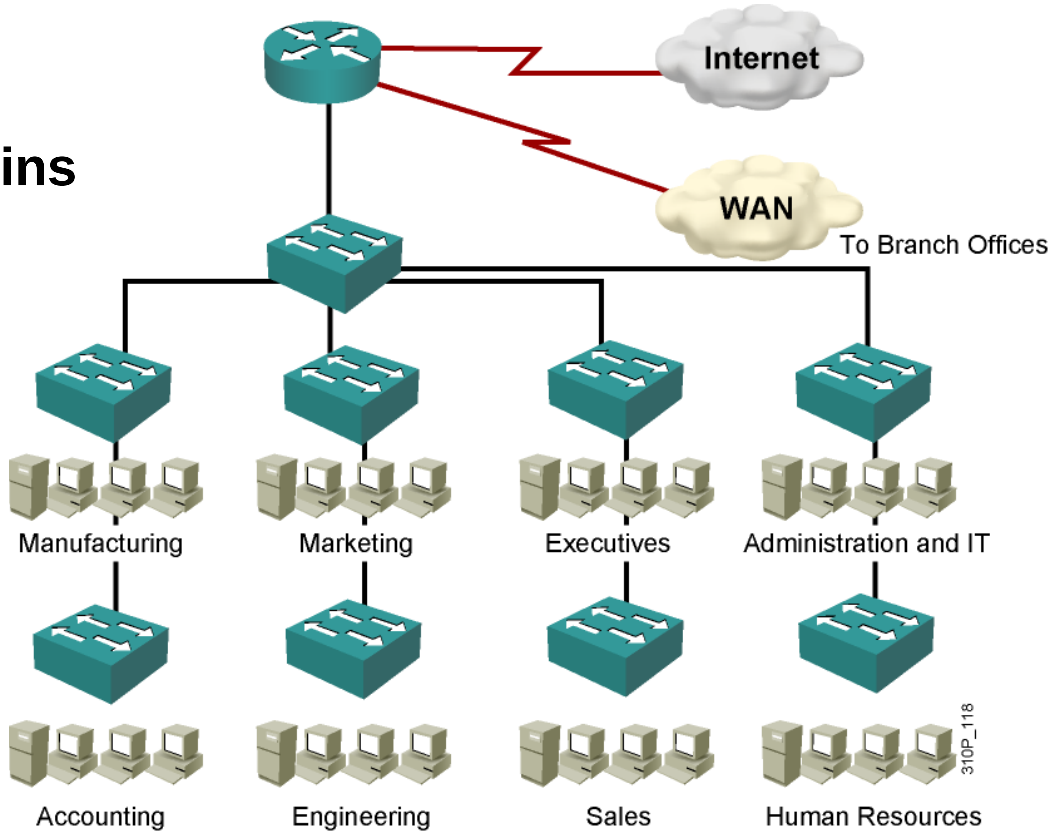
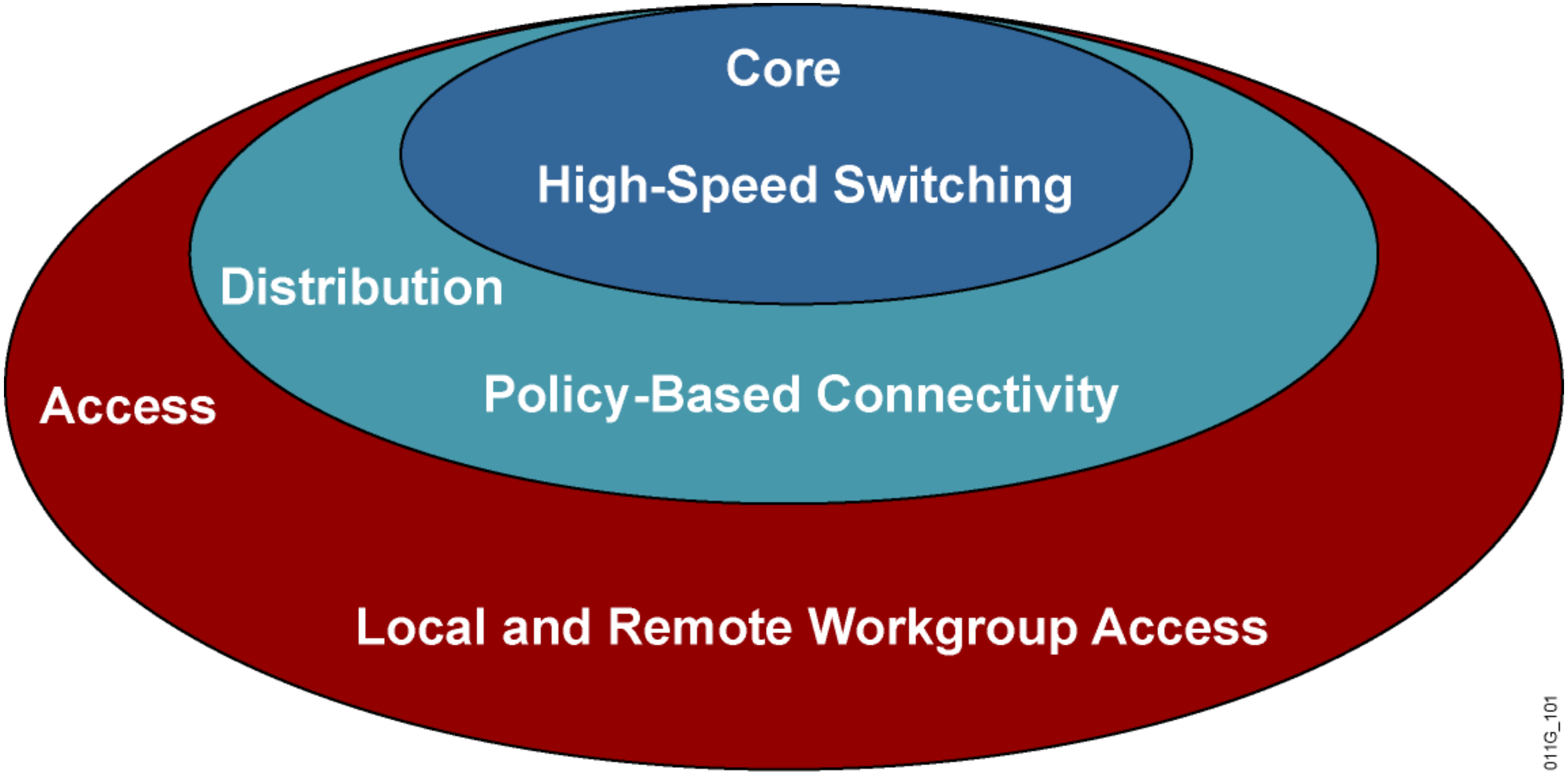
Topology Architectures And Network Components

Issues in a Poorly Designed Network

- Unbounded failure domains
- Large broadcast domains
- Large amount of unknown MAC unicast traffic
- Unbounded multicast traffic
- Management and support challenges
- Possible security vulnerabilities

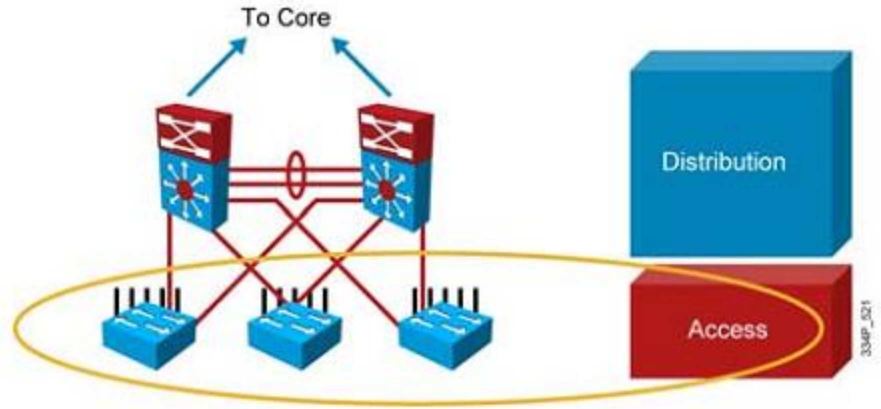


Layers in a Hierachical Model



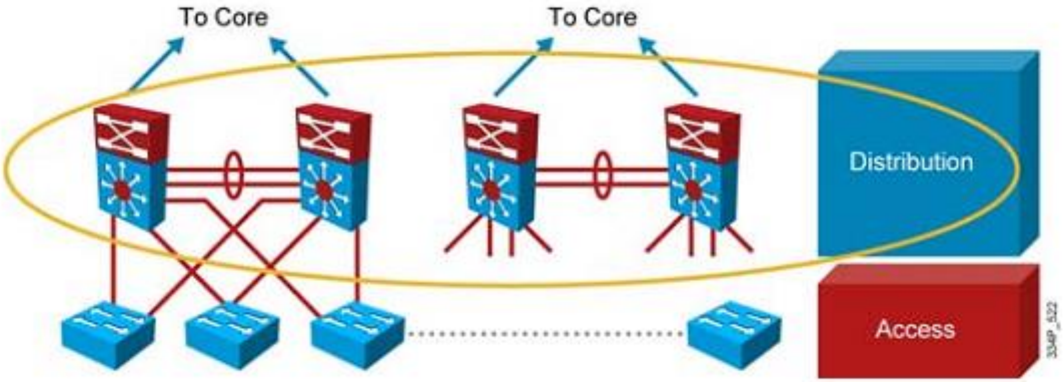
Access Layer

- Provides access and aggregation for users in a feature-rich environment
- Provides high availability through software attributes and redundancy
- Supports convergence for voice, wireless and data
- Provides security services to help control network access
- Offer QoS services including traffic classification and queuing
- Support IP multicast traffic for efficient network use



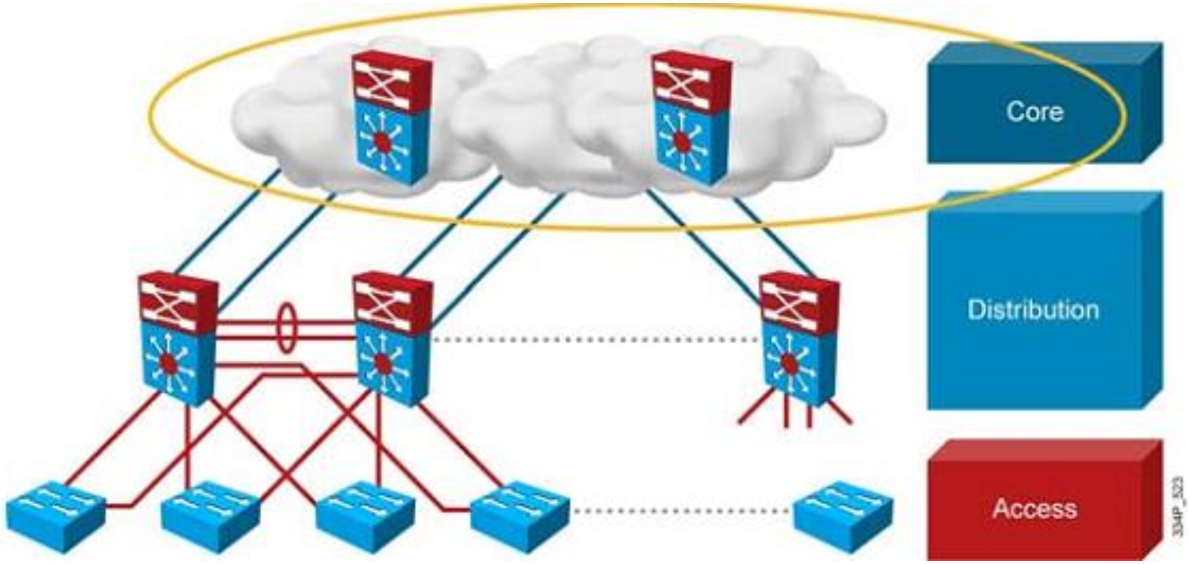
Distribution Layer

- Aggregate nodes and uplinks
- Provide redundant connections and devices for high availability
- Offers routing services such as summarization, redistribution, and default gateways
- Implementing policies including filtering, security, and QoS mechanisms
- Segments workgroups and isolates problems



Core Layer

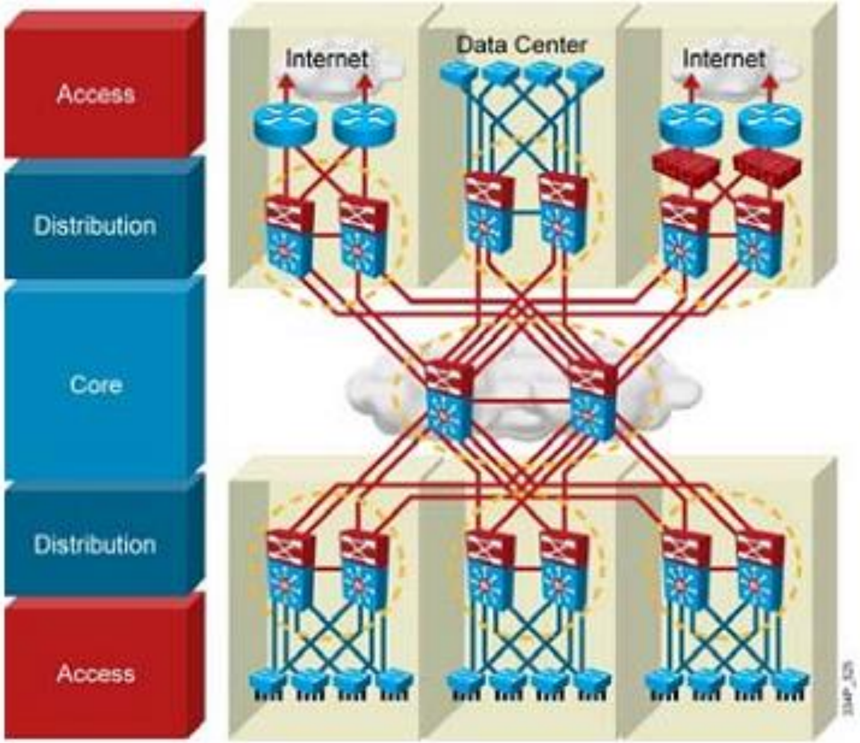
- The core layer is a high-speed backbone and aggregation point for the enterprise
- It provides reliability through redundancy and fast convergence
- The separate core layer helps in scalability during future growth



