AMG1001-T series

ADSL2+ 1-port Gateway

AMG1011-T series

ADSL2+ 1-port Ethernet/USB Gateway

Support Notes

Version 1.00
Jul. 2013

ZyXEL
Unleash Networking Power

OS Frequently Asked Questions (FAQ)

NOTE.

This support note is for AMG1011/1001-T10A, but only AMG1011 supports the USB features.

Therefore, the sections of the USB functions are only for AMG1011.

All the other designs are the same for AMG1011/1001-T10A as described in this document

The Command Line Interface is for Administrator use only, and it can be accessed via a telnet session.
Begin telnet session:
(1) Select “Start” on your desktop and select →“Run”
(2) Input “cmd” and then press the ENTER key.
(3) Input “telnet xxx.xxx.xxx.xxx” (note that there is a space between the two).
(4) Press ENTER to login to the CLI.

Note: It is protected by super password, “1234” as the factory default.

2. How do I update the firmware and configuration file?

You can do this if you access the AMG1011/1001-T10A as Administrator. You can upload the firmware and configuration file to AMG1011/1001-T10A from the web GUI, or using FTP software. You CAN NOT upload the firmware and configuration file via telnet because the telnet connection will be dropped while uploading the firmware. Please do not power off the router until after the FTP uploading is finished, the router will upload the firmware to its flash during that time.

(1) Update on web GUI page, Advanced Setup.
Maintenance -> Firmware

You can check your current firmware version and upgrade the firmware of the Router in this page. Make sure that the firmware you want to use is on the local hard drive of the computer. Click on the “Browse” button to browse through local hard drive and locate the firmware to be used for upgrade.

(2) Update firmware via FTP

a) Use the FTP client program in your PC to login to your AMG1011/1001-T10A.

Note: It is protected by a user name and password, “admin” and “1234” by default.

b) To update the firmware, you need to use the command: **put xx.bin ras** for firmware or **put xx.rom rom-0** for rom file.

xx.bin indicates the firmware on your local hard drive and xx.rom indicates the rom file on your local hard drive. You can simply drag them into the window.

Note: There may be firmware that cannot be upgraded from

the web GUI. In this case, ZyXEL will prepare special Upload Software for you. Please read the firmware release notes carefully when you want to upload a new firmware.

3. How do I restore the AMG1011/1001-T10A configurations by using a TFTP client program via the LAN?

a. Use the TELNET client program in your PC to login to your AMG1011/1001-T10A.
b. Enter CI command **'sys stdio 0'** to disable Stdio idle timeout.
c. To backup the AMG1011/1001-T10A configurations, use a TFTP client program to get file **"rom-0"** from the AMG1011/1001-T10A.
d. To restore the AMG1011/1001-T10A configurations, use a TFTP client program to put your configuration in file **rom-0** in the AMG1011/1001-T10A.

4. What should I do if I forget the system password?

In case you forget the system password, you can erase the current configuration and restore the device to its factory defaults in this way:

Use the **RESET** button on the rear panel of the AMG1011/1001-T10A to reset the router. After the router is reset, the LAN IP address will be reset to **'192.168.1.1',** the password will be reset to "**1234**"**.**

5. How to use the Reset button?

a. Power on the AMG1011/1001-T10A. Make sure the **POWER** LED is on (not blinking)
b. Press the **RESET** button for ten seconds **and** then release it. If the **POWER** LED begins to blink, the default configuration has been restored and the AMG1011/1001-T10A will restart.

6. What is SUA and when should I use it?

SUA (Single User Account) is a unique feature supported by the AMG1011/1001-T10A router that allows multiple people to access the Internet simultaneously for the cost of a single user account.

On the AMG1011/1001-T10A, SUA receives a packet from a local client destined for the Internet, it replaces the source address in the IP packet header with its own address and the source port in the TCP or UDP header with another value chosen out of a local pool. It then re-computes the appropriate header checksums and forwards the packet to the Internet as if it is originated from the AMG1011/1001-T10A using the IP address assigned by the ISP. When it replies packets from the Internet are received by the AMG1011/1001-T10A, the original IP source address and TCP/UDP source port numbers are written into

the destination fields of the packet (since it is now moving in the opposite direction), the checksums are recomputed, and the packet is delivered to its true destination. This is because SUA keeps a table of the IP addresses and port numbers of the local systems currently using it.

7. What is the difference between SUA and Full Feature NAT?

When you edit a remote node via the web GUI, Advanced Setup,
Advanced Setup -> NAT -> Number of IPs, there will be two options available:

- **Single**
- **Multiple**

Single means SUA (Single User Account). In previous versions, NAT is set with 2 rules: Many-to-One and Server. With SUA, 'visible' servers are mapped to different ports, since the servers share only one global IP.

The AMG1011/1001-T10A now has **Multiple,** which means for **Full Feature NAT,** and it supports five types of IP/Port mappings: One-to-One, Many-to-One, Many-to-Many-Overload, Many-to-Many-No Overload and Server. You can make special applications when you select Multiple. For example, with multiple global IP addresses, multiple severs using the same port (e.g., FTP servers using port 21/20) are allowed on the LAN for outside access.

The AMG1011/1001-T10A supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The AMG1011/1001-T10A supports 8 sets since there are 8 remote nodes.

8. Is it possible to access a server running behind SUA from the Internet, and what is the procedure?

Yes, it is possible because the AMG1011/1001-T10A delivers the packet to the local server by looking it up in a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured (you can configure it via the web GUI, Advanced Setup) **Advanced Setup -> NAT -> DMZ**.

9. When do I need to select Multiple IP address in NAT (Full Feature NAT)?

- Make multiple local servers on the LAN accessible from outside with multiple global IP addresses.

With Single IP (SUA), 'visible' servers are mapped to different ports, since the servers share only one global IP address. But, when you select **Multiple IPs**

(Full Feature), you can make multiple local servers (mapping the same port or not) on the LAN accessible from outside with multiple global IP addresses.

- Support Non-NAT Friendly Applications

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. Thus, users on the same network cannot login to the same server simultaneously. In this case, it is better to use Many-to-Many-No Overload or One-to-One NAT mapping types, thus each user that is logged into the server uses a unique global IP address.

10. What IP/Port mapping does Multi-NAT support?

There is a **Virtual Server** column in **Advanced Setup-> NAT.** We can configure a IP/Port mapping table there.

Multi-NAT supports five types of IP/port mapping: One-to-One, Many-to-One, Many-to-Many-Overload, Many-to-Many-No Overload, and Server. The details of the mapping between ILA and IGA are described below. Here we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA),

- **One-to-One**: In One-to-One mode, the AMG1011/1001-T10A maps one ILA to one IGA.
- **Many-to-One:** In Many-to-One mode, the AMG1011/1001-T10A maps multiple ILAs to one IGA. This is equivalent to SUA (i.e., PAT, port address translation).
- **Many-to-Many-Overload:** In Many-to-Many-Overload mode, the AMG1011/1001-T10A maps the multiple ILAs to a shared IGA.
- **Many One-to-One:** In Many One-to-One mode, the AMG1011/1001-T10A maps each ILA to a unique IGA.
- **Server:** In Server mode, the AMG1011/1001-T10A maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note that if you want to map each server to one unique IGA please use the One-to-One mode.

The following table summarizes the five types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1
Many-to-One (SUA/PAT)	ILA1<--->IGA1 ILA2<--->IGA1 ...
Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2 ...
Many One-to-One	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA3 ILA4<--->IGA4 ...
Server	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

11. How many network users can the SUA/NAT support?

The AMG1011/1001-T10A does not limit the number of users, but the number of the NAT sessions. The AMG1011/1001-T10A supports 1024 sessions.

12. How can I protect against IP spoofing attacks?

The filter sets of the AMG1011/1001-T10A provide a means to protect against IP spoofing attacks. The basic scheme is according to your need to set different filter types. There are three types of filters: IP/MAC Filter, Application Filter, and URL Filter. You can use IP/MAC filter to filter the input or output data to be filtered, or you may simply set filter conditions depending on your application or URL.

Product Frequently Asked Questions (FAQ)

1. How can I manage the AMG1011/1001-T10A?

- English web GUI for local and remote management
- CLI (Command Line Interface)
- Telnet support (Administrator Password Protected) for remote configuration change and status monitoring
- FTP sever, firmware upgrade and configuration backup and restore are supported (Administrator Password Protected)

2. What is the default password for the web GUI?

The factory default password for the AMG1011/1001-T10A web GUI is **1234**. You can login as an administrator. You can change the password after you login to the web GUI.

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

3. How do I know what is the WAN IP address of the AMG1011/1001-T10A that is assigned by the ISP?

You can view **" IP Address<from ISP>: x.x.x.x"** shown in the web GUI **Status->Device Info ->WAN**" to check this IP address.

4. What is traffic shaping?

Traffic shaping allocates the bandwidth to WAN dynamically and aims at boosting the efficiency of the bandwidth. If there are several VCs in the AMG1011/1001-T10A but only one VC activated at one time, the AMG1011/1001-T10A allocates all the bandwidth to the VC and the VC gets full bandwidth. If other VCs are activated later, the bandwidth yields to other VCs afterwards.

5. Why do we perform traffic shaping in the AMG1011/1001-T10A?

The AMG1011/1001-T10A must manage traffic fairly and provide bandwidth allocation for different sorts of applications, such as voice, video, and data. All applications have their own natural bit rate. Large data transactions have a fluctuating natural bit rate. The AMG1011/1001-T10A is able to support variable traffic among different virtual connections. Certain traffic may be discarded if the virtual connection experiences congestion. Traffic shaping defines a set of actions taken by the AMG1011/1001-T10A to avoid congestion; traffic shaping takes measures to adapt to unpredictable fluctuations in traffic flows and other problems among virtual connections.

6. What do the parameters (PCR, SCR, and MBS) mean?

Traffic shaping parameters (**PCR, SCR, MBS**) can be configured in the web GUI, Interface Setup, **Interface Setup -> Internet -> QoS**:

Peak Cell Rate (PCR): The maximum bandwidth allocated to this connection. The connection throughput of the VC is limited by PCR.

Sustainable Cell Rate (SCR): The least guaranteed bandwidth of a VC. When there are multi-VCs on the same line, the VC throughput is guaranteed by SCR.

Maximum Burst Size (MBS): The amount of cells transmitted through this VC at the Peak Cell Rate before yielding to other VCs. Total bandwidth of the line is dedicated to a single VC if there is only one VC on the line. However, as the other VCs are requesting for the bandwidth, the MBS defines the maximum number of cells transmitted via this VC with Peak Cell rate before yielding to other VCs.

The AMG1011/1001-T10A holds the parameters for shaping the traffic among its virtual channels. If you do not need traffic shaping, please set SCR = 0, MBS = 0 and PCR as the maximum value according to the line rate (for example, 2.3 Mbps line rate will result in a PCR of 5424 cell/sec).

7. What do the ATM QoS Types (CBR, UBR, VBR, rtVBR, nrtVBR) mean?

Constant Bit Rate (CBR): An ATM bandwidth-allocation service that requires the user to determine a fixed bandwidth requirement at the time the connection is set up so that the data can be sent in a steady stream. CBR service is often used when transmitting fixed-rate uncompressed video.

Unspecified Bit Rate (UBR): An ATM bandwidth-allocation service that does not guarantee any throughput levels and uses only available bandwidth. UBR is often used when transmitting data that can tolerate delays, such as e-mail.

Variable Bit Rate (VBR): An ATM bandwidth-allocation service that allows users to specify a throughput capacity (i.e., a peak rate) and a sustained rate but data is not sent evenly. You can select VBR for burst traffic and bandwidth sharing with other applications. It contains two subclasses:

Non-real time Variable Bit Rate (nrtVBR) and **Real time Variable Bit Rate (rtVBR).**

8. What is the difference between Bridge and Router mode that is supported by the AMG1011/1001-T10A?

When the ISP limits some specific computers to access the Internet, it means that only the traffic to/from these computers will be forwarded and the other traffic will be filtered. In this case, we use bridge mode, which works as an ADSL modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet.

For most Internet users having multiple computers and who want to share an Internet account for Internet access, they have to add another Internet sharing device, like a router. In this case, we use the router mode, which works as a general router plus an ADSL modem.

9. How do I know whether I am using PPPoE?

PPPoE requires a user account to login to the ISP. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check with your ISP about this. Please choose PPPoE as the encapsulation type in the AMG1011/1001-T10A if the ISP uses PPPoE.

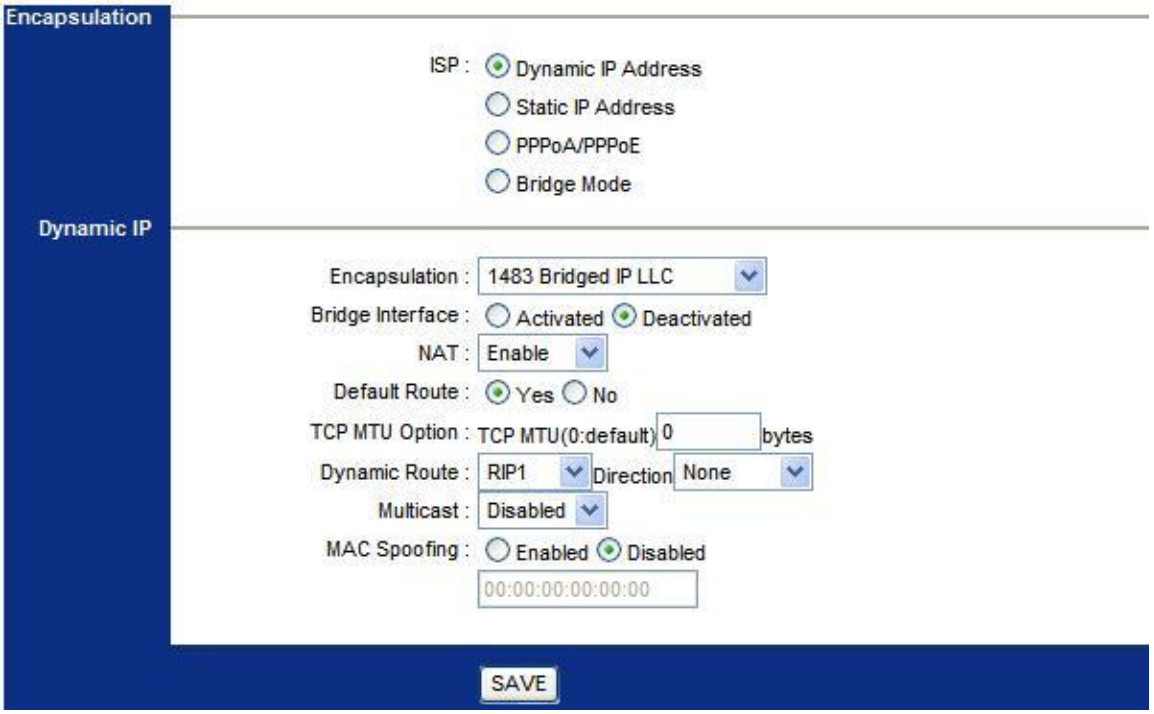
10. Why does my provider use PPPoE?

PPPoE emulates a familiar dial-up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and services including authentication, accounting, secure access and configuration management.

11. When do I need to choose a dynamic IP address?

If your ISP provides you an IP address automatically, typically used for cable service. In this case your computer gets an IP address dynamically assigned by the DHCP server.

To use this mode, you need to do some corresponding configurations on the web page: **Interface Setup -> Internet -> Encapsulation**:



Key setting:

Field	Description
Encapsulation	Choose one of the encapsulation modes used in Dynamic IP condition. There are four modes: 1483 Bridged IP LLC, 1483 Bridge IP VC-Mux, 1483 Route IP LLC (IPoA), and 1483 Route IP VC -Mux.
Bridge Interface	When activated, not only the router, but the bridge also connects. Meanwhile router and bridge use the same PVC. The LAN PC could get a WAN IP address which is assigned by the PPPoE server. So, we do not need two PVCs to perform multicast. When activated, not only the router, but the bridge also connects. Meanwhile
NAT	Choose to enable or disable NAT function.
Default Route	Choose “yes” to set the current PVC as a default gateway to the Internet from your device. Note that there must be only **one** default gateway. If you have configured more than one PVC as default gateway, the last one would be efficient. Choose “yes” to set the current PVC as a default gateway to the Internet from your device. Note that there must be only **one** default gateway. If you
TCP MTU Option	Set TCP MTU value. “0” is considered as default value.
Dynamic Route	Choose an RIP vision. You can choose the RIP direction. Choose “none” as the direction to disable the RIP function.
Multicast	Choose to enable or disable multicast function
MAC Spoofing	Choose to enable MAC spoofing function. You can set a wanted MAC Below.

12. What is DDNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free web servers such as http://www.dyndns.org/.

Without DDNS, we always tell the users to use the WAN IP address of the AMG1011/1001-T10A to reach our internal server. It is inconvenient for the users if this IP address is dynamic. With DDNS supported by the AMG1011/1001-T10A, you can apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., web server) from a DDNS server. The outside users can always access the web server using www.zyxel.com.tw regardless of the WAN IP address of the AMG1011/1001-T10A.

