Introduction to Network Management

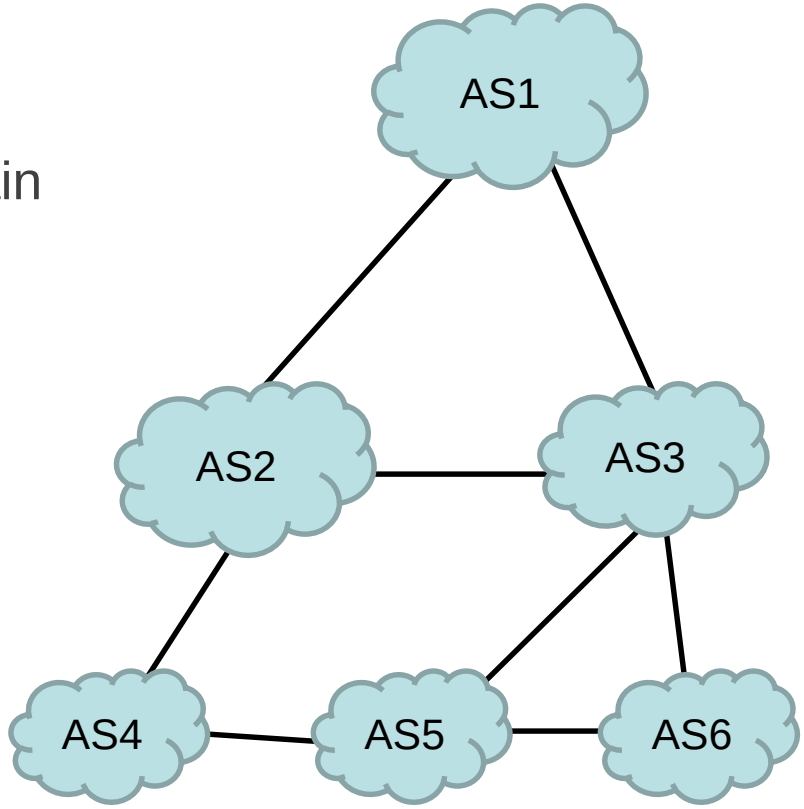
Network Management

Prof. Dr. Panagiotis Papadimitriou

Internet Structure

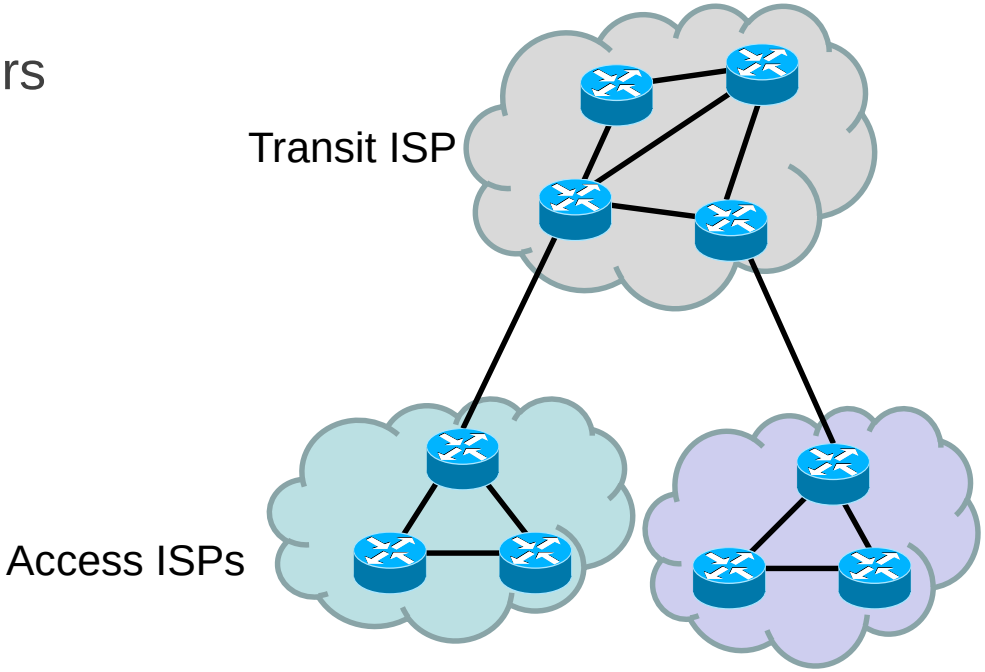
- Internet is composed of Autonomous Systems (ASes)
  - “Network of networks”

- Autonomous System (AS):
  - Independently administrative domain
  - More than 30.000 ASes
    - Internet Service Providers (ISPs)
    - Content Distribution Networks
    - Enterprise Networks
    - University Campus Networks



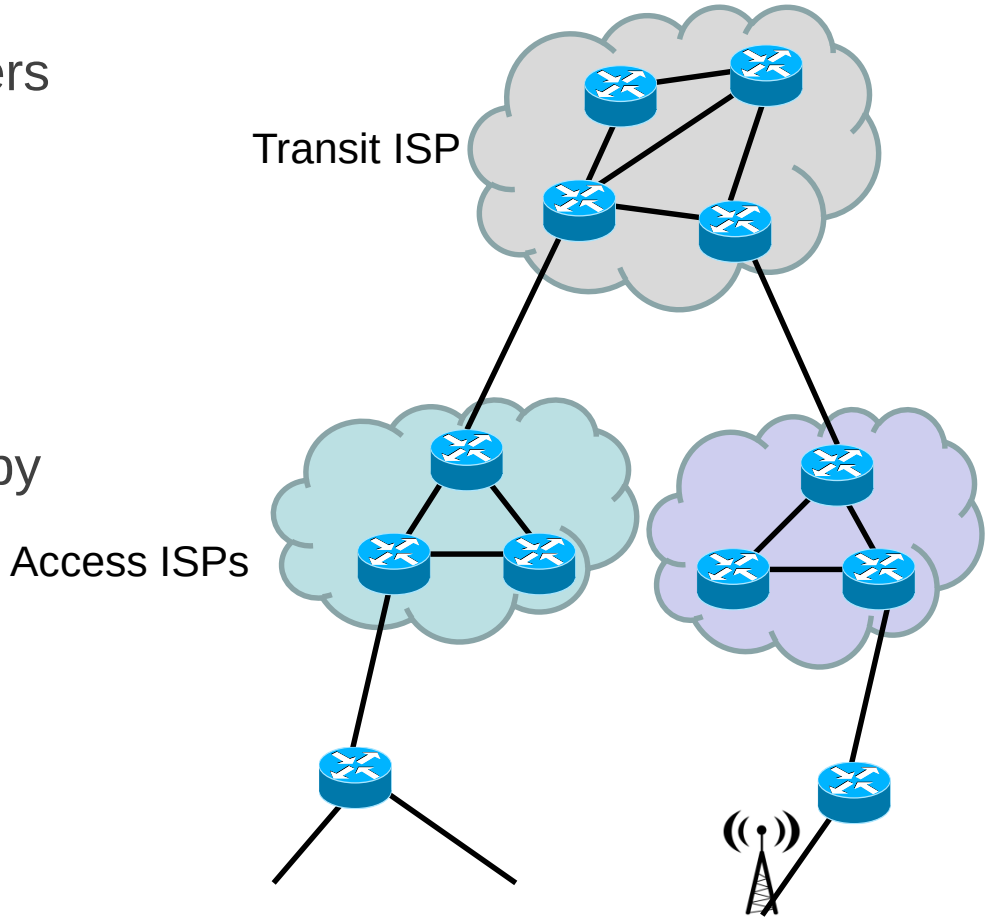
Internet Structure

- Internet Core:
  - Mesh of interconnected routers
  - Infrastructure offered by multiple ISPs



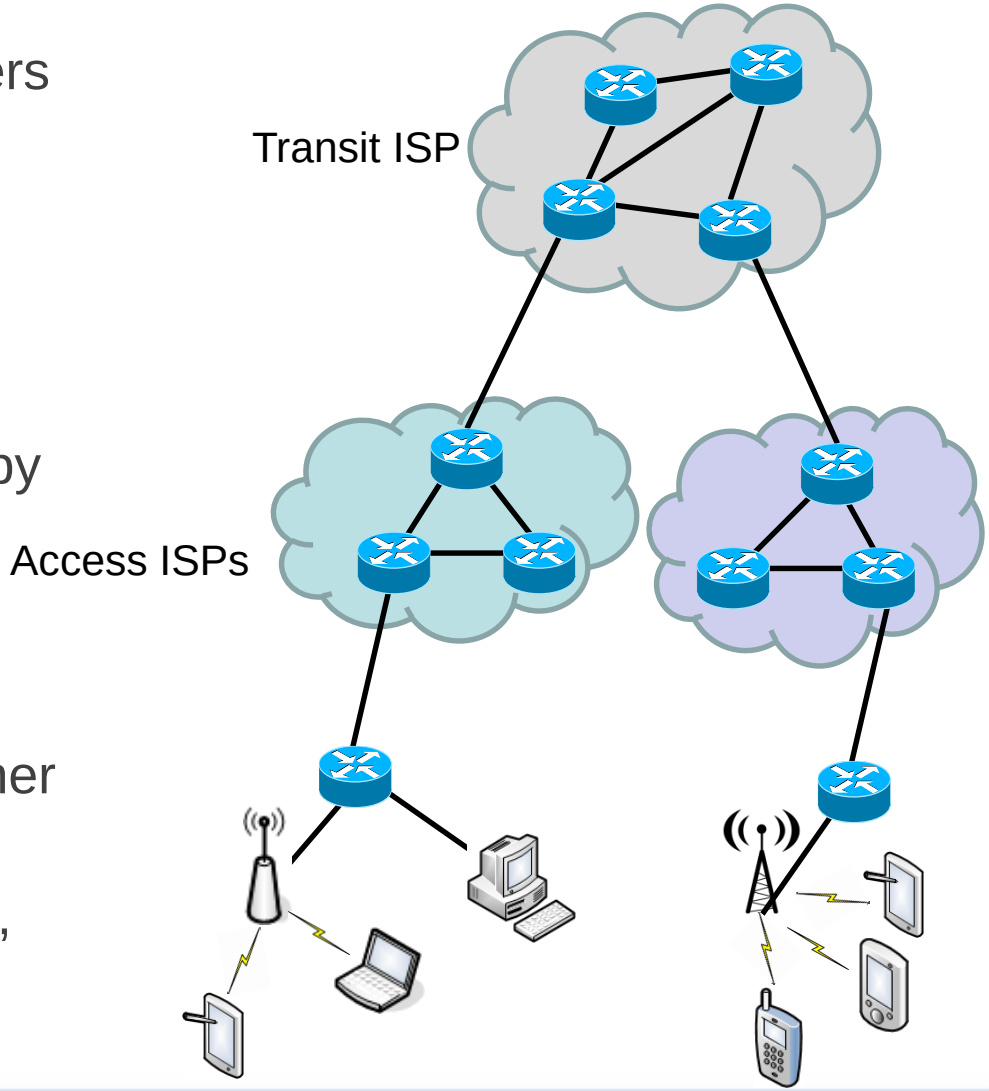
Internet Structure

- Internet Core:
  - Mesh of interconnected routers
  - Infrastructure offered by multiple ISPs
- Access Networks:
  - Connectivity service offered by ISPs or mobile operators



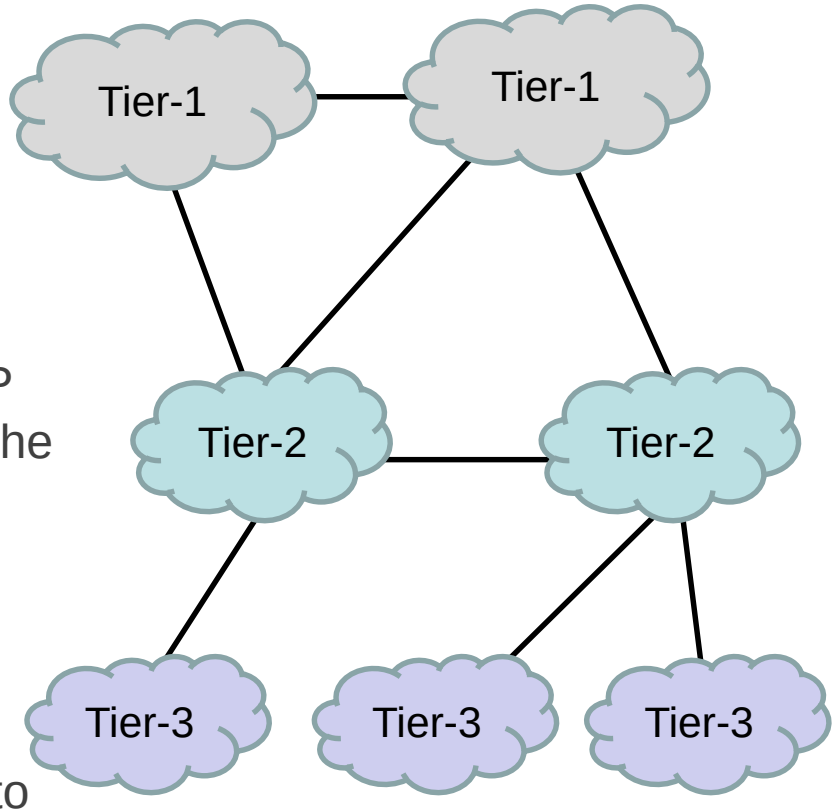
Internet Structure

- Internet Core:
  - Mesh of interconnected routers
  - Infrastructure offered by multiple ISPs
- Access Networks:
  - Connectivity service offered by ISPs or mobile operators
- End-systems:
  - Desktops, laptops, PDAs, other mobile terminals
  - Run applications (web, email, voice, video, etc.)