Campus Core Layer

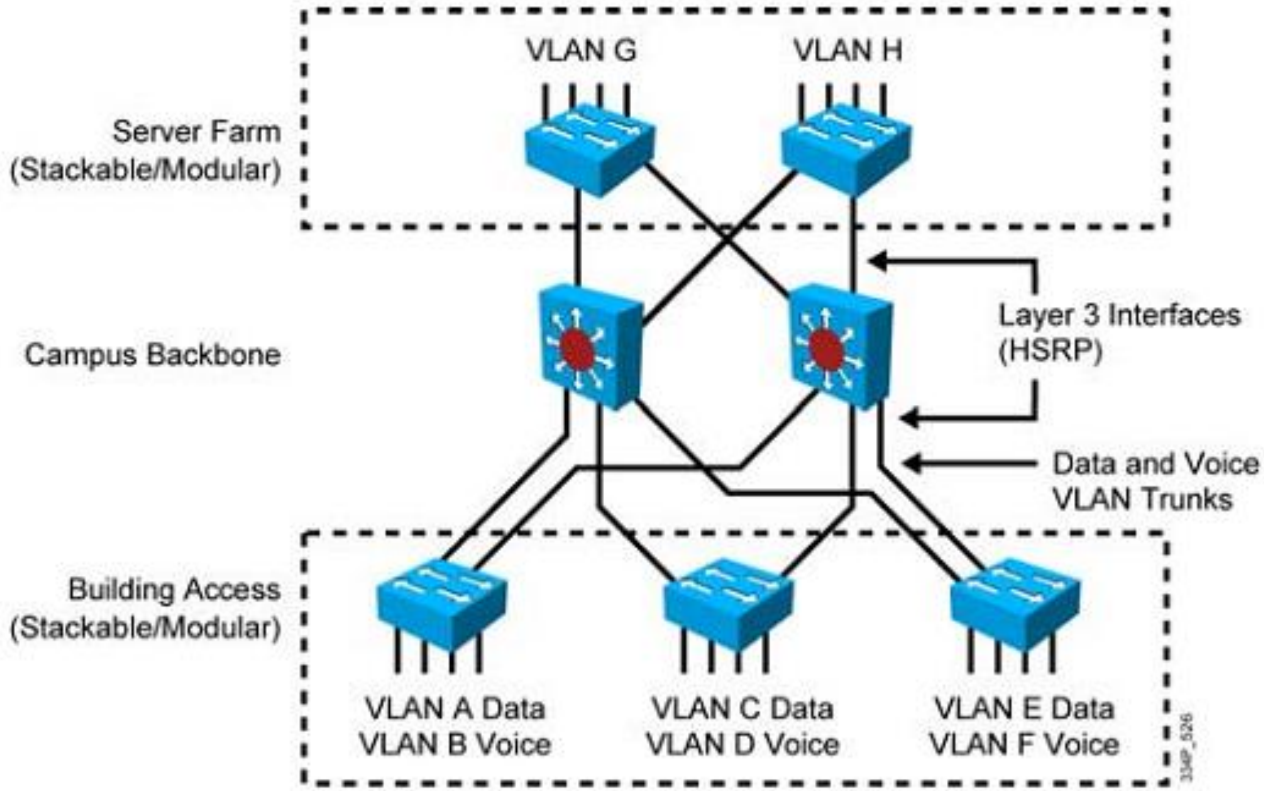
Benefits of a Campus Core:

- Distribution layer switches are connected hiearchically
- Less physical cabling is required
- Less routing complexity is imposed

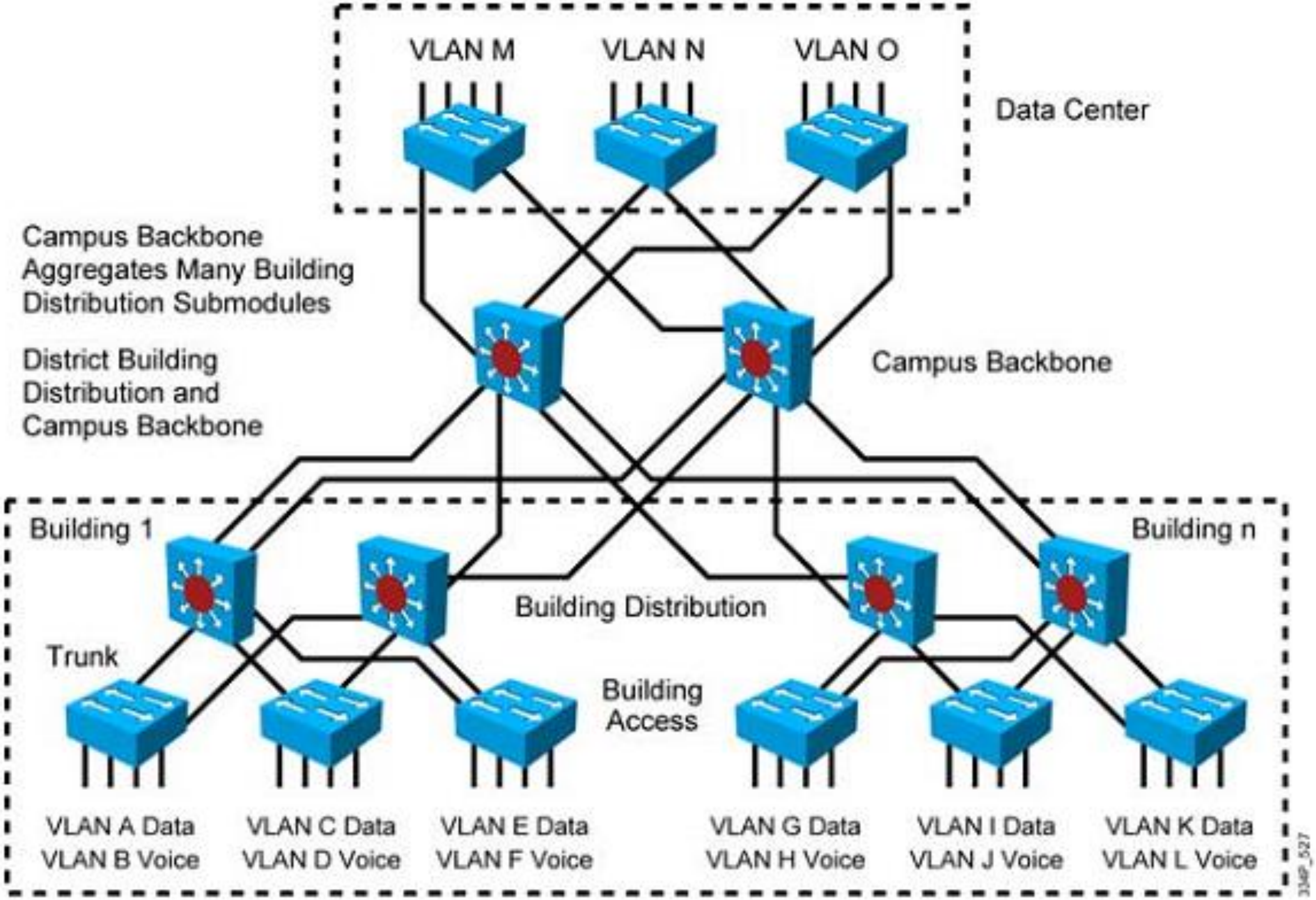


Small Campus Network

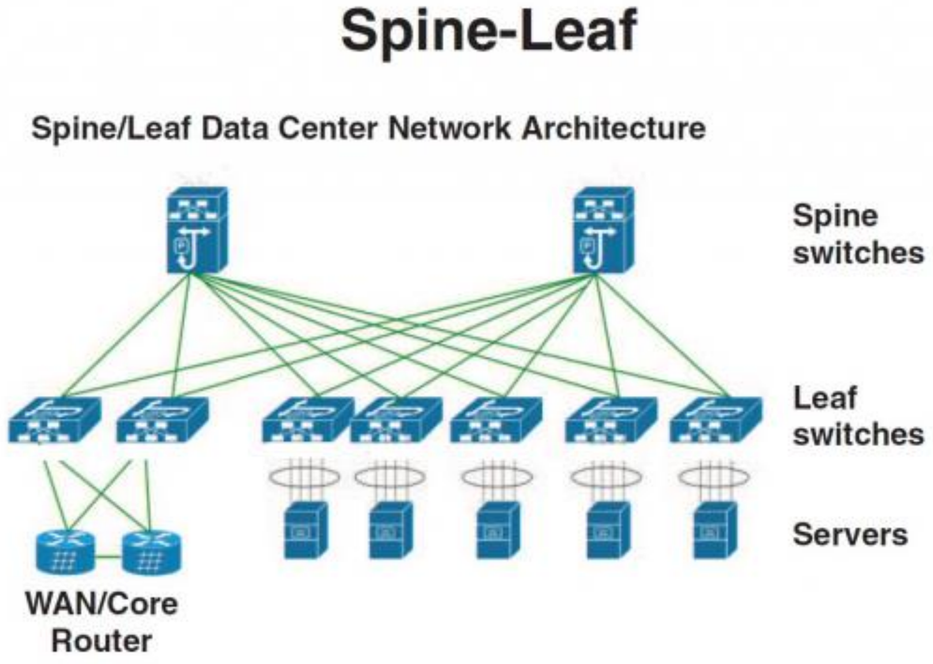
- Collapse the campus backbone and building distribution submodules in the campus backbone submodule
- Scale up to several building access switches

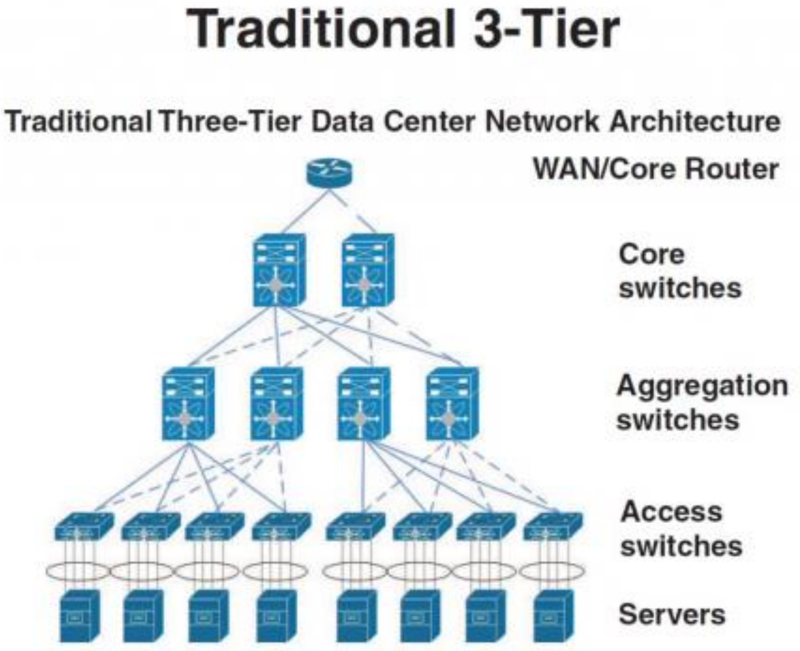

VLAN G
VLAN H
Server Farm (Stackable/Modular)
Campus Backbone
Layer 3 Interfaces (HSRP)
Data and Voice VLAN Trunks
Building Access (Stackable/Modular)
VLAN A Data
VLAN B Voice
VLAN C Data
VLAN D Voice
VLAN E Data
VLAN F Voice
334P_526

