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.

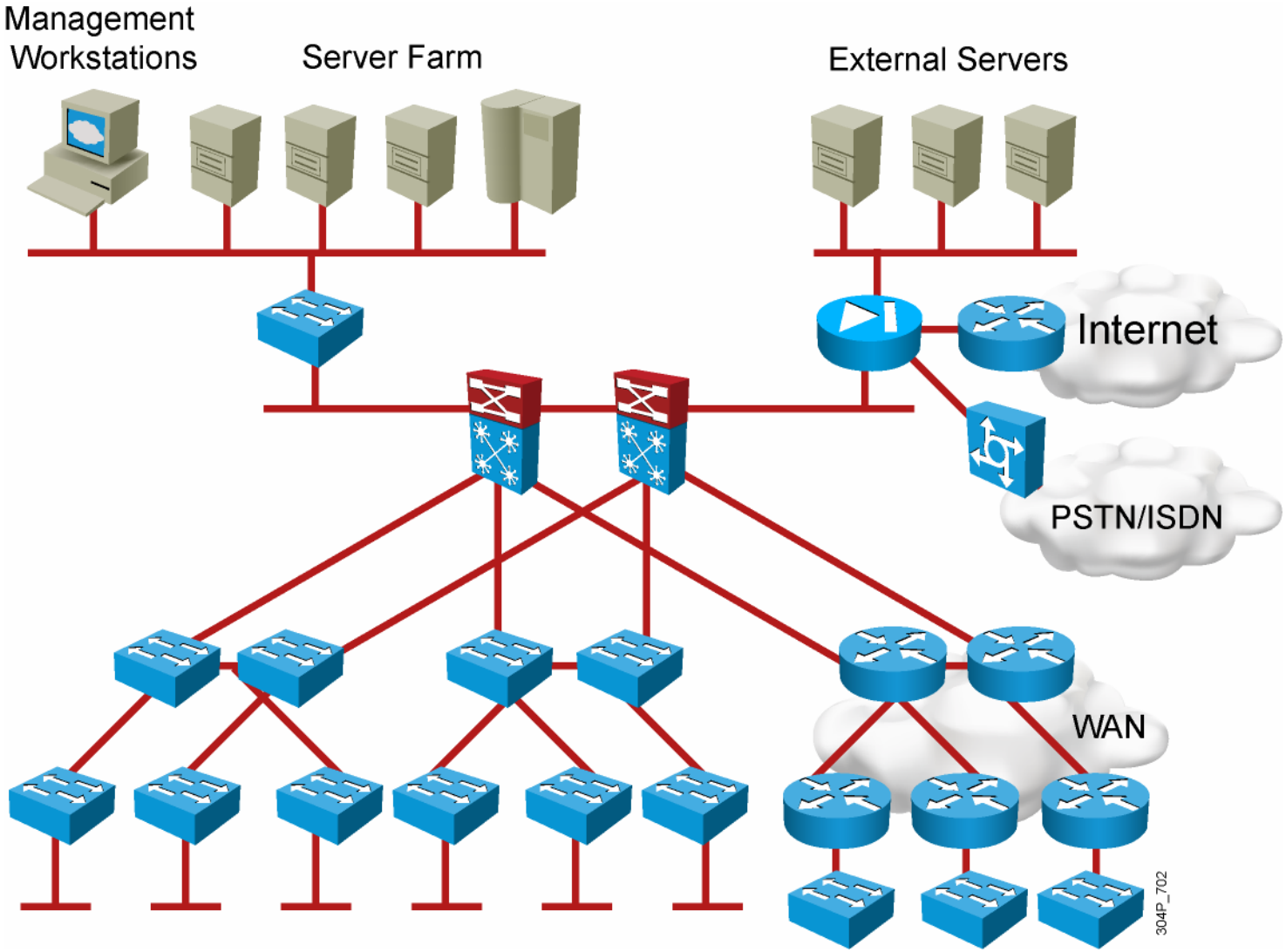
Identifying Major Features of the Network

- 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.

