

Standard No: NTW/STD/01

Status: Final v1.0

Date of Effect: 01/09/05

Revision date: 01/09/06

ICT STANDARD

IP Address Management Victorian Government Intranets

1 Introduction

The telecommunications industry agrees that all communication (voice, data, video, fixed and mobile) is progressively converging towards the use of a single technology, the technology used for the Internet, based on the Internet Protocol (IP). Central to the use on these networks is the allocation and management of the addresses that identify where to send the communication. Victorian Government departments and agencies need to adopt a consistent approach to the management of the addresses in order to:

1. Take advantage of applications and services that are shared across multiple agencies. (eg. Shared service for managing desktop computing, Common applications for Grants Management, Asset Management and Enterprise Content Management.);
2. To be able to use these IP technologies to carry voice telephony and video conferencing; and
3. To minimise the risk of security breaches and service interruptions due to the increasing complexity of managing inter-connected networks.

This will become more significant as agencies begin to take advantage of the attractive cost structures available under the TPAMS contract for data (IP) services.

This IP address management standard:

- Applies to networks that are internal to the Victorian Government (ie. Intranets).
- Is mandated only for that component of a departmental Intranet that is carried by TPAMS services.
- Ensures that no addresses within the TPAMS network are duplicated after the compliance date (12 months from endorsement of the standard).
- Is achieved by hierarchical allocation of addresses such that agencies retain control of the range of addresses allocated to them.

The approach mandated in this standard enables benefits 1 and 3, above, to be realised. To achieve benefit 2 it will be necessary for departments to extend this approach throughout a department's network.

The increasing use of IP networks to provide a range of services such as converged voice, video and data services across departmental boundaries highlights the need for a centralised approach to IP address management within the Victorian Government environment. These new services are likely to be ineffective in those networks where this address management approach is not applied.

2 The Requirements of this Standard

This standard is divided into 2 components:

- The elements that are **mandatory**.
- The elements that are **recommended**, but optional.

The elements that apply to **both the mandatory and recommended components** of this standard are:

1. This standard only applies to addresses used within departmental and WoVG Intranets (ie. not Internet-facing equipment).
2. The address ranges to be used by departments are to be allocated to departments by the Chief Technology Office (CTO).
3. CTO will allocate a range that supports 262,144 addresses to each department, with the option of more being provided where needed. DE&T will be allocated 2 ranges of this size.
4. Departments are to allocate and manage the use of addresses within the address range allocated to them by the CTO.
5. The address ranges, allocated to departments by the CTO, are to be from the private network range specified in the international industry standard IETF RFC1918.
6. The address ranges, allocated to departments by the CTO, are to be in accordance with the approach for Classless Inter-Domain Routing (CIDR) specified in the international industry standard IETF RFC 1519. (This approach allows smaller ranges of address to be allocated and therefore enables spare capacity for future purposes.)
7. No addresses from the public Internet address range are to be used. The public address ranges are those allocated to departments by the relevant international body (APNIC).
8. Departments are to advise the CTO of all public address ranges allocated to them. The CTO is to record these addresses in the Victorian Government Public IP address register.

The **mandatory element** of this standard that is to be met by departments are:

9. This standard only determines the allocation of addresses used by departments for services that make use of TPAMS TCS services.

The **recommended element** of this standard that is to be met by departments are:

10. It is recommended that the address allocation approach specified in this standard be applied to the whole of each department's Intranet.

Where departments choose not to follow this recommendation for the remainder of their Intranets, they may use their allocated public IP addresses within their Intranets.

3 Rationale

The rationale behind this Standard is to:

- Enable the Government's convergence policy objective. This policy aims to reduce costs and improve service levels by using a common network for data, voice and video.
- Provide a method of assuring that IP addresses used by Departments are unique across the Victorian Government Intranet.
- The management of a consistent WoVG address plan, that results in no duplication of addresses, is simpler than managing the current situation. This simplification reduces the possibility of errors and security breaches. Note that this benefit cannot be realised within the TPAMS TCS environment if one or more departments do not adopt the approach described in this standard.
- Facilitate the minimisation of Network Address Translation (NAT) by Government Departments. NAT can result in serious degradation of voice and video services, through the time delays it introduces into the communications path.
- Support controlled inter-connection between departments to enable the sharing of applications and data between departments and agencies. The sharing of applications and

data can be carried out without NAT by having unique addresses. This sharing is a key element in:

