

PPN Technical Reference

Date Created: September 5, 2008
Last Updated: September 9, 2010
Final Version: V1.2





Disclaimer

The Province of British Columbia cannot guarantee the accuracy of this document's contents. By proceeding with the information in this document, each reader waives and releases the Province of British Columbia, its employees, representatives and contractors, to the full extent permitted by law from any and all claims related to the usage of material or information made available. In no event shall the Province of British Columbia, its employees, representatives or contractors, be liable for any incidental or consequential damages resulting from the use of this material.

Copyright © Province of British Columbia

All rights reserved



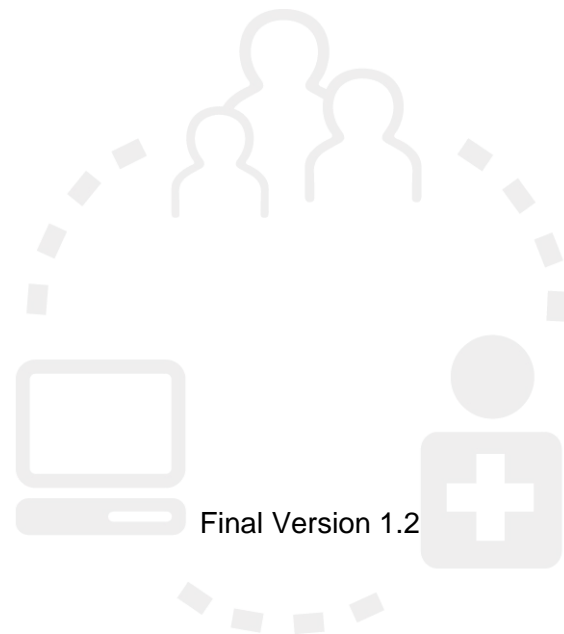
Table of Contents

1.0	Preparing for the PPN	6
1.1	TELUS Router	6
1.2	Demarc Location	6
1.3	Building Wiring	6
1.4	Practice Local Area Network (LAN)	7
	1.4.1 No Existing Practice LAN	7
	1.4.2 Existing Practice LAN	7
	1.4.3 Multi Practice Buildings	8
	1.4.4 Multi Location Practices	8
1.5	Firewalls	8
2.0	Connecting to the PPN	10
2.1	PPN Design Features	10
2.2	TELUS Router Equipment	10
	2.2.1 ADSL, Copper Routers	10
	2.2.2 Fibre Routers	12
2.3	PPN IP Addressing	13
2.4	Practice LAN	13
	2.4.1 Network Switch (layer 2) Configuration	14
	2.4.2 Special PPN2 Connection and Configuration Requirements	15
2.5	Email	17
Appendix A - TELUS Site Readiness Guidelines		18
Appendix B - PPN Core Firewall Rules		19
Appendix C – TELUS Router Sizing Options		21
Appendix D – Network Performance and the TELUS Router		22
D.1	Network Infrastructure Context	22
D.2	TELUS Router Performance Characteristics	22
D.3	PPN Internet Performance	23
D.4	Practice Performance Profile	23

Figures

Figure 1	ADSL, Copper Router Front Panel	10
Figure 2	ADSL, Copper Router Back Panel	11
Figure 3	Fibre Router Front Panel	12
Figure 4	Fibre Router Rear Panel	12
Figure 5	PPN2 Configuration Example	16

Tables





Purpose of This Document

This document provides key technical information useful in preparing for the Private Physician Network (PPN) installation, as well as configuring and connecting a practice's network to the PPN.

It is intended to be used primarily by the person(s) providing technical support services for the practice's local computer environment. As well, the person(s) in the practice who is leading the migration to the PPN should review the document sections on preparing for the PPN to ensure the practice completes all of the preparation activities well in advance of the PPN installation date.

Note: The information in this document does not apply to practices connecting to the PPN through a gateway at their local Health Authority (including Northern Health Physician Connect Network and Vancouver Coastal Health's Diamond Centre). These practices should, instead, refer to the ***“PPN Health Authority Gateway Primer”*** and dialogue directly with their Health Authority.

Related Documents

The following PPN documents are available on the PITO website at www.pito.bc.ca under its 'Document Library' section:

- Welcome to the PPN: A summary for physicians and staff of key PPN features;
- PPN Primer: A complete description of the PPN service and key practice responsibilities;
- EMR and PPN Implementation Checklist: Identifies the key activities involved in implementing a PITO-qualified EMR application and the PPN at a practice. It identifies which party is responsible for performing and managing each activity as well as the expected timeline to complete;
- PPN Support Quick Reference: A summary for physicians and staff outlining the support available to their practice through their EMR vendor and TELUS;
- EMR and PPN Support Responsibility Matrix: A detailed description of the roles and responsibilities for all parties involved in supporting EMR and PPN implementations through PITO;
- Remote Access to the PPN : A user guide for setting up and using the VPN service for staff who connect to the PPN from outside of the practice (e.g. home); and
- PPN Firewall Change Request Form: A form for practices to submit requests for additional Internet based applications to be allowed through the PPN core firewall.



1.0 Preparing for the PPN

1.1 TELUS Router

Working with the PITO relationship manager (RM), the practice needs to select the type, size and capacity of the TELUS router equipment to be installed at the practice. The RM will prepare the router order for the practice with the Ministry of Health Services and TELUS.



See Appendix C of this document for sizing options for the TELUS router installed at a practice.

For some rural or remote locations, TELUS will not have an ADSL/copper based service available in that area to allow for the 'PPN-1 – Asymmetric' or 'PPN-2 – 2X Asymmetric' router to be installed. In these cases, TELUS will then determine if a T1 based symmetric service called "PPN-1 (ER) – 1.5 Mbps" can be provisioned. If available, then on Ministry approval TELUS would proceed with its installation.

1.2 Demarc Location

The practice needs to determine the demarc location where TELUS will install the router equipment at the practice. The practice must collaborate in ensuring a high availability service by choosing a suitable and secure location for the TELUS router equipment, typically in an existing telephone or wiring closet. For effective support, the demarc location must also be easily accessible to any support staff arriving on site to troubleshoot problems with the equipment.