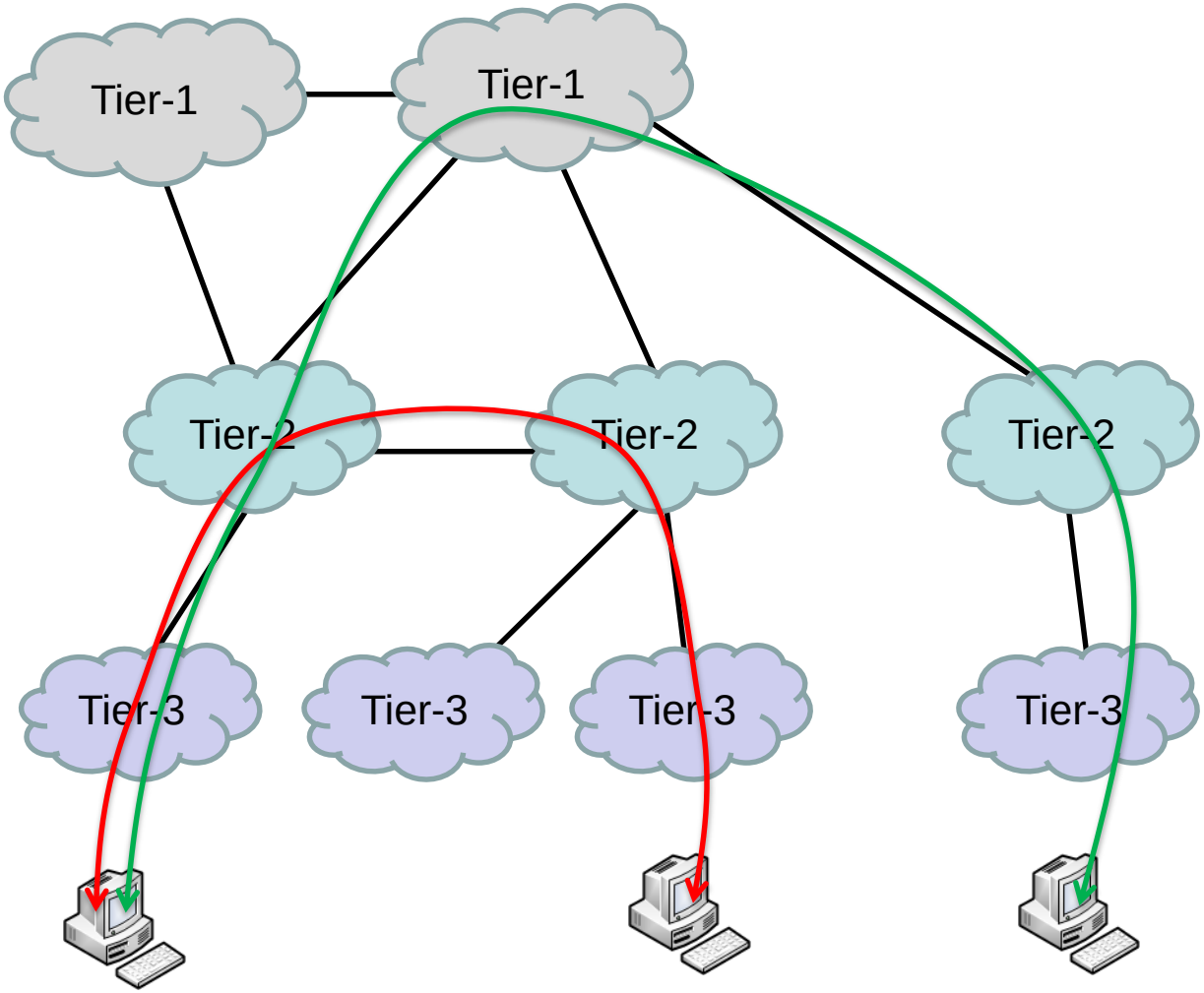


ISPs Taxonomy

- Tier-1 ISPs
  - Transit-free networks that peer with other Tier-1 ISPs
  - e.g., Sprint, Verizon, AT&T, Deutsche Telekom
- Tier-2 ISPs
  - Peer with other ISPs but still purchase IP transit to reach at least some portion of the Internet
  - Peer with at least one Tier-1 ISP
- Tier-3 ISPs
  - Solely purchase transit from other ISPs to reach the Internet
  - Peer with at least one Tier-2 ISP



Internet Paths Across Transit Providers



A Tier-1 ISP (Sprint)

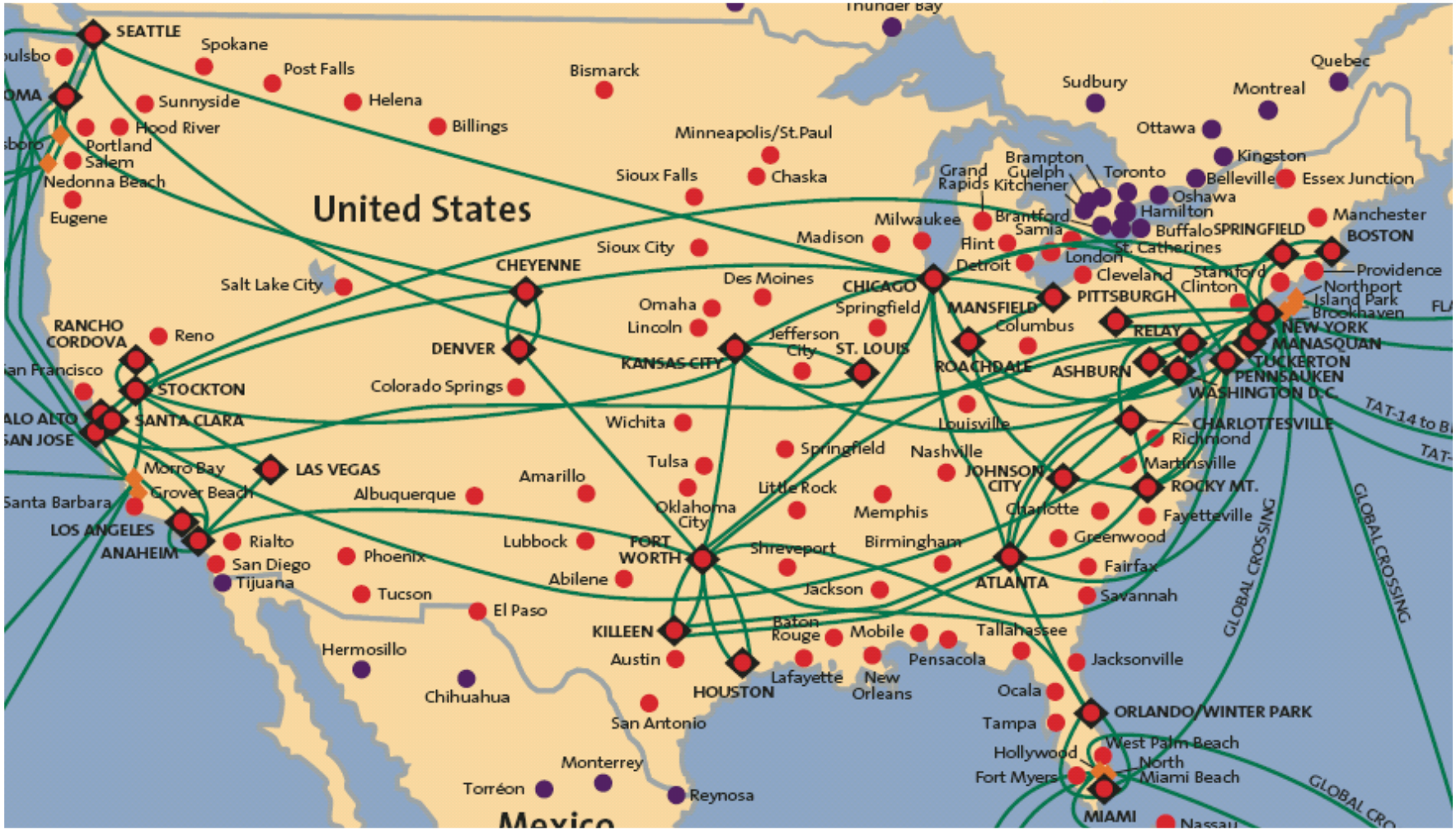
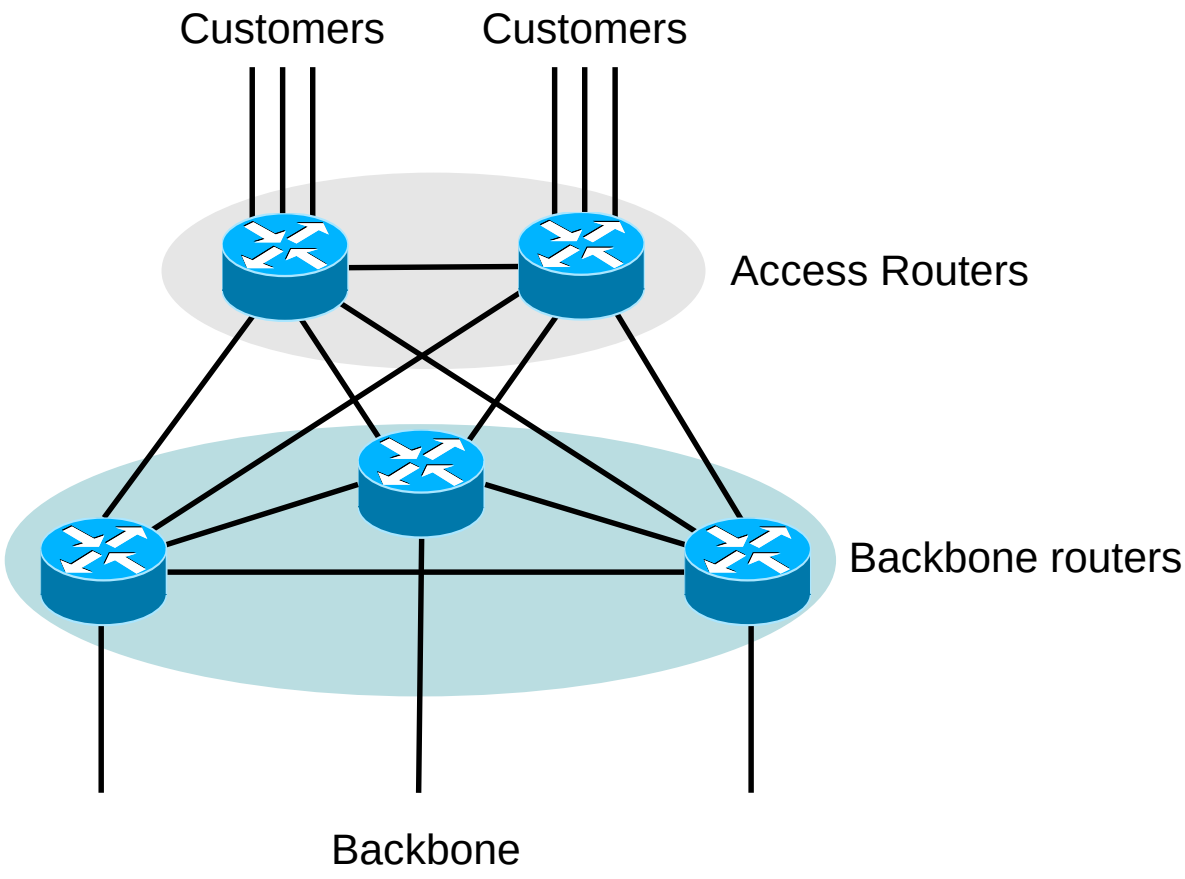


Figure from Computer Networking, A Top-Down Approach

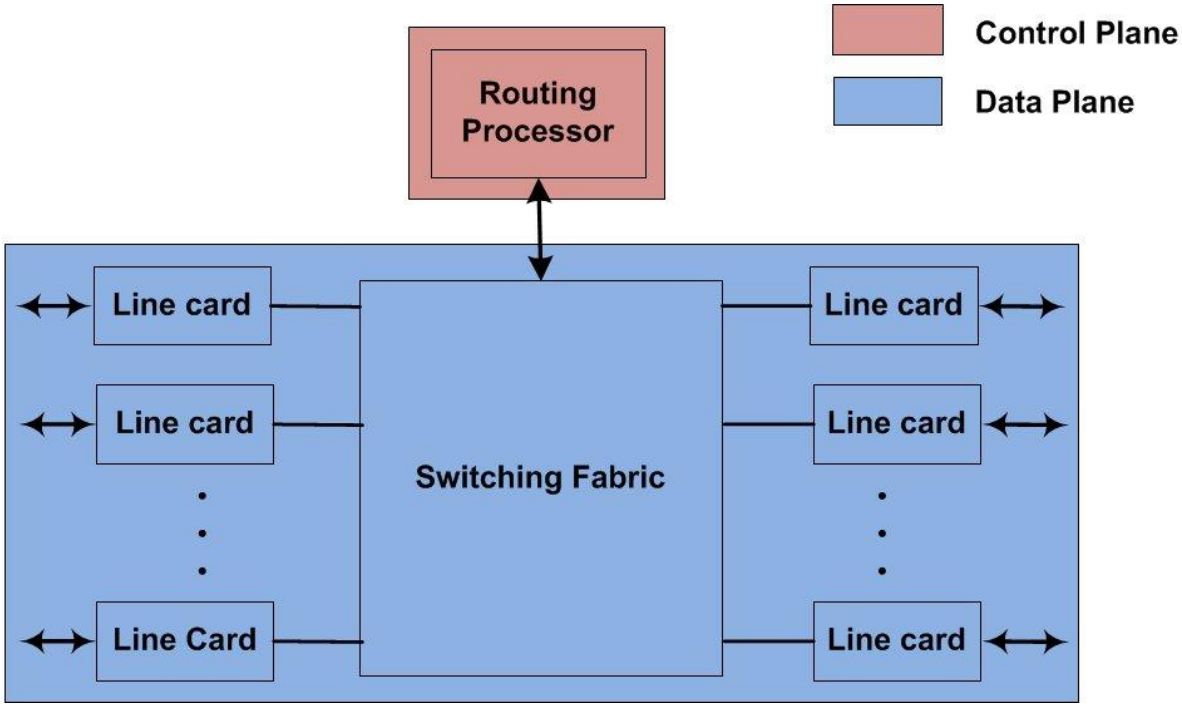
Point Of Presence (PoP)

- A Point of Presence (PoP) consists of access and backbone routers in a specific physical location (i.e., a city or large metropolitan area)



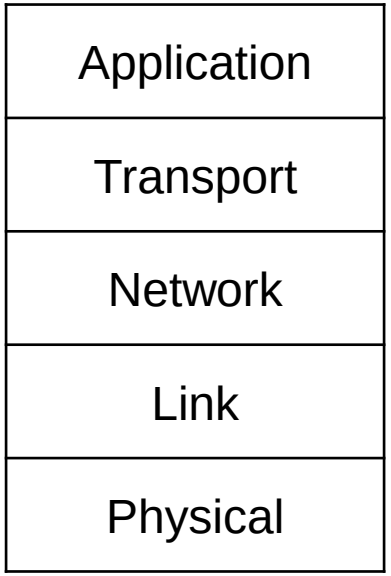
Routers

- Data plane:
  - Forwards packets from input to output (speed)
- Control plane:
  - Runs routing protocols to compute the paths that packets will follow



