



# Characterizing the Existing Network and Sites



## Applying a Methodology to Network Design

# Characterizing the Existing Network and Sites

- Gather documentation and query the organization.
- Perform a site and network assessment to help detail the network.
- Consider performing traffic analysis on the existing network and applications.

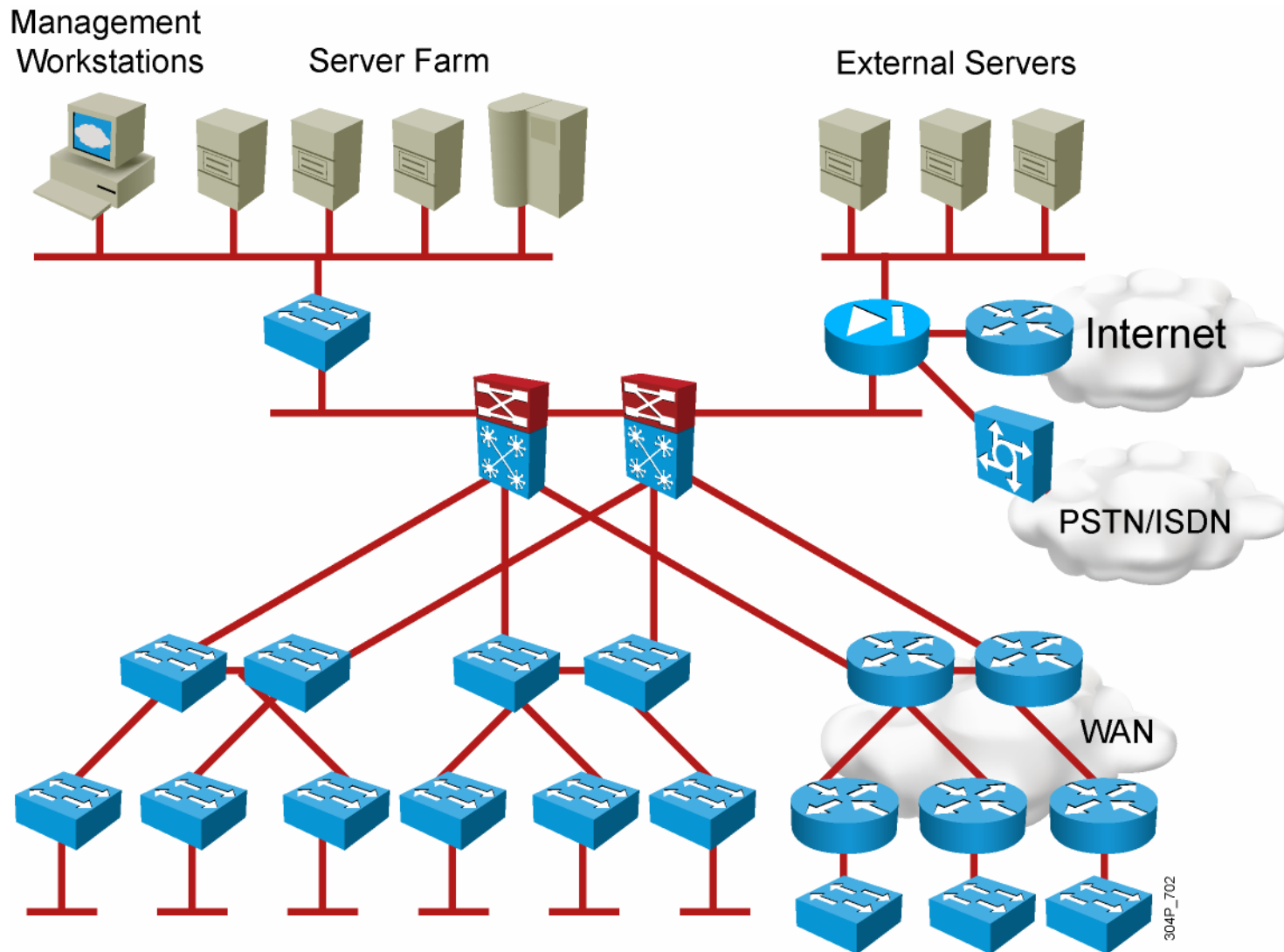
# Identifying Major Features of the Network

- Collect the information about the planned and existing network infrastructure:
  - Site contact information
  - Network topology such as network devices, physical and logical links, external connections, encapsulations, bandwidths, IP addressing, routing protocols
  - Network services such as security, QoS, high availability, IP telephony, storage, and wireless
  - Network applications such as unified communications and video delivery
- Collect the information about expected network functionality.
- Identify network modules based on the given information.

