

Virtual Education Networks

Network Policy Statements

June 21, 2006

Aims:

This set of policies is designed to give all members of the Virtual Private Network (VPN) a common set of guidelines which outline the operational requirements for software, hardware and network connections. It is recognised that these are evolving policies and that the specifications may change from time to time, as dictated by the requirements of members, and the technological infrastructure that supports the VPN. Comments relating to these policies are invited and should be submitted by email to: peterhills@virtualeducation.net.nz

Preamble:

Connection Check-list 3

Policies:

Network Service..... 4

External Network Connection 5

Internal Network Connection 6

Application Software Standards 7

Computer Hardware Standards 8

Data Standards 9

Internet Usage 10

Associate Member Users 11

VideoConference Networks..... 12

VideoConference Lessons 14

Onsite mail servers 15

General Network Usage 16

Appendix 1: IP Addressing Scheme 17

Appendix 2: Technical Standards for network carriers 18

Appendix 3: Time Servers 20

Appendix 4: Educational Activities for Associate Membership 21

Preamble

Connection Checklist

Organisations wishing to become members of the Virtual Private Network (VPN) must be able to satisfy VEN Ltd that their own computer network is able to be satisfactorily connected to the VPN. To this end the following checklist is provided which summarises the various policy elements in this document. All elements on this checklist should be met prior to connecting to the VPN.

Criteria:	Checked:
1. TCP/IP is installed on all devices to be connected to the VPN. IPX/Netware 3 is not supported.	<input type="checkbox"/>
2. External network transmission speed exceeds 256Kb/s	<input type="checkbox"/>
3. TCP/IP addressing scheme has been configured as per Appendix 1	<input type="checkbox"/>
4. Organisation network uses 10/100/1000Mb/s switched connectivity	<input type="checkbox"/>
5. A UPS is available for the router	<input type="checkbox"/>
6. At a minimum all PCs connected to the VPN use Windows 98 or Mac OS 8.1	<input type="checkbox"/>
7. Virus protection is in place on all computers with removable media	<input type="checkbox"/>
8. On-site technical support is available to configure computers and solve minor hardware issues	<input type="checkbox"/>
9. Support systems are in place to solve major hardware issues	<input type="checkbox"/>
11. The school has put in place cyber safety protocols as per the Internet Safety Group Netsafe Kit.	<input type="checkbox"/>

Network Service Policy

Rationale:

1. To provide a set of guidelines that specify the minimum service and security levels required to allow members to use the VPN for its intended purposes.
2. To inform the relevant companies and participating members about these policies.

Policies:

1. Members will have access to the World Wide Web.
2. All web-based access will be filtered for content (appropriateness and viruses) at the point that it enters the VPN.
3. Videoconferencing services (point-to-point and multi-point) will be available.
4. Email services will be negotiated with each member on an individual basis. Members who require email may use their own domain. Options for email include but are not limited to:
 1. member hosts own email using their own systems as an Onsite server.
 2. member has email hosted on the schools network by another school with an Onsite server.
 3. members use email boxes provided by the service provider.

Onsite server details will be discussed as needed with individual schools.

5. Access to secure internet services (SSL) such as the commercial banking services offered by ANZ, BNZ, National Bank, WestpacTrust, PSIS and others will be available.
6. All members will be required to connect to the VPN in accordance with the External Network Connection Policy.
7. FTP clients that directly access external servers will have no restrictions in place. Telnet traffic to external sites (e.g. online libraries) is not restricted.
8. All members will be required to implement desktop security in accordance with the Data Software Standards Policy, with particular reference to virus protection.
9. All members are encouraged to adopt time synchronisation as a standard to allow for accurate date and time stamping of all files. This will avoid problems that can arise from spurious time and date reconfiguration. See Appendix 3 for details.

External Network Connection Policy

Rationale:

1. To ensure that all network connections between internal VPN member's networks to external networks will meet known standards of operability.
2. To inform members of the minimum hardware requirements to ensure reliable external network connections.
3. To define minimum carrier standards for connectivity to the VPN.

