Unit 9: Windows 2000 Networking

9.5. Quality-of-Service and Security – RSVP and IPsec

Quality-of-Service (QoS)

- What is QoS?
  - QoS is about user perception
  - Providing the necessary service quality to applications…
- Enabling the network manager or administrator to manage resource allocation in the network...

Providing The Necessary Service Quality

- Playback multimedia applications need bandwidth guarantee (quantitative applications)
- Interactive multimedia applications need bandwidth and delay guarantees (quantitative applications)
- Mission critical applications need minimum delay bounds regardless of ambient network load (typically qualitative applications)

Managing Resource Allocation In The Network

- Prevent non-adaptive protocols (e.g., UDP) from abusing network resources
- Partition resources between “best-effort” traffic and higher priority traffic
- Reserve resources for entitled users/applications
- Prioritize access to resources based on user/application

Application QoS

- Quantitative applications' require bandwidth guarantees. This entails
  - strict admission control
  - knowledge of traffic routes
  - quantified resource requirements
- Qualitative applications' require delay bounds
  - Cannot rely on quantified requirements
  - Looser assurances (better than best effort)

QoS Mechanisms

- **RSVP**
- **802.1p** / ATM
- Differentiated Services
- Traffic Control
- Admission Control / Policy

Beyond the scope of this presentation

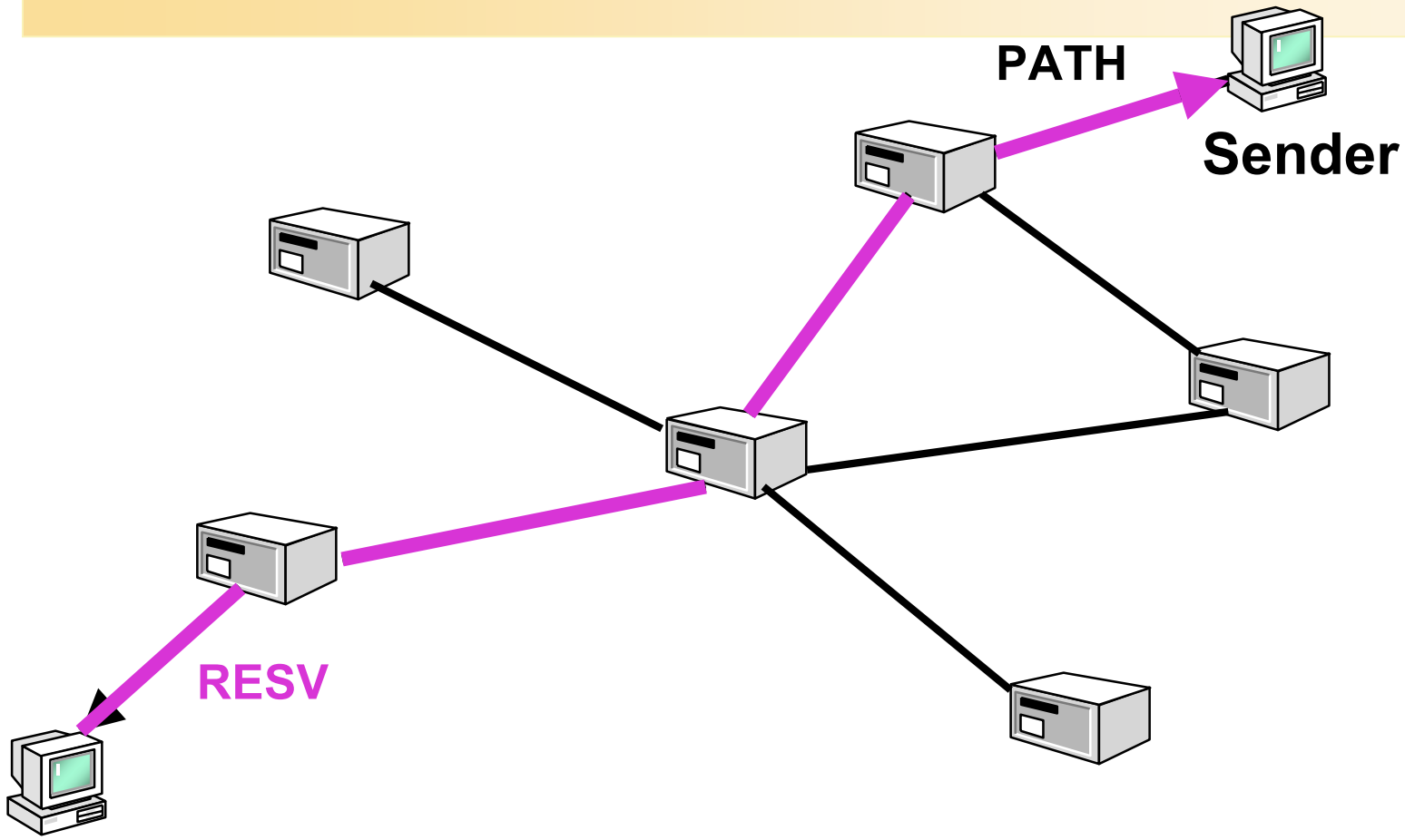
RSVP

- Resource reSerVation Protocol
- Signaling protocol
- Operates at Layer 3 (IP)
- Inherent topology awareness

RSVP Signaling

- Unidirectional
- Soft state. Refresh every 30 sec
- Signaling messages
  - PATH
  - RESV
- RSVP signaling messages carry
  - Flowspec - specifies type of service and quantity of resources required
  - Filterspec - specifies the flow that gets the QoS
  - Policy information – who am I, etc

RSVP Signaling



RSVP PATH messages

- Setup state through the network
- Carries QoS parameters advertised by the sender
- Carries policy data
  - User ID
  - Application ID

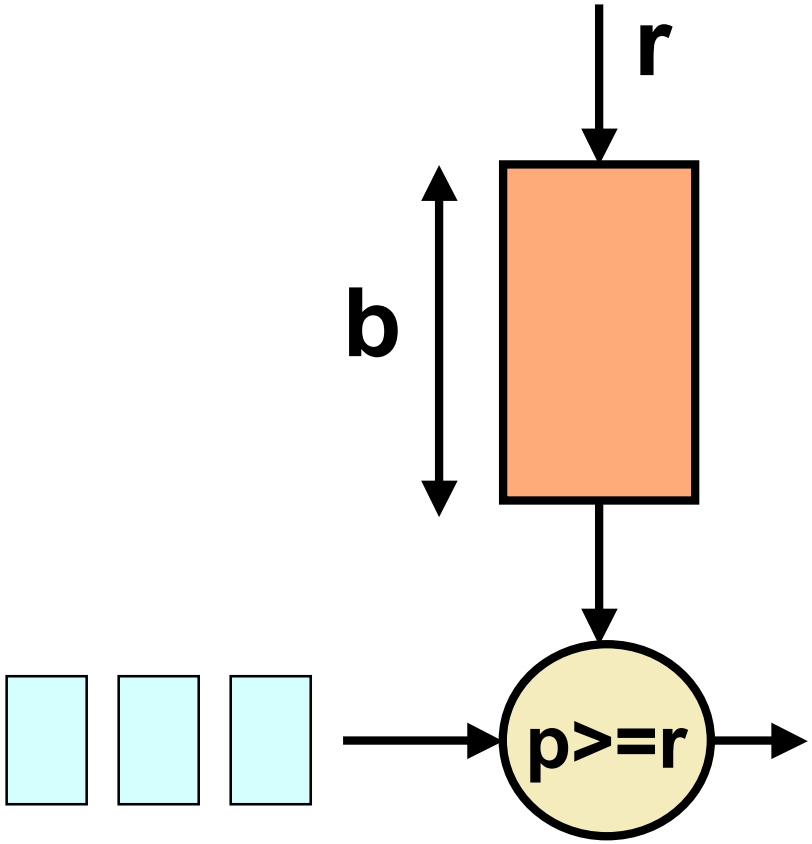
RSVP RESV Message

- Retraces same route as PATH
- Reserves resources in the network
- Carries QoS parameters requested by the receiver
- Carries policy objects
  - User ID
  - Application ID

