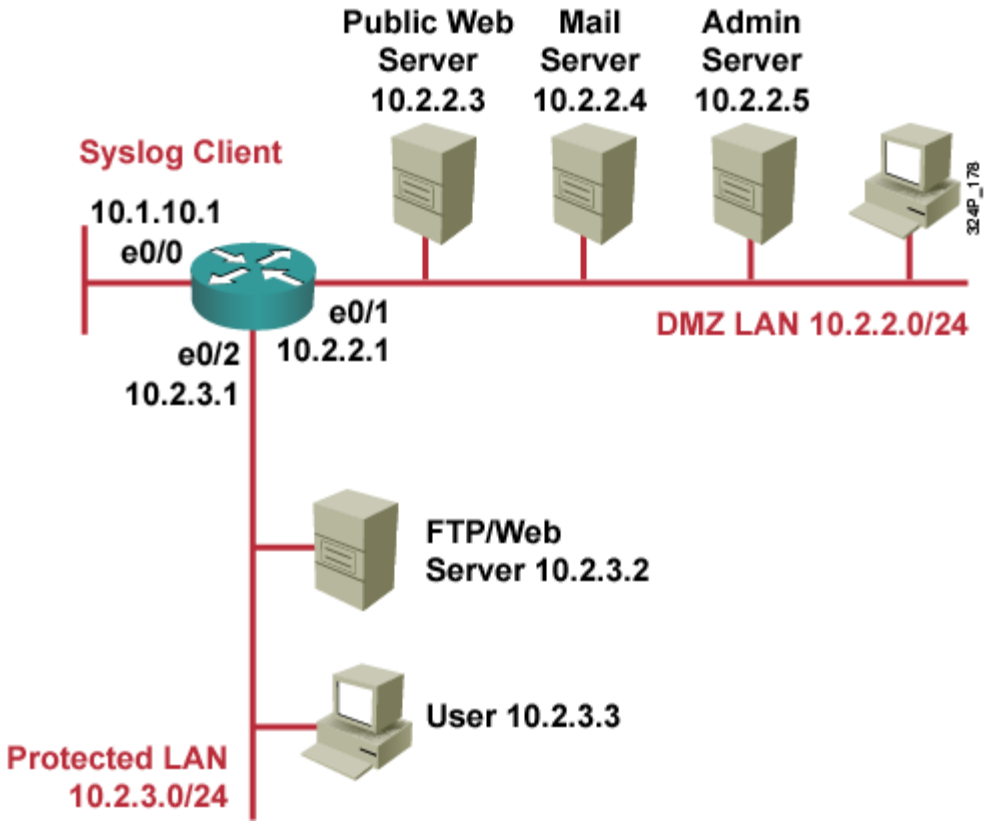
Syslog – SNMP – NTP – DNS

Implementing Log Messaging

- **Routers should be configured to send log messages to one or more of these:**
  - Console
  - Terminal lines
  - Memory buffer
  - SNMP traps
  - Syslog
- **Syslog logging is a key security policy component.**

Syslog Systems

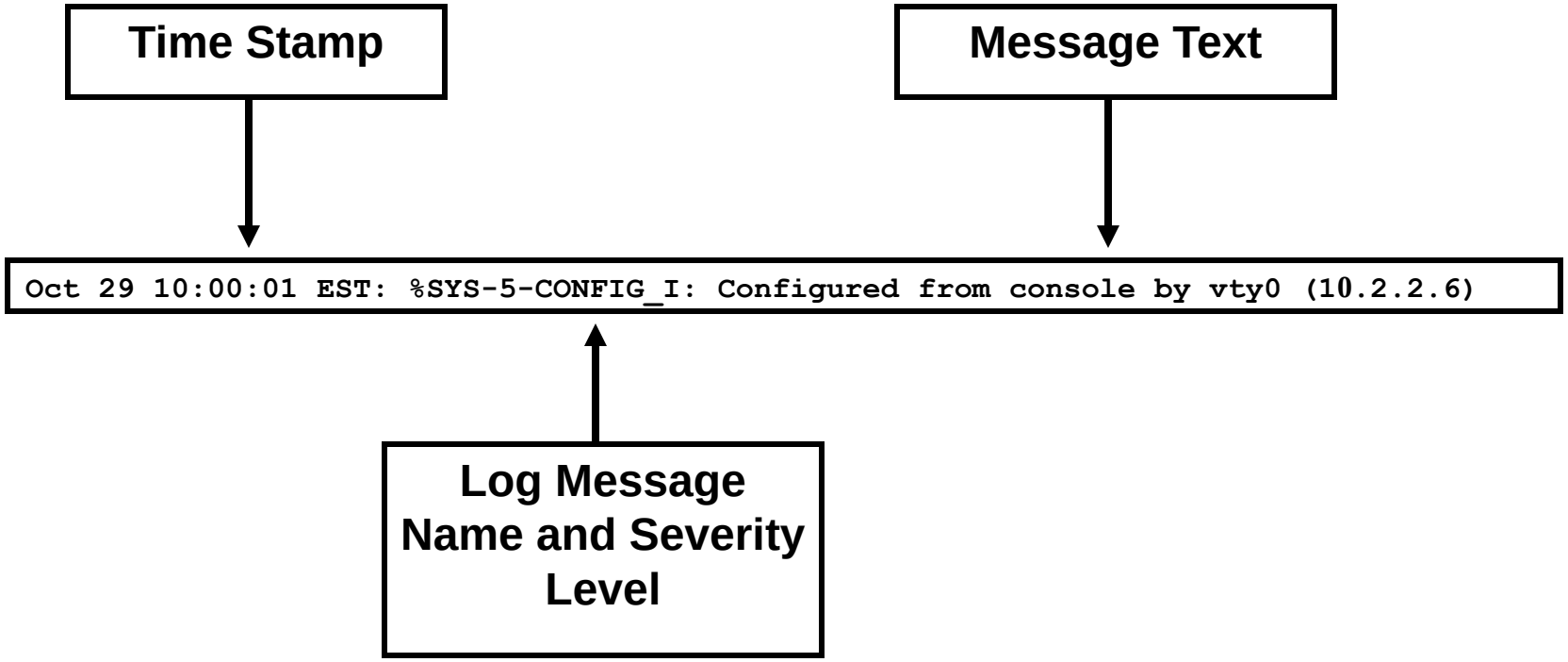


- **Syslog server:** A host that accepts and processes log messages from one or more syslog clients.
- **Syslog client:** A host that generates log messages and forwards them to a syslog server.

Cisco Log Severity Levels

Level	Name	Description
0	Emergencies	Router unusable
1	Alerts	Immediate action required
2	Critical	Condition critical
3	Errors	Error condition
4	Warnings	Warning condition
5	Notifications	Normal but important event
6	Informational	Informational message
7	Debugging	Debug message

Log Message Format



Configuring Syslog Logging

Configuring Syslog

```
Router(config)#
```

```
logging [host-name | ip-address]
```

1. **Sets the destination logging host**

```
Router(config)#
```

```
logging trap level
```

2. **(Optional) Sets the log severity (trap) level**

Configuring Syslog (Cont.)

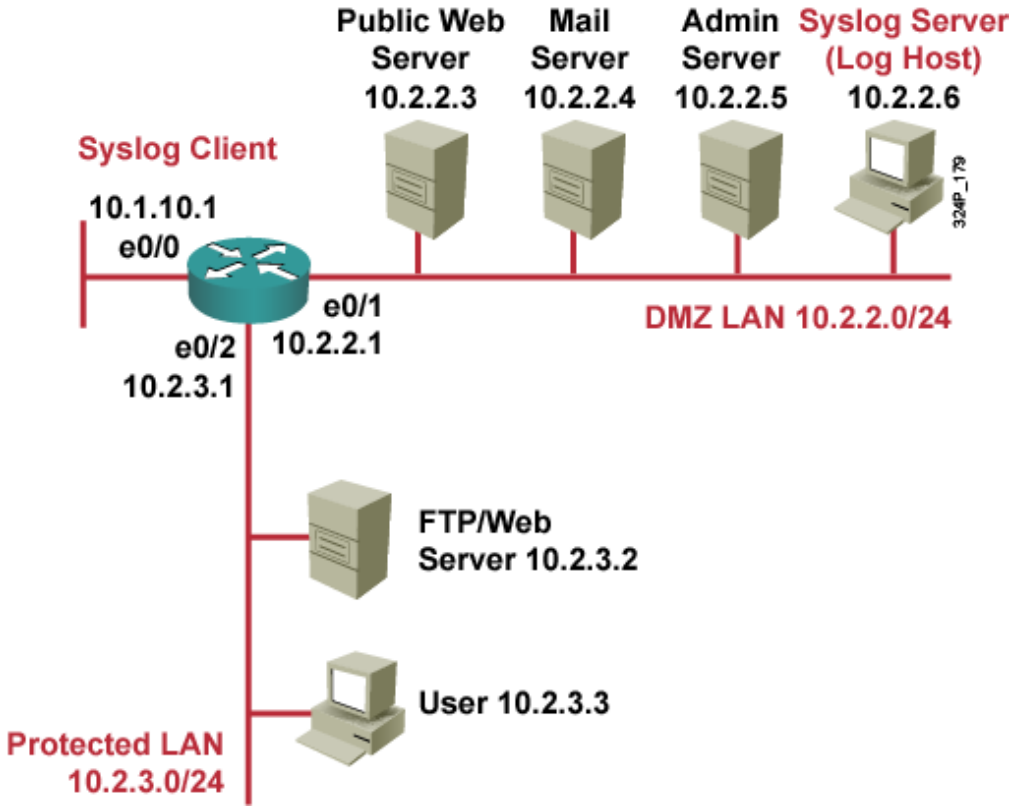
```
Router(config)#
logging source-interface interface-type interface-number
```

4. **(Optional) Sets the source interface**

```
Router(config)#
logging on
```

5. **Enables logging**

Syslog Implementation Example

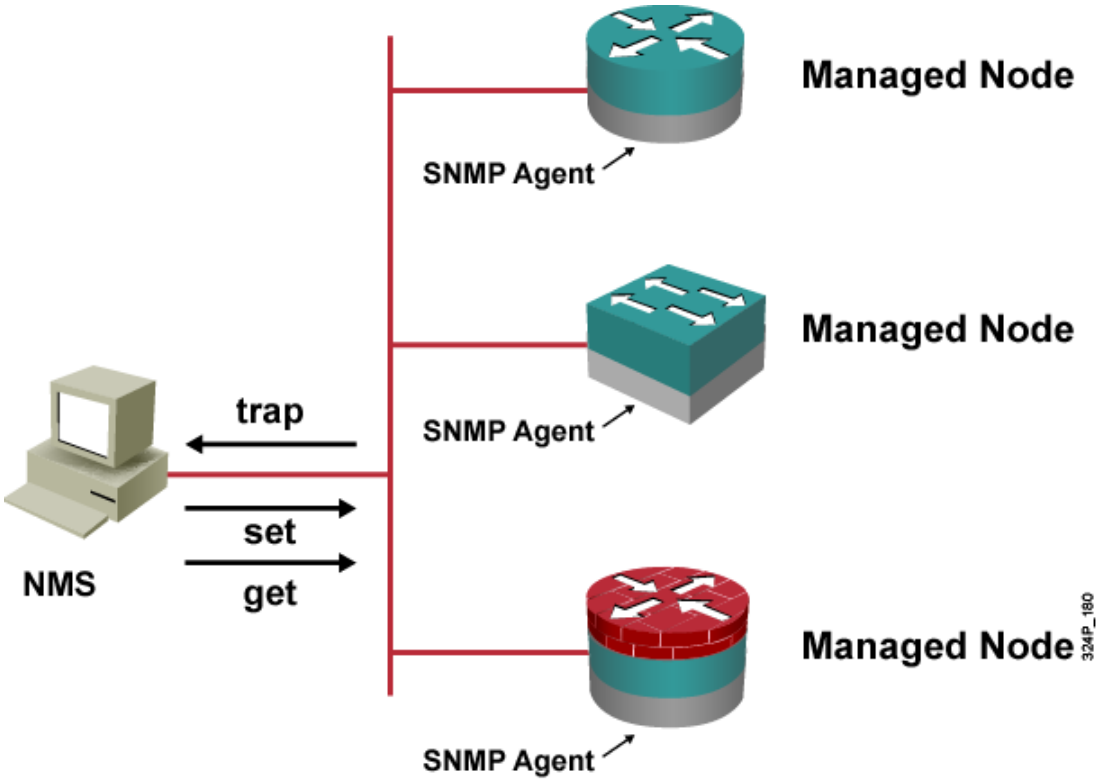



```
R3(config)#logging 10.2.2.6
R3(config)#logging trap informational
R3(config)#logging source-interface loopback 0
R3(config)#logging on
```

