FTTx Application Guide

For software version 1.16
October 2009
Document Part Number: 830-02024-02

Z H O N E™

Zhone Technologies
@Zhone Way
7001 Oakport Street
Oakland, CA 94621
USA
510.777.7000
www.zhone.com
info@zhone.com

Zhone Technologies makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability, non infringement, or fitness for a particular purpose.

Further, Zhone Technologies reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Zhone Technologies to notify any person of such revision or changes.

CONTENTS

ABOUT THIS GUIDE

This guide is intended for use by technicians, installers, system administrators and network administrators. It explains how to configure the Zhone products within the context of Fiber to the home, business, multi-dwelling unit (FTTx) application scenario.

This guide describes how to build a few basic bridging scenarios which are building blocks to creating advanced and complex networks. The idea is that as you build a scenario, you understand the implications of the commands you are using to build the scenario, then once the scenario is built you can test the scenario for the functions it provides.

For information on installing the MXK chassis and cards, refer to the *MXK Hardware Instlallation Guide. For* greater information about specific configuration procedures for the MXK, please refer to the *MXK Configuration Guide*.

Since OMCI based GPON zNIDs are mainly configured on the OLT (MXK), all the configuration information is in the MXK *Configuration Guide*. Hardware installation instructions for OMCI based zNIDs are in zNID xxxx Quick Installation Instructions, where xxxx is the model number of the zNID, for example zNID GPON 2510. For the OMCI based model used in this guide, see the zNID GPON 2510 Quick Installation Instructions.

For more information on the browser based zNIDs, see the *zNID Admin & Config Guide* and the *zNID Hardware Installation Guide*.

This guide only attempts to introduce technical topics. The idea is not to explain industry standards, but explain the Zhone perspective on the standard and how to implement solutions using Zhone products.

Style and notation conventions

The following conventions are used in this document to alert users to information that is instructional, warns of potential damage to system equipment or data, and warns of potential injury or death. Carefully read and follow the instructions included in this document.

Caution: A caution alerts users to conditions or actions that could damage equipment or data.

Note: A note provides important supplemental or amplified information.

Tip: A tip provides additional information that enables users to more readily complete their tasks.

WARNING! A warning alerts users to conditions or actions that could lead to injury or death.

WARNING! A warning with this icon alerts users to conditions or actions that could lead to injury caused by a laser.

Typographical conventions

The following typographical styles are used in this guide to represent specific types of information.

Bold	Used for names of buttons, dialog boxes, icons, menus, profiles when placed in body text, and property pages (or sheets). Also used for commands, options, parameters in body text, and user input in body text.
`Fixed`	Used in code examples for computer output, file names, path names, and the contents of online files or directories.
`Fixed Bold`	Used in code examples for text typed by users.
`Fixed Bold Italic`	Used in code examples for variable text typed by users.
Italic	Used for book titles, chapter titles, file path names, notes in body text requiring special attention, section titles, emphasized terms, and variables.
PLAIN UPPER CASE	Used for environment variables.
Command Syntax	Brackets [ ] indicate optional syntax. Vertical bar | indicates the OR symbol.

Related documentation

Refer to the following publication for additional information:

MXK Hardware Installation Guide—explains how to install the chassis and cards.

MXK Configuration Guide—describes how to configure the MALC for routing, for bridging and a number of other configurations.

Zhone CLI Reference Guide—explains how to use the Zhone command line interface (CLI) and describes the system commands and parameters.

zNID GPON 2510—describes installing the indoor zNID.

zNID Hardware Installation Guide—describes how to install the outdoor browser based zNIDs.

zNID Admin & Config Guide— describes how to configure the outdoor browser based zNIDs.

Refer to the release notes for software installation information and for changes in features and functionality of the product.

Acronyms

The following acronyms are related to Zhone products and may appear throughout this manual:

Table 1: Acronyms and their descriptions

Acronym	Description
ADSL	Asymmetrical digital subscriber line
ARP	Address resolution protocol
APC	Angled physical contact (for optical connectors)
ATM	Asynchronous Transfer Mode
DSL	Digital subscriber line
EFM	Ethernet in the First Mile
EAD	Ethernet Acess Devices
FTTH	Fiber to the Home
GPON	Gigabit PON (Passive Optical Network)
IAD	Integrated access device
MALC	Multi-access line concentrator
MIB	Management information bases
ODN	Optical Deployment Network

Table 1: Acronyms and their descriptions

Acronym	Description
OLT	Optical Line Terminator
OMCI	ONT Management Control Interface
ONT	Optical Network Terminator
ONU	Optical Network Unit
RIP	Routing Information Protocol
SHDSL	Symmetric high-bit-rate digital subscriber line
SLMS	Single Line Multi-Service
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
UPC	Ultra physical contact (for optical connectors)
ZMS	Zhone Management System
zNID	Zhone Network Interface Device

Contacting Global Service and Support

If your product is under warranty (typically one year from date of purchase) or you have a valid service contract, you can contact Global Service and Support (GSS) with questions about your Zhone product or other Zhone products, and for for technical support or hardware repairs.

Before contacting GSS, make sure you have the following information:

- Zhone product you are using
- System configuration
- Software version running on the system
- Description of the issue
- Your contact information

If your product is not under warranty or you do not have a valid service contract, please contact GSS or your local sales representative for a quote on a service plan. You can view service plan options on our web site at

http://www.zhone.com/support/services/warranty.

Technical support

The Technical Assistance Center (TAC) is available with experienced support engineers who can answer questions, assist with service requests, and help troubleshoot systems.

Hours of operation	Monday - Friday, 8 a.m. to 5 p.m, Pacific (excluding U.S. holidays)
Telephone (North America)	877-ZHONE20 (877-946-6320)
Telephone (International)	510-777-7133
E-mail	support@zhone.com
The Web is also available 24 x 7 to submit and track Service Requests (SR's)	www.zhone.com/support

If you purchased the product from an authorized dealer, distributor, Value Added Reseller (VAR), or third party, contact that supplier for technical assistance and warranty support.

Hardware repair

If the product malfunctions, all repairs must be authorized by Zhone with a Return Merchandise Authorization (RMA) and performed by the manufacturer or a Zhone-authorized agent. It is the responsibility of users requiring service to report the need for repair to GSS as follows:

- Complete the RMA Request form (http://www.zhone.com/account/sr/submit.cgi) or contact Zhone Support via phone or email:

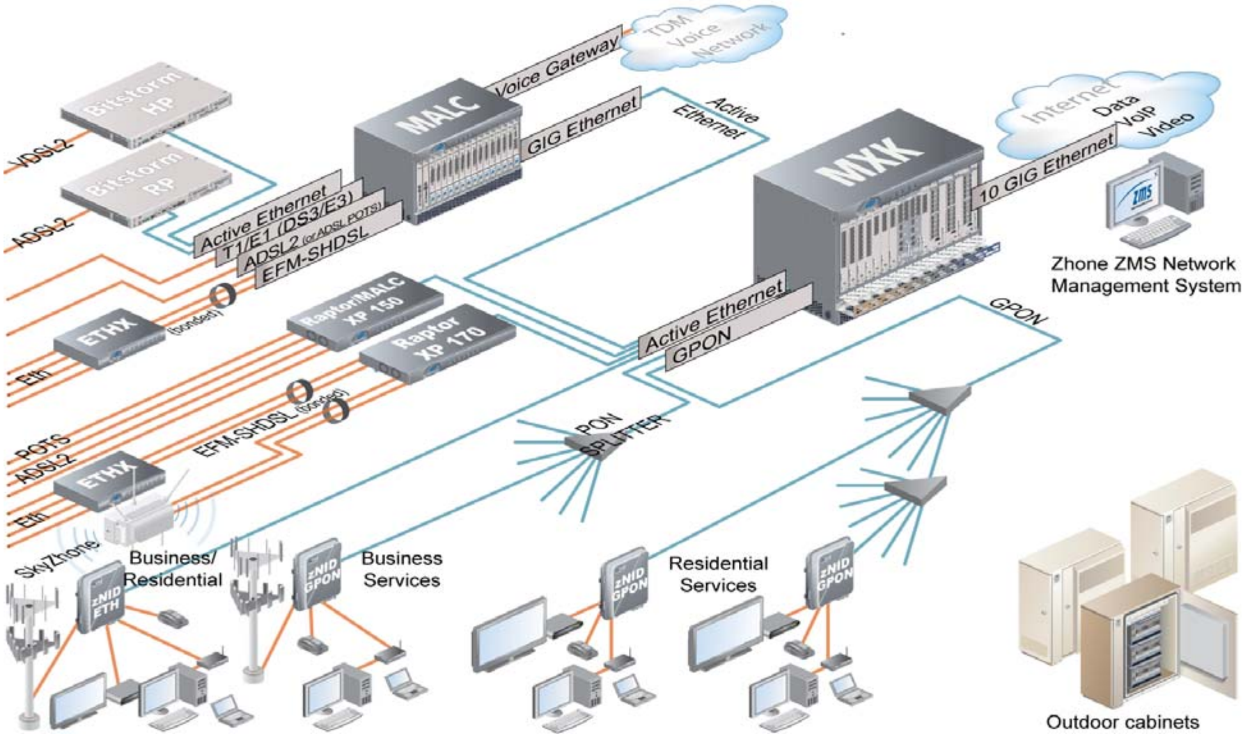
Hours of operation:	Monday Friday, 6:30am-5:00pm (Pacific Time)
E-mail:	support@zhone.com (preferred)
Phone:	877-946-6320 or 510-777-7133, prompt #3, #2

- Provide the part numbers and serial numbers of the product(s) to be repaired.
- All product lines ship with a minimum one year standard warranty (may vary by contract).
- Zhone will verify the warranty and provide a repair quote for anything not under warranty. Zhone requires a purchase order or credit card for out-of-warranty fees.

1 OVERVIEW

Zhone Technologies provides advanced fully integrated network access solutions. Zhone's vision is founded on intelligent access devices capable of quickly and easily deploying multi-play service packages which combine business broadband, Voice over IP (VoIP), Internet Protocol Television (IPTV), and Ethernet access on existing copper and fiber infrastructure with a migration path to an all IP network.

Central to Zhone's vision are the Multiple Service Access Platforms (MSAP), MXK and MALC. These flexible access platforms provide carriers a means to deploy premium services using copper and fiber while improving network agility and reducing costs.



Fiber-based solutions are growing in popularity in access technologies, mainly due to the increasing demand for subscriber bandwidth, the limits of copper technology, and the availability of capital for investment in the access network. Copper based solutions may provide dramatically high data rates, but an inherent limitation of the technology limits performance substantially as a function of distance. Fiber solutions provide high bandwidth over much longer distances.

Advanced copper access technologies such as VDSL2 and bonded ADSL2+ and EFM that aggregate multiple copper lines for higher performance often present a compelling balance of economy and performance. Other options include a combination of copper and fiber delivering fiber to the curb or basement and leveraging existing copper at short distances to reach the home or business. In each case, a balance must be struck considering the availability of capital, the quality of existing cabling and the cost of installation.

Zhone Sales representatives can help carriers consider available options and technologies to select the optimal combination of technologies given their market, competition, network infrastructure, and the availability of capital.

Fiber Solutions

Fiber solutions are often characterized by how far they reach into the access network. References include fiber extended to the curb, to the business, to the node, or after the node to the home and are usually grouped into the acronym "FTTx," meaning Fiber To The x, where x is any of these subscriber or near-subscriber endpoints. This document is primarily concerned with FTTH (Fiber To The Home), applications where endpoints are placed in the home (with distinct configurations for indoor and outdoor installations). Fiber-based solutions today generally center on one of two leading technologies — GPON (Gigabit Passive Optical Networks) and Active Ethernet.

In the carrier's access network, the Optical Line Terminator (OLT) provides access concentration and serves subscribers in either a star or cascading topology connections to the Optical Network Termination (ONT) at the subscriber home (in FTTH applications).

Zhone's MXK multi-service access platform is optimized for the high bandwidth and service intelligence required of OLT functions in FTTH applications. Zhone's broad line of zNID ONTs provide access services to residences and businesses with a range of interfaces and local routing features. Consult the Zhone Web site or your Zhone sales representative about the available models.

GPON and Active Ethernet

GPON and Active Ethernet are different transport technologies but they are both based on the same physical media. Using the ISO model as a guide, GPON and Active Ethernet specify Data Link or Layer 2 technologies carried on Layer 1 fiber physical media. Each Layer 2 technology supplies distinct characteristics which may solve different access problems.

GPON, with its point-to-multipoint architecture, is better suited for shorter reach settings, such as suburban developments. GPON cost-effectively splits a fiber signal to multiple subscribers and thus creates a lower cost for each subscriber by reducing the number of optical transceivers in the optical deployment network.

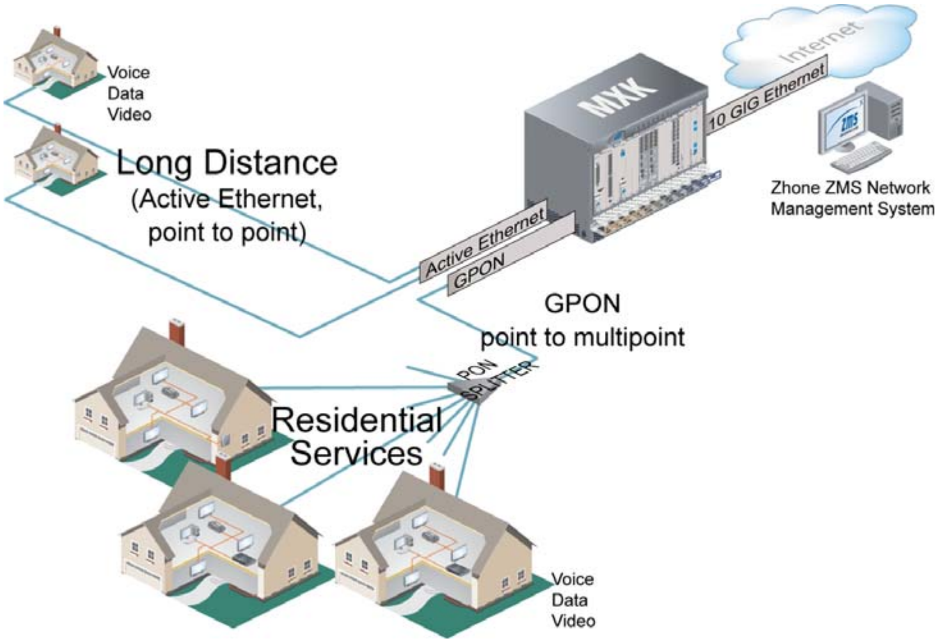
In contrast, Active Ethernet dedicates optical transceivers at both the OLT and the ONT for each subscriber with a point-to-point topology. This simple fact gives Active Ethernet the flexibility for longer reach and can be better suited for rural settings, where subscribers may be up to 50 miles from a central office. Further, because Active Ethernet dedicates an optical fiber for each subscriber, it is also well suited for the guaranteed bandwidth requirements of business subscribers.

GPON with class B+ optics provides a maximum of 2.5 Gbps downstream and 1.25 Gbps upstream traffic. GPON is a point-to-multipoint architecture which may be split up to 64 subscriber ends, so the 2.5 Gbps downstream/1.25 Gbps upstream is split among the subscribers. All information is sent out to all units. Encryption keeps information private.

Active Ethernet provides a dedicated symmetric 1 Gbps performance upstream and downstream. Since Active Ethernet is point to point there is no splitting/sharing of bandwidth per OLT port. However you can also share an Active Ethernet link by using an Ethernet switch instead of an ONT in the subscriber end of the connection. The difference from GPON to Active Ethernet in this case is that GPON does not require active components (like Ethernet switches and SFPs) to share the bandwidth in the subscriber side of the connection, which makes GPON cheaper to implement to multiple subscribers.

Under ideal circumstances, GPON can reach up to 20 or 30 km, however the practical limit is 12 km (about eight miles).

By comparison, under similar ideal circumstances, Active Ethernet can reach 80 km or nearly 50 miles.



Zhone supports both Active Ethernet and GPON. Read the Zhone White Paper, “Choosing the Right FTTx Architecture” or consult your Zhone sales representative about both GPON and Active Ethernet solutions.

Zhone GPON solutions: OMCI and browser based

Zhone has two types of zNIDs for GPON: those which are based on ONT Management Control Interface (OMCI) for configuration and management and those which use a browser based user interface (UI) as is common with modems, routers and residential gateways.

Most Zhone ONT models (zNIDs) are OMCI based, using Zhone’s easy to use Smart OMCI configuration tools. At this time no zNIDs support both OMCI and the browser based UI.

Note: This document uses the zNID 2510 as a reference model for the OMCI based zNIDs. The same procedures described in this document apply for OMCI based zNIDs.

Though Zhone's element management system, ZMS, manages both sets of models, the main differences between the OMCI-based solution and the browser-based solution are how you configure them. The OMCI based zNIDs may be configured directly through ZMS or via the CLI and Web UI (which are SLMS based). OMCI is a policy-based solution, designed to deal with larger numbers of zNIDs in a structured way.

Both browser based zNIDs, GPON and Active Ethernet (currently the 4200 series) are configured from a Web user interface. For example, to build a bridge for the subscriber devices connected to the browser based zNID, you configure a bridge on the zNID as well as on the MXK.

Note: This document uses the zNID GPON 4213 as a reference model for GPON browser-based zNIDs and the zNID ETH 4212 as a reference for the Ethernet browser-based zNIDs, mainly because the 4213 and 4212 have all the features of the 4200 family. The same procedures described in this document apply for all 4200 series zNIDs whether based on GPON transport media or Active Ethernet transport media.

For deploying similar configurations to multiple browser based zNIDs, you can copy and upgrade the configurations.

This application guide is organized into separate sections for configuring OMCI based and browser based zNIDs, to help reduce any confusion between the two methods. Browser based and OMCI based zNIDs may be used on the same network, even on the same bridge.

Deploying fiber solutions

Although this guide is primarily concerned with configuring Zhone equipment, we believe it is important to have a strong understanding of the underlying technology. This section attempts to define some general items to take into consideration, not to be a definitive resource. We also add an appendix to discuss these topics in greater detail to broach the subject and help locate reference resources with quickly evolving technologies.

GPON and Active Ethernet networks and terminology

There is a set of terminology for components in optical deployment network (ODN).

Components of optical deployment networks.

Optical networks are comprised of a number of components between the subscriber CPE devices. GPON networks have additional components for splitting signals (splitters).

- OLT

  Optical Line Terminator. This device is considered the head end of the ODN.

- Optical fiber

  The optical fiber is the physical cable.

- Splitters (GPON only)

  Optical splitters split a single optical signal to multiple optical signals.

- Couplers

  Couplers are connectorized means for splicing cables. Because couplers are connectors there is a an optical signal cost for connectors

- ONT or ONU

  Optical Network Terminator (ONT) and Optical Network Unit (ONU) are reasonably similar terms which are both defined in the ITU-T G.984 GPON standards. They both provide an end for the ODN and conversion to some electrical media; However, ONTs usually have multiple subscriber-side services and interfaces, like Ethernet LAN, POTS or coaxial cable for TV services. ONUs would have a GPON interface upstream (just like the ONT), but would connect to some other last mile copper access device, such as a VDSL2 DSLAM or MSAP.

- Attenuators

  Attenuation is the term for the loss of optical power on the ODN. Some devices may actually receive too high a signal power strength for the receiving device. This situation most commonly occurs in lab settings, such as we are building for the scenarios in this guide. An attenuator is actually a device that can adjust the power strength of the optical signal.

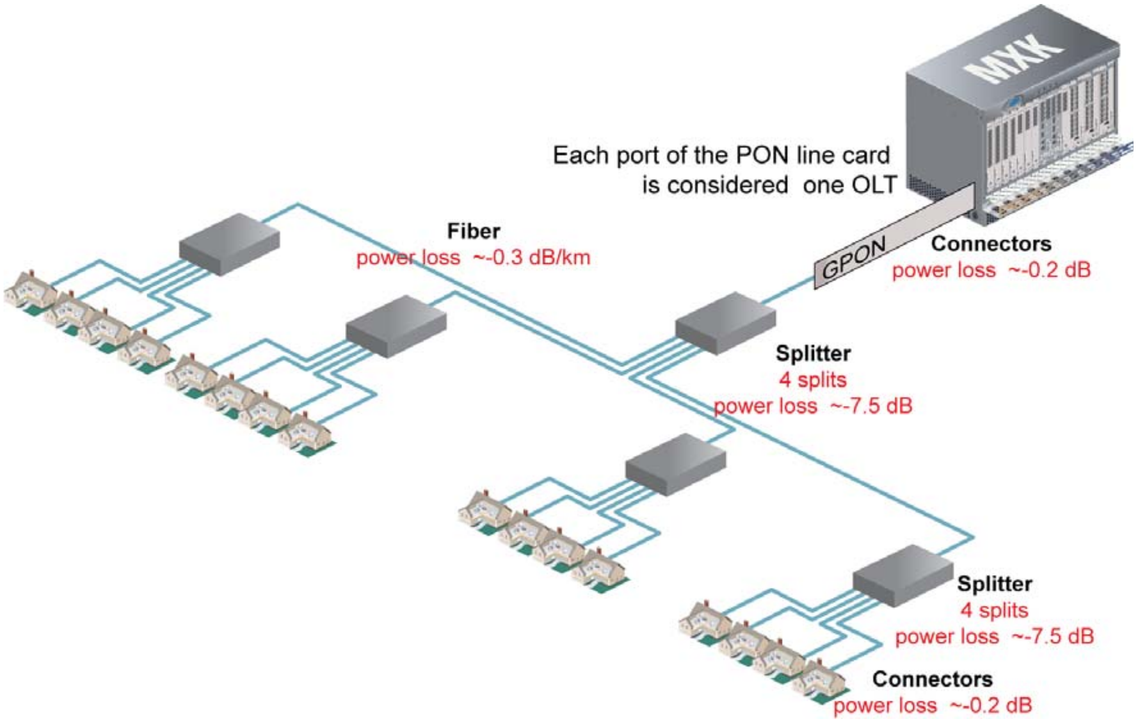
All the fiber components named above are important in planning and installing GPON networks.

Planning GPON networks

When deploying GPON networks, you have to think in optical terms, rather than electrical or copper based terms. With copper based solutions you think of distance and transport technology (“Will ADSL or VDSL reach from the CO to the subscribers?” is a significant network design question); with fiber based networks, and GPON in particular, you have to think in terms of optical link power loss budgets.

Link loss is the amount of signal attenuation as you proceed farther away from the OLT toward the subscribers’ ONTs. Each component, including the fiber cable itself, degrades the signal. Attenuation is the term used for describing the amount of signal degradation.

Figure 1: Link loss in an GPON Optical Deployment Network



The plan for both a GPON network and Active Ethernet network should include a link loss budget map that shows how each component, even the distance of each length of fiber, should affect signal attenuation. Because GPON lines are split into multiple lines which have a significant power loss, the link loss budget map is a more important requirement for GPON

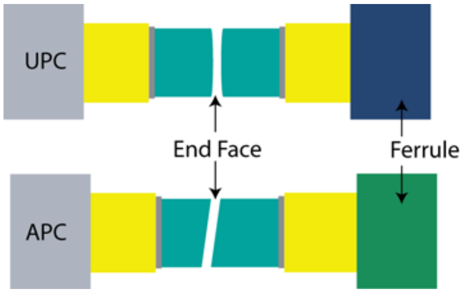
Component	Loss
Optical fiber	-0.3 dB per kilometer
Splitters	The link loss for splitters depends on the number of splits • 2 splits, -4 dB • 4 splits, -7.5 dB • 8 splits, -11 dB • 16 splits, -14 dB • 32 splits, -18 dB • 64 splits, -21.5 dB
Splices	-0.1 dB
Connectors	-0.2 dB
Couplers	Couplers are connectorized means for splicing cable. -0.4 dB

Installation testing

The theoretical link loss budget map is very important when installing fiber. Testing should be done before and after each component is added. Matching the actual signal attenuation with the theoretical link loss budget map helps identify problems such as

- macro bends in cables (too small a bend radius)
- connector loss from back reflection (the contact between the face ends of fiber in a connector, or a splice)
- incorrectly matching UPC and APC connectors may also create back reflections. UPC connectors (Ultra Physical Contact) have a slightly spherical end face. APC connectors (Angled Physical Contact) use an industry standard angle on the end face of the fiber. (Though you should be aware of older, non standard APC connectors which use a different angle.)

Figure 2: End face of UPC and APC connectors



There are testing tools on the market which can be used to test the components as added.

The actual figures that are discovered during installation testing should also be noted and filed as they may also be helpful when troubleshooting problems which may arise in the ODN in the future.

Handling fiber

Handling of fiber requires special precautions for those familiar with copper wiring.

WARNING!

Never look into an active optical fiber. Exposure to invisible LASER radiation may cause serious retinal damage or even blindness.

WARNING! Clean hands after handling optical fibers. Small pieces of glass are not always visible and can cause eye damage.

Get medical assistance immediately for any glass that comes into contact with your eye.

Fiber needs to be kept clean. Contaminents may obstruct the passing of light. Notable contaminents include

- oil from hands
- dust particles
- lint
- the residue which may be left when using wet cleaning methods
- scratches which may be from dry cleaning methods or mishandling fiber.

Fiber requires a handling discipline which includes

- inspecting fiber ends (with a fiber inspection probe)
- cleaning fiber, with either a wet cleaning method, dry cleaning method or both.
- fiber cannot be bent too far. Bending fiber too far will keep the optical signal from bending. You may see the light through the sheething of the cable. These macrobends may also create microfractures in the glass of the fiber resulting in signal loss.

Please see *Chapter A, Appendix: Handling fiber,* on page 107 for more detail with handling fiber optic cables and other important layer 1 physical issues.

Fiber scenarios in the application guide

The primary goal of the FTTH application guide is to show how to create triple play services via the OMCI based solution or the browser based solution. This document will show how to configure both the OLT and the ONT.

Zhone also has zNID 42xx models which use Active Ethernet transport technology. While the ODN may be different, the browser-based interface is the same for both GPON and Active Ethernet models of the 42xx.

For both the OMCI based and browser based models we will build examples of common residential access applications:

- Data
- Video
- Voice
- Triple Play (data, video, and voice on the same zNID)

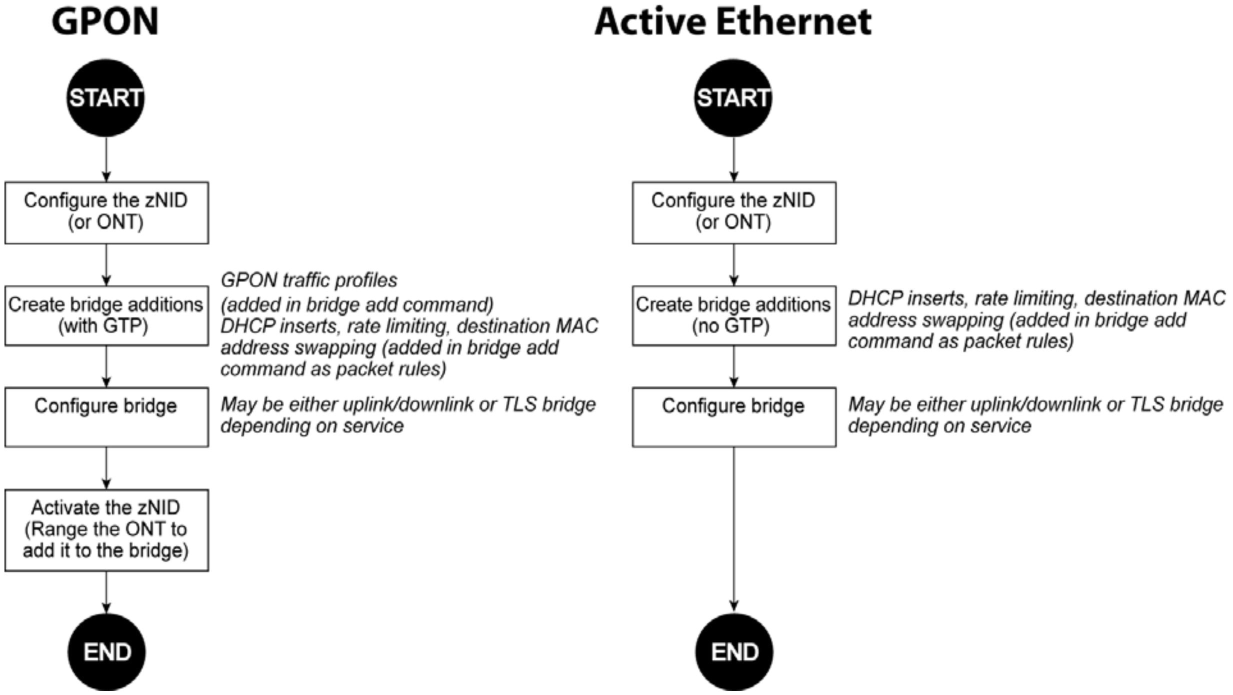
The guide takes you from opening the shipping boxes to configuring the solutions. For an understanding of the process, please see *Getting to work* on page 23. To get right to the configuration sections, please see *Chapter 3, OMCI based GPON zNID,* on page 43 or *Chapter 4, GPON and Active Ethernet UI based zNID,* on page 67.

Overview of the configuration process

We will configure each type of scenario — OMCI GPON, browser-based GPON, or browser-based Active Ethernet — separately to avoid confusion. However, to highlight the similarities among the three deployments we will describe the configuration process together and note the differences.