See Appendix A for site readiness guidelines, provided by TELUS, which each practice needs to comply with. Any practice activities to prepare the demarc location should be done well in advance of the PPN installation date.

1.3 Building Wiring

Practices are responsible for obtaining and arranging for all rights of way, permissions, and/or third party consents for TELUS to install or upgrade any required PPN network wiring from the property line to the practice's demarc location within their office building. This wiring will be either copper or fibre depending on the router selected for practice.

This is the standard approach for telephony and data services installation from industry vendors.

TELUS will identify any building and/or conduit upgrade requirements and if required communicates this to the practice's main contact for action. For fibre based services, TELUS assesses this during a pre-field inspection soon after the PPN is ordered. For ADSL based services, TELUS assesses this at time of install. The practice is responsible for any costs for the installation or upgrading of conduit required to run TELUS wire or cable from the property line to the practice's demarc location.

1.4 Practice Local Area Network (LAN)

The practice must arrange and provide for all of their LAN network equipment and wiring.

All computers that connect to the practice LAN must abide by PITO security policies that include use of up-to-date antivirus software and personal firewall technology. These security policies along with the technical architecture of the PPN exist to protect EMR data and physician workstations from external security threats.



Refer to the PITO Policies document under the 'Documents Library' section at www.pito.bc.ca, section 8-Privacy & Security Policies, for more information on computer and LAN security requirements.

One key security policy prescribes that the practice LAN (connected to the PPN) cannot interconnect to any other network including commercial Internet services. Yet additional requirements for connecting and integrating some practice networks with the PPN have been identified during the rollout to date. These requirements include remote LAN access for practice staff, remote LAN hardware and software support, practice managed business applications, and high Internet bandwidth needs. Technical solutions for these additional requirements are provided in an 'PPN Additional Requirement and Solution Summary' document.



Refer to the PPN Additional Requirement and Solution Summary document under the 'Documents Library' section at www.pito.bc.ca, for more information on additional practice requirements and technical solutions available to address them.

1.4.1 No Existing Practice LAN

Practices which do not currently have an Internet connection will need to arrange for network wiring installation in the practice (e.g. Cat 5E cabling) to connect:

- Computers and printers to a practice LAN; and
- The practice LAN into the TELUS router equipment.

The practice's technical support resource or a more specialized network vendor should be used for any network wiring installation.

1.4.2 Existing Practice LAN

Practices which already have LANs in place with high speed Internet connections may already meet the standards for connection to the PPN.

Preparing for the PPN also provides an opportunity to re-evaluate the practice's LAN needs. Any costs for upgrading a practice's LAN are the responsibility of the practice. Keeping the future in mind, consider the following:

- Are there additional locations in the practice where it would be useful to have network access?
- Are there additional computers, printers and other devices that should be added to the practice network?
- Can current wireless computers connect to a more reliable and high speed wired network connection? Using wired network connections is the recommended approach for security reasons.



Refer to the PITO Policies document under the 'Documents Library' section at www.pito.bc.ca, section 8-Privacy & Security Policies, for more information on wireless network security requirements.

1.4.3 Multi Practice Buildings

If multiple practices are located in the same building, the Ministry of Health Services may direct TELUS to install a PPN network router to be shared by PITO registered physicians in the building. This router will be placed in a secure location within the building (e.g. master telephone closet) and each practice will be connected to it. The network traffic passing from each practice through the router will not be visible to the other practices network traffic. Network speed will be equivalent or greater to that of a standalone practice connection.

1.4.4 Multi Location Practices

By default, as part of the PPN security, network traffic to and from one practice is not visible at other practices, and a practice LAN at one location cannot connect over the PPN to a LAN at a different location. For practices that operate over more than one business location where LAN visibility between the separate locations is required, they need to initiate a special request to TELUS through their PITO RM, to enable this.

1.5 Firewalls

TELUS manages a firewall within the PPN core to control Internet destined network traffic that passes in and out of the PPN. The Ministry of Health Services has provided firewall rules to TELUS to determine which traffic is allowed and denied. Note that these firewall rules also apply to network traffic between the physician office and their EMR application at EMR vendor's data centre.

The firewall rules allow for standard Internet traffic over HTTP (port 80) and HTTPS (port 443). This allows for a large majority of Internet sites to be accessed through the PPN. Applications that don't use standard Internet protocols are added on an exception basis based on clinic business need and an assessment of risk to PPN security. To date, a select set of applications required by the EMR/PPN solution and not using the standard Internet protocol/ports, have been allowed through the firewall.

See Appendix B for the list of current applications allowed through the PPN Core firewall. A summary of currently allowed applications are:

- Internet sites available through standards protocols/ports - HTTP/80 and HTTPS/443;
- PITO qualified EMR vendor applications;
- Health Authority portals: Access to VCH, VIHA, FHA, and IHA portals. PHSA and NH access will be allowed as practice needs arise;
- Email clients (e.g. MS Outlook) using standard protocols (POP,IMAP, SMTP); and
- Additional applications, included on a case by case basis.

As additional clinical application needs are identified during the rollout of the PPN to practices across the Province, the list of allowed applications is expected to expand.

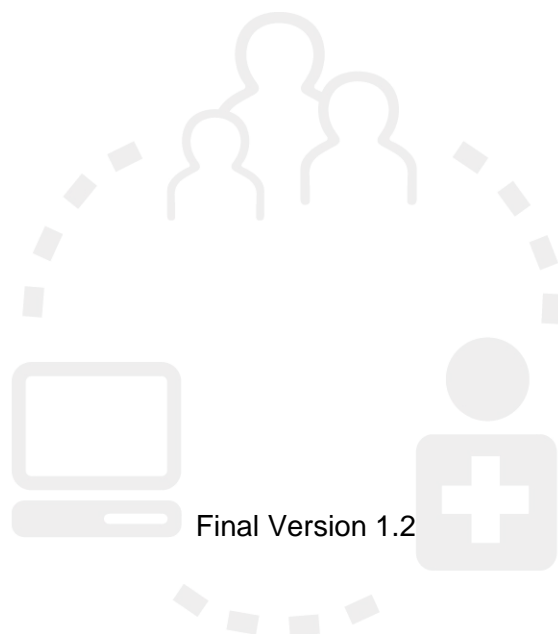
Each practice needs to assess which Internet based applications their staff uses, along with the network ports and protocols the application requires. The practice's technical support resource should be engaged to investigate this, as technical expertise is required.