- Reducing costs.
- Improving service delivery.
- Providing services that join capabilities between departments.
- Providing services that have a regional focus but extend across multiple department capabilities.
- Increase the efficiency of IP address allocation by the use of Classless Inter-Domain Routing. This provides for address ranges that may be needed for future services, without major changes in the network technologies.
- Move to a best practice approach to IP addressing for internal hosts through the use of Private IP addresses. This will mean that, should departments be asked to relinquish some of their allocated public addresses, they can do so with minimal consequences. Such a request could be made by the international allocating authority in response to the current scarcity of addresses.

4 Scope

4.1 Description

This standard is mandated for:

- Components of Department's/Agencies' Intranets that use (TPAMS) TCS services.

This standard is optional, but recommended, for:

- All parts of Department's/Agencies' Intranets.

This standard does not apply to the public Internet.

4.2 Applicability

This Standard is to apply to Victorian Government Inner Budget Departments and Agencies. In addition to this, all Government Agencies procuring data services through CTO TCS (TPAMS) contracts must comply with this Standard. Specifically this includes:

- Department of Justice;
- Victoria Police;
- Department of Sustainability and Environment/Department of Primary Industries
- Department of Education and Training
- Parliament of Victoria
- Department of Human Services
- Department of Innovation, Industry and Regional Development
- Department of Premier and Cabinet
- Department of Treasury and Finance
- Department of Infrastructure
- Department of Victorian Communities
- VicRoads
- State Revenue Office

- Environment Protection Authority
- All other Victorian Government Agencies participating in TCS

5 Compliance

5.1 Date

Departments should be compliant with this Standard within 12 months from approval of this Standard by the ICT Policy Committee.

5.2 Reporting requirements

At the initiation of this Standard, Departments will be required to report their Public IP address space to the CTO for inclusion in the Public IP address register.

6 References

6.1 General References

- IETF RFC1918/BCP0005 “Address allocation for private Internets”
- IETF RFC 1519 “Classless Inter-Domain Routing (CIDR): An address assignment and aggregation strategy”
- IETF RFC 3022 “Traditional IP Network Address Translator (Traditional NAT)”

6.2 Guidelines and tools

The Office of the CIO and CTO plans to investigate the possibility of selecting a tool for managing IP addresses that can be used by departments and agencies across the Whole of the Victorian Government (WoVG).

6.3 Prior Artefacts

- CTO WoVG IP Address Management Plan – Version 1.7 - 2nd May 2005
- TPAMS Program – IP Policy Project – January 2003

6.4 Related Principles, Policies and Strategies

6.4.1 STRATEGIES

This standard enables the following Victorian Government Strategies, in that it supports the ability to integrate services between departments and it is an enabler for achieving regional views of multiple services that span several departments.

- Growing Victoria Together (2): A vision for Victoria to 2010 and beyond. Mar 2005
- A Fairer Victoria: Creating opportunity and addressing disadvantage. April 2005

6.4.2 PRINCIPLES

The following Whole of Victorian Government (WoVG) ICT Principles have been used in the creation of this Standard:

- Reduce Integration Complexity

- Holistic Approach to Information
- Security, Confidentiality, Privacy & Protection of Information
- Proven Standards and Technologies
- Adopt Formal Methods of Engineering

6.4.3 NETWORK POLICY

This Standard is one of a suite of standards expected to be developed under the WoVG Network Policy.

6.5 Glossary of terms and abbreviations

Table 1—Glossary

Term	Meaning
APNIC	Asia Pacific Network Information Centre
Asia Pacific Network Information Centre	The international registry that allocates public IP addresses for this region of the world.
BCP	Best Current Practice
CIDR	Classless Inter-Domain Routing
IETF	Internet Engineering Task Force
IP	Internet Protocol
NAT	Network Address Translation
Public Address Register	The register of all public IP address blocks in use by Victorian government Departments. The register will be maintained by the CTO with appropriate input from government Departments that have IP address space registered with a Regional Internet Registry.
RFC	Request For Comment
TCS	Telecommunications Carriage Services. A Victorian Government program for the procurement of Voice, Mobile and Data telecommunications services.
WoVG	Whole of Victorian Government