Differences between GPON and Active Ethernet deployments

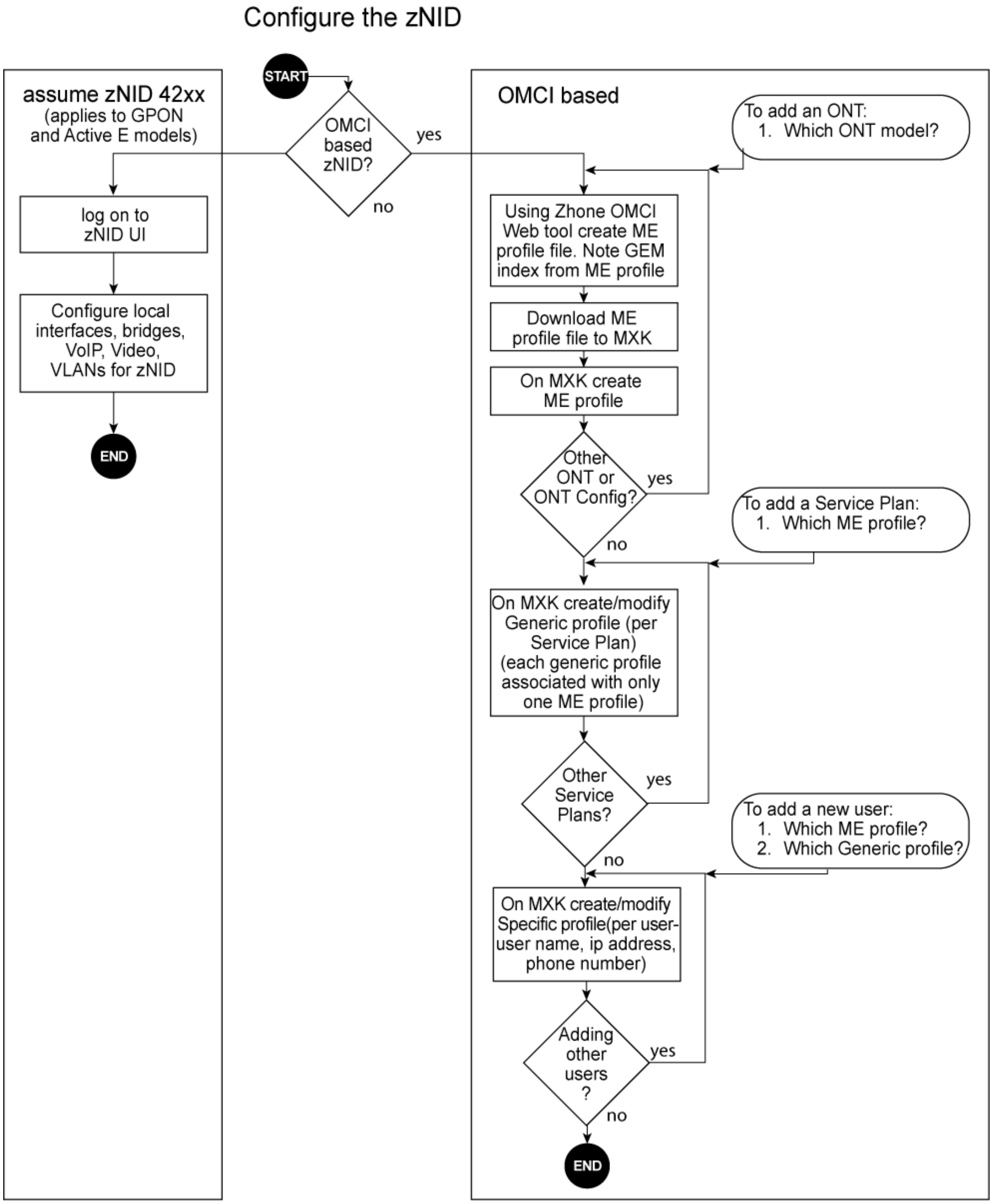
Configuring for GPON and Active Ethernet deployments are fairly similar, though there are some differences. With both you configure the zNID, create any bridge additions, then build the bridges with the bridge add command including the bridge addtions. With Active Ethernet once the zNID is configured and the bridges are built the zNID is on the network and communicating. With GPON you need to create a GPON traffic descriptor (GTP) as well as any of the other bridge additions. after you build the bridges for GPON (both OMCI and browser based) there is another step; you also need to activate the zNIDs, so they will appear to the OLT (in this case, the MXK).


GPON
START
Configure the zNID (or ONT)
Create bridge additions (with GTP)
GPON traffic profiles (added in bridge add command)
DHCP inserts, rate limiting, destination MAC address swapping (added in bridge add command as packet rules)
Configure bridge
May be either uplink/downlink or TLS bridge depending on service
Activate the zNID (Range the ONT to add it to the bridge)
END
Active Ethernet
START
Configure the zNID (or ONT)
Create bridge additions (no GTP)
DHCP inserts, rate limiting, destination MAC address swapping (added in bridge add command as packet rules)
Configure bridge
May be either uplink/downlink or TLS bridge depending on service
END

Differences between OMCI based and browser based solutions

The configuration process for OMCI based and browser based zNIDs are very different. With OMCI you have a profile for configuring models; there is a profile for adding a service plan; there is a profile for adding each user’s zNID. This configuring is done on the MXK, not the zNID itself.

With the browser based solution you configure the device directly via its UI.


Configure the zNID
START
OMCI based zNID?
yes
no
assume zNID 42xx
(applies to GPON and Active E models)
log on to zNID UI
Configure local interfaces, bridges, VoIP, Video, VLANs for zNID
END
OMCI based
To add an ONT:
1. Which ONT model?
Using Zhone OMCI Web tool create ME profile file. Note GEM index from ME profile
Download ME profile file to MXK
On MXK create ME profile
Other ONT or ONT Config?
yes
no
To add a Service Plan:
1. Which ME profile?
On MXK create/modify Generic profile (per Service Plan) (each generic profile associated with only one ME profile)
Other Service Plans?
yes
no
To add a new user:
1. Which ME profile?
2. Which Generic profile?
On MXK create/modify Specific profile(per user-user name, ip address, phone number)
Adding other users ?
yes
no
END

For the browser based zNID we will discuss structured deployment models (*Deploying and managing overview* on page 70).

Note that the activation process steps is only for GPON.

1 Configure the zNID

This step is different depending on whether the zNID is OMCI based or browser based.

OMCI based has you configure and add profiles which allow a structured policies based approach to adding ONT models, selecting their physical interfaces, defining service plans, then adding users. Most of the configuration is done on the OLT; in our examples, the MXK.

The browser based UI provides mechanisms much like a copper based residential gateway.

2. Create the bridge additions which will be used in the next step, the **bridge add** command

   GPON requires some additional information to configure a bridge. The required bridge addition is called a GPON traffic profile, which defines the rate traffic should pass on the connection.

   Other bridge additions, such as rate limiting bridge packet rules may also be added during this step.

3. Add the bridge

   This step creates the bridge interface record(s) which define the bridge.

4. **For GPON deployments only:** Activate the zNID

   This step includes two CLI commands. One to discover the ID of the zNID and one to activate the zNID.

The steps in the above procedure do not necessarily have to be followed in the order given. The GPON zNIDs may be activated prior to configuration or building the bridge on the MXK, however in some instances you may need to reboot or resync the zNID to have it funciton properly on the bridge. The above method eliminates that extra step.

Getting to work

This document is intended to give you hands on experience and information. While it should take less than an hour or two to complete all the scenarios and excercises, it should give you a good start to building your own networks.

Scenario building process

1. Turn up the solution

   This chapter will guide you through the process of setting up the hardware.

2. Build and test OMCI based GPON solutions

   This section will have you build the common residential applications using OMCI based zNIDs:

   - Data
   - Video
   - Voice
   - Triple play (combining data, voice and video)

3. Build and test browser based GPON and Active Ethernet solutions

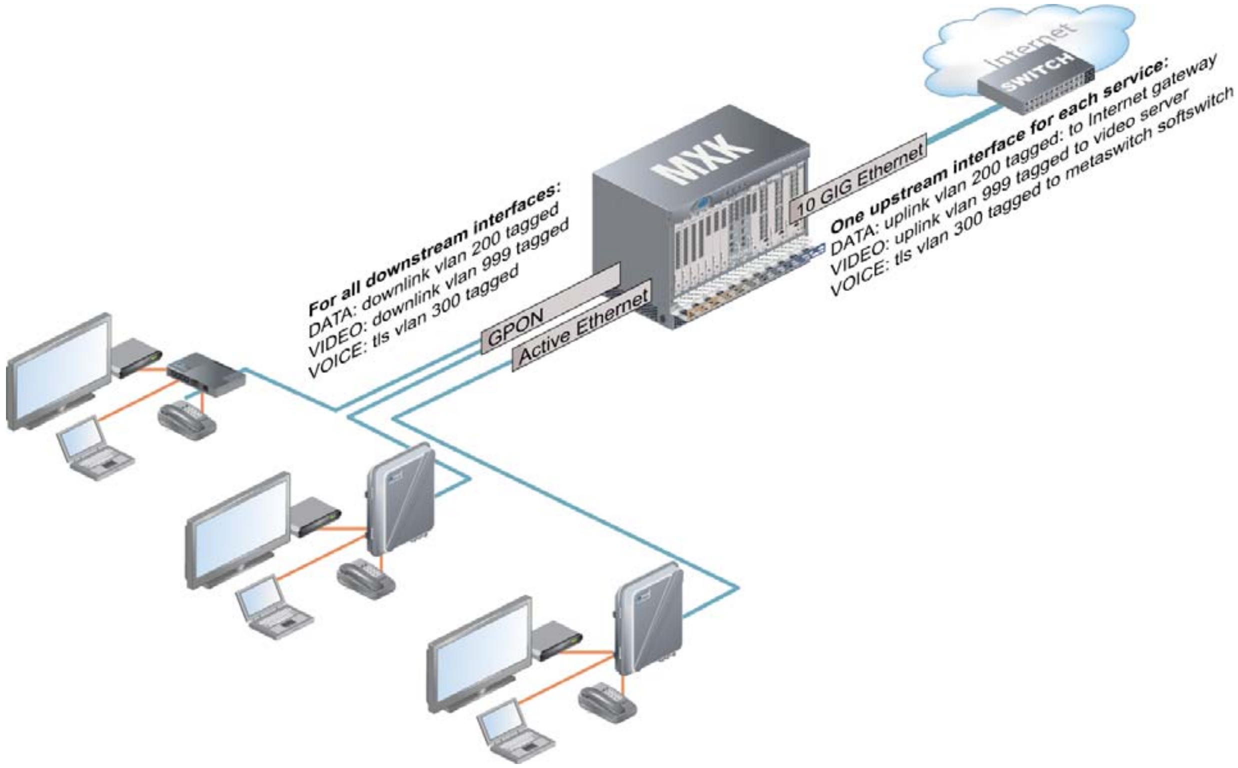
   This section will have you build the common residential applications using browser based zNIDs:

   - Data
   - Video
   - Voice
   - Triple play (combining data, voice and video)

VLANs for the data, video and voice services

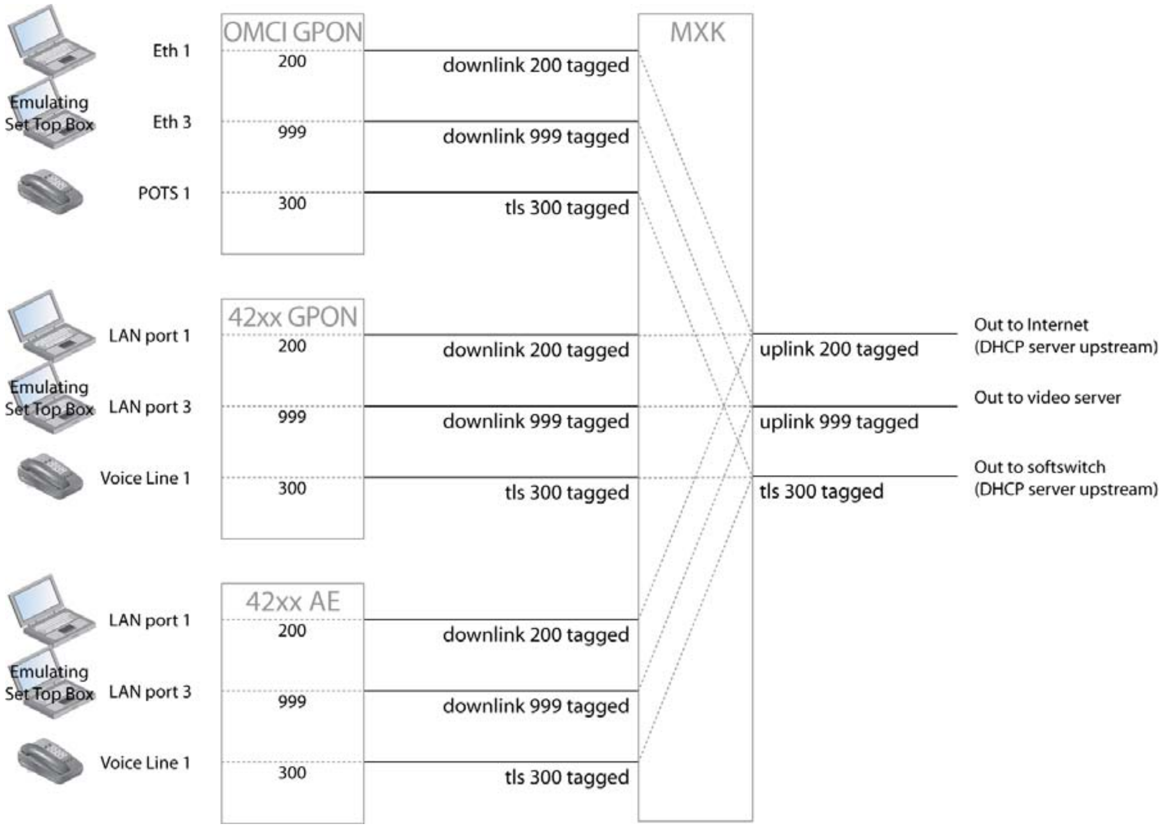
In most networks the voice and video traffic will be separated from data and management traffic in some way, most often with the use of VLANs. Video will be on its own VLAN and voice on its own VLAN. One of the benefits of segregating traffic type by VLAN is securing known traffic. For example, data traffic coming from the public Internet could have originated anywhere and we want to keep that traffic separate from known good traffic that originated inside of the service provider's network such as video traffic which originates from the provider's head end and voice traffic which originates, most likely, from the service provider's soft switch. So separating the video traffic into its own VLAN and voice traffic in its own VLAN means that we can be sure the known traffic is separated out from any unknown traffic.

Figure 3: The zNID supports triple play connected to upstream services


Internet
SWITCH
MXK
10 GIG Ethernet
One upstream interface for each service:
DATA: uplink vlan 200 tagged: to Internet gateway
VIDEO: uplink vlan 999 tagged to video server
VOICE: tls vlan 300 tagged to metaswitch softswitch
For all downstream interfaces:
DATA: downlink vlan 200 tagged
VIDEO: downlink vlan 999 tagged
VOICE: tls vlan 300 tagged
GPON
Active Ethernet

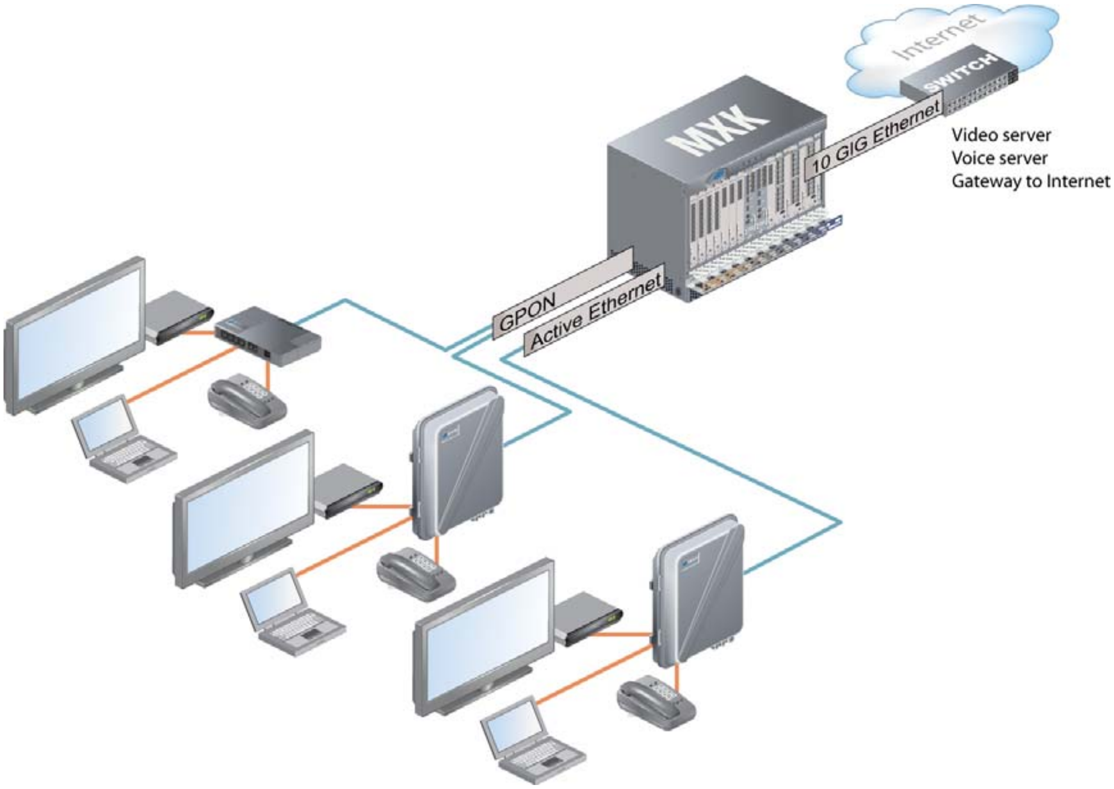
You should note that we are using the same VLAN for data for all three zNIDs discussed in this guide (VLAN 200). We are using the same VLAN for video (VLAN 999) and the same VLAN for Voice (VLAN 300)

Figure 4: Each zNID is using the same VLANs through the OLT (the MXK)



2 TURNING UP YOUR SOLUTION(S)

This chapter is the starting point for building the examples throughout this guide. Regardless of which scenario you build, the fundamentals of getting the solution up to a state where it can be configured are the same. Follow the process as described below which highlights the GPON variation of the installation process of the MXK.



There are two main turn up procedures:

- *Turning up the MXK (the OLT)*
- *Turning up the zNIDs (the ONTs)*

Please see corresponding information in the MXK *Hardware Installation Guide* for graphics and greater detail of the installation instructions (www.zhone.com/support/manuals, then select the MXK MSAP Family link).

Turning up the MXK (the OLT)

Verify the shipment and its contents, then install the MXK. For greater detail on specifics such as how to install cards, or connect power, please follow the directions from the Install the MXK chapter of the MXK *Hardware Installation Guide*.

This procedure highlights the specific configuration for the examples.

1. Install the MXK chassis into the rack.
2. Connect power and provide ground for the chassis.
3. Install the uplink and line cards.
   a. Install the FEGE uplink card.

      The uplink card must always go in slot a. The FEGE uplink cards can be used to create a redundant network ring, however in the examples presented we will not be creating a redundant network ring with two cards. We will use only a single FEGE uplink card in this document.

   b. Install the line cards

      In this example we have put a four port GPON line card in slot 4 of an MXK 819, though you could put it in any open slot of the MXK. If you select a slot other than slot 4 you will need to adjust your commands. When the example uses slot 4, you will need to change to the slot you have selected for the line card.

      We also have installed a dual slot 20 port Active Ethernet card (though it is displayed as one slot in the slots output).
4. Power up the MXK and conduct physical hardware verification tests
   a. Are the chassis power lights on for the power you have connected?

      It is recommended that you have power lines for power supply A and power supply B. If you have both supplying power, both power lights should come on.

   b. Does the FEGE uplink/controller card’s green active light blink, then stay on solid? Since the uplink card is also the controller for the MXK it has boot up software already. You do not need to load a card profile as is required with a line card.

   c. Do the GPON and Active Ethernet line cards’ green active lights blink?

      The amber fault light should stay on upon first start up because there is no line card profile loaded yet, so the card is not active. We will need to install the card profile for the cards.
5. Conduct out of band management tests
   a. Connect to serial port and log in

Connect the special RS232 adapter to the serial port of your PC and use an Ethernet cable to connect between the adapter and craft port of the uplink/controller card with the following settings: 9600bps, 8 data bits, No parity, 1 stop bit, No flow control.

b Log into the system (user name: admin, password: zhone).

c Are all the cards recognized?

Use the **slots** command to display the cards in the slots.

```
zSH> slots

Uplinks
 a:*MXK TWO TENGIGE EIGHT GIGE (RUNNING)
 b: MXK TWO TENGIGE EIGHT GIGE (RUNNING)
Cards
 4: MXK 4 PORT GPON (NOT_PROV)
13: MXK 20 ACT ETH (NOT_PROV)
```

Upon initial start up (or after a set2default command) the line cards need to be provisioned. With a second uplink card as shown here you would need to use a **card add b group 1** command to get the second uplink card to a **running** state.

If all cards are not displayed, be sure the cards are seated properly, then retry the slots command.

6 Connect cables

For the OMCI based solution using the zNID 2510

- We will use port 4 of the GPON card for the downstream interface to the zNID GPON 2510.
- The data port from the zNID GPON 2510 will be ETH 1.
- We will connect a laptop with video set top box STB emulation software on ETH 3 of the zNID GPON 250.
- The voice port from the zNID GPON 2510 will be POTS 1.

For the zNID GPON 4213 and zNID ETH 4212:

- For the GPON browser-based solution, we will use port 1 of the GPON card for the downstream interface to the zNID.
- For the Active Ethernet browser-based solution we will use port 1 of the Active Ethernet card for the downstream interface to the zNID.
- For both the GPON and Active Ethernet scenarios we will connect a laptop to the LAN 2 local port for managing.
- For both the GPON and Active Ethernet scenarios the data port for the subscriber computer will be LAN port 1.
- For both the GPON and Active Ethernet scenarios we will use a PC to emulate a set top box. This PC we will connect to LAN port 3.

– For both the GPON and Active Ethernet scenarios voice will be on VoIP line 1.

See *zNID GPON 4213 and zNID ETH 4212* on page 33 for greater detail.

7. Provision the MXK

   At this point we just need to get the MXK to a running state by loading software to the line cards. The uplink controller card will already have software loaded on it by default.

   Load the card profile

```
zSH> card add 4
zSH> card add 13
```

   Each card (or type of card) has a software binary for that card. The **card add** command with the slot locates the proper binary and loads it on the card.

   If you give the **slots** command you will see the cards loading.

```
Uplinks
 a:*MXK TWO TENGIGE EIGHT GIGE (RUNNING)
 b: MXK TWO TENGIGE EIGHT GIGE (RUNNING)
Cards
 4: MXK 4 PORT GPON (LOADING)
13: MXK 20 ACT ETH (LOADING)
```

   It takes a few minutes for the software to load; a message will be displayed to the CLI upon completion of the loading of the software.

   When the cards are running the slots command will show that it is running. The amber fault lights will go off and the green active lights will go on.

```
Uplinks
 a:*MXK TWO TENGIGE EIGHT GIGE (RUNNING)
 b: MXK TWO TENGIGE EIGHT GIGE (RUNNING)
Cards
 4: MXK 4 PORT GPON (RUNNING)
13: MXK 20 ACT ETH (RUNNING)
```

The rest of the configuration is scenario specific and will be provided in the following chapters:

- *Chapter 3, OMCI based GPON zNID,* on page 43
- *Chapter 4, GPON and Active Ethernet UI based zNID,* on page 67

These two chapters include multiple examples. It is recommended that you follow the building of the examples in a sequential order. The examples are designed to be quick, easily accomplished and demonstrate important fundamentals.

Turning up the zNIDs (the ONTs)

Both zNIDs follow a similar procedure for turn up:

1. Connect to the network
2. Connect power
3. Connect services

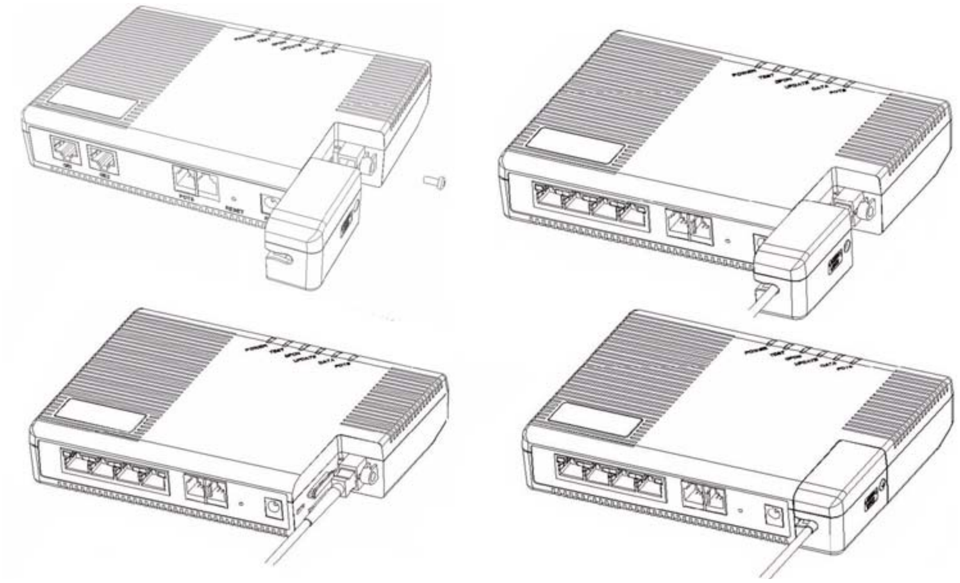
Once the zNIDs are turned up, verify by the LEDs that the zNID has powered up properly

zNID GPON 2510

The zNID GPON 2510 is an indoor model which has GPON as the upstream port. The dowstream ports are four Ethernet ports (10/100) and two POTS ports.

1. Connect to the network

   a. Remove the side screw which holds the laser lock door.



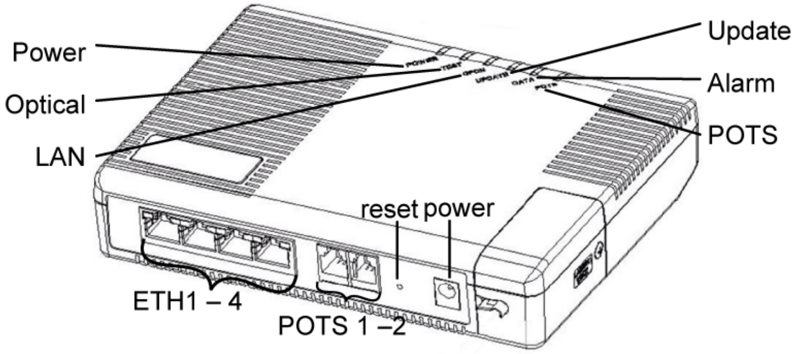
   b. Push the corner of the laser lock door to a 15 degree angle and pull the laser lock door away from the 2510.

   c. Remove the dust covers from the SC/APC optical connectors. Clean the connector if necessary

   d. Plug in the fiber connector to connect the 2510 to the network.

   e. Reattach the laserlock door onto the 2510 and replace the screw which holds the door.

2 Connect power



a Plug the circle two pin 12V DC power connector of power converter to 2510 power port.

b Plug the input of power converter into a live AC outlet.

c Verify that the power (POWER) LED on the 2510 is lit green indicating that local power is on and voltage is good.

3 Connect telephone (POTS) service

a Connect the phone line to a POTS telephone

b Plug the wire pair with RJ-11 connector into one of the 2510 RJ-11 phone jacks.

4 Connect Ethernet service

a Connect a PC with an Ethernet cable

b Plug the Ethernet cable into the ONT RJ-45 Ethernet port.

5 Verify that the zNID has powered up properly

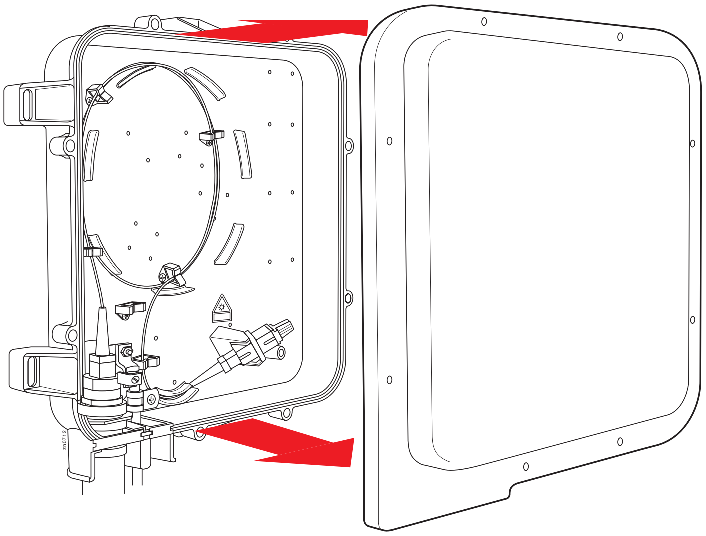
While the zNID is booting the POWER LED should be green and flash.

zNID GPON 4213 and zNID ETH 4212

Both the zNID GPON 4213 and zNID ETH 4212 are outdoor models. The 4213 has a GPON upstream port. Each has 3 Ethernet ports (10/100) and 2 POTS port downstream. Both use the same housing and follow the same installation procedures.

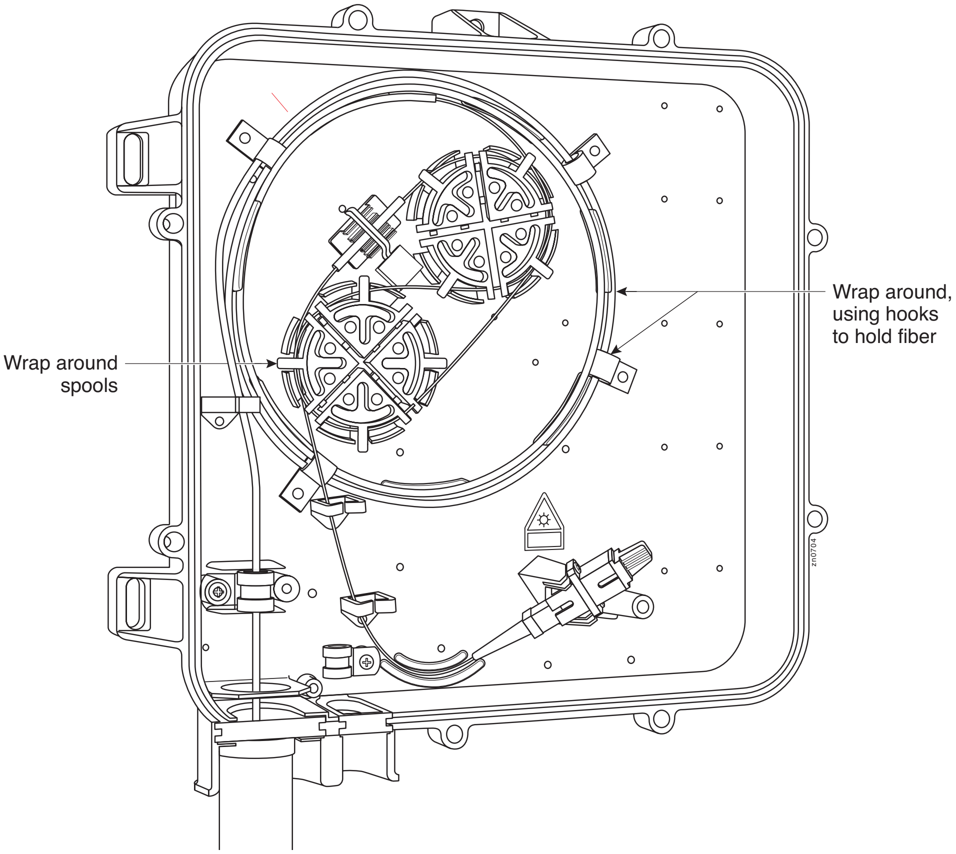
1 Connect to the network

a Remove the fiber tray cover, if necessary, by unscrewing the cover. Then place the cover in a safe location.



The cover may be returned to Zhone.

b Pull the fiber up into the fiber tray through the rubber grommets in the fiber entry point.

