ATM Signaling and Switched Virtual Circuits

ATM Switched Virtual Circuits (SVCs), as implemented by the SES node, are described in the following topics:

- ATM User Network Interface
- ATM SVC Addresses
- ATM Address Filtering
- Point-to-Point Switched Virtual Circuit Connections
- ATM Standards Compliance

**ATM User Network Interface**

The ATM User Network Interface (UNI) provides the interface for ATM end users—the ATM CPE—to attach to the SES node. This interface carries both ATM user data and ATM SVC signaling messages to the SES PNNI node. ATM UNI on the SES PNNI node supports the following configurations:

- ATM UNI Signaling Channel
- UNI Protocol Version
- ILMI Address Registration
- ATM Address Filtering

**ATM UNI Signaling Channel**

A PVC signaling channel is established by the PNNI controller between the ATM CPE, across the ATM UNI, and the SES PNNI node. The signaling channel is configured to pass signaling messages between the ATM CPE and the SES PNNI node and WAN switching network. These messages contain information elements, defined by the ATM Forum 3.0/3.1 specifications, and are used to dynamically establish, maintain, and clear ATM connections at the ATM UNI. This signaling channel terminates on the SES PNNI controller ATM interface (Figure 4-1).
Figure 4-1 ATM UNI signaling Channel

The illustration shows that the signaling channels use VPI 0 and VCI 5 at the ATM CPE end—the ATM UNI—as defined by the ATM Forum specifications.

Note
ILMI signaling uses VPI 0 and VCI 16. PNNI signaling uses VPI 0 and VCI 18.

The signaling VPI/VCI can be changed from the default (VPI 0, VCI 5) during the provisioning of the SES PNNI node with the cnfpnportsig command. The SES PNNI controller software assigns both the VPI/VCIs for the signaling channels at the UNI interface and at the SES PNNI controller end of the signaling channel.

UNI Protocol Version

The SES PNNI node is compliant with either of the following ATM Forum UNI protocol versions:

- ATM Forum 3.0
- ATM Forum 3.1

These ATM Forum specifications define interoperability standards between ATM-based products (such as a router or an ATM switch similar to the SES PNNI node) located in a private network and the ATM switches within public carrier networks. The ATM Forum specifications include:

- Background information on ATM technology and protocols used for broadband networking.
- Initial service attributes defined as the User Network Interface.
- Set of physical layer specifications supported for the carrying ATM cells.
- ATM layer specification common for all specified physical layer interfaces.
ILMI

ILMI is responsible for the following functions:
- ATM Address Registration
- ILMI Connectivity Procedures and Secure Link Procedures
- Change of Attachment Point Detection
- AutoConfiguration
- Modification of Local Attributes

Both PNNI and AutoRoute use ILMI to access link connectivity information. The PNNI also uses the ILMI 4.0 features to perform address registration and auto configuration. The ILMI applications running in the ILMI Manager use VSI pass through to send/receive messages to/from the ILMI IME resided on the BXM.

The BPX PNNI node provides both LMI and ILMI (ATM Forum ILMI 3.x and ILMI 4.0) operations. The BPX control point supports both LMI and ILMI configuration.

LMI and ILMI signaling VCCs terminate at the LMI or ILMI on the BXM in the SES PNNI node to communicate the connection status with the ILMI Manager on the SES PNNI Controller.

ILMI Address Registration

The dynamic exchange between ATM CPE and the SES PNNI node allows them to establish the ATM address(es) in effect. ILMI address registration reduces the need for the manual configuration of ATM CPE (end users) attached to the SES PNNI node. ILMI must be enabled for both the SES PNNI node and attached ATM CPE.

To establish ATM connections at the UNI, both the ATM CPE (end user) and the SES PNNI node (WAN switching network) must know the ATM address(es) that are in effect at that UNI. These ATM addresses can then be used in Calling Party Number information elements of signaling messages sent by the user, and in Called Party Number information elements of signaling messages sent to the user. The ILMI Address Registration procedures defined by the ATM Forum provide the means for the dynamic exchange of addressing information between the user and the network at the UNI during initialization or as required.

ILMI address registration enables the SES PNNI node to discover all ATM CPE attached to the UNI ports.