When the ISP assigns the AMG1011/1001-T10A a new IP address, the AMG1011/1001-T10A updates this IP address to the DDNS server so that the server can update its IP -to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

13. When do I need to use DDNS service?

When you want your internal server to be accessed using a DNS name rather than using the dynamic IP address you can use the DDNS service. The DDNS server allows you to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP address, the AMG1011/1001-T10A sends this IP address to the DDNS server for its updates.

14. What is DDNS wildcard and does the AMG1011/1001-T10A support it?

Some DDNS servers support the wildcard feature which allows the hostname, *.yourhost.dyndns.org, to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful when there are multiple servers inside and you want users to be able to use things such as www.yourhost.dyndns.org and still reach your hostname.

Yes, the AMG1011/1001-T10A supports DDNS wildcard of http://www.dyndns.org/. And you can choose to activate or inactivate this feature on the web configuration page. When using wildcard, you simply enter yourhost.dyndns.org on the web configuration page.

15. Can the SUA (Simple IP address) of he AMG1011/1001-T10A handle IPSec packets sent by the IPSec gateway?

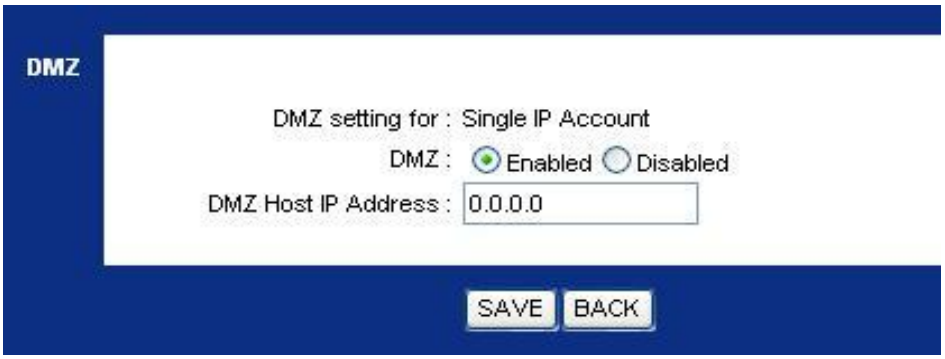
Yes, the SUA of AMG1011/1001-T10A can handle IPSec ESP tunneling mode. When packets go through the SUA; SUA will change the source IP address and source port for the host. To pass IPSec packets, SUA must understand the ESP packet with protocol number 50; replace the source IP address of the IPSec gateway with the router's WAN IP address. However, SUA should not change the source port of the UDP packets that are used for key management. Because the remote gateway checks this source port during connections, the port thus is not allowed to be changed.

16. How do I setup AMG1011/1001-T10A for routing IPSec packets over SUA?

For outgoing IPSec tunnels, no extra setting is required.

For forwarding the inbound IPSec ESP tunnel, A 'Default' server set is required. You can configure this in web GUI, Advanced Setup, **Advanced Setup -> NAT -> DMZ:**

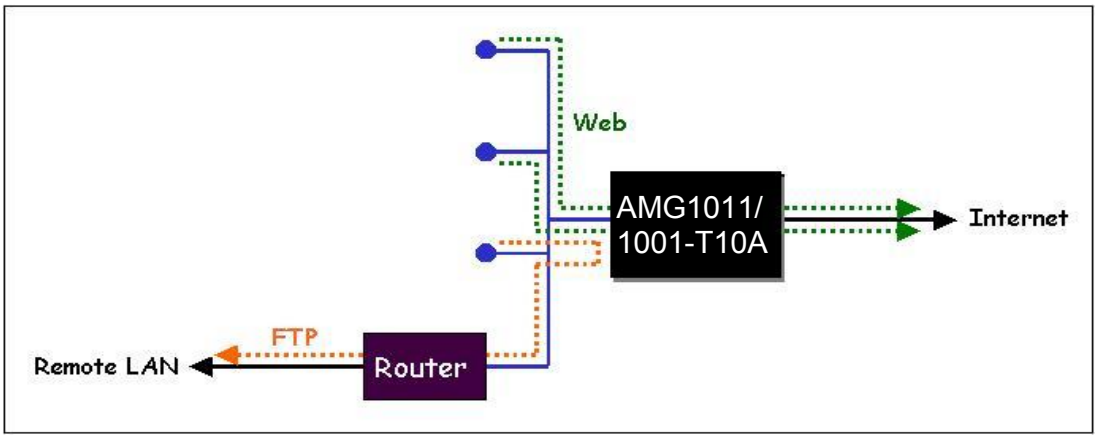
Note: First set **Number of IP**s as **Single** for SUA use.



Since SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. So, to make an internal server for outside access, we must specify the service port and the LAN IP address of this server via the web configuration page. Thus SUA is able to forward the incoming packets to the requested service behind SUA and the outside users access the server using the WAN IP address of the AMG1011/1001-T10A. So, you have to configure the internal IPSec client as a default server (unspecified service port) when it acts as a server gateway.

17. What is IP Policy Routing (IPPR)?

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Network administrators can use IPPR to distribute traffic among multiple paths. For example, if a network has both the Internet and remote node connections, you can route the web packets to the Internet using one policy, and route the FTP packets to the remote LAN using another policy. Refer to the figure below.



Use IPPR to distribute traffic along multiple paths

- Benefits

Source-Based Routing: Network administrators can use policy-based routing to direct traffic from different users through different connections.

Quality of Service (QoS): Organizations can differentiate traffic by setting the precedence or ToS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.

Cost Savings: IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost path while using low-path for batch traffic.

Load Sharing: Network administrators can use IPPR to distribute traffic among multiple paths.

18. How does the IPPR work?

A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, ToS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include routing the packet to a different gateway (and hence the outgoing interface) and the ToS and precedence fields in the IP header. IPPR follows the existing packet filtering facility of ZyNOS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A use defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with 6 policies in each set.

19. What is CWMP?

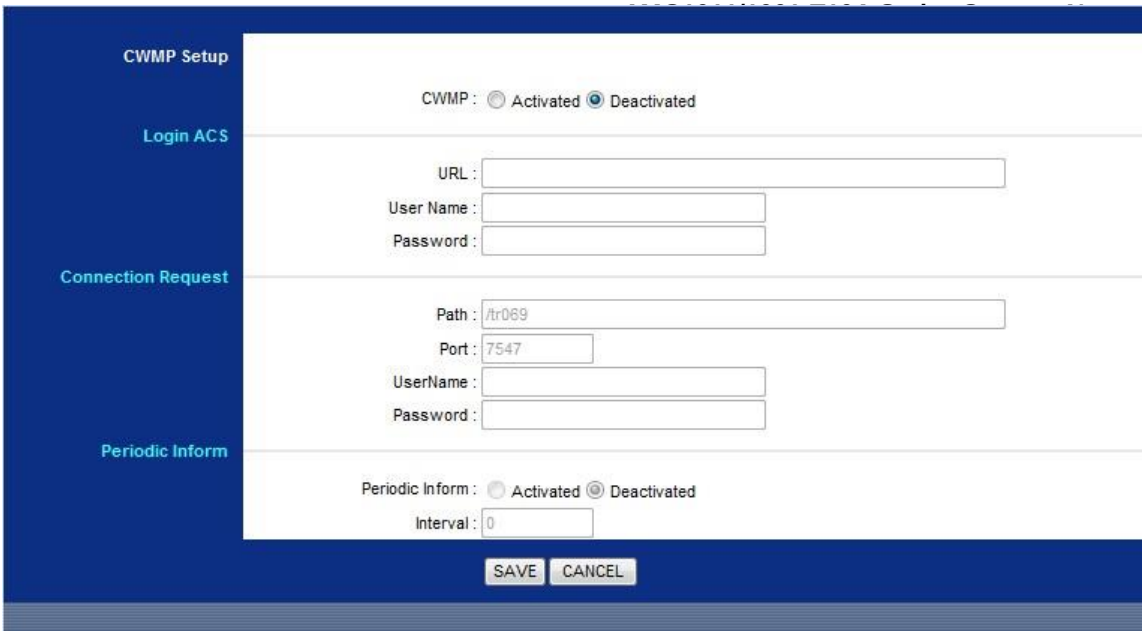
AMG1011/1001-T10A supports TR-069 Amendment 1 (CPE WAN Management Protocol Release 2.0) and TR-069 Amendment 2 (CPE WAN Management Protocol v1.1, Release 3.0).

TR-069 is a protocol that defines how the ZyXEL Device (**ZD**) can be managed via a management server (**MS**) such as ZyXEL's Vantage Access.

An administrator can use a management server to remotely set up the ZyXEL device, modify settings, perform firmware upgrades as well as monitor and diagnose the ZyXEL device. All you have to do is enable the device to be managed by a management server and specify the management server IP address or domain name and user name and password.

20. What is the procedure to configure CWMP on the AMG1011/1001-T10A?

You can set CWMP on the web configuration page: **Access Management -> CWMP -> CWMP Setup:**



Key Settings

Field	Description
Login ACS	Configure this part of the screen to log into the management server.
CWMP	Select **Activated** to allow the ZyXEL Device to be managed by a management Server, or select **Deactivated** to not allow the ZyXEL Device to be managed by a management server. Select **Activated** to allow the ZyXEL Device to be managed by a management
URL	Type the IP address or domain name of the management server.
User Name	Type a user name of up to xxx printable characters found on an English-language keyboard.
Password	Type a password of up to xxx printable characters found on an English-language keyboard. Spaces are not allowed.
Connection Request	Use this part of the screen to allow the management server to connect to the ZyXEL Device after a successful login.
Path	This is the path for verification from the ACS to the ZyXEL Device. It can be considered as the URL of the CPE. When the ACS initialize a session, it will connect with the CPE based on this path. This is the path for verification from the ACS to the ZyXEL Device. It can be
Port	The default port for access to the ZyXEL Device from the management server is the HTTP port (80). If you change it, make sure it does not conflict with another port on your network and it is recommended to use a port number above 1024 (not a commonly used port). The management server should use this port to connect to the ZyXEL Device. You may need to alter your firewall or NAT port forwarding rules if they were already configured. The default port for access to the ZyXEL Device from the management server is the HTTP port (80). If you change it, make sure it does not conflict with
Periodic Inform	Select **Activated** to have the ZyXEL Device periodically send information to the management server (recommended if CWMP is enabled) or select **Deactivated** to not have the ZyXEL Device periodically send information to the management server
Interval	Enter a value between 1 and 86400 seconds.

Note

1. There are two groups: user name and password. The first group is on the web configuration page to authenticate the ZyXEL Device when making a connection to the management server. This user name and password on the management server and the ZyXEL Device must be the same. The second group is used to authenticate the management server when making a connection.

2. The interval is the duration in seconds for which the ZyXEL Device MUST attempt to connect with the management server to send information and check for configuration updates.

21. What is the procedure to configure ACL?

You can configure ACL via the web configuration page: **Access Management -> ACL**

Key Settings:

Field	Description
ACL	Select **Activated** to enable access control on the ZyXEL Device or select **Deactivated** to disable it.
ACL Rule Index	Select an index rule number in order to edit or delete it.
Active	Select **Yes** to enable this active control rule or **No** to disable it.
Secure IP Address	Enter the range of IP addresses of computers that are allowed to access the device. 0.0.0.0 ~ 0.0.0.0 means that any computer can access the ZyXEL Device. If you want just one computer to be able to access the ZyXEL Device, then enter its IP address in both fields.
Application	Select the service through which the computer can access the device. • If you want to allow a user to connect to the ZyXEL Device using the web configuration page, select **Web**. • If you want to allow a user to connect to the ZyXEL Device using Telnet, select **Telnet**. • If you want to allow a user to upload firmware to the ZyXEL Device, select **FTP**. • If you want to allow an administrator to send SNMP commands, select **SNMP**. • If you want to allow a user to find the ZyXEL Device on the network (for troubleshooting purposes, for example), select **Ping**. • You can allow access for all services, select **ALL**. You cannot select a combination of services.
Interface	Select the port through which you can access the device. Select **Both** for access via either port. If you configure 0.0.0.0 ~ 0.0.0.0 **Secure IP Address**, **ALL** services and **WAN** interface, you will not be able to access the device at all from the **LAN**.
Access Control Listing	The summary table displays the configured parameters for the selected rule.
SAVE	Click **SAVE** to apply your settings to the ZyXEL Device.
DELETE	Select an access control rule index number and click **DELETE** to remove it.
CANCEL	Click **CANCEL** to reset the values to the previously-configured ones.

22. What is UPnP?

Universal Plug and Play (UPnP) is a set of computer network protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards.

23. How cam I access the Internet via the USB port?

You can access the Internet via the USB port after the USB driver installation. The USB driver for each model is available in the CD provided with the product. You can also download the driver from the ZyXEL global website: www.zyxel.com.

ADSL Frequently Asked Questions (FAQ)

1. How does ADSL compare to cable modems?

ADSL provides a dedicated service over a single telephone line; cable modems offer a dedicated service over a shared media. While cable modems have greater downstream bandwidth capabilities (up to 30 Mbps), that bandwidth is shared among all users on a line, and will therefore vary, perhaps dramatically, as more users in a neighborhood get online at the same time. Cable modem upstream traffic will in many cases be slower than ADSL, either because the particular cable modem is inherently slower, or because of rate reductions caused by contention for upstream bandwidth slots. The big difference between ADSL and cable modems, however, is the number of lines available to each. There are no more than 12 million homes passed today that can support two-way cable modem transmissions, and while the figure also grows steadily, it will not catch up with telephone lines for many years. Additionally, many of the older cable networks are not capable of offering a return channel; consequently, such networks will need significant upgrading before they can offer high bandwidth services.

2. What is the micro filter or splitter used for?

Generally, the voice band uses the lower frequency ranging from 0 to 4 KHz, while ADSL data transmission uses the higher frequency. The micro filter acts as a low-pass filter for your telephone set to ensure that ADSL transmissions do not interfere with your voice transmissions. For the details about how to connect the micro filter please refer to the user's manual.

3. How do I know if the ADSL line is up?

You can see the DSL LED become Green on the front panel of the AMG1011/1001-T10A when the ADSL physical layer is up.

4. Does the VC-based multiplexing perform better than the LLC-based multiplexing?

Though the LLC-based multiplexing can carry multiple protocols over a single VC, it requires extra header information to identify the protocol being carried on the virtual circuit (VC). The VC -based multiplexing needs a separate VC for carrying each protocol but it does not need the extra headers. Therefore, the VC-based multiplexing is more efficient.

We can choose one of them on the web configuration page: **Interface Setup -> Internet ->Dynamic IP ->Encapsulation:**

5. How do I know the details of my ADSL line statistics?

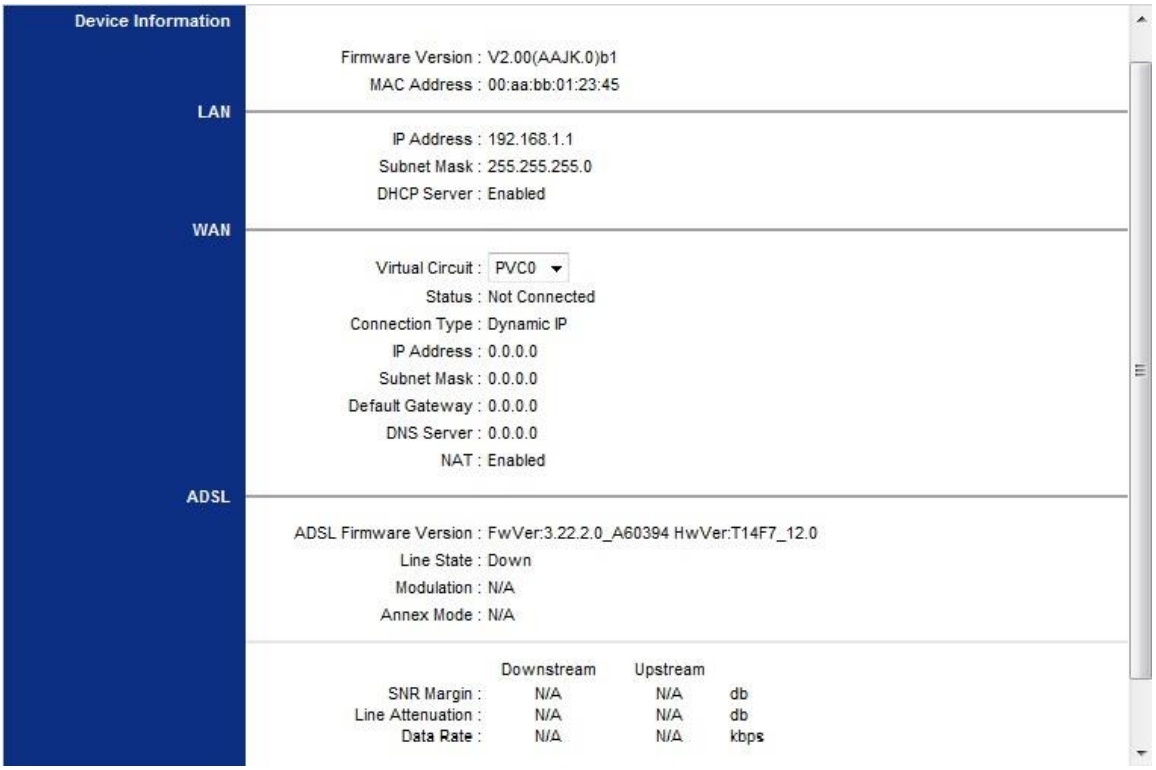
You can use the following CI commands to check the ADSL line statistics.
CI> wan adsl perfdata

CI> wan adsl status

CI> wan adsl linedata far
CI> wan adsl linedata near

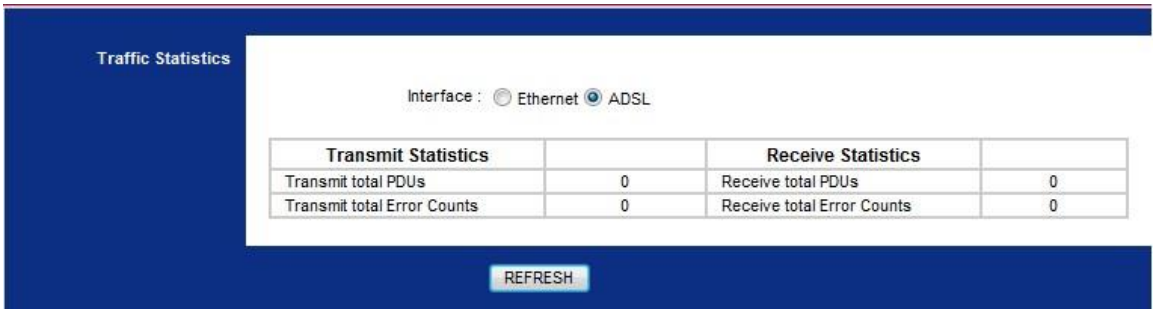
You can also see the detailed information via the web GUI status.

