

# Troubleshooting the ANI Discovery Used by Campus Manager and UserTracking

Document ID: 7948

---

## **Introduction**

### **Prerequisites**

- Requirements
- Components Used
- Conventions

### **ANI Discovery**

- Step 1 – Discover the Devices
- Step 2 – Read the VLAN Trunking Protocol (VTP) Domain
- Step 3 – Read the VLANs
- Step 4 – Read the MAC Addresses
- Step 5 – Map VLANs to Subnets
- Step 6 – Perform Ping Sweeps
- Step 7 – Resolve IP Addresses
- Step 8 – Resolve Host Names
- Step 9 – Resolve Phone Extensions
- Step 10 – Discover User Names

### **Troubleshooting Topology Services**

- Devices Are Not Discovered
- ATM Devices Are Not Discovered
- Devices Are In The Unconnected Devices View
- Links Are Missing Or Incorrect
- Devices Have A Question Mark In Their Icon
- Delete A Device From The Map
- The Initial Discovery Takes Longer Than The Subsequent Discoveries
- The ANI Discovery Takes Forever

### **Troubleshooting UserTracker**

- UserTracker Does Not Discover The MAC Addresses
- UserTracker Does Not Discover The IP Addresses
- UserTracker Does Not Discover The Hostnames
- UserTracker Does Not Discover The Phone Extensions
- UserTracker Is Not Discovering The Usernames On Windows Clients
- UserTracker Is Not Discovering The Usernames On Unix Clients
- UserTracker Is Discovering Duplicate MAC Addresses

### **NetPro Discussion Forums – Featured Conversations**

### **Related Information**

---

## **Introduction**

This document helps you troubleshoot the Asynchronous Network Interface (ANI) discovery used by Campus Manager and UserTracking.

## **Prerequisites**

## Requirements

There are no specific requirements for this document.

## Components Used

The information in this document is based on the Campus Manager Software Release 3.2 and 3.3.

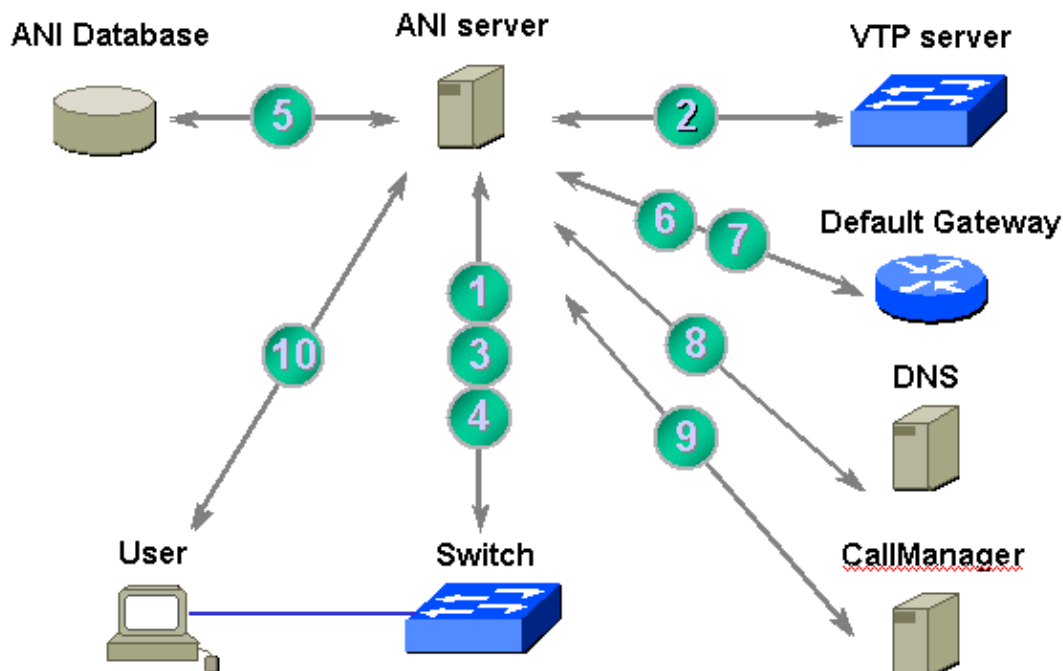
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## ANI Discovery

ANI is a foundation for the development of Cisco network management applications. The framework provides discovery and inventory services for applications such as Topology Services, UserTracker, and Path Analysis.



- Step 1. Discover the Devices
- Step 2. Read the VTP Domain
- Step 3. Read the VLANs
- Step 4. Read the MAC Addresses
- Step 5. Map VLANs to Subnets
- Step 6. Perform Ping Sweeps
- Step 7. Resolve IP Addresses
- Step 8. Resolve Host Names
- Step 9. Resolve Phone Extensions
- Step 10. Discover User Names

## Step 1 – Discover the Devices

The ANI discovery begins with a seed device provided by the user:

- Server Configuration → Setup → ANI Server Admin → Discovery Settings

ANI sends Simple Network Management Protocol (SNMP) requests to the seed device to learn its neighbors' tables. Each neighbor is then queried for its neighbors until all devices are discovered.

On Ethernet devices, ANI reads the CdpCacheEntry table from CISCO-CDP-MIB to learn the neighbor table.

**Example:** The seed device is linked to a device with IP address 172.17.246.48. The port on the seed device is 4/13. The remote port is 2/9. Get the IP address from the cdpCacheAddress table:

```
# snmpwalk <device>
1.3.6.1.4.1.9.9.23.1.2.1.1.4 cdpCacheAddress.87.1 : ac 11 f6
30
```

where **ac 11 f6 30** is the hex of 172.17.246.48.

The remote port is collected through the cdpCacheDevicePort object:

```
# snmpwalk
<device> 1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCacheDevicePort.87.1 : 2/9
```

The CISCO-CDP-MIB uses the same index as the IF-MIB. Find the local port by referencing the IF-MIB:

```
# snmpget <device>
1.3.6.1.2.1.31.1.1.1.1.87 ifName.87 : 4/13
```

On ATM devices, the neighbors are learned through the atmInterfaceConfEntry from the ATM-MIB.