SNMP

SNMPv1 and SNMPv2 Architecture

- **The SNMP NMS asks agents embedded in network devices for information, or tells the agents to do something.**



SNMP: Security is Not My Problem

Community Strings

Used to authenticate messages between a management station, and an SNMPv1 or SNMPv2 engine:

- **Read only community strings can get information, but can not set information in an agent.**
- **Read-write community strings can get and set information in the agent.**
- **Having read-write access is like having the enable password for the device.**

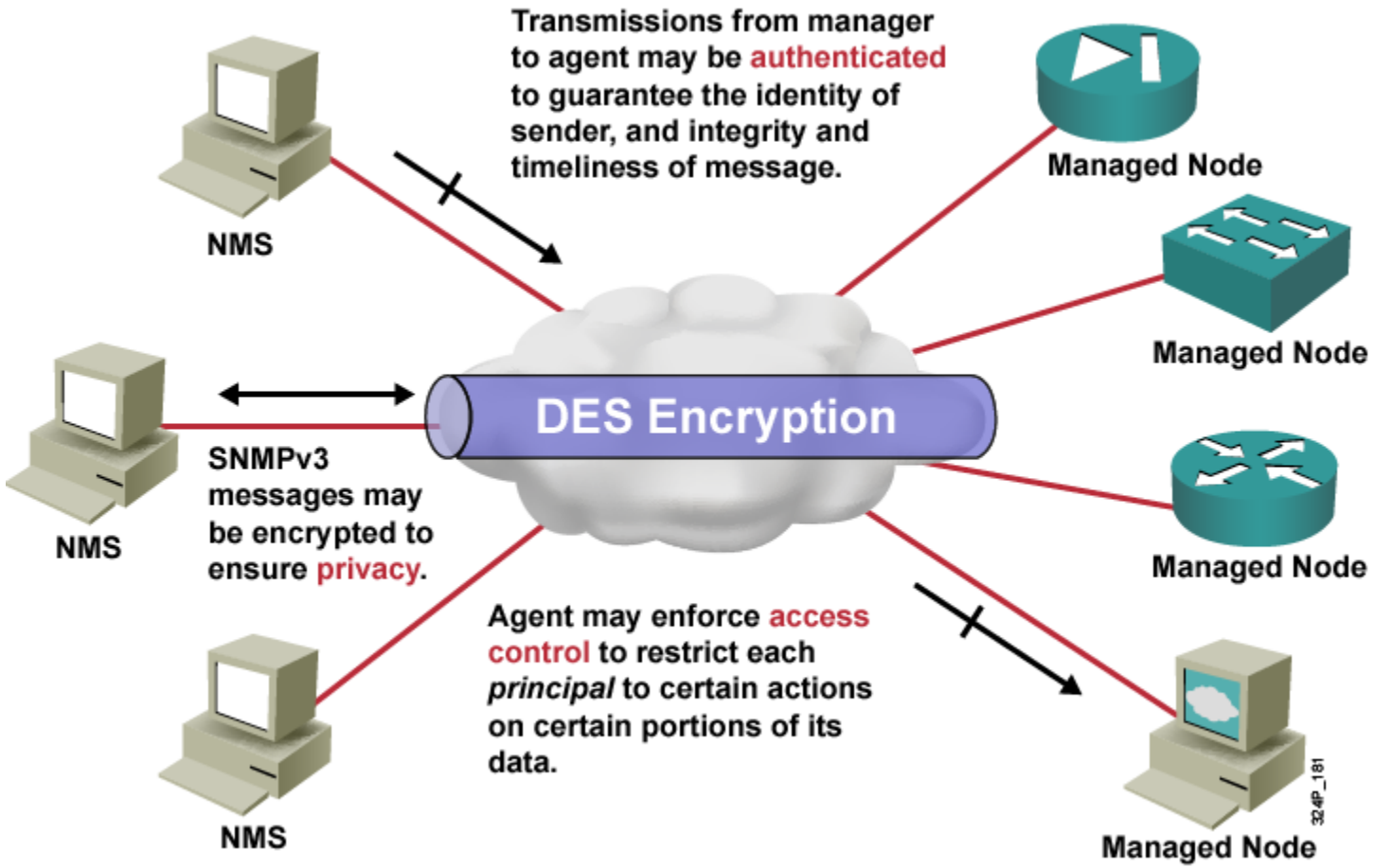
SNMP Security Models and Levels

Definitions:

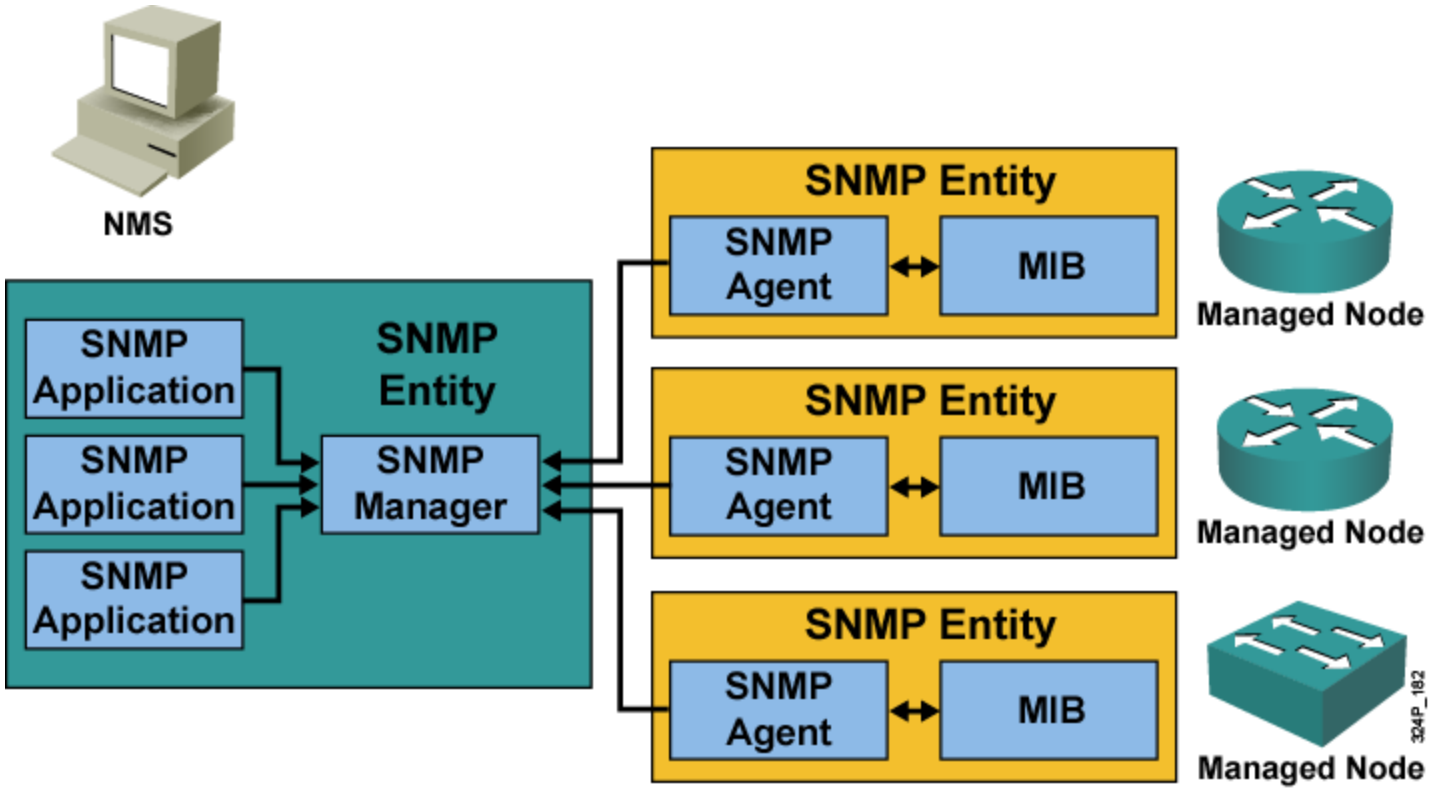
- **Security model** is a security strategy used by the SNMP agent
- **Security level** is the permitted level of security within a security model

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	• Authenticates with a community string match
v2	noAuthNoPriv	Community String	No	• Authenticates with a community string match
v3	noAuthNoPriv	Username	No	• Authenticates with a username
	authNoPriv	MD5 or SHA	No	• Provides HMAC MD5 or SHA algorithms for authentication
	authPriv	MD5 or SHA	DES	• Provides HMAC MD5 or SHA algorithms for authentication • Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard

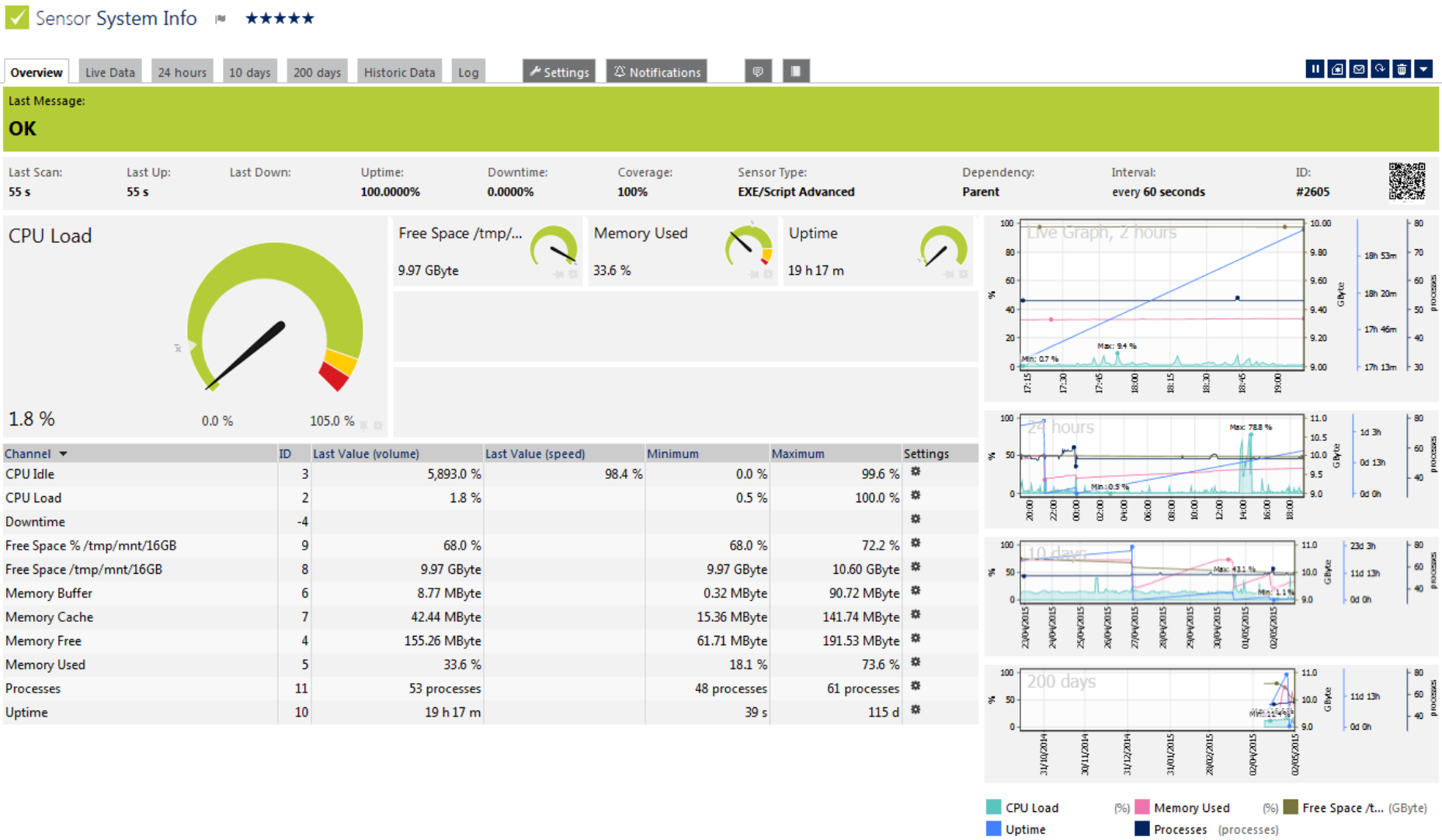
SNMPv3 Architecture



SNMP Operational Model



Example



Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
CPU Idle	3	5,893.0 %	98.4 %	0.0 %	99.6 %	
CPU Load	2	1.8 %		0.5 %	100.0 %	
Downtime	-4					
Free Space % /tmp/mnt/16GB	9	68.0 %		68.0 %	72.2 %	
Free Space /tmp/mnt/16GB	8	9.97 GByte		9.97 GByte	10.60 GByte	
Memory Buffer	6	8.77 MByte		0.32 MByte	90.72 MByte	
Memory Cache	7	42.44 MByte		15.36 MByte	141.74 MByte	
Memory Free	4	155.26 MByte		61.71 MByte	191.53 MByte	
Memory Used	5	33.6 %		18.1 %	73.6 %	
Processes	11	53 processes		48 processes	61 processes	
Uptime	10	19 h 17 m		39 s	115 d	