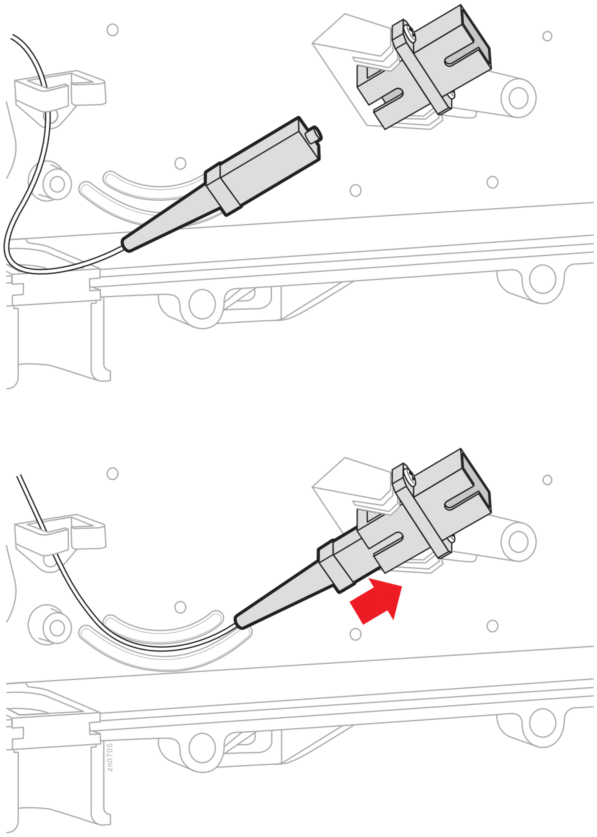


c Run the fiber through the fiber holder and tighten the holder to secure the fiber.

d Wrap the cable around the fiber spools.

Hooks may be adjusted to align the fiber with the fiber guides.

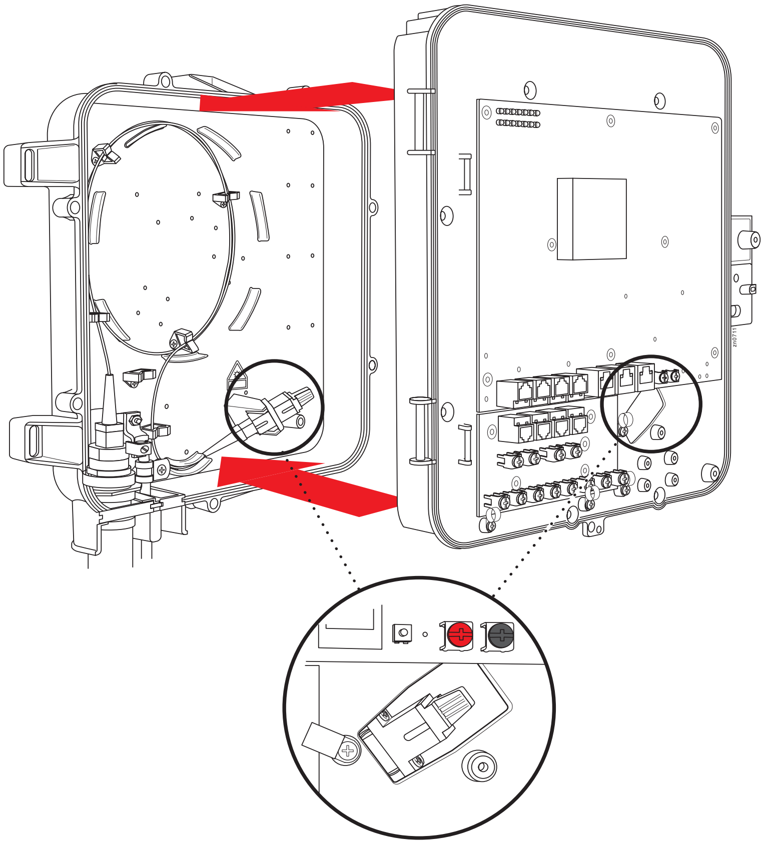
e Place SC connector end of fiber segment in SC adaptor.



f Line up the screw holes of the electronics enclosure with the screw holes of the fiber tray (eight holes).

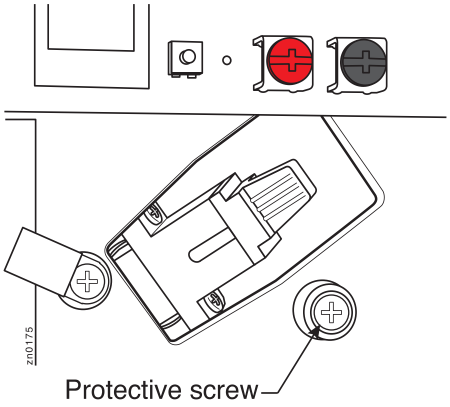
g Insert screws.

h Line up the holes for the SC connector on both the fiber tray and the electronics enclosure.



i Tighten screws.

j Insert and tighten the protective screw next to the SC connector to prevent the enclosure from being removed while the fiber is still connected.

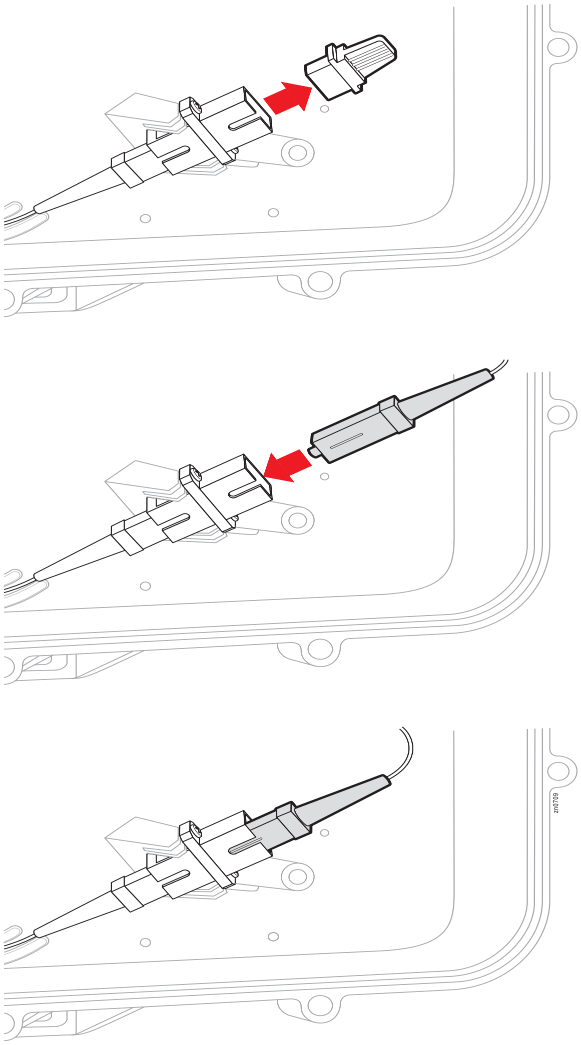


Note: Removing the electronics enclosure when the fiber is connected could break the fiber.

k Connect the SC connector.

WARNING! Risk of eye damage. At all times when handling optical fibers, follow the safety procedures recommended by your company.

Although Zhone optical products have a Class I certification, hazardous exposure to laser radiation can occur when fibers are connected, disconnected or broken. Handling of optical fibers without dust caps increases the risk of exposure. Exposure to either visible or invisible laser light can damage your eyes under certain conditions.

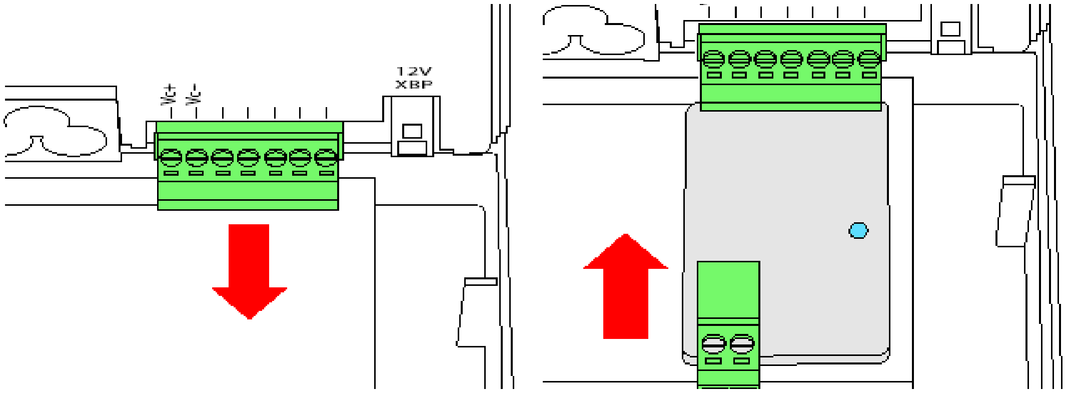


Note: This tray shows a typical fiber placement. Fiber wrapping may differ, depending on installation needs.

Caution: To prevent damage to the system, use only the screws provided in the installation kit.

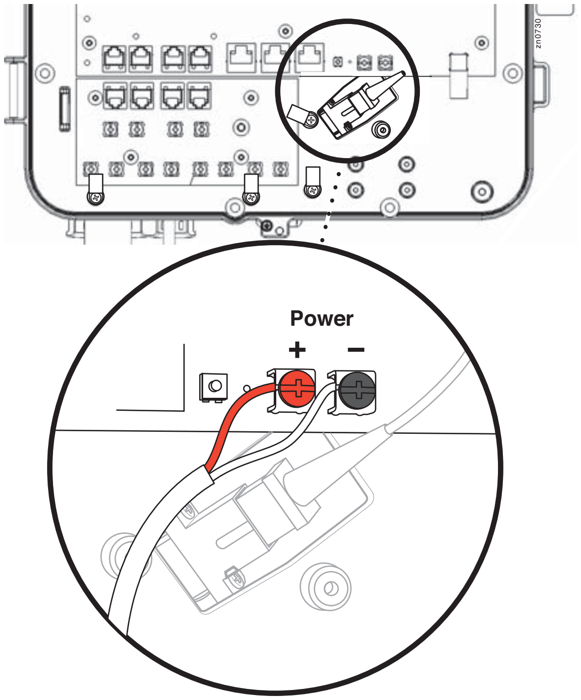
2 Connect power

a Remove the 7-wire battery alarm connector on the battery backup unit (BBU), then replace the 7-wire battery alarm connector with the 2-wire battery backup board shipped with the zNID.



b Connect the battery wires from the zNID to the BBU.

Make sure that the red wire is connected to “Vo +” and the white wire is connected to “Vo –”. If not an APC model, be sure to connect the correct wires to the + and - on the BBU.

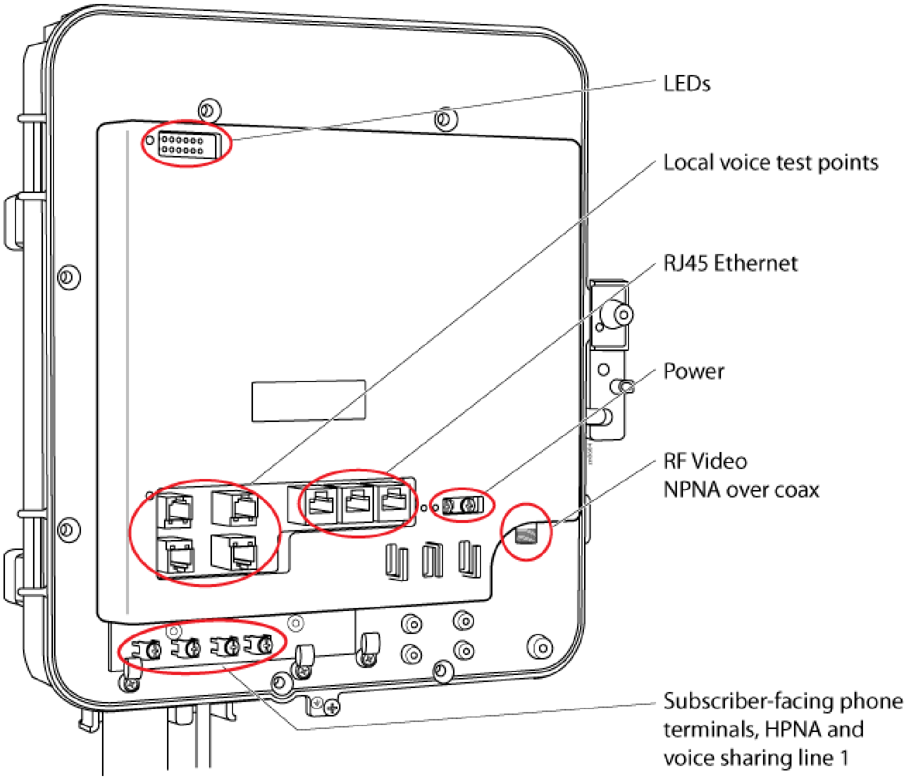


c Power up the BBU by plugging in the AC power.

3 Connect telephone (POTS) service

The zNID provides two phone lines. Line one can be used to provide both HPNA and POTS to deliver phone service and any packet services including IPTV, data, and VoIP. Line 2 is used to provide POTS service

For the FTTH Application Guide we will use Voice Line 1.



For our lab scenario we are going to connect data and video to one of the Ethnernet lines rather than connecting HPNA over the POTS line. We will connect a phone to the POTS port.

The zNID 42xx series is designed to support either RJ-11 connectors or individual tip ring lines. For the application guide we will describe connecting RJ-11.

a Provide a POTS telephone with RJ-11 cable attached.

b Remove the connector from the upper RJ-11 voice port.

c Attach the RJ-11 connector from the phone to the open voice port.

Note which telephone port as we will configure that port for VoIP in *Chapter 4, GPON and Active Ethernet UI based zNID*.

4 Connect Ethernet service

The zNID provides three RJ 45s for Ethernet connections. Ethernet connections can be used to deliver any packet services including IPTV, data, and VoIP.

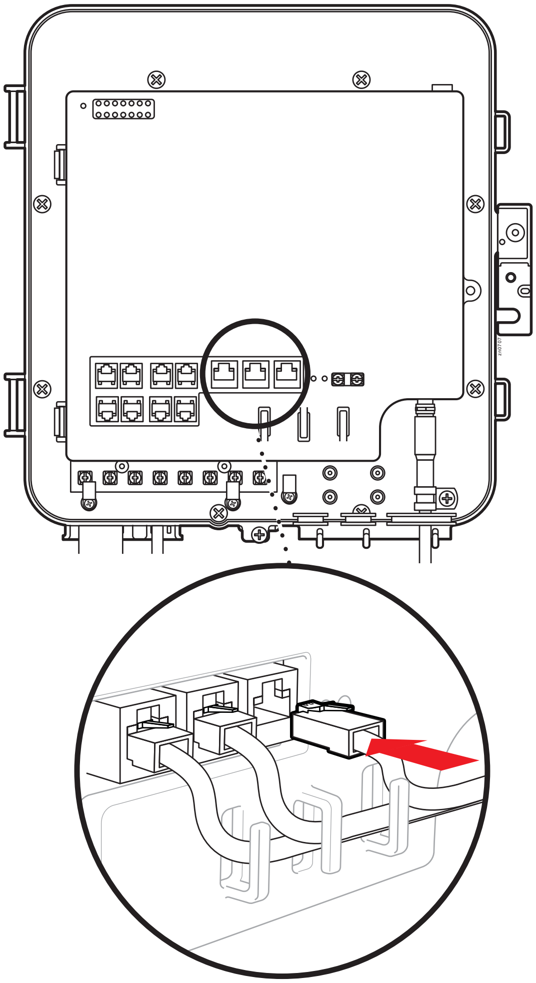
a Connect a Category 5 or a Category 6 cable to an RJ45 interface as shown in Figure 5.

For the FTTH Application Guide scenario we will connect the local port to LAN 2 for managing. The data port for the computer will be LAN port 1.

For the PC we will be using to emulate a set top box we will connect to LAN port 3.

Note: For wire management, it is recommended that the wire wraps around the wire management hooks from left to right.

Figure 5: Connect Ethernet port



b Note which LAN port you have connected.

Troubleshooting the turn-up procedures

Table 2: Troubleshooting turn up issues

Symptom	Discussion

Long boot-up time/long time loading software	It takes a few minutes for the software to load, but a message will be displayed to the CLI upon completion of the loading of the software.
	While the card is loading you can give the **bootstate 5** command, where “5” is the slot of the card. Normally you would not use the bootstate command, but it is a mechanism to verify that the MALC is still loading the card.
	Some parts of the boot up process take longer than others. “Loading Image over backplane” may
	`zSH> bootstate 5`
	`Boot State: Loading Image over backplane`
	`zSH> bootstate 5`
	`Boot State: BootMgr: In Application Start Gate: 7`
	`zSH> bootstate 5`
	`Boot State: BootMgr: In Application Start Gate: 14`
	`MAR 26 00:46:34: notice : 1/1/12  : shelfctrl: Card in slot 4 changed state to RUNNING.`

Cards do not appear in slots command	Reseat the card and watch for the activity lights on the card for start up. If you are sure you have the card seated properly and the activity lights go through their startup process, but you still do not see the card displayed in the slots command output, contact Zhone technical support If you reseat the card and do not see any activity lights, verify that the card is properly in its slot. If it is properly in the slot but there is no activity light, contact Zhone technical support.

3 OMCI BASED GPON ZNID

These examples are designed to be accomplished in a minimum amount of time and provide a foundation for understanding other important network edge access concepts.

Topics to be covered in this chapter:

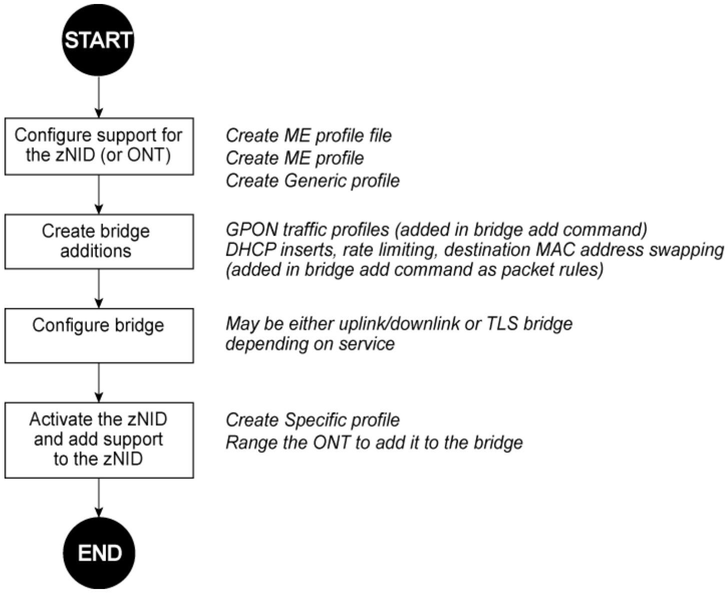
Overview of the configuration process

In this chapter we will talk about how to provision ONTs (or zNIDs) that require OMCI for configuring data, voice and video services. You can learn the latest supported OMCI based GPON zNID models by using the Smart OMCI web tool. How to use this tool will be described in this chapter.

In this chapter we will use ZNID-GPON-2510 as an example, and configure the triple play services one at a time.

The following flowchart covers the overall procedure to provisioning OMCI based zNID.

Figure 6: Overview of the OMCI based GPON zNID configuration process


START
Configure support for the zNID (or ONT)
Create ME profile file
Create ME profile
Create Generic profile
Create bridge additions
GPON traffic profiles (added in bridge add command)
DHCP inserts, rate limiting, destination MAC address swapping (added in bridge add command as packet rules)
Configure bridge
May be either uplink/downlink or TLS bridge depending on service
Activate the zNID and add support to the zNID
Create Specific profile
Range the ONT to add it to the bridge
END

For the detail configuration procedure of each step shown in the Figure 6, see below:

— The step of *Configure support for the zNID* is described in *Create Supports for zNID* on page 48.

— The rest of steps in the overall flowchart are described in following application sections:

Create High Speed Internet on GPON OMCI with Uplink and Downlink on page 55

Create Video Bridge on GPON OMCI with Uplink and Downlink on page 61

Create VoIP on GPON OMCI with TLS bridges on page 63

Here are brief descriptiond of each step:

- Configure the supports for zNID (or ONT)

  In this step, we will create an ME profile file and an ME profile for the selected ONT model, and create a Generic profile for desired service plans.

The Specific profile will be created on ONT in the last step at the bottom of the flowchart, *Activate the zNID and add support to the zNID*.

Once the OMCI profiles are created, if you have similar scenario in other MXKs, you can share the OMCI profile between MXKs by using the **gpononu profiles export me|gen|spec** and **gpononu profiles import me|gen|spec** commands.

- Create bridge additions

  Bridge additions include GPON traffic profile (GTP) and packet rule. A GPON traffic profile is added in the **bridge add** command for ONT GEM port; packet rules are also added in the **bridge add** command, such as DHCP insert, rate limiting, destination MAC address swapping.

  In this example, we will only describe how to create GPON traffic profile. GPON traffic profile could be used to prioritize traffic in service-based order. You can specify guaranteed upstream bandwidth and traffic class for different services in the GTP:

  – For high speed data service, you might consider specifying a higher upstream bandwidth than you would for voice and video. The minimum bandwidth 512 kbps is recommended for voice and video services.

  – Voice and video services need a constant and guaranteed cell rate during the lifetime of the connection, so traffic class CBR would be appropriate for those GEM ports running voice and video services. UBR would be appropriate for delay-tolerant or non-real-time application, such as data service.

- Configure bridge

  The bridge type we build depends on the service (data, video, or voice). For the data and video services we will use asymmetric bridges (uplink, downlink bridges).

  For the voice service we will use a TLS bridge. No matter which VoIP protocol, TLS bridges are better suited for downstream initiated calls, because in the worst case scenario you will always be able to get the MAC address of the VoIP supplying access device (in this case the zNID).

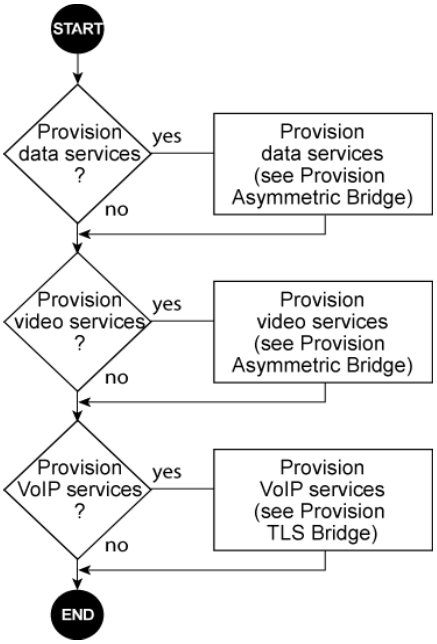
  If there is no activity on the VoIP bridge, then the MAC address of the VoIP supplying access device will eventually timeout the MAC address of the VoIP in the bridge forwarding table. Unlike the downlink of an asymmetric bridge, the TLS bridge will flood all the bridge interfaces of the TLS VoIP VLAN and rediscover the VoIP supplying access device.

- Activate the zNID and add support to the zNID.

  Make sure to provision the logical connections for data, video, and voice services in the MXK and ONTs before activating the ONTs in order to avoid having to re-sync or reboot the ONUs eventually.

  In this step we will create Specific profile on the zNID, and then activate the zNID.

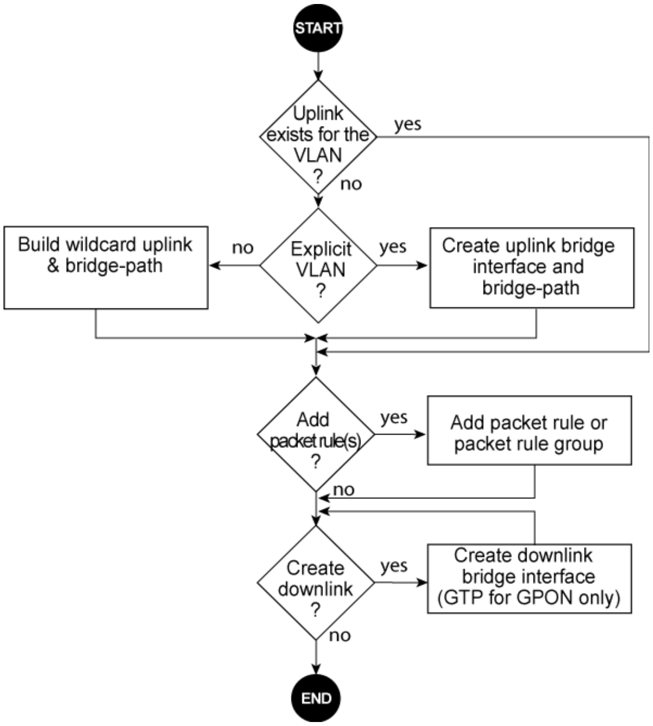
Figure 7: Configuring bridges by service type


START
Provision data services ?
yes
Provision data services (see Provision Asymmetric Bridge)
no
Provision video services ?
yes
Provision video services (see Provision Asymmetric Bridge)
no
Provision VoIP services ?
yes
Provision VoIP services (see Provision TLS Bridge)
no
END

The asymmetric bridge types include downlink, uplink, and intralink bridge interfaces. The intralink bridge interface type is used for subtending other MXKs, MALCs, MALC XPs, or Raptor XPs from the MXK via Active Ethernet cards. We will not talk about subtending devices in this chapter, so intralink bridge will not be discussed.

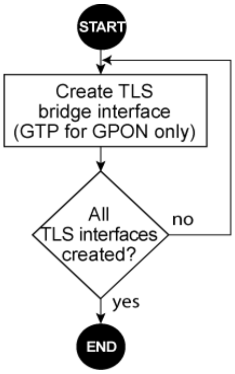
The uplink/downlink bridges we will build in this chapter are all based on specific VLANs — VLAN 100 for the data bridge and VLAN 999 for the video bridge. VLAN 100 is a gateway to the internet. VLAN 999 has a head-end video server.

Figure 8: Configuring asymmetric bridges for GPON


START
Uplink exists for the VLAN ?
yes
no
Explicit VLAN ?
no
yes
Build wildcard uplink & bridge-path
Create uplink bridge interface and bridge-path
Add packet rule(s) ?
yes
no
Add packet rule or packet rule group
Create downlink ?
yes
no
Create downlink bridge interface (GTP for GPON only)
END

We will use VLAN 300 for the VoIP bridge.

Figure 9: Configuring TLS bridge for GPON


START
Create TLS bridge interface (GTP for GPON only)
All TLS interfaces created?
no
yes
END

The behavior of the TLS bridge is better suited for the downstream initiated calls because the TLS VoIP bridge (VLAN 300 in our example) will be flooded with a request for the MAC address of the VoIP access device if the MAC address is timed out from the MXK’s forwarding table.

Create Supports for zNID

This procedure describes the creation of the ME profile file, the ME profile, and the Generic profile. In normal deployment you will create profiles for the ONT models and the service plans in initial deployment and seldom afterward, unless you want to add a new ONT model or define another service plan.

Adding OMCI support to each user's zNIDs by creating Specific profile will be covered in the application procedures.

For each application we will assume that the ME profile and Generic profile are configured and in place. In other words for each application we will begin with adding a new user, which is where you would normally begin in a normal deployment effort.

☑ **Note:** Each user's zNID may have only one ME profile, however, as a service provider, you may have multiple ME profiles for a zNID model for different deployments.

For ease of deployment it is recommended that you have a separate ME file only for different physical port configurations. For example, with the zNID 2510 which has four Ethernet ports and two POTS ports, if you want to have triple-play services, you may always have the POTS ports selected for voice service, but since the Ethernet ports may be either data or video ports you might have an ME profile which has one data and three video ports configured (a likely residential scenario). You may also have a scenario where you have three data ports and one video ports, or all data ports. In each scenario you would have a separate ME configuration file. In the deployment process you would associate the ME profile with the service plan.

For ME profiles which have all ports designated, such as the three video, one data configuration residential scenario described above, you could configure the service plan (Generic profile) to only use some of the ports.

Creating ME profile file for ONT

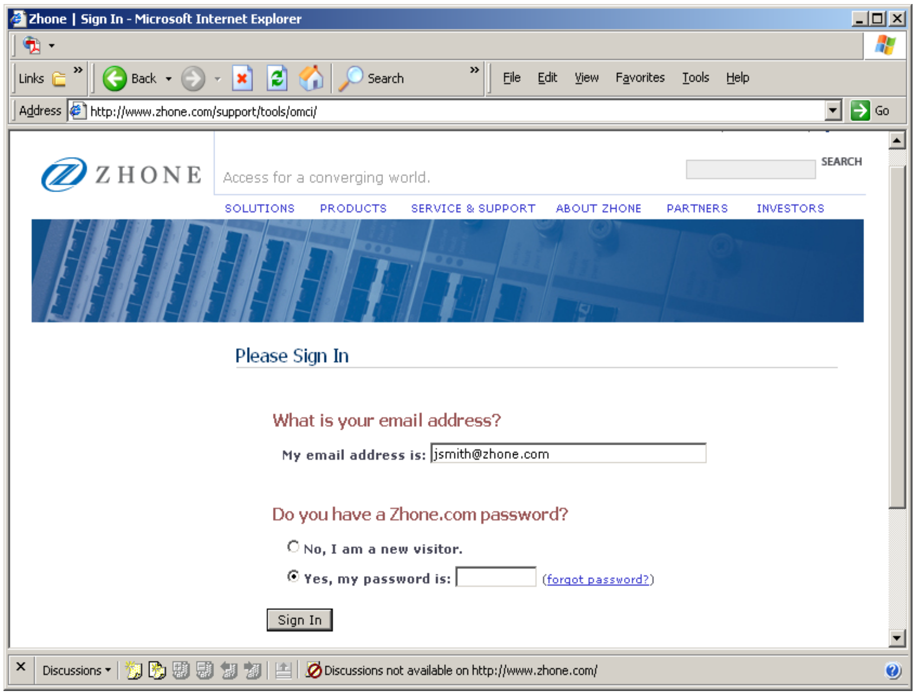
Create ME profile file with Zhone Smart OMCI web tool:

If you are adding a new ONT you would start at this point.

1. Navigate to the Zhone website at “http://www.zhone.com/support/tools/omci/”.

2. Access the website by entering the email address and the password selected at registration.

   Note: skip this step if you are already signed in.


Zhone | Sign In - Microsoft Internet Explorer
Links
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
http://www.zhone.com/support/tools/omci/
Go
ZHONE
Access for a converging world.
SEARCH
SOLUTIONS
PRODUCTS
SERVICE & SUPPORT
ABOUT ZHONE
PARTNERS
INVESTORS
Discussions
Discussions not available on http://www.zhone.com/

Please Sign In

What is your email address?

My email address is: jsmith@zhone.com

Do you have a Zhone.com password?

