Chapter 47

UPnP

Introduction

UPnP is an architecture that allows devices to automatically discover, negotiate, and request services. This implementation supports the Internet Gateway Device (IGD) Standard which allows UPnP compliant peer-to-peer applications (and host devices) to dynamically negotiate connectivity through firewall or NAT enabled gateway devices.

When UPnP is enabled, the router acts as an Internet Gateway Device (IGD). The IGD manages UPnP sessions between the private LAN and the public WAN over a firewall policy. The firewall policy can have one or more LAN interfaces and only one WAN interface. Because peers on the public side cannot initiate sessions or connections across the firewall by default, *control points* on the private side can create port maps for these sessions.

To use UPnP, the firewall must be available on your router.

For more information about this implementation of UPnP, see the How To Note "*Configuring the AR450S as a UPnP Internet Gateway Device with a Windows® XP® Machine as a UPnP Control Point*", which can be found at www.alliedtelesis.co.uk/en-gb/solutions/techdocs.asp?area=howto.

Important information about UPnP

Although every effort has been made to comply with the *Internet Gateway Device:1 Device Template Version 1.01 Standardized DCP,* this implementation has not been certified by the UPnP Implementers Corporation.

This implementation of UPnP supports only one firewall policy and one WAN interface. The device can have only one UPnP enabled firewall policy, and only one UPnP aware WAN interface within that policy.

When the *RequestConnection* action in the *WANPPPConnection* service attempts to bring up a PPP connection, the action does not return an error if the connection fails. The PPP connection appears to be successful. The most likely way that this action is invoked is by double-clicking on the Internet Connection icon in the Network Connections window. You can see if the PPP connection has failed because the Internet Connection icon does not appear in the system tray. If this happens, check that all connections to the network are intact.

Overview of UPnP

This section contains overviews of the following topics:

- UPnP Architecture
- UPnP Networking Phases
- UPnP and the Firewall

The information in this chapter is intended to provide a context for this implementation of UPnP. For details about the UPnP architecture, see the UPnP Forum web site at *www.upnp.org*.

UPnP Architecture

The UPnP architecture consists of several separate entities and stages. The interaction between these entities, and the stages they go through make UPnP sessions possible. The entities include *devices*, *services*, and *control points*. Devices advertise their services, and control points gather and distribute information about services.