Configuring NTP Client

Understanding NTP

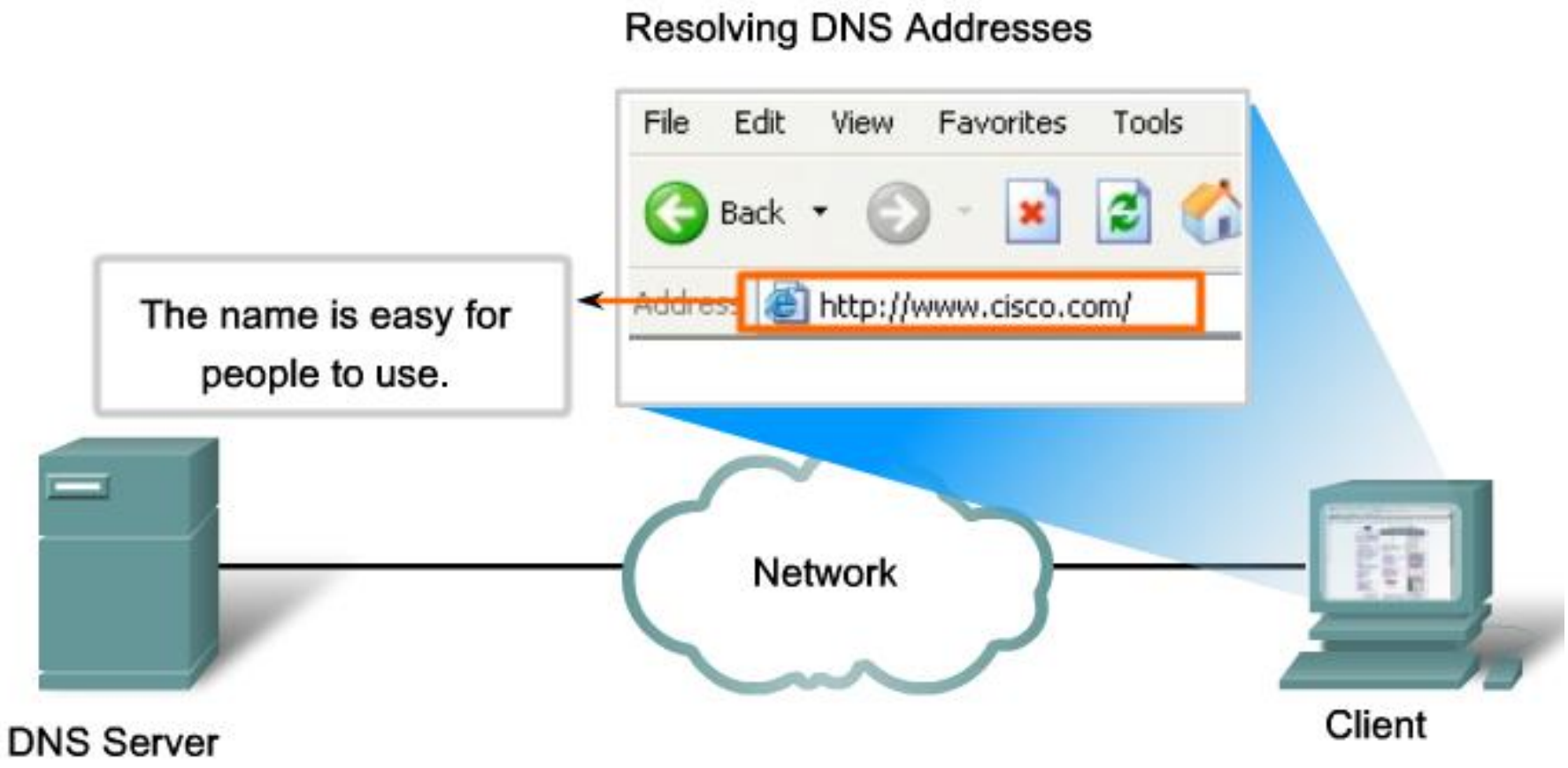
- **NTP is used to synchronize the clocks in the entire network.**
- **System clock is set by the battery system calendar during bootup.**
- **System clock can then be modified manually or via NTP.**
- **NTP runs over UDP port 123; current version is 4.**
- **Only NTP up to version 3 has been documented in RFCs.**
- **Stratum describes how many “NTP hops” away a machine is from authoritative time source.**
- **NTP establishes associations to synchronize time.**

Configuring NTP Associations

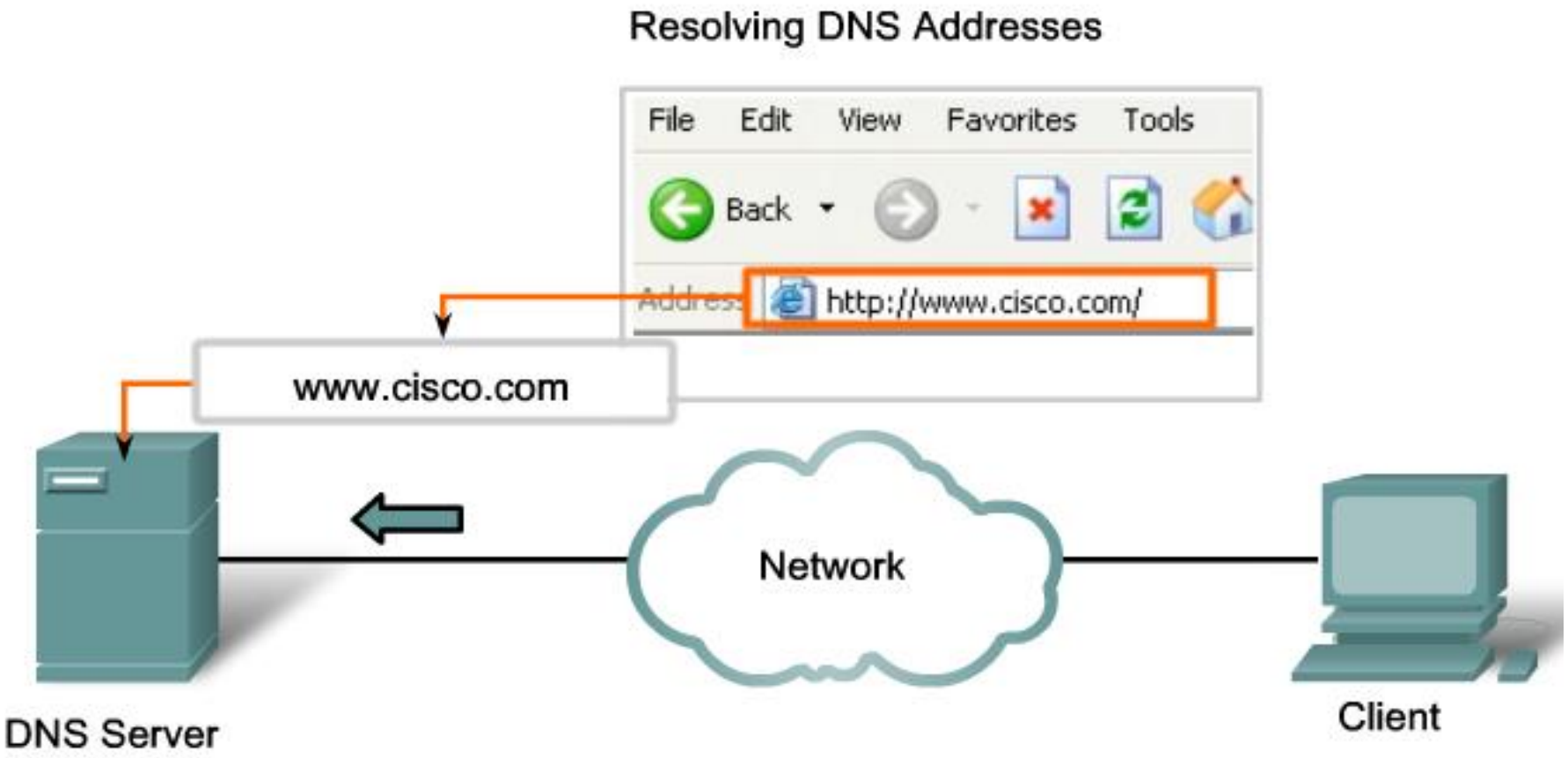
```
Router(config)#
ntp server {ip-address | hostname} [version number] [key
keyid] [source interface] [prefer]
```

