Table of Contents

Contents

1. AT&T VPN General Information ................................................................................................................. 4
   1.1. AT&T VPN Service Options (Types) ....................................................................................................... 4
   1.2. AT&T VPN Managed Router Option Exceptions ..................................................................................... 4
   1.3. AT&T VPN Managed CSU-Probe Option Exceptions .............................................................................. 5

2. General Customer Responsibilities and Expectations (applies to all AT&T VPN service types) .................. 5
   2.1. Account Profile Set Up and Ordering of Service – all Service Types .................................................. 5
   2.2. AT&T VPN Access Arrangements ........................................................................................................... 6
   2.3. Provisioning of Service – all Service Types .......................................................................................... 7
       2.3.1. Provisioning of Service – Managed Router and Managed CSU/Probe Options ......................... 9
   2.4. Trouble Resolution for Test and Turn-up – all Service Types ............................................................. 12
   2.5. Invoicing – all Service Types ............................................................................................................... 12
   2.6. Changes to Service and Disconnects: MACD Requests – all Service Types ...................................... 13
   2.7. AT&T BusinessDirect® - Network Reporting and Statistics ............................................................... 13

3. General AT&T Responsibilities (applies to All AT&T VPN service options) ............................................. 13
   3.1. Provisioning of Service – all Service Types .......................................................................................... 13
       3.1.1. Provisioning of Service – Managed Router and Managed CSU-Probe Options ..................... 15

4. Access and Access Site Requirements ......................................................................................................... 15
   4.1. Ethernet Access and Customer Site Requirements .............................................................................. 15
       4.1.1. US Sites ............................................................................................................................................ 15
       4.1.2. MOW Sites ..................................................................................................................................... 15
       4.1.3. Customer Site Requirements for Both US and MOW ..................................................................... 16
   4.2. Digital Subscriber Line (DSL) – All Service Options ........................................................................ 16

5. AT&T Network Suite .................................................................................................................................... 16
   5.1. Wireless Back-up for Automatic Failover Feature .............................................................................. 16
   5.2. Change Orders for AT&T Network Suite Services ........................................................................... 18

6. International/Most of World (MOW) Sites – all Service Options .............................................................. 18
   6.1. Network-to-Network Interconnections (NNIs) ...................................................................................... 18

7. Service Features and Options ....................................................................................................................... 19
   7.1. Multicast ................................................................................................................................................ 19
   7.2. Features in Controlled Introduction (CI) ............................................................................................... 19
   7.3. Order and Change Orders for Features / Capabilities in CI ............................................................... 19
       7.3.1. T1 Frame Encap Ports in the US ...................................................................................................... 19

8. Features and Equipment with Possible Provisioning Exceptions .............................................................. 20
   8.1. IPv4 / IPV6 Dual Stack Addresses – Moving to Dual Stack from IPv4 Addressing ............................. 20

9. AT&T VPN – to – AT&T Private Network Transport Interoperability Feature ....................................... 20

10. Managed Router and Managed CSU-Probe Features / Options .............................................................. 21
   10.1. Managed Router Option ...................................................................................................................... 21
       10.1.2. Multicast ....................................................................................................................................... 21
       10.1.3. Use of Autonomous System Numbers (ASNs) ......................................................................... 21
       10.1.4. ISDN Backup Testing .................................................................................................................... 22
       10.1.5. Reporting Primary Ethernet Access Down in a Resiliency Scenario ........................................... 22
       10.1.6. AT&T Network Based IP VPN Remote Access (ANIRA) Failover to AT&T VPN Enablement ........ 22
       10.1.7. NetFlow v5 Enablement. .............................................................................................................. 23
AT&T VPN Customer Implementation Guide

AT&T Virtual Private Network Service (AT&T VPN) enables you the ability to build an application aware, network-based Multi-Protocol Label Switching (MPLS) virtual private network (VPN) to link all your locations, allowing you to efficiently and securely transmit all your applications such as voice, data, and video over a single connection.

1. AT&T VPN General Information

1.1. AT&T VPN Service Options (Types)

AT&T VPN offers 6 service options (types) with varying management capabilities for you to choose based on individual location requirements:

1. AT&T VPN with Customer Managed Router (aka transport only) — choose to supply and manage your own customer premises equipment (CPE). Note: MPLS DSL connections are a special variation on this service type — see option 2.
2. AT&T VPN with DSL access and Customer Managed Router — choose to have AT&T provide you with DSL access, which we install and provide ongoing hardware break/fix maintenance, while you still provide your own CPE.
3. AT&T VPN with AT&T-owned / AT&T Managed Router — choose to have AT&T supply and manage your CPE on their behalf. This type includes network management and monitoring, performance reports, trouble shooting, testing tools and maintenance of the router.
4. AT&T VPN with Customer-owned / AT&T Managed Router — choose to supply your own CPE, but have AT&T manage the CPE on your behalf. This type includes network management and monitoring, performance reports, trouble shooting, testing tools and maintenance of your router.
5. AT&T VPN with Managed CSU-Probe and Enhanced Reports — choose to have increased visibility into their network and Application performance. The CSU-Probe is owned and managed by AT&T.
6. AT&T VPN with AT&T Lite Managed Router — choose a less stringent fix interval if your CPE should suffer a hardware failure and does not require site to site performance SLAs. This option is currently only available for sites within the continental United States (US).

1.2. AT&T VPN Managed Router Option Exceptions

AT&T VPN Service offers a Managed Router option that AT&T configures, installs, manages, and maintains the service and router on your behalf 7-days-a-week, 24-hours-a-day.

You can choose to have an AT&T-Owned Router or to purchase the router yourself, per AT&T specifications, from a Cisco VAR (Value Added Reseller), or directly from Cisco. If you choose to provide your own equipment, AT&T provides you with an equipment order list (EOL) that you must utilize to order your equipment.

Within the US, you may choose a Lite Managed router option. If you choose this option, rather than replacement hardware being dispatched 24-hours-a-day, 7-days-a-week with an objective to be onsite including an AT&T technician within 4-hours, the replacement hardware is dispatched on an 8-hours-a-day, 5-days-a-week with next business day objective basis. Your LCON is expected to receipt replacement hardware and install same; which might include opening the router chassis and installing a replacement card or memory stick. This option is not permitted for external CSU-Probe
For US sites, an integrated internal CSU is required for all speeds and must be purchased in conjunction with your equipment for each site. For Managed Router sites in MOW, the integrated CSU is provided by the PTT for speeds up to and including T1/E1 (except within Canada). For speeds above T1/E1, an integrated CSU is included in the EOL that AT&T provides you and must be ordered at the same time as your AT&T-owned router.

The Managed CSU-Probe option offers an external device that enables AT&T to provide you with increased visibility into your network and applications. Within the US, you have the option to purchase the Managed CSU-Probe from AT&T. For speeds of T1 and NTx1 speeds the device also delivers the integrated CSU function that is required within your router.

Within the US, AT&T-owned and managed router with an internal CSU and the Managed CSU-Probe options may be ordered and implemented on the same site. Each option is ordered and provisioned separately and appears as separate line items on the invoice.

The standard average provisioning interval varies based on whether the geographic location, port type/access ordered.

1.3. AT&T VPN Managed CSU-Probe Option Exceptions

Managed CSU-Probe is available for sites in the US region, and where available outside of the US, with and without Enhanced Reporting and s supported with or without the Managed Router option. The Managed CSU-Probe CPE must be AT&T-provided, there is no option for customer ownership.

With Managed CSU-Probe you may expect 7-days-per-week, 24-hours-per-day proactive monitoring, ticketing, and resolution, similar to the AT&T VPN Managed Router feature.

You are responsible for procuring and connecting the cable between the installed Managed CSU-Probe and your customer-managed router. AT&T verifies connectivity up to the CSU-Probe demarcation (the CSU-Probe port supporting the customer-provided cable). A detailed list of cabling requirements and connectivity diagrams (AT&T VPN Managed CSU-Probe Connectivity Diagrams) are available for your use (if unable to utilize the link, please request a copy of the document from your account team). When the Managed CSU-Probe option is ordered and installed in conjunction with the Managed Router option, AT&T provides and installs these cables on your behalf.

For US sites supporting T1 or fractional T1 access, Managed CSU-Probe option delivers an external CSU, that is managed and monitored 7-days-a-week, 24-hours-a-day. An appropriate router interface module is required to support all available access rates.

Data Delivery and Latency SLAs are defined between CSU-Probe site pairs when AT&T is not managing the CE router. Jitter SLAs are not supported for Managed CSU-Probe sites.

Enhanced Reports are available for deployed Managed CSU-Probes only.

2. General Customer Responsibilities and Expectations (applies to all AT&T VPN service types)

2.1. Account Profile Set Up and Ordering of Service – all Service Types

Account Profile Set Up. Prior to placing your first order (after contract finalization), you must set up your AT&T VPN account profile, which is usually a one-time event and must be completed prior to orders being submitted. Delays in setting up your account profile may slightly extend the scheduled due dates for installation of your initial sites.
Order Form Completion and Submission. You will be requested, with the support of your account/support team, as needed, to complete your order form, as appropriate.

