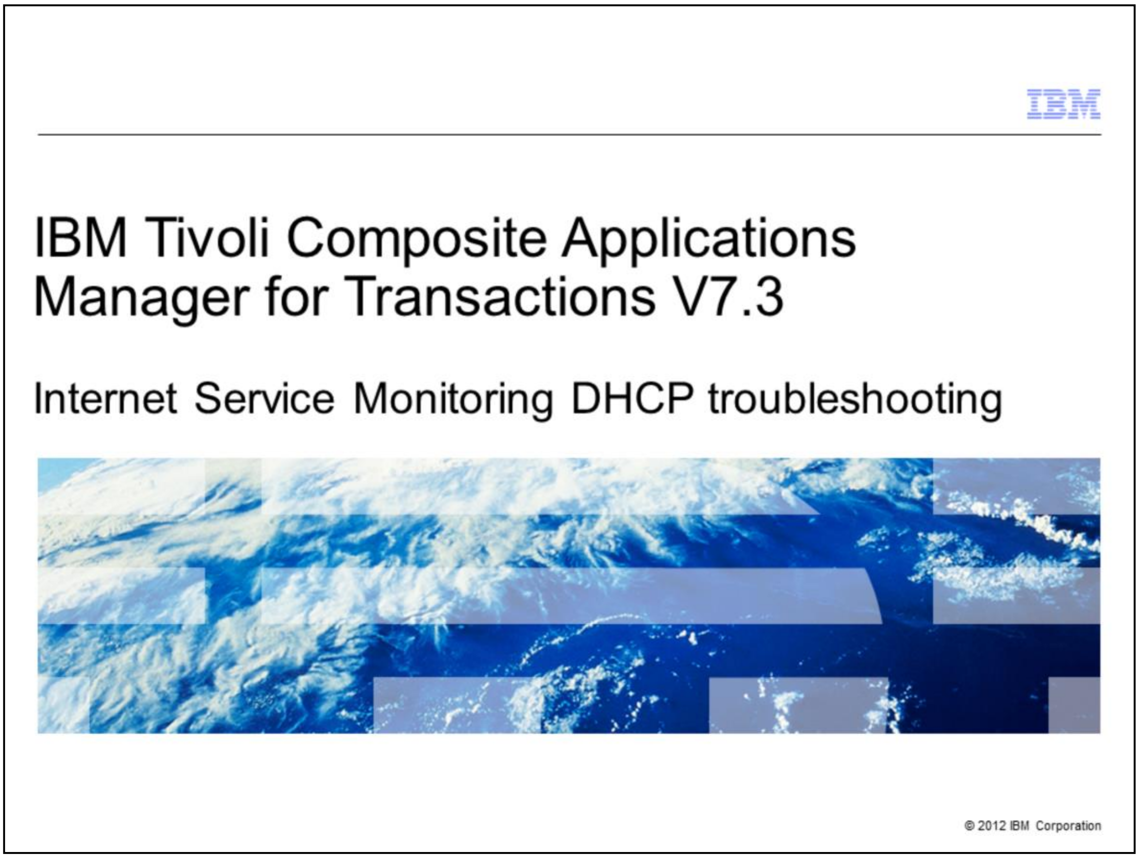
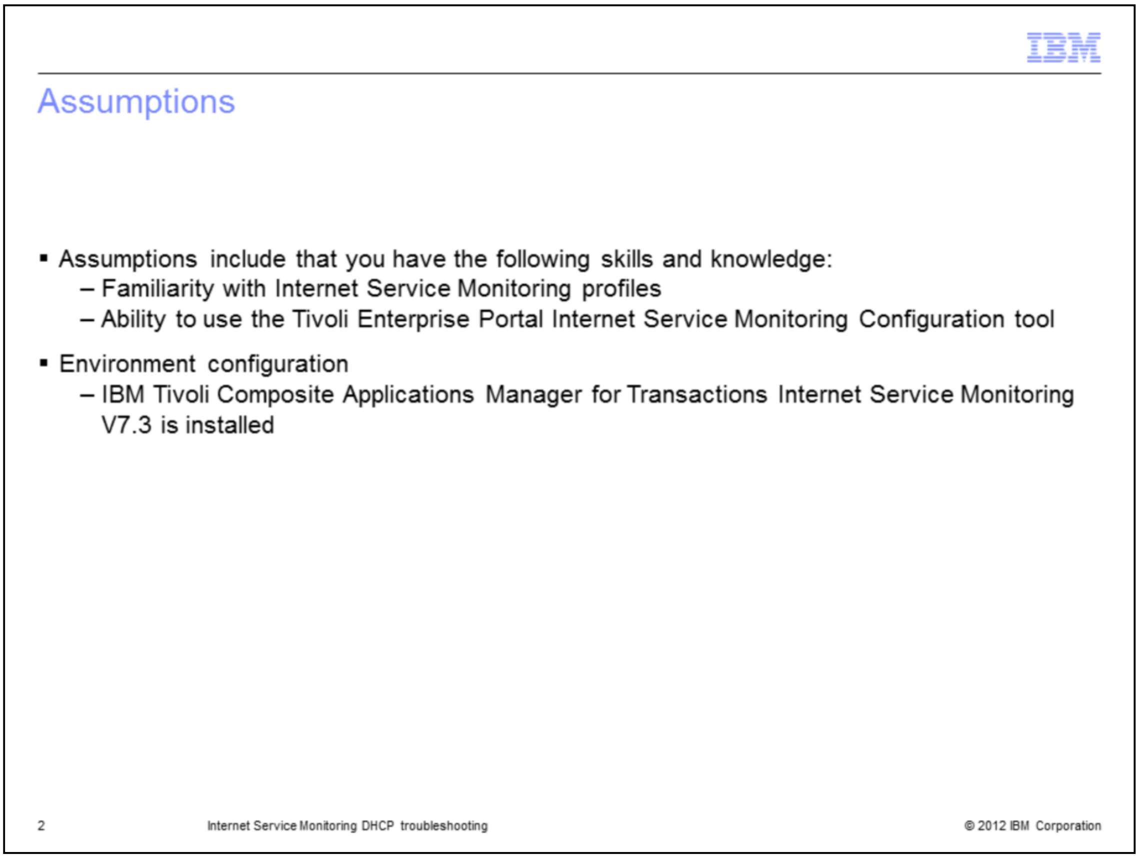


IBM Tivoli Composite Applications Manager for Transactions V7.3

Internet Service Monitoring DHCP troubleshooting

IBM Tivoli Composite Applications Manager for Transactions V7.3, Internet Service Monitoring Dynamic Host Configuration Protocol (DHCP) configuration and troubleshooting.

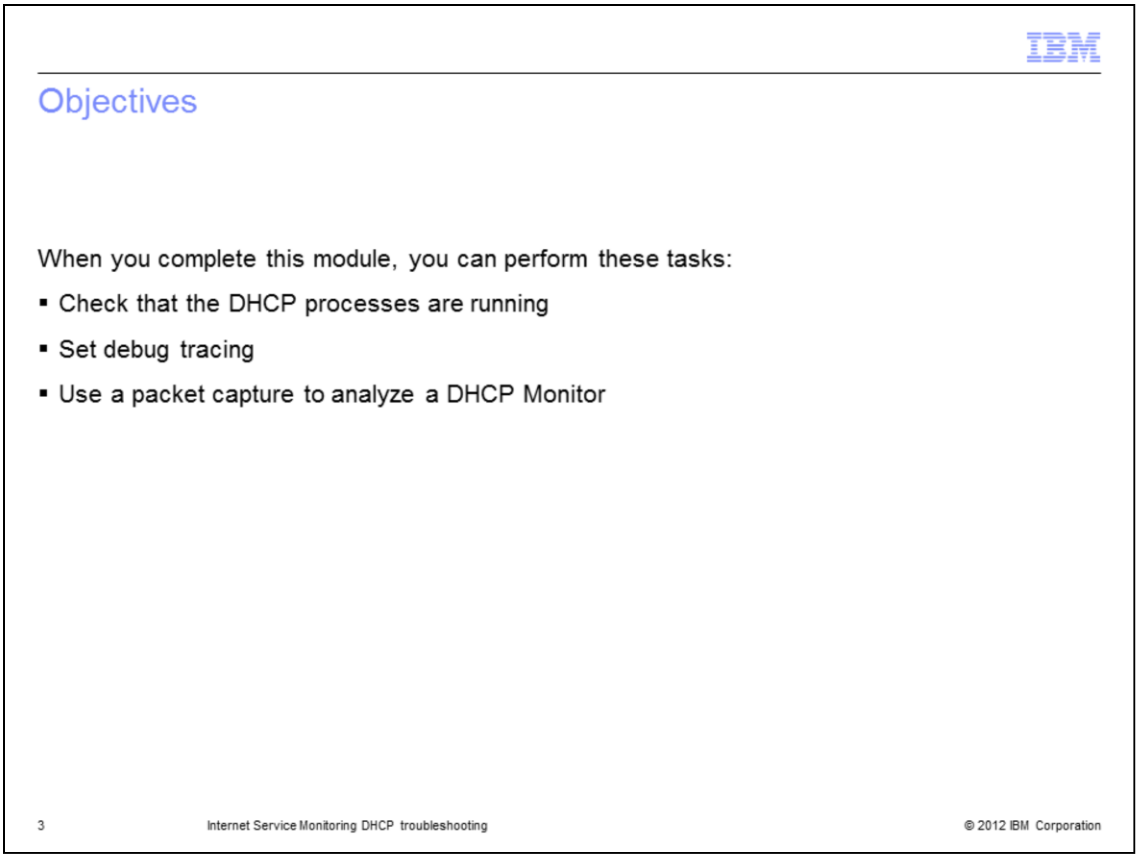


Assumptions

- Assumptions include that you have the following skills and knowledge:
  - Familiarity with Internet Service Monitoring profiles
  - Ability to use the Tivoli Enterprise Portal Internet Service Monitoring Configuration tool
- Environment configuration
  - IBM Tivoli Composite Applications Manager for Transactions Internet Service Monitoring V7.3 is installed

2 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

The developer assumes that you are familiar with Internet Service Monitoring configuration and that you completed IBM Tivoli Composite Applications Manager for Transactions Internet Service Monitoring installation.

