



CUSTDATA USER GUIDE

How to manage your Telstra Data
Services online



WELCOME TO CUSTDATA



As a Telstra Business, Enterprise or Wholesale customer, you can take full advantage of complimentary access to CustData to manage your services as and when it suits you.

CustData is a secure account information and management portal which is available to you 24/7. Simply log in to:

- configure your services
- test your services
- view outage reports and log faults
- use comprehensive service performance reporting tools
- manage your contact details
- check monthly usage reports
- manage your usage threshold alerts.

Obtaining the best results is as simple as making sure CustData is set up to meet your requirements. CustData makes it easy for you to monitor and manage your internet service.

For example, CustData could provide first evidence of a Denial of Service (DoS) attacks, mail relay issue, open proxy issue, virus activity or poor network configuration.

This guide will help you make the most of your CustData tools.



02 ACCESS AND MESSAGE SERVICES

Any access to CustData requires a secure login. You can access the login page at <https://www.telstra.net/custdata>

02.01 LOGGING IN

To log in, go to the login page and enter either your:

- **Account Number**;
- **Service ID (opshandle)**; OR
- **Full National Number (FNN)**;
- **PLUS your Password**.

(Initially this will be the password provided in your service configuration email.)

For assistance, contact the Technical Helpdesk – refer to Section 11 for contact details.

02.02 SETTING A NEW PASSWORD

Because of the critical data that can be accessed and controlled via CustData, it is essential to protect access to your CustData information with stringent password management procedures.

Your CustData password must be:

1. A minimum of 8 characters in length
 2. Dissimilar to your last five passwords used
 3. Made up from at least 3 of the 4 following character groups:
 - english uppercase (A through Z).
 - english lowercase (A through Z).
 - digits (0 through 9).
 - non-alphanumeric (for example !, \$, #, %).
- further assistance is available via **Online Help**.

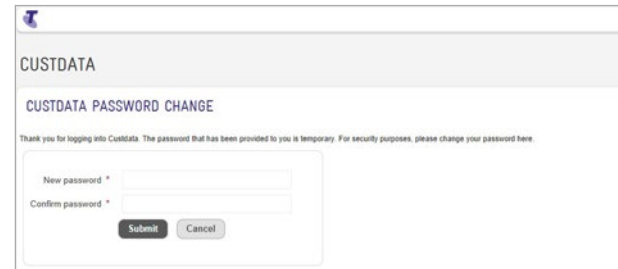
02.02.01 Change your initial password

If your Telstra service is new and is not associated to an existing CustData account, you will be provided with a default password in your configuration email.

This is a temporary password that you will be prompted to change the first time you log in.



Figure 1. Initial password change



02.02.02 Change your password

If you need your password reset for any reason, you will be issued with a temporary replacement. To prevent this replacement password from expiring, you must set a new password when you next log in to CustData.

1. On login, you may see a password expiry warning on your Welcome screen.
2. Click on **Account Management** link on the Home screen.
3. Click on **Change Password** tab.
4. Enter a new password, confirm your new password and click **Submit**.

Further assistance is available via **Online Help**.

02.02.03 If you forget your password

If you cannot remember your password, click **Forgot your password?** link on the CustData login page. This will take you to the **CustData Password Reset** screen.

1. You will need to enter your:
 - **Account number**;
 - **Service ID** (opshandle); and
 - **Full National Number** (FNN).

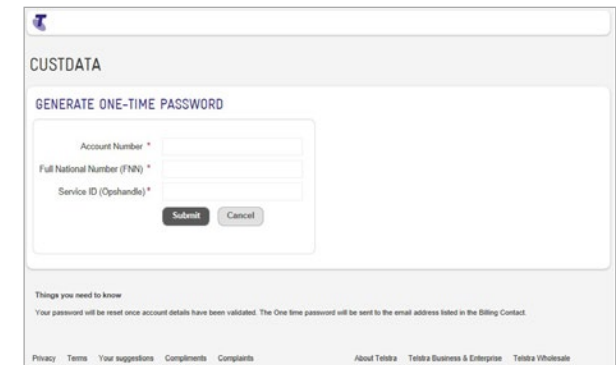
02 ACCESS AND MESSAGE SERVICES

2. Click the **Reset Password** button to validate your account details.
3. On successful validation, a temporary password will be generated and emailed to the contact listed in the **Update Contact Details** tab of the **Manage Account** screen. This is also known as your **Billing Contact Email ID**. If you need to change this address, see the Billing Contact information at 02.03 below.

* If you do not have an email listed in the billing contact section of CustData, you must contact the Technical Helpdesk for password resets – refer to Section 11 for contact details.

4. When you receive your temporary password, follow the steps for changing a reset password at 02.02.02 above.

Figure 2. Password Reset Screen



02.02.04 Password lifetime

Your CustData password is only valid for 180 days. If you don't change your password for 180 days it will expire and you will be required to change the password on your next login. You will get a warning on the login screen and you must set a new password as shown in figure 3.



Figure 3. Password Expiry – Change Password Screen

02.03 UPDATE CONTACT DETAILS

The **Account Summary** tab under **Manage – > Account** provides you a summary of your service and contact information. The contact summary allows you to nominate email addresses for receiving important service, usage and access notifications related to all services on your account.

The available options are:

- **Billing Contact** – your primary account contact for billing and product information, scheduled reports, reset passwords and Usage Alert emails. You can also enter a secondary email address for the billing contact
- **DNS Contact** – for notices about any primary or Secondary domain name system (DNS) services you have
- **Operations Contact** – for technical information, such as warnings about an overloaded service
- **Outage Contact** – for notices about any outages that may affect your service
- **Routing Contact** – for routing change authorisations and any routing issues
- **Statistics Contact** – for reports on service usage.

02 ACCESS AND MESSAGE SERVICES

You only need to enter contact details – a name, phone number and email address – for the services you require. Each option has an Edit function for changing or updating those details.

We recommend that you review your contact details on a regular basis to ensure they're accurate and up to date. For example, you will be unable to review any routing detail notifications if there is no nominated contact details set up in the Routing Contact field and you will not receive Usage Notification Alerts where there is an incorrect email address for Billing Contact.

Figure 4. Update Contact Details Screen

Type	Name	Location	Phone Number	Mobile Number	Email Address	Secondary Email Address	Edit
Billing	John Doe	ACT			joe.bloggs@abc.com		Edit
DNS	Stephen	ACT			testemailaddress@abc.com		Edit
Operations	Operations	ACT			testemail@abc.com		Edit
Outage							Edit
Routing	Routing	ACT			testemail@abc.com		Edit
Statistics							Edit

To edit your contact information:

1. Log in to CustData
2. Click on **Account Management** link which is available at the centre of the Home screen
3. Click on **Update Contact Details** tab
4. Locate the contact you need to change, scroll to the right and click on **Edit**
5. On the new screen that appears, enter the new authorised contact details and click on **Save**.

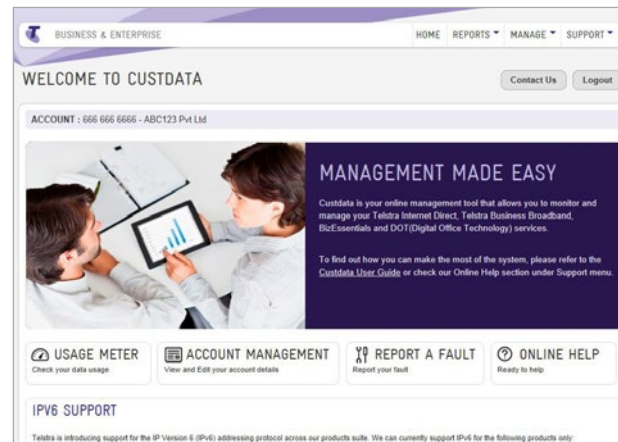


03 NAVIGATION AND FUNCTIONALITY

Each time you log in to CustData you'll see the Welcome Screen with further navigation options on the top right corner of the screen.

We'll look at the basic functionality of these menu options here.

Figure 5. Welcome Screen



03.01 HOME

The Home or the welcome screen provides menus to select reports, manage account and service(s) and other support options. This screen also provides quick links to Account Management and Reporting features of CustData.

03.02 REPORTS

The reports menu option provides access to the following reports:

03.02.01 Service Usage

This screen provides tabs to view usage summary and various daily and monthly reports

Usage Meter

View usage summary of your service(s). Also configure scheduled reporting:

- **Configure Usage Notification** – manage internet usage alerts for your service. See Section 04 for more details on Usage Threshold Notifications. There are also links to the following external URLs, which provide management functions and information for Telstra Business Broadband customers.
- **Configure scheduled reporting** – arrange to receive an aggregated monthly summary (in csv format) for services associated with your account or Multi Site plan for the most recent billing cycle period.

Monthly Reports

Tabular and graphical traffic data for your service over a selected billing cycle.

Daily Reports

Tabular and graphical traffic data for your service through selected start and end dates.

See Section 05 for information on viewing and interpreting reports.

03.02.02 Network Performance

Check network performance statistics, including Latency and Inter-capital Domestic Links.



03.03 MANAGE

03.03.01 Account

This screen provides tabs to view your account summary, update your contact and details and also allows you to change your login password.

- **Account Summary** – provides a summary of your services and DNS configurations.
- **Update Contact Details** – refer section 2.03.
- **Change Password** – refer section 2.02.

03.03.02 Service

- **Access Control** – refer section 06.
- **IP Routing** – refer section 07.
- **Additional IP** – refer section 10.
- **Bandwidth Change** – control your Ethernet Dual Uplink Premium Package bandwidth on demand.

03.03.03 DNS

- **Primary DNS** – refer section 9.01.
- **Secondary DNS** – refer section 9.02.
- **Reverse DNS** – manage your reverse DNS records; control .in-addr.arpa entries (up to a/25 IPv4 subnet, ie maximum 128 IP addresses) and ip6.arpa entries (up to 128 entries per allocated IPv6 prefix).

03.03.04 Secondary Mail Services

Use Telstra Internet Direct as a secondary mail exchange, to store emails if your Primary mail server is down.

03.04 SUPPORT

03.04.01 Diagnostic Toolkit

- **Network Visibility** – this tab provides feature to perform Node to Node or Node to Host Testing.
- **Node To Node Ping** – for real-time statistics between two Telstra Internet Direct (TID) nodes (Points of Presence).
- **Node To Host Ping** – for real-time statistics between a TID node and any given host.
- **Node To Host Trace** – for the network path between a TID node and any given host.
- **DNS Visibility** – allows to check status of your domain.
- **Mail Visibility** – allows testing reachability from Internet Direct to the mail server of a given domain.
- **BackChannel Tariff** – allows you to enter your expected traffic in and traffic out to calculate the possible Backchannel tariff should this tariff apply to your agreement with us.

Note: The testing feature is not available for Telstra services on the NBN.

03.04.02 Report a Fault

Submit a fault report online. A shortcut link for this function is also provided on the Welcome screen.

03.04.03 Contact Telstra

A list of key Telstra contact details. The Contact Us button provided on the Welcome screen will also take you there.

03.04.04 Online Help

Detailed guidance for using CustData functions. This feature is also available as a shortcut link on the Welcome Screen.

03.05 LOGOUT

This button (available on the Welcome screen) closes your secure session and returns you to the main login page.



04 USAGE THRESHOLD ALERTS

You won't be charged any fixed broadband excess data charges for your first two bills when you are a new customer or recontracting your service. It's part of our Peace of Mind Commitment. If you are eligible for Peace of Mind you will also see a notification which shows 'Peace of Mind Commitment applies' next to Data used section.

04.01 HOW TO RECEIVE USAGE THRESHOLD ALERTS

The Usage Threshold Alerts service is now built into all standard tiered plans, and will be provided as long as you've included an active email address in the Billing Contact line of the Update Contact Details screen. (Refer to 02.03 for details.)

Usage Threshold Alerts are not available for:

- Fixed and Unlimited plans
- Multi Site Volume Based plans
- Customised Pricing plans.

04.02 USAGE THRESHOLD ALERT TRIGGERS

A Usage Threshold Alert will be triggered when CustData recognises that you have reached the nominated percentage of the usage associated with your plan. You'll receive your alert email within approximately 48 hours. You may also nominate to include an additional email contact to receive this alert. You may also nominate to include an additional email contact in the secondary email billing address to receive this alert (refer to 02.03).

04.03 HOW TO DE-ACTIVATE USAGE THRESHOLD ALERTS

You can choose to **not** receive notices for any of the nominated threshold levels, by clicking the appropriate check box(es) in the Usage Alerts screen in the Account Management submenu.

1. Log in to CustData.
2. Navigate to **Manage** menu from the top right corner of the Home screen.

3. Select **Usage Notification** from the Manage menu.
4. Click the notification options that you do not want to receive. If you don't want any Usage Threshold Alerts, just select **I do not wish to receive notification for any of the listed thresholds**.
5. Click the **Save** button.
6. The confirmation message **Changes to your internet usage notifications have been amended** will appear.

