Network Services

DOMAIN 1.0

MODULE 5

Network Services Topics

DHCP

DNS

NTP

Corporate and Datacenter Network Architecture

Cloud Concepts and Connectivity Options

DHCP

Dynamic Host Configuration Protocol (DHCP)

An automated way to assign IP addresses to hosts on a network

Based on the earlier BOOTP protocol

Client issues a Layer 2 broadcast to request an IP address from any listening DHCP server

Server has pre-configured pool of available IP addresses

Server “leases” an address for a limited time to the client

Communications are in clear text with no authentication

Server port = UDP 67

Client port = UDP 68

DHCP DORA Process

Layer 2 Broadcast

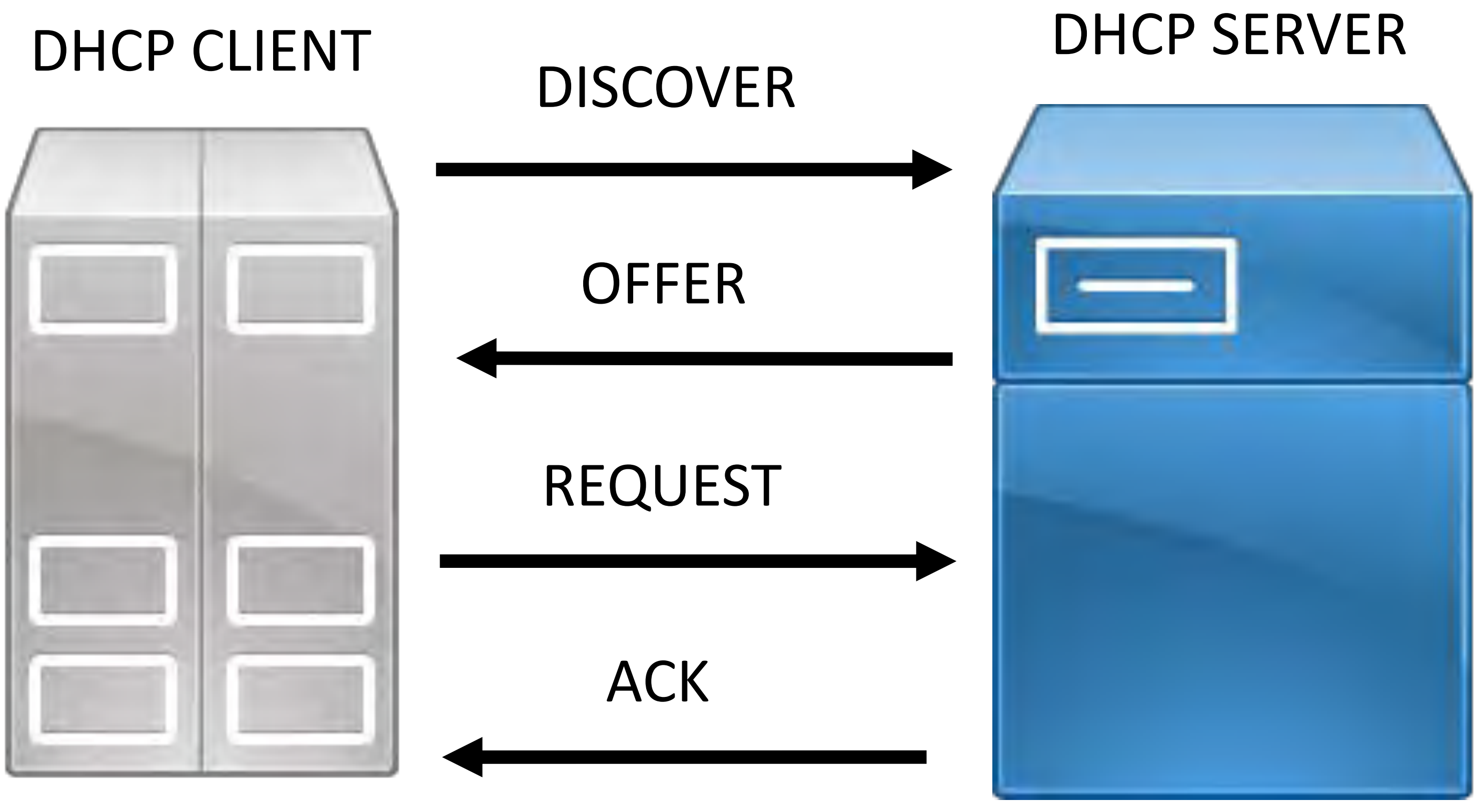
Lease can be limited time or indefinite

Lease will include:

- IP Address
- Subnet Mask

Lease can include options:

- Default Gateway
- DNS Server(s)
- DNS Domain Name
- Other options



Scope

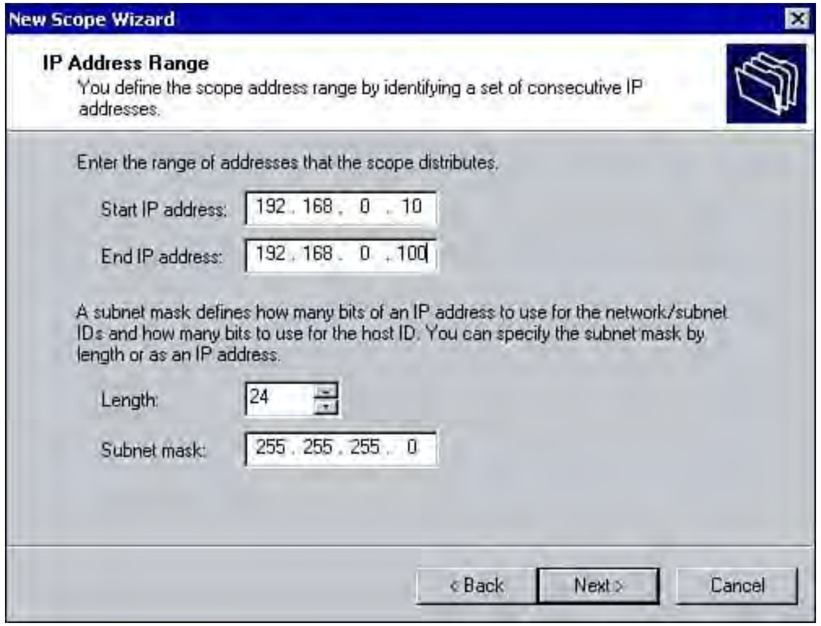
A DHCP scope is a set of configurations for a particular network segment

The scope is defined by its range of IP addresses and subnet mask

u cant chang3e tthe subnet mask

Contains the pool of addresses that can be leased to clients

After a scope is created, any of its settings can be modified except for the subnet mask



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 0 . 10

End IP address: 192 . 168 . 0 . 100

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

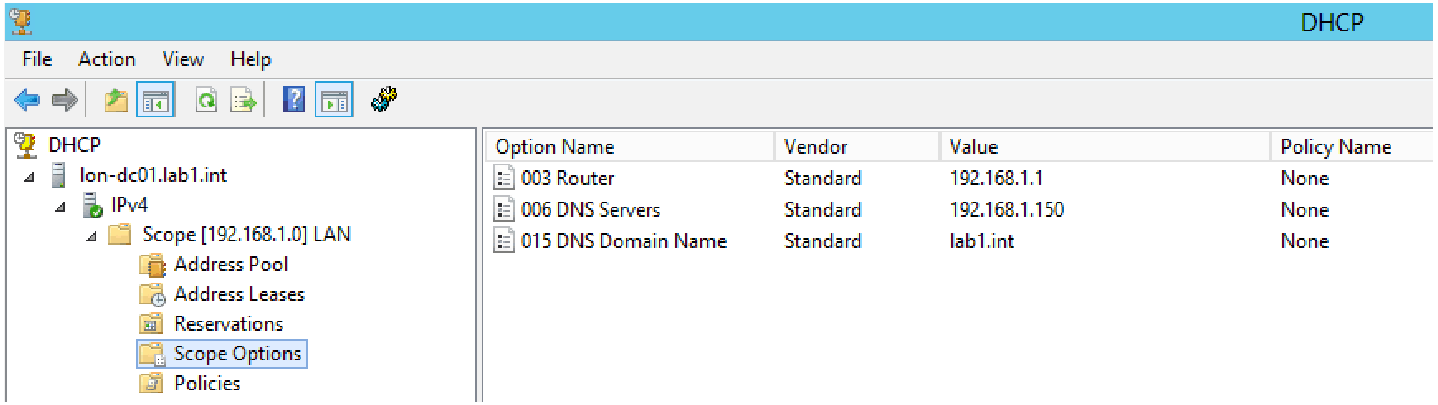
Scope Options

Scope options are additional information for the clients:

- Address of the default gateway
- Domain name to be used (a favorite technique of ISPs)
- Address of the WINS server (deprecated Microsoft LAN name resolution server)
- NetBIOS node type (deprecated)

Scopes also have other configuration options such as lease time, reservations, and exclusions

A DHCP server will have one scope for each network segment/subnet it services



Option Name	Vendor	Value	Policy Name
003 Router	Standard	192.168.1.1	None
006 DNS Servers	Standard	192.168.1.150	None
015 DNS Domain Name	Standard	lab1.int	None

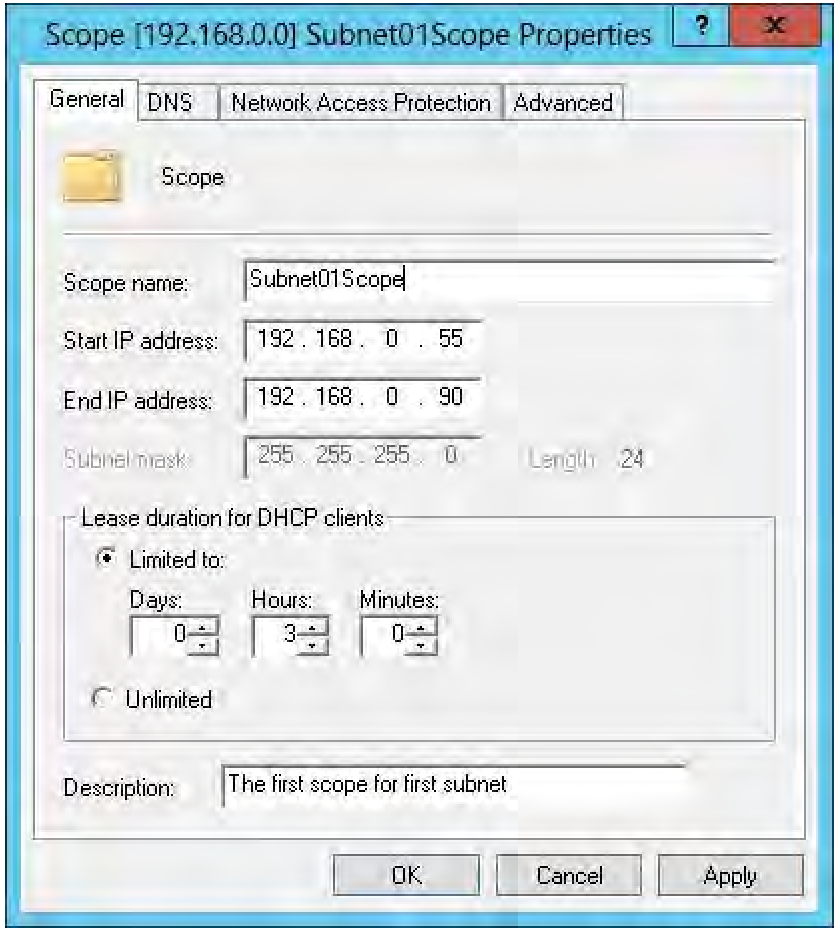
DHCP Lease Time

The length of time (in days or hours) that a client may use the IP address

The client is responsible for enforcing the lease and attempting to renew the lease before the lease time is up