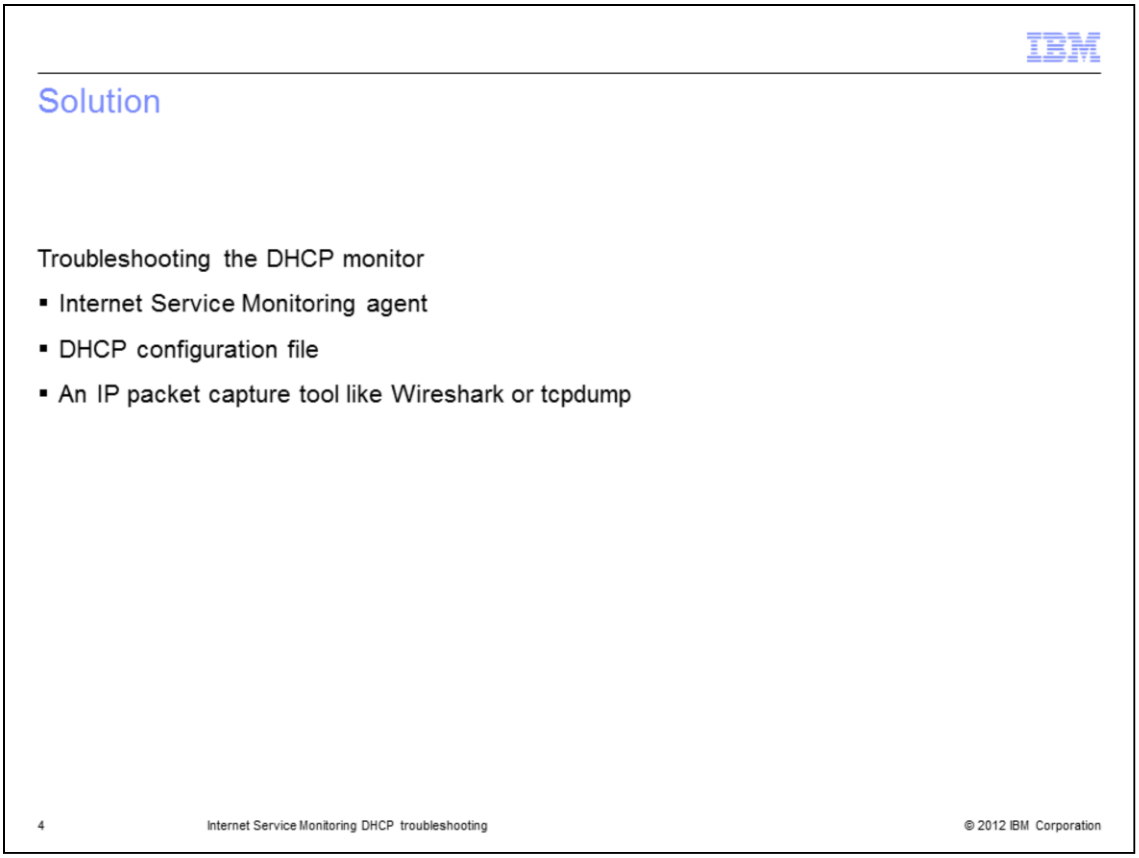


Objectives

When you complete this module, you can perform these tasks:

- Check that the DHCP processes are running
- Set debug tracing
- Use a packet capture to analyze a DHCP Monitor

When you complete this module, you can troubleshoot problems with the DHCP monitor in the IBM Tivoli Composite Applications Manager for Transactions Internet Service Monitoring agent. You can check that the required processes are running, set debug tracing, and analyze a packet capture.

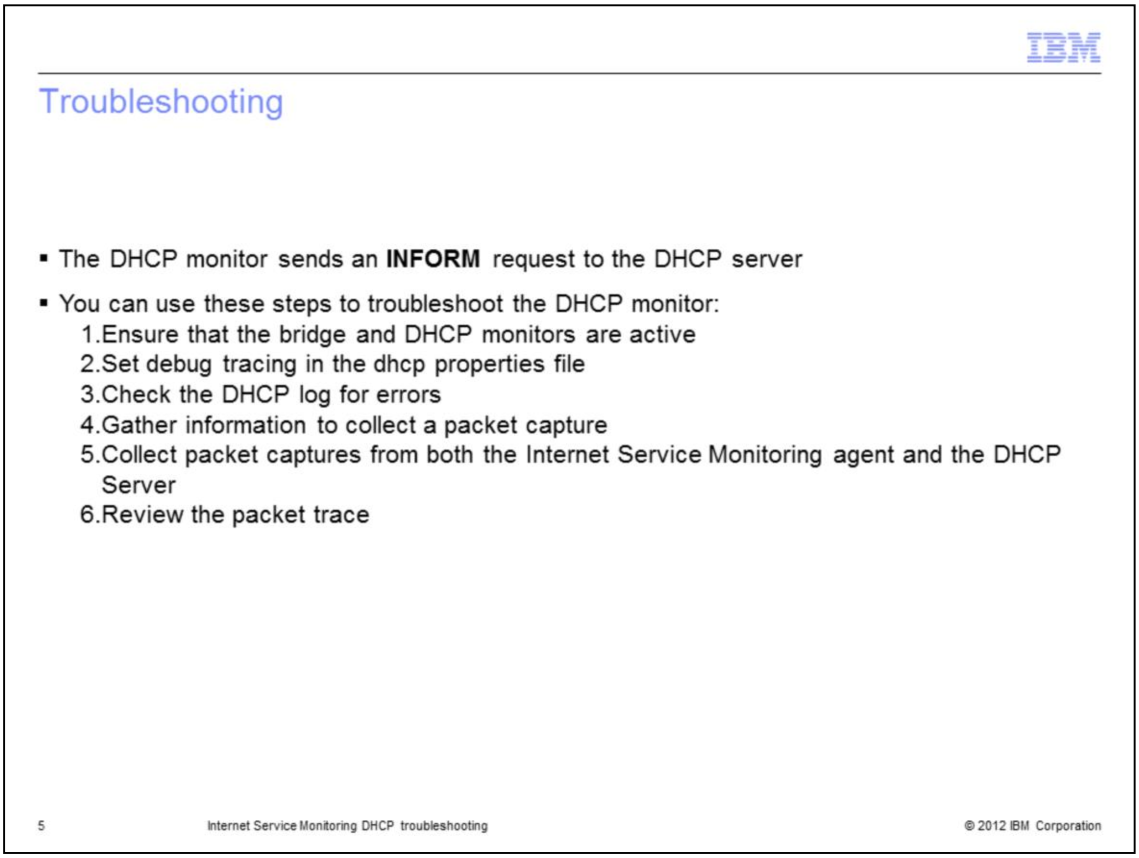


Solution

Troubleshooting the DHCP monitor

- Internet Service Monitoring agent
- DHCP configuration file
- An IP packet capture tool like Wireshark or tcpdump

There are several steps in troubleshooting the DHCP monitor. Troubleshooting uses the Internet Service Monitoring agent, the DHCP configuration file, and an IP packet capture tool like Wireshark or tcpdump.



Troubleshooting

- The DHCP monitor sends an **INFORM** request to the DHCP server
- You can use these steps to troubleshoot the DHCP monitor:
  1. Ensure that the bridge and DHCP monitors are active
  2. Set debug tracing in the dhcp properties file
  3. Check the DHCP log for errors
  4. Gather information to collect a packet capture
  5. Collect packet captures from both the Internet Service Monitoring agent and the DHCP Server
  6. Review the packet trace

5 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

The DHCP monitor functions by sending an INFORM request to the DHCP server. This list contains the six steps to troubleshoot the DHCP monitor:

1. Ensure that the bridge and DHCP monitors are active.

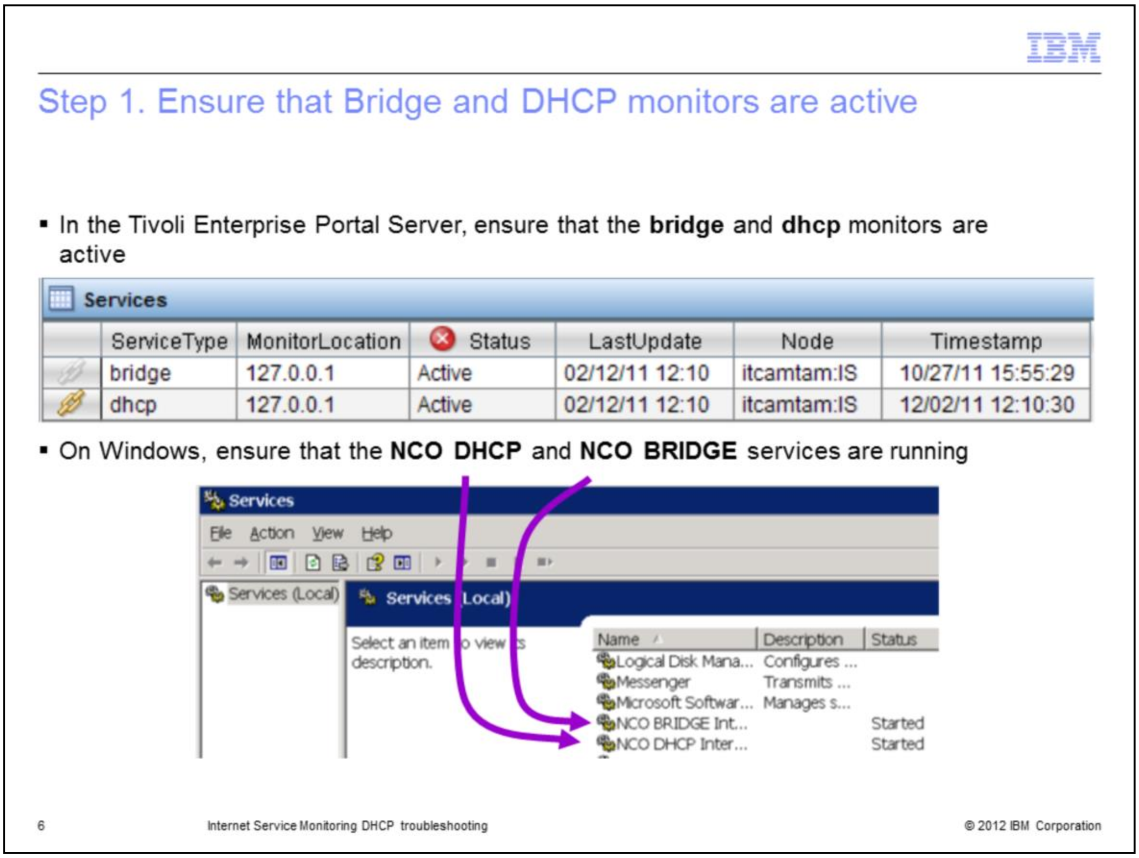
2. Set debug tracing in the dhcp properties file.