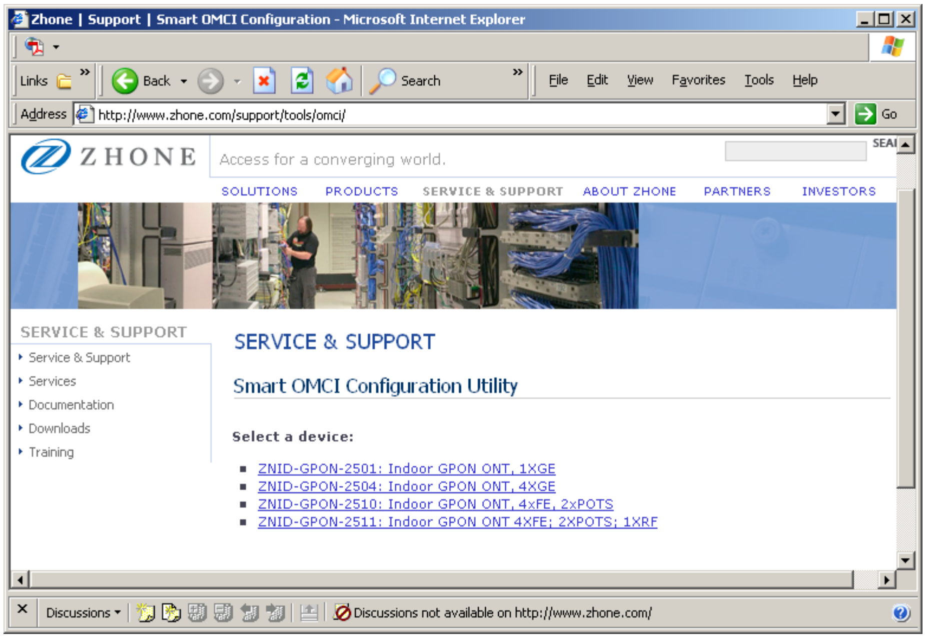
○ No, I am a new visitor.

● Yes, my password is: (forgot password?)

Sign In

3 Select ONT model.

In this example, we select ZNID-GPON-2510.



SERVICE & SUPPORT

Smart OMCI Configuration Utility

Select a device:

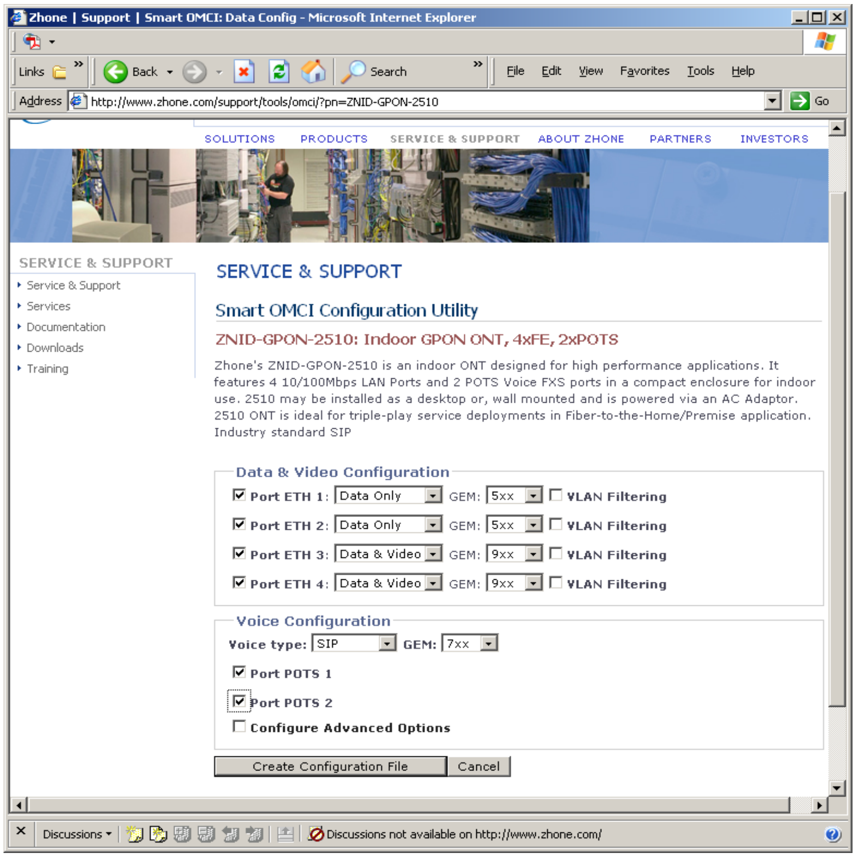
- ZNID-GPON-2501: Indoor GPON ONT, 1XGE
- ZNID-GPON-2504: Indoor GPON ONT, 4XGE
- ZNID-GPON-2510: Indoor GPON ONT, 4xFE, 2xPOTS
- ZNID-GPON-2511: Indoor GPON ONT 4XFE; 2XPOTS; 1XRF

4 Select the ports on the ONT for data, video and/or voice and associated GEM index.

This example creates GEM port ID 5xx for data service on port eth1 and eth2, GEM port ID 7xx for voice service on port POTS1 and POTS2, GEM port ID 9xx for video service on port eth3 and eth4.

Note: Take a note of the ports and GEM index you selected for different service.

They are required later when you provisioning services on bridges.



SERVICE & SUPPORT

Smart OMCI Configuration Utility

ZNID-GPON-2510: Indoor GPON ONT, 4xFE, 2xPOTS

Zhone's ZNID-GPON-2510 is an indoor ONT designed for high performance applications. It features 4 10/100Mbps LAN Ports and 2 POTS Voice FXS ports in a compact enclosure for indoor use. 2510 may be installed as a desktop or, wall mounted and is powered via an AC Adaptor. 2510 ONT is ideal for triple-play service deployments in Fiber-to-the-Home/Premise application. Industry standard SIP

Data & Video Configuration

☑ Port ETH 1: Data Only GEM: 5xx □ VLAN Filtering

☑ Port ETH 2: Data Only GEM: 5xx □ VLAN Filtering

☑ Port ETH 3: Data & Video GEM: 9xx □ VLAN Filtering

☑ Port ETH 4: Data & Video GEM: 9xx □ VLAN Filtering

Voice Configuration

Voice type: SIP GEM: 7xx

☑ Port POTS 1

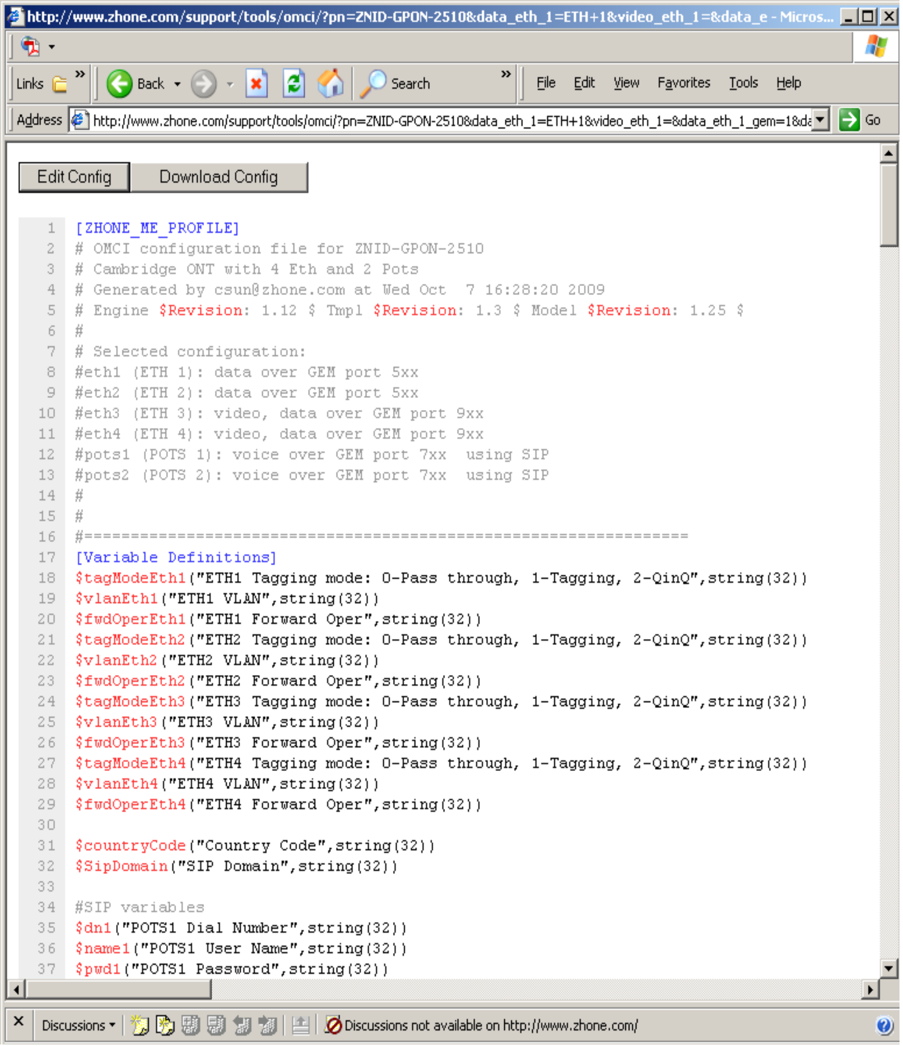
☑ Port POTS 2

□ Configure Advanced Options

Create Configuration File | Cancel

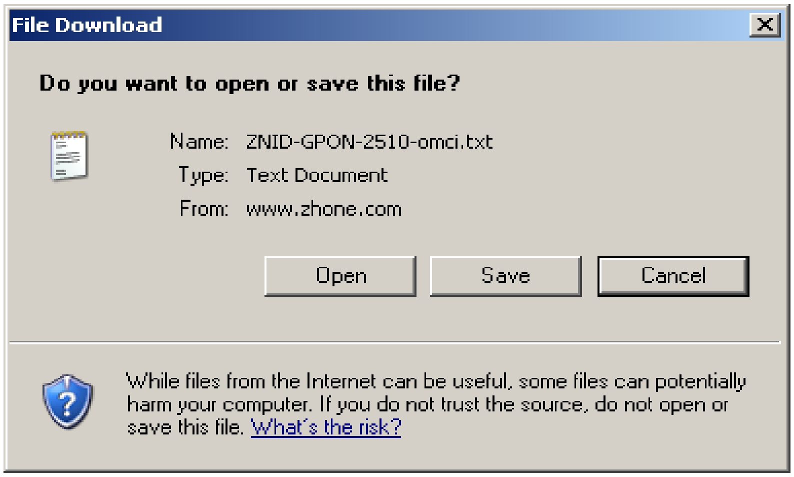
VLAN filtering is an optional field. After selecting VLAN Filtering, you can specify how many VLANs the ONT can filter on the LAN facing ports. And later in the Generic profile or Specific profile, you can assign the VLAN IDs for those VLAN filters.

5 Click **Create Configuration File** button to create an ME profile file.


http://www.zhone.com/support/tools/omci/?pn=ZNID-GPON-2510&data_eth_1=ETH+1&video_eth_1=&data_e - Micros...
Links
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
http://www.zhone.com/support/tools/omci/?pn=ZNID-GPON-2510&data_eth_1=ETH+1&video_eth_1=&data_eth_1_gem=1&da
Go
Edit Config
Download Config
Discussions
Discussions not available on http://www.zhone.com/

```
[ZHONE_ME_PROFILE]
# OMCI configuration file for ZNID-GPON-2510
# Cambridge ONT with 4 Eth and 2 Pots
# Generated by csun@zhone.com at Wed Oct  7 16:28:20 2009
# Engine $Revision: 1.12 $ Tmpl $Revision: 1.3 $ Model $Revision: 1.25 $
#
# Selected configuration:
#eth1 (ETH 1): data over GEM port 5xx
#eth2 (ETH 2): data over GEM port 5xx
#eth3 (ETH 3): video, data over GEM port 9xx
#eth4 (ETH 4): video, data over GEM port 9xx
#pots1 (POTS 1): voice over GEM port 7xx  using SIP
#pots2 (POTS 2): voice over GEM port 7xx  using SIP
#
#
#=================================================================
[Variable Definitions]
$tagModeEth1("ETH1 Tagging mode: 0-Pass through, 1-Tagging, 2-QinQ",string(32))
$vlanEth1("ETH1 VLAN",string(32))
$fwdOperEth1("ETH1 Forward Oper",string(32))
$tagModeEth2("ETH2 Tagging mode: 0-Pass through, 1-Tagging, 2-QinQ",string(32))
$vlanEth2("ETH2 VLAN",string(32))
$fwdOperEth2("ETH2 Forward Oper",string(32))
$tagModeEth3("ETH3 Tagging mode: 0-Pass through, 1-Tagging, 2-QinQ",string(32))
$vlanEth3("ETH3 VLAN",string(32))
$fwdOperEth3("ETH3 Forward Oper",string(32))
$tagModeEth4("ETH4 Tagging mode: 0-Pass through, 1-Tagging, 2-QinQ",string(32))
$vlanEth4("ETH4 VLAN",string(32))
$fwdOperEth4("ETH4 Forward Oper",string(32))

$countryCode("Country Code",string(32))
$SipDomain("SIP Domain",string(32))

#SIP variables
$dn1("POTS1 Dial Number",string(32))
$name1("POTS1 User Name",string(32))
$pwd1("POTS1 Password",string(32))
```

6 Click **Download Config** button to download the ME profile file



Do you want to open or save this file?

Name: ZNID-GPON-2510-omci.txt

Type: Text Document

From: www.zhone.com

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Creating ME profile for selected ONT model

Create ME profile on MXK:

1 Import the ME profile file to the MXK.

  a Create a directory on the MXK for ME profile file if one doesn’t exist.

```
zSH> mkdir /me
```

  b Download the ME profile file to the directory using the **file download** command.

  This example downloads the ME profile file *ZNID-GPON-2510-omci.txt* from source location 182.16.80.201 to the destination location *me* directory in the MXK, and renames it to *2510-me1.txt*.

```
zSH> file download 182.16.80.201 /
ZNID-GPON-2510-omci.txt /me/2510-me1.txt
Bytes copied 16397
File download successful
```

2 On MXK create and verify the ME profile.

  a Create an ME profile with the ME profile file (2510-me1).

```
zSH> gpononu profiles create me 2510-config1 /me/
2510-me1.txt
Profile created
```

  b To verify the newly created ME profile, enter:

```
zSH> gpononu profiles show me
2510-config1
```

Creating Generic profile for service plan

Create Generic profile on MXK:

If you want to add a new service plan you would start at this point.

1 On MXK create and modify Generic profile for the service plan, based on the ME profile (2510-config1).

```
zSH> gpononu profiles create gen 2510-service-plan1
2510-config1
Profile created
```

2 Update the Generic profile.

To assign or change a parameter, enter the line number, click Enter, then enter the value, at last enter **s** to save the profile.

Make sure to specify value to all the service plan related variables in the Generic profile. If there is no default or other value given for a variable, configuration will fail for this ONT when you are activating the ONT unless updates to the Generic profile or Specific profile to provide a value.

```
zSH> gpononu profiles update gen 2510-service-plan1
Generic Profile: 2510-service-plan1
   1  "ETH1 Tagging mode: 0-Pass through, 1-Tagging,
2-QinQ"
   2  "ETH1 VLAN (VID or COS,VID)"
   3  "ETH1 Forward Oper"
   4  "ETH2 Tagging mode: 0-Pass through, 1-Tagging,
2-QinQ"
   5  "ETH2 VLAN (VID or COS,VID"
   6  "ETH2 Forward Oper"
   7  "ETH3 Tagging mode: 0-Pass through, 1-Tagging,
2-QinQ"
   8  "ETH3 VLAN (VID or COS,VID"
   9  "ETH3 Forward Oper"
  10  "ETH4 Tagging mode: 0-Pass through, 1-Tagging,
2-QinQ"
  11  "ETH4 VLAN (VID or COS,VID"
  12  "ETH4 Forward Oper"
  13  "Country Code"
  14  "POTS1 Dial Number"
  15  "POTS1 User Name"
  16  "POTS1 Password"
  17  "POTS2 Dial Number"
  18  "POTS2 User Name"
  19  "POTS2 Password"
  20  "VOICE VLAN"
  21  "SIP Proxy IP"
  22  "SIP Host IP Option: 2-static, 3-DHCP"
  23  "SIP Host IP"
  24  "SIP Netmask"
  25  "SIP Gateway"
  26  "SIP Domain"
  27  "ETH 1 Admin Status: 0-Up, 1-Down"
  28  "ETH 2 Admin Status: 0-Up, 1-Down"
  29  "ETH 3 Admin Status: 0-Up, 1-Down"
  30  "ETH 4 Admin Status: 0-Up, 1-Down"
  31  "POTS 1 Admin Status: 0-Up, 1-Down"
  32  "POTS 2 Admin Status: 0-Up, 1-Down"
Enter OMCI edit command or [s]ave, [q]uit, [h]elp:h

Available Commands:
   E    - display edit data (short)
   H    - display help
   L    - display edit data (long)
   Q    - quit without save
   S    - save and exit
   1..n - edit variable #n
```

```
Enter OMCI edit command or [s]ave, [q]uit, [h]elp:1
Enter value: 1
Enter OMCI edit command: 2
Enter value: 100
Enter OMCI edit command: 3
Enter value: 1
Enter OMCI edit command: 4
Enter value: 1
...
Enter OMCI edit command: s
GENERIC profile has been saved
```

Create High Speed Internet on GPON OMCI with Uplink and Downlink

The High Speed Internet application uses uplinks and downlinks with a VLAN. You should notice from the flowchart and procedures that provisioning video also uses uplink/downlink bridge configuration, just the GEM port setup (from the OMCI profile), GTP and VLAN are different. For triple play services (As long as the OMCI profiles are configured properly) you can add the video bridge or VoIP bridge in the same process. For ease of discussion each of the applications is described separately in this chapter.

For data service we will create uplink/downlink bridges with VLAN 100.

Creating GPON Traffic Profile

GPON traffic profiles are a template for defining how traffic will be handled on the bridge with which the GTP is associated. GTPs are templates in that one GTP may be associated with many different bridges. The GTP in this procedure will create a high bandwidth configuration. The GTP defines how the traffic will be handled. GTPs may be used for multiple bridge configurations.

The following is recommended for high speed data configurations.

```
zSH> new gpon-traffic-profile 1
gpon-traffic-profile  1
Please provide the following: [q]uit.
guaranteed-upstream-bw: ->  {0}: 1024
traffic-class: ---------->  {ubr}:
compensated: ------------>  {false}:
shared: ----------------->  {false}:
dba-enabled: ------------>  {false}:
dba-fixed-us-ubr-bw: ---->  {0}:
dba-fixed-us-cbr-bw: ---->  {0}:
dba-assured-us-bw: ------>  {0}:
dba-max-us-bw: ---------->  {0}:
dba-extra-us-bw-type: --->  {nonassured}:
....................
Save new record? [s]ave, [c]hange or [q]uit: s
```

ubr is the default value

```
New record saved.
```

Creating uplink and downlink bridge

We will create an uplink and downlink bridge for VLAN 100:

1 Create the uplink bridge interface

a Add the bridge interface for the uplink.

Make sure VLAN ID matches the VLAN ID you assigned for data service in the Generic Profile. This example, data services uses VLAN 100.

```
zSH> bridge add 1-a-5-0/eth uplink vlan 100
Adding bridge on 1-a-5-0/eth
Created bridge-interface-record ethernet5/bridge
```

b Add the bridge-path for the uplink:

```
zSH> bridge-path add ethernet5/bridge vlan 100 default
Bridge-path added successfully

zSH> bridge-path show
VLAN/SLAN   Bridge                            Address
--------------------------------------------------------------------
       100 ethernet5/bridge                    Default
```

2 Create downlink bridge interface

Uses the GEM index assigned in the Smart OMCI web tool to calculate the GEM port ID with the following formula:

GEM port ID = GEM index + ONU ID

This example uses GEM index 5xx for data service, and ONT ID is 4/4/**1**, so the GEM port ID is 501.

```
zSH> bridge add 1-4-4-501/gponport gtp 1 downlink vlan 100 tagged
GEM Port 1-4-4-501/gponport has been created on ONU 1-4-4-1/gpononu.
Adding bridge on 1-4-4-501/gponport
Created bridge-interface-record 1-4-4-501-gponport-100/bridge
```

Creating Specific profile for new user

On MXK create and modify Specific profile for each user; in the case of specific profiles, the OMCI supports are associated with the ONT.

Only one Specific profile can be added on an ONT.

If you are adding a new user you would start at this point.

1 Create and modify Specific profile.

a Create the Specific profile, selecting the ME profile and Generic profile to associate with the Specific (user) profile.

```
zSH> gpononu profiles create spec 4/4/1
2510-config1 2510-service-plan1
Profile created
```

b Update Specific profile.

```
   zSH> gpononu profiles update spec 4/4/1
Specific Profile: 4/4/1
   1  "ETH1 Tagging mode: 0-Pass through, 1-Tagging,
2-QinQ"
   2  "ETH1 VLAN"
   3  "ETH1 Forward Oper"
   4  "ETH2 Tagging mode: 0-Pass through, 1-Tagging,
2-QinQ"
   5  "ETH2 VLAN"
   6  "ETH2 Forward Oper"
   7 "ETH3 Tagging mode: 0-Pass through, 1-Tagging,
2-QinQ"
   8  "ETH3 VLAN"
   9  "ETH3 Forward Oper"
  10  "ETH4 Tagging mode: 0-Pass through, 1-Tagging,
2-QinQ"
  11  "ETH4 VLAN"
  12  "ETH4 Forward Oper"
  13  "Country Code"
  14  "POTS1 Dial Number"
  15  "POTS1 User Name"
  16  "POTS1 Password"
  17  "POTS2 Dial Number"
  18  "POTS2 User Name"
  19  "POTS2 Password"
  20  "VOICE VLAN"
  21  "SIP Proxy IP"
  22  "SIP Host IP Option: 2-static, 3-DHCP"
  23  "SIP Host IP"
  24  "SIP Netmask"
  25  "SIP Gateway"
  26  "SIP Domain"
  27  "ETH 1 Admin Status"
  28  "ETH 2 Admin Status"
  29  "ETH 3 Admin Status"
  30  "ETH 4 Admin Status"
  31  "POTS 1 Admin Status"
  32  "POTS 2 Admin Status"
   Enter OMCI edit command: 14
   Enter value: 2012000984
   Enter OMCI edit command: 15
   Enter value: 2012000984
   Enter OMCI edit command: 16
   Enter value: password
   ...
   Enter OMCI edit command: s
SPECIFIC profile has been saved
```

2 Make sure every variable has value assigned, otherwise configuration fails unless updating Generic profile or Specific profile to assign a value.

To view the current settings of configuration variables on ONU 4/4/1 enter:

```
zSH> gpononu profiles show vars 4/4/1
              Variable Description                    Value         Source
    -------------------------------------------  ------------------  --------
  1 ETH1 Tagging mode: 0-Pass through, 1-Tagging, 2-QinQ 1           Generic
  2 ETH1 VLAN                                    100                 Generic
  3 ETH1 Forward Oper                            1                   Generic
  4 ETH2 Tagging mode: 0-Pass through, 1-Tagging, 2-QinQ 1           Generic
  5 ETH2 VLAN                                    1                   Generic
  6 ETH2 Forward Oper                            100                 Generic
  7 ETH3 Tagging mode: 0-Pass through, 1-Tagging, 2-QinQ 1           Generic
  8 ETH3 VLAN                                    999                 Generic
  9 ETH3 Forward Oper                            1                   Generic
 10 ETH4 Tagging mode: 0-Pass through, 1-Tagging, 2-QinQ 1           Generic
 11 ETH4 VLAN                                    999                 Generic
 12 ETH4 Forward Oper                            1                   Generic
 13 Country Code                                 0x348               Specific
 14 POTS1 Dial Number                            2012000984          Specific
 15 POTS1 User Name                              2012000984          Specific
 16 POTS1 Password                               password            Specific
 17 POTS2 Dial Number                            2012000985          Specific
 18 POTS2 User Name                              2012000985          Specific
 19 POTS2 Password                               password            Specific
 20 VOICE VLAN                                   300                 Specific
 21 SIP Proxy IP                                 172.16.60.51        Specific
 22 SIP Host IP Option: 2-static, 3-DHCP         3                   Specific
 23 SIP Host IP                                  0.0.0.0             Default
 24 SIP Netmask                                  0.0.0.0             Default
 25 SIP Gateway                                  0.0.0.0             Default
 26 SIP Domain                                   test.zhone.com      Specific
 27 ETH 1 Admin Status: 0-Up, 1-Down             0 (up)              Default
 28 ETH 2 Admin Status: 0-Up, 1-Down             0 (up)              Default
 29 ETH 3 Admin Status: 0-Up, 1-Down             0 (up)              Default
 30 ETH 4 Admin Status: 0-Up, 1-Down             0 (up)              Default
 31 POTS 1 Admin Status: 0-Up, 1-Down            0 (up)              Specific
 32 POTS 2 Admin Status: 0-Up, 1-Down            0 (up)              Specific
```

Activating ONT

Activate the ONT to add it to the system. If you are adding multiple services, you would range the ONT after all the services have been added.

Note: Only run the **gpononu set** command once to add the ONT. If the ONT has been activated and the OMCI profiles are configured for other service, you may add other bridges without resetting the ONT. If you change OMCI profiles you will need to resync/reboot the ONT. To resync ONT use the **gpononu resync <slot>[/<olt>[/<onu>]]** command. To reboot ONT use the **gpononu reboot <slot>[/<olt>[/<onu>]]** command.

1 To activate an ONT first run the **gpononu show** command to display the ONTs currently on the OLT, and discover the available serial numbers.

The **gpononu show** command has options to select by slot and OLT. If you run the command without defining the slot/OLT the command will check for ONTs on every port of every card and depending on the number of cards, may take a long time to complete.

```
zSH> gpononu show 4/4
Processing list of 128
This command may take several minutes to complete.
Do you want to continue?  (yes or no) [no] yes
Free ONUs for slot 4 olt 4:
    1    2    3    4    5    6    7    8    9   10   11   12
   13   14   15   16   17   18   19   20   21   22   23   24
   25   26   27   28   29   30   31   32   33   34   35   36
   37   38   39   40   41   42   43   44   45   46   47   48
   49   50   51   52   53   54   55   56   57   58   59   60
   61   62   63   64
Discovered serial numbers for slot 4 olt 4:
sernoID   Vendor  Serial Number     sernoID   Vendor  Serial Number
    1      CIGG    138543368
```

2 Run the **gpononu set** command to associate a serial number to the appropriate ONT:

```
zSH> gpononu set 4/4/1 1
Onu 1 successfully enabled with serial number CIGG
138543368
```

3 Run the **gpononu show** command to verify the ONT is enabled, and OMCI support is added into the ONT (the associated ME profile and Generic profile can be displayed).

```
zSH> gpononu show 4/4/1
                                  Serial
ONU       Name         Enabled     Number         OMCI files and profiles
=== ================= ======= =============== ================================
  1          1-4-4-1   Yes    CIGG 138543368 ME   2510-config1
                                             GEN  2510-service-plan1
```

4 Run the **gpononu status** command to verify the OMCI state is active.

```
zSH> gpononu status 4/4/1
ID          Onu           OperStatus   OmciState    GponOnuStatus
=== ==================== ============= ========= ====================
  1              1-4-4-1            Up    Active              Active
```

5 Run the **bridge show** command to view the MAC address of the connected PC.

```
zSH> bridge show
Type VLAN        Bridge                         St  Table Data
---------------------------------------------------------------------------------
upl Tagged 100   ethernet5-100/bridge           UP  S VLAN 100 default
dwn Tagged 100   1-4-4-501-gponport-100/bridge  UP  D 00:00:86:43:3c:e4 MAC of PC
```

Testing the data bridge

Verify that the user can get data on the PC:

1 Connect an ONT downlink ethernet port to a PC.

Make sure the ONT model matches the one you assigned with the Smart OMCI web tool. This example connects a ZNID-GPON-2510 to the PC.

And also make sure the ONT downlink ethernet port number matches the one you assigned with the Smart OMCI web tool for data service. In this example, you can connect either ETH 1 or ETH 2 to the PC.

2 Open a command prompt on the PC and enter **ipconfig** to verify that you can get an IP address from DHCP server for the PC.

3 Open an internet browser on the PC, you should be able to access the internet now.

Create Video Bridge on GPON OMCI with Uplink and Downlink

Video bridging is very similar to data bridging, it uses downlink/uplink bridge too, but the GTP, GEM ports and VLANs are different.

Creating GPON Traffic Profile

Add the GTP.

The following GTP is recommended for video:

```
zSH> new gpon-traffic-profile 2
gpon-traffic-profile 2
Please provide the following: [q]uit.
guaranteed-upstream-bw: ->  {0}: 512
traffic-class: ---------->  {ubr}: cbr
compensated: ------------>  {false}:
shared: ----------------->  {false}:
dba-enabled: ------------>  {false}:
dba-fixed-us-ubr-bw: ---->  {0}:
dba-fixed-us-cbr-bw: ---->  {0}:
dba-assured-us-bw: ------>  {0}:
dba-max-us-bw: ---------->  {0}:
dba-extra-us-bw-type: --->  {nonassured}:
....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

Creating uplink and downlink bridge

We will create an uplink and downlink bridge for VLAN 999:

1 Create an uplink bridge interface

a Create the uplink bridge interface

The following example creates a video uplink bridge interface with proxy reporting and 30 second igmp query interval.

```
zSH> bridge add 1-a-5-0/eth uplink vlan 999 tagged

Adding bridge on 1-a-5-0/eth
Created bridge-interface-record ethernet5-999/
bridge
```

b Add the bridge-path for the uplink. Note how the igmptimer is added to the bridge-path.

```
zSH> bridge-path add ethernet5-999/bridge vlan 998
default igmpsnooping enable igmptimer 30
Bridge-path added successfully
```

2 Create downlink bridge interface.

You create a downlink bridge on an GPON port with VLAN ID and GTP.

You can also specify option **video** *m*/*n*. *m* indicates the multicast control list, *n* indicates the maximum video streams. By specifying **video 0/4** in this example you can enable subscriptions up to four video streams on the interface without control list checking.

If you want to have multicast control list checking, use the **new mcast-control-entry** command to create a multicast control list first.

```
zSH> bridge add 1-4-4-901/gponport gtp 2 downlink vlan
999 tagged video 0/4
GEM Port 1-1-7-901/gponport has been created on ONU
1-1-7-1/gpononu.
Adding bridge on 1-1-7-901/gponport
Created bridge-interface-record
1-1-7-901-gponport-998/bridge
```

3. Run the **bridge show** command to view the MAC address of the connected PC.

```
zSH> bridge show
Type VLAN        Bridge                         St  Table Data
---------------------------------------------------------------------------
upl Tagged 100   ethernet5-100/bridge           UP  S VLAN 100 default
dwn Tagged 100   1-4-4-501-gponport-100/bridge  UP  D 00:00:86:43:3c:e4
upl Tagged 999   ethernet5-999/bridge           UP  S VLAN 999 default
dwn Tagged 999   1-4-4-901-gponport-999/bridge  UP  D 00:00:87:44:0c:e7  MAC of PC
                                                    D 01:00:5e:0a:0a:0a
```

Because Specific profile is already created on this ONT when configuring data application, you do not need to create a Specific profile again.

Since you only add the ONT once, you would normally run the **gpononu set** command after you have added all the services. You may add service after activating the ONT, however if you change the OMCI profiles later, you need to resync or reboot the ONT. See the Step 1 *Activate the ONT* in the data application for the command and greater detail on the operation.

Testing the IPTV bridge

Since we are using a PC and software to emulate a set top box (STB), we can ping out to the video server.

1. Connect an ONT downlink ethernet port to a customer video equipment. This example connects to a PC that runs a STB emulation software.

   Make sure the ethernet port number matches the one you assigned with the Smart OMCI web tool for video service. In this example you can connect either ETH 3 or ETH 4 to the PC.

2. Open a command prompt on the PC and enter **ipconfig** to verify that you can get an IP address for the PC.

3. Ping the video server

   a. Open a DOS window

   b. Ping the upstream gateway (provided in your environment setup)

4. Open the STB emulation software and connect to the video server

   As long as you can ping you are showing that you have a data path through the zNID and the MXK to the video server. You should be able to connect to the video stream with the STB emulation software.

Create VoIP on GPON OMCI with TLS bridges

For VoIP service we recommend to use TLS bridging.

Creating GPON Traffic Profile

Add the GTP.

The following GTP is recommended for up to four VoIP phones or four POTS ports.