7 Document Information

Table 2—Document version information

Title	IP Address Management	
Status	Draft	
Approval date	[d/m/yy TBD]	
Approver	[ICT Policy Committee]	
Author	Justin Bree and David Johnson	
Short description	Requirements for the management of IP addresses within agency Intranets when using TPAMS, shared services & applications, voice telephony and video conferencing.	
Keywords	IP Internet protocol Intranet address management CIDR clasless inter-domain routing	
File name	ICT-STANDARD-IPAddressManagement-240805-FINALv1.0-CIO.DOC	
Location	J:\Office of the CIO\WoVG ICT Strategy Policies Standards\Approved Artifacts\Networks\ICT-STANDARD-IPAddressManagement-240805-FINALv1.0-CIO.DOC	
This copy printed	22/03/2006 6:06:00 PM	
Version and date	v0.1.2	1 June 2005
Version history	Number	Comment
25/10/04	0.1	Draft
6/7/05	0.1.1	Draft: Technical content moved to appendix. Body rewritten.

8 Appendix A – Technical details of the requirements of this standard

The IP Addressing Standards proposed in '*this Standard*' are based on the utilisation of RFC 1519 Classless Inter-domain Routing (CIDR) and RFC 1918 private address space.

The IP Addressing Standard (is this 'this Standard' or RFC 1519 and RFC 1918) covers Supplier addressing, department addressing and also includes Public IP Address Register.

The use of Public IP addresses within private networks, while discouraged, remains an option for Departments under this Standard as long as the Department holds a valid licence for these Public addresses.

8.1 IP Address Management

Management of the IP addresses maintained under this Standard will be cooperative effort between the CTO and Departments. The CTO will maintain a high level summary of the IP address range assigned to the Departments only. It is not the intention of the CTO to provide management of individual IP addresses at the operational level, rather to ensure that all Departments have been assigned unique address space from the RFC 1918 ranges and public ranges.

The use of CIDR allows the CTO to assign an address block to a Department whilst providing the Department the operational freedom to decide how the allocated block will be subnetted and administered within the network environment.

It is the responsibility of each Department to manage the allocated address space to meet their needs. The systems, policies and procedures for the management of IP addresses assigned under the Department allocation will remain the responsibility of the individual Departments; the only requirement is that the Department remain within the allocated address block.

Departments that plan to utilise their existing Public IP addresses for their internal networks are responsible for the management, licensing and assignment of such public IP addresses.

8.2 Supplier Addressing

Suppliers providing network services to the Victorian Government will be assigned an IP address range so they can control and manage the network equipment and services that comprise the Supplier's network. The allocated IP address range will be administered by each individual Supplier. Each Supplier is initially assigned a /16 range of addresses. Should this prove to be insufficient, the Supplier may apply to the CTO for an additional range. The CTO will then assign an appropriate block to the Supplier. As shown in Table 3, the IP address range 10.1.0.0/13 has been assigned to the Supplier Addressing Plan. In addition to this 10.244.0.0/14 has been assigned to Telstra for the tranche 1 TCS Network.

Table 3: Core IP Address Allocations

1st Byte	2nd Byte	3 rd Byte	4th Byte	Subnet Bits	Allocation
10	1	0	0	/16	Free
10	2	0	0	/16	Free
10	3	0	0	/16	NEC - VOTS
10	5	0	0	/16	Free
10	6	0	0	/16	Free
10	7	0	0	/16	Free
10	8	0	0	/16	Free
10	244	0	0	/14	Telstra TCS T1

Carriage Suppliers may be required to use Public IP addresses within their networks in the instance that Internet services are procured at some future point. Carriage Suppliers may also be able to supply public IP addresses to the State should this be required.

8.3 Department Addressing

Under this Standard each Department will be assigned a private address range unless the Department is utilising registered public address space within their internal network. The Department will be assigned a /14 address range that accommodates a total possible 262,144 hosts. If Departments find that this is not sufficient to meet their requirements, additional IP address space may be allocated on an “as required” basis by the CTO. Table 4 shows the initial IP address allocations available to Departments.

One exception to this rule is the Department of Education and Training (DET), which requires a greater number of addresses due to the large number of hosts contained within their networks. The CTO have worked with DET to define their exact IP address space requirements in preparation for the implementation of this Standard.