If a client does not renew its lease, the DHCP server marks the address as potentially unused

- Eventually the IP address is returned to the pool for another client to use


Scope [192.168.0.0] Subnet01Scope Properties
?
✕
General
DNS
Network Access Protection
Advanced
Scope
OK
Cancel
Apply

Scope name: Subnet01Scope

Start IP address: 192 . 168 . 0 . 55

End IP address: 192 . 168 . 0 . 90

Subnet mask: 255 . 255 . 255 . 0 Length: 24

Lease duration for DHCP clients

● Limited to:

Days: 0 Hours: 3 Minutes: 0

○ Unlimited

Description: The first scope for first subnet

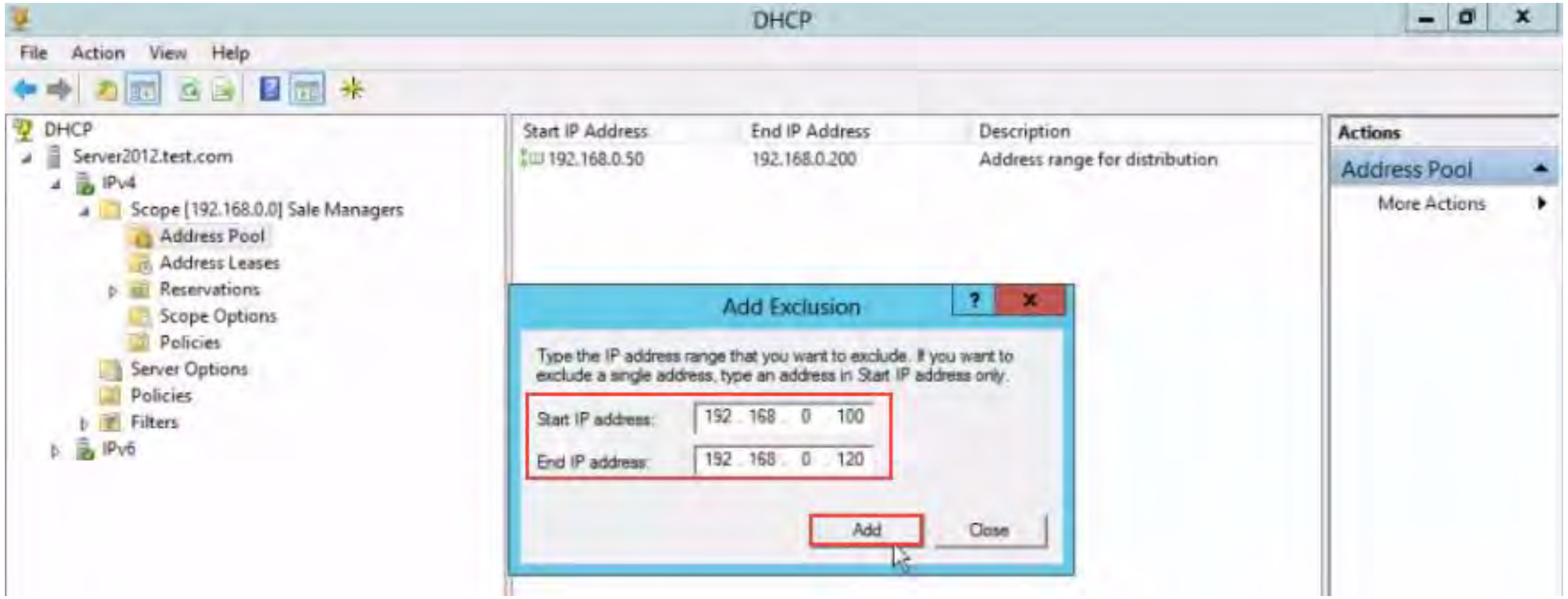
Exclusion Ranges

IP addresses in a subnet range that are set aside for static configuration

Ensures that these addresses are not accidentally leased out to clients

Exclusions often include the first 10, 20, or even more IP addresses in a subnet

Excluded addresses are statically assigned to the router, switches, servers, printers, and clients that cannot use DHCP



Start IP Address	End IP Address	Description
192.168.0.50	192.168.0.200	Address range for distribution

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: 192 . 168 . 0 . 100

End IP address: 192 . 168 . 0 . 120

MAC Reservations

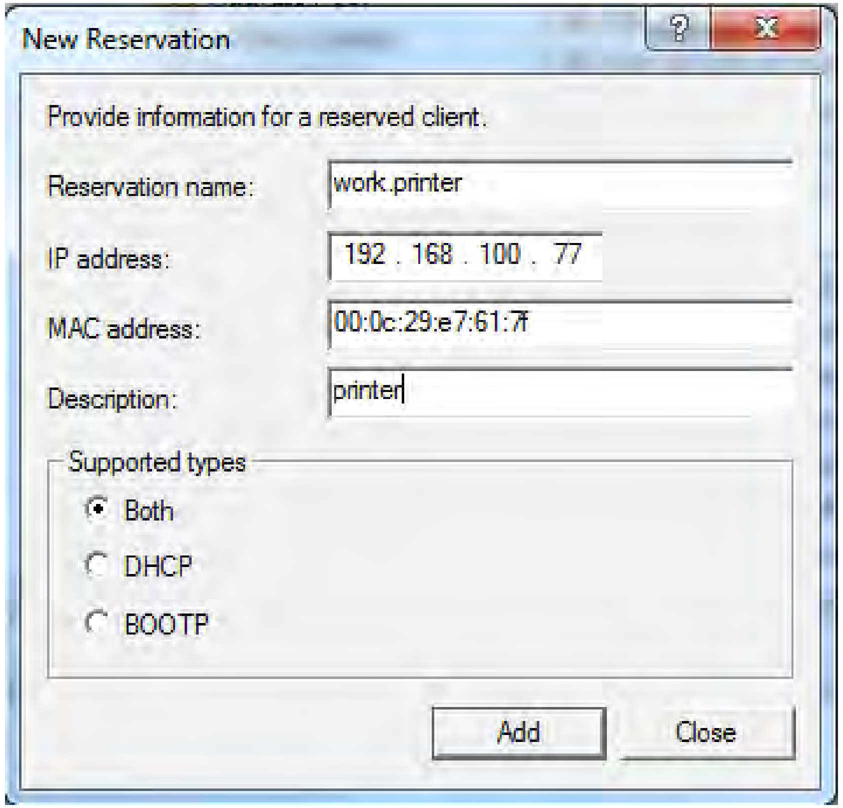
An IP address that is assigned to a specific MAC address

If a client has that MAC address, the server leases it that particular IP address

When the host broadcasts a discover message, the DHCP server checks to see if its MAC address matches any of the reservations

This ensures that the same MAC always gets the same IP address

Useful if you need to ensure that servers always have the same IP address, but that other DCHP configuration options might be updated


New Reservation

Provide information for a reserved client.

Reservation name: work.printer

IP address: 192 . 168 . 100 . 77

MAC address: 00:0c:29:e7:61:7f

Description: printer

Supported types

● Both

○ DHCP

○ BOOTP

DHCP Renewal Process

When 50% of the lease time has expired, the client attempts to contact the DHCP server to request a renewal

If the server does not respond, the client tries again at 87.5% of the lease time

If the server still does not respond, the client issues a DHCP DISCOVER broadcast in hopes of finding any DHCP that will respond

When the lease expires, the client either self-assigns an APIPA address or sets its address to 0.0.0.0

DHCP Relay Agent/IP helper

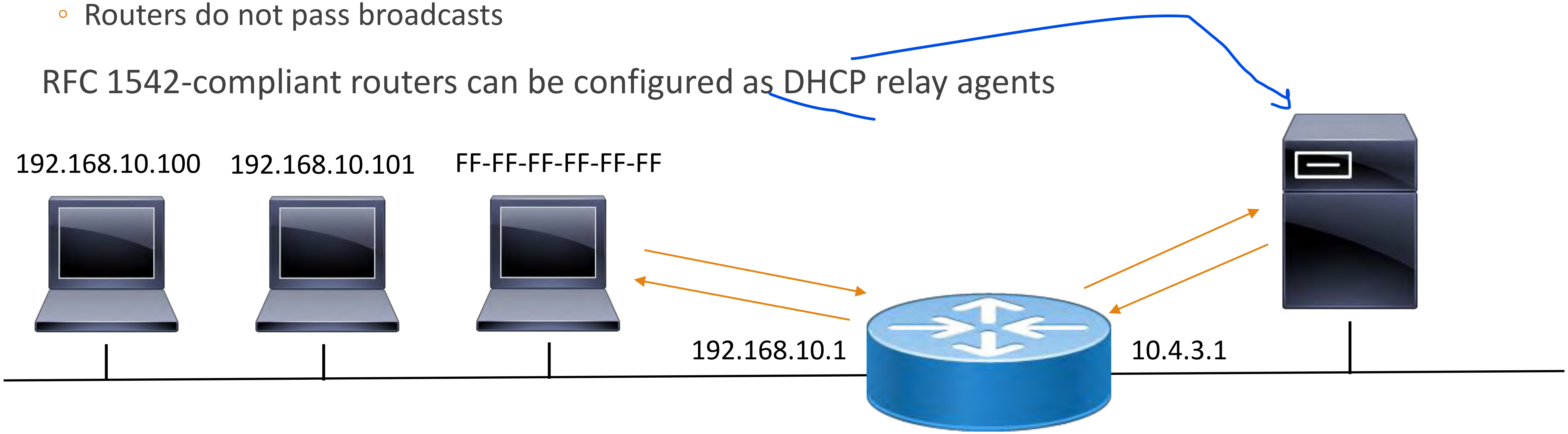
A hardware device or software program that can pass DHCP or BOOTP messages between DHCP clients and servers

