IP Gateways
IK2218/EP2120

Markus Hidell, mahidell@kth.se
KTH School of ICT

Acknowledgements

- The presentation builds upon material from
  - Previous slides by Markus Hidell, Björn Knutsson and Peter Sjödin
  - *Computer Networking: A Top Down Approach*, 5th ed. Jim Kurose, Keith Ross. Addison-Wesley.
  - *TCP/IP Protocol Suite*, 4th ed, Behrouz Foruzan. McGraw-Hill.

Outline

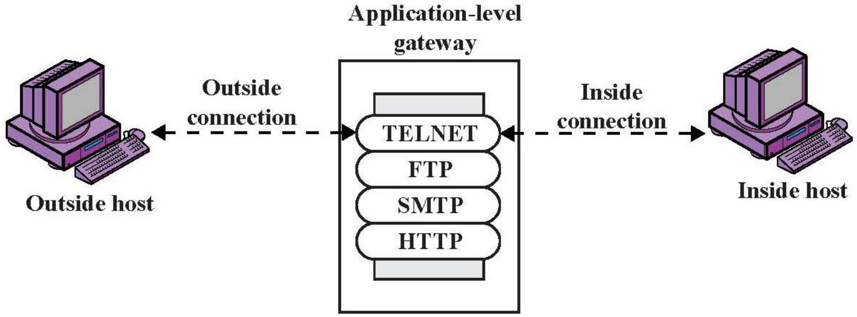
- Brief introduction
- What is a gateway?
- Firewalls
- NAT
- Some other gateways

Introduction

- We now have all the pieces theoretically required to build a network of networks and configure hosts
  - Has (hopefully) been covered in the course by now…
- Unfortunately, we are left with a substantial number of situations that do not fit into this model...
  - What if we don't want unrestricted forwarding of traffic?
  - What if we don't have enough available addresses?
  - What if we are away from our home network?
    - And need resources on our home network that we restrict access to from the outside?

What is a Gateway?

- A machine that sits between two interconnected networks and relays traffic between them
- **Assumption:** *Traffic cannot flow between the two networks without the assistance of the gateway*
- **Conclusion:** A ***router*** is a *network layer* gateway
  - But we can have other types of gateways, both at the network layer and elsewhere



Purposes with a Gateway

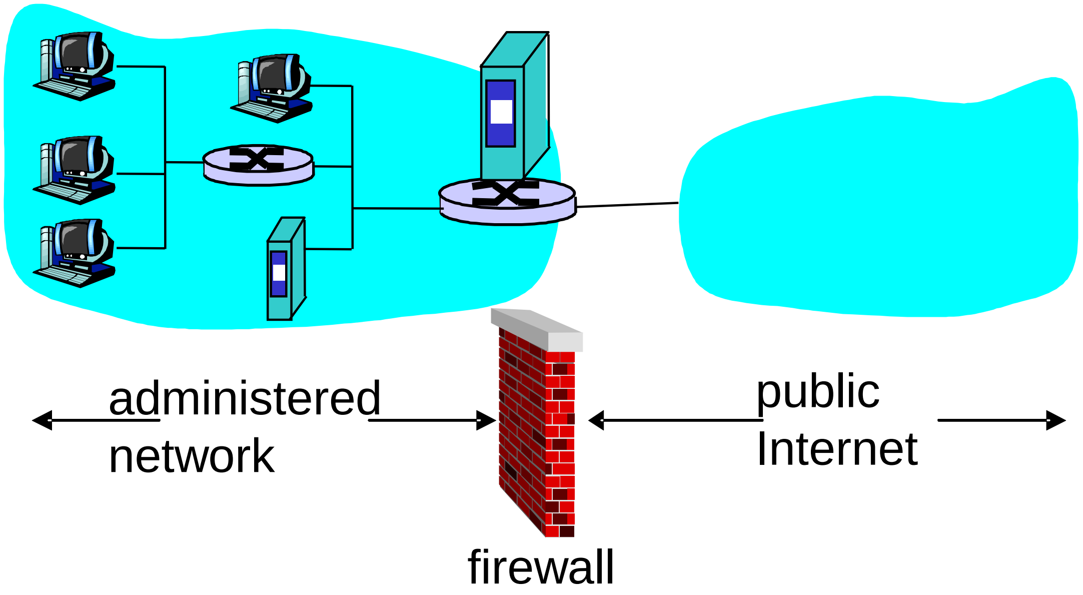
- What can we use other types of gateways for?
  - Connecting networks with incompatible address systems
    - IPv4 and IPv6
    - Two IPv4 networks with independent address domains
  - Restricting what traffic flows between two networks
    - Protective purposes
  - Redirecting traffic, possibly tunneling it
    - Mobility, VPNs, IPsec tunnels etc

NAT

Firewall

Firewalls

Firewall Definition



Isolates organization’s internal network from larger Internet, allowing some packets to pass and blocking others

Castle and Moat Analogy

- Maybe more like the moat around a castle than a firewall
  - Restricts access from the outside
  - Restricts outbound connections, too (!!)
    - Important: filter out undesirable activity from internal hosts!

Firewall—Design Goals

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.
3. The firewall itself is immune to penetration.

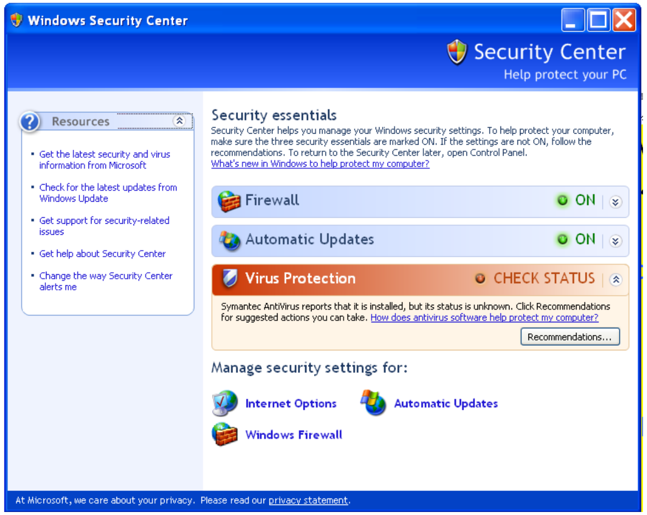
Bellovin, S., Cheswick, W. ”Network Firewalls.”
IEEE Communications Magazine, September 1994.