You will receive confirmation letters from AT&T during multiple steps in the order process. Please check the details of these letters for accuracy and immediately bring any discrepancies to our attention.

Any changes, especially those applicable to circuit specifications, site detail, address and/or room, or site contact detail, likely will result in significant delays to the due date of your installation.

Local On-Site Contact (LCON). When ordering service for each site you must provide us with the name and phone number, preferably a land line and cell, of a local on-site contact with whom AT&T or other access provider(s) may speak with regarding scheduling, building access, and problem resolution should the need arise. It is best to have a secondary contact as well in case the first site contact is not available. If your LCON changes, please ensure you contact your Order Specialist to update this information.

We recommend that your LCON comply with the following criteria to ensure a smooth installation and lifecycle support:

- Is located on-site and has two ways to be contacted – primary phone and cell
- Has access to the building and the exact site location for installation
- Is aware of any special access requirements (e.g., security clearance, access from only a certain door, only arrive after ‘x’-hour, etc.) and has the access granted
- Is familiar with the location where service is requested
- Has decision making power to address any requested service requirements
- Has authority to confirm the ready date for all your site requirements
- Communicates with the party who ordered service on scheduled due dates and test and turn-up
- Will, with the customer self-install Managed Router option, un-box the equipment, install equipment in rack, connect all cabling and work with DTAC (Data Test and Activation Center)
- Act as the eyes and ears on-site for problem determination purpose using the test and turn-up
- Will, with the Lite Managed Router option, receipt replacement hardware and install same on-site; which might include opening the router chassis and installing a replacement card or memory stick

2.2. AT&T VPN Access Arrangements

Sites within United States (US). You must obtain access between each installation site and an AT&T POP (Point of Presence on the AT&T network). You may contract for this access either from AT&T or from another service provider.

For Managed Router option, an internal channel service unit (CSU) is required. AT&T provides the CSU in the US and it is an additional additional router feature and billed as such or, if deployed in conjunction with the Managed CSU-Probe option, an external device may be utilized.

Sites in MOW (outside of the US). For sites outside of the US (designated within this document as Most-of-World (MOW) sites), access arrangements are provided by AT&T. For speeds up to T1/E1 an internal CSU is required. The CSU maybe included with the access (except for Canada), if not, you are responsible for ordering an appropriate CSU from the local access vendor. For Managed Router option, AT&T provides you with the required internal CSU. For speeds up to and including T1/E1 the CSU is included with the access (in Canada, a special request is required to be sent to the local access
provider to include the price of the CSU in the price of access). For speeds above T1/E1, the CSU is an additional router feature and billed as such.

The following limitations apply:

- Layer 2 PVCs (permanent virtual circuit) are not available.
- Access connection speeds for Frame Relay, ATM and Ethernet ports must be equal to the speed of the port to which the access connects.
- DSL access orders may fall out during the provisioning process due to the technical limitations of DSL; therefore, there should be a secondary access method pre-identified should the order be cancelled.
- An ‘Inside Move’ is a ‘Change Order’ request to move the current local channel access demarcation point from one room and/or floor to another is defined as a Site Level Move.
- An ‘Outside Move’ is defined as a Site Level move, where a ‘Change Order’ request to move the current local channel access to a local address where the local provider, technology, port type, port speed, POP, POP CLLI, City and Postal Code are not changing. Anytime a single circuit at a sight or the local provider, POP, POP CLLI, City and/or Postal Code changes, a disconnect order and new start order is required (Intra-city, intra-POP, intra postal code).

For additional information about Access, please see Section 4: Access and Access Site Requirements.

2.3. Provisioning of Service – all Service Types

Kick-Off Call. You and/or your LCON designate needs to participate in a kick-off call (also known as a technical assurance call) to verify the accuracy of all the order information for your sites. In the US, the AT&T Order Specialist, for MOW, the AT&T International Order Specialist, or for Managed Options, the AT&T Deployment Project Implementation Manager (DPIM), reviews the order for accuracy. During the initial kick off, AT&T confirms the site details with the appropriate site contact and validates the results with you during the call. (Note: DSL does not require a kick-off call for each site.)

Service-to-Service Interconnect (STSI) Orders. With your STSI order you will need to provide the Letter of Agency (LOA) number you received from the local exchange carrier (LEC) to your Order Specialist or DPIM, as appropriate. Not providing the LOA # for each site or an incorrect LOA # for that location may jeopardize your scheduled due date.

Service Scheduled Due Dates. After order issuance, an estimated due date is provided via an email confirmation. Ensure your LCON is prepared to participate in the test and turn up of the service on the scheduled due date.

Additionally, ensure your LCON provides timely access for each site installation, including for the access provider to install facilities and necessary equipment. You and/or your LCON will receive notification by e-mail of the installation schedule and any conflicts with this schedule should be resolved by contacting your Order Specialist. More than two failed dispatches will result in the automatic cancellation of an order.

Important Note. When ordering lower speeds, e.g., full and sub-rate T1.5, port and access for your AT&T VPN, AT&T is unable to issue requests with a due date more than 60-days past the future site readiness date, e.g., the customer requested due date (CRDD).

Delay of Scheduled Due Date. Notify your Order Specialist as soon as possible if, for any reason, prior to your scheduled due date, you determine that you will be unable to accept service on the scheduled due date. Customer requested/initiated delays in the turn up of service may result in the billing of monthly recurring charges prior to the physical installation of the service or cancellation of your order and/or cancellation charges.
For Managed sites, billing begins once AT&T completes test and turn-up and operational acceptance has occurred.

**Site (Facility and Equipment) Readiness.** If you are providing your own premises equipment, you should have your facilities ready for installation **no later than 15-days prior to the applicable scheduled due date**, and all of the premises equipment should be in place and **ready to operate 10-days prior to the applicable scheduled due date**.

Please contact your Order Specialist if you are experiencing difficulty installing your customer premises equipment. More than two failed dispatches result in the automatic cancellation of an order.

**Floor Space, Conduit and Electrical Power at Customer Site.** Please review the AT&T VPN Site Preparation Guide for each of your site(s) and:

- Confirm that installation sites have the necessary and appropriate equipment space, supporting structure, conduit and electrical power required to terminate service on-site to support the requested service; and
- Schedule your inside-wiring vendor to extend the DMARC prior to installation, if necessary.

**Please have the LCON and/or on-site personnel provide timely access** to each of your installation site(s) in order for the access provider to install facilities and necessary premises equipment. End-users receive notification by e-mail of the installation scheduled due date(s). Conflicts should be resolved by contacting your Order Specialist.

For additional information on site requirements and readiness, please see the AT&T VPN Site Preparation Guide.

**Test and Turn-up of Service for US and MOW Site(s).** In order to obtain service acceptance, your AT&T Order Specialist (the AT&T International Order Specialist for MOW Sites) will provide your LCON, via email, technical order details and a request to schedule the date and time for service test and turn-up.

The AT&T Order Specialist sets up a call, during the call, the LCON or your technical contact is required to be available to conduct ping testing of your premises router with AT&T, if required.

During the turn-up process, please note that circuits may not be available for viewing with the AT&T BusinessDirect® E-Maintenance on-line tool for up to 24-48 hours following the network activation date (NAD) completion. Please use the maintenance trouble reporting number provided by your account team if you encounter this problem.

AT&T requires you to participate in a hard loop back testing on the access for all IP port speeds. If the loop back testing on the access passes, AT&T will complete the end-to-end testing, including the port and we will notify you when the service is ready for use.

For Ethernet Access, your LCON is required to be available to ping test your router with AT&T if required.

For AT&T Telepresence Service, AT&T VPN personnel will participate in the test and turn-up of your AT&T Teleconference Service.

**For US sites:** Upon receipt of the e-mail request to schedule test and turn-up of your AT&T VPN Service for your sites within the continental 48 states, call +1-800-659- to schedule. For DSL
Access with your AT&T VPN Service in the US, please schedule your test and turn-up with the DSL Access Work Center located in the Alpharetta MPLS Center at +1-800-272-8262.

Once scheduled, your LCON at your site is sent an e-mail with the following information:
- Date scheduled for the test and turn-up
- Teleconference bridge number
- AT&T International Technician contact information

If you are located outside of the US and Canada and require assistance with test and turn-up of service for your US sites, you may utilize the AT&T USADirect® Country-specific Direct Dial Service (http://www.business.att.com/bt/dial_guide.jsp), To gain access to the AT&T network call the +1-800-659-8572 number.