An ILMI address registration sequence is as follows:
1. The SES PNNI node dynamically sends its AESA prefix to the ATM CPE.
2. In return, the ATM CPE prepends that prefix to its ESI and selector fields, forming a complete ATM AESA address.
3. The ATM CPE notifies the SES PNNI node of its complete ATM CPE address.
4. These ILMI registration SNMP messages are exchanged over VPI 0 and VCI 16.
5. Once ILMI address registration has been completed, the ATM SVC connection setup can begin.
ILMI address registration is either enabled or disabled for each ATM UNI Port during the provisioning of the SES PNNI node with the SES PNNI controller Configuration Interface.

**ILMI Connectivity Procedures and Secure Link Procedures**

ILMI connectivity procedures are used to detect the establishment and subsequent loss of ILMI connectivity. These events are used for auto-configuration and address registration. ILMI 4.0 specifies that for an ILMI, when a Loss of ILMI Connectivity is detected, the corresponding UNI or NNI signaling entity is not required to release all the SVCs associated with the entity. However, when a change of attachment is configured and detected, the corresponding signaling entity then must release all the SVCs associated with the entity.

The SES PNNI controller implements the secured link procedure for UNI by processing a loss of ILMI connectivity as an attachment change. When a change of attachment point is detected by the IME, it releases all the SVCs and send a coldStart Trap to its peer IME as described the ILMI specifications.

**ILMI Auto Configuration**

Auto configuration on an interface involves the reading of `atmfAtmLayerTable` objects by peer IMEs. These peers determine each other’s capabilities by reading the following objects:

- Maximum VCCs
- Maximum VPCs
- Maximum VPI bits
- Maximum VCI bits
- UNI Type
- UNI Version
- Device Type
- ILMI Version
- NNI Signalling Version
- Maximum SVPC VPI
- Maximum SVCC VPI
- Minimum SVCC VCI

These values are then used to determine the operational configuration for the interface:

- Interface type (public or private)
- Device type (user-side or network-side)
- UNI signaling version (UNI 3.0 or 3.1)
- NNI signaling version (IISP 3.0, IISP 3.1, or PNNI 1.0)
- ILMI version (3.x or 4.0)
- Maximum VCCs
- Maximum VPCs
- Maximum VPI bits
- Maximum VCI bits
- Maximum Switched VPC VPI
Chapter 4 ATM Signaling and Switched Virtual Circuits

ATM SVC Addresses

- Maximum Switched VCC VPI
- Minimum Switched VCC VCI

The operational configuration is used by SES PNNI controller to perform resource management and protocol stack configuration. The ILMI 4.0 specification contains details on auto-configuration. The negotiated configuration will be sent to the standby PNNI controller, and it will take precedence to operational configuration.

PNNI Signaling

PNNI signaling is based on a subset of UNI 4.0 signaling. PNNI Signaling is different from UNI 4.0 signaling as follows:

- PNNI is symmetric
- PNNI does not support proxy signaling
- PNNI does not support the leaf initiated join capability
- PNNI does not support user-to-user supplementary service
- PNNI uses DTLs to carry hierarchically complete source routes.
- PNNI uses crankback and alternate routing to find alternate paths when provisioning information inaccurate.
- PNNI uses associated signalling for operation over virtual path connections.
- PNNI supports soft permanent VPCs/VCCs (soft PVPC/PVCCs).

PNNI signaling makes use of information gathered by PNNI routing. Specifically, PNNI signalling uses route calculations derived from the reachability, connectivity, and resource information dynamically maintained by PNNI Routing. These routes are calculated as needed from the node’s view of the current topology.

Crankback

Crankback is a PNNI signaling mechanism that permits partial release and alternate routing of an active connection setup that has encountered a failure. When a call in progress is blocked along its specified route, the necessity to clear the call all the way back to the source node is not required. When the call cannot be processed according to the DTL (designated transit list), it is cranked back to the entry border node of its peer group, accompanied by an indication off the problem. The intermediary PNNI node in the route selects an alternate path over which to progress the call, or initiate further crankback of the call. The alternate path avoids the blocked PNNI node.

