PI-NetFlow and PacketCapture

Eric Tam, OSIsoft

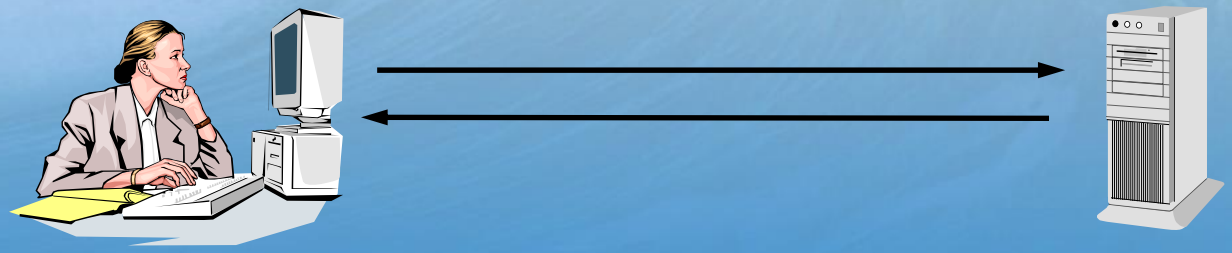
Topics

- Background material
  - TCP/IP network traffic
  - router functionality
  - Cisco routers and NetFlow protocol
- PI-NetFlow Interface and PacketCapture
  - practical applications
- Questions
  - please wait until the end of the presentation

Network Traffic

Web Client

Web Server



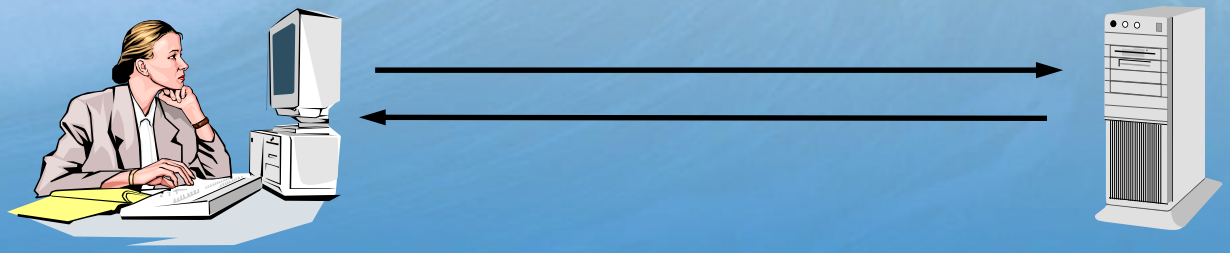
Internet Explorer

Internet Information Server

Network Traffic

PI Client

PI Server



PI-ProcessBook

PINetMgr
PIArchss
etc.

TCP/IP Network Traffic

Internet Explorer

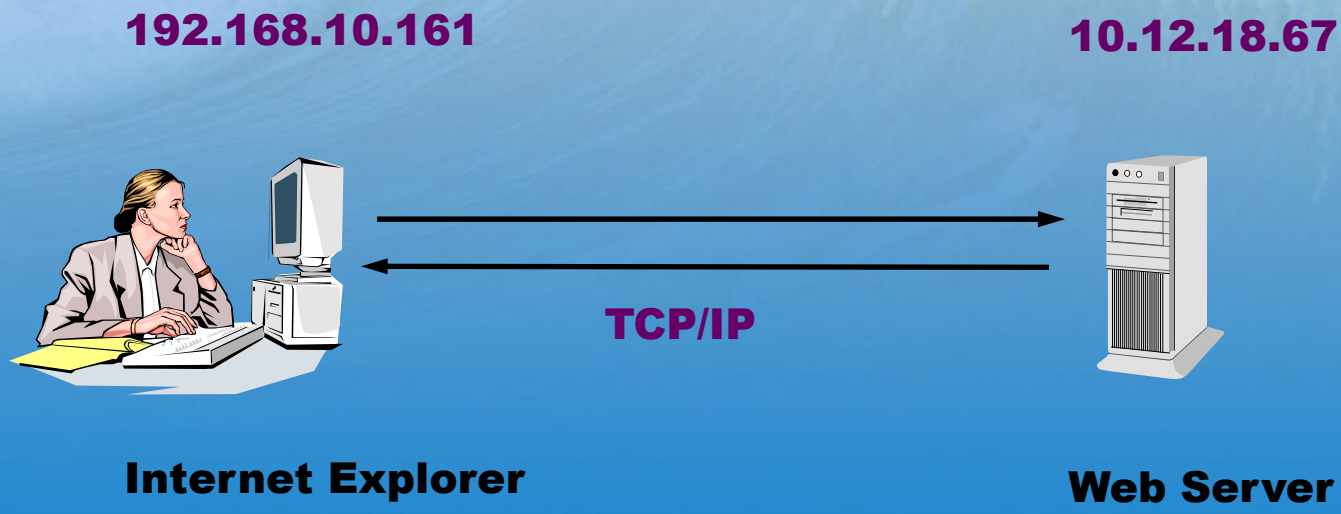
Web Server

PI-ProcessBook

PI Server

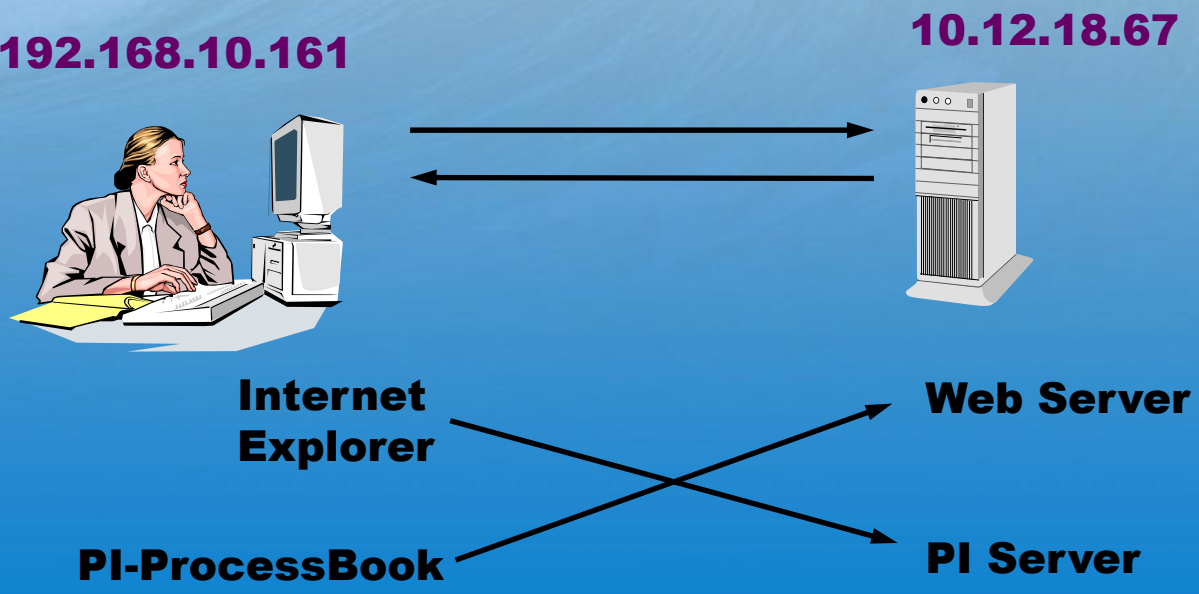
IP Addresses

- All TCP/IP network traffic is based on IP addresses



Multiple Network Programs

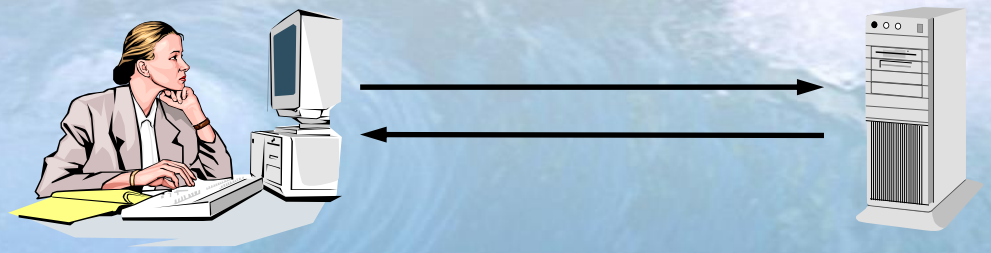
- More than 1 client program on a machine
- More than 1 server program on a machine
- Network traffic confusion?



Port Number

- Helps defines the application for the network traffic
- Server programs
  - Port number is defined by the program itself, sometimes at runtime (i.e., user configurable)
  - PI : 5450 or 545
  - Web server : 80
- Client programs
  - Port number is assigned by operating system

Multiple Network Programs



192.168.10.161

10.12.18.67

Internet Explorer

192.168.10.161 : 2024

Web Server

10.12.18.67 : 80

PI-ProcessBook

192.168.10.161 : 1026

PI Server

10.12.18.67 : 5450

TCP/IP Protocols

- TCP, UDP, ICMP
  - Chosen by the application developer
  - Protocol and port number define network application
- TCP
  - PI; port 5450 or 545
  - Web browsing (HTTP); port 80
- UDP
  - Network management (SNMP); ports 161 and 162
- ICMP
  - No port numbers involved
  - Ping

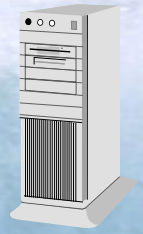
Summary of TCP/IP Traffic

- All TCP/IP traffic has these attributes
  - Source address (e.g., 192.168.10.161)
  - Source port (e.g., 2024)
  - Destination address (e.g., 10.12.18.67)
  - Destination port (e.g., 80)
  - Protocol type (e.g., TCP)
  - Size (e.g., number of bytes)