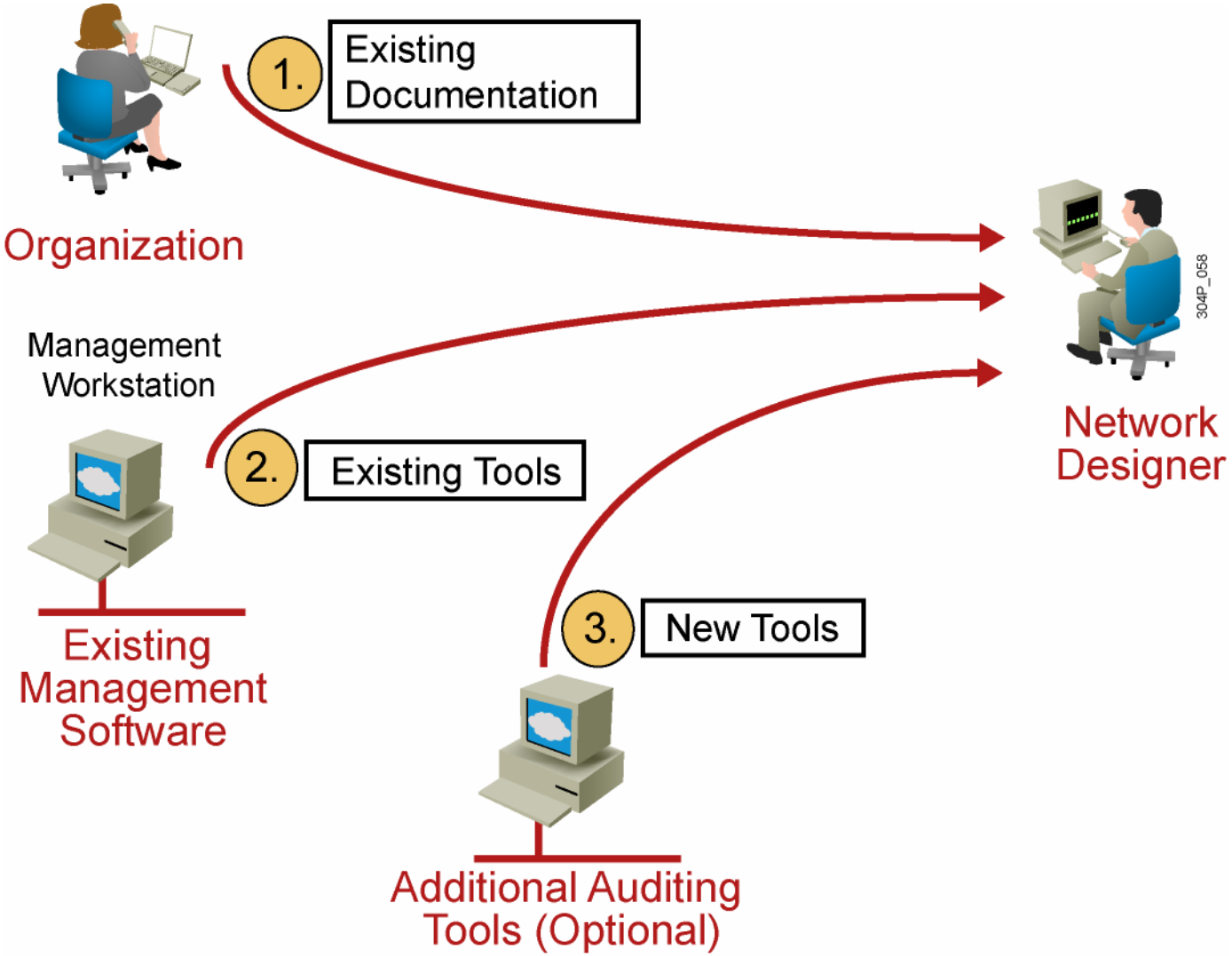
Sample Site Contact Questions

- 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?