QoS Parameters - Service Type

- Best effort
  - Default flow
  - Low priority
- Controlled load
  - Gets service equivalent to lightly loaded network
  - Medium priority
- Guaranteed service
  - Guaranteed delay bounds
  - Highest priority
- Qualitative service
  - Requested by Qualitative applications

QoS Parameters – Token Bucket Model



- Token rate (r)
- Peak rate (p)
- Bucket size (b)
- Max burst size
- Min policed size
- Latency
- Delay variation

802.1p

- Works at Layer 2 (e.g - Ethernet)
- 8 traffic classes
- Traffic class information carried in the layer 2 frame header
  - Token ring and FDDI have defined priority fields
  - Ethernet frames use VLAN tags (802.1q) to carry priority information

802.1p Priority Classes

Priority	Traffic Types
7	Network Control
6	Interactive Voice
5	Interactive Multimedia
4	Controlled Load Apps (Streaming Multimedia)
3	Excellent Effort
0	Best Effort (Default)
2	Spare
1	Background

Mapping Intserv Service Types to 802.1p priority

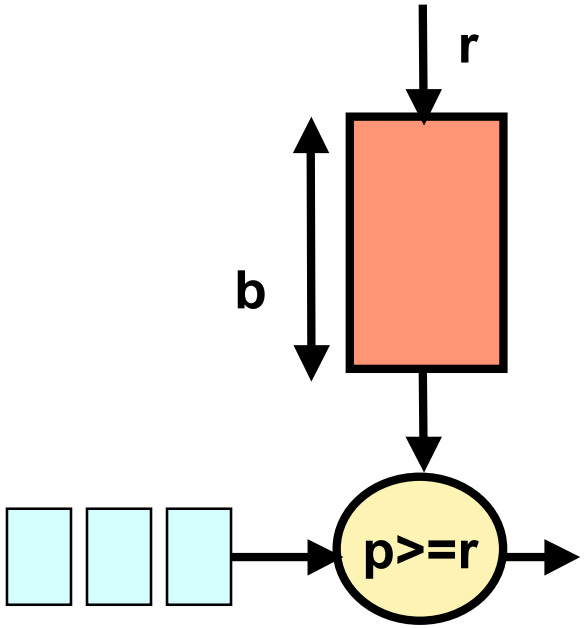
Service Type	802.1p Priority
Best Effort	**0**
Controlled Load	**4**
Guaranteed	**5**
Non Conforming	**1**

Using the GQOS API

- QoS invoked via Winsock2 calls
  - WSAIoctl(SIO_SET_QOS) - Request QoS on an existing socket
  - WSAConnect() - Request QoS while connecting the socket
  - WSAJoinLeaf() - Request QoS while joining a multicast group
- Monitoring QoS
  - Register for FD_QOS events via WSAEventSelect() or WSAAsyncSelect
  - WSAIoctl(SIO_GET_QOS)

Specifying QoS

```
typedef struct _QualityOfService
{
    FLOWSPEC        SendingFlowspec;
    FLOWSPEC        ReceivingFlowspec;
    WSABUF                  ProviderSpecific;
} QOS;

typedef struct _flowspec
{
    ULONG                   TokenRate;
    ULONG                   TokenBucketSize;
    ULONG                   PeakBandwidth;
    ULONG                   Latency;
    ULONG                   DelayVariation;
    SERVICETYPE     ServiceType;
    ULONG                   MaxSduSize;
    ULONG                   MinimumPolicedSize;
} FLOWSPEC;
```



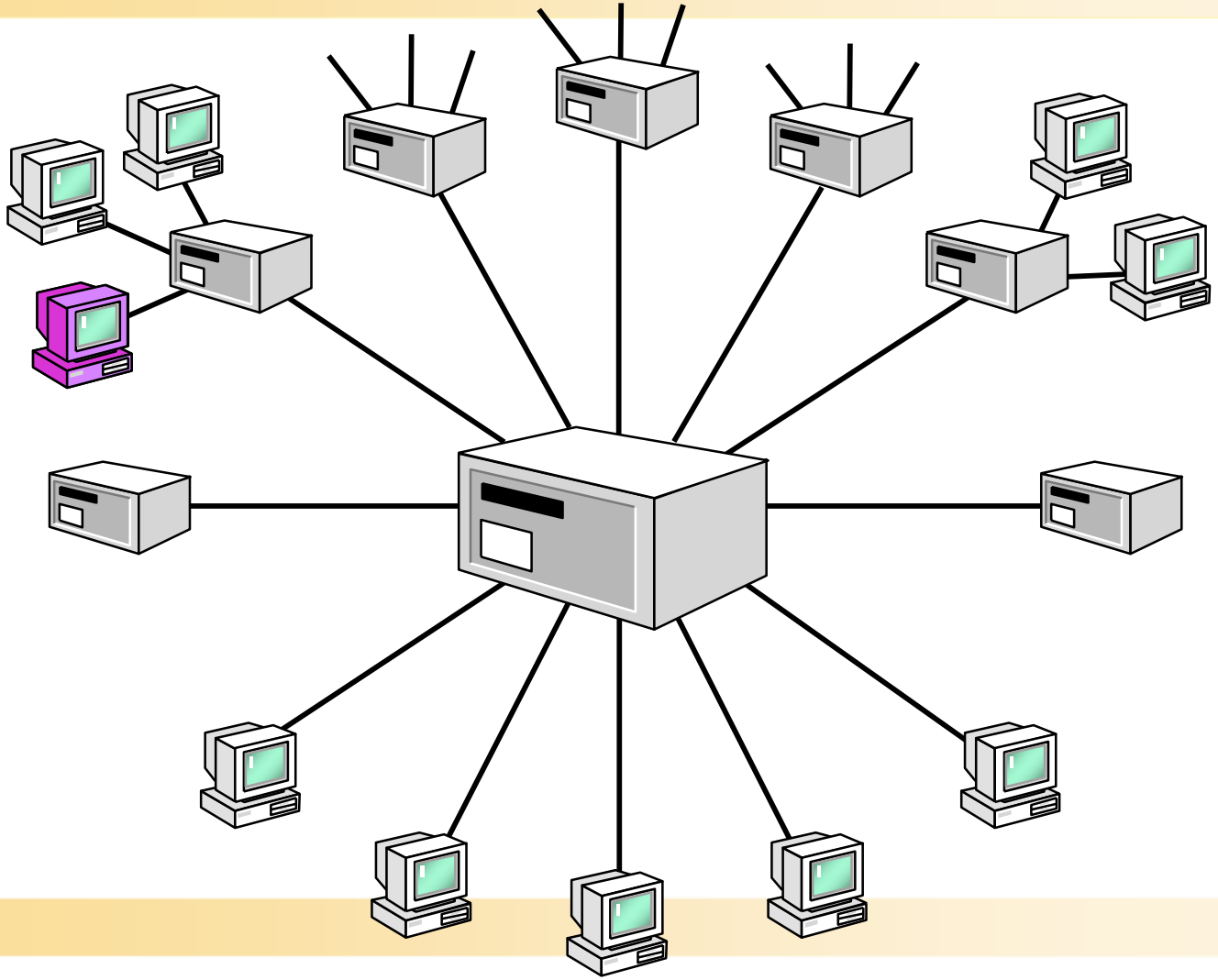
Example - WSAConnect()

```
SOCKET hSocket;
sockaddr_in          destAddress;
QOS                  qos;
// Create and bind the QOS socket
…
…

qos.SendingFlowspec.TokenRate = 8000;              // bytes/sec
qos.SendingFlowspec.TokenBucketSize = 3000;                // bytes
qos.SendingFlowspec.PeakBandwidth = 10000;                 // bytes/sec
qos.SendingFlowspec.Latency = QOS_NOT_SPECIFIED;
qos.SendingFlowspec.DelayVariation = QOS_NOT_SPECIFIED;
qos.SendingFlowspec.ServiceType = SERVICETYPE_GUARANTEED;
qos.SendingFlowspec.MaxSduSize = 1500;                     // bytes
qos.SendingFlowspec.MinimumPolicedSize = 1200;             // bytes
```