**Example:** An ATM switch is connected to an ATM switch with IP address 172.17.246.224. Read the IP address from the atmInterfaceMyNeighborIpAddress table:

```
# snmpwalk
<device> 1.3.6.1.2.1.37.1.2.1.11
atmInterfaceMyNeighborIpAddress.3 : 172.17.246.96
```

The remote interface is collected through the atmInterfaceMyNeighborIfName object:

```
# snmpwalk <device>
1.3.6.1.2.1.37.1.2.1.12 atmInterfaceMyNeighborIfName.3 :
ATM0/0/1
```

The entries are indexed by the ifIndex. Learn the local interface by reading the ifTable:

```
# snmpget
<device> 1.3.6.1.2.1.2.2.1.2.3 ifDescr.3 :
ATM0/0/2
```

After it discovers the devices, ANI tries to resolve the IP address of each device to its hostnames using Domain Name Server (DNS) or the host file. The reverse name resolution uses the IP address that ANI finds in the Cisco Discovery Protocol (CDP) cache when it first discovers the device. This works fine if you have configured your DNS with a reverse lookup for all the IP addresses on every interface

(router-serial1.cisco.com). However, the reverse name resolution fails if the IP address is not configured in DNS.

To resolve this, Campus Manager release 3.1 and later also uses the sysName as alternative to DNS. ANI reads the sysName in an SNMP request to the device. It tries to resolve the value of sysName to an IP address. Campus first checks if this IP address exists on the device. Then it tries to resolve it to a hostname in a reverse name resolution.

Example: ANI discovers a device with IP address 172.17.246.1. However, only the loopback address 10.0.0.1 is resolvable. Try to resolve the IP address found through CDP:

```
# nslookup
172.17.246.1 Server: ns.cisco.com Address: 172.17.246.224 ***
ns.cisco.com can't find 172.17.246.1: Non-existent host/domain
```

The address is not resolved. So you read the sysName on the device:

```
# snmpwalk <device> 172.17.246.1
sysName system.sysName.0 : DISPLAY STRING- (ascii):
router
```

Check if this hostname is in your DNS:

```
# nslookup router Server: ns.cisco.com
Address: 172.17.246.224 Name: router.cisco.com Address: 10.0.0.1
```

From now on, Campus Manager uses 10.0.0.1 as the IP address, and router.cisco.com as the hostname.

Campus 3.1 tries to find the best IP address by doing a forward lookup on the hostname it resolved because the discovered IP address is not always the preferred management address,. ANI assumes that the IP address it gets by doing a forward lookup is the IP address the user wants to see on the topology map. If the DNS server has multiple IP addresses configured for the same hostname, the reverse lookup gives you the best choice.

**Example:** ANI discovers a device with IP address 172.17.246.20. However, the loopback address 10.0.0.20 is a better choice. You first get the hostname:

```
#
nslookup 172.17.246.20 Server: ns.cisco.com Address:
172.17.246.224 Name: router.cisco.com Address: 172.17.246.48
```

Do a forward lookup to see if there is a better IP address:

```
#
nslookup router.cisco.com Server: ns.cisco.com
Address: 172.17.246.224 Non-authoritative answer: Name: router.cisco.com
Address: 10.0.0.20
```

## Step 2 – Read the VLAN Trunking Protocol (VTP) Domain

The next step is to discover the hosts in the network. ANI collects the hosts by reading the content-addressable memory (CAM) tables on the switches that are discovered in the device discovery. Cisco devices keep a separate table of Media Access Control (MAC) addresses for every virtual LAN (VLAN). ANI first needs to discover the VLANs and VTP domains in the Layer 2 network.

Campus Manager software releases earlier than release 3.1 only read the VLAN tables on the VTP server to decrease the overhead on the network and ANI server. Campus version 3.1 and later support transparent

switches. Each transparent switch is considered to be its own VTP domain and VTP server. It is represented as a separate VTP domain in Topology Services. The syntax is <domain name>\_<switch> (for example, VTPDomain1\_172.17.246.20).

The VTP domain of a switch is discovered with the help of the vlanManagementDomains table described in the CISCO-VTP-MIB. ANI learns if a device is a VTP client, server, or transparent switch with the help of the managementDomainLocalMode. The VTP domain name is discovered through the managementDomainName object. This is an example of how to read the VTP mode:

```
# snmpwalk <device>
1.3.6.1.4.1.9.9.46.1.2.1.1.3 managementDomainLocalMode.1 :
server
```

To collect the VTP domain, use this command:

```
# snmpwalk <device>
1.3.6.1.4.1.9.9.46.1.2.1.1.2 managementDomainName.1 :
DomainA
```

### Step 3 – Read the VLANs

Discover the VLAN of a port before you read the MAC address of the host that is attached to that port. To learn the VLAN that is assigned to a port, ANI reads the vmMembershipEntry from the CISCO-VLAN-MEMBERSHIP-MIB on the port the host is connected to. This gives you the VLAN.

The name of the VLAN is discovered through the vtpVlanEntry table described in the CISCO-VTP-MIB.

Example A host is connected to port 2/1. The port is assigned to VLAN 555. Before you read the VLAN, you need the ifIndex for port 2/1:

```
# snmpwalk <device> 1.3.6.1.2.1.31.1.1.1.1 | grep
2/1 ifName.20 : 2/1
```

The VLAN ID is collected through the vmVlan object:

```
# snmpget
<device> 1.3.6.1.4.1.9.9.68.1.2.2.1.2.20 vmVlan.20 :
555
```

Check whether the VLAN is enabled and active:

```
# snmpget <device>
1.3.6.1.4.1.9.9.68.1.2.2.1.3.20 vmPortStatus.20 : INTEGER:
active
```

Get the VLAN name for VLAN 555 from the vtpVlanTable:

```
# snmpget <device>
1.3.6.1.4.1.9.9.46.1.3.1.1.4.1.555 vtpVlanName.1.555 :
VLAN0555
```

### Step 4 – Read the MAC Addresses

ANI discovers hosts by reading the CAM tables from the discovered switches. Because packets get forwarded and flooded over the Layer 2 network, multiple switches learn the MAC address of a host. To avoid duplicate MAC address entries, ANI ignores ports that are connected to other switches. ANI only reads the forwarding tables from ports that are directly connected to a host.