Changes to your Usage Threshold Alert options will take effect immediately.

Figure 6. Usage Alerts Notification screen

The screenshot shows the 'USAGE NOTIFICATION' screen. At the top right are 'Contact Us' and 'Logout' buttons. Below the header, it says 'ACCOUNT : 666 666 6666 - ABC123 Pvt Ltd'. The main section is titled 'Notification Settings'. Under 'Account Level', there is a checkbox labeled 'I do not wish to receive notifications for any of the listed usage thresholds'. Below this, another section says 'I do not wish to receive usage notification when my download usage reaches the following percentage of my allowance:'. This section contains a list of checkboxes for percentages: 50%, 75%, 100%, 125%, 175%, and 250%. A 'Save' button is at the bottom of this list. At the very bottom of the screen are 'Reset' and 'Back' buttons. A small disclaimer at the bottom reads: 'I hereby acknowledge that I am the legal/authorized representative of this account to make the changes submitted'.



05 REPORTS

CustData makes it easy for you to monitor and manage your internet service by providing a range of valuable reports. Each offers different functionality and can be used to analyse usage trends and perform trouble shooting.

This regular monitoring of your services is highly recommended. Doing so can help you identify and remedy issues early. Early detection makes it a lot easier to diagnose a problem and put effective prevention in place.

By becoming familiar with the reports available from CustData, you can accurately identify trends and/or issues affecting your service. For example, you can now view monthly or daily statistics in both graphical and tabular formats, including usage data at an Account, Multi Site Aggregator or Single Service level.

05.01 ACCOUNT LEVEL AND MULTI SITE LEVEL USAGE REPORTING

Account level and Multi Site level reporting are supported for daily and monthly usage reporting. Scheduled reporting is also supported with frequencies aligned to your monthly billing cycle. Account or Multi Site level reports are not available for usage data recorded before 19 May 2009.

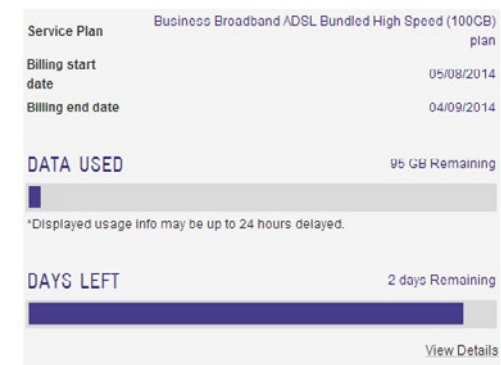
05.02 USAGE METER

CustData's Usage Meter provides a summary of your data usage for each service attached to your account. The first time you click on the Usage Meter feature, your first 10 services will be displayed on the left under "My Services". You can click the "Next" and "Previous" buttons to navigate through all your services.

Click on a service under "My Services" to display a summary of the usage as shown in the example below. The service ID is displayed at the top, followed by the service's plan name and billing cycle start and end dates.

The "Data Used" bar graphically illustrates the amount of data consumed from your data allowance. The "Days Left" bar points to the number of days remaining in the current billing cycle.

The "View Details" link directs you to the Monthly Reports page where you can run a more detailed report for the selected service.



There are two types of services shown in the usage meter – the services that you see under "My Services" will depend on the data plans purchased:

- **Individual services:** these are denoted by "Service ID" along with the service identifier and Full National Number (FNN). Individual services will display the usage meter for standalone data plans.
- **Aggregated/Multisite services:** these are denoted by "Aggregator ID" along with the aggregator/group plan identifier. These could be group plans for Digital Office Technology customers or multisite tiered/volume plans for TID customers. The data shown is the aggregation of all individual services under the group or multisite service. Individual services under an aggregated service will not be listed under "My Services". For usage details of individual sites, you can view current usage information via "Daily" and "Monthly" Reports.



05.03 DAILY USAGE REPORTS

Daily Usage Reports allow you to monitor your daily usage statistics at an Account, Multi Site Group or Individual Service level. Usage data is available at two levels of granularity: Daily Summary and 5 Minute Polling Data.

For Daily Summary reports, usage data is available for last seven years in Custdata. For 5 Minute Polling Reports, usage data is available for the last one year in CustData.

For 5 minute data older than one year (but not more than 7 years), please use the “Report A Fault” function in Custdata to request usage data for the required time period.

05.03.01 To produce Daily Usage Reports

1. Log in to CustData.
2. Navigate to the **Reports** menu on the top-right hand of the screen and select **Service Usage**.
3. Click on **Daily Reports** tab on the Service Usage Reports screen.
4. In the screen that appears, select the required service, account number or Multi Site Aggregator ID from the dropdown list in the **Service/Multi Site/Account** field.
5. Now select **Daily Summary** in the **Data Type** field.
6. Enter the **Start** and **Through to** dates for the days you want included; or select dates on screen by opening the **Calendar** icon (see 05.03.02 below).
7. Click on the **Generate Report** button.
(If you do not enter a **From** or **Through to** date, the day before the current day will be used by default.)

Further assistance is available via **Online Help**.

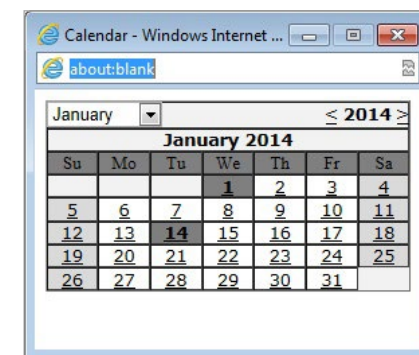
Figure 7. Daily reports screen

05.03.02 Using the Calendar Box

If required, CustData lets you choose reporting dates from a calendar.

Simply click the **Calendar** icon next to the **From** or **Through to** text fields to open the calendar window. The current month will be displayed by default, however you can select a different month from the dropdown list. This option is useful if you wish to view usage for a calendar month.

Figure 8. Report Calendar





05.03.03 Producing reports at the Service/ Multi Site/Account level

It is now possible to generate daily reports of your Account, Multi Site or Individual Service usage.

Figure 9. Daily Usage Summary Report screen

- 1-3. Access the **Daily Reports** screen as per section 05.03.01 above.
4. Select your account number from dropdown labelled **Service/Multi Site/Account**.
5. Choose your daily summary details by selecting the appropriate radio buttons under **Data Type**.
6. Enter your preferred **Start** and **Through to** dates in the text field, or click the **Calendar** icon to open and use the calendar window.
7. Click on the **Generate Report** button.

If you request an Account or Multi Site daily usage report, there may be a short delay as the data is processed.

The following message will be displayed: **Your request is being processed and may take up to 5 minutes to complete.** Followed by: **Process complete.**

5 Minute Polling Data is only available for Individual Service reports.

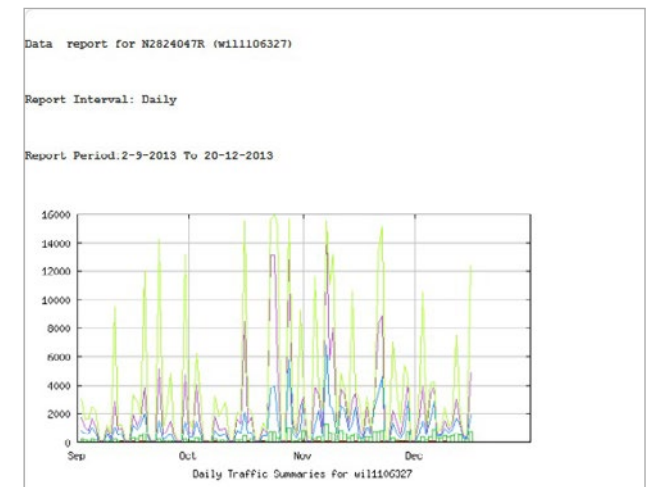
05.03.03.01 Account level Reports: Additional information

When you produce a daily usage report at the account level, the graph and data will be consolidated from all the services under that account. The report looks similar to an Individual Service report, however it has your account number in the header. There is no breakdown of Individual Service data within the Account level report.

The Account level report will also include data from cancelled services if they had billable usage during the selected reporting period.

5 Minute Polling Data isn't available on Account level reports and will be greyed out.

Figure 10. Daily Usage summary screens for an Account level report





DATE	Service Capacity (Kbps)		UPLOAD		DOWNLOAD		24 Hrs Average		4 Hrs Peak		1 Hr Peak		15 Min Peak	
	Volume (MB)	Line Occupancy	Volume (MB)	Line Occupancy	Volume (MB)	Line Occupancy	Line Speed (Kbps)	Line Occupancy	Line Speed (Kbps)	Line Occupancy	Line Speed (Kbps)	Line Occupancy	Line Speed (Kbps)	Line Occupancy
02/09/2019 20000	287	0%	2887	1%	239	0%	782	4%	1787	8%	3045	16%		
03/09/2019 20000	282	0%	2024	1%	187	0%	897	3%	1029	5%	1452	8%		
04/09/2019 20000	288	0%	1699	1%	187	0%	480	3%	826	4%	1700	9%		
05/09/2019 20000	236	0%	2764	1%	218	0%	897	5%	1465	9%	2831	15%		
06/09/2019 20000	238	0%	1847	1%	170	0%	700	4%	1103	6%	2243	11%		
07/09/2019 20000	12	0%	36	0%	3	0%	13	0%	69	0%	188	1%		
08/09/2019 20000	13	0%	45	0%	8	0%	14	0%	61	0%	188	1%		
09/09/2019 20000	202	0%	1499	1%	157	0%	624	2%	971	5%	1106	6%		
10/09/2019 20000	187	0%	667	0%	61	0%	163	1%	236	1%	529	3%		
11/09/2019 20000	212	0%	2956	1%	273	0%	1101	6%	2036	14%	3911	48%		
12/09/2019 20000	305	0%	1437	1%	133	0%	516	3%	883	4%	1235	6%		
13/09/2019 20000	384	0%	1744	1%	141	0%	592	3%	935	5%	1210	6%		
14/09/2019 20000	10	0%	34	0%	3	0%	13	0%	48	0%	188	1%		
15/09/2019 20000	19	0%	64	0%	5	0%	14	0%	61	0%	188	1%		
16/09/2019 20000	479	0%	4007	2%	371	0%	1185	6%	1978	10%	3340	17%		
17/09/2019 20000	288	0%	3012	1%	278	0%	874	4%	1151	6%	2909	15%		
18/09/2019 20000	412	0%	5456	3%	505	0%	1271	6%	1747	9%	1407	9%		
19/09/2019 20000	547	0%	6846	3%	633	0%	2022	10%	3819	19%	12014	60%		
20/09/2019 20000	68	0%	815	0%	75	0%	422	2%	646	3%	652	3%		
21/09/2019 20000	11	0%	31	0%	3	0%	13	0%	49	0%	194	1%		
22/09/2019 20000	10	0%	30	0%	3	0%	14	0%	62	0%	195	1%		
23/09/2019 20000	208	0%	3240	1%	289	0%	1622	8%	3102	24%	14246	71%		
24/09/2019 20000	148	0%	728	0%	67	0%	219	1%	910	3%	1023	5%		
25/09/2019 20000	106	0%	1098	1%	101	0%	411	2%	810	4%	2271	11%		

01/12/2019 20000	22	0%	87	0%	5	0%	16	0%	55	0%	188	1%		
02/12/2019 20000	70	0%	1088	0%	97	0%	565	2%	1426	7%	2865	12%		
03/12/2019 20000	243	0%	4130	2%	382	0%	1482	7%	3926	20%	10513	51%		
04/12/2019 20000	228	0%	1954	1%	180	0%	839	3%	703	4%	1161	6%		
05/12/2019 20000	439	0%	4319	2%	399	0%	1644	8%	3427	17%	4147	21%		
06/12/2019 20000	998	0%	9935	5%	910	0%	2849	14%	3944	20%	4559	21%		
07/12/2019 20000	144	0%	3688	2%	341	2%	459	2%	884	3%	793	4%		
08/12/2019 20000	197	0%	3613	2%	394	0%	484	2%	846	3%	988	4%		
09/12/2019 20000	371	0%	5444	3%	504	0%	930	5%	1828	8%	2405	12%		
10/12/2019 20000	208	0%	4371	2%	404	0%	479	3%	878	4%	1178	6%		
11/12/2019 20000	244	0%	5434	3%	503	0%	882	4%	1203	6%	1480	7%		
12/12/2019 20000	276	0%	6906	3%	639	0%	1713	3%	3049	15%	7003	35%		
13/12/2019 20000	312	0%	8730	3%	530	0%	1122	4%	1466	6%	1650	9%		
14/12/2019 20000	34	0%	324	2%	210	0%	397	2%	445	2%	554	3%		
15/12/2019 20000	32	0%	3274	2%	303	2%	244	2%	372	2%	541	3%		
16/12/2019 20000	326	0%	8019	4%	742	0%	1896	9%	4931	25%	12434	62%		
17/12/2019 20000	253	0%	5116	2%	473	0%	873	4%	1905	9%	3576	18%		
18/12/2019 20000	476	0%	3361	2%	311	0%	823	4%	1234	6%	2903	15%		
19/12/2019 20000	304	0%	1887	1%	146	0%	853	3%	1123	6%	1795	9%		
20/12/2019 20000	300	0%	2215	1%	205	0%	647	3%	1357	7%	2472	13%		
TOTAL	28209		333861											

Report Period: 159 Days

Total Mbytes UPLOADED to Telstra Internet : 28209

Total Mbytes DOWNLOADED from Telstra Internet : 333861

[Download Report](#)

Note: For Telstra services on the NBN only, the Service Capacity, Line Occupancy IN, Line Occupancy OUT, 24 Hour avg Kbps, 24 Hour avg Line Occupancy, 4 Hour peak Line Occupancy, 1 Hour peak Line Occupancy and 15 Min peak Line Occupancy will be reported as zero.

