Target Identifier Address Resolution Protocol

Some appications running on SONET devices identify these devices by a Target Identifier (TID). Therefore, it is necessary for the router to cache TID-to-network address mappings. As these devices usually run over OSI, the network addresses involved in the mapping are OSI Network Service Access Points (NSAP).

When a device sends a packet to another device, the device needs a way to request this information directly from the device, or from an intermediate device in the network. This functionality is provided by an address resolution protocol called TID Address Resolution Protocol (TARP).

Service providers need a dynamic method to map TIDS to NSAPs, and TARP serves this purpose. TARP runs over the Connectionless Network Protocol (CLNP) as a router must support CLN Service Routing to support TARP.

Prerequisites for TARP Support

If the router is configured as an IS, the router must be running IS-IS.

If the router is configured as an ED, then the router must be running ES-IS.

Restrictions and Limitations

- The commands “tarp allow caching” and “no tarp allow caching” may result in tarp resolution failures.
- Configuring multiple NSAP addresses are not supported.
- Avoid multiple configuring or changing tid and NSAP.

Types of TARP PDU's

- Type 1—Sent when a device has a TID for which it has no matching NSAP. Type 1 PDUs are sent to all Level 1 (IS-IS and ES-IS) neighbors. If no response is received within the specified time limit, a Type 2 PDU is sent. To prevent packet looping, a loop detection buffer is maintained on the router. A Type 1 PDU is sent when you use the **tarp resolve** command.

  A Type 1 PDU is sent when a device has a TID for which it has no matching NET information and is sent to all L1 neighbors. When a device receives a Type 1 PDU, it checks if the PDU matches the target TID of the device. When they match, a type 3 PDU is created and unicasted directly to the sender of the TARP PDU. In addition, if the update remote cache is set in the incoming PDU, the receiver updates (or creates) the cache entry for the originator. If the target TID does not match, the device propagates this PDU to all its L1 neighbors (except the originator of this PDU). If no response is received within the timeout period (15 seconds), a Type 2 PDU is originated.

  To prevent packet looping, a Loop Detection Buffer (LDB) is maintained. This consists of system ID - sequence number mappings. A packet is discarded if its sequence number is less than or equal to that found in the LDB for this system ID. If no entry is present, the LDB is updated, and the packet is processed. A sequence number of zero is treated specially, and will cause the entry in the cache to be superseded.

- Type 2—Sent when a device has a TID for which it has no matching NSAP and no response was received from a Type 1 PDU. Type 2 PDUs are sent to all Level 1 and Level 2 neighbors. A time limit for Type 2 PDUs can also be specified. A Type 2 PDU is sent when you use the **tarp resolve** command and specify the option 2.

  A Type 2 PDU is same as a Type 1, except that this PDU is sent to all (L1 and L2) neighbors. The default timeout is 25 seconds.

- Type 3—Sent as a response to a Type 1, Type 2, or Type 5 PDU. Type 3 PDUs are sent directly to the originator of the request.

- Type 4—Sent as a notification when a change occurs locally (for example, a TID or NSAP change). A Type 4 PDU usually occurs when a device is powered up or brought online.

- Type 5—Sent when a device needs a TID that corresponds to a specific NSAP. Unlike Type 1 and Type 2 PDUs that are sent to all Level 1 and Level 2 neighbors, a Type 5 PDU is sent only to a particular router. In addition to the type, TARP PDUs contain the sender NSAP, the sender TID, and the target TID (if the PDU is a Type 1 or Type 2). A Type 5 PDU is sent when you use the **tarp query** command.

TARP Features

The following are the features of TARP:

TARP Caching

TID - Network addresses mappings are stored in a cache, implemented as a hash table. A cache entry can be created dynamically when a router hears from another TARP device (e.g. as a result of a query addressed to the router), or statically via TARP "map" commands. All dynamically created TARP cache entries (i.e. those that are not static or flagged as "LOCAL") are aged out. The time out value is configurable.

TARP Timers

Configure the amount of time that the router waits to receive a response from a Type 1 PDU, a Type 2 PDU, and a Type 5 PDU and also configure the lifetime of the PDU based on the number of hops.