For MOW Sites. Upon receipt of the e-mail request to schedule test and turn-up of your AT&T VPN Service for MOW sites, please call +1-800-659-8572 to schedule test and turn-up. Once scheduled, your LCON at your site is sent an e-mail with the following information:
- Date scheduled for the test and turn-up
- Teleconference bridge number to conduct test and turn-up
- AT&T International Technician contact information who will be working with you

2.3.1. Provisioning of Service – Managed Router and Managed CSU/Probe Options

In addition to the customer responsibilities outlined above, if you are implementing a Managed option, either the Managed Router or the Managed CSU/Probe, you are required to complete the responsibilities outlined below.

Site Surveys. You are responsible for performing a site survey prior to installation. AT&T provides a site survey requirements within your Welcome and Timeline Letter to your LCON. The LCON needs to complete the site survey information and return it to the AT&T site deployment manager (SDM) as identified within your Welcome Letter.

Adequate space, power, and air-conditioning should be available no later than 15-days prior to the applicable due date.

Site Readiness. Adequate space, power, and air conditioning for the Managed Router, facilities should be ready for service provisioning no later than 15-days prior to the applicable due date.

Customers electing the Customer-Owned / AT&T Managed Routers options are required to:
- Purchase a new router. Refurbished or reused routers are not supported. You must purchase a router that listed on the approved AT&T-supplied Equipment Order List (EOL). We support only the router manufacturer and type listed on the EOL under the Customer-Owned Router option.
- Deliver the router to AT&T warehouse address that we will provide to you. You are responsible for and shall bear all shipping costs, including any risk during shipment, associated with supplying AT&T with a customer-owned router.
- AT&T acceptance of the router delivered shall be at AT&T sole discretion and shall be based on compliance with the EOL requirements that (a) the router hardware/software configuration are consistent with the configuration on the EOL; and (b) the router passes an operational (power-up) test.
- You are solely responsible for remediation of any issues that result in a noncompliant router. You are responsible for communication of any requirements to the router manufacturer to remediate noncompliant configurations or operational failures. You are also solely
responsible and shall bear all costs (including shipping, packaging, etc.) associated with router return or remediation and shall bear all risk of loss during shipment of returned or remediated routers.

**Self-Installation.** In the US, if you are electing to self-install your managed router you need your LCON to ensure that the following additional tasks are performed:

- extend the inside wiring;
- unbox the equipment and install the equipment in the rack;
- connect all cabling; and
- work with the DTAC (Data Test and Activation Center) during the test and turn-up, assisting them as their on-site eyes and ears for problem determination purposes.

To assist with the self-installation a Site Deployment Package is included in the box of the CPE you received for your use, plus a step-by-step guide on assembling and installing the CPE is available at [http://planner.bus.att.com/AT&T VPN/](http://planner.bus.att.com/AT&T VPN/).

**Out of Band Access for Diagnostic Capability and MACDs.** Out of Band access to your AT&T VPN CPE is essential to providing you with the highest level of service. It is required for diagnosing troubles during lifecycle support of your service as well as to address your MACD requests.

Customer responsibilities include provision of an analog line (aka POTS – Plain Old Telephone Service). This customer-provided analog line allows AT&T to dial directly into the diagnostic modem which AT&T provides.

**Dedicated POTS Lines.** The preferred option is for a dedicated analog line to be provisioned. This allows us 24 x 7 access in the event we detect a trouble or need to complete a requested change to your service. If there is a problem during the evening for example, we can begin diagnostics and potentially correct the problem before business hours begin. The telephone number of this line should be provided in your site survey form feedback.

**Alternatives to a Dedicated Line.** If you cannot or choose not to obtain a dedicated line for Out-of-Band access, you may opt to provide a borrowed line instead. In this case you to inform us that the line will not be dedicated and provide the telephone number of the borrowed line. This approach does have drawbacks. We may not be able to start diagnostics and trouble resolution of an issue ahead of your call and we will not be able to perform requested changes to your service until you have connected the borrowed line and advised us that it is ready for use.

Additionally, there are impacts to your SLAs. The “clock” for purposes of assessing SLAs may not begin until the borrowed line is connected, you have advised us that it is ready for use and we have tested to verify it is working. If you choose this option, understand that it is your responsibility to contact us in the event of a trouble, to advise us that the line is connected and available for use. If your location is not staffed around the clock, we likely will not be able to start resolution efforts until someone is in the office to connect the borrowed line. The borrowed line will need to remain connected for the duration of the outage, so the phone or fax that normally uses that line would be unavailable until the trouble is resolved.

We mentioned that analog lines are also used for MACD activity. They are tested in advance of each MACD activity. If you elect to use a borrowed line it will need to remain connected for the test and duration of each MACD activity.
Sites with No Out of Band Access. If no analog line is made available for Out-of-Band access, then AT&T’s resulting inability to remotely access the router may require site visits for work that could otherwise be done remotely and delay diagnostics and trouble resolution. AT&T may charge a fee where a POTS line has not been provided and where additional site visits are required.

Unfortunately some MACD activities simply cannot be done safely without Out-of-Band access and AT&T would decline requests to make these changes without an analog line. Examples of changes in this category are changes to:

- ASN
- DLCI or VPI/VCI
- Local DLCI
- IP Address - Serial (WAN)
- VRF-LITE (aka MIAB or MPLS in a box)
- IOS

LAN Support. You are responsible for the following tasks:

- Cabling to connect your LAN (Local Area Network) equipment to the router (whether AT&T-provided or customer-provided).
- Cabling to connect your router to the AT&T VPN Managed CSU-Probe, if the feature is configured on the site.
- Configuring, cabling, installing and maintaining your LAN and providing necessary application software.
- Administering individual IP addresses on your LAN.
- Providing LANs that use the protocols AT&T supports.
- Notifying AT&T of any changes to your LAN configuration(s).

ISDN Resiliency Connections. You are responsible for ordering an ISDN connection from an ISDN service provider, for your Managed Router sites with ISDN back-up resiliency option. Service must be installed and ready for use prior to Managed Router installation. You are responsible for the ISDN charges, including connection and usage charges. AT&T separately provides the diagnostics and trouble shooting of ISDN and any associated charges for such service, as defined in your service contract, which are applied to your invoices.

Additionally, provisioning and maintaining inside wiring to extend the leased line and the ISDN connections from the DEMARC minimum point-of-penetration to the location in the building where the telephone jack is located that is used to set up the equipment should be completed with the installation of your ISDN connection. This includes any inside wiring extension which requires conduit, repeaters, equipment, core drilling between floors, or other special efforts to extend the leased line connection circuit.

Security Controls. Ensuring that your systems and networks (including outsourced and educational environments), that directly connect with those belonging to your AT&T VPN or that use the Common Services Network features, AT&T implements appropriate security controls, designed to prevent loss, disclosure, unauthorized access or service disruption, by restricting AT&T network access and its use to your authorized personnel only. Use of the AT&T Global Network and its facilities is intended for the contracting customer only and not for those who may be interconnected with your systems.
2.4. Trouble Resolution for Test and Turn – all Service Types

Service Troubles. Please contact your Order Specialist if you experience any trouble on the AT&T-provided service components within the first seven (7) business days after test and turn-up of service. After that period, if you experience faults on the AT&T provided components, contact the AT&T Help Desk. If you do not have the number, you may use the default AT&T VPN trouble reporting number (866-287-6288). The Service Assurance team will create a trouble ticket on your behalf and begin the isolation process on your behalf.

2.5. Invoicing – all Service Types

General Invoicing. Invoicing for each site shall commence as of the Service Activation Date, regardless of the function of the site in your network (e.g., hub, spoke, remote, or head-end sites) or the provisioning status of other sites in your network. Invoicing for individual AT&T VPN service components begin on the Service Activation Date for that individual service component, if different than the original Service Activation Date.

AT&T establishes one AT&T VPN account for all of your locations unless noted otherwise.

AT&T provides one invoice for each country, rendered in the currency specified in the schedule of charges. The Multiple Location Billing option is not available. Please see the AT&T VPN Service Guide for any exceptions by country.

Invoicing of Access. Monthly domestic US AT&T access charges are invoiced separately. Monthly international MOW charges for access and AT&T VPN service components are billed on the same statement. AT&T generally invoices for AT&T VPN MPLS Ports, Managed Router feature, and other optional features on the 1st of the month, and invoicing can be in arrears or in advance, depending upon your location. Please refer to your invoice for regional differences.

Additional Fees and Taxes. Domestic US AT&T access services charges include a Federal Universal Service Fund (FUSF) cost recovery fee to help cover charges from our data transport suppliers pursuant to state and federal telecom regulations. This fee is not a tax or government required charge. Other charges affecting monthly rates include applicable taxes, fees and surcharges.

AT&T BusinessDirect® Electronic Invoicing (eBill). Electronic invoicing options for AT&T VPN are available via AT&T BusinessDirect eBill (View, Analyze and Pay Your Bill).


Invoicing Variations. Differences may exist in invoicing cycles between the AT&T access invoice and the AT&T VPN invoice. This may create unexpected variances on your first few monthly invoices. For example, your first invoice may include charges for the initial partial month of service – beginning from service activation date to first invoice date - plus, charges for your first full-month of service charged in advance. These prorated charges may cause the monthly rate to look lower or higher than the actual contracted rate. These prorated charges should even out within the first couple of months of service, at which time the actual contracted rate is what you should see on your invoice.