Status -> Device Info:



You may also view ADSL traffic status:

Status -> Statistics -> Traffic Statistics -> Interface-> ADSL



6. What are the signaling pins of the ADSL connector?

The signaling pins on the ADSL connector of the AMG1011/1001-T10A are pin 3 and pin 4. These are the middle two pins for an RJ-11 cable.

Application Notes

General Application Notes

1. Internet Access Using AMG1011/1001-T10A under Bridge mode

- Setup your workstation
- Setup your AMG1011/1001-T10A under bridge mode

If the ISP limits some specific computers to access the Internet, it means that only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use the AMG1011/1001-T10A, which works as an ADSL bridge modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet.

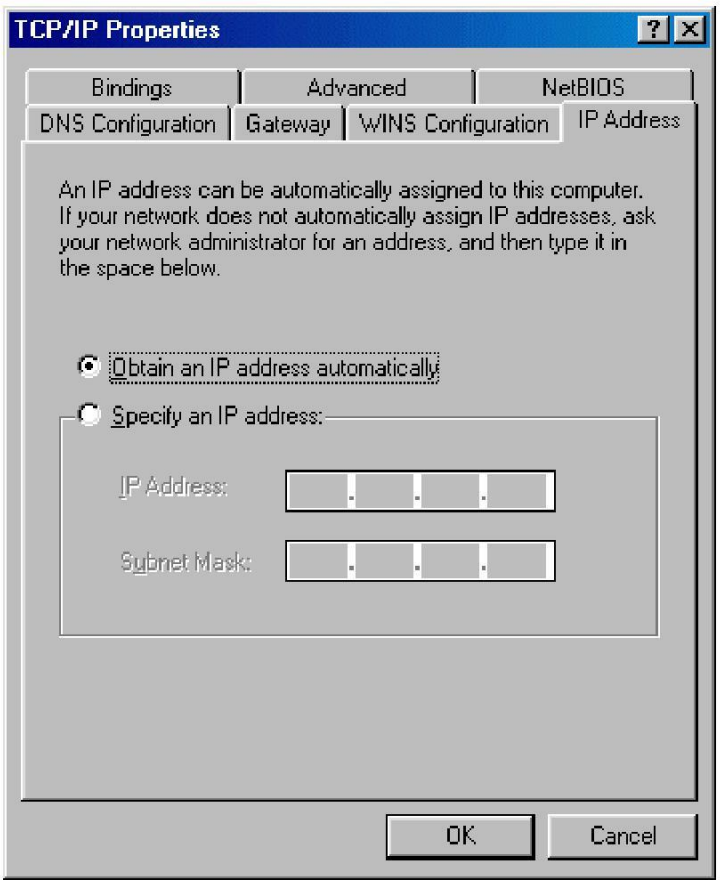
Set up your workstation

(1) Ethernet connection

To connect your computer to the LAN port of the AMG1011/1001-T10A, the computer must have an Ethernet adapter card installed. For connecting a single computer to the AMG1011/1001-T10A, we use an Ethernet cable.

(2) TCP/IP configuration

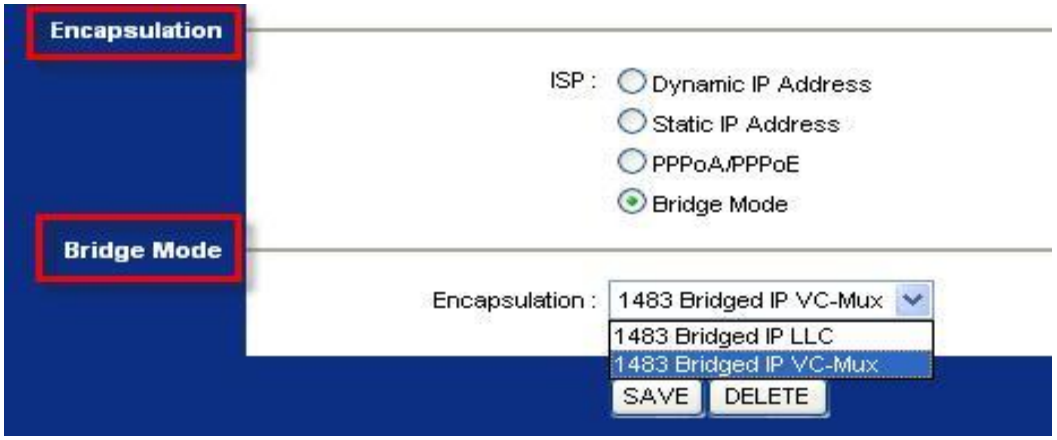
In most cases, the ISP assigns the IP address to the computer dynamically so you have to configure the computer as a DHCP client, which obtains the IP address from the ISP using DHCP protocol. The ISP may also provide the gateway, DNS via DHCP if they are available. Otherwise, please enter the static IP addresses for all that the ISP gives to you in the network TCP/IP settings. For the Windows OS, check the option ***'Obtain an IP address automatically'*** in its TCP/IP setup, please see the example shown below.



Setup your AMG1011/1001-T10A under Bridge mode

The following procedure shows you how to configure your AMG1011/1001-T10A as bridge mode. Use the web GUI to guide you through the related menu.

(1) Configure AMG1011/1001-T10A as bridge mode and configure the Internet setup parameters via the web GUI, Advanced Setup. **Interface Setup ->**
Internet -> Encapsulation.



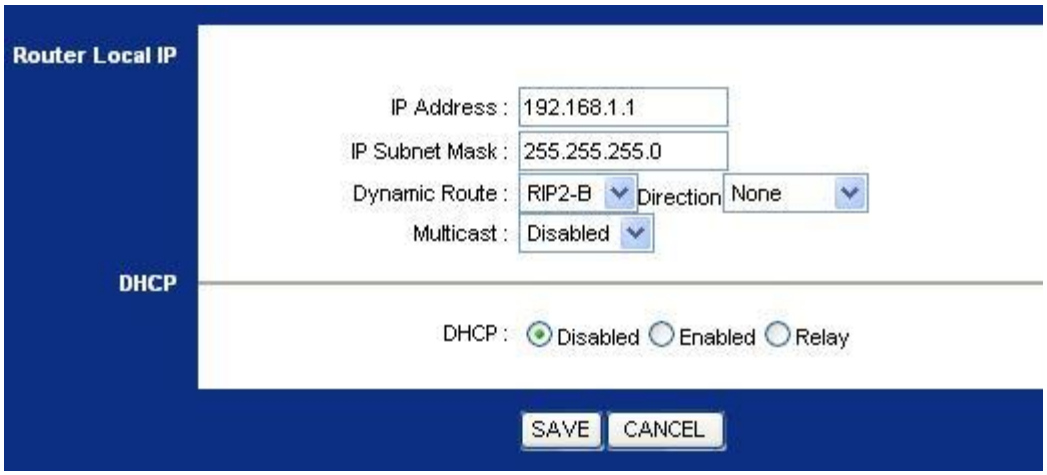
Key Settings:

Option	Description
Encapsulation	Select the correct Encapsulation type that your ISP supports. For example, Bridge mode.
Bridge Mode configuration	When selecting one encapsulation type, there would be a corresponding column below, such as Bridge Mode. Select the correct Multiplexing type that your ISP supports. For example, LLC.

(2) Turn off DHCP Server and configure a LAN IP address for the AMG1011/1001-T10A via the web GUI, Advanced Setup, Interface Setup -> LAN -> DHCP.. We use 192.168.1.1 as the LAN IP address for the AMG1011/1001-T10A in this case:

Step 1: Disable DHCP Server and save it:

Step 2: Assign an IP address to the LAN Interface of the AMG1011/1001-T10A, e.g.: 192.168.1.1



2. Internet Access Using AMG1011/1001-T10A under Routing mode

For most Internet users having multiple computers, and want to share an Internet account for Internet access, they have to install an Internet sharing device, like a router. In this case, we use the AMG1011/1001-T10A that works as a general router plus an ADSL modem.

Set up your workstation

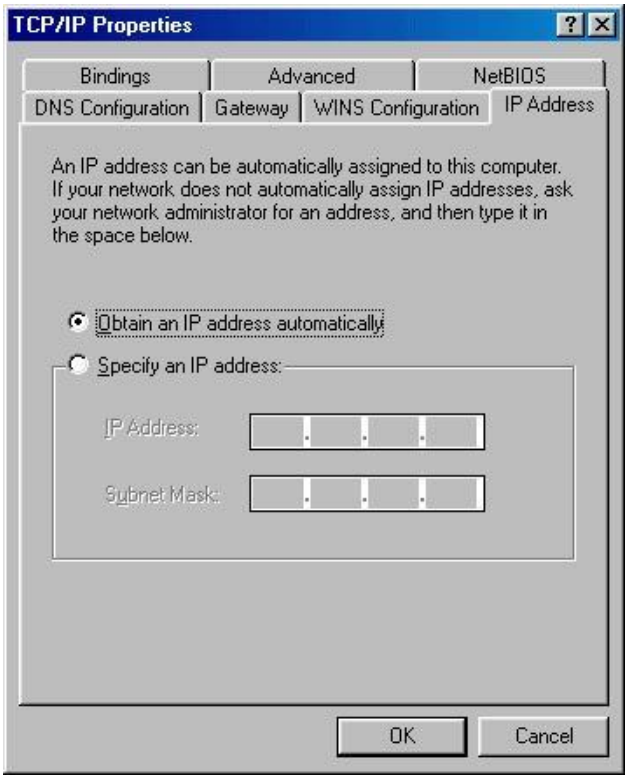
(1) Ethernet connection

Connect the LAN ports of all computers to the LAN Interface of the AMG1011/1001-T10A using an Ethernet cable.

(2) TCP/IP configuration

Since the AMG1011/1001-T10A is set to DHCP server as default, you only need to configure the workstations as the DHCP clients in the networking settings. In this case, the IP address of the computer is assigned by the AMG1011/1001-T10A.

The AMG1011/1001-T10A can also provide the DNS to the clients via DHCP if it is available. For this setup in the Windows OS, check the option ***'Obtain an IP address automatically'*** in its TCP/IP setup. Please see the example shown below.

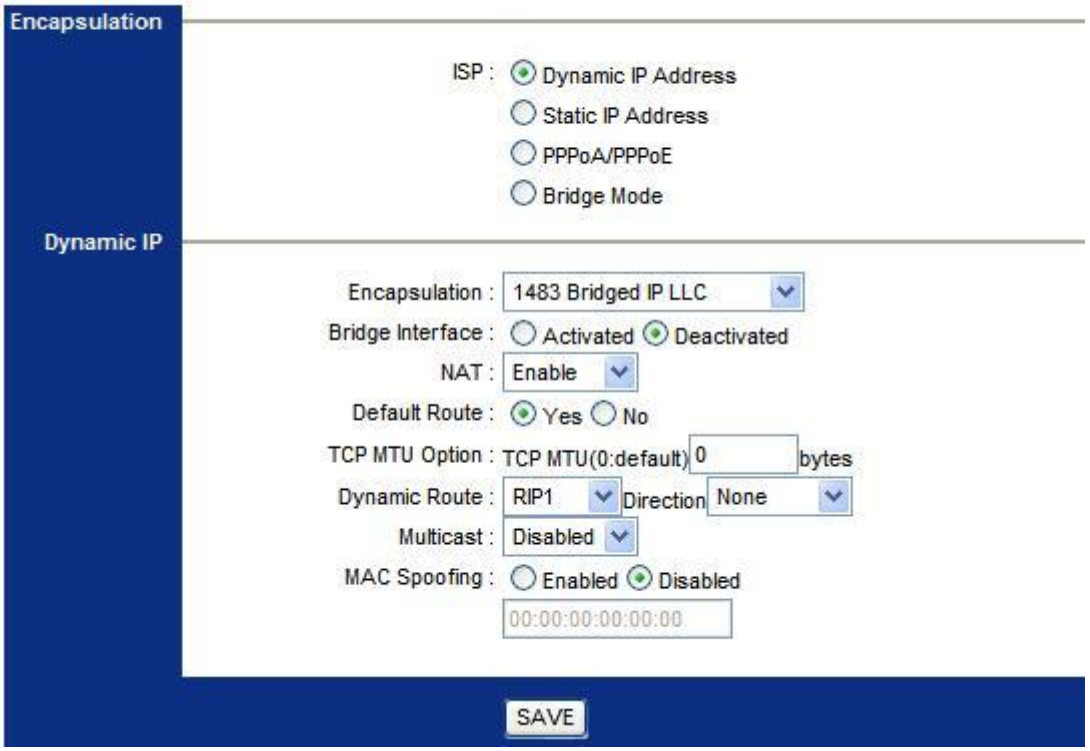


Set up your AMG1011/1001-T10A under Routing mode

The following procedure shows you how to configure your AMG1011/1001-T10A as Routing mode for routing traffic. Use the web GUI to guide you through the related menu.

(1) Configure AMG1011/1001-T10A as routing mode and configure Internet setup parameters via the web GUI, Advanced Setup, **Interface Setup ->**

Internet -> Encapsulation.

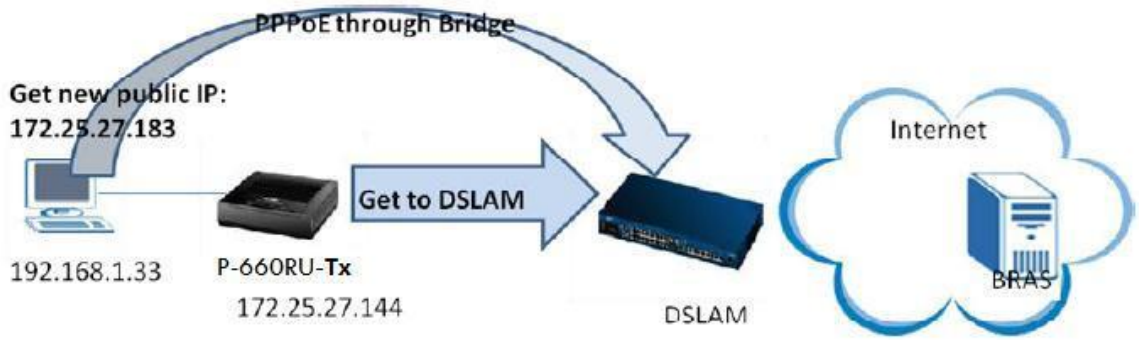


Here you can choose the first three types of Encapsulation for routing mode.

