Chapter 5

Designing Internet Systems and Servers

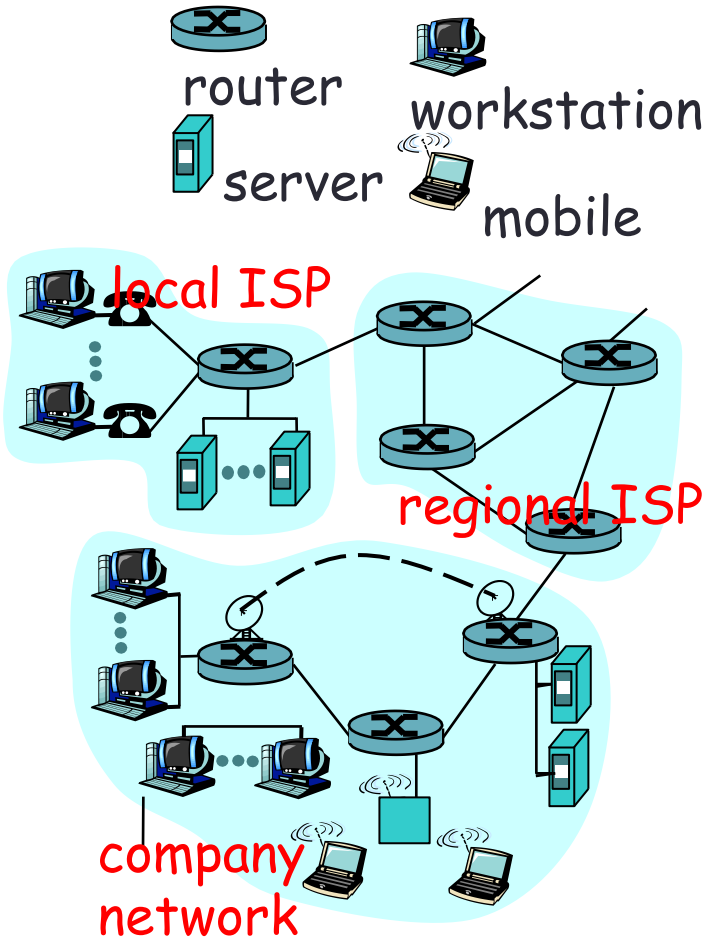
By Pavan Poudel

Overview

1. Designing of Internet System Network Architecture
2. Choice of platforms
3. Server Concepts: Web, Proxy, RADIUS, Mail
4. Cookies
5. Load Balancing: Proxy Arrays
6. Server Setup and Configuration Guidelines
7. Security and System Administration Issues, Firewalls and Content Filtering

What's the Internet: "nuts and bolts" view

- Millions of connected computing devices: *hosts, end-systems*
  - PCs, servers
  - PDAs, phones, etc. running *network apps*
- *Communication links*
  - Fiber, cable, radio, satellite
  - Residential access: modem, DSL, cable modem, satellite
  - Transmission rate = ***bandwidth***
- *Routers:* forward packets (chunks of data)



When those architectural techniques are used in the field of internet networking technology, it is referred as internet network architecture

Designing of Internet System Network Architecture

- Network design and architecture is of critical importance.
  - contributes directly to the success of the network
  - contributes directly to the failure of the network
- ***What is a well designed network?***
  - A network that takes into consideration of these important factors:
    - Physical infrastructure
    - Topological/protocol hierarchy
    - Scaling and Redundancy
    - Addressing aggregation (IGP and BGP)
    - Policy implementation (core/edge)
    - Management/maintenance/operations
    - Cost

Designing of Internet System Network Architecture

- **The Three-legged stool:**
  - Designing the network with resiliency in mind
  - Using technology to identify and eliminate single of failure
  - Having processes in place to reduce the risk of human error

Design

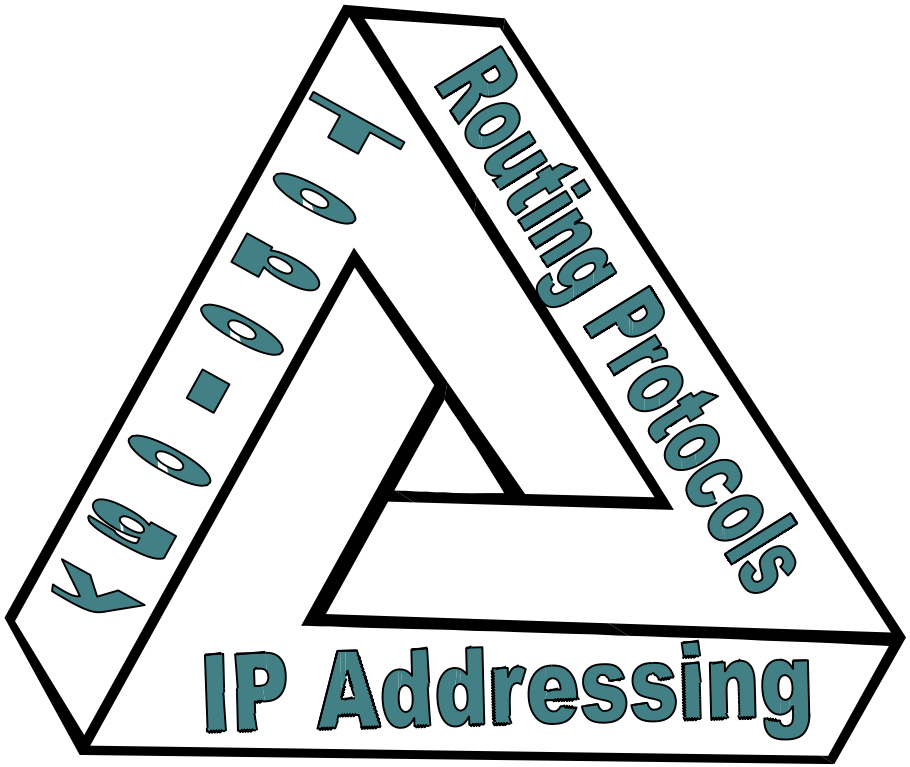
Technology

- All of these elements are necessary and all int ct with each other.
  - One missing leg results in a stool which will not stand.

Process

Designing of Internet System Network Architecture

- **Redundant Network Design:** (Concepts and Techniques)
  - Basic ISP Scaling Concepts:
    - Modular/Structured Design
    - Functional Design
    - Tiered/Hierarchical



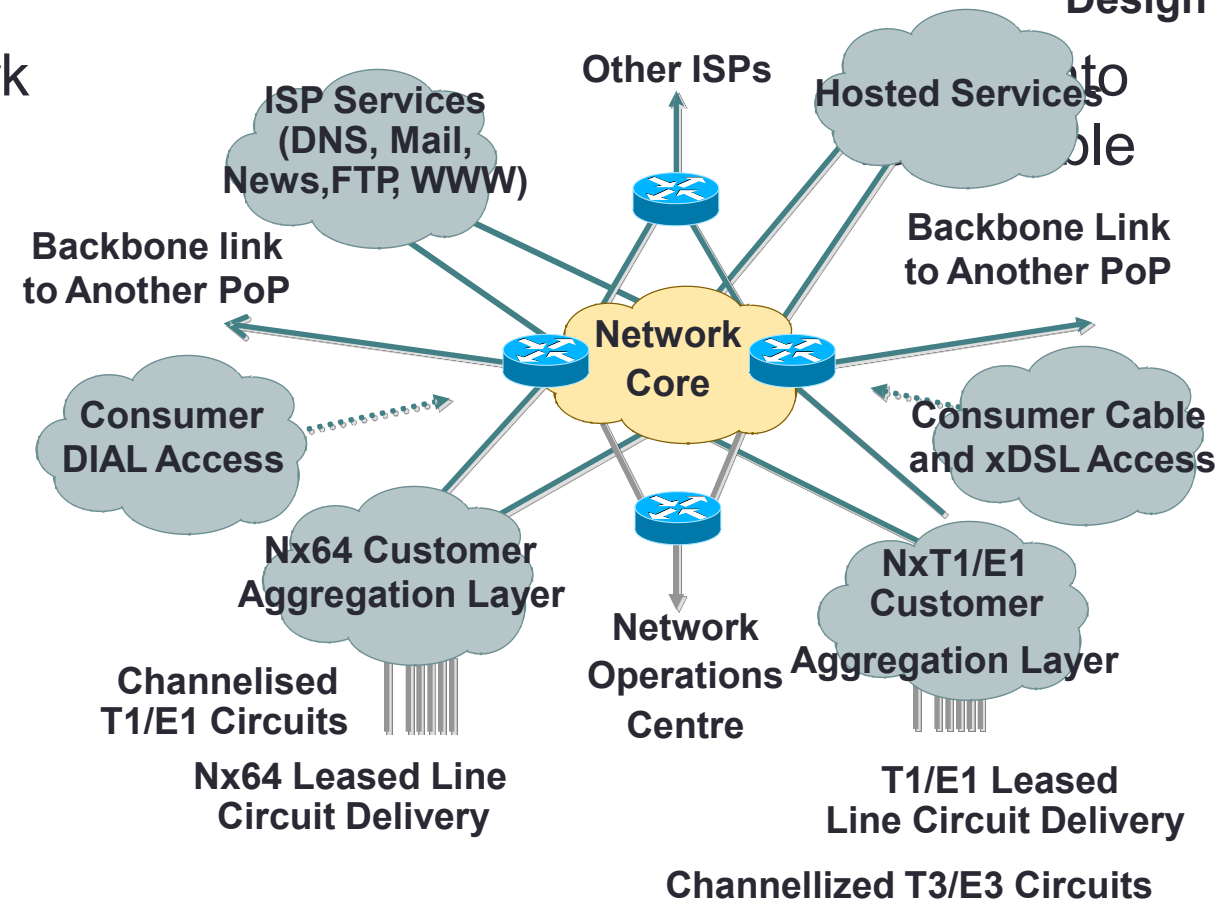
Design Discipline

Designing of Internet System Network Architecture

- **Modular/Structured Design**

Design

- Organize the network separate and modules
  - Backbone
  - PoP
  - Hosting Services
  - ISP Services
  - Support/NOC



Designing of Internet System Network Architecture

- **Modular/Structured Design**

- Modularity makes it easy to scale a network:
  - Design smaller units of the network that are then plugged into each other
  - Each module can be built for a specific function in the network
  - Upgrade paths are built around the modules, not the entire network

Designing of Internet System Network Architecture

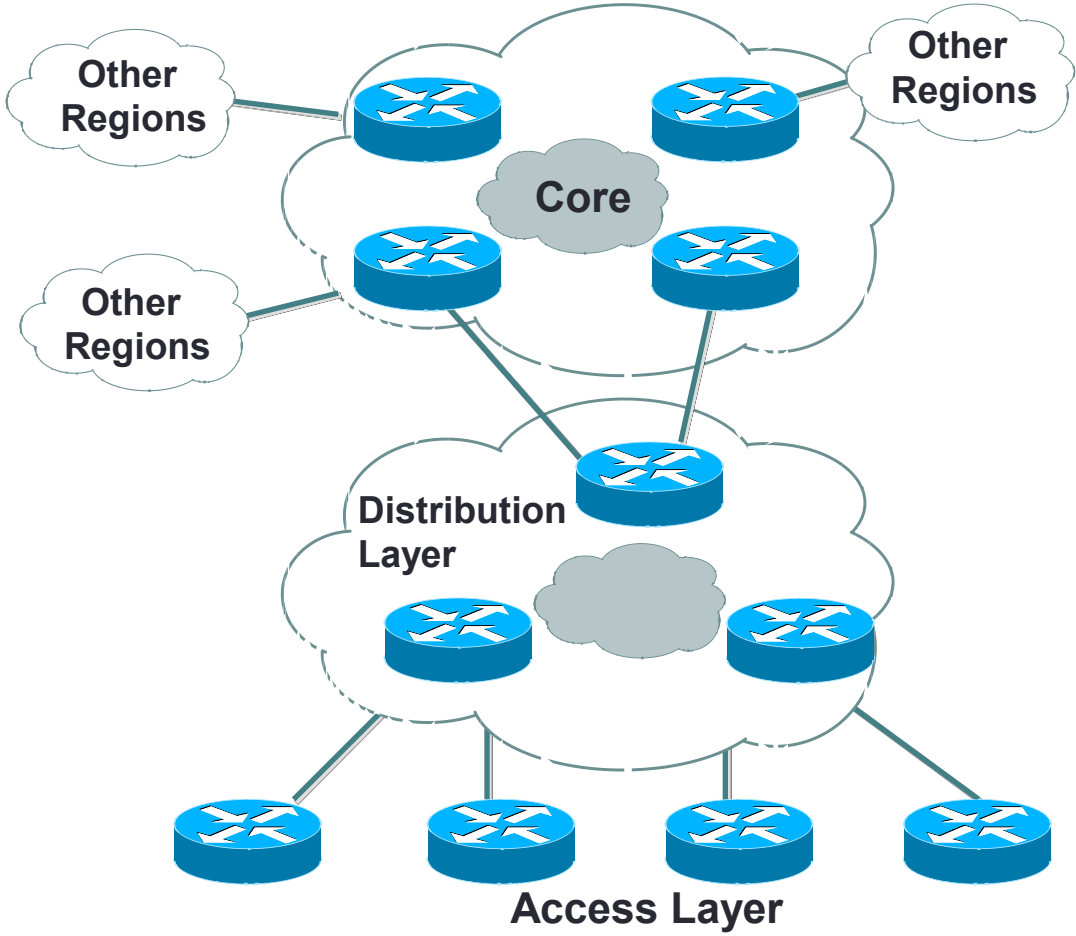
- **Functional Design**

- One Box cannot do everything
  - (no matter how hard people have tried in the past)
- Each router/switch in a network has a well-defined set of functions
- The various boxes interact with each other
- Equipment can be selected and functionally placed in a network around its strengths
- ISP Networks are a systems approach to design
  - Functions interlink and interact to form a network solution.

Designing of Internet System Network Architecture

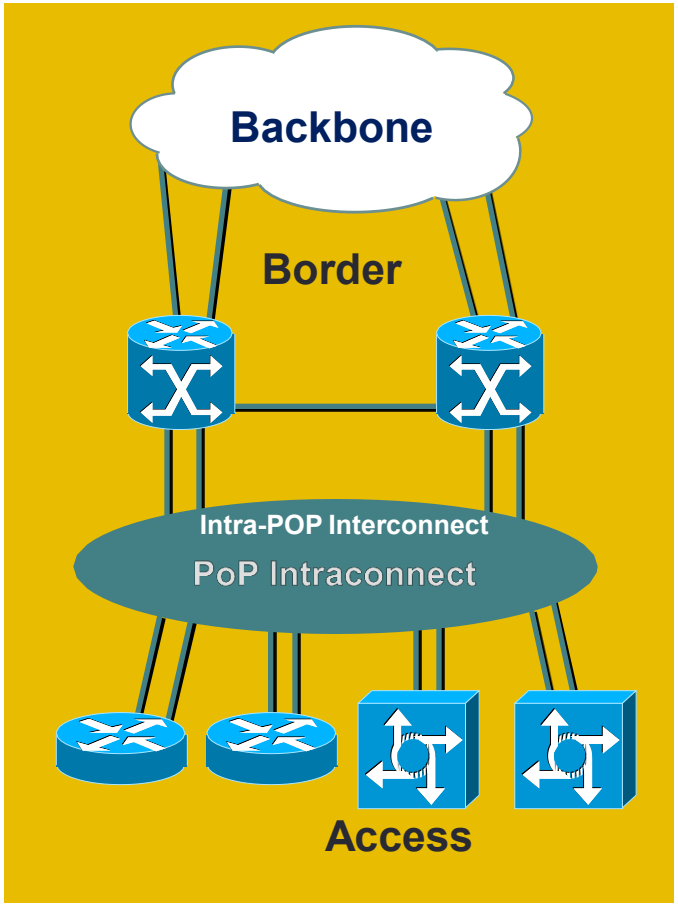
- **Tiered/Hierarchical Design:**

- Flat meshed topologies do not scale
- Hierarchy is used in designs to scale the network
- Good conceptual guideline, but the lines blur when it comes to implementation.



Designing of Internet System Network Architecture

- **Multiple Levels of Redundancy:**
- Triple layered PoP redundancy
  - Lower-level failures are better
  - Lower-level failures may trigger higher-level failures
  - L2: Two of everything
  - L3: IGP and BGP provide redundancy and load balancing
  - L4: TCP re-transmissions recover during the fail-over

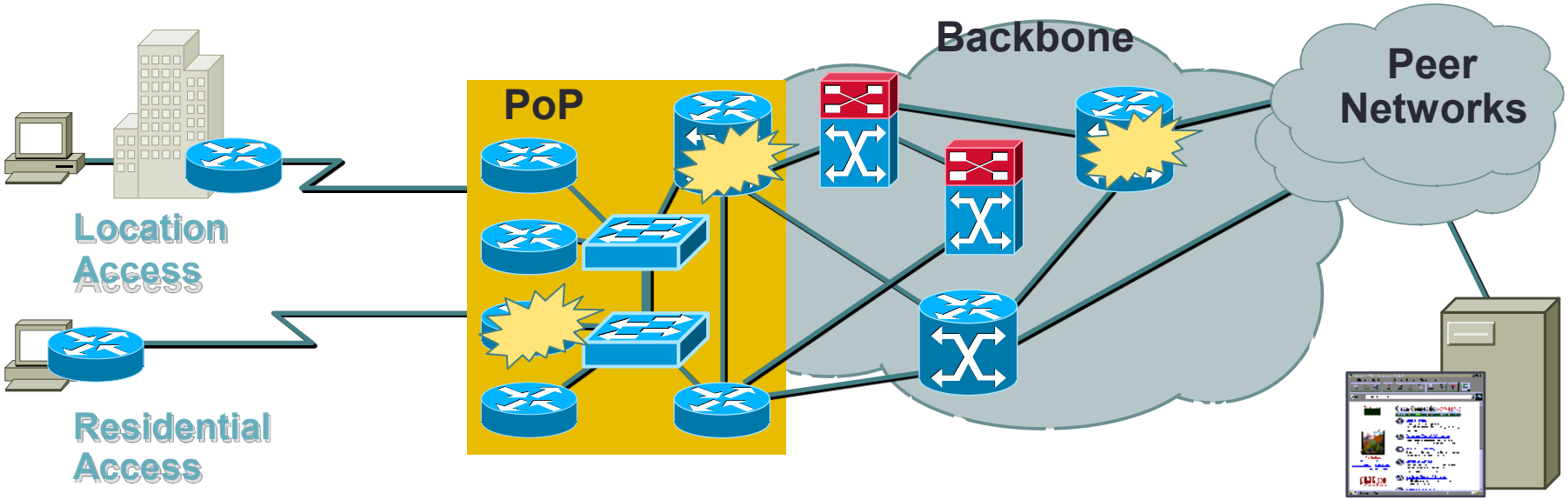


- Multiple levels also mean that one must go deep – for example:
  - Outside Cable plant – circuits on the same bundle – backhoe failures
  - Redundant power to the rack – circuit over load and technician trip

MIT (maintenance injected trouble) is one of the key causes of ISP outage.