Policies:

1. All external network connections to the VPN must be approved by VEN Ltd. In general network carriers must meet the minimum standards as defined by the video conferencing and technical standards.
2. All external network connections will use broadband as supplied by the approved telecommunications carrier.
3. External network transmission speeds should meet or exceed 256Kb/s for both uploading and downloading data.
4. The standard transmission protocol will be Transmission Control Protocol / Internet Protocol (TCP/IP). IPX protocols and Netware 3 are specifically unsupported.
5. All external network equipment will be supplied, installed and configured by an appointed and approved agent of the carrier.
6. All IP-connected devices will use an IP addressing scheme as defined by VEN Ltd. The IP addresses will be private "Class C" addresses in the range 10.x.y.z The values x and y will be defined to each member by VEN Ltd. See Appendix 1 for details. Additional Class C subnets will be available through to 10.x.y+15,254 with a subnet mask of 255.255.240.0
7. Network connections may be by way of a proxy server.
8. Network carriers and other suppliers will provide helpdesk support and professional development services.
9. Technical criteria for required network uptime, latency, jitter, fault resolution, fault notification processes etc will be defined in Appendix 2.

Internal Network Connection Policy

Rationale:

1. To ensure that all internal network connections meet or exceed the minimum requirements to allow data transfer at speeds that will allow users to interact meaningfully.
2. To ensure that users have a robust and stable network operating environment.
3. To inform members of the minimum hardware requirements to ensure meaningful user interaction between the internal and external components of their network.

Policies:

1. Members should be using 10/100/1000Mb/s switched connectivity.
2. The router and similar external network devices should be connected to internal devices either directly (the preference for video conferencing devices) or by means of a 10/100/1000Mb/s switch.
3. Internal video conferencing devices should connect to the external network through a maximum of two switches.
4. The internal network must be Transmission Control Protocol / Internet Protocol (TCP/IP) based. IPX and Netware 3 are specifically unsupported. All devices operating on the network which access the VPN must use TCP/IP.
5. A UPS with built-in surge protection should be used with externally connected devices.

Application Software Standards Policy

Rationale:

1. To ensure that all internally available application software meets or exceed the minimum requirements to allow users to complete their tasks.
2. To inform members of the minimum software requirements to ensure users can complete their tasks.

Policies:

1. Staff will receive professional development training and support to allow effective use of the VPN. This training and support is the responsibility of the member to organise.
2. VEN will endeavour to ensure there is an adequate supply of Professional Development trainers for the VPN for members to use.
3. Where data sharing is to take place between members that data must be sent in a format that the recipient can use. The onus is on the sender to provide data in a format that the recipient can use.

It is required that all members be able to support the following data formats as a minimum:

Word Processing:	Word 97/98, RTF, WordPerfect 6
Spreadsheets:	Excel 97/98
Database:	Access 97, FileMaker or AppleWorks
Graphics:	JPEG for photographs, GIF for anything else
PDF:	Acrobat, Preview
Compression:	Zip, Stuffit

4. All hosted applications being used across the VPN must have the prior and formal approval of VEN Ltd before they are used. All enquiries should be directed to peterhills@virualeducation.net.nz

Computer Hardware Standards Policy

Rationale:

1. To ensure that all computer hardware meets or exceeds the minimum requirements to allow users to complete their tasks.
2. To ensure that users have a robust and stable computing environment.
3. To inform members of the minimum hardware requirements to ensure meaningful user interaction.

Policies:

1. All VPN-connected computer hardware will support and utilise Transmission Control Protocol / Internet Protocol (TCP/IP). IPX and Netware 3 are specifically not supported.
2. All VPN-connected computers must be capable of reliably running, as a minimum, Microsoft Windows 98 operating system or Mac OS 8.1 operating system.
3. Members will set a budget that allows for the maintenance of their computer systems.
4. Members will maintain their VPN-connected computers so that they function as intended.
5. Members will make available on-site technical support to solve minor hardware issues. At a minimum this will involve fault tracing to a particular device (mouse, monitor, disk drive, keyboard, CD-ROM drive etc) and the replacement of that device.
6. Members will have systems in place to solve major hardware failures at the earliest possible time with minimum loss of service to network users.
7. Videoconferencing hardware will conform to guidelines that will be defined from time to time by VEN Ltd.
8. All hardware upgrades will operate within guidelines that will be defined from time to time by VEN Ltd.