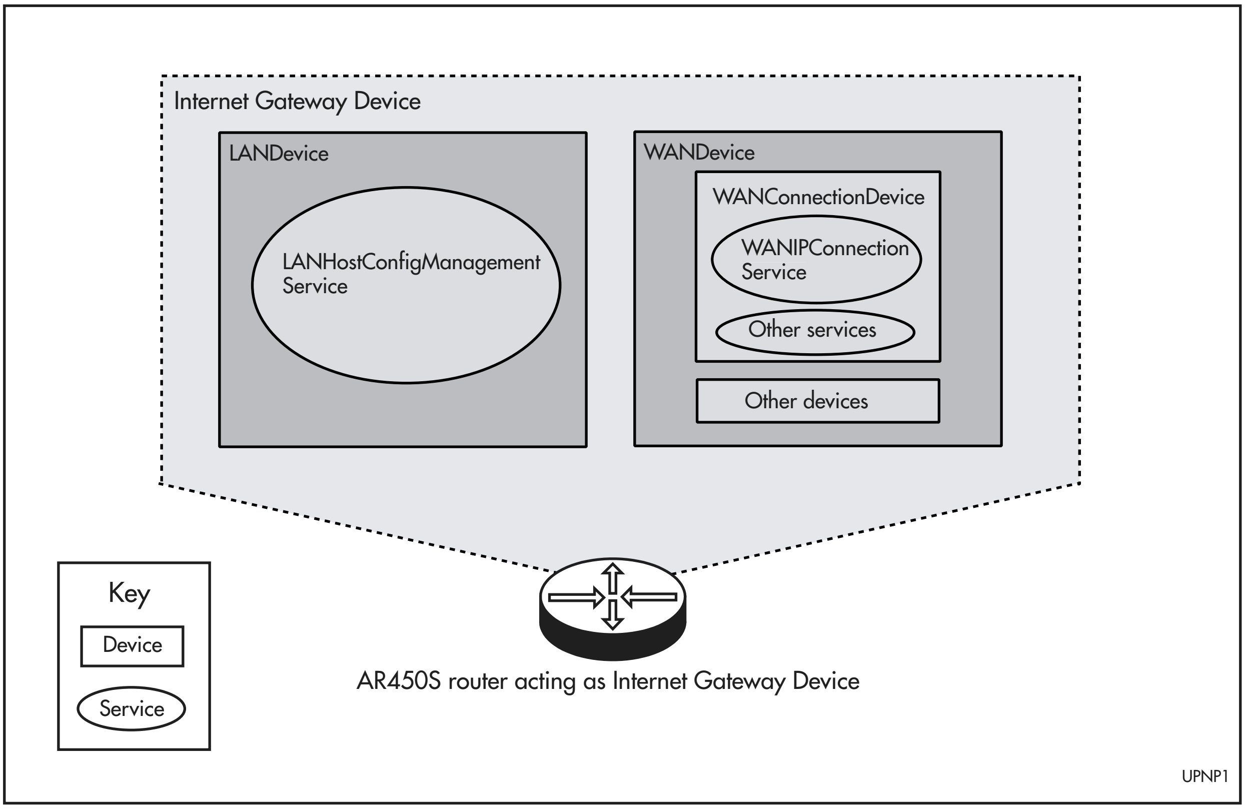
Devices

A *device* is a container for services and other nested devices. The router is the *RootDevice* for UPnP, known as the Internet Gateway Device (IGD). Within the IGD are other nested virtual devices, or sub-devices. For example, within the *RootDevice* are nested devices *WANDevice* and *LANDevice*, each of which are created when a WAN and LAN interface are added for UPnP. Within the *WANDevice* is the nested device *WANConnectionDevice* that contains the services needed to initiate a session over the WAN interface.

A UPnP enabled device may obtain an IP address, advertise its capabilities, learn about other connected UPnP devices and then communicate directly with those devices. The same device can terminate its connection cleanly when it leaves the UPnP community.

Device and service architecture is illustrated in Figure 47-1 on page 47-4. For details, see *Internet Gateway Device:1 Device Template Version 1.01 Standardized DCP*.

Figure 47-1: UPnP Internet Gateway Device architecture.



Services

Devices provide one or more *services* that other devices can invoke. Services advertise their actions to other devices on the network. An example of a service is the *WANCommonInterfaceConfig* service. This deals with the physical properties of the WAN interface on the IGD. This service contains actions such as *GetCommonLinkProperties.* This action contains variables such as *PhysicalLinkStatus* which has a status of **up** or **down**.

For security reasons, only clients on the LAN can request services from the IGD.

Control points

A control point can discover and control other devices. Control points do this by staying informed about devices on the network via messages it receives from devices. The messages describe the services on offer, and inform the control point about changes in the state of a service on a device. The control point knows about the actions available on a device because of the information delivered in these messages, and it can invoke actions. A control point may be embedded in a device, but is usually a PC such as a Windows® XP® machine.

State variables

Variables model the state of a service at run time. A variable represents key aspects of the service, such as the number of port maps.

UPnP Networking Phases

This section describes the phases and stages of communication that the UPnP use.

Addressing

Devices and control points search for a DHCP server to get an IP address. If no DHCP server is available, automatic IP addressing (Auto IP) is used to obtain an address.

Discovery

Devices advertise their services to control points on the network when they are added to the network. Discovery messages are exchanged with the Simple Service Discovery Protocol (SSDP). The messages have basic information about the device and its services, and a URL for device description.

When the router is enabled as the IGD, control points on the LAN know about its existence. On a Windows XP machine, an icon appears in My Network Places and Network Connections to show that the IGD is present.

Description

Control points retrieve descriptions of devices and their encapsulated services and actions from the URL provided in discovery messages. The description has more detail about the device capabilities than the discovery message. The description is expressed in XML syntax.

Control

Control points use the information supplied during the *description* phase to invoke actions on services using the Simple Object Access Protocol (SOAP).

Eventing

Services send event messages when the value of an evented variable for a particular action changes state. Control points interested in a particular service on a device can subscribe to the notification list for that service. Changes to the values of any evented state variables for that service are published to all control points on the service’s notification list. Event messages contain the name of one or more state variables and their current values. Event messages are expressed in XML syntax and are formatted with the General Event Notification Protocol (GENA).

Presentation

Control points can display a user interface provided by the device. A device may offer its URL as part of the description message. This URL can be presented via the client’s web browser. The client may be able to view the status of the device or manage it, depending on the capabilities of the device.

With this implementation of UPnP, you can access the router’s GUI and manage the device from the control point. Clicking the IGD icon in My Network Places brings up an authorisation dialogue box. If you know the username and password for the router, and have entered these details, a window opens with the home page for the GUI. You can then configure the router and its UPnP settings.

UPnP and the Firewall

This section describes how the firewall uses NAT, the problems that this creates for UPnP, and how NAT traversal overcomes these problems.

Firewall and Network Address Translation (NAT)

A firewall is a security device that protects the internal network by preventing unsolicited access from the outside. Due to the scarcity of the IPv4 address, Network Address Translation (NAT) allows multiple computers or devices on a private network to share a single, globally routable IPv4 address.

Firewall and NAT benefits internal or private networks, but they also cause problems for applications that need a public IP address and unique port number for each session where the session is initiated by an external client.