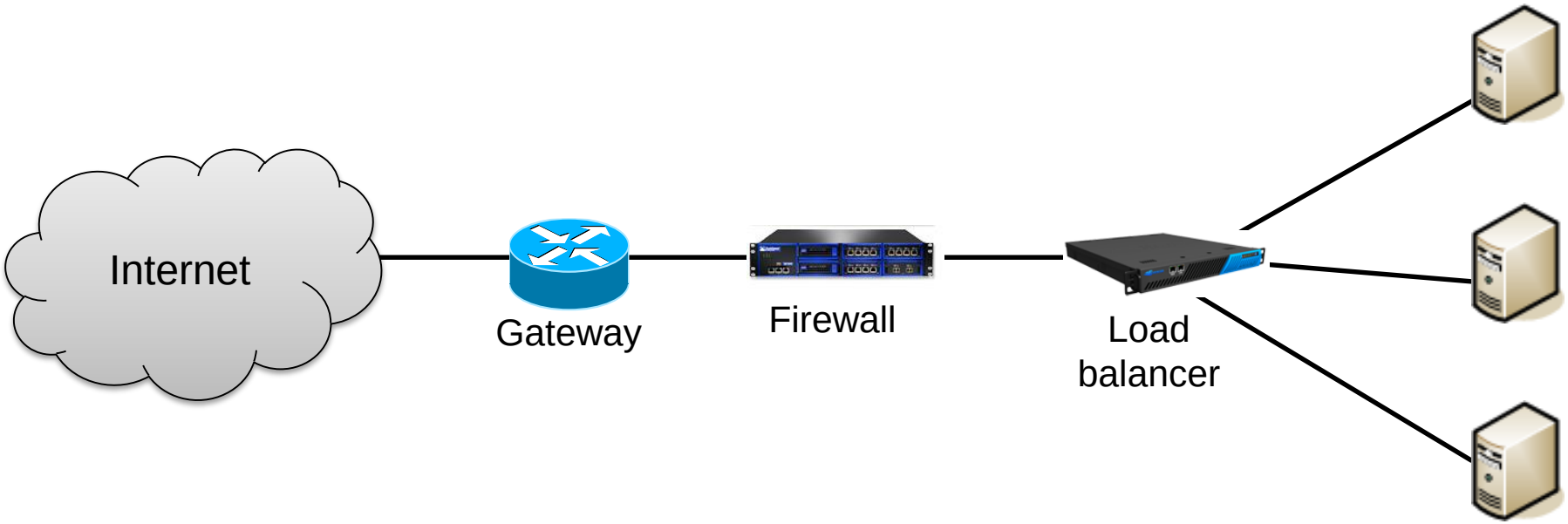
Proliferation of Network Devices

- "Middleboxes" (L3-L5)
  - Network address translation (NAT)
  - Firewall
  - Load balancing
  - Encryption
  - Intrusion detection
  - Redundancy elimination
  - …..
- Routers (L3)
- Switches (L2)

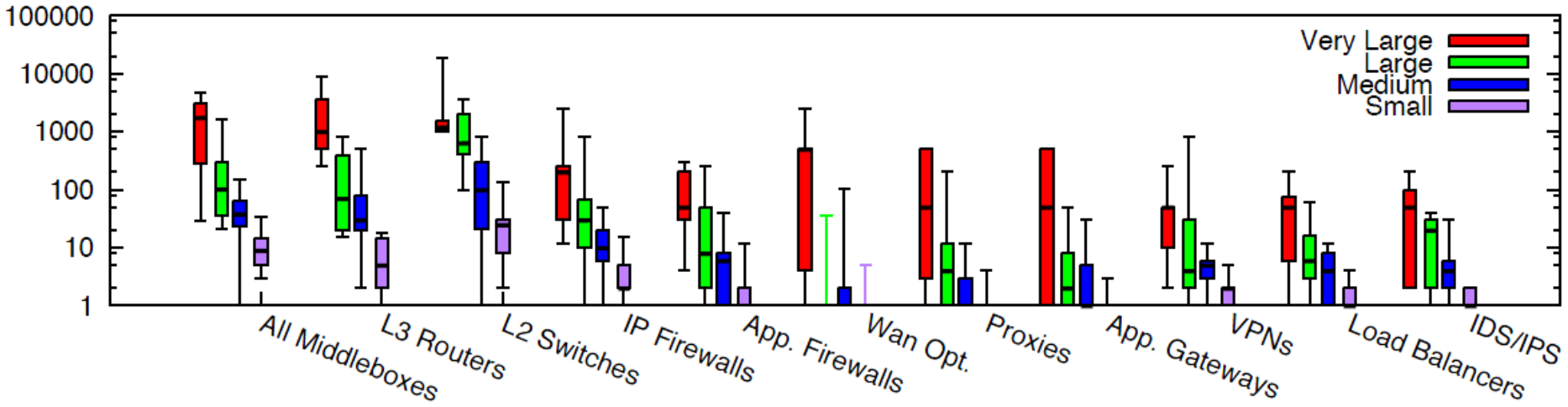


Middlebox Deployment

- Enterprise network with 2 middleboxes:
  - Firewall: filters incoming traffic
  - Load balancer: balances traffic across servers



Statistics of Middlebox Deployments



- Enterprise networks:
  - Small: < 1k hosts
  - Medium: 1k-10k hosts
  - Large: 10k-100k hosts
  - Very large: > 100k hosts

J. Sherry and S. Ratnasamy, “A Survey of Enterprise Middlebox Deployments”, 2012

Various Types of Networks (1)

- Transit networks:
  - Legacy equipment (e.g., routers)
  - Requirements:
    - Traffic engineering
    - Router configuration

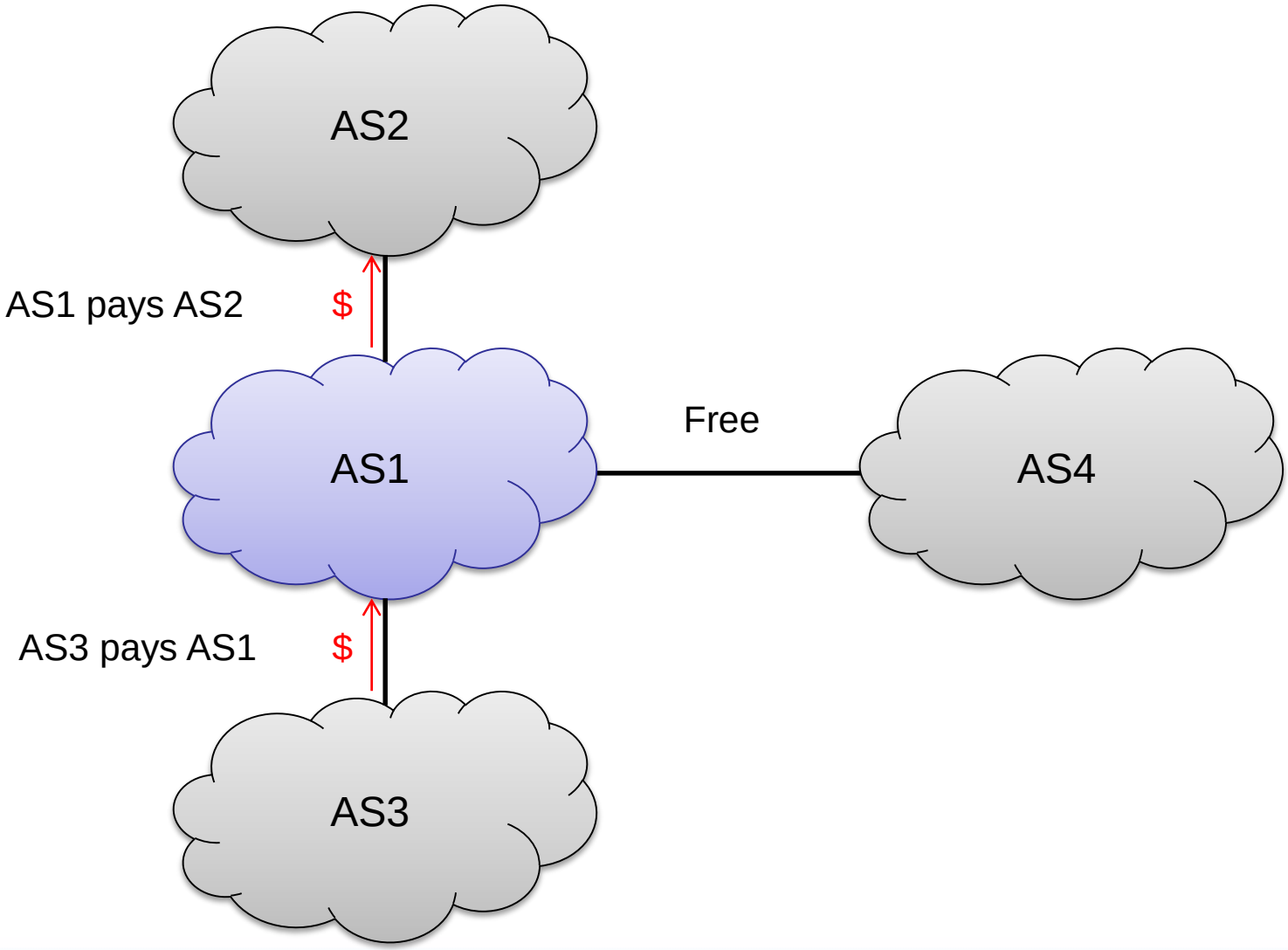
- Enterprise networks:
  - Network device diversity (e.g., switches, routers, middleboxes)
  - Requirements:
    - Network device configuration
      - Security policy
      - Access control
    - Scalability

Various Types of Networks (2)

- Virtual networks:
  - Requirements:
    - Flexible network operations
      - Elasticity
      - Fault management

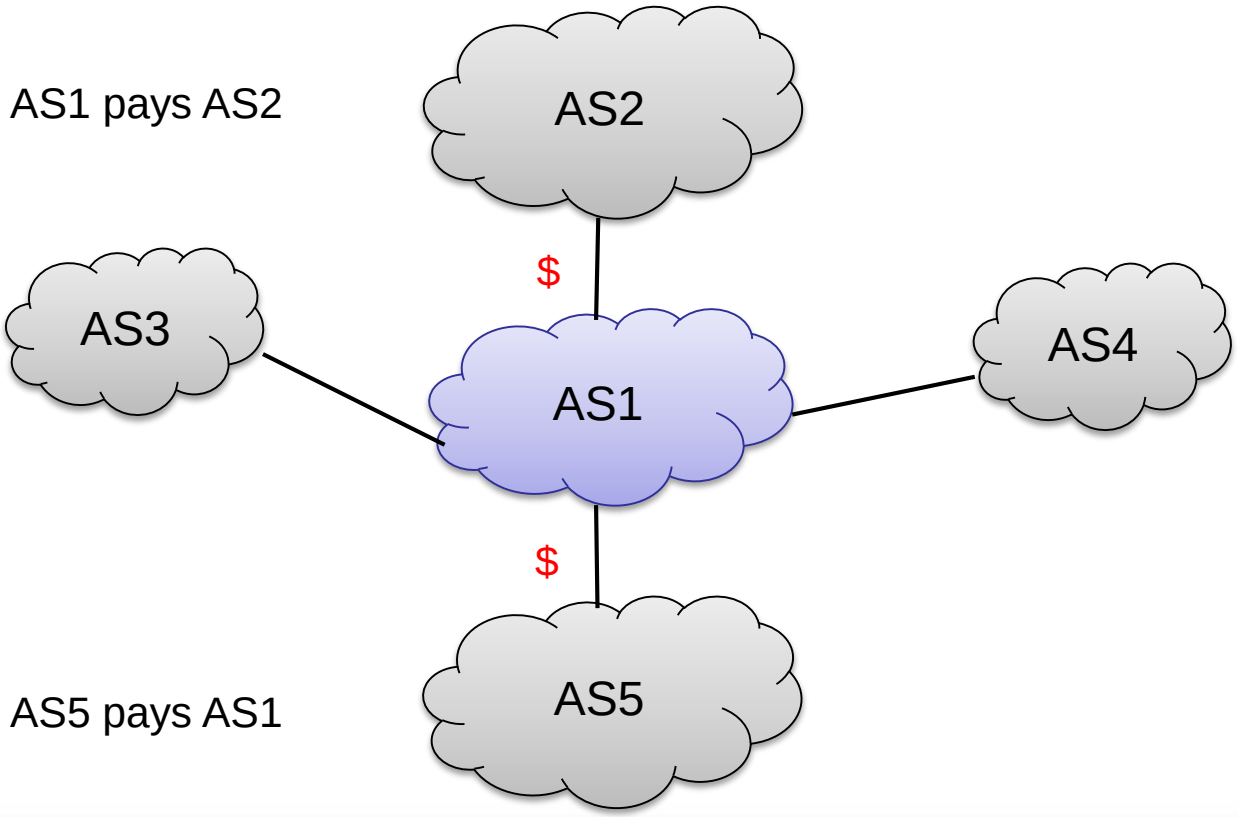
- Data-center networks:
  - Commodity hardware
  - Scale-out networking
  - Requirements:
    - Large bisection bandwidth
    - Exploitation of path redundancy
    - Energy efficiency

Peering Relationships



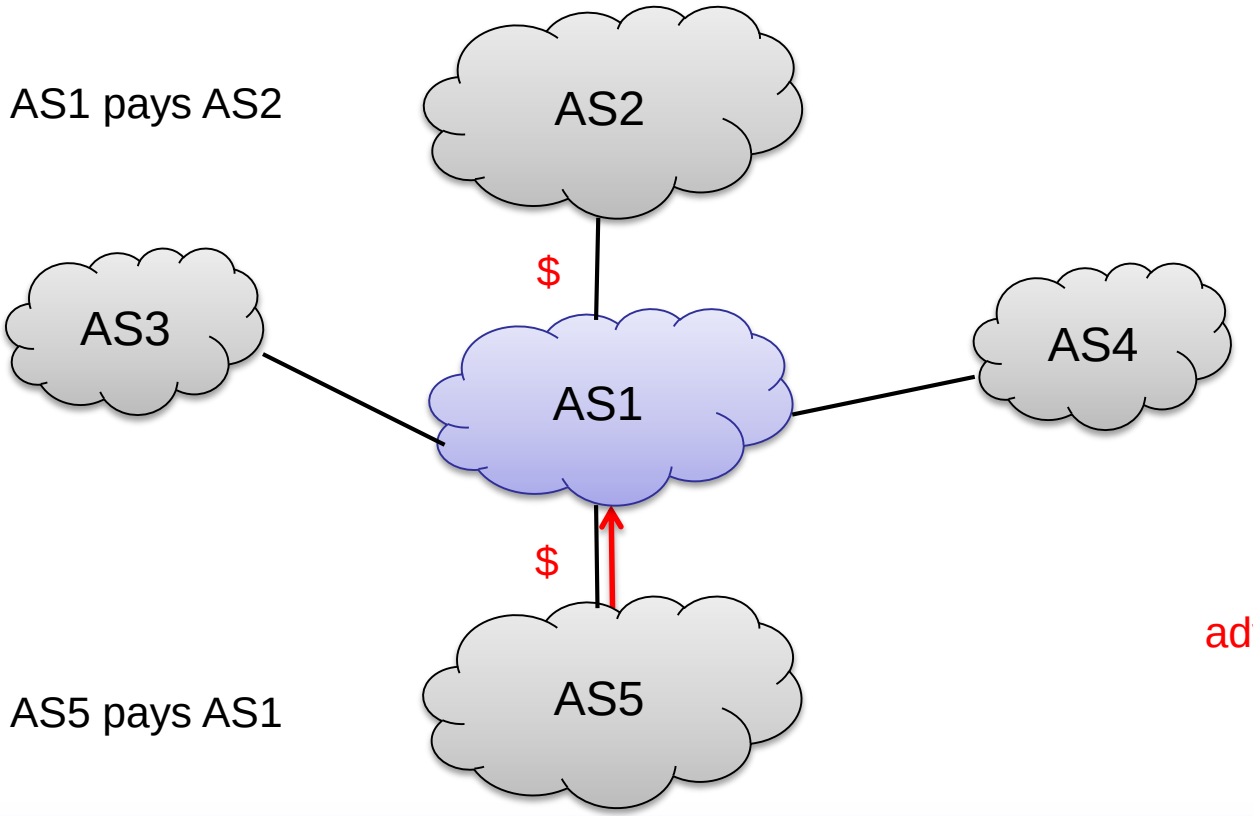
Paid Peering

- Customer – Provider:
  - Routes from customer: to everyone
  - Routes from provider: only to customers