3. Check the DHCP log for errors.

4. Gather information to collect a packet capture.

5. Collect packet captures from both the Internet Service Monitoring agent and the DHCP Server.

6. Review the packet trace.



Step 1. Ensure that Bridge and DHCP monitors are active

- In the Tivoli Enterprise Portal Server, ensure that the **bridge** and **dhcp** monitors are active

Services

	ServiceType	MonitorLocation	Status	LastUpdate	Node	Timestamp
	bridge	127.0.0.1	Active	02/12/11 12:10	itcamtam:IS	10/27/11 15:55:29
	dhcp	127.0.0.1	Active	02/12/11 12:10	itcamtam:IS	12/02/11 12:10:30

- On Windows, ensure that the **NCO DHCP** and **NCO BRIDGE** services are running

Name	Description	Status
Logical Disk Mana...	Configures ...	
Messenger	Transmits ...	
Microsoft Softwar...	Manages s...	
NCO BRIDGE Int...		Started
NCO DHCP Inter...		Started

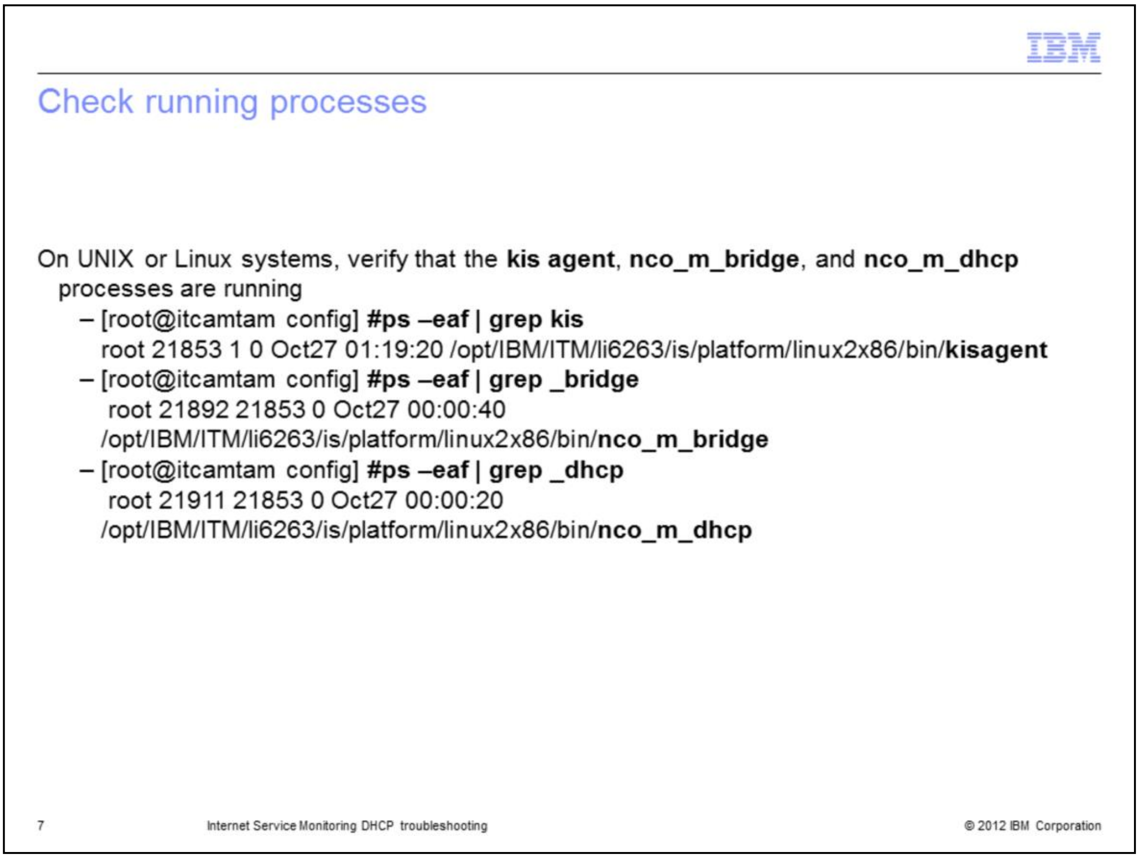
6 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

Step 1. Ensure that the monitors are active with the appropriate method for your system.

Use a Tivoli Enterprise Portal Server to navigate to **Internet Service Monitor > Monitor Status**, and ensure that the bridge and DHCP monitors are active as shown in the image.

For a Windows system, ensure that the same services are running by viewing the Services window as shown in the screen capture.

For Windows XP, to access Services, click **Start > Control Panel**. Then, on the Control Panel window, click **Administrative Tools > Services**.



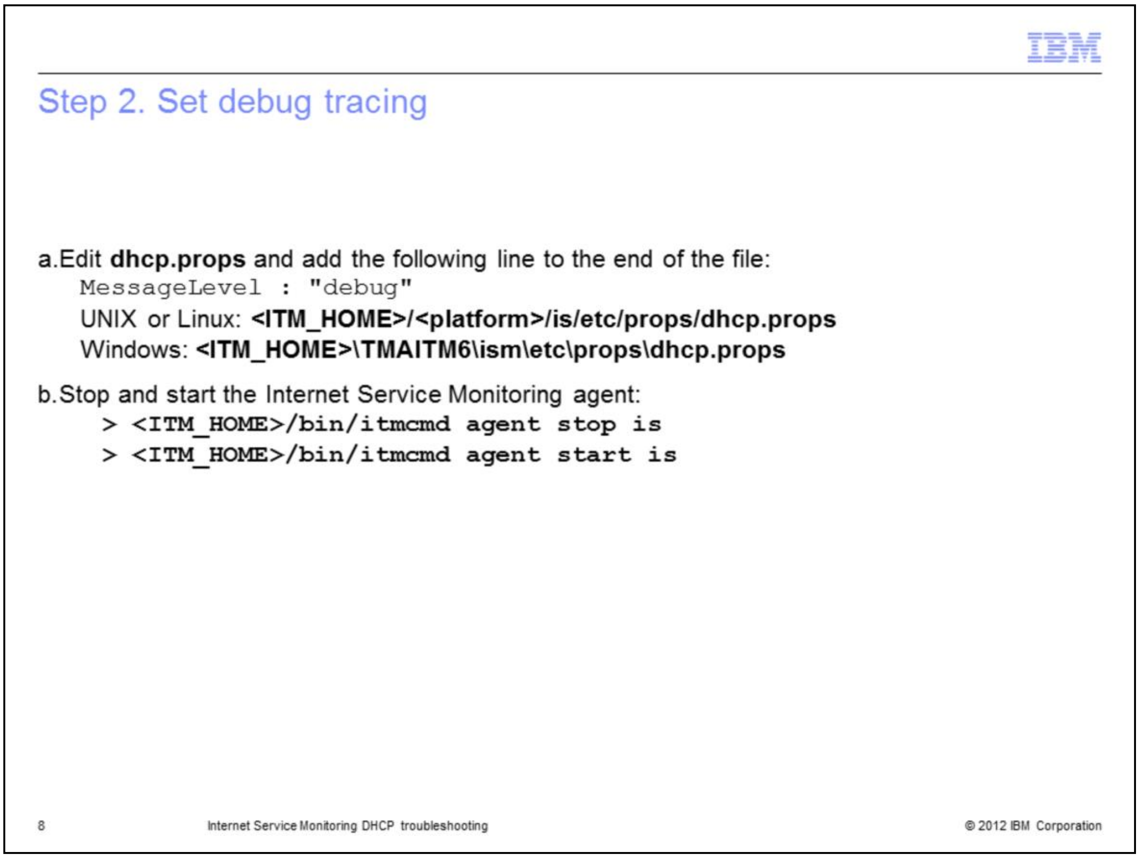
Check running processes

On UNIX or Linux systems, verify that the **kis agent**, **nco_m_bridge**, and **nco_m_dhcp** processes are running

- [root@itcamtam config] **#ps –eaf | grep kis**
  root 21853 1 0 Oct27 01:19:20 /opt/IBM/ITM/li6263/is/platform/linux2x86/bin/**kisagent**
- [root@itcamtam config] **#ps –eaf | grep _bridge**
  root 21892 21853 0 Oct27 00:00:40
  /opt/IBM/ITM/li6263/is/platform/linux2x86/bin/**nco_m_bridge**
- [root@itcamtam config] **#ps –eaf | grep _dhcp**
  root 21911 21853 0 Oct27 00:00:20
  /opt/IBM/ITM/li6263/is/platform/linux2x86/bin/**nco_m_dhcp**

7 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

On UNIX or Linux systems, verify that the **kisagent**, **nco_m_bridge**, and **nco_m_dhcp** processes are running with the command **ps -eaf | grep <*process*>** as shown. Each process should be running.



