OVERVIEW

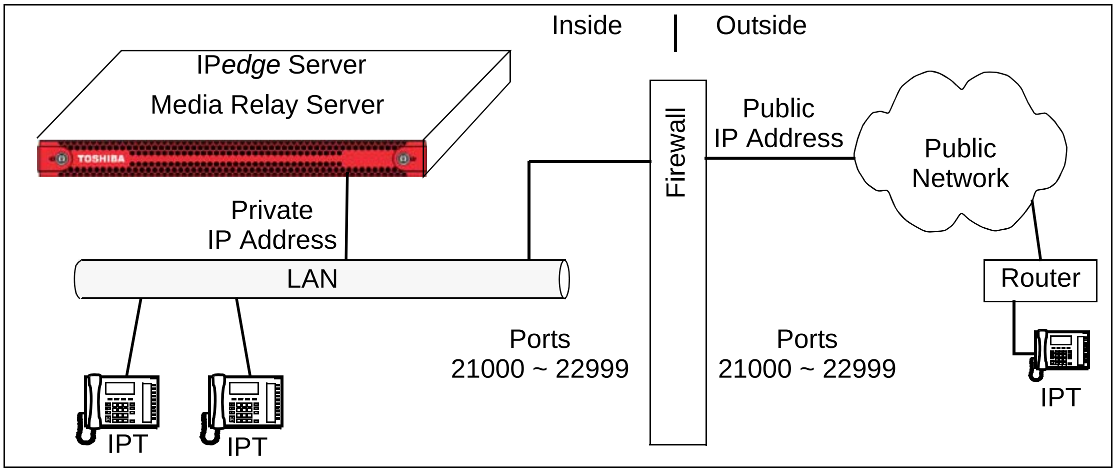
The IPedge Media Relay Server (MRS) changes VoIP packets so the IPT will send their audio stream to the IPedge system Public IP address instead of the IPedge system Private IP address. This helps alleviate audio problems during media operations.

Media Relay Server

The IPedge system Media Relay Server (MRS) alters VoIP packets so that IPT devices will be instructed to send their RTP (audio) stream to the IPedge system public IP address instead of the IPedge system private IP address. This can solve one-way audio conditions that may occur. Without the use of MRS, the remote IPT will not know the public IP address to which to send its audio stream. Similarly the MRS is also affects SIP Trunk RTP packet routing. However, the MRS is not a substitute for a SIP ALG router.

The MRS is configured by defining the Public IP address of the IPedge server and the port range to be used for calls. Each call requires two UDP ports for the audio streams (one port out bound, one port inbound).

Media Relay Server Enter the Public IP address of the IPedge server. Enter the port range to be used for calls. Each call requires two UDP ports for the audio streams (one port out bound, one port inbound).



PROGRAMMING

IPedge Configuration

1. Select **System > Media Relay Server**
    - Click on the **New** icon
    - Router Integration = Enable
    - Media Relay Server Service IDs = 1
    - Router IP Address = the Public IP Address of the Firewall
2. Click **OK**
3. Select the Port Forwarding Configuration.

Note: Typically; the Router Public Port Range values and the Media Relay Server Private Port Range values are the same.

- Router Public Port Range Low = Lowest port number (21000)
- Router Public Port Range High = Highest port number (22999)
- Media Relay Server Service ID = 1
- Media Relay Server Private Port Range Low = Lowest port number (21000)
- Media Relay Server Private Port Range High = Highest port number (22999)

4. Click on **OK**.
5. Select **Maintenance > System Maintenance > Core System Processes**.
6. Click the checkbox next to **Media Relay Server.**
7. Click on the **Send restart action** (double arrow) icon.
8. A dialog box warning that you are about restart the selected service will appear. Click on **OK**.
9. Click to check-mark **Call Processing**.
10. Click on the **Send restart action** icon.
11. A dialog box warning that you are about restart system will appear. Click on **OK**.
12. In the Send Command Parameters dialog box select **Normal start**.

Important! The next step will restart the system call processing. All calls will be dropped.

13. Click on **OK**.
14. Wait for the system to restart.

IPT Configuration

When the “IPT Data Auto Connection to MRS” is set to “Auto,” the IP*edge* system will determine whether the IPT is placed inside NAT or not, and specify the appropriate connection IP address in the SIP Session Description Protocol (SDP) information..