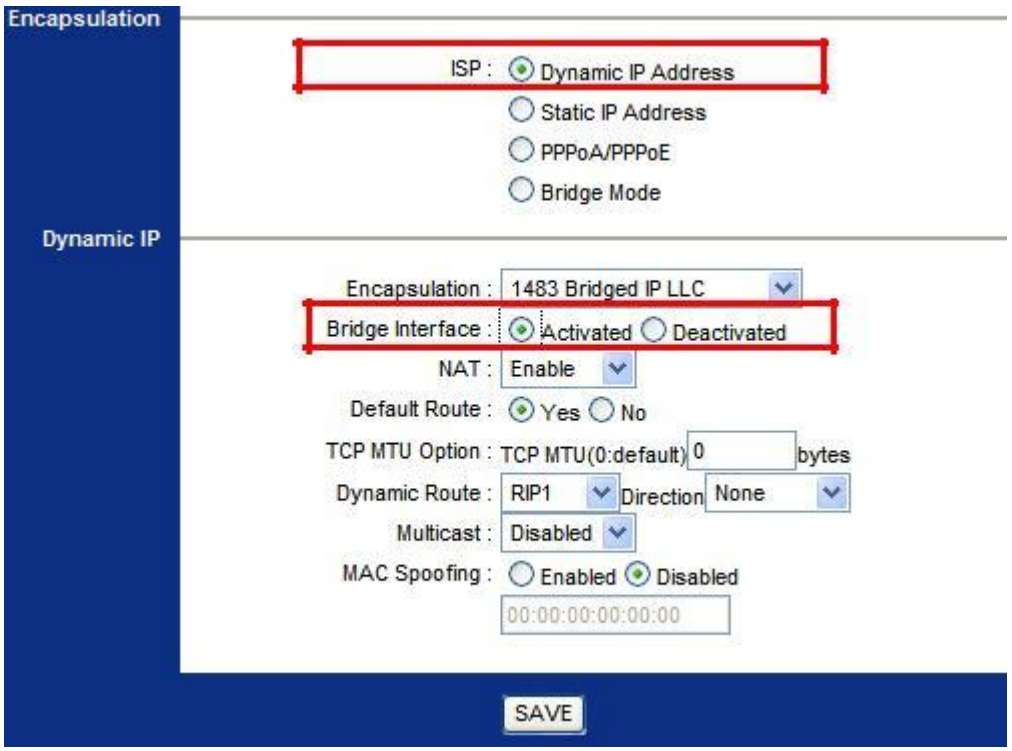
(2) Configure a LAN IP address for the AMG1011/1001-T10A and the DHCP settings via the web GUI, Advanced Setup, **Interface Setup -> LAN -> DHCP.**

3. Use Bridge Interface in Routing mode

Using the Bridge Interface in routing mode allows you to connect to the Internet with both routing and bridging. A route channel for your device and a bridge channel for your PC, but they use the same PVC so we do not need two PVCs to perform multicast. You also do not need to set a new VLAN on the DSLAM. Refer to the image below.



You can configure it via the web GUI, **Interface Setup -> Internet -> Encapsulation**



After configuration, your AMG1011/1001-T10A can get a public IP address in the way you select from the Encapsulation types (Dynamic IP Address, Static IP Address or PPPoA/PPPoE), while your computer can also get a public IP address through PPPoE.

4. Setup the AMG1011/1001-T10A as a DHCP Relay

What is DHCP Relay?

DHCP stands for Dynamic Host Configuration Protocol. In addition to the DHCP server feature, the AMG1011/1001-T10A supports the DHCP relay function. When it is configured as DHCP server, it assigns the IP addresses to the LAN clients. When it is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server. Please see figure 1.

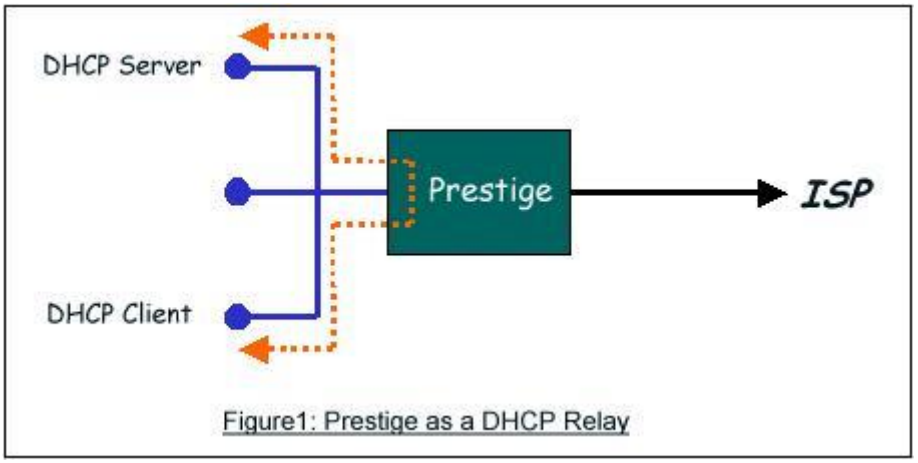


Figure1: Prestige as a DHCP Relay

Prestige means AMG1011/1001-T10A

Setup the AMG1011/1001-T10A as a DHCP Relay

Set the AMG1011/1001-T10A as a DHCP Relay by the following commands via the **CLI**:

Ip dhcp enif0 mode relay

Ip dhcp enif0 relay server [Server IP Address]

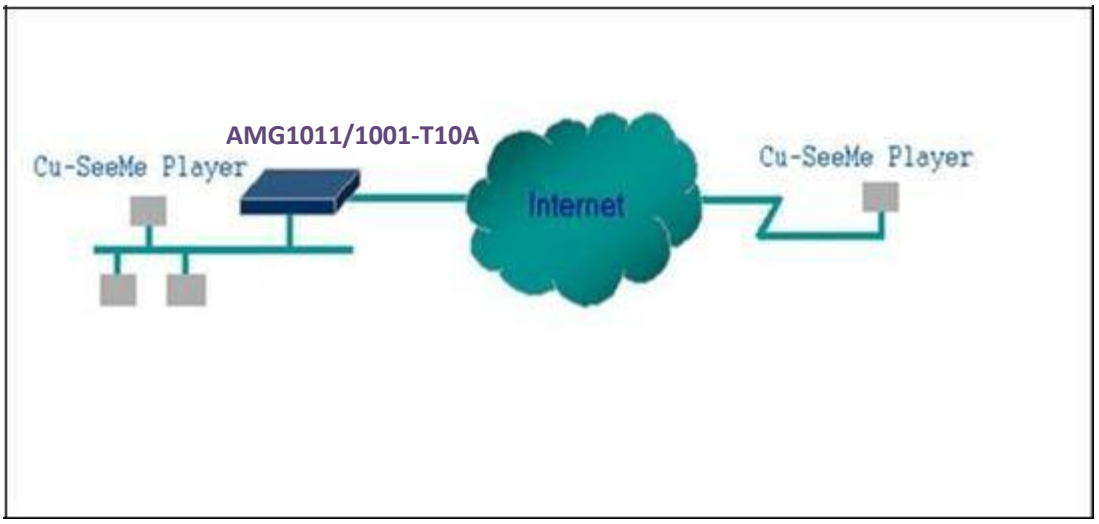
You can also configure it via the web configuration page:

Interface Setup -> LAN -> DHCP.

Click to choose “Relay”, input the Relay Agent IP and save the configuration.

5. SUA Notes

Tested SUA/NAT Applications (e.g., Cu-SeeMe, ICQ, NetMeeting)

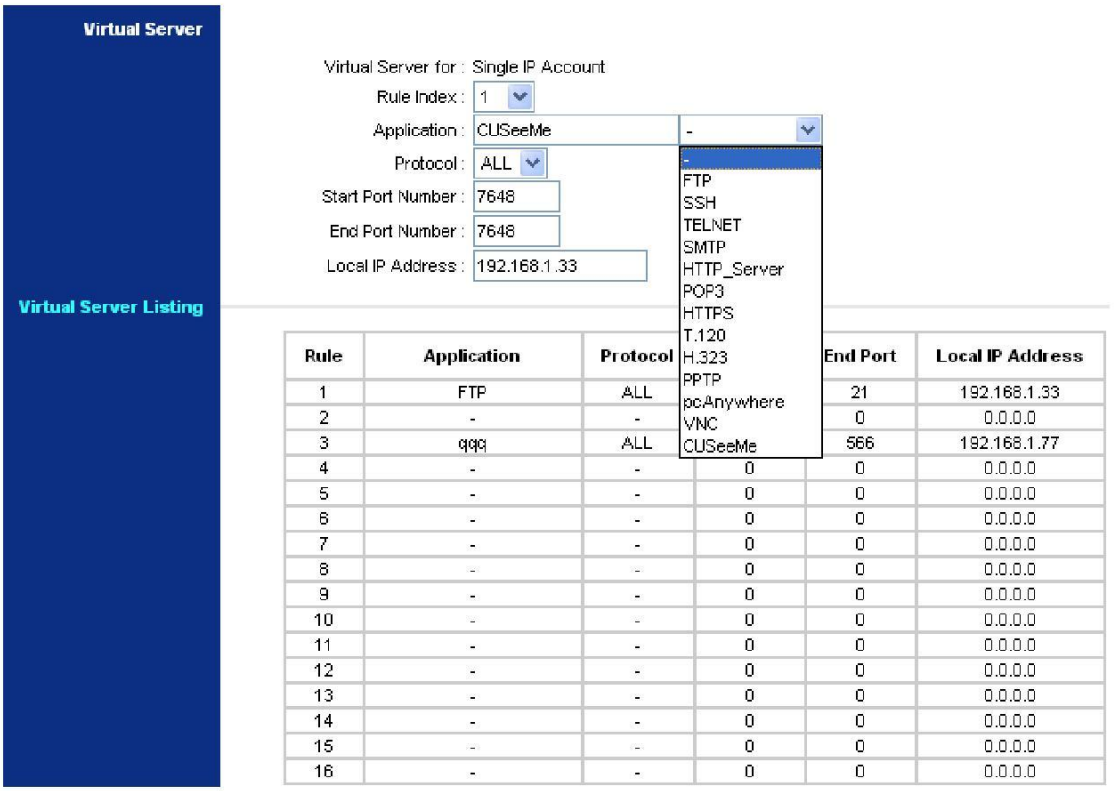


Introduction

Generally, SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. However, some applications such as Cu-SeeMe and ICQ will need to connect to the local user behind the AMG1011/1001-T10A. In such case, a SUA server must be configured to forward the incoming packets to the true destination behind SUA. After the required server is configured via the web GUI, Advanced Setup, **Advanced Setup -> NAT -> Virtual Server,** the internal server or client applications can be accessed by using the ***WAN IP*** **Address** of the MG1011/1001-T10A.

SUA Supporting Table

The following are required by the web GUI, Advanced Setup, **Advanced Setup -> NAT -> Virtual Server** for the various applications running in Single mode.



Application	Required Settings in **Port Forwarding** Port/IP	
	Outgoing Connection	Incoming Connection
FTP	None	21/client IP
SSH	None	22/client IP
TELNET	None	23/client IP (and active Telnet service from WAN)
SMTP	None	25/client IP
HTTP Server	None	80/client IP
POP3	None	110/client IP
HTTPs	None	443/client IP
T.120	None	1503/client IP
H.232	None	1720/client IP
PPTP	None	1723/client IP
pcAnywhere	None	5631/client IP
VNC	None	5900/client IP
CUSeeMe	None	7648/client IP

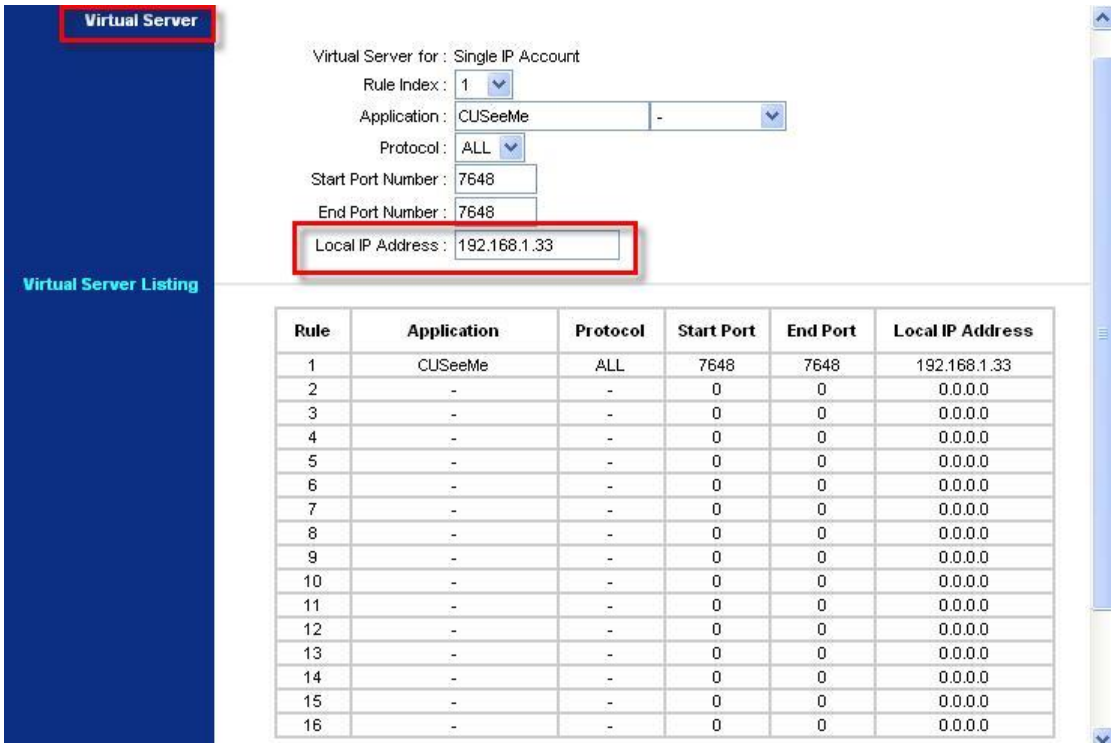
[1] Since SUA enables your LAN to appear as a single computer to the Internet, it is not possible to configure similar servers on the same LAN behind SUA.

[2] Because White Pine Cu-SeeMe uses dedicated ports (port 7648 & port 24032) to transmit and receive data; therefore, only one local Cu-SeeMe is allowed within the same LAN.

Configurations

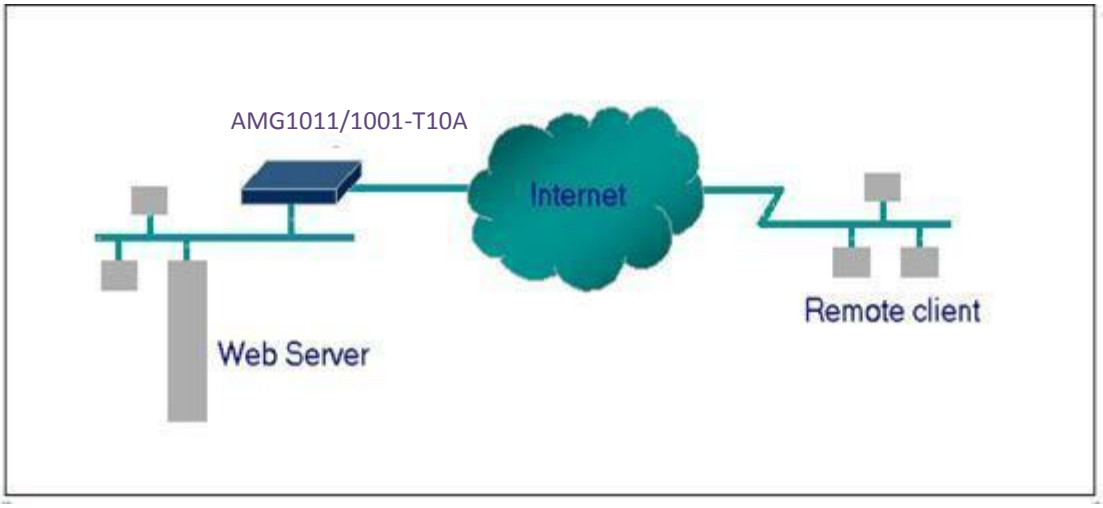
For example, if the workstation operating Cu-SeeMe has an IP address of 192.168.1.33, then the default SUA server must be set to 192.168.1.33. The peer Cu-SeeMe user can reach this workstation by using the ***WAN IP*** address of the AMG1011/1001-T10A, which can be obtained via the web GUI, **Status -> Device Info ->WAN**.

Virtual Server Configuration:



Rule	Application	Protocol	Start Port	End Port	Local IP Address
1	CUSeeMe	ALL	7648	7648	192.168.1.33
2	-	-	0	0	0.0.0.0
3	-	-	0	0	0.0.0.0
4	-	-	0	0	0.0.0.0
5	-	-	0	0	0.0.0.0
6	-	-	0	0	0.0.0.0
7	-	-	0	0	0.0.0.0
8	-	-	0	0	0.0.0.0
9	-	-	0	0	0.0.0.0
10	-	-	0	0	0.0.0.0
11	-	-	0	0	0.0.0.0
12	-	-	0	0	0.0.0.0
13	-	-	0	0	0.0.0.0
14	-	-	0	0	0.0.0.0
15	-	-	0	0	0.0.0.0
16	-	-	0	0	0.0.0.0

Configure an Internal Server behind SUA



Introduction

You can deploy internal servers (e.g., Web, FTP or mail server) that are accessible by outside users, even though SUA makes your LAN appear as a single machine to the outside world. A service is identified by the port number. Also, since you need to specify the IP address of a server behind the

AMG1011/1001-T10A, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time the AMG1011/1001-T10A is powered on.

