



# Wireshark and Cisco Network Assistant



**Mark Anderson**  
**Mesa Community College**

Cisco | Networking Academy®  
Mind Wide Open™



# What Are We Covering Today?

- **Wireshark**

  - Getting started

  - Capturing PDUs

  - What is all this Stuff?

  - Check out the VODs

- **Cisco Network Assistant**

  - Getting started

  - Discovering the Network

  - What else can I do?

- **Time to play**



# Wireshark





# What Is Wireshark?

(Formerly Ethereal)

- Wireshark is the world's foremost network protocol analyzer, and is the de facto (and often de jure) standard across many industries and educational institutions
- Wireshark development thrives thanks to the contributions of networking experts across the globe
- It is the continuation of a project that started in 1998

**Translation: You can capture Packet Data Units (PDU) and analyze them**





# Getting Started

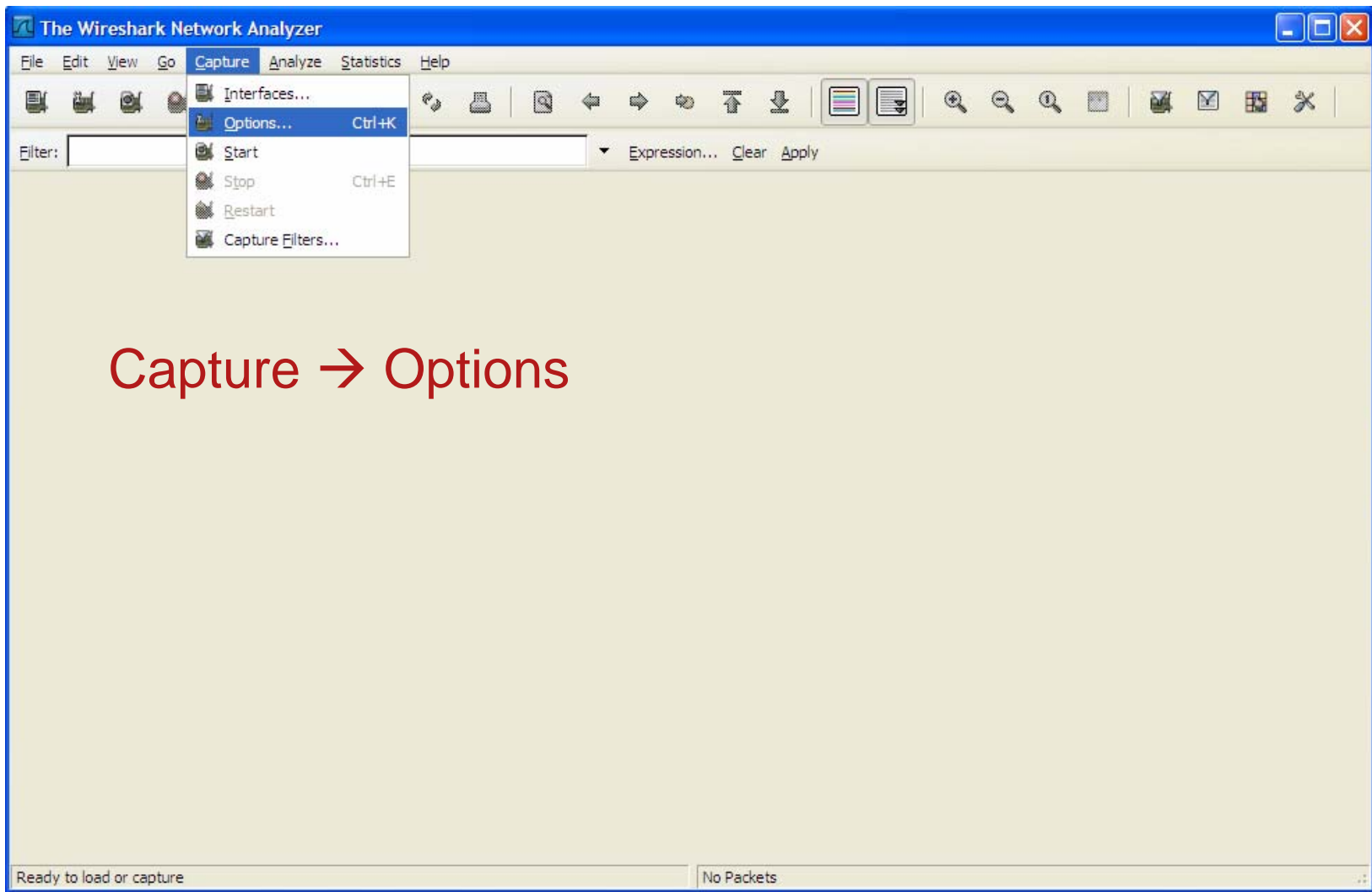
- Download [www.wireshark.org](http://www.wireshark.org)

Note: Wireshark 1.00 was released May 28, 2008, many security-related vulnerabilities have been fixed

- Install on host computer
- Connect host to Network via Fast Ethernet
- When connected to a switch only unicast packets destined to the host, as well as multicast and broadcast, will be captured
- Launch Wireshark



# Launching Wireshark



Capture → Options



# Setting Options

The image shows the 'Wireshark: Capture Options' dialog box. The 'Capture' section is highlighted with a red circle, containing the checked option 'Capture packets in promiscuous mode'. The 'Display Options' section is also highlighted with a red circle, containing the checked option 'Enable transport name resolution'. A red arrow points from the bottom of the dialog box to the 'Start' button.

**Wireshark: Capture Options**

**Capture**

Interface: [Microsoft's Packet Scheduler] : \Device\NPF\_{88E7B467-7486-40BA-8272-6B8C5A4B0296}

IP address: 192.168.40.30

Link-layer header type: Ethernet Buffer size: 1 megabyte(s) Wireless Settings

Capture packets in promiscuous mode

Limit each packet to 65535 bytes

Capture Filter: [ ]

**Capture File(s)**

File: [ ] Browse...

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

Buttons: Help Start Cancel



# Generating ARP Traffic

Generate ARP Traffic:

1. Bring up a command prompt (Start → Run → cmd )
2. Enter **arp -d** to clear the arp cache
3. Ping the broadcast for the local subnet

Example: **ping 192.168.1.255**

4. Enter **arp -a** to verify arp translations are in arp cache

See Next Slide →



# Generate ARP Traffic

```
C:\WINDOWS\system32\cmd.exe

IP Address . . . . . : 192.168.1.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

C:\Documents and Settings\manderson>ping 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.100: bytes=32 time<1ms TTL=255
Reply from 192.168.1.100: bytes=32 time<1ms TTL=255
Reply from 192.168.1.100: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

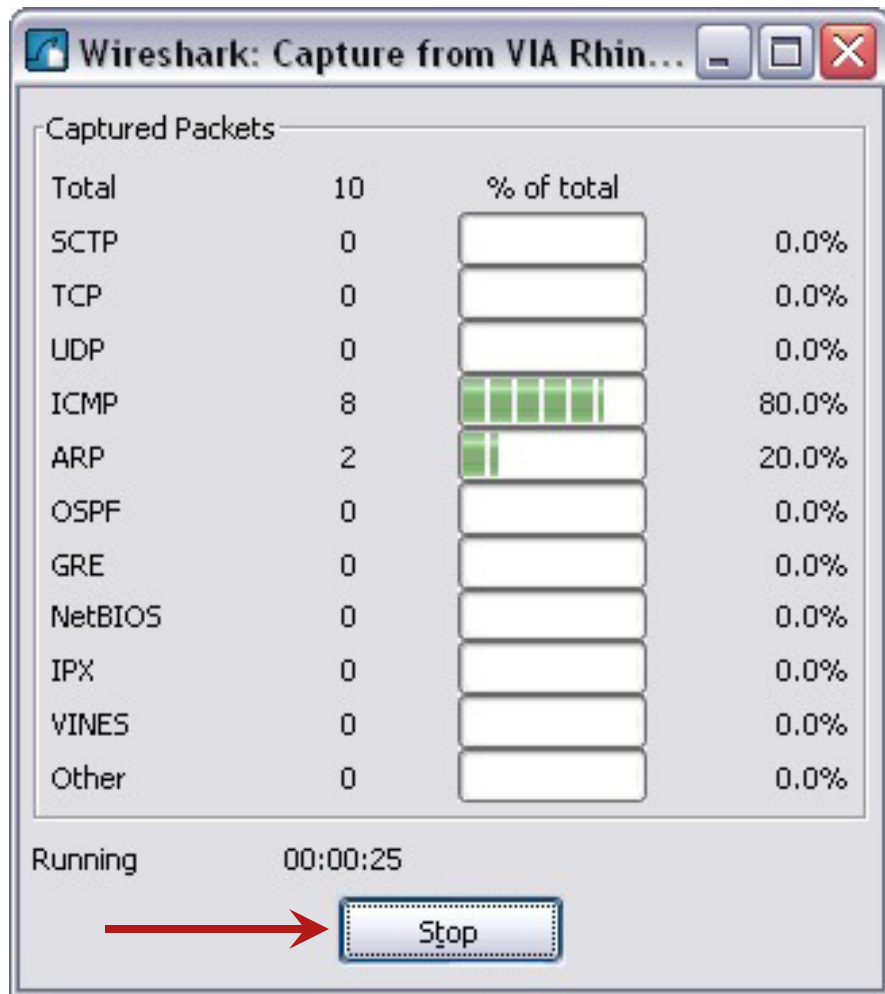
C:\Documents and Settings\manderson>arp -a

Interface: 192.168.1.10 --- 0x3
    Internet Address      Physical Address          Type
    192.168.1.1           00-1b-d4-47-29-20        dynamic
    192.168.1.2           00-1b-d4-44-8a-f8        dynamic
    192.168.1.100         00-1b-53-08-b1-c0        dynamic

C:\Documents and Settings\manderson>
```