05.03.03.02 Multi Site level reports: Additional information

Multi Site reports show aggregated usage data for all the services covered by your Multi Site plan. You must have a Multi Site plan to generate Multi Site reports. The displayed screens look similar to Account level reporting, but will reference your Multi Site plan and Aggregator ID.

These reports will not advise when you have reached your minimum spend threshold, so we recommend that you have details of your Multi Site plan on hand.

5 Minute Polling Data isn't available on Multi Site plan reports and will be greyed out.

Figure 11. Daily Usage summary screen for a Multi Site report

SERVICE USAGE REPORTS

Contact Us Logout

ACCOUNT : 666 666 6666 - ABC123 Pvt Ltd

USAGE METER

MONTHLY REPORTS

DAILY REPORTS

Service/MultiSite/Account

Data Type

Report Start Date

Report End Date

Aggregator ID (0684868570)

Daily Summary

dd-mm-yyyy

dd-mm-yyyy

Generate Report

05.03.04 Download reporting option

A **Download** button has been provided on all reporting screens. Selecting this button allows you to download your reported data, tabulated in an Excel spreadsheet. You can then use the data to create your own tables and charts as required.



05.04 MONTHLY USAGE REPORTS

Our enhanced Monthly Usage Reports allow you to check your service usage for a complete billing cycle at an Account, Multi Site Group or Individual Service level.

This billing cycle data replaces the calendar month basis of our previous monthly reporting option – and should prove more relevant for your account.

If you require calendar month reporting, we recommend you use the daily reporting function which allows you to select from the first to the last day of a specific month.

05.04.01 To produce Monthly Usage Reports

Figure 12. Monthly Usage Report screen

1. Log in to CustData.
2. Navigate to **Reports** menu at the top right corner of the screen and select **Service Usage**.
3. Click on **Monthly Reports** tab on the Service Usage Reports screen.
4. In the main screen, select the required service, account number or Multi Site Aggregator ID from the dropdown list in the **Service/Multi Site/Account** field.
5. Now select the required **Billing Cycle**.
6. Select the year of your required **Billing Cycle**.
7. Click on the **Generate Report** button.

The **Billing Cycle** dropdown at step 5 will automatically show the monthly billing cycle dates for the account you have selected, with our last complete billing cycle as the default. You can select any of the billing cycles for the period you wish to review – just remember to choose the correct year at step 6.

Note: Monthly reporting data is not available until 48 hours after the completion of the billing cycle.

Further assistance is available via **Online Help**.

05.04.02 Producing reports at the Service/Multi Site/Account level

You can generate monthly reports of your Account, Multi Site or Individual Service usage.

Simply select the desired Service, Multi Site or account number from the Service/Multi Site/Account dropdown at step 4 in the section above.

Account and Multi Site level reports will include data from cancelled services if they had billable usage during the selected billing cycle.



05.04.03 Monthly Report Table Headers

Once you have generated a Monthly Usage Report, the table header will reflect the level of reporting you have selected.

- **Account Name** and **Account Number** are the same as those that appear in the bar at the top of each screen in CustData.
- **Service Name** is the name that appears against the service on your account.
- **Deal Name** is the name of the plan you are on (this will appear only when viewing single service level reporting).
- **Multi Site Deal Name** is a generic name for all Multi Site plans. For details of your plan, please refer to your broadband service contract.
- **Aggregator Number** is the 10-digit number that appears on your account. This number is used to accrue and summarise all usage generated by the services within your Multi Site plan.

05.04.03.01 Sample Monthly Report Table Headers

Monthly Report: <Account Number> – <Bill Cycle>	
Account Name	<Account Name>
Account Number	<Account Number>
Monthly Total Data Volumes	
Mbytes Uploaded	<Acct Total Mbytes>
Mbytes Downloaded	<Acct Total Mbytes>
95% peak bandwidth	39.0 kbps

Monthly Report: <Service Name>	
Service Name	<service description>
Account Number	<nxxxxxxr>
Deal Name	<Deal Name>
Monthly Total Data Volumes	
Mbytes Uploaded	1111 Mbytes
Mbytes Downloaded	1111 Mbytes
95% peak bandwidth	62.0 kbps

Monthly Report: <Group Aggregator ID> – <Bill Cycle Date>	
Multi Site Deal Name	Multi Site Plan
Aggregator Number	<Aggregator Number>
Monthly Total Data Volumes	
Mbytes Uploaded	<Acct Total Mbytes>
Mbytes Downloaded	<Acct Total Mbytes>
95% peak bandwidth	39.0 kbps

Uploaded is connected service T0 Telstra 1000 Mbytes = 1 Gbyte (GB)
Downloaded is Telstra T0 connected service 1000 Gbytes = 1 Tbyte (TB)

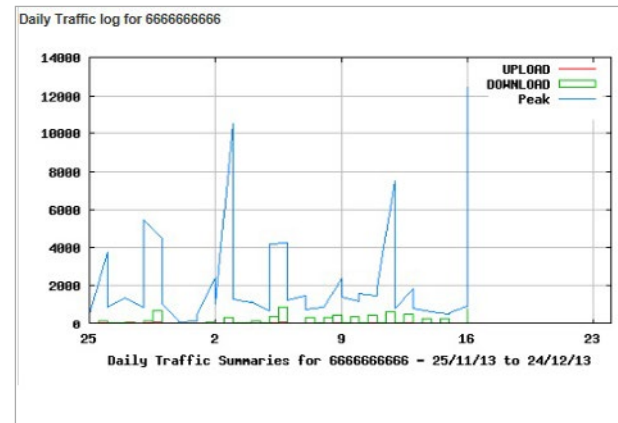
95th PERCENTILE (95%) PEAK BANDWIDTH or “bursting usage” is determined based on samples of your service’s peak utilisation taken every 5 minutes during the monthly billing cycle.

At the end of the month all 5 minute samples are sorted highest to lowest. The top 5% of the samples are excluded and the next sample value becomes the 95th percentile peak bandwidth for the month.

05.04.04 Daily Traffic Logs and Traffic Profiles

Included in the monthly report for Individual Services are the daily traffic log, 5 minute traffic log and traffic profile charts. These charts can assist you to identify peak periods during the billing cycle and provide a bandwidth profile of the traffic for your service. Daily traffic logs are also displayed for Account and Multi Site level reports, however, 5 Minute Polling Log and Traffic profile options are only available at the Individual Service level.

Figure 13. Daily Traffic Log screen – Account level



05.04.05 Daily Traffic Totals

The Daily Traffic Total table within the Monthly Usage Report provides day-by-day upload and download details for the Individual Service, Account or Multi Site plan.

Figure 14. Daily Traffic Totals screen – Account level

Daily Traffic Totals													
DATE	Service Capacity	UPLOAD		DOWNLOAD		24 Hrs Average		4 Hrs Average		1 Hr Peak		5 min Peak	
		Volume (Mi)	Line Occupancy	Volume (Mi)	Line Occupancy	Line Speed (Kbps)	Line Occupancy	Line Speed (Kbps)	line occupancy	Line Speed (Kbps)	line occupancy	Line Speed (Kbps)	line occupancy
25/11/2013	0	207	0%	3400	0%	333	0%	1370	0%	2206	0%	6891	0%
25/11/2013	0	57	0%	116	0%	0	0%	39	0%	135	0%	541	0%
26/11/2013	0	354	0%	1095	0%	175	0%	572	0%	1414	0%	3773	0%
26/11/2013	0	100	0%	363	0%	0	0%	112	0%	352	0%	869	0%
27/11/2013	0	120	0%	570	0%	0	0%	145	0%	587	0%	1332	0%
27/11/2013	0	427	0%	1271	0%	110	0%	336	0%	514	0%	1370	0%
28/11/2013	0	97	0%	216	0%	0	0%	71	0%	244	0%	877	0%
29/11/2013	0	745	0%	1793	0%	166	0%	762	0%	2605	0%	5421	0%
29/11/2013	0	1126	0%	7864	0%	737	0%	2033	0%	4245	0%	4495	0%
29/11/2013	0	61	0%	191	0%	0	0%	76	0%	294	0%	1061	0%
30/11/2013	0	24	0%	65	0%	6	0%	15	0%	51	0%	108	0%
30/11/2013	0	45	0%	87	0%	0	0%	15	0%	61	0%	106	0%
01/12/2013	0	22	0%	57	0%	5	0%	16	0%	55	0%	108	0%
01/12/2013	0	45	0%	113	0%	0	0%	34	0%	137	0%	520	0%
02/12/2013	0	75	0%	1063	0%	86	0%	563	0%	1427	0%	2364	0%
02/12/2013	0	39	0%	182	0%	0	0%	84	0%	338	0%	1093	0%
03/12/2013	0	287	0%	4172	0%	346	0%	1496	0%	3952	0%	10513	0%
03/12/2013	0	49	0%	362	0%	0	0%	163	0%	621	0%	1290	0%
04/12/2013	0	97	0%	637	0%	0	0%	160	0%	522	0%	1149	0%
04/12/2013	0	261	0%	1989	0%	154	0%	543	0%	708	0%	1167	0%
05/12/2013	0	84	0%	338	0%	0	0%	74	0%	219	0%	733	0%
05/12/2013	0	703	0%	4383	0%	406	0%	1654	0%	3444	0%	4154	0%
06/12/2013	0	1028	0%	8664	0%	913	0%	2677	0%	3959	0%	4258	0%
06/12/2013	0	58	0%	305	0%	0	0%	148	0%	586	0%	1226	0%
07/12/2013	0	43	0%	700	0%	0	0%	137	0%	522	0%	1493	0%
07/12/2013	0	144	0%	3688	0%	341	0%	459	0%	584	0%	793	0%
08/12/2013	0	51	0%	388	0%	0	0%	161	0%	848	0%	885	0%
08/12/2013	0	137	0%	3614	0%	335	0%	454	0%	566	0%	886	0%
09/12/2013	0	376	0%	5448	0%	504	0%	931	0%	1528	0%	2405	0%
09/12/2013	0	44	0%	659	0%	0	0%	259	0%	632	0%	1455	0%
10/12/2013	0	213	0%	4303	0%	458	0%	600	0%	881	0%	1178	0%
10/12/2013	0	55	0%	424	0%	0	0%	131	0%	468	0%	1634	0%
11/12/2013	0	356	0%	5440	0%	504	0%	805	0%	1189	0%	1474	0%
11/12/2013	0	51	0%	395	0%	0	0%	192	0%	620	0%	1912	0%
12/12/2013	0	313	0%	6943	0%	643	0%	1719	0%	3075	0%	7528	0%
12/12/2013	0	74	0%	342	0%	0	0%	85	0%	273	0%	856	0%
13/12/2013	0	331	0%	5750	0%	532	0%	1126	0%	1266	0%	1053	0%
13/12/2013	0	52	0%	166	0%	0	0%	55	0%	217	0%	840	0%
14/12/2013	0	97	0%	3355	0%	311	0%	357	0%	445	0%	864	0%
14/12/2013	0	35	0%	109	0%	0	0%	48	0%	191	0%	840	0%
15/12/2013	0	82	0%	3274	0%	303	0%	344	0%	372	0%	961	0%
15/12/2013	0	36	0%	127	0%	0	0%	44	0%	177	0%	584	0%
16/12/2013	0	51	0%	155	0%	0	0%	78	0%	301	0%	949	0%
16/12/2013	0	356	0%	8950	0%	745	0%	1910	0%	4940	0%	12435	0%
TOTAL		9036		94640									
Download Report													



05.04.06 Download Reporting option

A download button has been provided on all reporting screens. Selecting this button allows you to download your reported data, tabulated in an Excel spreadsheet. You can use the data to create your own tables and charts as required.

05.05 SCHEDULED REPORTS

If you wish to receive a regular monthly summary (aligned with your billing cycle) of usage for all the services associated with your account, Scheduled Reports will automatically deliver this data in csv format for you.

These reports will detail usage for all services on your Account and/or Multi Site plan.

This feature is not available for Telstra Wholesale customers with Virtual Internet Service Provider (vISP) Broadband Services.