If the IPedge system is unable to determine the location of the media relay server (for example you hear one-way audio) set “Connection To Media Relay Server” to “Manual.” This will ensure that the MRS is used for the IPT connections.

To set the IPT Data Connection to use the Media Relay Server use these steps.

1. In Enterprise Manager select **Station > Station Assignment**.
2. Click to select the DN of the IPT. Select the **IPT** tab.
3. In the **Connection To Media Relay Server** field select **Manual**.
4. Click on the **Save** icon.

NETWORK SECURITY

After the IPedge system is installed, and the SIP Trunks and/or Remote IP Telephones are operational, it is the responsibility of the installer and system user to setup the firewall to help prevent unauthorized access.

While this can be accomplished in many ways one basic method is using lists. For example; Cisco devices can be configured using ACL’s (access control lists) and, in SonicWALL by setting up rules to Deny or allow specific IP addresses, or other means in other firewalls.

For example; the firewall configuration could be set to only allow specific IP addresses. Contact your SIP Provider for a list of the IP addresses their Signaling and Media will use. For a remote IPT add the static IP to the safe list, if the remote IPT is a dynamic IP you could list a range ips for use by the IPT, or even better require the use of a hardware VPN for all remote phones and software VPN for softphones that are roaming.

Any specific programming of firewall rules to secure access to the network and IPedge server are the responsibility of the installing dealer and/or customer and vary by the needs and level of protection determined by the customer’s IT department. Toshiba technical support does not assume responsibility to provide specific commands or to verify a network or specific IPedge server is secure.

FIREWALL SETUP

This section discusses firewall setup. Be sure that all of the port numbers as shown below are programmed into the firewall, allowing these ports to access the IPedge server IP address.

Firewall Ports to Open

The following lists are the firewall ports that must be open for the IPedge system to function behind a firewall.

All Systems

These firewall ports must be open for every system.

Function	Type	Use
20 and 21	TCP	IPT firmware download and update
22	TCP	SSH (Secure Data Connection)
23	TCP	Telnet (Terminal connection)
80	TCP	Redirects to 8080
1000	TCP	SMDI (SMDI, Soft Keys, Voice Record)
1718 to 1719	UDP	Remote IP Telephone set registration
2944	TCP	Remote IP Telephone MEGACO signaling)
3000	UDP	LAN DSS (Call control IP*edge* Net)
3001	UDP	If survivable IP*edge* server is in public network, the IP*edge* server in private network needs this port open.
4029	TCP	IP*edge* Net (Connection Request)
6000	TCP	LAN BLF (Status display IP*edge* Net)
8080	TCP	Enterprise Manager (HTTP)
9443	TCP	Enterprise Manager (HTTPS)
10000	TCP	Webmin
12000 to 13791	TCP	IP*edge* Net (Connection Request)
16000 to 17999	RTP/RTCP	IP*edge* Net (Node to node)
18000 to 19999	RTP/RTCP	IP*edge* Net (Node to IPT)
21000 to 26999	UDP	Remote IP or SIP telephone audio Refer to Specific Applications.

Specific Applications

The firewall ports shown in the table below must be open for specific applications.

Application	Ports	Type	Use
IP Mobility	90	TCP	IPedge Messaging Mobile App Port
Messaging	1007	TCP	Use by the System monitor Applet
	1008	TCP	Fax printer driver and Email Callback app
SIP Trunks and Stations	5060	UDP	(SIP trunks or SIP telephones outside the firewall)
(Sheet 1 of 2)			

Application	Ports	Type	Use (continued)
HTTPS	443	TCP	HTTPS
	9443	TCP	HTTPS
Unifier	1100 to 1105	TCP	Systems connecting with Unifier
Meeting	443	TCP	Meeting and/or HTTPS
	1270	TCP	**Note:** Port 1270 must be open for every user that will share their desktop. Desktop sharing will be very slow if moderators or participants, who are sharing their desktop, do not have port 1270 open.
	1935	TCP	
	1945	TCP	
	8444	TCP	
Net Server	8767 and 8768	TCP	
Messing DCN	3306 and 5432	TCP	
FAX Driver	1007 and 1008	TCP	
(Sheet 2 of 2)			

The table below shows the end point port ranges used in different system configurations.