Medium Campus Network



Spine-Leaf Data Center Design





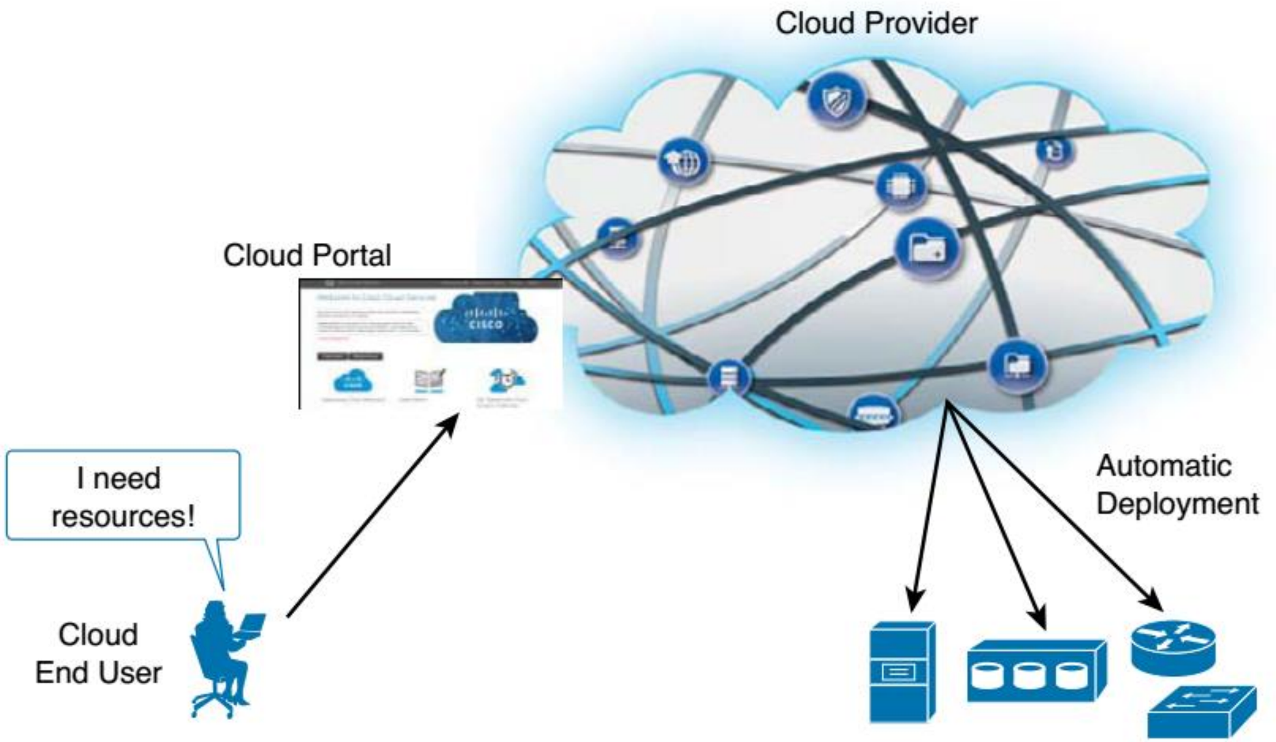
With the Spine-Leaf architecture, each leaf is one hop anyway from any other leaf switch; therefore, it promotes high-bandwidth, low-latency, nonblocking server-to-server connectivity.

Introducing Cloud Computing

What Is Cloud Computing

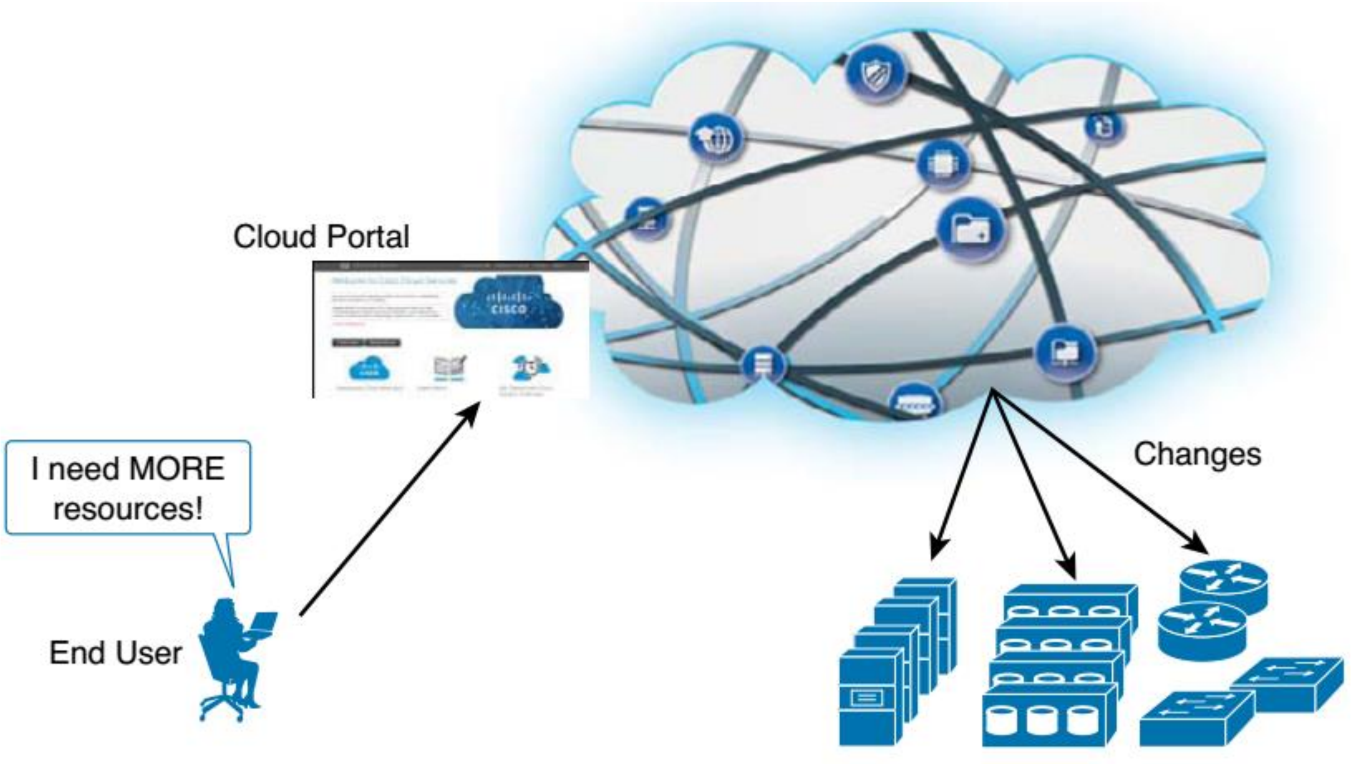
- **Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.**
- **Five essential characteristics that all cloud computing scenarios must share:**
  - **On-demand self-service**
  - **Rapid elasticity**
  - **Resource pooling**
  - **Measured service**
  - **Broad network access**

On-Demand Self-Service



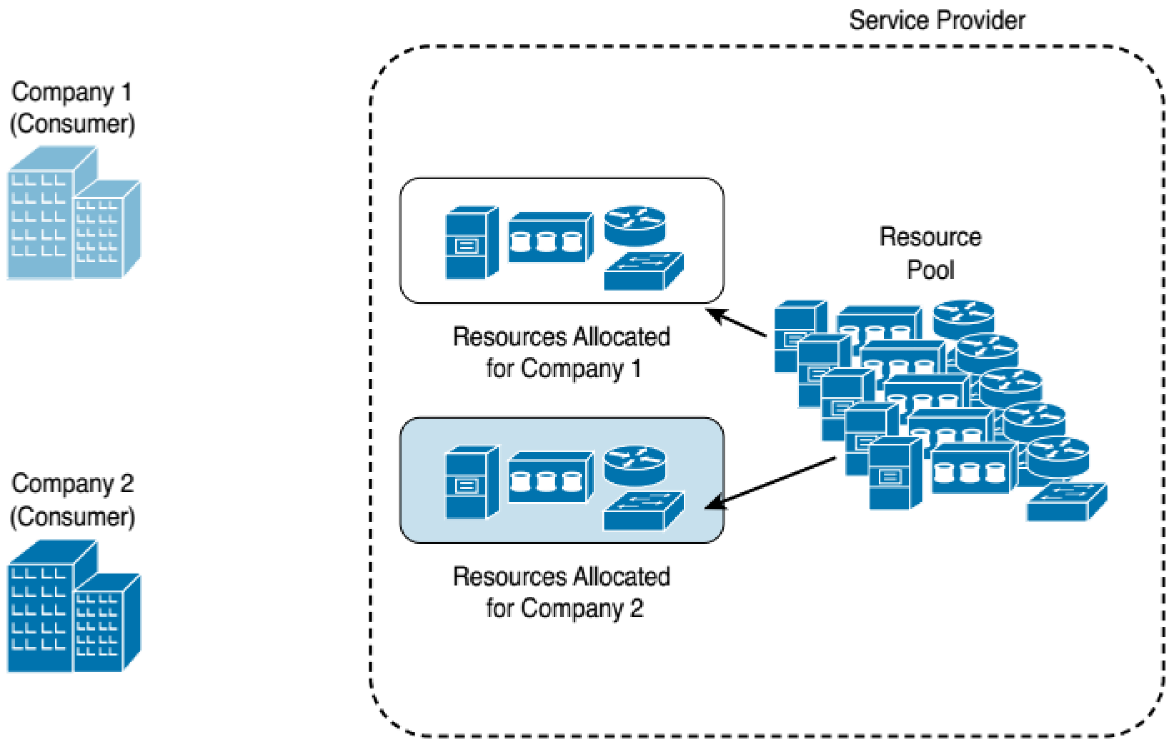
On-demand self-service means end users “can unilaterally provision computing capabilities…as needed automatically without requiring human interaction with each service provider”.

Rapid Elasticity



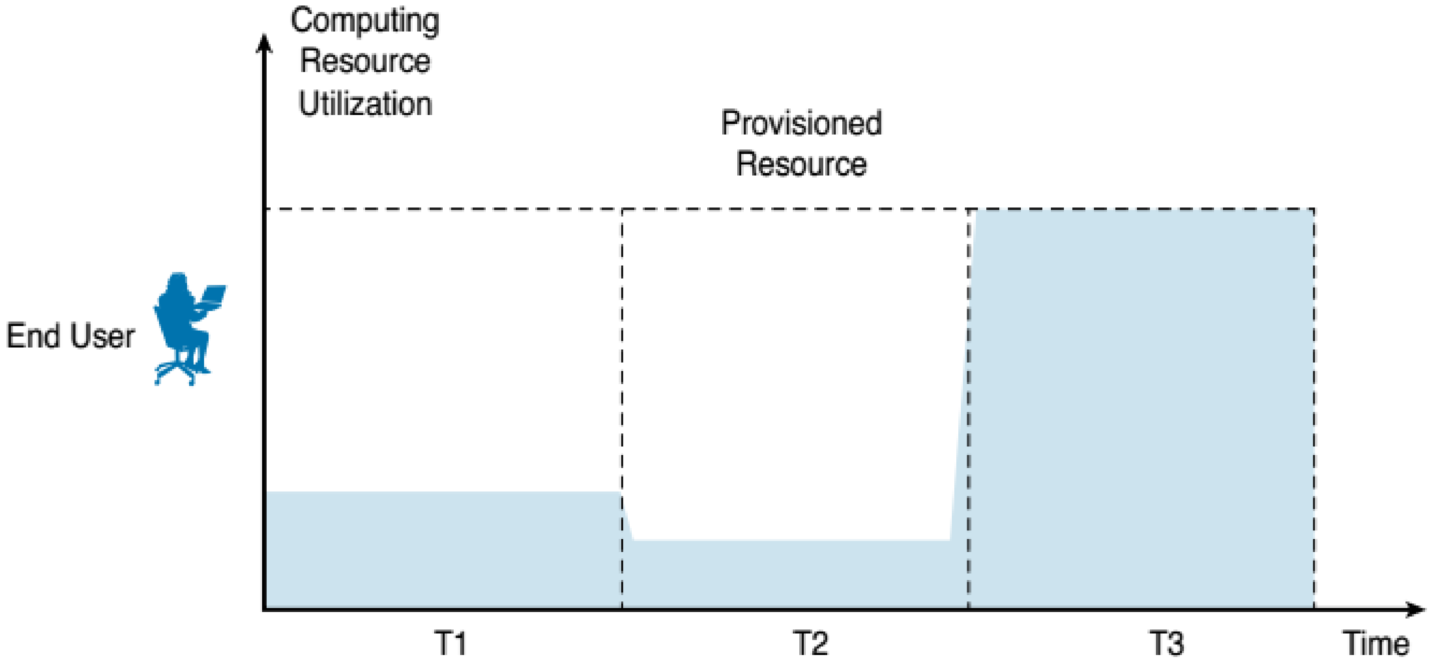
Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