Data Standards Policy

Rationale:

1. To ensure that all users will adopt safe computing practices.
2. To ensure that users have a robust and stable computing environment.
3. To inform members of the minimum standards for data stored and/or transmitted from their network.

Policies:

1. All data will be “risk free” in terms of viruses to the best extent possible.
2. All email will be filtered for viruses.
3. All email will be filtered for inappropriate language.
4. All computer use will meet the terms of the Internet Safety Kit as defined by the documents relating to internet safety at www.netsafe.org.nz. It will be the responsibility of the member to promote internet safety to all users with access to computing resources.
5. Objectionable material as defined in (2) above will not be stored or transmitted using equipment connected to this network.
6. All hosted applications being used across the VPN must have the formal approval of VEN Ltd.
7. No network scanning or probing is permitted by any application or user to ensure there is no unwanted network traffic.
8. All computers on the network must have up to date virus protection and should be free of viruses.
9. All computers on the network should be up to date with regards OS updates.

Internet Usage Policy

Rationale:

1. To ensure that all users will use the internet for educationally sound purposes.

Policies:

1. All internet use will have a sound basis in education or educational administration.
2. Internet use of a nature that consumes bandwidth at an unacceptable rate is specifically prohibited when there is no clear educational use. Examples of such use includes (but may not be limited to):
 1. illegal downloading of music, video or software
 2. any activity that is illegal in NZ
 3. playing online games
 4. accessing pornography
 5. file sharing services

It is recognised that there will be times when the downloading of music or video files will have a valid educational purpose. However, it is generally accepted that this will be under strict teacher supervision and that in all likelihood teaching staff will have downloaded such files in advance for students and made them available on the school's own network, rather than have the students each download their own copy separately.

There will also be additional legitimate reasons for downloading large files from time to time. Such activities could include (but are not limited to): software updates (e.g. Microsoft Office, Administration package updates, operating system updates (in which case administrative installations should be performed so that a separate download is not required for every computer within an organisation); or the downloading of other software that the organisation has purchased over the internet.

3. Internet email use should be designed not to place stress on the available bandwidth. Large files should be compressed when attached. Only material that is relevant to education or educational administration should be sent as an attachment. The use of email to send collections of pictures or dubious .exe files that have been gathered from the internet is considered unacceptable use.
4. Using any email account inside the VPN for the purposes of spam or to defame or "flame" any person or organisation is considered unacceptable use.
5. All users are to comply with the Netsafe guidelines (www.netsafe.org.nz).

Associate Members Policy

Rationale:

It is recognised that associate members will wish to join the VPN in order to supply services to other VPN users. This policy has as its rationale:

1. To ensure that associate members have sound educational reasons for joining the VPN.
2. To inform associate members of the range of activities that may be considered acceptable when using the VPN.

Policies:

1. All associate member use will have a sound basis in education, educational administration, community education, continuing education.
2. All associate members will provide quality educational resources for schools and their communities.
3. Associate membership will be granted by the VEN Management Committee by majority vote.
4. Associate member use of VPN services shall be charged to the associate member at a rate to be determined from time to time by VEN Ltd.
5. It is expected that the associate member will, in general, directly charge other VPN members who use their services.
6. All associate member use shall conform to all other usage policies as they apply to other VPN members.
7. Associate member users will require connection bandwidth from the VPN to their own organisations at a rate which is sufficient to meet the needs of the service that they are providing. The bandwidth connection must meet the minimum carrier standards as defined by VEN.
8. No associate member user is permitted to act in such a manner as to cause bandwidth congestion for any other VPN user who has not subscribed to the service(s) being offered.
9. Associate member users may not exploit the VPN to promote their services to VPN members directly.
10. All associate members will be subject to ongoing review and random monitoring.

Videoconferencing Networks Policy

Rationale:

This policy has as its rationale:

1. To define minimum video conference system standards.
2. To define minimum network standards.
3. To define minimum video bridge standards.