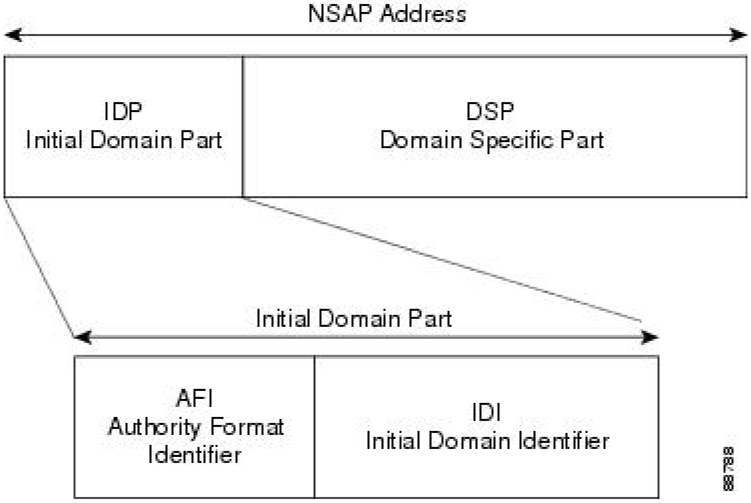
Set timers that control how long dynamically created TARP entries remain in the TID cache, and how long the system ID-to-sequence number mapping entry remains in the loop detection buffer table. The loop detection buffer table prevents TARP PDUs from looping.

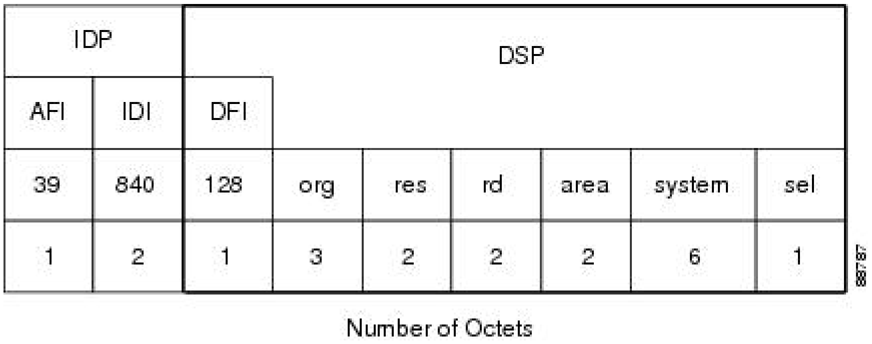
TARP Counters

TARP will maintain a list of useful counters, and will increment the relevant counter. There will also be extensive debugging support that will facilitate troubleshooting

NSAP Address Format

The OSI network address is referred to as a network service access point (NSAP). The NSAP is assigned to the end system (ES) or intermediate system (IS) device. Unlike in IP, which has an address for every network interface, the OSI network device receives only one address, the NSAP address. The NSAP address has two parts, the Initial Domain Part (IDP) and Domain Specific Part (DSP).





IDP		DSP						
AFI	IDI	DFI						
39	840	128	org	res	rd	area	system	sel
1	2	1	3	2	2	2	6	1

Number of Octets
88787

Determining TIDs and NSAPs

To determine an NSAP address for a TID or a TID for an NSAP address, use the following commands in EXEC mode:

Command	Purpose
Router # **tarp query** *nsap*	Gets the TID associated with a specific NSAP.
Router # **tarp resolve** *neighbour tid*	Gets the NSAP associated with a specific TID.

To determine the TID, the router first checks the local TID cache. If there is a TID entry in the local TID cache, the requested information is displayed. If there is no TID entry in the local TID cache, a TARP Type 5 PDU is sent out to the specified NSAP address.

To determine the NSAP address, the router first checks the local TID cache. If there is an NSAP entry in the local TID cache, the requested information is displayed. If there is no NSAP entry in the local TID cache, a TARP Type 1 or Type 2 PDU is sent out. By default, a Type 1 PDU is sent to all Level 1 (IS-IS and ES-IS) neighbors. If a response is received, the requested information is displayed. If a response is not received within the response time, a Type 2 PDU is sent to all Level 1 and Level 2 neighbors. Specifying the **tarp resolve** *tid 2* EXEC command causes only a Type 2 PDU to be sent.

You can configure the length of time that the router will wait for a response (in the form of a Type 3 PDU).