- **Forms a server association with another system**

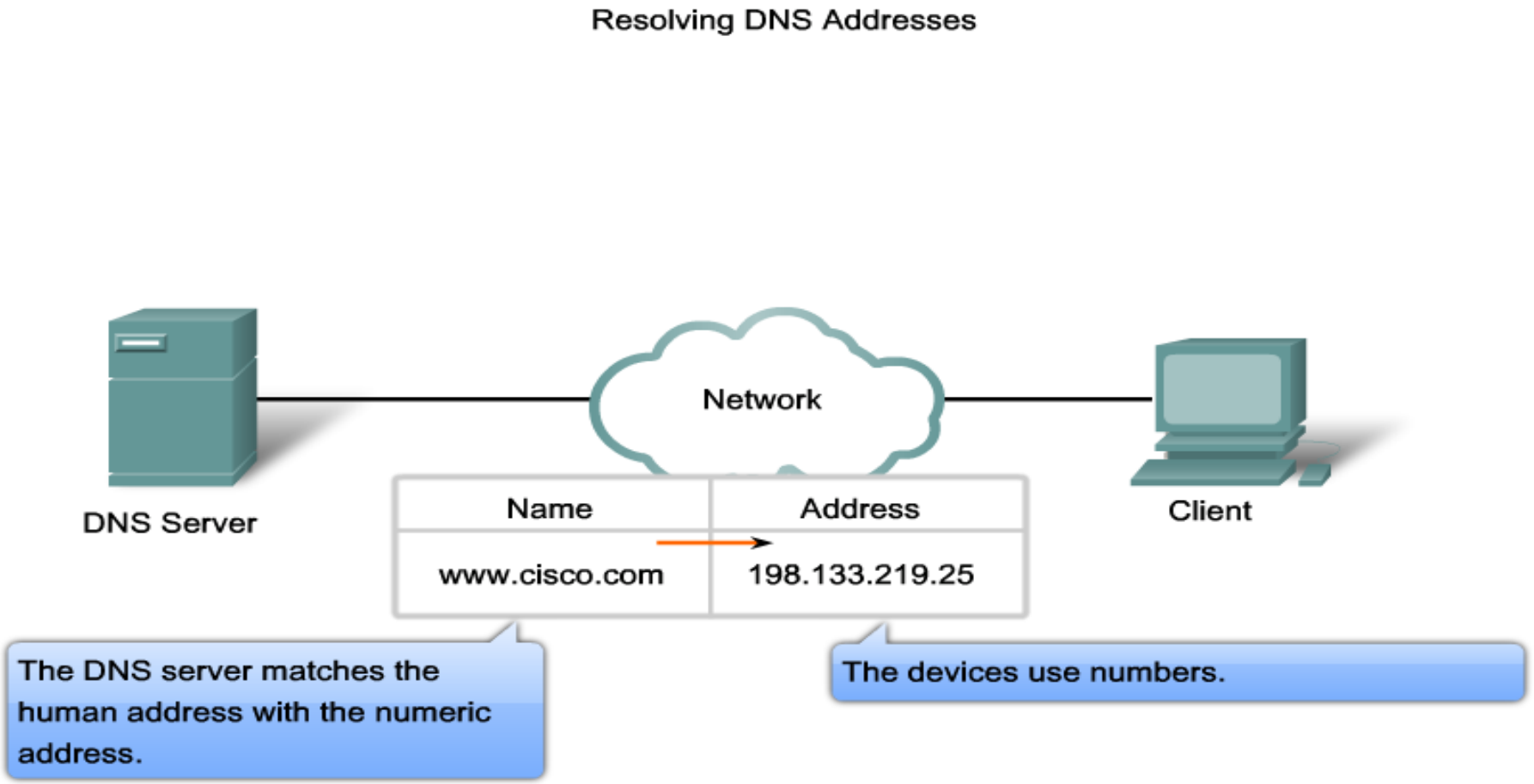
Domain Name Server - DNS



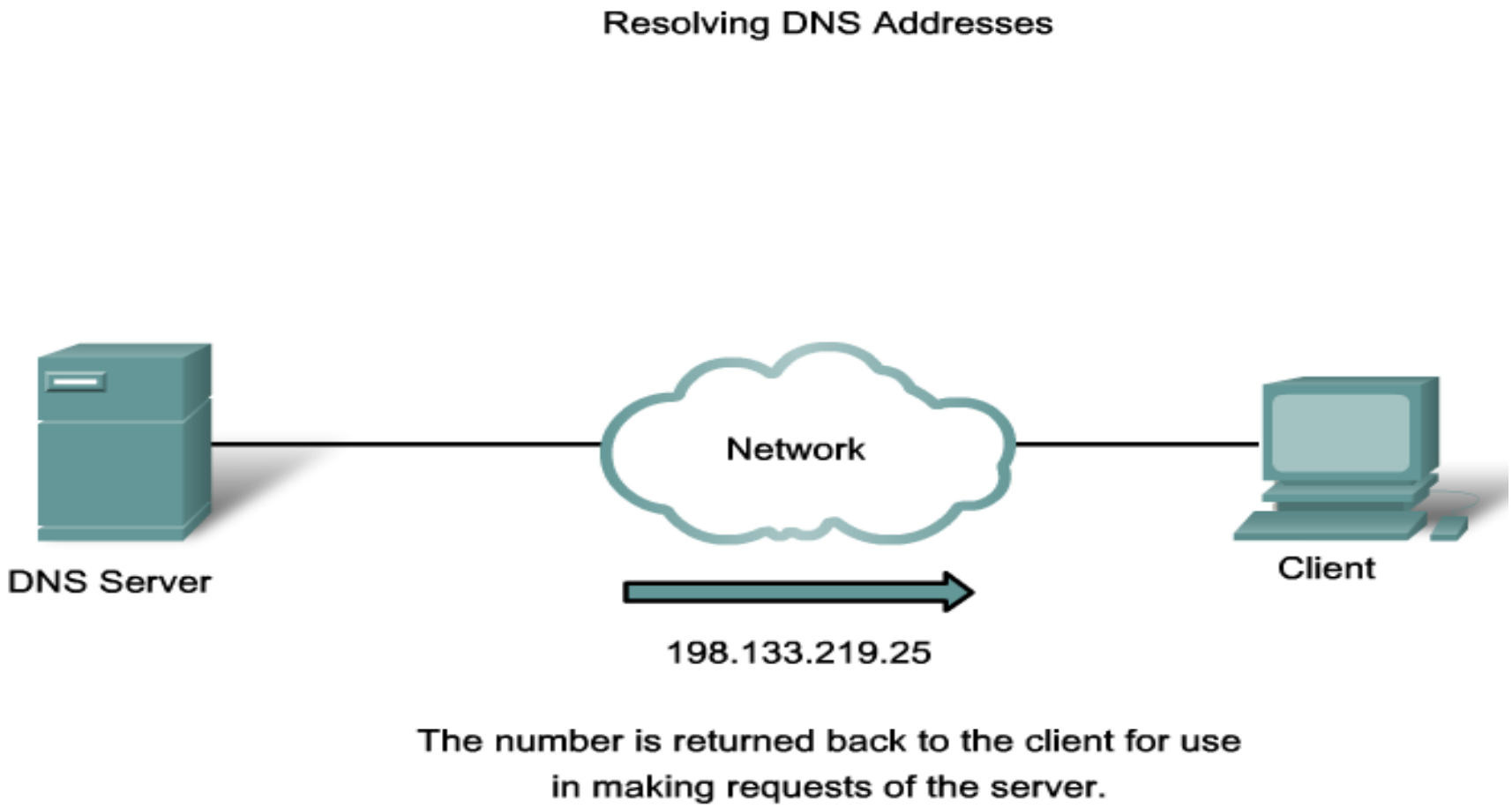
Domain Name Server - DNS



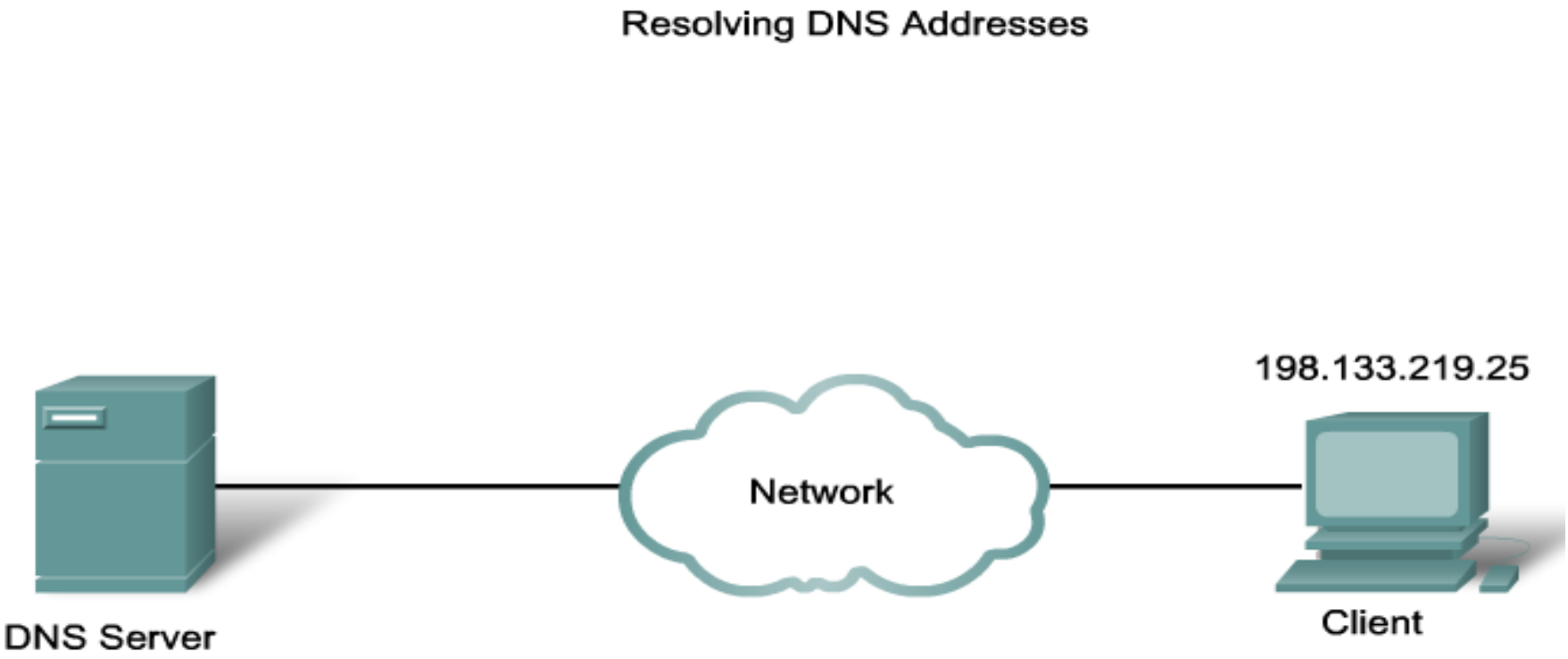
Domain Name Server - DNS



Domain Name Server - DNS



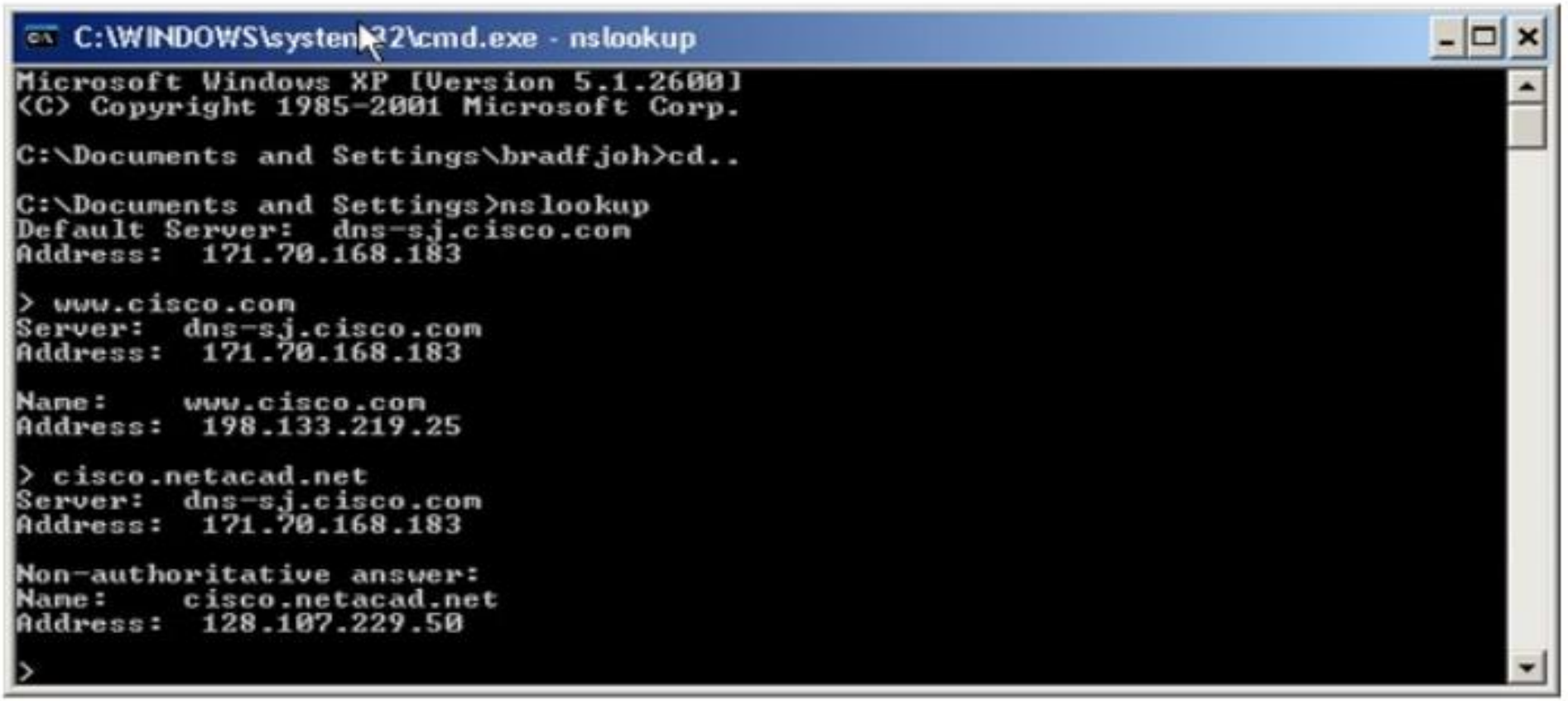
Domain Name Server - DNS



A human legible name is resolved to its numeric network device address by the DNS protocol.