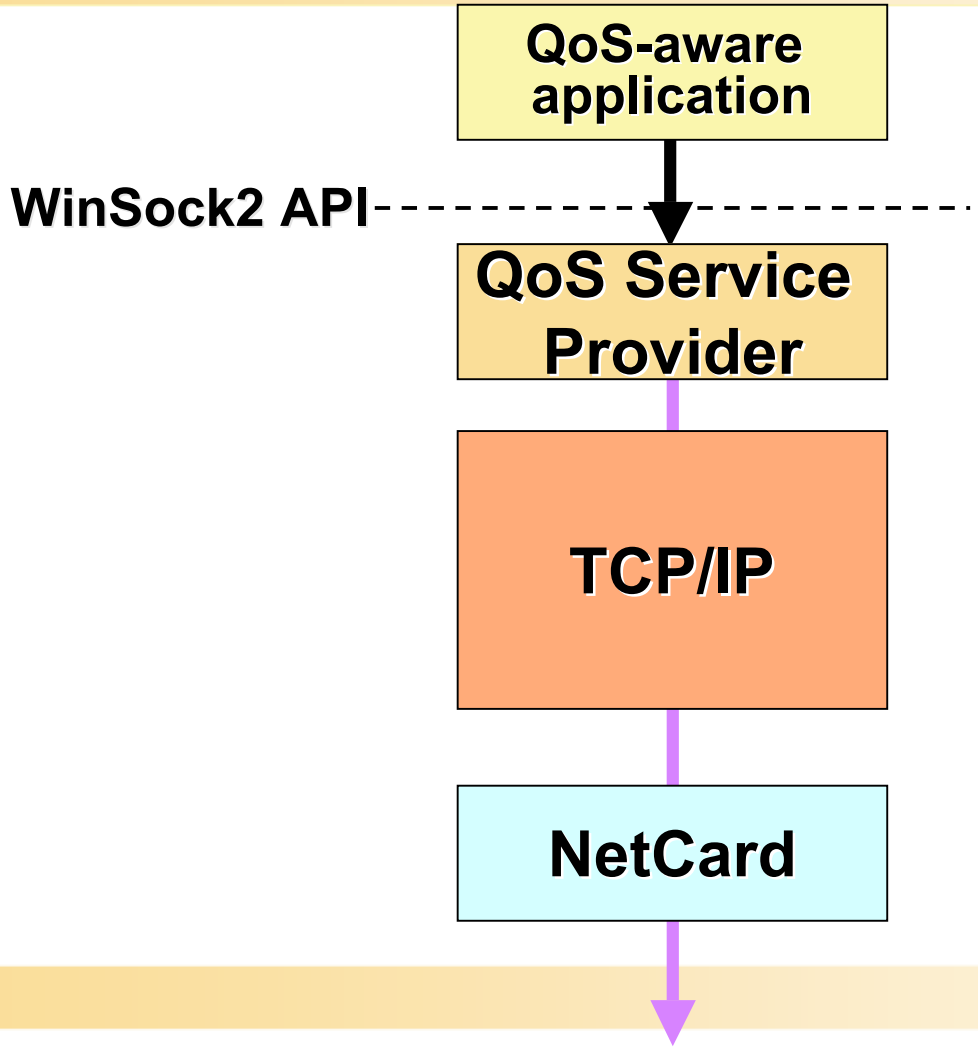
WSAConnect() (contd.)

```
qos.ReceivingFlowspec.TokenRate = 8000;                 // bytes/sec
qos.ReceivingFlowspec.TokenBucketSize = 3000;           // bytes
qos.ReceivingFlowspec.PeakBandwidth = 10000;            // bytes/sec
qos.ReceivingFlowspec.Latency = QOS_NOT_SPECIFIED;
qos.ReceivingFlowspec.DelayVariation = QOS_NOT_SPECIFIED;
qos.ReceivingFlowspec.ServiceType = SERVICETYPE_GUARANTEED;
qos.ReceivingFlowspec.MaxSduSize = 1500;                // bytes
qos.ReceivingFlowspec.MinimumPolicedSize = 1200;        // bytes
qos.ProviderSpecificBuffer = NULL;

 nRet = WSAConnect( hSocket, &destAddr, sizeof( sockaddr_in ),
                    NULL,   // Caller data
                    NULL,   // Callee data
                    &qos,
                    NULL ); // Group QOS
```