Router Functionality

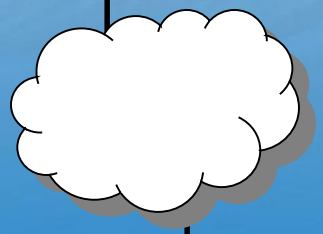
San Diego

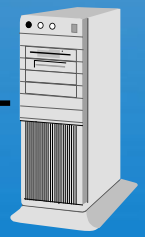
192.168.10.161



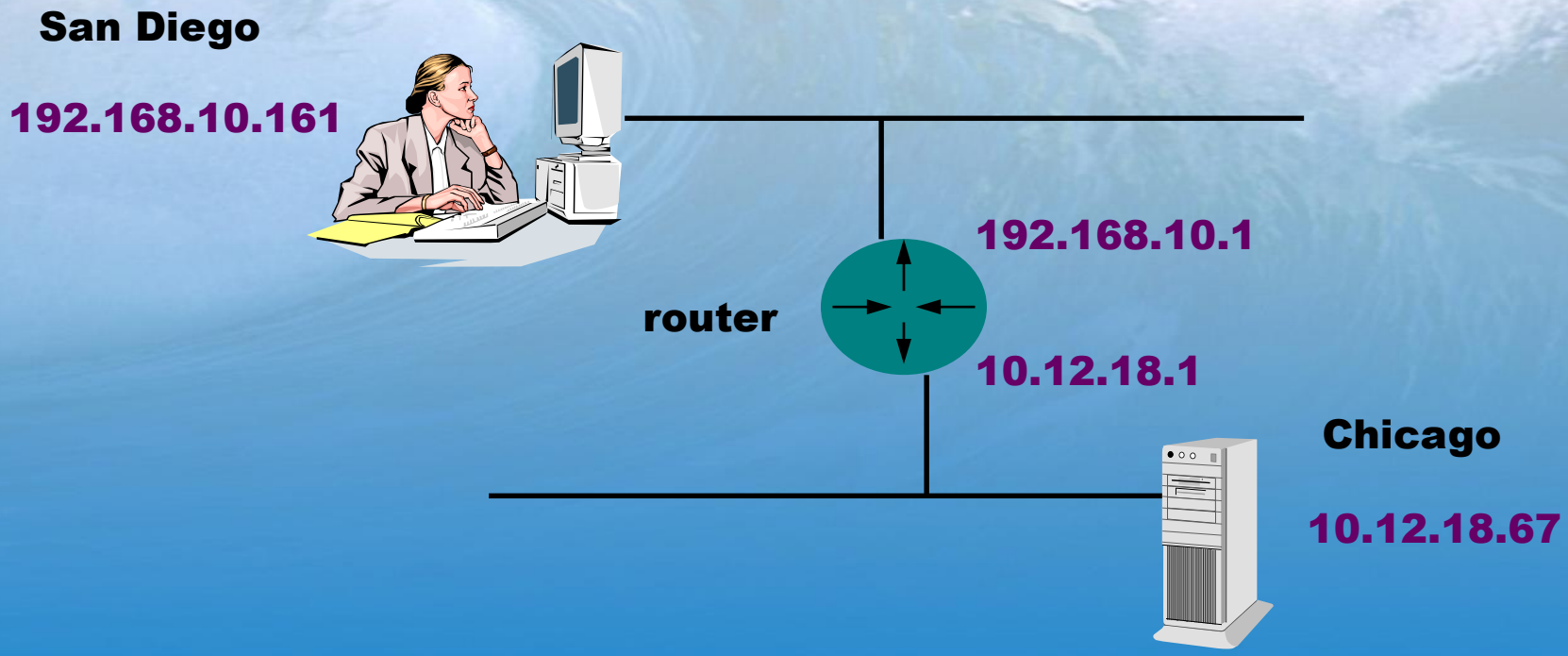
Chicago

10.12.18.67





Router Functionality



Router Functionality

Internet Explorer

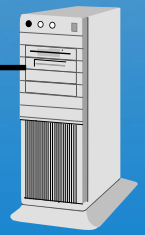
192.168.10.161

San Diego

router

Attributes of TCP/IP traffic:

- Source address: 192.168.10.161
- Source port: 2024
- Destination address: 10.12.18.67
- Destination port: 80
- Protocol: TCP
- Bytes: 100

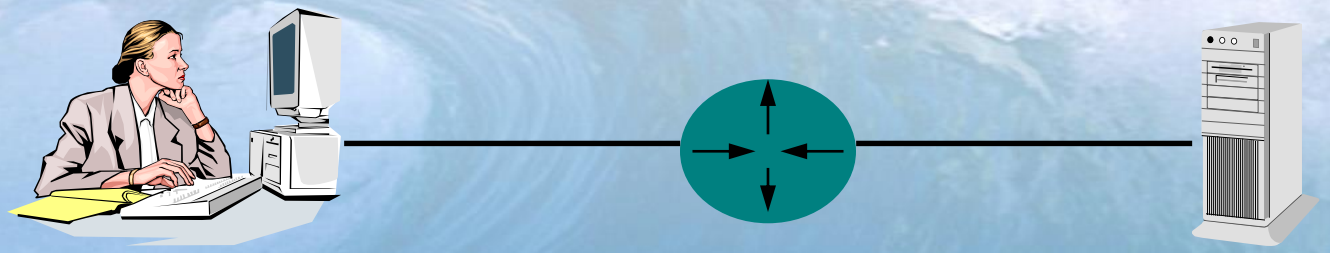


Web Server

10.12.18.67

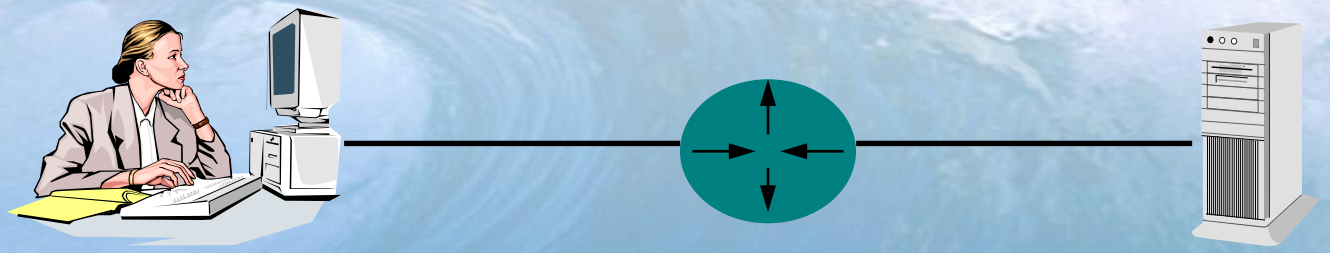
Chicago

Cisco Routers and Data Aggregation



1.	192.168.10.161 : 2024 →	10.12.18.67 : 80	100 bytes
2.	192.168.10.161 : 2024 ←	10.12.18.67 : 80	2100 bytes
3.	192.168.10.161 : 2024 →	10.12.18.67 : 80	120 bytes
4.	192.168.10.161 : 2024 ←	10.12.18.67 : 80	5300 bytes

Cisco Routers and Data Aggregation



1.	192.168.10.161 : 2024	→ 10.12.18.67 : 80	100 bytes
2.	192.168.10.161 : 2024	← 10.12.18.67 : 80	2100 bytes
3.	192.168.10.161 : 2024	→ 10.12.18.67 : 80	120 bytes
4.	192.168.10.161 : 2024	← 10.12.18.67 : 80	5300 bytes

NetFlow Data Aggregation

The 4 previous individual messages result in 2 NetFlow records

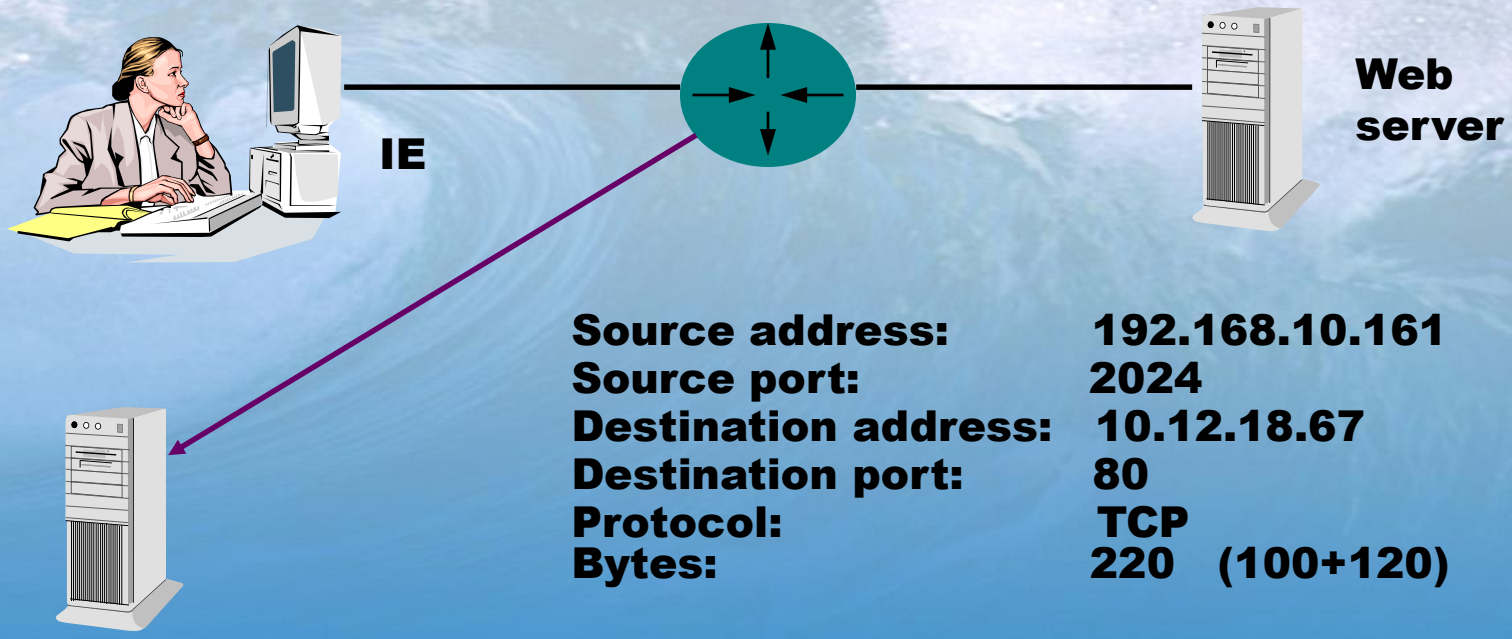
Client → Server

Source address:	**192.168.10.161**
Source port:	**2024**
Destination address:	**10.12.18.67**
Destination port:	**80**
Protocol:	**TCP**
Bytes:	**220 (100+120)**

Server → Client

Source address:	**10.12.18.67**
Source port:	**80**
Destination address:	**192.168.10.161**
Destination port:	**2024**
Protocol:	**TCP**
Bytes:	**7400 (2100+5300)**

NetFlow Data Export

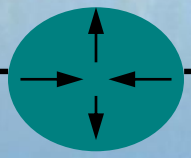


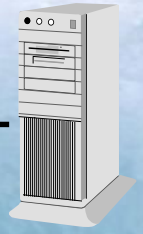
Source address:	192.168.10.161
Source port:	2024
Destination address:	10.12.18.67
Destination port:	80
Protocol:	TCP
Bytes:	220 (100+120)

Source address:	10.12.18.67
Source port:	80
Destination address:	192.168.10.161
Destination port:	2024
Protocol:	TCP
Bytes:	7400 (2100+5300)

Cisco Routers and Data Aggregation

Internet Explorer

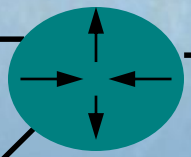


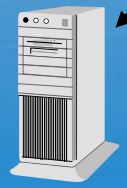


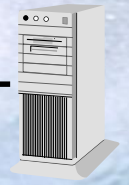
Web server

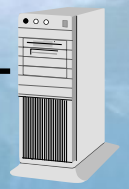
1.	192.168.10.161 : 2024 →	10.12.18.67 : 80	100 bytes
2.	192.168.10.161 : 2024 ←	10.12.18.67 : 80	2100 bytes
3.	192.168.10.161 : 2024 →	10.12.18.67 : 80	120 bytes
4.	192.168.10.161 : 2024 ←	10.12.18.67 : 80	5300 bytes