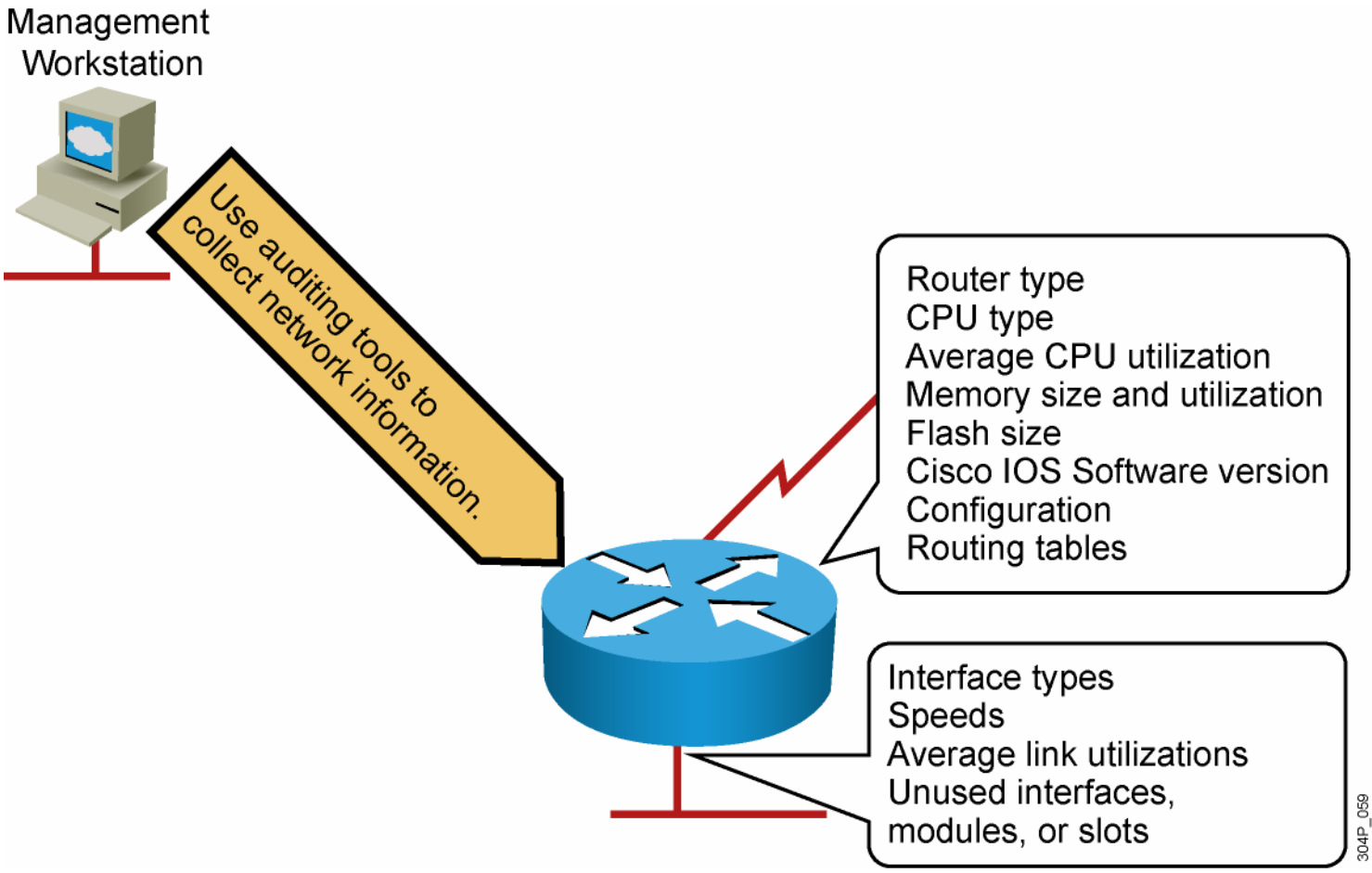
Example: Customer Network Diagram



Network Assessment Information Sources



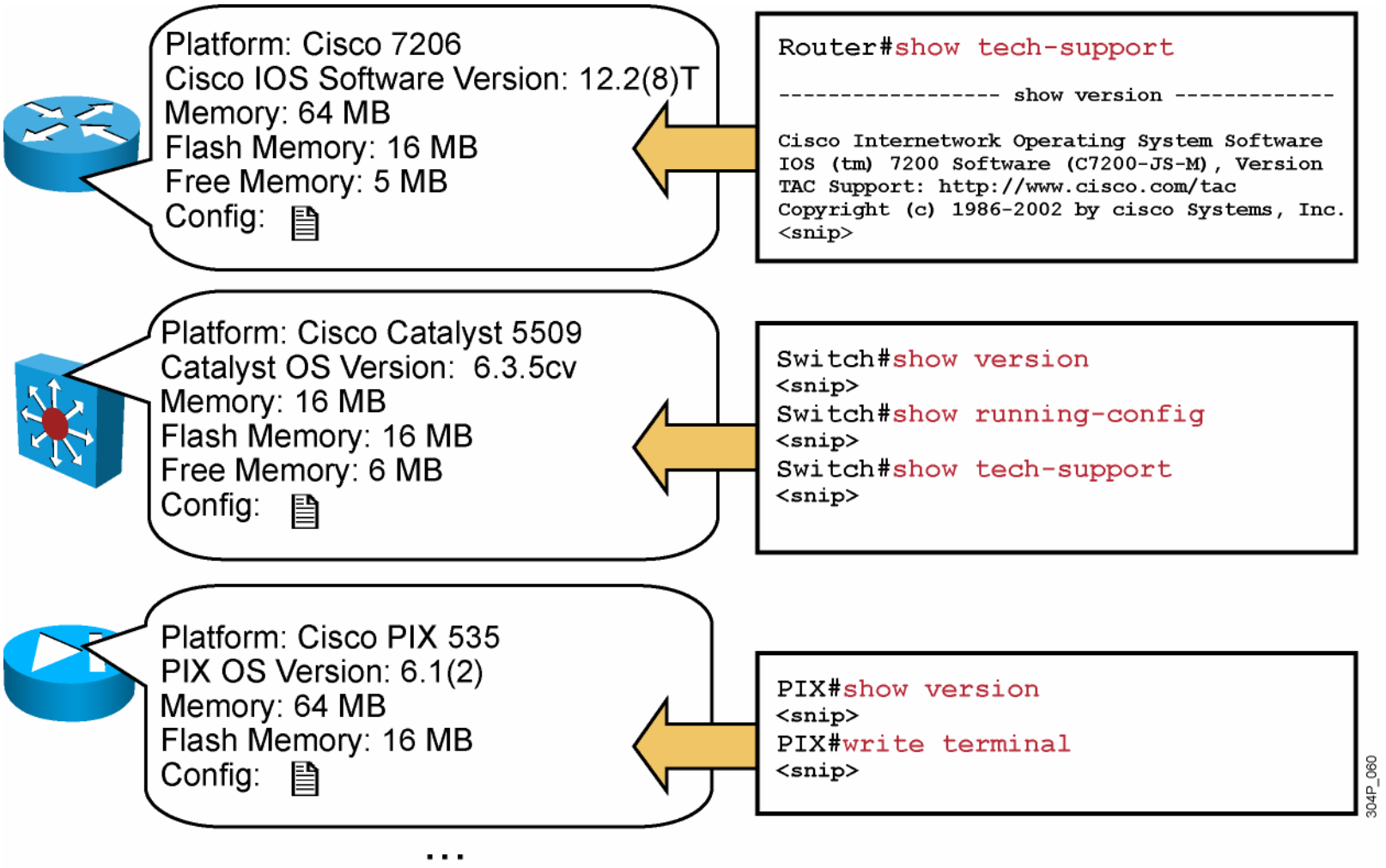
Example: Network Assessment



