SR16710480 ##14944EH79##

Service Request

Interface Security
170 Chastain Meadows Ct
Kennesaw, GA 30144

CTN3102777 SR16710480 Rev 0

ISS Helpdesk #: 800.554.9875 op 1, 1

SR Type: Circuit Upgrade (VTK TTU) Dispatch Type: (IN)

Reference Number: GS7738 End User Reference: I0473024

Date: 06/15/2021 Window: 10:00 to 10:00 EDT Expected Duration: 192 PO#: ISS_503996

Site Contact: MOD Phone: (973) 777-1303 Alt. Phone:
Company: GAMESTOP - 7738-GS7738, Address: 18 LEXINGTON AVE 18 LEXINGTON AVE
City: PASSAIC State: NJ Zip: 07055

TAC: 404.536.4721 (AT&T) | 678.332.8358 (Verizon) | 678.460.2530 (Other)

SR DETAILS

DESCRIPTION OF WORK

Circuit Upgrade (VTK TTU): Call TAC for Details

SR CHECKLIST

1. Upon arrival, log on with Genesis (via myESP or calling +1.800.493.0016).
2. Refer to the attached install guide for specific installation instructions.
3. Contact the appropriate customer helpdesk by chat or phone.
4. Verify all installation areas are clean and that you properly dispose of all trash.
5. Submit deliverables via myESP.
6. If any deliverables or the signed SR are still outstanding, submit via myESP or ESP within 24 hours.

To be completed by the Field Engineer (FE): 43398

Call Result: [ ] Successful [ ] Incomplete

Incomplete Reason:

Materials Used:

Description	Qty

Required for all calls:

Time at Log-on: _____:_____ EDT

Time at Log-off: _____:_____ EDT

Customer Heldesk Rep. Name: _____

Customer Call Closure Code: _____

Onepath TAC Rep. Name: _____

Onepath TAC Closure Code: _____

Installed Equipment:

Make/Model	Serial Number

RMA Equipment:

Make/Model	Serial Number

FE Initials	End-User Name (Please Print)	Title	End-User Signature	Date

SR16710480 ##14944EH79##

Description: Arrive onsite prepared to upgrade the existing broadband circuit with a new service. Locate the new broadband modem and verify sync and surf. Reconfigure the Starbox with the new IP scheme, connect the new modem and verify all services are operational with ISS TTU and the MOD.
Required Tools: Standard Telco + MyESP app (recommended but not required)
Required Materials: Standard Telco (which includes at least 200ft of cat5 and multiple RJ11/RJ45 jacks)
Required Skills: Telecom & Networking
RMA Handling: Look at the SR details section of your SR. If an RMA is required, the field RMA Required? will be set to yes. The RMA Equipment Make/Model field will indicate the equipment that needs to be boxed up. After successfully completing the upgrade, record the make/model/serial number of the device being returned and box up for call tag return. Take a photo of the RMA device in the box before sealing and submit via myESP. Explain the process to the MOD and alert TAC at closure of the RMA.
FE Overage Threshold: 3 hours
Last Guide Version: 02/14/2018 00:00

Notes:: bring store up on temp 4G,

Equipment:

March 11, 2021

Re: COVID 19 - City/County/State/Federal Orders

To whom it may concern:

Please be informed that the bearer of this letter is subcontracted by Genesis Networks, a communications and information technology company providing essential critical infrastructure as outlined by the Cybersecurity and Infrastructure Security Agency (CISA); an agency operating under the Department of Homeland Security.

Under CISA guidelines, these workers must be able to travel to and gain access to infrastructure facilities and offices during curfews and restricted travel periods. CISA identifies the following list as essential to continued critical infrastructure:

Communications:

• Maintenance of communications infrastructure- including privately owned and maintained communication systems- supported by technicians, operators, call-centers, wireline and wireless providers, cable service providers, satellite operations, undersea cable landing stations, Internet Exchange Points, and manufacturers and distributors of communications equipment

• Workers who support radio, television, and media service, including, but not limited to front line news reporters, studio, and technicians for newsgathering and reporting

• Workers at Independent System Operators and Regional Transmission Organizations, and Network Operations staff, engineers and/or technicians to manage the network or operate facilities

• Engineers, technicians and associated personnel responsible for infrastructure construction and restoration, including contractors for construction and engineering of fiber optic cables

• Installation, maintenance and repair technicians that establish, support or repair service as needed

• Central office personnel to maintain and operate central office, data centers, and other network office facilities

• Customer service and support staff, including managed and professional services as well as remote providers of support to transitioning employees to set up and maintain home offices, who interface with customers to manage or support service environments and security issues, including payroll, billing, fraud, and troubleshooting

• Dispatchers involved with service repair and restoration

Information Technology:

• Workers who support command centers, including, but not limited to Network Operations Command Center, Broadcast Operations Control Center and Security Operations Command Center

• Data center operators, including system administrators, HVAC & electrical engineers, security personnel, IT managers, data transfer solutions engineers, software and hardware engineers, and database administrators

• Client service centers, field engineers, and other technicians supporting critical infrastructure, as well as manufacturers and supply chain vendors that provide hardware and software, and information technology equipment (to include microelectronics and semiconductors) for critical infrastructure

• Workers responding to cyber incidents involving critical infrastructure, including medical facilities, SLTT governments and federal facilities, energy and utilities, and banks and financial institutions, and other critical infrastructure categories and personnel

• Workers supporting the provision of essential global, national and local infrastructure for computing services (incl. cloud computing services), business infrastructure, web-based services, and critical manufacturing

• Workers supporting communications systems and information technology used by law enforcement, public safety, medical, energy and other critical industries

• Support required for continuity of services, including janitorial/cleaning personnel

All persons performing critical operations have been instructed to comply with hygiene and social distancing requirements as established by the Centers for Disease Control and Prevention.