ATM SVC Addresses

To establish ATM SVCs, each ATM UNI end system must have an ATM end system address (AESA) that uniquely identifies an ATM endpoint. The ATM Forum has adapted the subnetwork model of addressing, in which the ATM layer is responsible for mapping network layer addresses to ATM addresses. Several ATM address formats have been developed—one for public networks and three for private networks. Typically, public ATM networks will use E.164 numbers, which are also used by Narrowband Integrated Services Digital Network (N-ISDN) networks.
Private ATM addresses are formatted as follows (Figure 4-2):

- Data Country Code (DCC)
- International Code Designator (ICD)
- Network Service Access Point (AESA) encapsulated E.164 addresses

**Figure 4-2  ATM Address Formats**

ATM address fields contain the elements shown in Table 4-1.

**Table 4-1  ATM Address Field Components**

<table>
<thead>
<tr>
<th>ATM Field</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFI</td>
<td>1-byte authority and format identifier. The AFI field identifies the type of address. The defined values are 45, 47, and 39 for E.164, ICD, and DCC addresses, respectively.</td>
</tr>
<tr>
<td>DCC</td>
<td>2-byte data country code.</td>
</tr>
<tr>
<td>DFI</td>
<td>1-byte data format identifier.</td>
</tr>
<tr>
<td>AA</td>
<td>2-byte administrative authority.</td>
</tr>
<tr>
<td>RD</td>
<td>2-byte routing domain.</td>
</tr>
<tr>
<td>Area</td>
<td>2-byte area identifier.</td>
</tr>
<tr>
<td>ESI</td>
<td>6-byte end system identifier, which is an IEEE 802 Media Access Control (MAC) address.</td>
</tr>
<tr>
<td>Sel</td>
<td>1-byte AESA¹ selector.</td>
</tr>
<tr>
<td>ICD</td>
<td>2-byte international code designator.</td>
</tr>
<tr>
<td>E.164</td>
<td>8-byte Integrated Services Digital Network (ISDN) telephone number. The native E.164 address is encapsulated in a private ATM address.</td>
</tr>
</tbody>
</table>

1. AESA was previously referred to as a Network Service Access Point (NSAP).

The ATM address formats are modeled on ISO AESA addresses, but they identify SubNetwork Point of Attachment (SNPA) addresses. Incorporating the MAC address into the ATM address facilitates mapping of ATM addresses into existing LANs.
Native E.164 Address

In addition to the private ATM address formats defined by the ATM Forum, the SES PNNI node also supports Native E.164 addresses. E.164 addresses are defined by the ITU-T for international telecommunication numbering, and are an evolution of standard telephone numbers.

You can configure a 15-digit (maximum) E-164 address on the SES PNNI node.

SES PNNI Node Default AESA Address

The default SES PNNI node ATM address—an AESA ICD address—is based on the SES PNNI controller MAC address, which allows all SES PNNI nodes to auto-configure within the same Peer Group at level 56 because they all share the same 7-octet prefix (0x 47 0091 8100 0000). Cisco has been assigned the 47.0091 ICD prefix.

Figure 4-3 SES PNNI Node ATM Address

Table 4-2 SES PNNI Node ATM Address Field Components

<table>
<thead>
<tr>
<th>ATM Field</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFI</td>
<td>1-byte authority format identifier (47).</td>
</tr>
<tr>
<td>Cisco ICD</td>
<td>2-byte Cisco specific International Code Designator (0091).</td>
</tr>
<tr>
<td>Address Type (reserved)</td>
<td>4-byte Cisco-specific information (8100 0000).</td>
</tr>
<tr>
<td>PXM MAC</td>
<td>6-byte PNNI controller MAC address.</td>
</tr>
<tr>
<td>ESI</td>
<td>6-byte end system identifier. This field repeats the PNNI Controller MAC address when the ATM address identifies the SES PNNI node. (When an ATM address identifies an ATM end system, that is ATM CPE attached to the SES PNNI nodes UNI port, the ESI field will be completed through ILMI registration with the end system. In this case, the ESI is typically the MAC address of the ATM CPE. The unique ESI field will distinguish that ATM end system [ATM CPE] from all other ATM end systems. )</td>
</tr>
<tr>
<td>SEL</td>
<td>1-byte that can be used to distinguish Classical IP interfaces that use the same physical interface (00).</td>
</tr>
</tbody>
</table>
The first 13 bytes of the SES PNNI node ATM address comprise the AESA ICD prefix. This is the default PNNI summary address prefix used for ILMI address registration.