Your agreement with AT&T contains important information you should review regarding processes and time frames for disputing billed charges.

Invoicing Changes: Once established, invoicing cycles cannot be changed or consolidated.
Invoicing Inquiries. For questions regarding invoices, please call the toll-free number that appears on your invoice.

2.6. Changes to Service and Disconnects: MACD Requests – all Service Types

Service Changes. Service changes for an AT&T VPN port speed upgrade (or downgrade) may result in an out-of-service condition while the work is being performed, please plan accordingly.

Service Disconnect. You may disconnect service component(s) by giving us at least 30-days prior written notice. Termination charges may apply as set forth in the AT&T VPN Service Guide. Recurring charges continue to apply for a period of up to 30-days from the date AT&T receives a disconnect order, or until the disconnect date specified in the disconnect order, whichever is later. You will need to provide access to AT&T personnel or their representatives, assisting us to retrieve the AT&T-owned equipment on your premises. If non-US access is terminated in less than one year, termination charges may apply.

At the end of the contract period, your AT&T Account team will notify you and initiate discussions on contract renewal with you. If the contract is not renewed, your AT&T VPN solution will continue under the current contract at your current rates and discounts. Your AT&T VPN contract is considered “Evergreen” and there is no automatic rerating.

2.7. AT&T BusinessDirect® - Network Reporting and Statistics

Performance Reports. To take full advantage of the AT&T VPN Performance Reports capabilities, you must contact the provisioning centers to complete the installation of each circuit. If this step is not taken for each circuit, the AT&T VPN Performance Reports will not reflect that circuit in the reports. The US Low Speed Service Delivery test and turn-up center can be reached at 800-659-8572 during business hours between 8:00 AM - 8:00 PM ET Monday - Friday.

Customers located outside of the US and Canada and require assistance for their US Sites may utilize the AT&T USA Direct® country-specific direct dial service, to gain access to the AT&T network to call the +1-800-659-8572 number.

AT&T BusinessDirect® Map. AT&T BusinessDirect® MAP function provides a topological view of your AT&T VPN for all service types.

3. General AT&T Responsibilities (applies to All AT&T VPN service options)

3.1. Provisioning of Service – all Service Types

Kick-Off Call: Your Account Executive/Order Specialist, or your DPIM for Managed Router options, may set up an initial kick-off call with your LCON (customer point-of-contact). (Note: If you have an alternate customer contact, please provide that information as soon as possible.)

During this initial call, AT&T reviews the customer responsibilities and AT&T responsibilities during the order entry and provisioning processes with you and/or your LCON and confirm your site details. (Note: DSL does not have a kickoff call for each site.)

Your Account Executive/Order Specialist contact is responsible for answering questions and providing status during the data gathering and implementation of your service.
For Managed Router and Managed CSU-Probe, the DPIM will review the site validations during this call.

**Notification of Significant Provisioning Developments.** You or your designated point of contact (LCON) will be contacted at set points throughout the implementation process with regard to touch points and provisioning timeframes throughout the provisioning process, including delivery due dates for service and test and turn-up notifications.

**Service Scheduled Due Dates.** After order issuance, AT&T sends a confirmation letter providing an estimated Due Date. The Negotiator Contact (NCON) and/or DPIM contacts you with your Scheduled Due Date and follows-up with a second confirmation letter approximately two days after the circuit is designed and AT&T has an Access Due Date from the access supplier. The time from order receipt to AT&T providing a firm Due Date is dependant upon multiple factors, but notification of firm Due Date is provided to you in a timely manner. AT&T will identify an AT&T contact who will provide further updates and additional information concerning order status to you.

**For MOW sites.** AT&T submits your order(s) to our in-country local Access providers and, within 10-15 business days of complete order receipt, AT&T will provide a firm due date to you. AT&T targets delivery of access 5-10 business days prior to your service due date, allowing for the local Access provider to complete any required work prior to your scheduled due date.

**Test and Turn-up of Service for US and MOW Site(s):** In order to obtain service acceptance, the AT&T Order Specialist (the AT&T International Order Specialist for MOW Sites) sends an email to your LCON, providing technical order details and a request to schedule the date and time for test and turn-up. The AT&T Order Specialist sets up a call with you, during the call, your LCON or designee is required to be available to conduct ping testing of the premises router with AT&T, if required.

AT&T targets Access delivery 5-10 business days prior to the scheduled service due date and begins testing no later than 3-5 business days prior to scheduled due date. The AT&T Order Specialist sends your LCON an email providing the technical order details and to schedule the date and time for test and turn-up.

**For US sites.**
- For access speeds of T1 and below – AT&T does auto loop back tests for T1 and below access (including NxT1).
- For low speed Frame Relay and ATM – AT&T’s standard process is to complete testing without contacting you, unless you indicate that you will not accept early turn-up of your service.
- For access speeds of T3 and above – AT&T requires that the Access circuits must be tested with you. The High Speed Service Delivery Center (HSSD) will contact you. If Access passes, AT&T does the end-to-end test of the service, including the port, typically without you.
- For speeds of T3 and above – AT&T requires that the day of service test and turn-up for T3 and above, to obtain service acceptance, your LCON should be available to test with AT&T if required.

**For MOW sites.**
- For Frame Relay, ATM and IP Ports – AT&T requires you to participate in hard loop back testing on the Access for all port speeds.
  - If the loop back testing on the Access passes, AT&T completes the end-to-end testing, including the port, without the your participation and notifies your that service is ready for use.
• For Ethernet ports – AT&T requires that on the day service test and turn-up for Ethernet, to obtain service acceptance, you are required to be available to ping test your router with AT&T.

3.1.1. Provisioning of Service – Managed Router and Managed CSU-Probe Options

Test and Turn-up. In addition to the AT&T responsibilities identified above in section 2.1 Test and Turn-up – for All Service Types, AT&T tests the premises router and initiates the router monitoring during the test and turn-up process. An AT&T Representative communicates to you the completion of these steps in order to complete test and turn-up of the Managed Router and/or The Managed CSU-Probe. If you have any questions during test and turn-up and its process, please contact your DPIM.

4. Access and Access Site Requirements

4.1. Ethernet Access and Customer Site Requirements

4.1.1. US Sites

Service Changes.

• Change Access Speed MACD for 1G/below only – Following vendors are supported: SBC, BellSouth, AT&T LNS, Verizon, Century Link (Includes Embarq), Cox, Fairpoint, Cincinnati Bell, Windstream, Time Warner, Level 3. Also AT&T Baseline arrangement, UVN is supported. All other vendors are not supported and require Disconnect/New Circuit Add order without IP address reuse.

• Delete Bi-direction Forwarding Detection (BFD) requires a coordinated disconnect between you and AT&T to avoid bringing down your interface on the AT&T end. Please contact your AT&T Account Executive for scheduling.

4.1.2. MOW Sites

Availability. Ethernet Access for MOW sites is in Controlled Introduction. Ethernet ports, Access, features and moves, ads and changes (MACDs) are subject to the availability of AT&T VPN Service Components and to individual approval and confirmation by AT&T.

Service Delivery Intervals. For access for all supported speeds: service deliveries Intervals follow standard process and timelines apply; intervals vary by country and supplier.

Ethernet limitations. The following limitations apply for Ethernet Access in MOW:

• Port speed must equal access speed
• Unilink, Multicast are not supported by all access providers
• Maximum Transmission Units (MTUs) higher than 1500 are not supported by all access providers

Service Changes. The following Moves, Adds, Cancels and Disconnect (MACD) service changes are available subject to individual approval and confirmation by AT&T:

• Change Port and / or VLAN Speed
4.1.3. Customer Site Requirements for Both US and MOW

AT&T strives to provide a smooth and successful installation experience for our customers. We do all that we can to ensure the project is completed on time and exceeds your expectations. Experience shows that customer site preparation issues are a frequent cause of major installation delays. Important requirements are summarized within an easy to use AT&T VPN Site Preparation Guide of site preparation work that needs to be completed according to the implementation project schedule to avoid the risk of delay. Close coordination and effective communication between your and AT&T is critical to ensuring the service is available when required.

AT&T will be placing the transport equipment necessary to deliver the requested services. An AT&T Network Services representative will provide the detailed application requirements for the equipment type in question at the time your site survey visit. The equipment types in question to deliver the requested services vary in many aspects and physical characteristics.

Please download a copy of the AT&T VPN Site Preparation Guide for your use to prepare your site for your AT&T VPN Service.

4.2. Digital Subscriber Line (DSL) – All Service Options

DSL Access Orders. Orders for DSL may require two visits to the your premises in order to first install the DSL Access and then install the AT&T-provided CPE. The MPLS DSL Access Connection includes the CPE but the CPE for MPLS ADSL Line Shared Connection must provided by the customer (i.e., you must install, configure and manage the CPE associated with the ADSL Line Shared Connection).