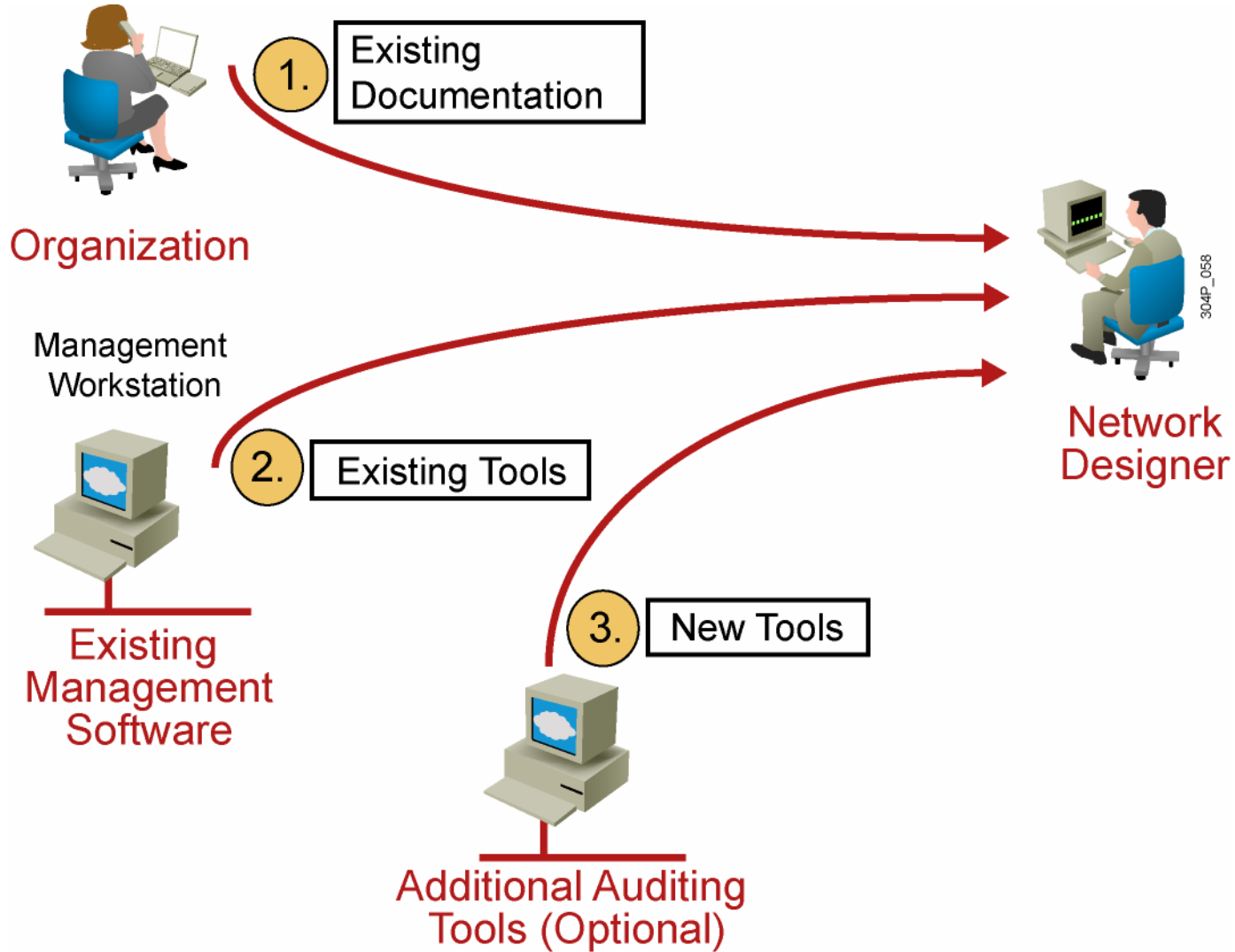
# Sample Site Contact Questions

- What is the site location or name?
- What is the site address?
- What is the shipping address?
- Who is the site contact?
- Is this site owned and maintained by the customer?
- Is this a staffed site?
- What are the hours of operation?
- What are the building or room access procedures?
- Are there any special security or safety procedures?
- Are there any union or labor requirements or procedures?
- What are the locations of the equipment cabinets and racks?