Resource Pooling



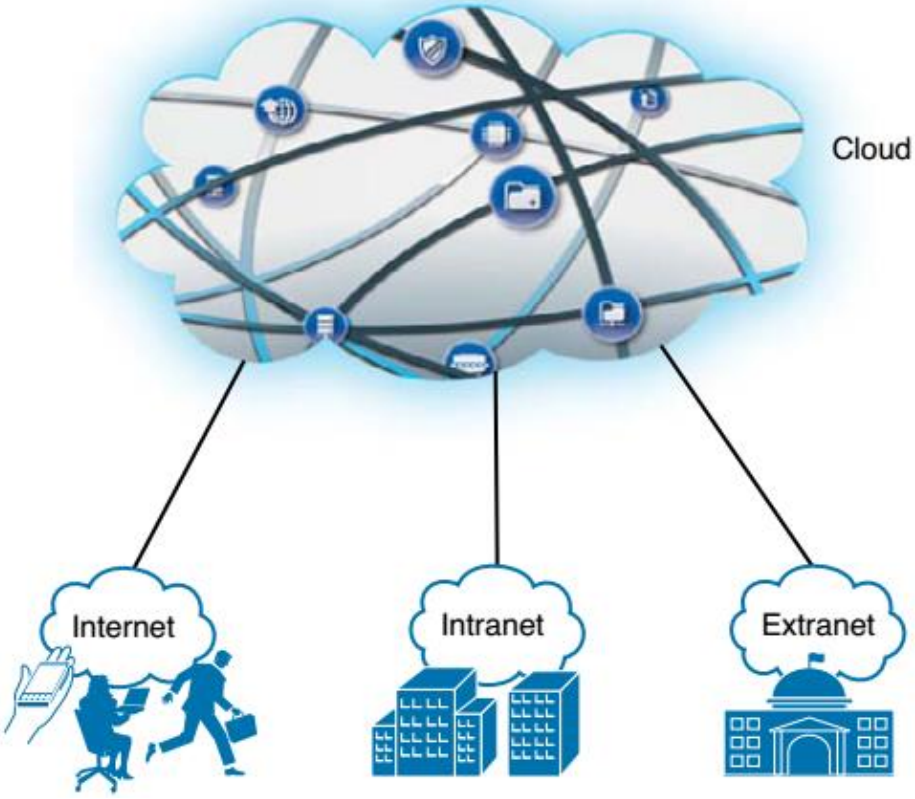
- **The grouping of resources to maximize advantages and minimize risks for the users of those resources.**
- **In IT, *resource pooling* refers to a set of computing resources (such as storage, processing, memory, and network bandwidth) that work in tandem as one big resource shared by many users.**

Measured Service



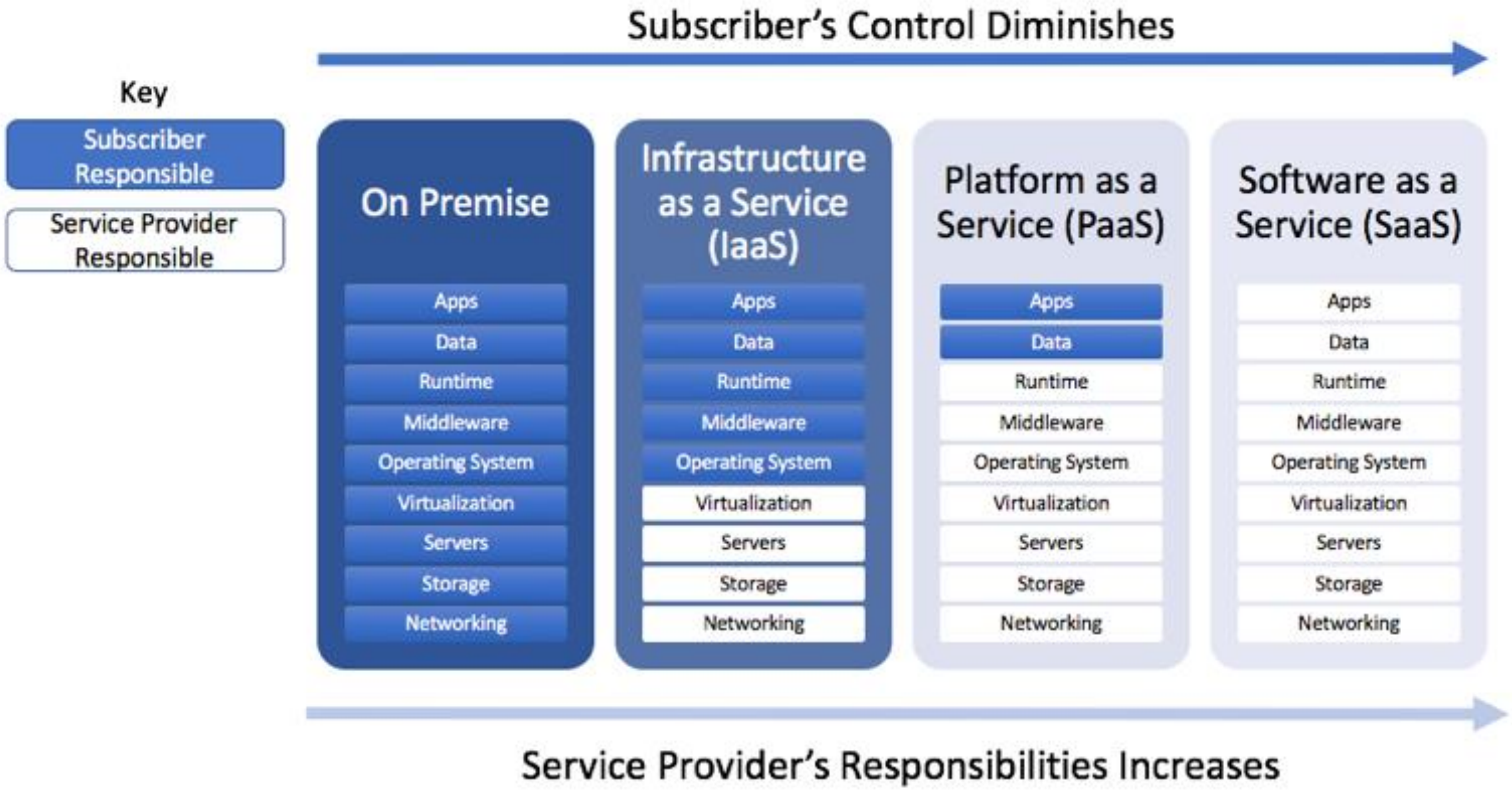
Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts)

Broad Network Access



Cloud services must be available over at least one of these networks and should be accessible through standard mechanisms compatible with the largest majority of client platforms, including smartphones, tablets, laptops, and workstations.

Service Models



Subscriber's Control Diminishes

Key

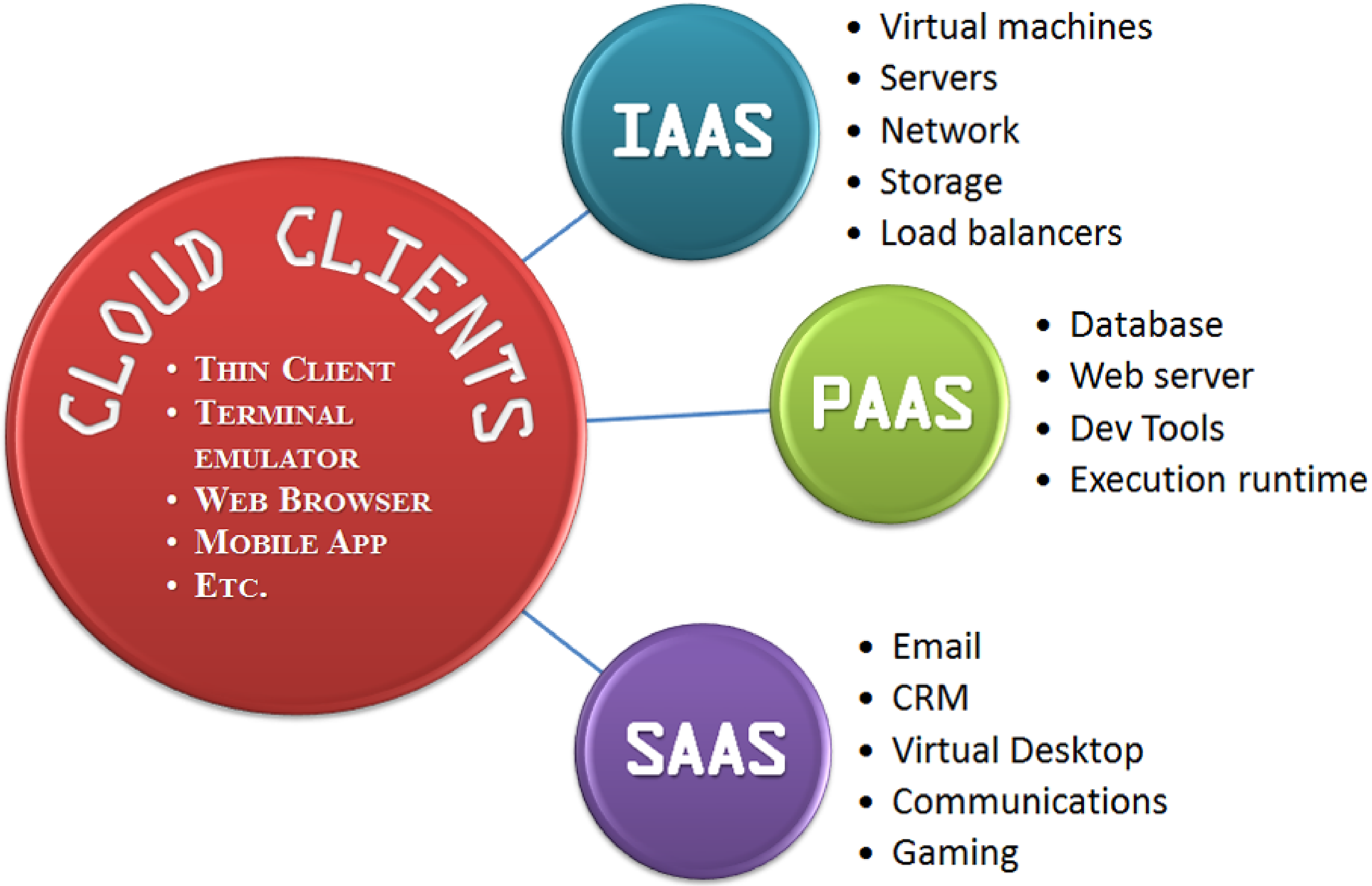
🟦 Subscriber Responsible

⬜ Service Provider Responsible

On Premise	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟦 Apps	🟦 Apps	🟦 Apps	⬜ Apps
🟦 Data	🟦 Data	🟦 Data	⬜ Data
🟦 Runtime	🟦 Runtime	⬜ Runtime	⬜ Runtime
🟦 Middleware	🟦 Middleware	⬜ Middleware	⬜ Middleware
🟦 Operating System	🟦 Operating System	⬜ Operating System	⬜ Operating System
🟦 Virtualization	⬜ Virtualization	⬜ Virtualization	⬜ Virtualization
🟦 Servers	⬜ Servers	⬜ Servers	⬜ Servers
🟦 Storage	⬜ Storage	⬜ Storage	⬜ Storage
🟦 Networking	⬜ Networking	⬜ Networking	⬜ Networking

Service Provider's Responsibilities Increases

Service Models (Cont)



CLOUD CLIENTS

- Thin Client
- Terminal emulator
- Web Browser
- Mobile App
- Etc.

IAAS

- Virtual machines
- Servers
- Network
- Storage
- Load balancers

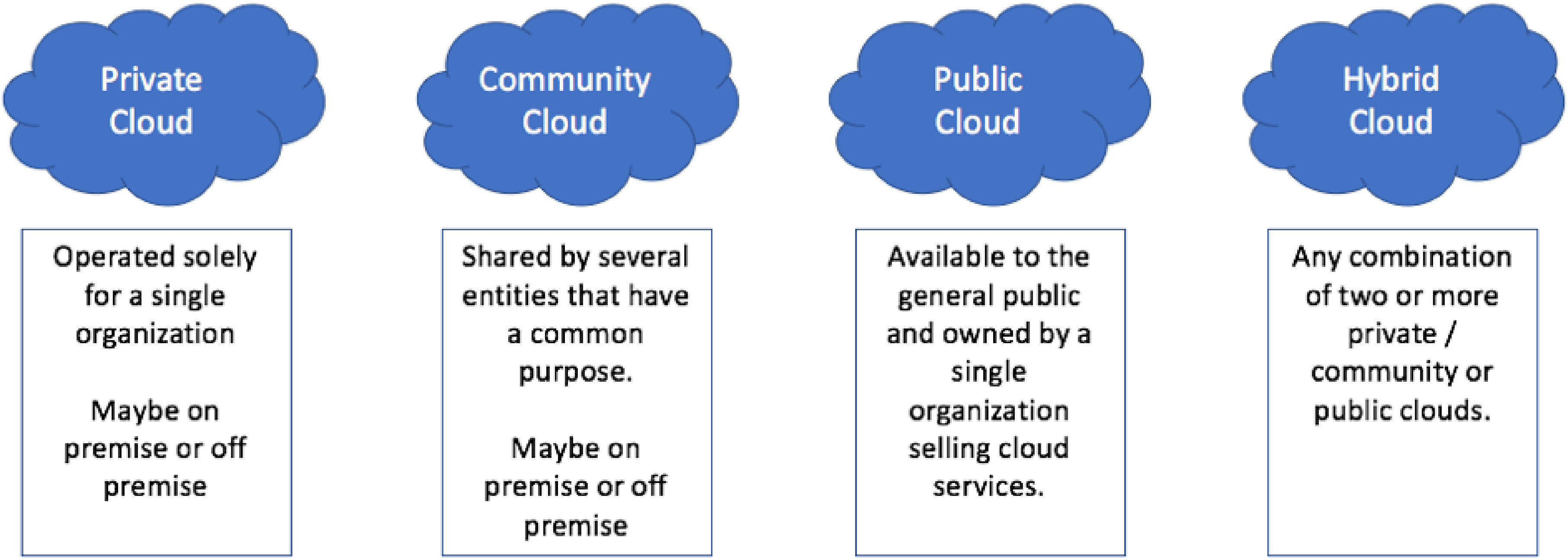
PAAS

- Database
- Web server
- Dev Tools
- Execution runtime

SAAS

- Email
- CRM
- Virtual Desktop
- Communications
- Gaming

Deployment Models



Private Cloud

Operated solely for a single organization

Maybe on premise or off premise

Community Cloud

Shared by several entities that have a common purpose.