For example, instant messaging applications such as Windows Messenger use the Session Initiation Protocol (SIP) for setting up a voice or video session with a remote peer. The Windows Messenger client in the internal network embeds its private address and dynamic port information in the SIP message it sends to the remote peer. The address and port information embedded in the SIP message are not subjected to NAT so the remote peer cannot contact the internal client.

Internet Gateway Device and NAT Traversal

The UPnP IGD addresses the issues caused by the firewall and NAT by providing support for NAT Traversal. The control point can detect and control the IGD using UPnP protocols. A UPnP enabled client application (such as Windows Messenger) can determine if a firewall and/or a NAT device is present. If so, the application learns the translated IP address and configures port mappings in the IGD.

For example, Windows Messenger in Windows XP (a control point) uses NAT Traversal to discover whether it is behind a NAT device. If so, it can retrieve the translated address and configure port mappings for the IGD. Messenger uses this information in the Session Initiation Protocol (SIP) message that is sent when setting up a voice or video session with a remote peer. The real-time communication session is established using the valid addressing details.

UPnP on the router

This section describes how to configure the router as an Internet Gateway Device (IGD). The UPnP implementation is closely related to the firewall. You must configure a firewall policy for UPnP. Several of the commands needed to configure UPnP are firewall commands. For details on the firewall, see Chapter 46, Firewall.

Enable the firewall on the router

If the firewall is not already enabled, enable it with the command:

```
enable firewall
```

Create a firewall policy for UPnP

UPnP needs a dedicated firewall policy that accepts UPnP sessions. Only one policy can be configured for UPnP. UPnP sessions originating from the WAN need to pass through the firewall because traffic from the WAN to the LAN is blocked by default. A control point on the LAN can create a port map on the policy using UPnP. The port map becomes a 'hole' though which WAN to LAN sessions are possible.

To create a firewall policy for UPnP called "upnp", use the command:

```
create firewall policy=upnp
```

Enable UPnP on the firewall policy

Once a firewall policy for UPnP has been created, this policy must be configured to accept UPnP sessions.

To enable UPnP on the firewall policy called "upnp", use the command:

```
set firewall policy=upnp upnp=enabled
```

Add interfaces for UPnP to the policy

The firewall policy can not create UPnP sessions until at least one LAN and a WAN interface have been added. You can add up to 64 LAN interfaces on the policy for UPnP, but only one WAN interface.

The WAN interface for UPnP must be configured as the default route. Use the ADD IP ROUTE command to configure a default static route. For example, to create a default route that points to a router at the remote end of a PPP link attached to interface ppp0, with the IP address 172.16.8.82, use the command:

```
add ip route=0.0.0.0 interface=ppp0 nexthop=172.16.8.82
   metric=1
```

For the InternalClient state variable in the AddPortMapping action to succeed, a UPnP interface must have been enabled for directed broadcast with the **add ip interface directedbroadcast=on** command.

To make vlan1 the private LAN interface for UPnP, use the command:

```
add firewall policy=upnp interface=vlan1 type=private
   upnptype=lan
```

To make eth0 the public WAN interface for UPnP, use the command:

```
add firewall policy=upnp interface=eth0 type=public
   upnptype=wan
```

Enable UPnP

Once UPnP is enabled, the router becomes an IGD and sends *discovery* messages to control points on the network. To enable UPnP, use the command:

```
enable upnp
```

Additional security configuration

It is possible to optionally configure advanced security features for UPnP. These features are not essential when configuring the router as an IGD, but they give you more control over port mappings and actions.

Disable certain ports for UPnP

You can enter the number of a port or ranges of ports that are to be unavailable to UPnP for port maps. This prevents the creation of a port map on the WAN side that coincides with a defined IETF standard service. For example, to make the Telnet and FTP port numbers unavailable to UPnP, use the command:

```
disable upnp l4port=23,25
```

These disabled ports can be re-enabled using the command:

```
enable upnp l4port=23,25
```

All ports are available to UPnP for port mappings by default.

Disable specific actions

You can disable a specific action on an interface's connection service instance. All actions are enabled by default. To execute the command you must retrieve details about the action name, and its enclosing interface instance from the output of the **show upnp** and the **show upnp interface=*interface*** commands respectively.

Use this command with caution. Do not disable an action unless you are aware of its consequences for UPnP networking.