Firewalls—General Techniques

- Service control
  - Determines the types of Internet services that can be accessed, inbound or outbound
    - Packet filtering, proxy software, hosting server software
- Direction control
  - Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall
- User control
  - Controls access to a service
- Behavior control
  - Controls how particular services are used
    - E.g., filter email to eliminate spam

Firewall Locations in the Network

- Between internal LAN and external network
- At the gateways of sensitive subnetworks within the organizational LAN
  - Payroll’s network must be protected separately within the corporate network
- On end-user machines
  - “Personal firewall”
  - Microsoft’s Internet Connection Firewall (ICF) comes standard with Windows XP



- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?

Firewall ● ON

Automatic Updates ● ON

Virus Protection ● CHECK STATUS

Symantec AntiVirus reports that it is installed, but its status is unknown. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

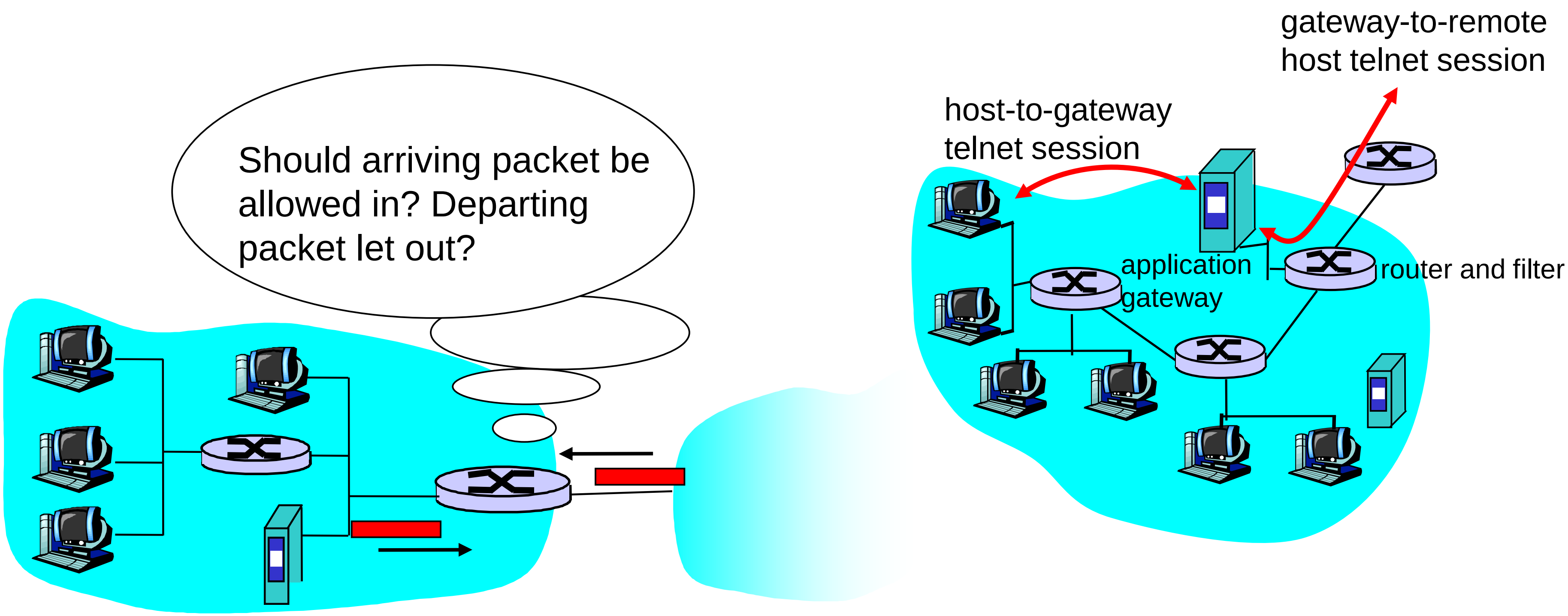
Manage security settings for:

At Microsoft, we care about your privacy. Please read our privacy statement.

Firewall Types

Packet filter:
internal network connected to Internet via *router firewall*

Application level gateway:
splices and relays two application-specific connections



Should arriving packet be allowed in? Departing packet let out?

gateway-to-remote host telnet session

host-to-gateway telnet session

application gateway

router and filter

Packet Filters

- For each packet, firewall decides whether to allow it to proceed
  - Decision must be made on per-packet basis
- To decide, use information available in the packet
  - IP source and destination addresses, ports
  - Protocol identifier (TCP, UDP, ICMP, etc.)
  - TCP flags (SYN, ACK, RST, PSH, FIN)
  - ICMP message type
- Filtering rules are based on pattern-matching
  - Deep packet inspection

Packet Filter Default Policies

Two default policies:

- Default = discard
  - That which is not expressly permitted is prohibited
- Default = forward
  - That which is not expressly prohibited is permitted

- Default = discard is more conservative
  - Services added on a case-by-case basis
  - Very visible to users....