Please do not hesitate to contact me should you have any questions regarding this letter or our operations.

Sincerely,

Bryan Hann

Area Vice President – Deployed Services, Genesis Networks

1354 N. Loop 1604 E., Suite 103 | San Antonio, TX 78232 | 210.489.6600

Cybersecurity & Infrastructure Security Agency
Washington, DC 20528

May 27, 2020

To Whom It May Concern:

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issues this letter to facilitate work in the interest of homeland security by Communications Sector workers identified in the CISA Essential Critical Infrastructure Workers advisory guidance, dated May 19, 2020.[1] CISA requests any courtesy that can be extended to essential workers involved in communications infrastructure operations, maintenance and restoration **in response to the COVID-19 Pandemic and any other regional disasters (e.g., hurricanes, tornadoes, wildfires, earthquakes) that may occur during any COVID-19 response phase**.

CISA developed the **Essential Critical Infrastructure Workers** advisory guidance identifying workers that conduct a range of operations and services deemed essential to continued critical infrastructure viability. This list is intended to support State, local, tribal, and territorial officials' decision-making as they work to protect their communities, while ensuring continuity of functions critical to public health and safety, as well as economic and national security.

In developing this advisory guidance, CISA determined that essential workers need access to jobsites based on our judgment that organizations affiliated with the Communications Sector engage in activity that could reasonably be included within the scope of "critical infrastructure" as that term is defined in law; and critical communications infrastructure is necessary to ensure first responder, emergency responder, and 911 communications capabilities are functional during this response and recovery period. In the course of providing this support, identified Essential Critical Infrastructure Workers in the Communications Sector should be able to travel to and access necessary critical infrastructure facilities in order to prevent loss of service or restore critical communications services.

CISA greatly appreciates your cooperation. For any questions or concerns related to this request, please contact the CISA at 888-282-0870 or CISAservicedesk@cisa.dhs.gov.

Sincerely,

Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency (CISA)

[1] "Guidance on the Essential Critical Infrastructure Workforce," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/publication/guidance-essential-critical-infrastructure-workforce.

Field Engineer- Please Read

Covid-19 Procedures and PPE Requirements

As the US starts to re-open, many customers have asked that Field Engineers agree to certain safety requirements as a condition for scheduling installations or break-fix visits. The requirements are summarized below:

1. Field Engineers are **required to wear face coverings and gloves at all times** when entering, working in, or exiting stores.
    a. This can include any of the following based on CDC guidelines: **reusable or disposable masks**.
    b. https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/diy-cloth-face-coverings.html

2. Field Engineers are **required to maintain social distancing** while in stores and follow all posted instructions for customer queuing/metering.

3. **CALL TAC IF THIS APPLIES BEFORE GOING TO SITE**: Field Engineers should refrain from visiting locations if they have a fever of 100.4 F (37.94 C) or higher, or have exhibited any symptoms of COVID-19 within 14 days of the scheduled visit, (ex: fever, cough, shortness of breath or difficulty breathing, chills, repeated shaking with chills, muscle pain, headache, sore throat, new loss of taste or smell).
    a. Or if in the last 14 days, they have been out of the country, traveled by plane/cruise ship or been to areas known to have high concentrations of COVID-19 infections, or been in close contact with a person(s) with a positive or presumed positive COVID-19 case.

4. If a Field Engineer is diagnosed with COVID-19 or shown symptoms of COVID-19 within 2 weeks of visiting a store, **inform TAC of the diagnosis**.

ATTENTION TECHNICIAN

This dispatch has special contact information that is not reflected in the guide. Please follow the below instructions to contact ISS for circuit upgrade and testing.

To complete circuit upgrade testing Call:

Interface Circuit TTU

800.554.9875 opt 1,1

Alarm system confirmation after upgrade:

Interface “Chat”

www.interfacesys.com/technicians

If you have any questions, please contact Onepath right away.

Real-Time Task Checklist

Please review the following checklist containing all tasks required for dispatch completion. Note that all of the tasks are considered real-time tasks, meaning you should use MyESP to take and submit photos while onsite. If you do not submit photos via MyESP, these will become Post Visit Completion (PVC) tasks you must fulfill after the dispatch is completed, which was standard process prior to the MyESP rollout. TAC must receive all required tasks in real-time. If for any reason you cannot meet all requirements with one photo, you can take multiple photos and submit via the MyESP app. Optional tasks become required if the situation described is encountered. If you have any questions about these tasks, contact TAC:

Task Requirement	Submission Method	Required?	Submitted?
Service Request (SR) signoff	Fax to ESP (1-888-539-4334) or upload via MyESP	**Yes**	☐
Before photo of head end	Upload at least one photo showing the Interface provided networking equipment, including the existing broadband modem. If the existing broadband modem is not co-located with the Interface networking equipment, upload multiple photos.	**Yes**	☐
After photo of head end	Upload at least one photo showing the Interface provided networking equipment and the new modem wall or backboard mounted. If modem relocation was not possible (due to cable modem), please upload multiple photos (even if the modem could not be relocated it still should be wall-mounted).	**Yes**	☐
After photo showing the installed modem and operational lights (sync/link lights)	Upload at least one close-up photo showing the new wall or backboard-mounted modem. In this photo, we should be able to see the operational lights of the modem (power, sync, LAN connectivity).	**Yes**	☐
Photo of RMA device in box	Upload a photo showing the RMA device in the return box before it is sealed. After the photo is taken, seal the box and hand to the Manager for call tag return.	**Yes**	☐
Photo of signed equipment return form	Please fill out the attached equipment return form fully and have the MOD sign it. This form asks the MOD to acknowledge that all RMA equipment was boxed up and left with them for a FedEx call tag.	**Yes**	☐
Photo of the signed certificate of completion	Upload a photo of the signed/completed Certificate of Completion	**Yes**	☐