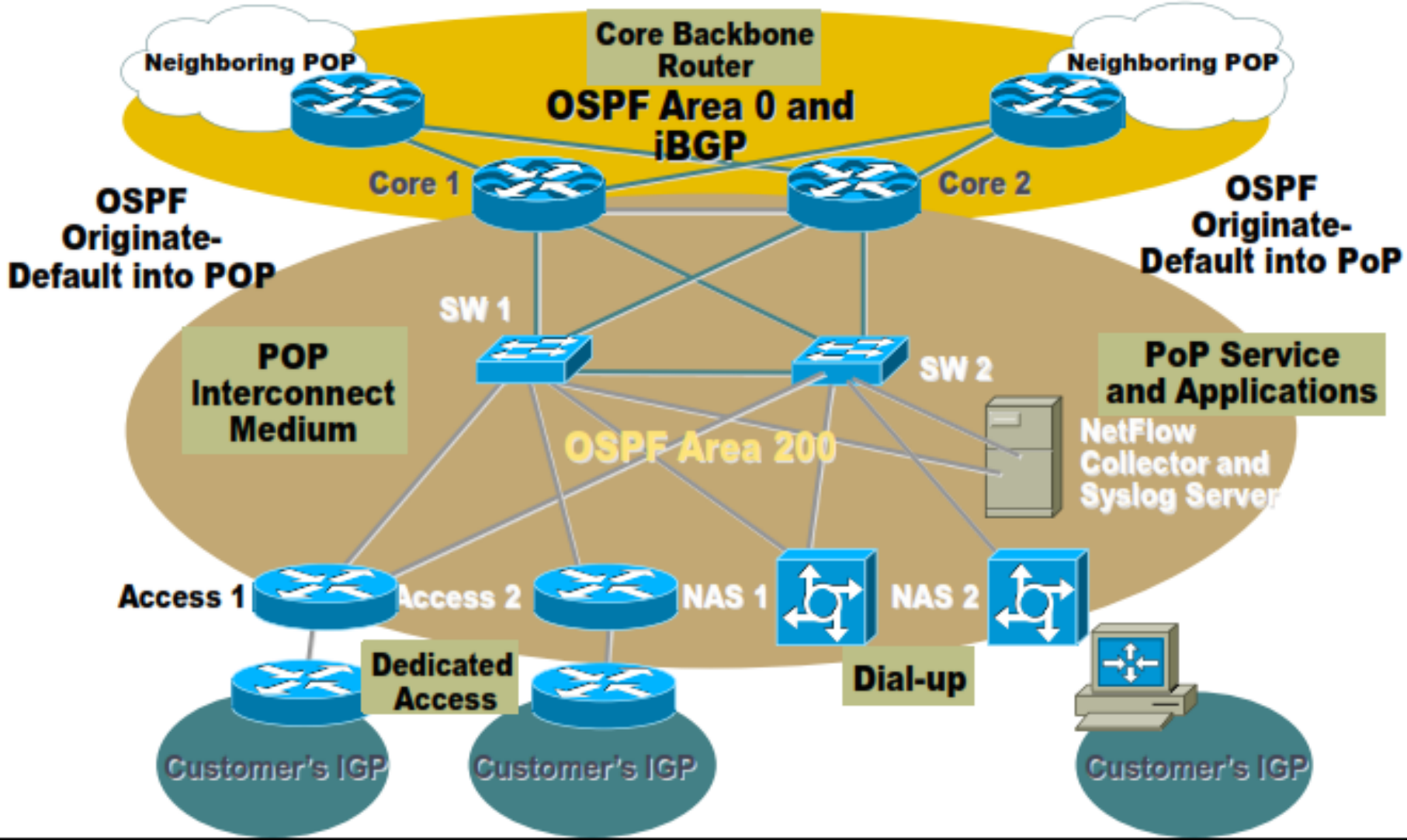
Designing of Internet System Network Architecture

- **Multiple Levels of Redundancy:**
- Objectives:
  - As little user visibility of a fault as possible
  - Minimize the impact of any fault in any part of the network
  - Network needs to handle L2, L3, L4, and router failure



Designing of Internet System Network Architecture

- **Multiple Levels of Redundancy:**



Redundant Network Design

- **The Basics: Platform**
  - Redundant Power
    - Two power supplies
  - Redundant Cooling
    - What happens if one of the fans
  - Redundant route processors
    - Consideration also, but less important
    - Partner router device is better
  - Redundant interfaces
    - Redundant link to partner device is better

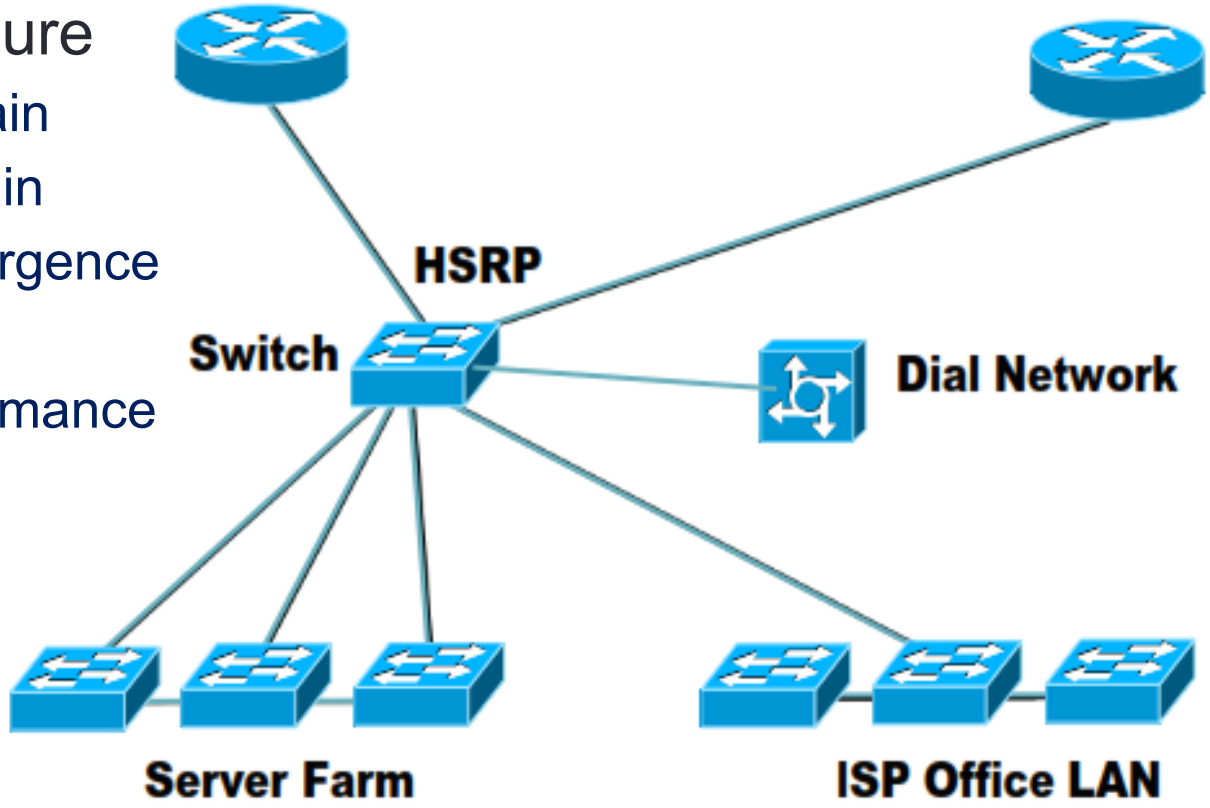
Redundant Network Design

- **The Basics: Environment**
  - Redundant Power
    - UPS source – protects against grid failure
    - “Dirty” source – protects against UPS failure
  - Redundant cabling
    - Cable break inside facility can be quickly patched by using “spare” cables
    - Facility should have two diversely routed external cable paths
  - Redundant Cooling
    - Facility has air-conditioning backup
    - …or some other cooling system?

Redundant Network Design: Within the Datacenter

- **Bad Architecture(1)**

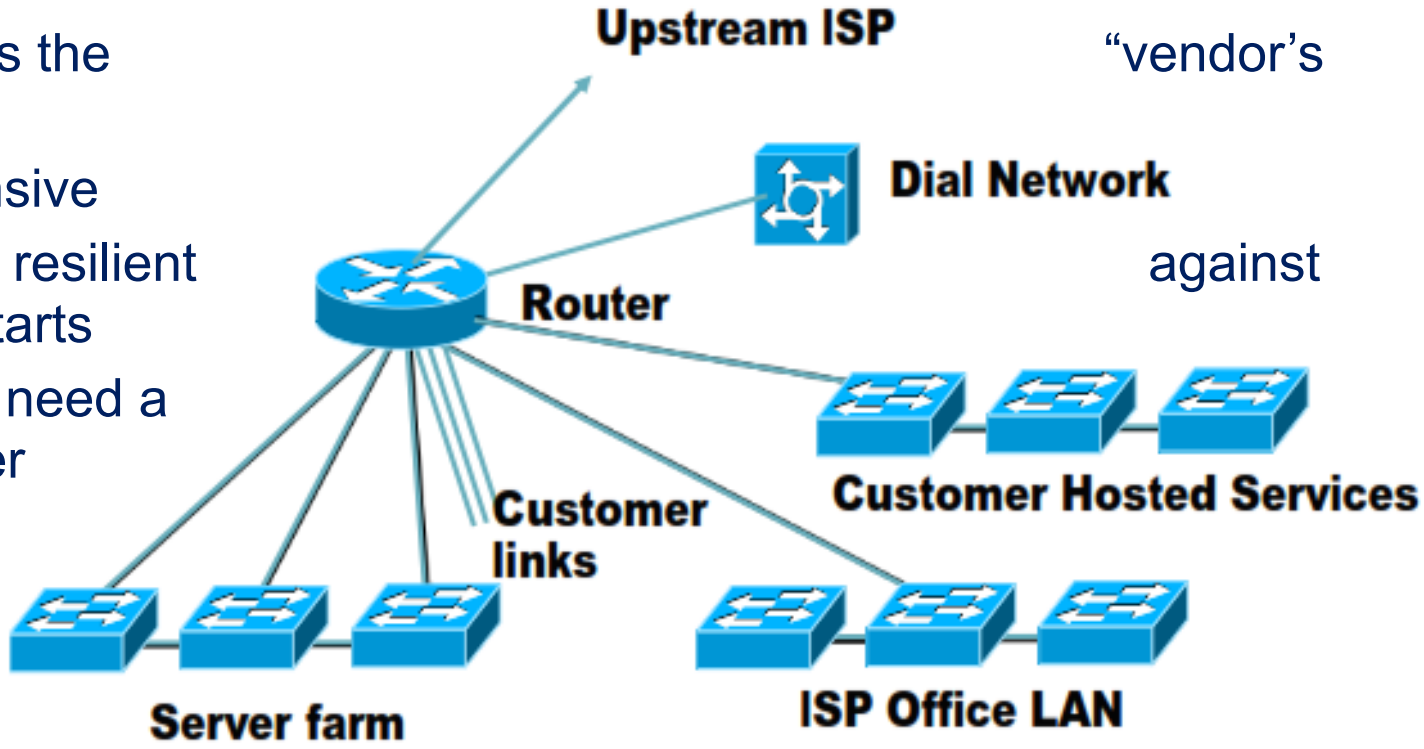
- A single point of failure
  - Single collision domain
  - Single security domain
  - Spanning tree convergence
  - No backup
  - Central switch performance



Redundant Network Design: Within the Datacenter

- **Bad Architecture(2)**

- A central router
  - Simple to build
  - Resilience is the problem"
  - More expensive
  - No router is resilient bugs or restarts
  - You always need a bigger router

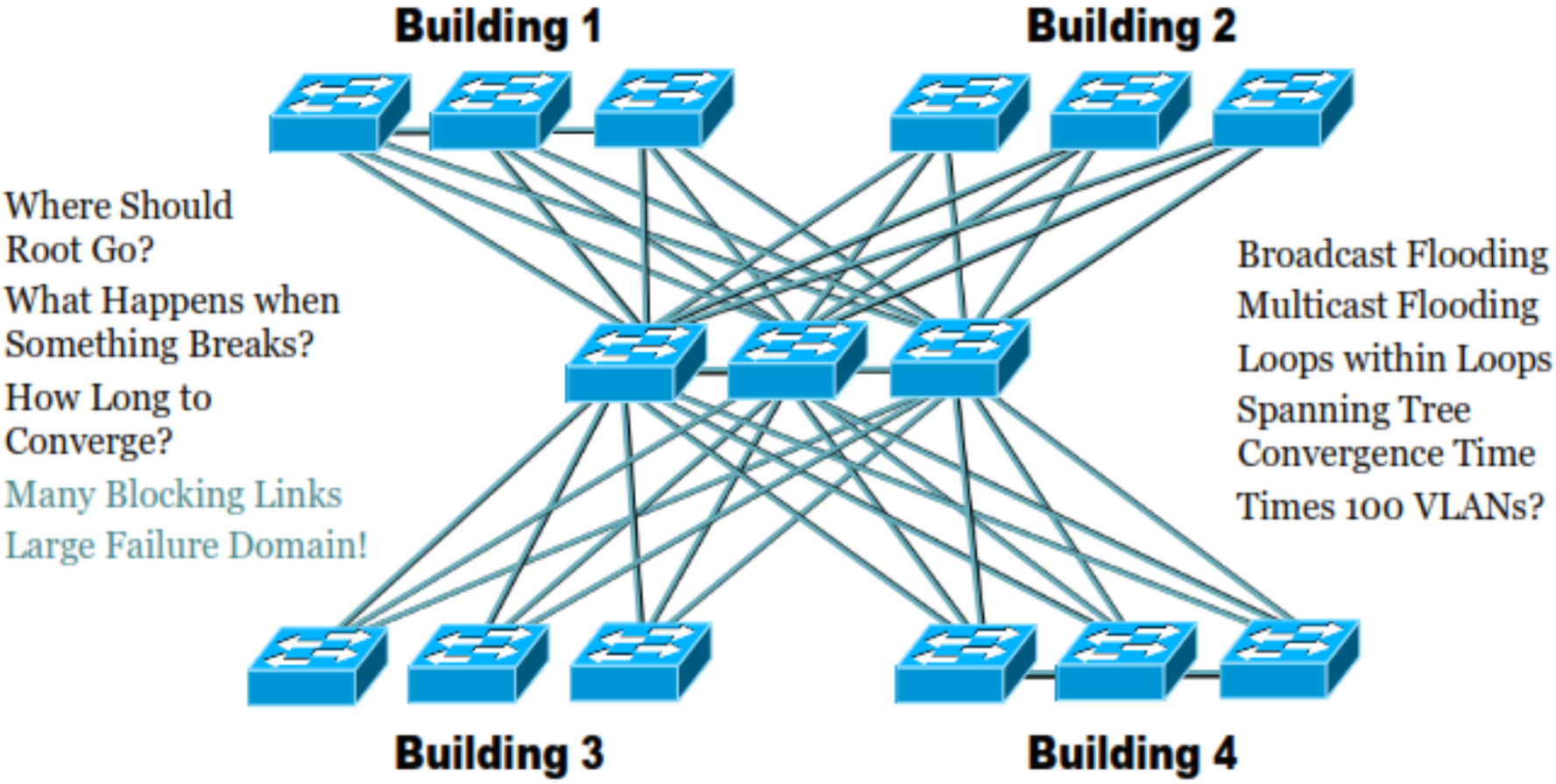


"vendor's

against

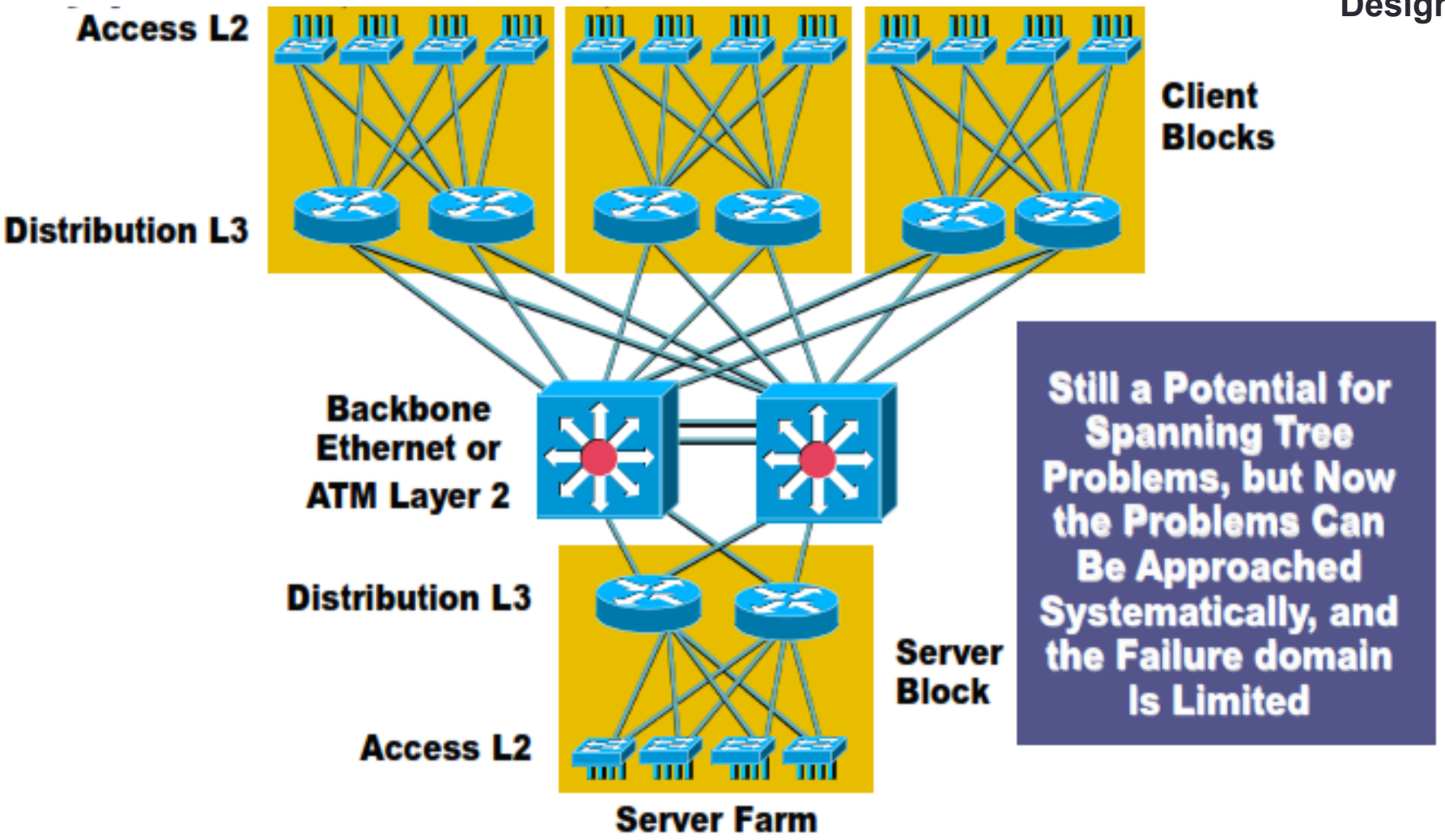
Redundant Network Design: Within the Datacenter

- **Even Worse !!**
- *Avoid highly meshed, non-deterministic large scale L2 design*