For example, to disable the UPnP action *ForceTermination* on the firewall policy called "upnp" for the service instance identified by the interface eth0-1, use the command:

```
disable upnp fwpolicy=upnp interface=eth0-1
   action=forcetermination
```

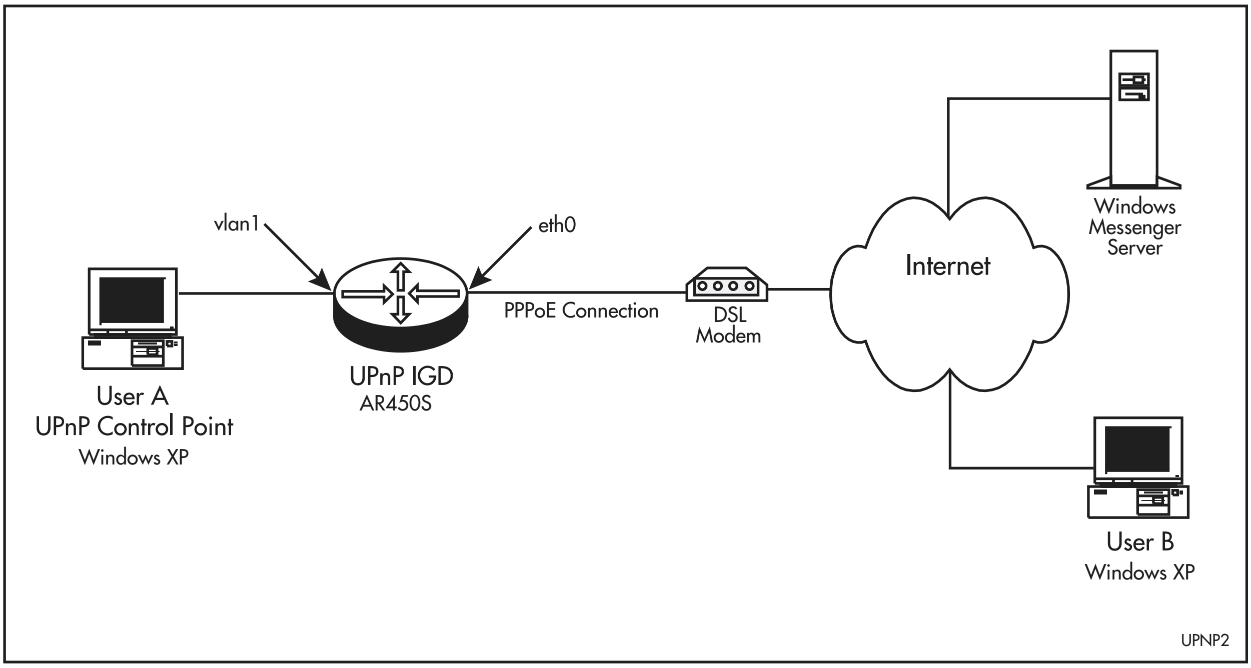
This action can be re-enabled using the command:

```
enable upnp fwpolicy=upnp interface=eth0-1
   action=forcetermination
```

Configuration Example

The following example illustrates the steps required to configure the router as an Internet Gateway Device using a PPPoE connection to the Internet, as illustrated in Figure 47-2 on page 47-9. In this example, User A can communicate with User B using Windows Messenger.

Figure 47-2: AR450S acting as UPnP IGD.



Configure PPP and IP interfaces and routes

1. **Set the system name for the router**

   Before configuring interfaces, assign the router a name. To give the router the name “AR450”, use the command:

```
set system name=ar450
```

2. **Create the PPP interface**

   To create a PPP interface over the physical interface eth0, with IP requests turned on, use the command:

```
create ppp=0 over=eth0-any iprequest=on
```

3. **Enable IP and IP options**

   To enable IP, use the command:

```
enable ip
```

   To enable the remote assignment of IP addresses for unnumbered IP addresses, use the command:

```
enable ip remoteassign
```

   To enable the router’s DNS relay agent, use the command:

```
enable ip dnsrelay
```

4. Add interfaces to IP

Add the previously created PPP interface to IP. This will be the WAN interface for UPnP. To assign the interface ppp0 the IP address 0.0.0.0, use the command:

```
add ip interface=ppp0 ip=0.0.0.0 mask=0.0.0.0
```

Add an interface to IP that will be the LAN interface for UPnP. To add vlan1 to IP with the IP address 192.168.1.1, use the command:

```
add ip interface=vlan1 ip=192.168.1.1
```

5. Add a static route for the WAN interface

Add a static route for the previously configured WAN IP interface. For UPnP sessions to succeed, this must be the default route. To make ppp0 the default route, use the command:

```
add ip route=0.0.0.0 mask=0.0.0.0 interface=ppp0
   next=0.0.0.0
```

Configure UPnP and its firewall policy

1. Enable UPnP

You must enable UPnP before you can create a firewall policy for UPnP. UPnP sessions can not commence until a firewall policy and interfaces are configured for UPnP. This is done in steps 2 to 5.

```
enable upnp
```

2. Configure a firewall policy for UPnP

To enable the firewall use the command:

```
enable firewall
```

Create a firewall policy specifically for UPnP. You can have only one policy for UPnP. Use a name for the policy that clearly shows its purpose. To create a policy for UPnP called “UPnP1”, use the command:

```
create firewall policy=upnp1
```