Maybe on premise or off premise

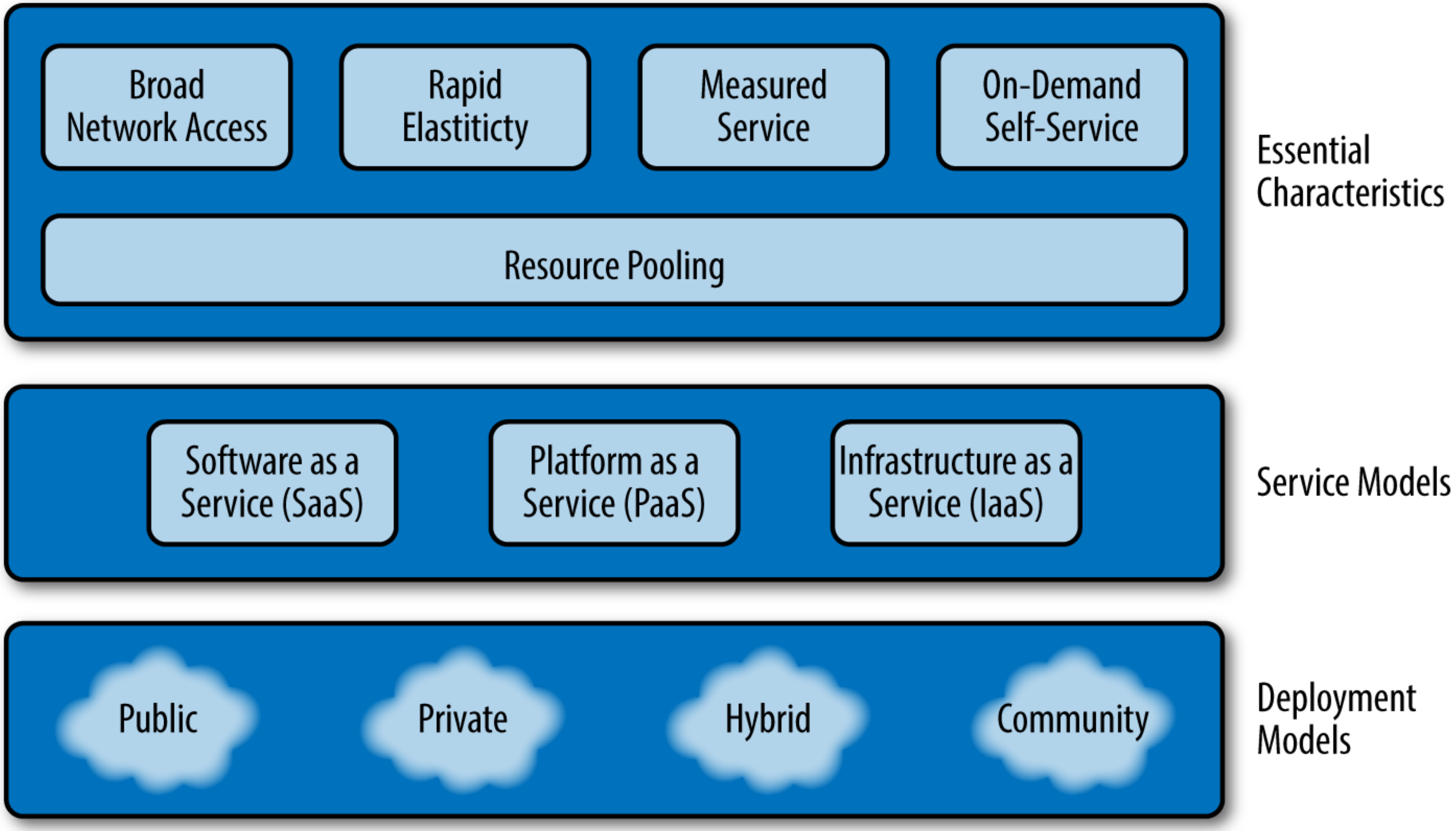
Public Cloud

Available to the general public and owned by a single organization selling cloud services.

Hybrid Cloud

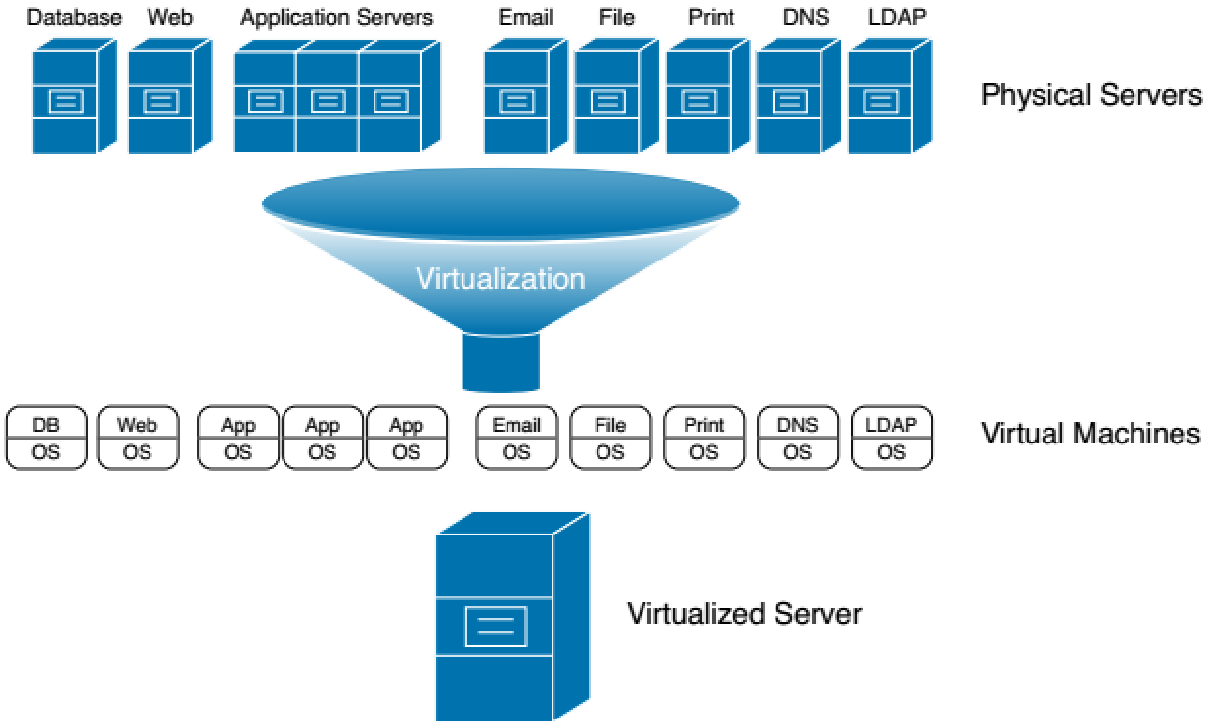
Any combination of two or more private / community or public clouds.

CLOUD COMPUTING



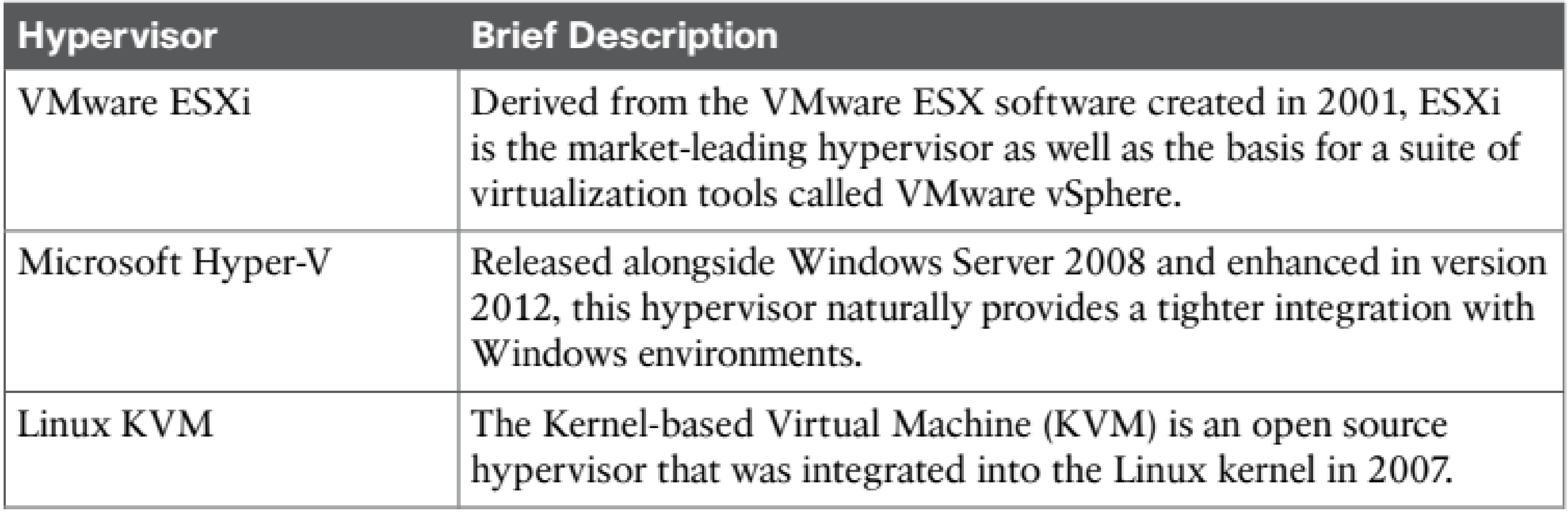
Introducing Server Virtualization

Server virtualization



- **Virtualization technique that involves partitioning a physical server into a number of small, virtual servers with the help of virtualization software.**
- **In server virtualization, each virtual server runs multiple operating system instances at the same time.**

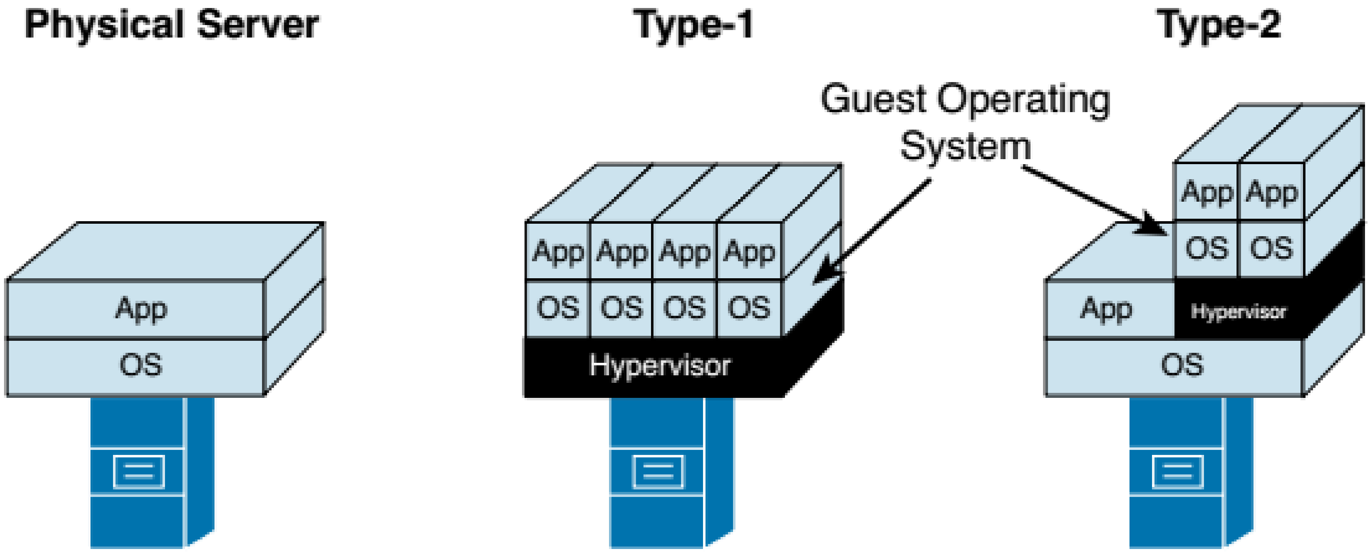
Hypervisor



Hypervisor	Brief Description
VMware ESXi	Derived from the VMware ESX software created in 2001, ESXi is the market-leading hypervisor as well as the basis for a suite of virtualization tools called VMware vSphere.
Microsoft Hyper-V	Released alongside Windows Server 2008 and enhanced in version 2012, this hypervisor naturally provides a tighter integration with Windows environments.
Linux KVM	The Kernel-based Virtual Machine (KVM) is an open source hypervisor that was integrated into the Linux kernel in 2007.

- **A hypervisor can be defined as a software component that can create emulated hardware (including CPU, memory, storage, networking, and peripherals, among other components) for the installation of a guest operating system.**
- **In the context of server technologies, a hypervisor is essentially a program that allows the creation of virtual servers.**

Hypervisor Types



- A Type- 1 hypervisor replaces the operating system as the software component that directly controls the hardware, and for this reason it is also known as a native or bare-metal hypervisor.

- A Type-2 hypervisor runs over a preexisting operating system. Also known as hosted hypervisors.