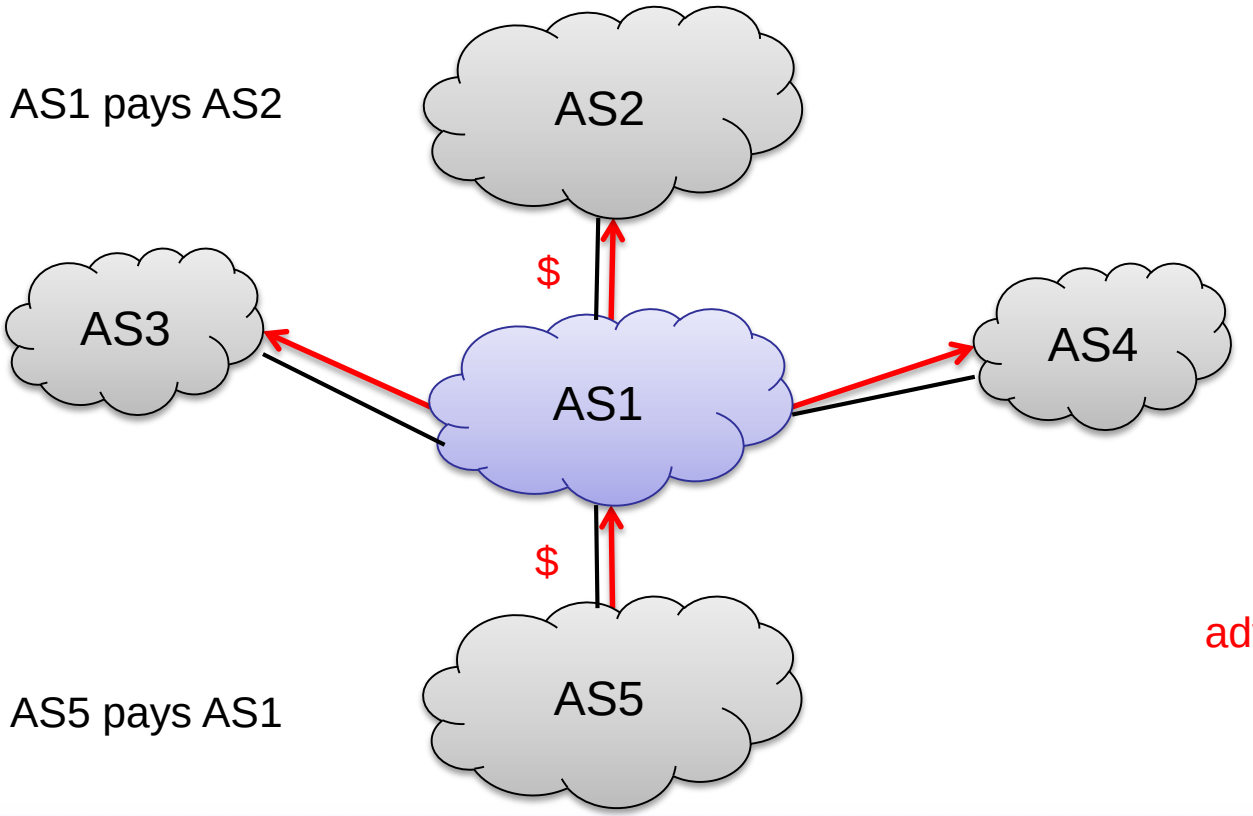
Paid Peering

- Customer – Provider:
  - **Routes from customer: to everyone**
  - Routes from provider: only to customers



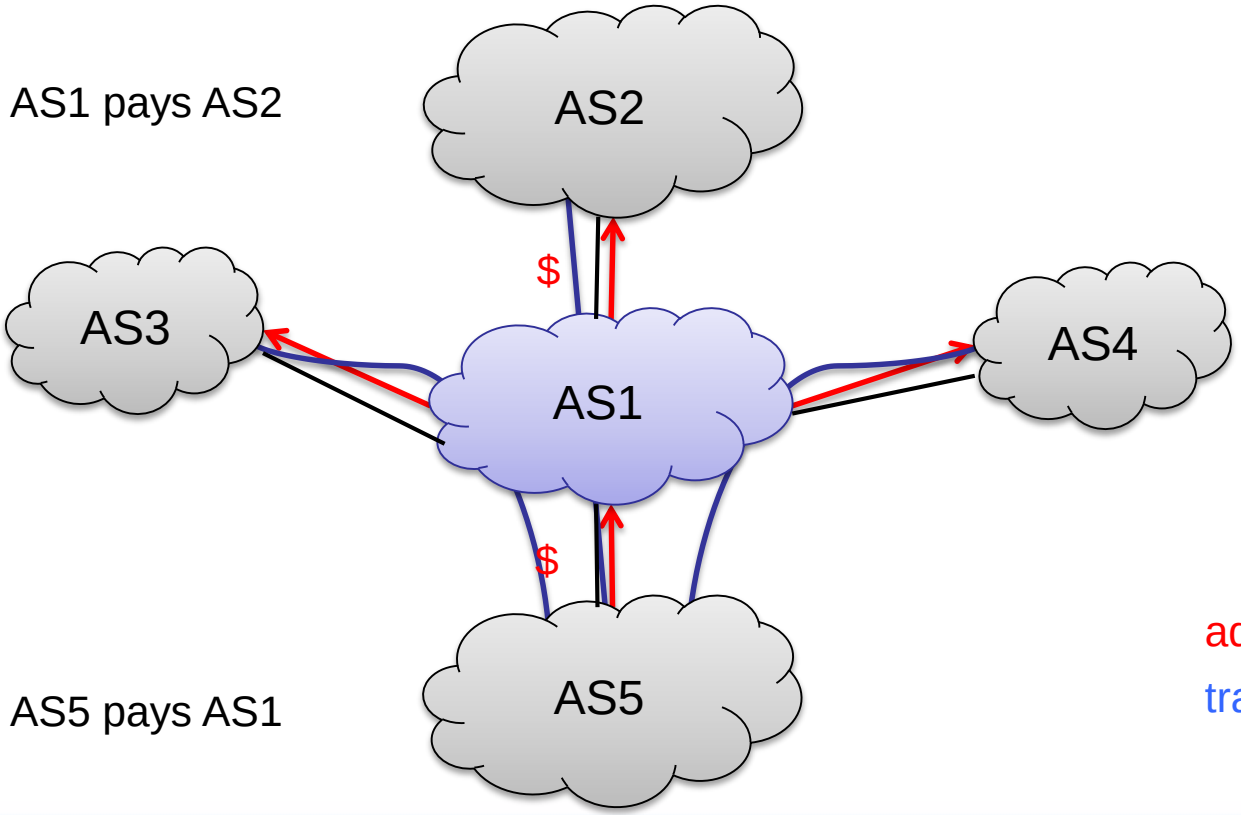
Paid Peering

- Customer – Provider:
  - **Routes from customer: to everyone**
  - Routes from provider: only to customers



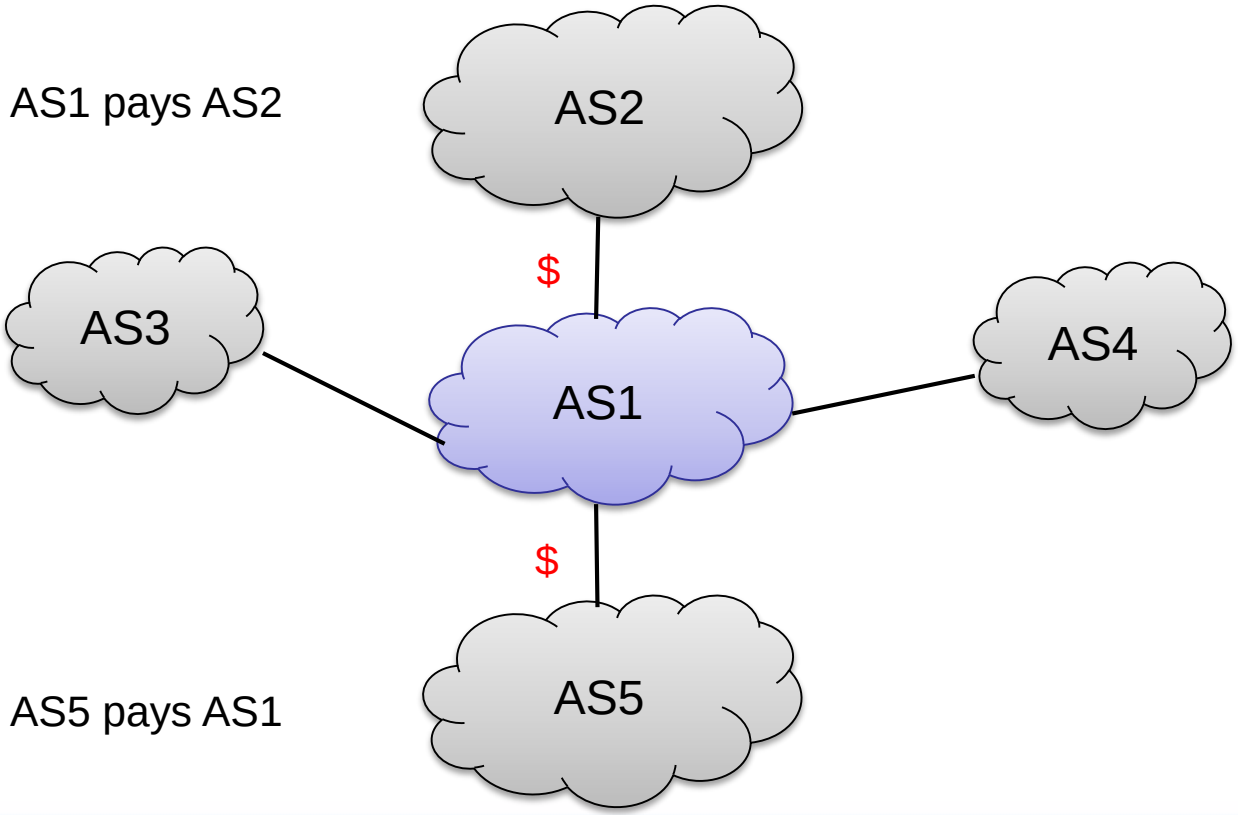
Paid Peering

- Customer – Provider:
  - **Routes from customer: to everyone**
  - Routes from provider: only to customers



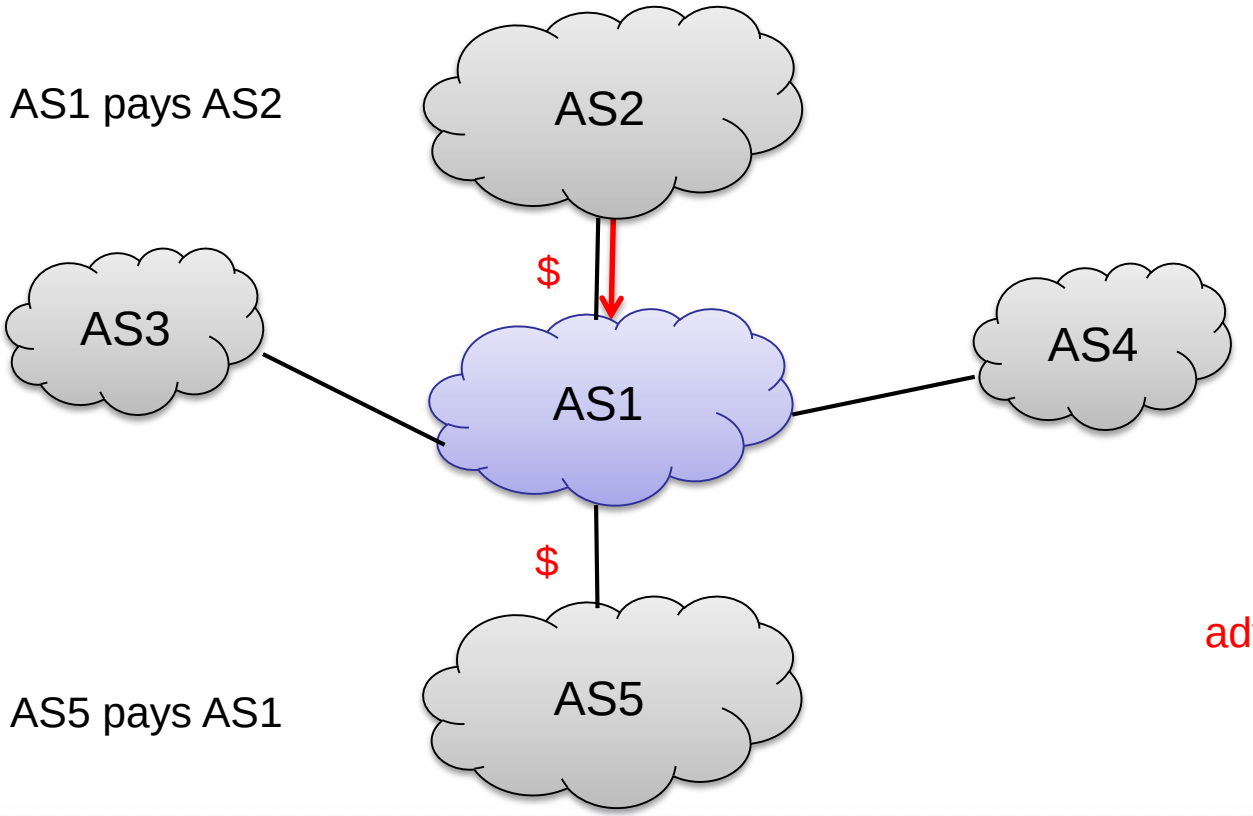
Paid Peering

- Customer – Provider:
  - Routes from customer: to everyone
  - **Routes from provider: only to customers**