Configuration

To make a server visible to the outside world, specify the port number of the service and the inside address of the server via the web GUI, Advanced Setup, **Advance Setup -> NAT -> DMZ.** The outside users can access the local server using the ***WAN IP*** address of the AMG1011/1001-T10A, which can be obtained via the web GUI, **Status -> Device Info**. For example: **Configuring an internal Web server for outside access** (suppose the Server IP address is 192.168.1.33).

Enable DMZ and specify the DMZ Host IP address. Click on the “Save” button.

Note that there are some default ports for different applications. If you want to change them, you can specify it in the start port number and end port number columns, and then click on the “Save” button to submit your settings.

Default port numbers for specific services

Service	Port Number
FTP	21
SSH	22
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80
POP3	110
HTTPs	443
PPTP	1723
VNC	5900
T.120	1503
H.232	1720

Configure a PPTP server behind SUA

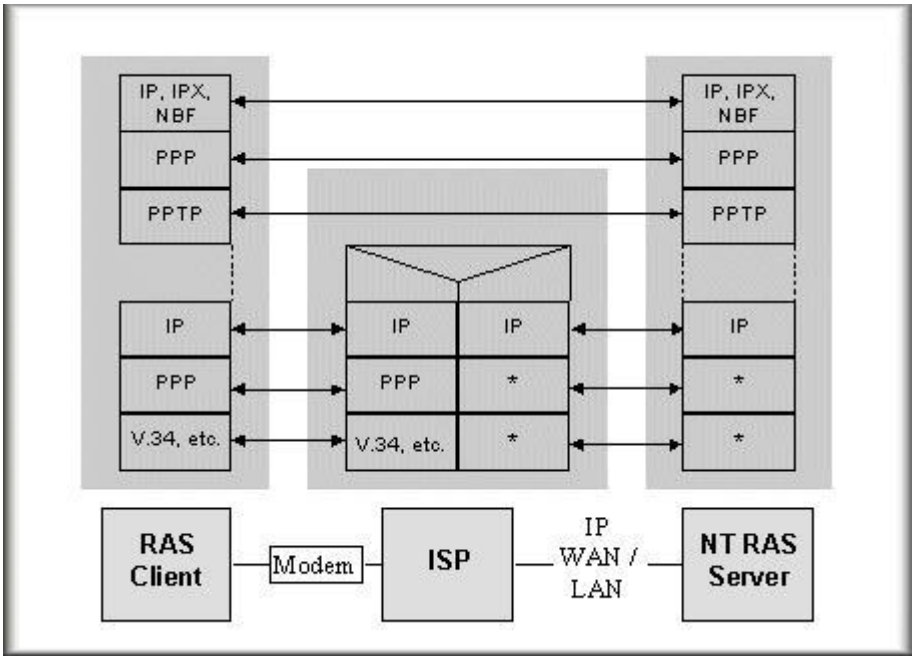
Introduction

PPTP is a tunneling protocol defined by the PPTP forum that allows PPP packets to be encapsulated within the Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself.

In order to run the Windows 9x PPTP client, you must be able to establish an IP connection with a tunnel server such as the Windows NT Server 4.0 Remote Access Server.

Windows Dial-Up Networking uses the Internet standard Point-to-Point (PPP) to provide a secure, optimized multiple-protocol network connection over dial-up telephone lines. All data sent over this connection can be encrypted and compressed, and multiple network level protocols (TCP/IP, NetBEUI and

IPX) can be run correctly. Windows NT Domain Login level security is preserved even across the Internet.



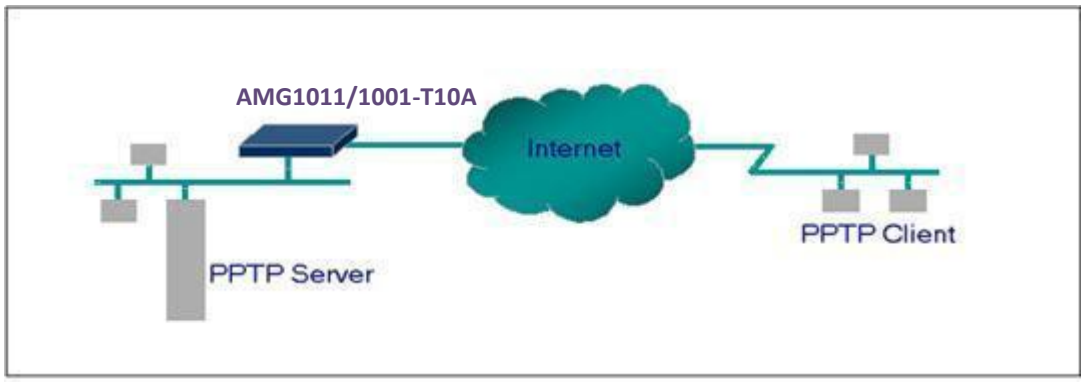
Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

PPTP appears as a new modem type (Virtual Private Networking Adapter) that can be selected when setting up a connection in the Dial-Up Networking folder. The VPN Adapter type does not appear elsewhere in the system. Since PPTP encapsulates its data stream in the PPP protocol, the VPN requires a second dial-up adapter. This second dial-up adapter for VPN is added during the installation phase of the Upgrade in addition to the first dial -up adapter that provides PPP support for the analog or ISDN modem.

The PPTP is supported in Windows NT and Windows 98 already. For Windows 95, it needs to be upgraded by the Dial-Up Networking 1.2 upgrade.

Configuration

This application note explains how to establish a PPTP connection with a remote private network in the AMG1011/1001-T10A SUA case. By default, the port number of the PPTP is 1723.



Example

The following example shows how to dial to an ISP via the AMG1011/1001-T10A and then establish a tunnel to a private network. There will be three items that you need to set up for a PPTP application; these are PPTP server (WinNT), PPTP client (Win9x) and the AMG1011/1001-T10A.

(1) PPTP server setup (WinNT)

- Add the VPN service from Control Panel ->Network
- Add a user account for a PPTP logged on user
- Enable the RAS port
- Select the network protocols from RAS such as IPX, TCP/IP NetBEUI
- Set the Internet gateway as the AMG1011/1001-T10A

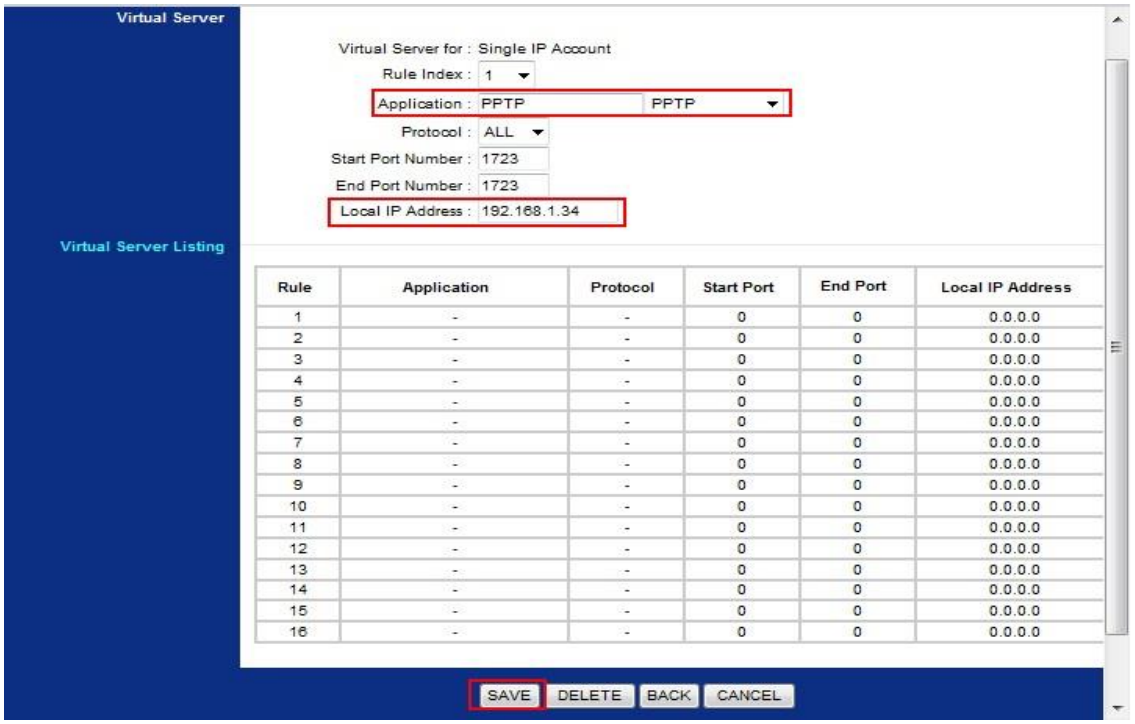
(2) PPTP client setup (Win9x)

- Add one VPN connection from Dial-Up Networking by specifying the correct username & password, and the IP address of the AMG1011/1001-T10A's Internet IP address for logging into the NT RAS server.
- Set the Internet gateway to the router that is connecting to ISP.

(3) AMG1011/1001-T10A setup

- Before making a VPN connection from Win9x to WinNT server, you need to connect the AMG1011/1001-T10A router to your ISP first.
- Enter the IP address of the PPTP server (WinNT server) and the port number for PPTP as shown below:

Select service name as „PPTP", specify the Server IP address, and then click on the "Save" button.



When you have finished the above settings, you can ping the remote Win9x client from WinNT. This ping command is used to demonstrate that the remote Win9x can be reached across the Internet. If the Internet connection between two LANs is achievable, you can place a VPN call from the remote Win9x client.

For example: C:\ping 203.66.113.2

When a dial-up connection to the ISP is established, a default gateway is assigned to the router traffic through that connection. Therefore, the output below shows the default gateway of the Win9x client after the dial-up connection has been established.

Before making a VPN connection from the Win9x client to the NT server, you need to know the exact Internet IP address that the ISP assigns to the AMG1011/1001-T10A router in SUA mode and enter this IP address in the VPN dial-up dialog box.

You can check this Internet IP address from the PNC Monitor or the web GUI, **Status -> Device Info.** If the Internet IP address is a fixed IP address provided by the ISP in SUA mode, then you can always use this IP address for reaching the VPN server.

In the following example, the ISP dynamically assigns the IP address ‘140.113.1.225’. You must enter this IP address in the 'VPN Server' dialog box for reaching the PPTP server. After the VPN link is established, you can start the network protocol application such as IP, IPX and NetBEUI.

6. Using Full Feature NAT

When the AMG1011/1001-T10A is in Routing mode, you can select the NAT Option as Multiple IPs (equal to Full Feature) in **Advanced Setup -> NAT-> Number of**
IPs:

Key Settings:

Field	Options	Description
Numbers of IPs	**Multiple**	When you select this option you can select Address Mapping Set Number 1~8 in the drop-down menu in **Virtual Circuit**.
	Single	When you select this option, this remote node will use default SUA Address Mapping Set. You can see it in CLI by using the command **ip nat lookup** **255**" is a read-only set with two rules: **Many-to-One** and **server** mapping. Select **Full Feature** when you require other mapping types.

Configuring NAT

Address Mapping Sets and NAT Server Sets

The AMG1011/1001-T10A has 8 remote nodes and allows you to configure 8 NAT Address Mapping Sets, You must specify which NAT Address Mapping Set (1~8) to use in the remote node when you select **Multiple IPs.** You can edit 8 rules for each Address Mapping Set.

The NAT Server Set is a list of LAN side servers mapped to external ports. We can configure it via the web GUI, Advanced Setup, **Advanced Setup -> NAT -> IP Address Mapping.** To use the NAT server sets that you have configured, a **Server** rule must be set up inside the NAT Address Mapping set. Please see NAT Server Sets for further information on how to apply it.

Configure Address Mapping Sets from the **web GUI** and **CLI**

Begin with the wen GUI

From the web GUI, Advanced Setup, **Advanced Setup -> NAT -> IP Address Mapping:**

This menu is for Address Mapping Set #1, you can edit 8 Address Mapping Rules for Set #1. You can edit or delete a rule by clicking the two buttons below the rule table.

Click to select the rule number you want to set from the drop-down menu, and then the rule type and Start/End IP addresses.

The following table explains the fields in the above screen.

Field	Description	Option/Example
Rule Index	This is the sequence number for Address Mapping Sets.	1~8
Rule Type	This is the NAT mapping types.	One-to-one, Many-to-One, Many-to-Many Overload, Many-to-Many No Overload and Server
Local Start IP	This is the starting local IP address (ILA).	0.0.0.0
Local End IP	This is the ending local IP address (ILA). If the rule is for all local IP addresses , then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for **One-to-One** type. This is the ending local IP address (ILA). If the rule is This is the ending local IP address (ILA). If the rule is	255.255.255.255
Public Start IP	This is the starting global IP address (IGA). If you have a dynamic IP address, enter 0.0.0.0 as the Global Start IP address. This is the starting global IP address (IGA). If you	0.0.0.0
Public End IP	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** types.	200.1.1.64

Note: All Local and Public End IP address must begin after the IP Start address, i.e., you cannot have an End IP address beginning before the Start IP address.

NAT Server Sets

The NAT Server Set is a list of LAN side servers mapped to external ports. If you wish, you can deploy inside servers for different services, e.g., Web or FTP, visible to the outside users, even though NAT makes your network appear as a single machine to the outside world. A server is identified by the port number, e.g., Web service is on port 80 and FTP on port 21.

As an example (see the following figure), if you have a Web server at 192.168.1.36 and an FTP server at 192.168.1.33, then you need to specify port 80 (Web) of the server at IP address 192.168.1.36, and for port 21 (FTP) at the IP address 192.168.1.33.

Please note that a server can support more than one service, e.g., a server can provide both FTP and Mail service, while another provides only Web service.

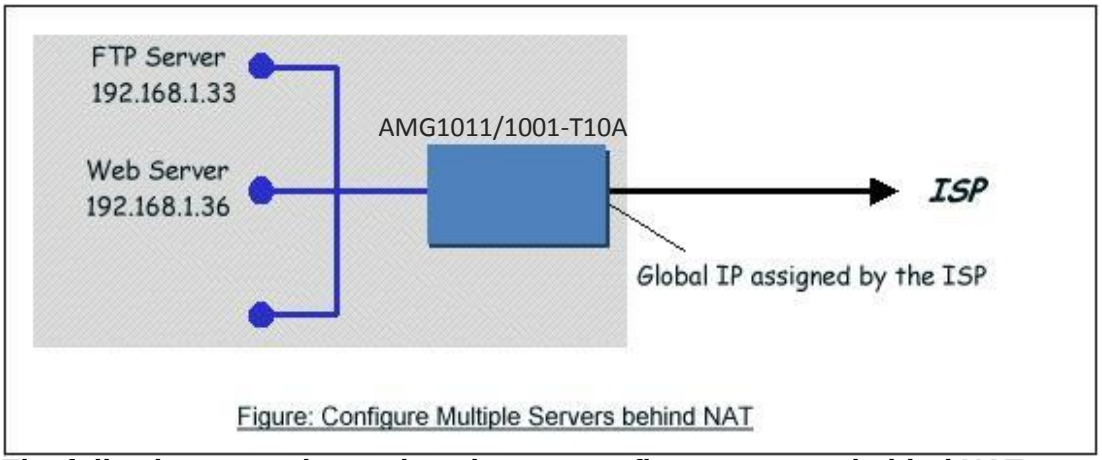
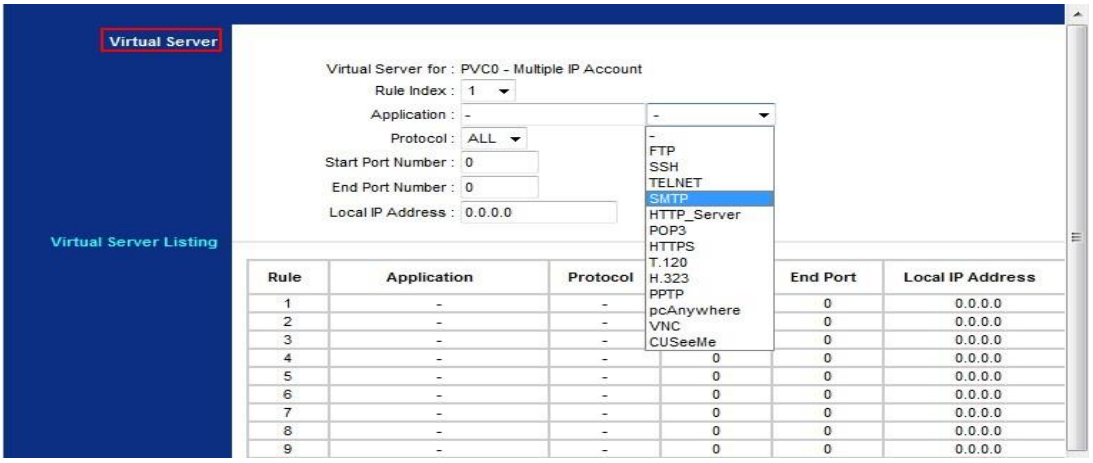


Figure: Configure Multiple Servers behind NAT

The following procedures show how to configure a server behind NAT.

Step 1: Login to the web GUI, **Advanced Setup -> NAT -> Virtual Server**

Step 2: Select the service name from the drop-down menu, and fill in the server address on "**Local IP Address**" and then save it.