The first 7 bytes are always 47 0091 8100 0000, followed by the SES PNNI controller MAC address, 6 bytes. This unique prefix identifies the SES PNNI node. This is the default UNI port prefix that enables the remaining 7 bytes of an ATM address to be configured by the ILMI address registration with the ATM CPE (ATM end user).

**Address Configuration**

SVC addresses can be set up in two ways for a UNI port. If ILMI is enabled on a UNI port, you can add up to 16 address prefixes for that port. The same ILMI prefix can be assigned to two or more ports. These ILMI prefixes will be advertised by PNNI so that SVCs to enable SVC routing to this node.

If ILMI is not enabled for a UNI port, the you can add up to 255 AESAs on that port, if within the maximum addresses per node limit. The addresses are not required to be unique in the node, therefore the same address can be assigned to other UNI ports. These addresses are provided to PNNI to be summarized and advertised.

For IISP configured ports, addresses can be added to build static routes by PNNI. The same address can be configured on more than one IISP port.

**ATM Address Filtering**

The PNNI node uses four forms of address filtering, as associated with the originating and the terminating nodes, when processing addresses during transport of SETUP messages across the network.

If the SETUP message is processed at the Originating Node, the PNNI can use:

1. Incoming Call-In Party Number Filtering
2. Incoming Called Party Number Filtering

If the SETUP message is processed at the Terminating Node, the PNNI can use:

1. Outgoing Called Party Number Filtering
2. Outgoing Called Party Number Filtering

---

**Note**

Address format conversion is performed at the originating node (from E.164 to AESA E164), and at the terminating node (AESAs E.164) if required.

All routing by the PNNI Route Agent is done using AESA-formatted numbers. Before a source route request can be made to the PNNI Route Agent at the originating node an incoming Called Number in native E.164 format must first be converted to AESA E.164 format. This is done by padding native E.164 address digits with leading semi-octets in the IDI field of the AESA E.164 number as described in UNI 3.x 3.1.1.3. The DSP part of the AESA E.164 address is set to zero.
You can configure either of two methods to convert a native E.164 address to AESAAESA E.164 address—either right justify or left justify—by using the `cnfe164justify` command.

- **Right justify** is specified in UNI 3.x and is the default setting.

**Note**

All nodes in a PNNI network should use the same justification. If the addresses are the same, but justification is different, the call may be rejected.

The SES PNNI controller ATM software uses access control lists to permit or deny incoming or outgoing calls on a port interface. It uses access control lists to filter calls based on the destination or source (or a combination of both) ATM address in the SETUP message.

Access control lists, or filters, are mapped to a port. Currently, two access control lists can be configured for each port—one for incoming calls, and the other for outgoing calls.

### Incoming Call-In Party Number Filtering

Incoming Call-in number filtering lets the network block or accept calls from specific source addresses. Incoming Call-in number (ingress) filtering filters incoming Call-in Party Numbers against an incoming Filtering List. An incoming call whose Call-in Party Number matches an address entry in the Incoming Filtering List is rejected or accepted depending on the filtering policy—either permit or deny—assigned to the entry on the list.

The filtering options are:

- **Permit**—If the filter address entry matches the digits of the Call-in Party considered for the address match in the SETUP message and has a permit filtering policy, then the call can be made.
- **Deny**—If the filter address entry matches the digits of the Call-in Party considered for the address match in the SETUP message and has a deny filtering policy, then the call is rejected.

The filter address entry and the digits of the cg/cd party may be configured as an exact match. The filter also contains options to match address prefixes and wildcards.

If a Call-in Party address does not match any address entry in the Incoming Filtering List, the call is accepted or rejected depending on how the filter option was set.

### Incoming Called Party Number Filtering

Incoming called number filtering lets the network block or accept calls to specific destination addresses. Incoming Called Number (Ingress) Filtering filters incoming Called Party Numbers against an Incoming Filtering List. An incoming call whose Called Party Number matches an address entry in the Incoming Filtering List is rejected or accepted depending on the filtering policy—either permit or deny—assigned to the entry in the list.