Congestion Avoidance In Fully Routed, RSVP-Enabled Network



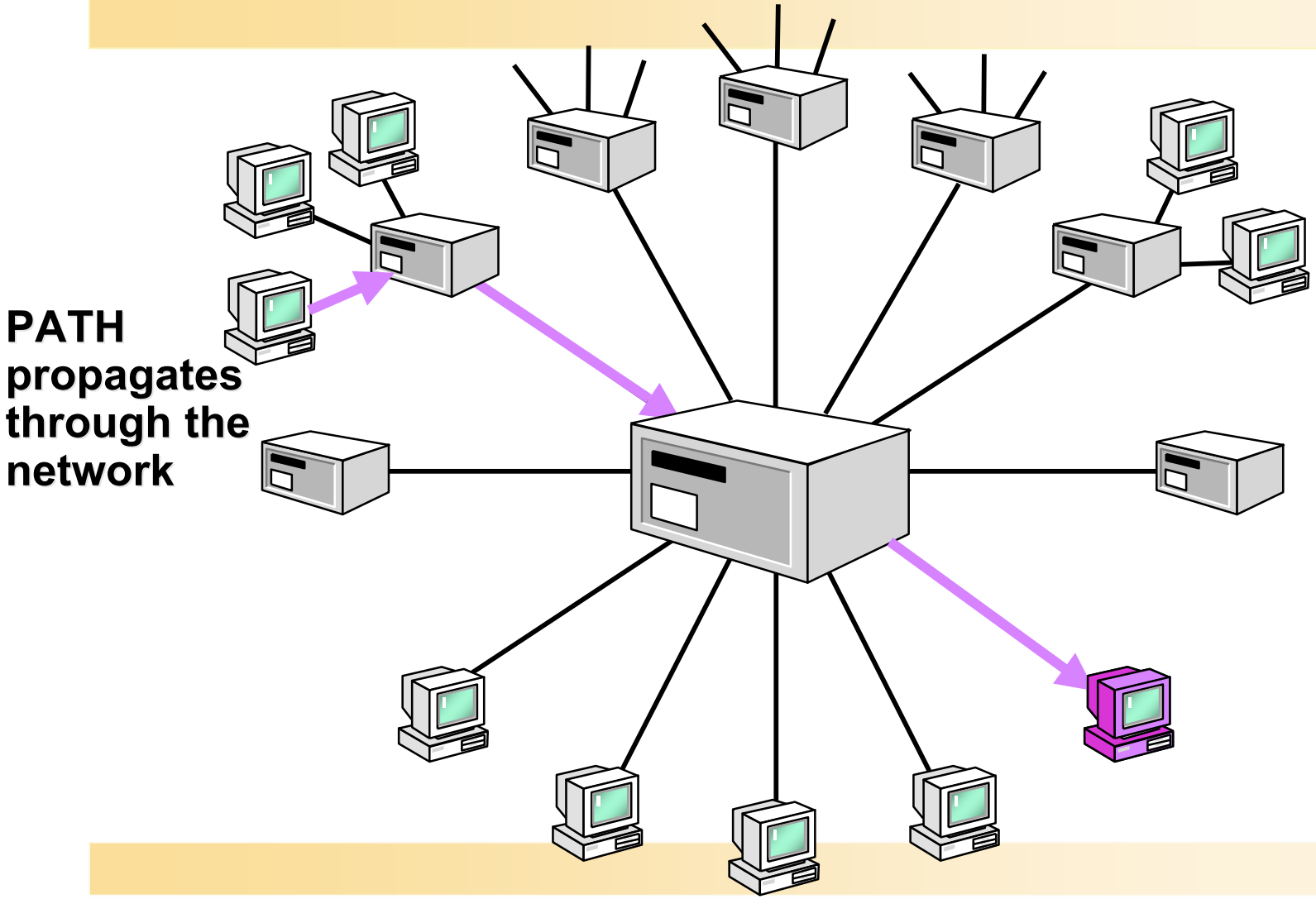
Application signals QoS Requirements



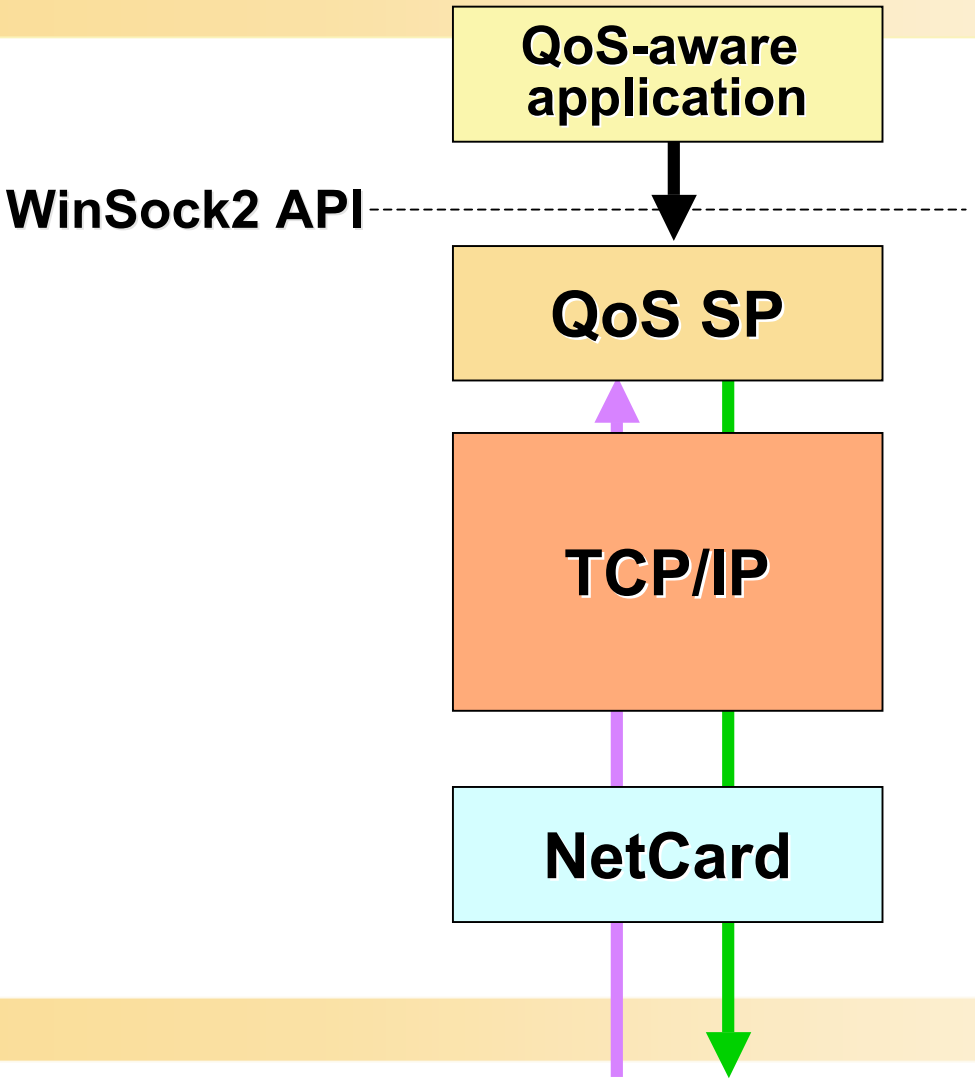
1. Application indicates that it is a QoS sender