ANI finds these end-user ports by looking for CDP neighbors on the ports. If a port has a CDP neighbor, the forwarding information for that port is ignored. If there are no CDP neighbors, the CAM table for that port goes into the UserTracking database.

Using the list of edge ports, the discovery sends SNMP requests to query the dot1dTpFdbAddress table from the BRIDGE-MIB.

**Note:** The BRIDGE-MIB keeps a separate instance of the dot1dTpFdbAddress table for every VLAN. To access a particular instance of the MIB, a community string index is used. The syntax is [community string]@[vlan number].

**Example:** A host with MAC address 00-c0-4f-95-af-1e is connected to port 2/1 on a switch. To collect the MAC address on the port, learn the ifIndex for that port:

```
# snmpwalk
<device> 1.3.6.1.2.1.31.1.1.1.1 | grep 2/1 ifName.20 :
2/1
```

The ifIndex of port 2/1 is 20. Check if the port is an end-user port. The ifIndex 20 should not have any CDP neighbors:

```
# snmpwalk <device>
1.3.6.1.4.1.9.9.23.1.2.1.1.4.20 no MIB objects contained under
subtree.
```

The bridge table does not use the same index as the ifTable., Map the ifIndex to the BRIDGE-MIB index. Use the community index to access the BRIDGE-MIB. In step 3, port 2/1 is in VLAN555. Use the [community string]@555 in your snmpwalk:

```
#
snmpwalk -c public@555 <device> 1.3.6.1.2.1.17.1.4.1.2 |
grep 20 dot1dBasePortIfIndex.193 : 20
```

The dot1dBridge index for port 2/1 is 193. Get the CAM table entries for this entry:

```
# snmpwalk -c public@555 <device>
1.3.6.1.2.1.17.4.3.1.2 | grep 193
dot1dTpFdbPort.0.192.79.149.175.30 : 193
```

This gives you the MAC address for port 2/1 in decimal format. To get the address in the normal hex format, use the dot1dTpFdbAddress object:

```
#
snmpget -c public@555 <device>
1.3.6.1.2.1.17.4.3.1.1.0.192.79.149.175.30
dot1dTpFdbAddress.0.192.79.149.175.30 : 00 c0 4f 95 af 1e
```

## Step 5 – Map VLANs to Subnets

The challenge in mapping VLANs to subnets is that Layer 2 devices only know about VLANs. However, they are oblivious to subnets. Layer 3 devices know about subnets. However, they do not know about VLANs. ANI uses its database to tie the two together.

The discovery creates groups of interfaces that are connected to the same link or segment in the database. ANI looks at all the CDP neighbors on a router interface until it finds a neighboring interface that is a port on a switch. The discovery reads the IP address and subnet mask on the router interface to learn the subnet. It reads the VLAN on the switch port to learn the VLAN. The MIB objects used to poll the subnet on a router

interface are ipAdEntAddr and ipAdEntNetMask from the IpAddrEntry table described in RFC1213–MIB.

**Example:** A router has Ethernet0/0 with subnet 172.17.246.0 connected to a switch on port 2/1 assigned to vlan 555. First read the ifIndex of the Ethernet0/0 interface on the router:

```
#
snmpwalk <device> 1.3.6.1.2.1.2.2.1.2 | grep
Ethernet0/0 ifDescr.7 : Ethernet0/0
```

The RFC1213–MIB uses the IP address on the interface as an index., Map the ifIndex to the RFC1213 index using the ipAdEntIfIndex object:

```
#
snmpwalk <device> 1.3.6.1.2.1.4.20.1.2 | grep
7 ipAdEntIfIndex.172.17.246.8 : INTEGER: 7
```

The subnet mask for the interface is read using the ipAdEntNetMask object:

```
# snmpget <device>
1.3.6.1.2.1.4.20.1.3.172.17.246.8 ipAdEntNetMask.172.17.246.8 :
255.255.255.0
```

Now that you know the subnet, tie that subnet to a VLAN. Locate a switch that is a CDP neighbor of Ethernet0/0:

```
# snmpwalk <device>
1.3.6.1.4.1.9.9.23.1.2.1.1.4.7 cdpCacheAddress.7.98 : ac 11 f6
30
```

where **ac 11 f6 30** is the hexadecimal value of 172.17.246.48.

The remote port is collected through the cdpCacheDevicePort object:

```
# snmpwalk
<device> 1.3.6.1.4.1.9.9.23.1.2.1.1.7.7
cdpCacheDevicePort.7.98 : 2/1
```

Read the VLAN from the 172.17.246.48 switch:

```
# snmpwalk 172.17.246.48
1.3.6.1.2.1.31.1.1.1.1 | grep 2/1 ifName.29 : 2/1
```

The VLAN ID is collected through the vmVlan object:

```
#
snmpget 172.17.246.48
1.3.6.1.4.1.9.9.68.1.2.2.1.2.29 vmVlan.29 : 555
```

## Step 6 – Perform Ping Sweeps

ANI maps the discovered MAC addresses to IP addresses by performing reverse ARP requests on the Layer 3 devices. By default, the ARP cache times out after 14,400 seconds. To make sure the ARP table is still fresh, ANI performs a ping sweep on the subnets that are discovered.

**Note:** The ping sweeps are optional. Disable them by going to UserTracking -> Edit -> Preferences -> Discovery -> Ping Sweep.

## Step 7 – Resolve IP Addresses

ANI contacts each router connected to the subnet of the discovered host and queries the ARP table using the ipNetToMediaEntry table from the RFC1213–MIB. ARP tables are often very large. ANI only polls those interfaces that are connected to subnets where hosts are discovered.