# Capturing PDUs



# See What Was Captured

The screenshot displays the Wireshark interface with the following components:

- Packet List Pane:** A table listing captured packets. The selected packet (No. 16) is an ICMP Echo (ping) request from 192.168.1.10 to 192.168.1.255.
- Packet Details Pane:** Shows the hierarchical structure of the selected packet:
  - Frame 1 (60 bytes on wire, 60 bytes captured)
  - Ethernet II, Src: 00:1b:53:08:b1:8b (00:1b:53:08:b1:8b), Dst: 00:1b:53:08:b1:8b (00:1b:53:08:b1:8b)
  - Configuration Test Protocol (loopback)
  - Data (40 bytes)
- Packet Bytes Pane:** Shows the raw bytes of the selected packet in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Info
16	21.326052	192.168.1.10	192.168.1.255	ICMP	Echo (ping) request
17	21.326568	00:1b:53:08:b1:c0	Broadcast	ARP	who has 192.168.1.10? Tell 192.168.1.100
18	21.326578	GlobalDa_ce:fd:4d	00:1b:53:08:b1:c0	ARP	192.168.1.10 is at 00:17:a4:ce:fd:4d
19	21.327000	192.168.1.1	192.168.1.10	ICMP	Echo (ping) reply
20	21.327081	00:1b:d4:44:8a:f8	Broadcast	ARP	who has 192.168.1.10? Tell 192.168.1.2
21	21.327087	GlobalDa_ce:fd:4d	00:1b:d4:44:8a:f8	ARP	192.168.1.10 is at 00:17:a4:ce:fd:4d
22	21.382414	00:1b:53:08:b1:8b	spanning-tree-(for	STP	Conf. Root = 32769/00:1b:53:08:b1:80 Cost = 0 Port = 0>
23	22.326308	192.168.1.10	192.168.1.255	ICMP	Echo (ping) request
24	22.326760	192.168.1.100	192.168.1.10	ICMP	Echo (ping) reply
25	22.327113	192.168.1.2	192.168.1.10	ICMP	Echo (ping) reply

```

0000  00 1b 53 08 b1 8b 00 1b 53 08 b1 8b 90 00 00 00  ..S.....S.....
0010  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..
0030  00 00 00 00 00 00 00 00 00 00 00 00  ..
  
```

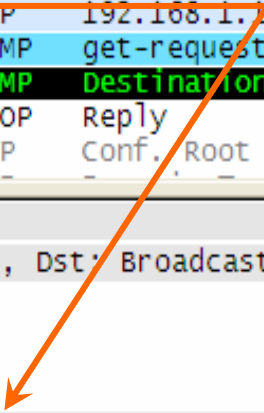


# Analyze an ARP Request

38	29.401877	00:1b:53:08:b1:8b	Spanning-tree-(for STP	Conf. Root = 32769/00:1b:53:08:b1:80	Cost
39	29.752733	GlobalDa_ce:fd:4d	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.10
40	29.753427	00:1b:d4:47:29:20	GlobalDa_ce:fd:4d	ARP	192.168.1.1 is at 00:1b:d4:47:29:20
41	29.753433	192.168.1.10	192.168.40.252	SNMP	get-request
42	29.754162	192.168.1.1	192.168.1.10	ICMP	Destination unreachable (Host unreachable)
43	30.013869	00:1b:53:08:b1:8b	00:1b:53:08:b1:8b	LOOP	Reply
44	31.407043	00:1b:53:08:b1:8b	Spanning-tree-(for STP	Conf. Root = 32769/00:1b:53:08:b1:80	Cost

- ⊕ Frame 39 (42 bytes on wire, 42 bytes captured)
- ⊖ Ethernet II, Src: GlobalDa\_ce:fd:4d (00:17:a4:ce:fd:4d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  - ⊕ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  - ⊕ Source: GlobalDa\_ce:fd:4d (00:17:a4:ce:fd:4d)
    - Type: ARP (0x0806)
  - ⊖ Address Resolution Protocol (request)
    - Hardware type: Ethernet (0x0001)
    - Protocol type: IP (0x0800)
    - Hardware size: 6
    - Protocol size: 4
    - Opcode: request (0x0001)
    - Sender MAC address: GlobalDa\_ce:fd:4d (00:17:a4:ce:fd:4d)
    - Sender IP address: 192.168.1.10 (192.168.1.10)
    - Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)
    - Target IP address: 192.168.1.1 (192.168.1.1)



← Notice the Target MAC Is Unknown





# Generating TCP 3-Way Handshake Traffic

## Generate TCP Traffic Using a Browser:

1. From the Host, bring up a browser
2. In the Address field, enter the IP address of any device on the network that has an IP address and http server enabled, such as a router, switch, webserver, Discovery server, or Eagle server

**Note: on router → `router(config)#ip http server`**

3. Once the browser brings up the home page of the device, you can stop the capture

# TCP 3-Way Handshake

Look for Three TCP

98 92.411956 192.168.1.10 192.168.1.1 TCP 1055 > http [SYN] Seq=0 Len=0 MSS=1260

99 92.413626 192.168.1.1 192.168.1.10 TCP http > 1055 [SYN, ACK] Seq=0 Ack=1 win=4128 Len=0 MSS=1260

100 92.413649 192.168.1.10 192.168.1.1 TCP 1055 > http [ACK] Seq=1 Ack=1 win=65535 Len=0

101 92.413774 192.168.1.10 192.168.1.1 HTTP GET / HTTP/1.1

102 92.445244 192.168.1.1 192.168.1.10 HTTP HTTP/1.1 401 Unauthorized

103 92.445754 192.168.1.1 192.168.1.10 TCP http > 1055 [FIN, RST, ACK] Seq=103 Ack=570 win=3550 Len=0

Internet Protocol, Src: 192.168.1.10 (192.168.1.10), Dst: 192.168.1.1 (192.168.1.1)

Transmission Control Protocol, Src Port: 1055 (1055), Dst Port: http (80), Seq: 0, Len: 0

Source port: 1055 (1055)

Destination port: http (80)

Sequence number: 0 (relative sequence number)

Header length: 28 bytes

Flags: 0x02 (SYN)

- 0... .... = Congestion window Reduced (CWR): Not set
- .0.. .... = ECN-Echo: Not set
- ..0. .... = Urgent: Not set
- ...0 .... = Acknowledgment: Not set
- .... 0... = Push: Not set
- .... 0... = Reset: Not set
- .... ..1. = Syn: Set
- .... ...0 = Fin: Not set

Window size: 65535

Checksum: 0xa0ec [correct]