IMPORTANT:

YOU ARE REQUIRED TO COMPLETE ALL ABOVE TASK ITEMS REGARDLESS OF ANY PREVIOUS DISPATCHES TO THIS SAME SITE. ASSUME THAT NONE OF THE ABOVE ITEMS HAVE BEEN PREVIOUSLY COMPLETED AND THAT THEY STILL NEED TO BE.

PROCESS UPDATES

The purpose of this dispatch is to complete a circuit upgrade for an Interface Security Systems customer. As part of the circuit upgrade, the broadband service provider completed an onsite visit to install a new modem. Following the install guide, your job will be to configure and test the new modem. If all tests are successful, you will work with TTU to disconnect the existing modem and cut the site over to the new device, which should supply the site with more bandwidth. You are responsible for the following:

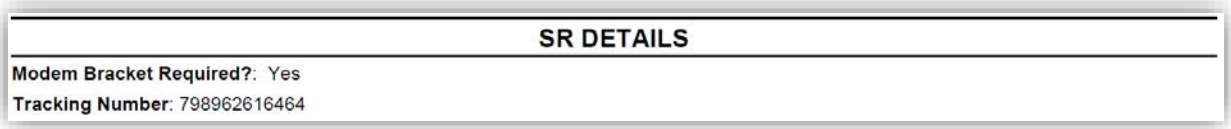
1. Locating any shipments sent to site by Interface/Onepath
2. Locating the existing broadband modem and Interface CPE
3. Extending the new circuit to the Interface CPE location (if needed)
4. Wall or backboard mounting the new modem (henceforth this will be referred to as "wall-mounted" to include both wall and backboard mounts)
5. Configuring and testing the new modem per the installation guide
6. Reconfiguring the existing Starlite for the new broadband connection
7. Completing the cutover to the new circuit
8. Completing equipment return (RMA) services, if required

The following sections provide additional detail on a few of the responsibilities listed above to **supplement** (not replace) the installation guide.

LOCATING INTERFACE/ONEPATH SHIPMENTS

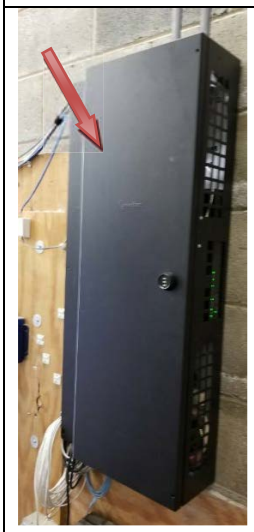
Prior to the dispatch, TTU will determine if the new modem installed by the LEC can wall-mounted without any additional hardware. If they determine the modem cannot be mounted without additional hardware (or they are unable to confirm), a mounting bracket will be shipped to site.

To determine whether a bracket shipped to your site, look at the SR Details section of your Service Request (SR). The two fields you are interested in for shipments to the site are "*Modem Bracket Required?*" and "*Tracking Number*". If *Modem Bracket Required* is set to yes, a tracking number should be available on your SR. If the tracking number is not present, call TAC for the information.



LOCATE EXISTING CPE AND EXTEND NEW CIRCUIT

The new modem should be installed near the existing Interface CPE so that any new cabling can be neatly routed to the downstream device. As needed, extend the circuit to the Interface CPE location. The Interface CPE will typically be installed on the wall or inside a cabinet as shown below:

Broadband cabinet	**Wall-mount cabinet**	**Wall-mount**
		

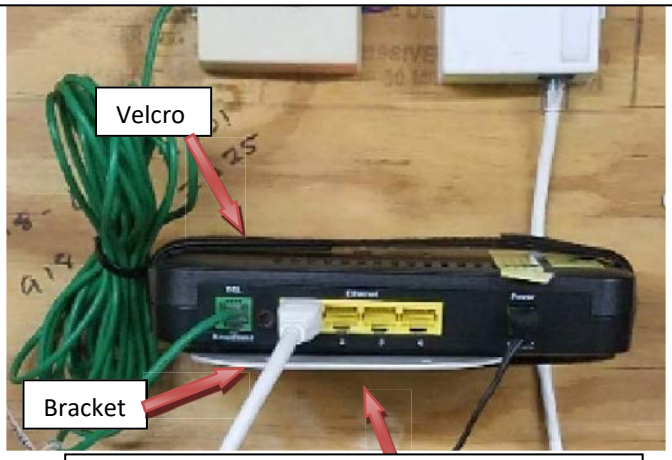
MOUNTING THE NEW MODEM

The new modem must be wall-mounted. The new modem cannot:

1. Be installed on a desk or shelf near the Interface equipment
2. Be installed in or on top of the locked Interface cabinet

The new modem MUST be wall-mounted near the Interface equipment. This can be accomplished by:

1. Utilizing the built-in screw eyelets on the modem
2. Utilizing the Interface provided mounting bracket

IF THE ISS MODEM BRACKET IS NOT PRESENT	IF THE ISS MODEM BRACKET IS PRESENT
	Screw the bracket into the backboard using two screws to create a shelf for the modem. Place the modem on top of the bracket. Secure the device to the bracket using Velcro. 
Built-in screw eyelets on the bottom of the modem allow you to insert two or more screws into the backboard. Slide the modem into the eyelets to secure it to the wall.	Modem secured to bracket by looping Velcro through existing holes in the bracket (not shown)

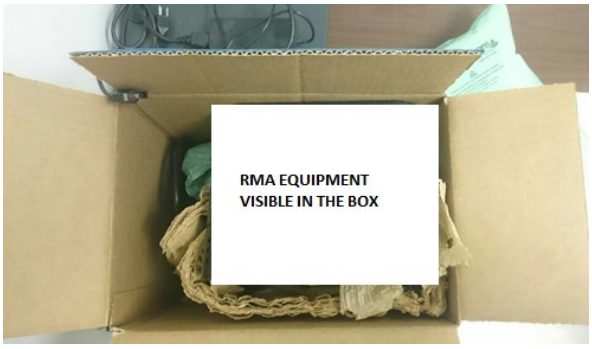
RMA PROCESS

To determine if equipment needs to be returned, look again at the SR details section of your SR. The two fields you are interested in for returns are "*RMA Required?*" and "*RMA Equipment Make/Model*". If the *RMA Required* field is set to yes, you will be required to box up the equipment listed in the *RMA Equipment Make/Model* field for call tag return.

SR DETAILS

Modem Bracket Required?: Yes
Tracking Number: 798962616464
RMA Required?: Yes
RMA Equipment Make/Model: **Equipment ABCD**

If an RMA is required, you are required to 1) complete the Interface Equipment Return Form and 2) submit a photo of the return equipment in a box. Both of these photos should be uploaded to myESP. After the photo is taken, seal the box and provide to the manager for call tag return. Let them know they should keep the equipment in a safe place and FedEx will be onsite in 1-5 business days to retrieve the box.



Interface Equipment Return Form

Please fill out the form below upon completion of the installation or trouble ticket for equipment that needs to be returned. Submit a photo of the completed form using myESP.

Decommissioned, unused or defective equipment/materials

Make/Model	Serial/ID No.	Condition (circle one)
		Decommissioned | Defective | Unused
		Decommissioned | Defective | Unused
		Decommissioned | Defective | Unused
		Decommissioned | Defective | Unused
		Decommissioned | Defective | Unused
		Decommissioned | Defective | Unused
		Decommissioned | Defective | Unused
		Decommissioned | Defective | Unused

Field Engineer – Please Complete

This form indicates you, the Interface Technician, boxed up and provided the existing/unused/defective equipment to the manager on duty for return. Please alert the manager on duty that FedEx will be onsite in 1-5 business days with a label to retrieve the equipment.

SR Number: _____ Installer Name: _____

Today's Date: _____ Installer Signature: _____

Manager on Duty – Please Complete

Please confirm the following:	Response (circle one)
The Field Engineer boxed up the return equipment	Yes | No
The Field Engineer sealed the box	Yes | No
The Field Engineer explained that FedEx will dispatch to your location within 1-5 business days to pick up the return box	Yes | No

Your signature indicates the Field Engineer explained the equipment return process and that you are taking possession of the equipment. FedEx will dispatch to your location to pick up the sealed box within 1-5 business days. A copy of this form will be kept on file at Interface Security Systems and will be used to document that the equipment was left onsite for return.

Employee Name: _____ Employee Signature: _____

Certificate of Completion and Acceptance

Your system was installed by trained technicians to meet the high standards of our quality assurance program.

Customer Name:_____ Branch #: _____

Installation Address:_____

City:_____ State:_____ Zip:_____ Install Date: _____

Job #1:_____ Install Ticket #:_____ P.O. #:_____

Job #2:_____ Install Ticket #:_____ P.O. #:_____

Job #3:_____ Install Ticket #:_____ P.O. #:_____

Account #:_____ Confirmation #: _____

Type of System:
◯ Secure Broadband ◯ Access Control ◯ Managed Access ◯ Structured Cabling
◯ Digital Voice ◯ Fire/Life Safety ◯ Camera Surveillance ◯ Supervisory System
◯ Intrusion ◯ Interactive Video ◯ Other:_____

Monitoring: ◯ Not Monitored ◯ Monitored by UL Listed Central Station ◯ Remote Video Monitoring
If Monitored, type of transmission link: ◯ Phone Lines ◯ Radio/Cellular/Broadband Backup
UL Listing *(if required):*_____ Type of Listing:_____ Certificate #:_____

I have received and understand the following:

◯ System Training & Operation ◯ Emergency Contact List ◯ Referral Program Details
◯ System User's Guides ◯ Backup Options ◯ Alarm Permit Information
◯ Monitoring Procedures ◯ Keys to Panel ◯ Other: _____

	yes	no
Was installation completed in accordance with the Agreement?	◯	◯
Were decals and/or signs installed to your satisfaction?	◯	◯
Was the installation completed to your satisfaction?	◯	◯
Are camera image views to your satisfaction? ◯ N/A	◯	◯
Was technician wearing protective shoe coverings when entering your location? *(Residential Only)*	◯	◯
Was the work area left clean and in order?	◯	◯
Were you properly instructed on the operation of the system?	◯	◯
Were our installers knowledgeable and helpful?	◯	◯
Did we meet your expectations?	◯	◯
Would you refer us to a friend or associate?	◯	◯
Are phones working properly?	◯	◯
Acknowledges receipt of the RMA equipment will be picked up by the shipping carrier within 3-5 business days.	◯	◯

Comments: _____

The customer named below hereby certifies that all equipment referred to in the Agreement, Schedule of Protection or Addendum has been delivered, is fully installed and it is in good operating order. Customer unconditionally accepts the equipment and authorizes commencement of billing in accordance with the Agreement.