If there is a clinical need to use an application not currently supported with existing PPN core firewall rules, the practice will need to make a request to add it. All requests are assessed by the Ministry of Health Services to ensure they do not pose an unacceptable security risk to the PPN network.



To send requests for additional Internet based application to be allowed through the PPN core firewall, complete the PPN Firewall Change Request Form available under the 'Documents Library' section at www.pito.bc.ca, and send to the contact identified within. This form captures the application name, the protocols and ports it requires to be opened in the firewall, and the clinical need for using the application.

While TELUS manages firewalls and security services within the PPN, each practice is responsible for managing firewall, anti-virus and other security software installation on the computers connecting to their LAN. Each practice is responsible for contracting with a computer support organization or individual to provide the practice-based technology required to run their business. Physicians should contact the resource(s) responsible for providing these services for more information about the security measures that should be established with local computers.





2.0 Connecting to the PPN

2.1 PPN Design Features

The key PPN design features to be considered when you are connecting your practice's LAN to the PPN are:

- Router capacity at each practice has been primarily sized for the network bandwidth required for use of the EMR vendor application (hosted at their data centre), and Internet browsing related to clinical activities;
- Firewall, antivirus, and intrusion protection appliances are installed in both of the PPN cores (Vancouver, Kelowna) sites and network traffic entering and leaving the PPN must flow through them;
- The PPN incorporates a private IP address space, and the IP addresses assigned to each practice are not resolvable on the public Internet;
- Network traffic that originates outside of the PPN will not be permitted into the network. Email services will continue to operate as before as requests to access, retrieve or send emails are always initiated within the PPN; and
- Dynamic, DHCP IP addressing is utilized for the PCs connecting within the practice LAN to the PPN. The capability to assign static IP addresses to select LAN devices (e.g. printers) is also provided.

Also by default (which can be changed by a special request to TELUS through your PITO RM):

- PPN network traffic to and from one practice is not visible at other practices; and
- A practice LAN at one location cannot connect over the PPN to a LAN at a different location.

2.2 TELUS Router Equipment

The practice LAN will need to connect to the PPN router equipment installed at the demarc location. TELUS routers are connected to via industry standard Ethernet connections.

Diagrams are provided below to depict representative PPN router equipment utilized by TELUS for both their ADSL, copper (PPN-1 / PPN-2) and fibre (PPN-3 / PPN-4) based services.

Note: that a dial up modem is installed in tandem with each router. It provides TELUS with another channel for monitoring their PPN router at each practice location.

2.2.1 ADSL, Copper Routers

For the 'PPN-1 – Asymmetric' and 'PPN-2 – 2X Asymmetric' routers, a Cisco 1841 router is provided below as a representative model - the actual model installed at your practice may vary.

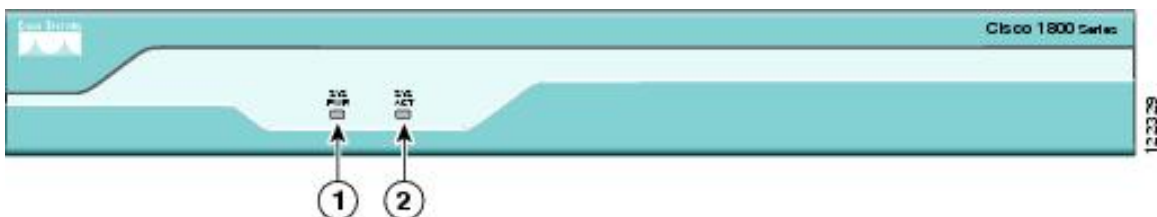


Figure 1 ADSL, Copper Router Front Panel

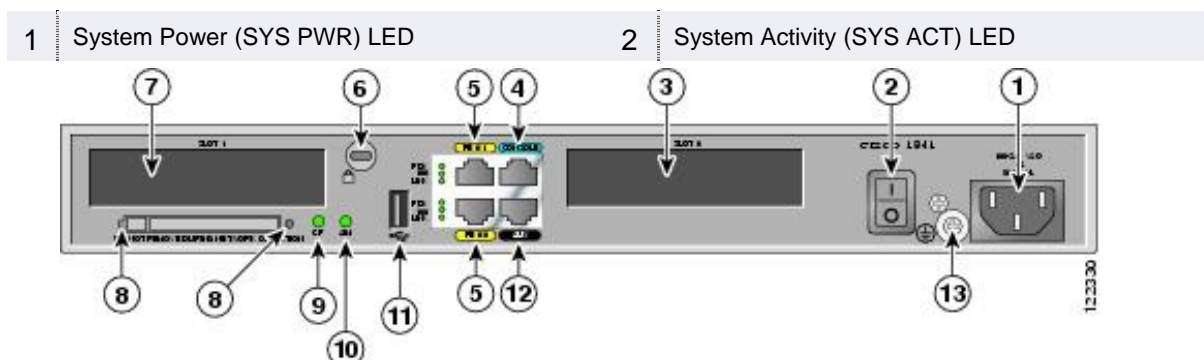


Figure 2 ADSL, Copper Router Back Panel

1	Input power connection	8	CompactFlash memory card slot
2	On/Off switch	9	CompactFlash (CF) LED
3	Slot 0 (WIC, VWIC—data only, or HWIC)	10	AIM LED
4	Console port	11	USB port
5	Fast Ethernet ports and LEDs	12	Aux port
6	Kensington™ security slot	13	Chassis ground connection
7	Slot 1 (WIC, VWIC—data only, or HWIC)		

LED	State	Meaning
SYS PWR	Off	No output from the internal power supply.
	Solid green	Router is receiving power, and the internal power supply is functional.
	Blinking green	During bootup, router is booting up normally. After bootup, router is operating in ROM monitor mode.
SYS ACT	Off	No packet transfers are occurring.
	Blinking	System is actively transferring packets and monitoring internal activity
CF	Off	The CompactFlash memory card is not being accessed.
	Blinking green	The CompactFlash memory card is being accessed.
FDX	Off	Fast Ethernet port next to the LED is operating in half-duplex mode.
	Solid green	Fast Ethernet port next to the LED is operating in full-duplex mode.
100	Off	Fast Ethernet port next to the LED is operating at 10 Mbps.
	Solid green	Fast Ethernet port next to the LED is operating at 100 Mbps.