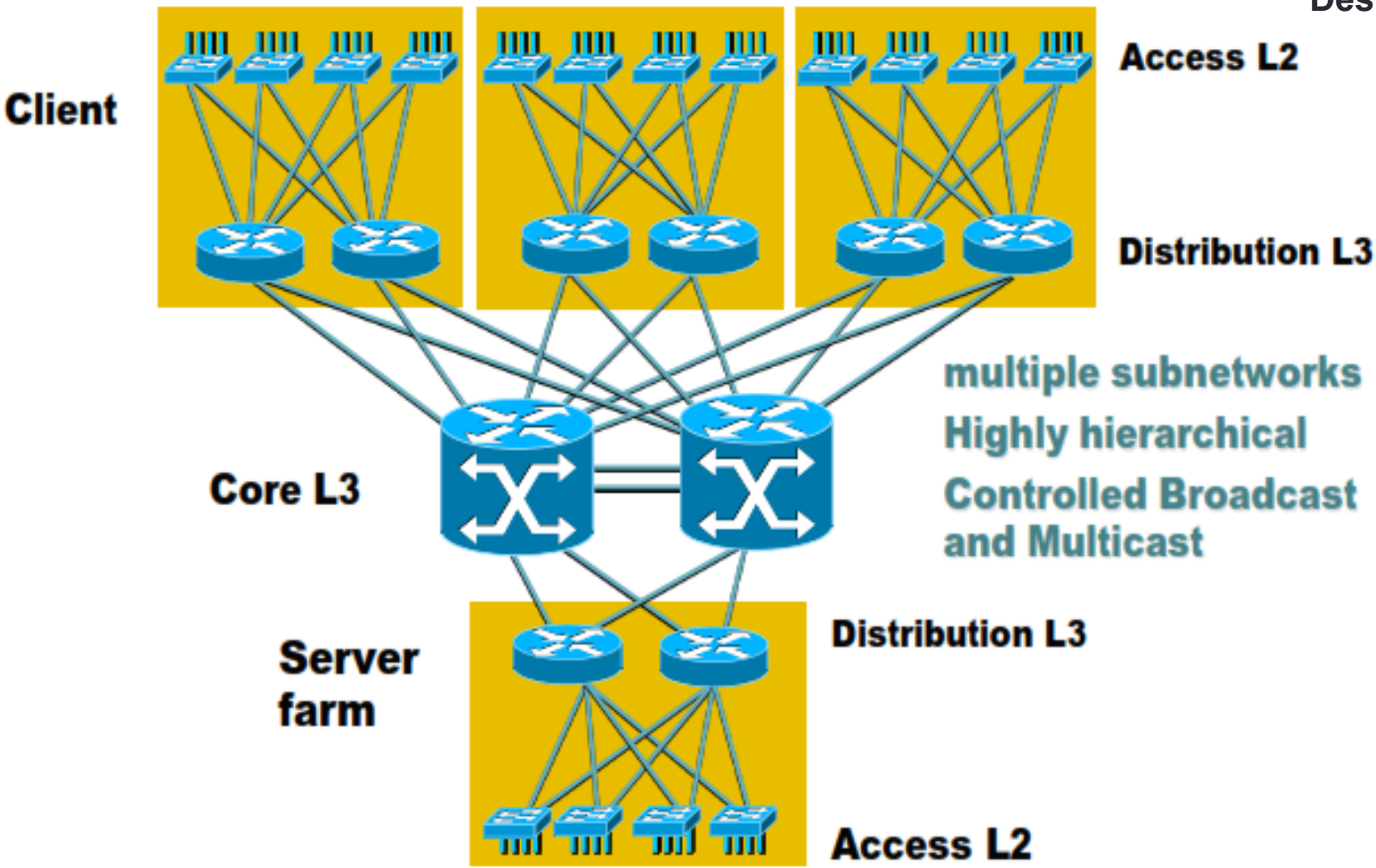
Redundant Network Design

- **Typical (Better) Backbone**



Redundant Network Design

- **The Best Architecture**

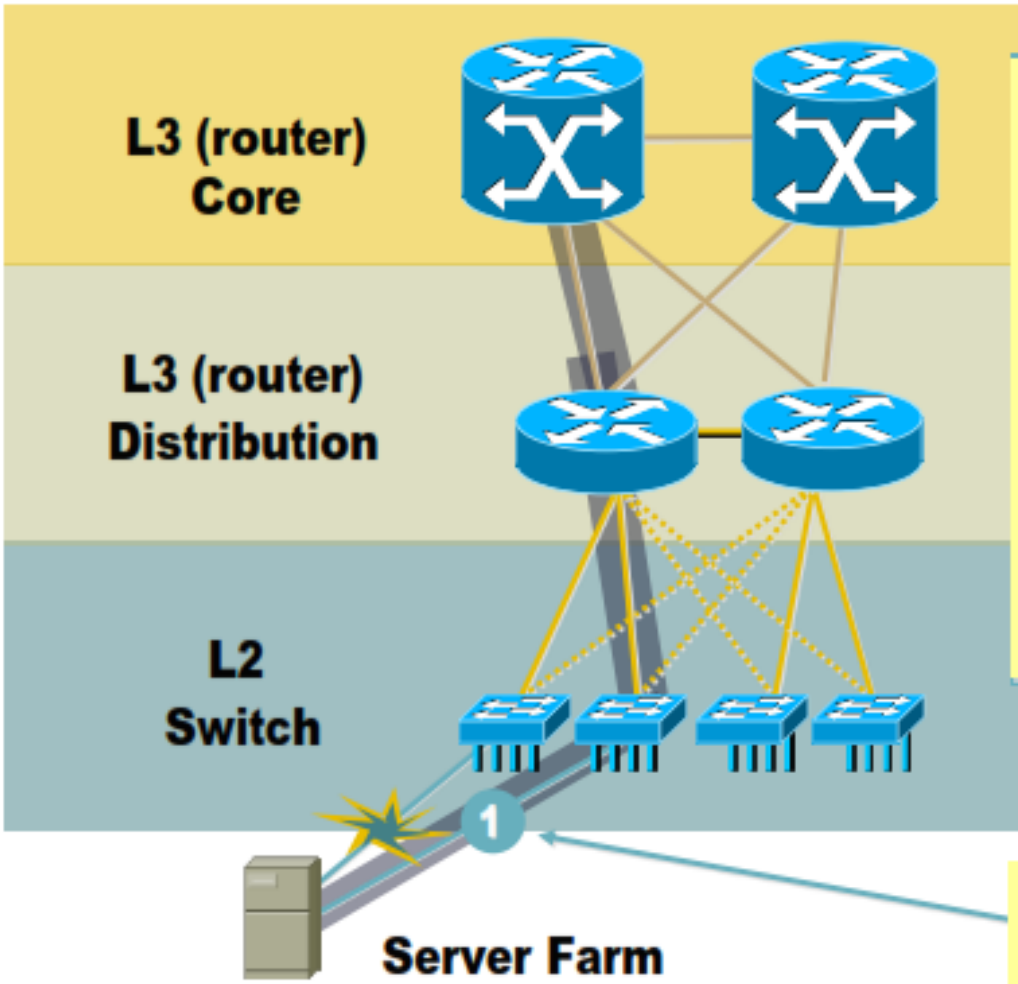


Redundant Network Design

- **Benefits of Layer 3 Backbone**
  - Multicast PIM routing control
  - Load balancing
  - No blocked links
  - Fast convergence OSPF/ISIS/EIGRP
  - Greater scalability overall
  - Router peering reduced

Redundant Network Design: Server Availability

- **Multi-homed Servers**



Technology

Using Adaptive Fault Tolerant" Drivers and NICs

NIC Has a Single IP/MAC Address (Active on one NIC at a Time)

When Faulty Link Repaired, Does Not Fail Back to Avoid Flapping

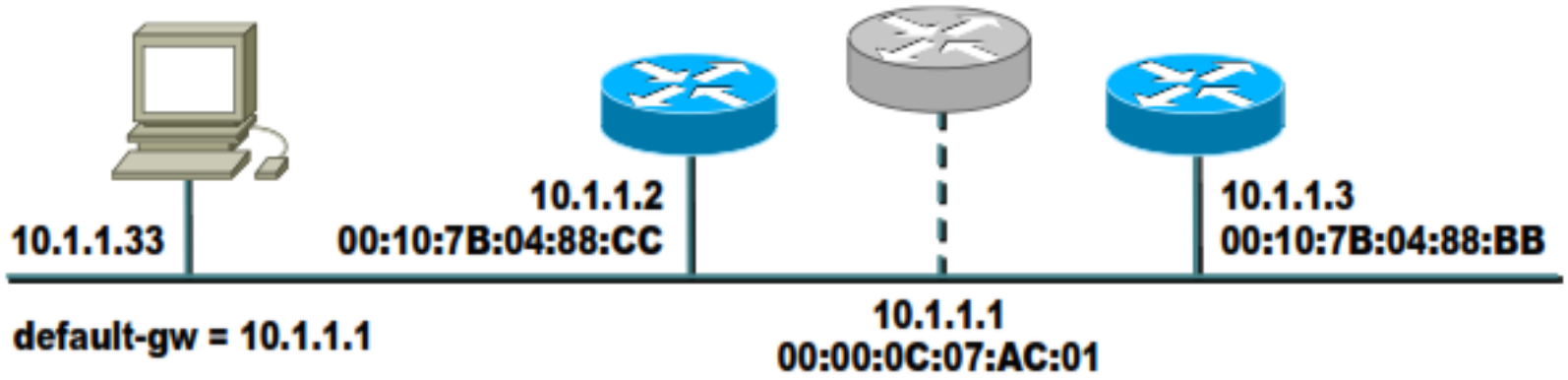
Fault-tolerant Drivers Available from Many Vendors: Intel, Compaq, HP, Sun

Many Vendors also Have Drivers that also Support etherchannel

Dual-homed Server—Primary NIC Recovery (Time 1–2 Seconds)

Redundant Network Design

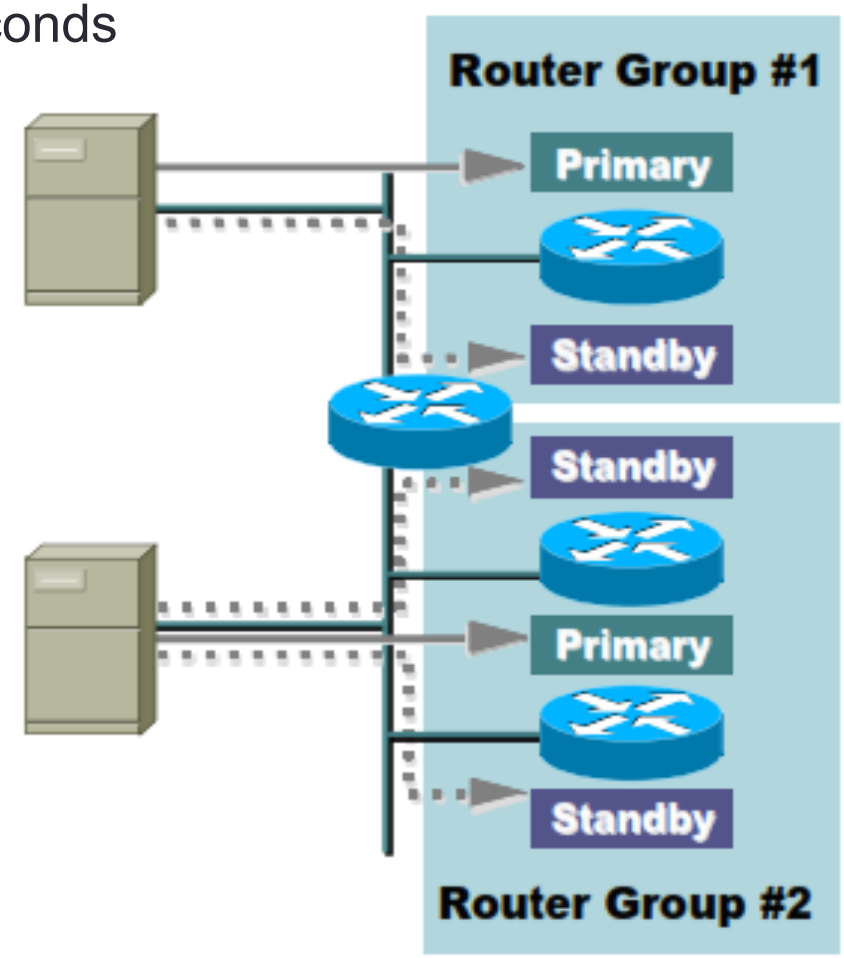
- **HSRP- Hot Standby Router Protocol**



- Transparent failover of default router
- “Phantom(something that is not real” router created
- One router is active, responds to phantom
- L2 and L3 addresses
- Others monitor and take over phantom addresses

Redundant Network Design

- **HSRP- RFC 2281**
- HSR multicasts hellos every 3 sec with a default priority of 100
- HSR will assume control if it has the highest priority and preempt configured after delay (default=0) seconds
- HSR will deduct 10 from its priority if the tracked interface goes down



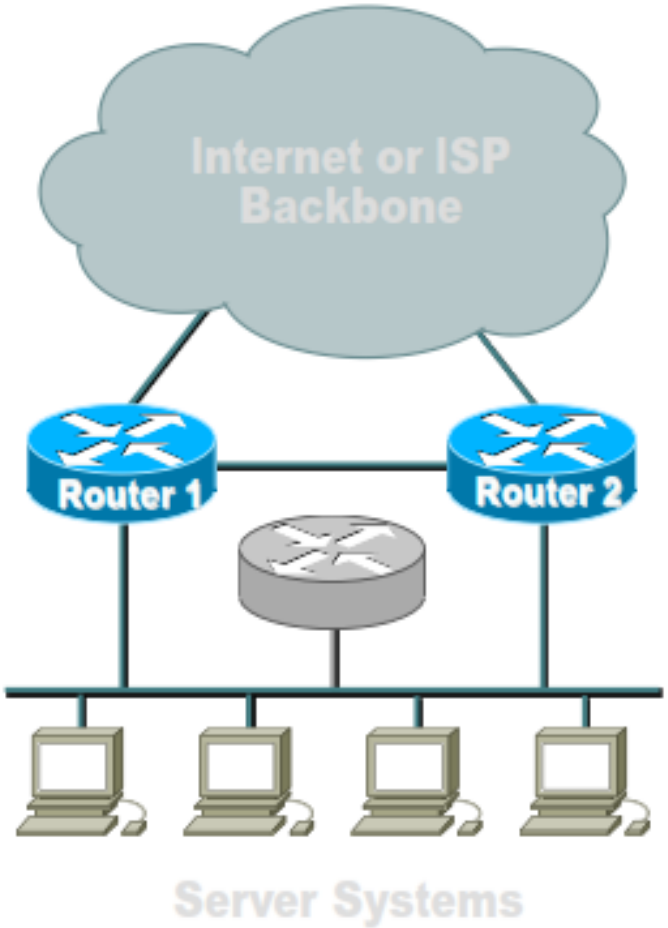
Redundant Network Design

Technology

- **HSRP**

```
Router1:
interface ethernet 0/0
ip address 169.223.10.1 255.255.255.0
standby 10 ip 169.223.10.254


Router2:
interface ethernet 0/0
ip address 169.223.10.2 255.255.255.0
standby 10 priority 150 pre-empt delay 10
standby 10 ip 169.223.10.254
standby 10 track serial 0 60
```

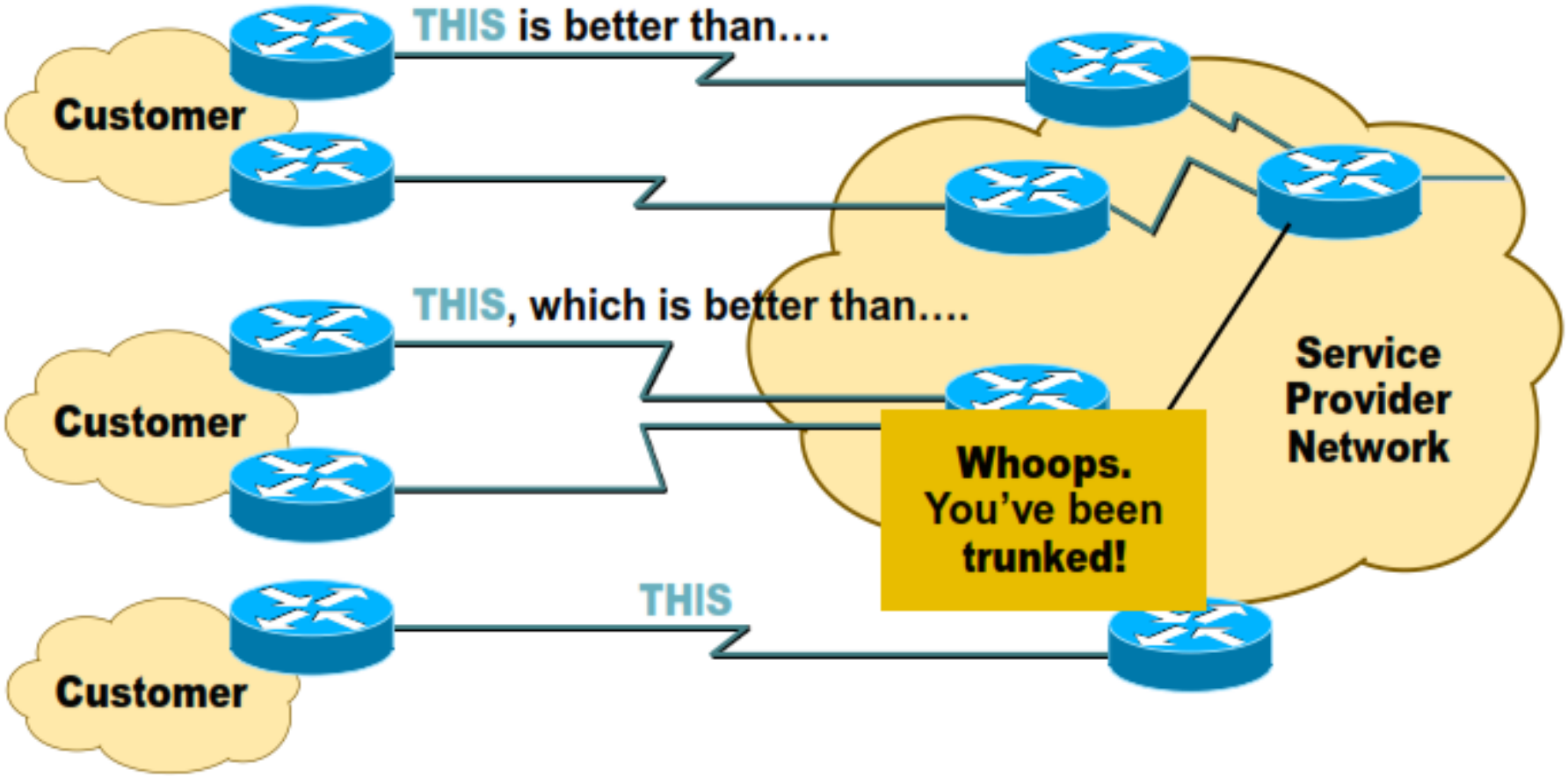


Redundant Network Design: **WAN Availability**

- **Circuit Diversity**
- Having backup PVCs through the same physical port accomplishes little or nothing
  - Port is more likely to fail than any individual PVC
  - Use separate ports
- Having backup connections on the same router doesn't give router independence
  - Use separate router
- Use different circuit provider (if available)
  - Problems in one provider network won't mean a problem for your network
- Ensure that facility has diverse circuit paths to telecommunication provider or providers
- Make sure your backup path terminates into separate equipment at the service provider
- Make sure that your lines are not trunked into the same paths as they traverse the network
- Try and write this into your Service Level Agreement with providers

Redundant Network Design: WAN Availability

- **Circuit Diversity**



Redundant Network Design: WAN Availability

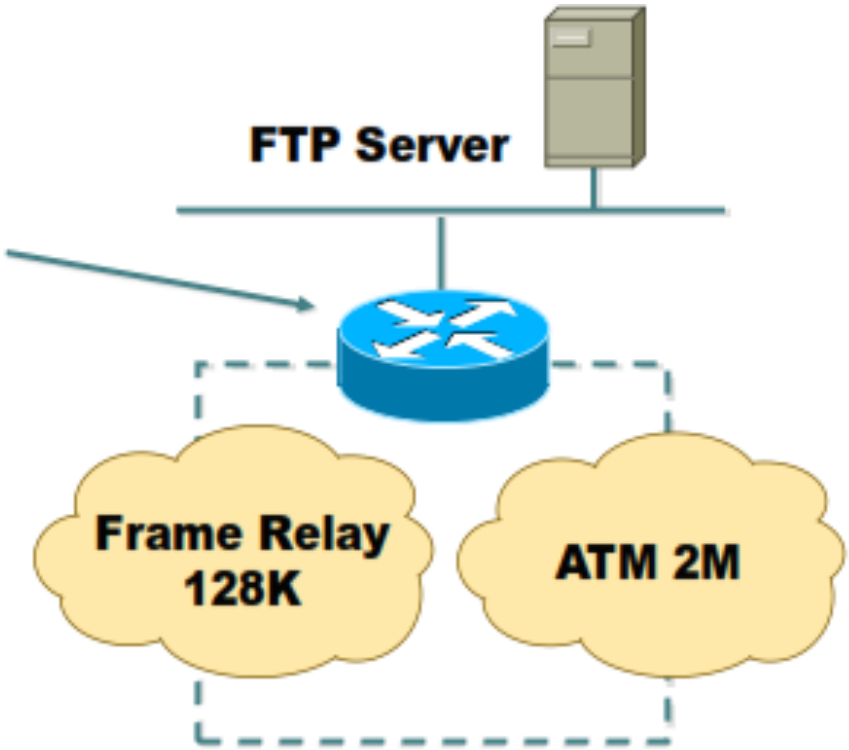
- **Circuit Bundling – MUX**
- Use Hardware MUX
  - Hardware MUXes can bundle multiple circuits, providing L1 redundancy
  - Need a similar MUX on other end of link
  - Router sees circuits as one link
    - Failures are taken care of by the MUX

Redundant Network Design: **WAN Availability**

- **Load Sharing**
- Load sharing occurs when a router has two (or more) equal cost paths to the same destination
- EIGRP also allows unequal-cost load sharing
- Load sharing can be on a per-packet or per-destination basis (default: per- destination)
- Load sharing can be a powerful redundancy technique, since it provides an alternate path to a route/path fail

Redundant Network Design: WAN Availability

- **Policy-based Routing**
- If you have unequal cost paths, and you don't want to use unequal-cost load sharing (you don't!), you can use PBR to send lower priority traffic down the slower path