_____ _____
Customer or Company Representative Signature *Date*

_____ _____
Customer or Company Representative Name Printed *Title*

Interface

Simplify To The Power Of One®

ACO 7245, 6860 Lic. # 469046

Broadband Carrier Change
Installation Instructions
Version 1.1.0 March 31, 2017

INSTALLATION TEST RESULTS

RECORD YOUR TEST RESULTS ON THIS PAGE AND FAX IT BACK WITH YOUR CLOSE-OUT PAPERWORK

1. Store Number: _____
2. Store Address: _____
3. Broadband information:
    a. PPPoE:
        i. Username: _____
        ii. Password: _____
    b. Static:
        i. IP address: _____ (If a range, use the 2nd useable)
        ii. Subnet Mask: _____
        iii. Gateway: _____
4. Primary Broadband type: _____ DSL _____ Cable _____T1 _____4G _____Other: _____
5. Primary 4G Carrier: _____Verizon _____AT&T _____Sprint _____ Other: _____
6. Primary 4G RSSI: _____ Primary 4G SINR: _____
7. Primary broadband circuit ID: _____
8. Primary broadband test results:

	Ping Time	**Download**	**Upload**
Test 1			
Test 2			
Test 3			

9. Comments / Issues Encountered: _____

    _____

10. TTU close out Date and time: _____ Close Code: _____

OVERVIEW:

The goal of this work order is to change the broadband connection to the Interface equipment to a newly provisioned circuit.

You will be:

- Locating the new broadband circuit.
- Testing the new broadband circuit.
    - Perform 3 speed tests on the new circuit.
- Connecting the new broadband circuit to the Starbox.
- Reconfiguring the Starbox for the new broadband circuit.
- Testing connectivity
- Reconnect the Starbox to the store router
- Test
    - Voice
    - Store operations

You will require a laptop with both wired Ethernet connection and wireless 802.11 connection.

REVISION CONTROL:

Previous version: 1.0.0 (12/19/2016)

Current Version: 1.1.0 (3/231/2017)

- Added instructions to install the modem mounting bracket, if supplied. (step 4.b)

TELEPHONE NUMBERS:

ISS TTU: 1-800-554-9875, Option 1: THIS NUMBER SHOULD BE USED FOR ALL NETWORK AND TELEPHONE SYSTEM PROGRAMMING.

INSTALLATION PROCEDURE:

Read this entire guide first. If you have any questions, call for assistance.

1. **ARRIVE ON SITE AND CHECK IN.**
    a. Before entering the customer's site, call:
        i. ISS TTU for pre-arrival login, and to get the broadband information (Circuit ID, Static IP information, PPPoE username and password…). Record this information on the "Installation Test Results" page.

2. **ENTER THE PREMISES AND INTRODUCE YOURSELF.**
    a. Enter the premises and introduce yourself as a representative of Interface Security Systems.
    b. Explain that you are on site convert the broadband service.
    c. Ask for the Site Contact.
    d. Quickly review with the Site Contact what work you will be performing, what areas you will be working in and where you will require access to.
    e. Ask the Site Contact to show you the locations of the following:
        i. Interface Broadband Cabinet
        ii. Telephone Demarcation point.
        iii. Any equipment the broadband carrier's technician installed.

3. **VERIFY CIRCUIT INSTALLATION AND PERFORM A SPEED TEST.**

NOTE: Cable modems mat automatically MAC bind to a device… you may need to power cycle the cable modem to release this MAC bind every time the device changes.

    a. Locate the new broadband modem that was delivered by the provider.
    b. The modem should be already powered up and connected to the internet.
    c. Verify the modem has sync.
    d. Connect your laptop to the new broadband modem with a CAT5 patch cable.
    e. Apply power to your laptop and let it boot normally.
    f. Open a web browser and navigate to several web pages. Make sure you are not loading cached pages.
    g. Navigate to a speed test site such as www.speedtest.com, www.speedtest.centurylink.com, or www.speedof.me (non-flash), and perform three or more speed tests. Record your results on the "Installation Test Results" page.

4. **IF DSL, BRIDGE THE MODEM.**
    a. See Appendix A for instructions for multiple modems. Call ISS TTU if you require assistance.
    b. If you were shipped a modem mounting bracket, mount the bracket to the wall with the supplied hardware kit and secure the modem to the bracket with a Velcro strap.