3. Enable UPnP on the firewall policy

Set UPnP as enabled on the newly created firewall policy for UPnP. To enable UPnP on the policy called “UPnP1”, use the command:

```
set firewall policy=upnp1 upnp=enabled
```

4. Add the LAN and WAN interface for UPnP to the firewall policy

Add at least one LAN interface to UPnP’s firewall policy. To make the previously configured vlan1 interface the LAN interface for the “UPnP1” policy, use the command:

```
add firewall policy=upnp1 interface=vlan1 type=private
   upnptype=lan
```

Add a WAN interface to UPnP’s firewall policy. You can only add one WAN interface to the policy for UPnP. To make the previously configured ppp0 interface the WAN interface for the “UPnP1” policy, use the command:

```
add firewall policy=upnp1 interface=ppp0 type=public
   upnptype=wan
```

5. Configure NAT on UPnP's interfaces

For UPnP sessions to succeed, you must configure enhanced NAT on the firewall policy for UPnP. The enable enhanced NAT on the policy called "UPnP1" for the LAN interface vlan1 and the WAN interface ppp0, use the command:

```
add firewall policy=upnp1 nat=enhanced interface=vlan1
   gblinterface=ppp0
```

Command Reference

This section describes the commands available on the router to enable, configure, control, and monitor UPnP. Several commands in this section are firewall commands that have been modified to support UPnP. New parameters in existing commands are in bold type. For details about firewall commands, see Chapter 46, Firewall. UPnP and the firewall require IP to be enabled and configured correctly. See Chapter 22, Internet Protocol (IP) for the commands required to enable and configure IP.

See "Conventions" on page lxv of About this Software Reference in the Software Reference for details of the conventions used to describe command syntax. See *Appendix A, Messages* in the Software Reference for a complete list of messages and their meanings.

disable upnp

Syntax

```
DISable UPNP
```

Description This command disables UPnP. UPnP is disabled by default. When this command is executed, the following occurs:

- A warning message is generated at the CLI,
- An event notification message is sent to control points on the LAN, and
- A log message is added to the router's logs.

Example To disable UPnP, use the command:

```
dis upnp
```

See Also **enable upnp**

disable upnp action

Syntax

```
DISable UPNP FWPolicy=name INTerface=interface
   ACtion=action-name
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are uppercase and lowercase letters, digits, and the underscore.
- *interface* is the interface that corresponds to a UPnP device instance.
- *action-name* is the name of a specific action.

Description

This command disables a UPnP action on the UPnP connection service of a specific interface. The service and action are identified by the interface name of the enclosing UPnP device instance. This allows you to prevent a control point from carrying out the specified action on an interface. For example, this command could prevent a control point on the LAN from deactivating or activating a PPP link on the WAN interface. All supported UPnP actions are enabled by default.

Use this command with caution. Do not disable an action unless you are aware of its consequences for UPnP networking.

The **fwpolicy** parameter is the name of the UPnP firewall policy.

The **interface** parameter is the interface that corresponds to a UPnP device instance. A UPnP service instance is identified by its enclosing device's interface name. You can see this name in the output of the **show upnp** command.

The **action** parameter is the name of a specific action. You can see this name in the output of the **show upnp interface=*interface*** command when you specify an interface.

Examples

To disable the UPnP action *ForceTermination* on the service instance identified by the interface eth0-1, use the command:

```
dis upnp fwp=upnp int=eth0-1 ac=forcetermination
```

See Also

disable upnp l4port
enable upnp action
enable upnp l4port
show upnp
show upnp interface

disable upnp l4port

Syntax

```
DISable UPNP L4PORT={0-65535}
```

Description This command disables the specified Layer 4 port or ports for UPnP. A UPnP *control point* can request a NAT mapping on the WAN side that coincides with a defined IETF standard service. By disabling certain ports, a client is not able to ask for mappings on the WAN side that correspond to the disabled ports. Without using spaces, enter numbers separated by commas, or use a hyphen to indicate a range of numbers. All ports are enabled by default.

Examples To set port 25 as disabled for UPnP, use the command:

```
dis upnp l4port=25
```

To set the TCP ports 0-1023 as disabled for UPnP, use the command:

```
dis upnp l4port=0-1023
```

See Also **disable upnp action**
enable upnp action
enable upnp l4port

enable upnp

Syntax

```
ENAble UPNP
```

Description This command enables UPnP. UPnP is disabled by default. When this command is executed, the following occurs:

- A warning message is generated at the CLI,
- An event notification message is sent to control points on the LAN, and
- A log message is added to the router’s logs.

UPnP sessions can not start until a firewall policy for UPnP has been created, a WAN and LAN interface added to the policy, and the policy is enabled for UPnP.

Example To enable UPnP, use the command:

```
ena upnp
```

See Also **disable upnp**

enable upnp action

Syntax

```
ENAble UPNP FWPolicy=name INTerface=interface
   ACtion=action-name
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are uppercase and lowercase letters, digits (0-9), and the underscore character ("_").
- *interface* is the interface that corresponds to a UPnP device instance.
- *action-name* is the name of a specific action.