```
zSH> new gpon-traffic-profile 3

gpon-traffic-profile  3
Please provide the following: [q]uit.
guaranteed-upstream-bw: ->  {0}: 512
traffic-class: ---------->  {ubr}: cbr
compensated: ------------>  {false}:
shared: ----------------->  {false}:
dba-enabled: ------------>  {false}:
dba-fixed-us-ubr-bw: ---->  {0}:
dba-fixed-us-cbr-bw: ---->  {0}:
dba-assured-us-bw: ------>  {0}:
dba-max-us-bw: ---------->  {0}:
dba-extra-us-bw-type: --->  {nonassured}:
....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved..
```

Creating TLS bridge

We will create a TLS bridge for VLAN 300:

1. Create a TLS bridge on the uplink interface.

```
zSH> bridge add 1-a-5-0/eth tls vlan 300 tagged
Adding bridge on 1-a-5-0/eth
Created bridge-interface-record ethernet5-300/bridge
```

2. Create a TLS bridge on the downlink interface.

```
zSH> bridge add 1-4-4-701/gponport gtp 3 tls vlan 300
tagged
```

```
GEM Port 1-4-4-701/gponport has been created on ONU
1-4-4-1/gpononu.
Adding bridge on 1-4-4-701/gponport
Created bridge-interface-record
1-4-4-701-gponport-300/bridge
```

3 On MXK, run the **bridge show** command to view the MAC address of the connected VoIP phone.

```
zSH> bridge show
Type VLAN       Bridge                        St  Table Data
---------------------------------------------------------------------------------
upl Tagged 100  ethernet5-100/brid            UP  S VLAN 100 default
dwn Tagged 100  1-4-4-501-gponport-100/bridge UP  D 00:00:86:43:3c:e4
upl Tagged 999  ethernet5-999/bridge          UP  S VLAN 999 default
dwn Tagged 999  1-4-4-901-gponport-999/bridge UP  D 00:00:87:44:0c:e7
                                                  D 01:00:5e:0a:0a:0a
tls Tagged 300  1-4-4-701-gponport-300/bridge UP  D 00:19:c7:02:9c:6b MAC of Phone
tls Tagged 300  ethernet5-300/bridge          UP  D 00:00:86:43:3c:e4
                                                  D 00:00:86:43:ec:69
                                                  D 00:01:47:1a:e4:74
                                                  D 00:03:e3:97:bb:00
                                                  D 00:50:04:78:56:85
                                                  D 00:50:04:bf:63:3e
```

Because a Specific profile is already created on this ONT when configuring data application, you do not need to create a Specific profile again.

Since you only add the ONT once, you would normally run the **gpononu set** command after you have added all the services. You may add service after activating the ONT, however if you change the OMCI profiles later, you need to resync or reboot the ONT. See the Step 1 *Activate the ONT* in the data application for the command and greater detail on the operation.

Testing the VoIP configuration

1 Connect an ONT downlink POTS port to a VoIP phone.

Make sure the POTS port number matches the one you assigned for voice service with the Smart OMCI web tool. In this example, you can connect either POTS 1 or POTS 2 to the PC.

2 Pick up the phone, you should be able to hear the dial tone and be able to make and receive a phone call.

Summary

All the applications described may be done in sequence as shown in the flowchart.

There must be synchronization between the OMCI profiles (particularly regarding GEM ports and VLAN).

By activating the ONT you can add it to the system. If you are adding multiple services, you would activate the ONT after all the services have been added. If the OMCI profiles are configured, you may add other bridges without resetting the ONT. If you changed OMCI profiles you will need to resent the ONT.

Troubleshooting

This section is basically what can go wrong, how to recognize and understand what went wrong, and how to fix it.

Table 3: Internet access troubleshooting table

Symptom	Discussion
You can see power LED is green on the ONT, but operational LED is red. And ONT OperStatus appears as Down when you use the **gpononu status** command.	This symptom shows the fiber connection might be loose or disconnected. Check the fiber connection on ONT, splitter, and MXK.
You can see a MAC address of the downstream laptop, but do not get the IP address.	This symptom actually happened when setting up the scenario. It is significant to note that with an uplink-downlink bridge as we have created in this scenario, addresses will not be learned until the downstream device sends a packet to the MXK. To rectify the situation we deleted the bridge and added it again this time with the downlink parameter. It is also possible that you do not have a DHCP server upstream from the MXK. The DHCP upstream from the MXK is a requirement of this scenario. And also make sure the VLAN you assigned is a routable VLAN.

Table 3: Internet access troubleshooting table

Symptom	Discussion
Your laptop has an IP address of 169.xx.xx.xx.	Microsoft adds these addresses when an IP address is not obtainable. Once you have the access situation rectified, (Assuming you are using a windows based machine) you may need to open a command prompt on the PC and do an **ipconfig/release**, then an **ipconfig/renew** to resolve it. Finally an **ipconfig/all** will verify the new ip address which should be in your subnet range.

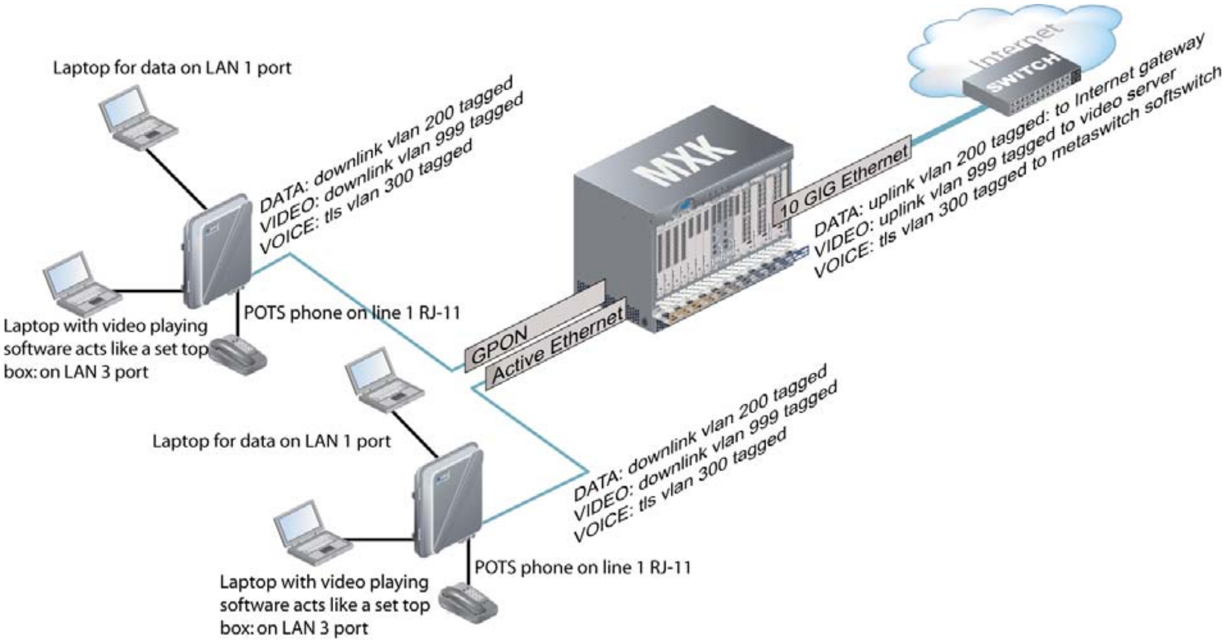
4 GPON and Active Ethernet UI based zNID

In this chapter we will build triple play solutions using the browser based GPON zNID, Active Ethernet zNID and the MXK by building bridges for each of the component solutions — data, video, and voice — on separate VLANs as they would be done in a real world environment.

As discussed earlier (*Section 1, VLANs for the data, video and voice services*) we will use separate VLANs for data, video and voice. Having each service on its own VLAN not only separates the known traffic from video and voice servers from the unknown traffic from the Internet gateway, it allows us to isolate the video traffic to use the Fast Path feature of the browser-based zNIDs.

Notice in Figure 10 that both the GPON and Active Ethernet solutions use the same uplink bridges (in fact the OMCI GPON solution does as well). Each solution has its own downlink. The downlink/downstream links for GPON are identical to each other. The Active Ethernet is only a bit different.

Figure 10: The zNID supports triple play connected to upstream services


Laptop for data on LAN 1 port
DATA: downlink vlan 200 tagged
VIDEO: downlink vlan 999 tagged
VOICE: tls vlan 300 tagged
Laptop with video playing software acts like a set top box: on LAN 3 port
POTS phone on line 1 RJ-11
MXK
Internet
SWITCH
10 GIG Ethernet
DATA: uplink vlan 200 tagged: to Internet gateway
VIDEO: uplink vlan 999 tagged to video server
VOICE: tls vlan 300 tagged to metaswitch softswitch
GPON
Active Ethernet
Laptop for data on LAN 1 port
DATA: downlink vlan 200 tagged
VIDEO: downlink vlan 999 tagged
VOICE: tls vlan 300 tagged
Laptop with video playing software acts like a set top box: on LAN 3 port
POTS phone on line 1 RJ-11

IPTV service requires high bandwidth for one traffic flow. Packet television is streamed down to a set top box (STB) at the rate of

2-8Mbps or even higher and all of the packets for one channel are in a single packet flow. That is, all of the packets for a single channel look nearly identical except for the data being transported. Source and destination addresses, Quality of Service (QoS) markings, and port numbers are the same for every packet streaming down from the provider's network to the end-user's STB.

In many networks multicast and unicast video streams constitute the majority of bandwidth used by the customer and therefore will probably represent the most processing work for the zNID. If the video traffic is on its own VLAN we can take advantage of a Zhone browser-based zNID feature called Fast Path. Fast Path acts as a short cut for packets traveling in the ingress and egress direction through the zNID. A VLAN configured for Fast Path will bypass the network processor functions of the zNID which is responsible for firewall, access lists, security, and any other function that would require the zNID to look at the packet/frame header values. The main benefit of enabling Fast Path is speed. By taking a processing load away from the zNID's network processor faster speeds can be achieved without concern for how many features are enabled on the unit.

For our configuration, as in the real world environment, you would have separate private networks for voice and video, and a public networks for data. Since we are expecting to get a separate IP addresses for voice termination and data on the zNID, this requires separate DHCP servers on separate networks in our lab environment and if you follow our example closely, your environment as well. DHCP servers can only provide one IP address per MAC address.

These examples are designed to be accomplished in a minimum amount of time and provide a foundation for understanding other important network edge access concepts.

Creating the browser-based GPON and Active Ethernet solutions are very similar

- Use the same Web based user interface
- Use the same uplinks/upstream bridge interfaces, VLANs, and upstream servers/gateways

The differences in creating the GPON and Active Ethernet solutions are

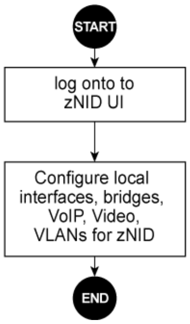
- In the Web UI you have WAN PON and WAN Ethernet physical interfaces
- The downlink/downstream bridge interfaces are based on transport media and there is a GPON specific parameter — GPON traffic profile
- Active Ethernet does not have an activation step for the OLT to recognize the zNID. Once the bridges are active and the zNID connected, it is ready to communicate.

The procedures for each solution will be covered separately to avoid confusion. If you read through both procedures you will see many of the same steps, even comments; the duplication of procedures is for those who only read the procedure that interests them.

Topics to be covered in the examples in this chapter:

Configuring the browser-based zNID is much like configuring modems, routers, gateways or other network access devices. You log into the zNID with a browser, then configure the zNID, adding bridges for the services you want the zNID to provide.

Figure 11: Configure the browser-based zNID


START
log onto to zNID UI
Configure local interfaces, bridges, VoIP, Video, VLANs for zNID
END

Deploying and managing overview

There are a couple of models for configuring and deploying the browser-based zNIDs:

- Design, build, test, copy and deploy
- TR-069 server

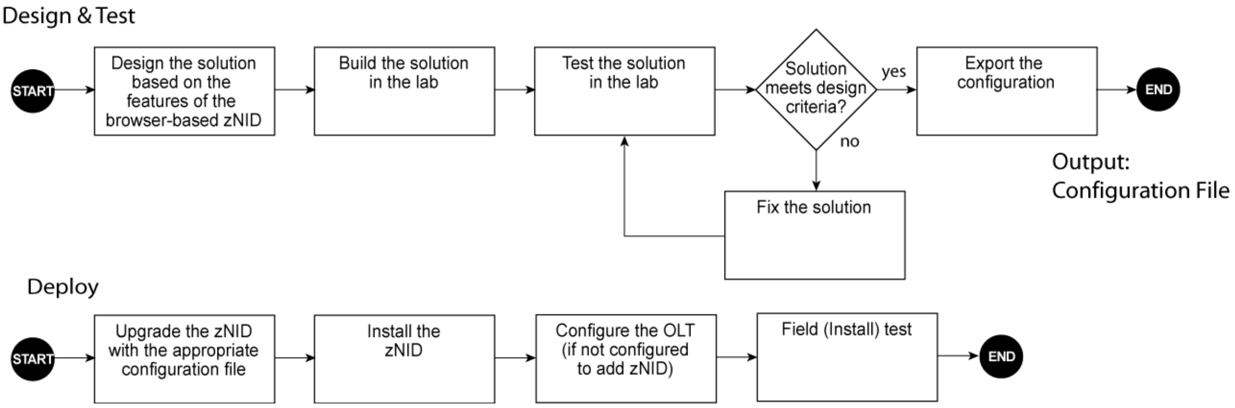
For this application guide we will use the design, build, test, copy and deploy deployment model.

Design, build, test and deploy

With the design, build, test, copy and deploy model, you design how you want the zNID to work using different configuration options. Once the zNID is configured as you want it to be, you can export the configuration, then import it to zNIDs before deploying them in the field. In this way you could have several different configurations ready for field deployment.

Once the unit is deployed in the field it is a simple operation to customize the zNID with customer specific information such as the phone number.

Figure 12: Flowchart for the design, build, test deploy model


Design & Test
START
Design the solution based on the features of the browser-based zNID
Build the solution in the lab
Test the solution in the lab
Solution meets design criteria?
yes
no
Export the configuration
END
Output: Configuration File
Fix the solution
Deploy
START
Upgrade the zNID with the appropriate configuration file
Install the zNID
Configure the OLT (if not configured to add zNID)
Field (Install) test
END

1. Design

   Decide which features you want to provide from the zNID.

2. Build

   In this step you configure the zNID.

3. Test

4. Export

   You export the tested configuration for importing to another unit. Multiple configurations could be created based on service plan criteria.

5. Upgrade

   Import a configuration file to another unit.

6 Deploy

At this point you would individualize the zNID for the specific customer. For example you would set the phone number at this time.

Once the unit is installed, if the zNID is configured (the MXK from our example), you should be able to field test the unit. The GPON zNID must be activated before testing.

TR-069 server

With the TR-069 server deployment model. You configure the file as above, but do not deploy to the unit. The file is used by the TR-069 server to upgrade the units in the field as they are brought online.

Please contact your Zhone Sales Representative for information about Zhone’s TR-069 server.

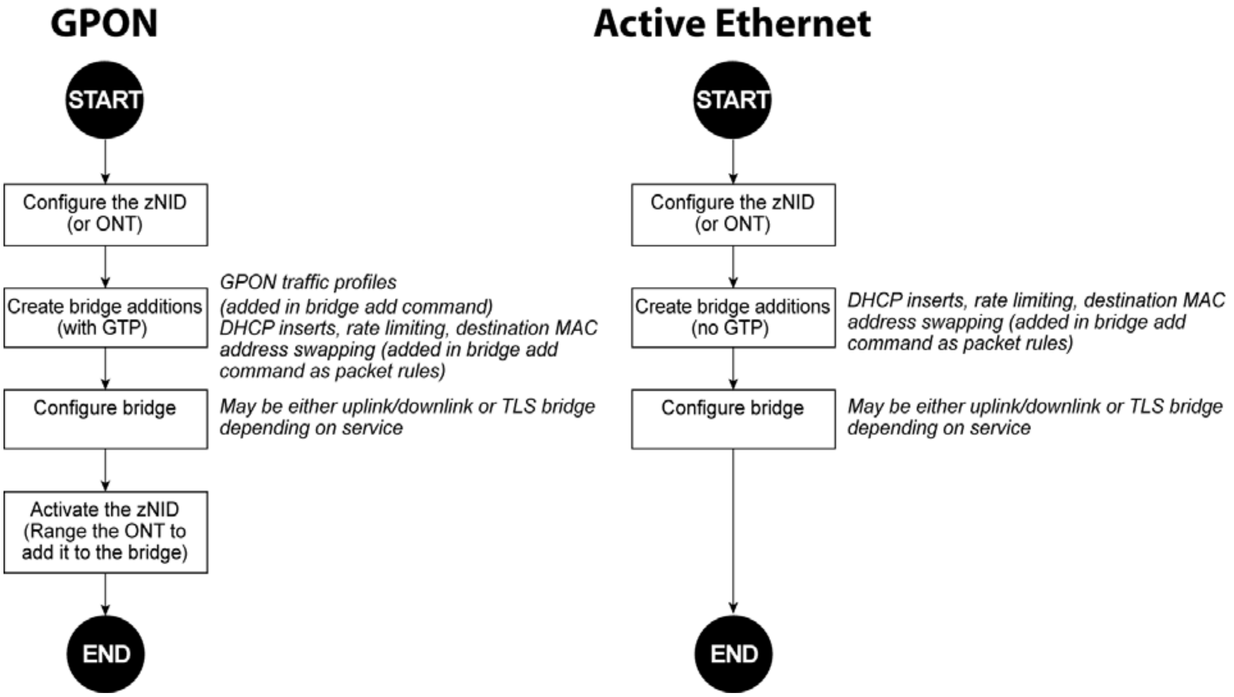
Overview of the configuration process

We are using separate procedures to reduce confusion; and though we could configure each zNID for all services at once and could configure all the bridges in one step as well, for the sake of clarity in our discussions we will configure the services one at a time. With the browser-based zNID the order is not as important. In fact, you can configure the bridges first, then configure the zNID. Unlike the GPON OMCI management model you can also activate the browser-based GPON zNID as soon as it is powered up and connected to the MXK, then build the bridges and configure the zNID without needing to reboot or resync the zNID (The Active Ethernet solution does not need the activation step).

For the purposes of presenting each service separately, however, we shall follow the flow chart, Configuring bridges by service type, page 73, adding each service one at a time.

We will only need to activate the GPON zNID the first time through, so if you are setting up only one service, you will need to make sure you have activated the GPON zNID.

Figure 13: Overview of the configuration process

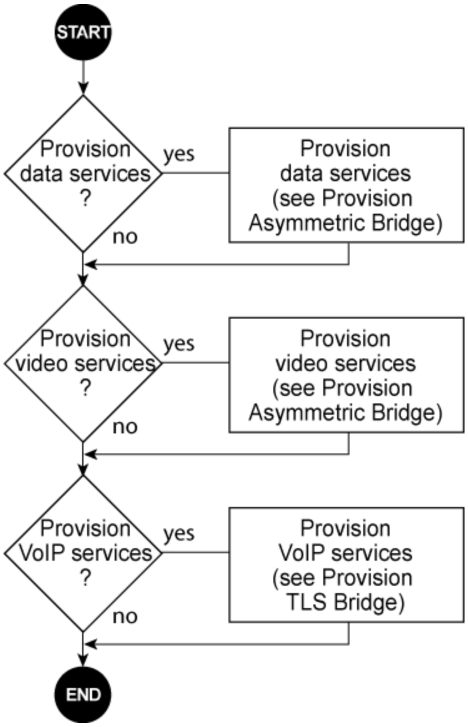

GPON
START
Configure the zNID (or ONT)
Create bridge additions (with GTP)
GPON traffic profiles (added in bridge add command) DHCP inserts, rate limiting, destination MAC address swapping (added in bridge add command as packet rules)
Configure bridge
May be either uplink/downlink or TLS bridge depending on service
Activate the zNID (Range the ONT to add it to the bridge)
END
Active Ethernet
START
Configure the zNID (or ONT)
Create bridge additions (no GTP)
DHCP inserts, rate limiting, destination MAC address swapping (added in bridge add command as packet rules)
Configure bridge
May be either uplink/downlink or TLS bridge depending on service
END

The bridge type we build depends on the service (data, video, or voice). For data and video we will use asymmetric bridges. The configuration on the MXK will be very similar. However on the zNID we will use FastPath, so the packets will bypass the zNID’s network processor.

For the voice service we will use a TLS bridge. TLS bridges are better suited for upstream initiated calls because in the worst case scenario you will always be able to get the MAC address of the VoIP supplying access device (in this case the zNID).

If there is no activity on the VoIP bridge, then the MAC address of the VoIP supplying access device will eventually time out the MAC address of the VoIP in the bridge forwarding table. Unlike the downlink of an asymmetric bridge, the TLS bridge will flood all the bridge interfaces of the TLS VoIP VLAN and rediscover the VoIP supplying access device.

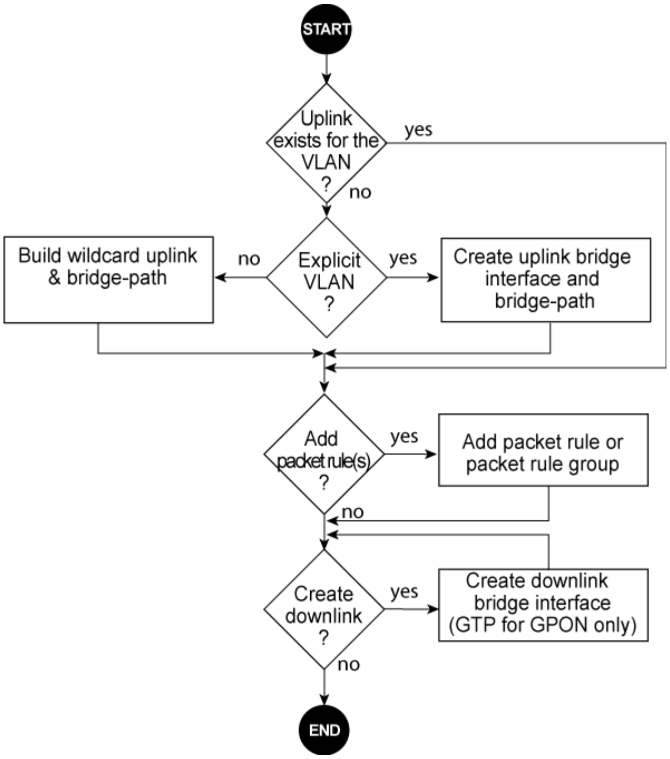
Figure 14: Configuring bridges by service type


START
Provision data services ?
yes
no
Provision data services (see Provision Asymmetric Bridge)
Provision video services ?
yes
no
Provision video services (see Provision Asymmetric Bridge)
Provision VoIP services ?
yes
no
Provision VoIP services (see Provision TLS Bridge)
END

Though the asymmetric bridge types include the intralink bridge interface type which is used for subtending other MXKs, MALCs, MALC XPs, or Raptor XPs from the MXK via Active Ethernet cards, we will not be creating intralink bridges in this document.

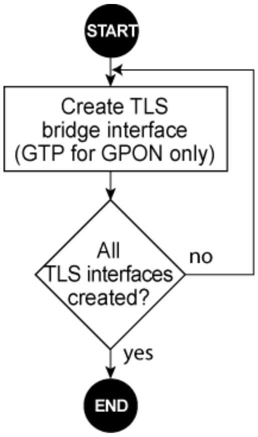
The uplink/dowlink bridges we will build are all based on specific VLANs — VLAN 200 for the data bridge and VLAN 999 for the video bridge. VLAN 200 is a gateway to the internet. VLAN 999 has a head-end video server.

Figure 15: Configuring asymmetric bridges for GPON


START
Uplink exists for the VLAN ?
yes
no
Explicit VLAN ?
no
Build wildcard uplink & bridge-path
yes
Create uplink bridge interface and bridge-path
Add packet rule(s) ?
yes
Add packet rule or packet rule group
no
Create downlink ?
yes
Create downlink bridge interface (GTP for GPON only)
no
END

We will use VLAN 300 for the VoIP bridge, and connect out to the Metaswitch softswitch server using SIP.

Figure 16: Configuring TLS bridge for GPON


START
Create TLS bridge interface (GTP for GPON only)
All TLS interfaces created?
no
yes
END

The behavior of the TLS bridge is better suited for upstream initiated calls because the TLS VoIP bridge (VLAN 300 in our example) will be flooded with a request for the MAC address of the VoIP access device if the MAC address is timed out from the MXK's forwarding table. Asymmetric bridges do not forward unknown unicast which are received on the uplink, so an asymmetric bridge is not a suitable option for the voice application.

Configuring browser-based GPON zNIDs

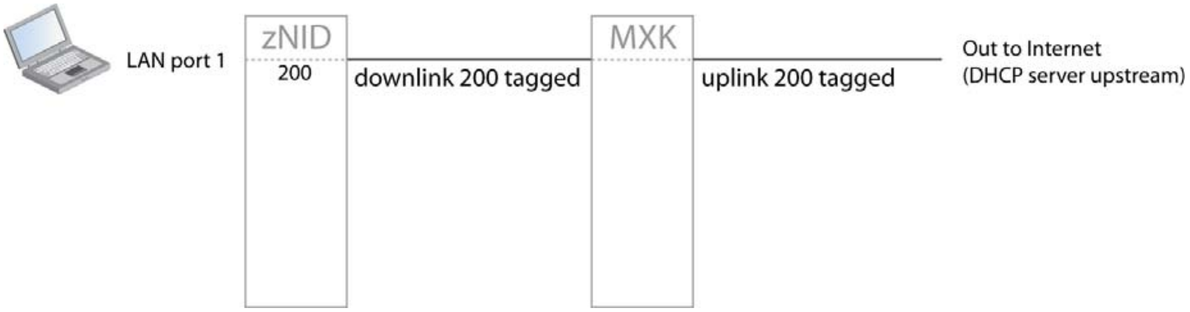
Configuring a bridge for data, GPON

To configure a bridge to the zNID, you must have a bridge on the MXK (The GPON card acts as the OLT; in fact, each port can be considered a separate OLT). To build a bridge that reaches the subscriber devices bridges need to be built on the zNID.

For each service we will be adding a separate bridge with its own VLAN. For the data and video services we will set up an uplink and downlink bridge. From the perspective of each access device, the MXK and zNID, this means creating a bridge from the upstream interface to the downstream interface.

For data services we will create a bridge on the MXK from the Internet uplink to the downlink. On the zNID we will create a bridge from the WAN PON interface to LAN 2 port. For data coming from the PC to the LAN port we will need to add a VLAN header, so the packets will be designated VLAN 200. Packets going downstream to the PC on LAN 2 port will likewise have the VLAN information stripped because the PC does not need tagged packets; only packets with VLAN 200 will be delivered to the LAN 2 interface.

Figure 17: Bridges on the MXK and zNID to pass data traffic



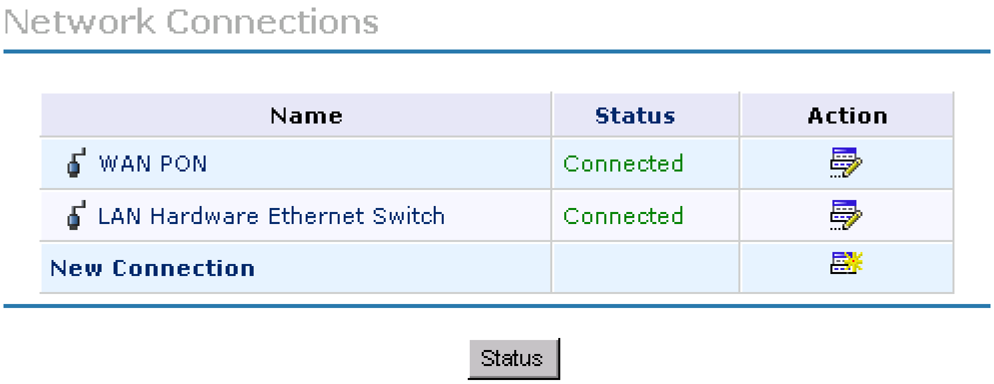
Clearing off the default settings of the zNID

We will remove the default connections, so we can go through the steps of creating a solution.

1 Click **Network Connections** in the left hand menu pane

2 In the **Network Connections** page, delete **Data VLAN 200** by clicking the delete action icon for that item, then click **OK** to confirm

3 Delete **Management VLAN 300** by clicking the delete action for that item, then click **OK** to confirm



Network Connections

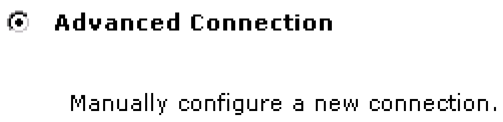
Name	Status	Action
WAN PON	Connected	✎
LAN Hardware Ethernet Switch	Connected	✎
New Connection		✎

Creating a bridge on the zNID

We will create a bridge on the zNID.

1 Add a VLAN ID on the WAN interface

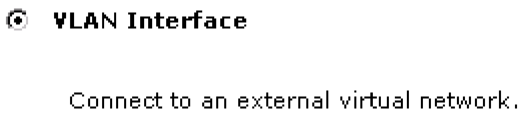
- **a** Click **Network Connections** in the left hand menu pane
- **b** In the **Networks Connection** page, click **New Connection**
- **c** In the **Connection Wizard** screen select **Advanced Connection** and click **Next**



● **Advanced Connection**

Manually configure a new connection.

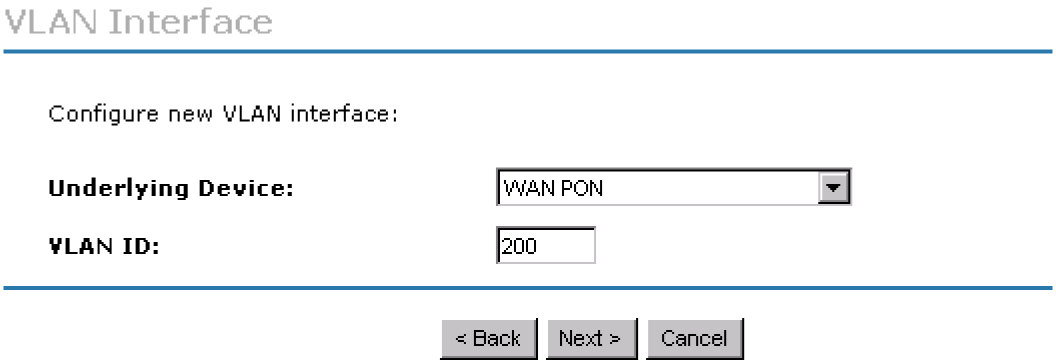
- **d** In the **Advanced Configuration** screen select **VLAN Interface** and click **Next** near the bottom of the screen



● **VLAN Interface**

Connect to an external virtual network.

e From the **Underlying Device** drop down select the physical WAN port (**WAN PON**) to associate with the VLAN ID



VLAN Interface

Configure new VLAN interface:

Underlying Device: WAN PON

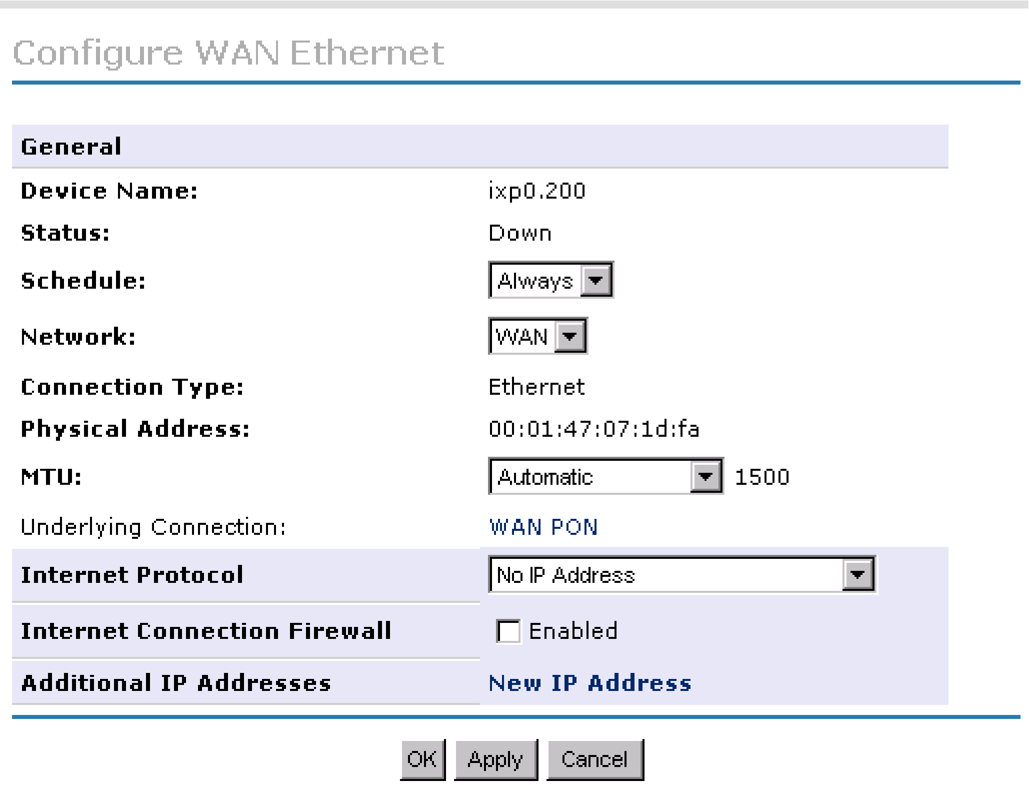
VLAN ID: 200

f In the **VLAN ID** text box enter the VLAN ID (200), then click **Next**

g In the **Connection Summary** screen select **Edit the Newly Created Connection**, then click **Finish**

h Verify the WAN Ethernet interface has been created, then click **OK**

Figure 18: The create WAN Ethernet interface



Configure WAN Ethernet

General	
Device Name:	ixp0.200
Status:	Down
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00:01:47:07:1d:fa
MTU:	Automatic 1500
Underlying Connection:	WAN PON
Internet Protocol	No IP Address
Internet Connection Firewall	☐ Enabled
Additional IP Addresses	**New IP Address**

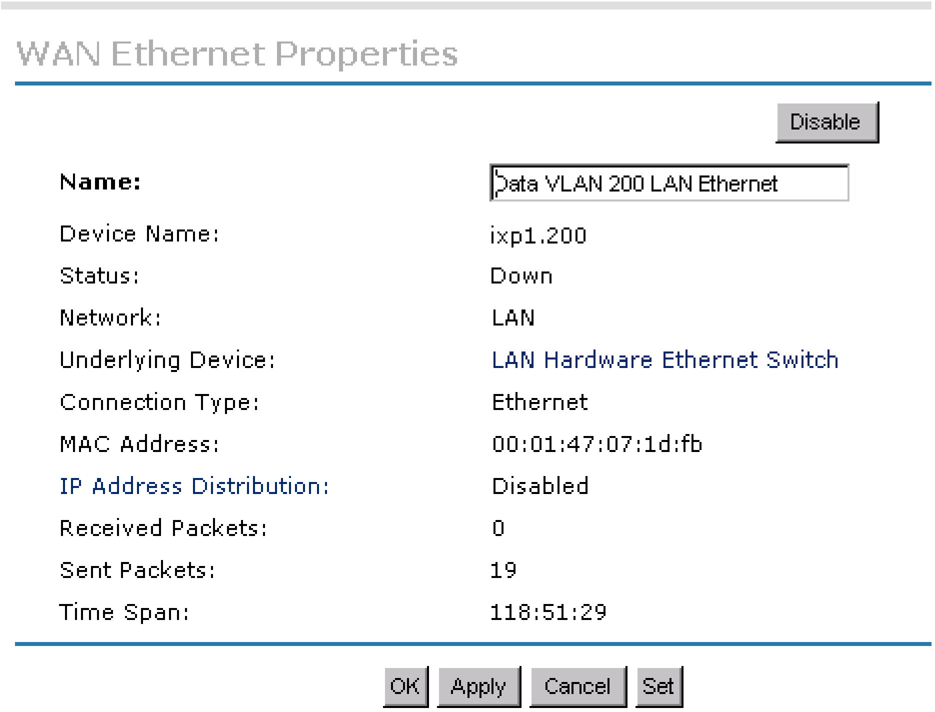
i Name the interface by clicking the edit icon for the **WAN Ethernet** interface you just created, then enter an appropriate name in the **Name** text box and click **OK**

We will use **Data VLAN 200 WAN Ethernet**.

2 Add a VLAN ID to the LAN switch

- **a** Click **Network Connections** in the left hand menu pane
- **b** In the **Networks Connection** page, click **New Connection**
- **c** In the **Connection Wizard** screen select **Advanced Connection** and click **Next**
- **d** In the **Advanced Connection** screen select **VLAN Interface** and click **Next**
- **e** From the **Underlying Device** dropdown select the Ethernet switch to associate with the VLAN ID (**LAN Hardware Ethernet Switch**)
- **f** In the **VLAN ID** text box enter the VLAN ID (200), then click **Next**
- **g** In the **Connection Summary** screen select **Edit the Newly Created Connection**, then click **Finish,** view the screen then click **OK**
- **h** Name the interface by clicking the edit icon for the **LAN Ethernet** interface you just created, then enter an appropriate name in the **Name** text box and click **Next**

  We will use **Data VLAN 200 LAN Ethernet**.



WAN Ethernet Properties

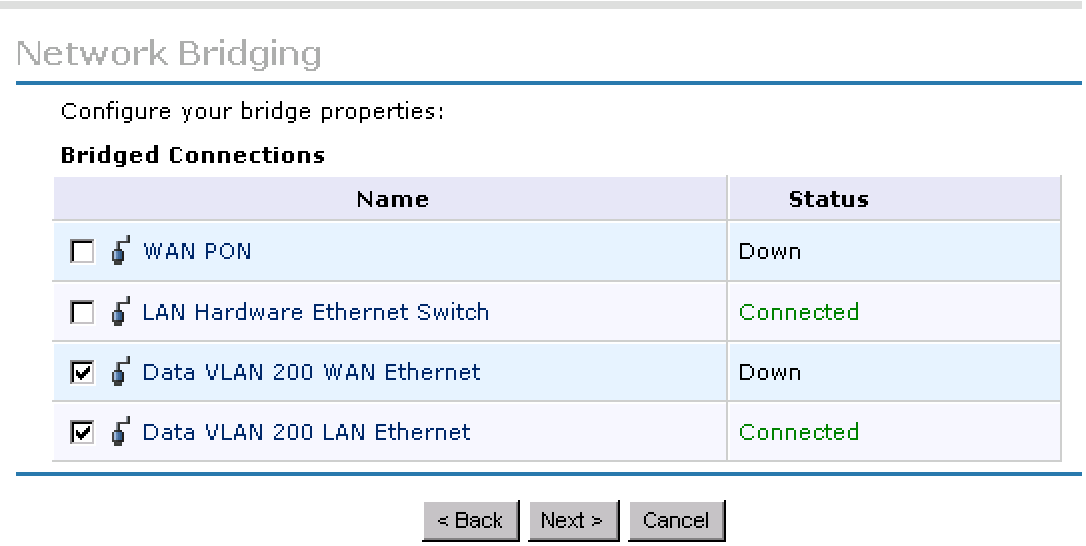
Name:	Data VLAN 200 LAN Ethernet
Device Name:	ixp1.200
Status:	Down
Network:	LAN
Underlying Device:	LAN Hardware Ethernet Switch
Connection Type:	Ethernet
MAC Address:	00:01:47:07:1d:fb
IP Address Distribution:	Disabled
Received Packets:	0
Sent Packets:	19
Time Span:	118:51:29

3 Build the bridge between (among) the interfaces

- **a** Click **Network Connections** in the left hand menu pane
- **b** In the **Networks Connection** page, click **New Connection**
- **c** In the **Connection Wizard** screen select **Advanced Connection** and click **Next**

d In the **Conneciton Wizard** screen select **Network Bridging** then click **Next**

e Select the connections to combine in the bridge (Data VLAN 200 WAN Ethernet and Data VLAN 200 LAN Ethernet) then click **Next**



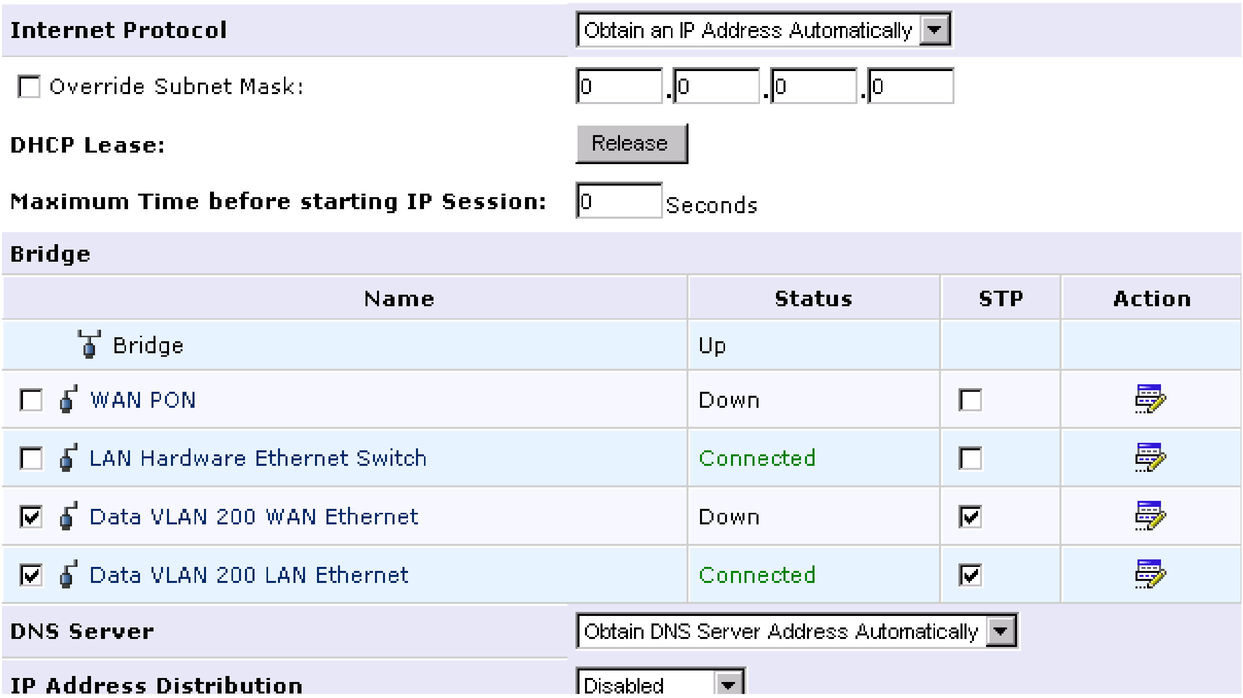
Network Bridging

Configure your bridge properties:

Bridged Connections

Name	Status
□ WAN PON	Down
□ LAN Hardware Ethernet Switch	Connected
☑ Data VLAN 200 WAN Ethernet	Down
☑ Data VLAN 200 LAN Ethernet	Connected

f In the **Connection Summary** screen select **Edit the Newly Created Connection** then click **Finish**



Internet Protocol	Obtain an IP Address Automatically ▾
□ Override Subnet Mask:	0 . 0 . 0 . 0
DHCP Lease:	Release
Maximum Time before starting IP Session:	0 Seconds

Bridge

Name	Status	STP	Action
Bridge	Up		
□ WAN PON	Down	□	✎
□ LAN Hardware Ethernet Switch	Connected	□	✎
☑ Data VLAN 200 WAN Ethernet	Down	☑	✎
☑ Data VLAN 200 LAN Ethernet	Connected	☑	✎

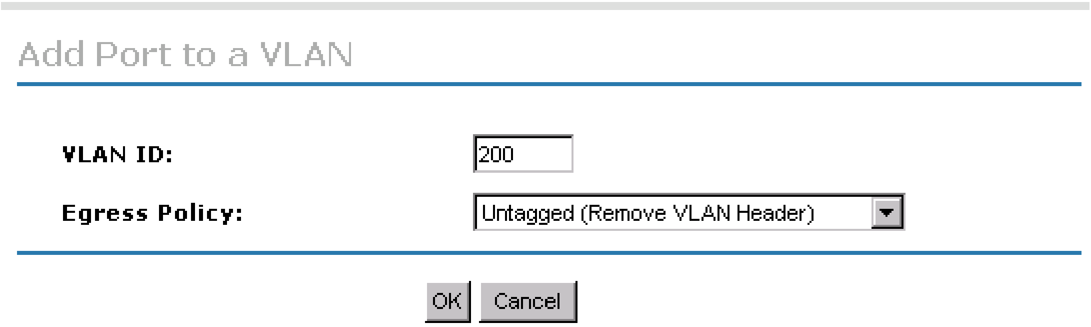
DNS Server	Obtain DNS Server Address Automatically ▾
IP Address Distribution	Disabled ▾

g In the **Internet Protocol** drop down you should have **Obtain an IP address automatically** selected; click **OK**

h Rename the bridge by clicking the edit icon for the bridge you just created in the **Network Connections** screen, then enter **Data VLAN 200 Bridge** in the **Name** text box and click **OK**

4 Map the VLAN ID to the physical port

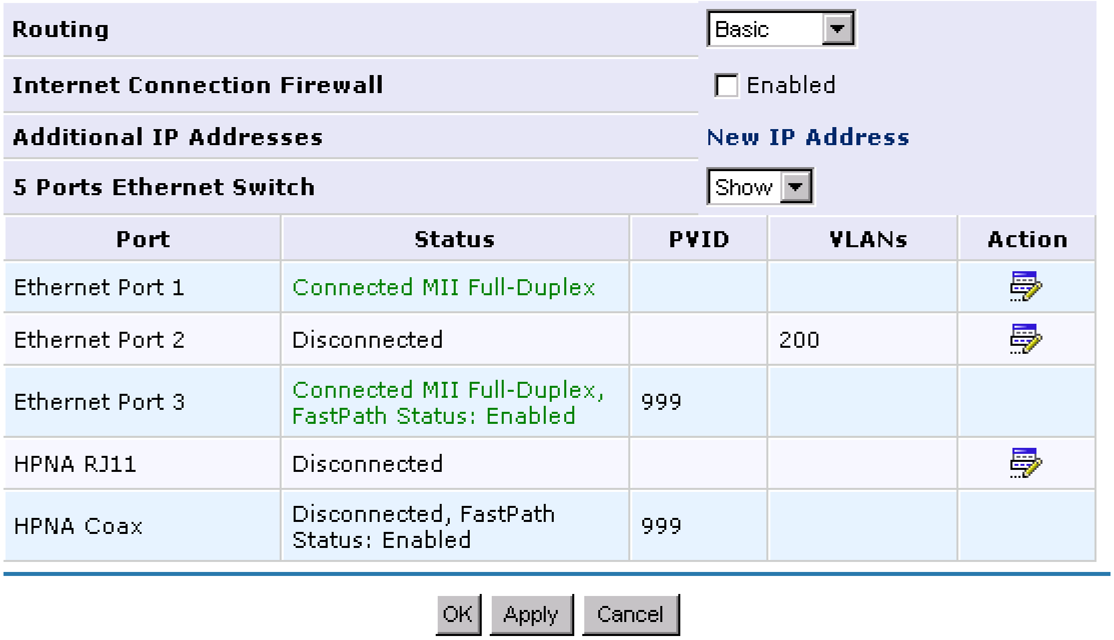
- **a** Click **Network Connections** in the left hand menu pane
- **b** In the **Network Connections** screen click on the **LAN Hardware Ethernet Switch** link
- **c** At the bottom of the **LAN Hardware Ethernet Switch Properties** screen click **Set** near the bottom of the screen
- **d** Near the bottom of the **Configure LAN Hardware Ethernet Switch** screen select the action button for the port (Ethernet Port 2) to associate the VLAN
- **e** In the **Port 2 Settings** screen, click **New Entry**



Add Port to a VLAN

VLAN ID:	200
Egress Policy:	Untagged (Remove VLAN Header)

- **f** Enter the VLAN ID (200) in the **VLAN ID** text box then click **OK**
- **g** Click **OK** again to confirm



Routing	Basic
Internet Connection Firewall	☐ Enabled
Additional IP Addresses	New IP Address
5 Ports Ethernet Switch	Show

Port	Status	PVID	VLANs	Action
Ethernet Port 1	Connected MII Full-Duplex			✎
Ethernet Port 2	Disconnected		200	✎
Ethernet Port 3	Connected MII Full-Duplex, FastPath Status: Enabled	999		
HPNA RJ11	Disconnected			✎
HPNA Coax	Disconnected, FastPath Status: Enabled	999		

Creating an uplink and downlink bridge on the MXK

We will create an uplink and downlink for VLAN 200.

1 Create uplink and add bridge-path

The switch which is upstream from our MXK is providing a network on VLAN 200. The packets are tagged from the switch.The bridge-path add command defines this bridge interface as the uplink for the VLAN 200 downlinks.

> ✓ **Note:** For all of the scenario examples in this application guide we are using the same uplinks/upstream interfaces, so if you have already created the uplink/upstream bridge interfaces, you will not need to recreate the data uplink/bridge-bridgepath here.