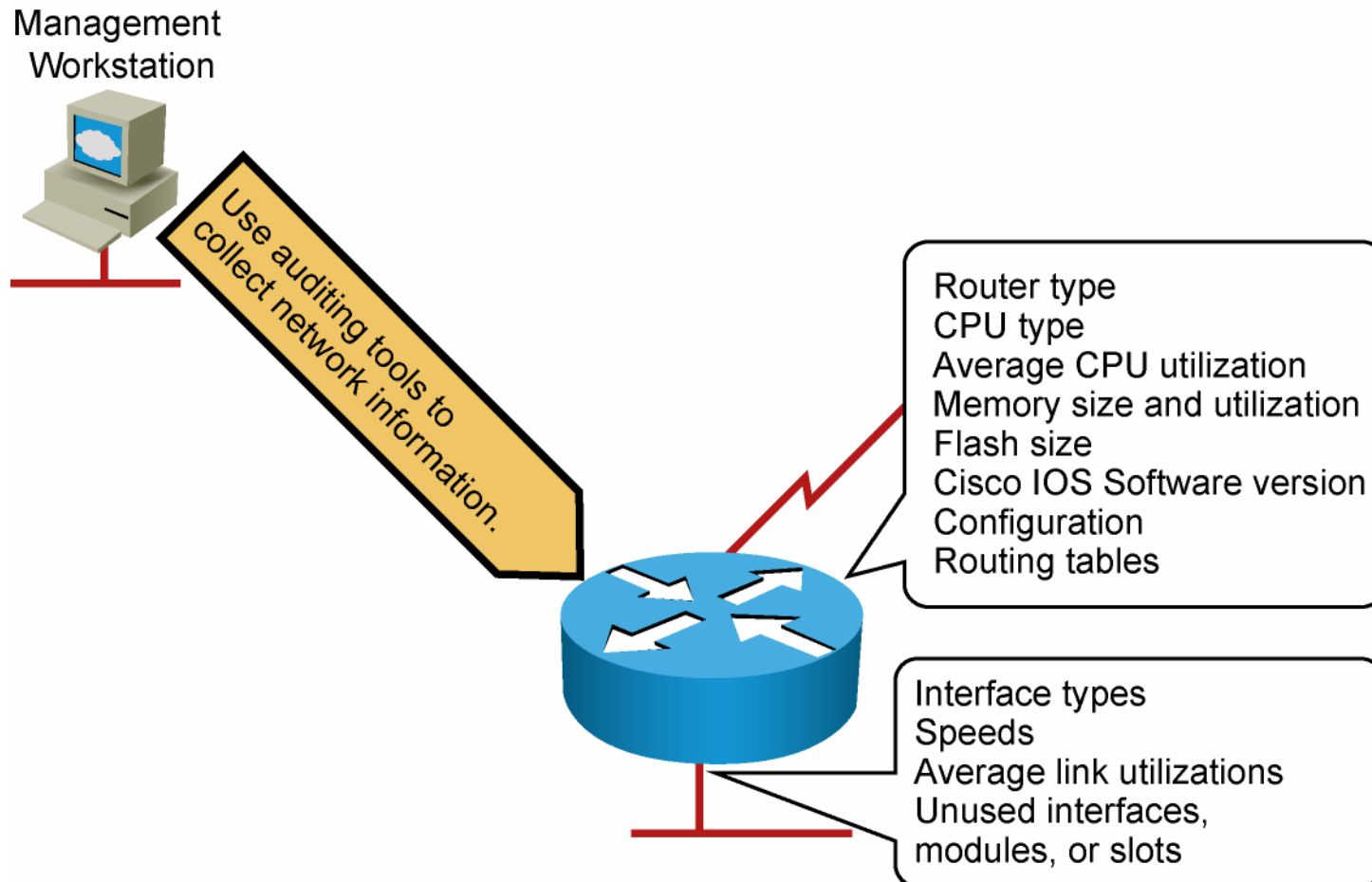
# Example: Customer Network Diagram



# Network Assessment Information Sources



# Example: Network Assessment



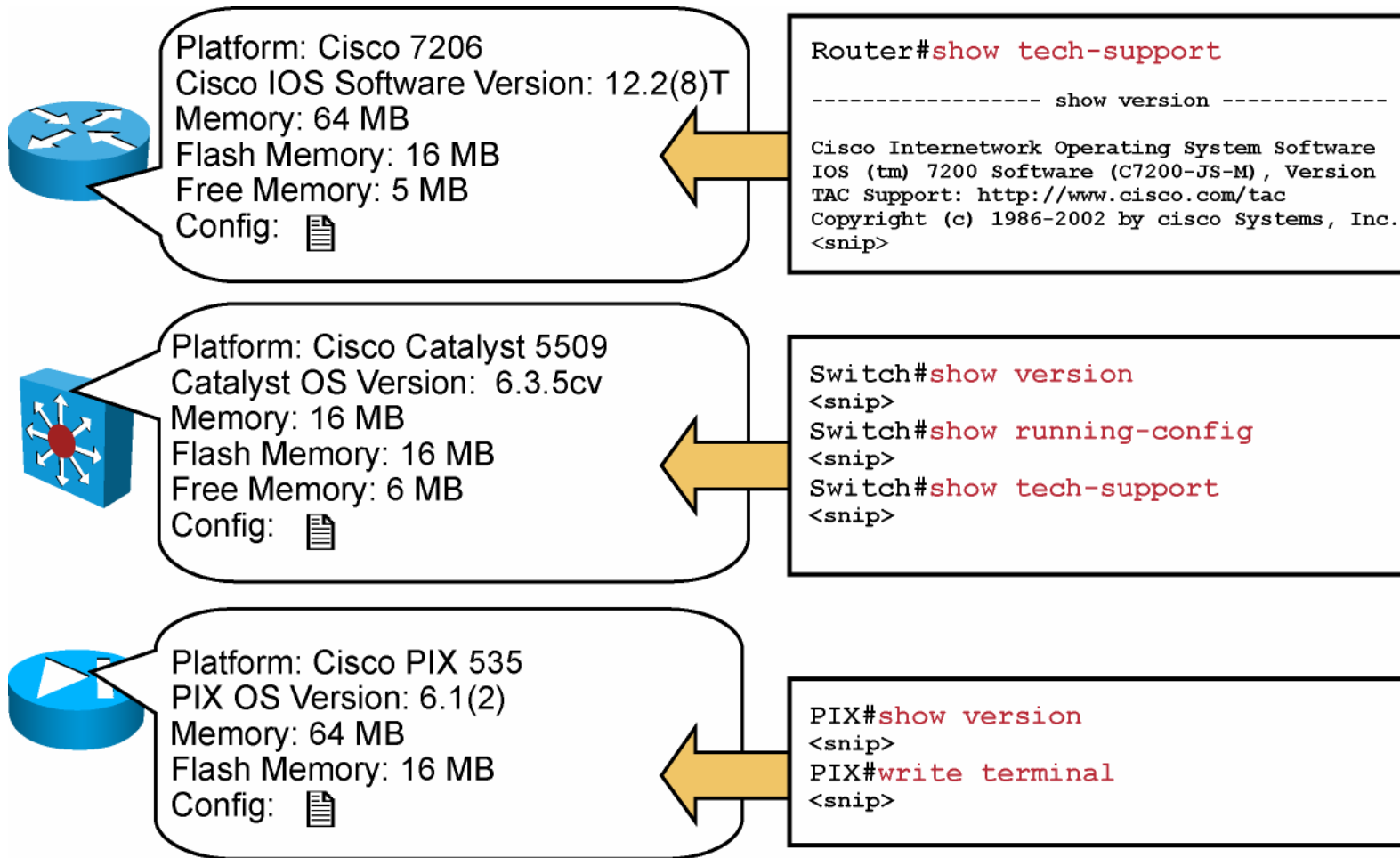
304P\_059



# Network Assessment Tools

- Manual assessment:
  - Use monitoring commands on network devices on small networks.
  - Use scripting tools to collect information on large networks.
- Use existing management and auditing tools:
  - CiscoWorks
  - Third-party tools such as WhatsUp Gold, Castle Rock SNMPc, open source Cacti, Netcordia NetMRI, and NetQoS NetVoyant
- Use other tools to collect relevant information for the network devices:
  - Third-party tools such as Network General Sniffer, AirMagnet software and devices, and WildPackets AiroPeek

# Commands for Manual Information Collection



...