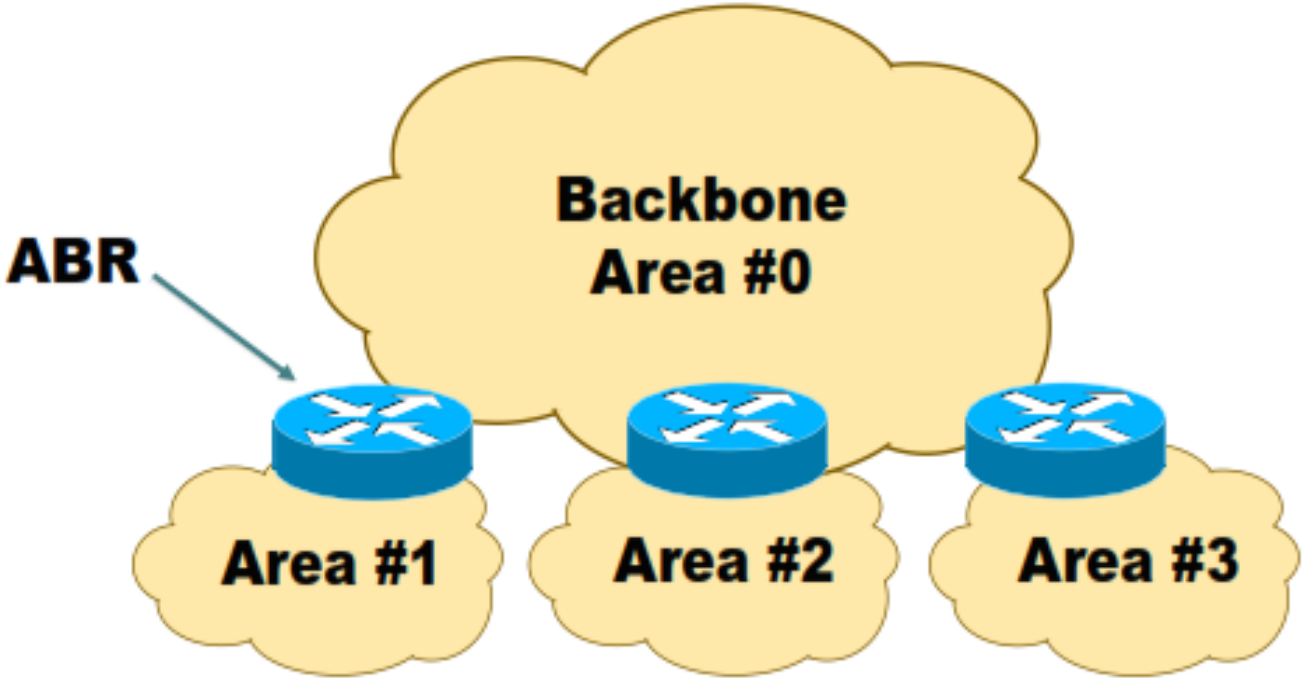


Redundant Network Design: **WAN Availability**

- **Convergence**
- The convergence time of the routing protocol chosen will affect overall availability of your WAN
- Main area to examine is L2 design impact on L3 efficiency
- Factors Determining Protocol Convergence
  - Network size
  - Hop count limitations
  - Peering arrangements (edge, core)
  - Speed of change detection
  - Propagation of change information
  - Network design: hierarchy, summarization, redundancy

Redundant Network Design: WAN Availability

- **OSPF – Hierarchical Structure**



- Topology of an area is invisible from outside of the area
  - LSA flooding is bounded by area
  - SPF calculation is performed separately for each area

Redundant Network Design: WAN Availability

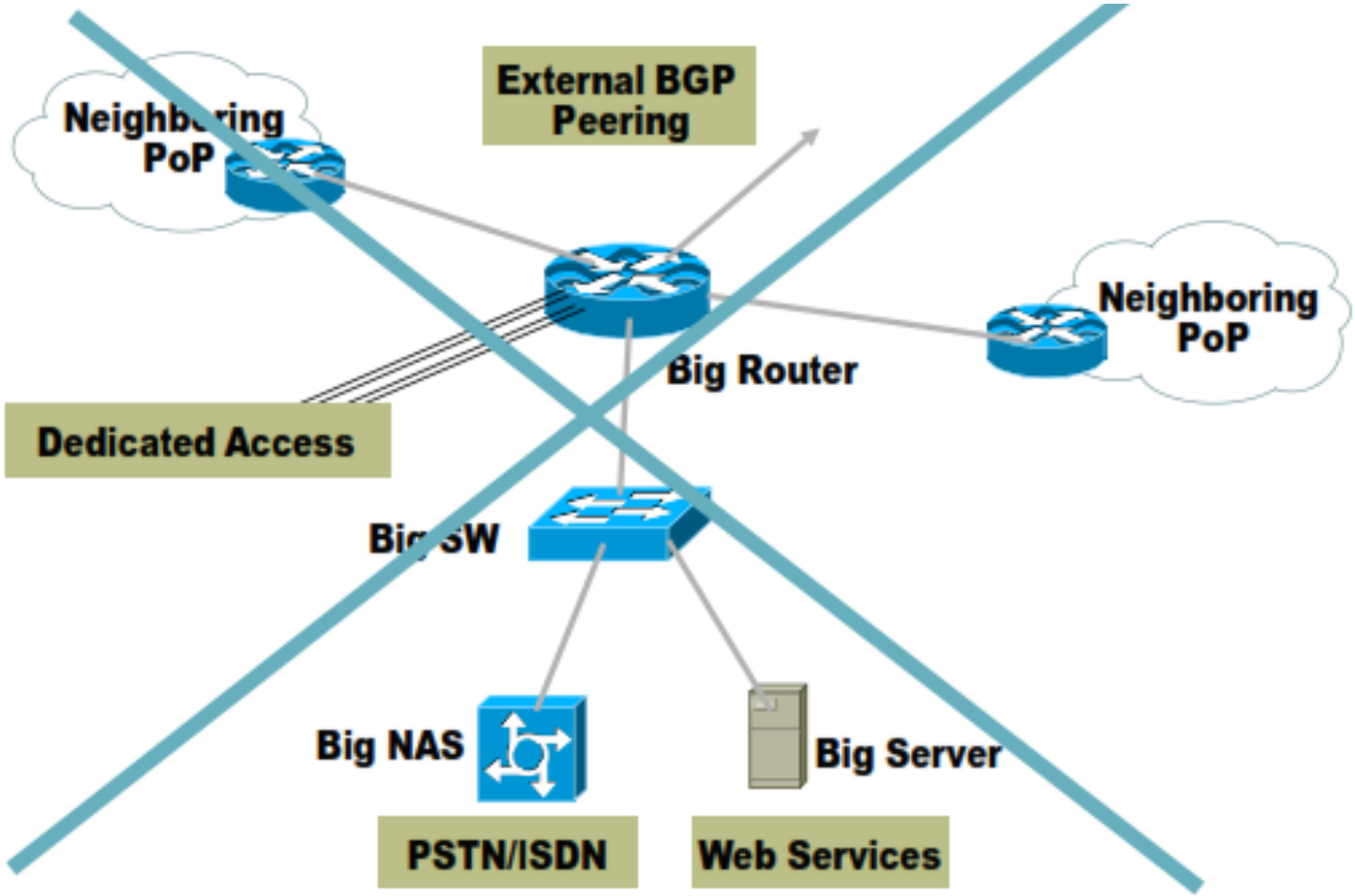
- **Factors assisting Protocol Convergence**
- Keep number of routing devices in each topology area small (15 – 20 or so)
  - Reduced convergence time required
- Avoid complex meshing between devices in an area
  - Two links are usually all that are necessary
- Keep prefix count in interior routing protocols small
  - Large numbers means longer time to compute shortest path

Redundant Network Design: Internet Availability

- **PoP Design**
- One router cannot do it all
  - *Redundancy !!! redundancy !!! redundancy !!!*
- Most successful ISPs build two of everything
- Two smaller devices in place of one larger device:
  - Two routers for one function
  - Two switches for one function
  - Two links for one function
- Two of everything does not mean complexity
- Avoid complex highly meshed network designs
  - Hard to run
  - Hard to debug
  - Hard to scale
  - Usually demonstrate poor performance

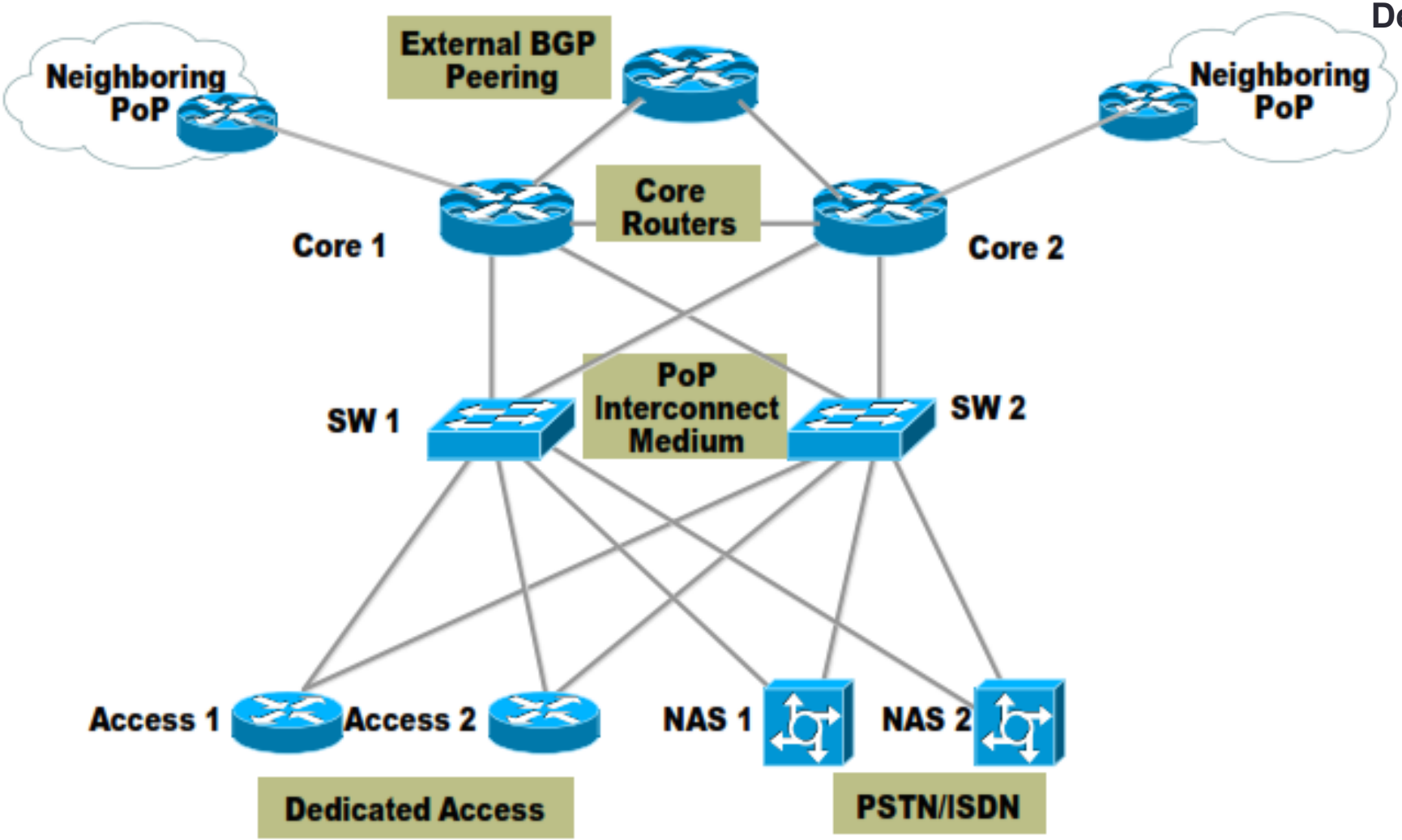
Redundant Network Design: Internet Availability

- **PoP Design - WRONG**



Redundant Network Design: Internet Availability

- **PoP Design - CORRECT**



Redundant Network Design: Internet Availability

- **Hubs vs. Switches**
- Hubs:
  - These are obsolete
  - Traffic on hub is visible on all ports
    - It's really a replacement for coaxial Ethernet
    - Security!?
  - Performance is very low
    - 10Mbps shared between all devices on LAN
    - High traffic from one device impacts all the others
  - Usually non-existent management

Redundant Network Design: Internet Availability

- **Hubs vs. Switches**
- Switches:
  - Each port is masked from the other
  - High performance
    - 10/100/1000Mbps per port
    - Traffic load on one port does not impact other ports
  - 10/100/1000 switches are commonplace and cheap
  - Choose non-blocking switches in core
    - Packet doesn't have to wait for switch
  - Management capability (SNMP via IP, CLI)
  - Redundant power supplies are useful to have

Redundant Network Design: Operations

Process

- **Network Operations Center (NOC)**

- NOC is necessary for a small ISP
  - It may be just a PC called NOC, on UPS, in equipment room.
  - Provides last resort access to the network
  - Captures log information from the network
  - Has remote access from outside
    - Dialup, SSH,…
  - Train staff to operate it
  - Scale up the PC and support as the business grows

Redundant Network Design: **Operations**

Process

- **Network Operations Center (NOC)**
- NOC is essential for all ISPs
  - Operational Procedures are necessary
    - Monitor fixed circuits, access devices, servers
    - If something fails, someone has to be told
  - Escalation path is necessary
    - Ignoring a problem won't help fixing it.
    - Decide on time-to-fix, escalate (poor path report garne)up reporting chain until someone can fix it
  - Modifications to network
    - A well designed network only runs as well as those who operate it
    - Decide and publish maintenance schedules
    - And then STICK TO THEM
    - Don't make changes outside the maintenance period, no matter how trivial they may appear

Redundant Network Design: SUMMARY

- In Summary, Implementing a highly resilient IP network requires a combination of the proper process, design and technology
- “and now abide the design, technology and process; but the greatest of these is process”

Server Setup and Configuration Guidelines

- Hardware/The Basics: Environment
- Operating System / Firewall
- Number of sessions and load balancing

Server Setup and Configuration Guidelines

- Hardware/The Basics: Environment
  - Redundant Power
    - Two power supplies
    - UPS source – protects against grid failure
  - Redundant Cooling
    - What happens if one of the fans fail?
    - Facility has air-conditioning backup
    - …or some other cooling system?
  - Redundant cabling
    - Cable break inside facility can be quickly patched by using “spare” cables
    - Facility should have two diversely routed external cable paths
  - Redundant processors
    - Consideration also, but less important
    - Partner router device is better
  - Redundant interfaces
    - Redundant link to partner device is better

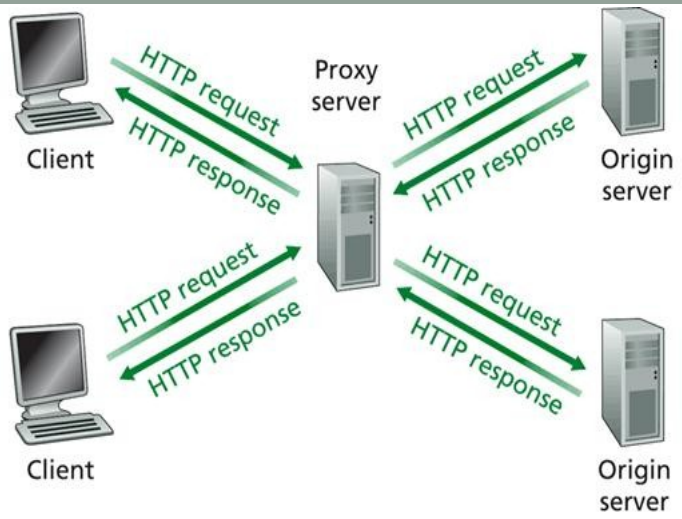
Server Setup and Configuration Guidelines

- Hardware/The Basics: Environment
  - RAID
  - RAID 0
  - RAID 1
  - RAID 5
  - RAID 10
  - RAID 15

Server Setup and Configuration Guidelines

- Operating System and Security
  - Platform
    - Windows
    - Linux
  - Should have corporate level firewall
    - Packet filtering
    - Application level
    - IDS
- Number of sessions and load balancing
  - Threading should be increased
  - Beside Threading there should be load balancing Hardware that should be responsible for load balancing in the server either packet wise or session wise in the replicated server.

Proxies



- Content (particularly stored, web content) is available from one source, but may also be available from other sources.
- Terminology:
  - Origin server: Original source of an object
  - Proxy server: Supplies object instead of origin server

♦ Clients requesting objects through a Web cache

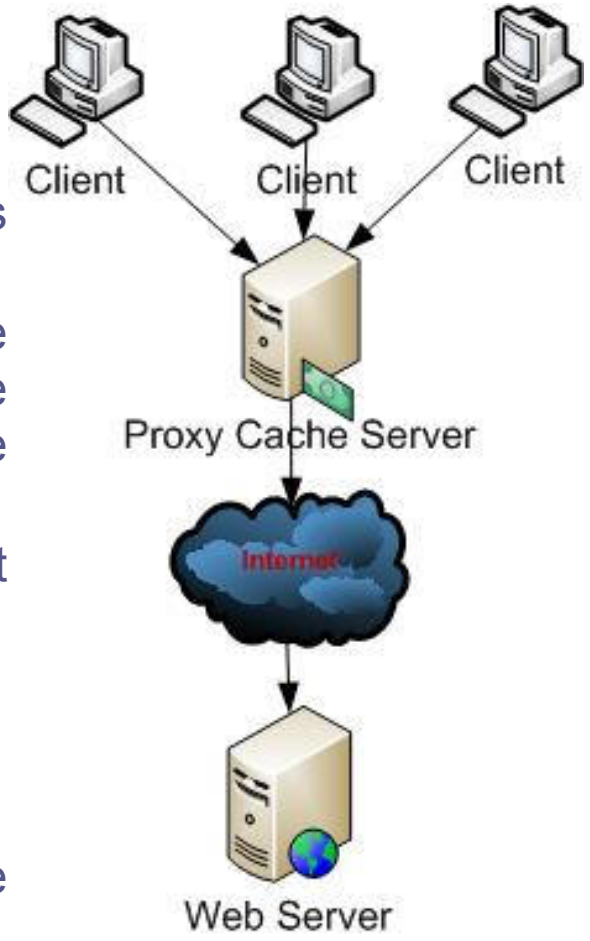
- Some (caches) are demand-driven: Acts as both a
  - server: responding to client's requests
  - client: forwarding requests that it cannot respond to towards the origin server
- Some are driven by supply and demand (e.g. proactive caching)
- Some are supply-driven: Content Distribution Networks

Caching Principle

- Fast resources are scarce e.g. storage close to clients (low propagation delay & fast links)
- Aim to locate commonly used objects in fast resource, other objects can remain in slower resources.
- Determining which objects are commonly accessed:
  - Accesses are often correlated, and are said to exhibit “locality”.
  - Temporal locality: Information accessed at one time is likely to be accessed again in the near future.
  - Spatial locality: Information accessed at one point is likely to be accessed also by nearby points.