1st Packet

# TCP 3-Way Handshake

Trailer: 0000

- ⊕ Internet Protocol, src: 192.168.1.1 (192.168.1.1), dst: 192.168.1.10 (192.168.1.10)
- ⊖ Transmission Control Protocol, src Port: http (80), dst Port: 1055 (1055), seq: 0, ack: 1, len: 0
  - Source port: http (80)
  - Destination port: 1055 (1055)
  - Sequence number: 0 (relative sequence number)
  - Acknowledgement number: 1 (relative ack number)
  - Header length: 24 bytes
  - ⊖ Flags: 0x12 (SYN, ACK)
    - 0... .. = Congestion window Reduced (CWR): Not set
    - .0.. .. = ECN-Echo: Not set
    - ..0. .... = Urgent: Not set
    - ...1 .... = Acknowledgment: Set
    - .... 0... = Push: Not set
    - .... .0.. = Reset: Not set
    - .... ..1. = Syn: Set
    - .... ...0 = Fin: Not set

**2<sup>nd</sup> Packet**

# TCP 3-Way Handshake

97	92.411956	192.168.1.10	192.168.1.1	TCP	1055 > 1055 [SYN] Seq=0 Len=0 MSS=1260
98	92.411956	192.168.1.10	192.168.1.1	TCP	1055 > 1055 [SYN, ACK] Seq=0 Ack=1 win=4128 Len=0 MSS=1260
99	92.413626	192.168.1.10	192.168.1.1	TCP	1055 > 1055 [ACK] Seq=1 Ack=1 win=65535 Len=0
100	92.413649	192.168.1.10	192.168.1.1	HTTP	GET / HTTP/1.1
101	92.413774	192.168.1.10	192.168.1.1	HTTP	HTTP/1.1 401 Unauthorized
102	92.445244	192.168.1.1	192.168.1.10	TCP	1055 > 1055 [ACK] Seq=102 Ack=570 win=355

⊕ Internet Protocol, Src: 192.168.1.10 (192.168.1.10), Dst: 192.168.1.1 (192.168.1.1)  
 ⊖ Transmission Control Protocol, Src Port: 1055 (1055), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0  
 Source port: 1055 (1055)  
 Destination port: http (80)  
 Sequence number: 1 (relative sequence number)  
 Acknowledgement number: 1 (relative ack number)  
 Header length: 20 bytes  
 ⊖ Flags: 0x10 (ACK)  
 0... .. = Congestion Window Reduced (CWR): Not set  
 .0.. .. = ECN-Echo: Not set  
 0... .. = Urgent: Not set  
 ...1 .. = Acknowledgment: Set  
 .... 0... = Push: Not set  
 .... .0.. = Reset: Not set  
 .... ..0. = Syn: Not set  
 .... ...0 = Fin: Not set  
 Window size: 65535

**3<sup>rd</sup> Packet**

# Flow Graph

The screenshot shows the Wireshark Network Analyzer interface. The main pane displays a list of network packets, with packet 99 selected. The left pane shows the details of packet 99, including Ethernet II, Internet Protocol, and Transmission Control Protocol (TCP) fields. The right pane shows the Statistics menu, with 'Flow Graph...' highlighted in blue. Other options in the menu include Summary, Protocol Hierarchy, Conversations, Endpoints, IO Graphs, Conversation List, Endpoint List, Service Response Time, ANSI, Fax T38 Analysis..., GSM, H.225..., MTP3, RTP, SCTP, SIP..., VoIP Calls, WAP-WSP..., BOOTP-DHCP..., Destinations..., HTTP, IP address..., ISUP Messages..., Multicast Streams, and ONC-RPC Programs.

The 'Wireshark: Flow Graph' dialog box is shown. It has three sections: 'Choose packets' with 'Displayed packets' selected; 'Choose flow type' with 'TCP flow' selected; and 'Choose node address type' with 'Standard source/destination addresses' selected. There are 'OK' and 'Close' buttons at the bottom.





The 'Graph Analysis' window displays a sequence of TCP packets between 192.168.1.10 and 192.168.1.1. The packets are shown as a series of arrows representing SYN, SYN, ACK, ACK, PSH, ACK - Len: 569, ACK - Len: 192, FIN, PSH, ACK, ACK, FIN, ACK, and ACK. The time axis ranges from 92.412 to 97.782. The comment column provides details for each packet, such as 'Seq = 0 Ack = 4162941681' for the first SYN packet.

Time	192.168.1.10	192.168.1.1	Comment
92.412	(1055) →	(80)	SYN Seq = 0 Ack = 4162941681
92.414	(80) ←	(1055)	SYN, ACK Seq = 0 Ack = 1
92.414	(80) ←	(1055)	ACK Seq = 1 Ack = 1
92.414	(80) ←	(1055)	PSH, ACK - Len: 569 Seq = 1 Ack = 1
92.445	(80) ←	(1055)	ACK - Len: 192 Seq = 1 Ack = 570
92.446	(80) ←	(1055)	FIN, PSH, ACK Seq = 193 Ack = 570
92.446	(80) ←	(1055)	ACK Seq = 570 Ack = 194
97.781	(80) ←	(1055)	FIN, ACK Seq = 570 Ack = 194
97.782	(80) ←	(1055)	ACK Seq = 194 Ack = 571



# Additional Resources

- VODs found on the Academy site under:  
Interactive Course Guides → Media Archive

	<h3>Working with Wireshark</h3> <p>Wireshark can be used to analyze traffic on local networks, and help students explain protocol operation. See how to set it up and use it in your Academy program.</p>	 (MOV 25MB) wireshark-2.mov	11/29/2007
	<h3>Wireshark in the Classroom</h3> <p>Join an Academy class as they enthusiastically discuss the use of Wireshark to analyze and explain traffic protocol operations on their network.</p>	 (MOV 48MB) wireshark-3.mov	11/29/2007



# Additional Resources

## Wireshark Labs:

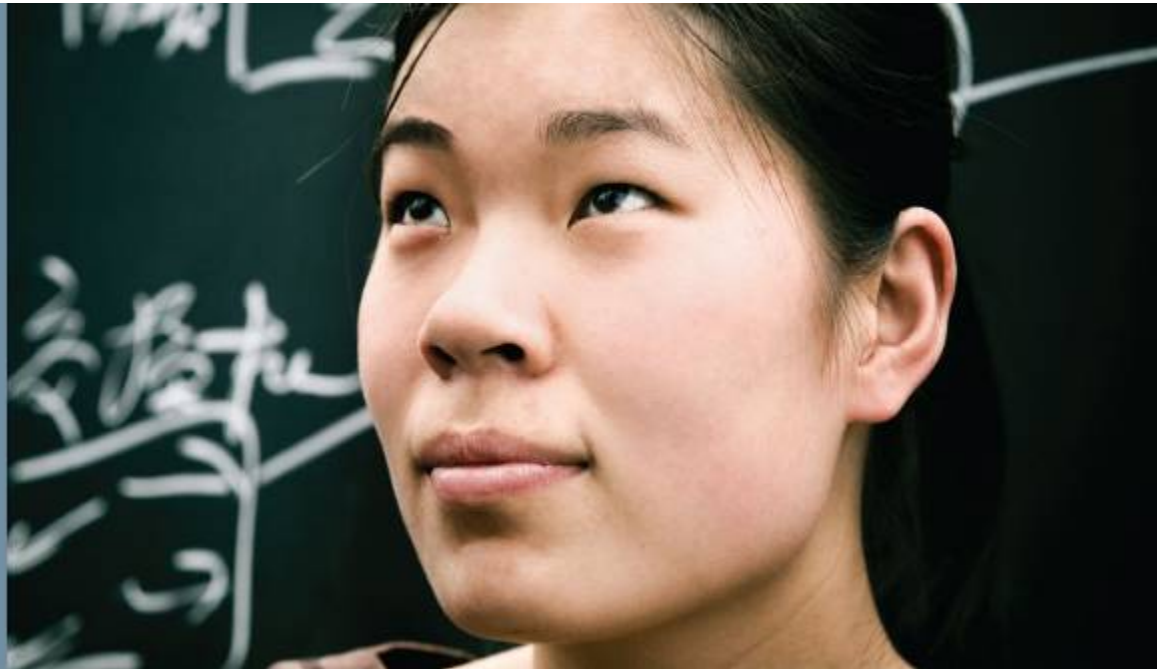
- Discovery 2 → Lab 8.3.2 Conducting a Network Capture with Wireshark
- \*Discovery 3 → Lab 1.2.2 Capturing and Analyzing Network Traffic
- Discovery 4 → Lab 1.4.3 Monitoring VLAN Traffic
- Exploration 1 → 2.6.2, 3.4.2, 3.4.3, 4.5.2\*\*, 4.5.3, 5.5.1, 6.7.2, 7.5.2, 9.8.1, 9.8.3, and 11.5.6