Link	Off	Fast Ethernet link is not established at the Ethernet port next to the LED.
	Solid green	Fast Ethernet link is established at the Ethernet port next to the LED.
AIM	Off	No AIM is installed
	Solid green	AIM is recognized by the router and is initialized.

2.2.2 Fibre Routers

For the 'PPN-3 – 10Mbps' and 'PPN-4 – 100Mbps' fibre based routers, a Cisco ME 3400-24TS model is provided below as a representative model.

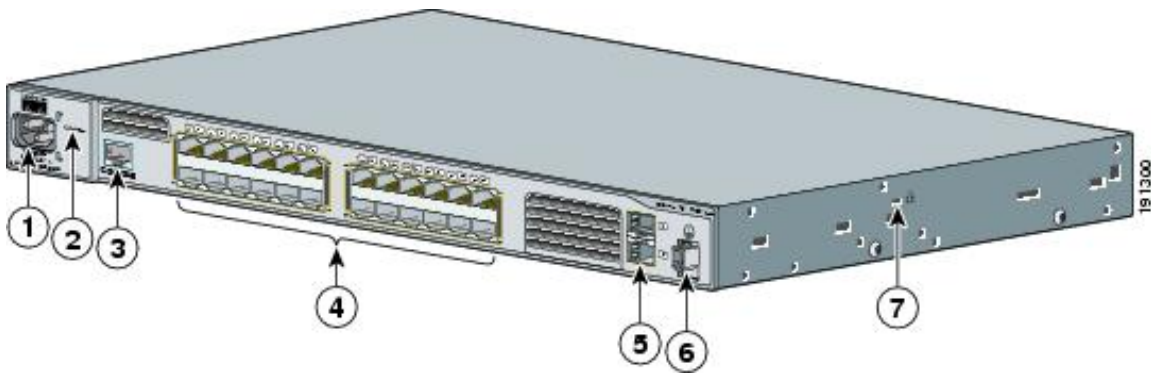


Figure 3 Fibre Router Front Panel

1	AC power connector	5	Gigabit Ethernet SFP module ports
2	System LED	6	Ground connector
3	Console port	7	Cable lock
4	10/100 Fast Ethernet ports		

Rear Panel

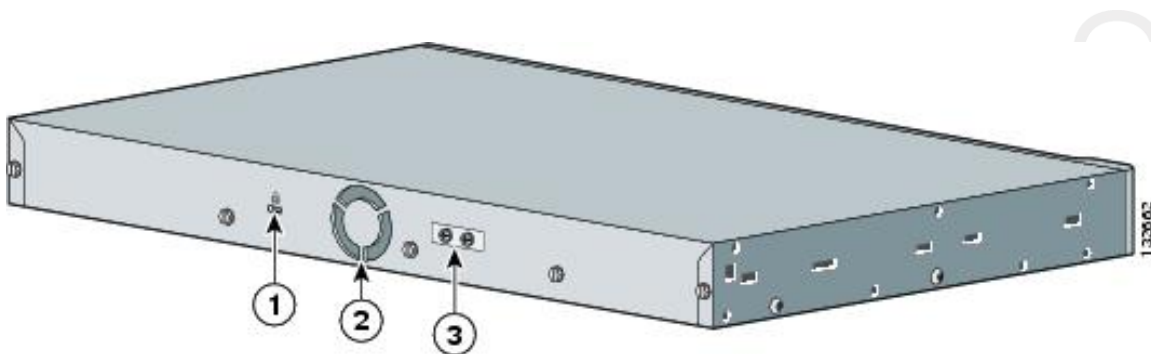
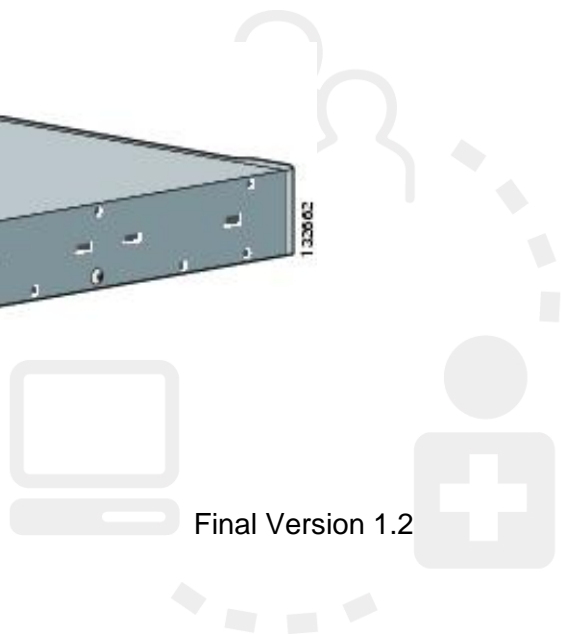


Figure 4 Fibre Router Rear Panel



- 1 Cable lock
- 2 Fan exhaust

- 3 Ground connector

LED	State	Meaning
System	Off	System is not powered on.
	Blinking green	POST is in progress.
	Green	System is operating normally.
	Amber	System is receiving power but is not functioning properly.
Port LED	Off	No link, or port was administratively shut down.
	Green	Link present but not sending or receiving data.
	Blinking green	Activity. Port is sending or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Amber	Port is disabled.

2.3 PPN IP Addressing

The PPN has been designed to primarily use dynamic IP addressing. Computers connecting to the PPN through the practice LAN are typically configured to request and receive a dynamic IP address (with lease) from the PPN DHCP servers residing within the core network. The TELUS network architecture utilizes two geographically redundant DHCP servers.