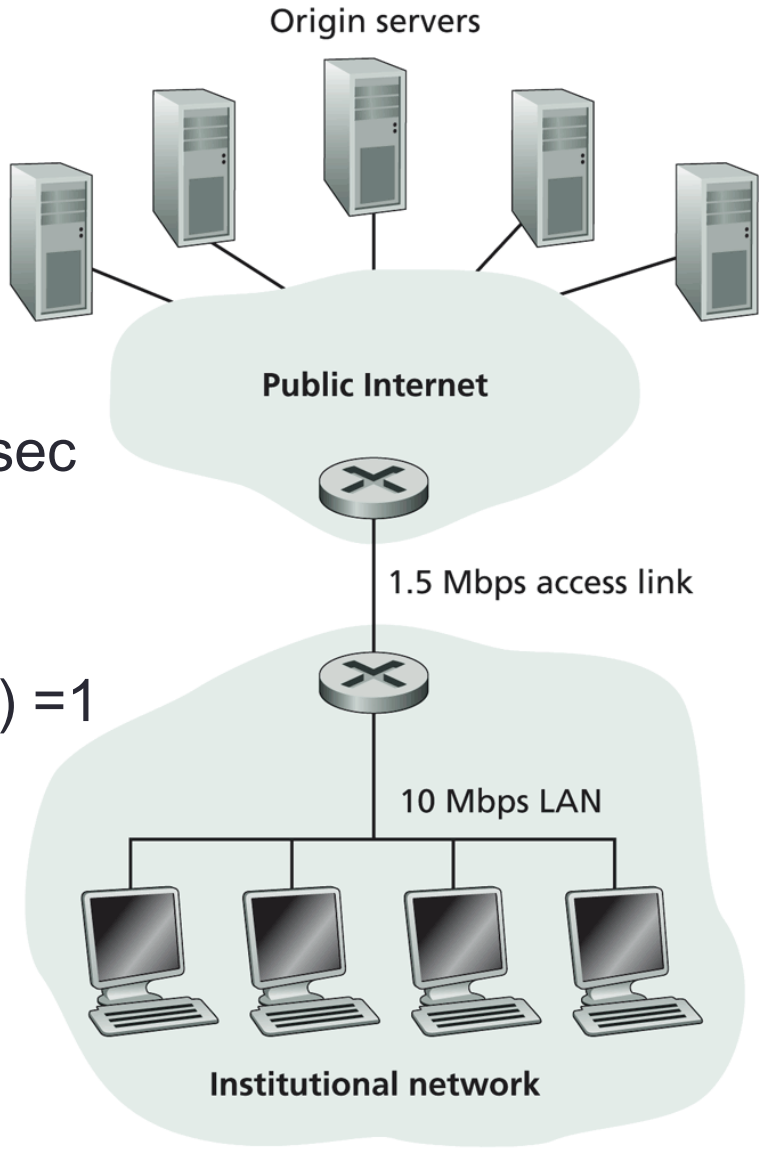
Proxy Server (Web Caching)

- Proxy server is a dedicated server that stores caching information in between the client and the web server in a shared location so that all clients can use the same shared data.
- Main Uses of proxy server:
  - Caching:
    - When a user accesses a web page, that page is temporarily stored in the proxy cache.
    - Then, when a subsequent user requests the same web page, they access the copy in the proxy cache, rather than having the web page sent again from the originating server.
    - It improves performance and frees up Internet bandwidth for other tasks.
  - Filtering:
    - Allows to block specific sites
  - Maintain Privacy:
    - Can hide actual IP address of Client from the outside world



Caching Example

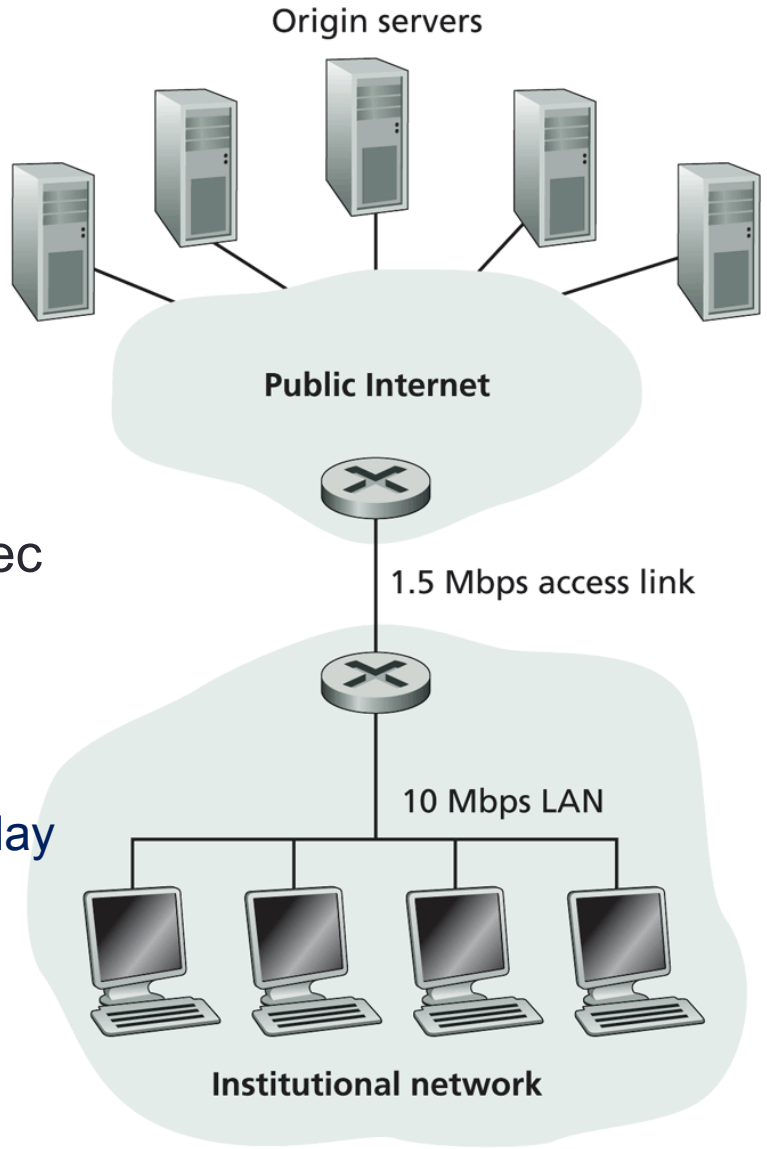
- **Assumptions**
- average object size = 100,000 bits
- avg. request rate from institution's browser to origin servers = 15req/sec
- Access bandwidth = 1.5Mbps
- Traffic Intensity = (15req/sec) *(100,000bits/request)/(1.5Mbps) =1



- Bottleneck between an institutional network and the Internet

Caching Example

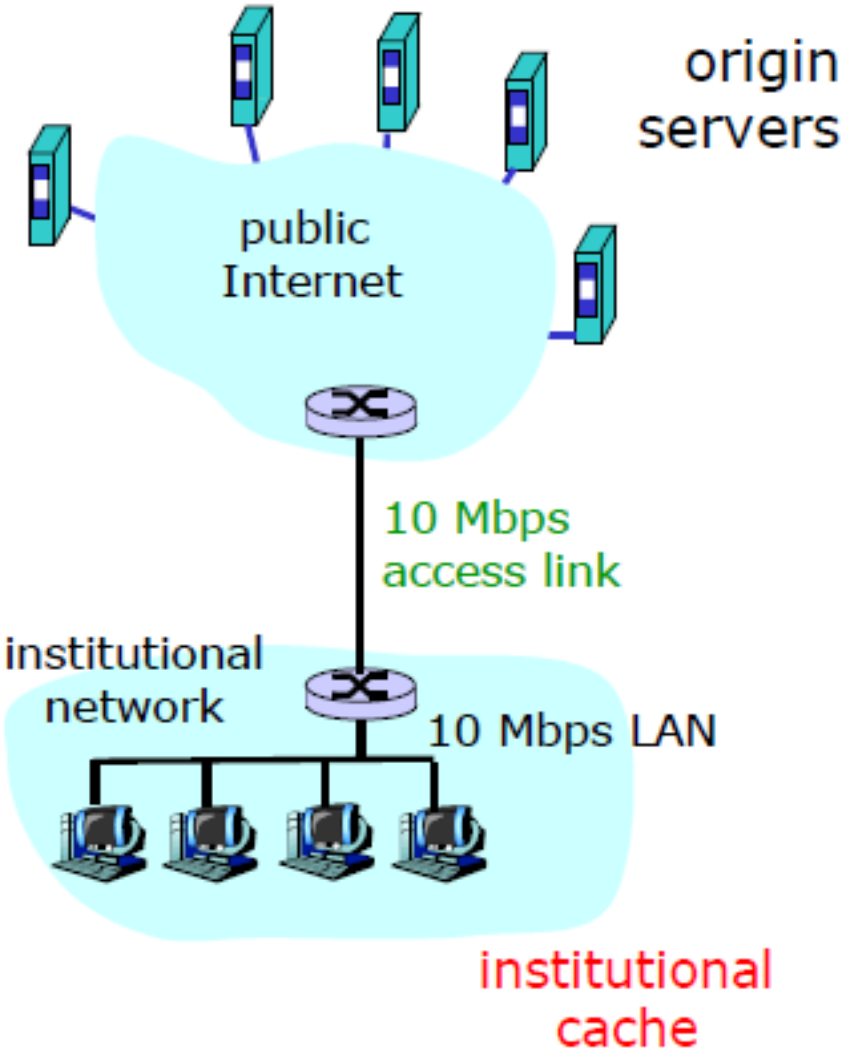
- **Assumptions**
- average object size = 100,000 bits
- avg. request rate from institution's browser to origin servers = 15req/sec
- delay from institutional router to any origin server and back to router = 2 sec
- Consequences
  - utilization on LAN = 15%
  - utilization on access link = 100%
  - total delay = Internet delay + access delay + LAN delay = 2 sec + minutes + milliseconds
- Generally LAN delays are very less approx 10ms or less in 10 Mbps



- Bottleneck between an institutional network and the Internet

Caching Example

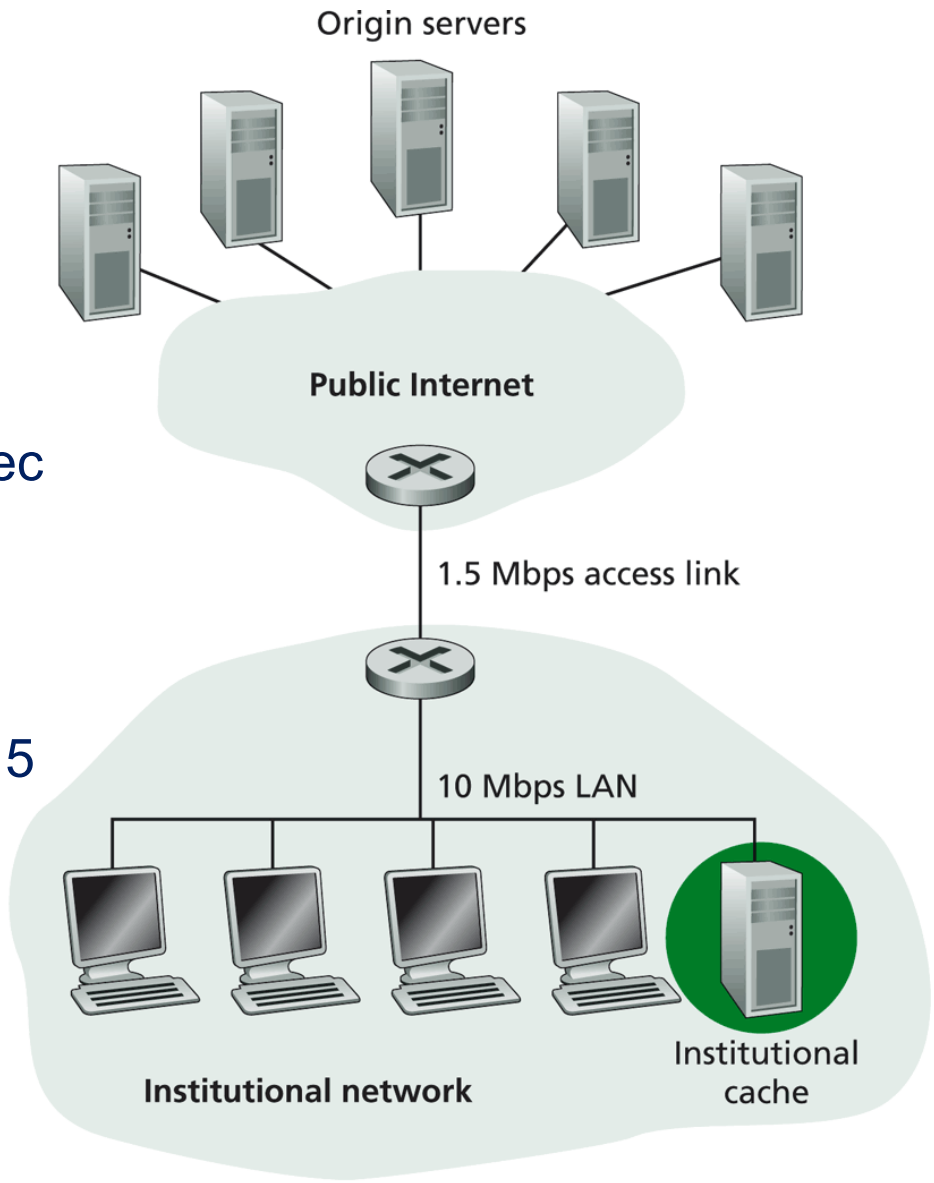
- Possible solution
  - increase bandwidth of access link to, say, 10 Mbps
- Consequences
  - utilization on LAN = 15%
  - utilization on access link =15%
  - Total delay = Internet delay + access delay + LAN delay= 2 sec + msecs + msecs
  - often a costly upgrade



Caching Example

- Assumptions
  - average object size = 100,000 bits
  - avg. request rate from institution's
  - browser to origin servers = 15req/sec
  - Access bandwidth = 1.5Mbps
  - LAN Bandwidth = 10Mbps
  - Traffic Intensity = (15req/sec)*

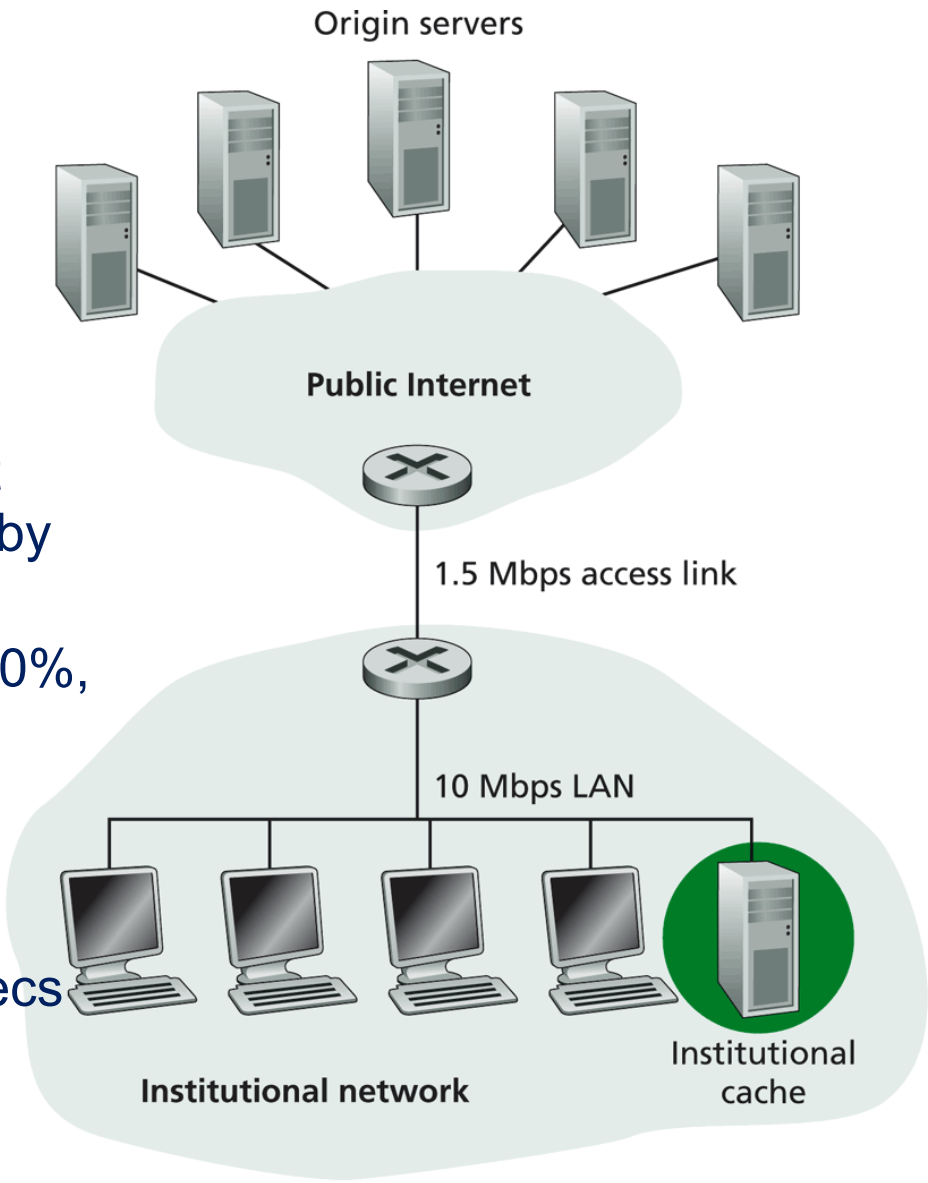
(100,000bits/request)/(10 Mbps) =0.15



♦ Adding a cache to the institutional network

Caching Example

- Install cache
  - suppose hit rate is 0.4
- Consequence
  - 40% requests will be satisfied almost immediately 60% requests satisfied by origin server
  - utilization of access link reduced to 60%, resulting in negligible delays (say 10 msec)
  - total delay = Internet delay + access delay + LAN delay = 0.6*2 sec + 0.6*0.01 secs + milliseconds < 1.3 secs

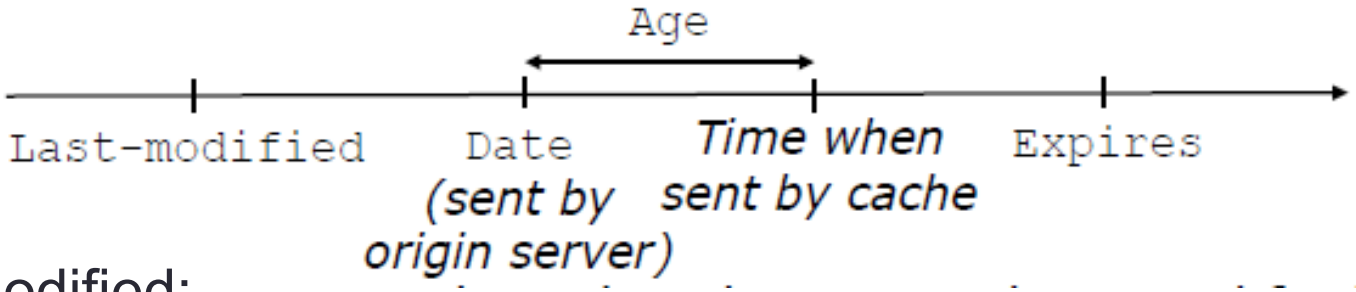


♦ Adding a cache to the institutional network

Benefits of Caching

- Benefits: Eliminate the need (in many cases) to:
  - Send request to origin server (reducing delay, and link use)
  - Send full response from origin server (reducing link use)
- Consequences:
  - Reduced delay
  - Directly benefits end-user.
  - May benefit service providers (ISPs or web servers) by making their service more popular to end-users.
  - Reduced traffic
  - Reduces load on network links
  - Reduces load on server
    - e.g. reducing “flash crowds”
  - Mask unavailability of origin server
    - e.g. when working offline, or during faults
  - Filter Requests
  - Security schemes
  - Logging

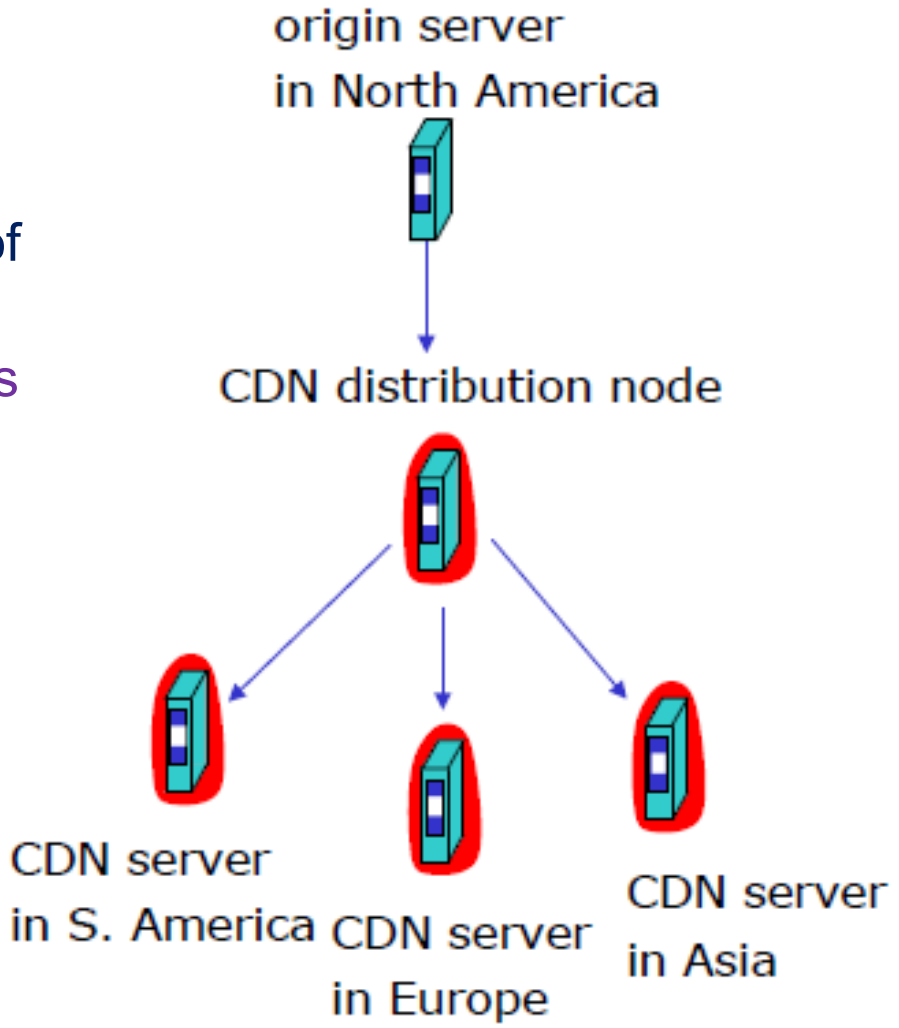
Lifecycle of an object



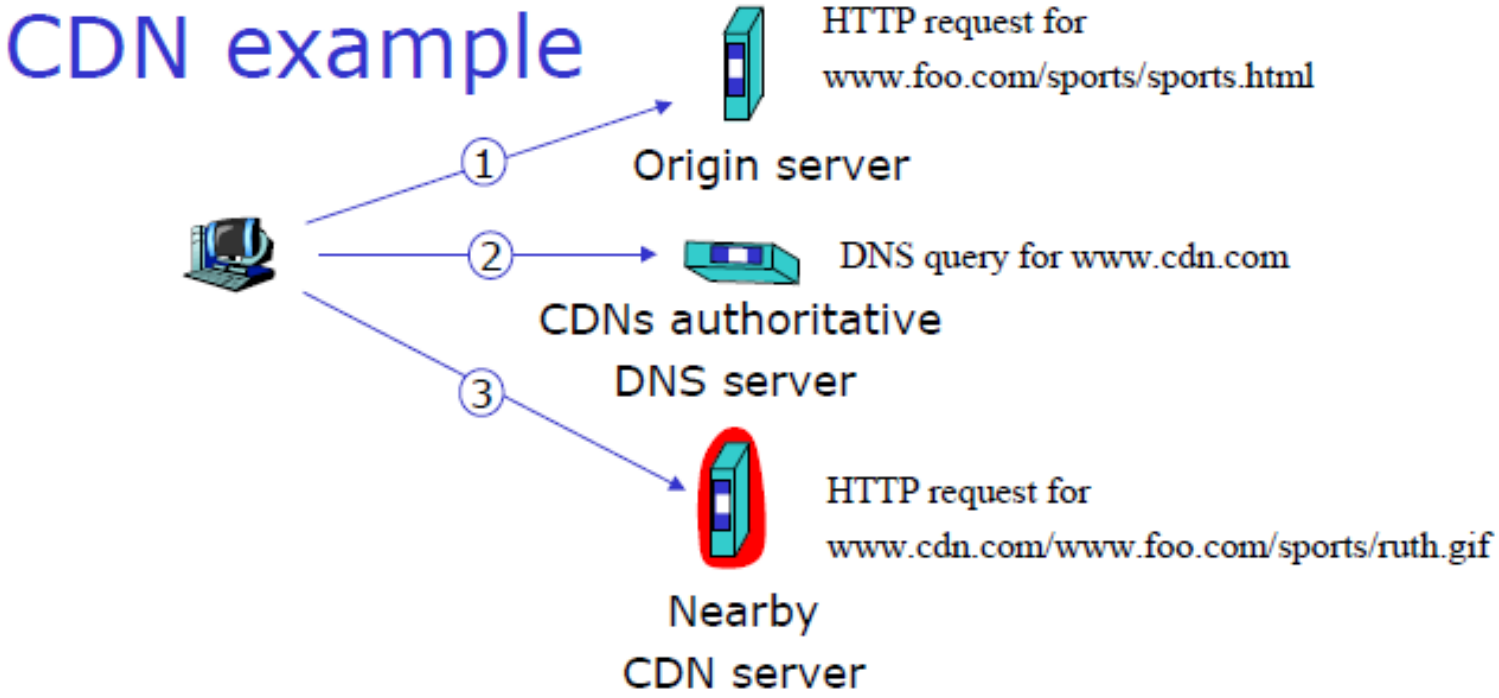
- Last-modified:
  - When the object was last modified at the origin server.
  - < Date of client's copy => OK to use copy
  - Date – Last-modified suggests frequency of change
- Date: When the object was sent by the origin server
  - last time known to be fresh.
  - + Age = Reference for checking for expiry
- Expires:
  - Server's prediction of when copies should be replaced.
- Age:
  - How long the object has spent in caches