5. **RECONFIGURE THE STARLITE FOR THE NEW BROADBAND CONNECTION**
    a. Connect your laptop to the LAN2 port on the Starlite.
    b. Reacquire an IP address:
        i. At your laptops command prompt, type: ipconfig /release and press 'Enter'.
        ii. Then type: ipconfig /renew and press 'Enter'.
        iii. This will list your current IP address under a heading similar to 'Ethernet Adapter Local Area Connection'.
        iv. You should now have an IP address in the 192.168.6.x or 10.100.240.x range.
        v. If you have a 169.X.X.X address, verify the StarLite is powered up. If this persists, contact TTU for support.
        vi. Record your Default Gateway address here: ____.____.____.____.
    c. Open a web browser, and navigate to https:// (the gateway address recorded above). e.g. https://10.100.240.1
    d. If a certificate warning appears, click on proceed or continue.
    e. When the authentication screen appears, use this information:
        i. Username: admin
        ii. Password: s2sadmin
    f. After logging in, click on the "StarLite Network" tab in the blue bar.
    g. Click on the "Configuration" tab.
        i. If you have a PPPoE circuit :
            1. Select the radio button for "Obtain IP Address via PPPoE". (click in the circle)
            2. Enter your PPPoE username and password in the spaces provided. (see your SR for this information)
        ii. If you have a Static IP circuit:
            1. Select the radio button for "Specify an IP Address". (click in the circle)
            2. Enter your static IP information in the spaces provided. (see your SR for this information)
            3. Scroll to the DNS settings and enter in DNS1 & DNS2
        iii. If you have a DHCP circuit
            1. Select the radio button for "Obtain an IP address automatically"
    h. Save changes
        i. Scroll to the bottom of the page, and click on "Save Changes"
        ii. When the page refreshes, scroll to the bottom again and click on "Reboot Sarbox"
        iii. Confirm the reboot.
    i. Verify the settings.
        i. Verify that you can surf to multiple web pages
        ii. If you have any problems, verify your configuration.
        iii. If problems persist, contact ISS TTU for assistance.
    j. After verifying surf, Disconnect your laptop and reconnect the Cisco router to the Starbox.

6. TEST THE SYSTEM

a. Verify telephone operation
    i. Verify you can make a call by calling your cell phone.
    ii. Verify you can take calls by calling the store number from your cell phone.
b. With the MOD, perform a full system test.
    i. Request the MOD verify operation of all point of sales terminals.
    ii. Request the MOD verify credit card transactions.
        1. Credit card sale.
        2. Credit card refund.
    iii. Request the MOD verify complete operation of all other network systems.
c. If these tests fail, contact TTU for assistance.

7. CLEAN UP AND CLOSE OUT

a. Pick up and debris left from your installation.
b. Dispose of any boxes and packing left over for your and the LEC's installation.
c. Perform your normal close-out process with ISS TTU.

APPENDIX A: INSTRUCTIONS FOR BRIDGING SEVERAL COMMON MODEMS

1. **AT&T Pace 4111N**
    a. Open a web browser
    b. Navigate to: http://192.168.1.254 (or default gateway)
    c. Click on Settings
    d. Click on Broadband
    e. Click on Link Configuration
    f. Beside ATM PVC Search, uncheck Enable.
    g. From the Connection Type drop-down menu, select the Direct IP (DHCP or Static) option.
    h. Click Save.
    i. In the Routing section, uncheck Enable. (Default is enabled. Routing disabled = Bridge Mode.)
    j. Click Save
    k. If prompted for a Password after clicking Save, enter the Device Access Code on the bottom of the modem.
    l. Put PPPoE credentials into the StarLite

2. **AT&T NVG510 / NVG589 Static IP**
    a. Under Home Network go to Subnets & DHCP:
    b. Ensure the Private LAN subnet is set to the following: Device IPv4 Address: 192.168.1.254
    c. Subnet Mask: 255.255.255.0 DHCPv4 Start Address: 192.168.1.64 DHCPv4 End Address: 192.168.1.253
    d. Ensure the Public Subnet is set to the following:
        i. Public Subnet Enable set to ON
        ii. Allow inbound traffic set to ON (this only applies to NVG589)
        iii. Public IPv4 address - set to our static gateway address
        iv. Public subnet mask - set to our static IP block subnet mask
        v. DHCPv4 Start address - set to first usable static IP
        vi. DHCPv4 End address - set to last usable static IP
        vii. Primary DHCP pool - set to public
    e. Click Save
    f. Under Home Network go to Wireless:
        i. Set Wireless Operation to OFF Click Save
    g. Under Firewall go to IP Passthrough:
        i. Allocation Mode: Passthrough
        ii. Passthrough Mode: DHCPS-dynamic
    h. Click Save

3. **AT&T NVG510 / NVG589 DHCP – No Static IP**
    a. Plug his computer into the modem.
    b. Navigate to his default gateway (usually 192.168.1.254).
    c. Under Home Network go to Wireless:
        i. Set Wireless Operation to OFF
    d. Click Save
    e. Under Firewall go to IP Passthrough:
        i. Set Allocation Mode to Passthrough
        ii. Set Passthrough Mode to DHCPS – Fixed
    f. Set Passthrough Fixed MAC Address to the MAC address of the device
    (Ex: CradlePoint MAC for site) MAC address should be in XX:XX:XX:XX:XX:XX format
    g. Click Save
    h. Power cycle the modem.

4. **AT&T Pace 5031**

NOTE: ***This modem can be hard reset at any time if you encounter issues with this configuration process***

    a. Confirm surf with laptop directly connected to the modem
    b. Connect the Starbox LAN1 port to the modem and move your laptop to the Starbox LAN2 port
    c. Log into the Starbox.
        i. Go to:
            1. Starbox network
            2. Configuration tab
            3. Configure the Starbox for “Obtain IP address automatically”
        ii. Save the Starbox configuration
        iii. Click “reboot Starbox”
    d. When the Starbox is back up, confirm surf on your laptop from behind the Starbox
    e. Move your laptop to another port on the modem and release/renew your IP address (both the Starbox and your laptop should be connected directly to the modem at this point)
    f. Log into the Pace modem, gateway should be 192.168.1.254 (if not consult your ipconfig results to determine your gateway address)
        i. Go to:
            1. Settings
            2. Broadband
            3. Link configuration
        ii. Under Supplementary Network, Check enable next to Add Additional Network
        iii. Enter the static Gateway and subnet in the router address fields.
        iv. Check Auto firewall open
        v. Click on Save (if the modem tells you supplementary network already in use – continue to the next step)
        vi. Go to LAN
            1. IP Address Allocation