Introducing NGFW & NGIPS

Firewall

- Are resistant to attack
- Are the only transit point between networks because all traffic flows through the firewall
- Enforce the access control policy

Firewall Type:

- Packet filtering
- Stateful inspection
- Application Gateway Firewall

Intrusion Prevention System

- An intrusion prevention system (IPS) is a system that monitors a network for malicious activities such as security threats or policy violations.
- The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.

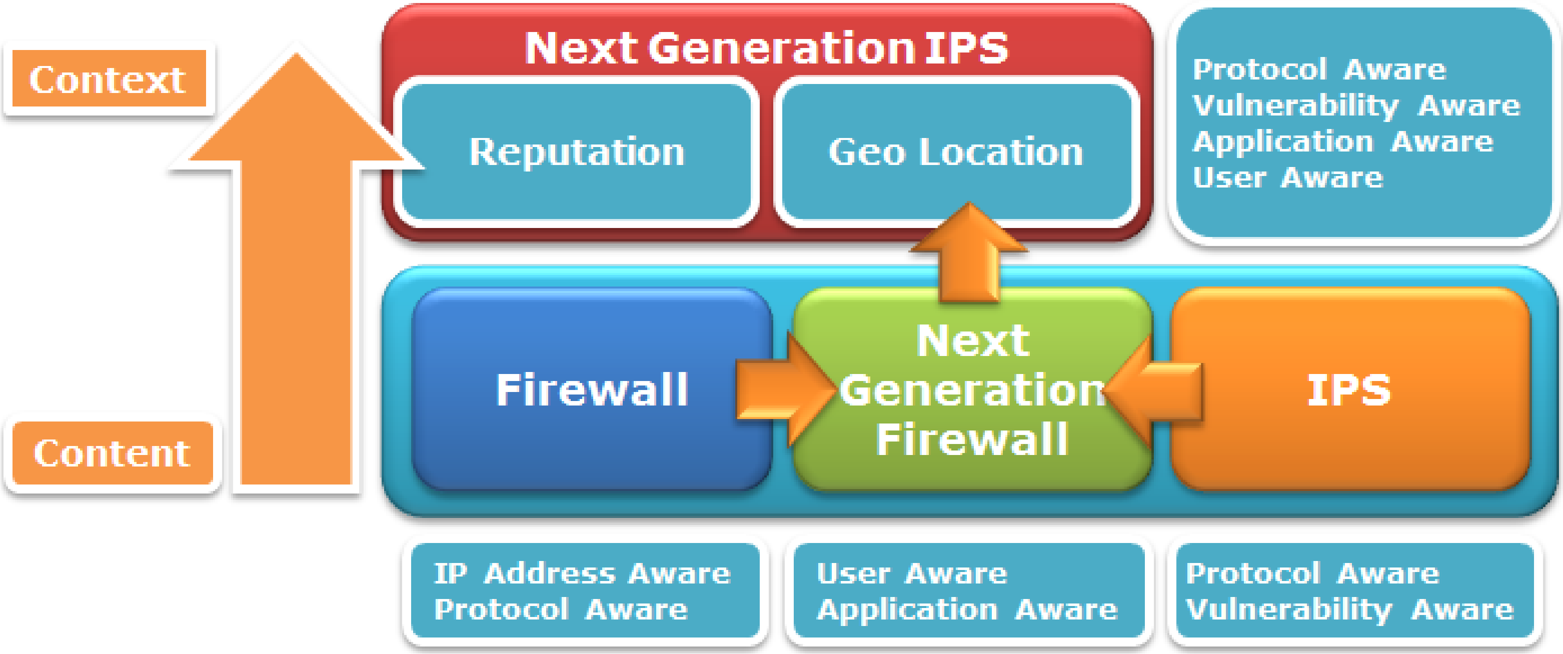
IPS Detection Methods

- Signature-based detection: Signature-based IDS monitors packets in the network and compares with predetermined attack patterns, known as “signatures”.
- Statistical anomaly-based detection: An anomaly-based IDS will monitor network traffic and compare it to expected traffic patterns.
- Stateful protocol analysis detection: This method identifies protocol deviations by comparing observed events with pre-determined activity profiles of normal activity.

Next Generation Firewall

- Granular identification, visibility, and control of behaviors within applications.
- Restricting web and web application use based on the reputation of the site.
- Proactive protection against Internet threats.
- Enforcement of policies based on the user, device, role, application type, and threat profile.
- Performance of NAT, VPN, and SPI.
- Use of an IPS.

NGFW & NGIPS

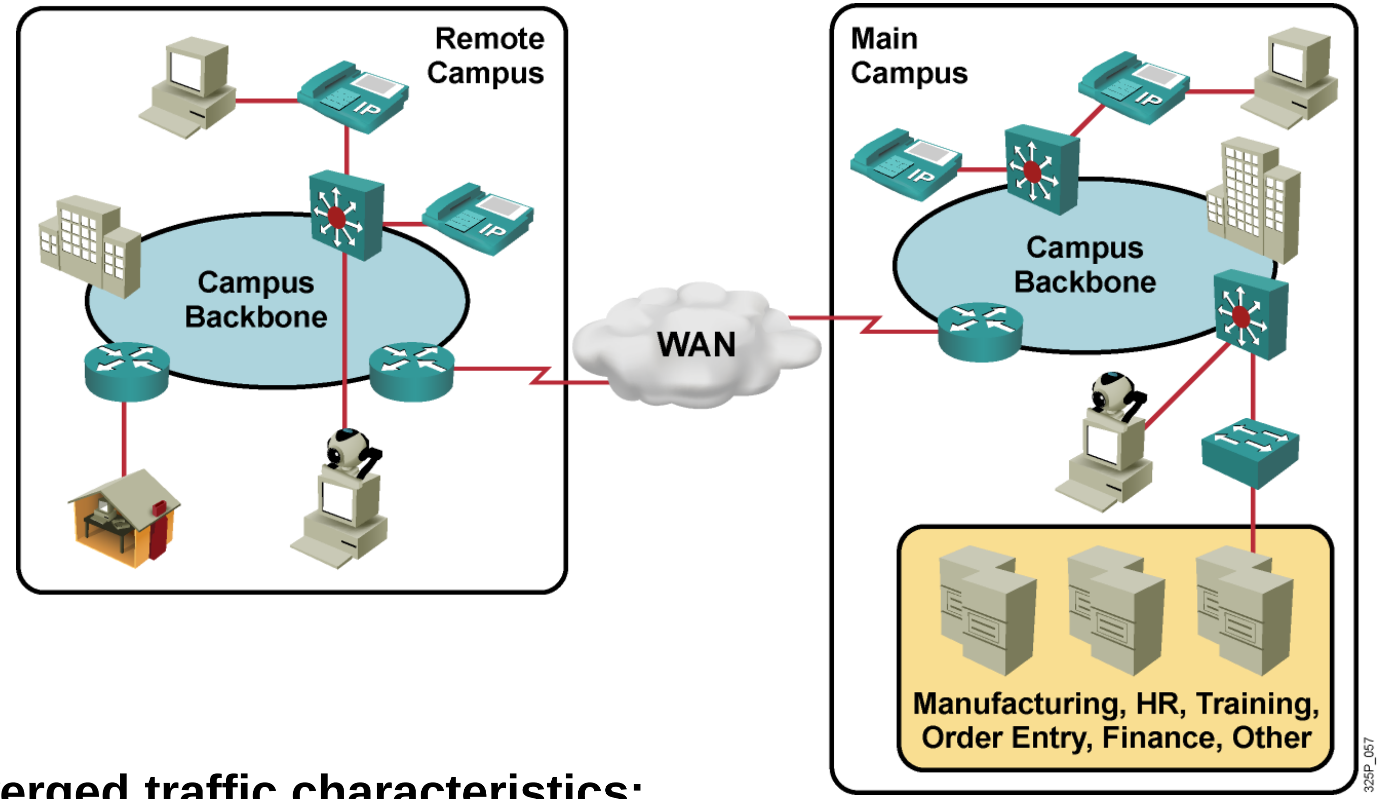


NG-IPSs are characterized by two main features:

- **They shift the enforcement of security policies from a content-based to a context-based model (where the context is defined by the interaction of user with applications);**
- **They leverage new technologies such as reputation and geo-location to provide the holistic view necessary to stop APTs.**

Introducing QoS

Converged Network Quality Issues



Converged traffic characteristics:

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

Converged Network Quality Issues (Cont.)

