and the biggest advantage is that, it allows for partial or three-layer solutions, where the Networks overlap in some but not all places, or where an intermediate layer that speaks to both protocols is created.

This documents defines the network standard, security and Interoperability and Interconnection of the Networks.

2. Internet Standards

The Standards Process described here is related with all protocols, procedures, and conventions that are used in or by the Internet, whether or not they are part of the TCP/IP protocol suite.

The Internet Standard is a specification that is stable and well understood, is technically competent, and has multiple, independent, and interoperable implementations.

The SWAN, may be built to incorporate any open standards available as per OSI layer. The network should support seamless transformation and integration of protocols as per the demand of the user for open standards. This will provide a fair, open, and objective basis for adopting Standards and developing high resilient Network.

Further, the Internet has been, and is expected to remain, an evolving system whose users regularly factor new requirements and technology into its design and implementation. The providers of the equipment, software, and services that support the SWAN should anticipate and embrace this evolution. The SWAN has to upgrade the network infrastructure/software to support new protocols adopted by Internet community. This has to be a continuous process. For example, migration from IPv4 to IPv6 as and when the transition is required.

SWAN must use the hardware devices, such as Internet routers, terminal servers, Internet systems that interface to Ethernets, or datagram-based database servers, which support open standards and have open NMS support for monitoring, configuring and measurement of the network resources.

2.1 Requirement Levels For Standards

To meet requirement levels to each of the technical specification or application specification in the standards, following action may be take by the implementation agency of the SWAN.

- Implementation of the referenced specification, as specified, is required to achieve minimal conformance. For example, IP and ICMP must be implemented by all Internet systems using the TCP/IP Protocol Suite.

- SWANs are strongly encouraged to include the functions, features, and protocols of Recommended Technical specification in their products, and should omit them only if the omission is justified by some special circumstance. For example, SSH (version 2) should be implemented in place TELNET by all systems that would benefit from remote access for enhanced security.

- Implementation of the referenced technical specification is optional within the domain of applicability of the application specification. However, a particular vendor may decide to implement it free of cost. For example, the latest version of SNMP MIB could be seen as valuable in an environment where the SNMP protocol is used.

SWANs should have following capabilities to follow OSI standards:

- Should be a TCP/IP based network.

- Each SWAN network equipments should have Ipv4 and IPv6 features.

- Shall have the capability to run IP routing protocols like OSPF (Open Shortest Path Find) version 2, OSPF v3, RIP v2, RIPng, OSPF over demand circuit, IS-IS, BGP4.

- Different SWAN may run different IP Routing protocols (like OSPF, EIGRP, BGP) depending on the individual design criteria of the SWAN. It is mandatory that the network should allow interaction between multiple routing protocols for keeping a unified network reachability table across the country.

- While two routing protocols are interacting to exchange routing updates, there should be the capability to selectively filter certain routes for security reasons.

- The SWAN should be capable to provision IP multicast based services. The same would require the capability of running industry standard IP multicast protocols like Protocol Independent Multicast (PIM) Sparse Mode and Dense Mode, Multicast OSPF (MOSPF), Multicast BGP (MBGP) and DVMRP.

- SWAN should have the multicast group management capability through Industry standard protocols like Internet Group Management Protocol (IGMP) version 1, 2 and 3.

- The voice networking of each SWAN should be based on IP for smooth integration across the country for all SWANs.

- The voice networking of the SWAN should be designed in such a way that a central call processing system is able to service phones at remote locations.

- Each SWAN should have the voice and video conferencing solution deployed based on industry standard protocols so that it is possible to have conferences between states and between the state and central ministry.

3. Network Interoperability

Network Interoperability is the continuous ability to send and receive data between interconnected networks providing the level of quality expected by the end user without any negative impact to the sending and or receiving networks.

Specifically, Network Interoperability is the functional inter working of a service across or between multi-vendor, multi-carrier inter-connections (i.e., node-to-node, or network-to-network) working under normal and stress conditions, and as per the applicable standards, requirements, and specifications.

The ability to characterize and analyze network interoperability depends significantly on characterizing and understanding the following issues:

a. The use of existing or emerging technologies to facilitate the development of interface and migration interoperability solutions.

b. The use of networking tools including test and measurement equipment and software as well as evaluation methods that aids in the design of alternative solutions and ensure that solutions meet goals and performance requirements. This includes tools for network simulation and emulation, network monitoring and management and security assessment and protection.

c. The judicious use of frameworks within which the interoperability requirements can be described and solved using structured methods and decision-making techniques.

3.1. Interoperability Methodology

The methodology of interoperability involving different SWAN each of which will implement a Data. Voice and Video over Standard Protocols by using different vendor solutions and different technologies. It has become necessary to make these systems capable of connecting each other. For interoperability of two technologies/ protocols requires a Gateway for interfacing the two different protocols like H323 to SIP Gateway.

The goal of the effort is to deploy a solution for interoperating respective ICT based SWANs. The SWANs will be implemented by state Governments that have similar missions so that. organizational considerations may not result in any technical constraints.

The interoperability should assure optimal reliability and interoperability of wireless, wire line. satellite. cable. and other public data networks. This includes facilitating the reliability. robustness. security. and interoperability of communications networks including emergency communications networks. The interoperability shall ensure the security and sustainability of communications networks throughout the country; ensure the availability of adequate communications capacity during events or periods of exceptional stress due to natural disaster. terrorist attacks or similar occurrences; and facilitate the rapid restoration of telecommunications services in the event of widespread or major disruptions in the provision of communications services.

For interoperability. all major traffic concentration points to be identified and then define the metric and thresholds that should be used to determine where traffic concentrations are unacceptably high.

3.2. SWANs Interoperability

States will implement the SWANs independently driven through multi-vendor who may use multi-technology. Each SWANs may deploy different topology, interfaces, components. services. traffic and utilization levels etc. Since. SWANs does not have centralized Planning and Unified architecture. the interoperability of SWANs has to be achieved through Internet. This means that every SWAN will have Internet Gateway and the exchange of information and interconnection of SWANs will be through Internet.

As basic needs, the SWAN should have:

- All communications happening over the various links within each SWAN should be encrypted using standard protocols like IPSec, 3DES & AES to ensure highly secure communication.

- SWAN should have the capability to control the interaction between two routing protocols (like OSPF and BGP). It should be possible to selectively filter certain routing updates being sent or being received from the peer network

- SWAN should have firewall for performing intelligent packet filtering, URL filtering, context based access control, blocking of malicious contents to maximize security.

- Implementation of gateway level anti-virus filtering for protection against viruses.

4. Interconnection with NICNET

NIC has a partial mesh Backbone network that connects all NIC State and District Centres. For enabling Internet access NICNET has Internet gateway connectivity.

As SWANs are designed and implemented independently, the inter connectivity among SWAN and to the NICNET can be achieved with the following options.

i) Through Internet
ii) Through National Internet Exchange (NIXI) as NIC has connectivity to NIXI.
iii) Each SWAN may also do peering independently with NICNET.

The SWANs implemented by NIC will be designed and architectured in a such a way that they are in sync with NICNET.

5. Security For SWANs

DIT, Ministry Of Communication and IT has setup CERT-In, to enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration. The CERT-In will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents.

The SWANs may follow the Security Guidelines issued by CERT-In from time to time.