The intention of the Department addressing scheme is to allow the retention of the existing IP address schema wherever possible. For example, a number of Departments utilise Public IP addresses for their internal IP address ranges. This Standard allows for the use of Public IP addresses should a Department require this. A record of such allocations would be recorded in the Public Address Register.

Table 4: Department IP Address Allocations

1 st Byte	2 nd Byte	3rd Byte	4th Byte	Subnet Bits	Allocation
10	8	0	0	/14	DOJ
10	12	0	0	/14	VicPol
10	16	0	0	/14	DSE/DPI
10	20	0	0	/14	DE&T
10	24	0	0	/14	PoV
10	28	0	0	/14	DHS
10	32	0	0	/14	DIIRD
10	36	0	0	/14	DPC/DTF
10	40	0	0	/14	DOI
10	44	0	0	/14	DVC
10	48	0	0	/14	VicRoads
10	52	0	0	/14	Free
10	56	0	0	/14	Free
10	60	0	0	/14	Free
10	64	0	0	/14	Free
10	68	0	0	/14	Free
10	72	0	0	/14	Free
10	76	0	0	/14	Free
10	80	0	0	/14	Free
10	84	0	0	/14	WoVG
10	128	0	0	/10	DE&T

Departments that currently utilise Public IP addresses for their internal networks may use their existing IP address range provided that the address range is registered to the Department by the appropriate regional Internet registry (APNIC).

Ideally, Departments should limit the use of external or Public IP addresses to a workable minimum in line with IETF best practice recommendations. NAT at the exit point of networks is the preferred method to provide static mappings to internal IP addresses that require external connectivity, i.e. departmental web servers that users access via the Internet.

Those Departments that utilise Public IP addresses are required to provide the CTO with the information for the Public Address Register.

8.4 Public Address Register

The Public Address Register is a register of all public IP address blocks in use by government Departments. The register will be maintained by the CTO with appropriate input from government Departments that have IP address space registered with a Regional Internet Registry.

The purpose of the register is to allow a single consolidated view of all IP address in use within the Government network environments. There is no intention to assume management of Departmental registered address space. Neither the OCIO nor the CTO wishes to assume management or control of public address space licensed to individual Departments. Address space licensed to individual departments is viewed as being, for all intents and purposes, the 'property' of the individual Department by the OCIO/CTO even though ownership of the registered address space remains with APNIC.

Individual Departments that have public address space will continue to be responsible for the management and administration of the public addresses; the CTO is simply seeking to establish and maintain a complete, comprehensive, and up to date view of the IP address space within the Victorian Government.

8.5 Network Address Translation

One of the objectives of this Standard is to reduce the dependence on NAT. The use of NAT has serious implications when examined in relation to latency intolerant applications, potentially impeding the introduction of technologies such as VoIP and video. This is contrary to the stated convergence policy of Government and as such the use of NAT and other latency inducing technologies should be eliminated or minimised wherever possible.

The use of network address translation under the IP addressing plan should be limited to the borders of the Private and Public Networks, i.e. Internet gateways. The limiting of NAT within the network eliminates the potential segmentation of Departmental networks and reduces the complexity and cost of maintaining IP networks.

The reduced reliance on NAT will ensure that the uptake of convergent applications is not impeded by the latency penalties imposed by the use of NAT.

9 Appendix B – Background on IETF Technical standards

A number of standards have been used as references by the CTO in the creation of this Standard. These standards have been drafted by the Internet Engineering Task Force (IETF), which defines standards and best practices for the use of TCP/IP and the Internet.

9.1.1 IETF RFC1918/BCP0005 “ADDRESS ALLOCATION FOR PRIVATE INTERNETS”

The IETF has published RFC 1918/BCP0005 “Address Allocation for Private Internets” as a Best Current Practice guide for the use of the IPv4 address space within private networks. RFC 1918 defines two types of addresses: Public IP addresses and Private IP addresses. To illustrate this point the RFC gives the following examples of public and private IP addresses:

Hosts within enterprises that use IP can be partitioned into three categories:

Category 1: *hosts that do not require access to hosts in other enterprises or the Internet at large; hosts within this category may use IP addresses that are unambiguous within an enterprise, but may be ambiguous between enterprises.*