05.05.01 To set up Scheduled Reporting

1. Log in to CustData.
2. Navigate to **Reports** menu at the top-right hand corner of the screen and select **Service Usage** menu item.
3. On the **Usage Meter** tab click on **Configure Scheduling Reporting**.
4. Choose your preferred **Scheduled Reporting** option and click save.

Your first report will be generated 48 hours after the completion of your current billing cycle, and 2 days after each subsequent billing cycle. The reports will be emailed to your nominated billing contact, as listed on your Update Contact Details screen. (Refer to section 02.03.)

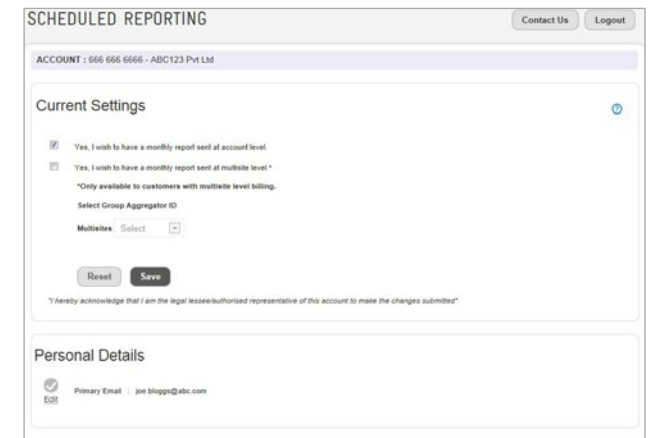
Note: Scheduled reports are generated for administration purposes only. They are not a substitute for your monthly Telstra invoice as we cannot guarantee the completeness of the supplied data.

05.05.02 Scheduled Reporting options

The following reporting options exist:

- a monthly report at the Account level, covering all services listed on your account
- a monthly report at the Multi Site level, covering all services within the nominated Multi Site plan. Simply select a Multi Site Aggregator ID from the dropdown list to activate this option. (You must have a Multi Site plan.)

Figure 15. Scheduled reporting screens





05.06 TREND ANALYSIS

The reporting tools available via CustData can enable you to carry out a trend analysis on your internet service usage. The process is a relatively simple matter of producing and analysing the available data.

05.06.01 Producing Reports for a Trend Analysis

1. Log in to CustData.
2. Navigate to **Reports** menu on the top-right corner of the screen and select **Service Usage**.
3. Click on **Daily Reports** tab on the Service Usage Reports Screen.
4. Choose the required **Service** from the dropdown list.
5. Now select **Daily Summary** in the **Data Type** field.
6. Enter the **Start** and **Through to** dates for the days you want included; or select dates on screen by opening the **Calendar** icon (see section 05.03.02 above).
7. Click on the **Generate Report** button.

Further assistance is available via **Online Help**.

Figure 16. Daily Reports screen

05.06.02 Reading the Daily Traffic Usage Graph

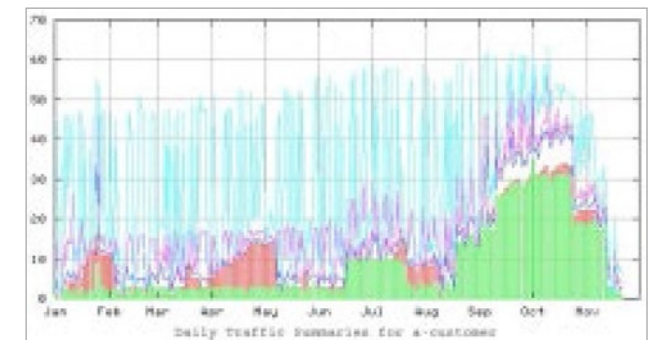
Reading the Daily Traffic Usage graph is relatively simple. You can find info about legends for traffic graphs from **Online Help** section which is available from the **Support** menu on the top right corner of the screen.

In every traffic graph:

- **cyan** – peak 15-minute usage (daily report only)
- **magenta** – peak 1-hour usage (daily report only)
- **blue** – peak 4-hour usage (daily report only)
- **red histogram** – average uploads (connected service to Telstra)
- **green histogram** – average downloads (Telstra to the connected service).

The numbers to the left of the graph represent bandwidth in kilobits per second.

Figure 17. Daily Report Graph



Your graphs may differ depending on service speeds and bandwidth usage.



05.06.03 Interpreting your data

The sample graph shows several jumps in usage over the reported period. If these can't be explained by changes in business activity, it is highly likely that other issues are affecting the service.

A more detailed analysis shows:

- an increase in uploads from the service to Telstra Internet Direct (in red) in January, April, July through August, and September through early November
- increasing downloads from Telstra Internet Direct to this service (in green) in January, July through August, and September through early November. Note that all downloads count as billable usage
- apparently normal usage in February/March and May/June
- looking closely, the red line (sent traffic) is almost equal to the green line (received traffic). When the green line is dominant, the red will appear as a stripe in the green histogram.

05.06.04 Analysing the trends

In the sample, the increasing uploads may still not have added billable charges to your account, as Telstra Internet Connect includes free uploads up to the Backchannel Threshold Ratio of 1:4. (ie upload traffic remains less than one-fourth of downloads.)

Similarly, significant increases in download traffic may not affect your bill if you had chosen a fixed price plan, but the speed of your service could be downgraded if downloads exceed the plan's preset level.

Regular monitoring of your service usage through CustData can help you become aware of increasing traffic levels before they impact your bill or service speed.

Important: Any further investigation should be conducted at the Individual Service level.

05.06.04.01 Analysing upload increases

Possible causes of increasing upload traffic include:

- significant increases in the number of emails being sent (a change to online catalogue distribution, for example)
- a server being hijacked and used as a launch site for spam
- malicious activity such as a Denial of Service (DOS) attack
- more frequent use of the website by the public (ie more content is being sent from the web server to other parties)
- PC, mail server or network malfunction.

Of course, this list is far from exhaustive and only illustrates some of the more common causes for increased traffic.

05.06.04.02 Analysing download increases

Possible causes of increasing download traffic include:

- a natural increase in online activity. Normally, however, such increases are more organic and don't occur in spurts
- malicious activity such as a virus or DOS attack
- large web downloads such as music and video can cause huge increases in activity.

Of course, this list is far from exhaustive and only illustrates some of the more common causes for increased traffic.

05.06.04.03 Analysing uploads over downloads

A service may generate more upload usage than download usage when:

- Data is rejected due to improper router configuration. When a data packet is sent, the receiving router consults its routing table and forwards the data to the appropriate interface. If your router isn't configured properly the data packet may be sent back to the default gateway (the Telstra Internet Direct access router in this case). The access router will then send the packet back to your router, in accordance with its routing table. In this way, a closed loop is established between the your misconfigured router and its default gateway – generating an endless traffic source.



- Equipment being used as a data relay. Data traffic, especially email, is often relayed via an intermediate router to affect delivery. However, allowing unknown users to relay data via your equipment (an Open Relay) increases traffic on your account. Services that use Open Relay type services include Open WEB Proxy, Open Mail Relay, Open Socks Proxy, and Anonymous FTP (for sending and receiving files and a host of others. Allowing Open Relay or Open proxy services on your equipment leaves your account open for abuse by spammers, amongst others. Your servers may even be blacklisted as a source of unwanted email.

Again, there are other reason why uploads may exceed downloads. However, this event always warrants careful scrutiny of your equipment and online activity.

05.07 DRILLING DOWN INTO SUSPECT USAGE

Once you have identified a period of inconsistent or suspect traffic usage, CustData allows you to drill down into that period to see the usage patterns in more detail.

05.07.01 Producing 5 Minute Polling Reports

1. Log in to CustData.
2. Navigate to **Reports** menu at the top-right hand corner and select **Service Reports** menu item.
3. Click on **Daily Reports** tab on the **Service Usage Reports** screen.
4. Choose the required **Service** from the dropdown list.

5. Now select **5 Minute Polling Data** in the **Data Type** field.
6. Enter the **Start** and **Through to** dates for the days you want included; or select dates on screen by opening the **Calendar** icon (see section 05.03.02).
7. Click on the **Generate Report** button.

Further assistance is available via **Online Help**.

Note: 5 Minute Polling is only available at the Individual Service reporting level.

05.07.02 Interpreting the graph

In 5 Minute Polling Graphs:

- red line – uploads (connected service to Telstra)
- green line – downloads (Telstra to the connected service).

Figure 18. Daily Report Traffic Plot



In this example, the uploads and downloads show a close correlation. This is unusual in itself. There is also little difference between day and night. A typical traffic pattern would have noticeable peak periods and a long quiet downtime.

So overall, these traffic patterns appear highly suspicious. This can be confirmed by checking the tabulated usage data for the same period, as shown below:

Figure 19. Daily Report Tabulated Data

Timestamp	UPLOAD (Kbps)	DOWNLOAD (Kbps)	UPLOAD (Bytes)	DOWNLOAD (Bytes)
02/09/2013 00:00	0	0	0	0
02/09/2013 00:05	0	0	0	0
02/09/2013 00:10	0	0	0	0
02/09/2013 00:15	0	0	0	0
02/09/2013 00:20	0	0	0	0
02/09/2013 00:25	0	0	0	0
02/09/2013 00:30	0	0	0	0
02/09/2013 00:35	0	0	0	0
02/09/2013 00:40	0	0	0	0
02/09/2013 00:45	0	0	0	0
02/09/2013 00:50	0	0	0	0
02/09/2013 00:55	0	0	0	0
02/09/2013 01:00	0	0	0	0
02/09/2013 01:05	0	0	0	0
02/09/2013 01:10	0	0	0	0
02/09/2013 01:15	0	0	0	0
02/09/2013 01:20	0	0	0	0
02/09/2013 01:25	0	0	0	0
02/09/2013 01:30	0	0	0	0
02/09/2013 01:35	0	0	0	0
02/09/2013 01:40	0	0	0	0
02/09/2013 01:45	0	0	0	0
02/09/2013 01:50	0	0	0	0
02/09/2013 01:55	0	0	0	0
02/09/2013 02:00	0	0	0	0
02/09/2013 02:05	0	0	0	0
02/09/2013 02:10	0	0	0	0
02/09/2013 02:15	0	0	0	0
02/09/2013 02:20	0	0	0	0

The tabulated report includes five data columns. From left to right, these are:

1. **Date:time**
2. **Upload bandwidth** in kilobits per second (kbps) averaged over the 5 minute period
3. **Download bandwidth** in kilobits per second (kbps) averaged over the 5 minute period
4. **Upload usage** for the 5 minutes, in bytes
5. **Download usage** for the 5 minutes, in bytes.

05.07.03 Analysing the results

Business data patterns will normally vary quite a bit over 24 hours – dropping considerably after hours, for example.

A typical office running a mail server with people accessing the web will probably send a lot more data than it receives, and encounter less traffic overnight. On the other hand, a business hosting a number of websites and/or mail services might have more data going out than in, and traffic at night could be quite high.

Carrying out regular trend analyses and establishing typical patterns for your business will make it easier to identify any unusual changes in your usage.

05.07.04 Identifying the cause

Going back to our example, the tabulated data confirms high traffic (with similar upload and download levels) outside normal business hours. This could well indicate that data is being turned around or rejected by a site. Some of the most common causes include:

- poorly configured router causing a routing loop (See section 05.06.04.03)
- malicious activity such as virus or Denial of Service (DOS) attacks
- your equipment is being used for proxy services. There are numerous proxy services that servers can offer, depending on the operating system and router configuration.

A few more common examples include:

- open web proxy – having a web proxy server that allows access by external internet users means an unknown user can have their browser set up to use your server as their proxy. This can result in high volumes of unwanted traffic being passed through your proxy server – clogging your service and causing excessive usage



- open sock proxy – this also allows unknown external users to generate unwanted data, emails, web requests, etc on your server
- your equipment is being used for Mail Relay. A mail server set up in Open Relay can be used by unknown parties to relay mail to unknown recipients or other mail servers. In other words, your server can be used to distribute spam or other illegal emails
- your equipment is being used as another kind of relay, FTP dump, etc. Allowing full access to 'anonymous FTP' can result in your server being used to store and forward very large data files to internet users worldwide – without your knowledge, but at your expense. If your site allows FTP services, it should be configured to prevent unknown users from writing data to your server.

Note: This is not an exhaustive list and you should consult with your IT support.

Be aware that servers found to be in open proxy or open relay may be included on Black Hole lists, and can have extreme difficulty sending legitimate mail and data to domains that subscribe to these lists.

05.07.05 Identifying the solution for Malicious activity

Introducing Telstra Cloud Applications

A security compromise such as a virus, Trojan or hacking is the most obvious cause of unauthorised data usage. Telstra offers a range of security options as Cloud based applications to help you protect your business information.

Email and Web Security applications

Telstra offers a number of applications which help you protect your business by providing state-of-the-art security for a low monthly fee through T-suite applications. Installation occurs over the web with updates applied automatically, even when you are out of the office, providing hassle-free access to the very latest virus detection every time your staff log on.