```
zSH> bridge add 1-a-5-0/eth uplink vlan 200 tagged

Adding bridge on 1-a-5-0/eth
Created bridge-interface-record ethernet5-200/bridge

zSH> bridge-path add ethernet5-200/bridge vlan 200 default
Bridge-path added successfully
```

2 Add the dowlink to the zNID

We are just passing the single tagged 200 packets down to the zNID. The zNID needs to know the VLAN ID to pass them through properly as well. We will configure the zNID for that as well.

```
DOC-MXK> bridge add 1-4-1-501/gponport gtp 1 downlink vlan 200 tagged

Adding bridge on 1-4-1-501/gponport

Created bridge-interface-record 1-4-1-501-gponport-200/bridge
```

If the GEM port already exists then the gtp parameter is not required. See *Creating GPON Traffic Profile* on page 55.

Activate the zNID

This first time through, we will activate the zNID, and will not need to activate it again. Actually we will not be able to activate it again once it is up.

We could have activated the zNID as soon as it was connected through the fiber to the MXK.

Activating the zNID is a matter of discovering the ID of the zNID using the **gpononu show** command, then activating the zNID using the **gpononu set** command.

1 Discover the open ONTs on the line using the **gpononu show** command

In the **gpononu show** command we will limit to the card to reduce the amount of time the discovery will take. We could even have limited it to the port as well (**gpononu show 4/1**). If there are a lot of optical distribution networks (ODNs) on the MXK, commands like **gpononu show** without further qualifiers will attempt to do discovery for all of them. The more ODNs it does discovery for, the longer it will take.

```
DOC-MXK> gpononu show 4
Processing list of 512
This command may take several minutes to complete.
Do you want to continue?  (yes or no) [no] y
Free ONUs for slot 4 olt 1:
   1    2    3    4    5    6    7    8    9   10   11   12
  13   14   15   16   17   18   19   20   21   22   23   24
  25   26   27   28   29   30   31   32   33   34   35   36
  37   38   39   40   41   42   43   44   45   46   47   48
  49   50   51   52   53   54   55   56   57   58   59   60
  61   62   63   64
Discovered serial numbers for slot 4 olt 1:
sernoID   Vendor  Serial Number     sernoID   Vendor  Serial Number
 5      ZNTS    466425
Free ONUs for slot 4 olt 2:
   1    2    3    4    5    6    7    8    9   10   11   12
  13   14   15   16   17   18   19   20   21   22   23   24
  25   26   27   28   29   30   31   32   33   34   35   36
  37   38   39   40   41   42   43   44   45   46   47   48
  49   50   51   52   53   54   55   56   57   58   59   60
  61   62   63   64
```

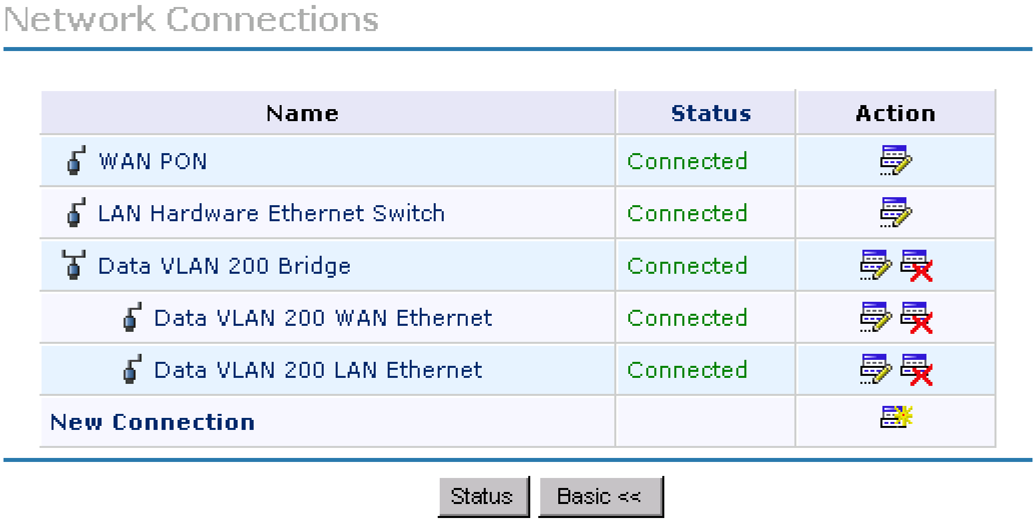
2 Set the discovered **sernoID** for the zNID

```
DOC-MXK> gpononu set 4/1/1 5
Onu 1 successfully enabled with serial number ZNTS 466425
```

Testing the data bridge

To test the connection, we will put the laptop on the LAN 2 port, ping to the Internet gateway and open a browser. Pinging to the Internet gateway proves the data path is open.

1 In the **Network Connections** screen you should see the **Status** as **Connected**



Network Connections

Name	Status	Action
WAN PON	Connected	✎
LAN Hardware Ethernet Switch	Connected	✎
Data VLAN 200 Bridge	Connected	✎ ✗
Data VLAN 200 WAN Ethernet	Connected	✎ ✗
Data VLAN 200 LAN Ethernet	Connected	✎ ✗
New Connection		✱

The view above is the advanced view (click the **Advanced** button).

2 Open a DOS window and ping the upstream gateway (provided in your environment setup)

If you cannot ping it means you do not have data access to your gateway. If you show connected on the WAN PON and the bridge, it means you have access on VLAN 200.

You should be able to verify the gateway is up by pinging from the MXK. On the MXK, just do a normal ping to the gateway as you would from a DOS window.

If you have access to the gateway from the MXK, do a few **bridge stats** commands to verify the bridge is accepting and receiving packets

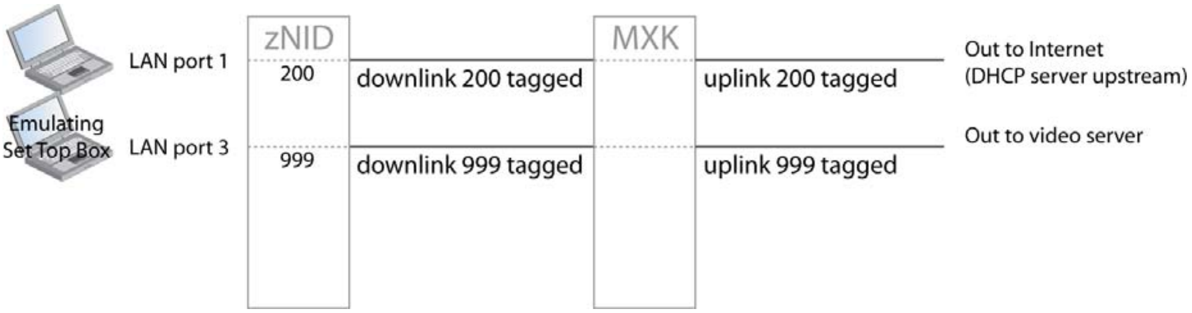
3 Open a browser to a public site

As long as you can ping you are showing that you have a data path through the zNID and the MXK to the Internet gateway. As long as that gateway has access to the Internet you should be able to open a browser and bring up a page.

Configuring IPTV, GPON

We will use the fast path feature to define a 999 VLAN which pushes the packets directly out to LAN port 3.

Figure 19: Passing data and video packets on separate bridges



Configuring the zNID for IPTV

1 Open Fast Path

a From the left hand menu pane, click **Advanced**

b Click the Fast Path icon

2 Select the ports

a Select the subscriber port(s)

We will select **Ethernet Port 3**

b From the WAN Device dropdown, select the WAN interface (WAN PON)

3 Define the VLAN by entering the VLAN ID (999) in the **VID** text box

4 In the **Priority** text box enter a priority (3)

5 Click **OK**

Configuring the MXK for IPTV

1 Create uplink and add bridge-path

The switch which is upstream from our MXK is providing a video stream on VLAN 999. The packets are tagged from the switch.The bridge-path add command defines this bridge interface as the uplink for the VLAN 999 downlinks.

Note: For all of the scenario examples in this application guide we are using the same uplinks/upstream interfaces, so if you have already created the uplink/upstream bridge interfaces, you will not need to recreate the video uplink bridge-path here.

```
zSH> bridge add 1-a-5-0/eth uplink vlan 999 tagged
```

```
Adding bridge on 1-a-5-0/eth
Created bridge-interface-record ethernet5-200/bridge

zSH> bridge-path add ethernet5-200/bridge vlan 200 default
Bridge-path added successfully
```

2 Add the dowlink to the zNID

Just as with the data bridge, we will be passing single-tagged packets, this time vlan 999.