Content Distribution Networks (CDN)

- The content providers are the CDN customers.
- Content replication
  - CDN company installs hundreds of CDN servers throughout Internet
    - in lower-tier ISPs, close to users
  - CDN replicates its customers' content in CDN servers. When provider updates content, CDN updates servers



Content Distribution Networks (CDN)



- Origin server
  - www.foo.com
  - distributes HTML
- Replaces:
  - http://www.foo.com/sports.ruth.gif

with

- http://www.cdn.com/www.foo.com/sports/ruth.gif

- CDN company
  - cdn.com
  - distributes gif files
  - uses its authoritative DNS server to route
  - redirect requests

Content Distribution Network (CDN)

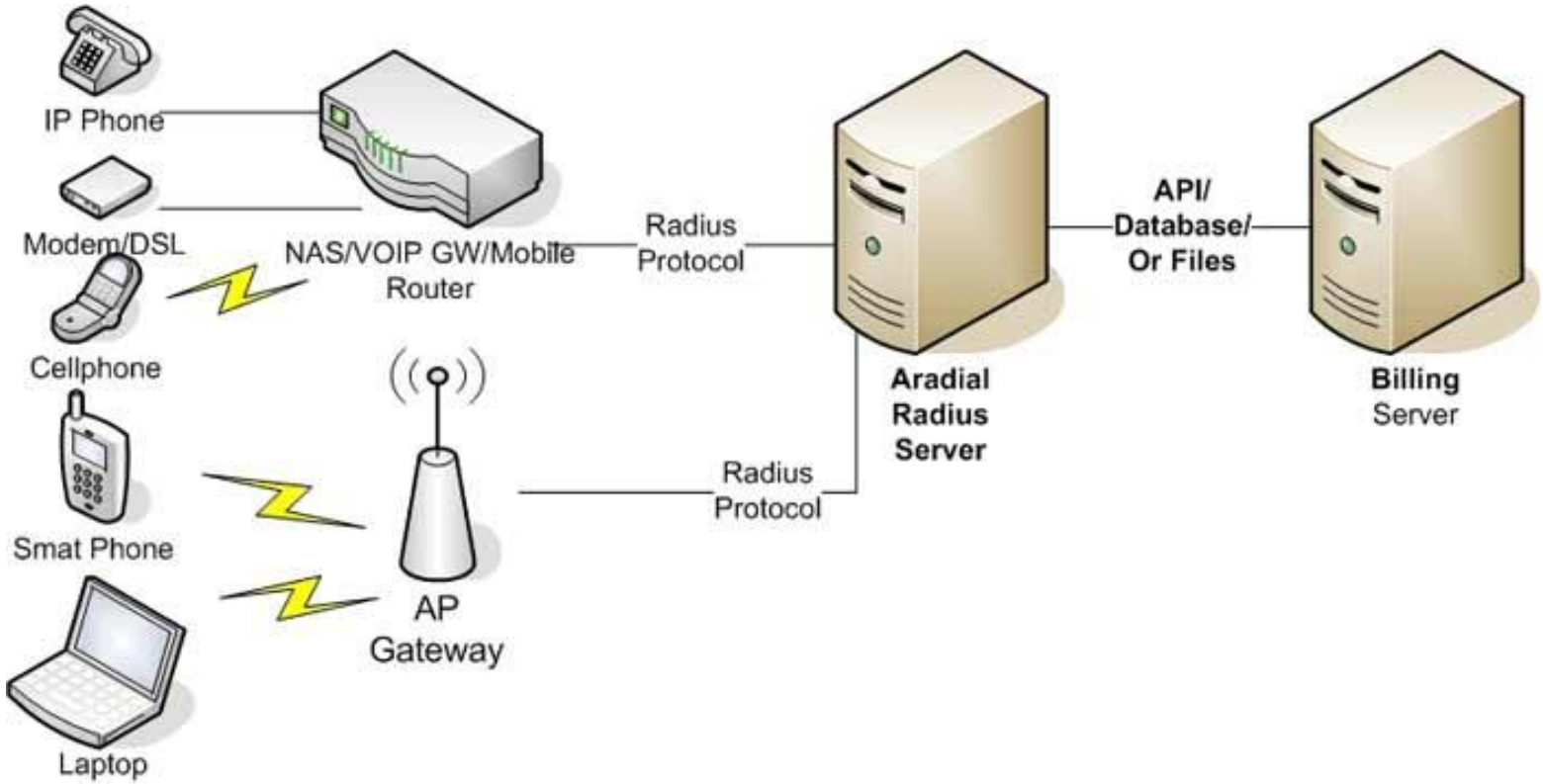
- routing requests
  - CDN creates a “map”, indicating distances from leaf ISPs and CDN nodes
  - when query arrives at authoritative DNS server:
    - server determine ISP from which query originates
    - uses “map” to determine best CDN server
  - not just Web pages
    - streaming stored audio/video
    - streaming real-time audio/video
  - CDN nodes create application-layer overlay network

RADIUS (Remote Authentication Dial In User Service)

- Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.
- RADIUS was developed by Livingston Enterprises, Inc., in 1991 as an access server authentication and accounting protocol and later brought in network.
- Because of the broad support and the universal nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services.
- These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.to the Internet Engineering Task Force (IETF) standards.

RADIUS

- RADIUS serves three functions:
  - to authenticate users or devices before granting them access to a network,
  - to authorize those users or devices for certain network services and
  - to account for usage of those services.



RADIUS

- Authentication:
  - Verify the user is who he/she claims to be
    - Use Password, Special Token card, Caller-ID, etc.
    - May issue additional ‘challenge’
- Authorization
  - Check that the user may access the services he/she wishes.
  - Check database or file information about the user
- Accounting
  - Record what the user has done.
    - Time online, Bytes sent/received, Services accessed, Files downloaded etc.

RADIUS

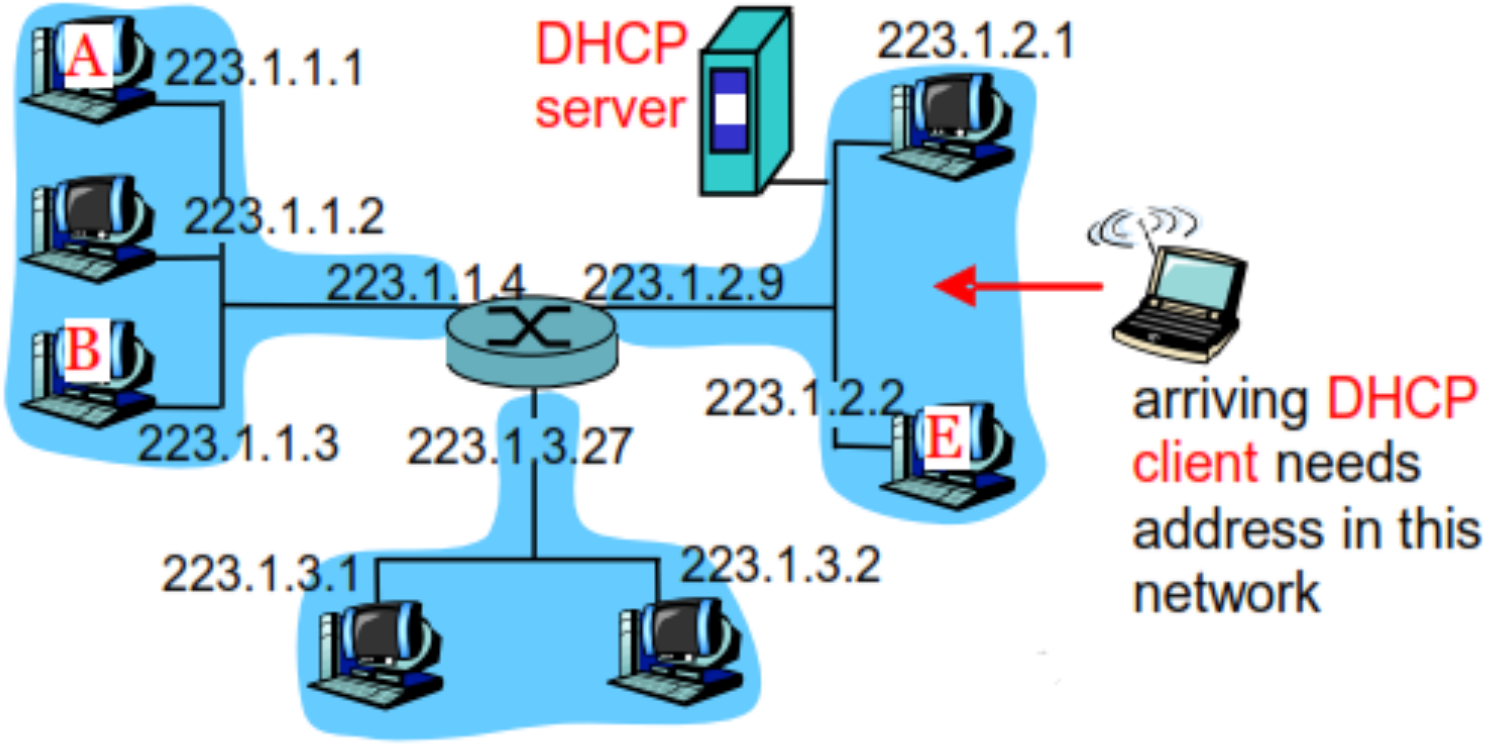
- Port number used by RADIUS
  - RADIUS has been officially assigned UDP ports 1812 for RADIUS Authentication and 1813 for RADIUS Accounting by the Internet Assigned Numbers Authority (IANA). However, prior to IANA allocation of ports 1812 and 1813, ports 1645 and 1646 (authentication and accounting).

DHCP Server

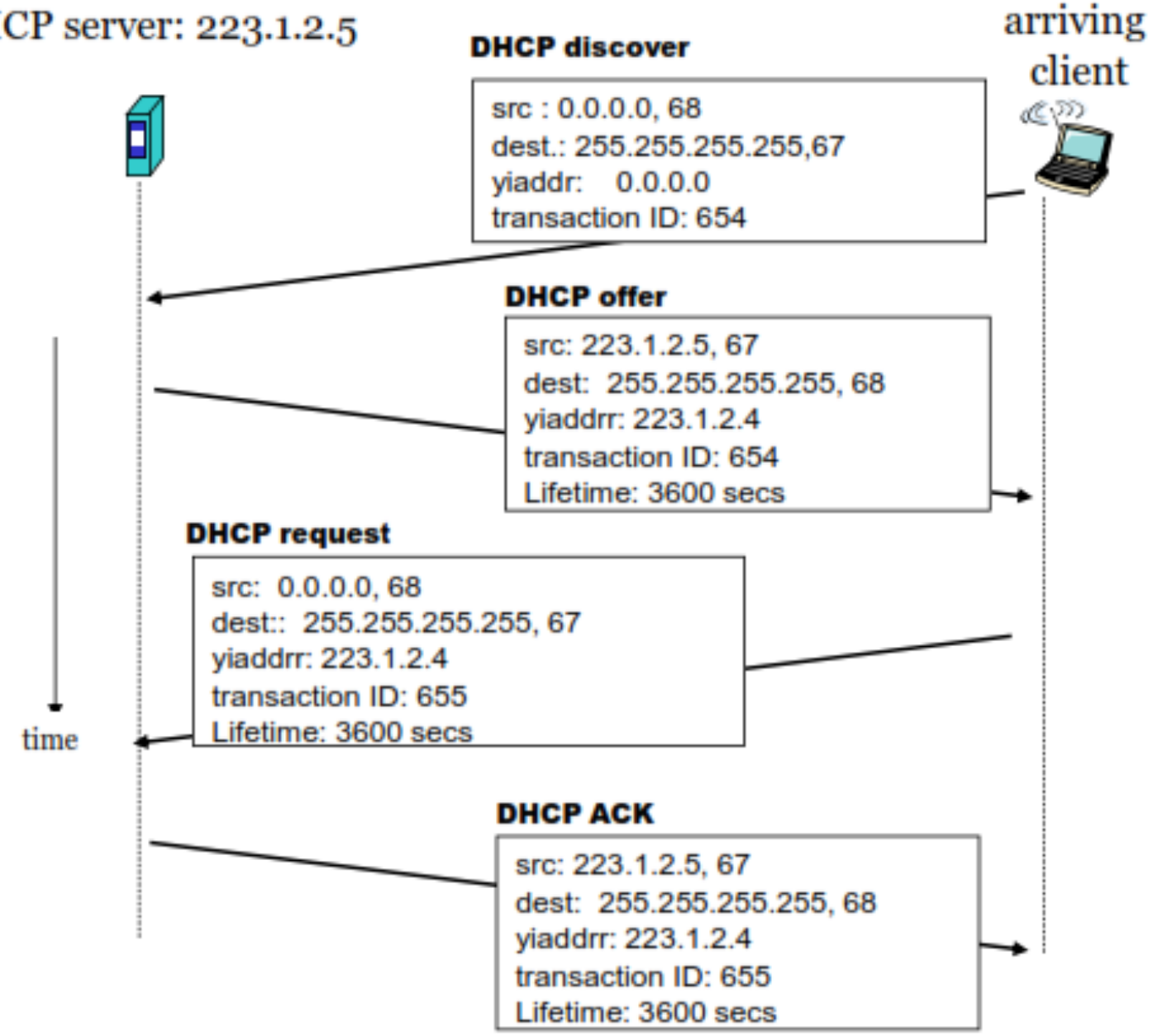
- How does a host get IP address?
  - hard-coded by system admin in a file
    - Windows: control-panel>network->configuration->tcp/ip->properties
    - UNIX: /etc/rc.config
  - DHCP: Dynamic Host Configuration Protocol: dynamically get address from a server
    - “plug-and-play”
- Goal: allow host to dynamically obtain its IP address from network server when it joins network
  - Can renew its lease on address in use
  - Allows reuse of addresses (only hold address while connected an “on”)
  - Support for mobile users who want to join network (more shortly)

DHCP

- host broadcasts “DHCP discover” msg
- DHCP server responds with “DHCP offer” msg
- host requests IP address: “DHCP request” msg
- DHCP server sends address: “DHCP ack” msg

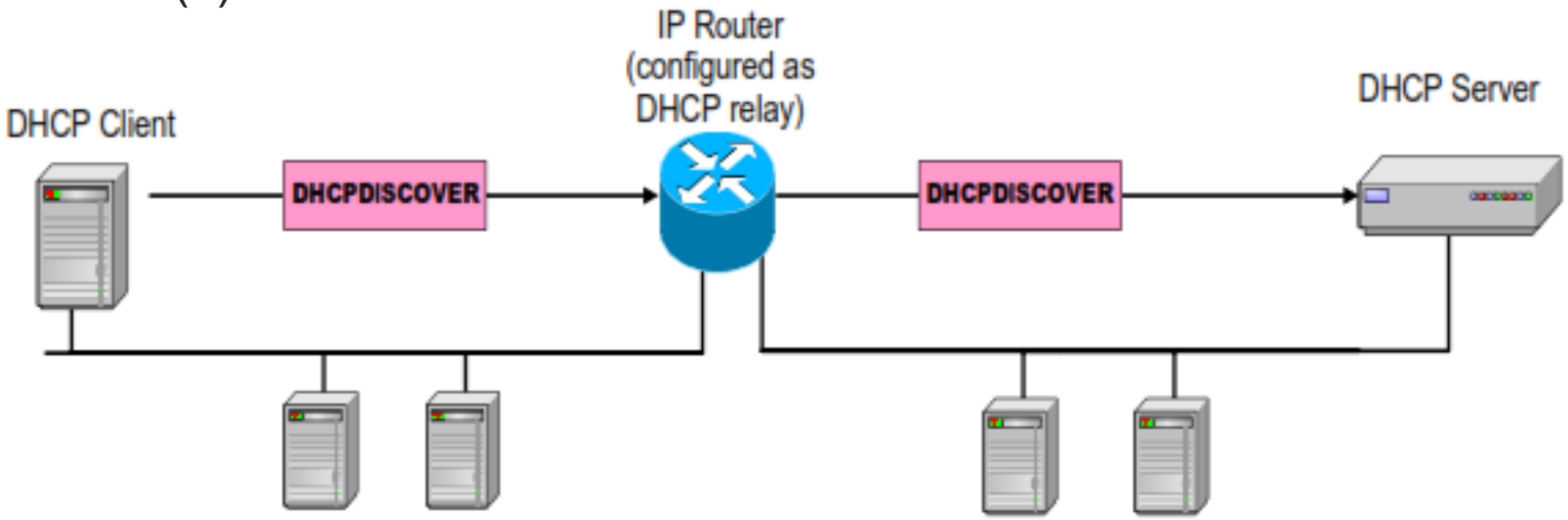


DHCP

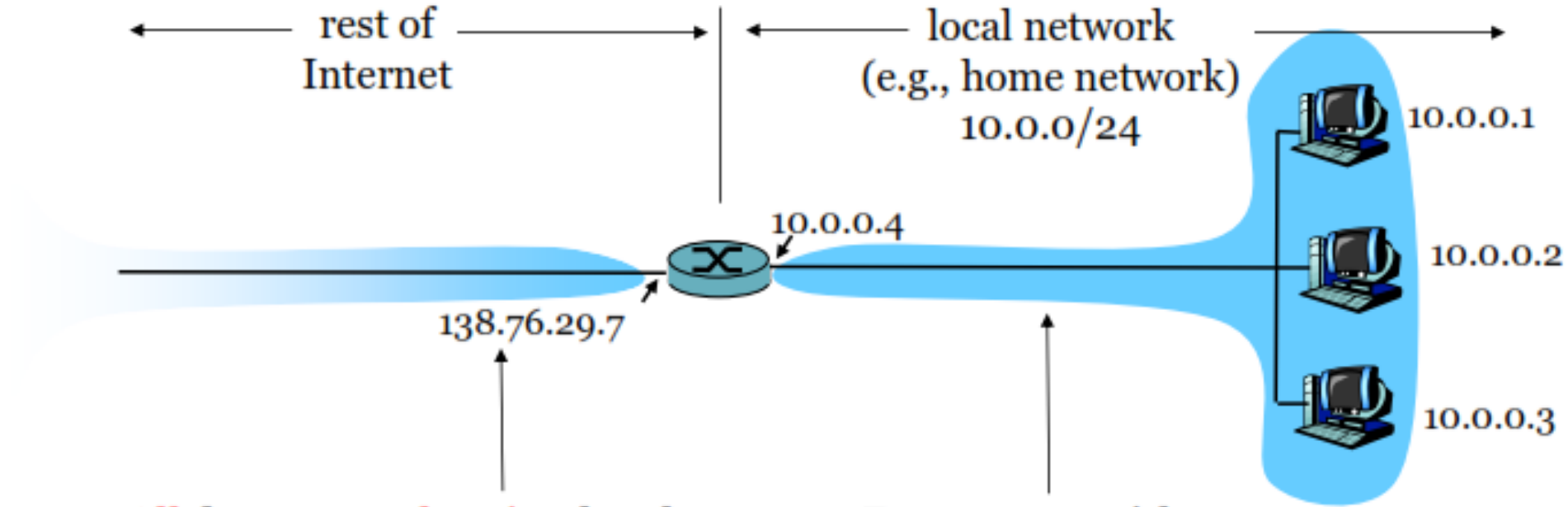

DHCP server: 223.1.2.5
arriving client
DHCP discover
src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654
DHCP offer
src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 654
Lifetime: 3600 secs
DHCP request
src: 0.0.0.0, 68
dest:: 255.255.255.255, 67
yiaddrr: 223.1.2.4
transaction ID: 655
Lifetime: 3600 secs
time
DHCP ACK
src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 655
Lifetime: 3600 secs

DHCP Relay Agent

- Problem: DHCP server and DHCP client are not on the same IP subnet.
- Destination address 255.255.255.255 is not forwarded by IP router.
- DHCP relay agent is a proxy that forwards DHCP requests to a DCHP server.
- DHCP relay agent is configured with IP addresses of DHCP server(s).