304P\_060

# Example: Manual Information Collection—Router CPU Utilization

```
Router#show processes cpu
```

```
CPU utilization for five seconds: 24%/20%; one minute: 45%; five minutes: 40%
```

PID	Runtime (ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
1	2464	468381	5	0.00%	0.00%	0.00%	0	Load Meter
2	44	44	1000	0.16%	0.04%	0.01%	66	Virtual Exec
3	0	2	0	0.00%	0.00%	0.00%	0	IpSecMibTopN
4	6326689	513354	12324	0.00%	0.25%	0.27%	0	Check heaps
5	0	1	0	0.00%	0.00%	0.00%	0	Chunk Manager
6	60	58	1034	0.00%	0.00%	0.00%	0	Pool Manager
7	0	2	0	0.00%	0.00%	0.00%	0	Timers
8	0	12	0	0.00%	0.00%	0.00%	0	Serial Backgroun
9	2139	468342	4	0.00%	0.00%	0.00%	0	ALARM_TRIGGER_SC
10	3851	78081	49	0.00%	0.00%	0.00%	0	Environmental mo
11	4768	44092	108	0.00%	0.00%	0.00%	0	ARP Input
12	4408	19865	221	0.00%	0.00%	0.00%	0	DDR Timers
13	4	2	2000	0.00%	0.00%	0.00%	0	Dialer event
14	16	2	8000	0.00%	0.00%	0.00%	0	Entity MIB API
15	0	1	0	0.00%	0.00%	0.00%	0	SERIAL A'detect
16	0	1	0	0.00%	0.00%	0.00%	0	Critical Bkgnd
17	57284	377088	151	0.00%	0.00%	0.00%	0	Net Background
18	15916	59331	268	0.00%	0.00%	0.00%	0	Logger

```
<more>
```

004G\_552

# Example: Manual Information Collection—Router Memory Utilization

```

Router# show processes memory
Total:          5611448,          Used: 2307548,  Free: 330390
  PID  TTY  Allocated      Freed      Holding      Getbufs      Retbufs  Process
   0   0    199592        1236      1907220       0           0      *Init*
   0   0         400        76928         400           0           0      *Sched*
   0   0   5431176     3340052     140760     349780           0      *Dead*
   1   0         256         256         1724           0           0    Load Meter
   2   0         264          0         5032           0           0      Exec
   3   0          0          0         2724           0           0    Check heaps
   4   0    97932          0         2852     32760           0    Pool Manager
   5   0         256         256         2724           0           0      Timers
   6   0          92          0         2816           0           0    CXBus hot stall
   7   0          0          0         2724           0           0    IPC Zone Manager
   8   0          0          0         2724           0           0    IPC Realm Manager
   9   0          0          0         2724           0           0    IPC Seat Manager
  10   0         892         476         3256           0           0    ARP Input
  11   0          92          0         2816           0           0    SERIAL A'detect
  12   0         216          0         2940           0           0    Microcode Loader
  13   0          0          0         2724           0           0    RFSS watchdog
  14   0   15659136   15658584     3276           0           0    Env Mon
  .
  .
  .
  77   0         116          0         2844           0           0    IPX-EIGRP Hello
                                     2307224 Total

```

004G\_682

# Example: Automatic Information Collection—Cacti Device List

console graphs

Console -> Devices Logged in as **iberry** (Logout)

Create

New Graphs

Management

Graph Management

Graph Trees

Data Sources

**Devices**

Collection Methods

Data Queries

Data Input Methods

Templates

Graph Templates

Host Templates

Data Templates

Import/Export

Import Templates

Export Templates

Configuration

Settings

Utilities

System Utilities

User Management

Logout User

**Devices** Add

Filter by host template:  Search:

<< Previous Next >>

Showing Rows 1 to 55 of 55 [1]

Description	Status	Hostname	Current (ms)	Average (ms)	Availability	
ADMIN01	Up	172.16.0.9	171.5	87.38	100%	<input type="checkbox"/>
ANNEX-RTR2600-COMCAST	Up	192.168.0.1	66.69	42.11	100%	<input type="checkbox"/>
ANNEX-SW3548-MDF-SW2	Up	172.16.100.3	265.92	324.09	100%	<input type="checkbox"/>
ANNEX-SW6509-MDF-SW1	Up	172.16.100.1	13.63	11.5	100%	<input type="checkbox"/>
BACKUP01	Up	172.16.0.15	2.53	2.52	100%	<input type="checkbox"/>
BORDER01	Up	172.16.0.16	95.17	49.25	100%	<input type="checkbox"/>
CITRIX01	Down	172.16.0.12	0	0	0%	<input type="checkbox"/>
FRANKFORD01	Up	192.168.6.2	8.59	11.01	100%	<input checked="" type="checkbox"/>
GHOST01	Up	172.16.0.17	1000	1000	100%	<input checked="" type="checkbox"/>
GRPWISE	Up	172.16.0.3	3.39	2.93	100%	<input type="checkbox"/>
HS-HPLJ4000-ADMIN	Down	172.16.2.28	0	0	0%	<input type="checkbox"/>
HS-HPLJ4000-LIB	Up	172.16.2.39	12.22	12.71	100%	<input type="checkbox"/>
HS-HPLJ4000-OFF	Up	172.16.2.25	15.22	14.22	100%	<input type="checkbox"/>
HS-HPLJ4000-RM110-1	Up	172.16.2.24	841.32	783.3	100%	<input type="checkbox"/>
HS-HPLJ4000-RM112-1	Down	172.16.2.21	0	0	0%	<input type="checkbox"/>
HS-HPLJ4000-RM112-2	Down	172.16.2.34	0	0	0%	<input type="checkbox"/>
HS-HPLJ4000-RM114-1	Up	172.16.2.22	13.37	13.33	100%	<input checked="" type="checkbox"/>
HS-HPLJ4000-RM114-2	Up	172.16.2.23	10.45	10.45	100%	<input checked="" type="checkbox"/>
HS-HPLJ4000-RM116-1	Down	172.16.2.33	0	0	0%	<input checked="" type="checkbox"/>
HS-HPLJ4000-RM116-2	Down	172.16.2.32	0	0	0%	<input checked="" type="checkbox"/>