Step 3: You can modify the Service name, Server IP Address, Start/End Port.

The commonly used port numbers are shown in the following table. Please refer RFC 1700 for further information about port numbers.

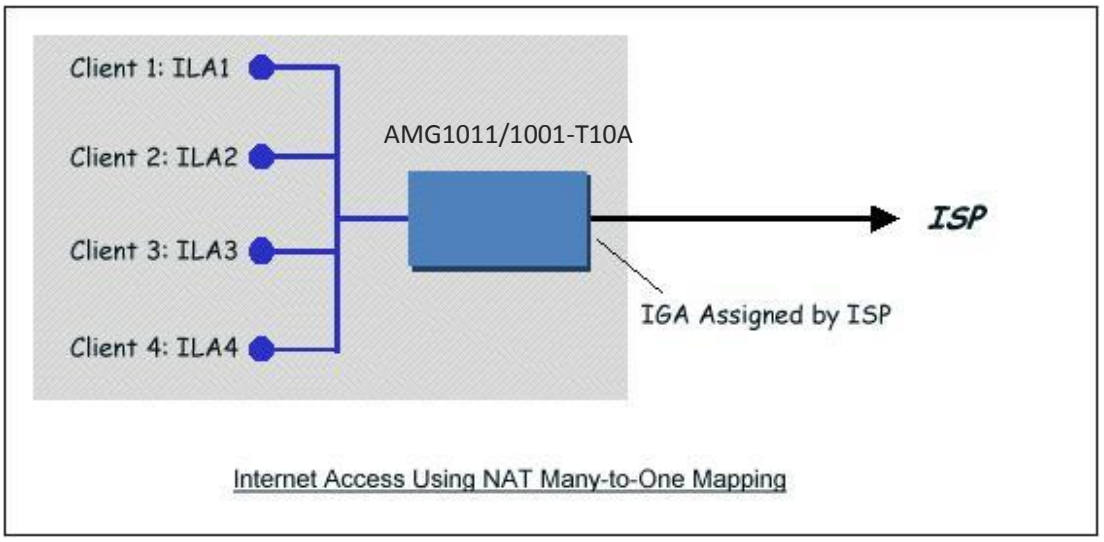
Service	Port Number
FTP	21
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

- **Examples**

- Internet Access Only
- Internet Access with an Internal Server
- Using Multiple Global IP addresses for clients and servers
- Support for Non NAT Friendly Applications

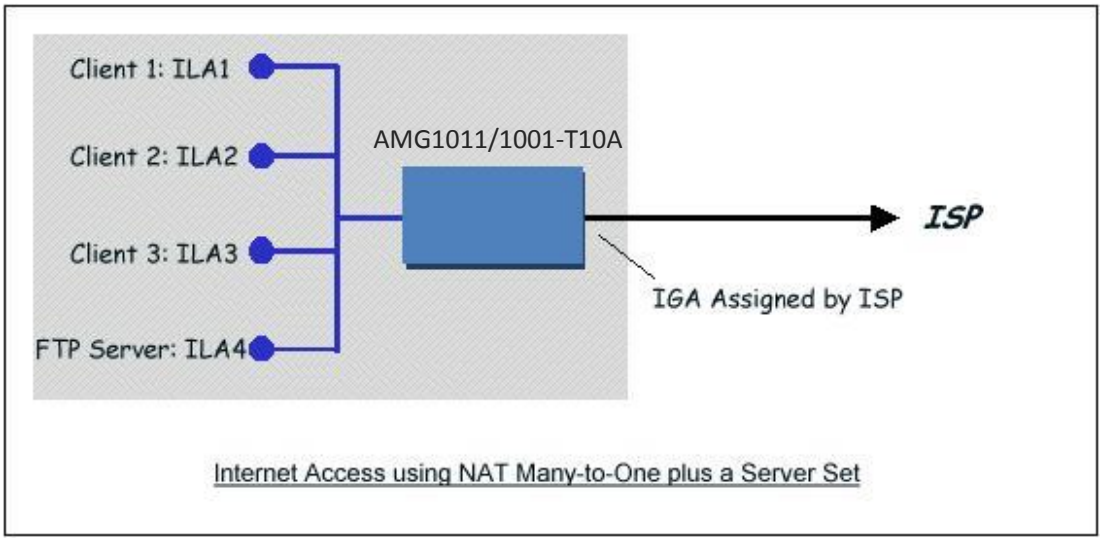
(1) Internet Access Only

In the Internet Access example, we only need one rule where all our ILAs map to one IGA assigned by the ISP. You can just use the d default **Single NAT** or you could select **Multiple NAT** and select an Address Mapping Set with a **Many-to-One** Rule. See the following figure.

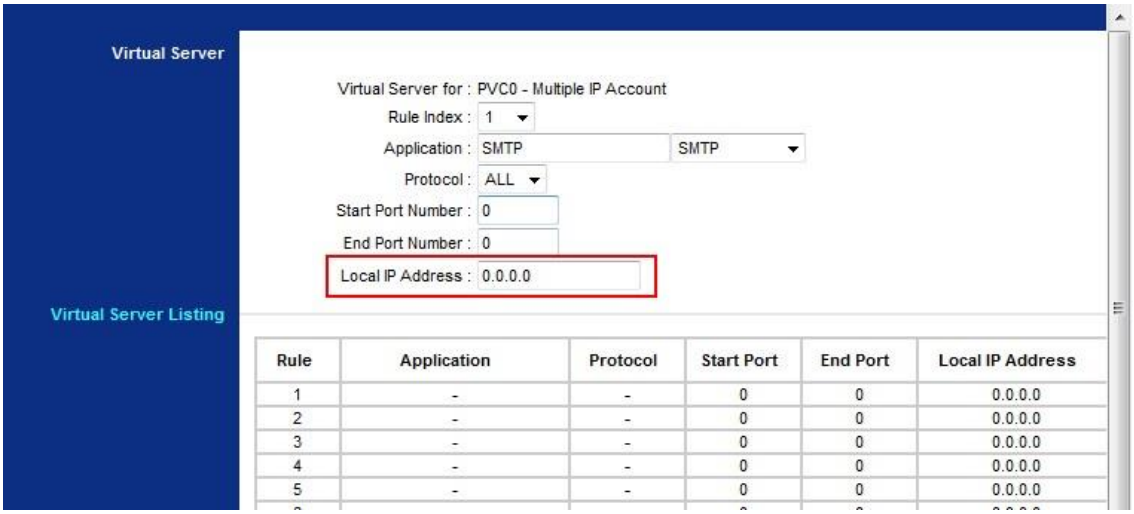


Internet Access Using NAT Many-to-One Mapping

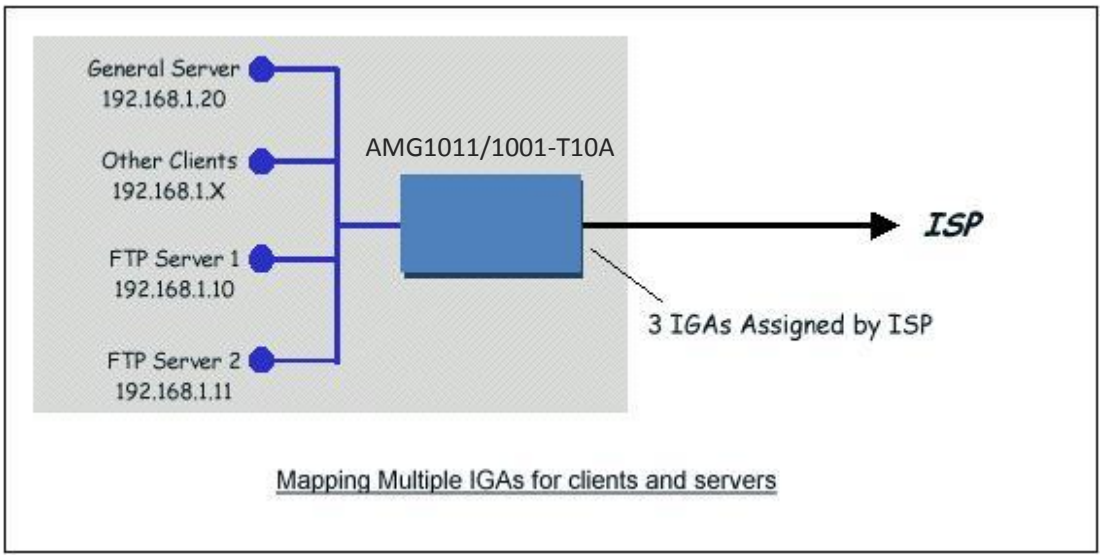
(2) Internet Access with an Internal Server



In this case, we do exactly as the figure (use the convenient pre-configured SUA Only set) and go to the web GUI, Advanced Setup, **Advanced Setup -> NAT -> Virtual Server** to specify the Internet Server behind the NAT, as shown below:



(3) Using Multiple Global IP addresses for clients and servers (One-to-One, Many-to-One, Server Set mapping types are used)



Mapping Multiple IGAs for clients and servers

In this case we have 3 IGAs from the ISP. We have two very busy internal FTP servers and also an internal general server for the web and mail. In this case, we want to assign the 3 IGAs by the following way using 4 NAT rules.

- Rule 1 (One-to-One type) to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.0.0.1).
- Rule 2 (One-to-One type) to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).
- Rule 3 (Many-to-One type) to map the other clients to IGA3 (200.0.0.3).
- Rule 4 (Server type) to map a web server and mail server with ILA3 (192.168.1.20) to IGA3. Type **Server** allows us to specify multiple servers, of different types, to other machines behind NAT on the LAN.

Step 1: In this case, we need to map ILA to more than one IGAs, therefore we must choose the **Multiple IPs** option from the **NAT** field in the currently active remote node, and assign IGA3 to the AMG1011/1001-T10A's WAN IP address.

Step 2: Go to the web GUI, Advanced Setup, **Advanced Setup-> NAT ->**

IP Address Mapping to begin configuring Address Mapping Set #1. We can see there are 8 blank rule tables that could be configured. See the following setup for the four rules in our case.

Rule 1 Setup: Select **One-to-One** type to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.0.0.1).

Rule 2 Setup: Selecting **One-to-One** type to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).

Rule 3 Setup: Select **Many-to-One** type to map the other clients to IGA3 (200.0.0.3).

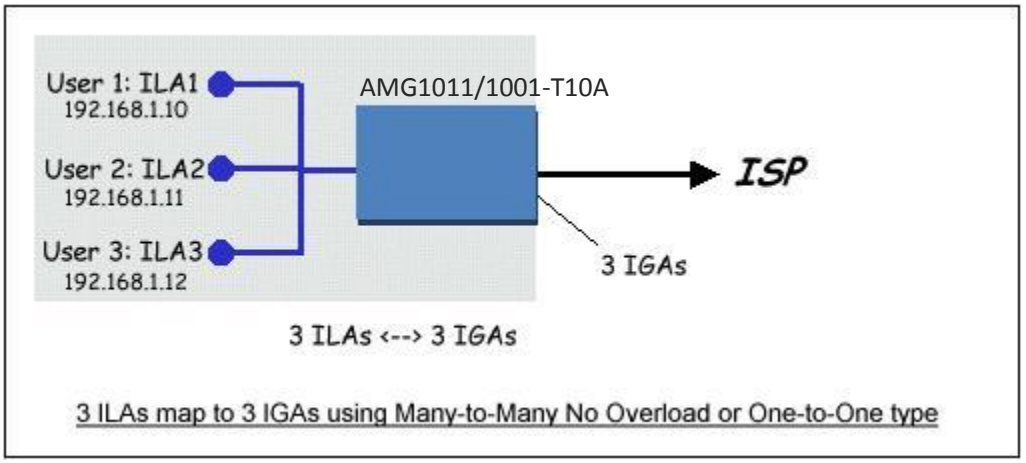
Rule 4 Setup: Select **Server type** to map our web server and mail server with ILA3 (192.168.1.20) to IGA3.

Menu **Network -> NAT -> Address Mapping** should look as follows:

Step 3: Now we configure all other incoming traffic to go to our web server and mail server via the web GUI.

(4) Support Non NAT Friendly Applications

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. In this case it is better to use Many-to-Many No Overload or One-to-One NAT mapping types, thus each user can login to the server using a unique global IP address. The following figure illustrates this.



3 ILAs map to 3 IGAs using Many-to-Many No Overload or One-to-One type

7. Using the Dynamic DNS (DDNS)

- What is DDNS?

The DDNS service, an IP Registry provides a public central database where information such as email addresses, hostnames; IPs etc. can be stored and

retrieved. This solves the problems if your DNS server uses an IP address associated with dynamic IP addresses.

Without DDNS, we always tell the users to use the WAN IP address of the AMG1011/1001-T10A to access the internal server. It is inconvenient for the users if this IP address is dynamic. With DDNS supported by the AMG1011/1001-T10A, you can apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP address of the AMG1011/1001-T10A. When the ISP assigns the AMG1011/1001-T10A a new IP address, the AMG1011/1001-T10A must notify the DDNS server about the change of this IP address so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) will still be usable.

The DDNS server that the AMG1011/1001-T10A currently supports is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP address.

- Setup the DDNS

1. Before configuring the DDNS settings in the AMG1011/1001-T10A, you must register an account from the DDNS server such as WWW.DYNDNS.ORG first. After the registration, you have a hostname for your internal server and a password that is used to update the IP address to the DDNS server.

2. Login to the web GUI, Advanced Setup, **Access Management -> Dynamic DNS** Select **'Active'** option:

Key Settings:

Option	Description
Service Provider	Currently, we support WWW.DYNDNS.ORG.
My Host Name	Enter the hostname that you subscribed from the above DDNS server. For example, zyxel.com.tw.
E-mail Address	Enter your e-mail address from which you can be contacted when necessary.
User Name	Enter the user name that the DDNS server gives to you.
Password	Enter the password that the DDNS server gives to you.
Enable Wildcard	Enter the hostname for the wildcard function that the WWW.DYNDNS.ORG supports. Note that Wildcard option is available only when the provider is http://www.dyndns.org/.

8. Network Management Using SNMP

- ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some AMG1011/1001-T10A routers. It is implemented based on the SNMPv1, so it will be able to communicate with SNMPv1 NMSs. Further, users can also add ZyXEL's private MIB in the NMS to monitor and control additional system variables. The ZyXEL's private MIB tree is shown in figure 3. For SNMPv1 operation, ZyXEL permits one community string so that the router can belong to only one community and allows trap messages to be sent to only one NMS manager.

Some traps are sent to the SNMP manager when anyone of the following events occur:

1. coldStart (defined in RFC-1215):

   If the machine cold starts, the trap will be sent after booting.

2. warmStart (defined in RFC-1215):

   If the machine warm starts, the trap will be sent after booting.

3. linkDown (defined in RFC-1215):

   If any link of ADSL or WAN is down, the trap will be sent with the port number. The port number is its interface index under the interface group.

4. linkUp (defined in RFC-1215):

If any link of ADSL or WAN is up, the trap will be sent with the port number. The port number is its interface index under the interface group.

5. authenticationFailure (defined in RFC -1215) :

When receiving any SNMP get or set requirement with wrong community, this trap is sent to the manager.

6. whyReboot (defined in ZYXEL-MIB) :

When the system is going to restart (warmstart), the trap will be sent with the reason of restart before rebooting.

(1) For intentional reboot:

In some cases (download new files, CI command "sys reboot", etc.), reboot is done intentionally. And traps with the message "System reboot by user!" will be sent.

(2) For fatal error:

System has to reboot for some fatal errors. Traps with the message of the fatal code will be sent.

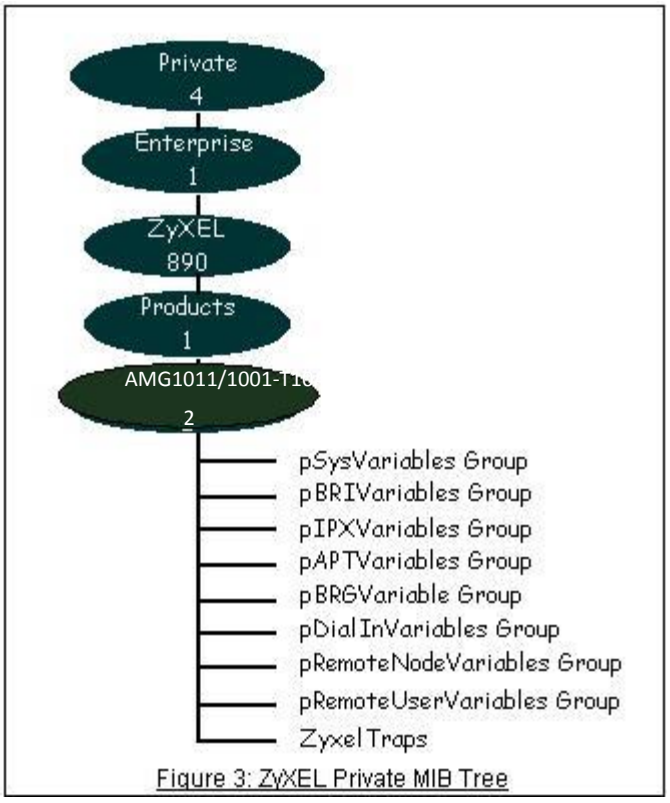
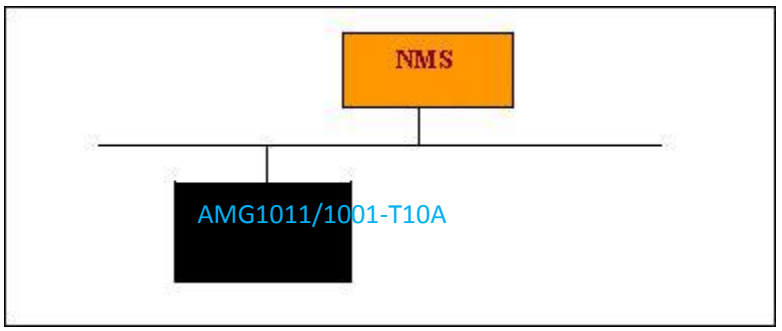


Figure 3: ZyXEL Private MIB Tree

Downloading ZyXEL's private MIB

- Configure the AMG1011/1001-T10A for SNMP



The SNMP related settings in AMG1011/1001-T10A are configured via the web GUI, Advanced Setup, **Access Management -> SNMP.**

Key Settings:

Get Community	Select to set the password for the incoming Get- and Get Next requests from the management station.
Set Community	Select to set the password for incoming Set requests from the management station.