Description

This command enables a UPnP action on the UPnP connection service of a specific interface. The service and action are identified by the interface name of the enclosing UPnP device instance. Use this command only if an action has previously been disabled with the **disable upnp action** command. All supported UPnP actions are enabled by default.

The **fwpolicy** parameter is the name of the UPnP firewall policy.

The **interface** parameter is the interface that corresponds to a UPnP device instance. A UPnP service instance is identified by its enclosing device's interface name. You can see this name in the output of the **show upnp** command.

The **action** parameter is the name of a specific action. You can see this name in the output of the **show upnp interface=*interface*** command when you specify an interface.

Examples

To enable the UPnP action *ForceTermination* on the service instance identified by the interface eth0-1, use the command:

```
ena upnp fwp=upnp int=eth0-1 ac=forcetermination
```

See Also

disable upnp action
disable upnp l4port
enable upnp l4port
show upnp
show upnp interface

enable upnp l4port

Syntax

```
ENAble UPNP L4PORT={0-65535}
```

Description

This command enables the specified Layer 4 port or ports for UPnP. This command only needs to be used if a port or ports has previously been disabled with the **disable upnp l4port** command. All ports are enabled by default.

Examples

To set port 25 as enabled for UPnP, use the command:

```
enable upnp l4port=25
```

To set the well known TCP ports 0-1023 as enabled for UPnP, use the command:

```
ena upnp l4port=0-1023
```

See Also

disable upnp action
enable upnp action
disable upnp l4port

show upnp

Syntax `SHow UPNP`

Description This command displays information about UPnP (Figure 47-3, Table 47-1).

Figure 47-3: Example output from the **show upnp** command

```
UPNP
-------------------------------------------------------------------------
Status:                                 Enabled
Time to next advertisement:             575
Disabled TCP/UDP ports for UPnP:        none
-------------------------------------------------------------------------
Services and Devices:
Device                    Service                      Interface
-------------------------------------------------------------------------
InternetGatewayDevice     Layer3Forwarding             igd-0
  WANDevice               WANCommonInterfaceConfig     eth0
    WANConnectionDevice   WANIPConnection              eth0-0
  LANDevice                                            vlan1-0
-------------------------------------------------------------------------
```

Table 47-1: Parameters in the output of the **show upnp** command

Parameter	Meaning
Status	Whether UPnP is Enabled or Disabled.
Time to next advertisement	The amount of time, in seconds, until the next time devices and services are advertised.
Disabled TCP/UDP ports for UPnP	The numbers for the TCP and/or UDP ports that are disabled for use by UPnP.
Device	The devices that are available for use by UPnP.
Service	The service instances that currently exist for the device.
Interface	The physical or logical interface associated with this service and device. Where “igd” is displayed, this represents the Internet Gateway Device.

Example To view information about UPnP, use the command:

```
sh upnp
```

See Also **show upnp interface subscriptions**

show upnp counter

Syntax `SHow UPNP COUnter`

Description This command displays the counters for UPnP (Figure 47-4 and Table 47-2).

Figure 47-4: Example output from the **show upnp counter** command

```
UPnP Counters
------------------------------------------------------------------------------

UDP
  inDatagrams ..................... 6       outDatagrams .................... 5
  inMcastDatagrams ................ 4       outMcastDatagrams .............. 10
  inUcastDatagrams ................ 2       outUcastDatagrams ............... 5
  inDatagramsDropped .............. 0

HTTP
  httpReqs ...................... 176       httpResps ..................... 176
  httpReqsRefused ................. 2       httpRespsFailed ................. 0

Discovery
  mSearchReqs ..................... 6       mSearchResps .................... 5
  mSearchReqsErrors ............... 0       notifyAliveMsgs ................ 10
                                            notifyByebyeMsgs ................ 0

Description
  descReqs ........................ 1       descResps ....................... 1
  deviceDescReqs .................. 1       deviceDescResps ................. 1
  serviceDescReqs ................. 0       serviceDescResps ................ 0
  descErrors ...................... 0

Control
  actionReqs .................... 171       actionResps ................... 171
  actionErrors .................... 2

Eventing
  subscrReqs ...................... 3       subscrResps ..................... 4
  newSubscrReqs ................... 3       eventsNotified .................. 4
  renewSubscrReqs ................. 0
  cancelSubscrReqs ................ 1
  subscrErrors .................... 0
------------------------------------------------------------------------------
```

Table 47-2: Parameters in the output of the **show upnp counter** command

Parameter	Meaning
UDP	**UPnP counters for UDP**
inDatagrams	The total number of UDP datagrams received.
inMcastDatagrams	The number of multicast UDP datagrams received.
inUcastDatagrams	The number of unicast UDP datagrams received.
inDatagramsDropped	The number of UDP datagrams dropped at Layer 4.
outDatagrams	The total number of UDP datagrams sent.
outMcastDatagrams	The number of UDP multicast datagrams sent.
outUcastDatagrams	The number of UDP unicast datagrams sent.