# Example: Automatic Information Collection—NetMRI Inventory

**NetMRI™** NetMRI Results Demo Network [Logout](#)

[Reports](#) [Issues](#) [Results](#) [Settings](#) [Tools](#) [Help](#)

**Inventory** Device Type: ALL Device Class: ALL

Model	Cnt
1 3Com stackSwitch4400	1
2 Cisco 3640	1
3 Cisco 3725	1
4 Cisco 7204VXR	1
5 Cisco 7905	14
6 Cisco 7920	1
7 Cisco 7960	42
8 Cisco 7970	10
9 Cisco AIRAP1100	60
10 Cisco AIRAP1210	25
11 Cisco Call Manager	1
12 Cisco CAP340	2
13 Cisco cat3548XL	94
14 Cisco cat4506	21
15 Cisco catalyst2924MXL	4
16 Cisco catalyst29408TT	2

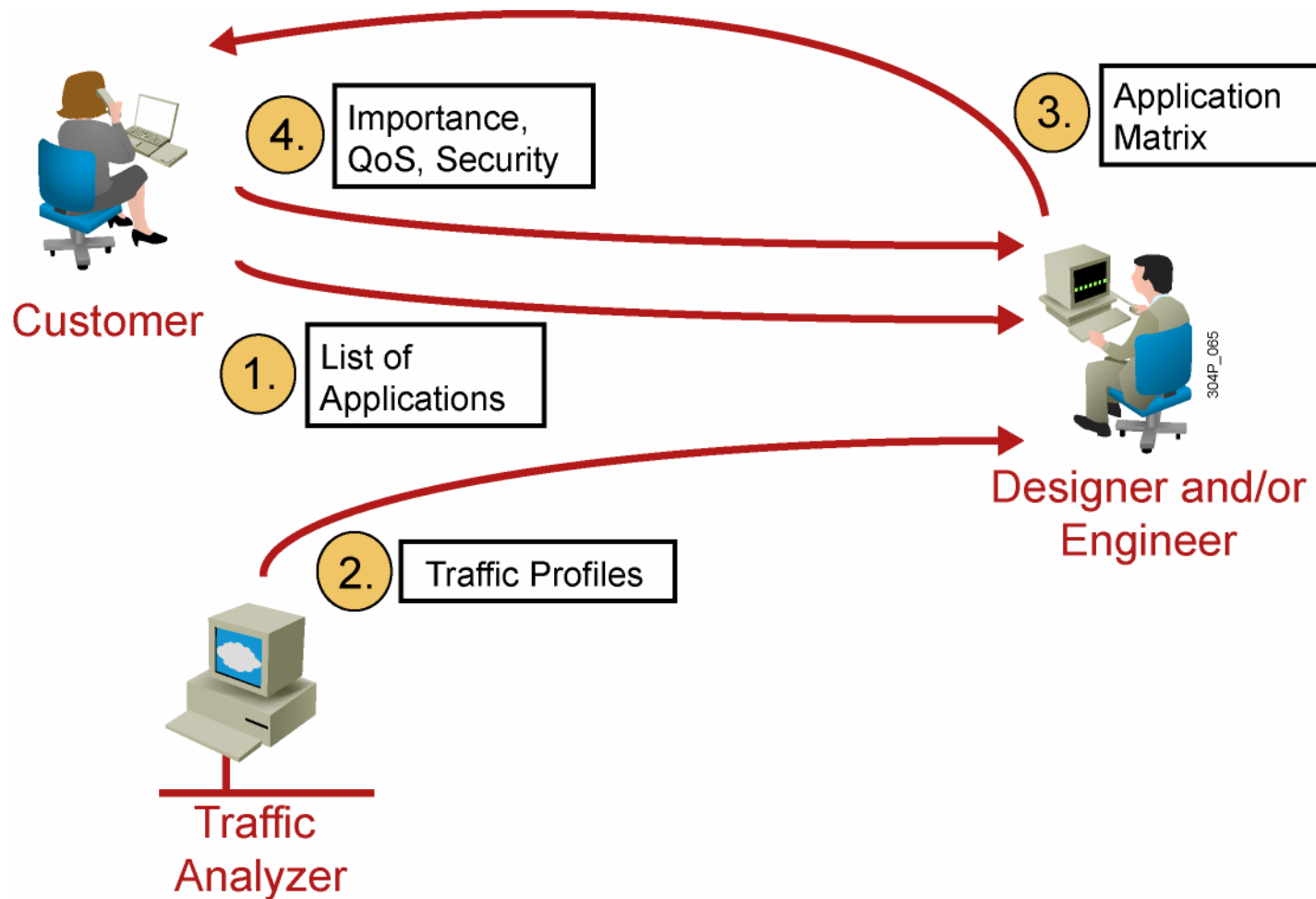
**Cisco cat4506** Rows 1-20 of 21 Standard View: 21/21