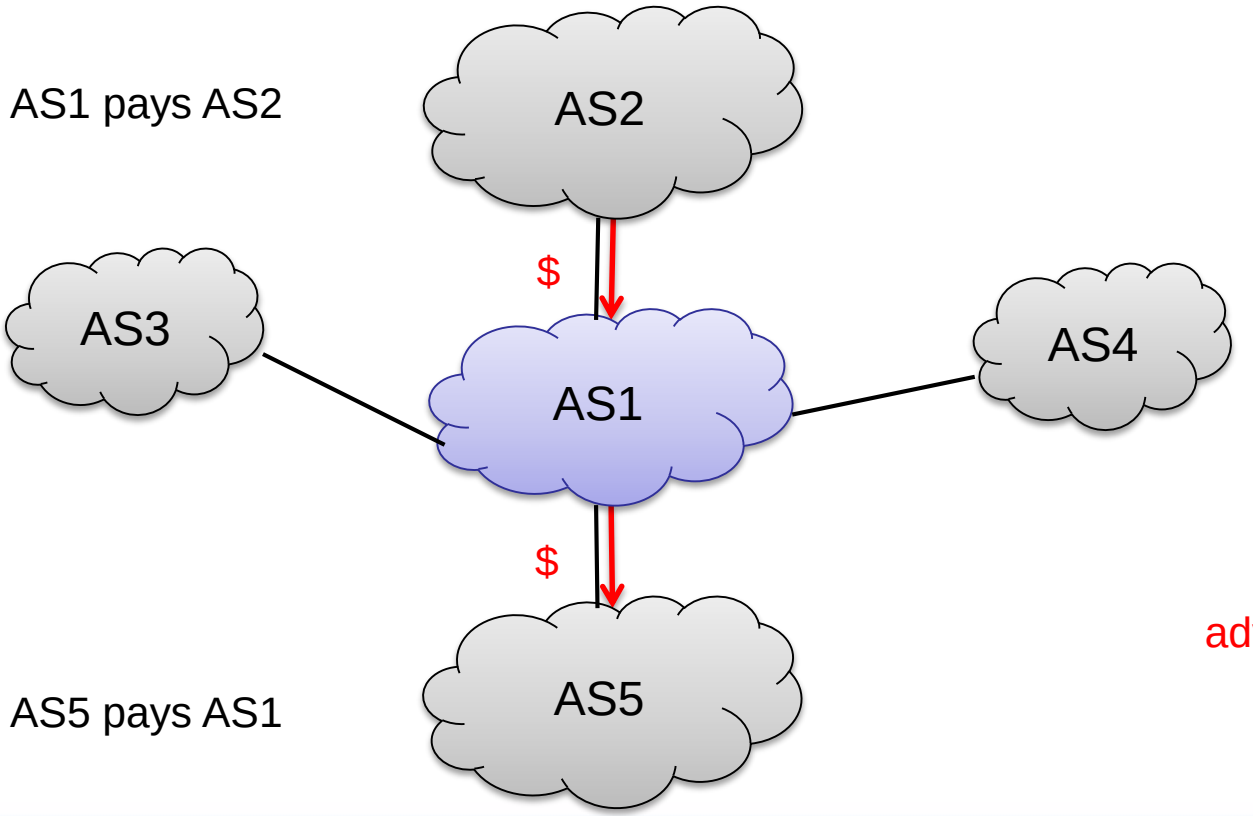
Paid Peering

- Customer – Provider:
  - Routes from customer: to everyone
  - **Routes from provider: only to customers**



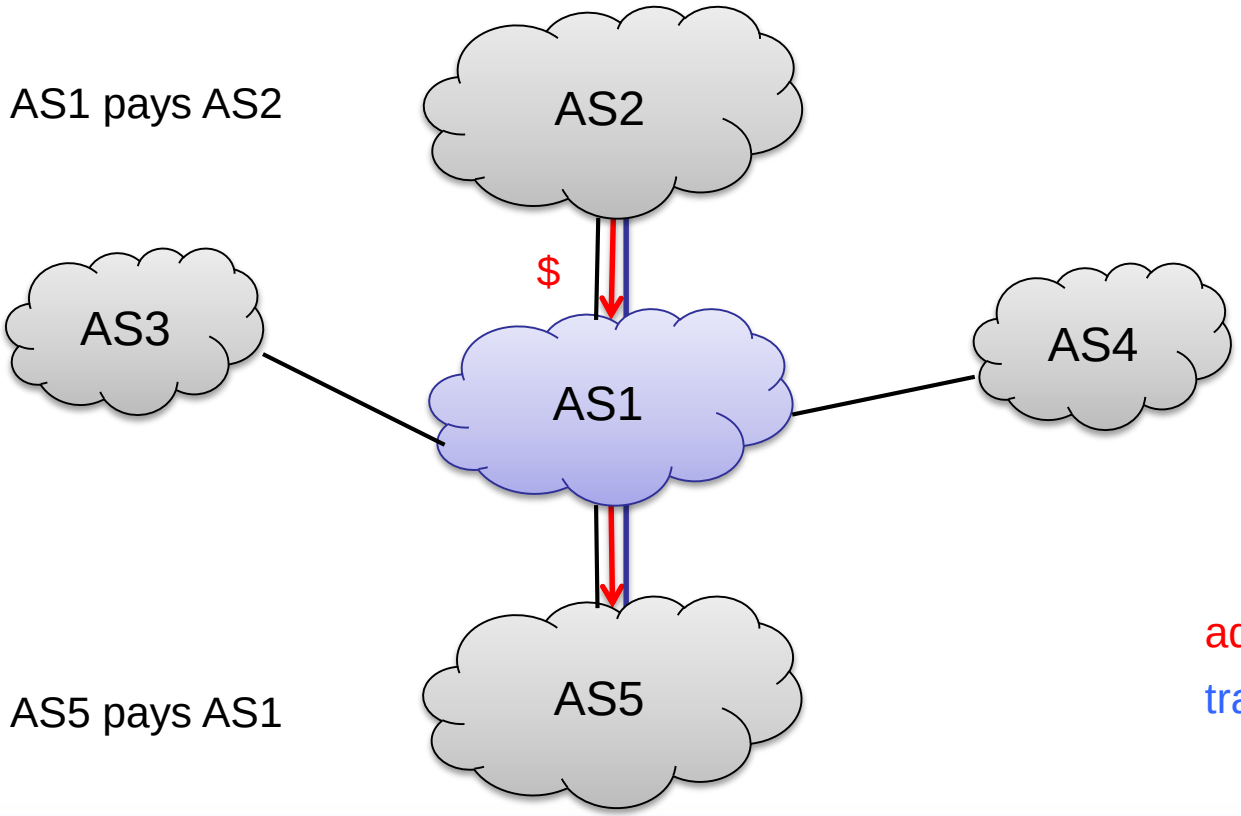
Paid Peering

- Customer – Provider:
  - Routes from customer: to everyone
  - **Routes from provider: only to customers**

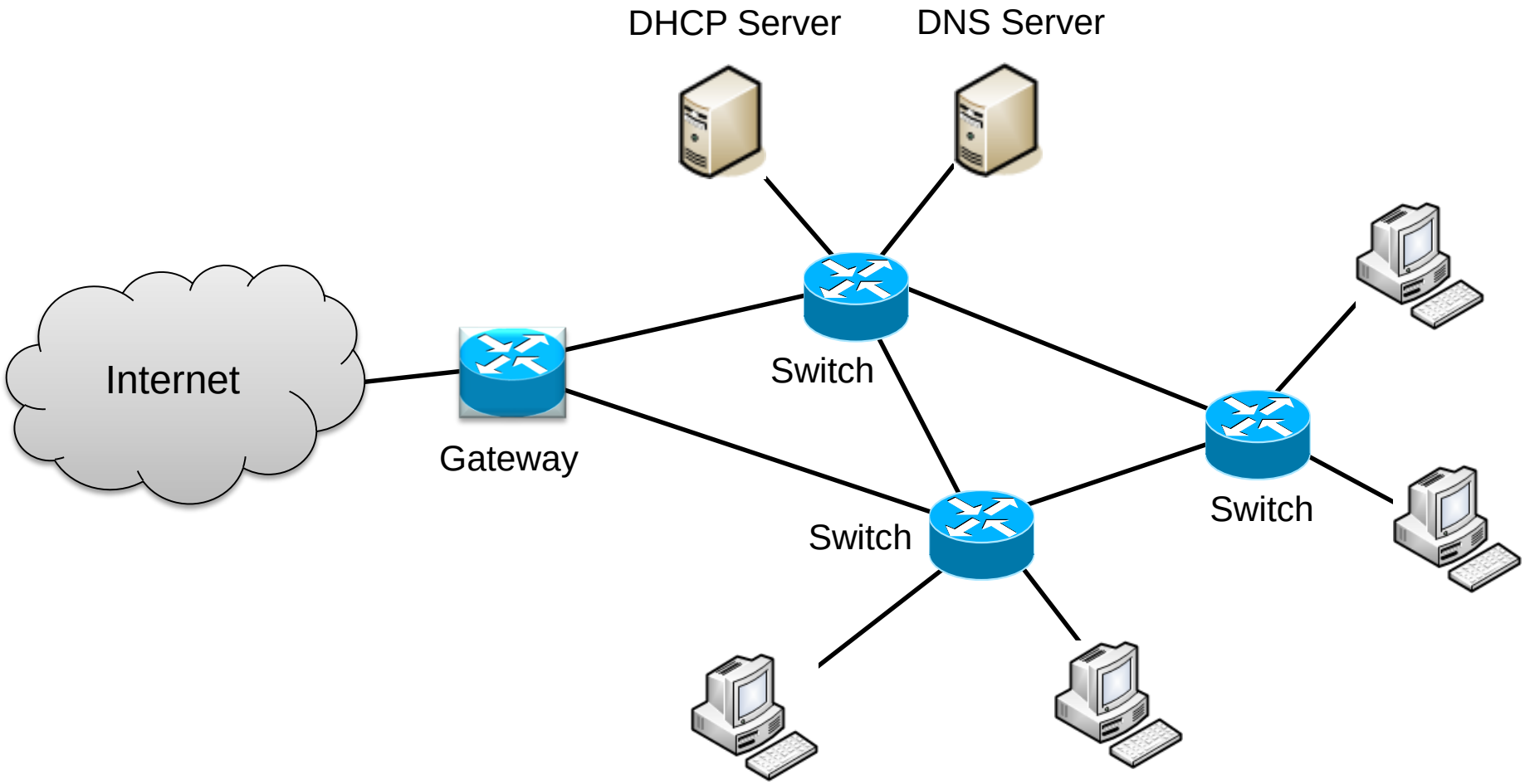


Paid Peering

- Customer – Provider:
  - Routes from customer: to everyone
  - **Routes from provider: only to customers**



Enterprise Network



Challenges in Large Enterprise Networks

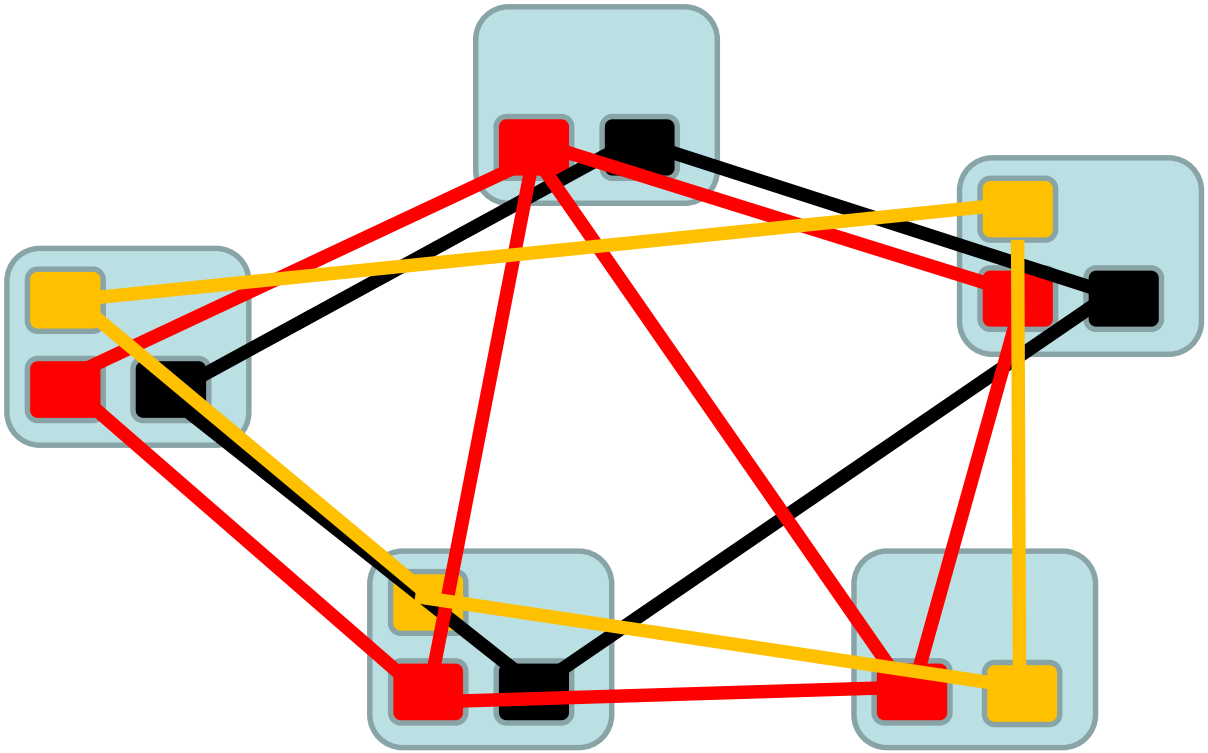
- Large scale:
  - Large enterprise networks include many thousands of hosts

- Minimal configuration overhead:
  - Host/service discovery
  - Host mobility
  - Network topology changes
  - Implementation of network-wide policies