Each physician practice is assigned a unique subnet range within the PPN with the size of the subnet associated to the size and capacity of the installed TELUS router equipment. The IP addresses within the subnet range are privately addressable within the PPN and are not resolvable on the public Internet.

Each provided subnet has a range of dynamic as well as static IP addresses for assignment to the computers and printers on the practice's LAN. The static IPs can be assigned to the devices (e.g. printers) that need to be permanently visible to the computers connecting to the practice LAN.

The PPN network assignments unique to each practice, including router identification and IP addressing, are provided to the practice's EMR vendor at the time of PPN installation, who then pass the assignments along to the main practice contact as required. Assignments include the practice's subnet and gateway address, as well as static and dynamic IP address ranges.

2.4 Practice LAN

The practice continues to be responsible for all of the practice related hardware, software and network (LAN) infrastructure, including its security up to the point of connection into the TELUS router equipment.

The practice must not install its own router between the PPN router equipment and its LAN. A network switch (layer 2) is expected to be the standard interconnection point between the practice's computers/devices and the TELUS router equipment.

The practice's technical support will configure its computers to acquire IP addresses from the PPN core DHCP server. They will also assign static IPs to devices (e.g. printers, servers) requiring permanent visibility on the practice LAN, from the assigned range provided by TELUS. Any practice devices that

have been assigned static IP addresses on a pre-existing LAN, must be changed to a PPN static IP address to be visible on the LAN after migrating to the PPN.

2.4.1 Network Switch (layer 2) Configuration

PPN Routers for the PPN-1, PPN-2, and PPN-3 services are by default configured to automatically negotiate speed and duplex settings with the practice network LAN switch (i.e. auto/auto setting). Most practice network LAN switches are expected by default to also 'auto-negotiate' both the speed and method of transmission (i.e. auto/auto) with the PPN router and, by doing so, should interoperate successfully.

On exception, a practice network LAN switch may not successfully negotiate speed and duplex settings with the PPN router. Some symptoms of this are, but are not limited to, data packet losses, slower PPN performance, problems with printing or other LAN devices.

To ensure successful interoperation, prior to or at time of turning up the practice LAN to run live over the PPN, your EMR vendor must arrange a interface test (practice LAN switch to PPN router) with a TELUS provisioner.



To schedule an interface test, EMR vendors send an email to PPNTURNUP@telus.com. A date/time is mutually agreed for practice technical support person, a TELUS provisioner, and optionally EMR vendor contact, to be on hand to test and if required correct or adjust the speed and duplex settings.

During the interface test, if determined the practice network LAN switch is not successfully negotiating speed and duplex settings with the PPN router:

- If a managed switch (able to configure through an interface) then the practice's technical support person should view the error log on the WAN-LAN interface and adjust the switch to the PPN router's default speed/method;
- If an un-managed switch (no configuration is possible), then the TELUS provisioner should configure the PPN router's default speed/method to a setting compatible with the LAN switch.

Based on experiences to date with connecting a variety of practice LAN switches to the PPN routers, it is recommended that:

- Practices over-ride the default 'auto-negotiate' LAN switch setting to assign a hardcoded value (e.g 10 or 100 full duplex) in conjunction with TELUS applying the **same** setting to the PPN router. If the hardcoded values on the LAN switch and PPN router are **different**, network interface and performance issues will result.
- Practices using an un-managed LAN switch should upgrade to a managed switch that can be manually configured to optimal settings, and provides diagnostic information when problems arise.

For any post go live issues with LAN/PPN speed and duplex settings, the practice's technical support person should follow regular support procedures through the EMR vendor Tier 1 helpdesk.

The practice technical support person can test the LAN/PPN interface at any time by pinging the gateway IP on the PPN router – an error free ping indicates the interface settings are valid. The steps to execute this test are:

1. Run a trace route to any Internet site to identify your practice's PPN gateway IP address:

Tracert 10.xxx.xxx.xxx

2. Ping the PPN gateway IP address (returned in the prior step) and review the result to identify if errors or packet loss has occurred – if so this indicates a likely speed or duplex mis-match:

```
Ping -n 100 10.xxx.xxx.xxx  
Pathping -n 10.xxx.xxx.xxx
```

2.4.2 Special PPN2 Connection and Configuration Requirements

If the PPN-2 (2 X Asymmetric) service is selected for the practice, TELUS installs 2 ADSL routers (essentially two individual PPN-1 services) at the practice demarc location. This service does not increase network bandwidth beyond that of a single PPN-1 (ADSL) service, yet it does increase capacity to allow more practice users to be connected concurrently to the PPN. Although two routers are installed, the PPN-2 service is not intended to provide automated failover between the two devices – the second router is to increase PPN capacity only.

To use the PPN-2 service, the practice LAN will need to simultaneously connect to both routers. The standard LAN configuration is expected to use an industry standard ('layer 2') network switch to interconnect both TELUS routers along with all of the other practice's devices (eg. PCs, printers).

The ports of the network switch into which the 2 PPN routers are connected, must be compatible with the routers' speed/duplex configuration (see previous section 2.4.1 for further details).

All devices (computers, printers, etc.) will be visible on the practice LAN even though two separate TELUS routers are providing the connection to the PPN.

With two PPN routers connected into the practice LAN switch, and each providing its own subnet of static and dynamic PPN IP addresses, the practice technical support resource has options to choose the best IP address allocation for the practice:

- For computers chosen for dynamic/DHCP address configuration, their broadcast for an IP address should randomly assign them to either PPN router, balancing the practice's network workload across both routers;
- For devices selected for static IP address allocation (e.g. printers, servers), consideration is required to assign devices to particular subnets to minimize network traffic between the routers when printing or copying files.

Technical characteristics of the PPN2 service are further depicted and described in the following diagram.