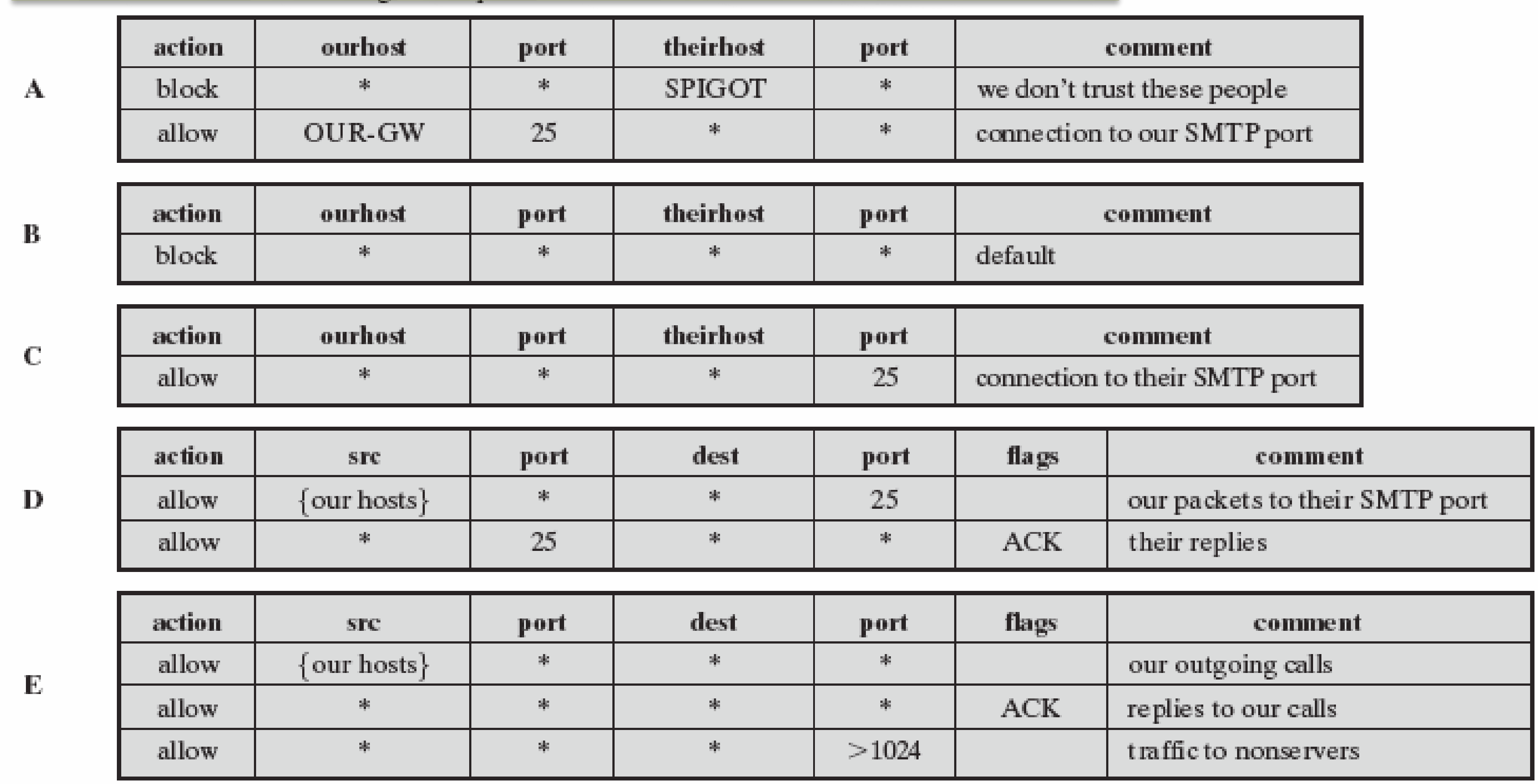
Packet Filtering—Examples

- Example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
  - All incoming and outgoing UDP flows carrying telnet connections are blocked.
- Example 2: Block inbound TCP segments with ACK=0.
  - Prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

TCP has a flag, called ACK, that is set on all but the first packet, the one that establishes the connection. So, if the firewall disallows packets from B without ACK set in the TCP header,
then we will have the desired effect, in general.

Packet Filters—Rule Sets

Rule sets here not formal—only for purpose of illustration



A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

In each rule set, rules are applied top to bottom. "*" is a wildcard matching everything.

Examples A-E, cont'd

A. Inbound mail allowed (port 25 is for SMTP incoming), but only to OUR-GW. Mail from SPIGOT is blocked.

B. Explicit statement of the default policy. All rule sets include this rule implicitly as the last rule.

C. Intended to specify that any inside host can send mail to the outside. TCP packets go to SMTP server on destination machine.

   - Problem: Outside machine could be configured to have some other application linked to port 25. An attacker could gain access to internal machines by sending packets with TCP src port = 25.

Examples A-E, cont’d

D. Achieves the intended result that was not achieved in ”C”. Once a connection is set up, ACK = 1 in TCP segment. Allow replies from outside, but not connection initiation. Furthermore, allow IP packets from ”our hosts” (list of designated internal hosts) and the destination TCP port 25.

E. An approach to handling FTP connections. FTP uses two TCP connections: one for control and one for data transfer. Most attacks target well-known ports (<1024). Rule set allows:

- Packets that originated internally
- Reply packets to a connection initiated by internal machine
- Packets destined for high-numbered ports on internal machines

Weaknesses of Packet Filters

- Do not prevent application-specific attacks
  - For example, if there is a buffer overflow in URL decoding routine, firewall will not block an attack string
- No user authentication mechanisms
  - … except (spoofable) address-based authentication
  - Firewalls don’t have any upper-level functionality
- Vulnerable to TCP/IP attacks such as spoofing
  - Attacker sends packets with IP src address belonging to the internal network
- Security breaches due to misconfiguration

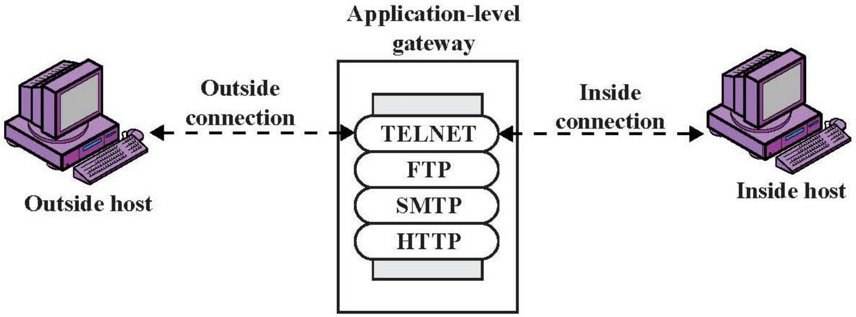
PF: Attacks and Countermeasures

- IP address spoofing
  - Attacker sends packet with internal src address
  - Countermeasure: discard packets with inside source address arriving on an external interface
- Source routing attacks
  - Use source routing to try to bypass security measures
  - Countermeasure: discard all packets with this IP option
- Tiny fragment attacks
  - Intruder uses IP fragmentation to create very small fragments to circumvent filtering on TCP header information
  - Countermeasure: Discard packets based on protocol type and IP fragment offset