\* Most informative lab in Discovery curriculum

\*\* Great lab covering TCP 3-way handshake



# Cisco Network Assistant





# What Is Cisco Network Assistant?



- A PC-based **network management application** that manages standalone devices and clusters of devices from anywhere in your intranet
- Supports Cisco Catalyst Intelligent switches from 2950 through 4506; uses GUI to **manage many critical switch functions** and **launch the device manager of Cisco routers and wireless AP**
- Auto discovery of network devices
- Topology view and front panel view
- Software upgrade
- Switch configuration
- Perform multiple configuration tasks without using command-line interface (CLI) commands; you can apply actions to multiple devices and ports at the same time for VLAN and QoS, inventory and statistics reports, link and device monitoring, software upgrades, and many other networking features





# Getting Started

- Download from the Classroom Setup Tab on the Academy Connection Tools page under CCNA Discovery “Designing and Supporting Computer Networks” <http://cisco.netacad.net>

**Tools**

Search

CCNA Discovery > Designing and Supporting Computer Networks

Back to Find Tools

Curriculum Course **Classroom Set Up**

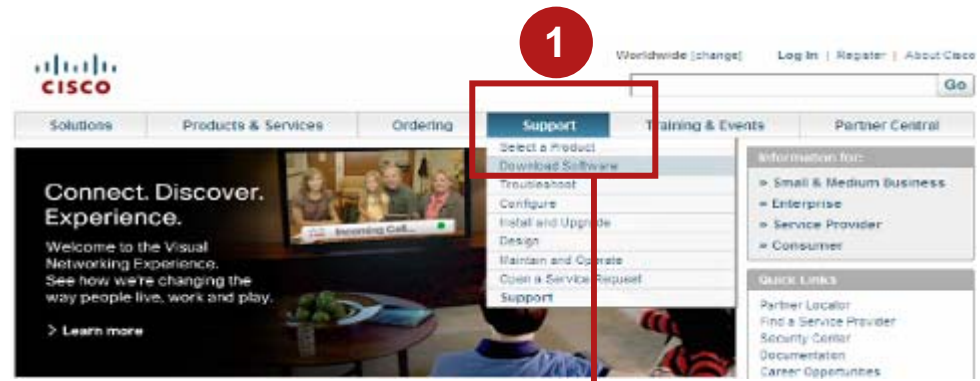
English	
Title	Document Type
Designing and Supporting Computer Networks> Version 4.0	
Cisco Network Assistant	EXE - 40.71 MB 12/05/2007
Cisco Network Assistant	

Note: As of June 1, 2008 the version in Tools section is only 5.2

Name: cna-windows-k9-installer-5-2-en.exe  
 Type: Application, 40.7 MB  
 From: downloads.netacad-cdn.net

# Optional

- Download [www.cisco.com](http://www.cisco.com)
- Need a CCO login account
- Present version 5.3  
[cna-windows-k9-installer-5-3-en.exe](#)  
Release Date: 18/Dec/2007  
Network Assistant 5.3 English Installer  
Size: 43891.87 KB
- Install on Host computer



## Support

### Download Software

You have reached this page because you are not logged in with a valid service contract associated with your Cisco.com user profile. In addition, access to most software is because you do not have a valid service contract as [Service Contract Center](#). For more information on the [Overview](#).

#### Select a Software Product Category

- [Application-Oriented Networking Software](#)
- [Application Networking Software](#)
- [Broadband Cable Software](#)
- [Cisco IOS Software](#)
- [CiscoWorks Software](#)
- [Contact Center Software](#)
- [Interoperability Systems Software](#)
- [Network Management Software](#)
- [Optical Networking Software](#)
- [Router Software](#)

Scroll Down Until You See the Following:

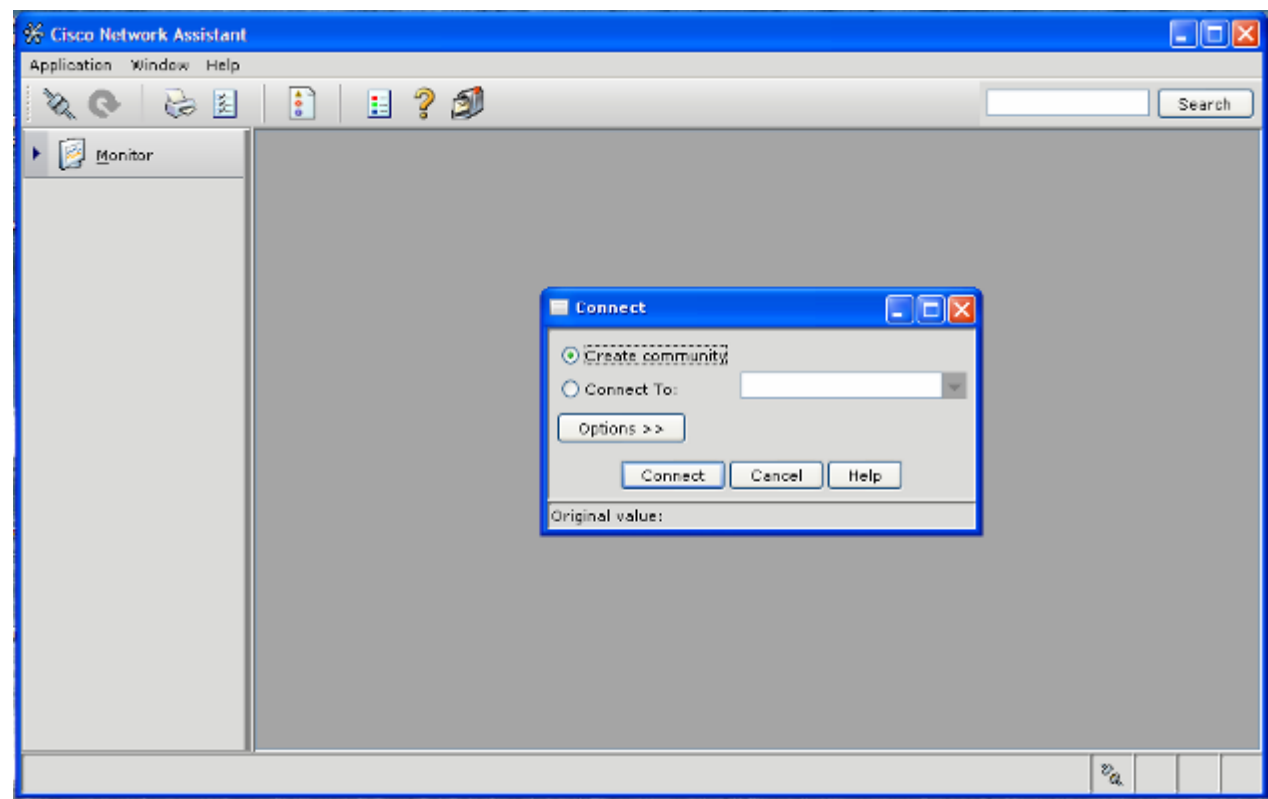
**LAN Network Management Software**  
[Cisco Network Assistant \(CNA\)](#)  
[Cisco Broadband Access Center for Broadband](#)