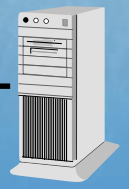
Cisco NetFlow Data Export

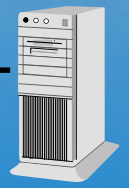












ProcessBook

Outlook

IE

Web

PI

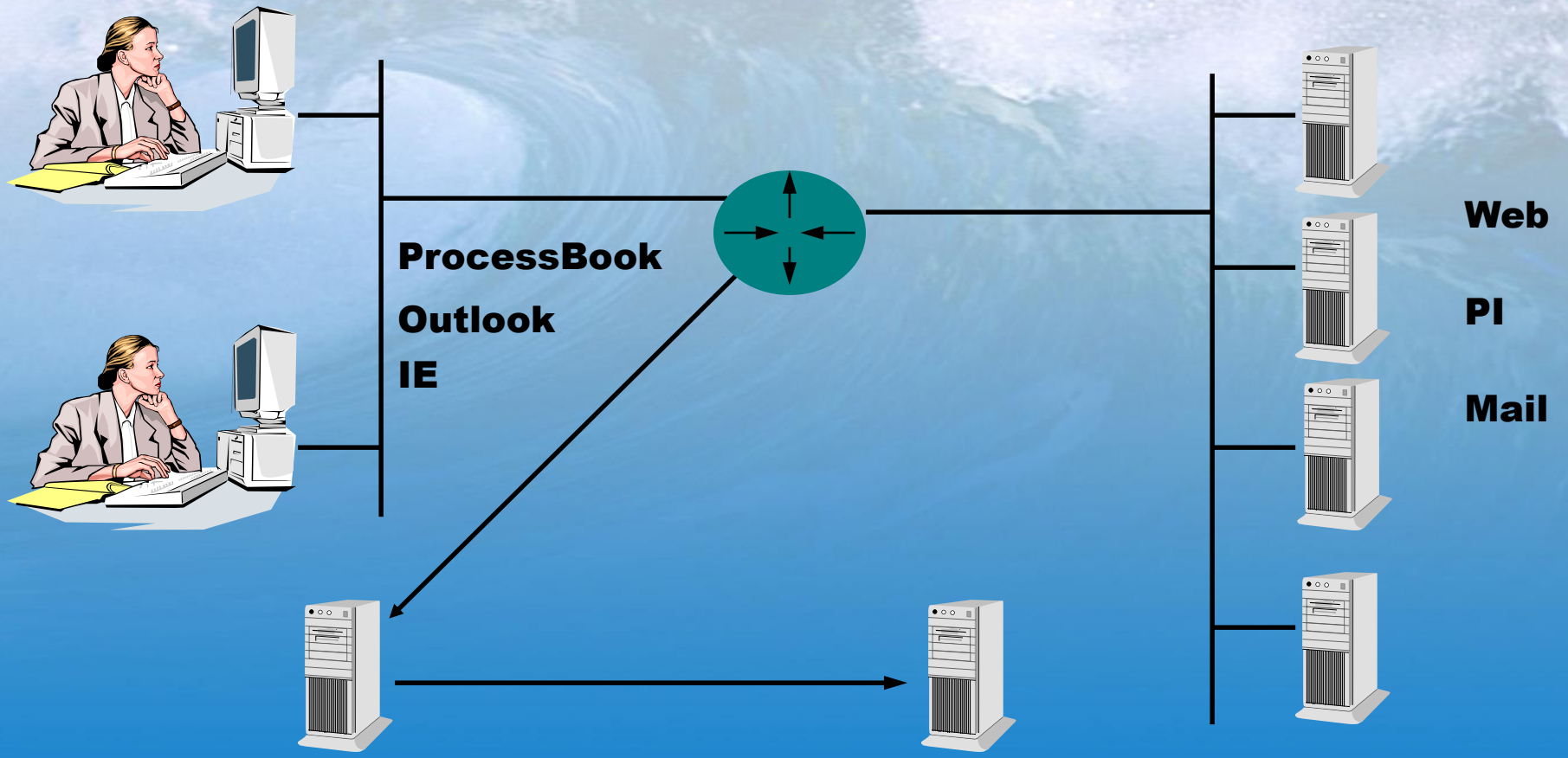
Mail

Continuous export of real-time network traffic information:

- source address
- source port
- destination address
- destination port
- protocol
- bytes

NetFlow Data Collector

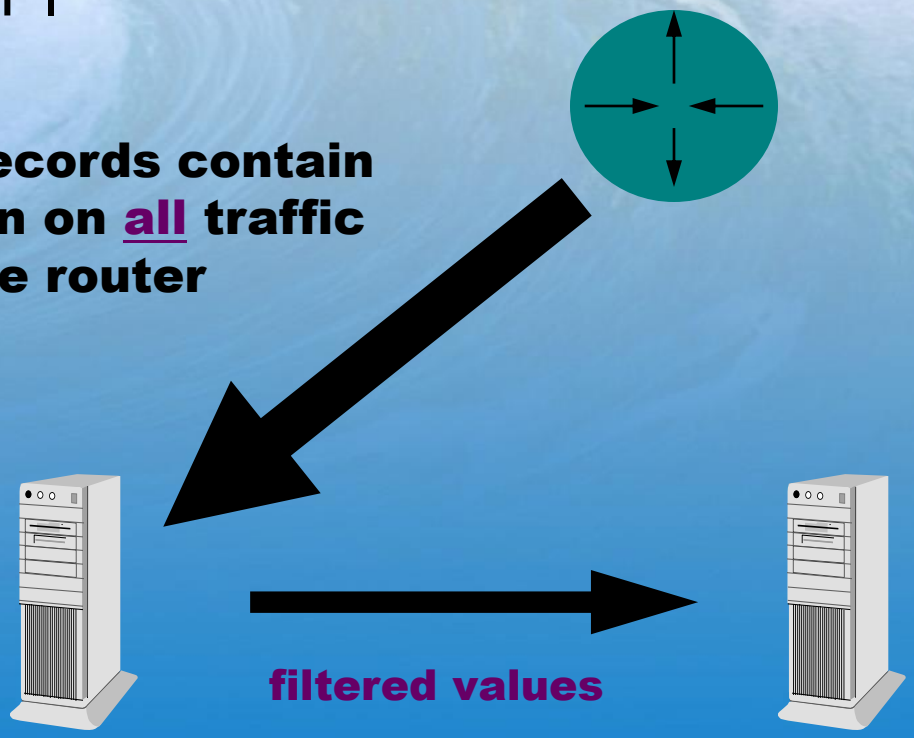
Real-time Network Monitoring



PI-NetFlow Interface

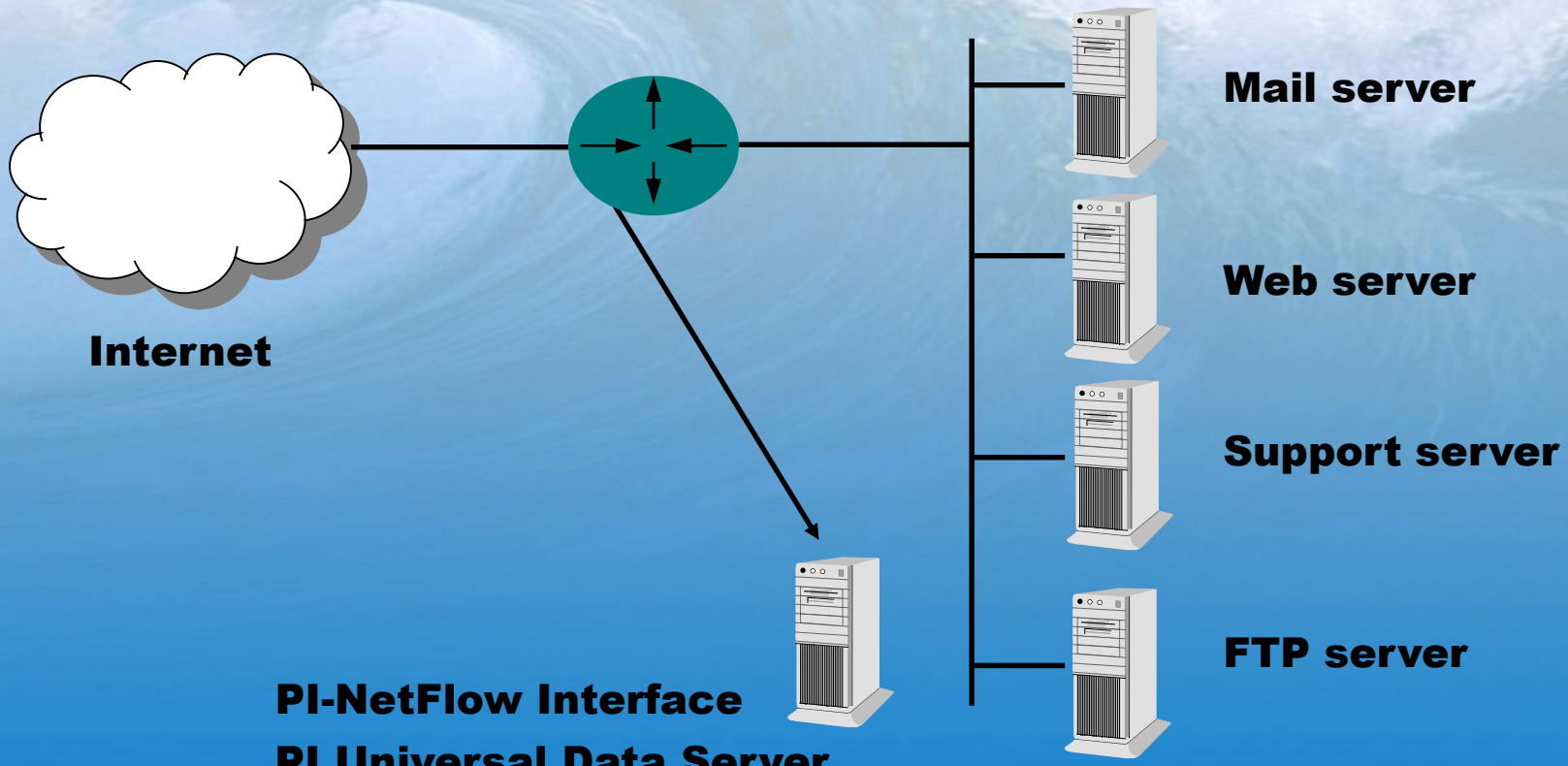
- PI-NetFlow filters NetFlow records before writing values to PI