Feature Availability with DSL. MPLS DSL Access Connections are not available with the Unilink feature. Class of Service (CoS) on MPLS DSL Access Connections is available; however; CoS is only available on the DSU or customer-provided Cisco WIC CPE option and not on the customer edge router (CER). AT&T does not invoice for CoS on the MPLS DSL Access Connections since CoS markings may not be preserved over the DSL supplier’s network. DSL Access is not supported with the AT&T VPN Managed Router and Managed CSU-Probe features.

5. AT&T Network Suite

5.1. Wireless Back-up for Automatic Failover Feature

If you contracted for the AT&T Network Suite with AT&T VPN with Wireless Back-up for Automatic Failover, you should be aware of the following, which includes limitations of the feature:

- You must have a signed AT&T Network Suite contract.
- AT&T VPN circuit is always the primary circuit and the wireless back-up is always the back-up circuit. The feature cannot be used to back-up AT&T IP Flexible Reach Service and cannot be deployed behind a firewall.
  - If the primary AT&T VPN circuit fails, the Managed Router standard reports and the Managed CSU-Probe Enhanced Reports will not be able to support performance details during the primary circuit outage.
- Wireless Back-up is available within the AT&T Mobile service areas on the LTE/4G/3G network platforms.
- Wireless Back-up is constrained by speeds and availability and is limited to 10MB or below. It is not suitable for customer “hub” sites (data centers with servers, typically sending data).
• Service is limited by the available Mobility bandwidth which may vary by day and critical data should be preferred for failover mode.

• Border Gateway Protocol (BGP) routing and Static Routing are both supported on the AT&T AT&T VPN access link.
  o Bi-direction Forward Detection (BFD) is required on Ethernet Access links when static route is default routing protocol.

Wireless Back-up CPE. With Wireless Back-up feature included in your AT&T Network Suite, AT&T provides a VPN Gateway and separate Mobility USB modem for your use.

For the Wireless Back-up included in your AT&T Network Suite, you are provided with a VPN Gateway and separate Mobility USB modem, but auxiliary antennae’s to boost your signal are not included with the service. An AT&T Representative will install the AT&T-provided equipment at each of your sites and conduct a failover pretest to ensure service availability. The wireless signal strength is validated during install and may require the VPN Gateway to be moved to a different on-site location to obtain a better signal.

Below is the VRRP failover routing protocol configurations you need to use to in order to set-up your premises router(s) prior to service activation to support your Wireless Back-up.

Virtual Routing Redundancy Protocol (VRRP) Configurations. For the Wireless Backup feature included in your AT&T Network Suite, customers are responsible for setting the VRRP Configurations on their routers, unless AT&T manages your CER on your behalf. Below are the VRRP failover routing protocol configurations that are required to be set-up on the premises router prior to your service activation. For AT&T VPN Managed Option customers, VRRP failover configurations are completed prior to shipment of your CPE to your premises.

During service delivery and prior to service test and turn-up, an AT&T Representative will visit your site to install your VPN Gateway and Mobility USB modem and test Wireless Back-up and conduct a failover pretest.

VRRP Timer Settings. The AT&T VPN Gateway and the customer premises router (CER) default to a VRRP advertisement interval of one second, no action is required to define this setting within the router configuration.

VRRP Priority. VRRP Priority defines which device functions as the virtual router master that accepts traffic sent to the VRRP Virtual IP Address. The CER should be set as the active device with the highest VRRP Priority under normal operations. Upon loss of WAN connection, the CER VRRP Priority must be decremented to fall below the VRRP Priority configured for the AT&T VPN Gateway.

The CER VRRP Priority should be set to “250” (higher than any possible AT&T VPN Gateway device VRRP Priority Value) then decremented by “249” upon failure of the primary WAN link leaving the VRRP Priority of the CER at “1” (lower than any possible VPN Gateway device VRRP Priority Value).

VRRP Tracking. Commands. A Tracking Object is monitored by VRRP and Priority is decremented when the state of an object changes. In the example below the tracked object is named “track 1” and is defined as the status of the line protocol associated with the WAN Link for Serial access links.

The matrix below outlines additional access link options:
track 1 interface Serial0/1/0 line-protocol (see matrix below for all tracking options based on access type and routing being used)

interface FastEthernet0/0
  ip address 10.10.10.1 255.255.255.0
  vrrp 1 ip 10.10.10.3
  vrrp 1 preempt delay minimum 60
  vrrp 1 priority 250
  vrrp 1 track 1 decrement 249

router bgp 65001
neighbor xx.xx.xx.xx timers 15 45

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Access Routing</th>
<th>Static</th>
<th>BGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial (T1, etc)</td>
<td>VRRP tracks line-protocol</td>
<td>VRRP tracks ip-routing</td>
<td></td>
</tr>
<tr>
<td>Ethernet</td>
<td>BFD Required; VRRP tracks [BFD route]*</td>
<td>VRRP tracks ip-routing</td>
<td></td>
</tr>
</tbody>
</table>

*BFD route] could be the default (0.0.0.0 0.0.0.0) or other appropriate route installed by BFD – Static Route Support. “track 1 ip route 0.0.0.0 0.0.0.0” might be the appropriate VRRP track statement, but the existence of that object is installed by the BFD process --which is not defined here.

5.1. Billing for AT&T Network Suite Services
Billing for each service included with your AT&T Network Suite begins, on a per site basis, on the activation date or the day after the communicated overall due date for each service implemented.

5.2. Change Orders for AT&T Network Suite Services
For any change orders you may require for your services or features with your AT&T Network Suite, please utilize your account team must submit any and all change orders on your behalf.

6. International/Most of World (MOW) Sites – all Service Options

6.1. Network-to-Network Interconnections (NNIs)
In certain countries, service connections may be offered using a Network-to-Network Interconnection (NNI). NNIs may be used to extend the reach of the service to specific locations within a country where AT&T provides the service, but our reach is limited in-country, or to allow a customer location to access the service from a country where AT&T does not have an AT&T presence, but may utilize a partner’s network to extend reach to that country.
When an NNI is used, the service provider’s network edge may be either a network edge that routes private IP traffic only and does not route Internet traffic or a network edge that routes private IP and Internet traffic.

Certain features and/or SLAs may not be available when the service is accessed using an NNI. Where class of service (CoS) is available on an NNI, CoS mapping may or may not apply. Customer traffic carried on an NNI is mapped to the closest equivalent AT&T VPN CoS where mapping is available. Otherwise, if not available, traffic may not be routed consistent with CoS traffic prioritization over the NNI between the NNI provider and the AT&T VPN MPLS port.

7. Service Features and Options

7.1. Multicast

Requests to upgrade / downgrade or add / delete Multicast to an existing Logical Channel, you should be aware that when Multicast functionality is added or deleted the BGP session may drop between the CE and PE. The expectation should be that the connection will be down for approximately 20-60 seconds, if the BGP session is dropped and has to be re-established and routes relearned. Your AT&T Account Team should work closely with you to ensure that the Multicast enablement (or disablement) is scheduled during an appropriate maintenance window or if you are willing to accept the possibility of a momentary BGP hit if the change is made during normal business hours. For existing PPP/MLPPP/PoS connections terminated on the Cisco provider edge routers, adding/deleting Multicast to the connection should NOT result in a BGP hit.

7.2. Features in Controlled Introduction (CI)

Initially, all new AT&T VPN Service features are made available during a period of controlled introduction (CI). features in CI available for delivery to customers; AT&T simply uses a CI period to ensure or validate that the systems and operational processes used to provision and support the service meet the high standards customers expect from AT&T.

CI implications may be:

- The interval required to deliver the feature may be longer as compared to an equivalent generally available (GA) feature as various AT&T controls and checks are in place. In addition, unforeseen issues may be encountered during the provisioning process. We request your kind patience should these unfortunate circumstances occur.
- Some feature capabilities, e.g., the ability to do feature change orders, may not be available initially.
- No expedites requests for services are supported.

7.3. Order and Change Orders for Features / Capabilities in CI

Some AT&T VPN features are available in CI or on an individual case basis (ICB). This means that orders or groups of orders for those service components, features or capabilities are subject to individual confirmation by AT&T, and may be subject to certain limitations and may not be subject to some or all Service Level Agreements (SLAs).

7.3.1. T1 Frame Encap Ports in the US

The following MACD order types are neither supported nor currently planned for use with T1 Frame Encap Ports in the US: speed changes, inside or outside moves, Provisioning Access Arrangement changes, protocol change orders (PPP to/from Frame Encap), or any feature changes.
involving multicast, route groups, hub & spoke, and diversity (SDO/PDO). If you require such changes, you will have to place new port orders instead (disconnect / new site-port add).