- Cisco IP helpers use UDP to carry the DHCP messages

Necessary if the DHCP server is on a different subnet from its clients

- Routers do not pass broadcasts

RFC 1542-compliant routers can be configured as DHCP relay agents



DNS

Domain Name System (DNS)

Maps IP addresses to “friendly” host names

Exists for human convenience

Uses a hierarchical naming scheme

- Places all organizations in that hierarchy (namespace)

Allows IP addresses to change

DNS servers exist at different levels of the namespace

- Database management is distributed
- organizations can manage their own records

Uses UDP and TCP port 53

- UDP for queries
- TCP for zone transfers (replication) between servers

Domain Name System (DNS) (cont’d)

Transmissions are in clear text

Records are stored as plain text files on DNS servers

Types of records – A, AAAA, CNAME, MX, PTR, NS, SOA, SRV, TXT, and others

DNSSEC – accompanying digital signature used to verify authenticity of a record

DNS Terminology

Term	Description
DNS namespace	The entire DNS tree structure, from root to the last subdomain
Zone	a specific portion of the DNS namespace that is managed by a specific organization or administrator Can be comprised of a single node, or related parent and child nodes
Zone file	A plain text file that contains all records for that zone A part of the DNS database
Zone transfer	Replication of a zone file from one DNS server to another
Start of Authority (SOA)	The original DNS server that was used to create the zone Record TTL and zone transfer intervals are defined on this server

DNS Terminology (cont’d)

Term	Description
Authoritative DNS server	Any DNS server with a copy of the zone file
Master (primary) DNS server	A DNS server with a writable copy of the zone file
Slave (secondary) DNS server	A DNS server with a read-only copy of the zone file
Caching DNS server	A DNS server that performs lookups for clients It does not have a copy of the zone, and thus must query other DNS servers It caches a copy of the record for the record’s time to live

DNS Hierarchy

The DNS hierarchy is comprised of the following elements

- Root Level, Top Level Domains, Second Level Domains, Sub-domain, and Hosts

The DNS root zone is the highest level in the DNS hierarchy tree

- It answers the requests for records in the root zone
- Provides a list of authoritative name servers for the appropriate TLD (top-level domain)
- They are the first step in resolving a domain name

The next level in the DNS hierarchy is Top level domains (there are many)

- They are organizational hierarchy and geographic hierarchy

DNS Hierarchy (cont’d)

The next level in the DNS hierarchy is Top level domains (there are many)

- They are organizational hierarchy and geographic hierarchy

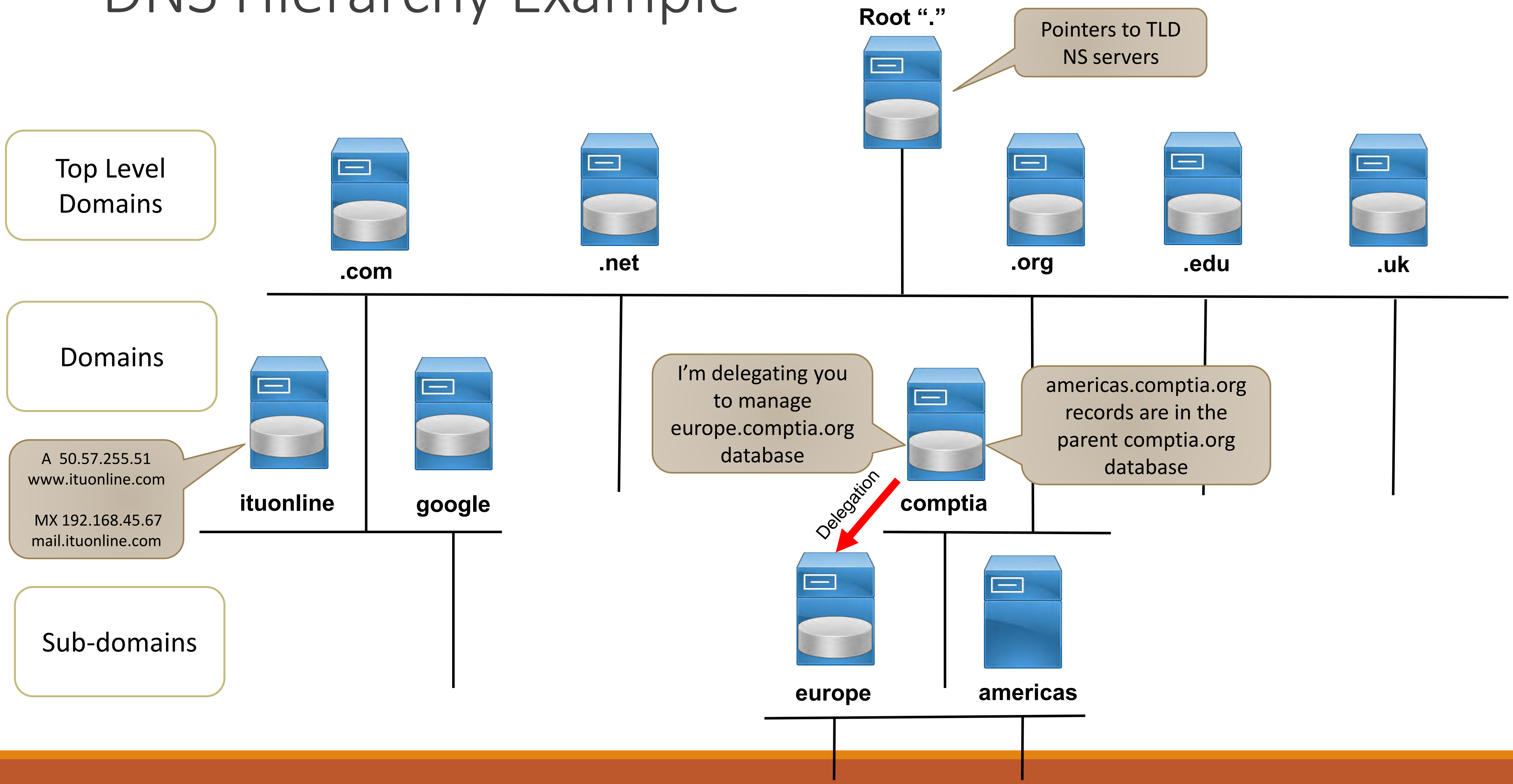
The next level in the DNS hierarchy is the Second Level Domains

- This includes the main part of the domain name

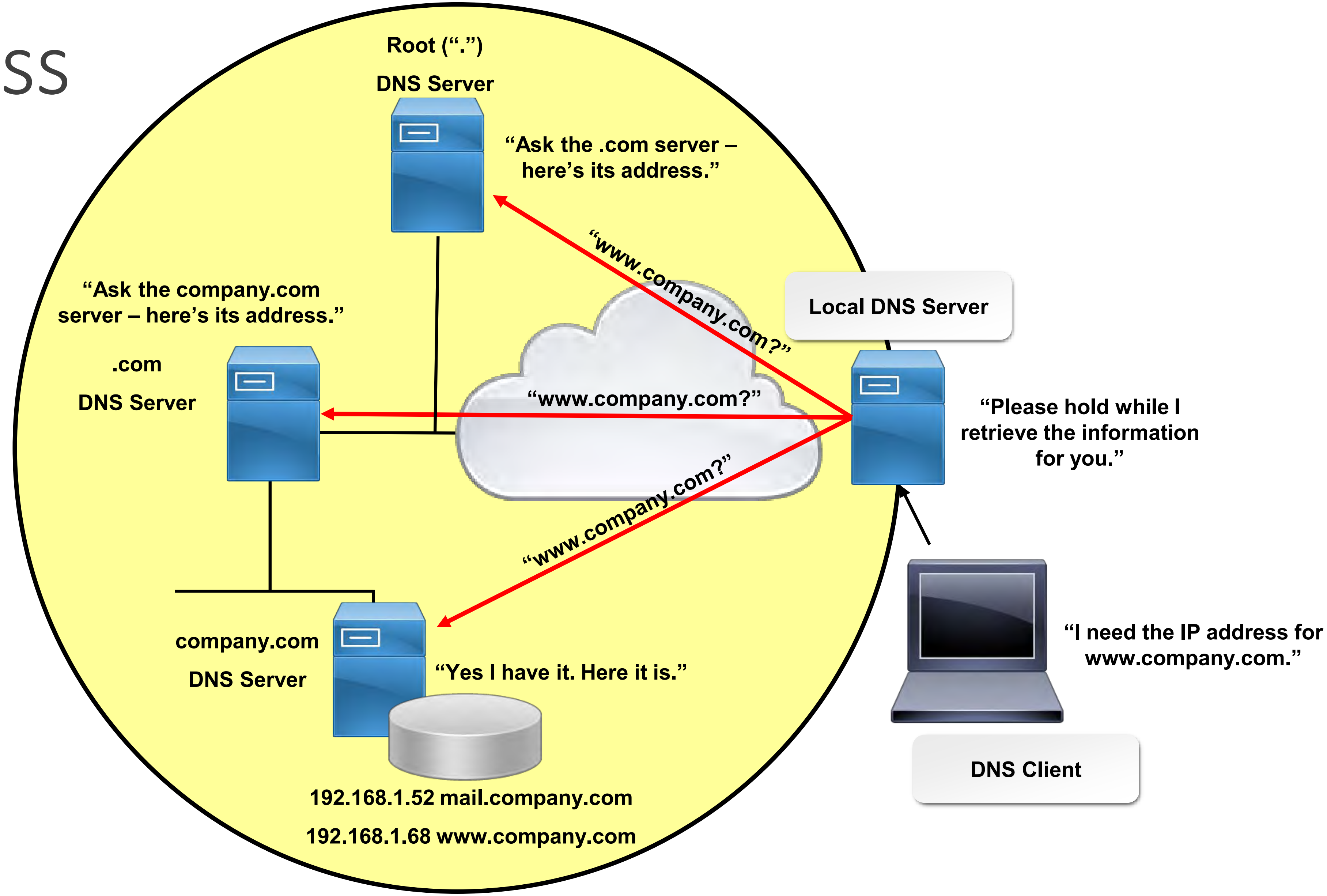
The sub-domain is the next level in the DNS hierarchy

- The sub-domain can be defined as the domain that is a part of the main domain
- The only domain that is not also a sub-domain is the root domain