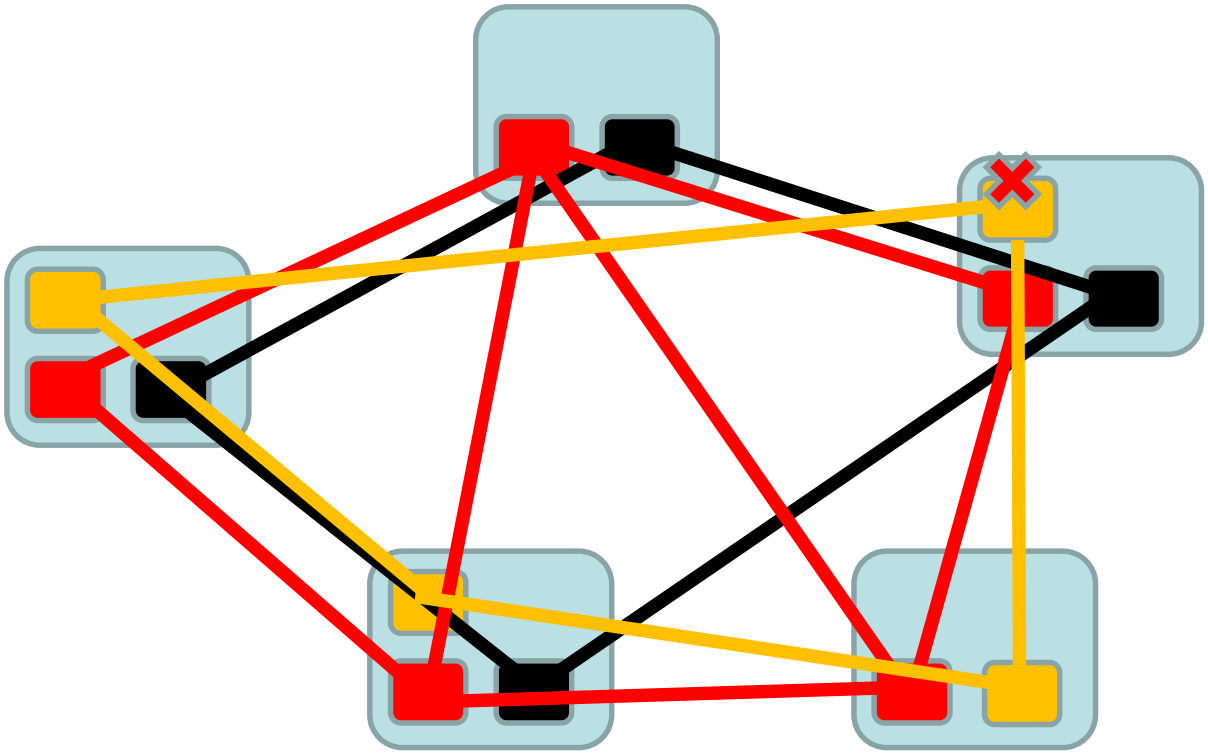
Management of Virtualized Network Infrastructures

- Goals:
  - Elasticity
  - Fault tolerance
  - Easy maintenance of physical equipment (e.g., servers)
- Main principle:
  - Decouple network operations from the physical infrastructure