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



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

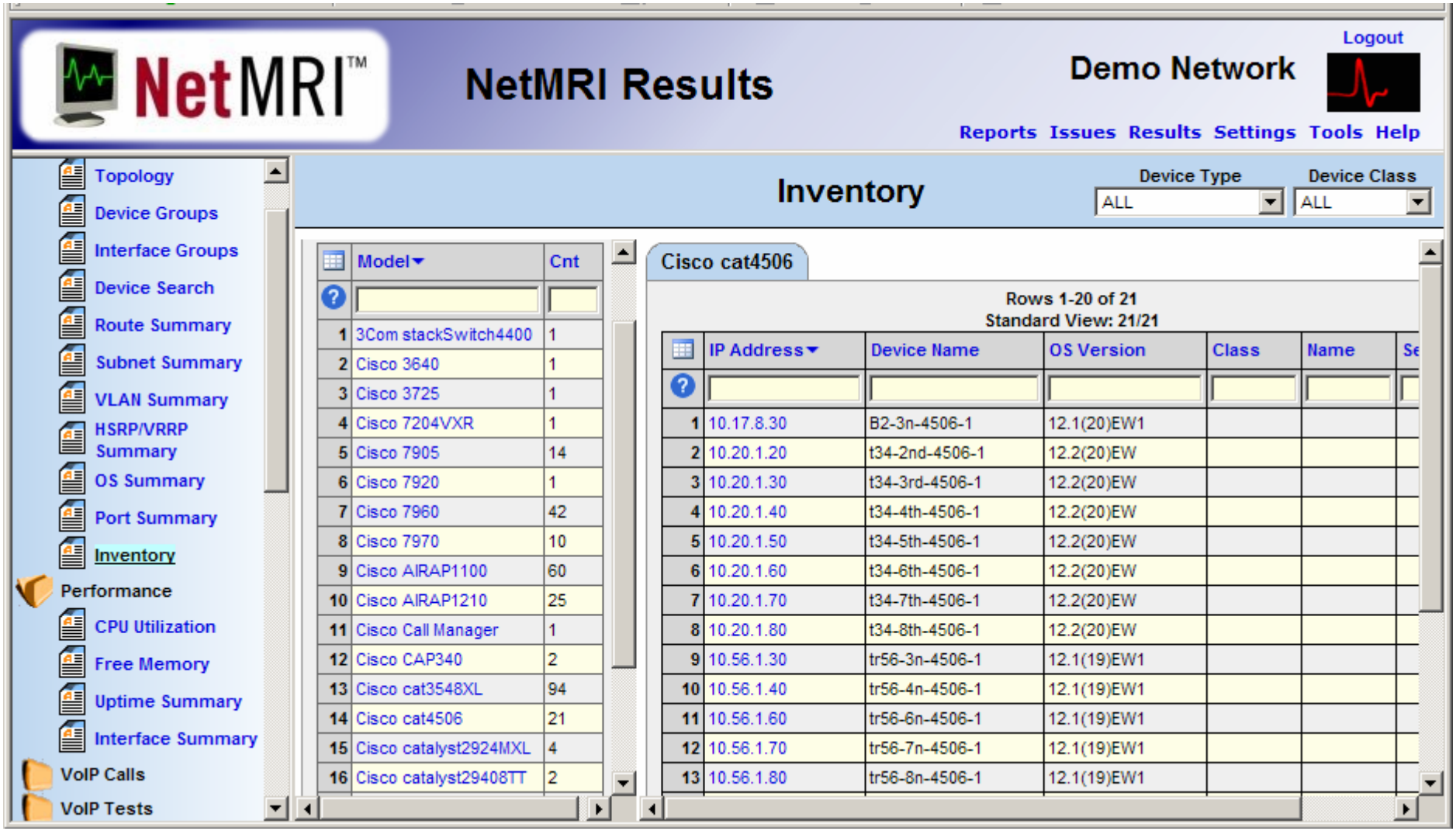
Example: Manual Information Collection—Router Memory Utilization