Example: The host with MAC address 00 c0 4f 95 af 1e has IP address 172.17.246.187. Under Reading the MAC Addresses, you have discovered that your host is in VLAN 555. Ethernet0/0 on your router is connected to VLAN 555 (Mapping VLANs to Subnets). Get the ifIndex for Ethernet0/0 with this command:

```
# snmpwalk
<device> 1.3.6.1.2.1.2.2.1.2 | grep Ethernet0/0 ifDescr.7 :
Ethernet0/0
```

Look in the ARP cache of ifIndex.7 for the host:

```
# snmpwalk <device> 1.3.6.1.2.1.4.22.1.2.7
| grep "00 c0 4f 95 af 1e"
ipNetToMediaPhysAddress.7.172.17.246.187 : 00 c0 4f 95 af 1e
```

## Step 8 – Resolve Host Names

The discovery makes a system call to the server to resolve the IP addresses to host names. Both DNS and hosts file are supported.

## Step 9 – Resolve Phone Extensions

If the discovered host is an IP phone, ANI needs to resolve the IP address to a phone extension instead of a host name. Because Cisco CallManagers send CDP packets like any other Cisco device, ANI discovers them at the time of the device discovery.

ANI collects the phone extensions by querying the ccmPhoneExtentionEntry table from the CISCO–CCM–MIB on all Cisco CallManagers that are discovered in the network. Every CallManager is contacted until an entry for the IP address is found.

**Example:** The IP phone with IP address 10.200.73.182 has extension number 2005. First, get the index number for the 10.200.73.182 entry:

```
# snmpwalk <callmanager>
1.3.6.1.4.1.9.9.156.1.2.2.1.3 | grep 10.200.73.182
ccmPhoneExtensionIpAddress.999 : 10.200.73.182
```

Using the index number 999, collect the extension number:

```
#
snmpget <callmanager>
1.3.6.1.4.1.9.9.156.1.2.2.1.2.999 ccmPhoneExtension.999 :
2005
```

## Step 10 – Discover User Names

### Windows clients

Before ANI discovers the user account that is logged into the Windows client, configure and run the UTLiteNT.bat on the client machine. This script installs and runs the UTLite.exe executable.

When UTLite.exe runs , it sends a User Datagram Protocol (UDP) packet to the ANI server every ten minutes to tell ANI who is logged into the host. The UTLite.exe does not get installed as a service. You need to set up the UTLiteNT.bat as part of the logon script to make sure every user has this executable running.

By default, UTLite.exe uses port 16236 on the CiscoWorks2000 server. If this port is already used by another process, change the port in both the UTLiteNT.bat script and on the CiscoWorks2000 server (Server Configuration -> Setup -> ANI Server Admin -> User and Host Acquisition -> Use port number).

The default locations for the UTLiteNT.bat script and UTLite.exe executable are:

```
/opt/CSCOpX/bin and C:\Program
Files\CSCOpX\bin
```

This is an example of a UTLiteNT.bat file. The NT domain is "Cisco". The IP address of the CiscoWorks2000 server is 10.1.1.1

```
if NOT EXIST %WINDIR%\UTLite.exe copy
%0\..\UTLite.exe %WINDIR% REM REM Specify the parameters below REM start
%WINDIR%\UTLite -domain Cisco -host 10.1.1.1 -port 16236
```

## Novell clients

NDS hosts are collected the same way as Windows clients are. The script for Novell hosts is called UTLiteNDS.bat.

## UNIX clients

ANI uses the **rusers** command to collect the Unix users. The rusersd daemon has to be enabled in the /etc/initt.d.conf file on the Unix hosts. This is an example:

```
# grep
rusersd inetd.conf rusersd/2-3 tli rpc/datagram_v,circuit_v wait
root /usr/lib/netshvc/rusers/rpc.rusersd rpc.rusersd
```

# Troubleshooting Topology Services

## Devices Are Not Discovered

If the missing device is an Ethernet device, check if it advertises its existence to its neighboring devices through CDP. Verify if the neighboring devices receive the advertisements.

### 1. Verify if CDP is enabled on the missing device.

```
Router1#show cdp % CDP is not enabled
```

To enable CDP on Cisco IOS software devices, enter this command:

```
Router1#cdp run
```

To enable CDP on CatOS devices, enter this command:

```
Switch1#set cdp enable CDP enabled globally
```

Check if the device is listed in the CDP cache on the neighboring device. In the examples, the missing device is Switch1. The neighboring device is Switch2.

## 2. The device is not listed using the `show cdp neighbor` command on the neighboring device:

Check if the device is listed in the CDP cache on the neighboring device. In the examples, the missing device is Switch1. The neighboring device is Switch2.

```
Switch2#show cdp neighbor No entry found.
```

If CDP is enabled, and the neighboring devices do not receive the CDP packets, the advertisements are either blocked by a firewall or the device does not send the CDP advertisements correctly. Verify if the missing device sends CDP packets:

```
Switch1#debug cdp
events CDP events debugging is on *Mar 3 00:14:13: CDP-EV:
Encapsulation on interface Dialer0 failed
```

In this example, the device does not send the CDP packet because the dialer map does not view the CDP packets as interesting traffic and does not bring up the line. Basic Rate Interfaces (BRIs) do not support CDP. Enhancement request CSCdu20683 is opened against this. As a workaround, configure a dialer map to send the CDP packets. CDP is supported on dialer interfaces.

Verify if the neighboring device receives the CDP packets:

```
Switch#debug cdp
packets CDP packet info debugging is on *Mar 3 00:34:14: CDP-PA:
version 2 packet sent out on Ethernet0/0 *Mar 3 00:34:14: CDP-PA: version 1
packet sent out on Ethernet0/0
```

In this example, the neighboring device sends CDP packets. However, it does not receive any CDP packets because a firewall blocks the advertisements. To resolve this, either open up the firewall or configure the device as additional seed device:

◆ Server Configuration → Setup → ANI Server Admin → Discovery Settings

**Note:** CatOS does not support debugging the CDP packets. Sniff the CDP packets for further troubleshooting.

## 3. The device is listed in the `show cdp neighbor` command on the neighboring device. However, the remote IP address is incorrect.