Table 47-2: Parameters in the output of the **show upnp counter** command (Continued)

HTTP	**UPnP counters for HTTP**
httpReqs	The number of HTTP requests received.
httpReqsRefused	The number of HTTP requests refused.
httpResps	The number of HTTP requests sent.
httpRespsFailed	The number of response connection errors.
Discovery	**Counters for the Discovery phase of UPnP networking**
mSearchReqs	The number of M-Search requests received.
mSearchReqsErrors	The number of M-Search requests received that contained errors.
mSearchResps	The number of M-Search responses sent.
notifyAliveMsgs	The number of notify *alive* messages sent.
notifyByeByeMsgs	The number of notify *byebye* messages sent.
Description	**Counters for the Description phase of UPnP networking.**
descReqs	The total number of Description requests.
deviceDescReqs	The number of requests for device descriptions.
serviceDescReqs	The number of requests for service descriptions.
descErrors	The number of description requests received that contained errors.
descResps	The number of description responses sent.
deviceDescResps	The number of device descriptions sent.
serviceDescResps	The number of service descriptions sent.
Control	**Counters for the Control phase of UPnP networking.**
actionReqs	The total number of action requests received.
actionErrors	The number of action requests received that contained errors.
actionResps	The number of action responses sent.
Eventing	**Counters for the Eventing phase of UPnP networking.**
subscrReqs	The total number of subscription requests received.
newSubscrReqs	The number of new subscription requests received.
subscrResps	The total number of subscription responses sent.
subscrErrors	The number of subscription requests that contained errors.
eventsNotified	The total number of event notifications.

Examples To display information about UPnP counters, use the command:

```
sh upnp cou
```

See Also

disable upnp
enable upnp
show upnp
show upnp interface
show upnp interface subscriptions

show upnp interface

Syntax `SHow UPNP FWPolicy=name INTerface=[{ALL|interface}]`

where:

- *interface* is the interface that corresponds to a UPnP device instance. A UPnP service instance is identified by its enclosing device's interface name.
- *name* is the name of the firewall policy for UPnP. *name* is a character string, 1 to 15 characters in length. Valid characters are uppercase and lowercase letters, digits, and the underscore.

Description This command displays information about the interfaces being used by UPnP, or a specific interface used by UPnP.

The **fwpolicy** parameter is the name of the firewall policy used by UPnP.

The **interface** parameter identifies the device and service instance for which information is displayed. You can see this name in the output of the **show upnp** command. If **all** is specified, all of the interfaces currently used by UPnP are displayed (Figure 47-5, Table 47-3 on page 47-21). If an interface name or service instance (such as "igd-0") is specified, more detailed information on that interface is displayed (Figure 47-6 on page 47-21, Table 47-3 on page 47-21). The default is **all**.

Figure 47-5: Example output from the **show upnp interface=all** command

```
UPNP Interfaces
-----------------------------------------------------
Firewall Policy:          net
-----------------------------------------------------
Interface:                vlan1-0
UPnP Device:              LANDevice:1
UPnP Service:             n/a
Subscriptions:            n/a
Subscriber Notifications: n/a

Interface:                eth0-0
UPnP Device:              WANConnectionDevice:1
UPnP Service:             WANIPConnection:1
Subscriptions:            0
Subscriber Notifications: 0

Interface:                eth0
UPnP Device:              WANDevice:1
UPnP Service:             WANCommonInterfaceConfig:1
Subscriptions:            0
Subscriber Notifications: 0

Interface:                igd-0
UPnP Device:              InternetGatewayDevice:1
UPnP Service:             Layer3Forwarding:1
Subscriptions:            0
Subscriber Notifications: 0
----------------------------------------------------
```

Figure 47-6: Example output from the **show upnp interface=*interface*** command

```
UPNP Interfaces
-------------------------------------------------------------------------
Firewall Policy:          net
-------------------------------------------------------------------------
Interface:                eth0
UPnP Device:              WANDevice:1
UPnP Service:             WANCommonInterfaceConfig:1
Subscriptions:            0
Subscriber Notifications: 0

-------------------------------------------------------------------------
Actions:                             Invoked:      Action Status
  GetCommonLinkProperties            0             Enabled
  GetTotalBytesSent                  0             Enabled
  GetTotalBytesReceived              0             Enabled
  GetTotalPacketsSent                0             Enabled
  GetTotalPacketsReceived            0             Enabled

Evented State Variables:
  PhysicalLinkStatus                 Down

Non-evented State Variables:
  WANAccessType                      Ethernet
  Layer1UpstreamMaxBitRate           10000000
  Layer1DownstreamMaxBitRate         10000000
  MaximumActiveConnections           1
  TotalBytesSent                     0
  TotalBytesReceived                 0
  TotalPacketsSent                   0
  TotalPacketsReceived               0
-------------------------------------------------------------------------
```