2. QoS service provider sends RSVP PATH message to network

RSVP in Action



QoS-aware App: Receiver

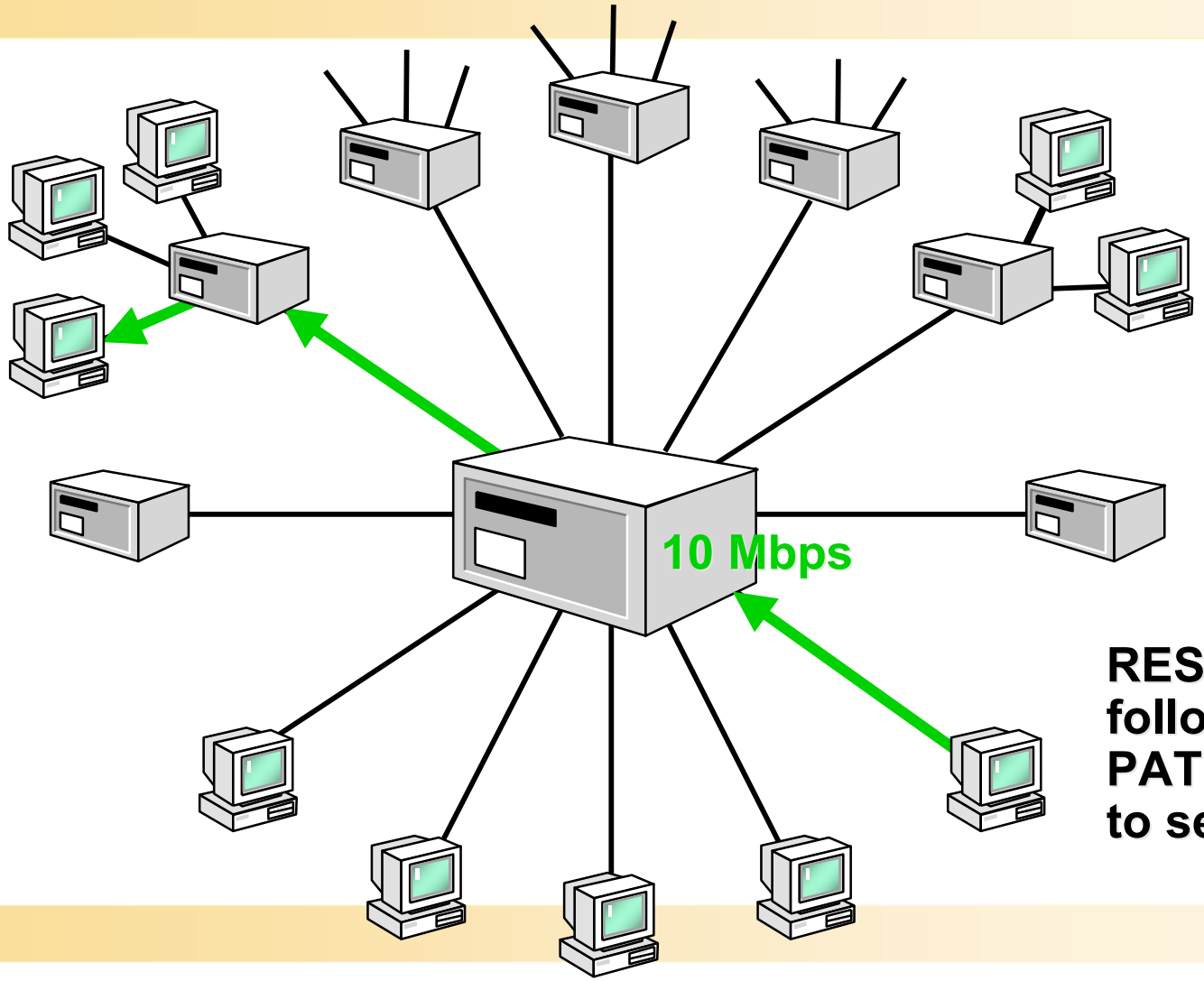


2. Application indicates that it is a Qos receiver

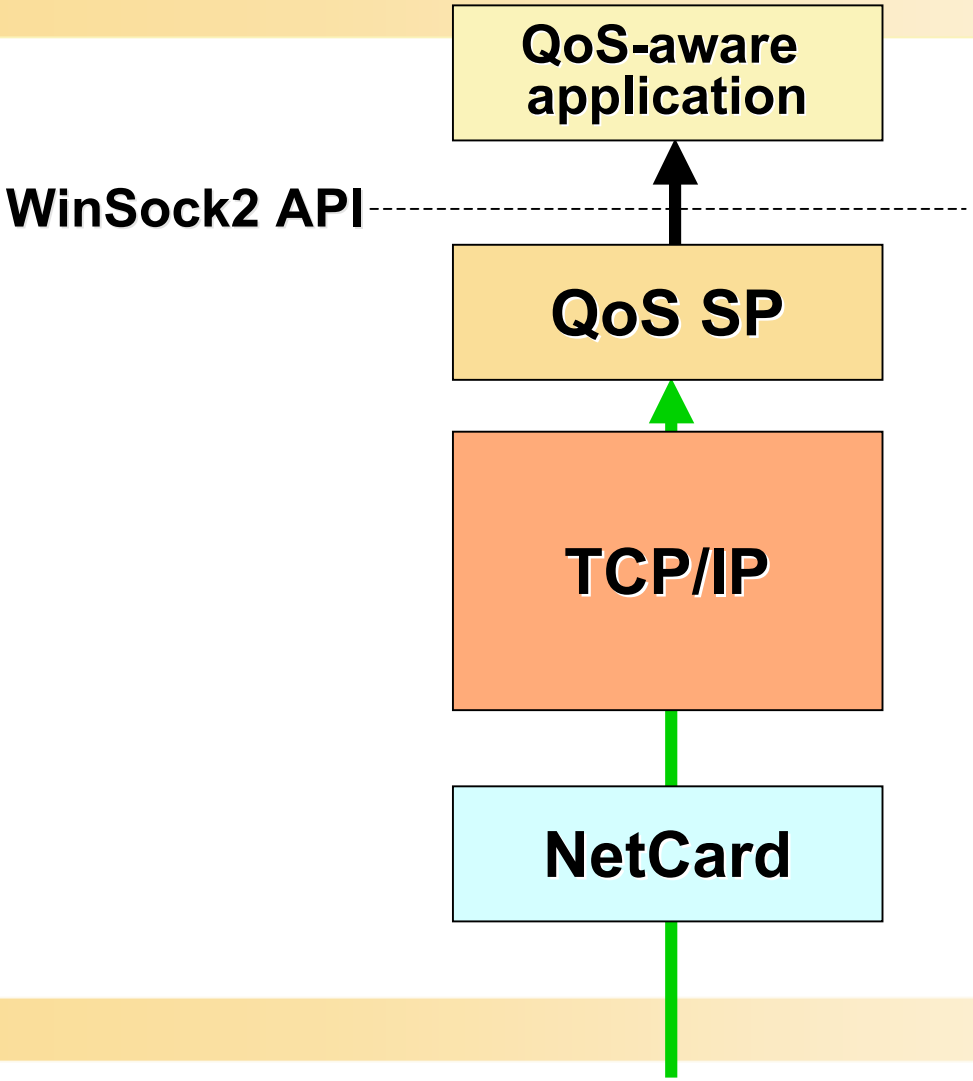
1. PATH message arrives at QoS SP

3. QoS SP sends RSVP RESV message to network

RSVP calls back



App receives QoS notification



2. QoS SP indicates to application that a reservation is in place

1. RESV arrives at sender's QoS SP

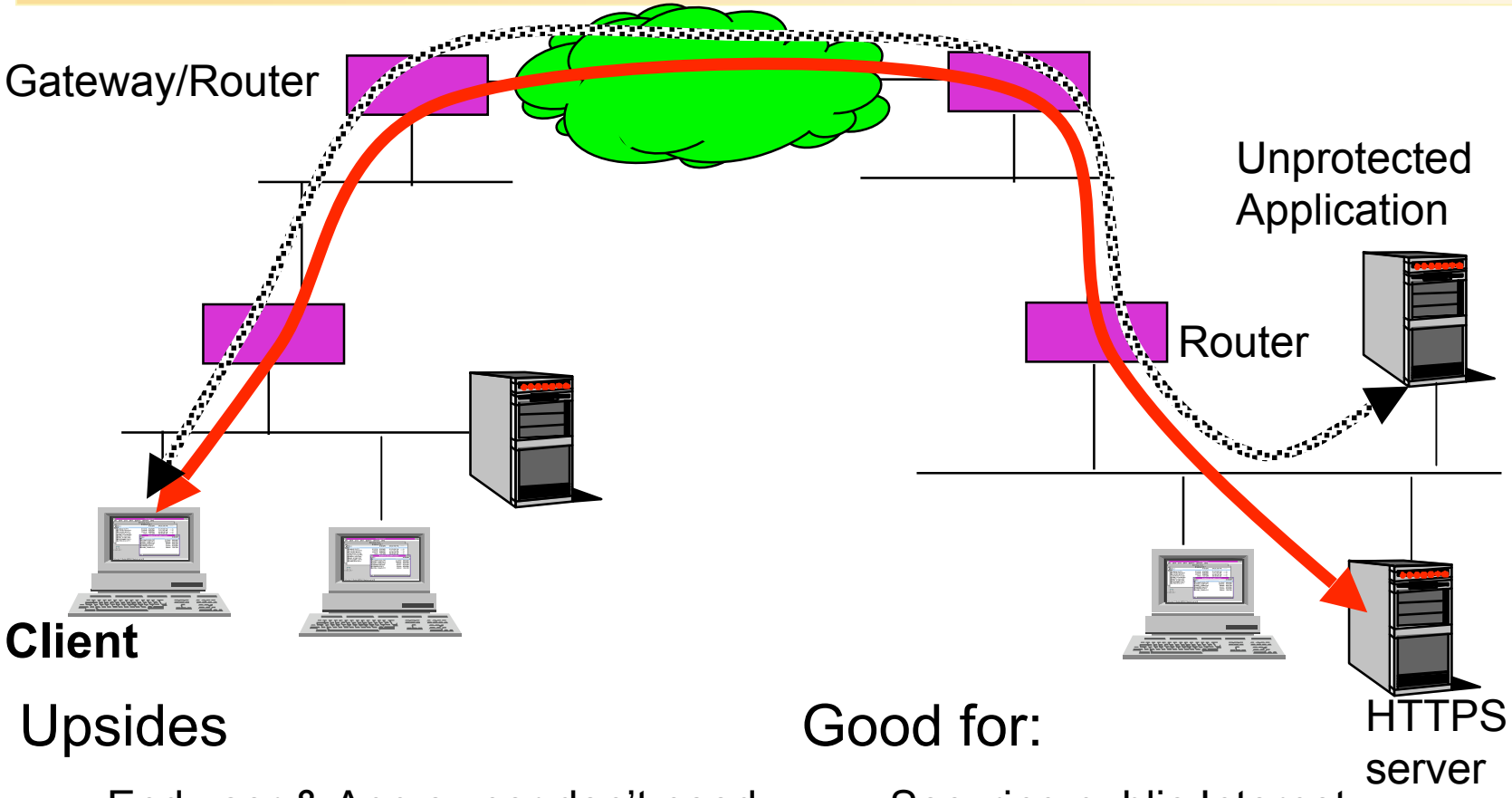
IP Security Protocol (IPSec)

- IETF Standard, RFC2401+
- Provides security for IP packets
  - Authenticity, Integrity, Anti-replay, Privacy (optional)
  - Per-Packet Protection – Filtering Rules
  - Encapsulation (tunneling)
- Usages