Stateful Packet Filters

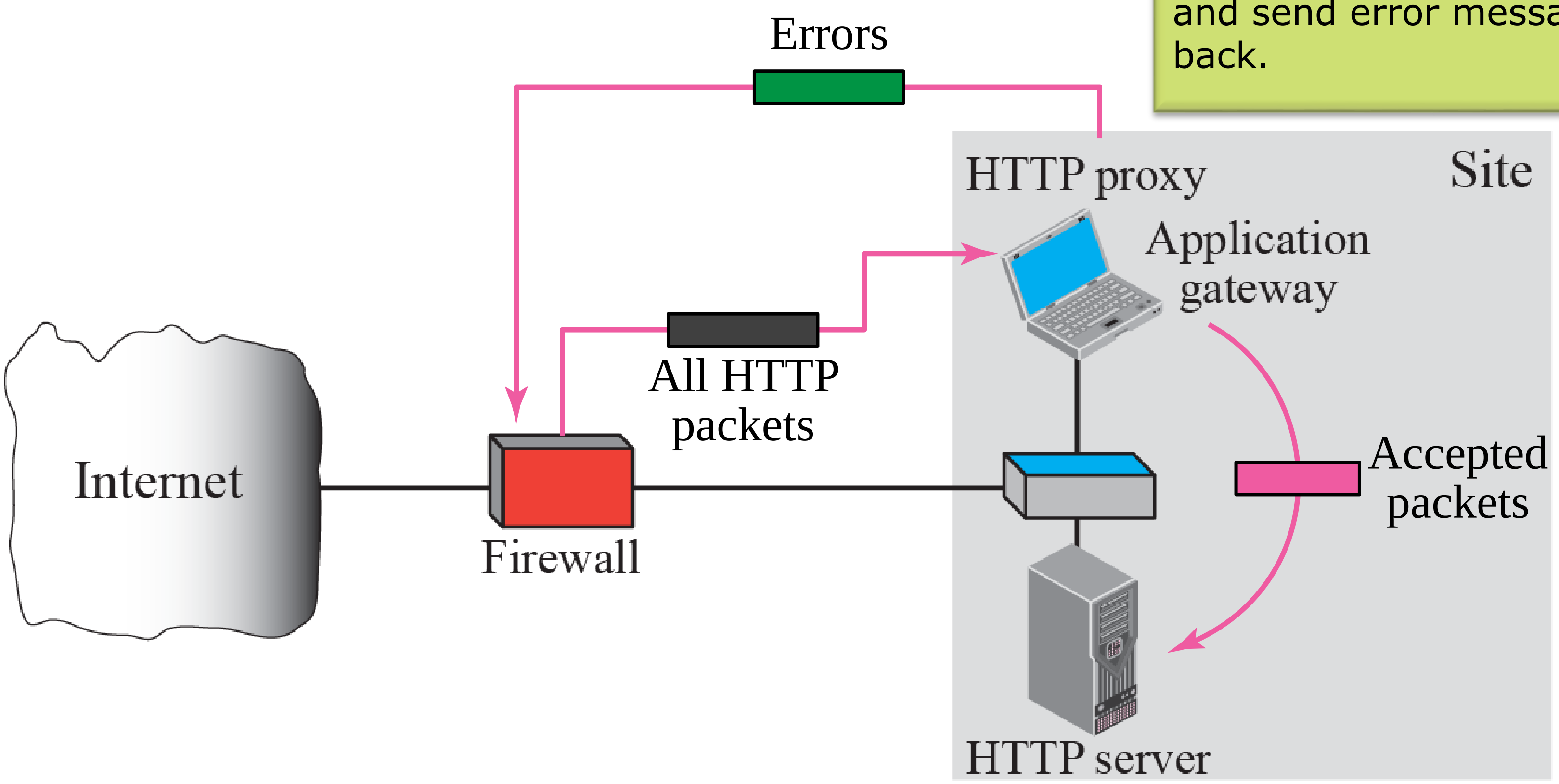
- There are protocols that require B to make a TCP connection to A, even though A initiated the session
  - FTP (control connection and data connection)
- Stateful packet filter
  - Note that connection was initiated from *s* (internal) to *d*
  - Allow (for some period of time) connections from *d* to *s*

Application-Level Gateway



- Splices and relays two application-specific connections
  - Common example: HTTP gateway (proxy server)
- Can support high-level user-to-gateway authentication
  - Log into the proxy server with your name and password
- Simpler filtering rules than for arbitrary TCP/IP traffic
- Each application requires implementing its own proxy
  - Proxy might be a performance bottleneck

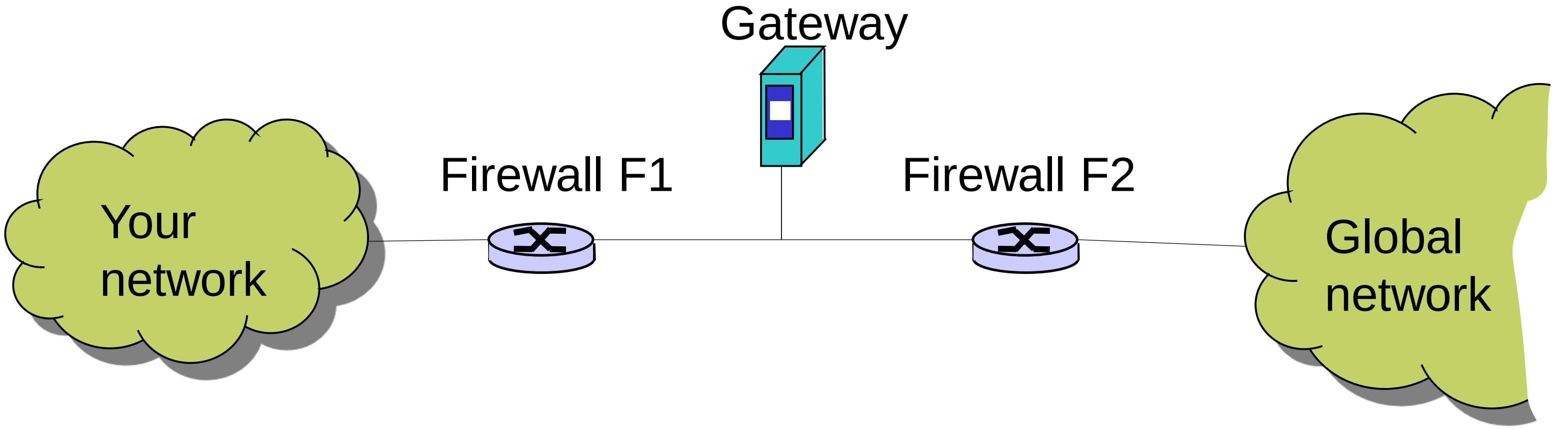
Proxy Firewall (same thing as application-level gateway)



If packet is legitimate, act as client and send packet to server. If not legitimate, drop and send error message back.