IP Address	Device Name	OS Version	Class	Name	Se
1 10.17.8.30	B2-3n-4506-1	12.1(20)EW1			
2 10.20.1.20	t34-2nd-4506-1	12.2(20)EW			
3 10.20.1.30	t34-3rd-4506-1	12.2(20)EW			
4 10.20.1.40	t34-4th-4506-1	12.2(20)EW			
5 10.20.1.50	t34-5th-4506-1	12.2(20)EW			
6 10.20.1.60	t34-6th-4506-1	12.2(20)EW			
7 10.20.1.70	t34-7th-4506-1	12.2(20)EW			
8 10.20.1.80	t34-8th-4506-1	12.2(20)EW			
9 10.56.1.30	tr56-3n-4506-1	12.1(19)EW1			
10 10.56.1.40	tr56-4n-4506-1	12.1(19)EW1			
11 10.56.1.60	tr56-6n-4506-1	12.1(19)EW1			
12 10.56.1.70	tr56-7n-4506-1	12.1(19)EW1			
13 10.56.1.80	tr56-8n-4506-1	12.1(19)EW1			

# Network Traffic Analysis

- Use organizational input to identify the applications used in the existing network and their relative importance.
- Perform a traffic analysis to reveal additional applications used in the network.
- Use the results and organizational input to define QoS and security-related requirements for discovered applications.

# Steps in Analyzing Network Traffic





# Example: Traffic Analysis

## Application No. 8:

- Description: Accounting software
- Protocol: TCP port 5151
- Servers: 2
- Clients: 50
- Scope: Campus
- Importance: High
- Average rate: 50 kbps with 10-second bursts to 1 Mbps

# Network Analysis Tools

- Cisco IOS Software analysis capabilities:
  - NBAR
  - NetFlow
- Cisco software-based network analyzers:
  - Cisco CNS NetFlow Collection Engine
- Third-party tools, such as:
  - Open source Cacti
  - Network General Sniffer
  - WildPackets EtherPeek and AiroPeek
  - SolarWinds Orion
  - Wireshark
  - RMON probes

# Example: NBAR Printout

```
Router#show ip nbar protocol-discovery
```

```
FastEthernet0/0.2
```

Protocol	Input		Output	
	Packet Count	Byte Count	Packet Count	Byte Count
-----				
	30 second bit rate (bps)		30 second bit rate (bps)	
-----				
http	46384	5073520	79364	64042528
	305		1655	
secure-http	2762	429195	2886	1486350
	0		0	
snmp	143	17573	10676	1679322
	0		0	
telnet	1272	122284	12147	988834
	0		0	
ntp	5383	624428	0	0
	0		0	
dns	305	31573	235	55690
	50		120	
23412	2632	15404	0	0 Net Background

<more>

004G\_564

# Example: Cisco IOS NetFlow Printout

```
Router#show ip cache flow
IP packet size distribution (12718M total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
    .000 .554 .042 .017 .015 .009 .009 .009 .013 .030 .006 .007 .005 .004 .004

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
    .003 .007 .139 .019 .098 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 4456448 bytes
65509 active, 27 inactive, 820628747 added
955454490 ager polls, 0 flow alloc failures
Exporting flows to 1.1.15.1 (2057)
820563238 flows exported in 34485239 udp datagrams, 0 failed
last clearing of statistics 00:00:03
```

Protocol	Total	Flows	Packets	Bytes	Packets	Active (Sec)	Idle (Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	2656855	4.3	86	78	372.3	49.6	27.6
TCP-FTP	5900082	9.5	9	71	86.8	11.4	33.1
TCP-FTPD	3200453	5.1	193	461	1006.3	45.8	33.4
TCP-WWW	546778274	887.3	12	325	11170.8	8.0	32.3
TCP-SMTP	25536863	41.4	21	283	876.5	10.9	31.3
TCP-BGP	24520	0.0	28	216	1.1	26.2	39.0
TCP-other	49148540	79.7	47	338	3752.6	30.7	32.2
UDP-DNS	117240379	190.2	3	112	570.8	7.5	34.7
UDP-NTP	9378269	15.2	1	76	16.2	2.2	38.7
UDP-TFTP	8077	0.0	3	62	0.0	9.7	33.2
UDP-Frag	51161	0.0	14	322	1.2	11.0	39.4
ICMP	14837957	24.0	5	224	125.8	12.1	34.3
IP-other	77406	0.1	47	259	5.9	52.4	27.0
...							
<b>Total:</b>	<b>820563238</b>	<b>1331.7</b>	<b>15</b>	<b>304</b>	<b>20633.0</b>	<b>9.8</b>	<b>33.0</b>