2. Scroll down to where the Starbox is listed as a device and select it
3. Set firewall to DISABLED
4. Set Address Assignment to "Public (select WAN IP Mapping)"
5. Set WAN IP Mapping to Public Fixed: XXX.XXX.XXX.XXX (First usable IP from our static IP range)

vii. Click on Save

viii. Go to LAN: Wireless

1. Disable the wireless interface

ix. Click on Save

x. Go to:

1. Settings
2. Firewall
3. Applications, pinholes and DMZ

xi. Select the Starbox – will appear as “Starbox _XXXXXX”

xii. Scroll to the very bottom of the page and select "Allow all applications (DMZplus mode)"

g. Click on save

h. Move your laptop back to the Starbox LAN2 port

i. Log back into the Starbox

i. Go to:

1. Starbox Network
2. Configuration tab
3. Configure the Starbox for “specify an IP address” – use the first usable IP address from our static IP range (the same one you set above).

ii. Save the Starbox configuration

iii. Click “reboot Starbox”

j. After the Starbox comes back up, confirm you are able to surf and then reconnect the Cisco 891 to LAN2 of the star box.

k. Log back into the modem and confirm that auto firewall is still set to open as you set above.

5. **AT&T 3801**
    a. Click Settings
    b. Click Broadband
    c. Click Link Configuration
    d. Select Add Additional Network
    e. Put your Gateway in the router address
    f. Put your Subnet in the subnet mask
    g. Click Auto Firewall Open
    h. Program the Starbox with statics.

6. **AT&T 3360, 6100, 6200 & 7550**
    a. Open a web browser
    b. Navigate to 192.168.1.254 determine the default gateway
    c. Click on the advanced tab
    d. Click on PPP location
    e. Select the PPP on computer
    f. Save changes and reboot
    g. Put PPPoE credentials into the Starbox

7. **CenturyLink/Qwest Zyxel 660R**
    a. Open a web browser
    b. Navigate to default gateway
    c. When prompted for a username and password. Click “login” with whatever info is already in the fields.
    d. Click Ignore
    e. Click ignore
    f. Click Diagnostics (Under Maintenance)
    g. (General-for F1 model)
    h. Click Network Layer
    i. Click Wan IP release
    j. Click “change to bridge mode” and wait for it to refresh.
    k. Power cycle the modem
    l. Put PPPoE credentials into the Starbox

8. **CenturyLink/Qwest Zyxel 660HW**
    a. Click Advanced Setup
    b. Under Maintenance click Diagnostics
    c. Click "Change to bridge mode"
    d. Now in bridge mode
    e. Put PPPoE credentials into the Starbox

9. **CenturyLink/Qwest PK5001**
    a. Open a web browser
    b. Navigate to http://192.168.0.1
    c. Log in to the modem. The username and password are on the bottom of the modem
    d. Select “Wireless Setup”
    e. Select the radio button for “Disable” in the “Wireless Radio Status” screen.
    f. Click on “Apply”
    g. Select “Advanced Setup”
    h. On the left-hand menu, under “IP Addressing” select “WAN Settings”
    i. In the “WAN Settings” Screen, select “Transparent Bridging” from the “ISP Protocol” drop-down.
    j. Click on “Apply” on the bottom of the screen
    k. Put PPPoE credentials into the Starbox

10. **CenturyLink/Qwest C1000**
    a. Surf to 192.168.0.1
    b. Go to Advanced
    c. Go to WAN
    d. Select Transparent Bridging.
    e. Hit Apply

11. **Frontier 7550 Static IP**
    a. Select advanced along the top right of the page. To the left of system monitoring.
    b. Click yes or ok to continue
    c. Click public LAN in the bottom right
    d. Ensure "Public LAN Enable" is checked
    e. Set the Modems Public IP address (enter the static Gateway)
    f. Enter the subnet mask
    g. Click Apply.
    h. Modem will reboot.
    i. Log back into the modem and go to advanced
    j. (Setup wizard may come up. If it does ensure the FE turns off wireless.)
    k. Click on Private LAN in the bottom right
    l. Uncheck "Private LAN DHCP server Enable".
    m. Confirm that the Modem IP address is 192.168.254.254
    n. Click Apply.
    o. Enter static IPs into the Starbox

12. **Megapath Comtrend AR5220u**
    a. Browse to the gateway IP – 192.168.1.1
        i. Username: root
        ii. Password: 12345
    b. Select “Advanced Setup”
    c. Select “Add”

NOTE: If there is already an ATM interface you will need to go to WAN services on the left hand navigation Panel and delete the existing WAN Service. Then go back to Advanced Setup and delete existing ATM Interface before Adding a new configuration.

    d. Choose “EoA” under select DSL link type
    e. For Encapsulation Mode select “LLC/SNAP-BRIDGING”
    f. Select “Apply/Save”
    g. Make note of the interface name on this screen (ex: atm0)
    h. From the left navigation area choose “WAN Service”
    i. Select “Add”
    j. Choose the ATM interface you previously created (ex: “atm0/(0_0_35)”)
    k. Select “Next”
    l. Select “Bridging” under WAN service type
    m. Select “Next”
    n. Select “Apply/Save”
    o. Enter the PPPoE Credentials into the Starbox