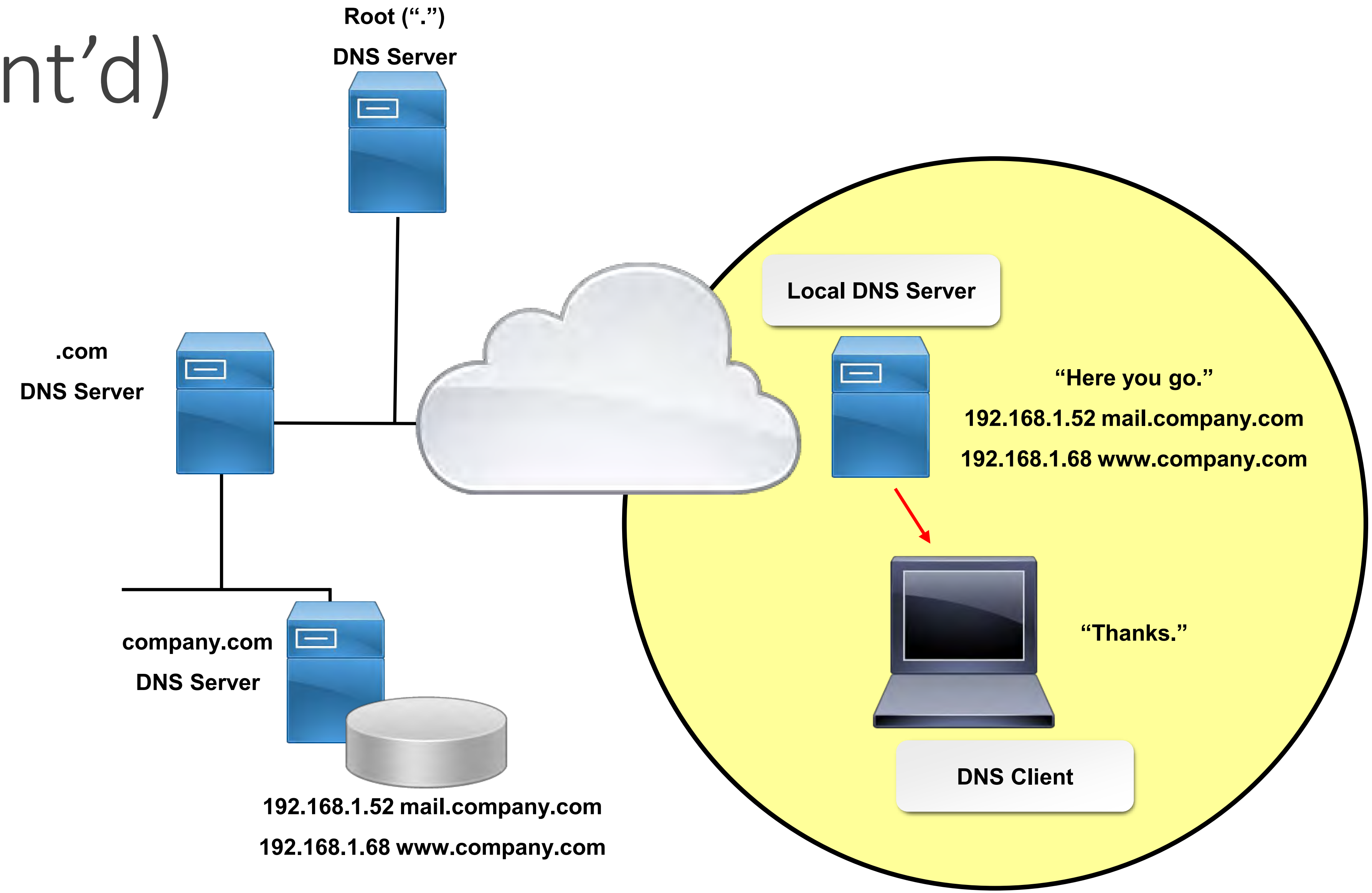
DNS Hierarchy Example


Root "."
Pointers to TLD NS servers
Top Level Domains
.com
.net
.org
.edu
.uk
Domains
ituonline
google
A 50.57.255.51 www.ituonline.com
MX 192.168.45.67 mail.ituonline.com
I'm delegating you to manage europe.comptia.org database
comptia
americas.comptia.org records are in the parent comptia.org database
Delegation
Sub-domains
europe
americas

DNS Process


Root (“.”)
DNS Server
“Ask the .com server – here’s its address.”
“www.company.com?”
“Ask the company.com server – here’s its address.”
.com
DNS Server
Local DNS Server
“www.company.com?”
“Please hold while I retrieve the information for you.”
“www.company.com?”
company.com
DNS Server
“Yes I have it. Here it is.”
“I need the IP address for www.company.com.”
DNS Client
192.168.1.52 mail.company.com
192.168.1.68 www.company.com

DNS (cont’d)


Root (“.”)
DNS Server
.com
DNS Server
company.com
DNS Server
192.168.1.52 mail.company.com
192.168.1.68 www.company.com
Local DNS Server
“Here you go.”
192.168.1.52 mail.company.com
192.168.1.68 www.company.com
“Thanks.”
DNS Client

Forward vs. Reverse Lookup

Forward lookup = you know the name but you need the IP

Reverse lookup = you know the IP but you need the name

- Commonly used as a security mechanism to verify host authenticity

Nslookup is a useful command line tool to query a DNS server

- It uses reverse lookups
- You won’t be able to use it to query a DNS server that does not have a reverse lookup zone configured

Address Record (A, AAAA)

The most basic type of DNS record

Map a friendly name to an IP addresses

The AAAA (aka quad-A) specifies an IPv6 address for a given host

- It works the same way as the A record

Canonical Name (CNAME) Record

Domain name aliases

Computers on the Internet often perform multiple roles such as web-server, ftp-server, chat-server etc.

- To mask this, CNAME records can be used to give a single computer multiple names (aliases)
- For example, a server may be both a web-server and an ftp-server, so two CNAME records configured

You also need the original A record to contain the actual IP address of the host

- The CNAME records point to the A record
- If the IP address changes, you only update the A record
- You do not need to update any CNAME records

Mail Exchanger (MX) Record

Used to specify the e-mail server(s) responsible for a domain name

Each MX-record points to the name of an e-mail server and holds a preference number for that server

If a domain name is handled by multiple e-mail servers, a separate MX-record is used for each e-mail server

You also need the A record to know the actual IP address of the server

Name Server (NS) Record

The DNS servers that are authoritative for a zone

A zone should contain one NS-record for each DNS server (both primary and secondary servers)

- This is important for zone transfer (replication) purposes

NS records have the same name as the zone in which they are located

A very important function of the NS-record is delegation

- A DNS server that is higher up in the name space tree points down to the next DNS server that has the records for an independent child domain
- For example, the .com DNS server delegates control to the Microsoft.com server

Service (SRV) Record

Specifies the location of a service

The record is made of 3 parts:

- Service
- Protocol (usually TCP/UDP)
- Domain name

A common implementation is in Active Directory

- SRV records point to the domain controllers responsible for various roles in Active Directory

Pointer (PTR) Record

Used for reverse lookups

Maps IP addresses to friendly names

- The reverse of what A-records and AAAA-records do

An IPv4 PTR record shows the IP address in reverse, with "in-addr.arpa" appended to the end

An IPv6 PTR record shows each hex digit of the IP address in reverse order

- dots between each digit
- "ip6.arpa" appended to the end

PTR records are often used for security

- A node using an IP address must be able to identify the domain it’s from

TXT (SPF, DKIM) Record

TXT (Text) records contain free form text of any type

- A fully qualified domain name may have many TXT records
- TXT records usually easily read information about a server, network, data center, or other information

The most common uses for TXT records are:

- Sender Policy Framework (SPF)
- DomainKeys (DK)
- DomainKeys Identified E-mail (DKIM)

An SPF record is a type of DNS record that identifies which mail servers are permitted to send email on behalf of an organization

DKs are a deprecated e-mail authentication system

- Verify the domain name of an e-mail sender and the message integrity

DKIM is an email authentication method designed to detect email spoofing

Internal vs. External DNS

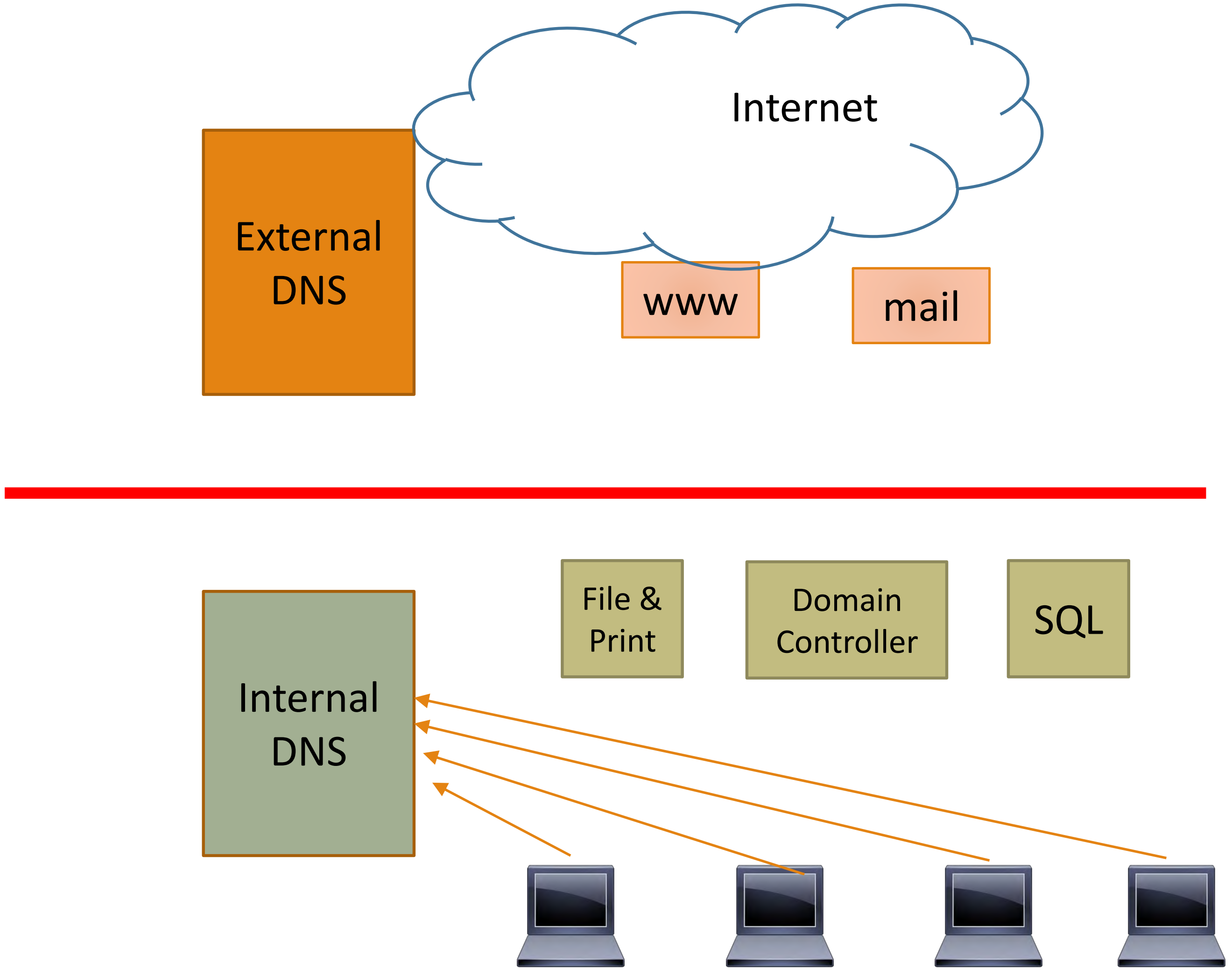
An External DNS server contains only records that the general public needs to know:

- Web server
- Mail exchanger
- Public DNS servers

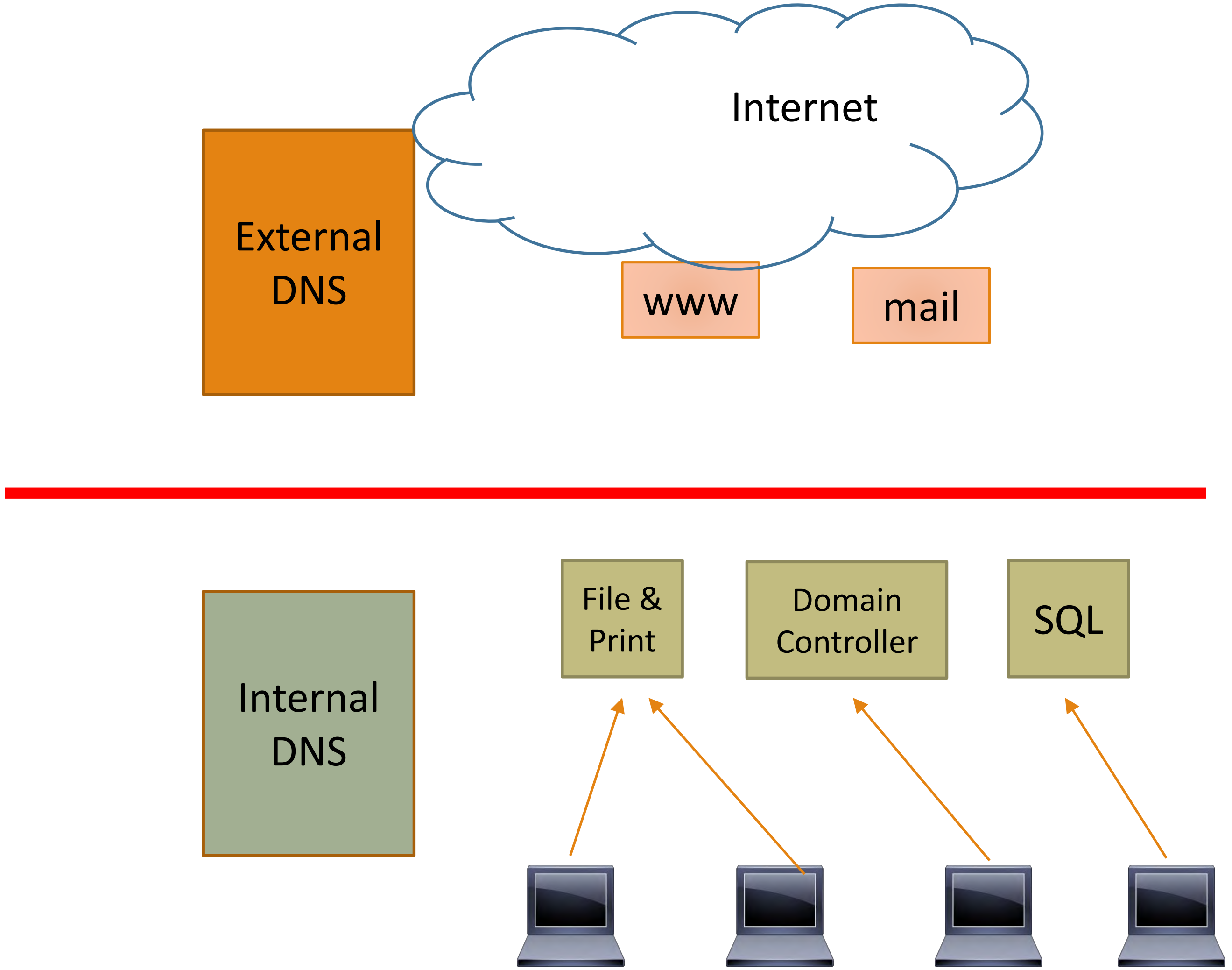
An Internal DNS server contains all of the private DNS records that the company uses (for all of the internal servers and resources)

- It might also include public records for internal clients that need to go out to the Internet to access those services

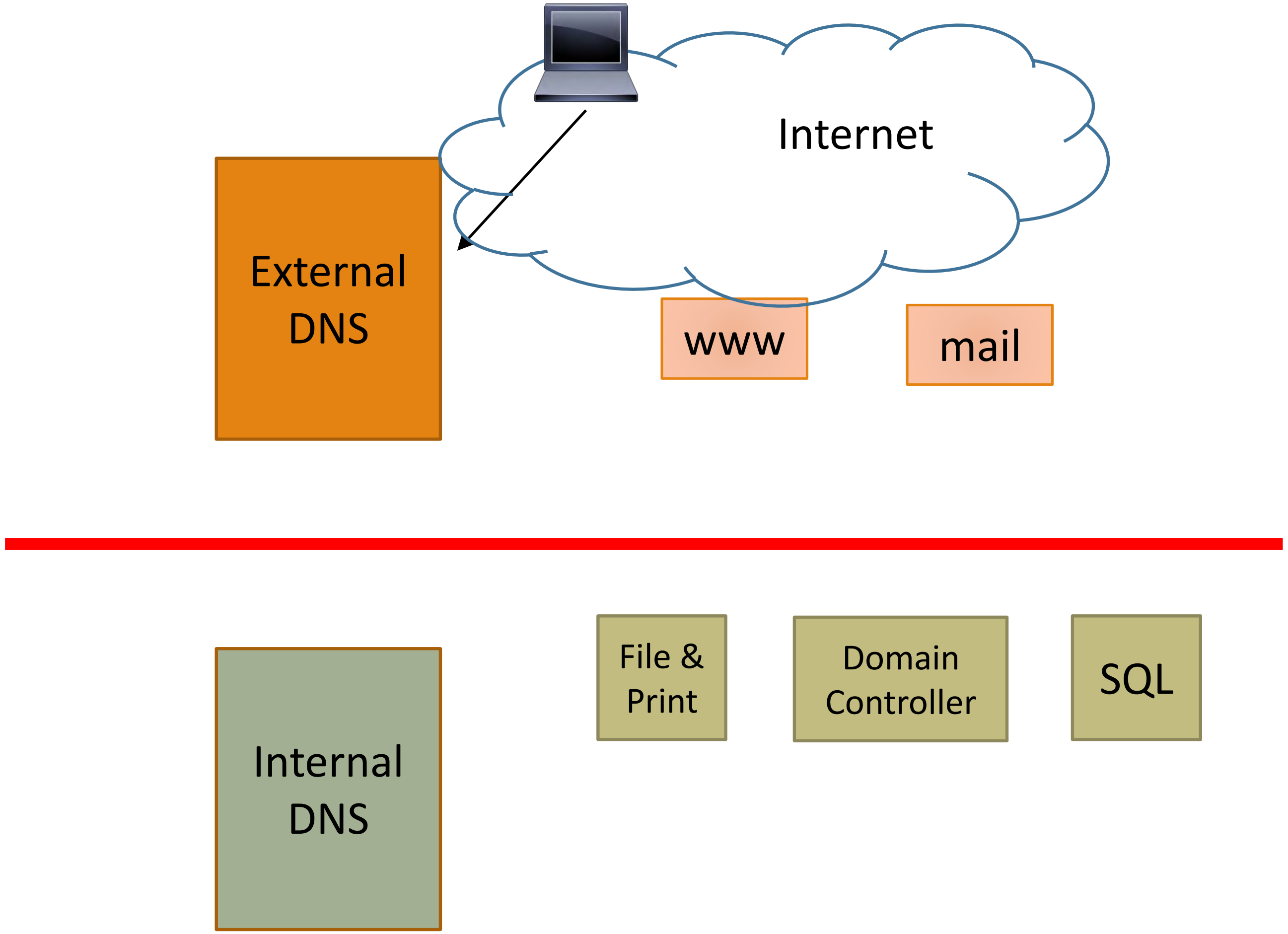
Internal vs. External DNS Example



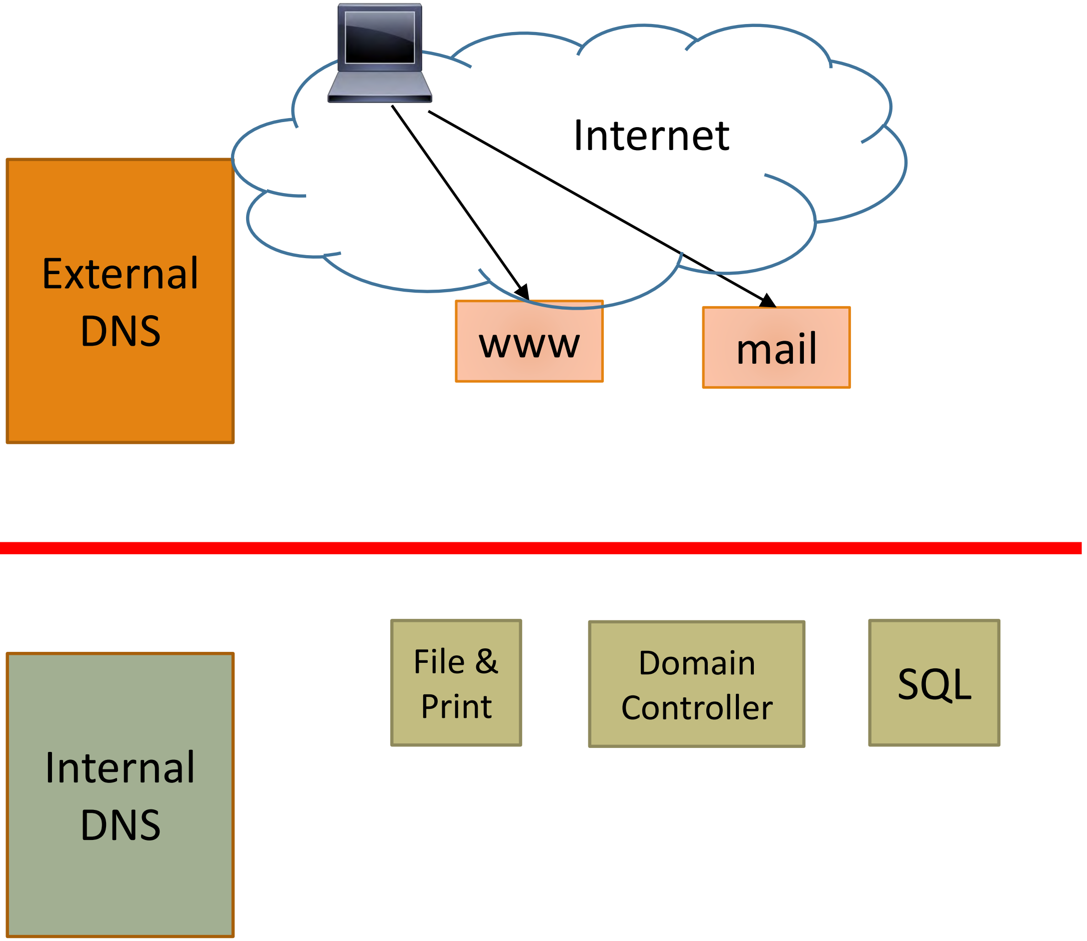
Internal vs. External DNS Example



Internal vs. External DNS Example



Internal vs. External DNS Example



Third-party/Cloud-hosted DNS

You can outsource the management of your DNS servers to a third party

Most commonly done for public records

Also done as part of a cloud deployment

Advantages:

- Faster resolution of external facing servers
- Internal to external resolution
- Better security and protection against newest threats
- Redundancy to avoid single-points of failure

Disadvantages:

- You might not have direct control over the records
- You might have to request the provider update the records for you, resulting in delay times

NTP

Network Time Protocol (NTP)

Used to synchronize clocks on a network

- Synch is updated every 10 minutes

UDP 123

NTP hierarchy is organized into stratums (levels)

- 0 – 15
- Stratum 0 = Device with an atomic clock
- Stratum 1 = Server that connects to a Stratum 0 device
- Stratum 2 = Server that synchs with a Stratum 1 server
- ...

NTP is often used to

- Synchronize your organization's time server to an external source
- All other devices in your network then synchronize to your time server

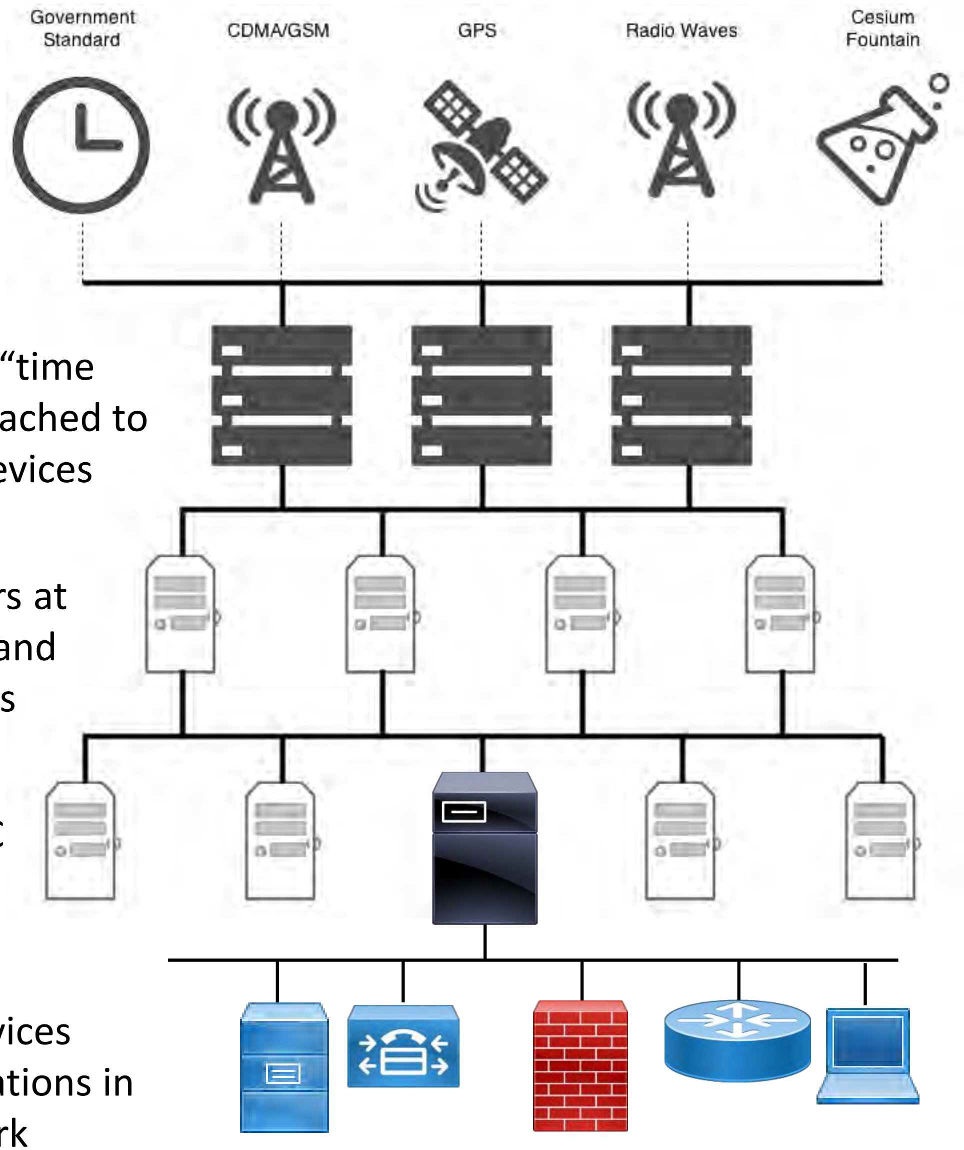
You need all devices in your network to refer to a single time source:

- Accurately cross-reference an event on different devices on the network
- Ensure that authentication happens in an acceptable time frame
  - Microsoft Active Directory requires all domain members to synchronized to within 5 minutes of the time server (PDC Emulator)

NTP Enterprise Time Coordination Example

NIST Cesium Fountain Atomic Clock

The U.S. Naval Observatory Alternate Master Clock at Schriever AFB (Colorado)



Stratum 0
Has Atomic Clock

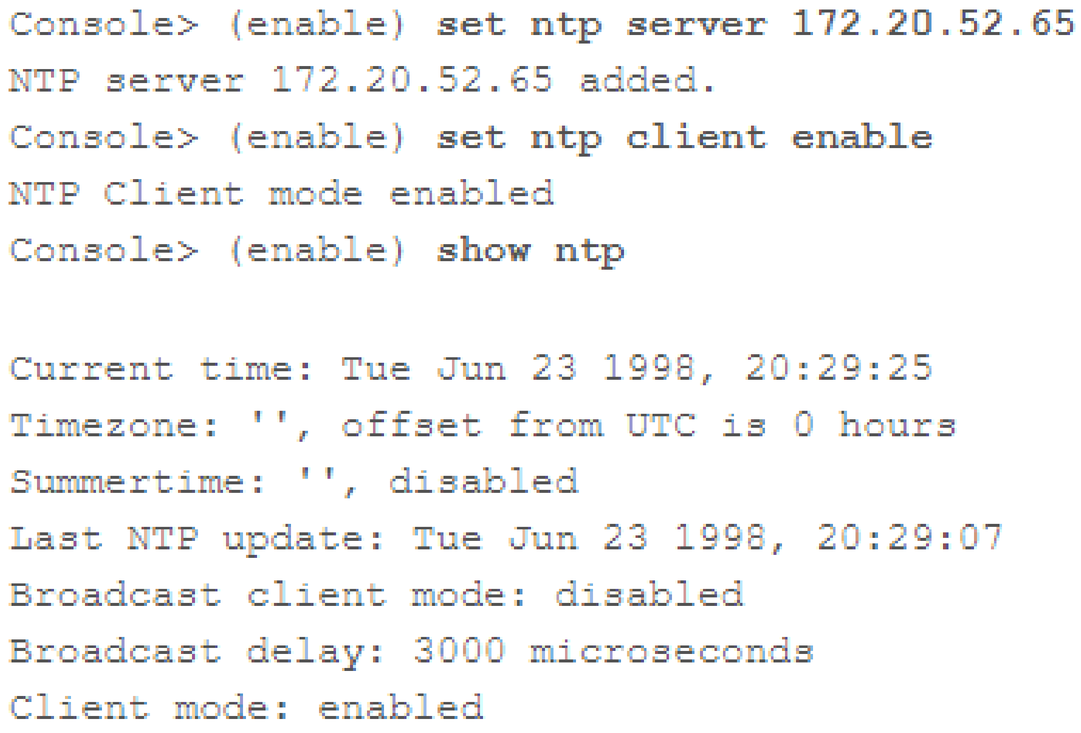
Stratum 1
Computers (“time servers”) attached to Stratum 0 devices