Email and Web Security applications include:

- McAfee® SaaS Endpoint Protection (server and desktop security)
- Symantec™ Email Protect.cloud (email anti-virus and anti-spam)
- Symantec.cloud Email Safeguard (emails anti-virus and anti-spam, and blocks inappropriate email use)
- Symantec.cloud Web Safeguard (web anti-virus and anti-spyware, and also controls and monitors web use)
- Symantec.cloud Email and Web Safeguard.

Along with a low monthly subscription, most T-Suite applications include a 30-day free trial.

To find out more about the benefits of using T-Suite applications and how these services make protecting your business easy:

- visit telstrabusiness.com
- call 1800 878 483 9am to 5pm AEST, Monday to Friday.

05.08 CHECKING SERVICE CHANGES

Every time you make a change to your service, it's best to check that the changes haven't caused an adverse effect.

The data shown in Figures 18 and 19 in 05.07.02, for example, highlight an incorrectly configured router which can then be fixed. The graph below shows 5 Minute Polling Data for approximately 12 days on the same service – before and after the router was reconfigured.



Figure 20. Daily Report Traffic Plot.



There was a sharp decline in traffic as soon as the offending router was fixed. From that point there is a distinct difference between business and non-business hours, with almost no traffic on weekends. There is also a significant difference between upload and download traffic, which represents normal usage patterns.

05.09 ACCOUNT LEVEL REPORT ANALYSIS

Account level reporting can be used to identify trends across the entire account, with both graphical and tabular data being available.

Account level analysis is best managed by using the Scheduled Reporting option. (Refer to section 05.05.)

Schedule Reports are sent automatically after each billing cycle and detail the account level records with aggregated service usage data.

You can use the data to follow some of the suggested trend analysis activities outlined above.

05.10 MULTI SITE REPORT ANALYSIS

Multi Site reporting allows you to review and analyse aggregated usage data for a whole Multi Site plan. Both graphical and tabular data is available on screen.

As with Account level analysis, Multi Site data is best managed with scheduled reporting. (Refer to section 05.05.)

Schedule reports are sent automatically after each billing cycle and will provide aggregated details of usage for the Multi Site plan.

You can use the data to follow some of the suggested trend analysis activities outlined above.



06 ACCESS CONTROL LISTS

You can use CustData to create, manage and apply Access Control Lists (ACLs) on Ethernet, ATM and Serial (eg Megalink) interfaces. Your ACLs are then applied outbound on the interface pointing to your service.

Up to 20 lines can be entered into each list.

Internet Protocol version 4 (IPv4) ACLs are supported for Ethernet, ATM and Serial services.

Internet Protocol version 6 (IPv6) ACLs are supported for Ethernet services only.

Note: You are responsible for understanding and managing the ACLs on your Telstra Internet Direct Service:

- you need to read and accept (via a web button) the Conditions of Use, and provide an Operations Contact, before you can implement any ACLs
- you will not be able to create an ACL that blocks you from accessing CustData. You must be able to manage your own ACLs
- we cannot apply any ACLs on your behalf.

ACLs are **not** available with ADSL, BDSL, FTTP, NBN or Frame Relay services, for technical and security reasons.

06.01 TIPS FOR USING ACLS

By default, an ACL is NOT applied to your service. Once you configure an ACL entry via CustData, it will have an implied "deny ip any any" (deny everything) rule at the end of the list.

06.01.01 Priorities

All ACLs are read from top to bottom. Once a rule has been met, the checking stops.

For example, in the list:

1. permit tcp any host 10.10.10.10 eq smtp
2. deny ip any any
3. permit tcp any eq www any

The **first line** will allow mail through from any address to the host 10.10.10.10

The **second line** will deny any IP from any address to any address.

The **third line**, allowing www data through, will never be read – because the second line has already provided a criterion for all addresses.

So this access list will allow mail through to 10.10.10.10 and deny everything else.



06.01.02 Wildcards

Incorrect addresses and wildcards will be accepted, as any valid IP address can be added to an ACL. Therefore, wildcard masking must be clearly understood and correctly applied. An incorrect wildcard mask may produce unexpected results.

Here are some examples of IPv4 address wildcard masking:

Network	Netmask	CIDR Notation	Network/Wildcard
10.10.10.0	255.254.0.0	10.10.10.0/23	10.10.10.0.0.1.255
10.10.10.0	255.255.255.0	10.10.10.0/24	10.10.10.0.0.0.255
10.10.10.0	255.255.255.128	10.10.10.0/25	10.10.10.0.0.0.127
10.10.10.0	255.255.255.192	10.10.10.0/26	10.10.10.0.0.0.63
10.10.10.0	255.255.255.224	10.10.10.0/27	10.10.10.0.0.0.31
10.10.10.0	255.255.255.240	10.10.10.0/28	10.10.10.0.0.0.15
10.10.10.0	255.255.255.248	10.10.10.0/29	10.10.10.0.0.0.7
10.10.10.0	255.255.255.252	10.10.10.0/30	10.10.10.0.0.0.3

IPv6 ACLs follow a simpler format compared to IPv4. Wildcards are not used, rather, the prefix length identifies the valid IPv6 range much like IPv4 CIDR notation.

For example, an IPv6 network identified as 2001:db8:e::/60 is specified in the ACL with an address of 2001:db8:e:: and a prefix length of 60.

Supported prefix lengths are/0 to/64. Host/128 entries are also supported. See **RFC4291** for valid text representations of IPv6 addresses.

06.01.03 Protocol errors

Errors will occur if an incorrect protocol is added to an ACL, as CustData may accept lines that cannot be accepted by the router.

When the **Apply Access List** button has been clicked the following error message may be returned: **Failed to add access list to the access router. For further assistance, please ring the Technical Helpdesk. Refer to Section 11.01 for contact details.**

In these cases, the line in error will simply not be added to the router's configuration. However any correct lines will still be added to the router's configuration.

06.01.04 Syntax errors

CustData can recognise incorrect syntax and generate an error message. The line containing the error will not be added to the ACL.

For example, the line:

permit tcp host 10.10.10.10 eq any gt 1

will result in an error message because a port number must be added after the match "eq" statement.

(If an access line is to cover all ports, select N/A in the **Match** area.)

06.01.05 Planning

The easiest way to avoid errors in your ACLs is to design your rules first, using a spreadsheet.

CustData will allow you to reorganise the lines of your ACL, however it is good practice to design your ACL (reading from top to bottom) first. Doing so can help you check that the list will behave as expected and provide you with a record of your intentions.



The best method is to write your intention, and then the ACL line. For example:

Rule	ACL Line
Permit any tcp reply to requests generated here	permit tcp any any established
Permit any host mail access to host 10.10.10.10	permit tcp any host 10.10.10.10 eq 25
Permit host 10.6.6.6 telnet access to servers 8 through 11	permit tcp host 10.6.6.6 10.10.10.8 0.0.0.3 eq 23
Permit hosts in the 2001:db8:e::/60 network to access the web server	permit tcp 2001:db8:e::/60 host 2001:db8:e::401 eq 443

Note: These tips are provided to highlight a few of the common traps to avoid when using ACLs with CustData. This is not intended to be a substitute for proper training in the design and writing of ACLs.

06.02 ACL MANAGEMENT

Before you can enter the Access Control List Management area of CustData, you must provide an Operations Contact and agree to the Conditions of Use.

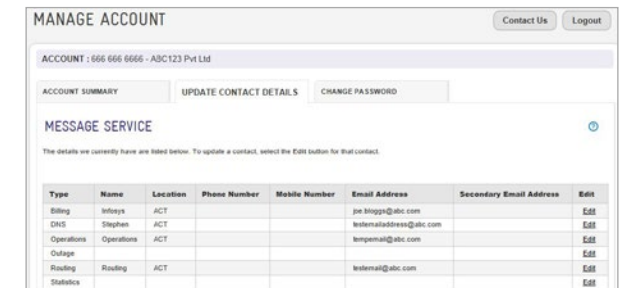
06.02.01 Provide an Operations Contact

1. Log in to CustData.
2. Click on **Account Management** quick link provided on the home page.
3. Click on the **Update Contact Details** tab.
4. Click the **Edit** button next to the Operations line.

You'll then be able to enter and save contact details for your Operations Contact.

06 ACCESS CONTROL LISTS

Figure 21. Manage Account screen

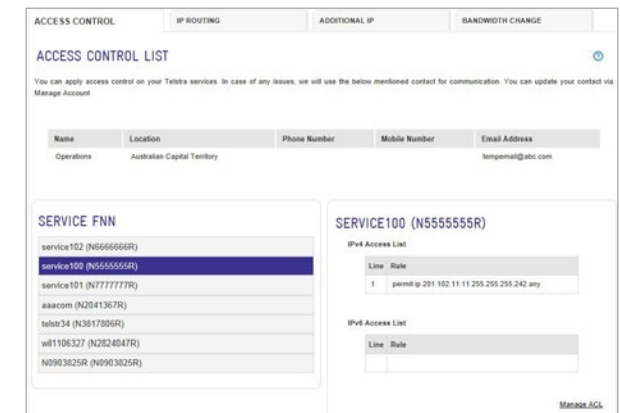


06.02.02 Access Control Lists Page

To view the ACL Summary screen, select **Service** from **Manage** menu on the top right hand corner of Custdata. The Access Control screen will show you all IPv4 and IPv6 Access Lists for your respective Service.

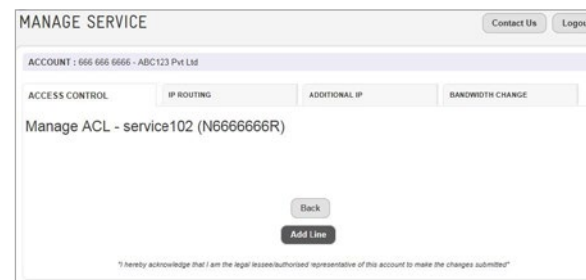
To view or edit an ACL simply select the service from the list provided in the **Access Control List** screen.

Figure 22. Access Control Lists page



06.03 MANAGE ACLS

Figure 23. Create/Amend Access Control Lists



To create or modify ACLs for a service, select appropriate Service on the Access Control List page and click on **Manage ACL** link provided at the bottom right corner of the ACL frame. You will be taken to the Manage ACL page.

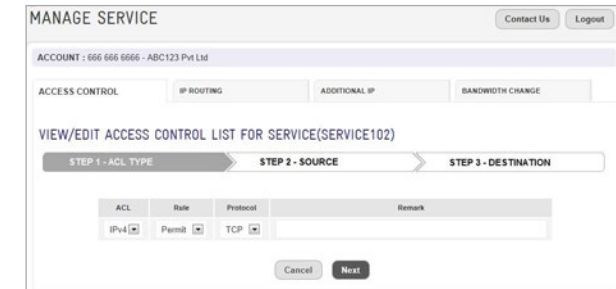
To create a new rule, click on **Add Line** button (your rules must comply with the criteria for creating an ACL on a Cisco Router).

06.03.01 Step 1 – ACL Type

Each ACL line must start with the ACL address family (IPv4 or IPv6), a Rule type (Deny, Permit, or Remark) and the protocol (must be ICMP, IP, IPv6, TCP or UDP).

Select appropriate values from **ACL**, **Rule** and **Protocol** drop down fields respectively.

Figure 24. View/Edit ACL – ACL Type



06.03.02 Step 2 – Source Address and Ports

Each ACL line must have Source Address Details (Any, Host, or Network).

Any does not require an address.

Host requires a specific host IPv4 or IPv6 address.

Network is defined by a starting address and wildcard (A.B.C.D) for IPv4 or prefix length for IPv6.

IPv4 eg Address 10.10.10.10 wildcard 0.0.0.127 – for an address range of 10.10.10.0/25

IPv6 eg Address 2001:db8:e::1 prefix length 60 – for an address range of 2001:db8:e::/60

Each line must also have a rule for matching the type and ports (or range of ports):

eq (equal to) must have a specific port number.

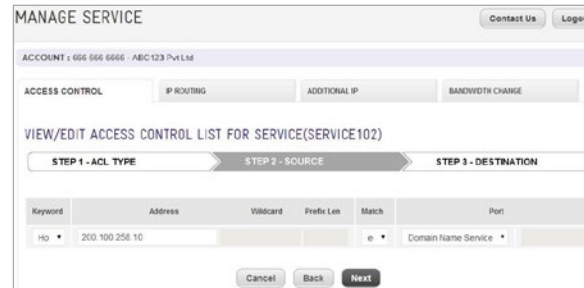
gt (greater than) must have a specific port number.

lt (less than) must have a specific port number.

neq (not equal to) must have a specific port number range, with the starting port and the ending port separated by a space, eg “135 140” means “from ports 135 to 140” (inclusive).

N/A (not applicable) is used when all ports are affected by the rule.

Figure 25. View/Edit ACL – Source



06.03.03 Step 3 – Destination Address and Ports

Each ACL line must include Destination Address Details (Any, Host, or Network).

Any does not require an address.

Host requires a specific host IPv4 or IPv6 address.