Policies:

1. Video Conference System Standards

a. Must be international standards based:

- i. H.320 and H.323 compliant
- ii. Must be audio standards compliant
 - G.722 G.722.1, G.711, G.728
- iii. Must be video standards compliant
 - H.261, H.263++
- iv. Graphics - H.261 Annex D, 4 x CIF minimum in the H.320 and H.323 environments.
- v. FEC - Far End Camera Control - H.245
- vi. transmission of DMTF tones

b. Must be able to register with an H323 gatekeeper:

If a separate VPN uses their own H.323 gatekeeper software then that VPN neighbouring gatekeeper software must register with that of existing schools' networks.

c. Must be managed to maintain network operational standards as specified by VEN. The end point system must have web based management that enables:

- i. Sending a fault request to the centralised management system
- ii. Fault logging and recording
- iii. Software upload
- iv. Active monitoring
- v. Call detail records
- vi. Global address books
- vii. System management

d. Must be capable of 384k IP connectivity, and uphold the current network standard of 256k plus, reliably and consistently.

- e. Must send and receive H261 graphics inside a point to point and a multipoint environment in an H323 call.
- f. Must handle packet loss up to 2% without degradation to video or audio

2. Network Standards

- a. Discrete Virtual Private Networks must be reachable via a gateway
- b. Internet based routing between disparate networks should be avoided due to lack of reliability and QOS (Quality of Service).
- c. Must use an H323 enabled router and H323 enabled/capable firewall.
- d. The video conference endpoint must support Network Address Translation (NAT) and fixed ports if required, for communicating outside the VPN or through a DSL modem.
- e. Must be able to register with a gatekeeper with H323 identification and E.164 extension.
- f. Must support a 384k video call allowing for 20% overheads and nil packet loss
- g. latency below 300ms
- h. jitter below 30ms

3. Bridge Standards

- 1. Must be reliable and manageable
- 2. Must be international standards based: H.320 and H.323 (preferably in same chassis).
- 3. Must support Annex D graphic transfer = H.261 and H.263
- 4. Must have MCU cascade H.231 and H.243
- 5. Must have options of CP (Continuous Presence) with minimum of 4 x points of presence and audio switching.
- 6. Must enable IP to ISDN connectivity (Gateway facility).
- 7. Minimum audio specification G.711
Recommended audio specs include G.722, G722.1 and G.728
- 8. Minimum video specification H.261
Recommended video specs include H.262+ and H.263++, H264.
- 9. Data Standard H.243 LSD. (T.122/T.125 optional).
Channel aggregation H.221, bonding mode 1.

Videoconference Curricular Support Policy

Rationale:

This policy has as its rationale:

1. To define appropriate videoconference standards for schools, teachers and students.
2. To enable effective scheduling and timetabling of classes

Policies:

1. Every effort will be made by VEN and users to facilitate and accommodate those wishing to participate in VC activities. The timetabling of classes, tutorials, discussion forums and Professional Development activities requires a collaborative approach by users.
2. Scheduling of classes and enrolments of students need to be coordinated effectively. Use of the National Video Conference Website (currently managed by The Correspondence School) via coordinators is strongly recommended.
3. Where there is limited access to online classes or staffing, priorities will be identified (by school and cluster coordinators) along with the national broker to establish equitable access across the clusters.
4. Standards of behaviour and conduct in videoconference classes mirror those expected in face-to-face educational environments. The obligation to maintain these standards extends to all users - communities, business or others visiting the school and using the equipment. Standards of behaviour are the host schools responsibility.
5. Privacy issues for sites being dialed means that random calls via the VC equipment are not to be encouraged.
6. Minimum standards for the school support of teaching staff and students using the videoconference network include:
 - (a) Maximum class size of 4 sites x 4 students per site.
 - (b) Staff training to a professional level in the use of VC equipment i.e. Certificate in Tele teaching or its equivalent, by a provider recognized by VEN.
 - (c) Coordinated support, training and supervision of students in videoconferencing classes.
 - (d) Adequate provision of VC equipment and facilities (room and decor, furniture, lighting, phone line etc) to enable teaching staff to offer curricular support and classes of a high quality.
7. VEN fully supports and encourages schools to use the Learning communities online information found on the MoE website.