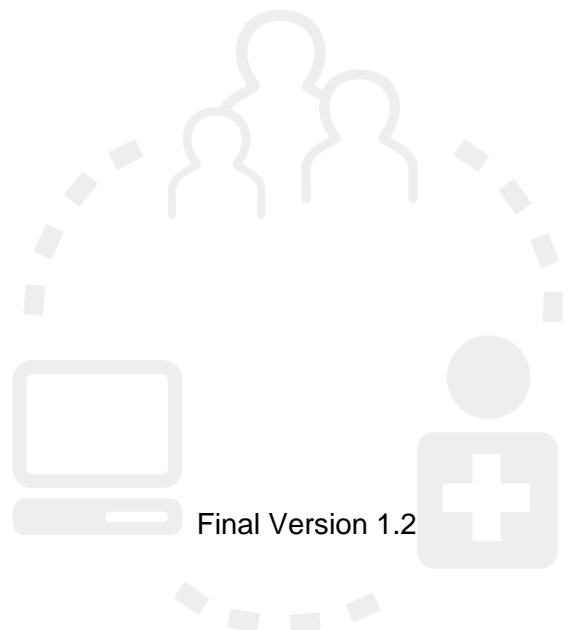
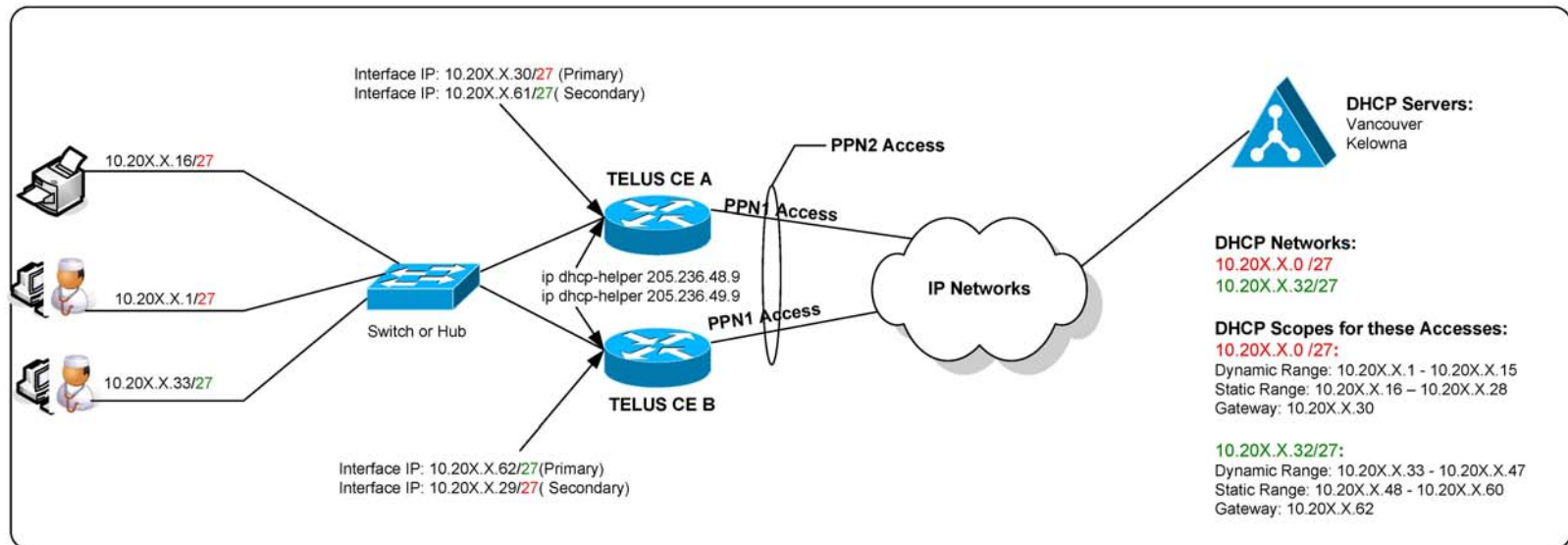
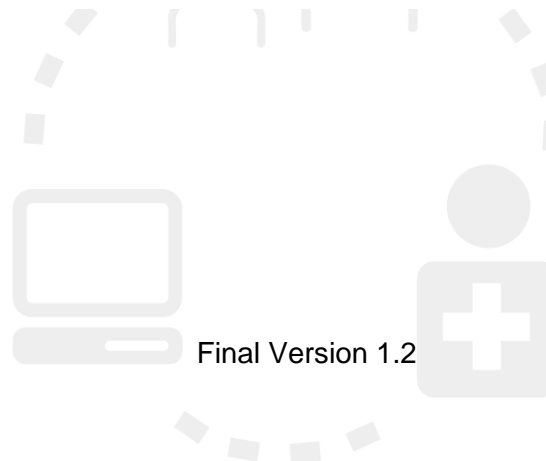


Figure 5 PPN2 Configuration Example



Notes:

- DHCP request is broadcast to both CE's, and to both DHCP servers
- Responses are returned via both CE's, from both DHCP servers
- The Client will complete a DHCP transaction with the first scope to respond
- The first one to complete will become the Gateway
- Gateway assignment by this method is random, however is very likely to produce a reasonably balanced distribution of traffic
- There is a required single flat layer 2 network assumed here (Single VLAN switch or dumb hub)
- All users and devices will find each other via the LANside interface of the CE's



2.5 Email

The PPN supports access to a practice's external email service (e.g. Shaw, Yahoo, Gmail) either through web access or an email client.

Web Access (or webmail):

- Is available for external email services that provide this feature (e.g. <https://webmail.shaw.ca>). Access to the external email service (using HTTPS protocol) is allowed through the PPN firewall.