8. Features and Equipment with Possible Provisioning Exceptions

8.1. IPv4 / IPV6 Dual Stack Addresses – Moving to Dual Stack from IPv4 Addressing

Change Requests. For you existing AT&T VPN IPv4-only ports which you would like to submit requests to upgrade to IPv4/IPv6 Dual Stack (Dual Stack) must:

1. Submit a new service order for the Dual Stack port.
2. Once the Dual Stack port is turned up, a disconnect order for the IPv4-only port must be issued and processed.

This change request may result in:

1. Billing for both the IPv4-only and Dual Stack ports during the transition.
2. Disconnect charge for the AT&T VPN IPv4-only port and/or access.
3. Non-recurring charges for the new Dual Stack port and/or access and/or applicable features.

EXCEPTION: AT&T offers a Change IP Address Handling MACD order that allows existing AT&T VPN IPv4-only IP port to transition to an AT&T VPN Dual Stack IP port. This MACD is available for existing customers with the Customer Managed Router (aka Transport) Service Type, for use with IP-to-IP ports within the US on the Cisco GSR32 provider edge router to the Juniper T640 platform. During test and turn-up, service testing should include base AT&T VPN Service PLUS any “Add on Services”.

Customer Premises Equipment (CPE) Requirements. If you supply your own equipment and would like to upgrade your ports from IPv4 addressing to Dual Stack, you must ensure that your equipment is Dual Stack capable, meaning that the devices are able to support both IPv4 and IPv6 address traffic in parallel. Dual Stack enabled CPE allows hosts to simultaneously reach IPv4 and IPv6 content, so it offers a very flexible coexistence strategy. CPE manufacturers will indicate which models, via their model number, support IPv4-only or Dual Stack. Ensuring CPE supports Dual Stack configurations is a pre-requisite prior to submitting the AT&T VPN IPv4 address to IPv4/IPv6 Dual Stack address Migration change request.

9. AT&T VPN – to – AT&T Private Network Transport Interoperability Feature

Interoperability between VPN Services. The AT&T VPN – AT&T MPLS Private Network Transport (PNT) Interoperability (“PNT Interoperability feature”) allows for sites with AT&T VPN service implemented and sites with AT&T PNT VPN service to be interconnected, to permit the AT&T VPN ports and MPLS PNT ports to interoperate and allow any-to-any communications between these sites.

The PNT Interoperability feature may not be compatible with all AT&T VPN features or capabilities or with all MPLS PNT features or capabilities.

SLAs for Interoped Sites. Service components interconnected using the PNT Interoperability feature qualifies for SLAs that are expressly applicable to the respective service. Implementation of the PNT Interoperability feature does not change the testing or measurement of performance obligations applicable to or reporting available for a service component. For example, and without limiting the forgoing, when AT&T VPN and MPLS PNT VPN sites are interconnected by the PNT Interoperability feature, the MPLS PNT port is not included in the measurement of the AT&T VPN MPLS Port-to-MPLS Port Latency and AT&T VPN MPLS Port Data Delivery SLAs, and a failure by AT&T to meet the performance objective for these SLAs shall not make the MPLS PNT ports eligible for service credits under the AT&T VPN SLAs. When making a claim for a service credit, follow the defined SLA credit request process applicable to the respective service for which the credit is to be claimed.
10. Managed Router and Managed CSU-Probe Features / Options

10.1. Managed Router Option


Managed Router feature offers you with read-only access (ROA) to the AT&T VPN Managed Routers via a SNMP community string. This allows access to select router management information bases (MIBs) via your network management system(s). The CER is access-list protected and limits SNMP access to no more than two customer network management servers. Overuse of SNMP access may place excessive demands on the CER’s processor or other service components, which may negatively affect performance of the service. AT&T is not liable for any SLA failures that are caused by your SNMP ROA activities.

10.1.2. Multicast

Consistent with all AT&T VPN Managed Routers implementations, AT&T tests and turns up the multicast configurations. However for AT&T VPN Managed Router implementations that includes Multicast, delivery intervals may be longer than standard unicast implementations. The Multicast feature is available only across other AT&T VPN Managed Router sites.

10.1.3. Use of Autonomous System Numbers (ASNs)

AT&T VPN with the Managed Router feature uses ASNs for network management any time Border Gateway Protocol (BGP) is used. AT&T requires that you provide AT&T with the ASNs that are to be used within your networks. The numbers could be public or private ASNs, as long as it doesn’t conflict with any of those that AT&T uses.

Use of the following ASNs will prevent AT&T from being able to manage your routers and should not be used:

- 65525
- 65526
- 65527
- 65315

If you are deploying the following services, in conjunction with your AT&T VPN (either Transport or Managed Router feature), should not use the following numbers:

- Network Based Firewall (NBFW): 65533, 65534
- AT&T Network Based IP Remote Access (ANIRA):
  - US: 65000
  - EMEA: 65001
  - AP: 65002
  - CA: 65003
  - LA: 65004

Note: ASNs 65000-65004 conflict with the ANIRA service. If this connection is to communicate directly with an ANIRA site, set ASN Override to Yes or contact your DNC/TSC for routing consultation.
10.1.4. ISDN Backup Testing

If you are deploying the ISDN backup feature, AT&T does performs an annual test, at no additional charge, ensuring that the ISDN backup connection is operating properly. The test lasts for approximately five (5) minutes in duration. This is an intrusive test that requires that the AT&T VPN connection to be disrupted so the ISDN backup connection can be initiated and diagnosed. You will incur ISDN utilization charges for the period of the test. This annual test will be scheduled in advance with you.

In addition, AT&T can perform a monthly test of the ISDN connection, if requested by you. The test lasts for approximately five (5) minutes in duration. This test is non-intrusive, and is provided at no additional charge. If you select this option, you will incur ISDN utilization charges for the period of the test. If you select this option, you may specify the time/date of this monthly test.

10.1.5. Reporting Primary Ethernet Access Down in a Resiliency Scenario

You must open a trouble ticket if the primary link goes down in a primary / backup Ethernet connection scenario. The systems will automatically fail the primary over to backup, but a trouble ticket will not be opened automatically. Once you open a ticket, it will be treated as a severity 1 trouble ticket and picked up by the help desk for resolution.

10.1.6. AT&T Network Based IP VPN Remote Access (ANIRA) Failover to AT&T VPN Enablement

If you order an AT&T Network-based IP VPN Remote Access (ANIRA) circuit as a backup for an AT&T VPN Managed Router, you should be aware of the following:

- Must have a signed ANIRA contract.
- AT&T VPN circuit is always the primary circuit and ANIRA is always the backup circuit.
- If the primary fails, the Managed Router standard reports and Managed CSU-Probe Enhanced Reports will not have performance details during the primary circuit outage.
- AT&T VPN and ANIRA circuits must be installed and turned-up, prior to requesting the failover configuration. An AT&T VPN Service MACD order must be submitted supplying the customer-provided static IP address and requesting configuration of VRRP on the AT&T VPN router at Service Interworking (SIW) solution site.
- AT&T is responsible for planning, coordinating and testing SIW solution on-site.
- Pre-identified LCON is required to be on site during SIW solution test and turn-up and participate in status calls with AT&T.
- Both AT&T VPN Managed router and ANIRA sites are billed once test and turn-up is completed. Failover configurations are ordered as a separate MACD after both the sites are up and running.
- You are responsible for all Internet connectivity issues and for any managing repair or failure of the third party ISP router and/or access.
- At sites using 3G wireless access, you are required to order wireless service and to configure the NetGate equipment. You are responsible for your interface to cellular carrier and shall be responsible to resolve any and all issues regarding the wireless service.
• You are responsible to configure the 3G-wireless connection in an “Always-on” mode to enable AT&T to proactively monitor 3G-wireless-enabled NetGate routers.

• You are responsible to configure the 3G-wireless connection in a “Dial as Primary 3G Cellular Connection” mode to enable AT&T to reactively monitor 3G-wireless-enabled NetGate routers.

10.1.7. NetFlow v5 Enablement

NetFlow Enablement. NetFlow v5 is a Cisco IOS application that provides statistics on packets flowing through the AT&T VPN Managed Router devices in the network. As an option for the AT&T VPN Managed Router feature, AT&T shall enable NetFlow v5 as specified by you. AT&T configures AT&T CPE, so that NetFlow statistics are sent to your NetFlow collection server.

NetFlow is supported:
• Only on ingress traffic. (NetFlow statistics are gathered only on traffic that is entering the router or ingress traffic.)
• On a single WAN port per router. It is not supported on a single router dual access configuration where NetFlow needs to be configured on both access links.

Class of Service (CoS). NetFlow traffic bypasses the COS (class of service) feature implemented for the AT&T VPN Managed Router. As such, AT&T has no control of the NetFlow traffic and no ability to prioritize voice and data traffic higher than NetFlow traffic. Therefore, NetFlow traffic will always take precedence over voice and data traffic during periods of network congestion.

Network Performance. NetFlow traffic may adversely impact the network performance, available bandwidth, and router utilization. AT&T reserves the right to disable NetFlow if it is determined that NetFlow is the cause of network performance problems.