9. Using system log

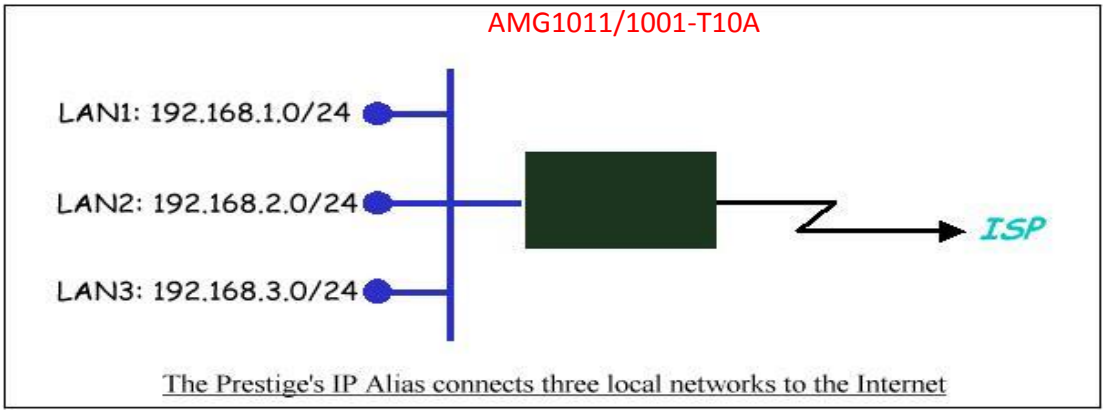
Our ADSL Router keeps a running log of events and activities occurring on the router. If the device is rebooted, the logs are automatically cleared.

You can check your log via the web GUI, Advanced Setup, **Status -> System Log.**

10. Using IP Alias

- **What is IP Alias?**

In a typical environment, a LAN router is required to connect two local networks. The AMG1011/1001-T10A can connect three local networks to the ISP or a remote node; we call this function **'IP Alias'**. In this case, an internal router is not required. For example, the network manager can divide the local network into three networks and connect them to the Internet using AMG1011/1001-T10A's single user account. See the figure below.



The Prestige's IP Alias connects three local networks to the Internet

The AMG1011/1001-T10A supports three virtual LAN interfaces via its single physical Ethernet interface. The first network can be configured via the web GUI, Advanced Setup, **Interface Setup -> LAN -> DHCP**. The second and third networks can be configured via the telnet CLI.

There are three internal virtual LAN interfaces for the AMG1011/1001-T10A to route the packets from/to the three networks correctly. They are **enif0** for the major network, **enif0:0** for the IP alias 1, and **enif0:1** for the IP alias 2. Therefore, three routes are created in the AMG1011/1001-T10A as (shown below) when the three networks are configured. You can edit IP alias routes of the AMG1011/1001-T10A by a command in the **CLI**: **lan index [index number]**

Usage: index number =1 main LAN 2
IP Alias#1 3
IP Alias#2

lan ipaddr <ip address> <Mask>
lan save

If the AMG1011/1001-T10A's DHCP is also enabled, the IP pool for the clients can be any of the three networks.

AMG-1011-T10A > ip if

```
enif0: mtu 1500
    inet 192.168.1.1, netmask 0xffffff00, broadcast 192.168.1.255
    RIP RX:Ver 1 & 2, TX:Ver 1 compatible,  chan: enet0 804db490
    [InOctets        233217] [InUnicast      3795] [InMulticast          317]
    [InDiscards           0] [InErrors          0] [InUnknownProtos         0]
    [OutOctets       241466] [OutUnicast     3494] [OutMulticast           4]
    [OutDiscards          0] [OutErrors         0]
enif0:0: mtu 1500
    inet 192.168.2.1, netmask 0xffffff00, broadcast 192.168.2.255
    RIP RX:None, TX:None,  chan: enet0 804db490
    [InOctets             0] [InUnicast         0] [InMulticast             0]
    [InDiscards           0] [InErrors          0] [InUnknownProtos         0]
    [OutOctets            0] [OutUnicast        0] [OutMulticast            0]
    [OutDiscards          0] [OutErrors         0]
enif0:1: mtu 1500
    inet 192.168.3.1, netmask 0xffffff00, broadcast 192.168.3.255
    RIP RX:None, TX:None,  chan: enet0 804db490
    [InOctets             0] [InUnicast         0] [InMulticast             0]
    [InDiscards           0] [InErrors          0] [InUnknownProtos         0]
    [OutOctets            0] [OutUnicast        0] [OutMulticast            0]
    [OutDiscards          0] [OutErrors         0]
enif0:2: mtu 1500
    inet 0.0.0.0, netmask 0x00000000, broadcast 0.0.0.0
    RIP RX:None, TX:None,  chan: enet0 804db490
    [InOctets             0] [InUnicast         0] [InMulticast             0]
    [InDiscards           0] [InErrors          0] [InUnknownProtos         0]
    [OutOctets            0] [OutUnicast        0] [OutMulticast            0]
    [OutDiscards          0] [OutErrors         0]
enif0:3: mtu 1500
    inet 0.0.0.0, netmask 0x00000000, broadcast 0.0.0.0
    RIP RX:None, TX:None,  chan: enet0 804db490
    [InOctets             0] [InUnicast         0] [InMulticast             0]
    [InDiscards           0] [InErrors          0] [InUnknownProtos         0]
    [OutOctets            0] [OutUnicast        0] [OutMulticast            0]
    [OutDiscards          0] [OutErrors         0]
```

You can edit filter rules to accept or deny LAN packets from/to the IP alias 1/2 go through the AMG1011/1001-T10A by command in **CLI**:

lan index [index number]

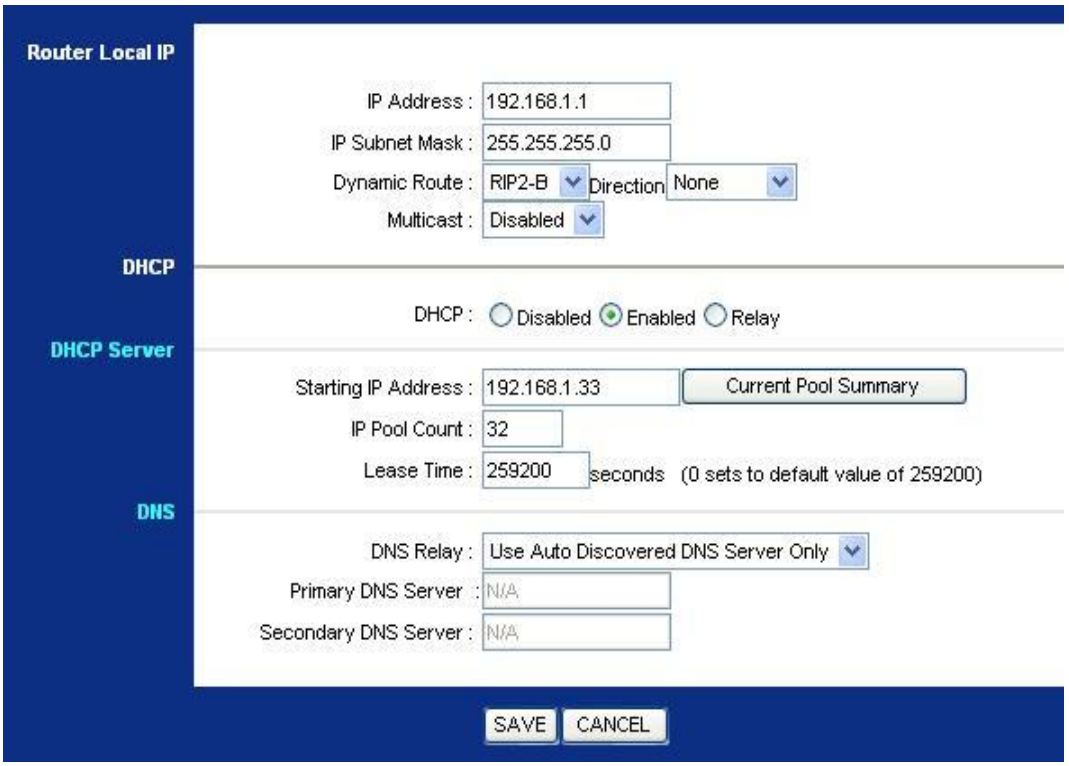
Usage: index number =1 main LAN 2
IP Alias#1 3
IP Alias#2

lan filter <incoming|outgoing> <tcpip|generic> [set#]

Usage: set#= the corresponding filter set number you have configured **lan save**

- IP Alias Setup

(1) Edit the first network via the web GUI, Advanced Setup, **Interface Setup -> LAN -> DHCP** by configuring the AMG1011/1001-T10A's first LAN IP address.



Key Settings:

DHCP	If the AMG1011/1001-T10A's DHCP server is enabled, the IP pool for the clients can be any of the three networks.

(2)The second and third networks can be configured via the CLI with the commands mentioned above.

11. Using IP Multicast

- **What is IP Multicast?**

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. H ost groups are identified by class D IP addresses, i.e., those with "1110" as their higher-order bits. In dotted decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. Among them, 224.0.0.1 is assigned to the

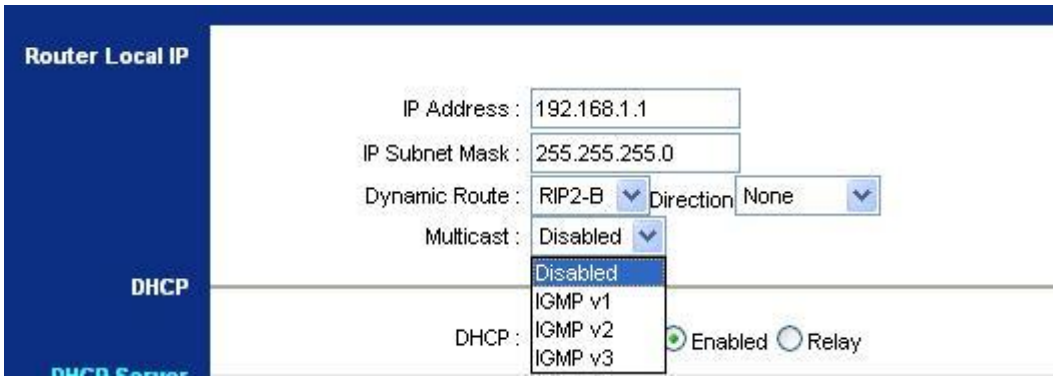
permanent IP hosts group, and 224.0.0.2 is assigned to the multicast routers group.

IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC2236). IP hosts use IGMP to report their multicast group membership to any immediate -neighbor multicast routers so the multicast routers can decide if a multi cast packet needs to be forwarded. At start up, the AMG1011/1001-T10A queries all directly connected networks to gather group membership.

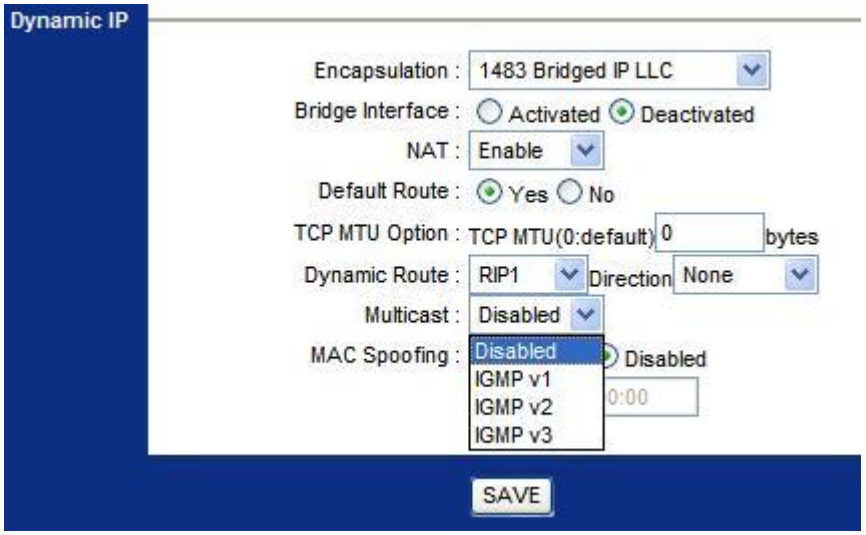
After that, the AMG1011/1001-T10A updates the information by periodic queries. The AMG1011/1001-T10A implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.

- **IP Multicast Setup**

(1) Enable IGMP in the AMG1011/1001-T10A's LAN via the web GUI, Advanced Setup,
Interface Setup -> LAN -> Router Local IP.



(2) Enable IGMP in the AMG1011/1001-T10A's remote node via the web GUI, Advanced Setup, **Interface Setup -> Internet -> Dynamic IP.**



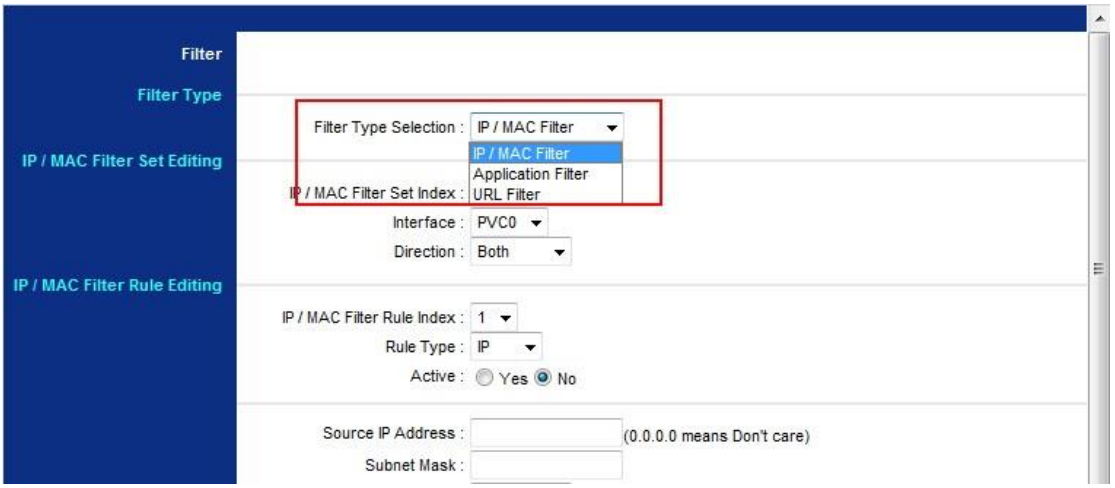
Key Settings:

Multicast	IGMP-v1 for IGMP version 1, IGMP-v2 for IGMP version 2. IGMP-v3 for IGMP version 3.

12. What is the procedure to configure packet filter on the AMG1011/1001-T10A?

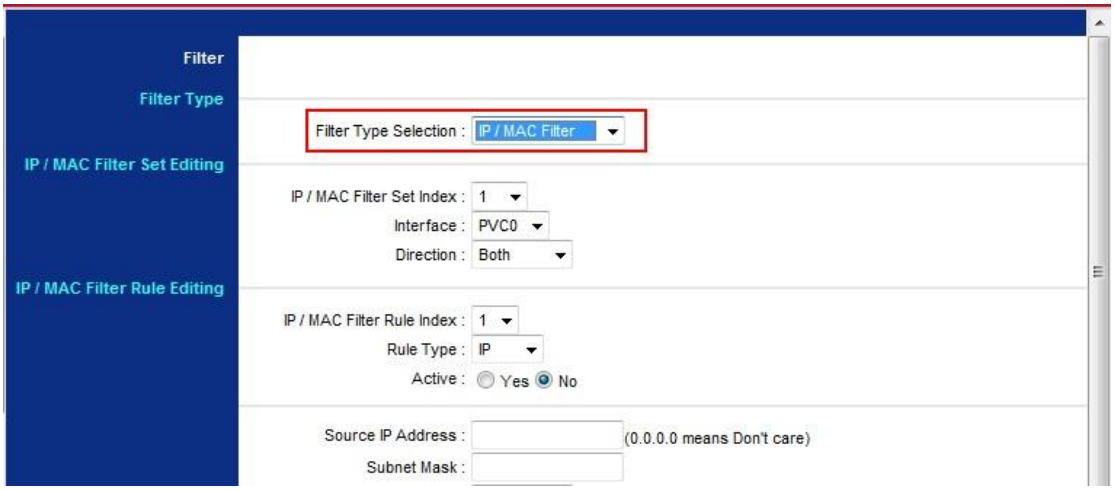
The AMG1011/1001-T10A allows you to configure up to three types: IP/MAC filter; Application filter; URL filter.