```
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

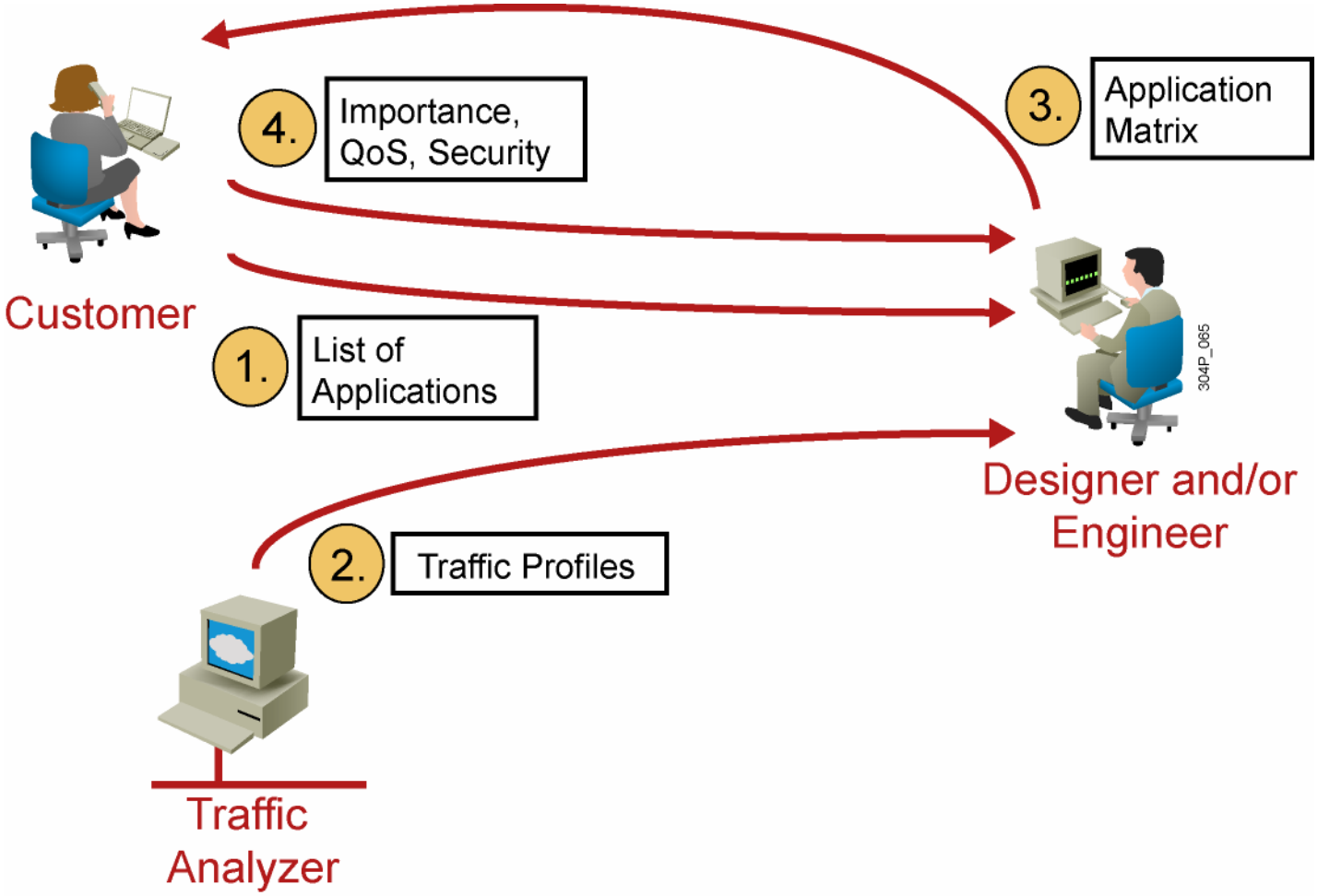
Example: Automatic Information Collection—NetMRI Inventory



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