Customer Responsibilities:
• You must provide and support NetFlow Collection Server(s) and devices using network management data and supply AT&T with information on your NetFlow collection server(s) as necessary for AT&T to enable NetFlow on AT&T VPN Managed Routers.
• You are responsible for the collection, analysis and formatting of all NetFlow data
• If your CPE / router must be upgraded to support NetFlow (e.g., configured with additional memory), you are expected to purchase the additional hardware required.

10.1.8. 4G/LTE Mobility – Primary and Failover Access

Mobility Backup and Failover. If you have selected either the 4G/LTE wireless backup/failover option or the wireless primary access option, you must ensure that adequate wireless signal strength exists at the location the managed router is to be placed by utilizing your mobile device as an option. Building structures and equipment racks can create wireless interference which can impact signal strength. Adequate wireless signal strength is defined less than -90dB RSSI (Received Signal Strength Indicator) when measured with LTE capable device connected to the AT&T Global Network.

To convert the bubbles/bars on an AT&T iPhone to an RSSI reading: dial *3001#12345#* and press call. This call will not permanently change the signal strength reading on the phone to an RSSI number. RSSI conversion instructions for additional vendor devices are available from the manufacturer or via an internet search. There are also apps available for phones that can be used to provide the RSSI readings.
Adequate wireless signal strength at a site must be confirmed on your Site Survey form that must be submitted to AT&T prior to test and turn-up your site. In addition, ensure the RSSI reading at the site is recorded on the Site Survey form.

AT&T supplies two 10’ coaxial cables with antenna extensions with each wireless router to provide some flexibility in antenna positioning and to improve signal strength.

Note: for optimal LTE signal receptions, the two LTE antenna should be positioned 17 inches apart. Therefore, you should always use the cables provided to position the antenna 17 inches apart, as opposed to attaching the antenna directly to the antenna connections on the router itself. An AT&T Representative will install the AT&T-provided equipment at each of your sites and conduct a wireless connectivity test as part of the test and turn-up process. They can assist with wireless antenna positioning.

The Site Survey form also asks you to indicate how you would like AT&T to proceed with the installation if we determine that inadequate wireless signal strength exists during test and turn-up. There are two options:

1. Proceed with installation and turn up wireline connection only (the option only applies to primary/backup or failover arrangements); or
2. Cancel the entire installation.

Note: you will need to notify your AT&T account team to submit the change order to remove the wireless failover portion of your order (option #1) or to cancel the installation altogether (option # 2), depending upon which option you prefer.

You will need to supply the private IP addresses to be used for the wireless interface on each wireless router. These addresses will be assigned dynamically to each wireless device from the address range supplied (/30 – 30 addresses, minimum). Note: the AT&T Mobility network only supports IPv4 addressing at this time.

You must also identify two IP addresses as Multipoint GRE (mGRE) tunnel termination sites in your network. These two sites must be AVPN wireline sites (TDM or Ethernet) and can not utilize the wireless failover feature.

10.2. Dual Router, Single Access (Warm Standby) Resiliency Option

If you selected this resiliency arrangement, you must connect the standby/backup Managed Router to the primary Managed Router at a site via a dedicated cross-over Ethernet cable. If the primary AVPN Managed Router fails, you are also responsible for physically moving the wide area networking (WAN) connection and the local area networking (LAN) connection from the primary Managed Router to the standby Managed router. AT&T will dispatch a technician to repair the primary Managed Router, and once repaired, will return the primary Managed Router to service and disable the standby Managed Router.

10.3. Managed CSU-Probe

10.3.1. Enhanced Reporting

Your first site order for Enhanced Reports will initiate a one-time activity related to AT&T BusinessDirect® Portal Registration. You are expected to provide your Company Administrator
User Name, for which the Enhanced Reports will be enabled. Additional users may be added to AT&T BusinessDirect® by your Company Administrator.

10.4. Managed Router and Managed CSU-Probe

10.4.1. Basic Inside Wiring Extension for US Sites
Inside Wiring within the US, except for Alaska, Hawaii and US Territories, is provided under certain provisions. Please refer to section 5.3.5 Basic Inside Wire Feature in your AT&T VPN Service Guide (http://serviceguidenew.att.com) for full details on what is provided.

10.4.2. Basic Inside Wiring Extension for MOW Sites
Inside Wiring outside of the US is not standard with AT&T VPN, but may be available on an individual case basis (ICB) depending on the country. Requests for support require custom review and approval, which your Account Team can assist you with this process.

10.4.3. Disconnects
Managed Router Option. With the AT&T-Owned/AT&T-Managed option, the Managed Router is owned by AT&T and is made available to customers for use as part of AT&T VPN Service. Upon termination of the service or de-installation of any site, you are required to make the AT&T CPE at such site available for removal by AT&T or a third-party as designated by AT&T and return it in the same condition as originally installed, ordinary wear or tear excepted, or your shall be responsible to pay for restoration of the AT&T CPE to such condition.

With the Customer-owned/AT&T-Managed option, customers purchase the Managed Router that is used as part of AT&T VPN Service. Upon termination of the service or de-installation of any site, your shall make the Customer-Owned/AT&T Managed CPE at such site available to AT&T to allow AT&T to remove confidential AT&T Information from the router configuration.

Managed CSU-Probe. The Managed CSU-Probe is owned by AT&T and is made available to customers for use as part of AT&T VPN Service. Upon termination of the service or de-installation of any site, you are required to make the AT&T CPE at such site available for removal by AT&T or a third-party as designated by AT&T and return it in the same condition as originally installed, ordinary wear or tear excepted, or the you shall be responsible to pay for restoration of the AT&T CPE to such condition.

11. Service Testing, Maintenance and Repair – All Service Options

11.1. AT&T VPN Service Testing, Maintenance and Repair
Maintenance and Repair. AT&T typically remotely tests and maintains service for AT&T provisioned facilities only. In the event that AT&T determines that its service is functional, you will perform trouble shooting on facilities not provided by AT&T. If AT&T dispatches repair resources to your site at your request to perform testing or repairs in connection with a reported trouble, and testing discloses that the AT&T service is working correctly, then an additional charge may apply.

AT&T also remotely tests and maintains service for AT&T Managed Customer Provided Routers. In the event that AT&T determines that the trouble is on the customer rovided equipment and AT&T Managed Router feature is not responding to the diagnostics, AT&T will perform trouble shooting. If the source of the problem is with the router, AT&T dispatches repair resources to your site to perform
testing or repairs in connection with the reported trouble. This service is included in the charges of the AT&T VPN Managed Router service.

11.2. AT&T VPN Service Availability and Maintenance

Service Availability and Maintenance. The AT&T Global Network is generally available 24-hours-a-day, 7-days-a-week, 365-days-a-year, except for possible outages during scheduled maintenance. AT&T utilizes the scheduled maintenance windows to upgrade equipment, software, and facilities which may add capacity, new features, resiliency and which may provide fixes to known problems to help ensure high network performance. The scheduled maintenance windows are typically used to maintain many backbone sites. Customer outages, if they occur, should be significantly less than the duration of the scheduled window.

Scheduled maintenance times are:

<table>
<thead>
<tr>
<th>WINDOW</th>
<th>LOCAL ROUTER TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Middle East</td>
</tr>
<tr>
<td></td>
<td>Friday</td>
</tr>
<tr>
<td>Weekly</td>
<td>Start</td>
</tr>
<tr>
<td></td>
<td>End</td>
</tr>
<tr>
<td>Monthly 8 Hour Extended Windows</td>
<td>Start</td>
</tr>
<tr>
<td></td>
<td>End</td>
</tr>
</tbody>
</table>

Latin America, USA and Canada maintenance times are in EST
Europe, Middle East and Africa maintenance times are in CET
Asia Pacific maintenance times are in JST
Middle East (Qatar, Saudi, Egypt) maintenance times are in UAE – The window is on the Friday before date noted.

PLEASE NOTE:
- The new Middle East region includes Qatar, UAE, Saudi and Egypt. (Israel remains in the CET timeframe)
- Both IFR and IATM Network Maintenance could potentially impact IFR/IATM service interworking customers.

*If the 2nd or 3rd Sunday of the month falls on a holiday or other special day, AT&T may reschedule the monthly maintenance window.

Below is the AT&T 2016 AT&T Virtual Private Network Service Network Maintenance Windows schedule.
When possible, you may receive an initial notification of this schedule, with a follow-up notification sent approximately three to four weeks prior to each window stating if there will be an impact to your network.