Onsite mail servers

Rationale:

1. Appropriate steps must be taken to ensure that schools do not act as an open mail relay

Policies:

These policies only apply to schools with an onsite mail server.

1. Open relays must be blocked by the school system to ensure that spammers are not able to use the school server to send unsolicited email.
2. All schools operating an Onsite server must ensure that only authenticated users can send email. E.g. refer to <http://www.msexchange.org/pages/article.asp?id=54>

General Network Usage

Rationale:

The network has an overarching prerogative that it is based in sound education and educational pedagogy.

This policy has as its rationale:

- 1 To ensure the network is used for valid educational outcomes.
- 1 To ensure that school needs are always at the forefront of VEN Ltd.
- 2 To define appropriate educational users and commercial activities within the VPN.
- 3 To define the levels of support expected.

Policy:

- 1 The VPN must be used for approved teaching and learning programmes. Such programmes are those undertaken by schools in their daily educational business. In addition schools may conduct classes outside of the normal school hours for programmes such as community education (see Appendix 4 for examples of acceptable usage)
- 2 Schools needs are always at the forefront of VEN Ltd. Each user will have the opportunity to share its views as to how VEN works. Regular communication will be actively encouraged and representation from the users will be sought on the VEN board of directors.
- 3 Schools are those as defined by the Ministry of Education. <http://www.tki.org.nz/e/schools>.
- 4 All suppliers of services within the VPN must support the users with a helpdesk approved by VEN Ltd. The criteria for a helpdesk is as defined in Appendix 5.

Appendix 1: IP Addressing Scheme

All TCP/IP-connected devices will use an IP addressing scheme as defined by VEN Ltd. The IP addresses will be private “Class C” addresses in the range 10.x.y.z. The values x and y will be defined to each member by VEN Ltd.

z values are defined as:

The IP addresses 10.x.y.51 to 10.x.y.254 will be dynamically allocated to workstations by the router with an infinite lease. No other DHCP server will be permitted to operate on the network.

The IP addresses 10.x.y.1 to 10.x.y.50 will be static and will be allocated as follows:

10. x.y.1	router
10. x.y.2	member’s own central server
10. x.y.3	member’s own proxy server (if it exists)
10. x.y.5 - 10.x.y.10	reserved for future allocation
10. x.y.11 - 10.x.y.30	for general use by the member as the member sees fit
10. x.y.31 - 10.x.y.50	network connected printers

The router will dynamically deliver the gateway address of 10.x.y.1 to those computers that are able to accept it. Other computers will need to have this gateway address set manually.

The subnet mask will be 255.255.255.0 and the gateway IP will be 10.x.y.1

Additional IP address ranges are available through to 10.x.y+15,254/255.255.240.0

Required DNS servers are available at 172.31.232.10 (primary) and 172.31.232.5 (secondary).

If a member wishes they may operate their own DHCP server instead of using the supplied router. However, all members will need to ensure that their addressing scheme complies with the above requirements. DNS and Gateway addresses can be distributed by the DHCP server on the router.

Video Conferencing units will be allocated a specific private IP number in a different range to permit the prioritisation of VC data on the network. This IP number is 10.250.x.y+2 and additional addresses are available to IP 10.250.x.y+14

The subnet mask will be 255.255.255.240 and the gateway IP will be 10.250.x.y+1

The gatekeeper IP will be at 10.120.0.70:1719

Where possible connect VC equipment directly to a port on the router to eliminate local network congestion.

Members may connect via their own proxy server and keep their existing IP scheme, in which case the upstream NIC must conform to the IP addressing scheme and the local proxy server must be capable of authenticating to the upstream proxy servers. Members will then be responsible for managing their own proxy server themselves.

See: <http://www.virtualeducation.net/nz/nzip/index.asp>

Appendix 2: Technical standards for carriers

Telecommunications Carrier Standards for Videoconferencing

1. Compliance with VEN Ltd policies

Telecommunication carriers must be a member of the Virtual Private Network administered by Virtual Education Networks (VEN) Ltd, and must use reasonable endeavours to comply with the relevant policies promulgated by VEN.