Domain Name Server - DNS

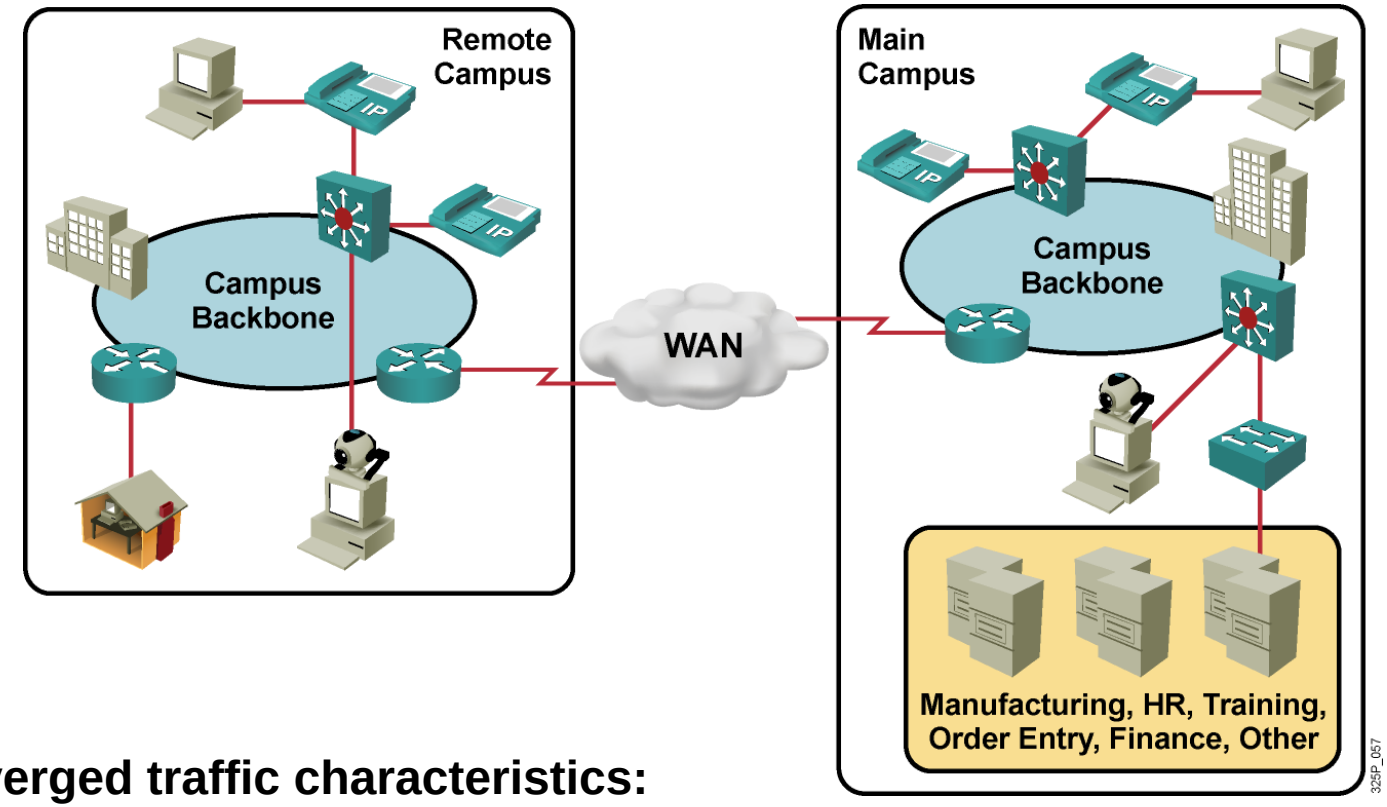
Using nslookup



Introduction to IP QoS

Introducing QoS

Converged Network Quality Issues



Converged traffic characteristics:

- Constant small-packet voice flow competes with bursty data flow.
- Critical traffic must get priority.
- Voice and video are time-sensitive.
- Brief outages are not acceptable.

Converged Network Quality Issues (Cont.)

- **Lack of bandwidth:** Multiple flows compete for a limited amount of bandwidth.
- **End-to-end delay (fixed and variable):** Packets have to traverse many network devices and links that add up to the overall delay.
- **Variation of delay (jitter):** Sometimes there is a lot of other traffic, which results in increased delay.
- **Packet loss:** Packets may have to be dropped when a link is congested.

QoS Defined

The ability of the network to provide better or "special" service to a set of users or applications or both to the detriment of other users or applications or both