Step 2. Set debug tracing

a. Edit **dhcp.props** and add the following line to the end of the file:

```
MessageLevel : "debug"
```

UNIX or Linux: **<ITM_HOME>/<platform>/is/etc/props/dhcp.props**

Windows: **<ITM_HOME>\TMAITM6\ism\etc\props\dhcp.props**

b. Stop and start the Internet Service Monitoring agent:

```
> <ITM_HOME>/bin/itmcmd agent stop is
> <ITM_HOME>/bin/itmcmd agent start is
```

8 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

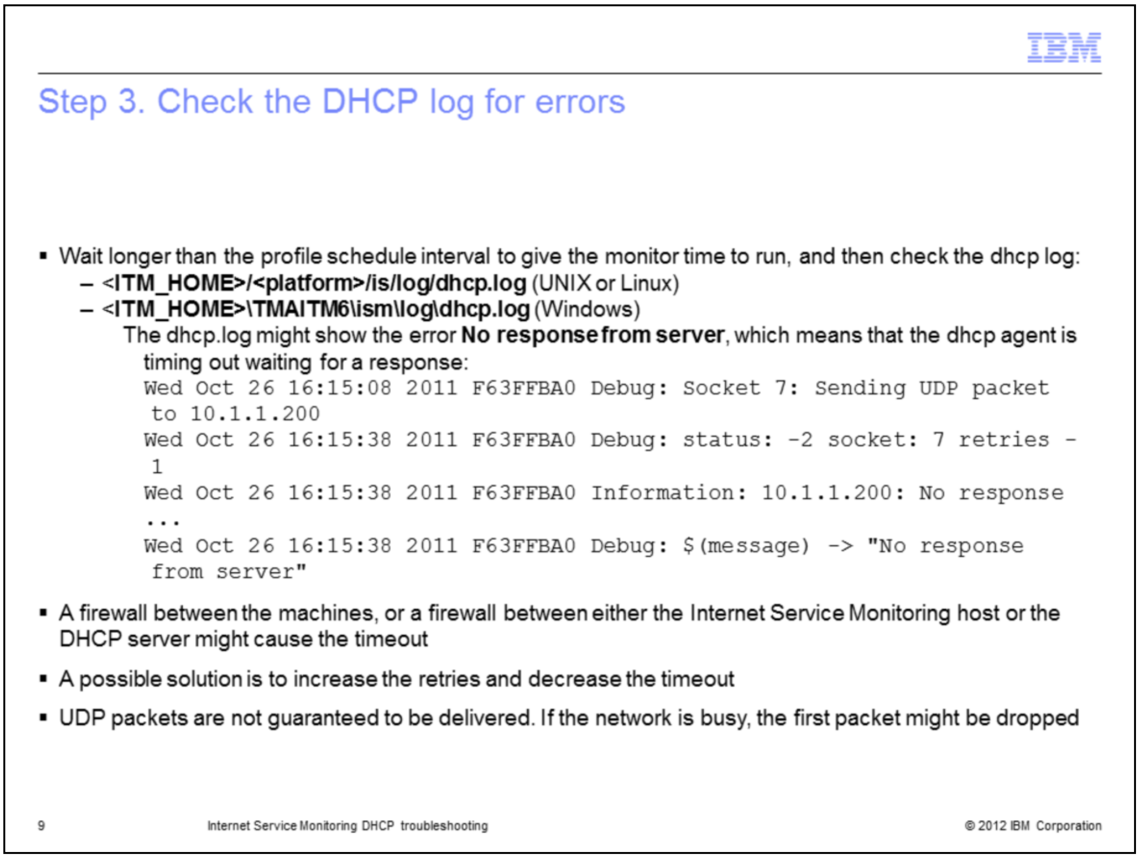
Step 2. To set debug tracing, you must perform a couple of tasks.

a. Edit the **dhcp.props** file by adding this line to the end of the file:

MessageLevel : "debug"

Use the directory indicated on the slide for your system type.

b. Stop and start the Internet Service Monitoring agent with the commands shown. When the agent starts, it picks up the new parameter.



Step 3. Check the DHCP log for errors

- Wait longer than the profile schedule interval to give the monitor time to run, and then check the dhcp log:
  - <**ITM_HOME>/<platform>/is/log/dhcp.log** (UNIX or Linux)
  - <**ITM_HOME>\TMAITM6\ism\log\dhcp.log** (Windows)

  The dhcp.log might show the error **No response from server**, which means that the dhcp agent is timing out waiting for a response:

```
Wed Oct 26 16:15:08 2011 F63FFBA0 Debug: Socket 7: Sending UDP packet
 to 10.1.1.200
Wed Oct 26 16:15:38 2011 F63FFBA0 Debug: status: -2 socket: 7 retries -
 1
Wed Oct 26 16:15:38 2011 F63FFBA0 Information: 10.1.1.200: No response
...
Wed Oct 26 16:15:38 2011 F63FFBA0 Debug: $(message) -> "No response
 from server"
```

- A firewall between the machines, or a firewall between either the Internet Service Monitoring host or the DHCP server might cause the timeout
- A possible solution is to increase the retries and decrease the timeout
- UDP packets are not guaranteed to be delivered. If the network is busy, the first packet might be dropped

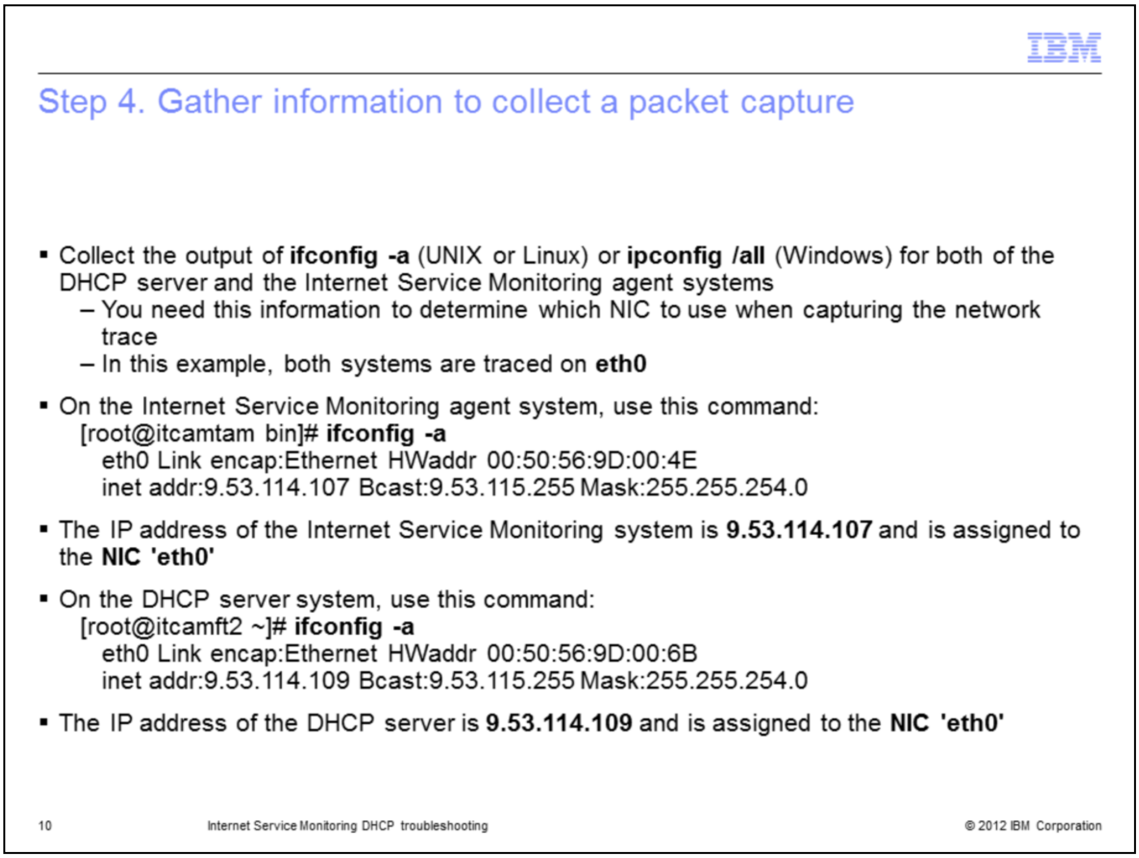
Step 3. Check the DHCP log for errors.

Before you check the DHCP log for data, wait for the monitors to run.

Check the profile that is used to run the DHCP monitor to see how often the monitor is scheduled to run. Wait long enough for the schedule period to expire.

The **dhcp.log** file might show the error **No response from server**. This error means that the dhcp agent is timing out while waiting for a response. The slide shows a sample of this type of error.

A firewall between the machines, or on either the Internet Service Monitoring host or the DHCP server can cause this error. A possible solution is to increase the retries and decrease the timeout. UDP packets are not guaranteed to be delivered. If the network is busy, the first packet might be dropped.