Category 2: *hosts that need access to a limited set of outside services (e.g., E-mail, FTP, netnews, remote login), which can be handled by mediating gateways (e.g., application layer gateways). For many hosts in this category an unrestricted external access (provided via IP connectivity) may be unnecessary and even undesirable for privacy/security reasons. Just like hosts within the first category, such hosts may use IP addresses that are unambiguous within an enterprise, but may be ambiguous between enterprises.*

Category 3: *hosts that need network layer access outside the enterprise (provided via IP connectivity); hosts in the last category require IP addresses that are globally unambiguous.*

Hosts in the first and second categories are referred to as "private".

Hosts in the third category are referred to as "public".

Many applications require connectivity only within one enterprise and do not need external (outside the enterprise) connectivity for the majority of internal hosts. In larger enterprises it is often easy to identify a substantial number of hosts using TCP/IP that do not need network layer connectivity outside the enterprise.

The goal of RFC 1918 is to conserve the globally unique address space by not using it where global uniqueness is not required. The advice contained in RFC 1918 is generally accepted as a ‘best practice’ and has been used as a guideline by the CTO when creating this IP Address Management Standard.

As the vast majority of Victorian Government hosts fall into Category 2, RFC 1918 has been used to provide the private IP address space that forms the basis of this Standard. The guidelines and definitions contained within the RFC have been used in this Standard and must be followed if the integrity of the IP address space for all government users is to be maintained. Departments also have requirements for hosts in Category 3.

9.1.2 IETF RFC 1519 “CLASSLESS INTER-DOMAIN ROUTING (CIDR): AN ADDRESS ASSIGNMENT AND AGGREGATION STRATEGY”

RFC 1519 discusses a number of methods to reduce waste of IP address space within the Internet. The key solutions described in the RFC are Classless Inter-Domain Routing (CIDR) and variable length subnetting.

Historically, the IP address “class” system used five classes to define the number of hosts that a network could contain. The three primary classes that have been assigned in the past are A, B

and C class networks. As shown in Table 5, classes A, B and C have a defined number of networks and hosts.

Table 5: IP Address Classes

Address Class	No. of network bits or "prefix"	No. of networks available	No. of Hosts per network
A	8	126	16,777,214
B	16	65,000	65,534
C	24	2,031,616	254

The problem with this approach is that the three network sizes do not fit all requirements. For example if a site needed 100 hosts within a single network and uses a class C network, 154 hosts will be wasted.

Classless Inter-Domain Routing (CIDR) is a replacement for the process of assigning Class A, B and C addresses with a generalized network "prefix". Instead of being limited to network identifiers (or "prefixes") of 8, 16 or 24 bits, CIDR currently uses prefixes anywhere from 8 to 27 bits. Thus, blocks of addresses can be assigned to networks as small as 32 hosts or to those with over 500,000 hosts. This allows for address assignments that much more closely fit network administrator's specific needs.

CIDR address allocations are expressed as "IP address / number of bits in network prefix". By way of example, the designation 10.8.0.0 / 14 represents a network that must be uniquely identified in the first 14 bits of the IP address. This example could support a large number of addressable IP devices in the network (2^{18} minus 2), the equivalent of four class B networks. Typically, a site would also employ further subnetting of this large address space.

The uptake of CIDR has rendered the use of Class nomenclature as a legacy practice.

RFC 1519 has been used to form the basis of subnetting in this Standard and CIDR subnetting must be used.

9.1.3 IETF RFC 3022 "TRADITIONAL IP NETWORK ADDRESS TRANSLATOR (TRADITIONAL NAT)"

The primary standard for NAT is IETF RFC 3022 "Traditional IP Network Address Translator". IETF RFC 3022 covers how NAT should be performed, the types of NAT implementations available, issues associated with NAT and implementation advice.

The need for IP Address translation arises when a network's internal IP addresses cannot be used outside the network either because they are invalid for use outside, or because the internal addressing must be kept private from the external network.

In many cases address translation allows hosts in a private network to transparently communicate with destinations on an external network and vice versa. There are applications and protocols that do not function well when passed through a network address translator.