Network is defined by a starting address and wildcard (A.B.C.D) for IPv4 or prefix length for IPv6.

IPv4 example: Address 10.10.10.10 wildcard 0.0.0.127 – for an address range of 10.10.10.0/25

IPv6 example: Address 2001:db8:e::1 prefix length 60 – for an address range of 2001:db8:e::/60

Each line must also have a rule for matching the type and ports (or range of ports):

eq (equal to) must have a specific port number.

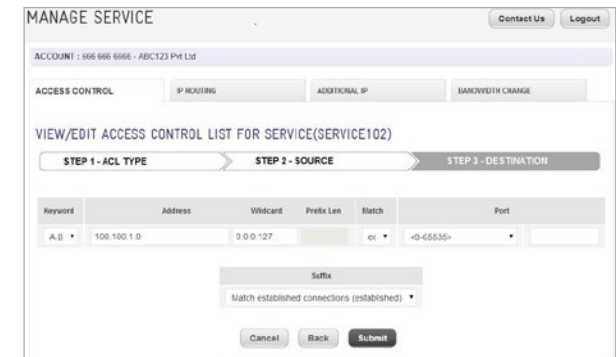
gt (greater than) must have a specific port number.

lt (less than) must have a specific port number.

neq (not equal to) must have a specific port number range, with the starting port and the ending port separated by a space, eg “135 140” means “from ports 135 to 140” (inclusive).

N/A (not applicable) is used when all ports are affected by the rule.

Figure 26. View/Edit ACL – Destination



06.03.04 Suffix

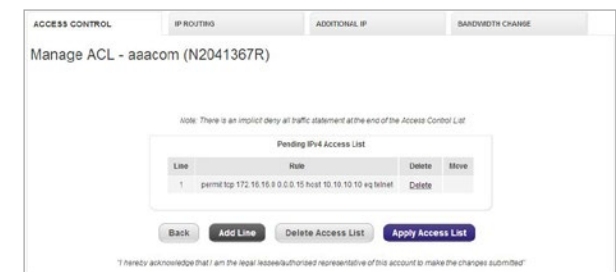
An ACL line may also contain the ‘Established’ suffix.

This is a TCP option, used when the session has already been established at the destination end or by a previously enacted rule.

06.03.05 The ‘Apply Access List’ button

Once you have gone through the steps in sections 6.03.01 through 6.03.04, click on the **Submit** button.

Figure 27. Manage ACL – Apply Access List



Note the implied “deny ip any any” at the end of the list shown above. (If applied, this list would only permit the address range 172.16.16.0 to 15 to access telnet on host 10.10.10.10. All other traffic would be denied.) Click on **Apply Access List** to apply to router.

06.04 EXAMPLE OF A POOR ACL

Figure 28. Incorrect entries in a pending Access Control List

IPv4 Access List	
Line	Rule
1	permit tcp 172.16.16.0 0.0.0.15 host 10.10.10.10 eq telnet
2	permit udp any 10.10.10.0 0.0.0.255 eq finger
3	deny ip any any
4	permit tcp any any established
5	permit tcp any eq smtp host 10.10.10.10

The Access Control List shown on this screen has several problems:

- **Line 1:** permit TCP 172.16.16.1.1.15 host 10.10.10.10 eq telnet The rule is valid and will allow telnet access from 172.16.16.0/28 to 10.10.10.10.
- **Line 2:** permit udp any 10.10.10.0 0.0.0.255 eq finger. While this line may look fine, 'finger' is a TCP option and is not available in UDP. This line will not be written to the router and CustData will display an error message after the ACL is applied.
- **Line 3:** "deny ip any any statement" This line is valid. However, recall that ACLs are read from the top down and stopped when a match has been found. As this line will match any address on any port, it will act on all traffic that didn't match one of the earlier rules and no further lines will be read.
- **Line 4:** This line was probably intended to allow any outgoing requests to receive a response. With good ACL design, it would have been more efficient to write this line early. Then fewer lines would need to be red in many cases, speeding up the data handling.
- **Line 5:** This line would have allowed mail servers to respond to mail being sent to them – however this was probably not the intention. Line 5 was more likely intended that mail could be sent to the mail server, and should have been written as "permit tcp any host 10.10.10.10 eq 25".

This list highlights the importance of constructing and writing ACLs carefully. While ACLs can be reorganised within CustData, correctly designing access lists on paper or a spreadsheet first will save time and the reduce the likelihood of introducing errors.

06.05 TESTING YOUR ACL

Once you have created your ACL, you should test it from a remote site.

To test the example given in Figure 28:

Telnet from devices in the 172.16.16.0.255.255.240 network to host 10.10.10.10 (Use devices from both end of the range, as well as in the middle).

06.06 DELETING AN ACL

To delete an access control list, navigate to the Manage ACL page (refer section 06.03), then click on the **Delete Access List** button. This will clear the ACL from the router and from CustData.

Figure 29. Delete ACL

Note: There is an implicit deny all traffic statement at the end of the Access Control List

Existing IPv4 Access List			
Line	Rule	Delete	Move
1	permit tcp 172.16.16.0 0.0.0.15 host 10.10.10.10 eq telnet	Delete	▼
2	permit udp any 10.10.10.0 0.0.0.255 eq finger	Delete	▲ ▼
3	deny ip any any	Delete	▲ ▼
4	permit tcp any any established	Delete	▲ ▼
5	permit tcp any eq smtp host 10.10.10.10	Delete	▲

Back Add Line Delete Access List Apply Access List

07 MANAGING YOUR ROUTING

CustData gives you the ability to manage many routing options for your Telstra Internet Direct service. This means you can better control and customise your service, at any time that it suits you.

Note: The Routing feature is not available for Telstra services on the NBN.

07.01 MAINTAINING YOUR CONTACT DETAILS

Before you can use CustData to manage the routing to your service, you need to set up a **Routing contact** in the **Update Contact Details** tab of **Manage Account** section. (See section 02.03 for instructions.)

When a change is made to your routing via CustData, an email requesting approval for the change will be sent to the contact for the relevant IP address block, as listed in the register of the body that allocates that IP address range.

While the Routing contact you nominate in CustData Update Contact Details section does not have to be the same as this registered contact, it is preferable.

It is important that both sets of contact details are updated if the listed person leaves your organisation and/or their email address changes.

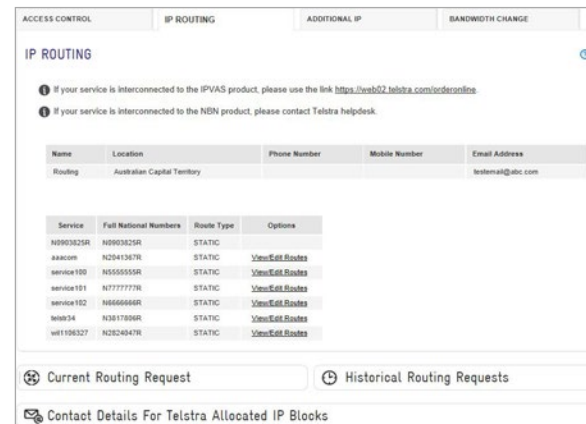
07.01.01 IP addresses allocated by Telstra

You must take the time to maintain accurate contact details. Here's how to check the current registered contact details for an IP address range allocated by Telstra:

1. Log in to CustData
2. Select **Service** menu option from **Manage** menu on the top right corner of the **Home** screen.
3. Click on **IP Routing tab** on the **Manage Service** screen.
4. At the bottom of the screen, click on **Contact details for Telstra-allocated IP blocks**
5. Check that the email address is correct. Remember, this email address is where approval requests for all routing changes will be sent for confirmation before they are actioned
6. Make any required changes and click on the **Submit button**.

Further assistance is available via **Online Help**.

Figure 30. IP Routing screen



ACCESS CONTROL IP ROUTING ADDITIONAL IP BANDWIDTH CHANGE

IP ROUTING

1 If your service is interconnected to the IPVAS product, please use the link <https://web02.telstra.com/orderonline>.

1 If your service is interconnected to the NBN product, please contact Telstra helpdesk.

Name	Location	Phone Number	Mobile Number	Email Address
Routing	Australian Capital Territory			testemail@abc.com

Service	Full National Numbers	Route Type	Options
N090325R	N090325R	STATIC	
aaacom	N2041367R	STATIC	View/Edit Routes
service100	N5555555R	STATIC	View/Edit Routes
service101	N7777777R	STATIC	View/Edit Routes
service102	N8888888R	STATIC	View/Edit Routes
win34	N3317896R	STATIC	View/Edit Routes
will108327	N2824847R	STATIC	View/Edit Routes

Current Routing Request Historical Routing Requests

Contact Details For Telstra Allocated IP Blocks

07.01.02 IP addresses not allocated by Telstra

07.01.02.01 Non-Telstra IPv4 subnets

You will need to call the Telstra Business Technical Helpdesk (refer to Section 11 for contact details) if you are subnetting Class B or Class C IPv4 address ranges not assigned to you by Telstra. (If you're not sure who your IP Address registrar is, you can check by using the Whois lookup service at www.apnic.com). Please note that the minimum subnet advertisement that can be propagated between ISPs is a/24 subnet (Class C).

If you intend to assign a smaller subnet than this (/25 to /32) from your non-Telstra allocated IP address range to any of your Broadband services, you will need to call the Technical Helpdesk (refer to Section 11 for contact details) to establish a/24 summary route before you request routing changes through CustData.

07.01.02.02 Non-Telstra IPv6 subnets

The longest IPv6 prefix length advertisement which can be propagated between ISPs is a/48 subnet. The /48 prefix route must be originated from the customer AS. The longest prefix-length that Telstra will accept for a route advertised to it using BGP is /48. Telstra Internet Direct customers may use address blocks of prefix-length up to /56 for prefix delegation on their ADSL Services.

07.02 CHANGING ROUTING TO YOUR SERVICE

You can use CustData to control the routing to your service.

However, the following important notes apply:

1. **use extreme care** – a mistake could remove your IP networks from the internet
2. **if you have IP Addresses that are not allocated by Telstra**, refer to section 07.01.02 for important routing policy information. (You may need to contact the Technical Helpdesk (refer to Section 11 for contact details) for assistance with creating summary routes
3. **Routing change implementation** is scheduled at 08:05, 10:05, 12:05, 14:05, 16:05, 18:05, 20:05, 22:05 and 00:05 AEST (or AEDT during daylight savings period in eastern states) daily
4. **RADIUS server login authentication.** Telstra Internet Direct connections via ADSL set up user details in the Telstra Internet Direct access router and use a RADIUS server for login authentication. If you submit a routing request for one of these services you will need to disconnect from the service and reconnect at least 1 hour after the change has been authorised and implemented. Authorised routing changes will not take effect until after you have disconnected and reconnected
5. **test your service.** Once changes have been implemented, we highly recommend that you use CustData to test your service for correct configuration. Please see Section 08 for information about Routing Tests.



07.02.01 To change routing to your service

1. Log in to CustData.
2. Select **Service** menu item from the **Manage** menu on the top right corner of the Home screen.
3. Click on **IP Routing** tab on the **Manage Service** screen.
4. Click on the **View/Edit Routes** button for the relevant service you would like to view or modify.
5. Add, change or delete routes as described below.

07.02.02 Add Static Routes

Use this procedure if your service uses Static routing.

1. Access the **View/Edit Routes** screen as described in Section 07.02.01.
2. Enter the new route in the **Network Address** field and select the **CIDR** value.

Network Address		CIDR
201.35.218.215	/	24

Add

3. Click the **Add** button after you have entered the prefix details.
4. In the next confirmation screen, clicking the **Submit** button will automatically send an authorisation email to the registered contact of the prefix. It is imperative that this email is responded to promptly and exactly as instructed. The request will be in **Pending Approval** status until it has been authorised.
5. When authorisation is received the request will be updated to **Approved Pending Action** status.
6. The new static route will be added to the access router at the next scheduled implementation time (see note 3 in Section 07.02 for routing implementation schedule).

07.02.03 Add BGP Routes

Use this procedure if your service uses BGP routing. To update your AS Filter, refer to Section 07.02.06.

1. Access the View/Edit Routes screen as described in Section 07.02.01.
2. If you only need to add a single prefix to your BGP filter/prefix list, leave the **Variable Prefix** checkbox unticked, enter the new prefix in the **Network Address** field and select the **CIDR** value. See the screenshot below for an example – this would be an exact match for prefix 203.50.0.0 with subnet mask 255.255.252.0.

Variable Prefix	Network Address		CIDR	ge ?	le ?
<input type="checkbox"/>	203.50.0.0	/	22		

Add

If you want to specify a range of prefix lengths for a given prefix, tick the **Variable Prefix** checkbox, enter the new prefix in the **Network Address** field and select the **CIDR** value. Then select the upper and lower bounds of the prefix length to match on using the **ge** (greater than or equal to) and **le** (less than or equal to) fields. See the screenshot below for an example – this would match on any prefix in the IP address block 203.50.0.0/16 with a prefix length between 20 and 24 bits, inclusive.