004G\_565

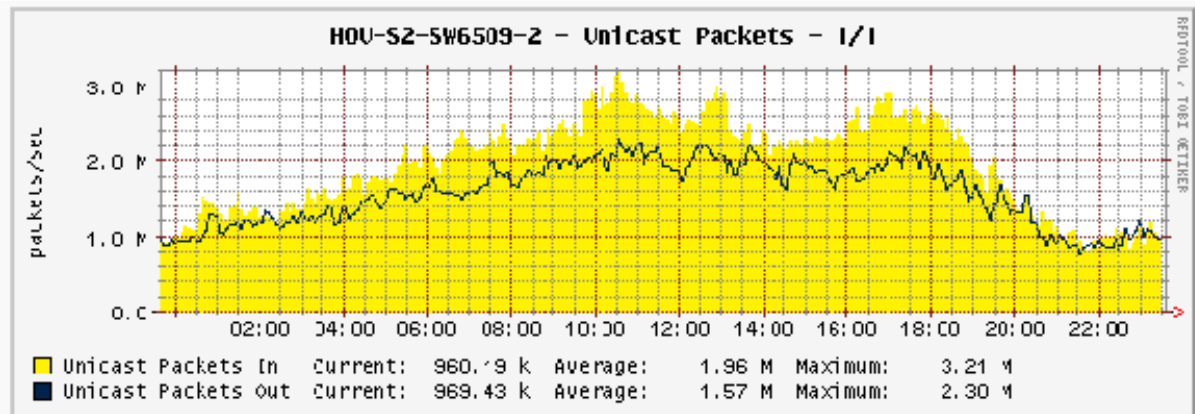
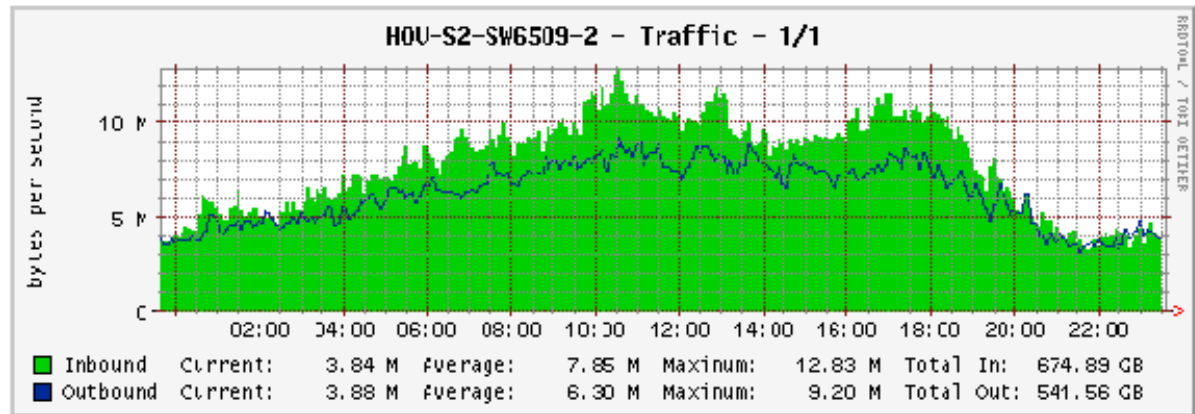
# Example: Cacti Graph

- [-] Arlington, MA
- [-] Charlotte, NC
- [-] Charlottesville, VA
- [-] Columbus, GA
- [-] Dallas, TX
  - [-] Switches
    - Host: HOU-S2-SW3548-1
    - Host: HOU-S2-SW6509-2**
  - [-] Data Center Core
    - Host: HOU-A4-ATM-1
    - Host: HOU-A4-ATM-2
    - Host: HOU-A4-ATM-3
    - Host: HOU-A4-ATM-4
- [-] Dayton, OH
- [-] Detroit, MI
- [-] Harrisburg, PA
  - [-] Web Hosting Farm
    - Host: HAR-CUS1-WWW0
    - Host: HAR-CUST-WWW1
    - Host: HAR-CUST-WWW2
    - Host: HAR-CUST-WWW3
    - Host: HAR-CUST-WWW4
    - Host: HAR-CUST-WWW5

Tree: Dallas, TX -> Host: HOU-S2-SW6509-2

Data Query: SNMP - Interface Statistics

Port 1/1



# Example: Solarwinds Orion

The screenshot displays the Solarwinds Orion Network Management Tools interface. At the top, there is a navigation bar with the Solarwinds logo and the text 'SOLARWINDS.NET Network Management Tools'. Below this is a secondary navigation bar with 'Network Performance Monitor' and a menu with items: Home, Top 10, OverView, Events, Alerts, SysLog, Reports, Logout, Help. A 'Powered By SOLARWINDS.NET' logo is on the right. The main content area is titled 'Current Percent Utilization - Top 25 Interfaces' and includes a 'PRINTABLE VERSION' button. A table lists the top 25 interfaces with columns for Node, Interface, Average Xmit+Recv Percent Utilization, Status, Transmit Traffic, and Receive Traffic.

Node	Interface	Average Xmit+Recv Percent Utilization	Status	Transmit Traffic	Receive Traffic
sw1.atl1	FastEthernet40	8 %	●	8.96 Mbps	8.71 Mbps
www2.SolarWinds.Net	TEAM : InternetTeam	8 %	●	15 Mbps	409 Kbps
gsacoc	Serial0.1	7 %	●	55 Kbps	162 Kbps
gsacoc	Serial0	6 %	●	71 Kbps	137 Kbps
sw1.atl1	FastEthernet48	6 %	●	6.65 Mbps	6.51 Mbps
dilbert	PIX Firewall 'inside' interface	5 %	●	746 Kbps	246 Kbps
Gateway	Serial0	4 %	●	22.8 Kbps	104 Kbps
dilbert	PIX Firewall 'outside' interface	4 %	●	340 Kbps	495 Kbps
ratmcma	Tunnel10516	2 %	●	253 bps	248 bps
www3.solarwinds.net	Intel(R) PRO/100 S Desktop Adapter	2 %	●	3.84 Mbps	141 Kbps
ratmcma	Tunnel16	2 %	●	253 bps	176 bps
sw1.atl1	FastEthernet32	1 %	●	1.39 Mbps	840 Kbps

# Summary Report

Characterization of the existing network results in a summary report that is used to:

- Describe the software features required in the network
- Describe possible problems in the existing network
- Identify the actions needed to prepare the network for the implementation of the required features
- Influence the customer requirements

# Example: Equipment Summary Report

The network uses 895 routers:

- 655 routers use Cisco IOS Software Release 12.2(10).
- 240 routers use an older Cisco IOS Software version.