IPedge Server Address	End Point IP Address	RTP Port Range for the MRS [1]
Public	Public	27000 ~ 27999 [2]
	Private (NAT)	27000 ~ 27999 [2]
Private	Public	21000 ~ 26999 [3]
	Private behind remote NAT	21000 ~ 26999 [4]
	Private	27000 ~ 27999 [2]
	Private behind local NAT	27000 ~ 27999 [2]
Set the MRS connection mode to Manual during NAT traversal and SIP/SIP Trunk.		21000 ~ 26999 [3]

1. RTP connection as ‘seen’ from the end point.
2. MRS internal port range is 27000 ~ 27999. This range is fixed.
3. MRS External port range is programmable. The range is 21000 ~ 26999.
4. MRS External port range is programmable. The range is 21000 ~ 26999.

Important! When the "IPT Data Auto Connection to MRS" is set to "Auto," the IP*edge* system will determine whether the IPT is placed inside NAT or not, and generate appropriate SDP.

If the IP*edge* system is unable to determine whether the IPT is placed inside NAT or not, (for example; if you hear one-way audio) set IPT Data Auto Connection to MRS" is set to "Manual.” This will ensure that the MRS is used for the IPT connections.

Internal System Ports

The table belowis a list of ports used by the IP*edge* system. Do not assign any of these ports to applications such as CSTA.

Port Numbers
20 ~ 23
25
68
90
110
111
123
143
161
162
443
993
1000
1100 ~ 1105
1270
1718 ~ 1720
1935
1945
(Sheet 1 of 4)
2020
2944
3000
3001
3306
4003
4029
5060
5070
6000
6379
6678
6800
7000 ~ 7009
7577
7583
8005
8009
(Sheet 2 of 4)
8080
8100
8443
8444
8445
8767
8768
9101 ~ 9103
9443
9999
10000
10030
10100 ~ 10103
10200
10201
12000 ~ 13791 (TCP)
12000 ~ 14511 (UDP)
(Sheet 3 of 4)
13000 ~ 19999
20023
20161
21000 ~ 26999
27000 ~ 29999
30000 ~ 30999
40000 ~ 40003
40005
40006
41088
54445
(Sheet 4 of 4)

CAPACITY

N/A

AVAILABILITY

N/A

RESTRICTIONS

When using MRS, most home office and small office routers require no configuration in the firewall and NAT locally as they tend to initiate the connection and save state for the inbound connection. In some cases this may not work and the ports references in Requirement 1 may also have to be opened on the home router.

Using the MRS the IPedge system dynamically and automatically configures port forwarding rules for any NAT traversal related issues. If, for some reason a remote IP telephone still cannot register due to local NAT router issues, configure the remote IP telephone’s station programming to use the Static MRS parameter. This will resolve any NAT issues that prevent registration of the IP telephone.

HARDWARE

No additional hardware is necessary for this feature.

FEATURE INTERACTION

Client Applications

ACD

The ACD application provides call centers with the ability to determine how calls are best routed to their ACD Agents. ACD call centers may be Telemarketing, Customer Service, Technical Support, or any other group that handles large call volume. With the ACD application, calls may be directed in a variety of ways to ensure that calls are handled quickly and efficiently.

Attendant Console

The CIX Attendant Console is designed to handle all call activity within a single Call Monitor Screen. All calls will appear in a single list. Calls are marked with icons to show the current status. Features such as Paging, Call Pickup, Call Park offer many alternatives. The Administration window enables which option is the primary operation for that Attendant. For example, if two zones are used for paging, as well as the All Call, then an option pull down arrow is next to the icon. Clicking the icon starts the All Call Page, then the Attendant can select one of two page zones.

DSS (Direct Station Selection) / BLF (Busy Lamp Field)

[DSS] buttons can be placed on Toshiba IP telephones, add-on modules and DSS consoles.

When placed on one of these devices, these buttons serve two functions: DSS: to make direct calls or transfer calls to other stations; and BLF: to display the status of other stations and [PDNs].

Server Applications

SMDI

SMDI is an industry standard method of integrating a telephone system with voice mail or other peripheral systems. IPedge include the messaging Messaging application which provides voicemail.

SMDR

Station Message Detail Reporting send details of the call, including the originating station or trunk, the start time of the call, its duration, authorization codes, to an accounting package. If a station user dials “911,” the IPedge will also generate a record at the beginning of the call as part of its internal notification that an emergency call is in progress.

Traffic Measurement

Technicians and System Administrators can monitor the effectiveness of the system resources for proper traffic balance.These traffic statistics are necessary for the system administrator to both monitor the effectiveness of the system and determine whether the system has enough resources or improper traffic balance