©The McGraw-Hill Companies, Inc., 2000

Bastion Host



- Bastion host: gw placed behind firewall router(s)
  - Trusted system (secure version of its operating system)
  - Firewalls refuse to forward anything unless to/from the application-level gateway
  - All non-essential services are turned off
  - Application-specific proxies for supported services
    - E.g., Telnet, DNS, FTP, SMT
    - Reduced S/W complexity, no disk access (apart from reading conf)
  - Support for user authentication

Some Comparisons

- Packet filter can do its job without requiring software changes in the communicating nodes
  - Allowed conversations proceed normally (in most cases)
- An application level gateway is visible to the users
  - Need to connect to the gateway
- Application level gateway can be more powerful than packet filters—e.g., look at data inside email messages
  - Gateway is application-aware

General Problems with Firewalls

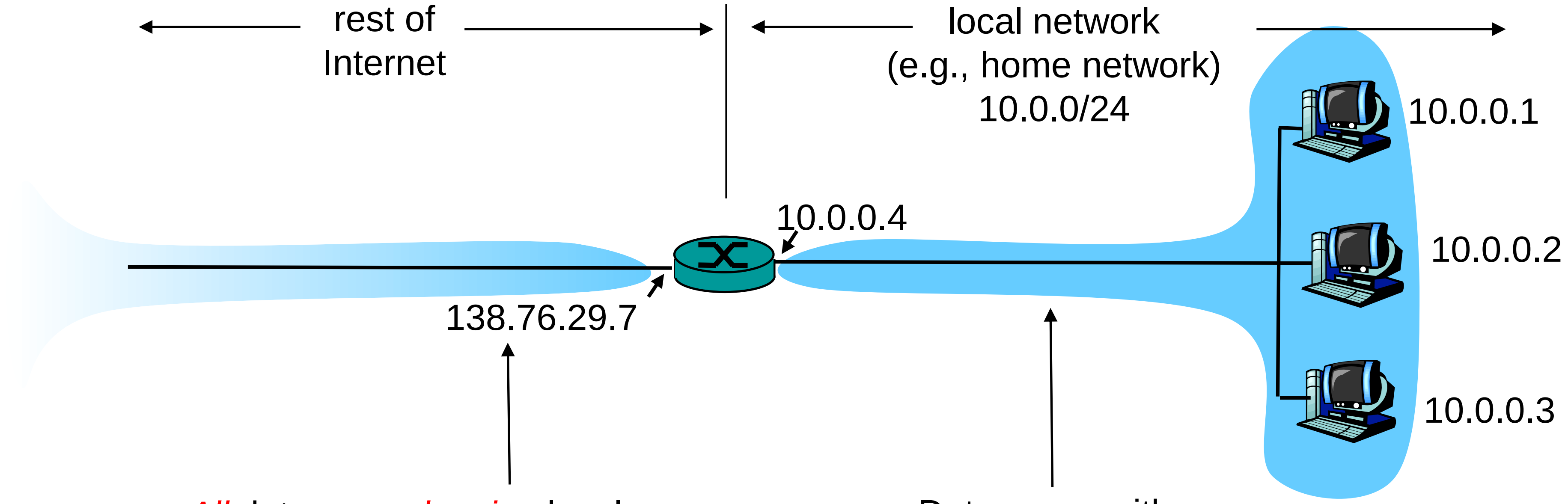
- Interfere with networked applications
  - Can make it difficult for legitimate user to get the work done
- Many problems not solved with firewalls
  - Buggy software (like buffer overflow exploits)
  - Firewall friendly protocols
    - Run IP over HTTP.....
- Don’t prevent insider attacks
- Increasing complexity and potential for misconfiguration

ROYAL INSTITUTE OF TECHNOLOGY

NAT Gateways

NAT—Network Address Translation

What if we have many computers, but only a single public IP address?
Use private addresses on LAN, let gateway translate



All datagrams *leaving* local network have same single source NAT IP address: 138.76.29.7, different source port numbers

Datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

NAT—Motivation

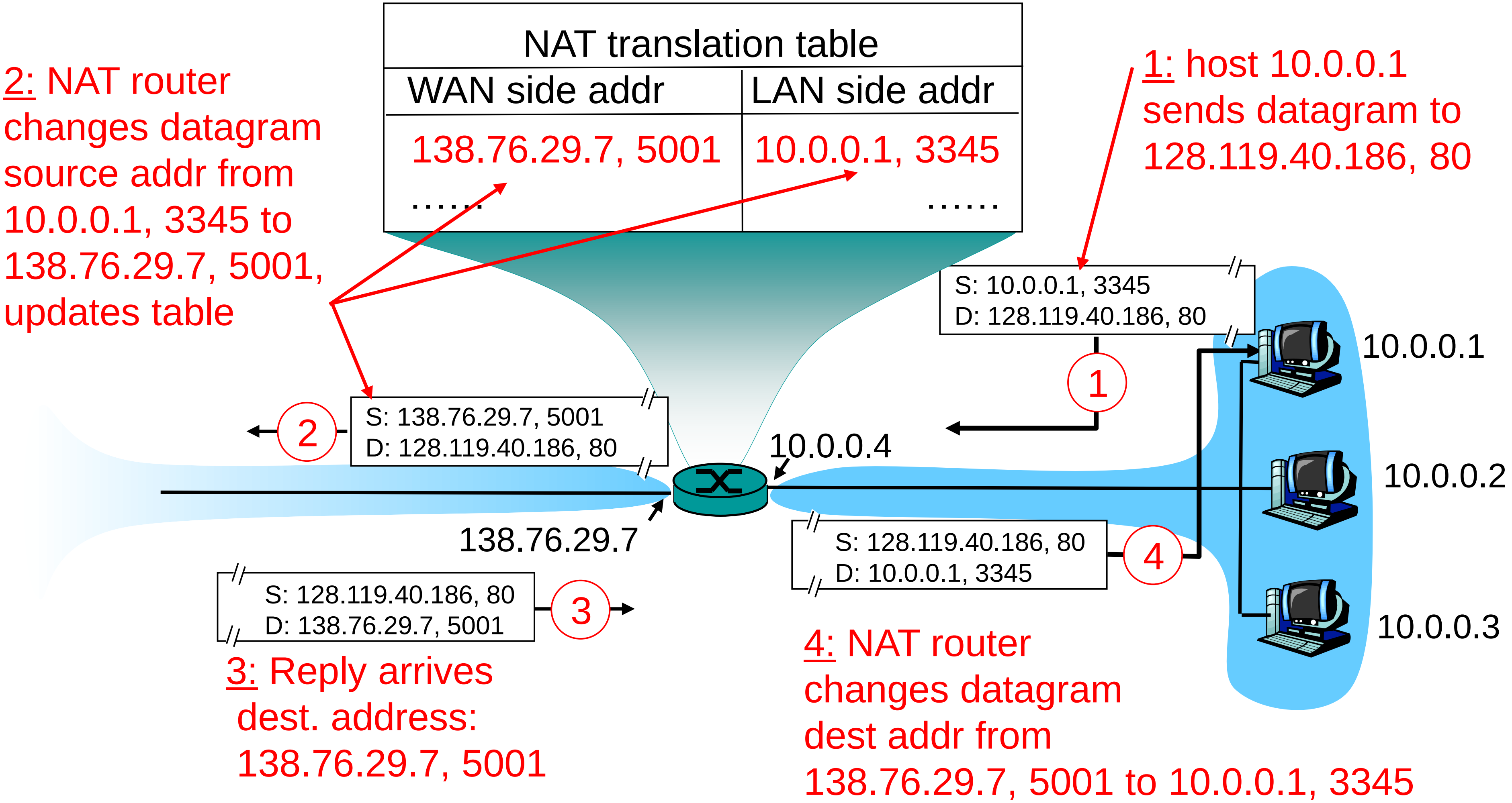
- Local network uses just one IP address as far as outside world is concerned:
  - range of addresses not needed from ISP: just one IP address for all devices
  - can change addresses of devices in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - devices inside local net not explicitly addressable, visible by outside world (a security plus).