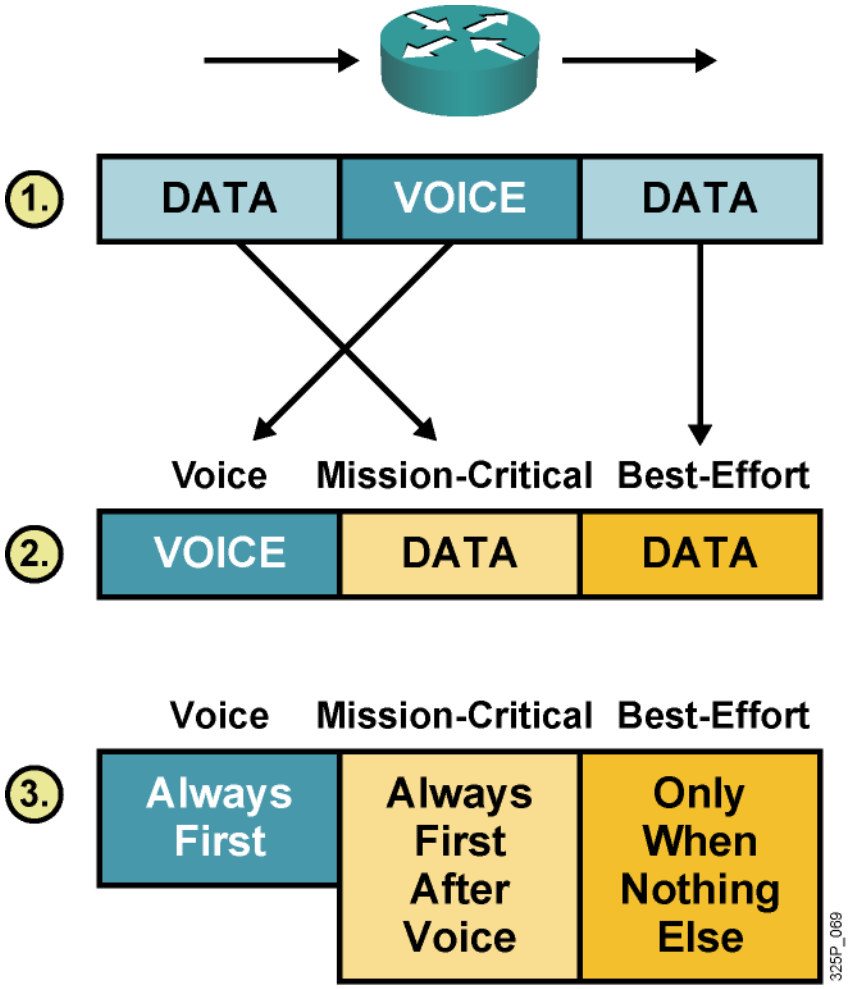
325P_068

Voice – Video – Data

Consistent and Predictable Performance

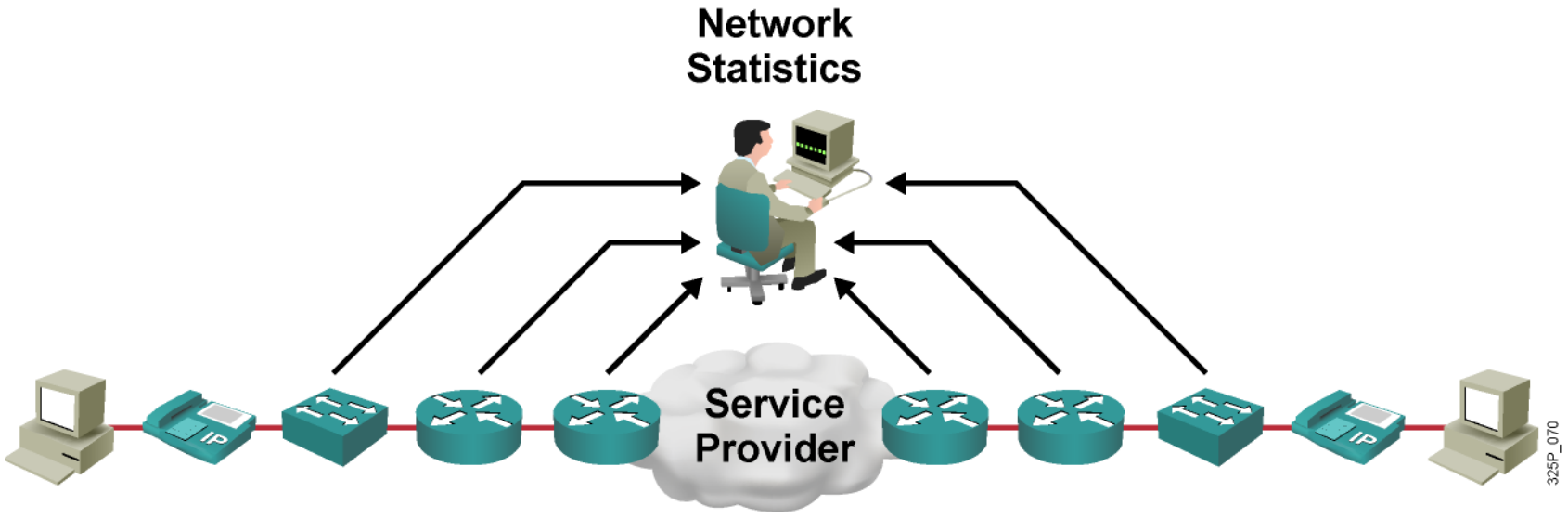
Implementing QoS

1. Identify traffic and its requirements.
2. Divide traffic into classes.
3. Define QoS policies for each class.

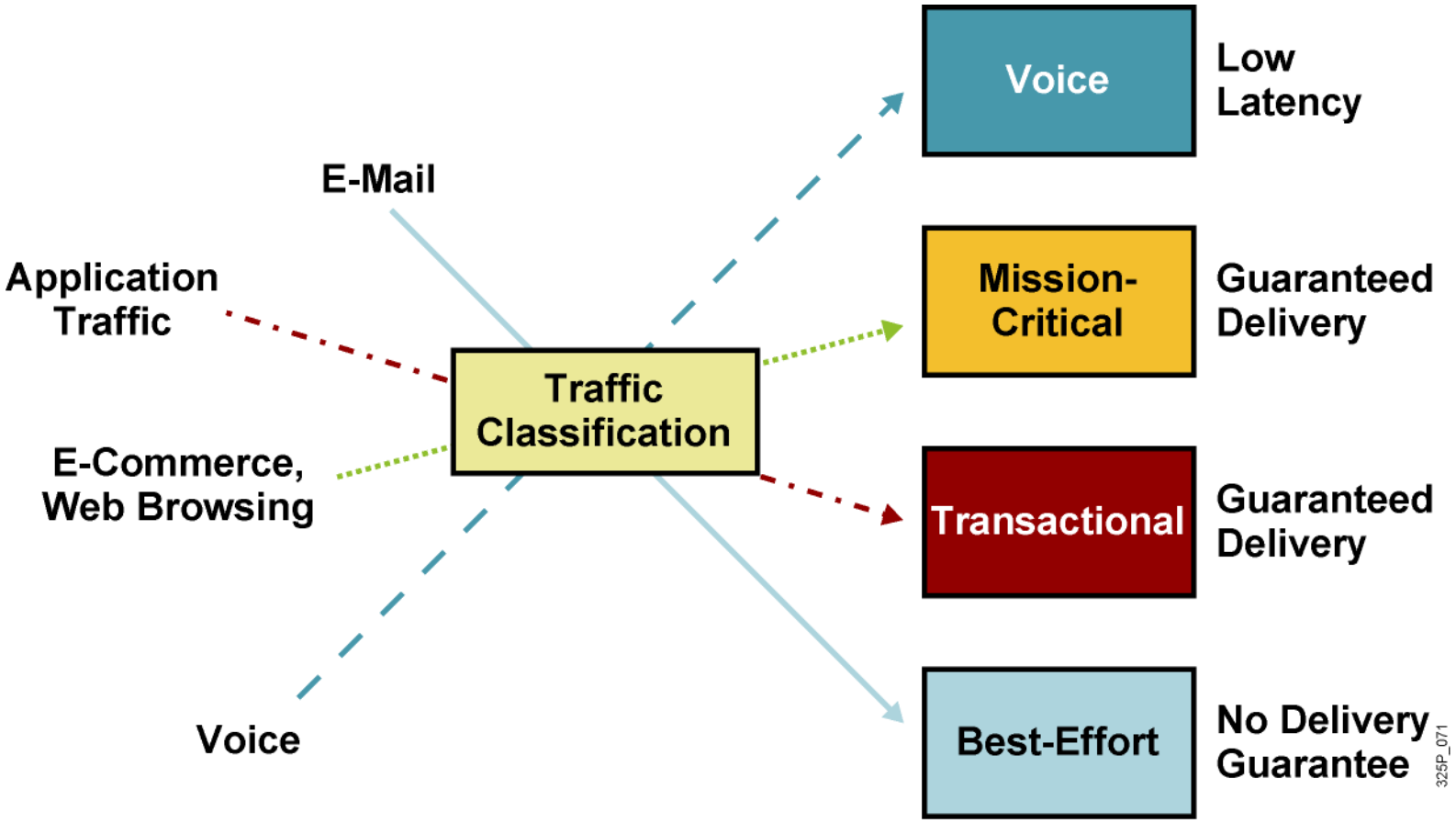


Identify Traffic and Its Requirements

- **Network audit:** Identify traffic on the network.
- **Business audit:** Determine how important each type of traffic is for business.
- **Service levels required:** Determine required response time.

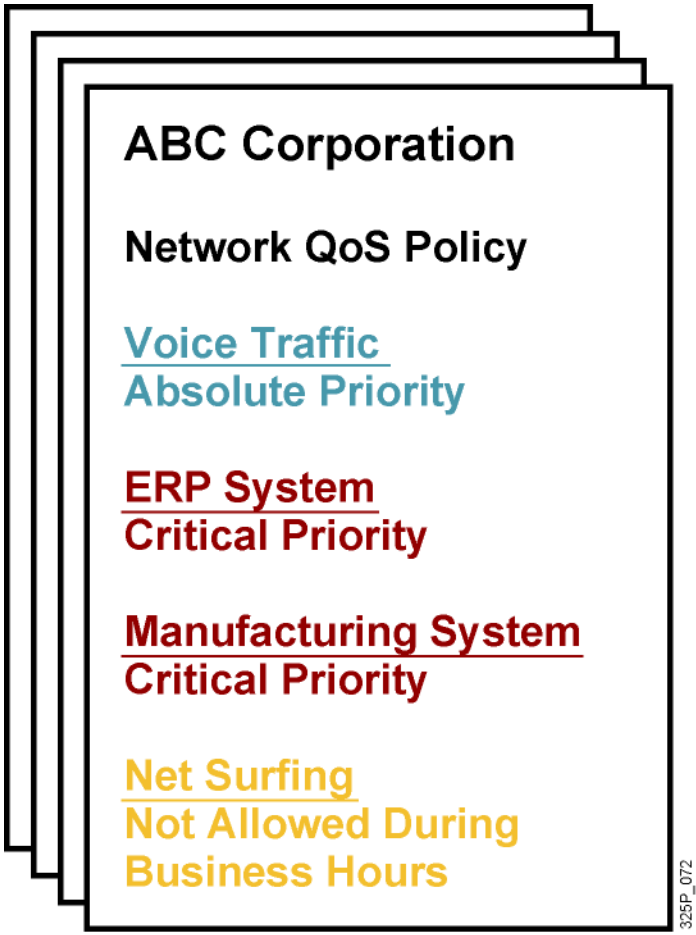


The Requirements of Different Traffic Types



QoS Policy

- **A networkwide definition of the specific levels of QoS assigned to different classes of network traffic**



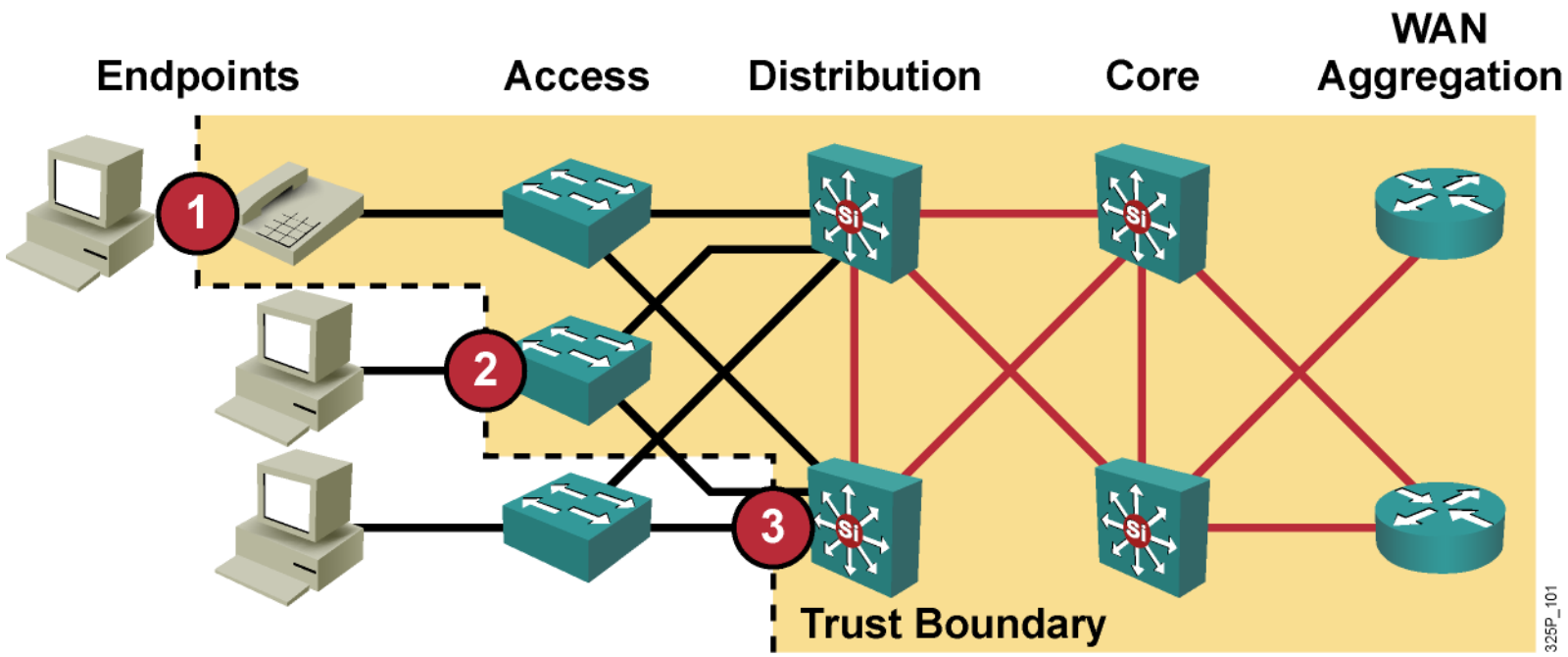
Classification

- **Classification is the process of identifying and categorizing traffic into classes, typically based upon:**
  - Incoming interface
  - IP precedence
  - DSCP
  - Source or destination address
  - Application
- **Classification is the most fundamental QoS building block.**
- **Without classification, all packets are treated the same.**

Marking

- **Marking is the QoS feature component that “colors” a packet (frame) so it can be identified and distinguished from other packets (frames) in QoS treatment.**
- **Commonly used markers:**
  - **Link layer:**
    - CoS (ISL, 802.1p)
    - MPLS EXP bits
    - Frame Relay
  - **Network layer:**
    - DSCP
    - IP precedence

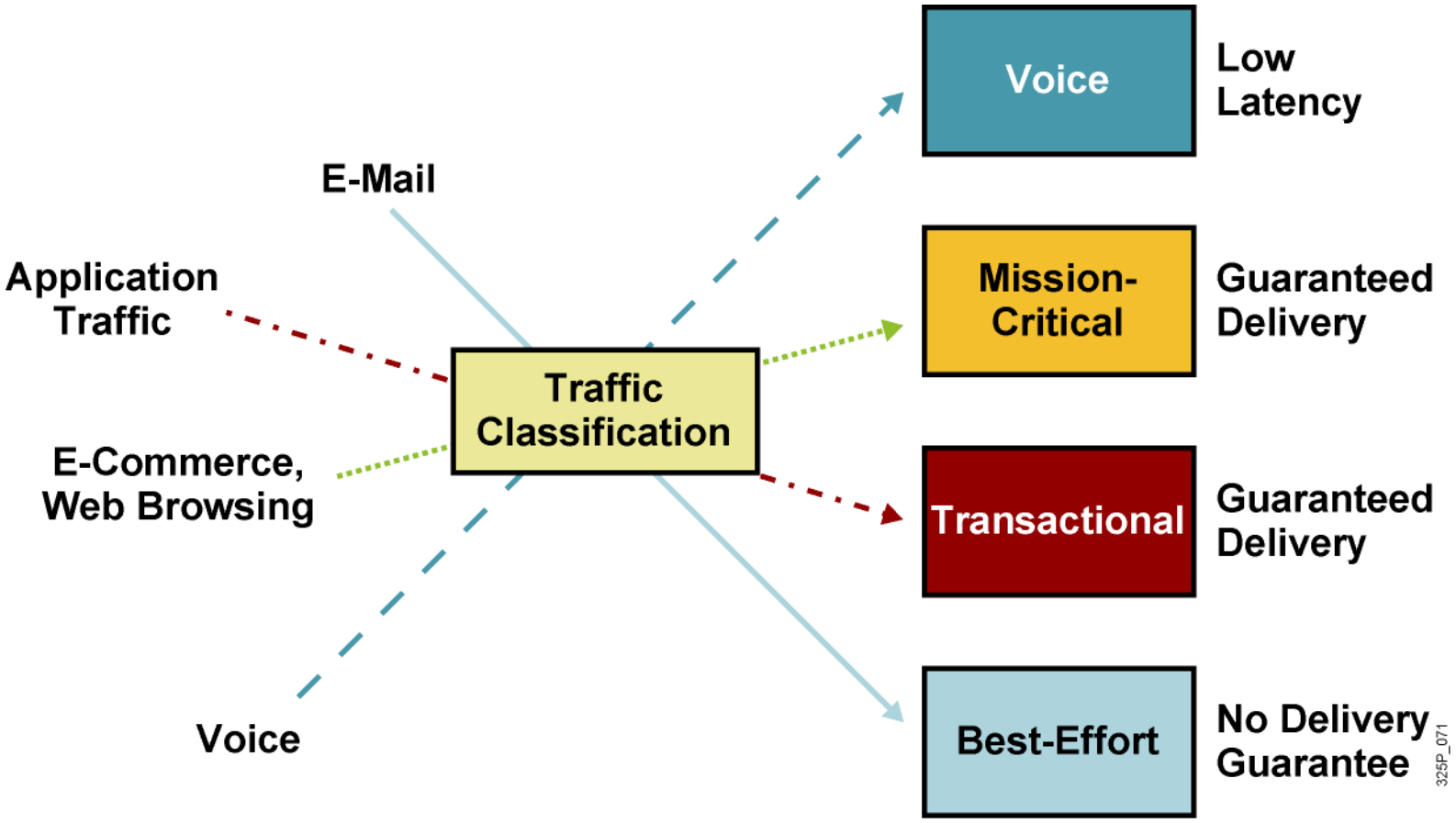
Trust Boundaries: Classify Where?