Variable Prefix	Network Address		CIDR	ge ?	le ?
<input checked="" type="checkbox"/>	203.50.0.0	/	16		

Add

3. Click the **Add** button after you have entered the prefix details.
4. In the next confirmation screen, clicking the **Submit** button will automatically send an authorisation email to the registered contact of the prefix. It is imperative that this email is responded to promptly and exactly as instructed. The request will be in **Pending Approval** status until it has been authorised.
5. When authorisation is received the request will be updated to **Approved Pending Action** status.
6. The new prefix will be added to the access router at the next scheduled implementation time (see note 3 in Section 07.02 for routing implementation schedule).



07.02.04 Subnetting

1. Follow 07.02.01 and 07.02.02 (above) to change the size of your IP address range.
2. Once the new range has been added, it will be safe to delete the existing range. (The same email authorisation and action procedures apply as for adding address ranges.)

Note: If your IP address range is not allocated by Telstra, you need to call the Technical Helpdesk (refer to Section 11 for contact details) to confirm that any routing changes will not remove your broadband service from the internet.

If your subnet address range is less than Class C (/24) then a summary route will need to be established before you request routing changes through CustData.

07.02.05 Delete routes

1. Access the **View/Edit Routes** screen as described in 07.02.01.
2. Click on the **Delete** button at the right of the range To be deleted.
3. The request will be listed as **Pending Approval**.
4. CustData will automatically send an authorisation email to the registered contact. It is imperative that this email is responded to promptly and exactly as instructed.
5. When authorisation is received the changes will be implemented in the next scheduled session. (See Note 3 of 07.02 for times.)

07.02.06 Update AS Path Filter

Use this procedure if your service uses BGP routing and you want to update your Autonomous System (AS) path filter.

1. Log in to CustData.
2. Select **Service** menu item from the Manage menu at the top right hand of the Home screen.

3. Select **IP Routing** tab from the **Manage Service** screen.
4. Click on the **View/Edit AS Filters** button.
5. Enter the AS number in the **Add AS Number** field.
6. Select whether the AS is terminating, transiting or terminating and transiting using the **AS Type** drop-down.

Terminating – TID network will accept routes that have originated from the specified AS.

Transiting – TID network will accept routes that have passed through the specified AS. If you are using AS path prepending to influence route selection, set the prepended AS numbers as Transiting.

Transiting and Terminating – TID network will accept routes that have originated from or passed through the specified AS.

7. Click **Submit** to confirm the changes. Your AS path filter will be updated on the access router at the next scheduled implementation time (see note 3 in Section 07.02 for implementation schedule).

Please be aware that in some cases adding more than 31 transiting AS Numbers will be unsuccessful without warning. Please contact Telstra for assistance in such cases.



07.03 MANAGE THE IPV6 PREFIX DELEGATION FOR YOUR ADSL SERVICE

This section applies only to IPv6-enabled (ie dual-stack) ADSL services.

You can use CustData to manage the Delegated IPv6 Prefix associated with your ADSL service. The term **Delegated IPv6 Prefix** refers to a RADIUS attribute that carries an IPv6 prefix to be delegated to you, for use in your network. For example, a prefix in a Delegated IPv6 Prefix attribute can be further delegated to another node through DHCP Prefix Delegation.

The following **important notes** apply:

1. **use extreme care** – a mistake could disconnect you from the internet
2. **customers with IPv6 prefixes allocated by Telstra** are only permitted to view their Delegated IPv6 Prefix
3. **customers with IPv6 prefixes not allocated by Telstra** (ie provider-independent allocations) are permitted to view and modify their Delegated IPv6 Prefix. Refer to section 07.01.02 for important routing policy information
4. **IPv6 Prefix change implementation** is scheduled to occur every hour on the hour
5. **RADIUS server login authentication.** Telstra Internet Direct connections via ADSL use a RADIUS server for login authentication. If you submit a delegated IPv6 prefix change request, you will need to reset your modem after the change has been authorised and implemented in order for the change to take effect
6. **test your service.** Once changes have been implemented, we highly recommend that you use CustData to test your service for correct configuration. Please see Section 08 for information about Routing Tests.

07 MANAGING YOUR ROUTING

07.03.01 View Delegated IPv6 Prefix

1. Log in to CustData.
2. Select **Service** menu item from the **Manage** menu at the top right hand of the Home screen.
3. Select **IP Routing** tab from the Manage Service screen.
4. Click on the **Manage Delegated IPv6 Prefix** button.
5. The ADSL Delegated IPv6 Prefix Management page will display the Delegated IPv6 Prefix assigned to your service.
6. For customers using provider-independent ranges, you can Add, Modify or Delete your Delegated IPv6 Prefix as described below.

07.03.02 Add Delegated IPv6 Prefix

1. Access the **Manage Delegated IPv6 Prefix** screen as described in 07.03.01 above.
2. Enter the new IPv6 prefix in the **Add Delegated IPv6 Prefix** field using CIDR notation eg 2001:db8:e::/56.
3. The add prefix request will be listed as **Pending Approval**.
4. CustData will automatically send an authorisation email to the registered contact. It is imperative that this email is responded to promptly and exactly as instructed.
5. When authorisation is received the add prefix request will be updated to **Approved Pending Action** status.
6. The new prefix will be added to RADIUS at the next scheduled implementation time, after which the ADSL modem will need to be reset for the changes to take effect.



07.03.03 Modify Delegated IPv6 Prefix

1. Access the **Manage Delegated IPv6 Prefix** screen as described in 07.03.01 above.
2. Click on the **Update** button.
3. Enter the new IPv6 prefix using CIDR notation, eg 2001:db8:e::/56 and click Update.
4. The modify prefix request will be listed as **Pending Approval**.
5. CustData will automatically send an authorisation email to the registered contact. It is imperative that this email is responded to promptly and exactly as instructed.
6. When authorisation is received the modify prefix request will be updated to **Approved Pending Action** status.
7. The new prefix will be updated in RADIUS at the next scheduled implementation time, after which the ADSL modem will need to be reset for the changes to take effect.

07.03.04 Delete Delegated IPv6 Prefix

1. Access the **Manage Delegated IPv6** screen as described in 07.03.01 above.
2. Click the **Delete** button.
3. The delete prefix request will be listed as **Pending Approval**.
4. CustData will automatically send an authorisation email to the registered contact. It is imperative that this email is responded to promptly and exactly as instructed.
5. When authorisation is received the delete prefix request will be updated to **Approved Pending Action** status.
6. The prefix will be removed from RADIUS at the next scheduled implementation time, after which the ADSL modem will need to be reset for the changes to take effect.

07.04 TEST YOUR CHANGES

Once any routing changes have been implemented, we highly recommend that you use CustData to test your service for correct configuration. Please see Section 08 for information about Routing Tests.

Further assistance is available via **Online Help**.

08 ROUTING TESTS

Once you have set up routing to your service (see Section 07 above) you should use CustData to perform a **Node to Host Trace** to check that the routes are correct.

CustData's **Network Visibility** feature provides end-to-end visibility of your internet service to enable you to resolve issues with less delay. To access the Network Visibility feature, select **Diagnostic Toolkit** menu-item from the Support menu available at the top right corner of CustData screen, then click the **Network Visibility** tab. This tab has three functions:

- **Node to Node Testing:** Ping test between two TID Points of Presence (POP)
- **Node to Host Testing:** Ping or trace test between a TID POP and any Internet host
- **Route Lookup:** Query TID's BGP routing tables.

It is important to use a routing test after adding or removing an IP address range, to confirm that your proposed routing changes have been implemented.

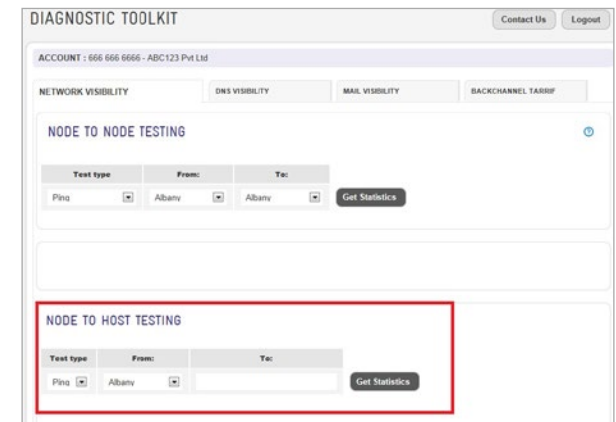
- **Successfully Adding IP Addresses** will result in a successful trace, as described under 08.02.01 below.
- **Successfully Deleting IP addresses** may return a result similar to that under 08.02.02 below.

Note: The Testing feature is not available for Telstra services on the NBN.

08.01 HOW TO TEST YOUR ROUTING

08.01.01 Node to Host Testing

Figure 31. Node to Host Testing



The screenshot shows the 'DIAGNOSTIC TOOLKIT' interface. At the top right are 'Contact Us' and 'Logout' buttons. Below is the account information: 'ACCOUNT : 666 666 666 - ABC123 Pty Ltd'. There are four tabs: 'NETWORK VISIBILITY' (selected), 'DNS VISIBILITY', 'MAIL VISIBILITY', and 'BACKCHANNEL TARIFF'. Under 'NETWORK VISIBILITY', there is a 'NODE TO NODE TESTING' section with a table. The table has columns 'Test type', 'From', and 'To'. The 'Test type' is 'Ping', 'From' is 'Albany', and 'To' is 'Albany'. There is a 'Get Statistics' button. Below this is another 'NODE TO HOST TESTING' section, which is highlighted with a red box. It has the same table structure, but the 'To' field is empty, and the 'Get Statistics' button is also present.

1. Log in to CustData.
2. Select **Diagnostic Toolkit** menu item from **Support** menu on the top right hand corner of the Home screen.
3. On the **Network Visibility** tab scroll down to the **Node to Host Testing** section.
4. In the Test type field, select either **Ping** or **Trace** based on your testing requirement.

- In the **From** field, select a remote Telstra Internet Direct PoP from the list. Be sure to choose a remote PoP as your local PoP may not detect a 'routing loop' caused by incorrect router configuration.
- In the **To** field, enter the IPv4 or IPv6 address that you wish to trace or ping.
- Click on the **Get Statistics** button.

Your test results may take some time to come back, especially if the test is made to a device that is not correctly configured.

08.01.02 BGP Route Lookup

Figure 32. Diagnostic Toolkit BGP Route lookup



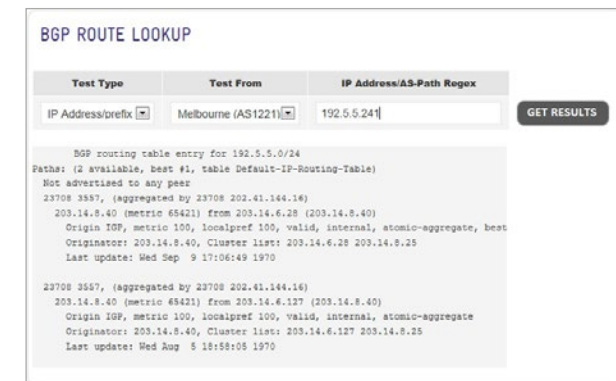
The Route Lookup tool allows you to query TID's BGP routing tables. There are two query types:

• IP Route:

- Log in to **CustData**.
- Navigate to **Support** menu on the top right hand menu and select **Diagnostic Toolkit** menu item.
- On the **Network Visibility** tab, scroll down to **BGP Route Lookup** section at the bottom of the screen.
- In the **Test Type** field, select IP Address/prefix and in the **Test From** field select the appropriate site to lookup from.
- In the **IP Address/AS-Path Regex** field, enter an IPv4 or IPv6 address/route.
- Click on **Get Results** button.

The example in the figure below shows the BGP routing table entries for the route to the 'F' root name server at 192.5.5.241. The command executed on the route server was 'show ip bgp 192.5.5.241'

Figure 33. Diagnostic Toolkit BGP Route Output



• AS Path (regex):

- Log in to **CustData**.
- Navigate to **Support** menu on the top right hand menu and select **Diagnostic Toolkit** menu item.
- On the **Network Visibility** tab, scroll down to **BGP Route Lookup** section at the bottom of the screen.
- In the **Test Type** field, select AS-Path regex and in the **Test From** field select the appropriate site to lookup from.
- In the **IP Address/AS-Path Regex** field, enter an AS number or regular expression to query the AS paths in the BGP table.
- Click on **Get Results** button.

The example below shows the output when querying the BGP routing table for AS paths that terminate in ASN 3557. The command executed on the route server was 'show ip bgp regexp _3557\$'.