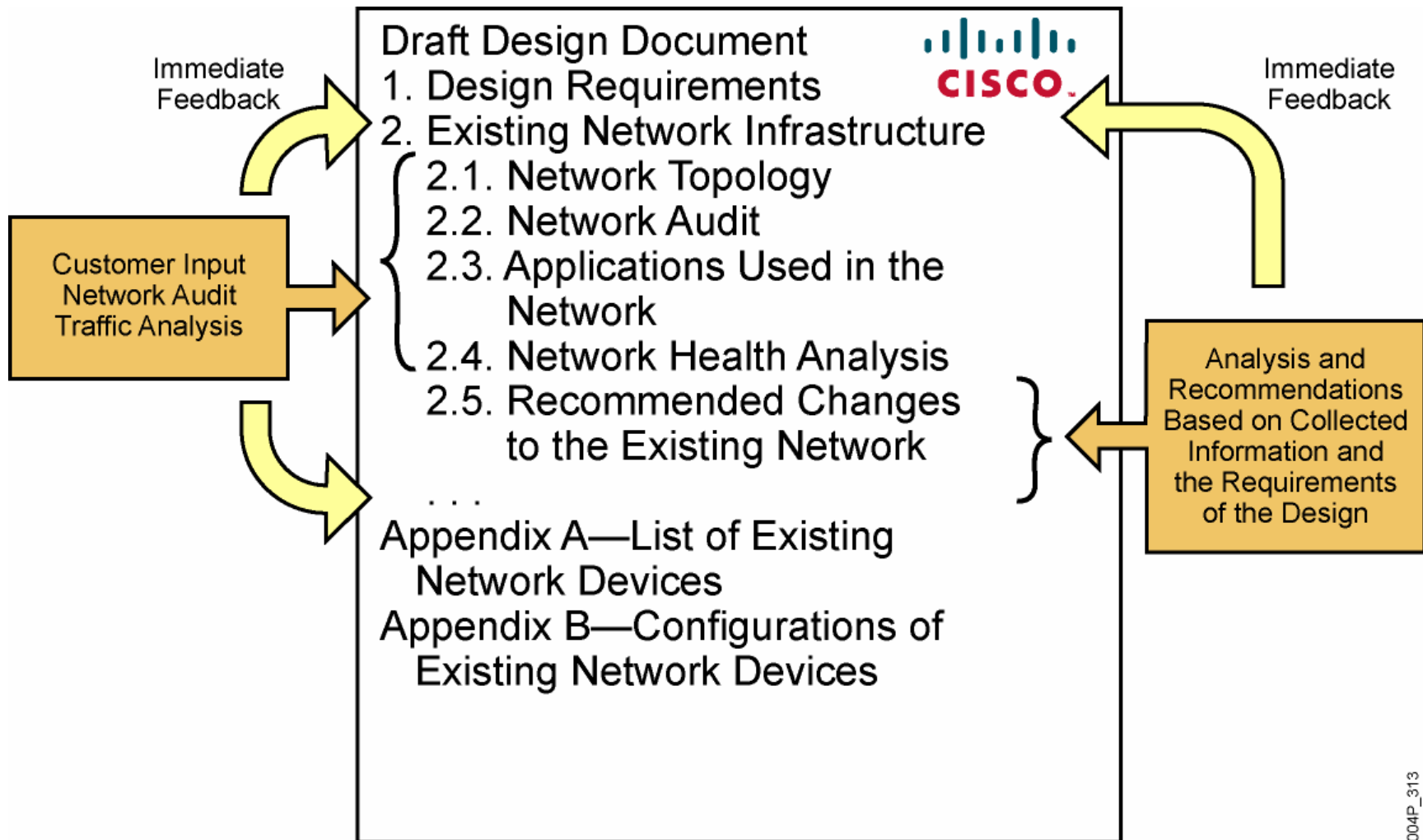
# Example: Summary Report Problem Statement

- Requirement: Queuing in the WAN
- Identified problem:
  - Existing Cisco IOS Software version does not support new queuing technologies.
  - 15 out of 19 routers with older Cisco IOS Software are in the WAN.
  - 12 out of 15 routers do not have enough memory to upgrade to Cisco IOS Software Release 12.3 or later.
  - 5 out of 15 routers do not have enough flash memory to upgrade to Cisco IOS Software Release 12.3 or later.

# Example: Summary Report Recommendations

- Recommended action:
  - 12 memory upgrades to 64 MB
  - 5 flash memory upgrades to 16 MB
- Options:
  - Replace hardware and software to support queuing.
  - Find an alternative mechanism for that part of the network.
  - Find an alternative mechanism and use it instead of queuing.
  - Evaluate the consequences of not implementing the required feature in that part of the network.

# Documenting an Existing Network



004P\_313

# Network Characterization Hour Estimates

	Small Network 1–20 Switches/Routers		Medium Network 20–200 Switches/Routers		Large Network 200–800 Switches/Routers		Huge Network >800 Switches/Routers	
a) Interview management team	4	4	8	8	12	12	16	16
b) Interview network team	4	4	6	6	8	12	24	24
c) Review documentation	4	4	6	6	8	12	16	16
d) Set up network discovery tool	4	4	6	6	8	8	16	16
e) Resolve SNMP access and similar problems	4	4	8	16	16	48	80	160
f) Allow tools to gather data								
g) Analyze captured data	4	8	16	16	24	24	40	40
h) Prepare high level Layer 3 diagrams	4	4	4	8	8	16	16	32
i) Prepare report stating conclusions	16	16	32	32	48	48	80	80
j) Incrementally prepare network diagrams								
Estimated manpower in hours	44–48		86–98		132–180		288–384	

# Summary

- Characterizing an existing network entails gathering as much information about the network as possible. Organization input, a network audit, and traffic analysis provide the key information that you need.
- Identifying major features of the network involves gathering network documentation and querying the organization.
- The auditing process adds detail to the initial network documentation that you created from existing documentation and customer input.
- You can manually audit a small network, but you typically need automated tools to audit a large network.
- Traffic analysis verifies the set of applications and protocols used in the network and determines the traffic patterns of the applications.

## Summary (Cont.)

- Tools used for traffic analysis range from manual identification of applications using Cisco IOS Software commands in combination with NBAR or NetFlow to those where dedicated software- or hardware-based analyzers capture live packets or SNMP data.
- The result of the network characterization is a summary report describing the health of the network.