  - End-to-end security
  - Virtual Private Network (VPN) connections
    - Gateway-to-Gateway
    - Client to Gateway

Windows 2000 IPSec Strengths

  - Network administrator customized configuration
  - Scalable desktop configuration via Group Policy and Active Directory
  - Customizable, automatic key management
  - Application transparent security
  - Hardware acceleration of encryption
  - 3 trust models, Windows 2000 Kerberos default
  - Support for advanced security scenarios using IPSec tunnel mode
- VPN
  - Integrated with Layer 2 Tunneling Protocol (L2TP) tunneling for alternative to PPTP

TLS/SSL
Requires application support



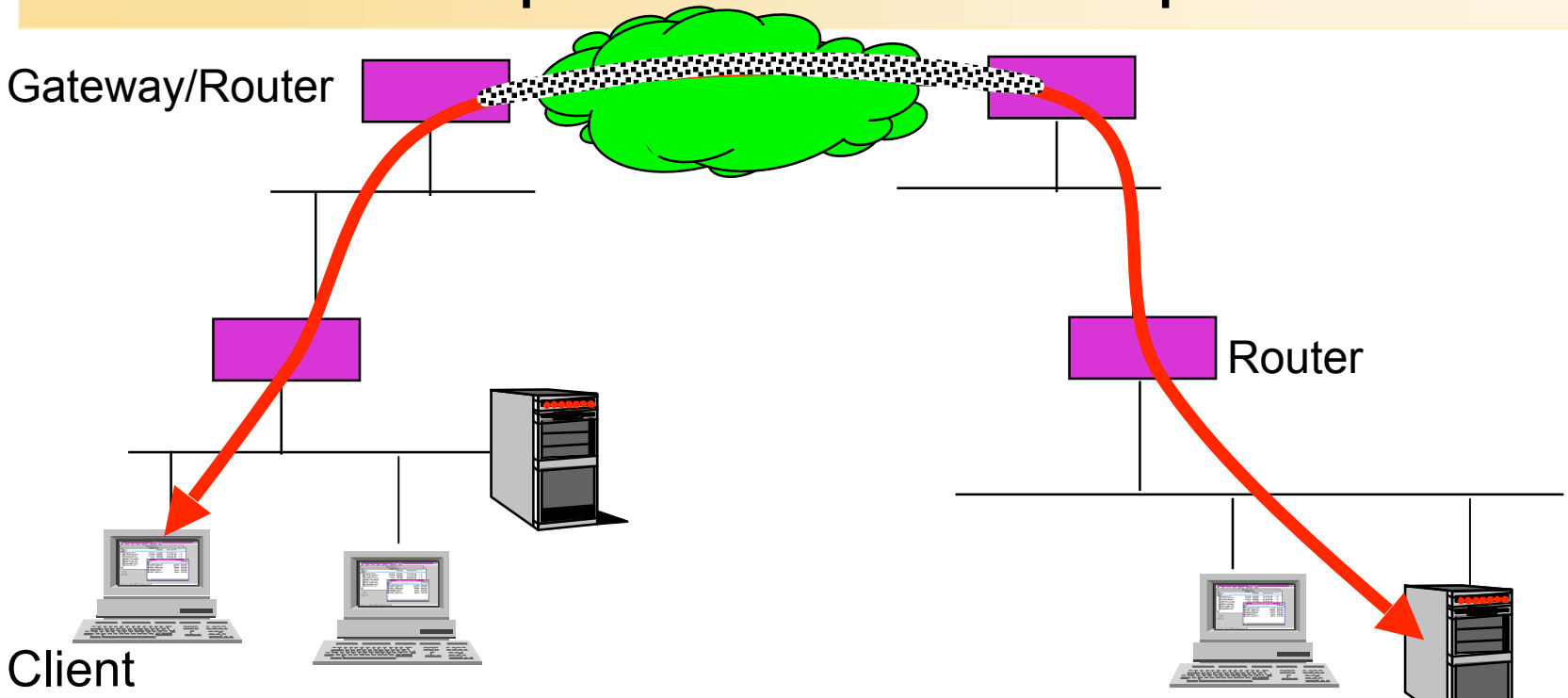
Upsides

- End user & App owner don't need to worry about each other

Good for:

- Securing public Internet applications

Hardware protection
Must protect all links in path



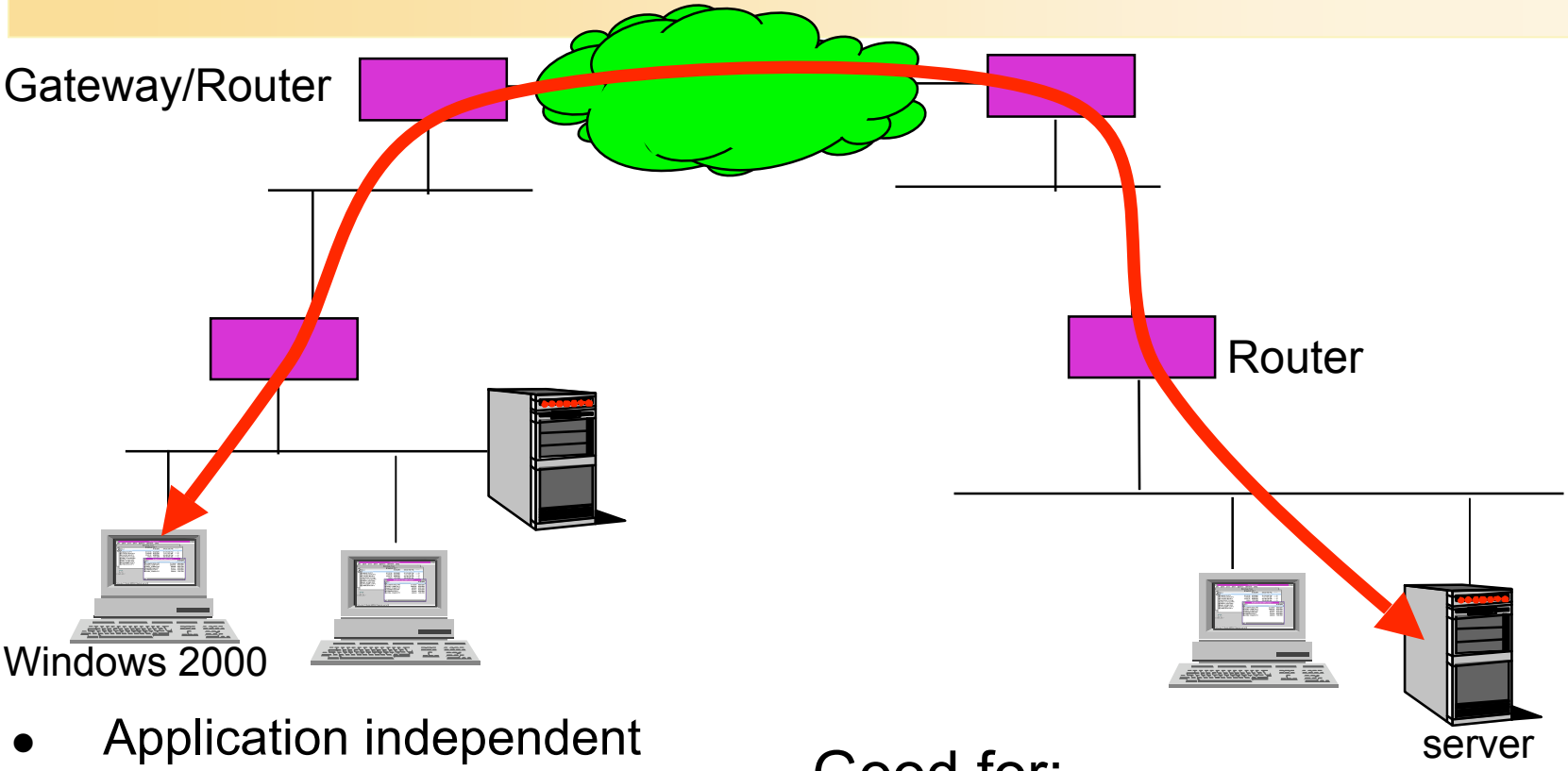
Upsides

- Works for all apps and protocols
- High performance

Good for:

- Managed network service
- Closed network

Ideal Protection: End-to-End

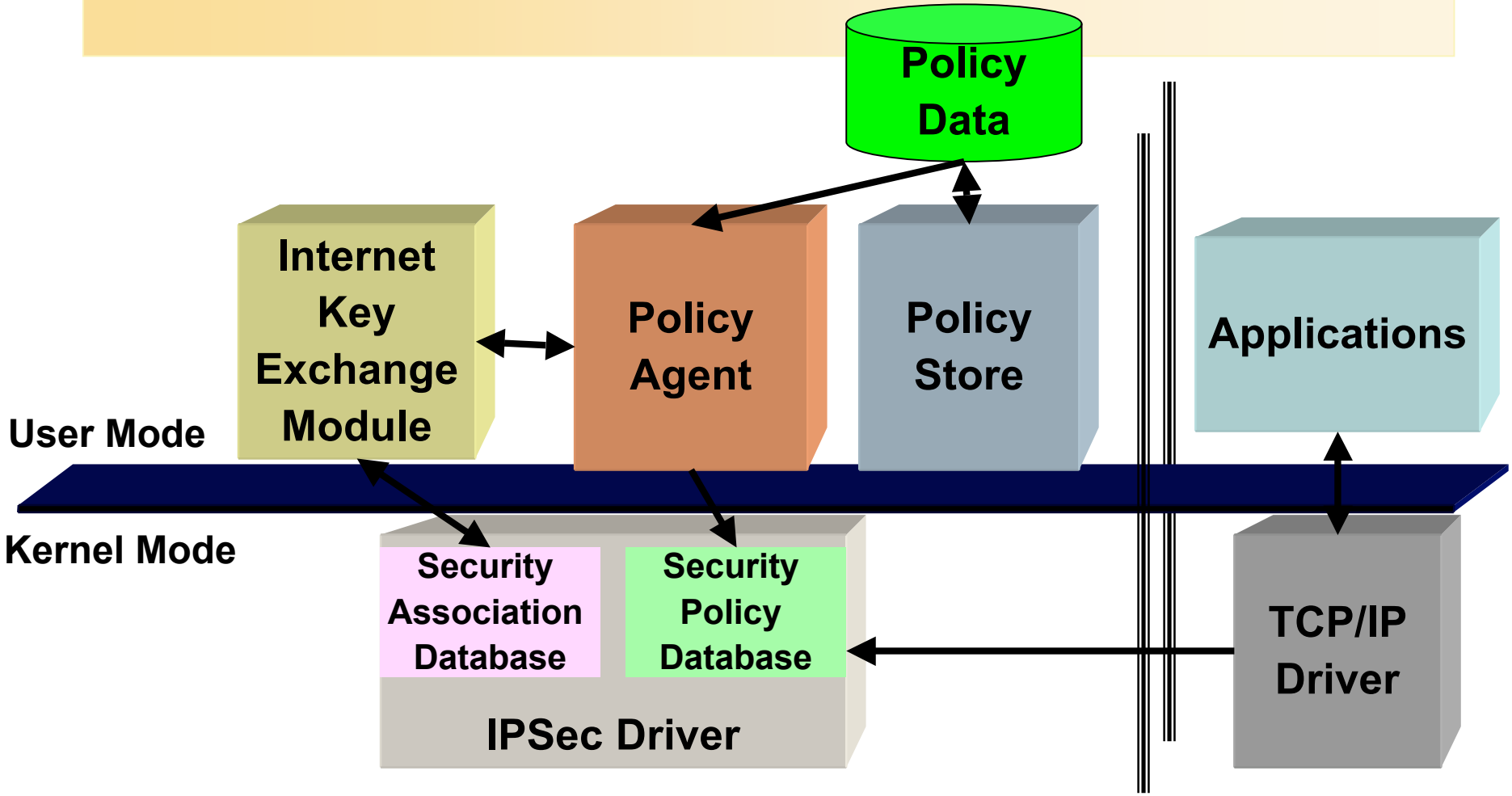


- Application independent
- Multi-protocol (with L2TP)
- Independent of network/device support