### 2016 NETWORK MAINTENANCE WINDOWS

<table>
<thead>
<tr>
<th>January 10</th>
<th>May 15</th>
<th>September 18</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 24</td>
<td>May 22</td>
<td>September 25</td>
</tr>
<tr>
<td>February 14</td>
<td>June 12</td>
<td>October 9</td>
</tr>
<tr>
<td>February 28</td>
<td>June 26</td>
<td>October 16</td>
</tr>
<tr>
<td>March 13</td>
<td>July 10</td>
<td>November 6</td>
</tr>
<tr>
<td>March 20</td>
<td>July 31</td>
<td>November 13</td>
</tr>
<tr>
<td>April 10</td>
<td>August 14</td>
<td></td>
</tr>
<tr>
<td>April 17</td>
<td>August 28</td>
<td></td>
</tr>
</tbody>
</table>

**PLEASE NOTE:**
Circumstances may require a modification to any of the above scheduled dates and times. There may also be additional dates added to ensure that the quality of service is continually upgraded and maintained. All changes to the planned dates or times will be provided as early as possible to ensure you have advanced timely notification.

These maintenance activities are necessary to help us provide the latest in communications technology and the highest quality service.

**Extended Maintenance Windows**
AT&T may perform extended maintenance up to four times per year, and AT&T may need to schedule planned maintenance at other times due to, for example, government inspections or power maintenance. AT&T will use reasonable efforts to give Customers at least 30-days notice of such scheduled or extended maintenance. However, AT&T reserves the right to perform maintenance at any time in order to maintain the network.

**Customer Maintenance Window**
In addition to the standard non-flexible Maintenance Windows as the customer you can select additional change slots on the condition that it only impacts your own resources. These change slots must be agreed via your AT&T Account Team or GCSC management region in an effort to resolve an on-going problem. Please use the InfoWeb tool to document scheduled site outages.

**Emergency Changes**
Although all maintenance is planned to take place during the Maintenance Windows, due to unforeseen circumstances it may be necessary to change the production environment outside the maintenance windows. When this interrupts the service, AT&T will inform affected customer(s).

The above refers to changes initiated by AT&T. If there are planned changes in your environment which may affect the service, or for which AT&T’s assistance is required, you should contact your AT&T Business Solutions Account Team for a MACD (move, add, change, or delete) to be processed.
11.3.  AT&T Lifecycle Support Information and Contact Numbers – All Service Options / Types

To report any troubles and receive status on submitted troubles, please use AT&T Express Ticketing available on www.att.com. You may also report any troubles or get ticket status and history via the AT&T BusinessDirect® Portal using the ticketing system.

If you require immediate assistance or would like to speak with the helpdesk, please utilize the number identified below.

11.3.1.  AT&T VPN Global Customer Service Center for all Regions – All Service Options / Types

AT&T VPN customers may call the AT&T VPN Customer Support Centers at 1-866-AVPN-ATT or 1-866-287-6288 within the continental US. If you are calling from outside the US, please call +1-770-750-7572 and:

1. Choose option 1 to report problems related to AT&T VPN Transport sites.
2. Choose Option 2 to report problems related to AT&T VPN Managed Router sites (with or without Managed CSU-Probe)
3. Choose Option 3 to report problems related to standalone AT&T VPN Managed CSU-Probe sites.

You may also receive status on open tickets by utilizing the call information above. You will be directed to whether you are opening a new trouble ticket or status on an existing ticket.

You may also reach the AT&T VPN Transport Maintenance Center by calling 877-ATT-FIXX (877-288-3499) and selecting Option 2 from within US. If you are calling from outside US, you can call the US direct by dialing the country access code. Specific country access code information may found at the following websites: http://www.usa.att.com/traveler/index.jsp or www.att.com/business_traveler.

11.3.2.  International Regional Helpdesks – All Service Options / Types

If you are outside of the US and would prefer to speak to an in-region helpdesk or require in-language assistance, you may call the AT&T Worldwide Customer Support Center for all service options / types via the appropriate regional telephone numbers or toll-free numbers (as available):

<table>
<thead>
<tr>
<th>Calling from Region</th>
<th>Dial the number</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific</td>
<td>1-888-910-7550</td>
<td>New ticket creation: choose prompt #1</td>
</tr>
<tr>
<td></td>
<td>800-2255-4288 or +44 15 27 51 3 950</td>
<td>Status on existing ticket: choose prompt #2</td>
</tr>
<tr>
<td></td>
<td>Use prompt #4 for APAC region, then</td>
<td>In Language: please listen for prompt</td>
</tr>
<tr>
<td>Europe, Middle East and Africa (EMEA)</td>
<td>1-888-910-7550</td>
<td>New ticket creation: choose prompt #1</td>
</tr>
<tr>
<td></td>
<td>800-2255-4288 or +44 15 27 51 3 950</td>
<td>Status on existing ticket: choose prompt #2</td>
</tr>
</tbody>
</table>
Managed Service Options – Global Customer Support Center. The Global Customer Support Center (GCSC) provides post-installation support for Customers deploying the Managed Router feature. The GCSC, as part of the service, proactively diagnoses the network for predefined failures. These thresholds are set by AT&T across all customers and are not customizable. AT&T does not diagnose network performance against customer defined criteria and does not provide analytical or consultative support regarding their network design. For customers looking for additional consultative support, a broad array of professional services is available under separate agreement.

In the occurrence of failure, a ticket is raised and a GCSC representative will contact Customer to notify them that there is an issue and it is being handled. Incidents are defined as unusual events that affect AT&T service delivery. In some cases the incident may not be detected by AT&T systems, therefore, the GCSC also supports customer trouble reports.

### 11.3.3. Problem Severity Code Definitions

The Customer defines the severity of a problem when the call is placed. The following definitions are provided as guidance to assist the Customer to appropriately assign the severity of a problem.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical problem that stops Customer from functioning. The network, service or product is unusable and Customer is completely out of service.</td>
</tr>
<tr>
<td>2</td>
<td>Major problem with severe impact on Customer business, but does not stop it from functioning. The network, service or product is interrupted or severely degraded and Customer is not able to work at expected levels of performance and productivity. Also used for Severity 1 problems with a 100% bypass but awaiting final resolution.</td>
</tr>
<tr>
<td>3</td>
<td>Minor problem that does not seriously affect service or network availability or functionality used in Customer business.</td>
</tr>
<tr>
<td>4</td>
<td>No problem. Customer business is not impacted. There is no significant impact to the user. Incident may be a request for service information or a suggestion</td>
</tr>
</tbody>
</table>

### 11.3.4. Mean time to Repair Objectives – Managed Router / Managed CSU-Probe

Mean time to repair objectives is as follows:

- 4 hours for failures that do not require technician dispatch
- 8 hours for failures requiring technician dispatch
\textbf{Note 1}: Actual restoration of an AT&T VPN Managed Router failure that requires technician dispatch will vary based on availability of parts, labor, and customer's location within the country.

\textbf{Note 2}: Actual restoration of an AT&T VPN Managed CSU-Probe failure that requires technician dispatch will vary based on availability of parts, labor, and customer's location within the country.

If customer has a Lite Managed Router feature these intervals do not apply when a failure requires replacement hardware dispatch.

11.3.5. \textbf{Maintenance for Sites in China – Managed Router / Managed CSU-Probe}

Onsite maintenance repair and restoration within 12-hours is not available for all in-country locations. Locations outside the cities listed below, Shanghai Symphony Telecommunications Co. Ltd (SST) will deploy an engineer with spare parts to the customer site, offering Next Business Day or Best Effort commitment, dependent upon the customer location.

\textbf{City List}: Beijing, Shanghai, Guangzhou, Chengdu, Suzhou, TaiCang, KunShan, JiaXin, JiaShan, Hangzhou, Zhongshan, Shenzhen, ZhuHai, FoShan, SheKou, DongGuan, Tianjin, Zhang JiaKou, Changzhou, Wuxi, Nanjing, Ningbo, Shantou, ShanWei, Huizhou, ChengDe, Chongqing.

12. \textbf{References and Resources}

AT&T VPN Service documents authored by the AT&T Network Design & Consulting Division are available on AT&T BusinessDirect® under Insight & News /Tech Specs. These guides are also available for distribution to customers who have signed a contract with AT&T. \textit{The current topic list includes}:

- \textbf{AT&T VPN Service Customer Router Configuration Guide}
  This guide assists AT&T you with the configuration of your edge routers connecting to AT&T VPN.

- \textbf{AT&T VPN Service Customer Migration Guide}
  This guide outlines a set of technical steps for migrating from traditional frame relay, ATM or private line to the AT&T VPN. This guide is applicable to AT&T VPN without managed options sites only.

- \textbf{AT&T Network Based Class of Service Features Configuration Guide}
  This guide assists your in understanding and using the network-based CoS features of AT&T IP services. This guide is applicable to both Transport and Managed sites.

- \textbf{AT&T MPLS Service Multicast Customer Configuration Guide}
  This guide assists you in the configuration of your multicast-enabled edge routers connecting to AT&T VPN. This guide is applicable to AT&T VPN without managed options sites only.

- \textbf{AT&T VPN Ethernet Access Customer Router Configuration Guide}
  This guide assists you in the configuration of your routers connecting to AT&T VPN with Ethernet access. This document focuses on customer managed routers.