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

QoS Defined

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

325P_068

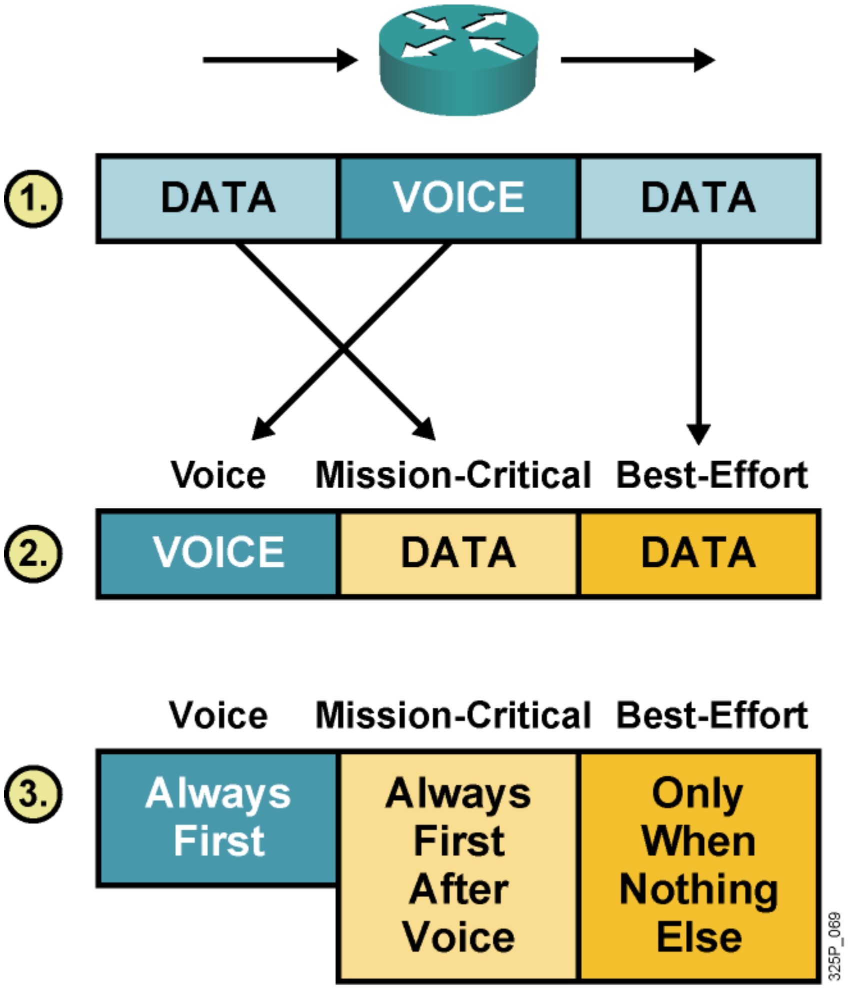
Voice – Video – Data

↓

Consistent and Predictable Performance

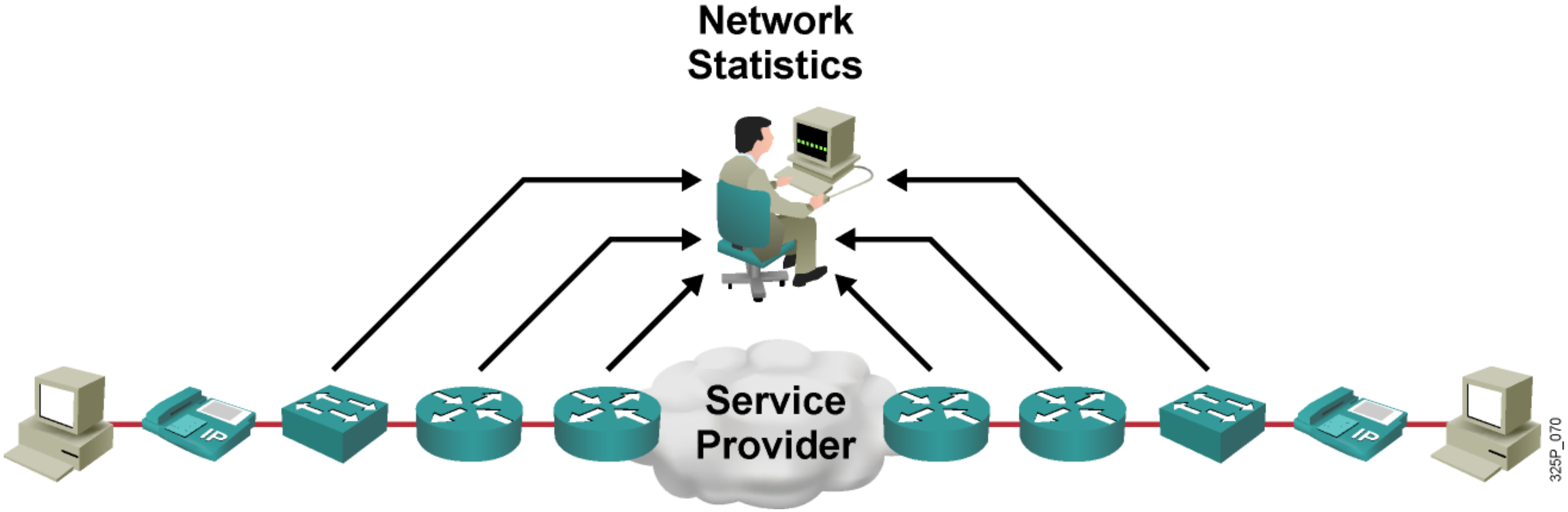
Implementing QoS

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

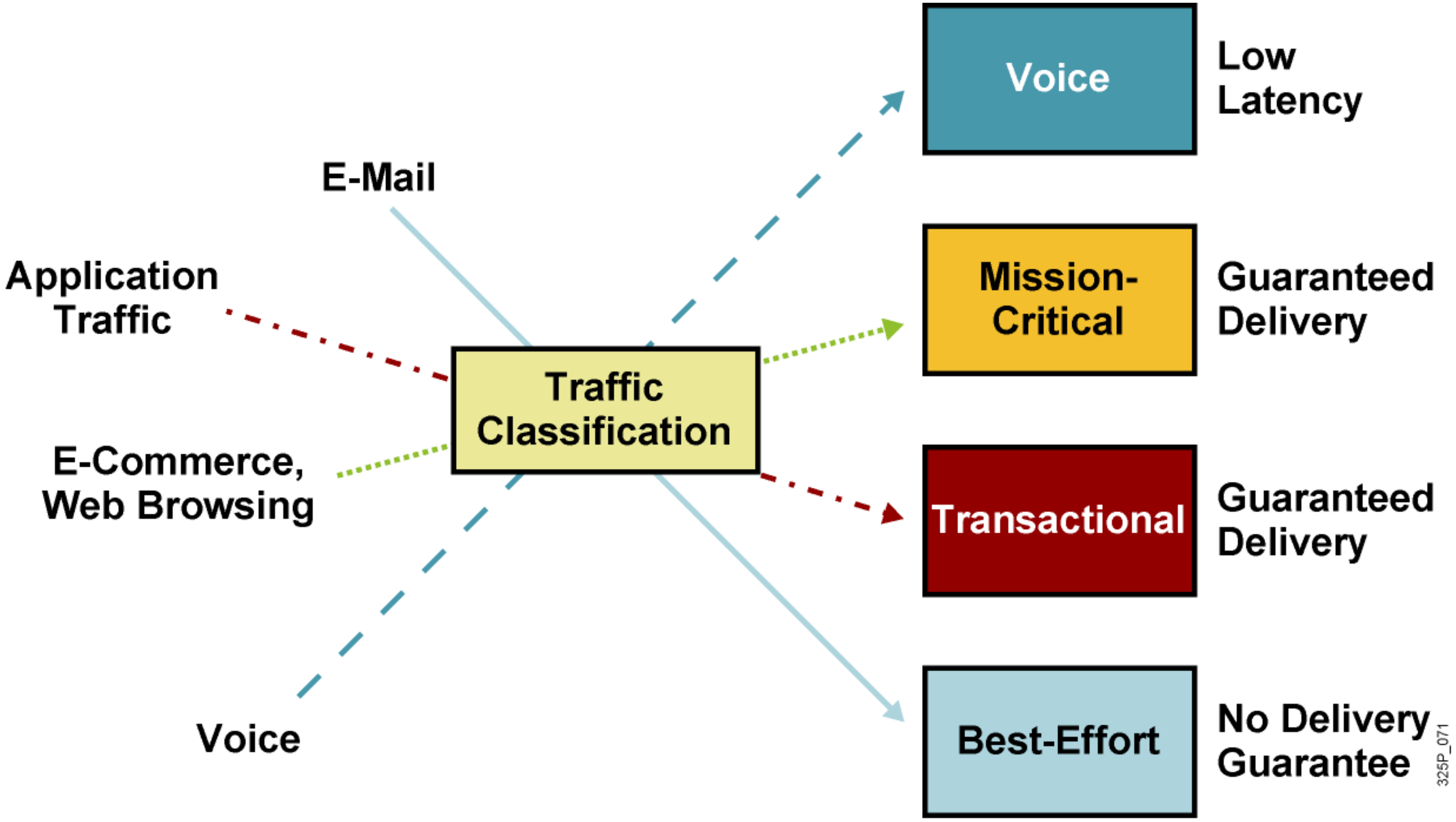


Identify Traffic and Its Requirements

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

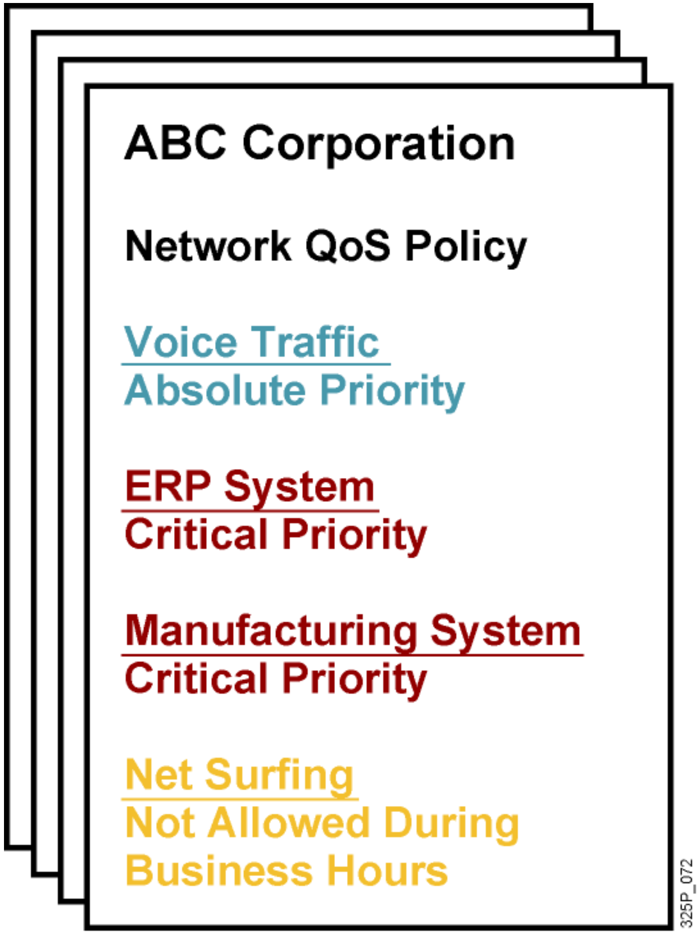


The Requirements of Different Traffic Types



QoS Policy

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



ABC Corporation

Network QoS Policy

Voice Traffic
Absolute Priority

ERP System
Critical Priority

Manufacturing System
Critical Priority

Net Surfing
Not Allowed During
Business Hours

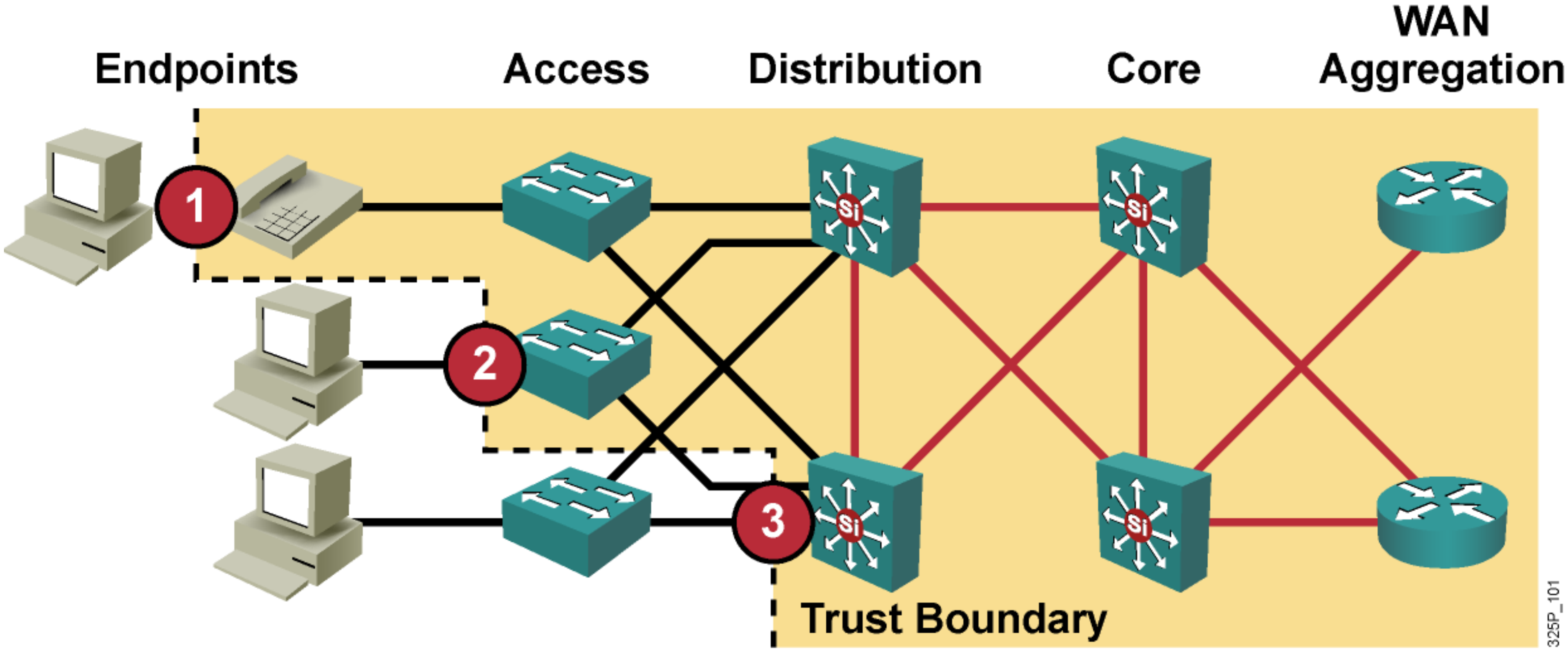
Classification

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

Marking

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

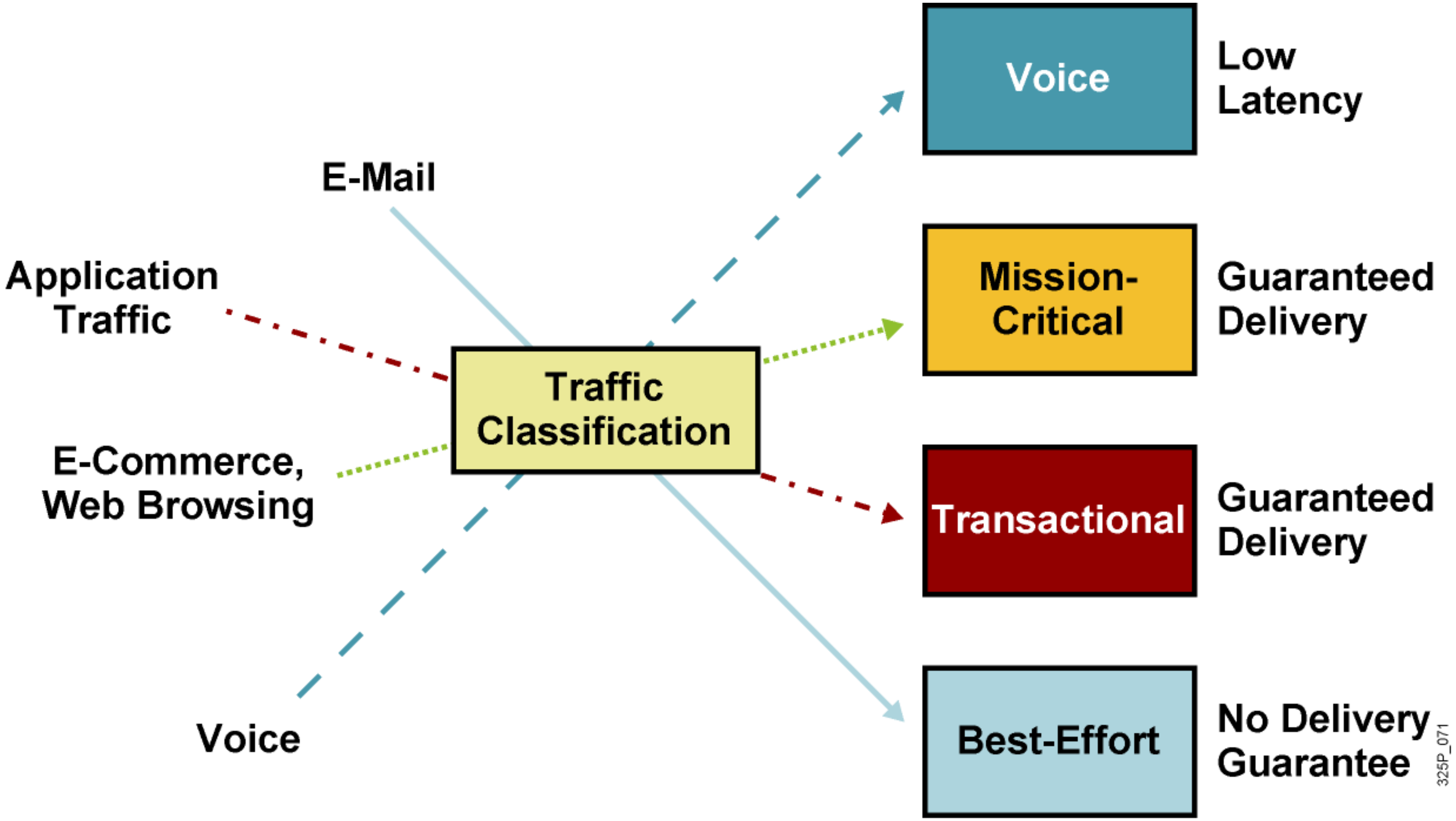
Trust Boundaries: Classify Where?