Network Address Translation (NAT)



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)

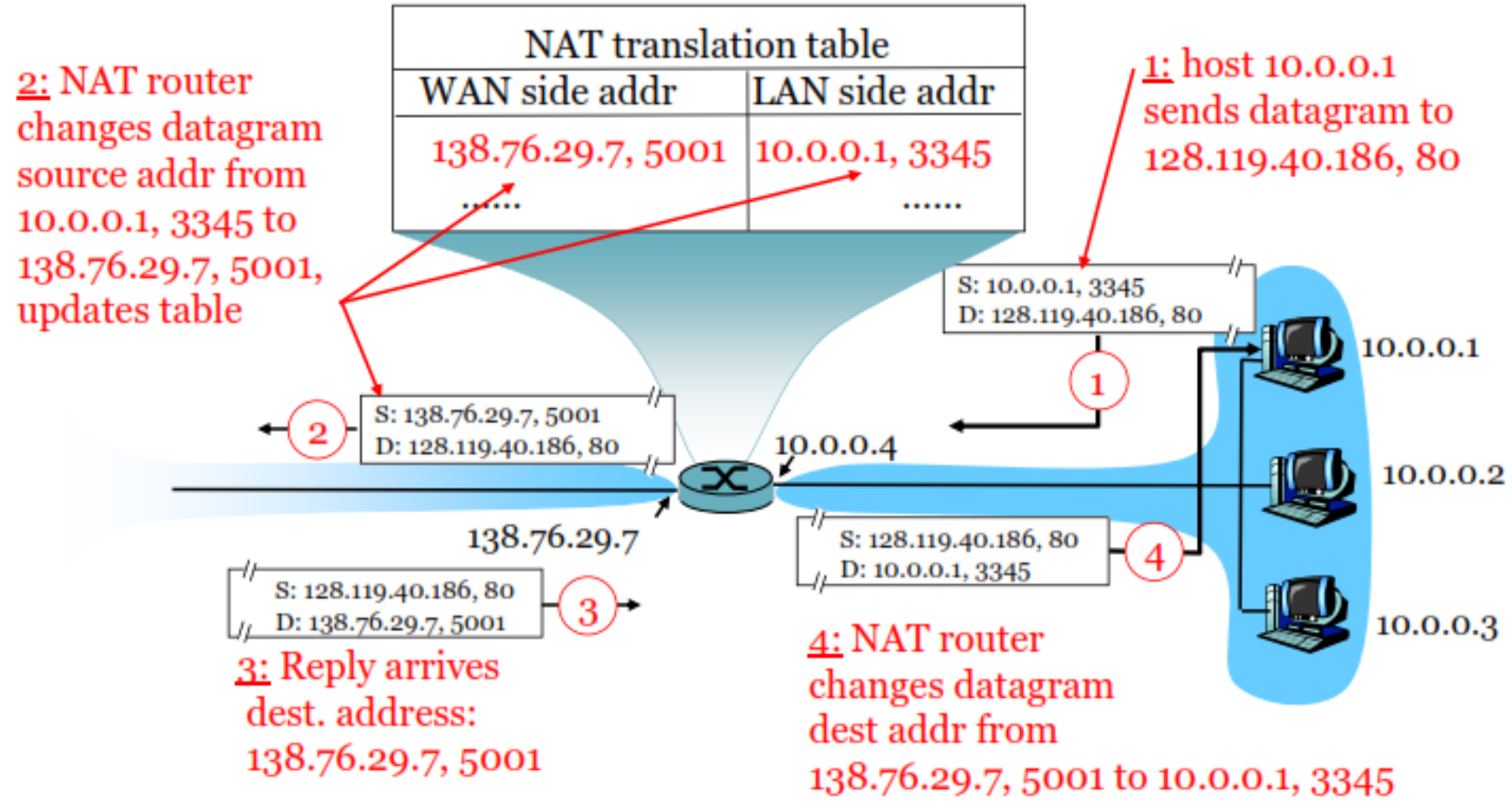
Network Address Translation (NAT)

- 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 network not explicitly addressable, visible by outside world (a security plus).

Network Address Translation (NAT)

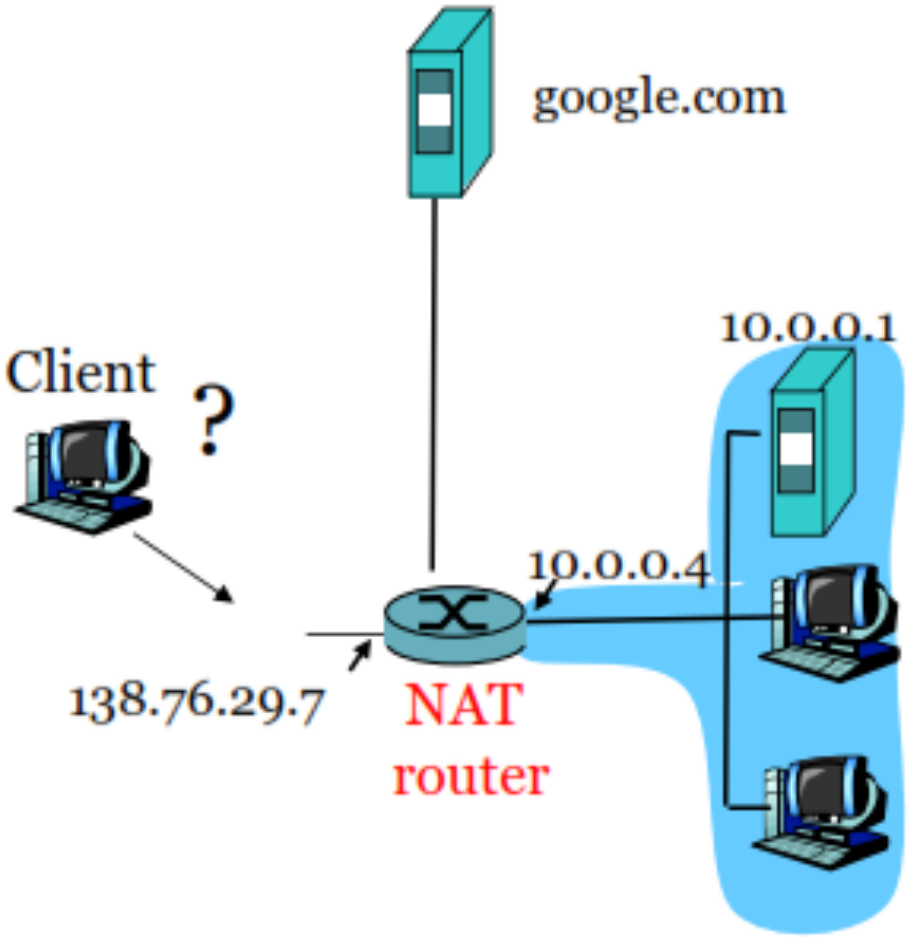
- Implementation: NAT router must:
  - *outgoing datagrams*: replace (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
    - . . . remote clients/servers will respond using (NAT IP address, new port #) as destination address.
  - remember (in NAT translation table) every (source IP address, port #) to (NAT IP address, new port #) translation pair
  - *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

Network Address Translation (NAT)

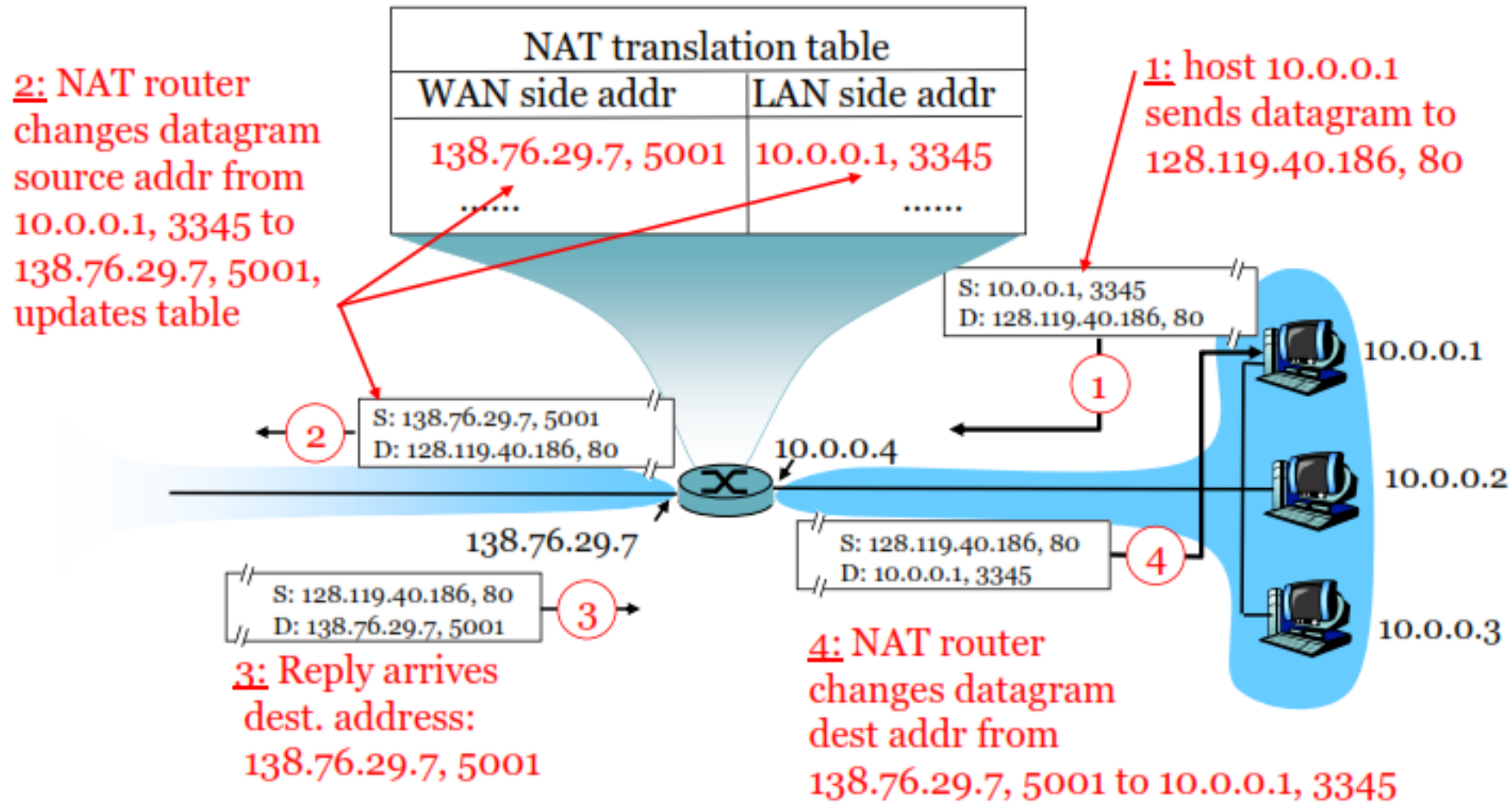


NAT Types

- Source NAT
- Destination NAT

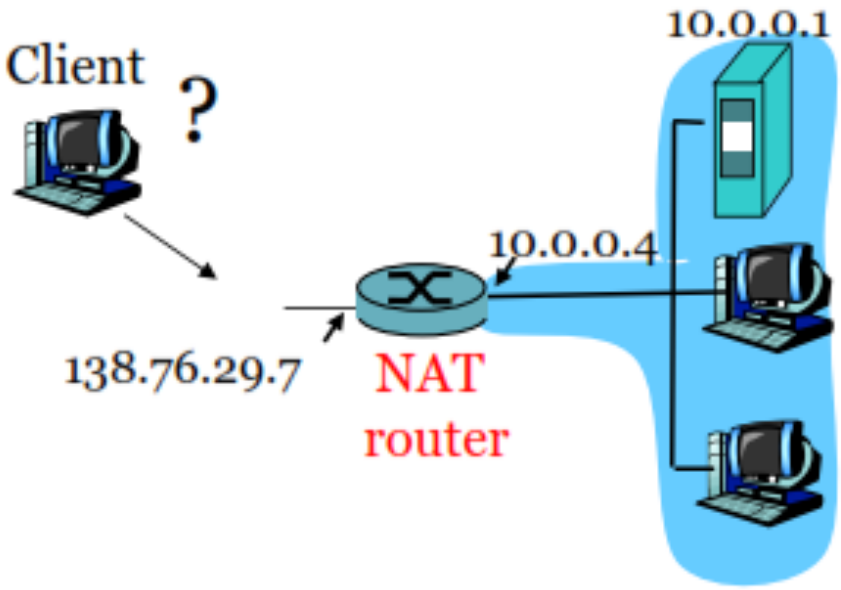


SNAT


NAT translation table
WAN side addr
LAN side addr
138.76.29.7, 5001
10.0.0.1, 3345
.....
.....
2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table
1: host 10.0.0.1 sends datagram to 128.119.40.186, 80
S: 10.0.0.1, 3345
D: 128.119.40.186, 80
1
10.0.0.1
10.0.0.2
10.0.0.3
10.0.0.4
2
S: 138.76.29.7, 5001
D: 128.119.40.186, 80
138.76.29.7
S: 128.119.40.186, 80
D: 10.0.0.1, 3345
4
S: 128.119.40.186, 80
D: 138.76.29.7, 5001
3
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

DNAT

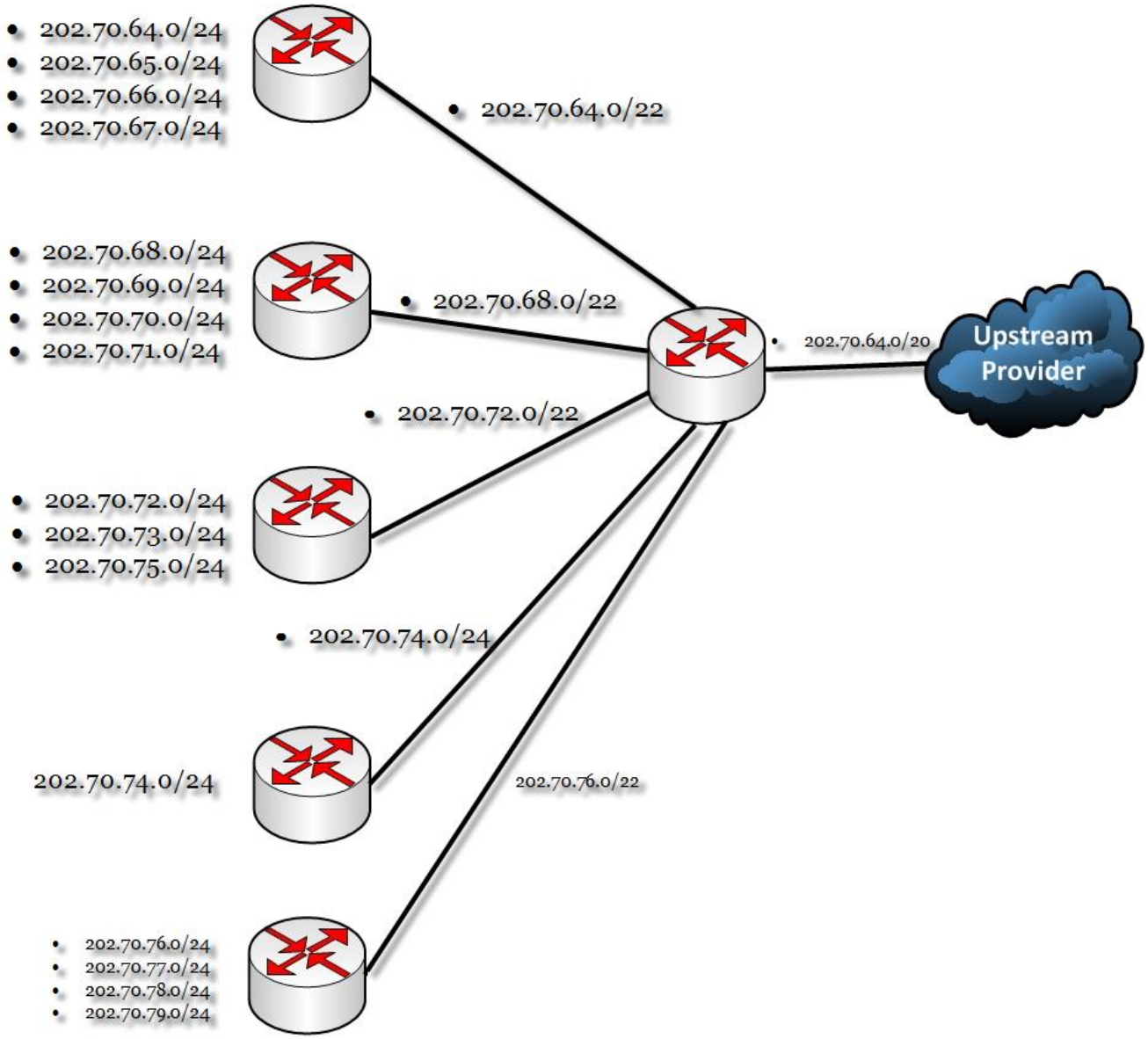
- DNAT is commonly used to publish a service located in a private network on a publicly accessible IP address.
- client wants to connect to server with address 10.0.0.1
  - server address 10.0.0.1 local to LAN (client can't use it as destination address)
  - only one externally visible NATted address: 138.76.29.7
- solution 1: statically configure NAT to forward incoming connection requests at given port to server
  - e.g., (138.76.29.7, port 80) always forwarded to 10.0.0.1 port 80



Route Aggregation

- VLSM allows an organization to use more than one subnet mask within the same network address space.
- VLSM implementation maximizes address efficiency and is often referred to as subnetting a subnet.
- Classfull routing protocols require that a single network use the same subnet mask.
- Routing protocols that allows VLSM gives the network administrator freedom to use different subnet masks for network within a single AS.
- When VLSM is used, it is important to keep the sub network numbers grouped together in the network to allow for aggregation.
- The use of CIDR and VLSM prevents address waste and promotes route aggregation or route summarization.
- Without route summarization, internet backbone routing would likely have collapsed.