2

3



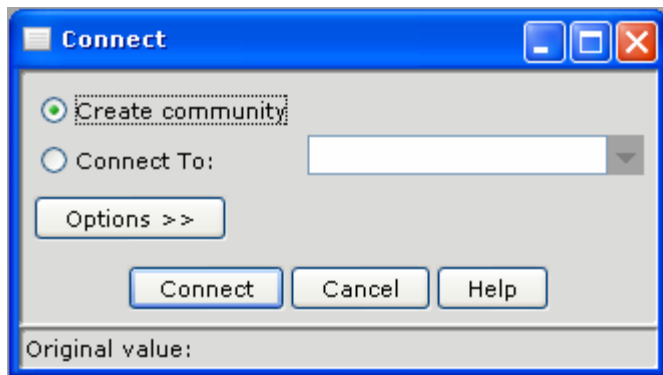
# Launch Cisco Network Assistant



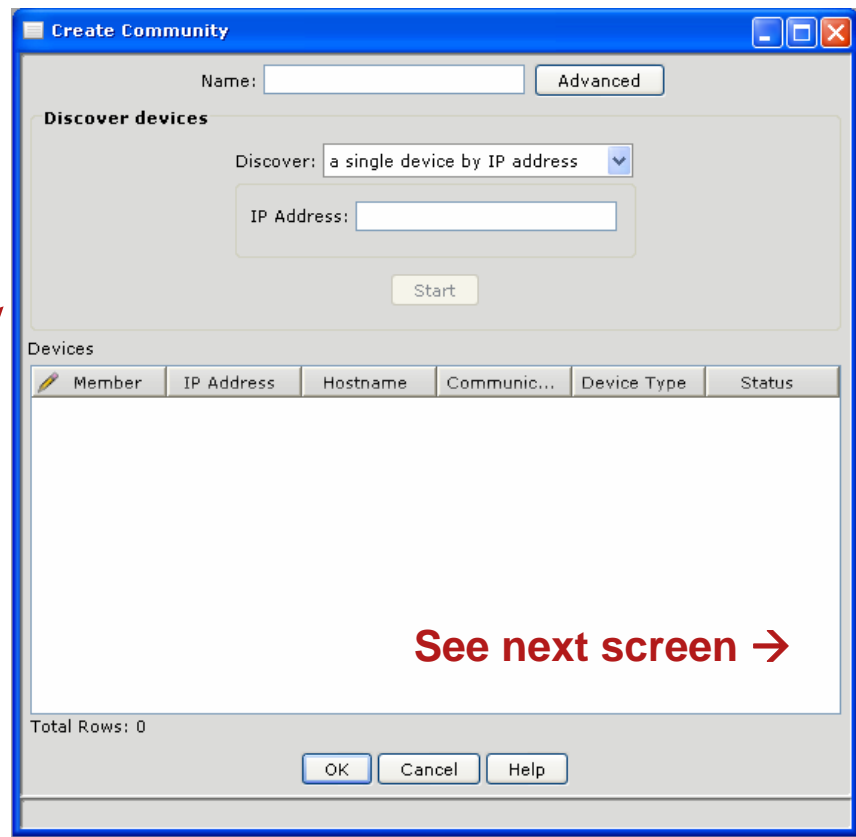


# Create a Community

- A community is a defined cluster of devices grouped by an IP address range



Select **Create Community**,  
Then click **Connect**





# Name Community and Method of Discovery

1

2

**Create Community**

Name:

**Discover devices**

Discover:

IP Address:

- a single device by IP address
- devices using a seed IP address
- devices on a subnet
- devices in an IP address range

**Devices**

Member	IP Address	Hostname	Communic...	Device Type	Status
--------	------------	----------	-------------	-------------	--------

Total Rows: 0

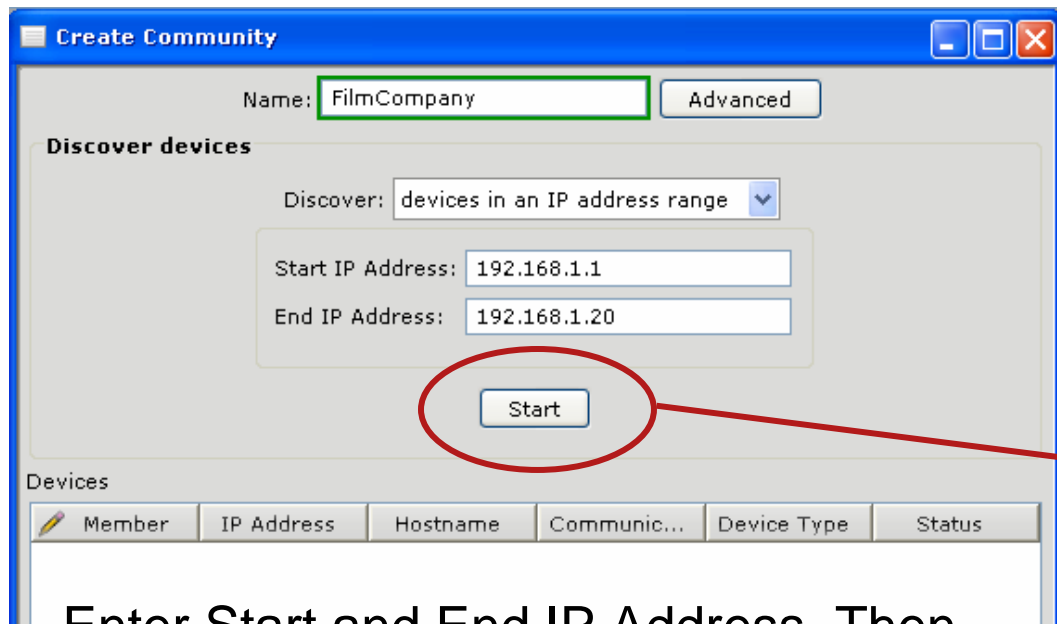
Discover:

IP Address:

- a single device by IP address
- devices using a seed IP address
- devices on a subnet
- devices in an IP address range



# Start the Discovery Process

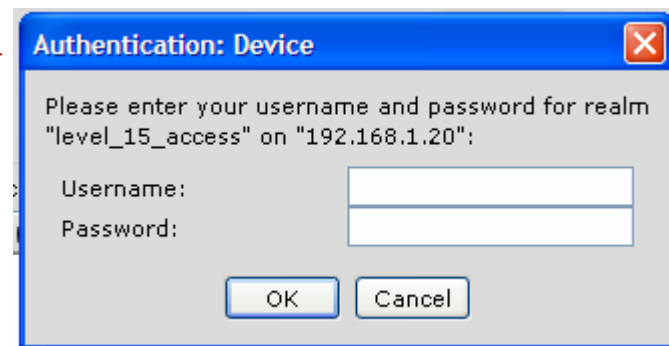


## Level 15 Authentication:

- Enable: No Username just password
- Login account: Both Username and password

Enter Start and End IP Address, Then Click Start to Start the Discovery Process

Note: Discovery Process Attempts to Connect to All IP Addresses in Range, So Be Selective to Avoid Long Delays



Note: Will Be Prompted for Each Device that Has Different Authentication

Don't Bother Me  
I'm Discovering Devices!



**Create Community**

Name:

**Discover devices**

Discover:

Start IP Address:

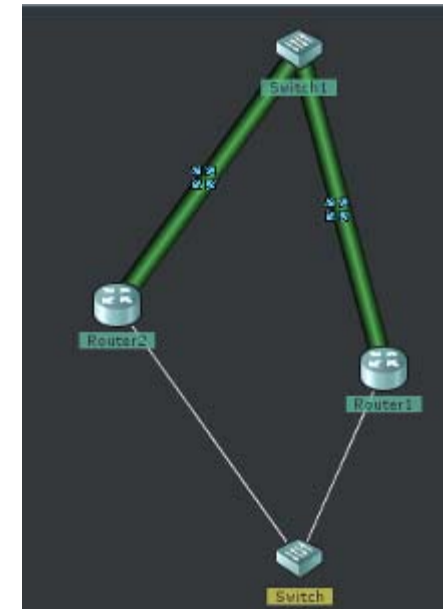
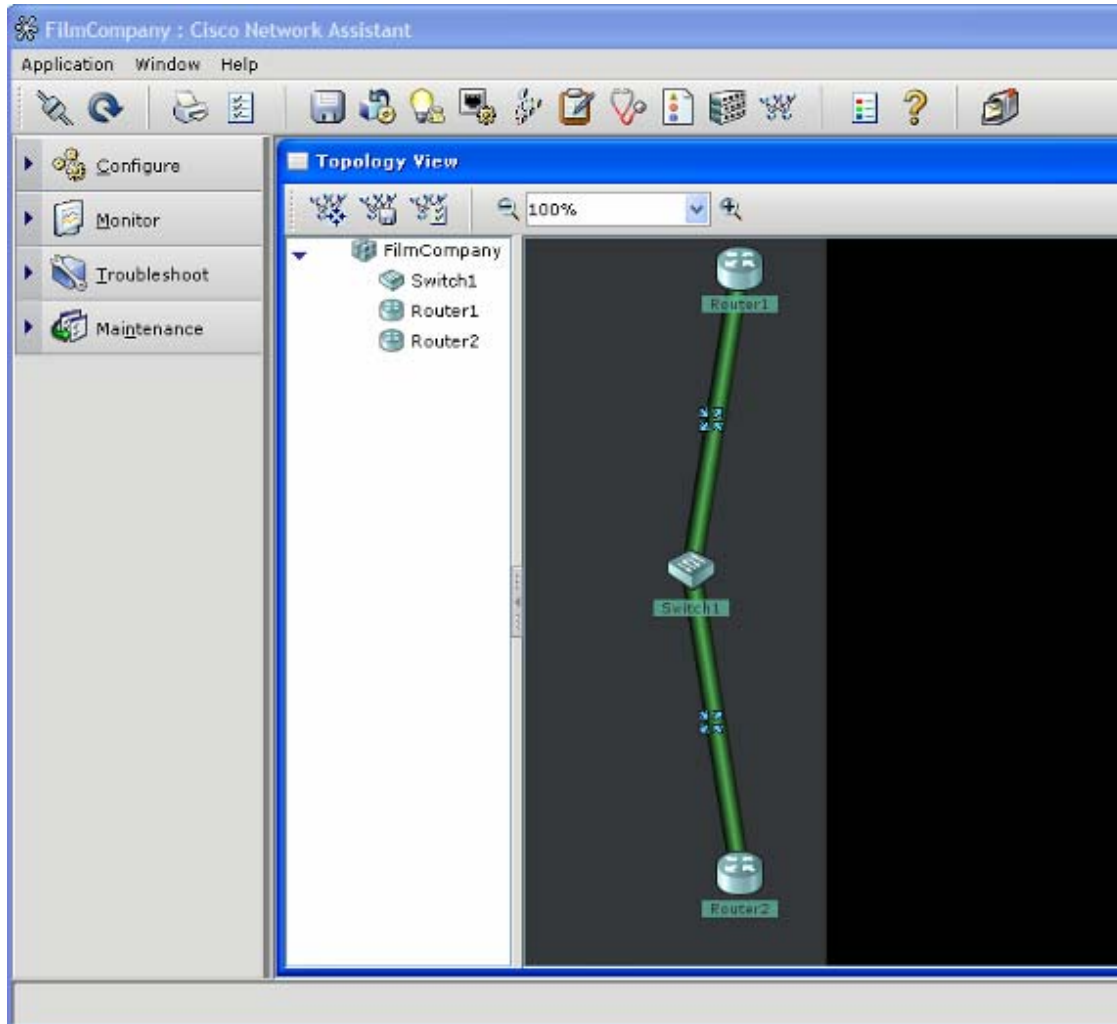
End IP Address:

**Devices**

Member	IP Address	Hostname	Communicatio...	Device Type	Status
<input type="checkbox"/>	192.168.1.15		http		❌ Connection Failed
<input type="checkbox"/>	192.168.1.7		http		❌ Connection Failed
<input checked="" type="checkbox"/>	192.168.1.20	Switch1	http	WS-C2960-24TT-L	✅ Discovered
<input type="checkbox"/>	192.168.1.11		http		❌ Connection Failed
<input type="checkbox"/>	192.168.1.14		http		❌ Connection Failed
<input type="checkbox"/>	192.168.1.6		http		❌ Connection Failed
<input type="checkbox"/>	192.168.1.18		http		❌ Connection Failed
<input checked="" type="checkbox"/>	192.168.1.1	Router1	http	2811	✅ Discovered
<input checked="" type="checkbox"/>	192.168.1.2	Router2	http	2811	✅ Discovered

Total Rows: 20

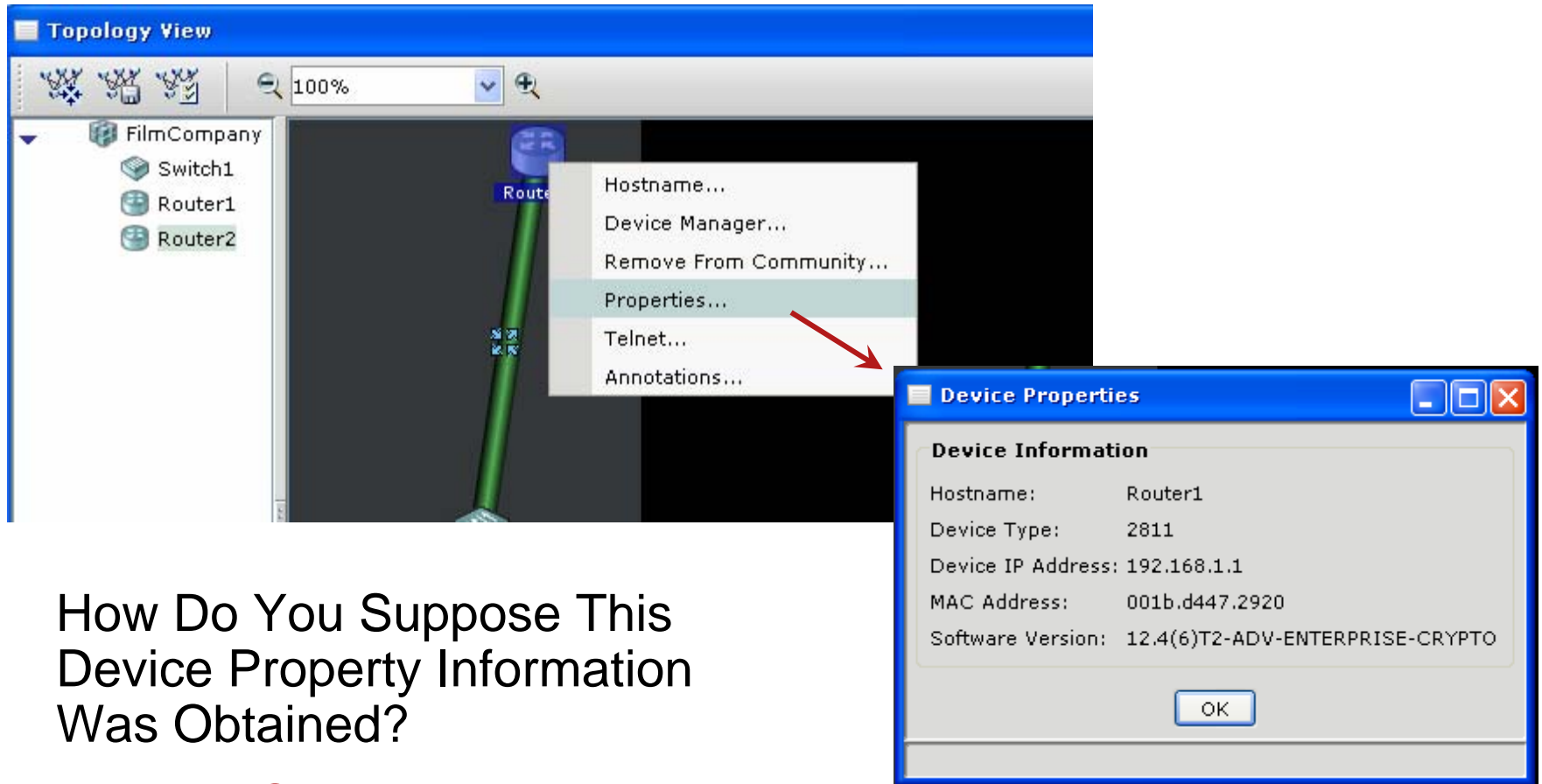
# Topology View



Devices Discovered Within Range Have Bold Connection; Devices not in Range Only a Line, but Can Be Added to the Community



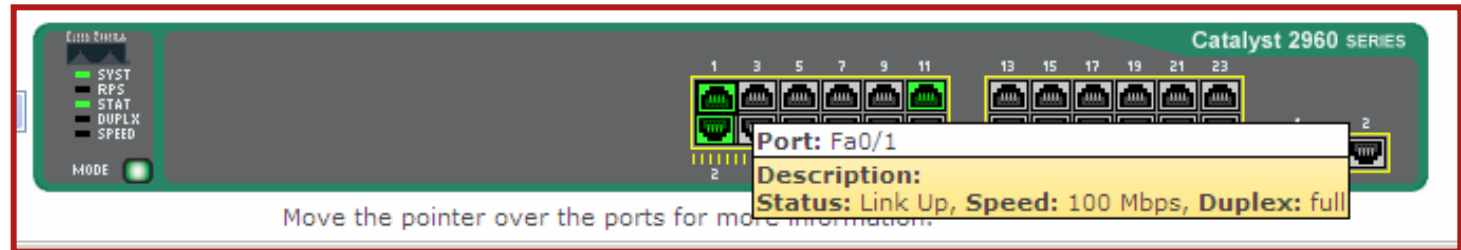
# Device Management Options (Right Click)



How Do You Suppose This Device Property Information Was Obtained?