Even though the device is listed in the `show cdp neighbor` output, the device might not advertise an IP address that is accessible to the ANI server. To check if the device advertises a valid IP address, display the CDP neighbor details.

```
Switch2# show cdp neighbor 3/1 detail
Port (Our Port): 3/1 Device-ID: Router Device Addresses: IP
Address: 127.0.0.4 Holdtime: 143 sec Capabilities: ROUTER Version: Cisco
Internetwork Operating System Software IOS (tm) L3 Switch/Router Software
(CAT4232-IN-M), Version 12.0(14)W5(20) RELEASE SOFTWARE Copyright (c) 1986-2001
by cisco Systems, Inc. Compiled Thu 01-Mar-01 18:18 by integ Platform: cisco
Cat4232L3 Port-ID (Port on Neighbors's Device): GigabitEthernet3 VTP Management
Domain: unknown Native VLAN: unknown Duplex: unknown
```

In this example, the CDP neighbor advertised IP address 127.0.0.4. Try pinging the address from the Campus server:

```
CW2000server#
ping 172.0.0.4 no answer from 172.0.0.4
```

The IP address displayed in the `show cdp neighbors detail` command is not pinged. If the ANI

cannot ping the IP address, the CiscoWorks2000 server either does not have a route to the IP address and you need to check the routers between the server and the device, or the IP address that is being advertised is not a valid IP address.

In the example, the device advertises a loopback address because the interface that sends the CDP packets does not have an IP address configured. After assigning a valid IP address to the interface, the problem is resolved.

4. **The device is listed in the `show cdp neighbor` command on the neighboring device and the IP address is correct.**

```
Switch2#show cdp neighbor Port Device-ID
Port-ID Platform -----
3/1 Switch1 GigabitEthernet3 ciscoCat4232L3
```

If the device is listed in the `show cdp neighbors` command, and is not displayed in the Layer 2 View and VTP Domain Views of Topology Services, check if the device is listed in the Unconnected Devices View (Campus Manager -> Topology Services -> Network Views -> Unconnected Devices View).

Unconnected means that ANI is not able to access the device or ANI is not able to determine where the device should be placed on the map. See the Devices Are In The Unconnected Devices View section of this document to find out how to resolve this.

If the device is listed in the `show cdp neighbors` command, and is not listed as unconnected, check if ANI is able to query the neighboring device for its CDP cache through SNMP:

```
# snmpwalk
<switch2> 1.3.6.1.4.1.9.9.23.1.2.1.1.4 no MIB objects
contained under subtree.
```

If the missing device is not listed, you might be running into a bug in the SNMPagent. Try to upgrade to the latest software version on the neighboring device.

## ATM Devices Are Not Discovered

If the missing device is an ATM device, check if the neighboring devices are able to discover the existence of the device through ILMI.

1. **The device is not listed in the `show atm ilmi-status` command on the neighboring ATM device.**

```
#show atm ilmi-status
Interface : ATM0/0/2 Interface Type : Unknown ILMI VCC : (0, 16) ILMI Keepalive
: Disabled Addr Reg State: WaitDevType Configured Prefix(s) :
47.0091.8100.0000.0010.073c.5101
```

To find out why the neighboring device does not discover its peer, enable the debugging:

```
ILMI(ATM0/0/2): Querying peer device type. ILMI:peerDeviceTypeQuery
not completed ILMI:peerPortTypeQuery not completed ILMI: Retrying on (ATM0/0/2)
ILMI: Retry expired on (ATM0/0/2)
```

In this case, the queries to peer time out because the remote interface fails. If you are unable to determine the cause of the problem, try to add the ATM device as additional seed device (Server Configuration -> Setup -> ANI Server Admin -> Discovery Settings).

2. **The device is listed in the `show atm ilmi-status` command on the neighboring ATM device, but has Peer IP Addr 0.0.0.0:**

```
# show atm ilmi-status Interface : ATM1/0/2
Interface Type : Private NNI ILMI VCC : (0, 16) ILMI Keepalive : Disabled ILMI
State: UpAndNormal Peer IP Addr: 0.0.0.0 Peer IF Name: ATM1/0/2 Peer
MaxVPIbits: 8 Peer MaxVCIBits: 14 Peer MaxVPCs: 255 Peer MaxVCCs: 16383 Peer
MaxSvccVpi: 255 Peer MinSvccVci: 35 Peer MaxSvpcVpi: 255 Configured Prefix(s) :
47.0091.8100.0000.0060.4799.fd01
```

Here, the local interface has an entry for its peer. However, the IP address that is listed is 0.0.0.0. ANI is unable to contact the device. When ILMI gets a request for its IP address, it replies with the IP address that is configured on the ATM0 interface. If the interface does not have an IP address assigned, it replies with the IP address on the Ethernet interface.

Here the peer only has a loopback address assigned. The ATM1/0/0 interface and Ethernet2/0/0 are unassigned. To resolve this, configure an IP address on the Ethernet2/0/0 interface.

### 3. The device is listed and has a valid IP address.

```
#show atm
ilmi-status Interface : ATM1/0/2 Interface Type : Private NNI
ILMI VCC : (0, 16) ILMI Keepalive : Disabled ILMI State: UpAndNormal Peer IP
Addr: 10.200.10.34 Peer IF Name: ATM1/0/2 Peer MaxVPIbits: 8 Peer MaxVCIBits:
14 Peer MaxVPCs: 255 Peer MaxVCCs: 16383 Peer MaxSvccVpi: 255 Peer MinSvccVci:
35 Peer MaxSvpcVpi: 255 Configured Prefix(s) :
47.0091.8100.0000.0060.4799.fd01
```

If the device is listed in the **show cdp neighbors** command, and is not displayed in the Layer 2 View and ATM Domain Views of Topology Services, check if the device is listed in the Unconnected Devices View (Campus Manager → Topology Services → Network Views → Unconnected Devices View).