Step 4. Gather information to collect a packet capture

- Collect the output of **ifconfig -a** (UNIX or Linux) or **ipconfig /all** (Windows) for both of the DHCP server and the Internet Service Monitoring agent systems
  - You need this information to determine which NIC to use when capturing the network trace
  - In this example, both systems are traced on **eth0**
- On the Internet Service Monitoring agent system, use this command:

```
[root@itcamtam bin]# ifconfig -a
  eth0 Link encap:Ethernet HWaddr 00:50:56:9D:00:4E
  inet addr:9.53.114.107 Bcast:9.53.115.255 Mask:255.255.254.0
```

- The IP address of the Internet Service Monitoring system is **9.53.114.107** and is assigned to the **NIC 'eth0'**
- On the DHCP server system, use this command:

```
[root@itcamft2 ~]# ifconfig -a
  eth0 Link encap:Ethernet HWaddr 00:50:56:9D:00:6B
  inet addr:9.53.114.109 Bcast:9.53.115.255 Mask:255.255.254.0
```

- The IP address of the DHCP server is **9.53.114.109** and is assigned to the **NIC 'eth0'**

10 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

Step four is to collect a packet trace from the Internet Service Monitoring agent system and the DHCP server system.

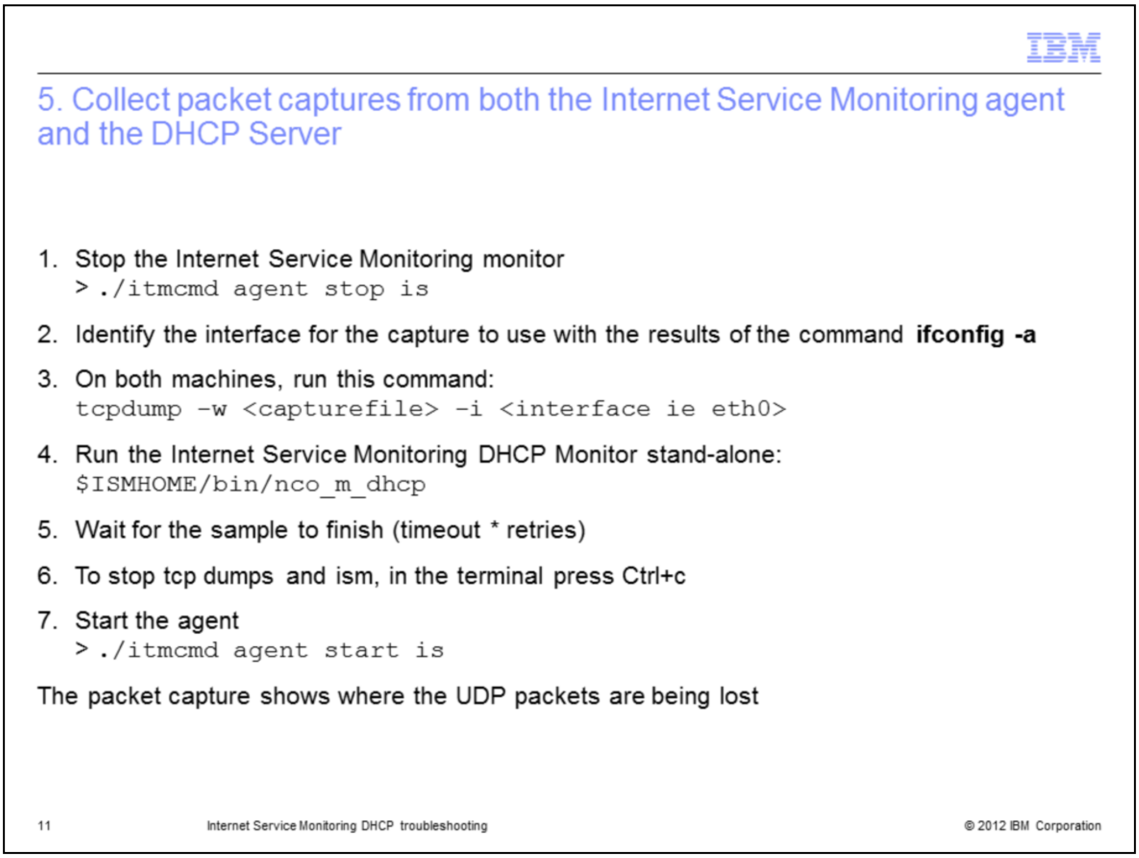
Run the correct command for your system to collect the configuration output for both the DHCP server and the Internet Service Monitoring agent systems.

For UNIX or Linux systems, use the command **ifconfig -a**.

For Windows systems, use the command **ipconfig /all**.

The example is for a UNIX system.

Collect packet captures from both the Internet Service Monitoring agent and the DHCP Server.

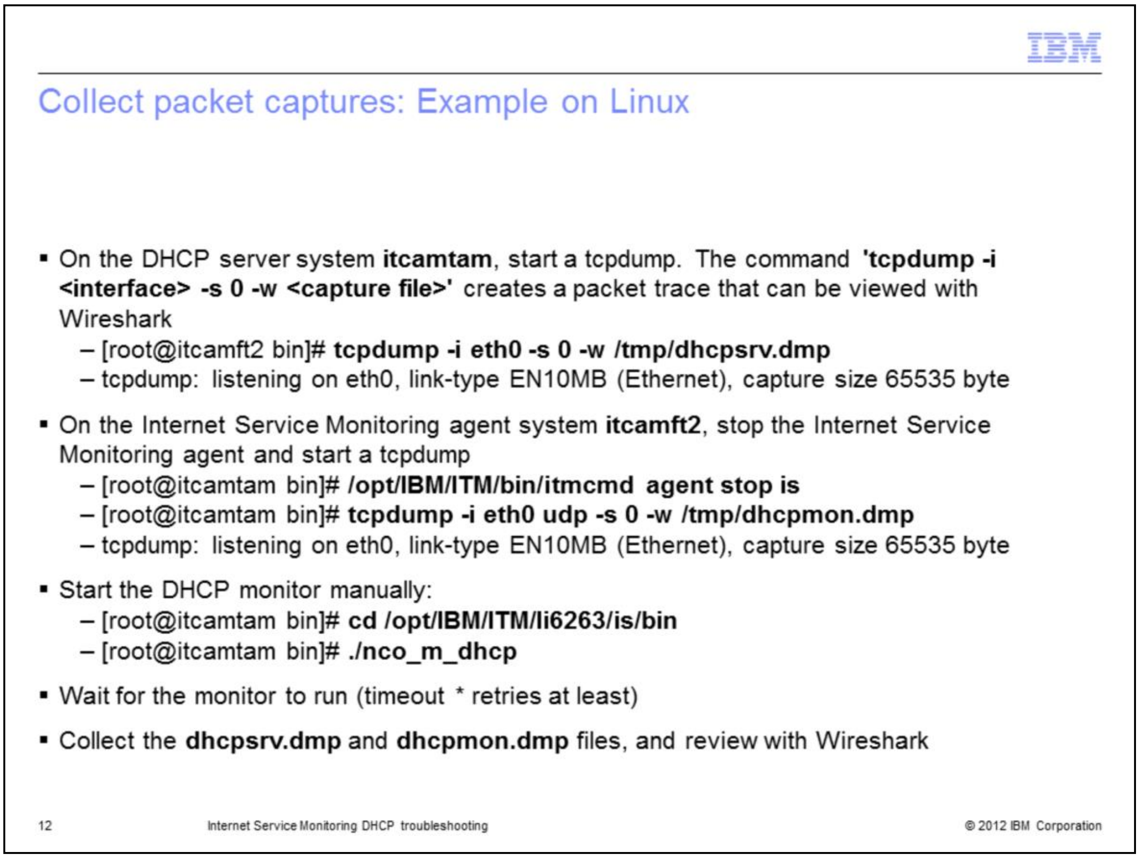


5. Collect packet captures from both the Internet Service Monitoring agent and the DHCP Server

1. Stop the Internet Service Monitoring monitor
   ```
   > ./itmcmd agent stop is
   ```
2. Identify the interface for the capture to use with the results of the command **ifconfig -a**
3. On both machines, run this command:
   ```
   tcpdump -w <capturefile> -i <interface ie eth0>
   ```
4. Run the Internet Service Monitoring DHCP Monitor stand-alone:
   ```
   $ISMHOME/bin/nco_m_dhcp
   ```
5. Wait for the sample to finish (timeout * retries)
6. To stop tcp dumps and ism, in the terminal press Ctrl+c
7. Start the agent
   ```
   > ./itmcmd agent start is
   ```

The packet capture shows where the UDP packets are being lost

After you determine which network adapter the DHCP uses, get a packet capture on both the Internet Service Monitoring agent system and the DHCP server system.