NAT—Implementation

NAT router must:

- for outgoing datagrams: replace (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
- . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr.
- remember (in NAT translation table) every (source IP address, port #) to (NAT IP address, new port #) translation pair
- for incoming datagrams: replace (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

NAT—Operation



NAT translation table

WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
……	……

1: host 10.0.0.1 sends datagram to 128.119.40.186, 80

2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

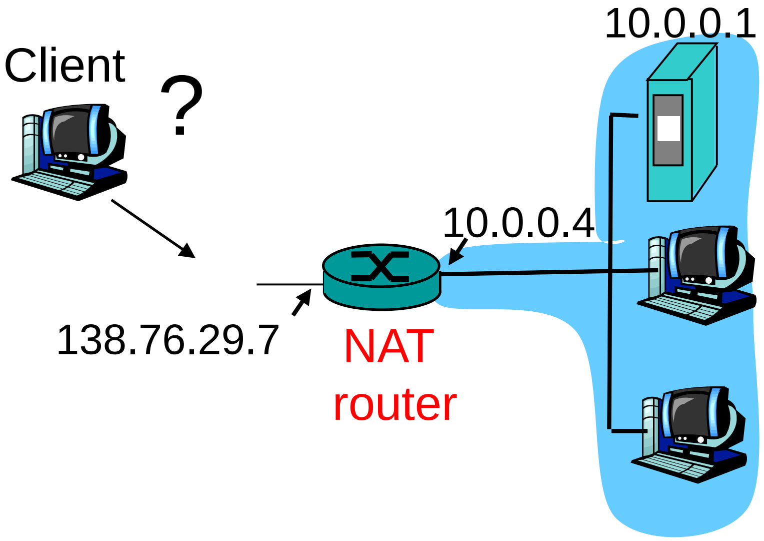
3: Reply arrives dest. address: 138.76.29.7, 5001

4: NAT router changes datagram dest addr from 138.76.29.7, 5001 to 10.0.0.1, 3345

NAT Issues and Concerns

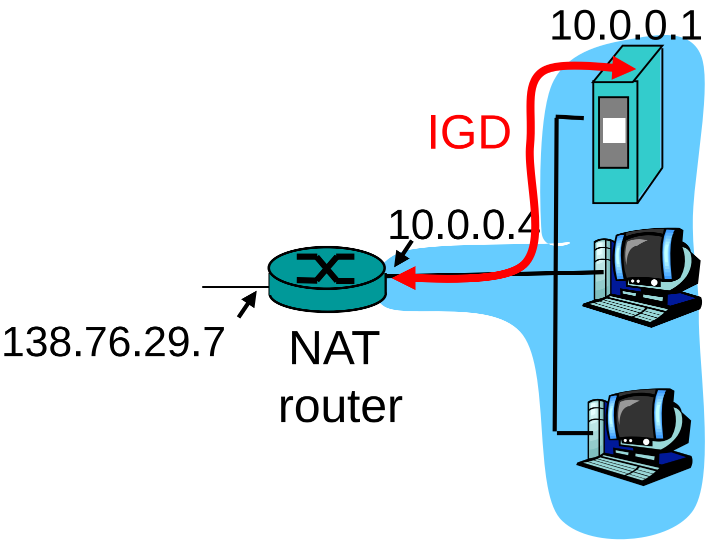
- 16-bit port-number field:
  - 60,000 simultaneous connections with a single LAN-side address!
- NAT is controversial:
  - routers should only process up to layer 3
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, e.g., P2P applications
  - address shortage should instead be solved by IPv6

NAT Traversal Problem



- Client wants to connect to server with address 10.0.0.1
  - server address 10.0.0.1 local to LAN (client can’t use it as destination addr)
  - only one externally visible NATed address: 138.76.29.7
- Solution 1: statically configure NAT to forward incoming connection requests at given port to server
  - e.g., (123.76.29.7, port 2500) always forwarded to 10.0.0.1 port 2500