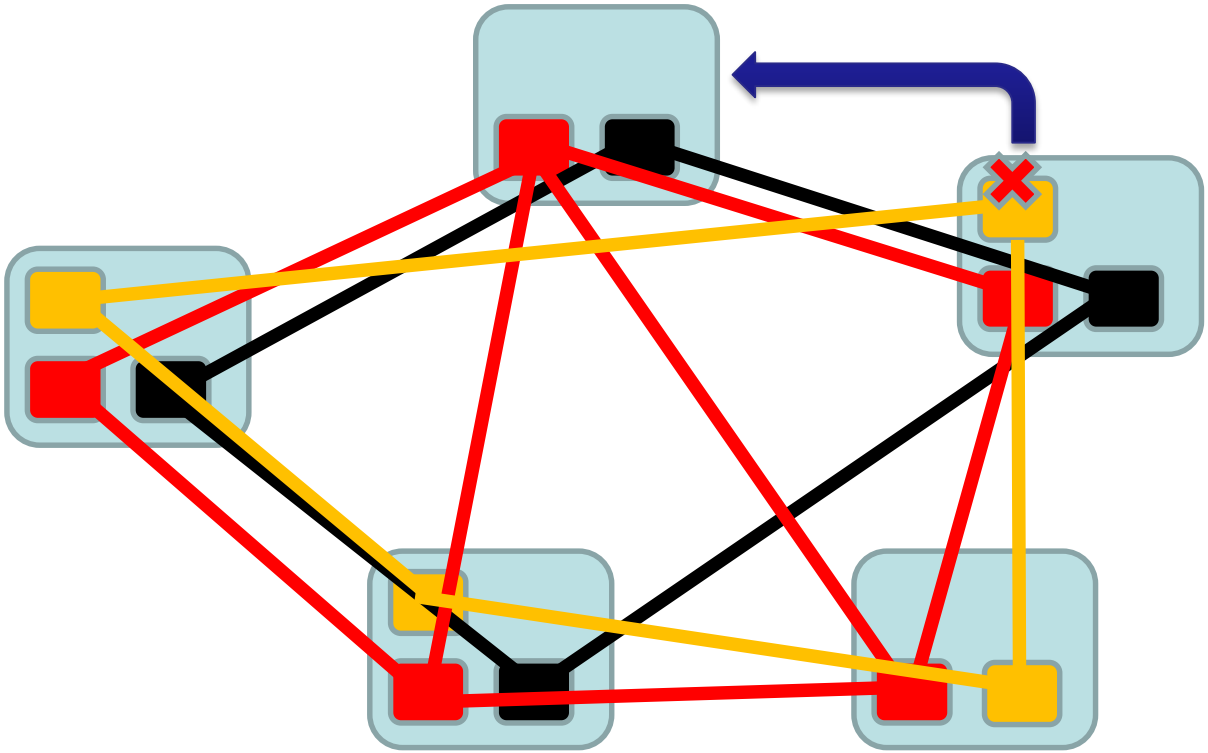
Virtual Network



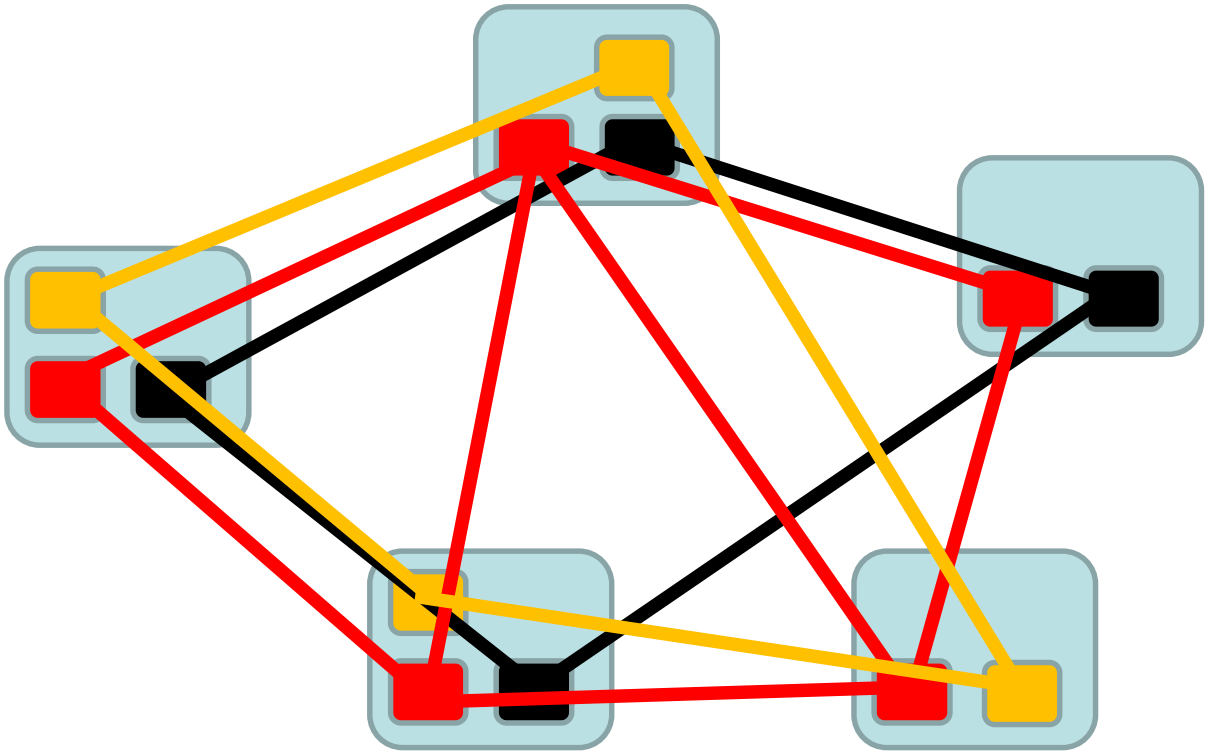
Virtual Network Fault-Management



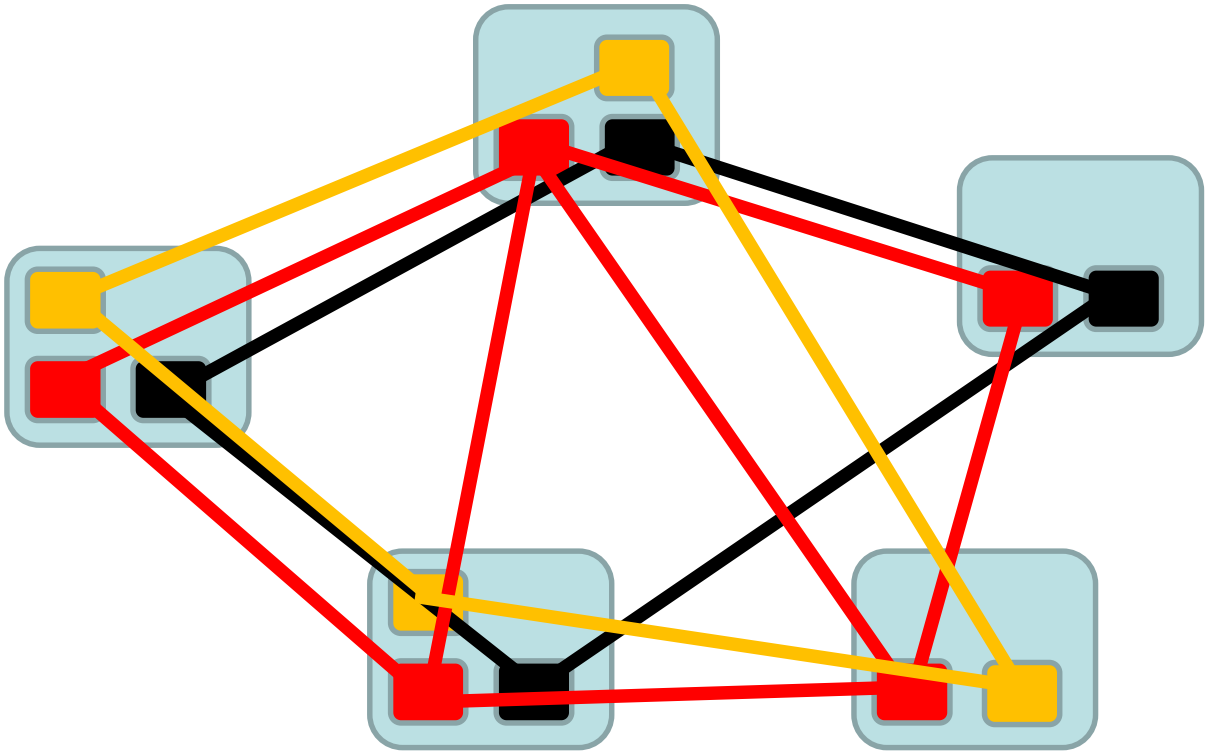
Virtual Network Fault-Management



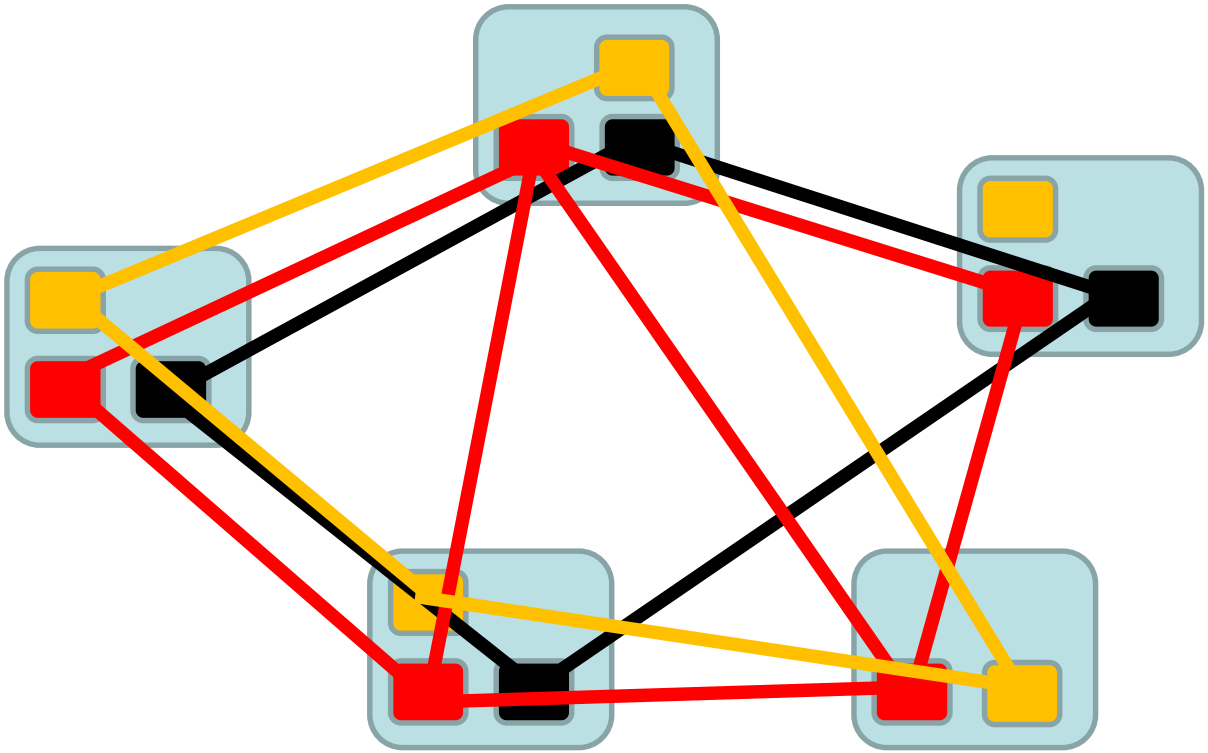
Virtual Network Fault-Management



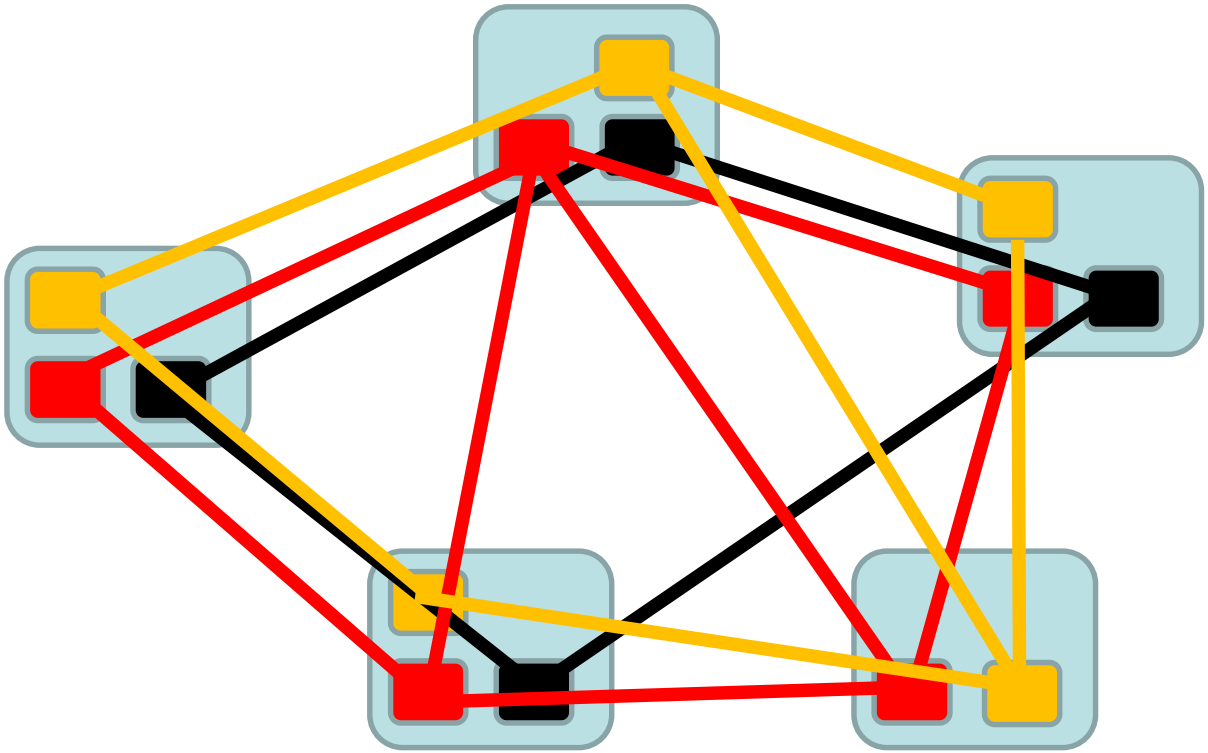
Virtual Network Elasticity



Virtual Network Elasticity



Virtual Network Elasticity

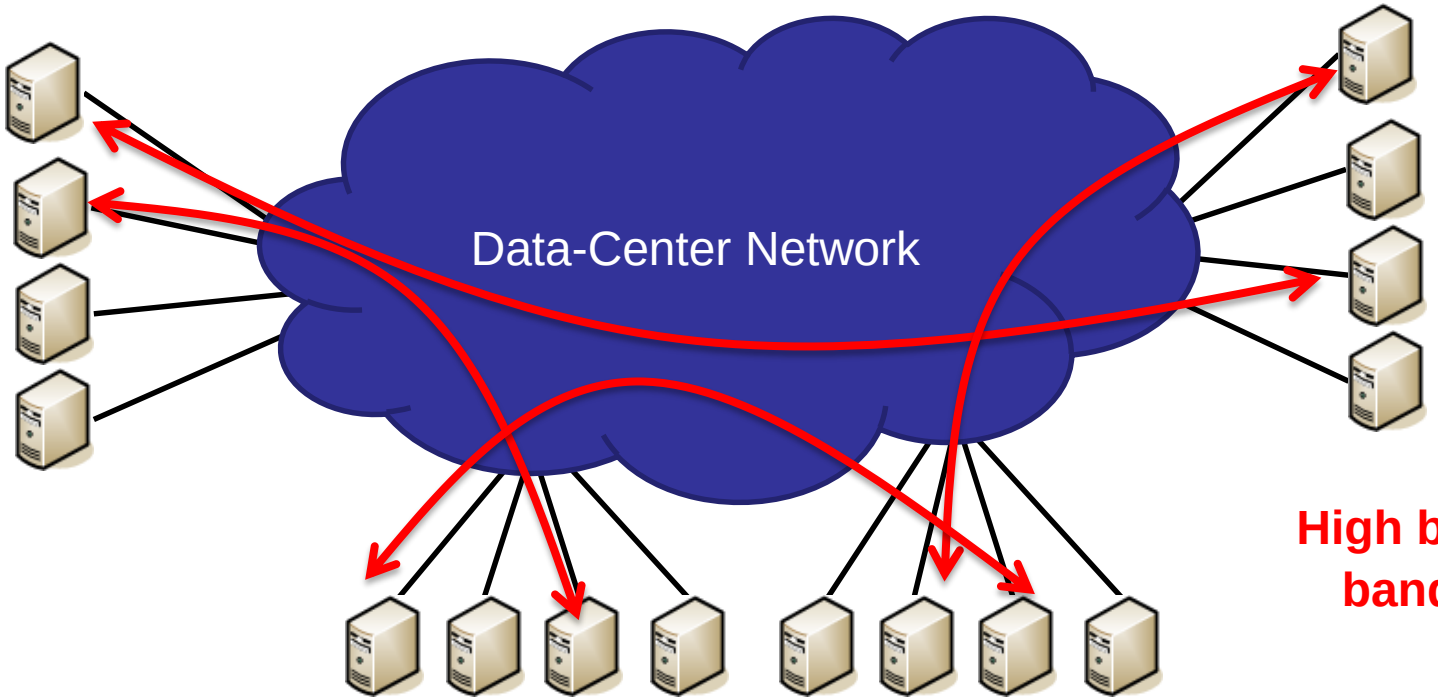


Data Centers

- Major players build and operate data centers:
  - Amazon, Google, HP, Microsoft, Facebook, etc.

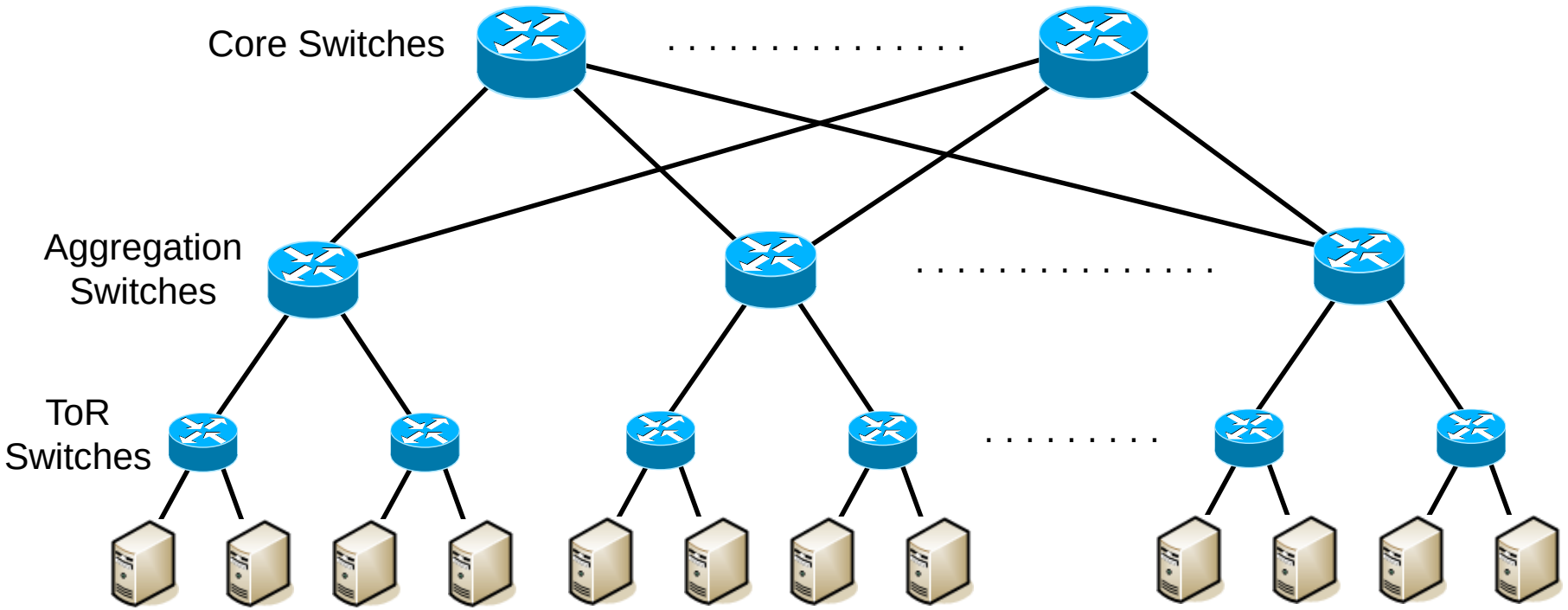
- Features:
  - Massive scale:
    - Usually tens of thousands servers (up to hundreds of thousands servers
  - Commoditization:
    - Wide use of commodity (inexpensive) hardware (i.e., servers and switches)
  - Server virtualization:
    - Widespread adoption of server virtualization to maximize resource utilization
    - A large number of virtual machines may be hosted on a single server using technologies such as VMWare, Xen, etc.

Data-Center Networks

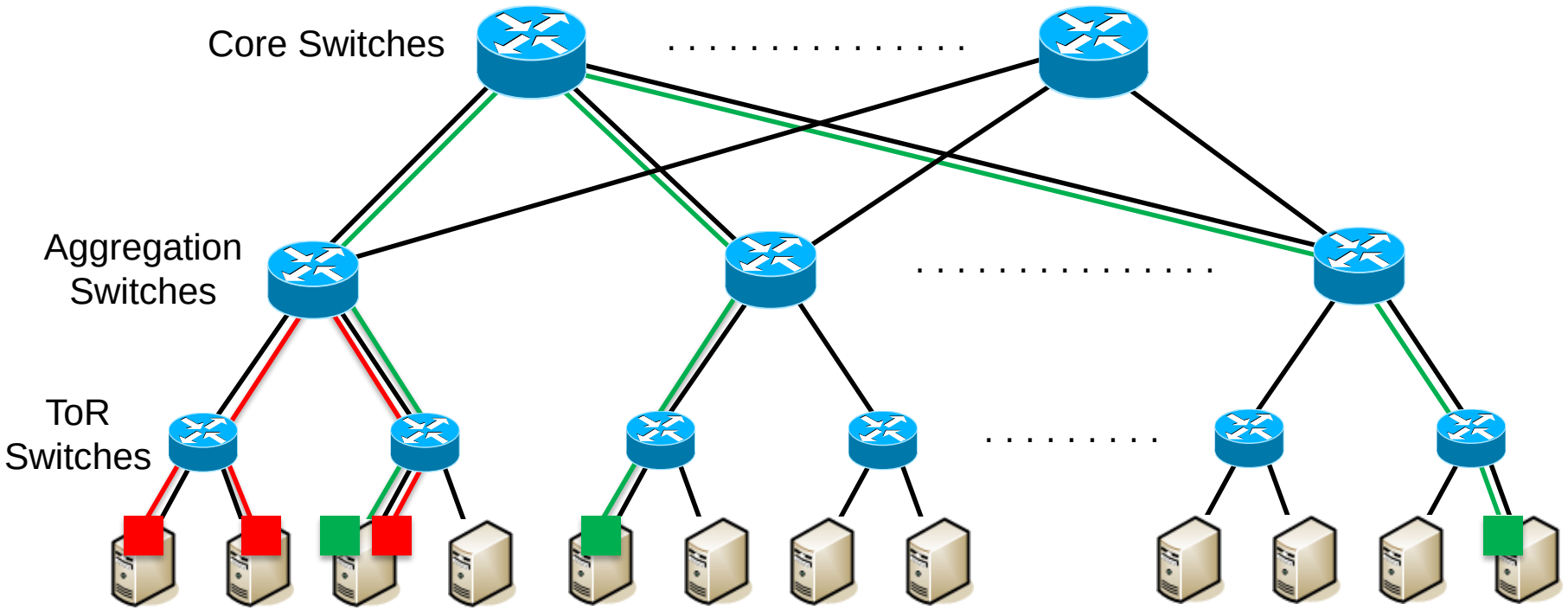


High bisection bandwidth

Data-Center Network Topology



Multi-Tenant Data-Center Networks



- Two different virtual-cluster (VC) assignments
  - VC ■ uses more bandwidth and switching capacity

Network Management Overview

Network Management: A Definition

- “Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost”

T. Saydam and T. Magedanz, “From Networks and Network Management into Service and Service Management”, Journal of Networks and Systems Management,1996

Network Management Tasks (1)

- Detecting network interface failures at hosts or routers:
  - Detect if a network port is down
- Host monitoring:
  - Detect if a host is not operational or compromised due to a security attack
- Traffic monitoring:
  - Detect network/link overload

Network Management Tasks (2)

- Detecting route flapping:
  - Detect rapid changes in the routing tables that indicate routing instabilities
- Monitoring for Service Level Agreements (SLAs):
  - Monitor traffic (e.g., throughput, latency) to infer whether established SLAs are maintained
- Instrusion detection:
  - Examine incoming flows to detect malicious activity, such as denial of service (DoS) attacks or port scans

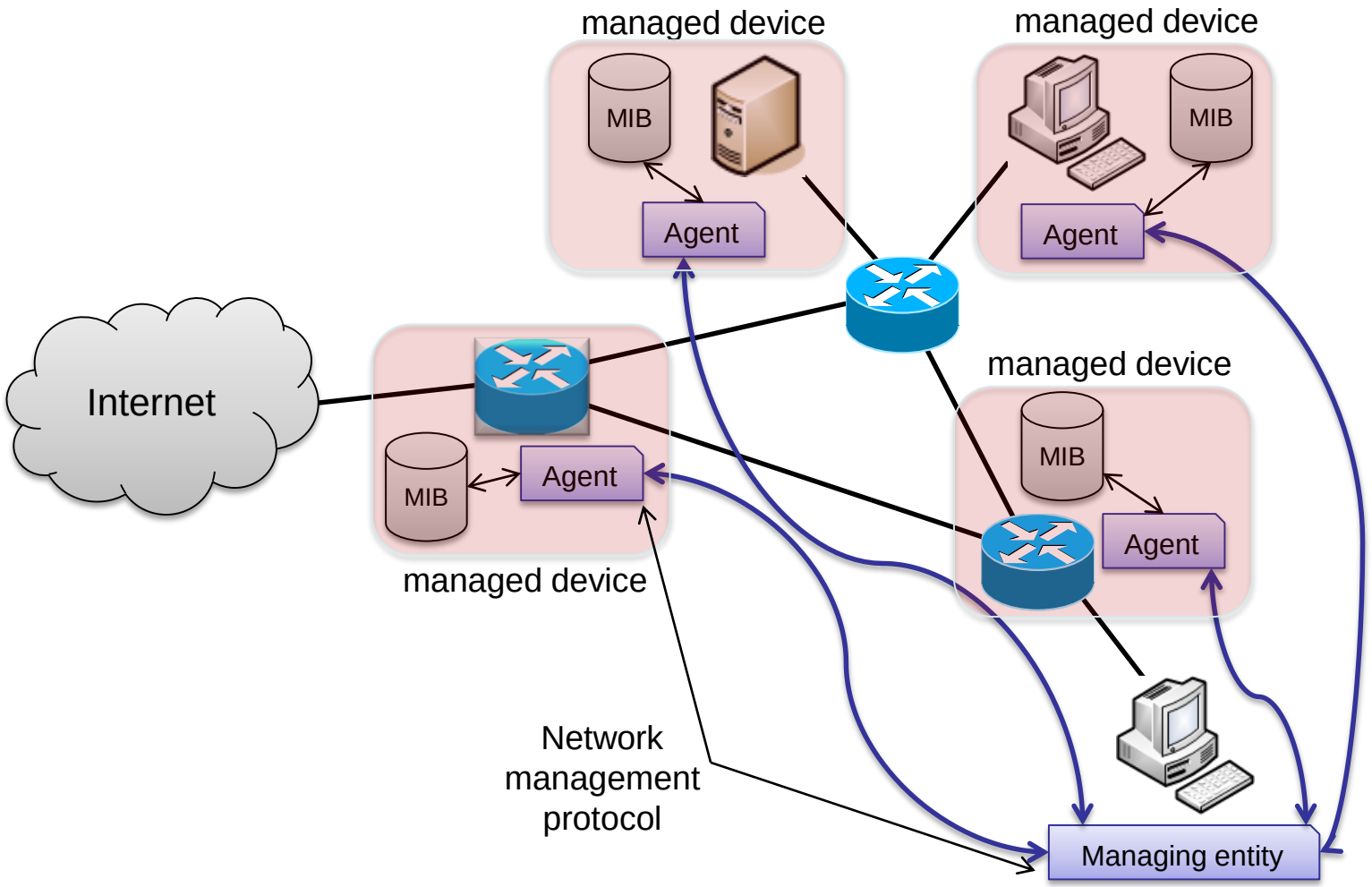
Network Management Areas (1)