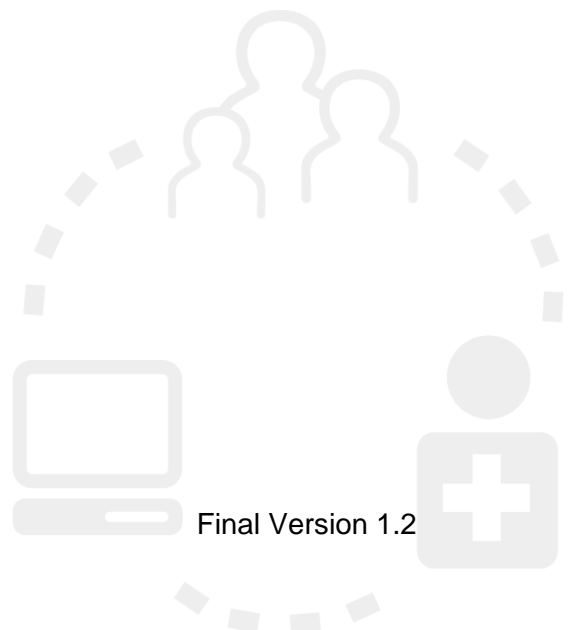
Email Client:

- Standard email clients (e.g. MS Outlook, Thunderbird) are able to access external mail services (e.g. Shaw, Yahoo, etc) from the PPN, yet the practice's technical support will need to investigate, apply and test any special email client configuration requirements after connecting to the PPN.
- The PPN restricts the assignment of any outgoing mail (SMTP) server to a specific TELUS server ('smtp.telus.net'). This TELUS 'smtp' server has security mechanisms in place to detect and block SPAM from being sent out of the PPN network. Except for the outgoing mail server assignment, the practice's technical support will follow all other email client configuration instructions provided by the email service provider.

NOTE: As an example, if Shaw email is used, their configuration instruction states that Shaw's outgoing email server cannot be used when not on a Shaw Internet connection. Here is the Shaw guidance on configuring various email clients to access their service:

<http://www.shaw.ca/en-ca/CustomerCare/InternetSupport/Residential/Email/RemotePOPAccess.htm>

For the PPN, all Shaw instructions would be followed except the outgoing mail server (SMTP) for any email client must be set to 'smtp.telus.net'.





Appendix A - TELUS Site Readiness Guidelines

As TELUS provides, installs and monitors their router equipment at the practice location, space and environment guidelines must be adhered to by the practice. In order for TELUS to provide, install and monitor their equipment in a safe and effective manner, the practice must provide the following:

Physical Security:

- Please note that the physician or practice contact must adhere to all PITO physical security requirements for the equipment. TELUS will install to the identified demarcation point, but the clinic is responsible for any equipment or facilities beyond the demarcation.

DSL or Asymmetric Based Services – PPN-1, PPN-2:

- A/C power from a dedicated 15 amp circuit ;
- Note: TELUS prefers to install router equipment (or CIU, Customer Interface Unit) in an equipment rack if available in a telecom or data equipment room;
- Ideally provide a telephone closet with rack or wall mounting space;
- At the very least, a shelf or dedicated space must be provided for the router and modem. This equipment is different from consumer based services, with a larger router (about the size of a large laptop) and an associated dial up modem. It is continually monitored and any disruption to power or cables will cause alarms;
- The equipment must be well ventilated and not subjected to high temperatures; and
- The equipment cannot be on the floor or under a desk or on a desk or in a location where it might be expected to encounter conditions that could cause disruption.

Fibre Based Services – PPN-3, PPN-4:

- A/C power from a dedicated 15 amp circuit ;
- Note TELUS prefers to install router equipment (or CIU, Customer Interface Unit) in an equipment rack if available in a telecom or data equipment room;
- For locations using a PPN fibre service, provide a minimum 4 foot by 4 foot space on the wall in the main telephone room to mount the patch panel and associated router and modem; and
- Network termination equipment rooms shall be well lit with good access to the equipment. Rooms shall be well ventilated and not subjected to high temperatures.



Appendix B - PPN Core Firewall Rules

The list of applications whose network traffic is allowed through the PPN firewall is provided in the table below.

Note that any application that uses Internet standard HTTP (port 80) or HTTPS (port 443) will be permitted by default through the PPN firewall.

Application	Network Protocols / Ports Used	Comments
Web Browser(s) – general internet sites	HTTP: port 80 HTTPS: port 443	For general Internet sites using standard protocols, browser access to a variety of Internet websites is permitted, including: <ul style="list-style-type: none"> ○ Search engines (eg. Google) ○ Instant Messaging (MSN, etc) ○ Clinical information/online references such as Epocrates and UptoDate, Excelleris MD consult etc ○ Business contact sites (Plaxo, Linked-In) ○ WEBEX web conferencing site which uses port 80 as second option ○ Banking sites ○ Updates/Downloads from Microsoft: Office and OS ○ Antivirus, Antispyware Updates: Norton, Symantec, AVG, McAfee ○ Internet fax service: My Fax ○ Software Updates: Adobe ○ Personal email webaccess (Shaw, Telus, Yahoo, Hotmail etc) ○ BCMA videoconferencing access ○ Evernote: note capture and indexing
Web Browser(s) – clinical applications	HTTP: port 80 HTTPS: port 443	For clinically related Internet sites using standard protocols, browser access to a variety of these sites is permitted, including: <ul style="list-style-type: none"> ○ CDM toolkit: https://healthregistry.moh.hnet.bc.ca/ (for production) and https://hnwe1.moh.hnet.bc.ca/ (for training).
Health Authority Portals	Variety of ports / protocols.	Access is provided to Health Authority portals. To date, access has been provided to VCH, VIHA, FHA and IHA.
Email Client(s)	POP, IMAP: (any) SMTP: (restricted)	Standard email client retrieval access (Outlook, Thunderbird) to email servers is allowed.

Application	Network Protocols / Ports Used	Comments
		Outgoing SMTP email client traffic is restricted to 'smtp.telus.net' – see section 2.5.1 above.
PharmaNet (using Ministry compliant 3 rd party software, and HNSecure)	Various TCP ports	For access to: <ul style="list-style-type: none"> ○ HNgard production access: hngard1.hnet.bc.ca and hngard2.hnet.bc.ca ○ HNgard training access: hngard1d.hnet.bc.ca and hngard2d.hnet.bc.ca
Medinet 6 (to seagull.medi.net)	SSH/SFTP port 22	Medinet 6 client
MedRay Medical Imaging	Outbound port 5022	PACS (Picture Archiving Communication Systems) provider, Intelrad and Inteleviewer software program for physician to view images of patient's x-ray
Blackberry UMA	Outbound UDP ports 500 and 4500	For access to Blackberry 'Unlicensed Mobile Access' (UMA)
Debit Machines	Outbound ports 19000-19999	For Debit machine access
Philips Zymed Holster Monitoring/Scans	Outbound TCP/UDP Ports 20023 and 20024 (to specific Philips Zymed remote link server)	For access to Philips Holster Monitoring application





Appendix C – TELUS Router Sizing Options

PPN services are delivered over copper (ADSL) or fibre optic cables.