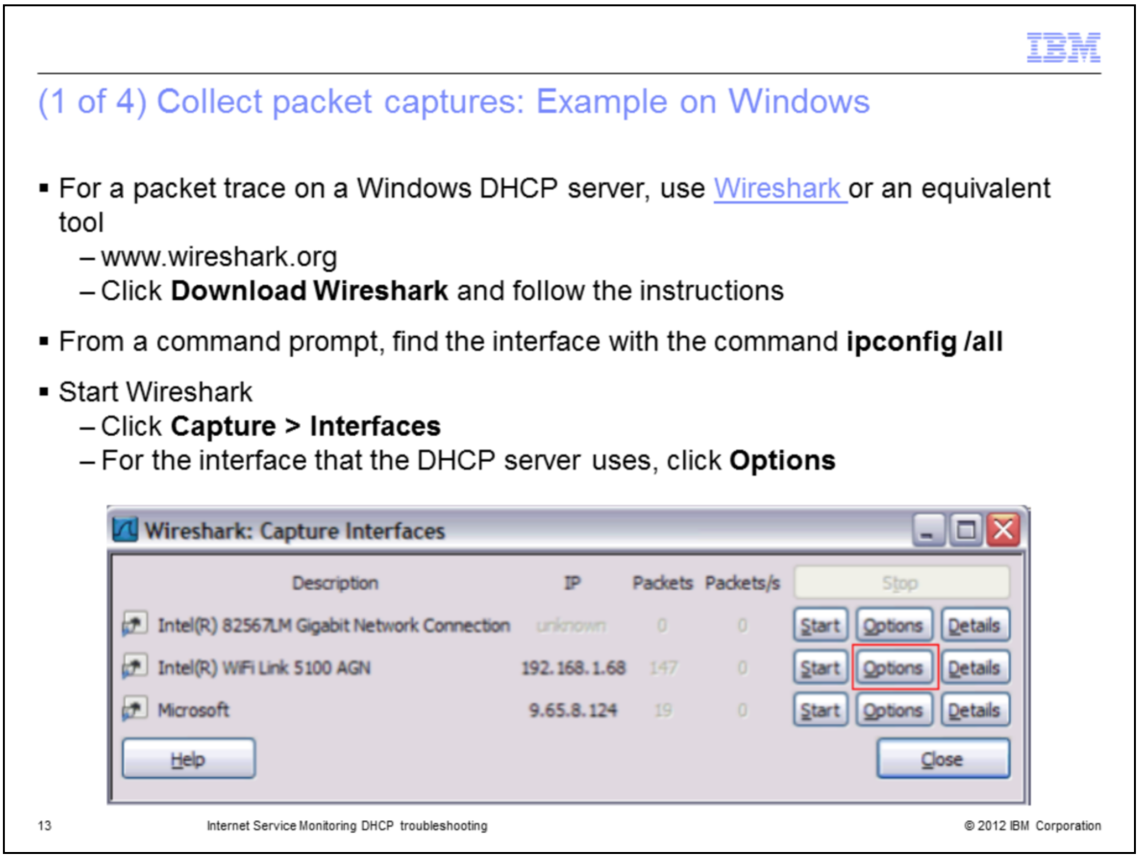
IBM

Collect packet captures: Example on Linux

- On the DHCP server system **itcamtam**, start a tcpdump. The command **'tcpdump -i <interface> -s 0 -w <capture file>'** creates a packet trace that can be viewed with Wireshark
  - [root@itcamft2 bin]# **tcpdump -i eth0 -s 0 -w /tmp/dhcpsrv.dmp**
  - tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
- On the Internet Service Monitoring agent system **itcamft2**, stop the Internet Service Monitoring agent and start a tcpdump
  - [root@itcamtam bin]# **/opt/IBM/ITM/bin/itmcmd agent stop is**
  - [root@itcamtam bin]# **tcpdump -i eth0 udp -s 0 -w /tmp/dhcpmon.dmp**
  - tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
- Start the DHCP monitor manually:
  - [root@itcamtam bin]# **cd /opt/IBM/ITM/li6263/is/bin**
  - [root@itcamtam bin]# **./nco_m_dhcp**
- Wait for the monitor to run (timeout * retries at least)
- Collect the **dhcpsrv.dmp** and **dhcpmon.dmp** files, and review with Wireshark

12 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

To get a clean packet capture on the Internet Service Monitoring agent system, stop the Internet Service Monitoring agent, start the packet capture, and then run the DHCP monitor manually. On UNIX and Linux systems, use **tcpdump** or **tshark** to collect a packet capture. Give the DHCP monitor time to run and then stop the capture.



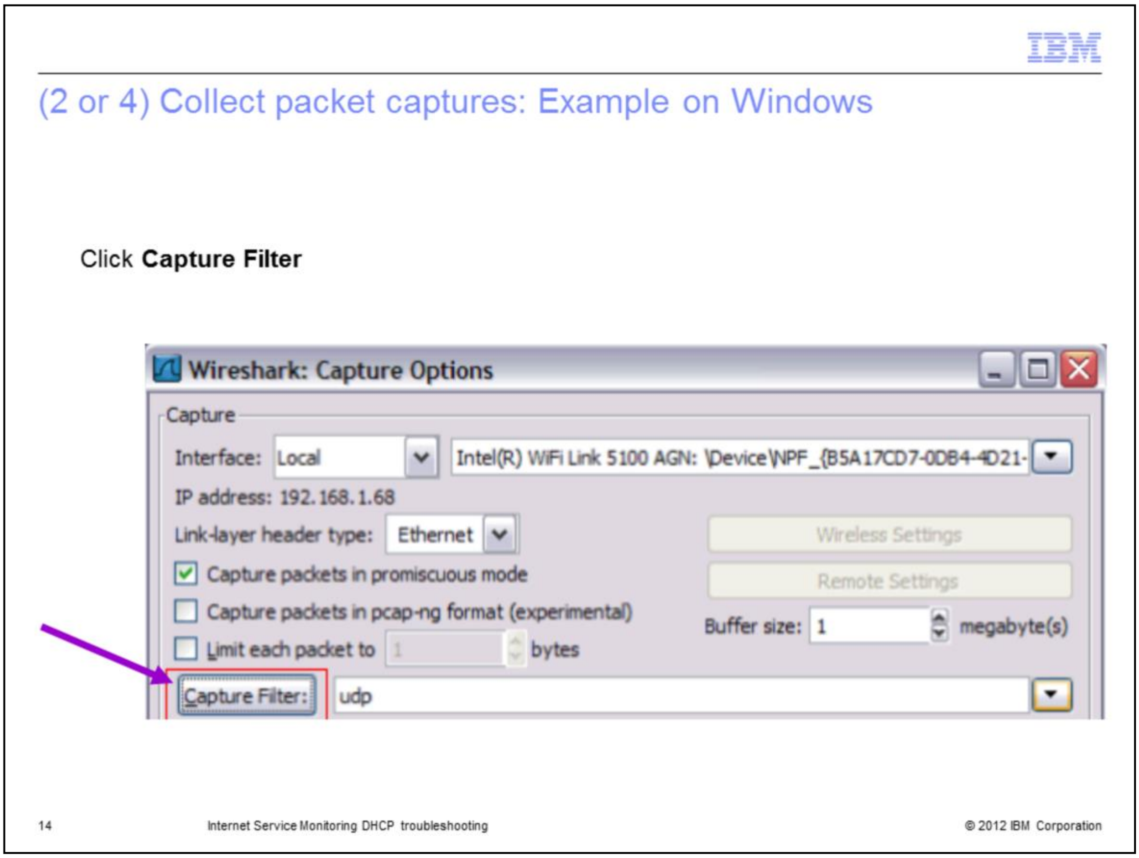
(1 of 4) Collect packet captures: Example on Windows

- For a packet trace on a Windows DHCP server, use Wireshark or an equivalent tool
  - www.wireshark.org
  - Click **Download Wireshark** and follow the instructions
- From a command prompt, find the interface with the command **ipconfig /all**
- Start Wireshark
  - Click **Capture > Interfaces**
  - For the interface that the DHCP server uses, click **Options**

Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s
Intel(R) 82567LM Gigabit Network Connection	unknown	0	0
Intel(R) WiFi Link 5100 AGN	192.168.1.68	147	0
Microsoft	9.65.8.124	19	0

On Windows systems, you can use Wireshark or an equivalent tool to collect the packet capture.



(2 or 4) Collect packet captures: Example on Windows

Click **Capture Filter**

Wireshark: Capture Options

Capture

Interface: Local Intel(R) WiFi Link 5100 AGN: \Device\NPF_{B5A17CD7-0DB4-4D21-

IP address: 192.168.1.68

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

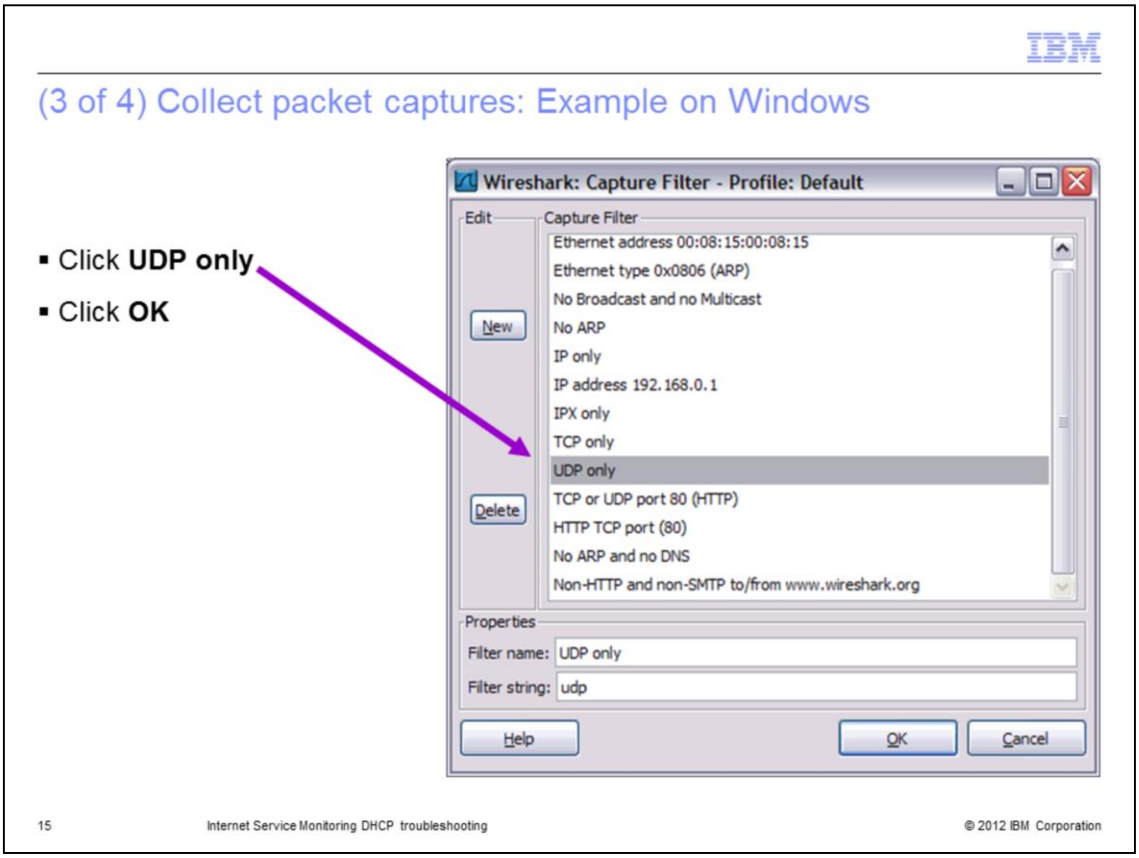
□ Capture packets in pcap-ng format (experimental)

□ Limit each packet to 1 bytes

Buffer size: 1 megabyte(s)

Capture Filter: udp

When you use Wireshark, use a capture filter to collect only UDP packets.