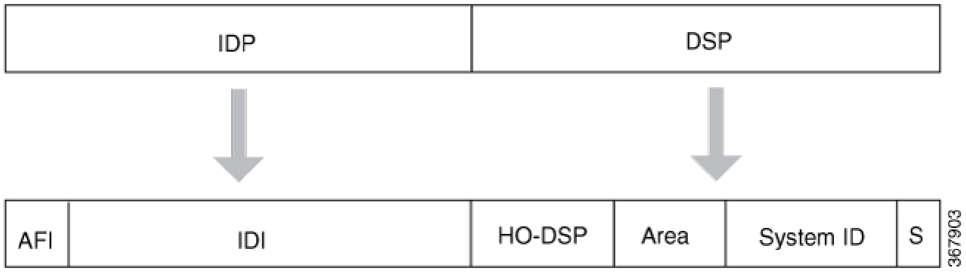
Understanding NSAP

Addresses in the ISO network architecture are referred to as network service access point (NSAP)addresses and network entity titles (NETs). Each node in an OSI network has one or more NETs. In addition, each node has many NSAP addresses. Each NSAP address differs from one of the NETs for that node in only the last byte. This byte is called the N-selector. Its function is similar to the port number in other protocol suites.

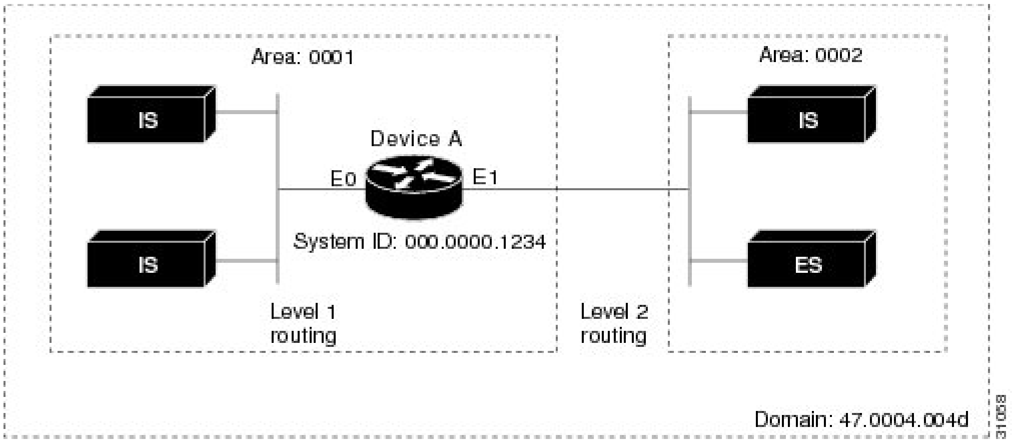
Our implementation supports all NSAP address formats that are defined by ISO 8348/Ad2; however, Cisco provides ISO Interior Gateway Routing Protocol (IGRP) or Intermediate System-to-Intermediate System (IS-IS) dynamic routing only for NSAP addresses that conform to the address constraints defined in the ISO standard for IS-IS (ISO 10589).

An NSAP address consists of the following two major fields, as shown in Figure 1:

- The initial domain part (IDP) is made up of 1-byte authority and format identifier (AFI) and a variable-length initial domain identifier (IDI). The length of the IDI and the encoding format for the domain specific part (DSP) are based on the value of the AFI.
- The DSP is made up of a High Order DSP (HO-DSP), an area identifier, a system identifier, and a 1-byte N-selector (labeled S).



Assign addresses or NETs for your domains and areas. The domain address uniquely identifies the routing domain. All routers within a given domain are given the same domain address. Within each routing domain, you can set up one or more areas, as shown in Figure 2. Determine which routers are to be assigned to which areas. The area address uniquely identifies the routing area and the system ID identifies each node.



The key difference between the ISO IGRP and IS-IS NSAP addressing schemes is in the definition of area addresses. Both use the system ID for Level 1 routing (routing within an area). However, they differ in the way addresses are specified for area routing. An ISO IGRP NSAP address includes three separate fields for routing: the domain, area, and system ID. An IS-IS address includes two fields: a single continuous area field (comprising the domain and area fields) and the system *ID*.

