BYO Gateway with Telstra Business Broadband on the nbn™ network

Not all ADSL gateways can support services over the **nbn** network. If you're using an existing gateway that wasn't purchased as part of your Telstra Business Broadband service, please note that Telstra is unable to provide assistance with its set-up.

For Fibre to the Node (FTTN) & Fibre to the Building (FTTB) technology you must have a VDSL compatible gateway which meets specific requirements, therefore Telstra does not recommend the use of a BYO (bring your own) Gateway.

nbn co has provided Telstra with a list of requirements that must be met before opting to BYO a VDSL gateway. If a gateway does not meet these requirements, or the gateway information is not provided to Telstra before **nbn** is connected, we cannot guarantee that the Telstra Broadband on **nbn** service will work faultlessly. Please refer to the section "UNI VDSL2 Equipment Compatibility" in the Product Technical Specification guide nebs-product-tech-spec-fttb-fttn. A VDSL gateway (hardware and firmware) intended for use with the UNI-DSL must be able to demonstrate compatibility with all of the requirements listed in this section.

Please refer to the nbn co WBA doc. page:

http://www.nbnco.com.au/sell-nbn-services/supply-agreements/wba2.html - this link will refer to the latest version of the product technical specification that is subject to change from time to time.

Note 1: Customers who want to retain voice continuity (PSTN service) should be aware that specific VDSL splitters may be required. (Please refer to Section 7.3 Central Splitter).

Note2: Any cabling termination to a second socket (in the case of FTTB) could degrade the VDSL performance, and as such, unless required, all secondary cabling termination should be disconnected.

If you are opting to use non-Telstra equipment with your Telstra Business Broadband on **nbn** service you should refer to the manufacturer's equipment guides, or seek assistance from a qualified network integrator. The information contained below is of a general nature to assist your network integrator.

To use a non-Telstra-provided Gateway, the device must:

- Support WAN on an Ethernet port. If not, please consider purchasing a business gateway from us.
- Support xDSL port for VDSL with Vectoring (FTTN & FTTB deployments only).
- Use Ethernet full duplex with auto-negotiation on so that the gateway signals to UNI-D (nbn network termination device port) that it's full duplex capable, avoiding duplex mismatch (excluding FTTN & FTTB deployments).
- Operate as a gateway with a single MAC address assigned to the port.
- Not configured as a bridge or hub.
- Support NAT.
- Use DHCPv4 to 'request' the IP address (this is essential to create the IP session on our service edge. The DHCP response will contain DNS information, as well as the allocated static address). The network will return both IPv4 and IPv6 assigned address information.
- Be configured to transmit all upstream data untagged.
- Not use 802.1p priority or VLAN tagging as this will be ignored (subject to change).

- Be configured to mark all upstream traffic to 'DSCP 0' (zero).

- Ensure the L2 maximum frame size (also known as Maximum Transfer Unit - MTU) of no larger than 1500 octets.

- Shape upstream traffic to the Speed Level of the service purchased (e.g. shape upstream to 5Mbps on a Speed Level 2 service i.e. 25Mbps downstream, 5 Mbps upstream).

Additionally, we may:

- Attempt to remotely connect to your gateway.
- Suspend or disconnect the service if the device is interfering with the service or the network.

 We may also:

- Attempt to communicate with the device in normal operation and assurance scenarios.
- Require changes to device configuration or additional device capability.
- Remotely configure or upgrade the firmware of the device.
- From time to time make life cycle and service improvement changes that invalidate some device settings.

Other important notes:

- No user name or realm authentication requirement.
- As there is no authentication required on access due to DHCP, the UNI-D needs to be secure to limit any possible illegal use.
- It's possible to access the internet via a PC or Host directly (this differs to PPPoE).
- The DHCPv4 response will also contain the Netmask, Gateway and DNS. You may substitute your preferred DNS.

Advanced Features:

1. Customer with IPVPN setup
    1.1. Please take special note that the current DHCP lease time is 4 hours with renew request in the first hour and subsequent 2 hours of the lease.

    You MUST make sure that there are no ACL's blocking the return DHCP requests from the ASP Radius control panel.

    Reasons: If DHCP renew request is missed within the DHCP lease window it will force a renew on the WAN interface potentially locking up the interface e.g. For a Cisco 1941 we have to add " permit udp any eq bootps any eq bootpc " into the inbound ACL.

    1.2. You must check the configuration to support any default route entry that may be overridden by DHCP.

    IPSec tunnels may have alternate default route and NS entries for VPN traffic.

    1.3. You MUST mark ALL traffic to DSCP-0, build a new QoS policy to reflect this requirement outbound. This also affects ICMP, Trace route, PING, TACAC's.