(3 of 4) Collect packet captures: Example on Windows

- Click **UDP only**
- Click **OK**

Capture Filter

- Ethernet address 00:08:15:00:08:15
- Ethernet type 0x0806 (ARP)
- No Broadcast and no Multicast
- No ARP
- IP only
- IP address 192.168.0.1
- IPX only
- TCP only
- UDP only
- TCP or UDP port 80 (HTTP)
- HTTP TCP port (80)
- No ARP and no DNS
- Non-HTTP and non-SMTP to/from www.wireshark.org

Properties

Filter name: UDP only

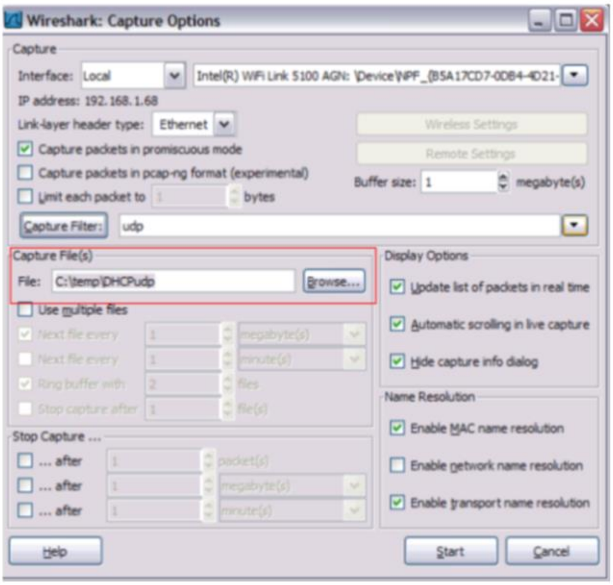
Filter string: udp

15 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

Use the Wireshark Capture Filter dialog box to set the UDP filter.

(4 of 4) Collect packet captures: Example on Windows

- Set a name for the **Capture File**
- Click **Start**
- Wait for the monitor to run (timeout * retries at least)
- Collect the trace files and review with Wireshark



Wireshark: Capture Options

Capture

Interface: Local | Intel(R) WiFi Link 5100 AGN: \Device\NPF_{B5A17CD7-0DB4-4D21-

IP address: 192.168.1.68

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

□ Capture packets in pcap-ng format (experimental)

□ Limit each packet to 1 bytes

Buffer size: 1 megabyte(s)

Capture Filter: udp

Capture File(s)

File: C:\temp\DHCPudp

□ Use multiple files

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

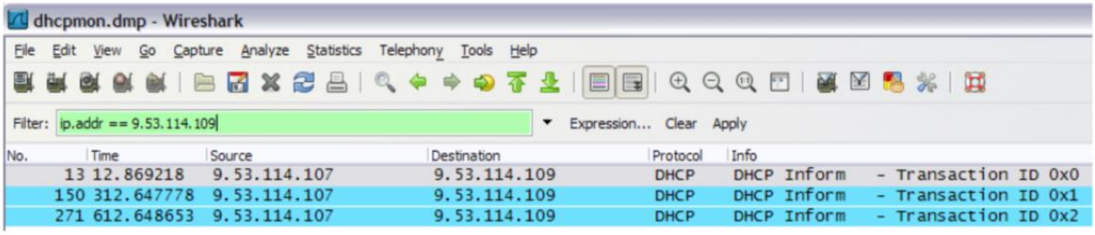
☑ Enable transport name resolution

Enter a name for the capture file, start the capture, and wait for the DHCP monitor to run.

Step 6. Review the packet trace

Here is an example of a failure:

- The DHCP server is **9.53.114.109**
- The Internet Service Monitoring agent is **9.53.114.107**
- This trace shows the UDP packets that are captured on the Internet Service Monitoring system. There are **Inform** requests that range from **9.53.114.107 (ISM)** to **9.53.114.109 (DHCP Server)**, but no responses


dhcpmon.dmp - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: ip.addr == 9.53.114.109

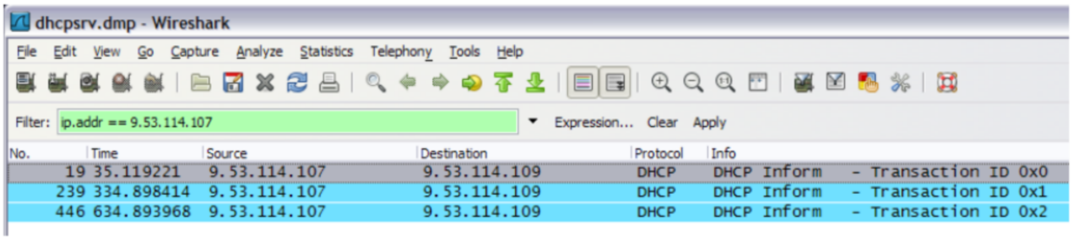
```
No.   Time        Source         Destination    Protocol  Info
   13 12.869218   9.53.114.107   9.53.114.109   DHCP      DHCP Inform   - Transaction ID 0x0
  150 312.647778  9.53.114.107   9.53.114.109   DHCP      DHCP Inform   - Transaction ID 0x1
  271 612.648653  9.53.114.107   9.53.114.109   DHCP      DHCP Inform   - Transaction ID 0x2
```

Here is an example of one possible failure. In the capture, there are UDP packets that travel from the Internet Service Monitoring system to the DHCP server, but no responses are seen.

UDP data from DHCP server

Here is the data from the DHCP server system that is taken at the same time

- There are **Inform** requests from **9.53.114.107 (ISM)**, but the DHCP server is not responding
- The DHCP server is not configured to respond to **Inform** requests


dhcpsrv.dmp - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: ip.addr == 9.53.114.107

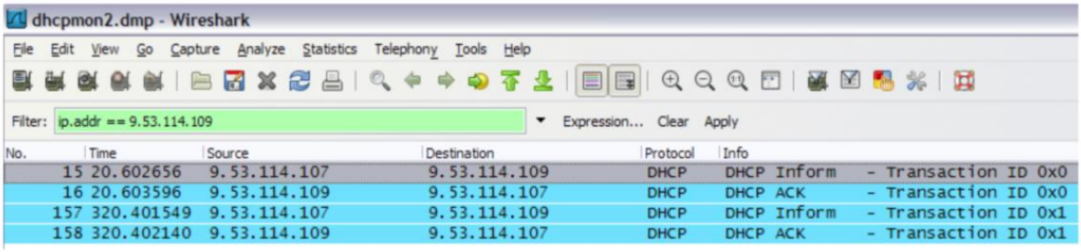
```
No.   Time         Source          Destination      Protocol  Info
   19 35.119221    9.53.114.107    9.53.114.109     DHCP      DHCP Inform   - Transaction ID 0x0
  239 334.898414   9.53.114.107    9.53.114.109     DHCP      DHCP Inform   - Transaction ID 0x1
  446 634.893968   9.53.114.107    9.53.114.109     DHCP      DHCP Inform   - Transaction ID 0x2
```

This screen capture shows the UDP data from the DHCP server viewpoint. The system is receiving the **DHCP Inform** requests, but is not responding. In this case, the DHCP server was not configured to respond to Inform requests.

Example of DHCP monitor working correctly

Here is an example of a trace from a correctly working Internet Service Monitoring system