For scalability, classification should be enabled as close to the edge as possible, depending on the capabilities of the device at:

1. **Endpoint or end system**
2. **Access layer**
3. **Distribution layer**

Implementing QoS Policy Using a QoS Service Class



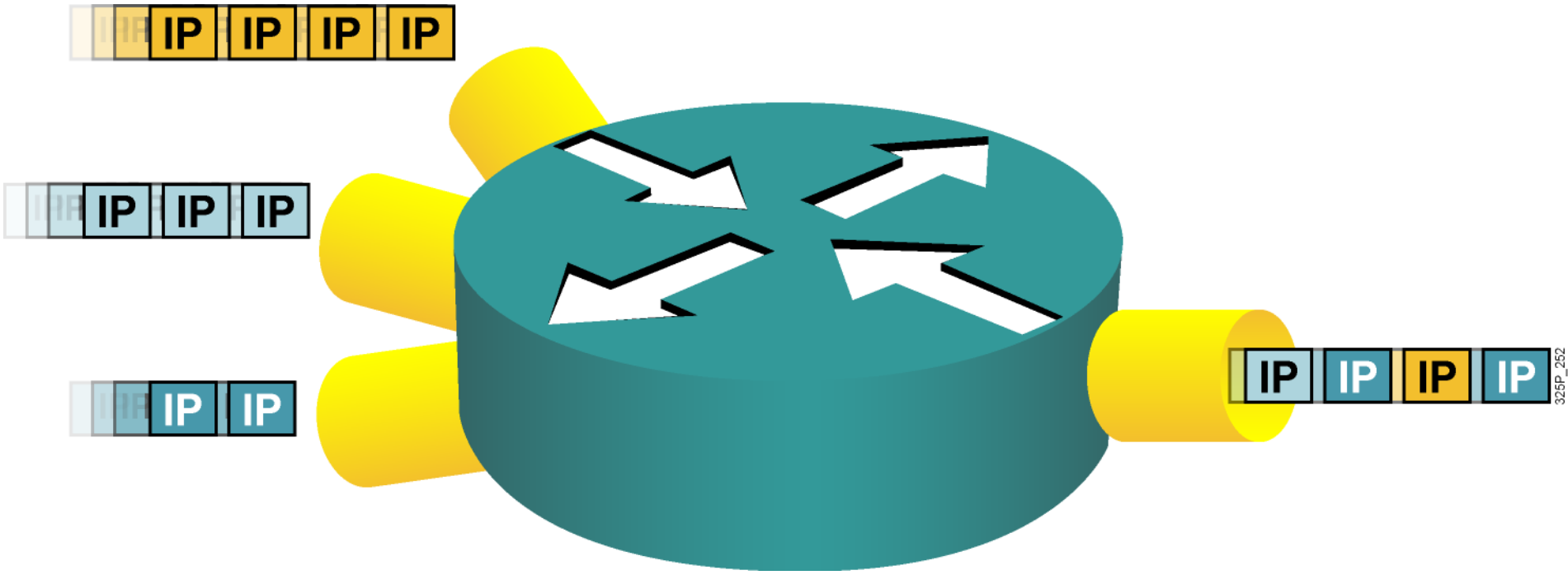
Implementing QoS Policy Using a QoS Service Class (Cont.)

- **Profile applications to their basic network requirements.**
- **Do not overengineer provisioning; use no more than four to five traffic classes for data traffic:**
  - Voice applications: VoIP
  - Mission-critical applications: Oracle, SAP, SNA
  - Interactive applications: Telnet, TN3270
  - Bulk applications: FTP, TFTP
  - Best-effort applications: E-mail, WWW
  - Scavenger applications: Nonorganizational streaming and video applications
- **Do not assign more than three applications to mission-critical or transactional classes.**
- **Use proactive policies before reactive (policing) policies.**
- **Seek executive endorsement of relative ranking of application priority prior to rolling out QoS policies for data.**

Implement the DiffServ QoS Model

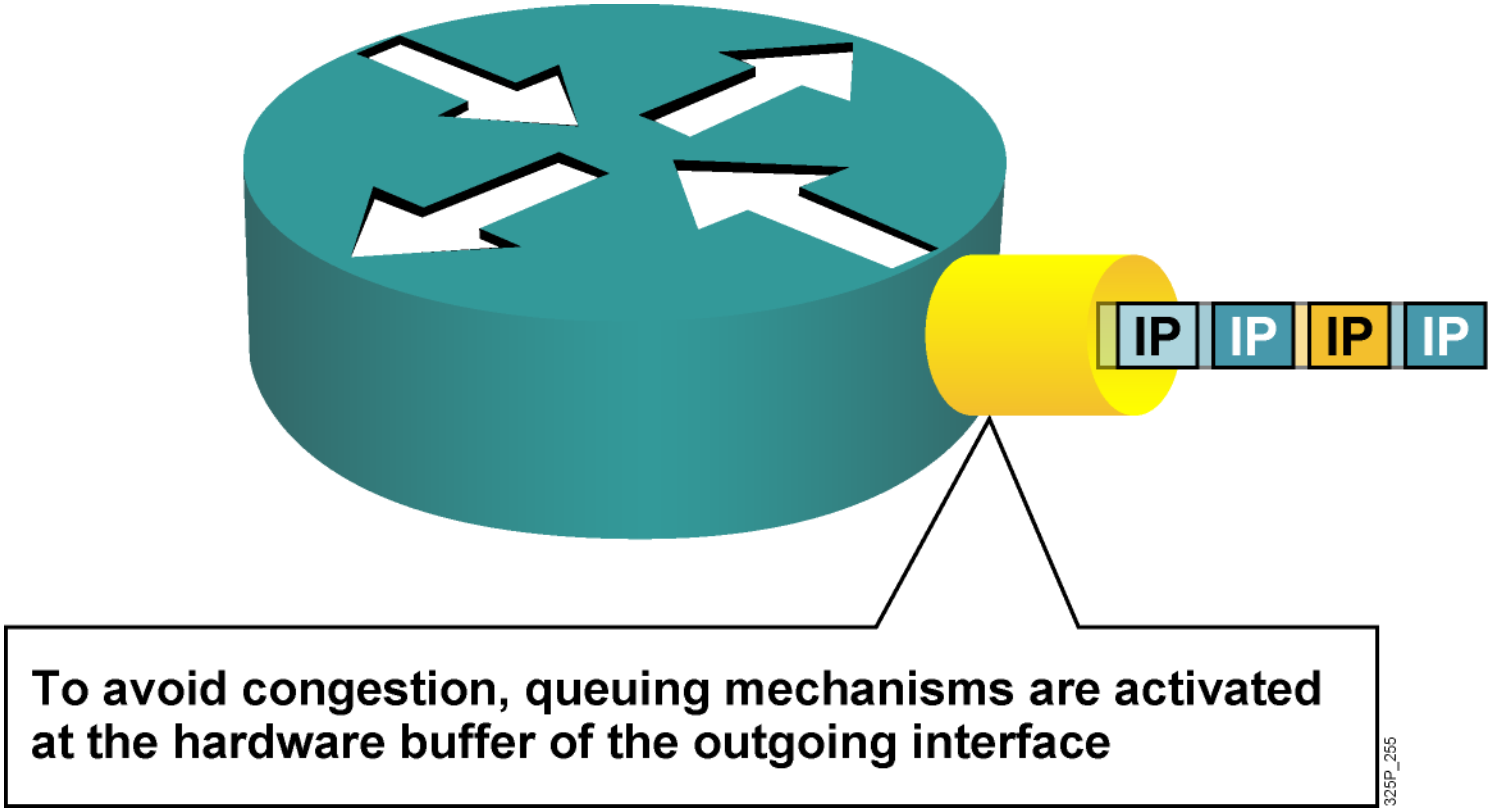
Introducing Queuing Implementations

Congestion and Queuing



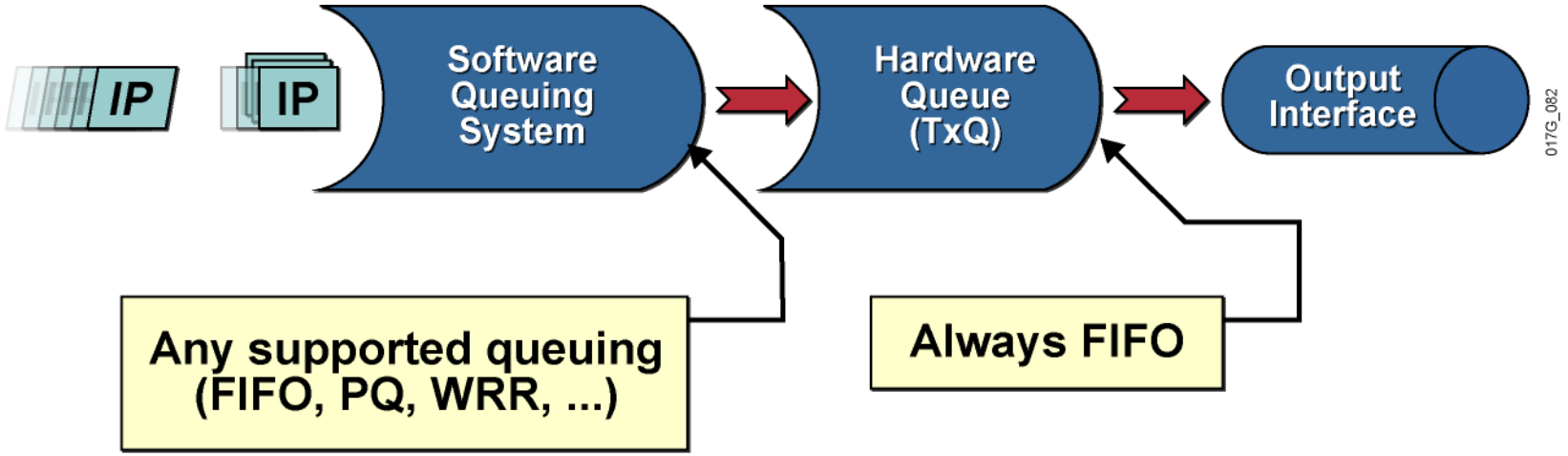
- Congestion can occur at any point in the network where there are points of speed mismatches or aggregation.
- Queuing manages congestion to provide bandwidth and delay guarantees.

Congestion and Queuing



Queuing Algorithms

- First in, first out (FIFO)
- Priority queuing (PQ)
- Round robin
- Weighted Fair Queue.
- Class Based Weighted Fair Queue.



Implement the DiffServ QoS Model

Introducing Traffic Policing and Shaping

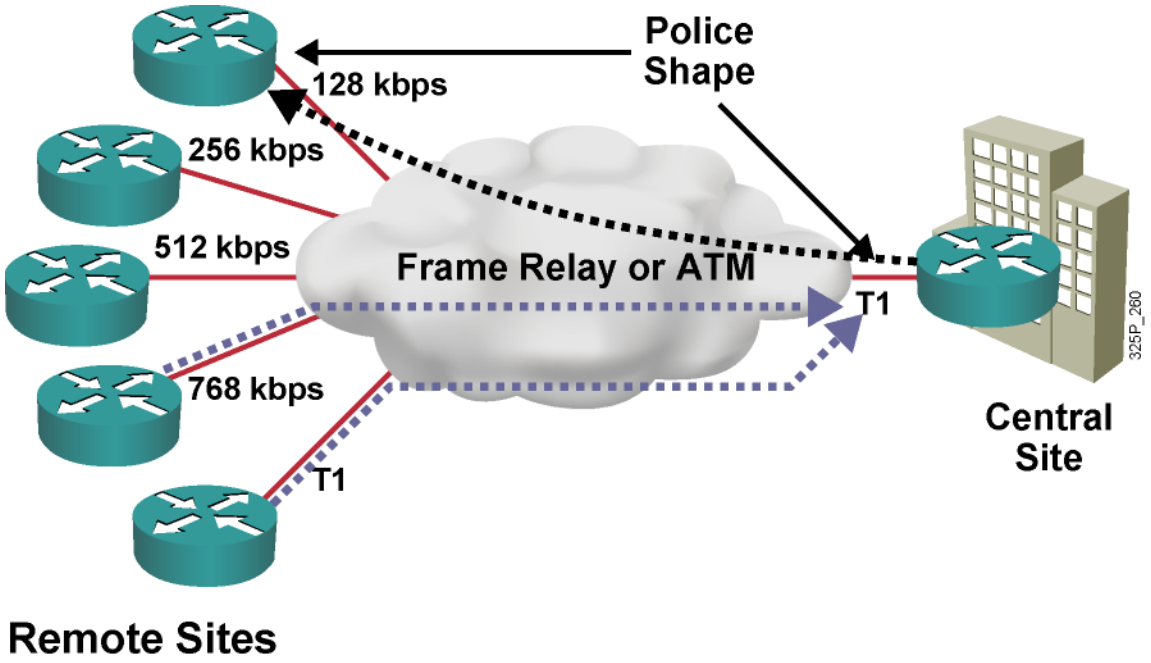
Why Use Shaping?