- Performance management:
  - Measure, report, analyze and control the performance of different network components
- Fault management:
  - Log, detect and respond to fault conditions in the network
- Configuration management:
  - Track the hardware and software configurations of devices on the managed network

Network Management Areas (2)

- Accounting management:
  - Specify, log and control user and device access to network resources
- Security management:
  - Control access to network resources according to some well-defined policy

Infrastructure for Network Management

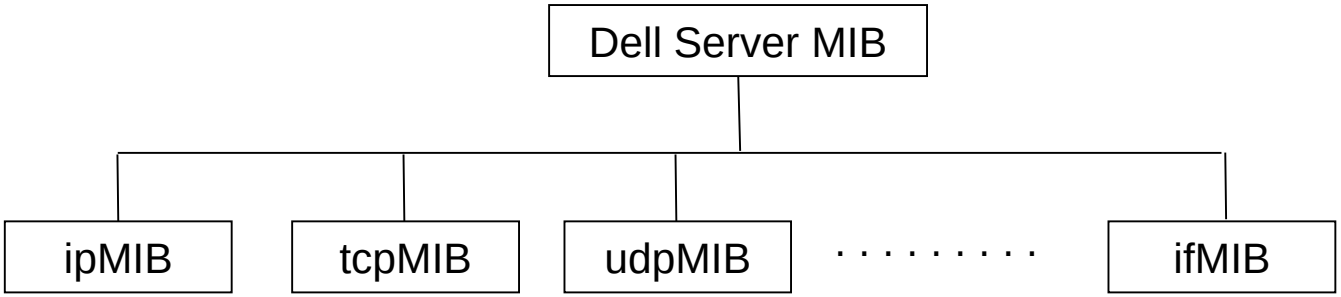


Network Management Standards

- Management Information Base (MIB):
  - Collection of network management objects at managed devices
- Structure of Management Information (SMI):
  - Data definition language for MIB objects
- Simple Network Management Protocol (SNMP):
  - Application-layer protocol for IP network management
  - Communicates management data and commands between the management entity and the managed device

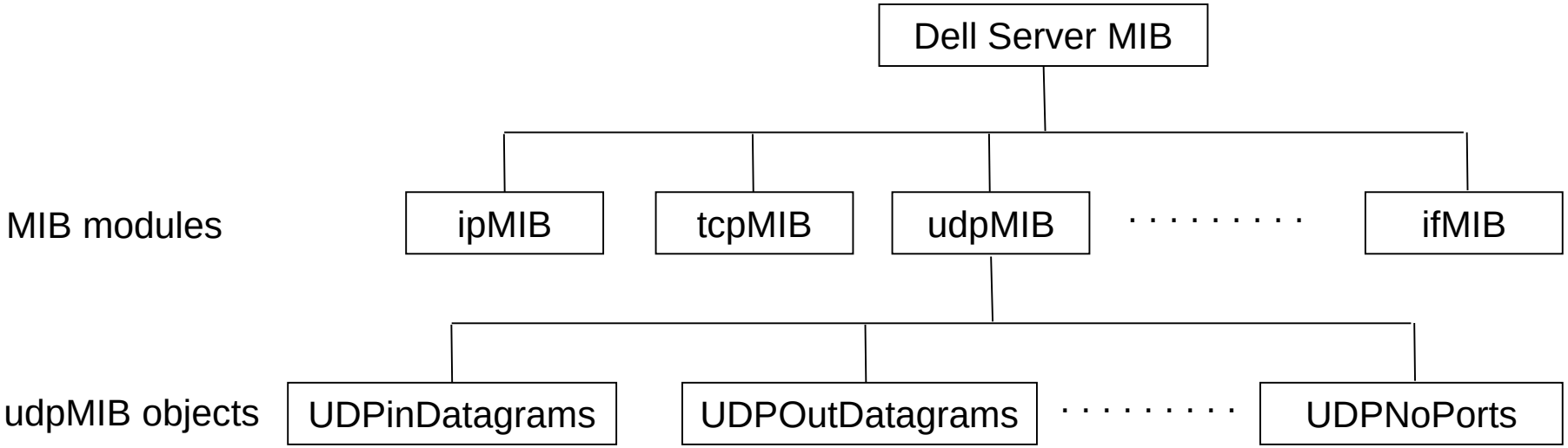
MIB Modules

- MIB is a collection of modules:
  - An MIB module includes all the configuration and reporting information for a component/protocol of a managed device
  - Number of standardized MIB modules depend on device (e.g., host, switch, router) and vendor
  - Each MIB module has a unique identity (e.g., ipMIB, tcpMIB, udpMIB, ifMIB)



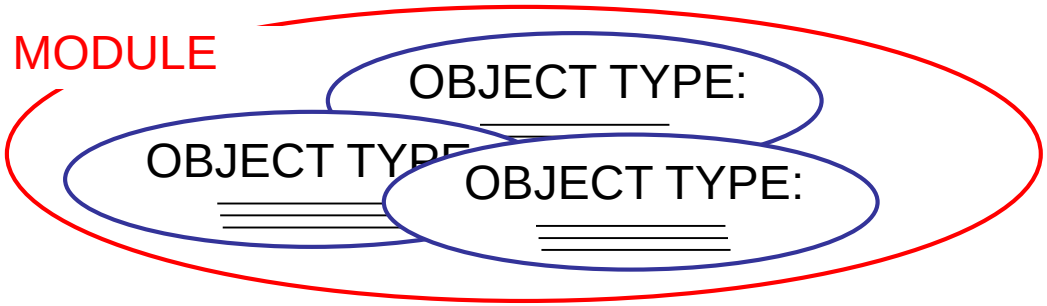
MIB Module Objects

- A MIB module contains a list of objects:
  - Each object has the following attributes:
    - unique identifier
    - name
    - data type
    - module identity (i.e., to which MIB module it belongs)



Structure of Management Information (SMI)

- SMI defines the syntax and semantics of management data stored in MIBs:
  - MIB module via MODULE-IDENTITY construct
  - MIB module object via OBJECT-TYPE construct:
    - data type (e.g., integer, IP address, etc.)
    - level of access (e.g., read-only, read-write)
    - status (current or deprecated)
    - description of managed object



ipMIB Module Specification


```
ipMIB MODULE-IDENTITY
      LAST-UPDATED "200602020000Z"
      ORGANIZATION "IETF IPv6 MIB Revision Team"
      CONTACT-INFO
            "Editor:
             Shawn A. Routhier
             Interworking Labs
             ……."
 DESCRIPTION
            "The MIB module for managing IP and ICMP implementations, but
             excluding their management of IP routes."
      REVISION      "200602020000Z"
  ……
  ……
  ::= { mib-2 48 }
```

Object-Type Specification


```
ipDefaultTTL OBJECT-TYPE
    SYNTAX     Integer32 (1..255)
    MAX-ACCESS read-write
    STATUS     current
    DESCRIPTION
          "The default value inserted into the Time-To-Live field of
           the IPv4 header of datagrams originated at this entity,
           whenever a TTL value is not supplied by the transport layer
           protocol.

           When this object is written, the entity should save the
           change to non-volatile storage and restore the object from
           non-volatile storage upon re-initialization of the system.
           Note: a stronger requirement is not used because this object
           was previously defined."
    ::= { ip 2 }
```

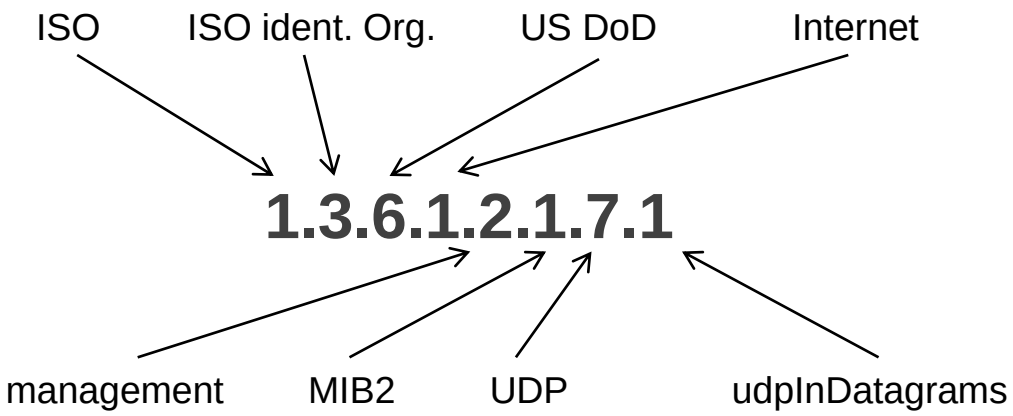
SMI: Basic Data Types

- SMI defines the following object data-types:

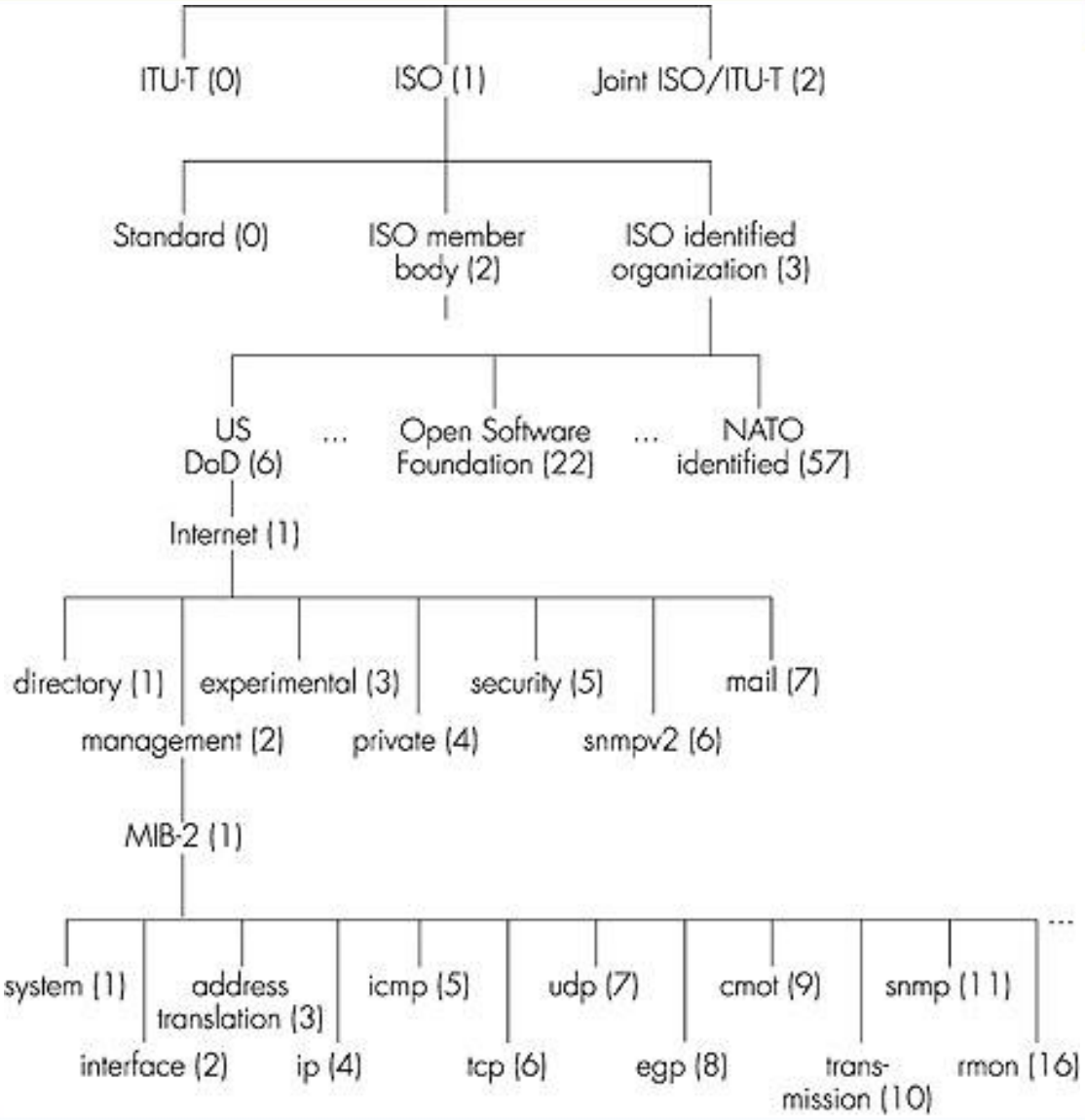
Data Type	Description
Integer32	32-bit integer
Unsigned32	Unsigned 32-bit integer
OCTET STRING	String for binary/text represenation
IPaddress	32-bit Internet address
Counter32	32-bit counter
Counter64	64-bit counter
Gauge32	32-bit integer
TimeTicks	Time (in 1/100ths of a sec)

MIB Object Naming

- OSI Object Identifier tree provides hierarchical naming of all standardized objects:
  - each branchpoint has a name and number



OSI Object Identifier Tree



References

- T. Saydam and T. Magedanz, **From Networks and Network Management into Service and Service Management**, Journal of Networks and Systems Management,1996
- K. McCloghrie, et al., **Structure of Management Information Version 2 (SMIv2)**, RFC 2578, 1999
- J. Sherry and S. Ratnasamy, **A Survey of Enterprise Middlebox Deployments**, 2012
- G. Iannaccone, et al., **Feasibility of IP Restoration in a Tier 1 Backbone**, IEEE Network, 2004