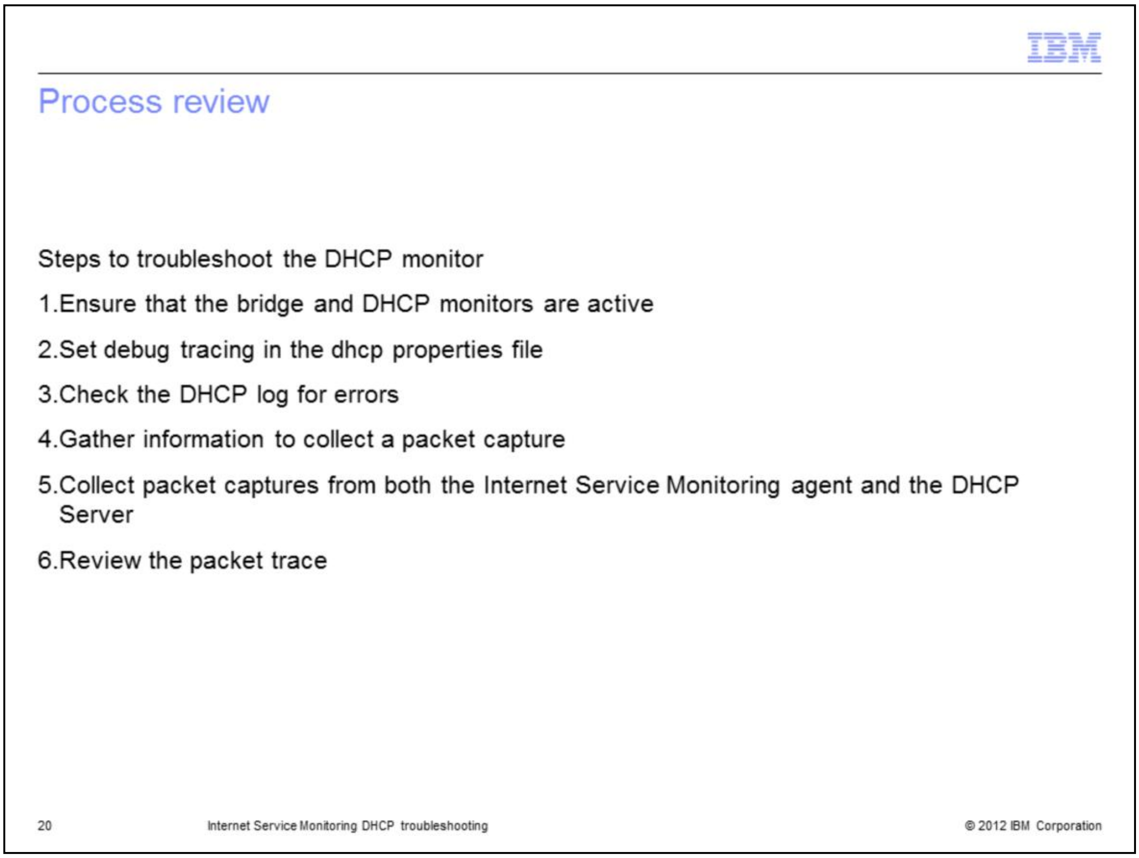
The trace shows the **DHCP Inform** request that goes from **9.53.114.107 (ISM)** to **9.53.114.109 (DHCP Server)**, followed by a **DHCP ACK** that flows from **9.53.114.109 (DHCP Server)** to **9.53.114.107 (ISM)**



Filter: ip.addr == 9.53.114.109

```
No.   Time        Source         Destination    Protocol Info
   15 20.602656   9.53.114.107   9.53.114.109   DHCP     DHCP Inform   - Transaction ID 0x0
   16 20.603596   9.53.114.109   9.53.114.107   DHCP     DHCP ACK      - Transaction ID 0x0
  157 320.401549  9.53.114.107   9.53.114.109   DHCP     DHCP Inform   - Transaction ID 0x1
  158 320.402140  9.53.114.109   9.53.114.107   DHCP     DHCP ACK      - Transaction ID 0x1
```

This example shows a trace from an Internet Service Monitoring system where the DHCP monitor is working correctly. It shows the Inform request from the DHCP monitor and the acknowledge response from the DHCP server system.



Process review

Steps to troubleshoot the DHCP monitor

1.Ensure that the bridge and DHCP monitors are active

2.Set debug tracing in the dhcp properties file

3.Check the DHCP log for errors

4.Gather information to collect a packet capture

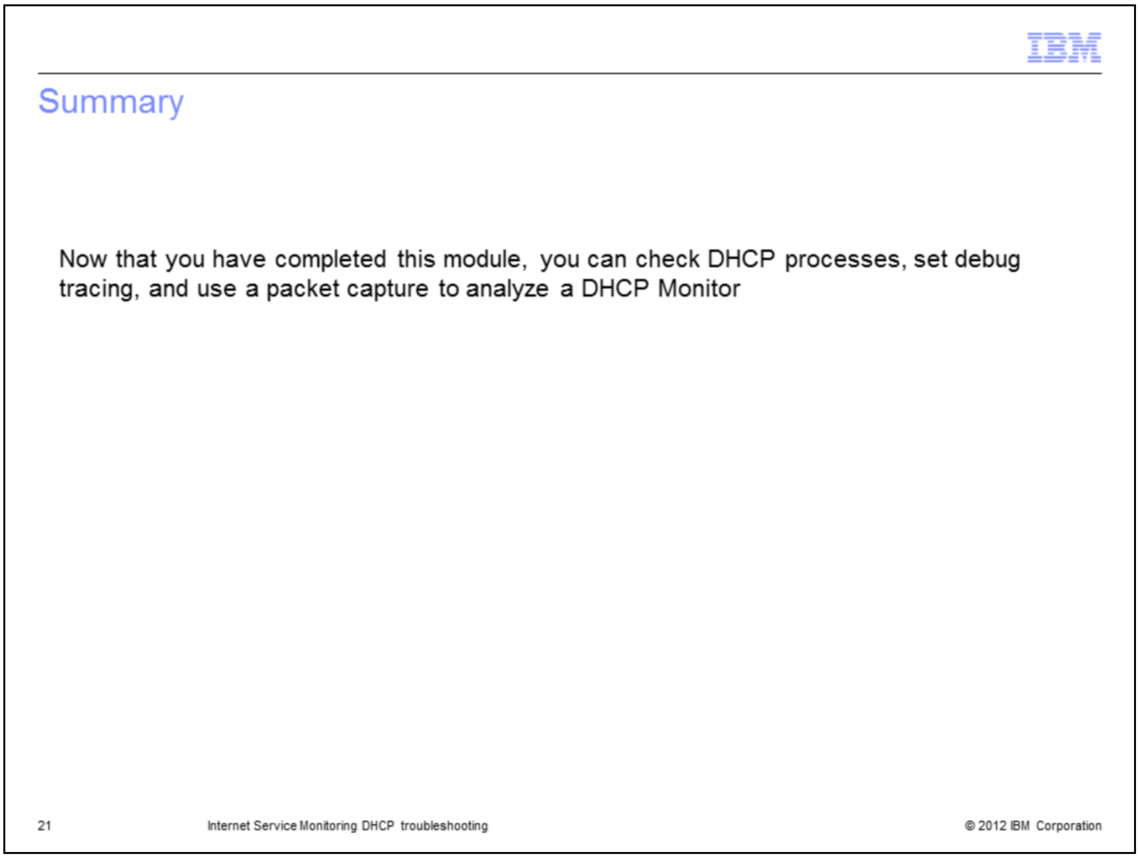
5.Collect packet captures from both the Internet Service Monitoring agent and the DHCP Server

6.Review the packet trace

20 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

Process review; these are the major troubleshooting steps:

1. Ensure that the bridge and DHCP monitors are active
2. Set debug tracing in the dhcp properties file
3. Check the DHCP log for errors
4. Gather information to collect a packet capture
5. Collect packet captures from both the Internet Service Monitoring agent and the DHCP Server
6. Review the packet trace

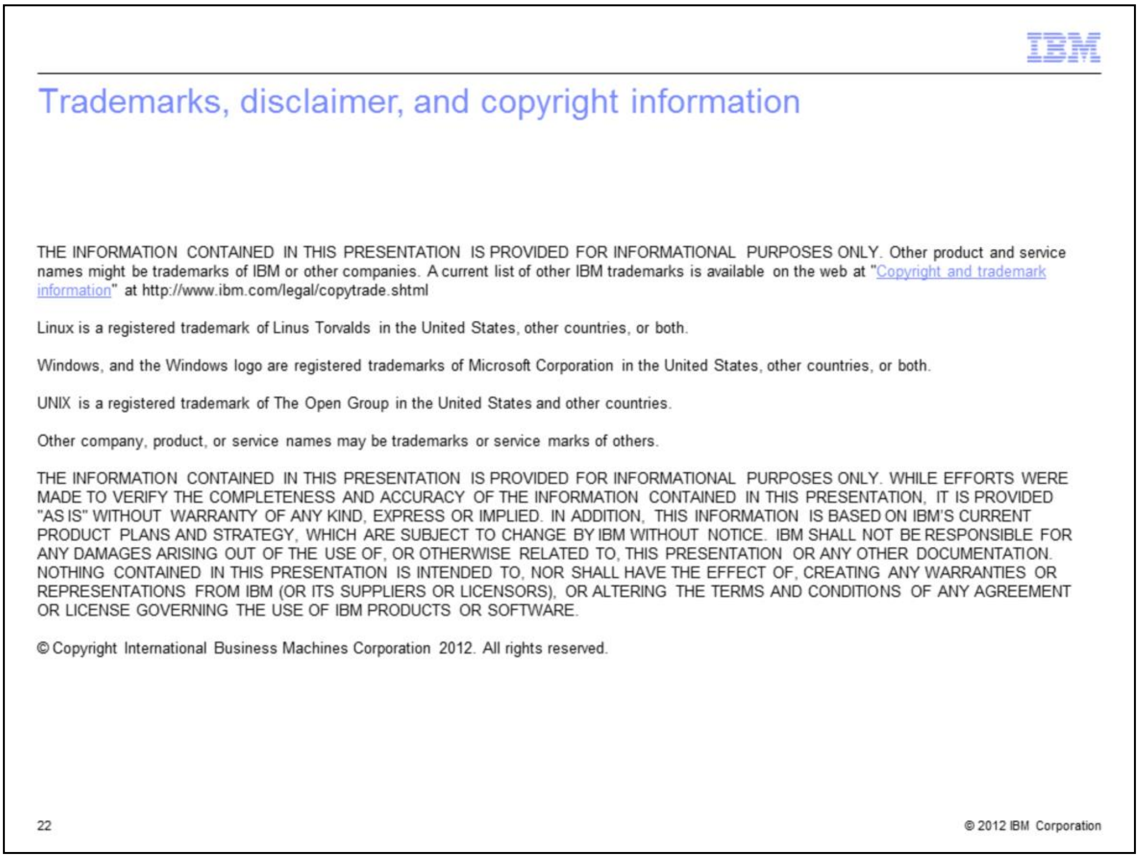


Summary

Now that you have completed this module, you can check DHCP processes, set debug tracing, and use a packet capture to analyze a DHCP Monitor

21 Internet Service Monitoring DHCP troubleshooting © 2012 IBM Corporation

Now that you completed this module, you can check DHCP processes, set debug tracing, and use a packet capture to analyze a DHCP Monitor.



Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.