13. **Megapath Zyxel 660**
    a. Under network select WAN

b. Mode - change to bridge.
c. Encapsulation should be RFC – 1483
d. VPI- 0 VCI – 35
e. Select apply

14. **Windstream Sagemcom 1704 and 4320**

IP-Passthrough Configuration (For use with the Starbox)

Gateway - 192.168.254.254

UN: admin PW: admin

a. Go to Advanced::WAN Service
b. You will see the detail of the WAN configuration.
c. At the far right click on the edit icon.
    a. Uncheck NAT and Firewall checkboxes.
    b. Save settings.
d. Go to Wireless.
    a. Uncheck enable wireless
    b. Save setting.
e. Go to Advanced::LAN
    a. Check the "Configure the second IP address and Subnet Mask for LAN interface" box. This opens additional text boxes.
    b. Enter the first usable (Gateway IP) in the IP Address field
    c. Enter subnet in the Subnet Mask field
    d. Uncheck LAN DHCP server.
    e. Save Settings
f. Put the Statics into the Starbox.

15. **Windstream 4300**
    a. Open a web browser
    b. Navigate to http://192.168.254.254 and click on login on the left hand side of the screen.
        i. Username: admin
        ii. Password: admin
    c. Click on setup and it will expand further and then choose WAN Interface.
    d. Click on the top delete button next to the disable button on the virtual circuit. Everything will disappear.
    e. Click on Add a New VC.
    f. Change the VCI from 32 to 35 and click the next button at the bottom of the screen.
    g. Select RFC2684 Bridged
    h. Click next
    i. No changes click next
    j. Click finish
    k. Click on "DHCP" on the left hand side below Host under the Setup category.
    l. Then disable DHCP and scroll to the bottom of the screen and click save settings.
    m. Click the “Reboot” button.
    n. The modem will now do a 45 second countdown and reboot
    o. Put PPPoE credentials into the Starbox

16. **Verizon D-Link 2750**
    a. Open Browser to http://192.168.1.1
    b. Click on Settings Tab
    c. Log in with
        i. Username: admin
        ii. Password (refer to back label of 2750B)
    d. Click on Wireless Tab and disable the wireless
    e. Click Apply
    f. Select MY Network-> Internet
        i. From the drop down menu next to Connection type select “LAN-WAN Bridged Ethernet Connection over ATM (Bridged ETHoA)”
        ii. Click Apply
    g. You will see a browser reload message, click OK
    h. Browse to System->Network Connections and Click “WAN-LAN Bridge”
    i. Go to the Settings tab
        i. Under Internet Protocol, change the setting to “No IP Address”
        ii. Click Apply
    j. Upon seeing the Browser Reload message, click OK
    k. Go to FIREWALL SETTINGS tab; you are on OVERVIEW page
        i. Click Radial button for MINIMUM SECURITY; changed from default TYPICAL SECURITY
        ii. Click Apply
    l. Go to ADVANCED FILTER sub-tab/page
        i. Scroll down to ALG RULE section
            1. Uncheck “INPUT RULE ID #2; Operation ALG SIP”
            2. Uncheck “OUTPUT RULE ID #8; Operation ALG SIP”
        ii. Click Apply
    m. Reboot the Modem and connect to the Starbox LAN1 port

17. **Verizon Westel 6100**
    a. Surf to 192.168.1.1
    b. Click my network
    c. Network Connections
    d. Broadband Connections (Check the Connection Profile – It will be either PPP or in a Routed Bridge)
    e. Routed Bridge (This is a DHCP circuit configure the StarLite for obtain automatically):
    f. Click the RED Release button under Action
    g. Click the edit button to the right of the VPI/VCI information
    h. Change Protocol to Bridge
    i. Mode to Bridged
    j. Save Settings
    k. PPP (This is a PPPoE circuit configure the StarLite with open PPPoE Credentials):
    l. Click the edit button to the right of the VPI/VCI information
    m. Change Protocol to Bridged
    n. Change Bridge Mode to Bridged
    o. Save Settings
    p. Click my Network
    q. Network Connections - LAN
    r. Uncheck Private DHCP server enable (Leave Private LAN enabled)
    s. Click Apply
    t. Power cycle the modem and configure the StarLite.

18. **Verizon – Actiontech 784**
    a. Username: Admin
    b. Password: on the bottom
    c. Click the Wireless setup
        i. Click disable
        ii. Click apply
    d. Click Advanced setup
        i. Go to the WAN IP setting section of the page
        ii. RFC 1483 Transparent Bridging
    e. Click “apply” until the modem tells you it's going to reset.
    f. Configure the StarLite with open PPPoE Credentials

Closure Details

Representative	Group	Closure Code / Hold Time
Ex: Bob Smith	**NOC**	**BS1215 / 10 min**

Milestone	Time
Ex: Time Onsite	**10:00**
Ex: Time Offsite	**12:15**
Time Onsite	
Time Offsite	

Time Breakdown (Email to tb@1path.com)	Reason
Example: 10:00-11:00	**Arrival onsite, extending demarc from back of store to front counter**

Equipment Installed (Make/Model)	Serial Number
Example: Cisco 1941	**FTX1254789**

Equipment Retrieved	Serial Number	Tracking Number
Example: Cisco 1941	**FTX1254789**	**1275864520100**

Materials Used	QTY	FE/Onepath/Customer Provided?
Example: Cat5e UTP	**127 ft**	**FE / Onepath / Customer**
Cat5e UTP		FE / Onepath / Customer
RJ-45 jacks		FE / Onepath / Customer
RJ-11 jacks		FE / Onepath / Customer