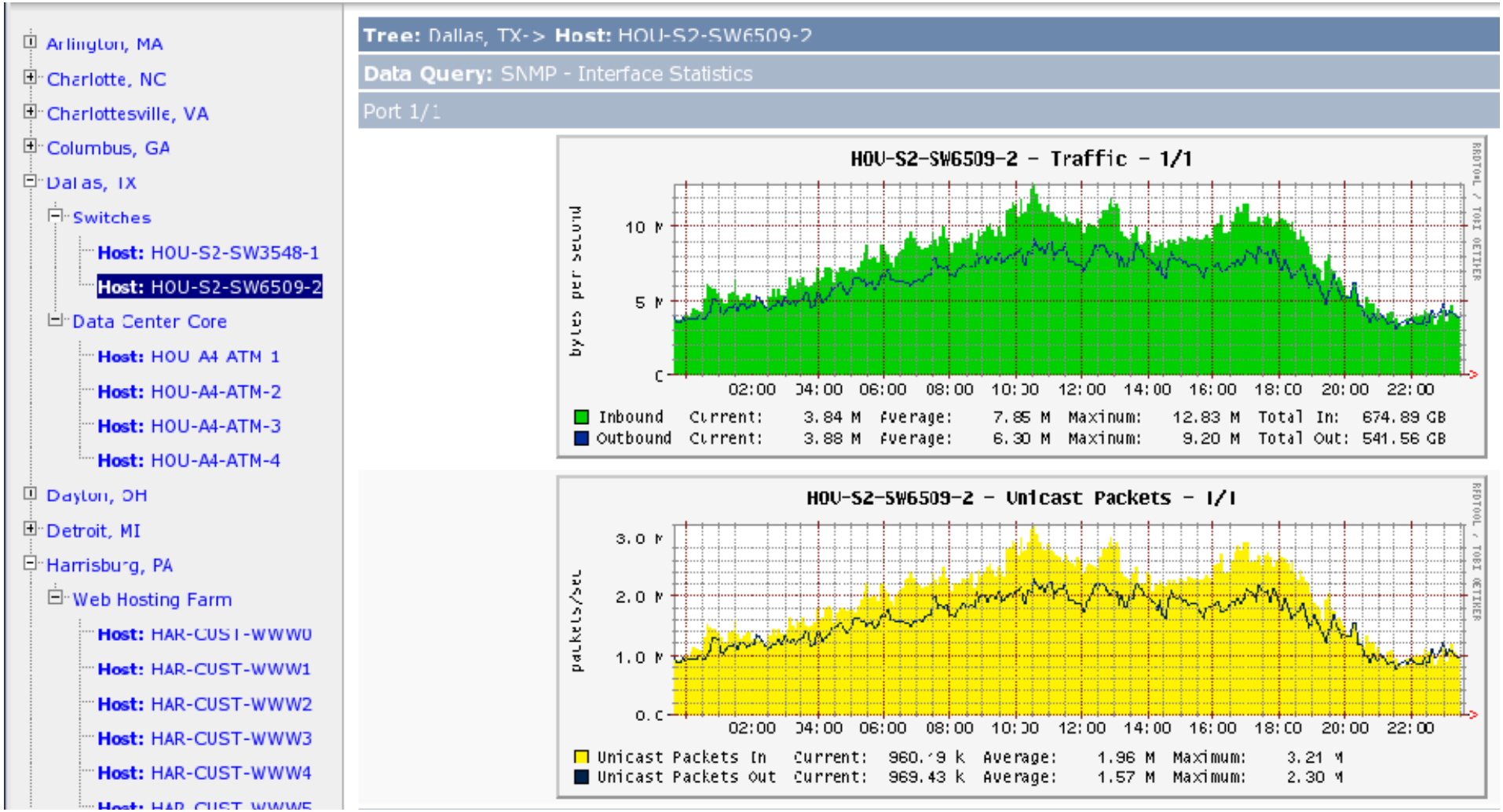
004G_554

Example: Cisco IOS NetFlow Printout

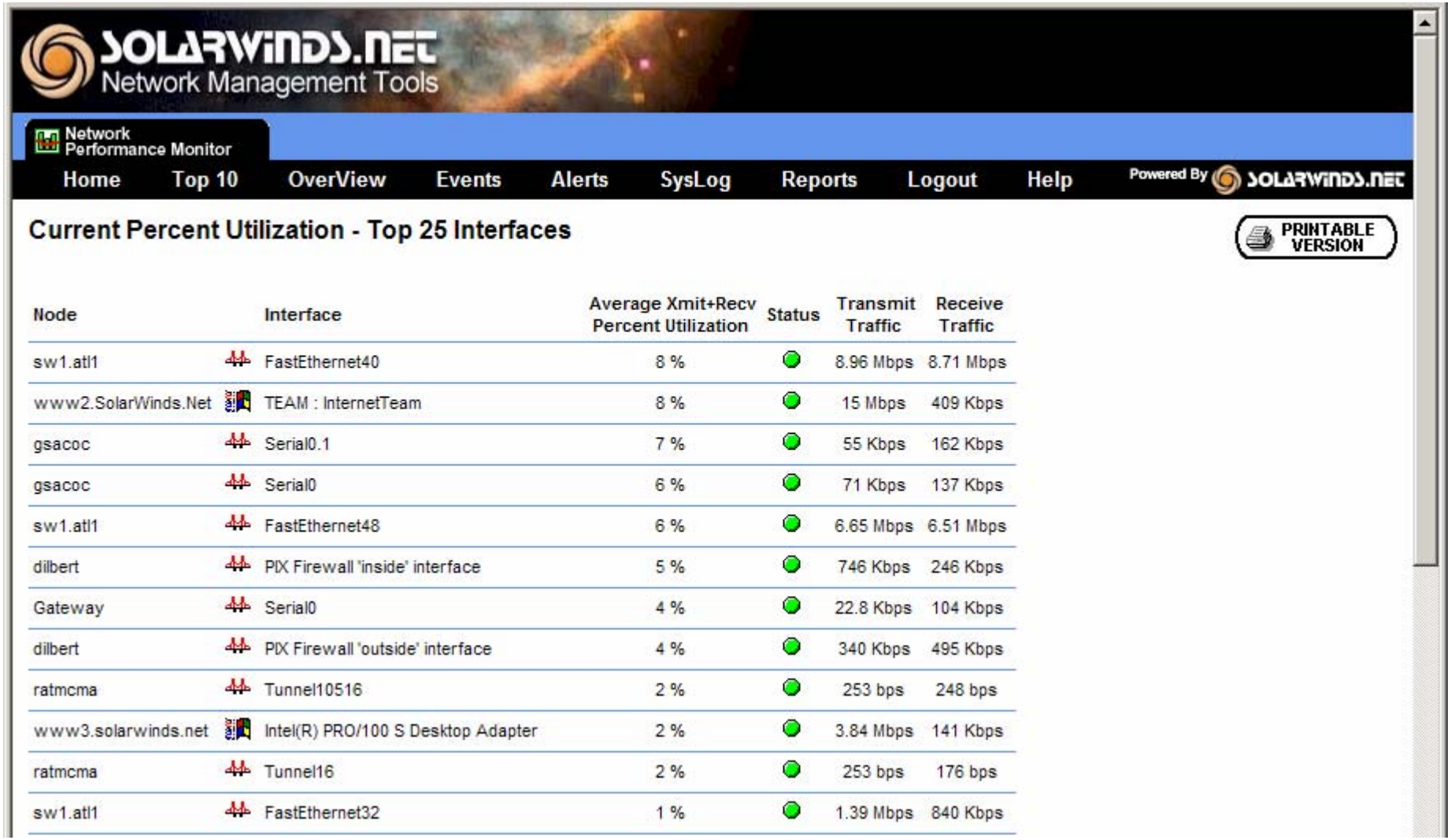
```
Router#show ip cache flow
IP packet size distribution (12718M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .554 .042 .017 .015 .009 .009 .009 .013 .030 .006 .007 .005 .004 .004

    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
...