**Answer: CDP Protocol**

# Device Manager



**Catalyst 2960 Series Device Manager - Switch1** Language: English

Refresh Print Smartports Software Upgrade Legend Help

Uptime: 1 day, 5 hours, 31 minutes Next refresh in 9 seconds

View: Status

Move the pointer over the ports for more information.

**Contents**

- Dashboard
- Configure
- Monitor
- Maintenance
- Network Assistant

**Dashboard**

**Switch Information**

Host Name: Switch1  
Product ID: WS-C2960-24TT-L  
IP Address: 192.168.1.20  
MAC Address: 00:1B:53:08:B1:80  
Version ID: V02  
Serial Number: FOC1108Z5TR  
Software: 12.2(25)SEE2  
Contact:  
Location:

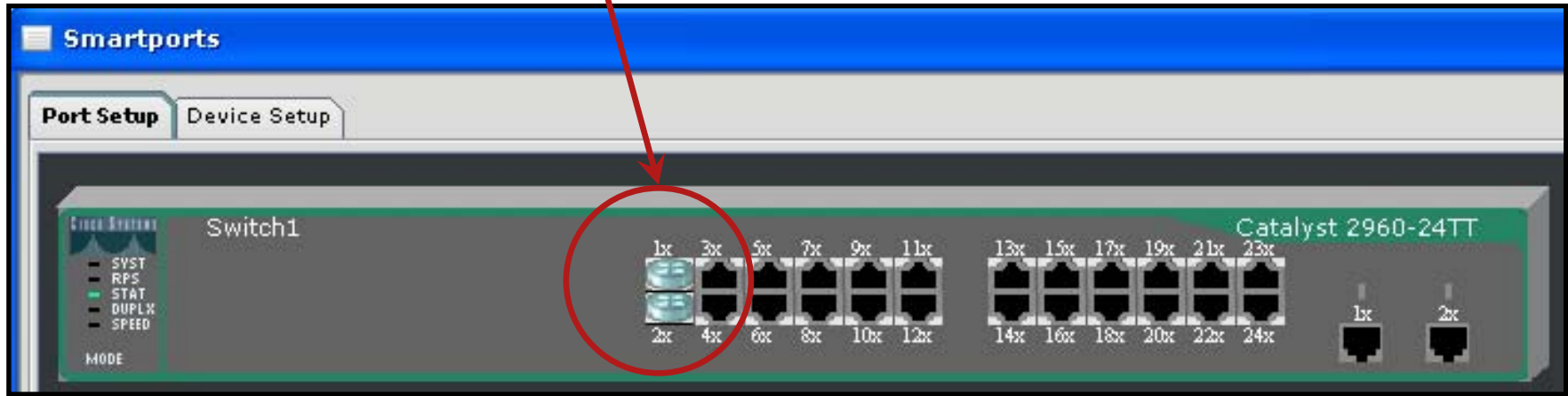
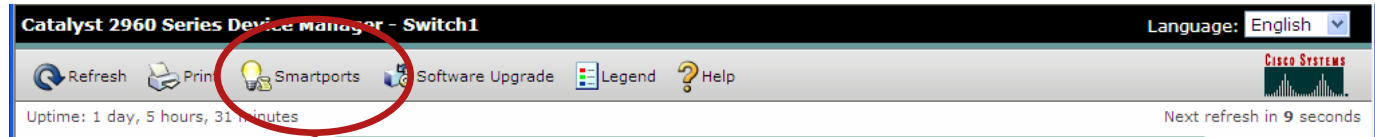
**Switch Health** [View Trends](#)

Bandwidth Used	Packet Error	Fan	Temp
0%	0%	OK	OK

**Port Utilization** [View Trends](#) | [View Port Statistics](#)



# Smartports



Smartports will discovery what Cisco devices are connected to the ports and insert a representative icon over the port, such as a router, switch, or Cisco IP phone

# Feature Bar: Monitor → Reports

The screenshot shows the Cisco Network Assistant interface. The left sidebar has a 'Monitor' section with a 'Reports' sub-section. A red arrow points from 'Inventory...' in the Reports list to the 'Inventory' window. Another red arrow points from 'Link Graphs...' in the Reports list to the 'Link Graphs' window.

**Inventory Table:**

Hostname	Device Type	Serial Number	Version ID	MAC Address	IP Address	Software Version	Sys Location	System Up...
Router2	2811	FTX1118A1MA	V04	001b.d444.8af8	10.0.0.2, 192.16...	12.4(6)T2-ADV-ENTERPRI...		8 hours, 22...
Router1	2811	FTX1118A1L6	V04	001b.d447.2920	10.0.0.1, 192.16...	12.4(6)T2-ADV-ENTERPRI...		8 hours, 22...
Switch1	WS-C2960-24TT-L	FOC110825TR	V02	001b.5308.b180	192.168.1.20	12.2(25)S12.4(6)T2-ADV-ENTERPRISE-CRYPTO		day, 5 ho...

**Link Graphs - Interfaces:**

Hostname: Switch1 Interface: Fa0/1

Type: Bar  Log Scaling Zoom: [Zoom In] [Zoom Out] Data: % Utilization Next poll: 0:03

The graph shows % Utilization on the y-axis (0.00000 to 0.00200) and time on the x-axis (4:20 PM to 4:28 PM). The utilization is low, with a peak of approximately 0.0011 at 4:21 PM.



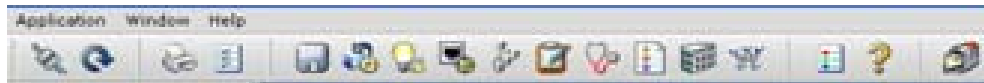
# Router Device Manager

- Router management is limited to what is available on the router
- Example: If SDM is on the router, it will be launched. If not, then only the http server will be launched





# Tool Bar Icons



Connect	Launches the <a href="#">Connect window</a> , where you identify a <a href="#">community</a> or a <a href="#">cluster</a> for Network Assistant to manage.
Refresh	Refreshes the Front Panel view and the Topology view by polling the community members or the <a href="#">command device</a> of the cluster. Network Assistant updates the status of the devices and ports, and displays any new members.
Print	Sends a print file for a graph, a report, or online help selections to a printer.
Preferences	Launches the <a href="#">Preferences window</a> , where you can set user preferences for the user interface.
Save Configuration	Makes permanent the changes that you make to the device configuration; that is, your changes remain in effect after the device is powered off and powered on again.
Software Upgrade	Launches the <a href="#">Software Upgrade window</a> , where you upgrade all the community or cluster members or selected members.
Smartports	Launches the <a href="#">Smartports window</a> , where you configure ports and devices by applying <a href="#">roles</a> . <b>Note:</b> The Smartports feature is not supported on blade switches.
Port Settings	Launches the <a href="#">Port Settings window</a> , where you can view the status of ports on a selected device and modify port settings.
VLAN	Launches the <a href="#">VLAN window</a> , where you can view VLAN information, assign interfaces to VLANs, modify VLAN options, and perform other tasks related to VLANs.
Inventory	Launches the <a href="#">Inventory window</a> , which displays the inventory for the community or cluster—device types, serial numbers, IP addresses, and software versions—or the inventory for a single device.
Health	Launches the <a href="#">Health window</a> , where you can monitor a number of device <i>health</i> measurements to avoid downtime and to ensure that your network is running efficiently.
Event Notification	Launches the <a href="#">Event Notification window</a> , which describes network conditions that you should be aware of and that might require your action.
Front Panel	Launches the <a href="#">Front Panel view</a> , which shows a hierarchical list of the devices in the community or cluster, a wiring-closet graphic of the devices, and the status of each device and its ports.
Topology	Launches the <a href="#">Topology view</a> , which shows a network map of the community or cluster members, and much more, depending on the topology options that you choose.