The capacity or bandwidth of the connection for each practice is based on the size of the practice. The PITO relationship manager (RM), working with practice staff, will determine the *number of concurrent users* who will on average be using the network connection at any one time. Standard sizing rules have been designed to select the appropriate TELUS router capacity, which are listed in the table below. Note that this ‘concurrent’ number does not include staff working remotely outside of the practice location.

Table 1 TELUS Router Sizing Options

TELUS Router Type	Approximate Bandwidth	# of Physicians	# of Concurrent Users
PPN-1 – Asymmetric ¹ (one ADSL router)	1 - 5 Mbps ²	1 – 4	1 – 8
PPN-2 – 2 X Asymmetric ¹ (two ADSL routers)	1 - 5 Mbps (for each router)	5 – 8	9 – 16
PPN-3 – 10Mbps (one fibre router)	10 Mbps	9 - 100	17 – 199
PPN-4 – 100Mbps (one fibre router)	100 Mbps	101 +	200+

NOTE: For rural or remote locations where an ADSL/copper based service is not available to provision a ‘PPN-1 – Asymmetric’ or ‘PPN-2 – 2X Asymmetric’ service, a T1 based symmetric service called “PPN-1 (ER) – 1.5 Mbps” may be installed if available and approved by Ministry.

¹ These access options are asymmetric access based, which provides faster download over upload speeds. This fits the profile of typical network use, where significantly more data is pulled down from internet servers (e.g. EMR systems), than is sent up to the servers.

² Millions of Bits Per Second.



Appendix D – Network Performance and the TELUS Router

D.1 Network Infrastructure Context

Starting with the TELUS router installed at a practice, the PPN provides only one component of the end to end network solution. The practice LAN network, as well as EMR vendor data centre network, complete the network links required to access an EMR application from the practice location.

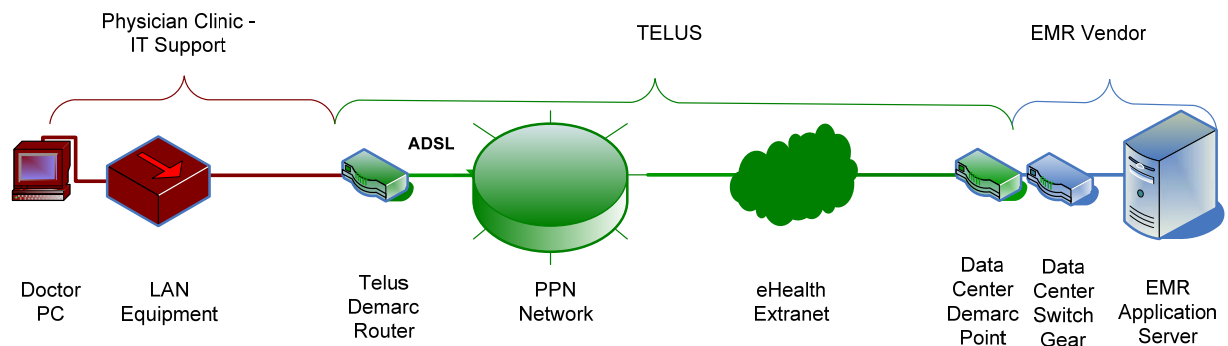


Figure 6 End to End Network Infrastructure Context

If performance issues arise, an integrated support model is in place for the practice to report any problems to the EMR Vendor Tier 1 help desk – who will triage the problem and assign either back to the practice, to TELUS Tier 2 support, or their own internal support group, depending on where they best assess the root cause lies.



See the “EMR and PPN Support Quick Reference” for a summary on the technical support the practice can expect to receive when experiencing EMR and PPN related problems, as well as what they are responsible to resolve. This document is available on the PITO web site at www.pito.bc.ca under the ‘Document Links’ section

D.2 TELUS Router Performance Characteristics

PPN-1 and PPN-2 services are based on TELUS business grade ADSL asymmetric services. These services are provisioned over copper loops from the serving TELUS

central office (CO) to the practice location. The performance of ADSL services is dependent on the length of the copper loop, and generally the longer the distance from the CO to the practice location the slower the speeds for both downstream and upstream data transmission. Prior to installing PPN-1 or PPN-2 services, TELUS prequalifies all copper loops, and tests to ensure they meet PPN requirements.

TELUS is in the midst of a Province wide process for all of their customers to upgrade ADSL based services to next generation ADSL2+ technology. ADSL 2+ is recognized as a more stable protocol and supports delivery of higher bandwidth services although it is still subject to copper loop length constraints. PPN-1 and PPN-2 services will be provisioned on the ADSL2+ platform if available at the serving TELUS CO.

PPN-3 and PPN-4 services use fibre optic cable transport facilities from the serving TELUS CO to the physician location. These services are designed to provide 10Mbps or 100Mbps symmetric bandwidth between the practice and serving CO.

D.3 PPN Internet Performance

The PPN provides Internet access from the practice location through the PPN core network, which include security appliances for firewall, antivirus and intrusion prevention/detection. With Internet traffic passing through these PPN core security appliances, the practice may experience slightly “slower” performance than the direct Internet access provided by other commercial Internet service providers. This tradeoff is required to protect practice systems and LANs from Internet threats.

TELUS has established an Internet site hosted in BC (atlantis.bb.telus.com) for the practice’s technical support resource to test Internet performance to. This test site can be used for download/upload of files of varying sizes, and reports back throughput results.

D.4 Practice Performance Profile

On installing a PPN router at a practice, TELUS captures a variety of performance metrics that are documented and made available to the practice’s EMR vendor. These metrics provide a baseline performance profile for each practice router that can be referenced by the EMR vendor Tier 1 helpdesk staff if a practice reports any future performance issues. The practice, through their PPN contact, can also request this performance report through their EMR Vendor help desk.