NetFlow records contain information on all traffic seen by the router



Use of PI-NetFlow at OSIsoft

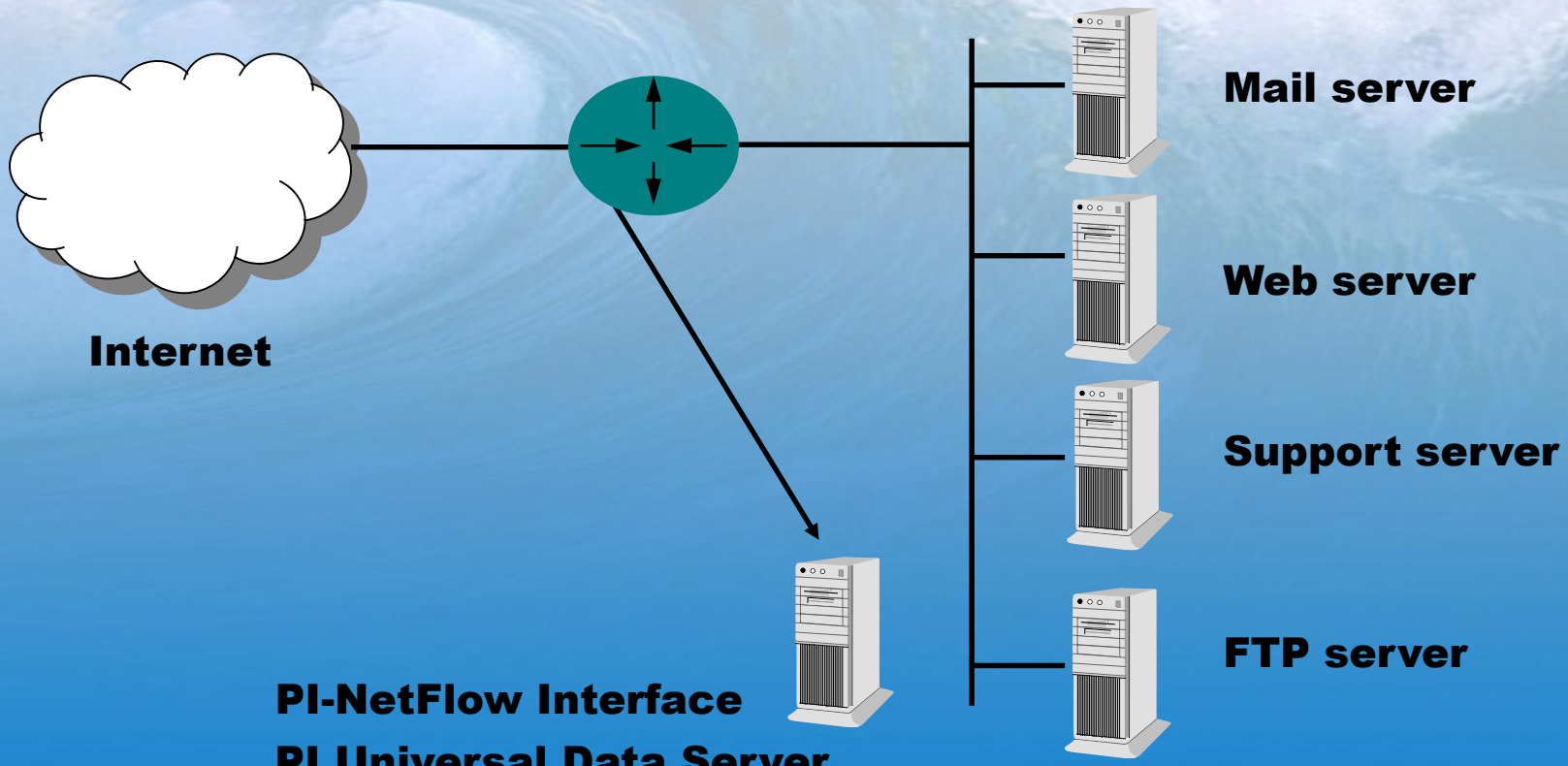
(Monitoring usage for specific servers)



Demonstration

Use of PI-NetFlow at OSIsoft

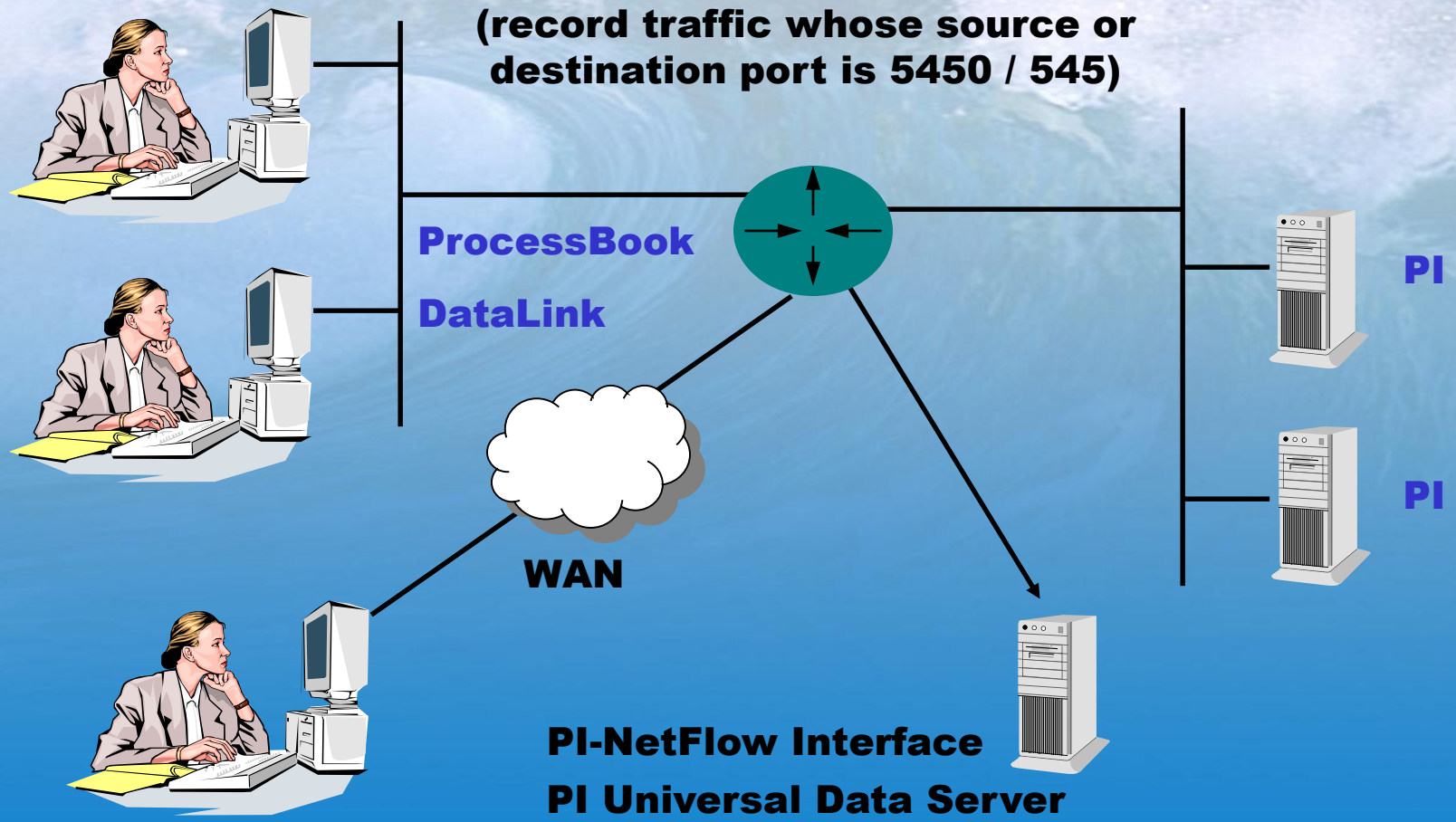
(Monitoring usage for specific servers)



Expanding the Power of PI

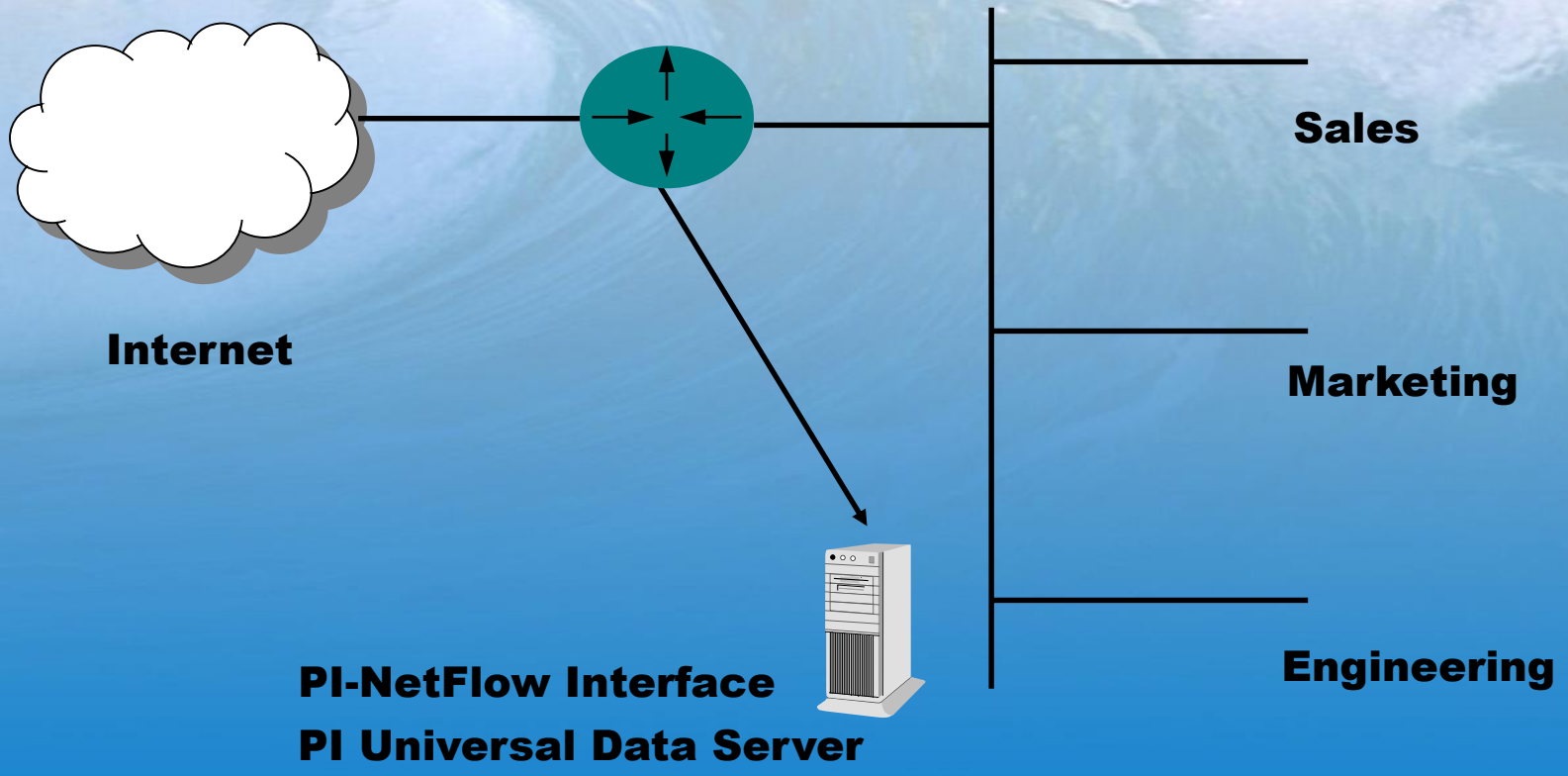
- Practical applications for PI-NetFlow
- Ability to monitor and manage your networking infrastructure

How Much Traffic Is PI-related?