Figure 1 shows an example of the basic NAT function. Host B sends a packet to host A using the external address of 152.64.122.1. The NAT device looks up the address 152.64.122.1 in its NAT table and finds that 152.64.122.1 translates to the internal IP address 10.1.1.1. The NAT device modifies the IP header in the IP packet to change the destination address from 152.64.122.1 to 10.1.1.1 (the source IP address remains 152.64.121.7) and forwards the packet to Host A.

Host A then responds to Host B and sends a return packet with the source IP address of 10.1.1.1 and destination IP address of 152.64.121.7. The NAT device receives this packet and sees that this packet needs to be translated. The NAT device does a table lookup in its NAT table and finds that 10.1.1.1 needs to be translated to 152.64.122.1. The NAT device modifies the IP header in the IP packet to change the source address from 10.1.1.1 to 152.64.122.1 (the destination IP address remains 152.64.121.7) and forwards the packet to Host B.

Figure 1: Network Address Translation

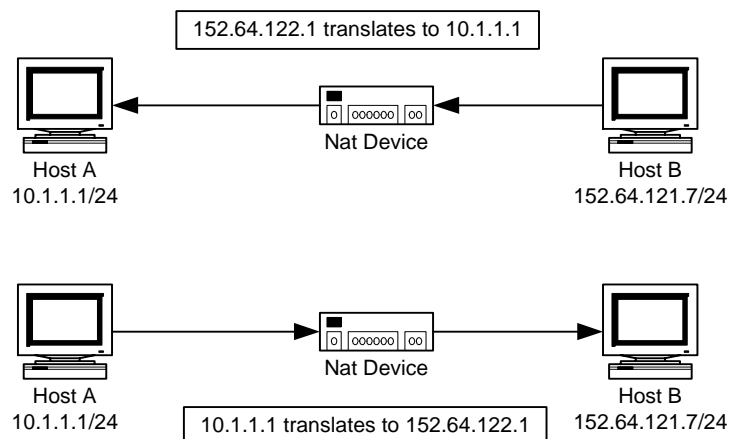


Figure 1 shows a simple NAT implementation; there are a variety of flavours of NAT that have been developed to suit a range of environments. This Standard does not attempt to define a standard NAT implementation. It is advisable that each D&A implements NAT to suit its individual needs as required.

9.1.3.1 Advantages of NAT

- Conserves the legally registered addressing scheme. Enterprises and ISPs benefit since they can reduce the number of legally registered IP addresses.
- Network design is simplified by now-limitless availability of addressing schemes.
- Merging and changing of networks is simplified. For an enterprise, it is possible to change the ISP vendor without having to completely renumber the network.

9.1.3.2 Disadvantages of NAT

- Multiple instances of NAT within a department LAN/WAN environment may impede the introduction of convergent technologies; this would contradict the stated convergence policy.
- Loss of end-to-end IP traceability; for example, the command "trace route" will not be of great help anymore.
- Applications that send IP addressing information within their data (e.g., IPSec, video conferencing, FTP) will require special handling.
- Applications that utilize dynamic TCP or UDP port numbering will require special handling.

10 Appendix C – Impact of this standard

10.1 Benefits

The benefits of this standard are outline in §3 Rationale.

10.2 Work to be done to comply with this standard

To comply with **mandatory elements of this standard**, without applying it to whole departmental Intranets:

- Departments will need to manage an additional address range for the TPAMS TCS components of their Intranets.
- If there is an overlap between the range of addresses they currently use on their Intranets and the range allocated for TPAMS, they may, either:
 - Introduce Network Address Translation (NAT) equipment, or
 - Manage the individual addresses so there are no address clashes.
- As most departments will be able to adopt this address approach from the first TPAMS services, there should be no migration required.
- The work to comply is expected to be minimal.

To comply with **recommended elements of this standard**, ie. Applying it to whole departmental Intranets:

- Departments may need to manage the allocation and migration to a new address range. This depends on whether the range currently in use is compliant with the approach specified in this standard and is available for allocation by the CTO.
- This migration to new addresses would involve minimal effort for equipment that operates with dynamically allocated IP addresses.
- However, for equipment that operates with static IP addresses, this migration would involve more significant effort.
- Departments will need to manage the new address range within their address management tools. During migration they will also need to manage the old addresses.
- Departments using NAT should take the opportunity to remove that equipment, where it does not perform a security function