Unconnected means that ANI is not able to access the device or ANI is not able to determine where the device should be placed on the map. See *Devices Are In The Unconnected Devices View* to find out how to resolve this.

If the device is listed in the **show atm ilmi-status** command, and is not listed as unconnected, check if ANI is able to query the device for its ILMI cache through SNMP:

```
# snmpwalk <device>
1.3.6.1.2.1.37.1.2.1.11 atmInterfaceMyNeighborIpAddress.1 :
10.200.10.34
```

If the missing device is not listed in the snmpwalk, you might be running into a bug in the SNMPagent. Try to upgrade to the latest software version on the device.

## Devices Are In The Unconnected Devices View

Campus Manager puts a device in the Unconnected Devices View if ANI does not have SNMP access on the device or if ANI has not discovered any neighbors for that device.

- **The device is listed as Unreachable in the Unconnected Devices View and the icon is red on the topology map.**

Unreachable means that ANI is not able to poll the device through SNMP for its device type and neighbors. It does not necessarily mean that ANI is not able to ping the device.

First, test if there is SNMP connectivity from the CiscoWorks2000 server to the device.

- ◆ The device does not reply .

```
CW2000Server# snmpget <device>
1.3.6.1.2.1.1.5.0 snmpget: No response arrived before timeout.
snmpget: Possible causes include invalid community name, agent is not running
or the node is inaccessible.
```

Check if SNMP is enabled on the device. Verify the read community string. Make sure there is no access list or firewall between ANI and the device that blocks SNMP traffic.

- ◆ The device replies .

```
CW2000Server# snmpget <device>
1.3.6.1.2.1.1.5.0 sysName.0 : Switch1
```

Make sure Campus Manager has the correct community strings configured (Server Configuration -> Setup -> ANI Server Admin -> Discovery Settings).

By default, the SNMP configurations are stored in these locations:

- ◇ C:\Program Files\CSCOpX\etc\cws\anismsnp.conf
- ◇ /opt/CSCOpX/etc/cws\anismsnp.conf

**Note:** ANI only needs the read community string to discover the network. However, Campus Manager needs the write community strings when the user makes configuration changes using the Campus Tools:

- ◇ Campus Manager -> Topology Services -> Tools -> ATM Management
- ◇ Campus Manager -> Topology Services -> Tools -> VLAN Management
- ◇ Campus Manager -> Topology Services -> Tools -> LANE Management
- ◇ Campus Manager -> Topology Services -> Tools -> VLAN Port Assignment

- **The device is listed as Reachable in the Unconnected Devices View and the icon is Green on the topology map.**

ANI has placed the devices in the Unconnected Devices View because the device discovery is not able to link the device to any of the other devices that are discovered. See the Devices Are Not Discovered section of this document for more information.

## Links Are Missing Or Incorrect

When ANI discovers a link, the discovery first reads the interface information on the local port of the device. The ANI discovery then contacts the CDP neighbor of that interface. It reads the interface information of the remote port on the neighboring device. ANI also performs the same procedure on the neighboring device. The result should be the same. In case there are multiple CDP neighbors on the interface (that is, the interface is attached to a hub and there are multiple Cisco devices attached to that hub), ANI repeats the process for every CDP neighbor.

Instead of showing a single link on the map, Campus represents the hub as a segment. If a link is missing, this means that the devices that are connected to the link do not see each other through CDP. Something blocks the CDP packets or one of the devices do not advertise itself to its neighbors.

If Campus wrongly shows links that directly connect two devices as segments, check if the information on both ends of the link is the same. This is an example of two **show cdp neighbors** command outputs that do not add up:

```
Switch1# show cdp neighbor Port Device-ID
Port-ID Platform -----
3/1 Router1 GigabitEthernet3 ciscoCat4232L3 3/2 Router1 GigabitEthernet4
ciscoCat4232L3 3/2 Router1 Port-channel1.1 ciscoCat4232L3 Router1#
show cdp neighbor Device ID Local Intrfce Holdtme
```

```
Capability Platform Port ID Switch1 Port-channel1.1 163 T S WS-C4006 3/2
Switch1 Port-channel1.1 163 T S WS-C4006 3/1
```

The switch sees the router on three interfaces (remote interfaces GE3, GE4, and PC1.1) while the router sees the switch on two interfaces (remote ports 3/1 and 3/2). The result is that Campus shows the switch and router on a segment instead of three separate links. This behavior also occurs on Etherchannels.

To resolve these discrepancies, make sure that all the ports in the channel have CDP enabled.

## Devices Have A Question Mark In Their Icon

If the discovery is unable to determine the device type of a router or switch, the device is listed as "Unknown" in Topology Services. The icon on the topology map has a question mark in it.

To find out if a device is supported, first collect the object ID (OID) of the device:

```
#
snmpget <device> 1.3.6.1.2.1.1.2.0
sysObjectID.0 : 1.3.6.1.4.1.9.5.29
```

If the device is not listed, upgrade your Campus Manager to a later release. The support lists for the Campus Manager versions are posted at Supported Devices.

## Delete A Device From The Map

You can delete a device by right-clicking on it and selecting "Delete Devices". However, because the discovery is automatic, the device reappears on the next discovery. To remove a device, filter its IP address from the discovery by following these steps:

1. Delete the device.
2. Go to **Server Configuration -> Setup -> ANI Server Admin -> Discovery Settings -> Filter Using IP addresses**.
3. Select **Do not discover devices in these ranges**.
4. Enter the IP address of the device.

## The Initial Discovery Takes Longer Than The Subsequent Discoveries

This is normal behavior. During the initial discovery, ANI queries the devices sequentially starting at the seed device. In subsequent discoveries, all the previously discovered devices are treated as seed devices. Because seed devices are queried in parallel, the discovery is a lot faster.