The filtering options are:

- **Permit**—If the filter address entry matches the digits of the Called Party considered for the address match in the SETUP message and has a permit filtering policy, the call can then be made.
- **Deny**—If the filter address entry matches the digits of the Called Party considered for the address match in the SETUP messages and has a deny filtering policy, the call is then rejected.
The filter address entry and the digits of the cg/cd party may be configured as an exact match. The filter also contains options to match address prefixes and wildcards.

If a Called Party address does not match any address entry in the Incoming Filtering List, the call is accepted or rejected depending on how the filter option was set.

Outgoing Called Party Number Filtering

Outgoing calling number filtering lets the network block or accept calls from specific source addresses. Outgoing (egress) Calling Number Filtering filters outgoing Calling Party Numbers against an Outgoing Filtering List. An outgoing call whose Calling Party Number matches an address entry in the Outgoing Filtering List is rejected or accepted depending on the filtering policy—either permit or deny—assigned to the entry in the list.

The filter options are as follows:

- **Permit**: If the filter address entry matches the digits of the Calling Party considered for the address match in the SETUP message and has a permit filtering policy, the call can then be made.
- **Deny**: If the filter address entry matches the digits of the Calling Party considered for the address match in the SETUP message and has a deny filtering policy, the call is then rejected.

If a Calling Party address does not match any address entry in the Outgoing Filtering List, the call is accepted or rejected depending on how the filter option was set.

Outgoing Called Party Number Filtering

Outgoing called number filtering lets the network block or accept calls for specific destination addresses. Outgoing (egress) Called Party Filtering filters outgoing Called Party Numbers against an Outgoing Filtering List. An outgoing call whose Called Party Number matches an address entry in the Outgoing Filtering List is rejected or accepted depending on the filtering policy—either permit or deny—assigned to the entry in the list.

The filter options are:

- **Permit**: If the filter address entry matches the digits of the Called Party considered for the address match in the SETUP message and has a permit filtering policy, the call can then be made.
- **Deny**: If the filter address entry matches the digits of the Called Party considered for the address match in the SETUP message and has a deny filtering policy, the call is then rejected.

If a Called Party address does not match any address entry in the Outgoing Filtering List, the call is accepted or rejected depending on how the filter option was set.

The number of filter addresses are limited by amount of memory on the system.

Address Translation

Address translation is performed from Native E.164 address numbers to E.164 AESA and vice versa. This conforms with AF/98-0016R1 contribution at ATMF.
Point-to-Point Switched Virtual Circuit Connections

The SES PNNI node supports point-to-point ATM SVC connections. These connections, which can be unidirectional or bidirectional, support the following features:

- Point-to-Point switched virtual circuit connections
- Connection with asymmetrical bandwidth requirements
- CBR, VBR, and UBR service classes
- Alternate call routing
- Called number screening (Ingress screening)
- Calling number screening (Egress screening)
- Native E164 and AESA address formats

Typical Call Setup and Teardown

Using the example shown in Figure 4-4, this section describes SVC connection establishment across a simple point-to-point switched virtual circuit connection. The dotted line represents the signaling connection; the solid line represents the actual data transfer that occurs after the call is setup.

Figure 4-4  Point-to-Point ATM SVC Connection

The sequence for establishing an SVC connection is as follows:

1. A SETUP message from an ATM CPE is routed from the switch into the ATM Signaling Stack of the PNNI controller. A finite state machine in the Call Control is triggered.
2. The Call Control requests the PNNI Route Agent to find an optimal route path for this SVC.
3. The Route Agent provides a DTL (designated transit list) to Call Control to route the call. Call Control then checks RM (resource manager) to see whether the interface has enough resources (BW, LCNs, VCIs, and so forth) to support this connection. If it does not, the call is rejected. Otherwise, the call proceeds.
4. The SETUP message is sent back to the BPX switch from the ATM Signaling Stack. The BPX switch sends out the SETUP message through a port defined by the DTL.
5. Each intermediate succeeding node passes the message from ingress to egress via that node’s PNNI controller.
6. The destination node forwards the setup message to the user’s ATM CPE.
7. When the called party accepts the call, a CONNECT message is returned to the Call Control following the reverse direction of the DTL path.

8. Call Control sets up the BPX BXM cross-connects through Connection Manager and VSI Master and changes this connection operation state to ACTIVE.

ATM Standards Compliance

See Appendix A, “Technical Specifications”, for the ATM specifications to which the SES PNNI node complies.