```
DOC-MXK> bridge add 1-4-1-901/gponport downlink vlan 999 tagged
Adding bridge on 1-4-1-901/gponport
Created bridge-interface-record 1-4-1-901-gponport-999/bridge
```

3 Verify the bridge using the **bridge show** command

```
DOC-MXK> bridge show

Type VLAN        Bridge                         St  Table Data
-------------------------------------------------------------------------


tls Tagged 160   ipobridge-160/bridge           UP  D 00:01:47:1a:fe:64
tls Tagged 160   1-4-1-501-gponport-160/bridge  UP
tls          160 ethernet4/bridge               UP  D 00:00:86:43:3c:e4
                                                    D 00:00:86:43:ec:69
upl Tagged 999   ethernet5-999/bridge           UP  S VLAN 999 default
dwn Tagged 999   1-4-1-901-gponport-999/bridge  UP  D 00:10:a4:b1:f0:bf
                                                    D 01:00:5e:0a:0a:0a
dwn Tagged 200   1-4-1-501-gponport-200/bridge  UP  D 00:01:47:07:1d:fa
upl Tagged 200   ethernet5-200/bridge           UP  S VLAN 200 default
```

Because the zNID is already active on the line it does not need to be activated.

Testing the IPTV bridge

Since we are using a laptop and software to emulate a set top box, we can ping out to the video server.

1. Ping the upstream gateway (provided in your environment setup)

   If you cannot ping it means you do not have data access to your gateway. If you show connected on the WAN PON and the bridge, it means you have access on VLAN 200.

   You should be able to verify the gateway is up by pinging from the MXK. On the MXK, just do a normal ping to the gateway as you would from a DOS window.

   If you have access to the gateway from the MXK, do a few **bridge stats** commands to verify the bridge is accepting and receiving packets

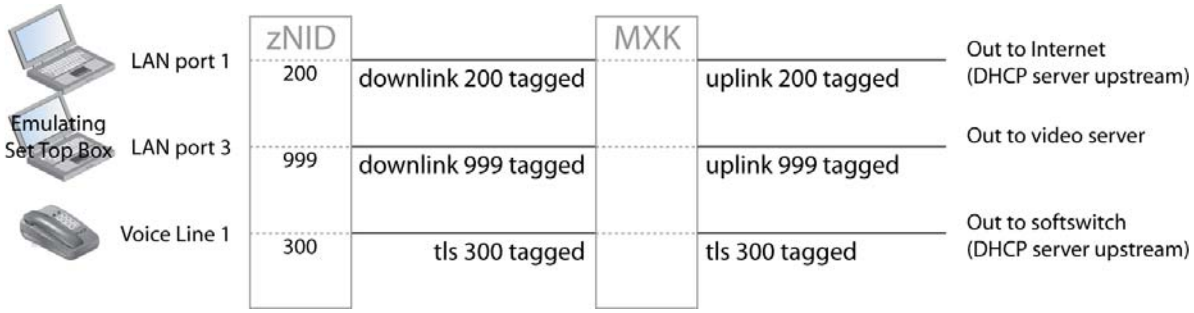
2. Open the STB emulation software and connect to the video server

   As long as you can ping you are showing that you have a data path through the zNID and the MXK to the video server. You should be able to connect to the video stream with the STB emulation software.

Configuring VoIP, GPON

Instead of using an uplink-downlink bridge for VoIP, we will use a TLS bridge. The TLS bridge allows for bridge forwarding table timeouts, so if the MAC address has timed out, incoming calls from the softswitch will flood the TLS bridge and relearn the MAC address.

Figure 20: Adding a TLS bridge for voice services



Configuring the zNID for VoIP

1 Add a VLAN ID on the WAN interface as we did when building the data bridge

a Click **Network Connections** in the left hand menu pane

b In the **Networks Connection** page, click **New Connection**

c In the **Connection Wizard** screen select **Advanced Connection** and click **Next**

d In the **Advanced Configuration** screen select **VLAN Interface** and click **Next** near the bottom of the screen

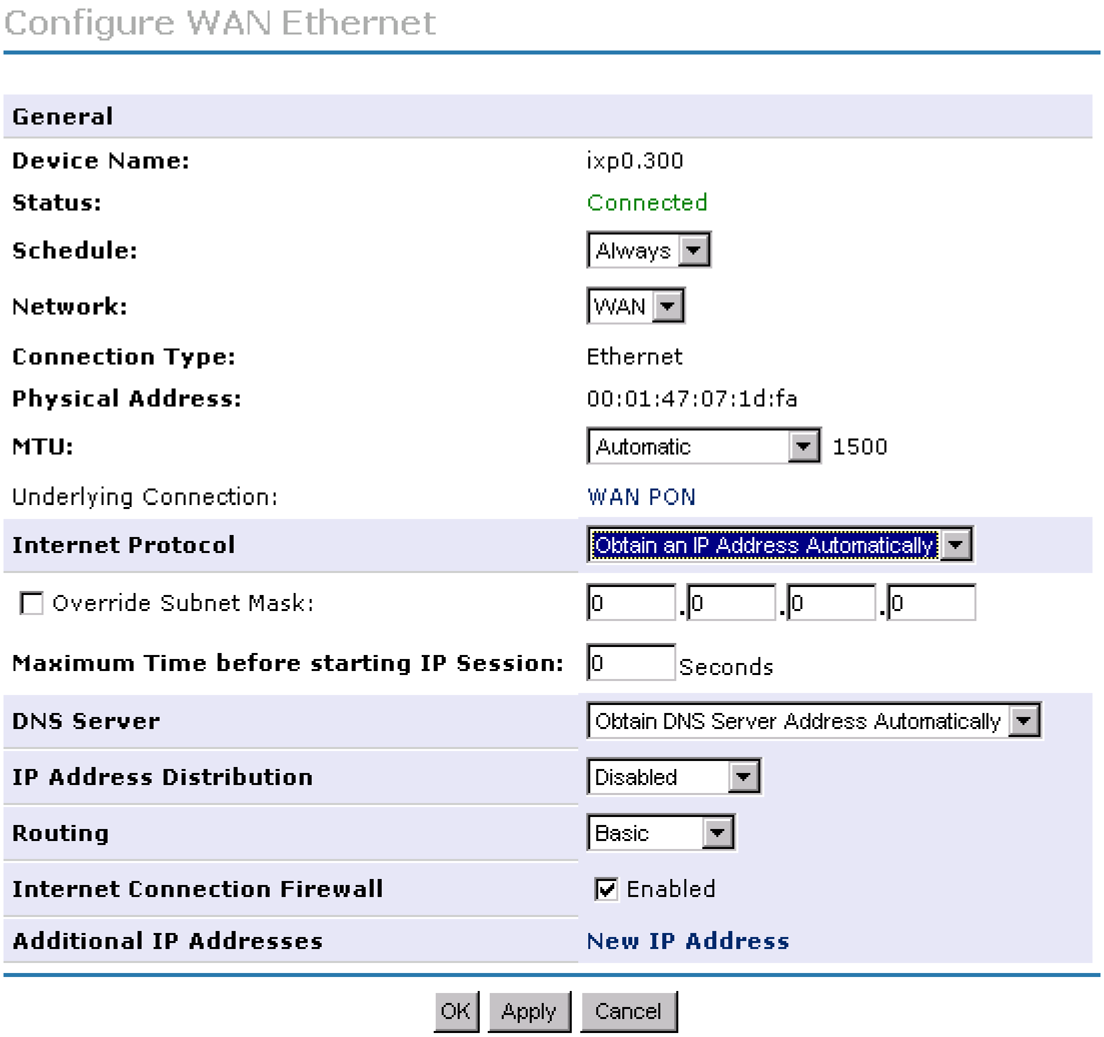
e From the **Underlying Device** drop down select the physical WAN port (**WAN PON**) to associate with the VLAN ID

f In the **VLAN ID** text box enter the VLAN ID (300), then click **Next**

g In the **Connection Summary** screen select **Edit the Newly Created Connection**, then click **Finish**

h From the **Internet Protocol** drop down in the **Configure WAN Ethernet** screen (the interface you just created), select Obtain an IP Address Automatically.

From the DNS Server drop down you should have selected Obtain DNS Server Address Automatically



Configure WAN Ethernet

General	
Device Name:	ixp0.300
Status:	Connected
Schedule:	Always ▼
Network:	WAN ▼
Connection Type:	Ethernet
Physical Address:	00:01:47:07:1d:fa
MTU:	Automatic ▼ 1500
Underlying Connection:	WAN PON
Internet Protocol	Obtain an IP Address Automatically ▼
□ Override Subnet Mask:	0 . 0 . 0 . 0
Maximum Time before starting IP Session:	0 Seconds
DNS Server	Obtain DNS Server Address Automatically ▼
IP Address Distribution	Disabled ▼
Routing	Basic ▼
Internet Connection Firewall	☑ Enabled
Additional IP Addresses	New IP Address

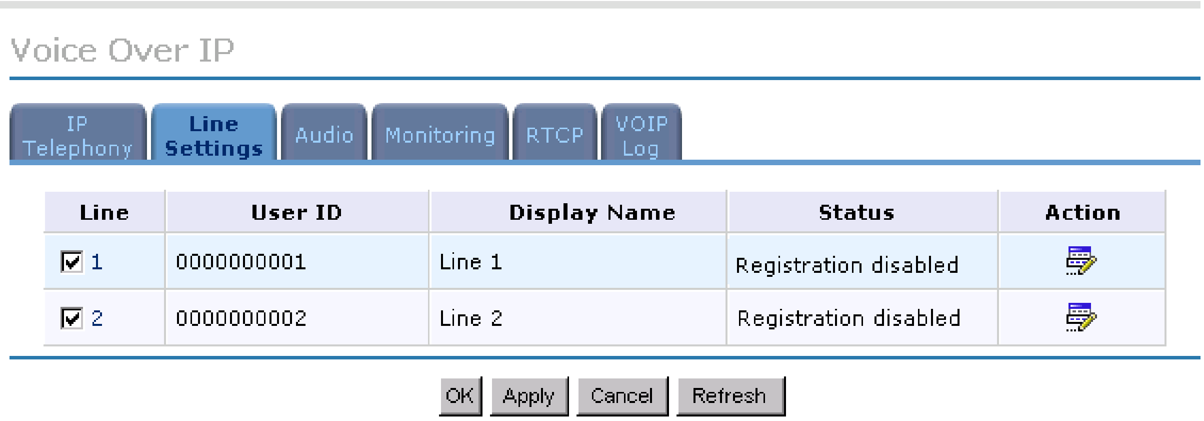
i Click **OK**

j Rename the interface by clicking the action icon for the **WAN Ethernet** interface you just created, entering **VoIP VLAN 300 Ethernet** in the **Name** text box, then click **OK**

2 Name the phone connection

a In the left hand menu pane, click **Voice Over IP**

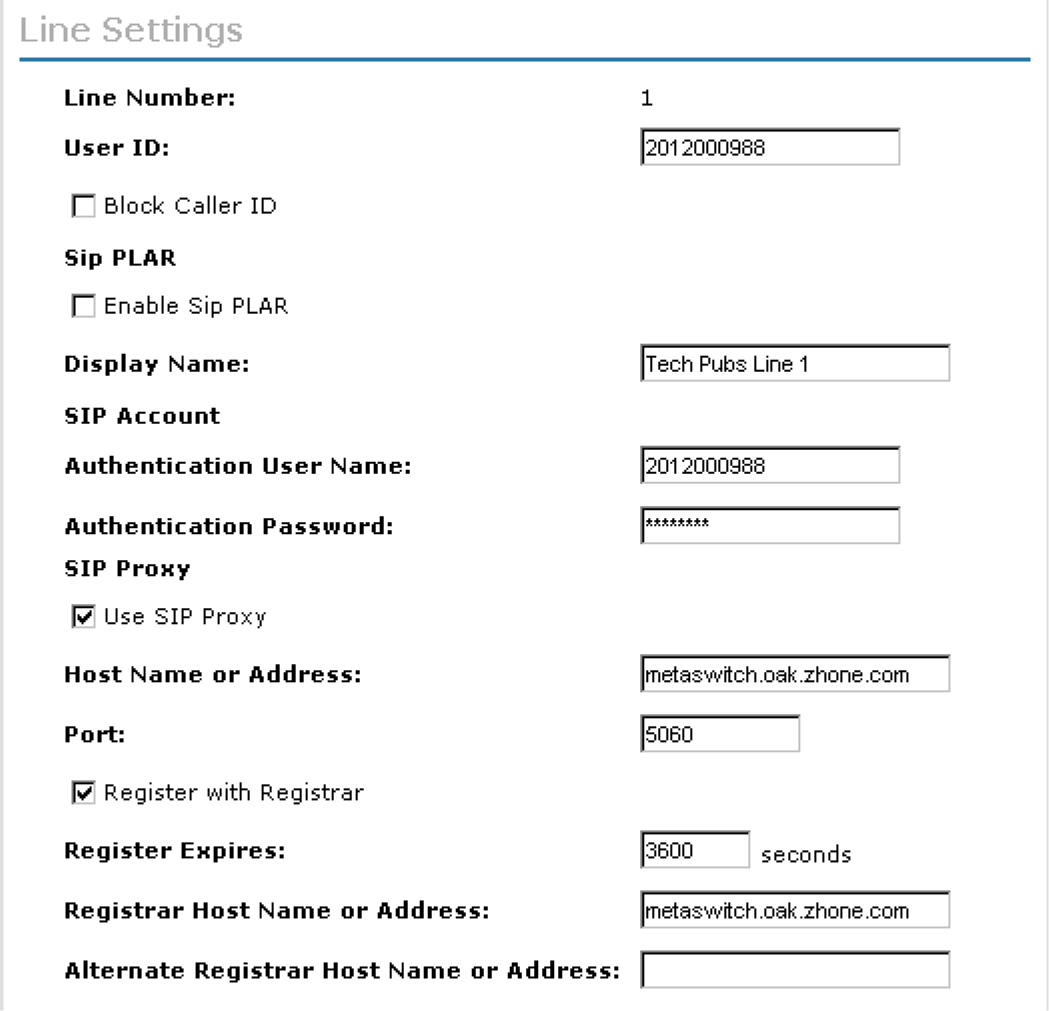
b In the **Voice Over IP** screen, select the **Line Settings** tab



Line	User ID	Display Name	Status	Action
☑ 1	0000000001	Line 1	Registration disabled	✎
☑ 2	0000000002	Line 2	Registration disabled	✎

c In the **Line Settings** tab click the action button for the line text box enter the assigned phone number

d In the **User ID** text box enter the assigned User ID



Line Number:	1
User ID:	2012000988
□ Block Caller ID	
Sip PLAR	
□ Enable Sip PLAR	
Display Name:	Tech Pubs Line 1
SIP Account	
Authentication User Name:	2012000988
Authentication Password:	********
SIP Proxy	
☑ Use SIP Proxy	
Host Name or Address:	metaswitch.oak.zhone.com
Port:	5060
☑ Register with Registrar	
Register Expires:	3600 seconds
Registrar Host Name or Address:	metaswitch.oak.zhone.com
Alternate Registrar Host Name or Address:	

e In the **Display Name text** box enter a name for the phone connection

3 Enter the authentication information

   a In the **Authentication User Name** text box under **SIP Account** enter the assigned user name

   b In the **Authentication Password** text box enter the assigned password

4 Select the phone connection type.

   We will use SIP Proxy.

   a Select Use **SIP Proxy**

   b In the **Host Name or Address** text box under **SIP Proxy** enter the fully qualified address for the softswitch server.

   c In the **Registrar Host Name or Address** text box under **SIP Proxy** enter the fully qualified address for the softswitch server.

   d Click **OK**

Configuring the MXK for VoIP

1 Add a TLS bridge interface on the uplink card

> **Note:** For all of the scenario examples in this application guide we are using the same uplinks/upstream interfaces, so if you have already created the uplink/upstream bridge interfaces, you will not need to recreate the voice upstream link here.

```
DOC-MXK> bridge add 1-a-5-0/eth tls vlan 300 tagged
Adding bridge on 1-a-5-0/eth
Created bridge-interface-record ethernet5-300/bridge
```

2 Add a TLS bridge interface on the GPON line card

```
DOC-MXK> bridge add 1-4-1-701/gponport tls vlan 300 tagged
Adding bridge on 1-4-1-701/gponport
Created bridge-interface-record 1-4-1-701-gponport-300/bridge
```

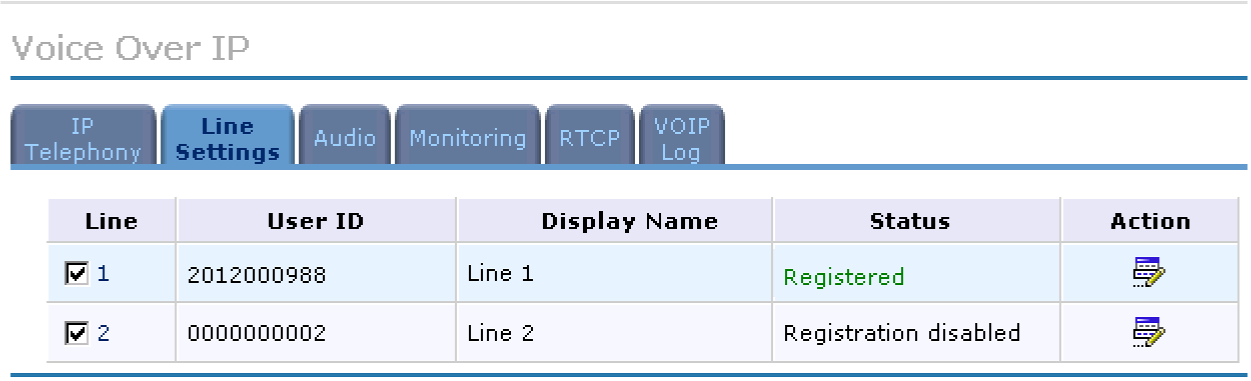
3 Verify the bridge using the **bridge show** command

```
DOC-MXK> bridge show

Type VLAN        Bridge                         St  Table Data
-------------------------------------------------------------------------

tls Tagged 160   ipobridge-160/bridge           UP  D 00:01:47:1a:fe:64
tls Tagged 160   1-4-1-501-gponport-160/bridge  UP
tls          160 ethernet4/bridge               UP  D 00:00:86:43:3c:e4
                                                    D 00:00:86:43:ec:69
upl Tagged 999   ethernet5-999/bridge           UP  S VLAN 999 default
dwn Tagged 999   1-4-1-901-gponport-999/bridge  UP  D 00:10:a4:b1:f0:bf
                                                    D 01:00:5e:0a:0a:0a
tls Tagged 300   ethernet5-300/bridge           UP  D 00:00:86:43:3c:e4
```

```
                                                    D 00:00:86:43:ec:69
                                                    D 00:01:47:1a:e4:74
                                                    D 00:01:47:1a:fe:64
                                                    D 08:00:20:b8:f6:58
tls Tagged 300   1-4-1-701-gponport-300/bridge  UP  D 00:01:47:07:1d:fa
dwn Tagged 200   1-4-1-501-gponport-200/bridge  UP  D 00:01:47:07:1d:fa
upl Tagged 200   ethernet6-200/bridge           UP  S VLAN 200 default
```

Testing the VoIP configuration

1 When the VoIP connection accesses the softswitch it will show as registered on the Voice Over IP page



Line	User ID	Display Name	Status	Action
☑ 1	2012000988	Line 1	Registered	✎
☑ 2	0000000002	Line 2	Registration disabled	✎

2 Making or receiving a phone call

Configuring Triple Play: Data, Video and Voice, GPON

If you have already followed the above procedures for configuring data, video and voice, then you should have triple play working for your solution.

- *Configuring a bridge for data, GPON* on page 75
- *Configuring IPTV, GPON* on page 84
- *Configuring VoIP, GPON* on page 87

Configuring browser-based Active Ethernet zNIDs

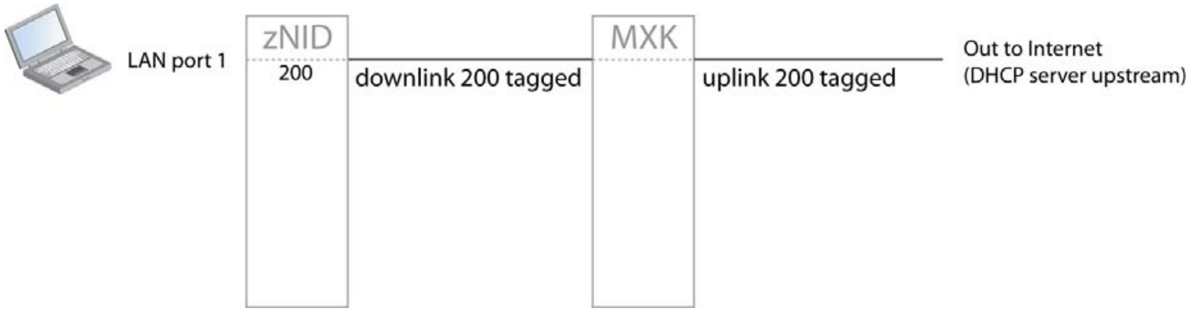
Configuring a bridge for data, Active Ethernet

Just as with the GPON solution to configure a bridge to the zNID, you must have a bridge on the MXK (The Active Ethernet card acts as the OLT; in fact, each port can be considered a separate OLT). To build a bridge that reaches the subscriber devices bridges need to be built on the zNID.

For each service we will be adding a separate bridge with its own VLAN. For the data and video services we will set up an uplink and downlink bridge. From the perspective of each access device, the MXK and zNID, this means creating a bridge from the upstream interface to the downstream interface.

For data services we will create a bridge on the MXK from the Internet uplink to the Active Ethernet downlink. On the zNID we will create a bridge from the WAN Ethernet interface to LAN 2 port. For data coming from the PC to the LAN port we will need to add a VLAN header, so the packets will be designated VLAN 200. Packets going downstream to the PC on LAN 2 port will likewise have the VLAN information stripped because the PC does not need tagged packets; only packets with VLAN 200 will be delivered to the LAN 2 interface.

Figure 21: Bridges on the MXK and zNID to pass data traffic



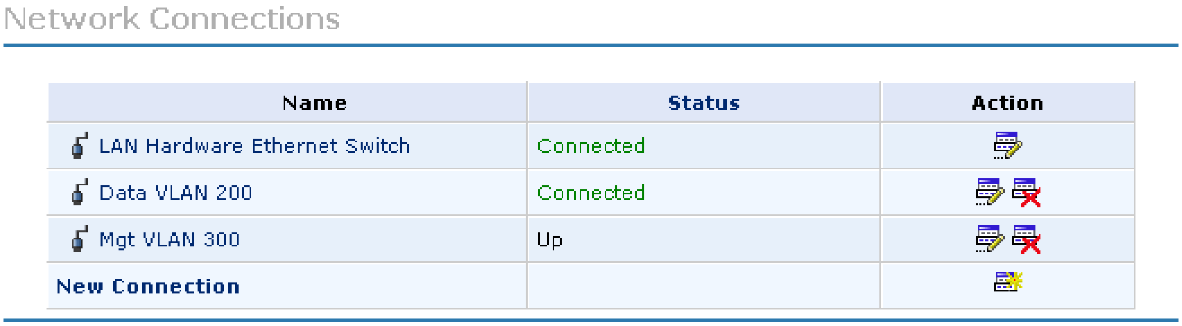
Clearing off the default settings of the zNID

We will remove the default connections, so we can go through the steps of creating a solution.

1 Click **Network Connections** in the left hand menu pane

2 In the **Network Connections** page, delete **Data VLAN 200** by clicking the delete action icon for that item, then click **OK** to confirm

3 Delete **Management VLAN 300** by clicking the delete action for that item, then click **OK** to confirm



Network Connections

Name	Status	Action
LAN Hardware Ethernet Switch	Connected	✎
Data VLAN 200	Connected	✎ ✗
Mgt VLAN 300	Up	✎ ✗
New Connection		✱

Creating a bridge on the zNID

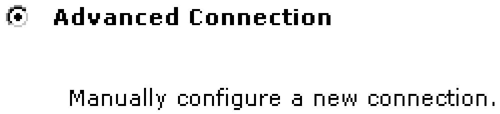
We will create a bridge on the zNID.

1 Add a VLAN ID on the WAN interface

a Click **Network Connections** in the left hand menu pane

b In the **Networks Connection** page, click **New Connection**

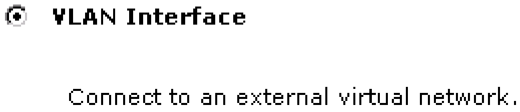
c In the **Connection Wizard** screen select **Advanced Connection** and click **Next**



● **Advanced Connection**

Manually configure a new connection.

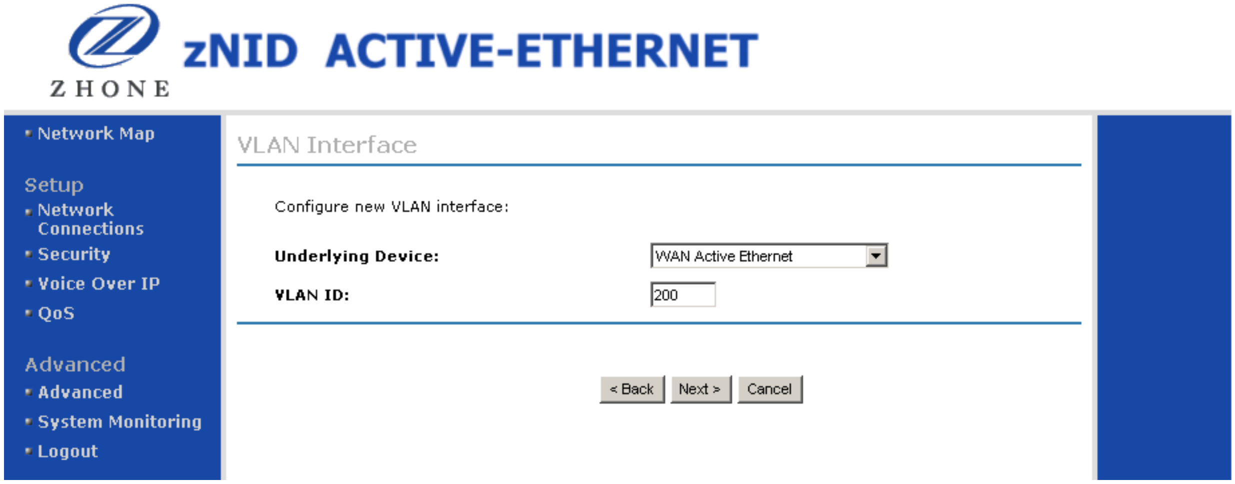
d In the **Advanced Configuration** screen select **VLAN Interface** and click **Next** near the bottom of the screen



● **VLAN Interface**

Connect to an external virtual network.

e From the **Underlying Device** drop down select the physical WAN port (**WAN Active Ethernet**) to associate with the VLAN ID



VLAN Interface

Configure new VLAN interface:

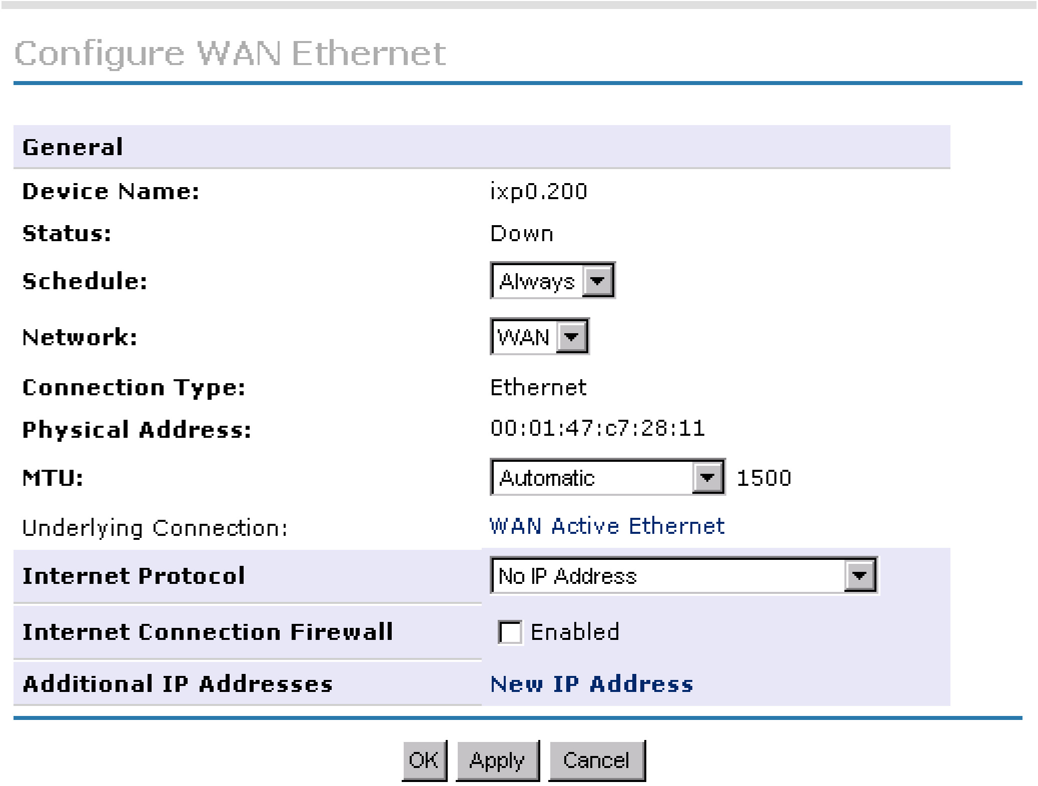
Underlying Device:	WAN Active Ethernet
VLAN ID:	200

f In the **VLAN ID** text box enter the VLAN ID (200), then click **Next**

g In the **Connection Summary** screen select **Edit the Newly Created Connection**, then click **Finish**

h Verify the WAN Ethernet interface has been created, then click **OK**

Figure 22: The create WAN Ethernet interface



Configure WAN Ethernet

General	
Device Name:	ixp0.200
Status:	Down
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00:01:47:c7:28:11
MTU:	Automatic 1500
Underlying Connection:	WAN Active Ethernet
Internet Protocol	No IP Address
Internet Connection Firewall	□ Enabled
Additional IP Addresses	New IP Address

- **i** Name the interface by clicking the edit icon for the **WAN Ethernet** interface you just created, then enter an appropriate name in the **Name** text box and click **OK**

  We will use **Data VLAN 200 WAN Ethernet**.

2 Add a VLAN ID to the LAN switch

- **a** Click **Network Connections** in the left hand menu pane
- **b** In the **Networks Connection** page, click **New Connection**
- **c** In the **Connection Wizard** screen select **Advanced Connection** and click **Next**
- **d** In the **Advanced Connection** screen select **VLAN Interface** and click **Next**
- **e** From the **Underlying Device** dropdown select the Ethernet switch to associate with the VLAN ID (**LAN Hardware Ethernet Switch**)
- **f** In the **VLAN ID** text box enter the VLAN ID (200), then click **Next**
- **g** In the **Connection Summary** screen select **Edit the Newly Created Connection**, then click **Finish,** view the screen then click **OK**
- **h** Name the interface by clicking the edit icon for the **LAN Ethernet** interface you just created, then enter an appropriate name in the **Name** text box and click **Next**

  We will use **Data VLAN 200 LAN Ethernet**.

3 Build the bridge between (among) the interfaces

- **a** Click **Network Connections** in the left hand menu pane
- **b** In the **Networks Connection** page, click **New Connection**
- **c** In the **Connection Wizard** screen select **Advanced Connection** and click **Next**
- **d** In the **Conneciton Wizard** screen select **Network Bridging** then click **Next**
- **e** Select the connections to combine in the bridge (Data VLAN 200 WAN Ethernet and Data VLAN 200 LAN Ethernet) then click **Next**
- **f** In the **Connection Summary** screen select **Edit the Newly Created Connection** then click **Finish**
- **g** In the **Internet Protocol** drop down you should have **Obtain an IP address automatically** selected; click **OK**
- **h** Rename the bridge by clicking the edit icon for the bridge you just created in the **Network Connections** screen, then enter **Data VLAN 200 Bridge** in the **Name** text box and click **OK**

4 Map the VLAN ID to the physical port

- **a** Click **Network Connections** in the left hand menu pane b In the **Network Connections** screen click on the **LAN Hardware Ethernet Switch** link

c At the bottom of the **LAN Hardware Ethernet Switch Properties** screen click **Set** near the bottom of the screen

d Near the bottom of the **Configure LAN Hardware Ethernet Switch** screen select the action button for the port (Ethernet Port 2) to associate the VLAN

e In the **Port 2 Settings** screen, click **New Entry**

f Enter the VLAN ID (200) in the **VLAN ID** text box then click **OK**

g Click **OK** again to confirm

Creating an uplink and downlink bridge on the MXK

We will create an uplink and downlink for VLAN 200.

1 Create uplink and add bridge-path

If you are adding

The switch which is upstream from our MXK is providing a network on VLAN 200. The packets are tagged from the switch.The bridge-path add command defines this bridge interface as the uplink for the VLAN 200 downlinks.

Note: For all of the scenario examples in this application guide we are using the same uplinks/upstream interfaces, so if you have already created the uplink/upstream bridge interfaces, you will not need to recreate the data uplink/bridge-path here.

```
zSH> bridge add 1-a-5-0/eth uplink vlan 200 tagged

Adding bridge on 1-a-5-0/eth
Created bridge-interface-record ethernet5-200/bridge

zSH> bridge-path add ethernet5-200/bridge vlan 200 default
Bridge-path added successfully
```

2 Add the dowlink to the zNID

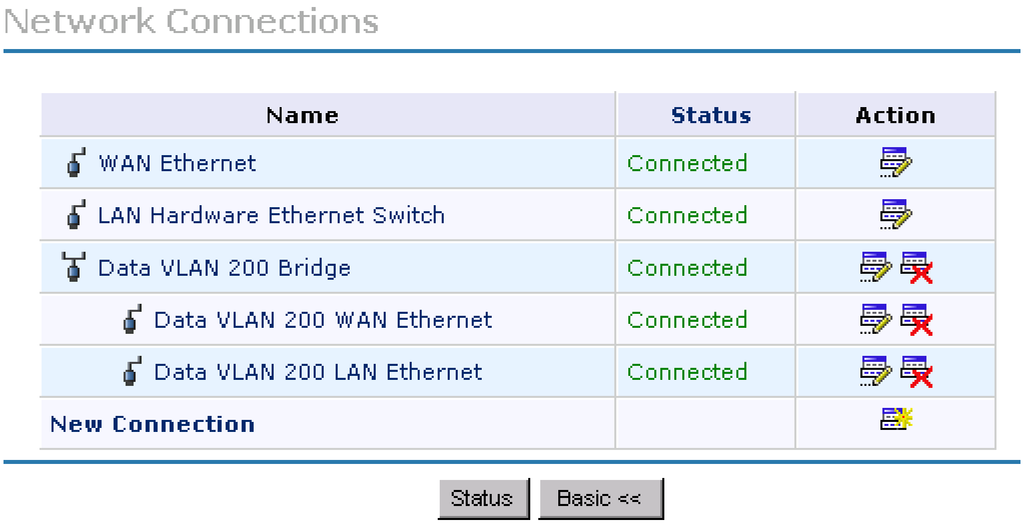
We are just passing the single tagged 200 packets down to the zNID. The zNID needs to know the VLAN ID to pass them through properly as well. We will configure the zNID for that as well.