NAT Traversal Problem, cont’d

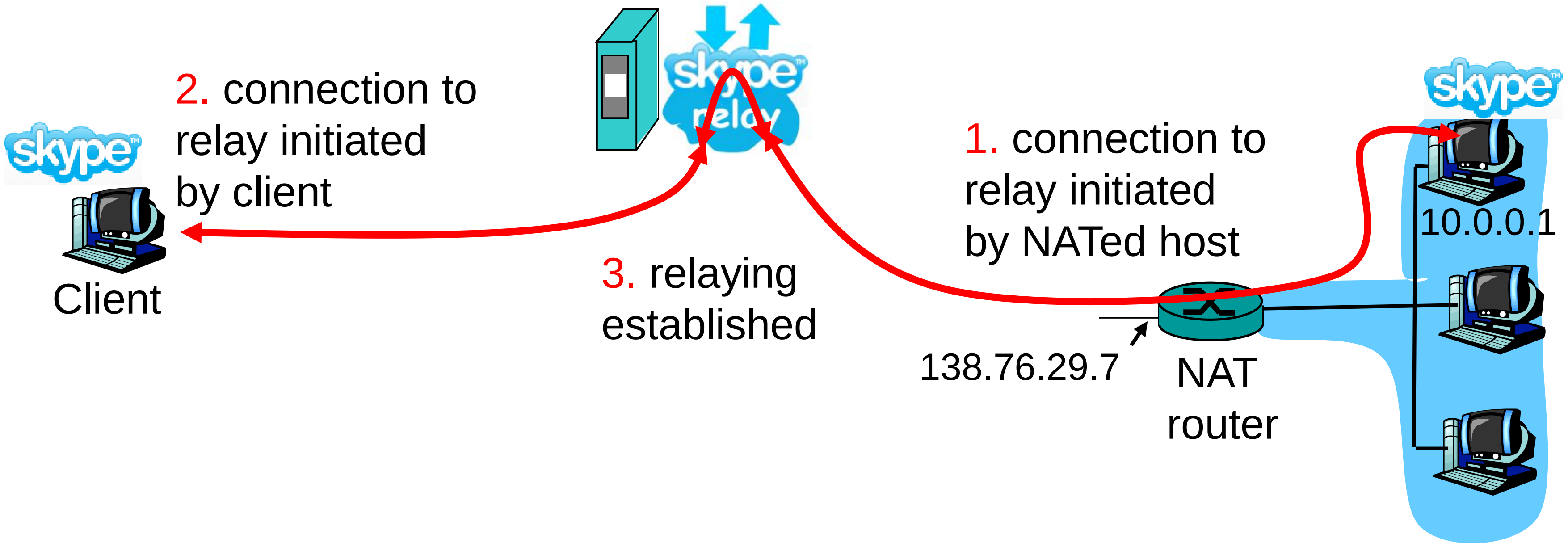


- Solution 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATed host to:
  - learn public IP address (138.76.29.7)
  - add/remove port mappings (with lease times)

That is, we have *automated* static NAT port map configuration

NAT Traversal Problem, cont'd

- External client wants to connect to NATed client
- Solution 3: relaying (used in Skype)
  - NATed client establishes connection to relay
  - External client connects to relay
  - Relay node bridges packets between to connections

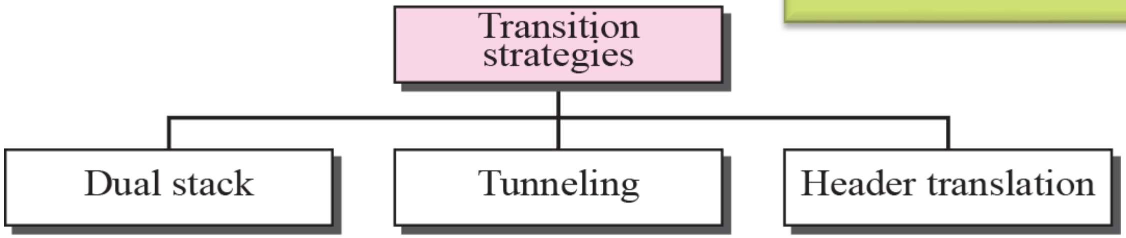


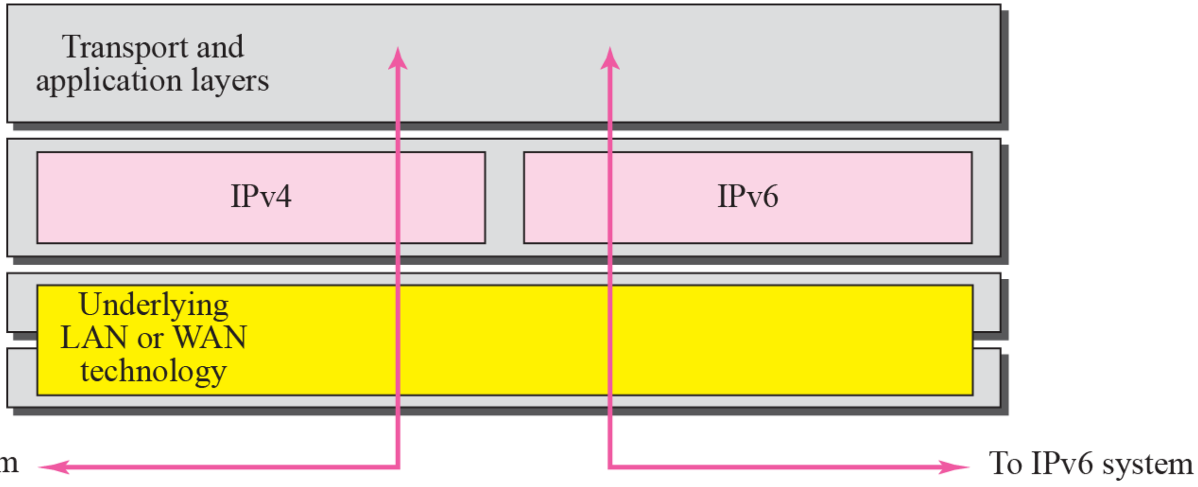
skype relay
skype
Client
2. connection to relay initiated by client
3. relaying established
1. connection to relay initiated by NATed host
skype
10.0.0.1
138.76.29.7
NAT router

