APPENDIX B

Troubleshooting Connectivity Problems Using Campus Manager Applications

A common network problem is loss of IP connectivity between two end points (A and B). Table B-1 shows the Campus Manager tools to use to verify and localize this type of problem. The steps listed are not exhaustive; other steps might be required to further identify and troubleshoot the failure. However, the table does take you through a process of investigation using Campus Manager tools.

Table B-1 Troubleshooting Using Campus Manager Applications

	Action	Menu Sequence	Result	Next Step
Step 1	Make sure the ANI server has the most current network information.	1. Select **Campus Manager > Topology Services**. 2. Check the status bar for the last discovery date and time.	If there have been no network changes since the last discovery, you can proceed. If you believe there have been changes to the network since the last discovery cycle, do a rediscovery of the network.	Step 2 Locate the affected end-user host in the network.
Step 2	Locate the affected end-user host in the network.	1. Select **Campus Manager > User Tracking** 2. Select **Query > Show All** or **Simple Query**.	Obtain IP addresses of end-user hosts.	Step 3 Check for duplicate MAC addresses.
Step 3	Check for duplicate MAC addresses.	1. Select **Campus Manager > User Tracking**. 2. Select **Reports > Duplicate MAC**.	If a duplicate MAC address exists, User Tracking reports the offending end-user hosts. Investigate further.	Step 4 Check for duplicate IP addresses.
Step 4	Check for duplicate IP addresses.	1. Select **Campus Manager > User Tracking**. 2. Select **Reports > Duplicate IP**.	If a duplicate IP address exists, User Tracking reports the offending end-user hosts. Investigate further.	Step 5 Run a path trace from end-user host A (source) to end-user host B (destination).

Table B-1 Troubleshooting Using Campus Manager Applications (continued)

	Action	Menu Sequence	Result	Next Step
Step 5	Run a path trace from end-user host A (source) to end-user host B (destination).	1. Select **Campus Manager > Path Analysis**. 2. Enter the IP address of end-user host A in the **From** field and the IP address of end-user host B in the **To** field. 3. Select **Action > Start Trace.**	No trace or "Could not reach source" error on status line could indicate that the problem is related to IP connectivity at end-user host A (source).	Step 6 Run a reverse path trace from end-user host B (source) to end-user host A (destination).
			Partial trace helps you localize the problem.	Step 8 Highlight trace in Topology view.
			A successful trace indicates that there is probably not an IP connectivity problem. This might suggest a different problem, perhaps at the application layer.	Step 14 Check firewall and filter configuration on each potentially affected device. or Step 15 Check servers and applications.

Table B-1 Troubleshooting Using Campus Manager Applications (continued)

	Action	Menu Sequence	Result	Next Step
Step 6	Run a reverse path trace from end-user host B (source) to end-user host A (destination).	1. Select **Campus Manager > Path Analysis**. 2. Enter the IP address of end-user host B in the **From** field and the IP address of end-user host A in the **To** field. 3. Select **Action > Start Trace**.	If the reverse trace is also unsuccessful or a "Could not reach source" error displays on the status line, there might be a problem between the CiscoWorks2000 server and the end-user hosts that is preventing Path Analysis from performing the trace between end-user hosts A and B.	Step 7 Run a path trace between the CiscoWorks 2000 server and both end-user hosts.
			If the reverse trace provides a partial trace, this information helps you localize the problem.	Step 8 Highlight trace in Topology view.
Step 7	Run a path trace between the CiscoWorks 2000 server and both end-user hosts.	1. Select **Campus Manager > Path Analysis**. 2. Enter the IP address of the CiscoWorks2000 server in the **From** field and the IP address of end-point A in the **To** field. 3. Select **Action > Start Trace**. 4. Enter IP address of the CiscoWorks2000 server in the **From** field and the IP address of end-point B in the **To** field.	An unsuccessful or partial trace might indicate that there is a connectivity problem related to the subnet where the CiscoWorks2000 server resides. A successful path trace might indicate that you are able to reach both end points independently, but the end points cannot communicate with each other.	Diagnose and correct the problem; then continue localizing the original problem with Step 5.

Table B-1 Troubleshooting Using Campus Manager Applications (continued)

	Action	Menu Sequence	Result	Next Step
Step 8	Highlight trace in Topology view.	1. From Campus Manager, select **Topology Services**. 2. Return to the Path Analysis window where the result of the trace you just performed is displayed. 3. Select **Action > Highlight Path in Network View**.	Locate the highlighted path, and check for possible signs of failure, for example a red link. This could indicate a port failure (bad NIC or MAU), loose connector, or bad cable.	If none of these are the cause, do one of the following: • Step 9 Investigate link attributes. • Step 10 Investigate port attributes.
Step 9	Investigate link attributes.	1. Select affected link. 2. Select **Reports > Link Attributes**.	Check the following fields for information: • Type. The port could be configured as the wrong media type. • Speed. The port could be set to a different speed than the port on the other side of the link. • Mode. The port could be set to a different duplex mode than the port on the other side of the link.	Step 10 Investigate port attributes.

Table B-1 Troubleshooting Using Campus Manager Applications (continued)

	Action	Menu Sequence	Result	Next Step
Step 10	Investigate port attributes.	1. Select affected device. 2. Select **Reports > Port Attributes**.	Check the following fields for information: • AdminStatus. The port could have been brought down administratively. • IsTrunk. The port could be incorrectly configured as a trunk port or not configured for the required VLAN. • Speed. The port could be set to a different speed than the port on the other side of the link. • Duplex Mode. The port could be set to a different duplex mode than the port on the other side of the link. • Protocols Enabled. The port could be configured pass incorrect protocols. (Applies to MLS devices only.) • Protocols Seen. The port could be filtering out required protocols. Compare with protocols enabled. (Applies to MLS devices only.) • Port type misconfiguration. • Incorrect protocol configuration (missing necessary protocol).	Step 11 Check physical discrepancies in Topology Services

Table B-1 Troubleshooting Using Campus Manager Applications (continued)

	Action	Menu Sequence	Result	Next Step
Step 11	Check physical discrepancies in Topology Services	1. From Campus Manager, select **Topology Services**. 2. Click **Network Views**. 3. Select **Reports > Discrepancie**s.	Check for physical discrepancies, such as link, duplex, and speed mismatch and trunk/non-trunk mismatch.	Step 12 Check logical discrepancies in Topology Services.
Step 12	Check logical discrepancies in Topology Services.	1. From Campus Manager, select **Topology Services**. 2. Click **Managed Domains**. 3. Select **Reports > Discrepancie**s.	Check for logical discrepancies, such as VLAN and VTP inconsistencies or ATM network misconfiguration.	Step 13 Use CiscoView (or telnet) to reach suspect devices and investigate further.
Step 13	Use CiscoView (or telnet) to reach suspect devices and investigate further.	1. Select **Campus Manager > Topology Services**. 2. Select desired view and select **View > Display View**. 3. Select the affected device. 4. Right click and select **CiscoView** or **Telnet**.	Variable.	Step 14 Check firewall and filter configuration on each potentially affected device.

Table B-1 Troubleshooting Using Campus Manager Applications (continued)

	Action	Menu Sequence	Result	Next Step
Step 14	Check firewall and filter configuration on each potentially affected device.	1. Select **Campus Manager > Topology Services**. 2. Select desired view and select **View > Display View**. 3. Select the affected device. 4. Right click and select **Telnet**.	Firewall or filter could be blocking traffic that needs to pass through.	Step 15 Check servers and applications.
Step 15	Check servers and applications.	None.	Variable.	Variable.