How To Configure TARP

To configure TARP on the router, perform the tasks in the following sections:

Enabling TARP and Configuring a TARP TID

TARP must be explicitly enabled before the TARP functionality becomes available, and the router must have a TID assigned. Also, before TARP packets can be sent out on an interface, each interface must have TARP enabled and the interface must be able to propagate TARP PDUs.

The router will use the CLNS capability to send and receive TARP PDUs. If the router is configured as an IS, the router must be running IS-IS. If the router is configured as an ES, the router must be running ES-IS.

To turn on the TARP functionality, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **tarp run**	Turns on the TARP functionality.
Router(config)# **tarp tid** *tid*	Assigns a TID to the router.

To enable TARP on one or more interfaces, use the following command in interface configuration mode

Table 1:

Command	Purpose
Router(config-if)# **tarp enable**	Enables TARP on the interface.

TARP on Gigabit Ethernet Interface

The following example shows how to enable TARP on the router and Ethernet interface 0. The router is assigned the TID name.

```
interface GigabitEthernet0/2/5
ip address 172.16.1.2 255.240.0.0 àip address for gig
ip router isis 1 -- to enable the isis configured under gig
negotiation auto
clns router isis 1 --- to assign it to clns
isis circuit-type level-1 --- isis level type
tarp enable
```

TARP on SDCC

The following example shows how to enable TARP on the SDCC interface. The router is assigned the TID name.

```
interface SDCC0/3/3
ip address 192.168.10.7 255.255.0.0
encapsulation lapd
lapd t200 200
lapd role user
‘lapd role network’ by default
clns mtu 512
clns router isis 1
isis circuit-type level-1
no isis hello padding
isis retransmit-interval 10
isis lsp-interval 512
tarp enable

tunnel source GigabitEthernet0/4/7
interface GigabitEthernet0/4/7
ip address 172.16.1.1 255.240.0.0
negotiation auto

Router#sh run | sec Tunnel1
interface Tunnel1
ip address 172.16.2.2 255.240.0.0
ip router isis 1
```

```
tunnel source GigabitEthernet0/4/7
tunnel destination 192.168.1.2
clns router isis 1
isis circuit-type level-1
tarp enable
```

For more information on SDCC, Configuring Data Communication Channel

How to Configure TARP

TARP must be explicitly enabled before the TARP functionality becomes available, and the router must have a TID assigned. Also, before TARP packets can be sent out on an interface, each interface must have TARP enabled and the interface must be able to propagate TARP PDUs.

The router uses the CLNS capability to transfer and receive TARP PDUs. If the router is configured as an IS, the router must be running IS-IS. If the router is configured as an ES, the router must be running ES-IS.

TARP feature can be optionally enabled or disabled through CLI. Furthermore, all interfaces over which TARP packets that need to be sent must have TARP configured. Propagation of TARP packets can be disabled on an interface basis, on an adjacency basis, or on a global basis. Origination of TARP packets can be disabled on a global basis.

To configure TARP on a Gigabit Ethernet Interface, use the following commands:

Procedure

Step 1 **configure terminal**

Enter global configuration mode.

Step 2 **tarp run**

```
Router (config)# tarp run
```

Enable TARP functionality.

Step 3 **tarp tid** *id*

```
Router (config)# tarp tid 500
```

Assign TID to the router.

Step 4 **tarp enable** *interface name*

```
Router (config)#tarp enable Te0/12/0
```

Enables TARP on an interface.

TARP Configuration Examples

The following example shows how to enable TARP on the router and Ethernet interface 0. The router is assigned the TID myname.

```
clns routing
 tarp run
 tarp tid myname
```

```
interface ethernet 0
 tarp enable
```

Configuring TARP Features

To configure TARP features on the router, perform the tasks in the following sections.

Configuring Static TARP Adjacency and Blacklist Adjacency

In addition to all its IS-IS/ES-IS adjacencies, a TARP router propagates PDUs to all its static TARP adjacencies. If a router is not running TARP, the router discards TARP PDUs rather than propagating the PDUs to all its adjacencies. To allow TARP to bypass routers en route that may not have TARP running, TARP provides a static TARP adjacency capability. Static adjacencies are maintained in a special queue.

To create a static TARP adjacency, use the following command in global configuration mode:

Command	Purpose
Router(config)# **tarp route-static** *nsap* **[all | message-type {unknowns** | type-number} [type-number] [type-number]]	Enters a static TARP adjacency.