If the initial discovery takes too long, configure multiple devices as seed devices (Server Configuration -> Setup -> ANI Server Admin -> Discovery Settings).

The Discovery Settings are stored in these configuration files:

- /opt/CSCOpX/etc/cwsi/ANIServer.properties
- C:\Program Files\CSCOpX\etc\cwsi\ANIServer.properties

Example:

- Discovery.seed=172.17.246.96:172.17.246.45:172.17.246.7:172.17.246.37

ANI allows you to tune the number of devices the discovery contacts in parallel (Server Configuration -> Setup -> ANI Server Admin -> Performance Settings).

Configuring a high CDP usage causes the ANI server to contact more devices at the same time. The discovery takes less time. However, the ANI server uses more network resources and utilizes more CPU and memory on the server.

## The ANI Discovery Takes Forever

Campus Manager software versions prior to release 3.1 do not support non ASCII characters in the hostname, system contact, or system location (bug ID CSCdr74161).

Special UNICODE characters above the ASCII range such as French, German, and Greek characters cause the ANI database to corrupt and the discovery to hang. To resolve this, either upgrade to Campus 3.1, or remove all non-English characters from the devices and reinitialize the database.

To reinitialize the database in Unix:

```
# /etc/init.d/dmgttd stop #  
/opt/CSCOpX/bin/reinitdb.pl -restore # /etc/init.d/dmgttd start
```

To reinitialize the database in NT or Windows2000:

```
# net  
stop crmdmgttd # perl C:\PROGRA~1\CSCOpX\bin\reinitdb.pl -restore # net start  
crmdmgttd
```

## Troubleshooting UserTracker

### UserTracker Does Not Discover The MAC Addresses

ANI discovers hosts by reading the CAM tables from the discovered switches. If UserTracker does not list some of the hosts in the network, find out where the discovery went wrong.

Select a missing MAC address at random. Use this example to determine where the discovery went wrong:

```
Switch1# show cam dynamic 2/2 VLAN  
Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type] ----  
----- 555  
00-03-32-b8-ed-05 2/2 [ALL] Total Matching CAM Entries Displayed  
=1
```

- **The device discovery is not able to read the device type of the switch the host is connected to.**

ANI only collects the CAM tables from the switches. If ANI is unable to read the device type, or if the device type is not known by ANI, the discovery has no way of knowing if the device is a router or a switch. It does not attempt to read the CAM table.

Check if all the switches in your network are discovered and reachable by ANI. See [Devices Are Not Discovered](#) and [Devices Are In The Unconnected Devices View](#) for more details.

Verify if ANI is able to determine the device type of your switches. See [Devices Have A Question Mark In The Icon](#) for more details.

- **The SNMPagent on the switch does not return the correct information when ANI queries the CAM table through SNMP.**

Verify if the missing MAC address is present in the BRIDGE-MIB on the device.

```
# snmpwalk -c public@555 Switch1
1.3.6.1.2.1.17.4.3.1.1 | grep "00 03 32 b8 ed 05"
dot1dTpFdbAddress.0.3.50.184.237.5 : 00 03 32 b8 ed 05
```

Use the VLAN as community string index to access the BRIDGE-MIB (public@555). If the community string index is not used, the device only returns the CAM table for VLAN1.

If the device does not return the MAC address, you are probably running into a bug in the BRIDGE-MIB code. Try to upgrade the switch to the latest software version.

- **ANI thinks the port that connects the host to the switch is part of the backbone and not an edge port.**

ANI ignores ports that are connected to other switches. ANI only reads the forwarding tables from ports that are directly connected to a host. If a port has a CDP neighbor, the forwarding information for that port is ignored.

First, collect the ifIndex for that port:

```
# snmpwalk Switch1
1.3.6.1.2.1.31.1.1.1.1 | grep 2/2 ifName.20 : 2/2
```

The ifIndex of port 2/2 is 20. The CDP cache for index 20 should not have any CDP neighbors:

```
# snmpwalk Switch1
1.3.6.1.4.1.9.9.23.1.2.1.1.4.20 cdpCacheAddress.20.1 : ac 11 f6
30
```

Here, the port has a CDP neighbor. So the port is ignored.

There is a hub between the switch and the host. Another CDP enabled device is also connected to that hub. To resolve this problem, connect the CDP neighbor to another port.

- **ANI does not discover the VLAN configured on the port.**

Campus Manager releases prior to version 3.1 are unable to read the VLANs on transparent switches. If you run Campus release 3.01 or earlier, make sure that all your switches have a VTP domain configured and are either in VTP server or VTP client mode. Also make sure that at least one of the VTP servers is discovered in Campus.

```
Switch1#
show vtp domain Domain Name Domain Index VTP Version
Local Mode Password -----
----- Cisco 1 2 server - Vlan-count Max-vlan-storage Config Revision
Notifications ----- 19 1023
0 enabled Last Updater V2 Mode Pruning PruneEligible on Vlans -----
----- 172.17.246.45 enabled disabled
2-1000
```

## UserTracker Does Not Discover The IP Addresses

ANI reads the ARP table from the Layer 3 devices it discovered to map the MAC addresses to IP addresses. If UserTracker shows the MAC addresses, and the IP address and hostname fields are empty, chances are that ANI does not discover the default gateway of the host correctly.

Note the default gateway configured on the host:

```
# ipconfig # more
/etc/defaultrouter
```

- **The device discovery is not able to read the device type of the default gateway.**

ANI only collects the ARP tables from the routers that are discovered. The ARP tables on the switches are ignored. If ANI is unable to read the device type or if the device type is not known by ANI, the discovery has no way of knowing if the device is a router or a switch. It does not read the ARP table.

Check if the default gateway is discovered and reachable by ANI. See [Devices Are Not Discovered](#) and [Devices Are In The Unconnected Devices View](#) for more details.

Verify if ANI is able to determine the device type of the default gateway. See [Devices Have A Question Mark In The Icon](#) for more details.