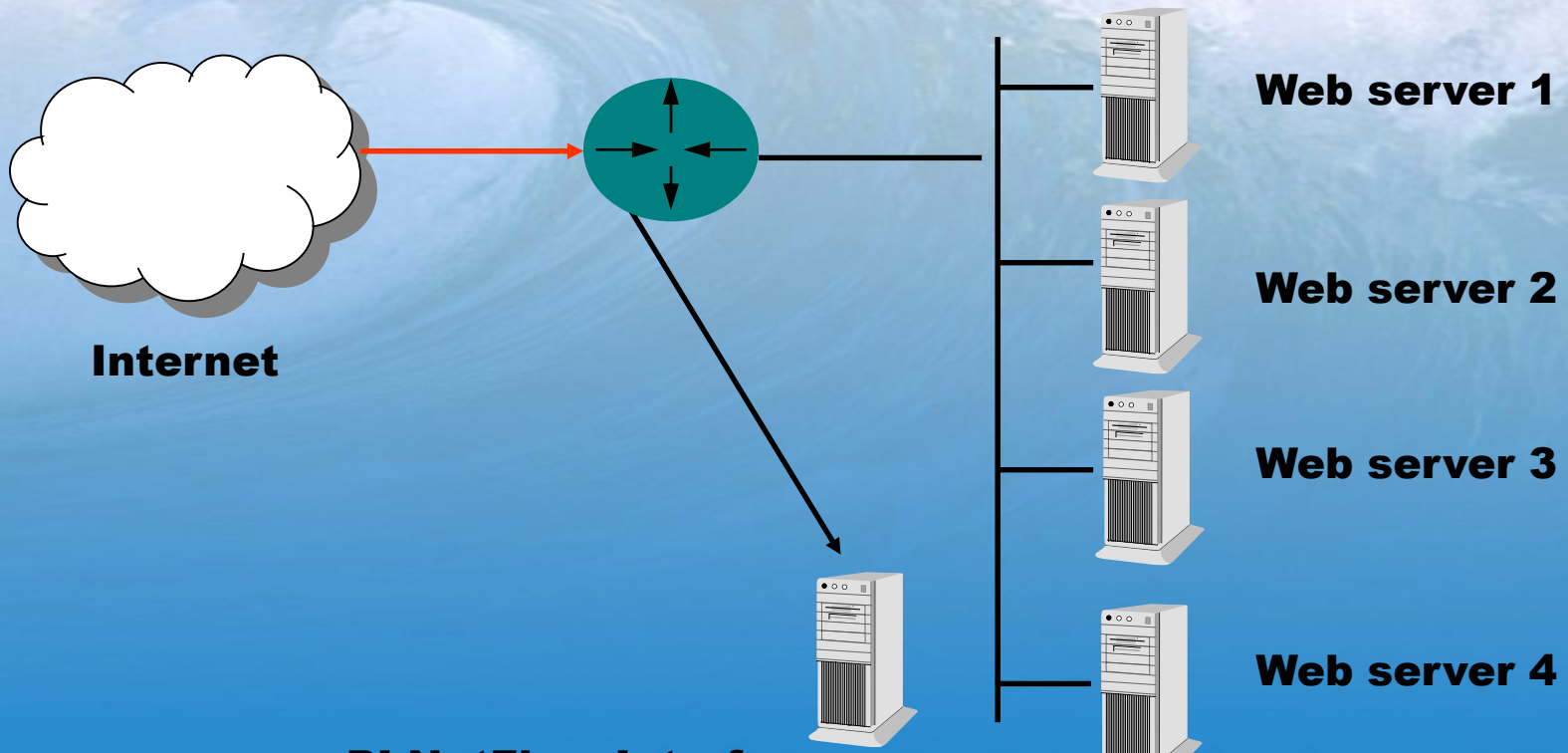
Billing Applications

(determine which department is using Internet connection the most)



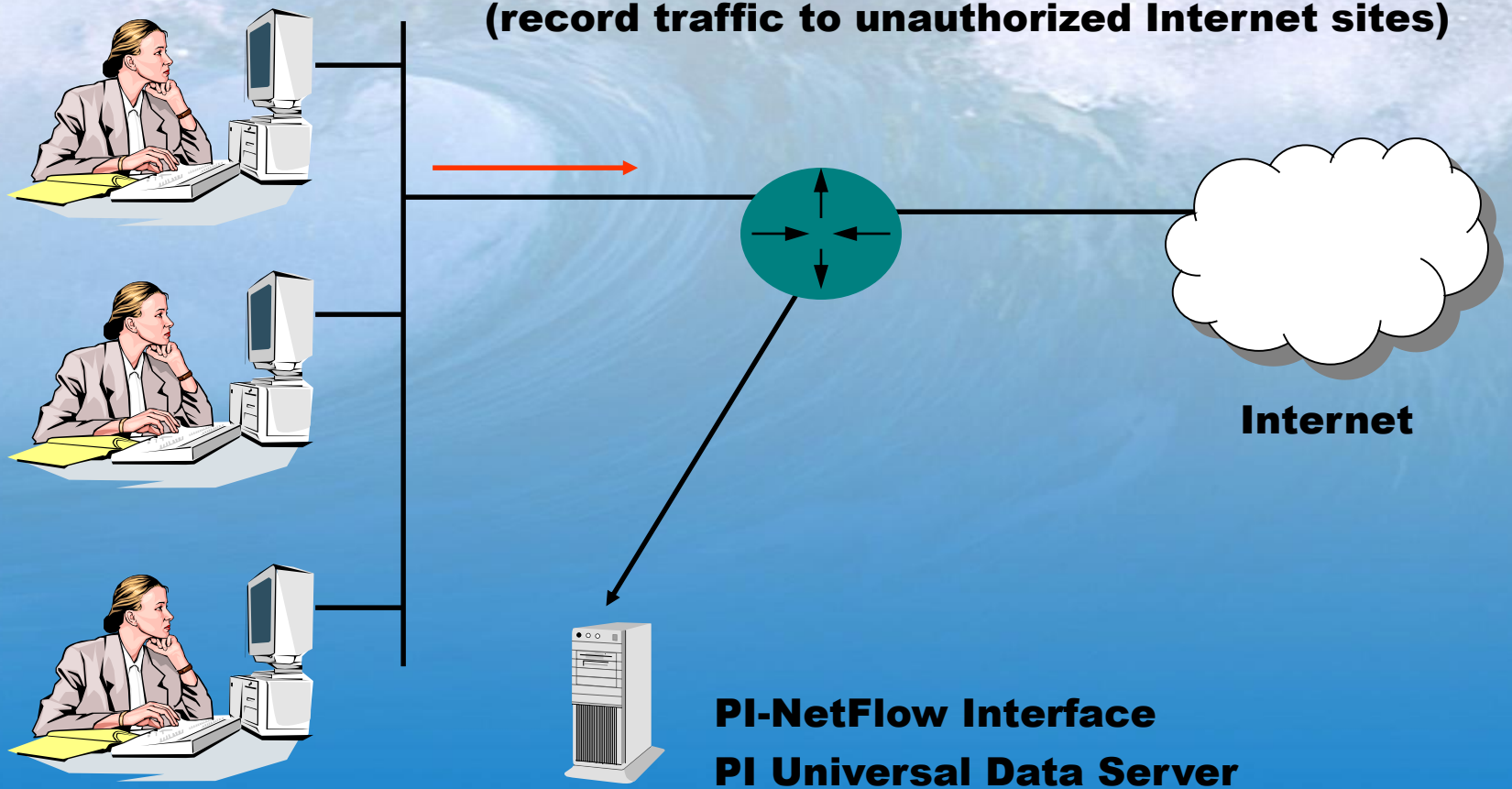
Detection of Illegal Inbound Traffic

(record traffic whose destination port is 80)



Detection of Illegal Outbound Traffic

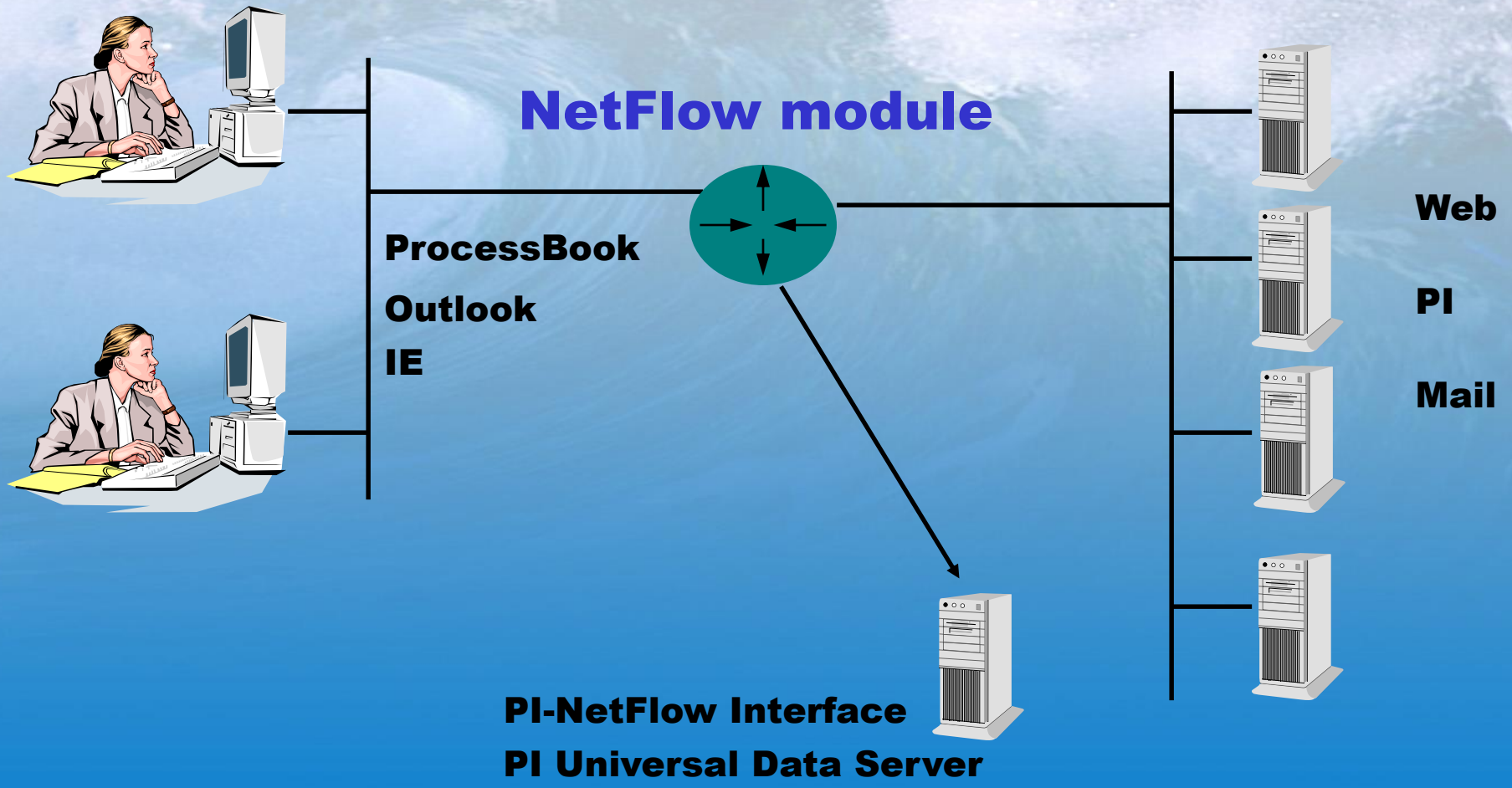
(record traffic to unauthorized Internet sites)