Figure 34. Diagnostic Toolkit BGP Route AS Path Output

BGP ROUTE LOOKUP

Test Type	Test From	IP Address/AS-Path Regex
AS-PATH regex	Melbourne (AS1221)	_3557\$

GET RESULTS

BGP table version is 0, local router ID is 203.14.6.122

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, R Removed

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 1192.5.4.0/23	134.159.124.195	65	0	4637	6461 1280 3557 i
**i	134.159.160.247	65	0	4637	174 1280 3557 i
* 1192.5.4.0	134.159.124.195	65	0	4637	1280 3557 i
**i	134.159.160.247	65	0	4637	1280 3557 i
**>1192.5.5.0	203.14.0.40	100	100	0	23708 3557 i
* i	203.14.0.40	100	100	0	23708 3557 i

Total number of prefixes 3

08.02 COMMON TRACEROUTE RESULTS

Once you conduct a test, a table similar to that illustrated in Figure 35 will come up.

- **Network Device** shows the pathway that traffic will follow from the nominated PoP to your nominated IP address.
- **Round Trip Times** indicate the time taken for traffic to bounce from one access point to another.

Figure 35. Node to Host Trace results

NODE TO HOST TESTING

Test type	From:	To:
Trace	Albany	google.com

Get Statistics

#	Network Device	Round Trip Times
1	serial5-0.wel-core4.perth.telstra.net (203.50.112.36)	0 msec 12 msec 0 msec
2	gigabitethernet10-0-2-2.wel-core3.perth.telstra.net (203.50.113.17)	12 msec 12 msec 12 msec
3	bundle-ether7.ifi-core1.adelaide.telstra.net (203.50.11.18)	40 msec 44 msec 44 msec
4	bundle-ether9.win-core1.melbourne.telstra.net (203.50.11.91)	56 msec 52 msec 52 msec
5	bundle-ether12.ken-core4.sydney.telstra.net (203.50.11.12)	64 msec 64 msec 64 msec
6	bundle-ether1.ken-edge901.sydney.telstra.net (203.50.11.95)	64 msec 64 msec 64 msec
7	gao1154859.lnk.telstra.net (130.130.213.54)	64 msec 64 msec 64 msec
8	66.249.95.232 [AS 15169]	64 msec 64 msec 76 msec
9	72.14.237.135 [AS 15169]	60 msec 60 msec 64 msec
10	syd01s12-4n-k3.1e100.net (74.125.237.99) [AS 15169]	64 msec 64 msec 64 msec

08.02.01 Successful trace results

- **Result** – The trace goes to your service, which responds with a message that the appropriate host is reachable and the trace stops.

Note: When doing the trace from a server, a series of question marks and asterisks may be returned, even though your router and/or device has been properly configured. This occurs when the trace is denied access by the server – and will be indicated by an **!A**** notation in the **Round Trip Times** column.

08.02.02 Unsuccessful trace results

The following results will help you interpret some of the more common results from an unsuccessful test, however this is not a complete list.

There are many other reasons for unusual or unsuccessful trace routes, including the service not being connected when the trace is conducted.

If you require help interpreting a test result, we suggest you consult with your IT support.

08.02.02.01 Traceroute to an unconfigured route

• Result 1 – Route is unconfigured

The trace goes to your Telstra Internet Direct access router and stops, with a series of question marks and asterisks appearing on the last line of the report. This often indicates that the access device is not properly configured. You should check the configuration and/or seek assistance from your supplier or IT support. Telstra Business also offers a range of IT support options for Telstra Business Broadband available through the 'Business Support' Extra. Consult with your Telstra Business Account Executive or call 13 2000.

• Result 2 – Routing Loop

The trace goes past the Telstra Internet Direct access router to your network router, is returned to the access router, which returns it to the network router, and so on. This routing loop can lead to abnormally high usage and poor service performance.

To resolve this issue, the route needs to be terminated at your end by correctly configuring your router. You should seek the assistance of your router supplier or IT support as the correct termination/configuration method will depend on your specific device.

Alternatively, you can simply delete the tested IP address.

Routing loops can easily occur if you have a number of advertised IP addresses but only use a few – leaving the rest unconfigured. You can check the subnets routed to a service by clicking the **View/Edit Routes** button.

08.02.02.02 Trace route to an unconfigured device

- **Result 1** – The trace ends at your link, then returns a series of question marks and asterisks. This often indicates that your access device is not properly configured and you should seek assistance from your router supplier or IT support.
- **Result 2** – If your trace is directed to an address range that isn't in the routing tables of the access router will usually stop at the Telstra Internet Direct Core Router with a series of question marks and asterisks.

The address range (having been deleted) is simply undeliverable and this result does not affect your service.

Note: A similar result may occur if your Telstra Internet Direct service is not connected at the time of the test.

Figure 36. Node to Host Trace results for a trace to an unconfigured device

NODE TO HOST TESTING		
Test type	From:	To:
Ping	Warmambool	www.example.com
Get Statistics		
#	Network Device	Round Trip Times
1	serial5-0.wel-core4.perth.telstra.net (203.50.112.36)	8 msec 12 msec 8 msec
2	gigabitethernet0-0-2.wel-core3.perth.telstra.net (203.50.113.17)	12 msec 12 msec 12 msec
3	bundle-ether7.fli-core1.adelaide.telstra.net (203.50.11.10)	40 msec 44 msec 44 msec
4	bundle-ether9.win-core1.melbourne.telstra.net (203.50.11.81)	56 msec 52 msec 52 msec
5	bundle-ether12.ken-core4.sydney.telstra.net (203.50.11.12)	64 msec 64 msec 64 msec
6	bundle-ether1.ken-edge901.sydney.telstra.net (203.50.11.95)	64 msec 64 msec 64 msec
7	pool1154859.lnk.telstra.net (139.130.213.54)	64 msec 64 msec 64 msec
8	***	***
9	***	***
10	***	***

09 DOMAIN NAME SERVICE

The Domain Name Service (DNS) functions of CustData are divided into two sections – Primary DNS management and Secondary DNS management.

Both are found in the Manage DNS Screen (Navigate via Manage – > DNS), and both are available to Telstra Business, Enterprise and Wholesale customers. However, their use is only recommended if you are managing a small network.

- Use Primary DNS if your DNS zone is hosted on the Telstra Internet Direct nameservers.
- Use Secondary DNS if your DNS zone is hosted by another provider.

09.01 MANAGING A PRIMARY DNS

The Primary DNS allows you to host and configure your Domain Name on the Telstra Internet Direct nameservers. Once your domain has been configured on CustData, you will need to have your registrar (MelbourneIT, Ausregistry, etc) delegate the domain so all DNS queries are successfully passed to Telstra Internet Direct.

The relevant delegation details are:

- Primary DNS ns0.telstra.net 139.130.204.47
- Secondary DNS ns1.telstra.net 139.130.4.5

Note: CustData's Primary DNS feature does not support zone transfers to non-Telstra DNS servers (e.g. using the 'allow-transfer' directive). However, the full zone file is viewable from within CustData's View Zone function, or can be delivered as a text file upon request.

09.01.01 To record a new Primary DNS

1. Log in to CustData.
2. Select **DNS** menu item from the **Manage** menu on the top right hand corner of the Home screen.
3. In the **Add Domain** section on the **Primary DNS** tab enter the Domain Name and the email address of the person responsible for managing that domain.
4. Set the **TTL** (or leave as the default if unsure).
5. Click on the **Add** button.

09.01.02 To update an existing Primary DNS

If you've already entered a Primary DNS on CustData, you can update the:

- **Start of Authority (SOA).** Change the email details of the person responsible for the domain, and change the TTL (Time To Live)
- **Assign IP Address.** Enter the IP address against the domain name, so web users can access your web server without using 'www'.



- **Assign hosts or aliases.** Select one of the following record types:
 - A** – links a hostname with an IPv4 address
 - AAAA** – links a hostname with an IPv6 address
 - CNAME** – Canonical Name records are used as an alias for a host name
 - NS** – Name Server records are used for subdomain delegation
 - MX** – Mail Exchanger records link a domain name to Message Transfer Agents (mail servers) for that domain
 - HINFO** – Host Info records describe the type of computer/operating system a host uses
 - SRV** – Service records define the hostname and port number of servers for specified services
 - TXT** – Text records carry arbitrary data (must be enclosed within double quotes eg "MS=ms722939").
1. Log in to **CustData**.
 2. Select **DNS** menu item from the **Manage** menu on the top right hand corner of the Home screen.
 3. Scroll down to the **Manage DNS Domain** section of the **Primary DNS** tab and click the **Update** button next to the relevant domain.
 4. Select and update the information you wish to change or, if a host/alias is no longer required, click **Delete** next to that alias.
 5. Click on the **Submit** button.

09.02 MANAGING A SECONDARY DNS

09.02.01 To record a Secondary DNS

The Secondary DNS screen allows you to set Telstra as the secondary server for your domain, while it is being primarily hosted on another provider's nameserver.

To do this, you need to:

- Enter the Primary Server's IP address and your Domain Name on CustData
- Ensure that the Primary Server accepts AXFR queries from the Internet Direct Secondary DNS ns1.telstra.net (139.130.4.5).

09.02.02 To record a Secondary DNS

1. Log in to CustData.
2. Select **DNS** menu item from the **Manage** menu at the top right hand corner of the Home screen.
3. Click on **Secondary DNS** tab on the Manage DNS screen.
4. Enter the Domain Name and the email address of the person responsible for managing that domain.
5. Add the Domain Name and IP address of the primary nameserver.
6. Click on the **Add** button.

09.03 CANCELLING AN ACCOUNT

If CustData is used to Host your Domain Name Service (DNS) and you are cancelling all services on your account, you will need to align your DNS hosting with another account or arrange for your DNS to be hosted with an alternate Internet Service Provider.

10 ADDITIONAL IP ADDRESS SERVICES

To order additional IP address blocks in Custdata, follow the steps below:

1. Log in to **CustData**.
2. Select **Service** from **Manage** menu on the top left-hand menu.
3. On the **Manage Service** screen, click on **Additional IP** tab.

The IP Address Form screen will open up in a different tab on your Internet browser.

This feature is not available for Telstra services on the NBN – please contact your Telstra Representative or call us on **13 2000** should you require additional IP address space for your Telstra services on the NBN.

This feature is also not available to Telstra Wholesale customers.

The following is a brief description of the rules that apply for requesting additional IP addresses.

A reference to Telstra Internet Direct (TID) includes TID that is provided as part of a Business Broadband service.

TID will allocate provider-based non-portable IP address space to those direct clients of the TID service who are single-homed to TID, as a component of the services TID provides to its customer base.

Those parties who are multi-homed (connected to more than one Internet Service Provider), and large Internet Service Providers should contact the **Asia Pacific Network Information Centre** for allocation of ISP provider space or large enterprise address space.

APPLICATION JUSTIFICATION

If you are requesting up to 16 IPv4 Addresses (4 BITS), you will need provide information describing the proposed use of the requested address block.

If you are requesting larger IPv4 Blocks, ie more than 16 IPv4 addresses or additional IPv6 prefixes (eg/48), you will need to provide information describing the proposed use of the requested address block as well as a network diagram or plan that shows the proposed use of requested addresses.

For all requests, you will need to include responses to the following:

- are you using all your currently allocated IP addresses?
- what is your forecasted growth for IP address use?
- description of network topology
- description of network routing plans
- why NAT or private addressing is not an option?
- Subnetting Plan.

Note:

- The address space allocation will be provisional on you remaining connected to TID. When the connection ceases, the addresses will be reclaimed.
- Addresses allocated via this mechanism will only be routed by TID – they cannot be used with a different service provider.
- All of the address space allocated must be routed and visible to the global internet – the addresses must not be used in a private context.
- You will need to provide your 10 digit account number before addresses can be allocated.
- Applications for IP addresses will usually be processed within 7 days of receipt.
- If we accept your application, any usage of the IP addresses will be governed by the terms and conditions set out in our agreement with you.

11 CONCLUSION

Using CustData can be a vital part of your Broadband management strategy. Using the tools and reports provided here will help to ensure your service is properly configured.

While it is almost impossible to remedy a problem after the fact, regular checking of your service statistics can enhance your network's performance and reduce your costs.

Of course it is also essential to maintain your hardware and security systems, keeping both up to date by installing all applicable patches and updates as recommended by the vendors.

The Internet is a powerful business tool. We hope we can help it play a key role in your ongoing success.

11.01 Further Assistance

Further assistance is available via CustData's Online.

Help feature – simply click on the **Online Help** button available on the **Home** screen (**Online Help** option is also available from the **Support** menu on the top right hand corner of Custdata screens).

For CustData Faults:

Use the **Report A Fault** function in CustData or contact the Technical Helpdesk using one of the numbers below:

- Telstra Business customers can call 132999
- Telstra Enterprise and Government customers can call 1800 066 594
- Telstra Wholesale customers can call 18 02288 (Option2, Option1).

For Internet Service Faults:

Telstra Business customers can call **132999** for assistance with the following broadband products:

- Business Broadband
- BizEssentials
- DOT (Digital Office Technology)™
- T-Biz (NBN).

Telstra Enterprise and Government customers can call 1800 066 594 for assistance with Telstra Internet Direct.

Telstra Wholesale customers can call 18 02288 (option 2, option 1) for assistance with the following products:

- Telstra Wholesale Internet (TWI)
- Virtual Internet Service Provider (vISP) Broadband.