- **The ARP cache entry for the host times out.**

ANI performs ping sweeps on the subnets that are discovered before it reads the ARP table to make sure the ARP cache is fresh.

Verify that the ping sweep option is enabled if you suspect the ARP entries time out (User Tracker -> Edit -> Preferences -> Discovery -> Ping Sweep).

- **The SNMPagent on the default gateway does not return the correct information when ANI queries the ARP table through SNMP.**

Make sure the missing IP address is present in the RFC1213-MIB on the device.

```
# snmpwalk <device>
1.3.6.1.2.1.4.22.1.2 | grep 172.17.246.187
ipNetToMediaPhysAddress.7.172.17.246.187 : 00 c0 4f 95 af 1e
```

If the device does not return the MAC address to IP address mapping, you are probably running into a bug in the SNMP code. Try to upgrade the router to the latest software version.

## UserTracker Does Not Discover The Hostnames

The discovery makes a system call to the server to resolve the IP addresses to hostnames.

Make sure that the CiscoWorks2000 does a reverse name resolution of the IP address:

```
CW2000Server#
nslookup 172.17.246.105 Server: ns.cisco.com
Address: 172.17.246.224 Name: host1.cisco.com Address: 172.17.246.105
```

## UserTracker Does Not Discover The Phone Extensions

ANI collects the phone extensions by sending an SNMP request to the Cisco CallManagers that are discovered. The ANI discovery does not contact the IP phones directly.

- **The MAC addresses of the IP phones are not discovered.**

The same troubleshooting tips apply to IP phones as for hosts. See [Usertracker does not discover the MAC addresses](#) for more information.

- **ANI is unable to resolve the IP address of the IP phones.**

The same troubleshooting tips apply to IP phones as for hosts. See Usertracker does not discover the IP addresses for more information.

- **ANI is unable to discover the CallManagers in the network.**

ANI discovers Cisco CallManager in the same way as other Cisco devices are discovered. Make sure that the CallManagers send CDP packets. Verify that the neighboring devices see the CallManager.

Check if all the CallManagers in your network are discovered and reachable by ANI. See Devices Are Not Discovered and Devices are in the Unconnected Devices View for more info.

Verify if ANI is able to determine that the device is a CallManager. See Devices Have A Question Mark In The Icon for more information.

- **The SNMPagent on the CallManager does not return the correct information when ANI queries the CCM-MIB.**

Test if you are able to manually poll the extension table:

```
#  
snmpwalk <callmanager> 1.3.6.1.4.1.9.9.156.1.2.2.1.2 | grep  
2005 ccmPhoneExtension.999 : 2005
```

If the device does not return the extensions, try to upgrade the CallManager to the latest software version.

## UserTracker Is Not Discovering The Usernames On Windows Clients

Before ANI discovers the user account that is logged into the Windows client, you need to configure and run the UTLiteNT.bat on the client machine. See Discover User Names for more information on how to configure the UTLiteNT.bat script.

- **The UTLite.exe does not run on the windows clients.**

Open Task Manager. Verify that the UTLite.exe process still runs on the client. If it does not run , check the login script on your domain controller (User Manager for Domains -> Select the user -> Profile -> Logon Script Name). The logon script should contain a line that executes the UTLiteNT.bat script.

- **The windows clients send the UTLite packets, but the CiscoWorks2000 server does not receive them.**

By default, UTLite sends the user information to port 16236 on the CiscoWorks2000 server. Make sure that this port is not blocked by an access list or firewall between the windows client and the CiscoWorks2000 server.

## UserTracker Is Not Discovering The Usernames On Unix Clients

ANI uses the **rusers** command to discover the users on Unix hosts. If the UserName fields are empty for the Unix hosts, try to run the **rusers** command manually:

```
# rusers host1 host1 root
```

See Discover User Names for more information on how to configure the rusersd daemon.

## UserTracker Is Discovering Duplicate MAC Addresses

- **UserTracker lists duplicate MAC addresses because hosts have moved.**

UserTracker keeps historical data about the hosts that are discovered. By default, a discovered host remains in the database forever. If a host moves from one port to another, the host has two entries in UserTracker. Find out which entry is the old one and which is the new one by looking at the LastSeen field.

**Note:** The LastSeen field is only supported in Campus Manager version 3.1. Results are unpredictable in versions earlier than this release. Remove old entries from the UserTracking database manually:

1. Select **UserTracker** -> **Edit** -> **Preferences** -> **Delete**.
2. Select a timeout value.
3. Click the **Delete now** button.

Configure UserTracker to delete old entries automatically:

1. Select **UserTracker** -> **Edit** -> **Preferences** -> **Delete**.
2. Select a timeout value.
3. Enable the **Delete after every discovery** option.

- **UserTracker lists duplicate MAC addresses because the topology is not discovered correctly.**

ANI discovers hosts by reading the CAM tables from the discovered switches. Because packets get forwarded and flooded over the Layer 2 network, multiple switches learn the MAC address of a host.

To avoid duplicate MAC address entries, ANI ignores ports that are connected to other switches. ANI only reads the forwarding tables from ports that are directly connected to a host. ANI finds these end-user ports by looking for CDP neighbors on the ports.

If a port has a CDP neighbor, the forwarding information for that port is ignored. If there are no CDP neighbors, the CAM table for that port goes into the UserTracking database.

If you see a lot of duplicate MAC addresses in UserTracker, chances are that ANI has mistakenly discovered one of your trunk or backbone links as an edge port. In other words, ANI thinks the MAC addresses in the CAM table of the backbone interface are directly connected to the interface through a hub. To resolve this, note the Device and Port that are listed in UserTracker for each duplicate MAC address. Verify the CDP neighbors on that device.

```
# show cdp neighbor  
<mod>/<port> No entry found.
```

See Devices Are Not Discovered for more information on how to troubleshoot CDP.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Network Management
Network Infrastructure: Network Management
Virtual Private Networks: Network and Policy Management

---

## Related Information

- [CiscoWorks Campus Manager](#)
  - [Technical Support – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 17, 2006

Document ID: 7948

---