# Additional Resources

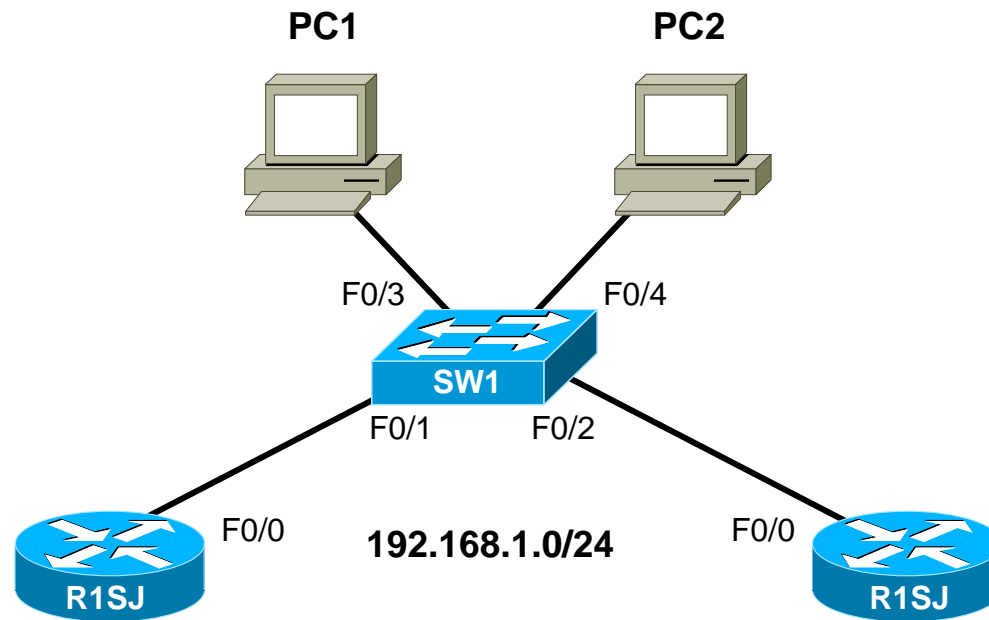
## Cisco Network Assistant Labs:

- Discovery 4 → Lab 2.1.6 Observing Traffic Using Cisco Network Assistant
- Discovery 4 → Lab 2.5.2 Monitoring Network Performance  
[Expands on 2.16]
- Discovery 4 → Lab 3.1.2 Creating a Logical Network Diagram  
[Students discover an unknown precabled and preconfigured network; preferably students only have physical access to the designated “Administrator PC”]

**Note:** This is the only place in both Exploration and Discovery curriculum where Cisco Network Assistant is discussed or used in lab. Suggestion: add it to Exploration 3 and Discovery 3 since this is where switches are covered. If you agree this should be part of the curriculum then submit a request to the online Help Desk.



# LAB Topology

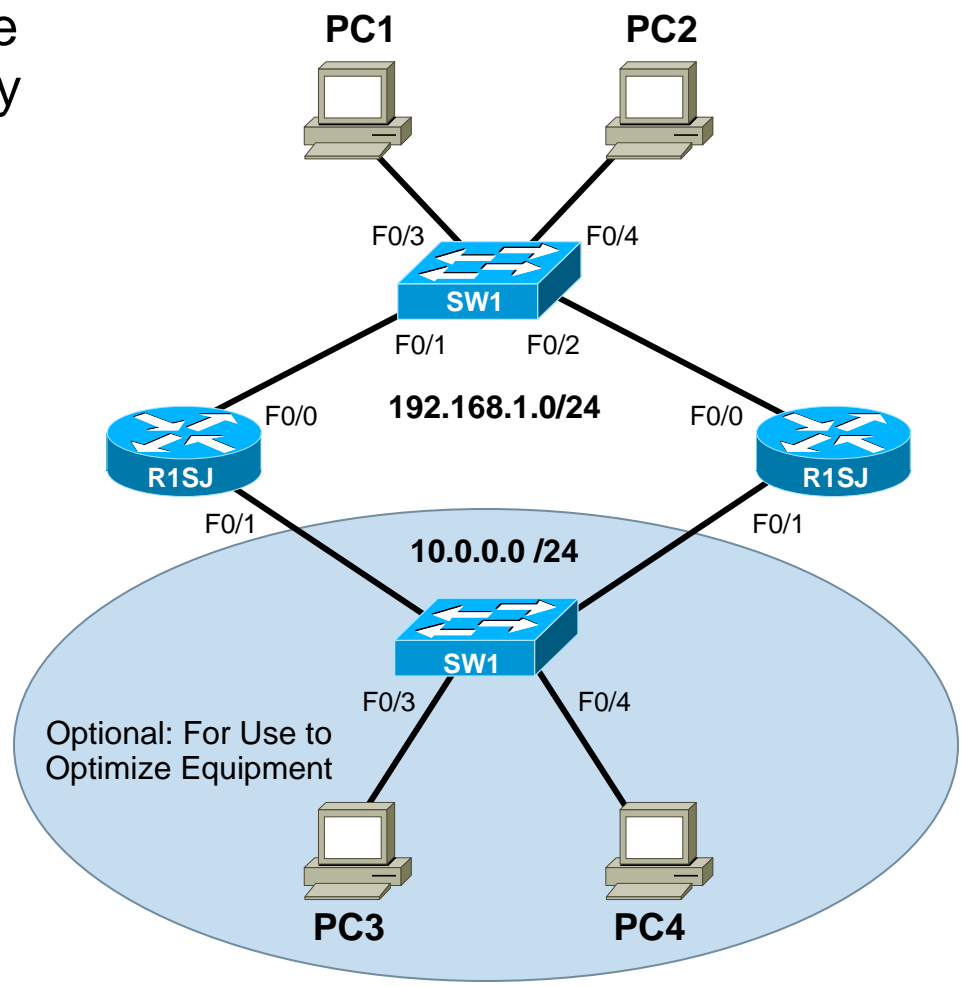


- This topology will be used for both Wireshark and Cisco Network Assistant (CNA)
- Each host can run Wireshark and also CNA



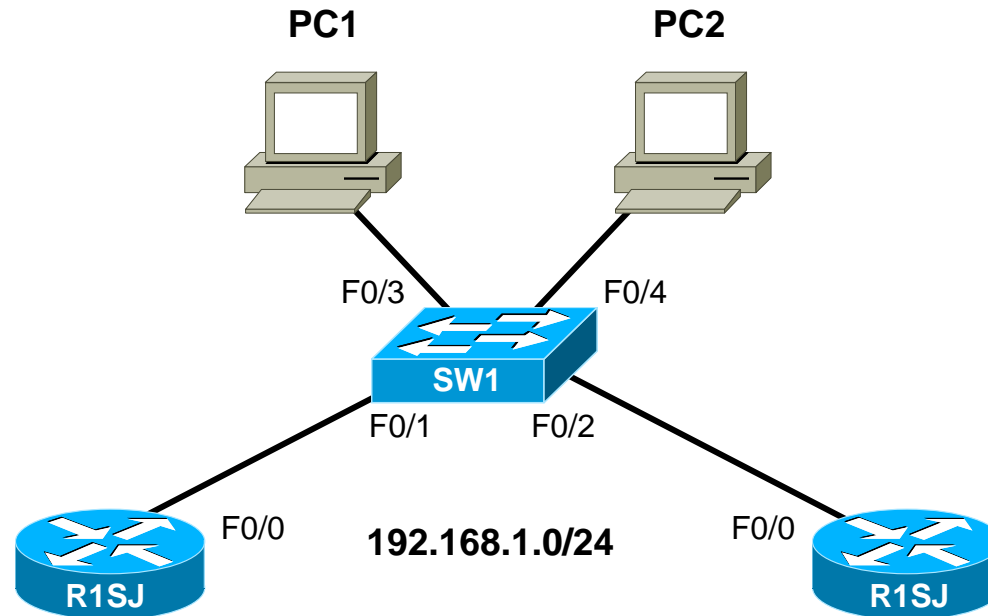
# Alternate Lab Topology

- With the addition of one more switch, this alternate topology provides optimization of equipment to instructors
- The top half is network 192.168.1.0/24 and the bottom half is 10.0.0.0/24
- Each host will work on their subnet, however, it also provides flexibility to expand across subnets





# Demonstration of Lab





# Summary of What We Covered Today?

- **Wireshark**

Purpose of Wireshark is a protocol analyzer that is available to everyone to capture and analyze network traffic

We learned how to Capture PDUs and do basic analysis

Additional resources—VODs and labs in curriculum

- **Cisco Network Assistant (CNA)**

A PC-based network management application that is used to discover, configure, and manage Cisco devices. Critical functions can be monitored and modified through a GUI interface on switches and through Security Device Manager (SDM) on newer routers

The discovery process is a feature that builds a logical network topology of the network

# Q and A



# Cisco | Networking Academy<sup>®</sup>

Mind Wide Open<sup>™</sup>



**CISCO**