Route Aggregation



Route Aggregation

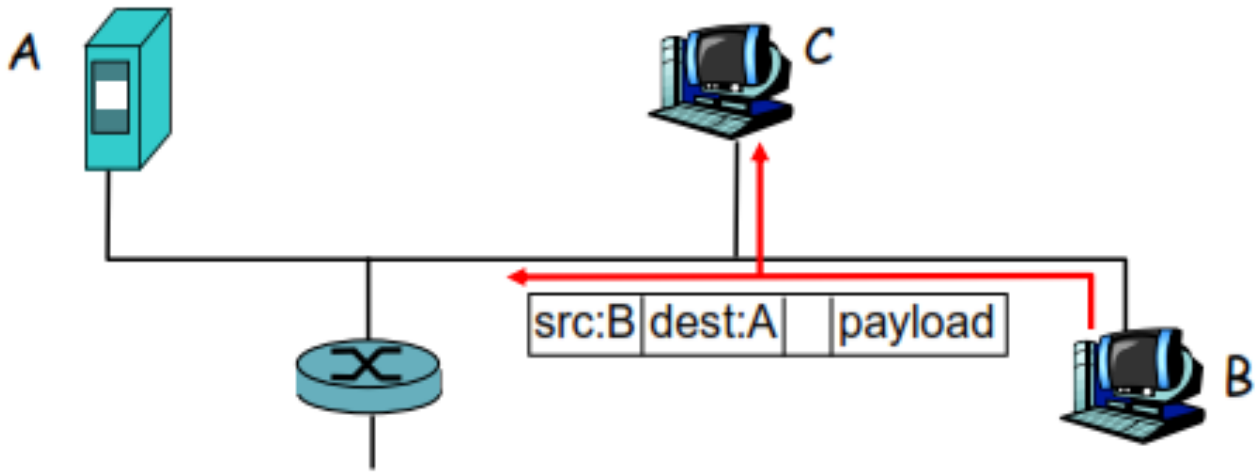
- If we don't have a route summarization technique then each and every IP should be forwarded to the Main ISPs, forwarding it to the main ISP may take time as well as Main ISPs have to maintain huge database.
- So IP address should be carefully assigned in a hierarchical fashion so that summarized address will share the same high order bits.

Internet Security Threat

- Mapping:
  - before attacking: “case the joint” – find out what services are implemented on network
  - Use *ping* to determine what hosts have addresses on network
  - Port-scanning: try to establish TCP connection to each port in sequence (see what happens)
  - nmap (http://www.insecure.org/nmap/) mapper: “network exploration and security auditing”
- Mapping: countermeasures
  - record traffic entering network
  - look for suspicious activity (IP addresses, ports being scanned sequentially)

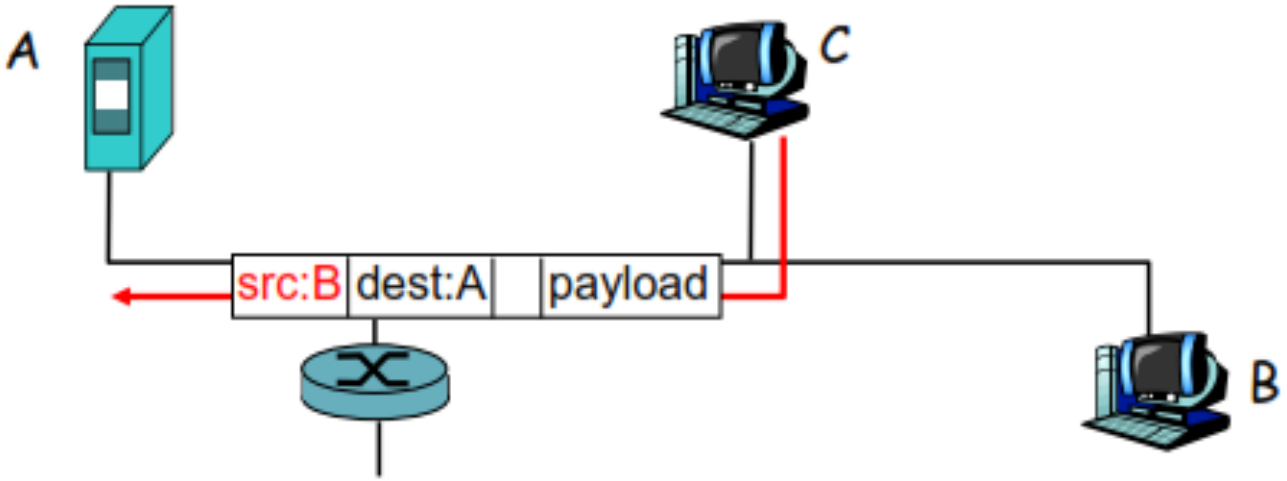
Internet Security Threat

- Packet sniffing:
  - broadcast media
  - promiscuous NIC reads all packets passing by
  - can read all unencrypted data (e.g. passwords)
    - e.g.: C sniffs B's packets
- Packet sniffing: countermeasures
  - all hosts in organization run software that checks periodically if host interface in promiscuous mode.
  - one host per segment of broadcast media (switched Ethernet at hub)



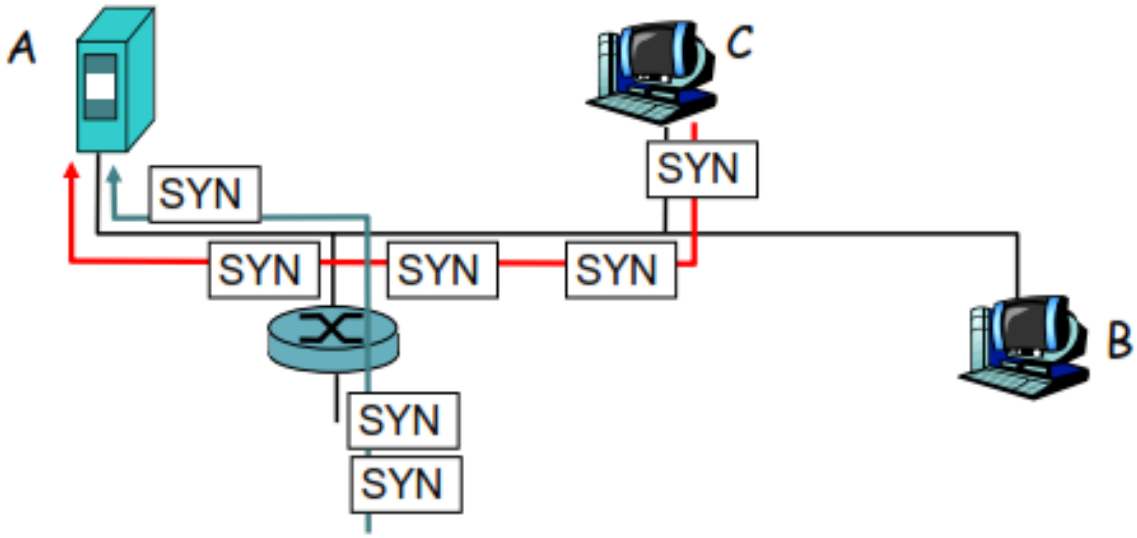
Internet Security Threat

- IP Spoofing:
  - can generate “raw” IP packets directly from application, putting any value into IP source address field
  - receiver can’t tell if source is spoofed
    - e.g.: C pretends to be B
- IP Spoofing: ingress filtering
  - routers should not forward outgoing packets with invalid source addresses (e.g., datagram source address not in router’s network)
  - great, but ingress filtering can not be mandated for all networks



Internet Security Threat

- Denial of service (DOS):
  - flood of maliciously generated packets “swamp” receiver
  - *Distributed DOS (DDOS)*: multiple coordinated sources swamp receiver
    - e.g., C and remote host SYN-attack A
- Denial of service (DOS): countermeasures
  - filter out flooded packets (e.g., SYN) before reaching host: throw out good with bad
  - traceback to source of floods (most likely an innocent, compromised machine)

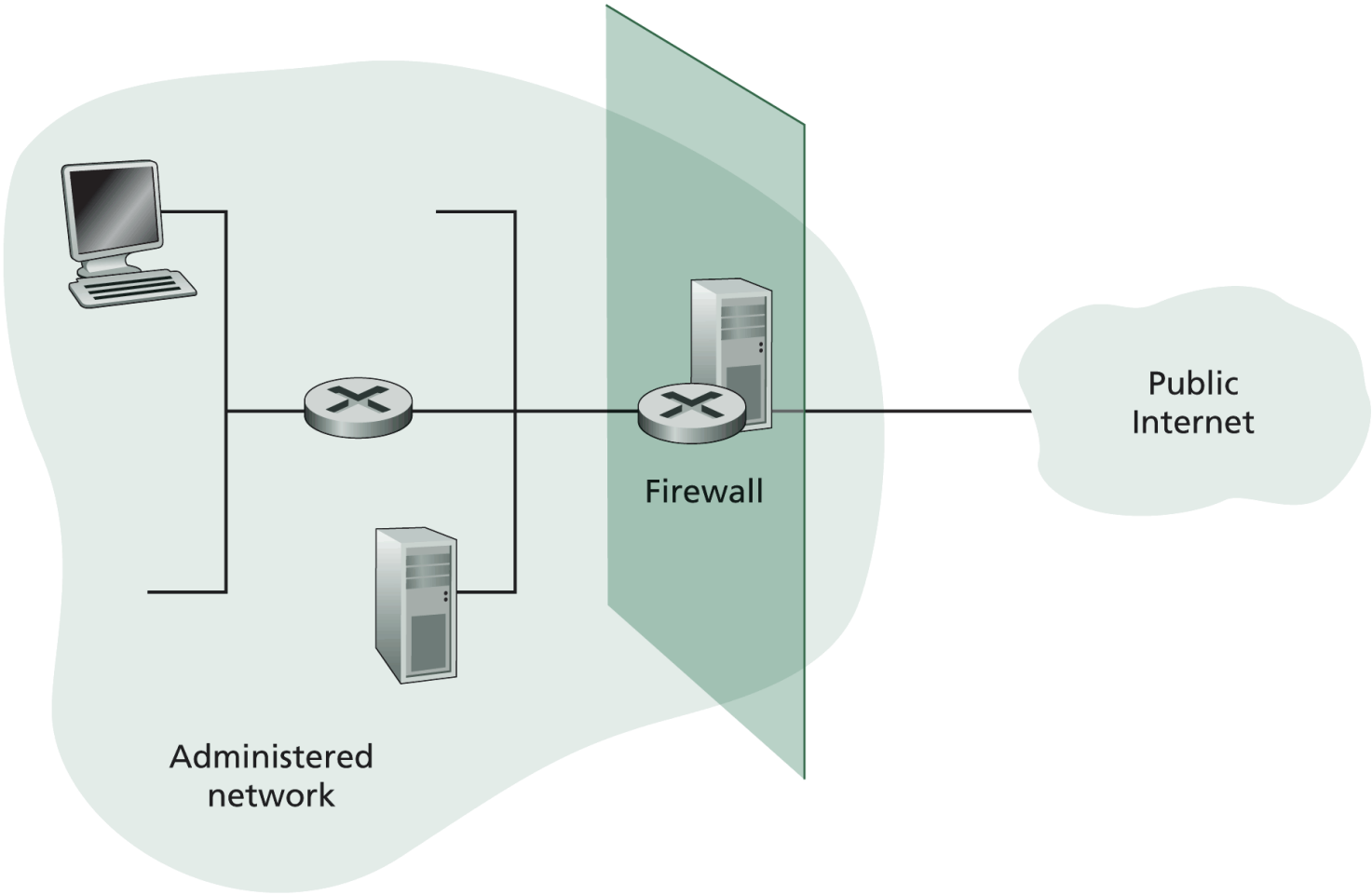


Firewall

- A firewall is a combination of hardware and software that isolates an organization's internal network from the Internet at large, allowing specific connections to pass and blocking others.
- Organizations employ firewalls for one or more of the following reasons:
  - To prevent intruders from interfering with the daily operation of the internal network.
    - denial of service attack, SYN FIN Attack
  - To prevent intruders from deleting or modifying information stored within the internal network.
  - To prevent intruders from obtaining secret information.

Firewall Types

- Packet Filtering
- Application Level Gateway



Packet Filtering

- Filtering Based on
  - Source/Destination IP address.
  - TCP or UDP source and destination port.
  - ICMP message type.
  - Connection initialization datagrams using the TCP ACK bit

Application Level Gateway

- In order to have a finer level security, firewalls must combine packet filters with application gateways.
- Application gateways look beyond the IP/TCP/UDP headers and actually make policy decisions based on application data.
- An application gateway is an application-specific server through which all application data (inbound and outbound) must pass.
- Multiple application gateways can run on the same host, but each gateway is a separate server with its own processes.

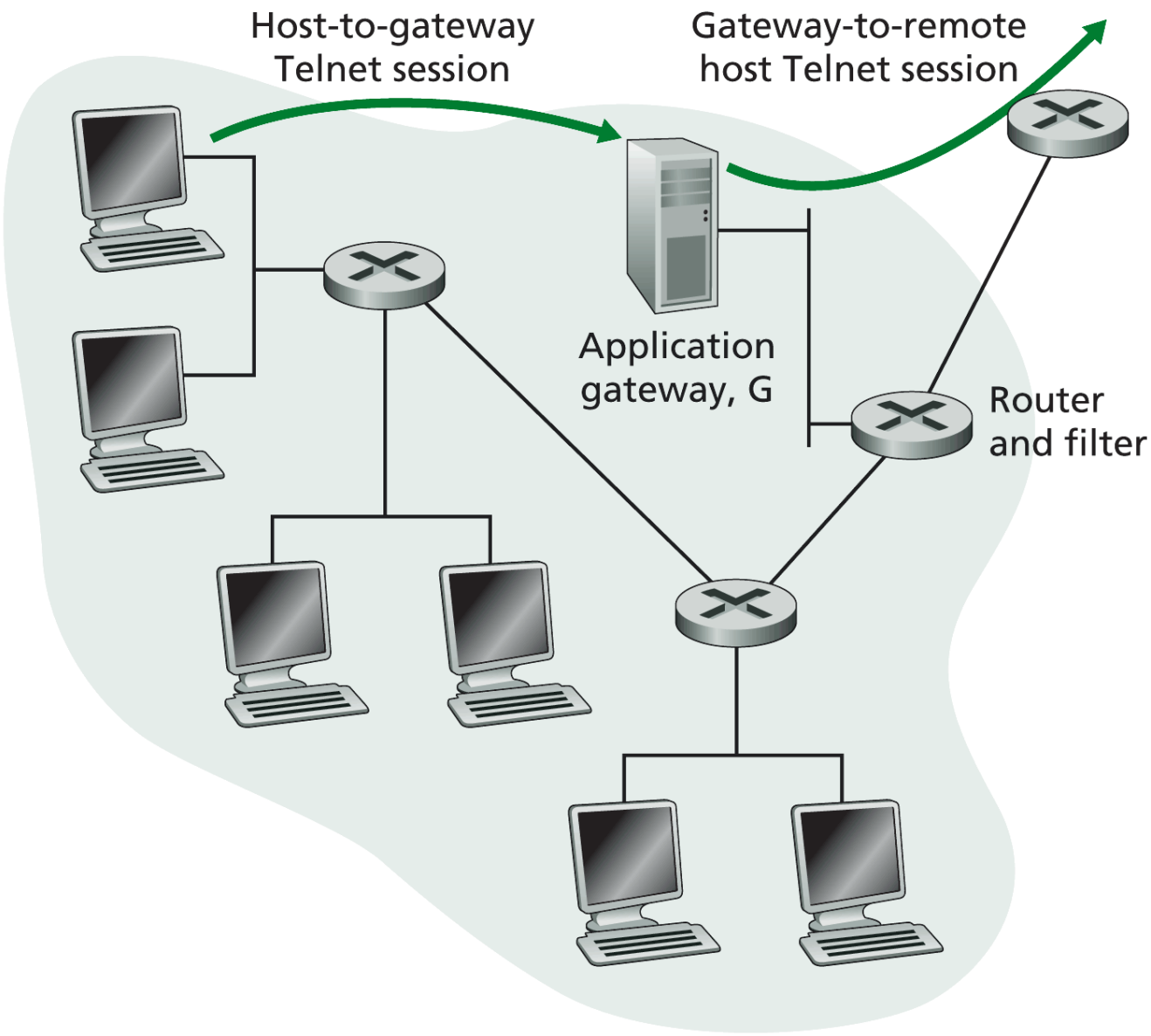
Application Level Gateway

- Design a firewall that allows only a restricted set of internal users to Telnet outside and prevents all external clients from Telneting inside.
- Such a policy can be accomplished by implementing a combination of a packet filter (in a router) and a Telnet application gateway.
- The filter is configured to block all Telnet connections except those that originate form the IP address of the application gateway.
- Such a filter configuration forces all outbound Telnet connections to pass through the application gateway.
- When a internal user wants to Telnet to the outside world, it first sets up a Telnet session with the gateway.
- The gateway prompts Firewalls the user for its user id and password; when the user supplies this information, the gateway checks to see if the user has permission to Telnet to the outside world.

Application Level Gateway

- If not, the gateway terminates the Telnet session.
- If the user has permission, then the gateway
  1. prompts the user for the hostname of the external host to which the user wants to connect,
  2. sets up a Telnet session between the gateway and the external host,
  3. relays to the external host all data arriving from the user, and relays to the user all data arriving from the external host.
- Thus the Telnet application gateway not only performs user authorization but also acts as a Telnet server and a Telnet client.

Application Level Gateway



Limitations of firewalls and gateways

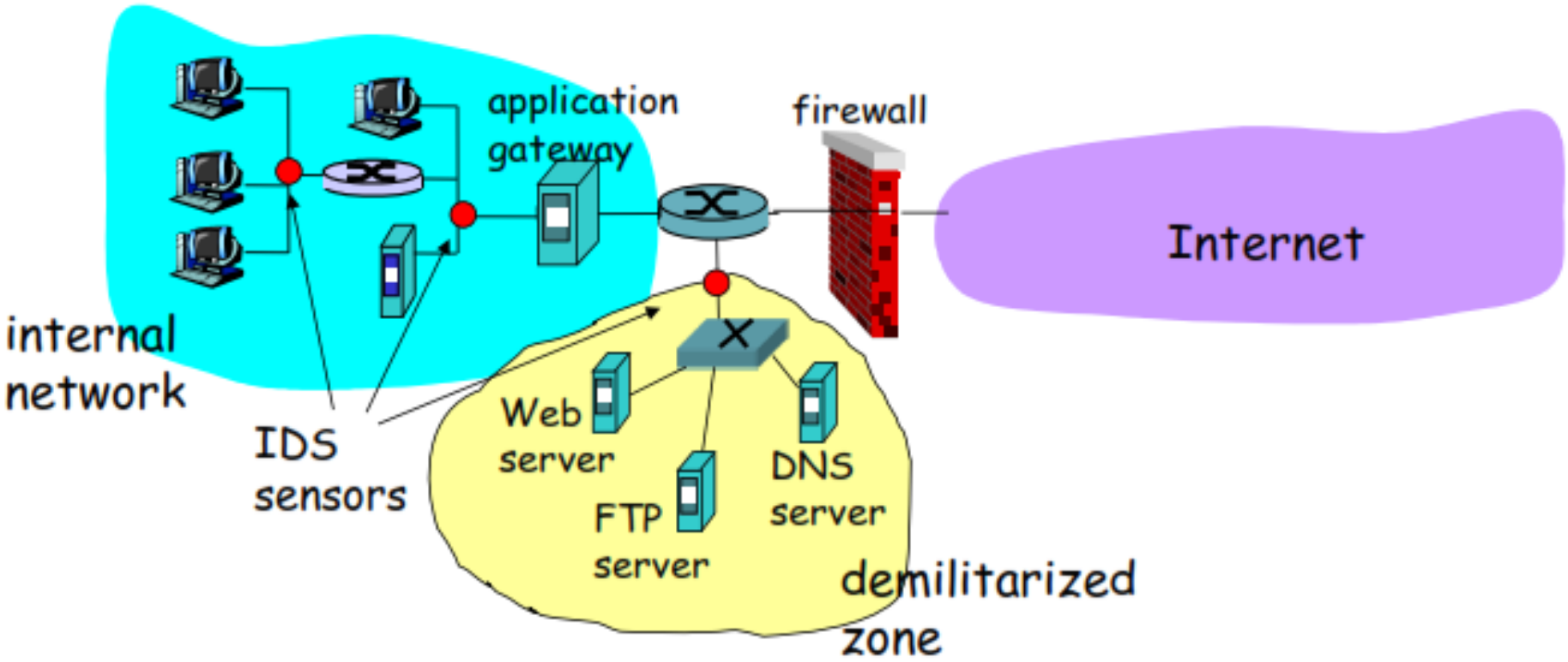
- IP spoofing: router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP.
- tradeoff: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.

Intrusion Detection Systems

- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - deep packet inspection: look at packet contents
    - (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack

Intrusion Detection Systems

- multiple IDSs: different types of checking at different locations



Intrusion Detection Systems

- Used to monitor for “suspicious activity” on a network
- Can protect against known software exploits, like buffer overflows
- Open Source IDS: Snort, www.snort.org
- Uses “intrusion signatures”
  - Well known patterns of behavior
    - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.
- Example
  - IRIX vulnerability in webdist.cgi
  - Can make a rule to drop packets containing the line
    - “/cgi-bin/webdist.cgi?distloc=?;cat%20/etc/passwd”
- However, IDS is only useful if contingency plans are in place to curb attacks as they are occurring.

Thank You !!!