To stop TARP from propagating PDUs to an IS-IS/ES-IS adjacency that may not have TARP running, TARP provides a blacklist adjacency capability. The router will not propagate TARP PDUs to blacklisted routers. To blacklist a router, use the following command in global configuration mode:

To blacklist a router, use the following command in global configuration mode:

Command	Purpose
Router(config)# **tarp blacklist-adjacency** *nsap*	Bypasses a router not running TARP.

Configuring TARP Timers

TARP timers provide default values and typically need not be changed.

You can configure the amount of time that the router waits to receive a response from a Type 1 PDU, a Type 2 PDU, and a Type 5 PDU. You can also configure the lifetime of the PDU based on the number of hops.

You can also set timers that control how long dynamically created TARP entries remain in the TID cache, and how long the system ID-to-sequence number mapping entry remains in the loop detection buffer table. The loop detection buffer table prevents TARP PDUs from looping.

To configure TARP PDU timers, control PDU lifetime, and set how long entries remain in cache, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **tarp t1-response-timer** *seconds*	Configures the number of seconds that the router will wait for a response from a TARP Type 1 PDU.

Command	Purpose
Router(config)# **tarp t2-response-timer** *seconds*	Configures the number of seconds that the router will wait for a response from a TARP Type 2 PDU.
Router(config)# **tarp post-t2-response-timer** *seconds*	Configures the number of seconds that the router will wait for a response from a TARP Type 2 PDU after the default timer has expired.
Router(config)# **tarp arp-request-timer** *seconds*	Configures the number of seconds that the router will wait for a response from a TARP Type 5 PDU.
Router(config)# **tarp lifetime** *hops*	Configures the number of routers that a TARP PDU can traverse before it is discarded.
Router(config)# **tarp cache-timer** *seconds*	Configures the number of seconds a dynamically created TARP entry remains in the TID cache.
Router(config)# **tarp ldb-timer** *seconds*	Configures the number of seconds that a system ID-to-sequence number mapping entry remains in the loop detection buffer table.

Configuring Miscellaneous TARP PDU Information

TARP default PDU values typically need not be changed.

You can configure the sequence number of the TARP PDU, set the update remote cache bit used to control whether the remote router updates its cache, specify the N-selector used in the PDU to indicate a TARP PDU, and specify the network protocol type used in outgoing PDUs.

To configure miscellaneous PDU information, use the following commands in global configuration mode:

Table 2:

Command	Purpose
Router(config)# **tarp sequence-number** *number*	Changes the sequence number in the next outgoing TARP PDU.
Router(config)# **tarp urc [0 | 1]**	Sets the update remote cache bit in all subsequent outgoing TARP PDUs so that the remote router does or does not update the cache.
Router(config)# **tarp nselector-type** *hex-digit*	Specifies the N-selector used to identify TARP PDUs.
Router(config)# **tarp protocol-type***hex-digit*	Specifies the protocol type used in outgoing TARP PDUs. Only the hexadecimal value 0xFE (to indicate the CLNP) is supported.

TARP Configuration Task List

To configure TARP on the router, perform the tasks in the following sections. Only the first task is required; all other tasks are optional.

Disabling TARP Caching

By default, TID-to-NSAP address mappings are stored in the TID cache. Disabling this capability clears the TID cache. Reenabling this capability restores any previously cleared local entry and all static entries.

To disable TID-to-NSAP address mapping in the TID cache, use the following command in global configuration mode:

Command	Purpose
Router(config)# **no tarp allow-caching**	Disables TARP TID-to-NSAP address mapping.

Disabling TARP PDU Origination and Propagation

By default, the router originates TARP PDUs and propagates TARP PDUs to its neighbors, and the interface propagates TARP PDUs to its neighbor. Disabling these capabilities means that the router no longer originates TARP PDUs, and the router and the specific interface no longer propagate TARP PDUs received from other routers.

To disable origination and propagation of TARP PDUs, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **no tarp originate**	Disables TARP PDU origination.
Router(config)# **no tarp global-propagate**	Disables global propagation of TARP PDUs.

To disable propagation of TARP PDUs on a specific interface, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **no tarp propagateall | message-type {unknowns***type-number} [type-number] [type-number]]*	Disables propagation of TARP PDUs on the interface.