Similarly, Telecommunication carriers must impose a similar requirement on any customers who will have access to the Videoconferencing Service.

2. IP addressing

All TCP/IP connected devices will use the IP addressing scheme defined by, and as amended from time to time by, VEN Ltd.

3. Standards

The Telecommunication carrier's videoconference service must be international standards based:

- i. H.320 and H.323 compliant
- ii. Compliant with the audio standards: G.722, G.722.1, G.711, and G.728
- iii. Compliant with the video standards: H.261 and H.263.
- iv. Compliant with the graphics standard H.261 Annex D, providing 4 x CIF minimum in the H.320 and H.323 environments.
- v. Compliant with the H.245 standard for Far End Camera Control.
- vi. Provide for the transmission of DTMF tones.

4. Bandwidth

The Telecommunication carrier's network must support a minimum of 256kb/s and a maximum of 384kb/s video call allowing for 20% overheads and nil packet loss.

5. Availability

Availability of Telecommunication carrier's network must be sufficient to allow a video conference (end-to-end) service availability of greater than 99.3%, 24x7.

6. Packet Loss

Packet loss is not to exceed 2%. (Averaged over 1 Month)

7. Latency

Latency should not exceed 300ms.

8. Jitter

Jitter must not exceed 30ms.

9. Security

A H.323 enabled router and a H.323 enabled/capable firewall must be used.

Must be able to register with a gatekeeper with H.323 identification and E.164 extension.

10. Faults

Telecommunication carriers must provide first level fault reception and diagnosis, in order to, as far as possible, locate whether the fault is within the customer's equipment, Telecommunication carriers network, or the MoE bridge. In relation to those faults believed to be within the MoE bridge, Telecommunication carriers should report the fault to the MoE through the MoE's nominated channels and provide the MoE with any relevant diagnostic information. Telecommunication carriers must not advise the customer to call the MoE in relation to the fault.

Fault reception should be available 24x7.

Fault handling should be provided 7am – 7 pm, Mon-Fri.

Any planned outages should be scheduled to occur between the hours of 2am to 7am.

11. Guest Access

Guest access (by non-school participants) will be covered by separate commercial arrangements between the parties. Guest access is not provided for under the standard access agreement for the MoE bridge.

12. Reporting and information

Telecommunication carriers must advise MoE of the identities of all parties (i.e. customers and any other parties) provided with access to the bridge.

Telecommunication carriers must report to VEN at least quarterly on the achievement against items 5, 6, 7, and 8 above.

13. Service Experience

Connections to the MoE videoconference bridge originating on Telecommunication carriers network, must not degrade the service experience of users on other Networks connected to the MoE bridge.

14. Help Desk

Telecommunication carriers should provide a Help Desk service to assist customers make effective use of their videoconference service. This help desk should be available 8am – 5pm, Mon-Fri.

Appendix 3: Time Servers

It is seen as desirable to ensure that all users have a consistent method for accessing time services within the VPN.

To this end VEN Ltd would strongly encourage all members to adopt time synchronisation as a standard to allow for accurate date and time stamping of all files and thus avoid problems that can arise from spurious time and date reconfiguration from otherwise well intentioned users.

1. All administrators of Win32 servers at IP 10.x.y.2 are encouraged to use the following software for time services:

Atomic Clock Sync v2.6 - download for free from <http://www.worldtimeserver.com>

This software should synchronise time with the time server at 205.188.185.33

2. All computers on the local network should synchronise their time with the local server.
3. A time server is available on the SchoolZone VPN at:

172.31.232.2:123

Details for Linux / Unix / Apple systems have yet to be finalised.

Appendix 4: Educational activities for Associate Membership

The following are typical groups who may apply for associate membership and the activities that they may undertake:

- Teacher training institutes
- Teacher support services
- Teacher education programmes
- Qualification providers
- Subject associations
- Curriculum deliverers
- Special event course suppliers
- Community Education course suppliers
- Continuing education programmes
- Board of Trustee meeting
- Students and parent interviews
- Guest speaker
- Invitational forum
- Peer support
- Staff and student forums
- Education application software suppliers
- Star funded course suppliers