- **To prevent and manage congestion in ATM, Frame Relay, and Metro Ethernet networks, where asymmetric bandwidths are used along the traffic path**
- **To regulate the sending traffic rate to match the subscribed (committed) rate in ATM, Frame Relay, or Metro Ethernet networks**
- **To implement shaping at the network edge**

Why Use Policing?

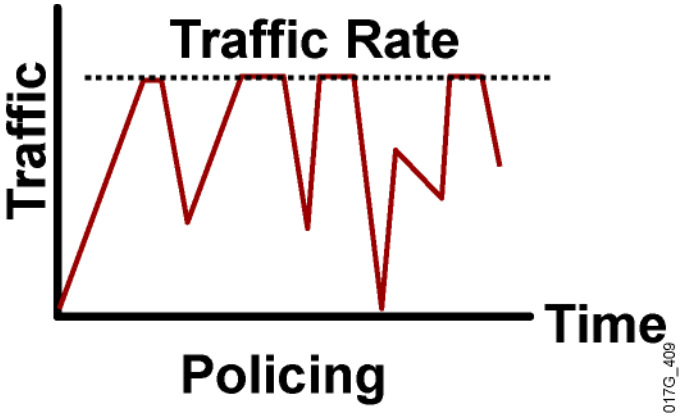
- **To limit access to resources when high-speed access is used but not desired (subrate access)**
- **To limit the traffic rate of certain applications or traffic classes**
- **To mark down (recolor) exceeding traffic at Layer 2 or Layer 3**

Traffic Policing and Shaping Example

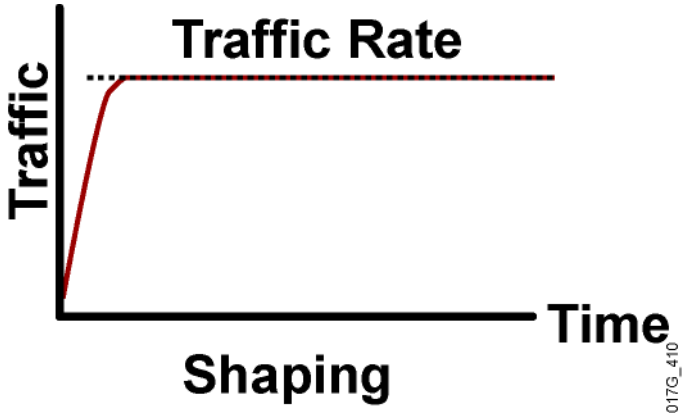


- Central to remote site speed mismatch
- Remote to central site oversubscription
- Both situations result in buffering and in delayed or dropped packets.

Policing vs. Shaping

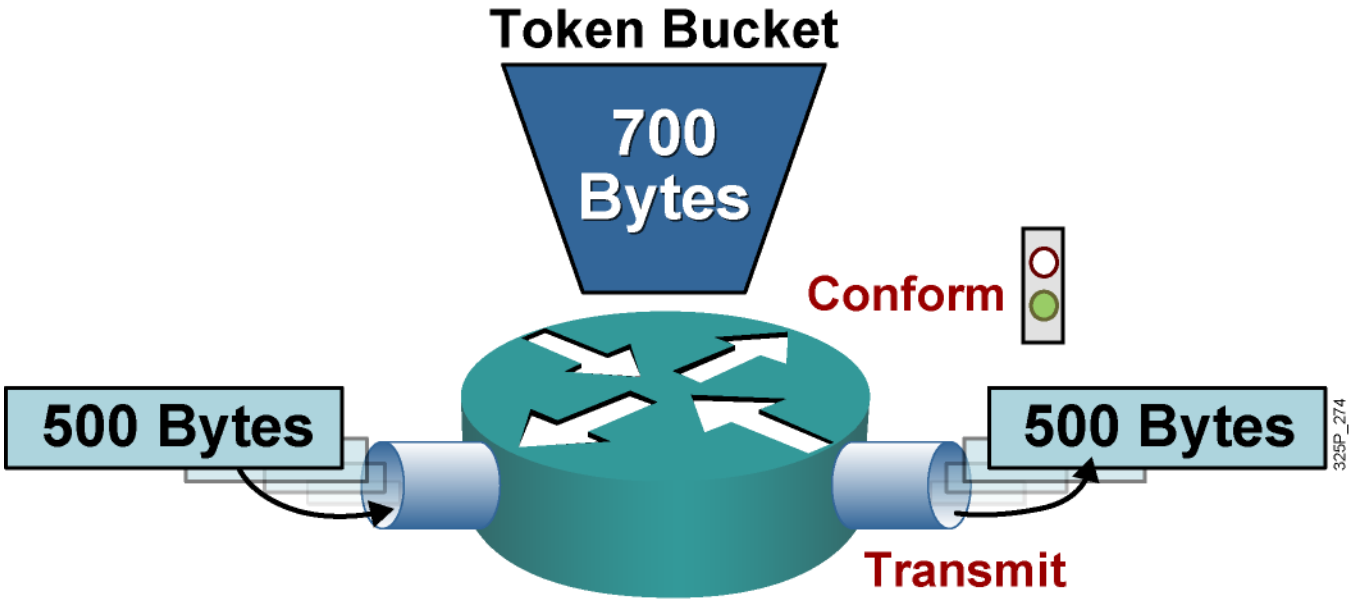


- Incoming and outgoing directions.
- Out-of-profile packets are dropped.
- Dropping causes TCP retransmits.
- Policing supports packet marking or re-marking.



- Outgoing direction only.
- Out-of-profile packets are queued until a buffer gets full.
- Buffering minimizes TCP retransmits.
- Marking or re-marking not supported.
- Shaping supports interaction with Frame Relay congestion indication.

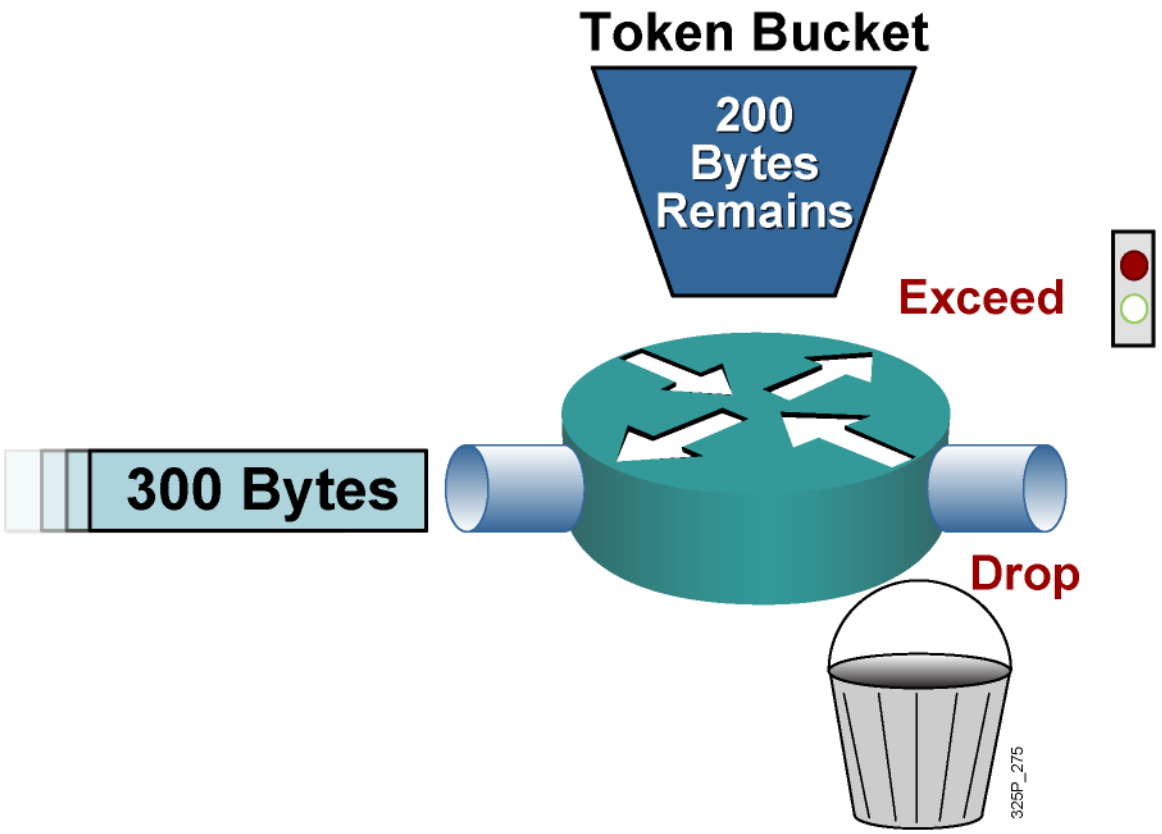
Single Token Bucket



If sufficient tokens are available (conform action):

- **Tokens equivalent to the packet size are removed from the bucket.**
- **The packet is transmitted.**

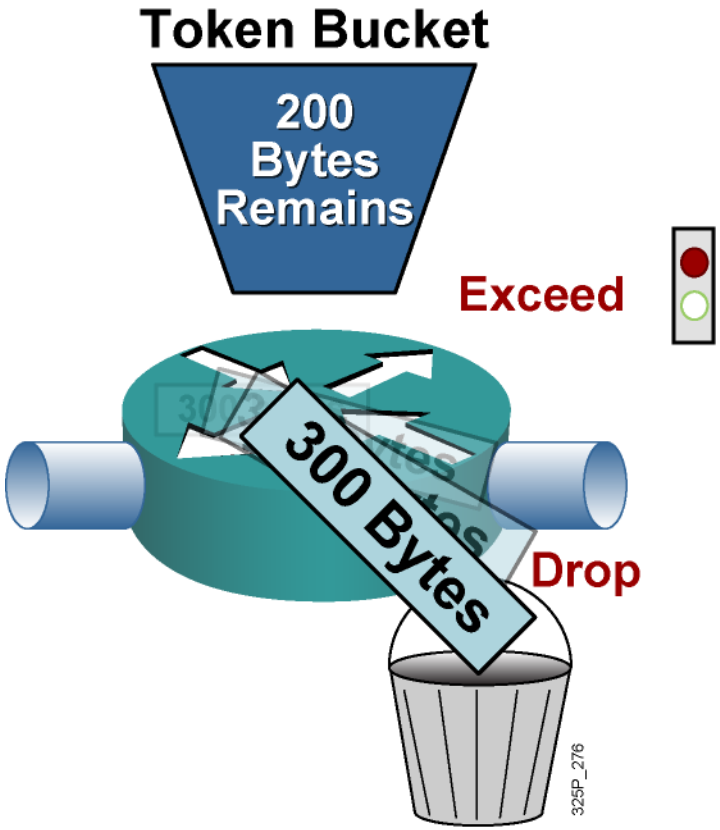
Single Token Bucket (Cont.)



If sufficient tokens are not available (exceed action):

- **Drop (or mark) the packet.**

Single Token Bucket (Cont.)



If sufficient tokens are not available (exceed action):

- **Drop (or mark) the packet.**


CISCO