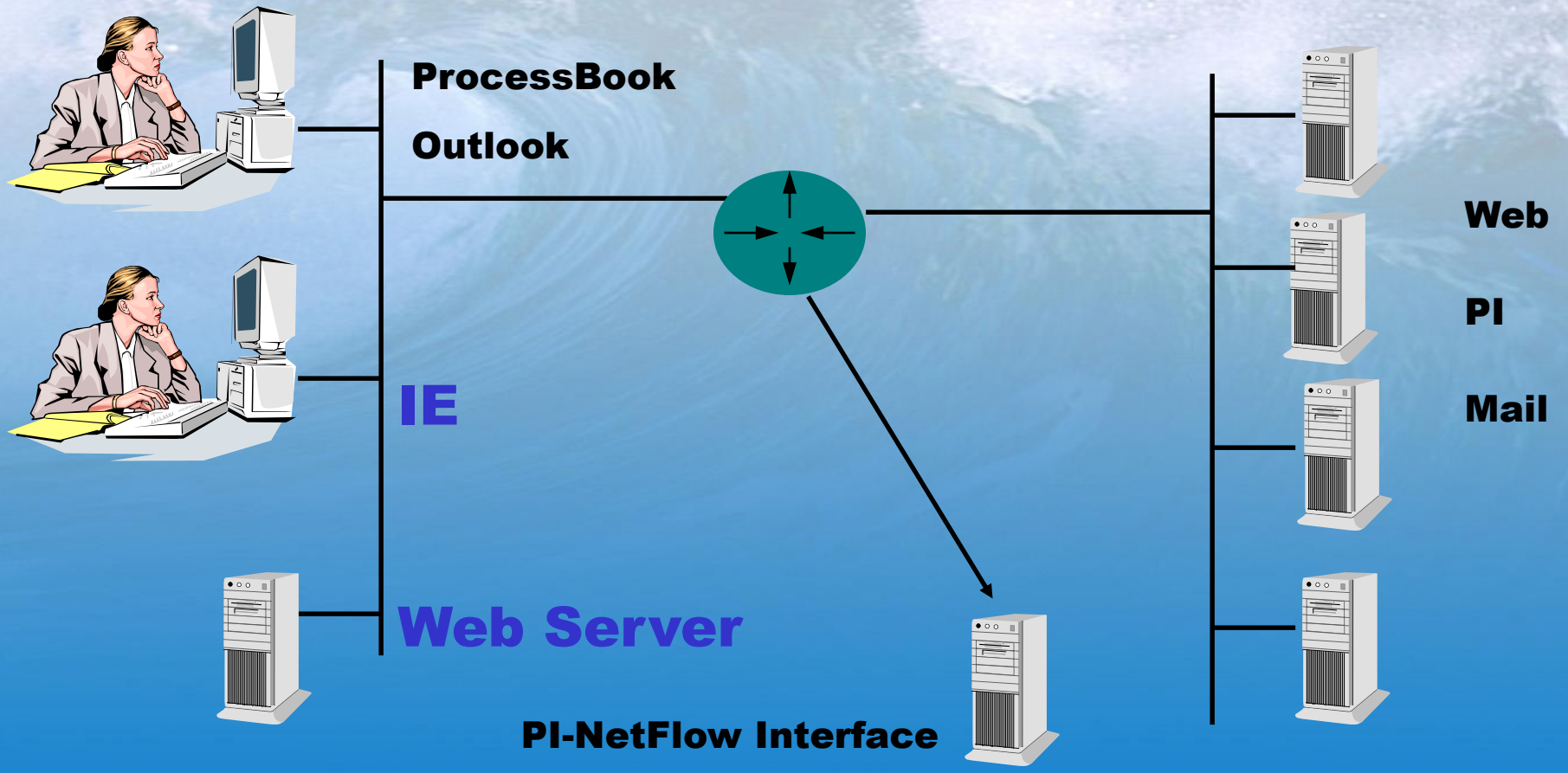
PI-NetFlow Interface

PI Universal Data Server

Limitations of PI-NetFlow?



Limitations of PI-NetFlow?



PI-NetFlow Limitations

- So, PI-NetFlow cannot monitor network traffic if
  - No Cisco router in the network
  - Cisco router exists, but NetFlow does not
  - Router is not involved
- What to do?

Summary of TCP/IP Traffic

- All TCP/IP traffic has these attributes
  - Source address (e.g., 192.168.10.161)
  - Source port (e.g., 2024)
  - Destination address (e.g., 10.12.18.67)
  - Destination port (e.g., 80)
  - Protocol type (e.g., TCP)
  - Size (e.g., number of bytes)

Ethernet Segment – Party Line!

192.168.10.6

192.168.10.5

192.168.10.20

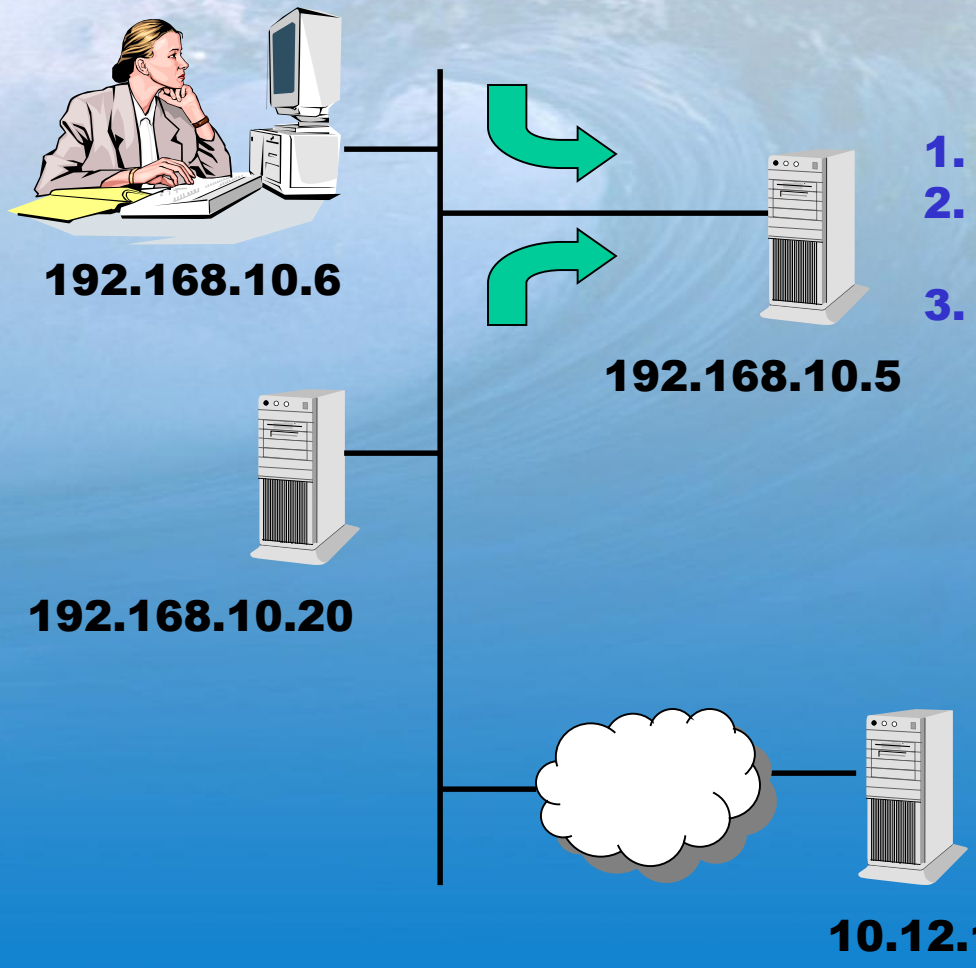
10.12.18.67

With the proper application, 192.168.10.5 can see the attributes of all TCP/IP traffic on the segment:

192.168.10.6 : 1026
192.168.10.20 : 5450

192.168.10.6 : 1124
10.12.18.67 : 80

Packet Capturing

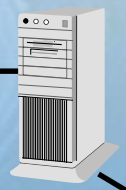


1. See/capture traffic
2. Aggregate traffic information (source IP, source port, etc.)
3. Create records of NetFlow format

OSIsoft PacketCapture

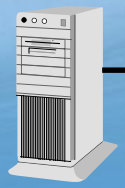
192.168.10.6

PacketCapture

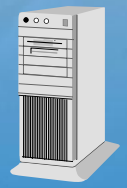


192.168.10.5

1. See/capture traffic
2. Aggregate traffic information (source IP, source port, etc.)
3. Create records of NetFlow format