Table 47-3: Parameters in the output of the **show upnp interface** command

Parameter	Meaning
Firewall policy	The firewall policy name used by UPnP.
Interface	The physical or logical interface about which device and service information is displayed.
UPnP Device	The UPnP device name.
UPnP Service	The UPnP service name.
Subscriptions	The number of control points that have subscribed to this service instance.
Subscriber Notifications	The number of subscriber notifications sent.
Actions	Actions provided by this service.
Invoked	The number of times the action has been invoked.
Action Status	The number of times the action has been invoked.
Evented State Variables	The state variables provided by this service that are evented. When the variable changes state, an event message is sent.
Non-evented State variables	The state variables provided by this service that are not evented. If the variable changes state, an event message is not sent by the enclosing device.
Value	The state variable’s value.

Examples To display information about the *WANIPConnection* service that has a *service-id* of 6, use the command:

```
sh upnp fwp=wanipconnection int=6
```

See Also

disable upnp
enable upnp
show upnp
show upnp counter
show upnp interface subscriptions

show upnp interface subscriptions

Syntax

```
SHow UPNP FWPolicy=name INTerface={ALL|interface}
   SUBScriptions
```

where:

- *name* is the name of the firewall policy for UPnP. *name* is a character string, 1 to 15 characters in length. Valid characters are uppercase and lowercase letters, digits, and the underscore.
- *interface* is the interface that corresponds to a UPnP device instance. A UPnP service instance is identified by its enclosing device's interface name. You can see this name in the output of the **show upnp** command.

Description

This command displays detailed information about the current service subscriptions on the firewall policy for UPnP. There may be none or multiple subscriptions to a service instance.

The **interface** parameter identifies the service instance for which information is displayed. If **all** is specified, information about all of the interfaces currently used by UPnP are displayed (Figure 47-7, Table 47-4 on page 47-24). If an interface name is specified, information about it and its services is displayed (Figure 47-8 on page 47-24, Table 47-4 on page 47-24).

Figure 47-7: Example output from the **show upnp interface=all subscriptions** command

```
UPNP Subscriptions
-------------------------------------------------------------------------
Firewall Policy:      net
-------------------------------------------------------------------------
Interface:            vlan1-0
UPnP Service:         None
There are no subscriptions.
-------------------------------------------------------------------------
Interface:            eth0-0
UPnP Service:         WANIPConnection:1

Delivery URL:         http://192.168.0.16:5000/notify
Subscriber IP/Port:   192.168.0.16:5000
SID:                  uuid:e3638fe2-aa7c-4034-eac8-deef22fed51d
Time to Live:         1722 Seconds
Sequence Number:      3
-------------------------------------------------------------------------
Interface:            eth0
UPnP Service:         WANCommonInterfaceConfig:1

Delivery URL:         http://192.168.0.16:5000/notify
Subscriber IP/Port:   192.168.0.16:5000
SID:                  uuid:c9239093-dc79-4077-a835-156bc242ffdb
Time to Live:         1722 Seconds
Sequence Number:      2
-------------------------------------------------------------------------
Interface:            igd-0
UPnP Service:         Layer3Forwarding:1
There are no subscriptions.
-------------------------------------------------------------------------
```

Figure 47-8: Example output from the **show upnp interface=*interface* subscriptions** command

```
UPNP Subscriptions
-------------------------------------------------------------------------
Firewall Policy:      net
-------------------------------------------------------------------------
Interface:            eth0-0
UPnP Service:         WANIPConnection:1

Delivery URL:         http://192.168.0.16:5000/notify
Subscriber IP/Port:   192.168.0.16:5000
SID:                  uuid:e3638fe2-aa7c-4034-eac8-deef22fed51d
Time to Live:         1707 Seconds
Sequence Number:      3
-------------------------------------------------------------------------
```

Table 47-4: Parameters in the output of the **show upnp interface subscriptions** command

Parameter	Meaning
Interface	The physical or logical interface about which subscription information is displayed
UPnP Service	The UPnP service name.
Service Status	The status of the service instance; one of Enabled of Disabled.
Delivery URL	The URL to receive event messages.
Subscriber IP/Port	The subscriber's IP address and port in IP address:port format.
SID	The unique subscription identifier.
Time to Live	The amount of time, in seconds, until the subscription expires.
Sequence Number	The sequence number of the last notification message sent for this subscription.

Examples To display subscription information about the WANIPConnection service that has an identifying interface of eth0-1, use the command:

```
sh upnp int=eth0-1 subs
```

See Also disable upnp

enable upnp

show upnp

show upnp counter

show upnp interface