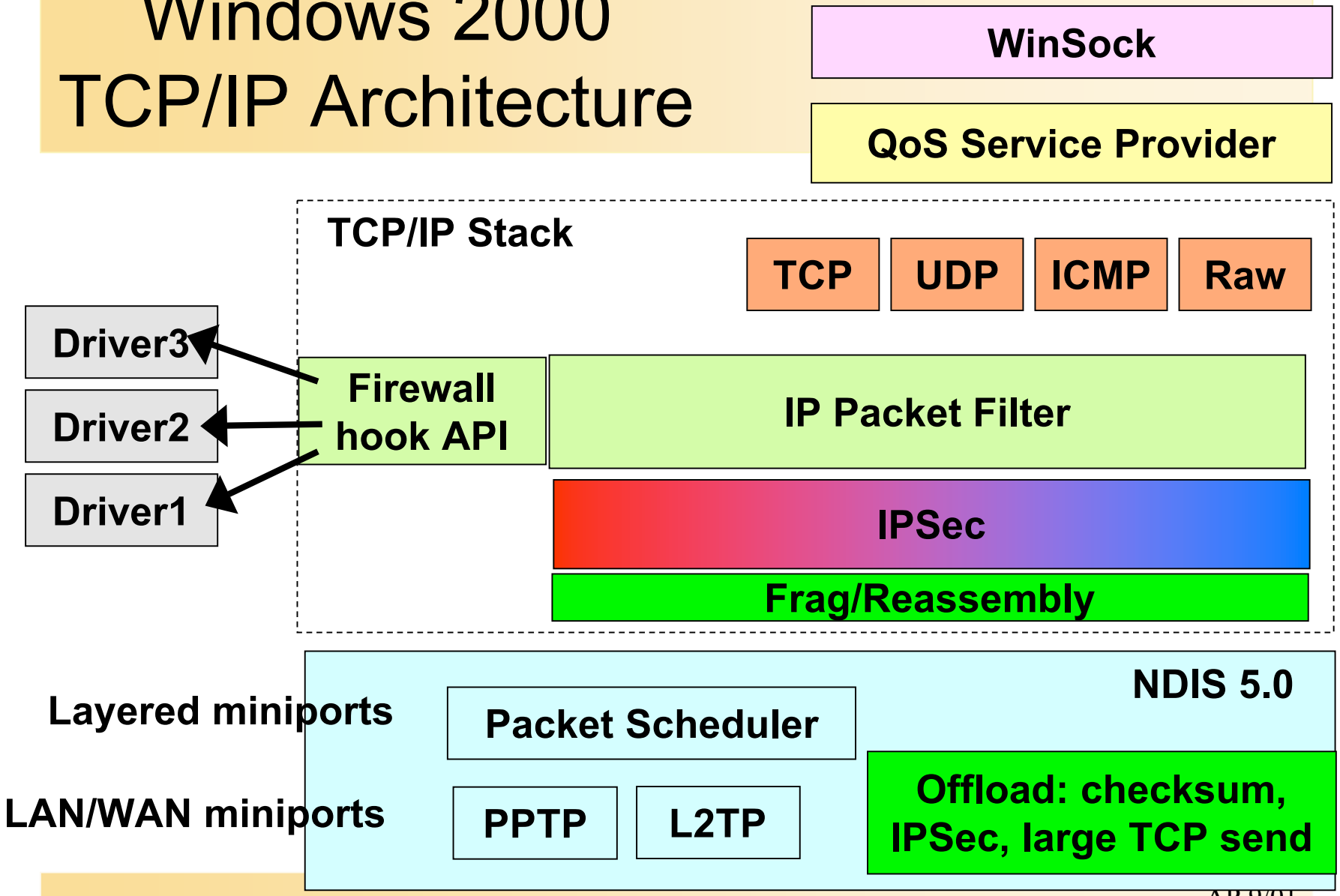
Good for:

- Corporate comms where end-points are managed

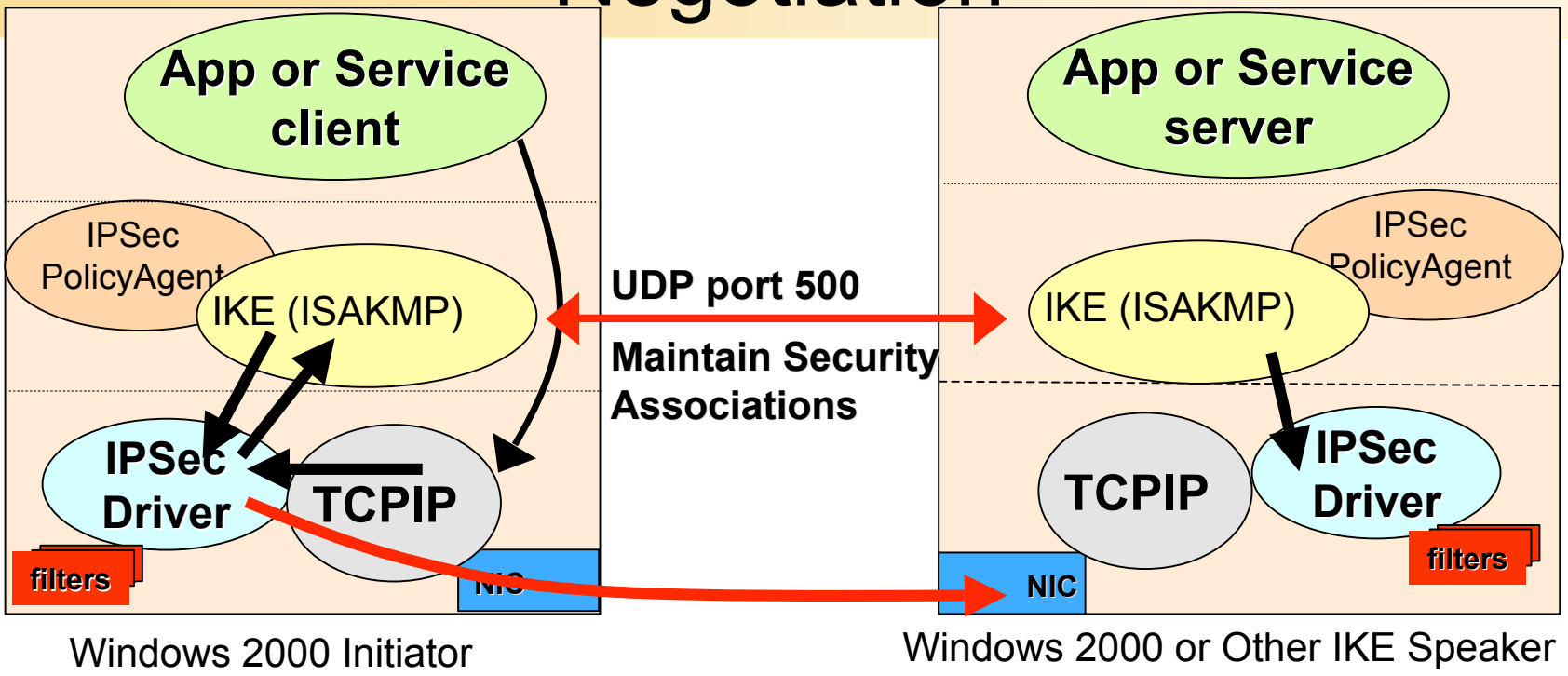
Windows 2000 IPSec Components



Windows 2000 TCP/IP Architecture



IPSec With Internet Key Exchange Negotiation



Windows 2000 Initiator

Windows 2000 or Other IKE Speaker

- IPSec driver compares each outbound IP packet header against filters contained in IPSec policy
- If packet matches a filter, stall packet in queue and call IKE to negotiate Security Association