You can configure this via the web configuration page: **Access Management -> Filter**



For each type, there are different filter rules for you to define.

Filter by IP/MAC

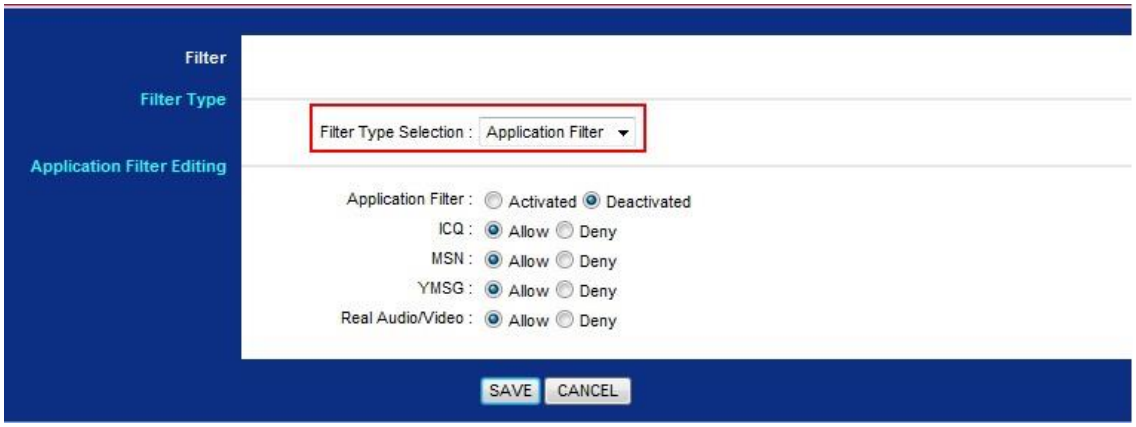


ZyXEL

Key Settings:

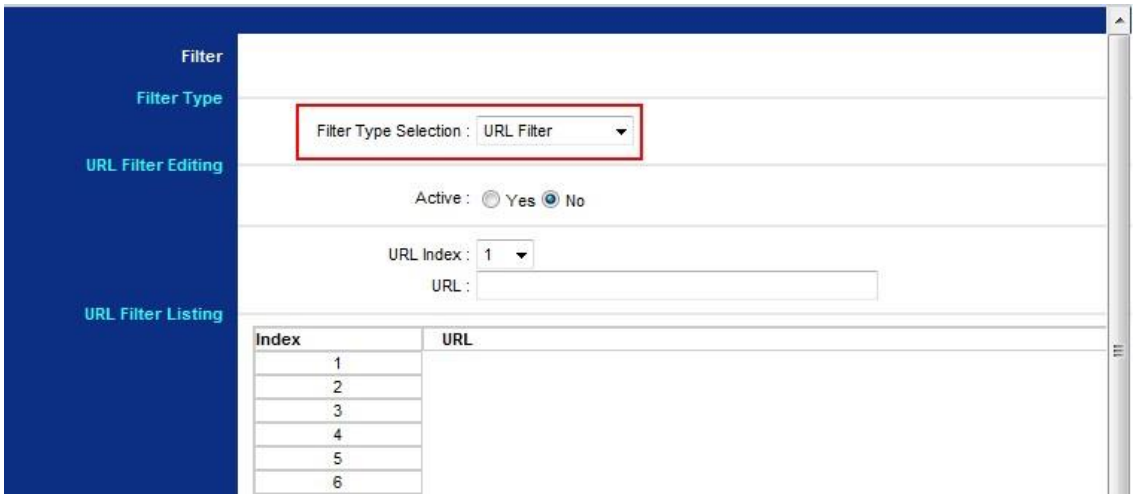
IP/MAC Filter Set Editing	IP/MAC Filter Set Index	Select to define set index number. There are twelve sets in all
	Interface	Choose to set an active PVC from the drop-down menu.
	Direction	Choose one filter direction: Both, Incoming, Outgoing.
IP/MAC Filter Rule Editing	IP/MAC Filter Rule Index	Choose a number as a rule index. There are 6 rules you can configure
	Rule Type	You can choose to filter by IP or MAC. If you choose filter by IP, you will need to set source and destination IP as well as port number of those packets that you want to filter address according to your need; if you choose MAC as filter condition, you may need to set their MAC addresses from/to where the packets come/go
	Protocol	You can choose one of the protocols: (TCP, UDP or ICMP) to filter the packets.
	Rule Unmatched	Define the action that the AMG1011/1001-T10A would take when the packets meet none of the rules.
Ip/MAC Filter Listing	You can check your filter rules that you have set according to the set Index.	

Filter by Application



You can set filter conditions by applications.

Filter by URL



Here you can set filter rules by URL. Click to choose an index number and input its URL. Click “save” then you can find the rule listed below. You can set 16 rules here in all.

By factory default, ZyXEL has preconfigured many filter sets for your reference; you can check them via the web configuration page as shown above. This could satisfy most requirements. You could select on demand any of them to apply to the WAN node or LAN Interface.

Support Tools

1. LAN/WAN Packet Trace

The AMG1011/1001-T10A packet traces records and analyzes packets running on LAN and WAN interfaces. It is designed for users with technical backgrounds who are interested in the details of the packet flow on LAN or WAN end of the AMG1011/1001-T10A. It is also very helpful for diagnostics if you have compatibility problems with your ISP or if you want to know the details of a packet for configuring a filter rule.

The format of the display is as shown below:

Packet:

[index] [timer/second][channel-receive/transmit][length] [protocol] [sourceIP/port] [destIP/port]

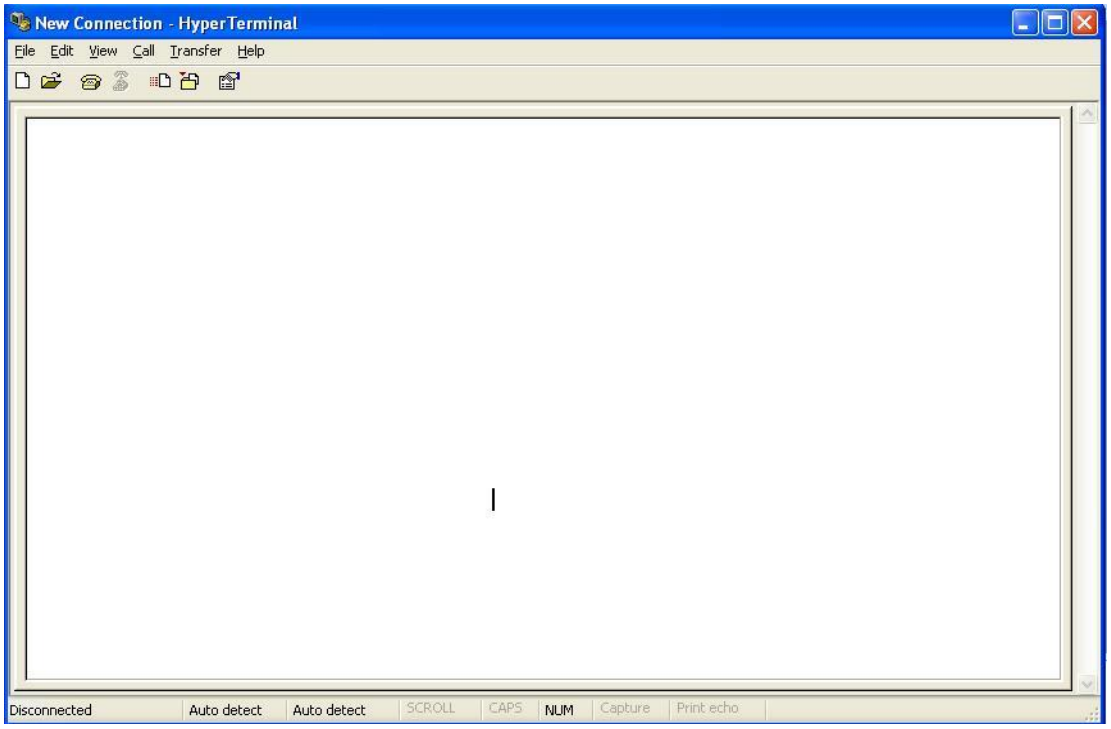
There are two ways to dump the trace:

Online Trace- - display the trace in real-time on the screen

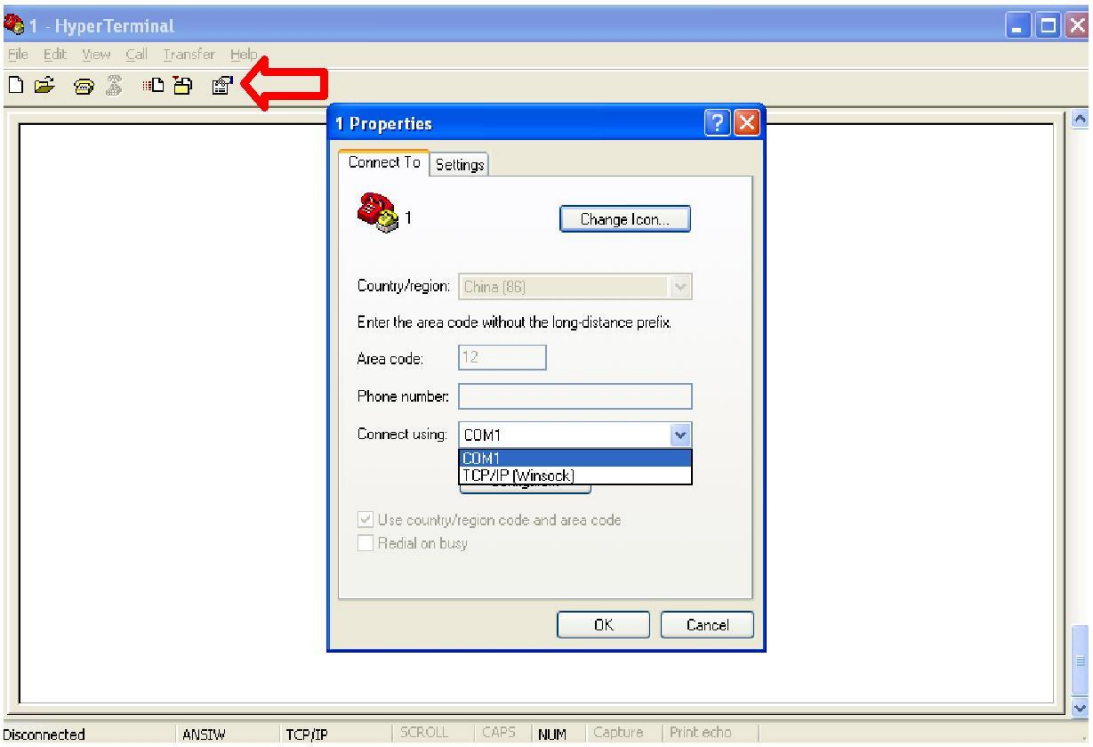
Offline Trace -- capture the trace first, and display later

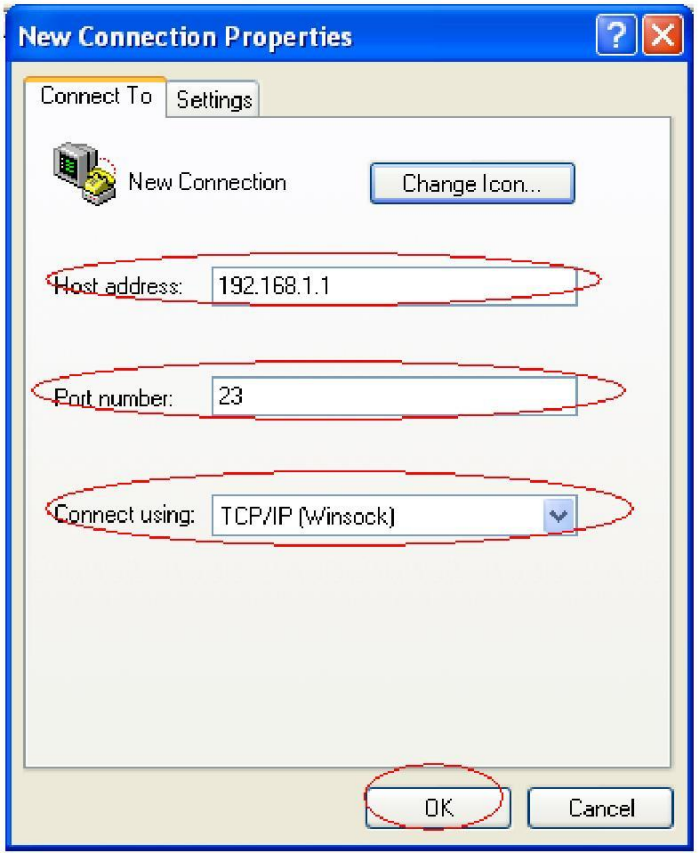
Trace packet by telnet

Step 1: Initiate a hyper terminal connection from your PC (suppose you are connected to the LAN port of AMG1011/1001-T10A).

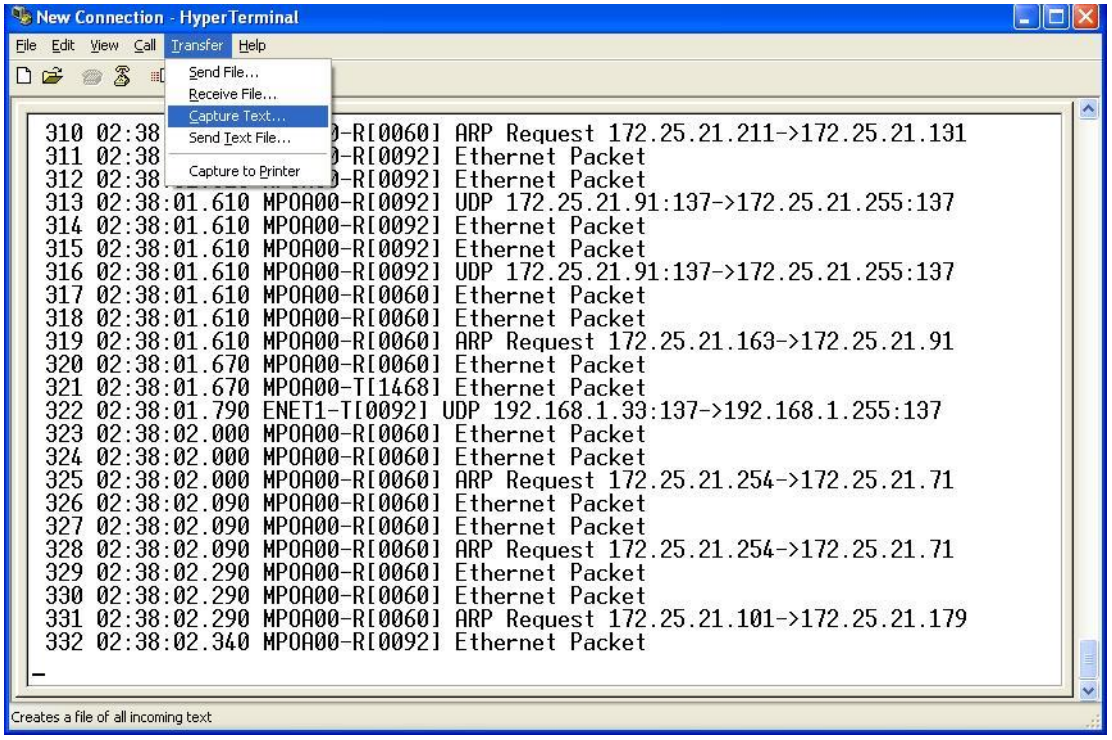


Step 2: Click “Properties‟ to configure parameters to telnet into the AMG1011/1001-T10A.





Step 3: After you issue the relevant commands, you can save the logs that you have captured.



CI Command Reference

Command Syntax and General User Interface

CI has the following command syntax:

command <*iface* | *device* > **subcommand** [*param*]
command subcommand [*param*]
command ? **| help**
command subcommand ? | help

General user interface:

1.	**?**	Shows the following commands and all major (sub)commands
2.	**exit**	Exit Subcommand

The latest CI Command list is available in the release notes of every ZyXEL firmware release. Please go to ZyXEL public web site http://www.zyxel.com/support/download_index.php to download the firmware package (*.zip). You should unzip the package to get the release notes in PDF format.