```
DOC-MXK> bridge add 1-13-1-0/eth downlink vlan 200 tagged

Adding bridge on 1-13-1-0/eth

Created bridge-interface-record 1-13-1-0-eth-200/bridge
```

Testing the data bridge

To test the connection, we will put the laptop on the LAN 2 port, ping to the Internet gateway and open a browser. Pinging to the Internet gateway proves the data path is open.

1 In the **Network Connections** screen you should see the **Status** as **Connected**



Network Connections

Name	Status	Action
WAN Ethernet	Connected	✎
LAN Hardware Ethernet Switch	Connected	✎
Data VLAN 200 Bridge	Connected	✎ ✗
Data VLAN 200 WAN Ethernet	Connected	✎ ✗
Data VLAN 200 LAN Ethernet	Connected	✎ ✗
New Connection		✱

The view above is the advanced view (click the **Advanced** button).

2 Open a DOS window and ping the upstream gateway (provided in your environment setup)

If you cannot ping it means you do not have data access to your gateway. If you show connected on the WAN PON and the bridge, it means you have access on VLAN 200.

You should be able to verify the gateway is up by pinging from the MXK. On the MXK, just do a normal ping to the gateway as you would from a DOS window.

If you have access to the gateway from the MXK, do a few **bridge stats** commands to verify the bridge is accepting and receiving packets

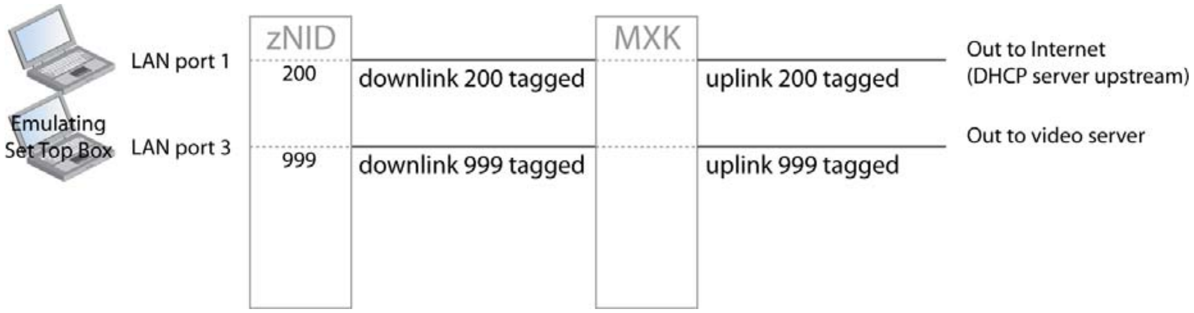
3 Open a browser to a public site

As long as you can ping you are showing that you have a data path through the zNID and the MXK to the Internet gateway. As long as that gateway has access to the Internet you should be able to open a browser and bring up a page.

Configuring IPTV, Active Ethernet

We will use the fast path feature to define a 999 VLAN which pushes the packets directly out to LAN port 3.

Figure 23: Passing data and video packets on separate bridges



Configuring the zNID for IPTV

1 Open Fast Path

- **a** From the left hand menu pane, click **Advanced**
- **b** Click the Fast Path icon

2 Select the ports

- **a** Select the subscriber port(s)

  We will select **Ethernet Port 3**
- **b** From the **WAN Device** dropdown, select the WAN interface (WAN PON)

3 Define the VLAN by entering the VLAN ID (999) in the **VID** text box

4 In the **Priority** text box enter a priority (3)

5 Click **OK**

Configuring the MXK for IPTV

1 Create uplink and add bridge-path

The switch which is upstream from our MXK is providing a video stream on VLAN 999. The packets are tagged from the switch.The bridge-path add command defines this bridge interface as the uplink for the VLAN 999 downlinks.

Note: For all of the scenario examples in this application guide we are using the same uplinks/upstream interfaces, so if you have already created the uplink/upstream bridge interfaces, you will not need to recreate the uplink/bridge-path here.

```
zSH> bridge add 1-a-5-0/eth uplink vlan 999 tagged
```

```
Adding bridge on 1-a-5-0/eth
Created bridge-interface-record ethernet5-200/bridge

zSH> bridge-path add ethernet5-200/bridge vlan 200 default
Bridge-path added successfully
```

2 Add the dowlink to the zNID

Just as with the data bridge, we will be passing single-tagged packets, this time vlan 999.

```
DOC-MXK> bridge add 1-13-1-1/eth downlink vlan 999 tagged
Adding bridge on 1-13-1-1/eth
Created bridge-interface-record 1-13-1-1-eth-999/bridge
```

3 Verify the bridge using the **bridge show** command

```
DOC-MXK> bridge show

Type VLAN        Bridge                         St  Table Data
-------------------------------------------------------------------------


tls Tagged 160   ipobridge-160/bridge           UP  D 00:01:47:1a:fe:64
tls          160 ethernet4/bridge               UP  D 00:00:86:43:3c:e4
                                                    D 00:00:86:43:ec:69
upl Tagged 999   ethernet5-999/bridge           UP  S VLAN 999 default
dwn Tagged 999    1-13-1-2-eth-999                UP  D 00:10:a4:b1:f0:bf
                                                    D 01:00:5e:0a:0a:0a
dwn Tagged 200   1-13-1-1-eth-200/bridge          UP  D 00:01:47:07:1d:fa
upl Tagged 200   ethernet5-200/bridge           UP  S VLAN 200 default
```

Testing the IPTV bridge

Since we are using a laptop and software to emulate a set top box, we can ping out to the video server.

1 Ping the upstream gateway (provided in your environment setup)

   If you cannot ping it means you do not have data access to your gateway. If you show connected on the WAN PON and the bridge, it means you have access on VLAN 200.

   You should be able to verify the gateway is up by pinging from the MXK. On the MXK, just do a normal ping to the gateway as you would from a DOS window.

   If you have access to the gateway from the MXK, do a few **bridge stats** commands to verify the bridge is accepting and receiving packets

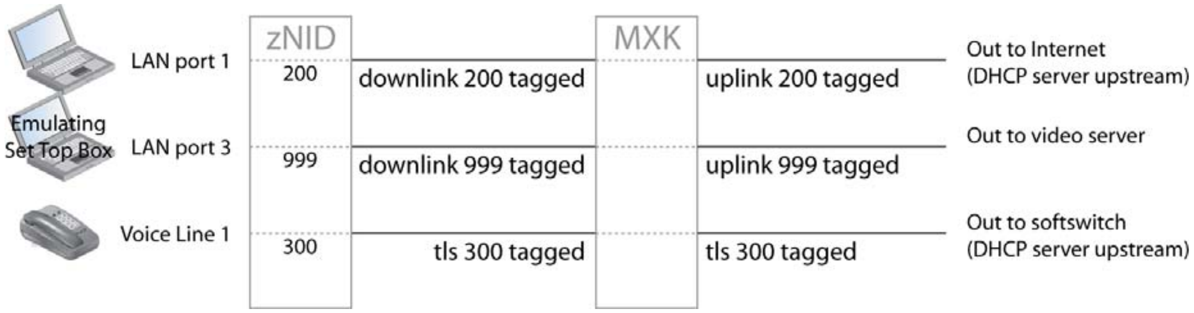
2 Open the STB emulation software and connect to the video server

   As long as you can ping you are showing that you have a data path through the zNID and the MXK to the video server. You should be able to connect to the video stream with the STB emulation software.

Configuring VoIP, Active Ethernet

Instead of using an uplink-downlink bridge for VoIP, we will use a TLS bridge. The TLS bridge allows for bridge forwarding table timeouts, so if the MAC address has timed out, incoming calls from the softswitch will flood the TLS bridge and relearn the MAC address.

Figure 24: Adding a TLS bridge for voice services



Configuring the zNID for VoIP

1 Add a VLAN ID on the WAN interface as we did when building the data bridge

   a Click **Network Connections** in the left hand menu pane

   b In the **Networks Connection** page, click **New Connection**

   c In the **Connection Wizard** screen select **Advanced Connection** and click **Next**

   d In the **Advanced Configuration** screen select **VLAN Interface** and click **Next** near the bottom of the screen

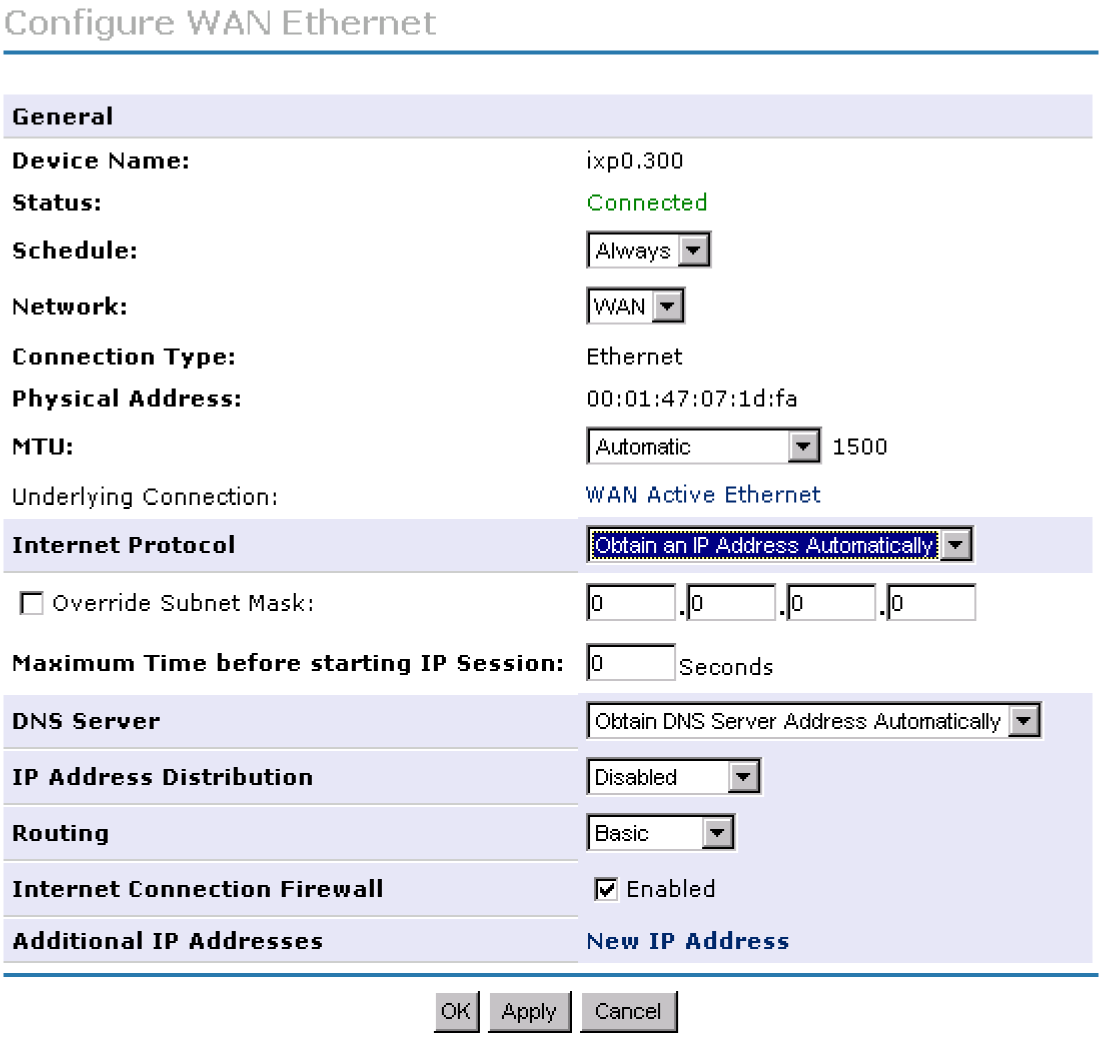
   e From the **Underlying Device** drop down select the physical WAN port (**WAN Ethernet**) to associate with the VLAN ID

   f In the **VLAN ID** text box enter the VLAN ID (300), then click **Next**

   g In the **Connection Summary** screen select **Edit the Newly Created Connection**, then click **Finish**

   h From the **Internet Protocol** drop down in the **Configure WAN Ethernet** screen (the interface you just created), select **Obtain an IP Address Automatically**.

From the DNS Server drop down you should have selected **Obtain DNS Server Address Automatically**



Configure WAN Ethernet

General	
Device Name:	ixp0.300
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00:01:47:07:1d:fa
MTU:	Automatic 1500
Underlying Connection:	WAN Active Ethernet
Internet Protocol	Obtain an IP Address Automatically
□ Override Subnet Mask:	0.0.0.0
Maximum Time before starting IP Session:	0 Seconds
DNS Server	Obtain DNS Server Address Automatically
IP Address Distribution	Disabled
Routing	Basic
Internet Connection Firewall	☑ Enabled
Additional IP Addresses	New IP Address

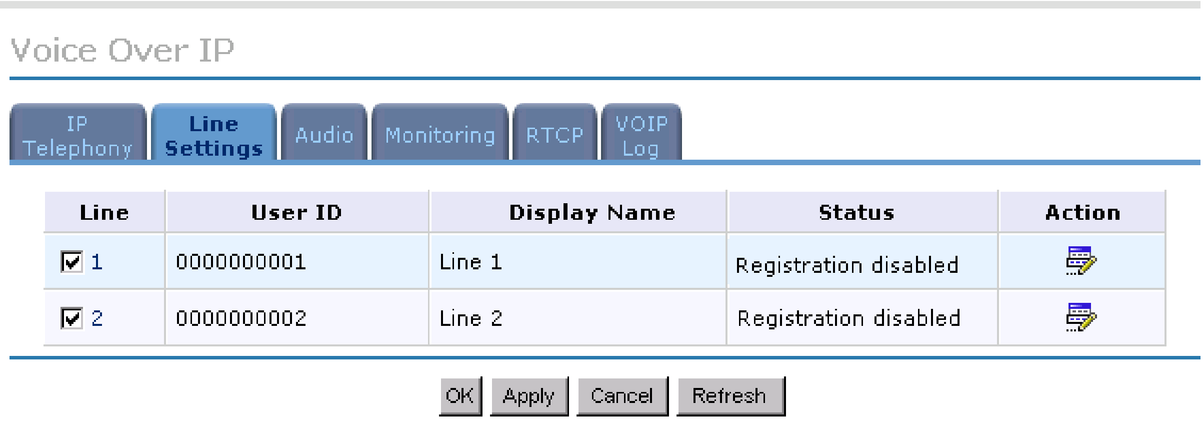
i Click **OK**

j Rename the interface by clicking the action icon for the **WAN Ethernet** interface you just created, entering **VoIP VLAN 300 Ethernet** in the **Name** text box, then click **OK**

2 Name the phone connection

a In the left hand menu pane, click **Voice Over IP**

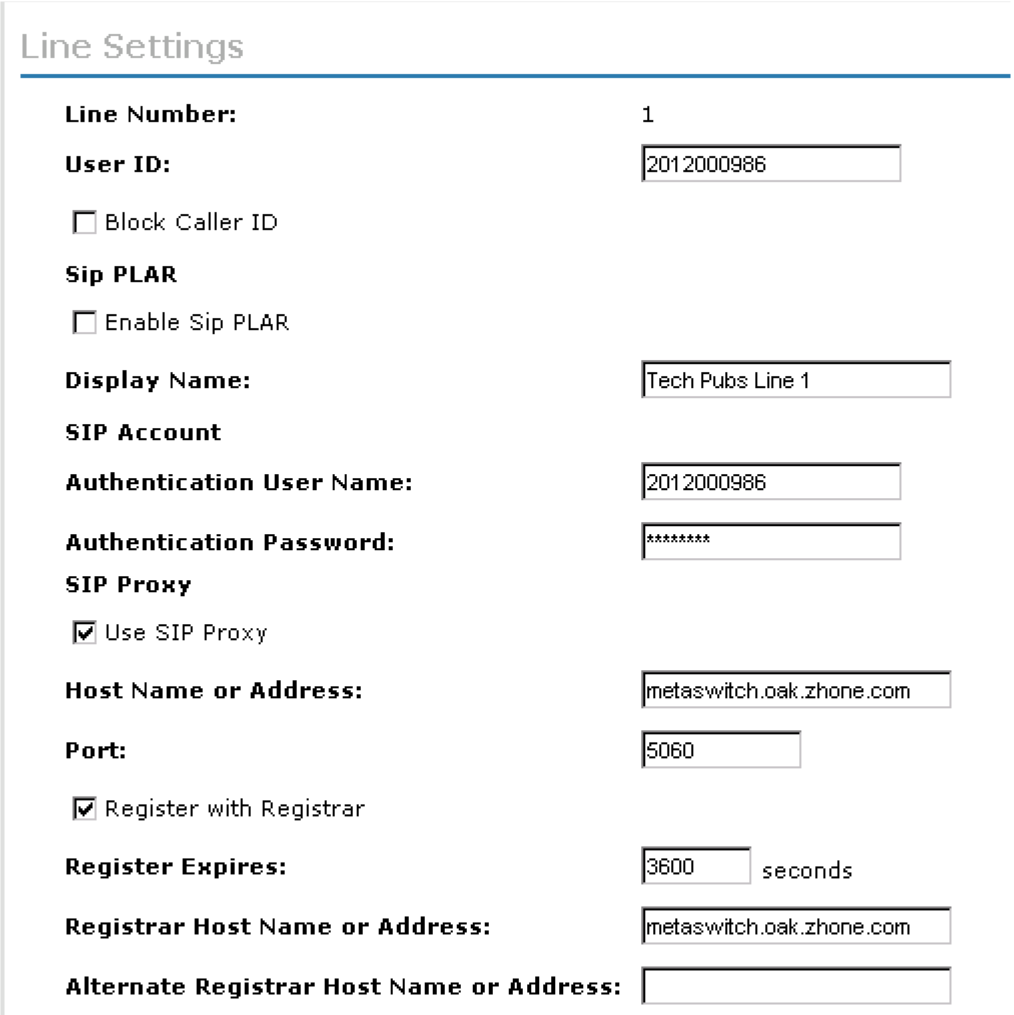
b In the **Voice Over IP** screen, select the **Line Settings** tab



Line	User ID	Display Name	Status	Action
☑ 1	0000000001	Line 1	Registration disabled	✎
☑ 2	0000000002	Line 2	Registration disabled	✎

c In the **Line Settings** tab click the action button for the line text box enter the assigned phone number

d In the **User ID** text box enter the assigned User ID



Line Number:	1
User ID:	2012000986
□ Block Caller ID	
Sip PLAR	
□ Enable Sip PLAR	
Display Name:	Tech Pubs Line 1
SIP Account	
Authentication User Name:	2012000986
Authentication Password:	********
SIP Proxy	
☑ Use SIP Proxy	
Host Name or Address:	metaswitch.oak.zhone.com
Port:	5060
☑ Register with Registrar	
Register Expires:	3600 seconds
Registrar Host Name or Address:	metaswitch.oak.zhone.com
Alternate Registrar Host Name or Address:	

e In the **Display Name text** box enter a name for the phone connection

3 Enter the authentication information

- **a** In the **Authentication User Name** text box under **SIP Account** enter the assigned user name
- **b** In the **Authentication Password** text box enter the assigned password

4 Select the phone connection type.

We will use SIP Proxy.

- **a** Select Use **SIP Proxy**
- **b** In the **Host Name or Address** text box under **SIP Proxy** enter the fully qualified address for the softswitch server.
- **c** In the **Registrar Host Name or Address** text box under **SIP Proxy** enter the fully qualified address for the softswitch server.
- **d** Click **OK**

Configuring the MXK for VoIP

1 Add a TLS bridge interface on the uplink card

> **Note:** For all of the scenario examples in this application guide we are using the same uplinks/upstream interfaces, so if you have already created the uplink/upstream bridge interfaces, you will not need to recreate the upstream link here.

```
DOC-MXK> bridge add 1-a-5-0/eth tls vlan 300 tagged
Adding bridge on 1-a-5-0/eth
Created bridge-interface-record ethernet5-300/bridge
```

2 Add a TLS bridge interface on the GPON line card

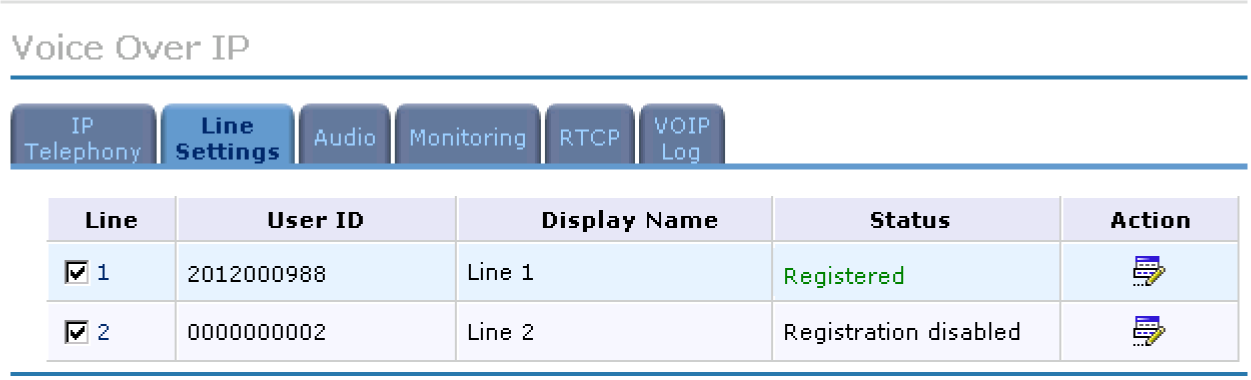
```
DOC-MXK> bridge add 1-13-1-3/eth tls vlan 300 tagged
Adding bridge on 1-13-1-3/eth
Created bridge-interface-record 1-13-1-3-eth-300/bridge
```

3 Verify the bridge using the **bridge show** command

```
DOC-MXK> bridge show

Type VLAN        Bridge                         St  Table Data
-------------------------------------------------------------------------


tls Tagged 160   ipobridge-160/bridge           UP  D 00:01:47:1a:fe:64
tls          160 ethernet4/bridge               UP  D 00:00:86:43:3c:e4
                                                    D 00:00:86:43:ec:69
upl Tagged 999   ethernet5-999/bridge           UP  S VLAN 999 default
dwn Tagged 999    1-13-1-2-eth-999                UP  D 00:10:a4:b1:f0:bf
                                                    D 01:00:5e:0a:0a:0a
tls Tagged 300   ethernet5-300/bridge           UP  D 00:00:86:43:3c:e4
                                                    D 00:00:86:43:ec:69
                                                    D 00:01:47:1a:e4:74
                                                    D 00:01:47:1a:fe:64
                                                    D 08:00:20:b8:f6:58
tls Tagged 300   1-13-1-3-eth-300/bridge        UP  D 00:01:47:07:1d:fa
upl Tagged 200   ethernet6-200/bridge           UP  S VLAN 200 default

dwn Tagged 200   1-13-1-1-eth-200/bridgeUP  D 00:01:47:07:1d:fa
```

Testing the VoIP configuration

1 When the VoIP connection accesses the softswitch it will show as registered on the Voice Over IP page



Voice Over IP

Line	User ID	Display Name	Status	Action
☑ 1	2012000988	Line 1	Registered	✎
☑ 2	0000000002	Line 2	Registration disabled	✎

2 Making or receiving a phone call

Configuring Triple Play: Data, Video and Voice, Active Ethernet

If you have already followed the above procedures for configuring data, video and voice, then you should have triple play working for your solution.

- *Configuring a bridge for data, Active Ethernet* on page 92
- *Configuring IPTV, Active Ethernet* on page 99
- *Configuring VoIP, Active Ethernet* on page 102

APPENDIX: HANDLING FIBER

In this appendix we will briefly introduce some issues when working with a fiber optic network. This section is not intended to be comprehensive, nor to describe any of the issues in great detail, but more as a warning that fiber, while it has many performance advantages than copper, fiber requires a different discipline than copper in its use.

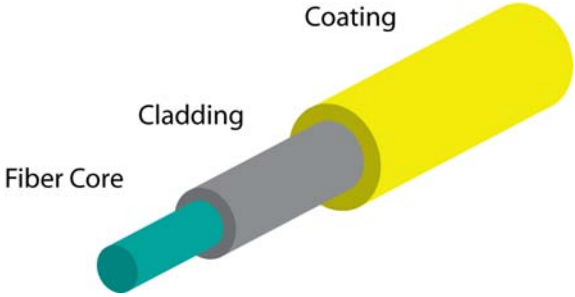
Topics to be covered in the examples in this appendix:

- Parts of the fiber optic cable, page 108
- Fiber connector types, page 108
- Installation testing, page 110
- Physical layer issues, page 110
- Cleaning and inspecting fiber connections, page 111
- Warnings, page 111
- Fiber handling best practices, page 109

Parts of the fiber optic cable

Fiber cable consists of three main parts: the fiber core, cladding and coating. The core is the media where the light travels.

Figure 25: Parts of the cable



- Fiber Core

  The glass transport media

- Cladding

  Cladding is a cushioning layer of glass resin which reflects light back into the core.

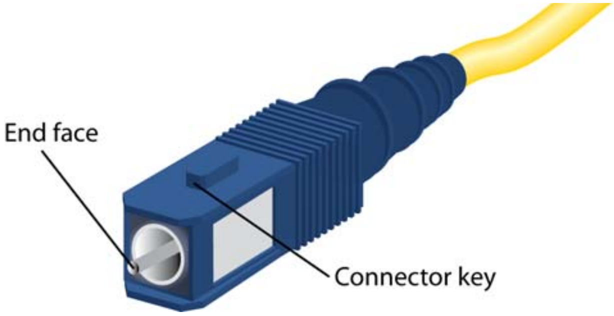
- Coating

  The coating layer is usually a durable plastic, teflon, rubber, or similar material to protect the cladding and fiber core.

- End eace

  The End face is the part of the connector which makes contact with the fiber transceiver. Connector failure is usually due to dirty or damaged end face.

  Fiber cables need to be aligned to pass light correctly. The mechanical part of the connector is keyed so the cable will be aligned properly.



Fiber connector types

There are two types of Fiber connectors which Zhone uses:

- UPC (Ultra Physical Contact) connectors

UPC connectors are used for connecting to the MXK GPON line card. UPC connectors have a -.55dB reflectance value.

- APC (Angled Physical Contact) connector

  APC connectors are used for connecting to zNIDs. APC connectors have an industry standard 8 degree angle on the end face of ferrule and have a -.65db reflectance value.

Do not use APC and UPC except where they belong because the mismatch of the UPC end (slightly spherical end) and the APC (angled end) could result in an air gap between the two connectors, creating back reflection or other optical loss conditions.

APC and UPC connectors use a coding standard:

- Blue: UPC
- Green: APC

✓ **Note:** Older APC connectors may not use the industry standard 8 degree angle and the difference between the standardized end face and a non-standard angled end face could result in an air gap condition.

Zhone uses SC connectors only, not FC connectors.

Fiber handling best practices

You should never look into the end of a fiber connector or opening with the naked eye. You should always use a scope.

- Do not handle pieces of optical fiber with fingers. Use tweezers or adhesive tape to lift and discard any loose optical fiber ends.

  Grasp only the connector housing when plugging or unplugging connectors. Do not touch the fiber ends with bare fingers. If you accidentally touch the end face of the fiber, inspect and clean the fiber end face. If there is the possibility of fiber clippings wash your hands immediately as the small bits of glass may not be visible and can cause eye damage.

- You should wear rubber gloves when cleaning optical connections. The gloves prevent contamination of the ferrule from skin oils. The gloves also protect your hands from the isopropryl alcohol.
- You should use caution when handling optical fibers. Fiber clippings should be put in a plastic container used solely for that purpose. Put the optical fibers in a safe location during installation.
- Keep all optical ports and connectors securely covered with a connector cap or a clean dust cap.

- Store unused dust caps in re-sealable containers to prevent them from becoming contaminated with dust or other particulates which could then contaminate the ferrule.

Installation testing

When installing fiber, especially GPON installations, you should have a link loss budget map, then as you install components, test the attenuation before and after each component. This testing should include testing before and after long leads. Matching the actual results with the theoretical link budget loss figures should help identify problems with the installation.

Testing equipment

There are a number of tools which can be used for testing optical lines.

- PON optical power meter

  Tests the strength of the optical signal, use for testing transmit and receive power levels

- Optical Time Domain Reflectometer (OTDR)

  OTDRs help identify breaks and stresses in spans and splices. OTDRs also help identify losses from splitters.

  The OTDR creates a trace of signal power received against the time a pulse is launched into the fiber. The OTDR analyzes the signals that are returned by reflections caused by connectors, splices, bends or other issues (such as errors in the fiber that cause reflections). These reflections from the fiber are seen as events along the time axis

- Light source

  Provides a signal for testing.

- Fiber probe

  The fiber probe is basically a handheld microscope which has a viewing screen to inspect connectors and cable ends which are being prepared for splicing.

Physical layer issues

Bend radius

Optical cables may not be bent smaller than a certain radius. The signal will refract rather than bend along with the cable. You may actually be able to see light through the insulation which means the light is not being efficiently transmitted down the cable. The tighter the bend radius, the greater the signal reduction.

Bending the fiber optical cable too far may also damage the fiber itself by creating micro cracks in the glass. Most industry standards describe one inch as the minimum bend on a fiber optic cable, though a good rule of thumb is to keep the bend radius greater than two inches.

Connector loss

Each connector or component in the Optical Deployment Network may have an effect on signal loss. Special fiber coupling gels may be applied between glass surfaces to reduce signal loss at connectors.

Fibers must be aligned. The fiber connectors are keyed so they will be aligned. Even with the keyed fibers you may need to jiggle the connector slightly so the connectors will match properly.

With testing before and after components, these types of connector loss problems may be quickly identified and resolved.

Cleaning and inspecting fiber connections

Dirt, dust, oil or other substances may obstruct the passing of light through the end faces. Upon delivery the ends of fiber connectors usually have (and should have) a cover to keep the connector clean. Because many common particulates may interfere with the optical connection, discipline in keeping fiber clean is very important.

Notable contaminents include:

- Oil from hands
- Dust particles
- Lint
- The residue that may be left when using wet cleaning methods
- Scratches which may be from dry cleaning methods or the mishandling of the fiber

Warnings

WARNING! Never look into

- **an active optical fiber**
- **an optical fiber connector opening of an active or powered-up unit**

WARNING! Prevent direct exposure to optical fiber ends or optical connector ends where laser signals are directly accessed

WARNING! Exposure to invisible LASER radiation may cause serious retinal damage or even blindness.

WARNING! Verify the optical source is disabled through the use of an optical power meter before handling optical fibers

WARNING! Wear safety glasses when installing optical fibers

WARNING! Clean hands after handling optical fibers

- **Small pieces of glass are not always visible and can cause eye damage**
- **Get medical assistance immediately for any glass that comes into eye contact.**

WARNING! Follow the manufacturer instructions when using an optical test set. Incorrect calibration or control settings can create hazardous levels of radiation