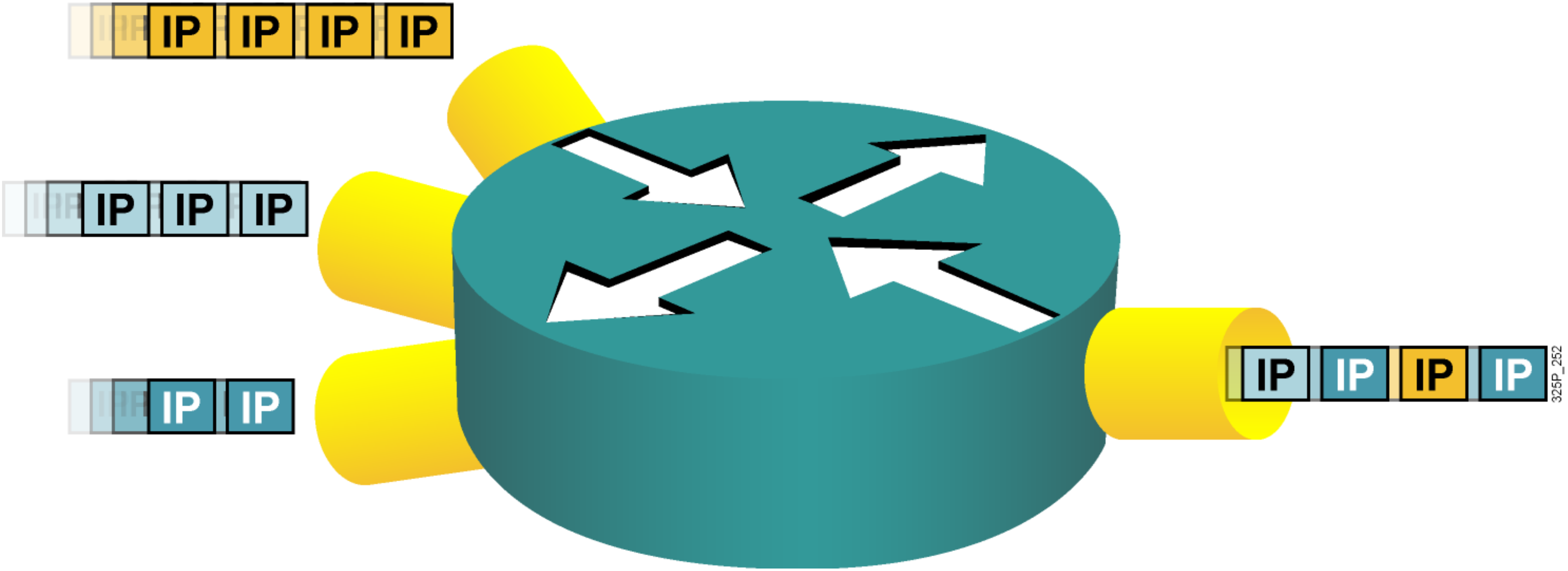
For scalability, classification should be enabled as close to the edge as possible, depending on the capabilities of the device at:

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

Implementing QoS Policy Using a QoS Service Class

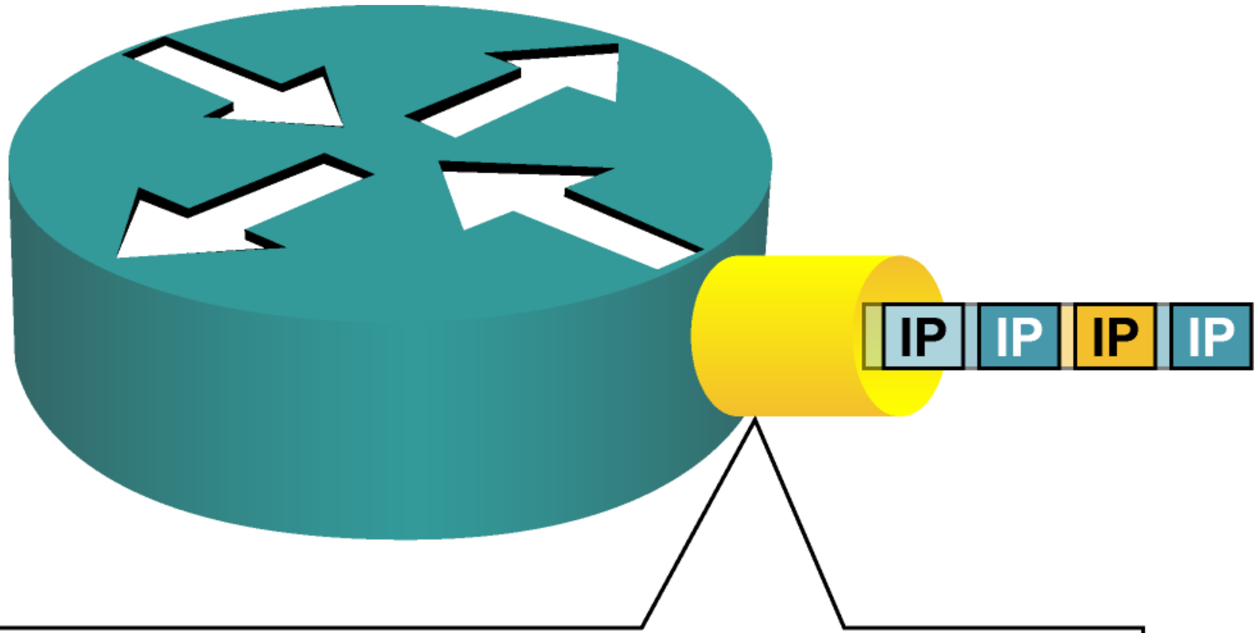


Congestion and Queuing



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

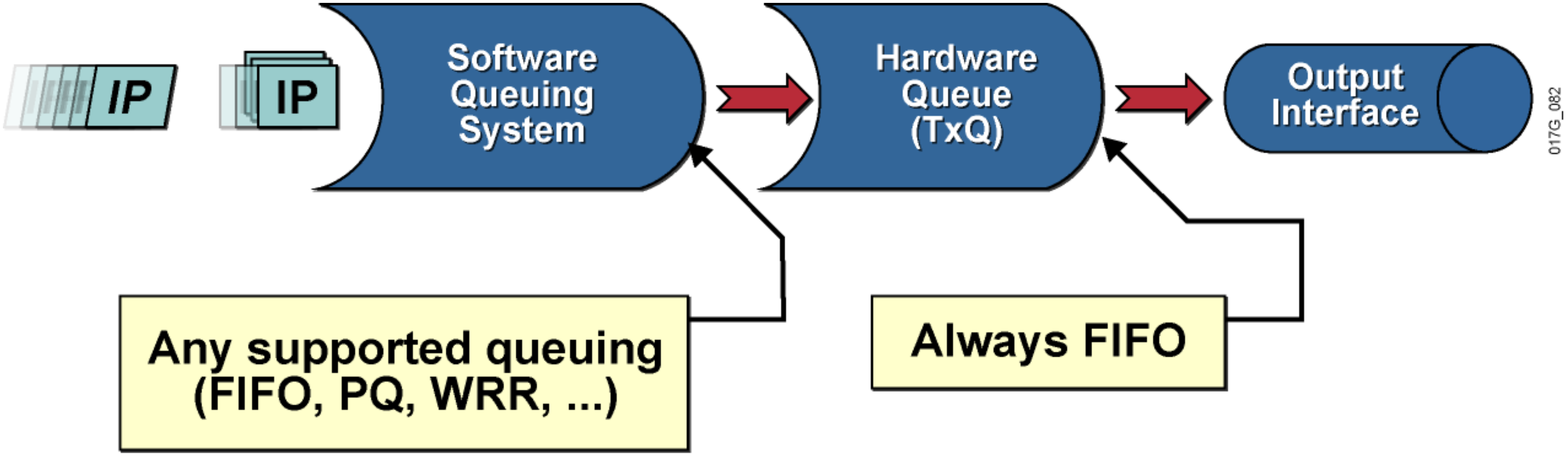
Congestion and Queuing



To avoid congestion, queuing mechanisms are activated
at the hardware buffer of the outgoing interface

Queuing Algorithms

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



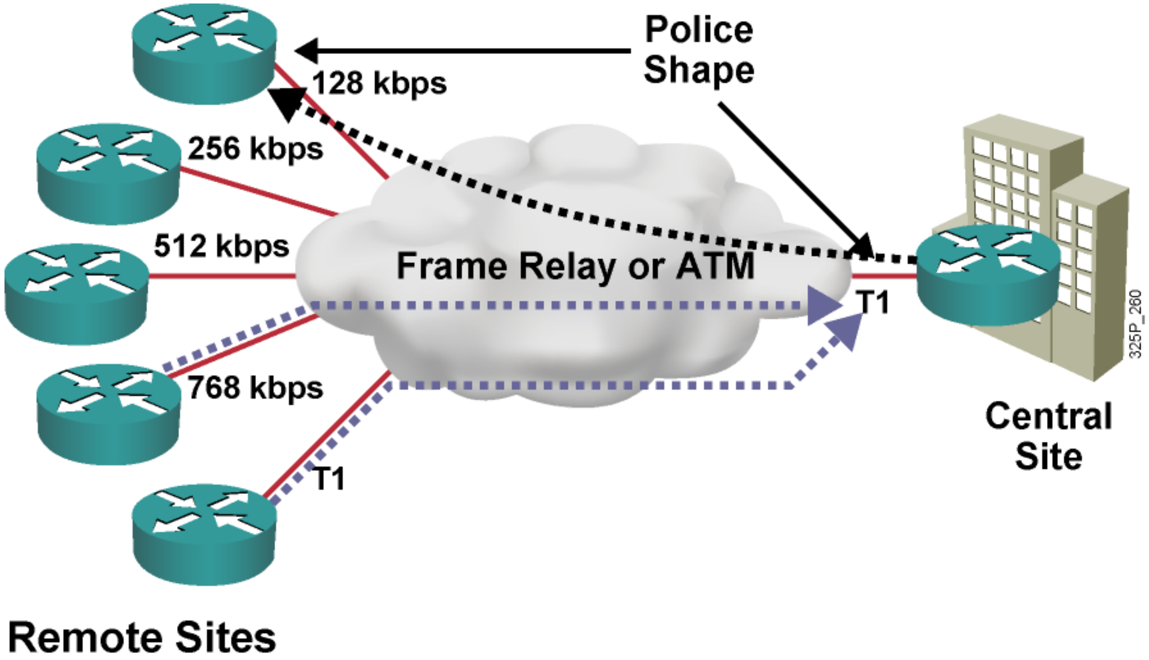
Why Use Shaping?

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

Why Use Policing?

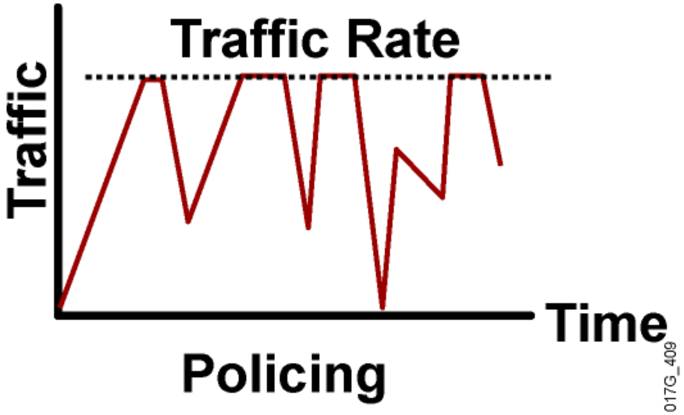
- To limit access to resources when high-speed access is used but not desired (subrate access)
- To limit the traffic rate of certain applications or traffic classes
- To mark down (recolor) exceeding traffic at Layer 2 or Layer 3

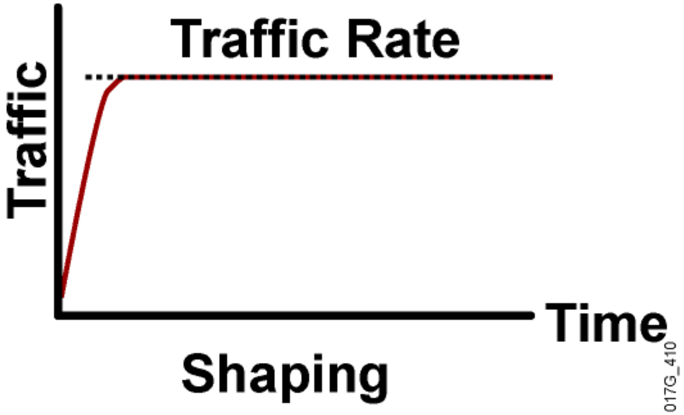
Traffic Policing and Shaping Example



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

Policing vs. Shaping





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

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

CISCO