192.168.10.20



PI-NetFlow Interface

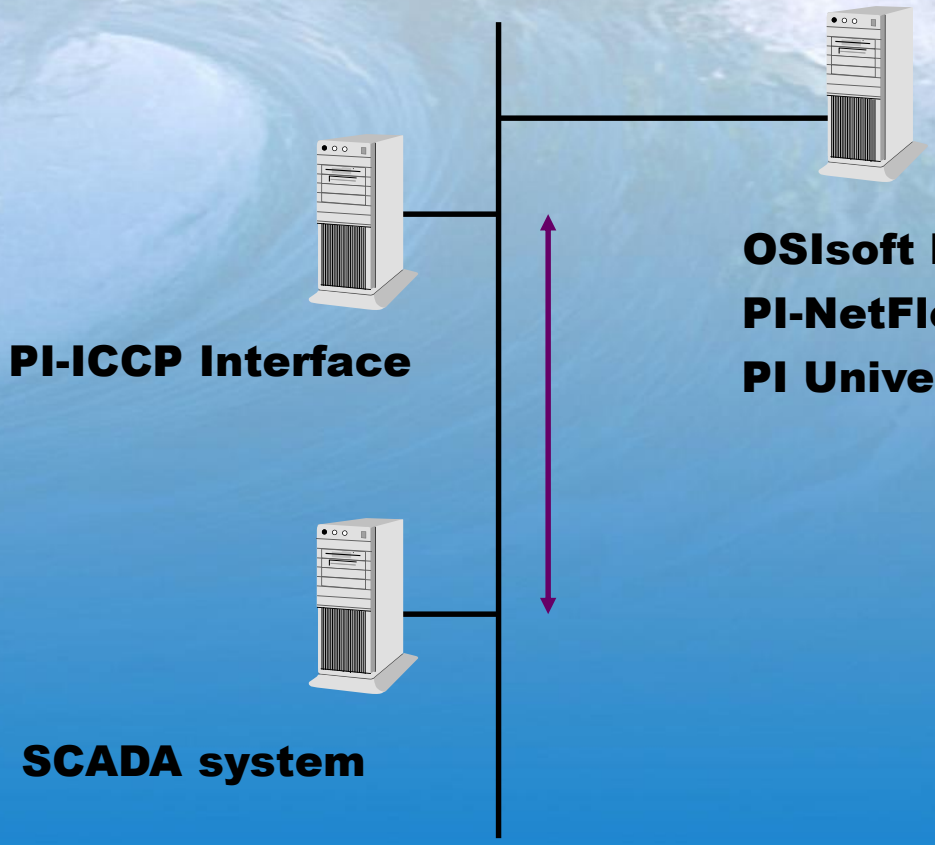
PI Universal Data Server

10.12.18.67

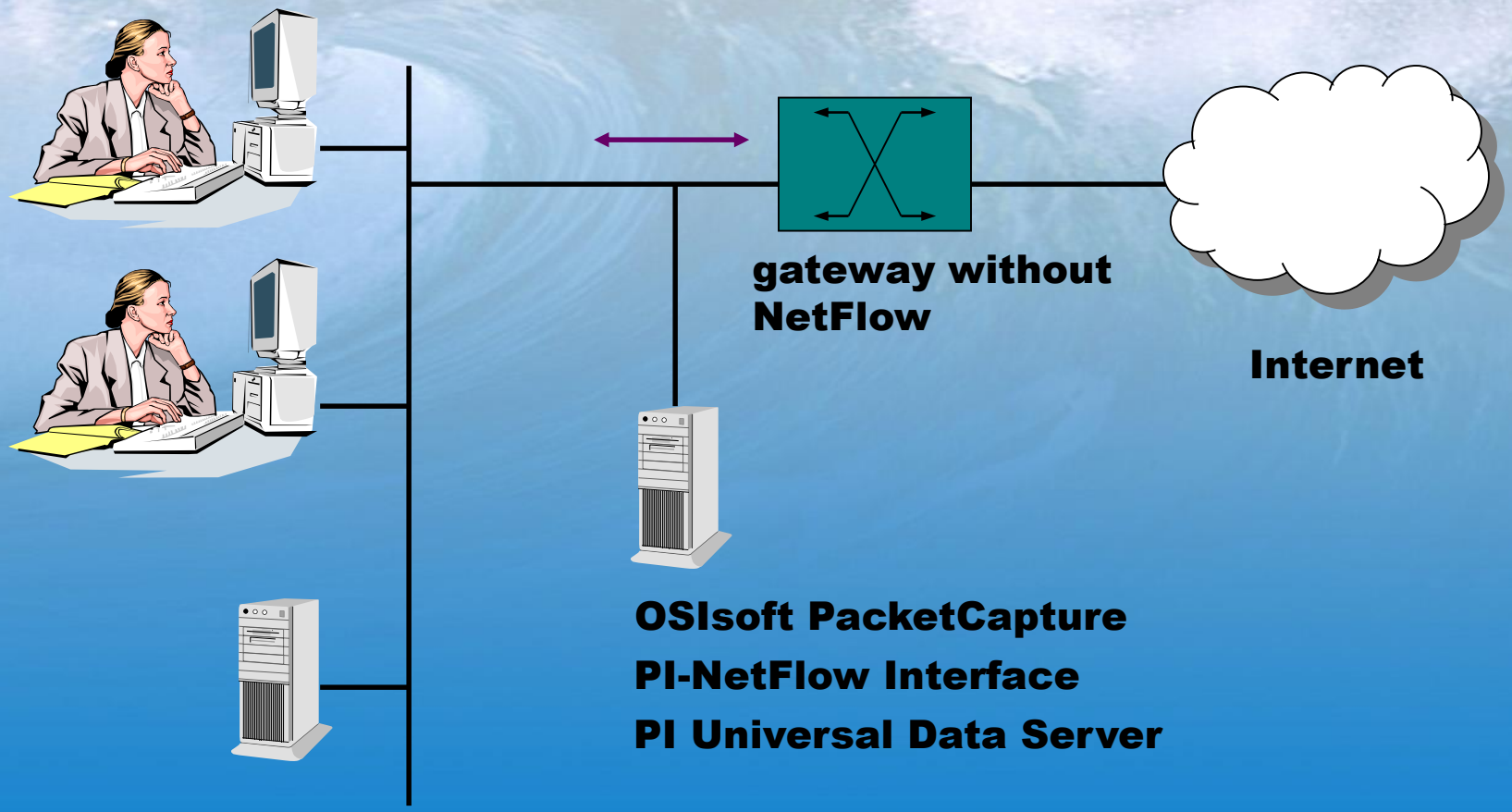
PacketCapture with PI-NetFlow

- No need for a foreign (i.e., non-OSIsoft) device to supply the data
- Monitor traffic on different LAN segments
- Monitor traffic that does not go through a router

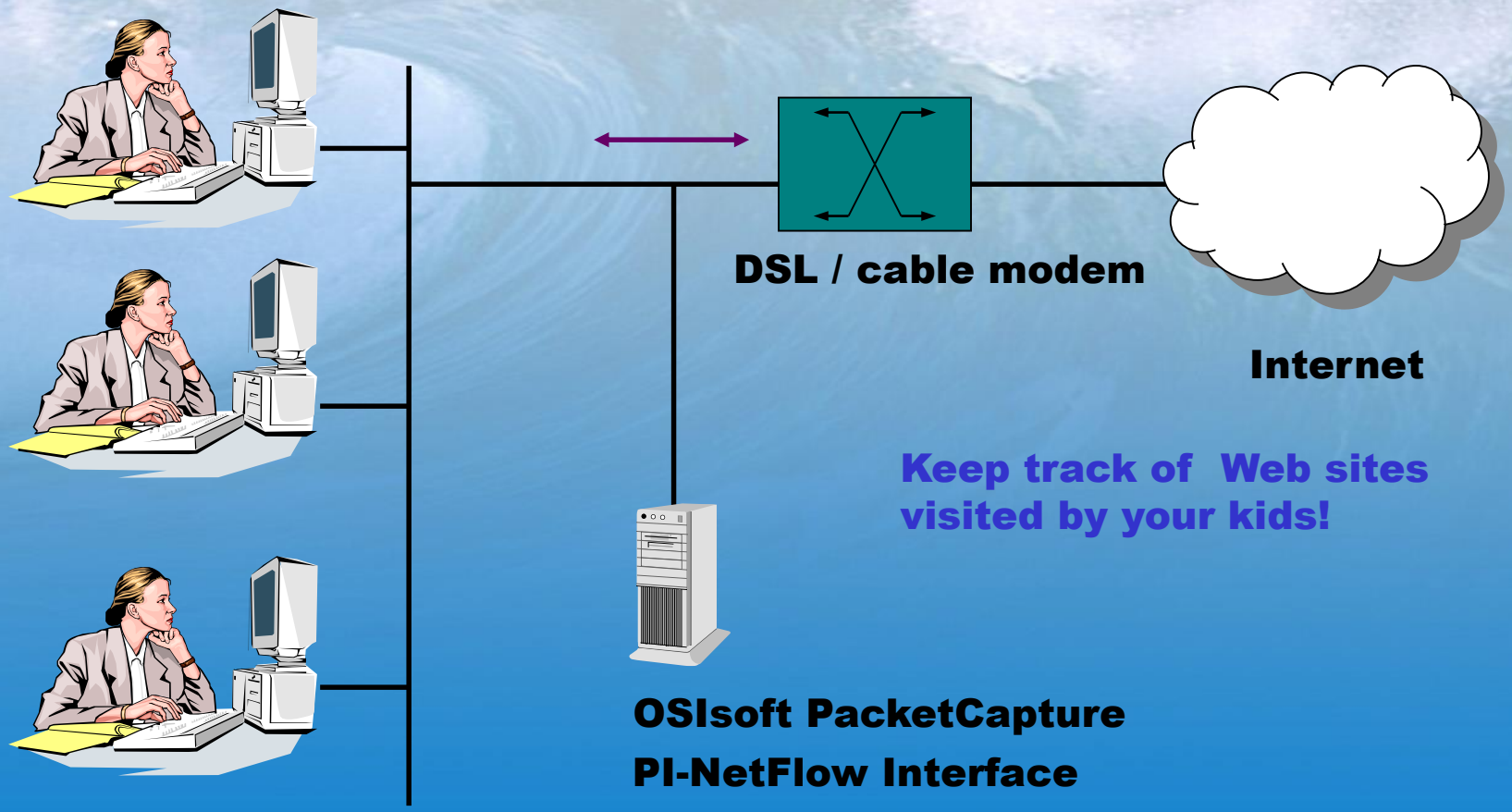
Monitor PI-Interface Traffic



Use with Network Gateways



Use in Small Office / Home Office



Keep track of Web sites visited by your kids!

OSIsoft PacketCapture

PI-NetFlow Interface

PI Universal Data Server

Expand the Power of PI

- Discover the network management capabilities of a PI System!
- Demonstration room Tuesday afternoon

Questions and Answers

- Availability?
  - Approximately 1 month from now
- Contact information
  - OSIsoft sales representative
  - Eric Tam (software developer of PI-NetFlow)
    - Email: **etam@osisoft.com**
    - Phone: **1-510-297-5803**

Additional Information

- Next slides provide additional information that may be helpful in understanding the details of PI-NetFlow and PacketCapture