2. DSCP Mapping
    2.1. Telstra Business Broadband uses UNI-D DSCP mapping. This maps upstream traffic to nbn co TC-4 via DSCP markings, and discards all tagged traffic.
    This is why you MUST mark all or any existing tagged traffic to DSCP-0. If not, any traffic marked differently will be dropped.

3. Customers who have their gateways in server rooms:
    3.1. Please ensure that your server room is properly protected, secured and electrical equipment is clearly marked e.g. of the 240V power supply circuit.

Guidelines on Gateway Configuration for Internet Connectivity

1. To continue to use your existing CPE, you'll need to refer to your original user instructions. If that's not possible, you may be able to source the instructions on the manufacturer's website.

2. If you're unable to locate your user instructions, the following guidelines may help you in configuring your gateway to operate successfully with **nbn** access.

    For a graphical user interface (GUI)–based device, open your internet browser and enter the device's default IP address into the address bar. This will give you access to the device's user interface.

    If you don't know the default device IP address, it can be determined by:

    Clicking 'Start'

    Clicking 'Run'

    Typing 'CMD' into the 'Open' field

    Typing 'ipconfig' at the prompt

    Note the Default Gateway address of your device

    Skip to step 6 if you have command line– driven device; for example, a CISCO 1941.

3. You may be presented with a screen prompting you to log in to your device. Different devices will have different default log-in details. Check the device's serial number sticker or user guide as a quick reference.

4. In some instances the gateway setup may require you to disable the ADSL interface. In the example shown, it's located under the Administration menu option. The WAN port is enabled when the DSL interface is disabled.
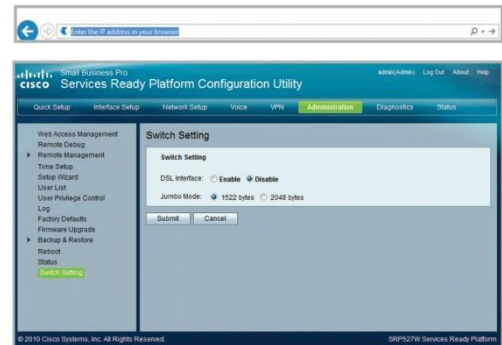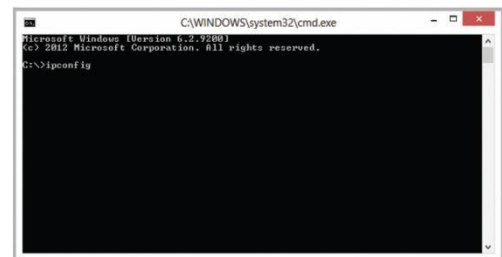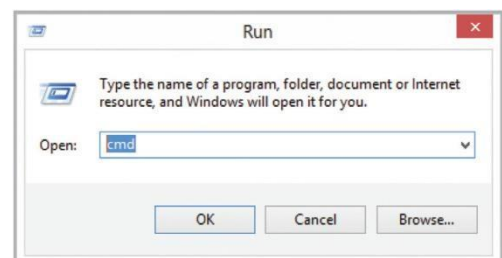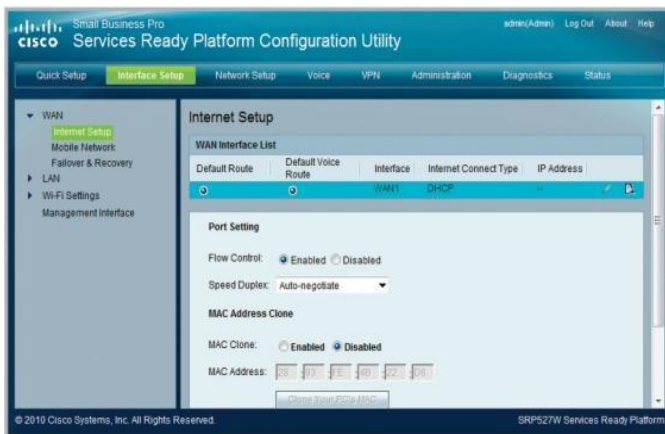
5. When the WAN port is enabled, you may see a number of different settings or options. If you're not sure, use the default settings. Unlike ADSL, Telstra Business Broadband on **nbn** does not require a username and password to authenticate. Each service is provided with a static IP address via a DHCP that's used to connect you to the internet.

6. Here you can see a basic interface configuration for the WAN port and NAT addressing required for a Cisco 1900 series gateway.

    You must update any configured settings and features that used the previous IP address provided by the ADSL network and interface. Such settings include, but are not limited to, Default Route and NAT Destination.

    Please note: NAT support in the gateway is only applicable to IPv4.

    For further information please refer to Cisco's basic configuration guide for the 1900 series gateways on the Cisco website