Some Other Gateways

IPv4/IPv6 Gateways

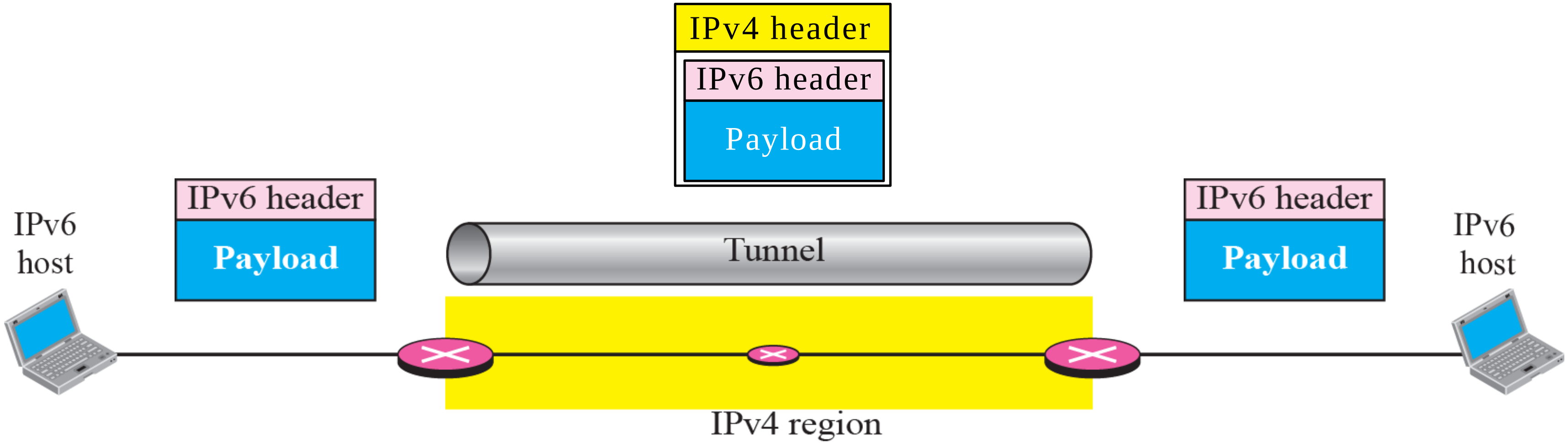
IPv4 to IPv6 transition is based on dual-stacks, tunneling, and header translation....




Transport and application layers
IPv4
IPv6
Underlying LAN or WAN technology
To IPv4 system
To IPv6 system

IPv4/IPv6 Gateways, cont'd

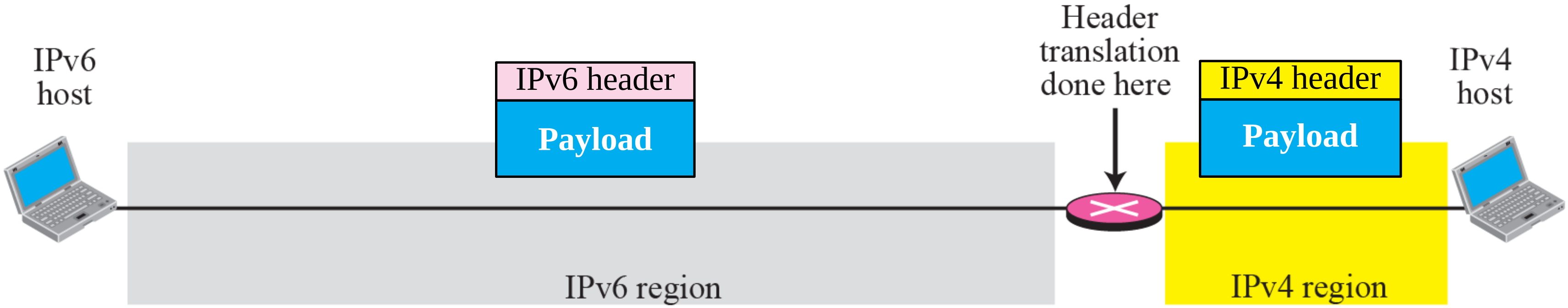
Tunneling IPv6 in IPv4:
We use gateways to do the job...



©The McGraw-Hill Companies, Inc., 2000

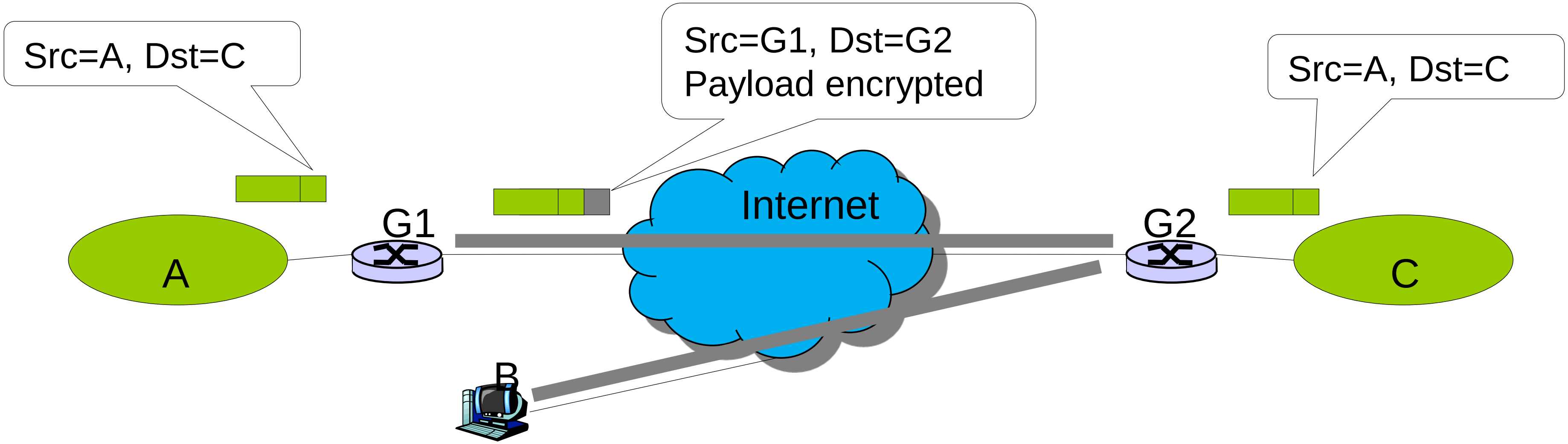
IPv4/IPv6 Gateways, cont’d

Header translation IPv6/IPv4:
We use gateways to do the job…



©The McGraw-Hill Companies, Inc., 2000

IPsec Gateways—Encrypted Tunnels



Let’s revisit tunneling and VPN:

- VPN based on encrypted IPsec tunnels
- Internet treated like an insecure wire
- Gateways do the job
  - Computers in corporate networks ”unaware” of tunnel
  - Computer attached from outside needs a tunnel endpoint

Summary

IP gateways are used in many situations

- Firewalls
  - Packet filter
  - Application-level gateways (proxy firewalls)
- NAT
- IPv4 to IPv6 transitions
- IPsec VPNs

ROYAL INSTITUTE
OF TECHNOLOGY

Thanks for listening