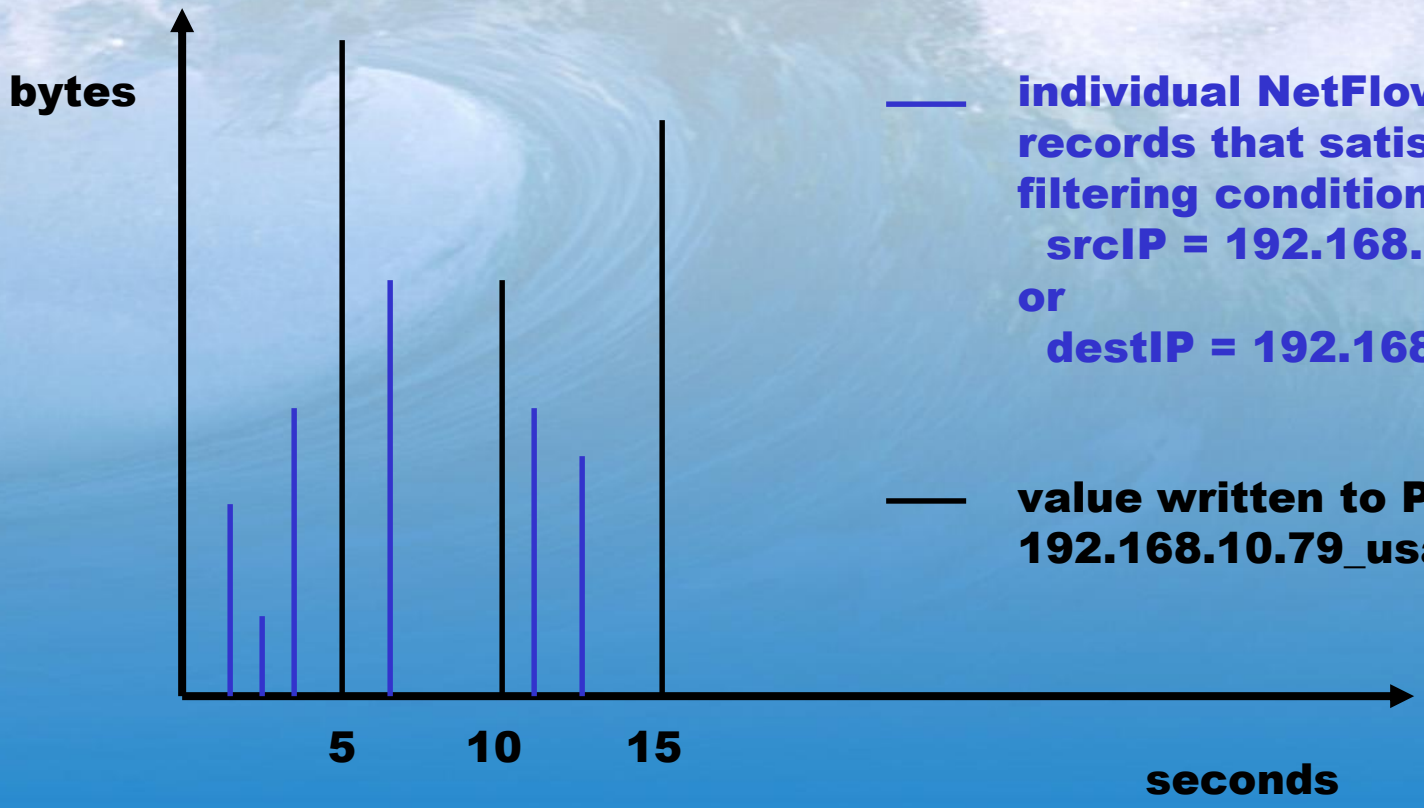
Data Collection Example

- Want to monitor traffic sent to and from machine with IP address of 192.168.10.79
  - Tagname: **192.168.10.79_usage**
  - Filtering condition 1
    - destination IP: 192.168.10.79
  - Filtering condition 2
    - source IP: 192.168.10.79

Data Collection Example

- Want to monitor traffic sent to and from machine with IP address of 192.168.10.79
  - Tagname: **192.168.10.79_usage**
  - Filtering condition 1
    - destination IP: 192.168.10.79
  - Filtering condition 2
    - source IP: 192.168.10.79
- For every NetFlow record received, PI-NetFlow
  - Applies the user-specified filtering conditions
  - Calculates a running sum of the number of bytes in those records that satisfy criteria
  - Periodically writes this sum to **192.168.10.79_usage**

Value Written to PI



individual NetFlow records that satisfy filtering conditions
srcIP = 192.168.10.79
or
destIP = 192.168.10.79

value written to PI tag 192.168.10.79_usage

Data Collection Example

- "Base" tag – running sum of bytes
  - Created by the user
  - **192.168.10.79_usage**
- "Detail" tags – fields of NetFlow records
  - Created by PI-NetFlow itself
  - Tagnames are derived from "base" tag
  - **192.168.10.79_usage_detail_srcIP**
  - **192.168.10.79_usage_detail_srcPort**
  - **192.168.10.79_usage_detail_destIP**
  - **192.168.10.79_usage_detail_destPort**
  - **192.168.10.79_usage_detail_octet**
  - **192.168.10.79_usage_detail_prot**

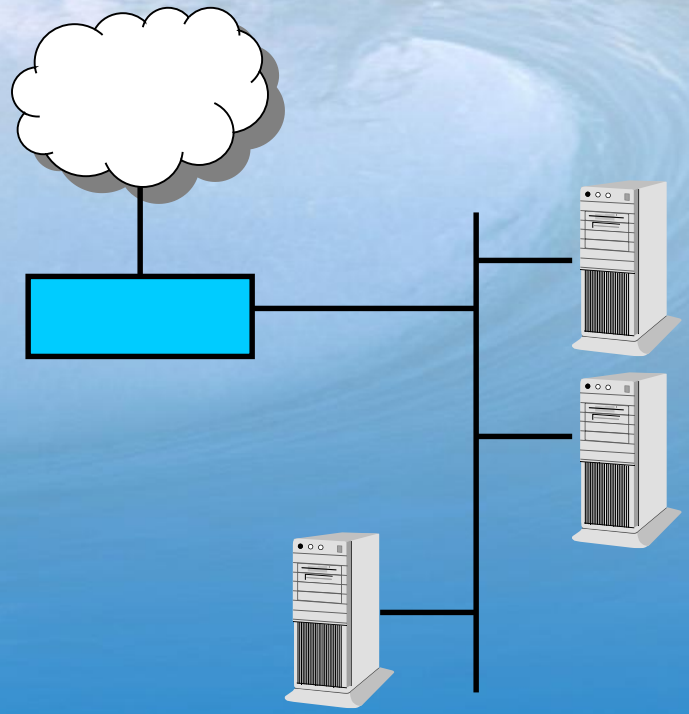
PacketCapture Limitations

- Standard Ethernet only, won't see traffic on
  - dial-up connections
  - ATM networks
  - token ring networks
  - fibre networks
- Captures only the traffic that it sees
  - Won't see traffic for other machines if switched network is involved

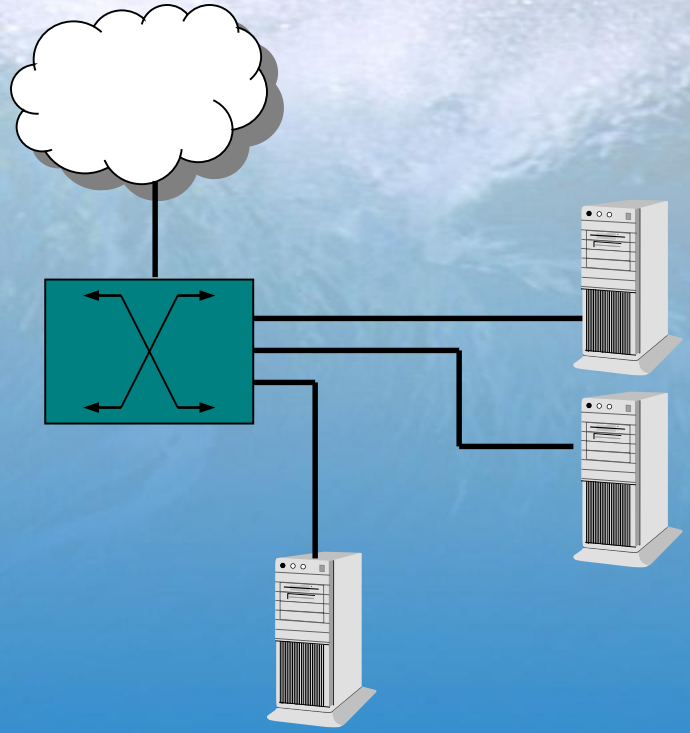
Comparison of Programs

- PI-NetFlow
  - PI interface program; uses PI-API and PI-SDK
  - Receives NetFlow records sent by an external device (e.g., Cisco router or PacketCapture)
  - Writes values to PI tags
- PacketCapture
  - Not an interface; does not use PI-API or PI-SDK
  - Measures TCP/IP traffic on Ethernet
  - Creates and sends NetFlow records
  - Not a replacement for Cisco NetFlow

Hub vs. Switch

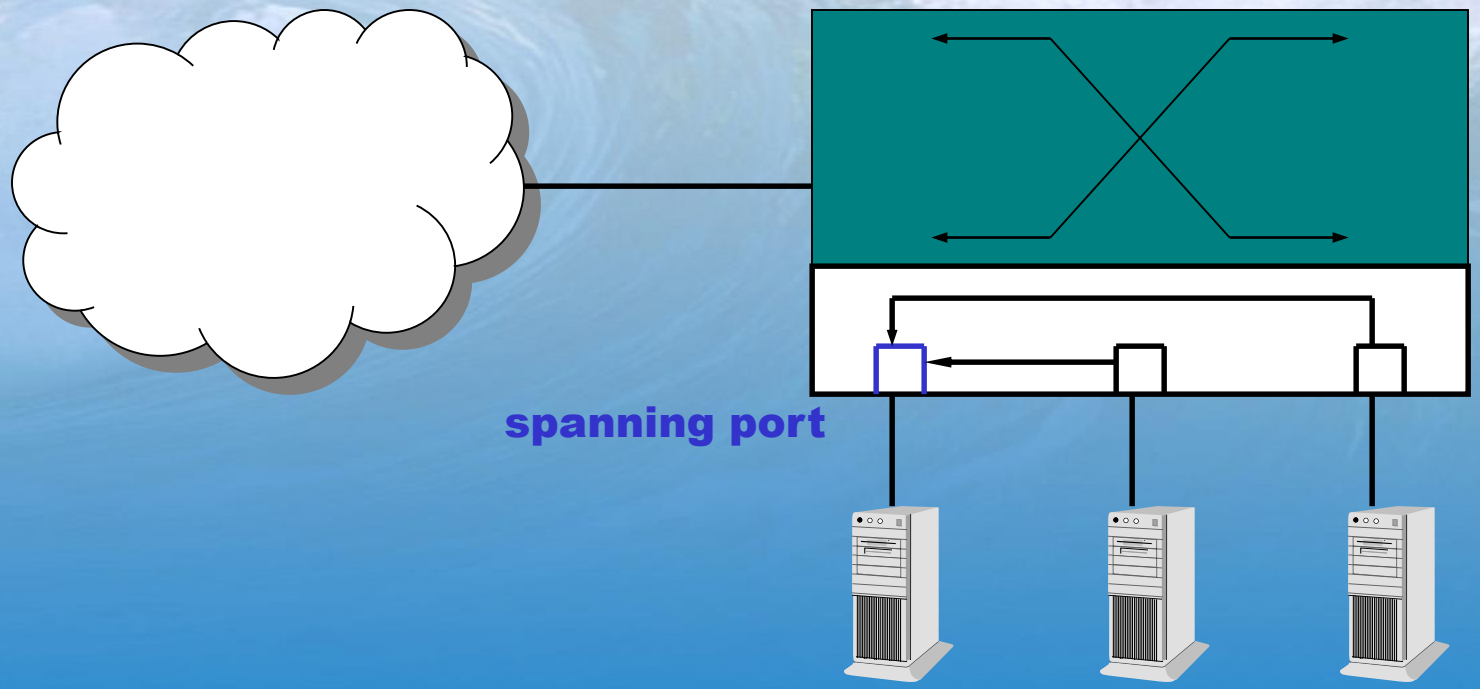


OSIsoft PacketCapture
PI-NetFlow Interface
PI Universal Data Server



OSIsoft PacketCapture
PI-NetFlow Interface
PI Universal Data Server

Managed Switch



OSIsoft PacketCapture

PI-NetFlow Interface

PI Universal Data Server