Total:        820563238  1331.7        15   304  20633.0       9.8      33.0
```

004G_555

Example: Cacti Graph



Example: Solarwinds Orion



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.

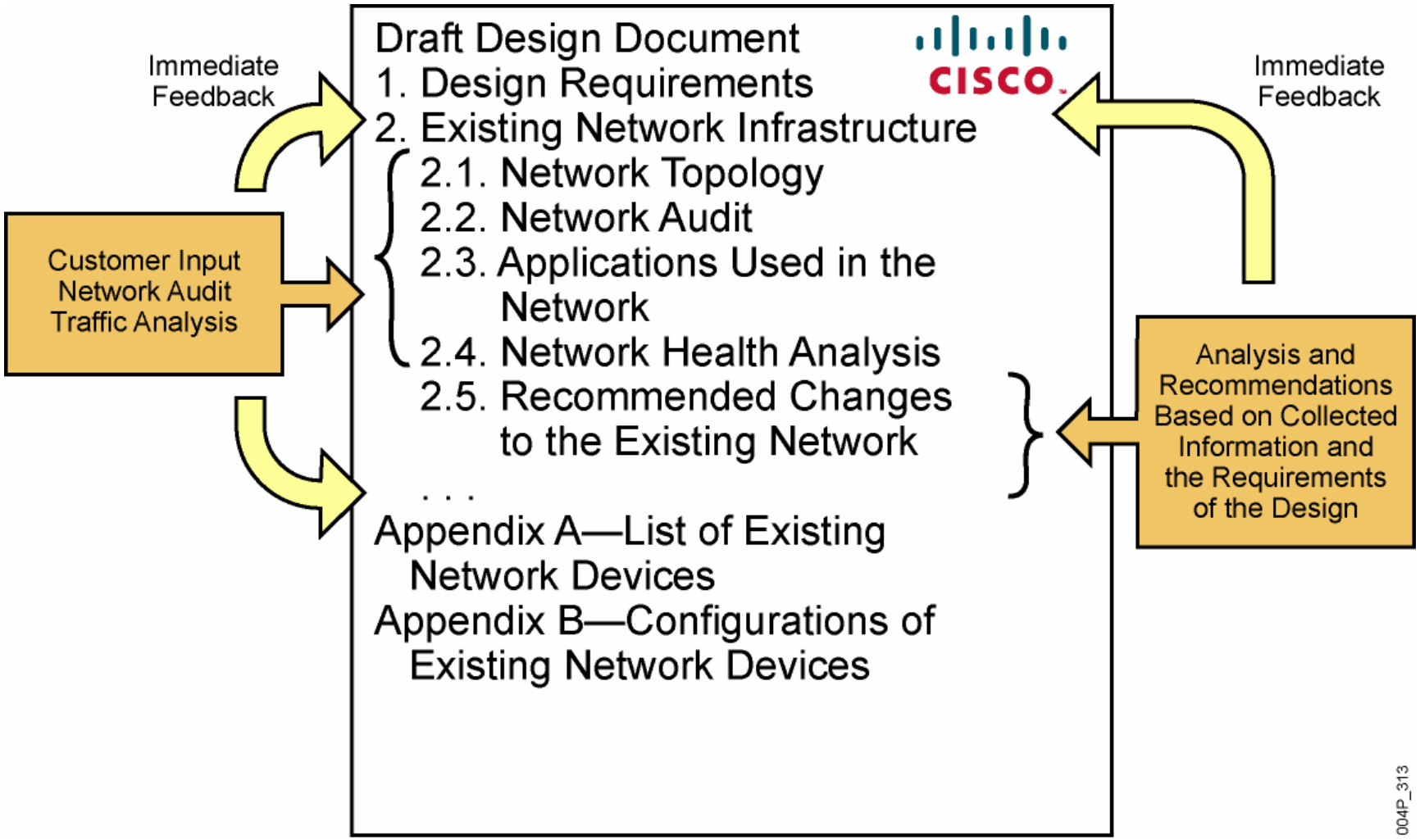
Example: Summary Report Problem Statement

- 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



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.