Stratum 2
Public servers at universities and organizations

Stratum 3
Your AD PDC Emulator

Stratum 4
Servers, devices and workstations in your network

Configuring NTP on a Cisco Device Example



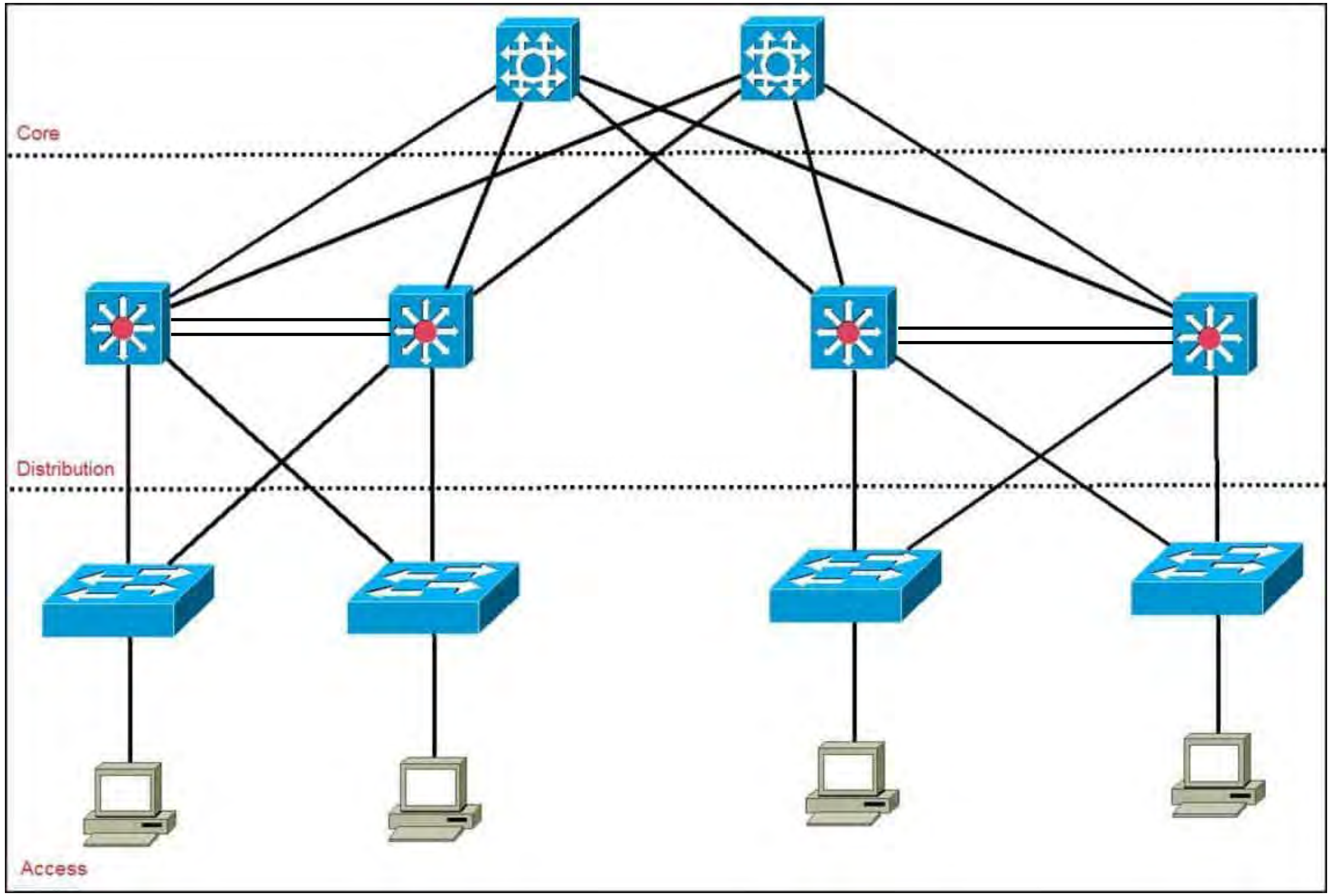
```
Console> (enable) set ntp server 172.20.52.65
NTP server 172.20.52.65 added.
Console> (enable) set ntp client enable
NTP Client mode enabled
Console> (enable) show ntp

Current time: Tue Jun 23 1998, 20:29:25
Timezone: '', offset from UTC is 0 hours
Summertime: '', disabled
Last NTP update: Tue Jun 23 1998, 20:29:07
Broadcast client mode: disabled
Broadcast delay: 3000 microseconds
Client mode: enabled
```

Your corporate time server

Corporate and Datacenter Network Architecture

Classic Cisco Three-Tier Model

Tier	Description
Core	• Datacenter backbone • High-speed switching • Connect to campus core or edge router
Distribution	• VLAN Routing • Policy • Redundancy for Access layer • Traffic aggregation
Access	• Connectivity for end devices (clients and servers) • VLAN membership



Software-Defined Networking (SDN)

A software-based approach to network management

Separates the routing logic (control plane) from the actual traffic movement (forwarding plane)

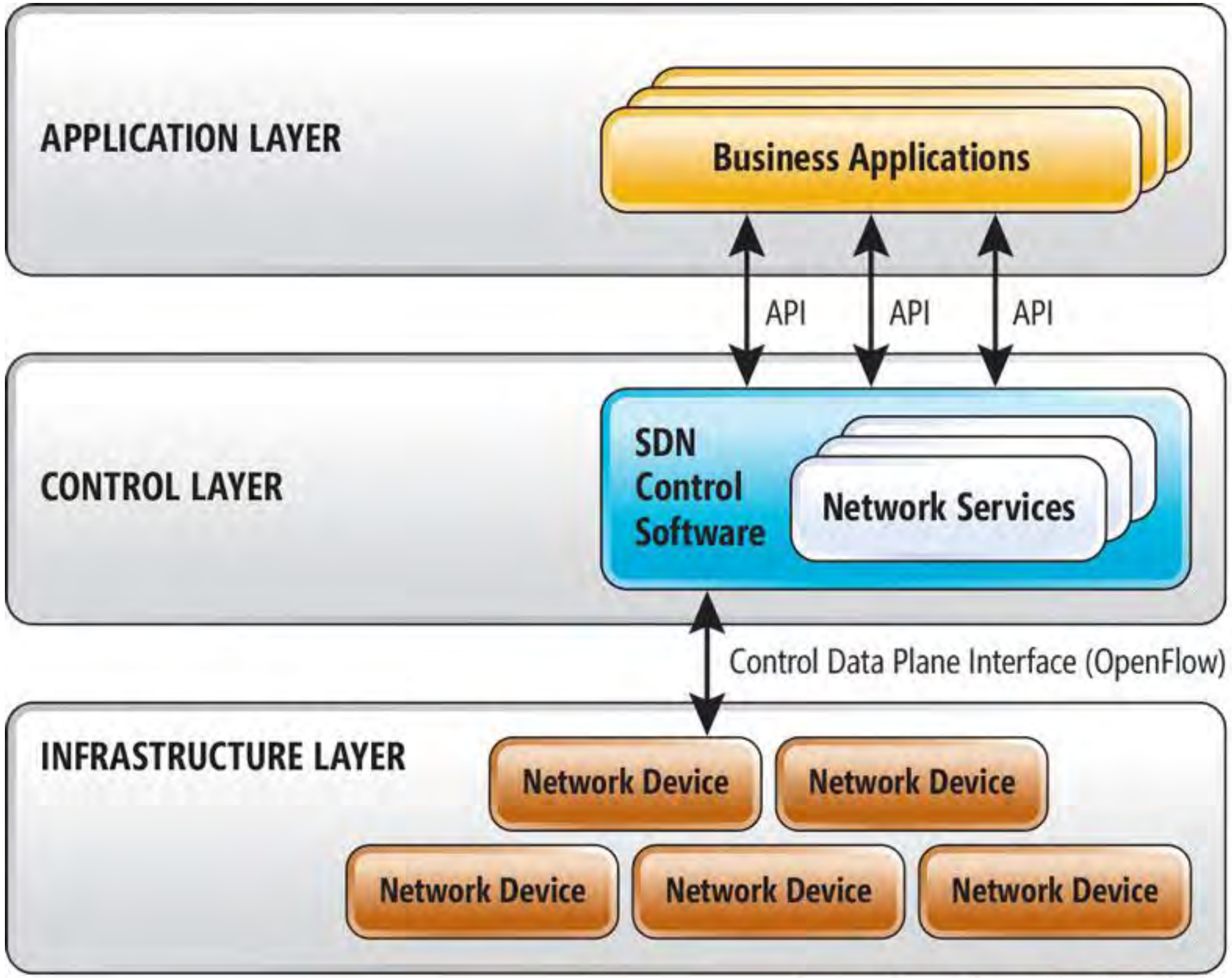
Physical network devices in the forwarding plane are “white box”

- Do not have their own configurations

Uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure

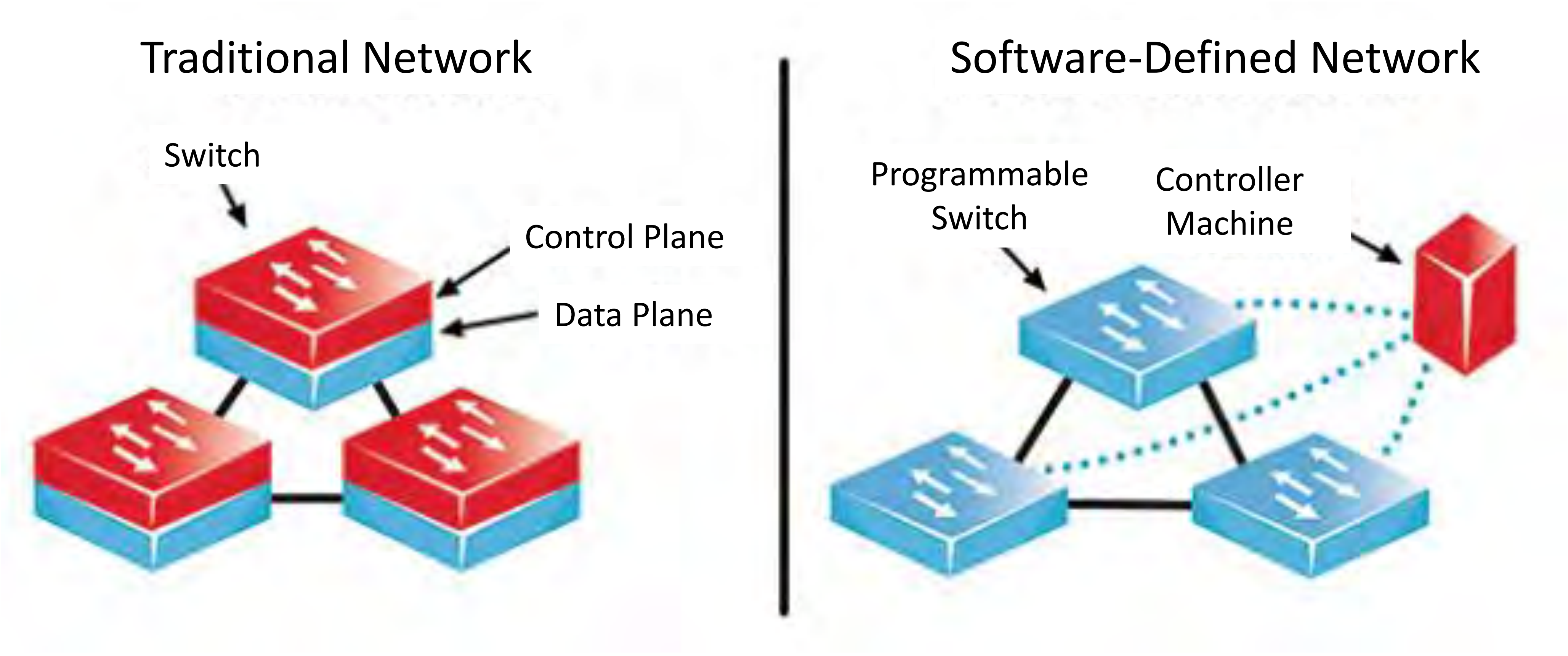
Used heavily in datacenters where infrastructure is virtualized

SDN Conceptual Model



Source: Open Networking Foundation

SDN Example


Traditional Network
Switch
Control Plane
Data Plane
Software-Defined Network
Programmable Switch
Controller Machine

Spine and Leaf

Two switching layers – spine and leaf

Leaf Layer:

- Aggregate traffic from servers
- Connects directly to spine (core)

Spine Layer:

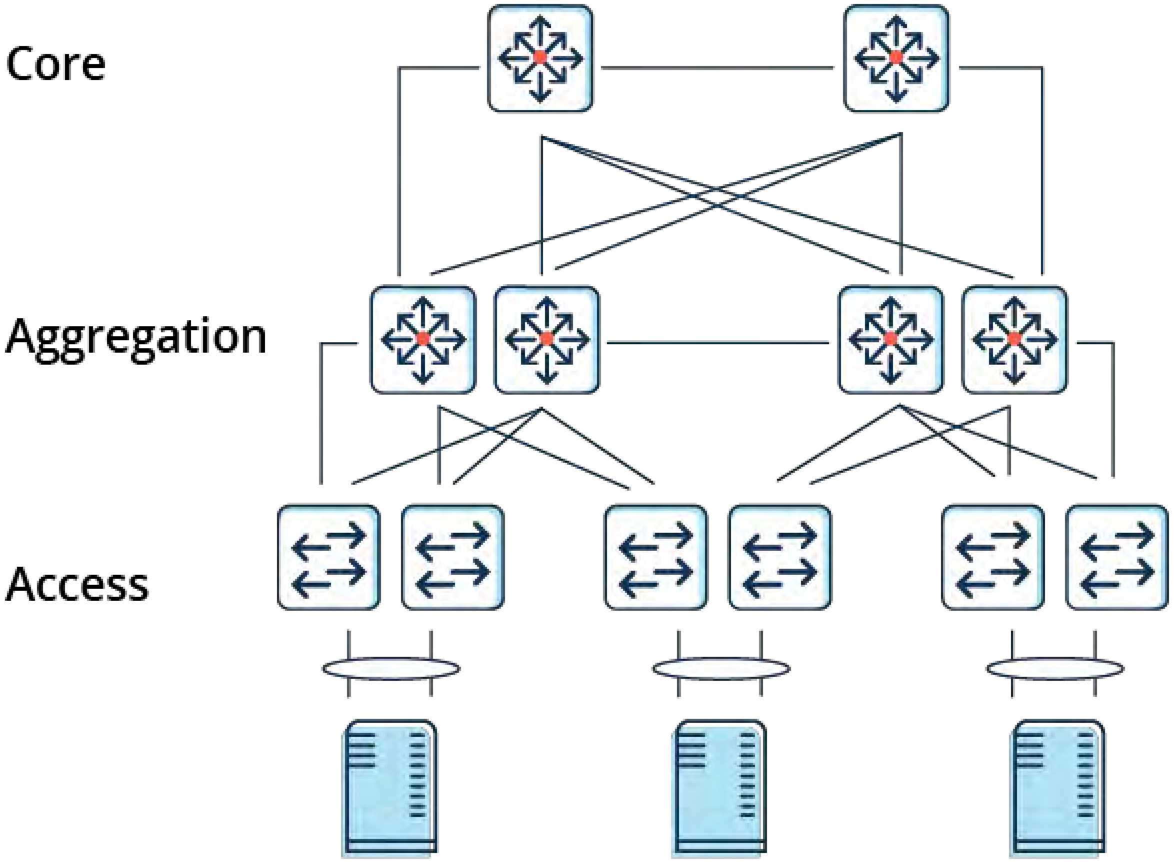
- Spine switches interconnect all leaf switches
- Full mesh topology
- Traffic flow is more East-West than traditional North-South

Better performance and scalability

- No more spanning tree
- Load balancing across all available paths
- Physical links are higher speed 25- 40- and 100gb

Traditional 3-Tier vs Spine-Leaf

Traditional 3-Tier Architecture

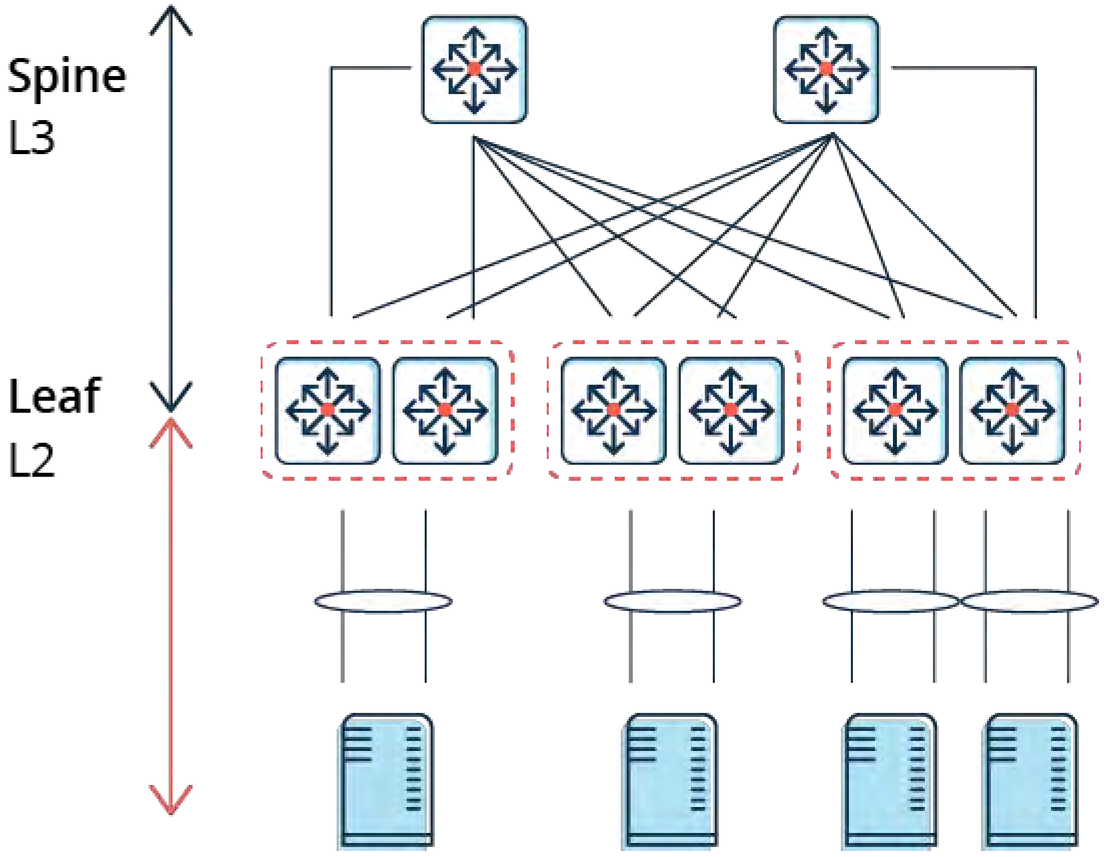


Core

Aggregation

Access

2-Tier Spine-Leaf Architecture



Spine
L3

Leaf
L2

Top of Rack (ToR) Datacenter Design

"Per Rack" architecture

L3 fiber optic switches are placed at the top of a rack (ToR)

- ToR switch aggregates traffic at the rack level

Other devices connect to the ToR switch

- L2 switches, servers, network appliances, storage are in the same rack, below the ToR switch

All ToR switches then connect to a nearby aggregation switch

ToR Considerations

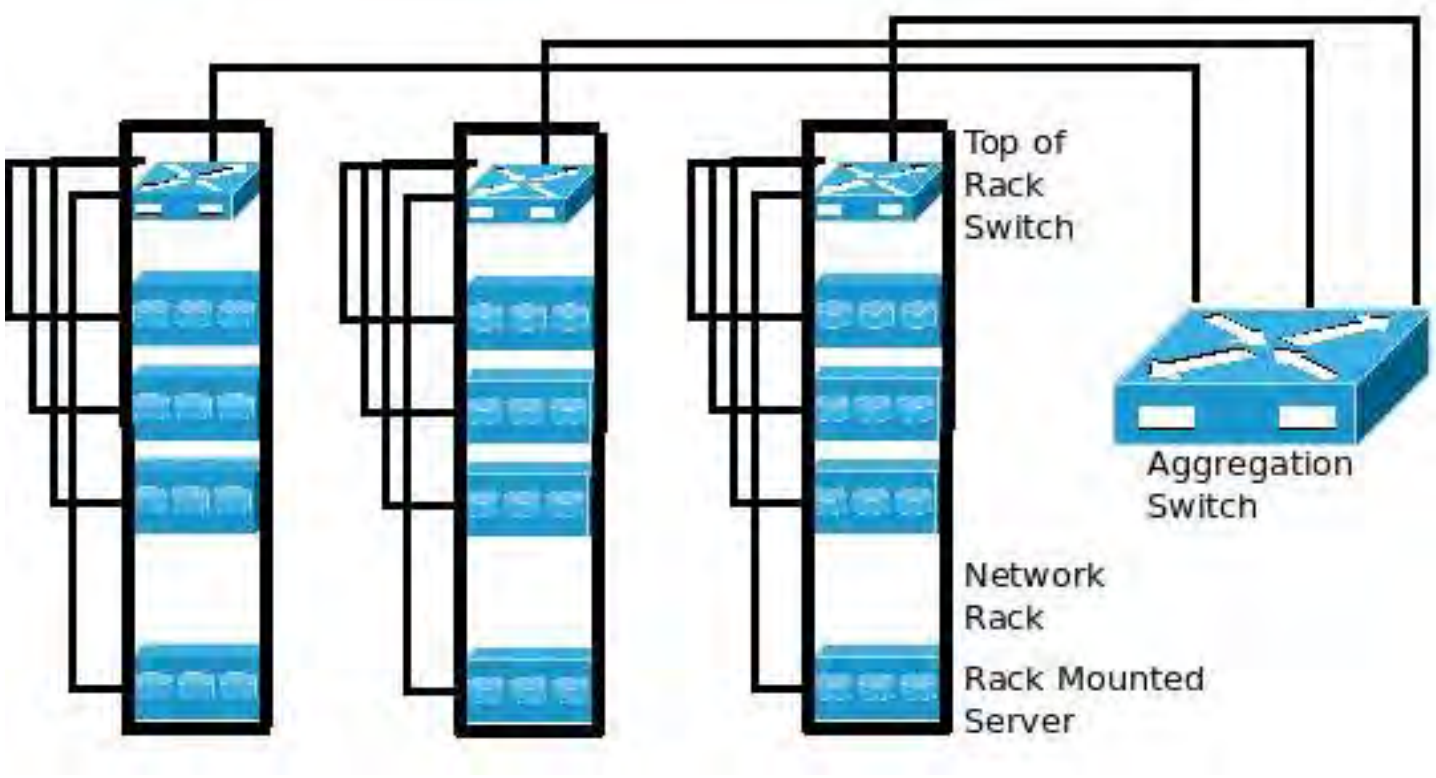
ToR Reduces cabling complexity

- Most connectivity and aggregation occurs within the rack
- Better cable management
- Fewer high speed links need to leave the rack

High-end switches in racks might be under-utilized

Popular design for SDN

Top of Rack Example

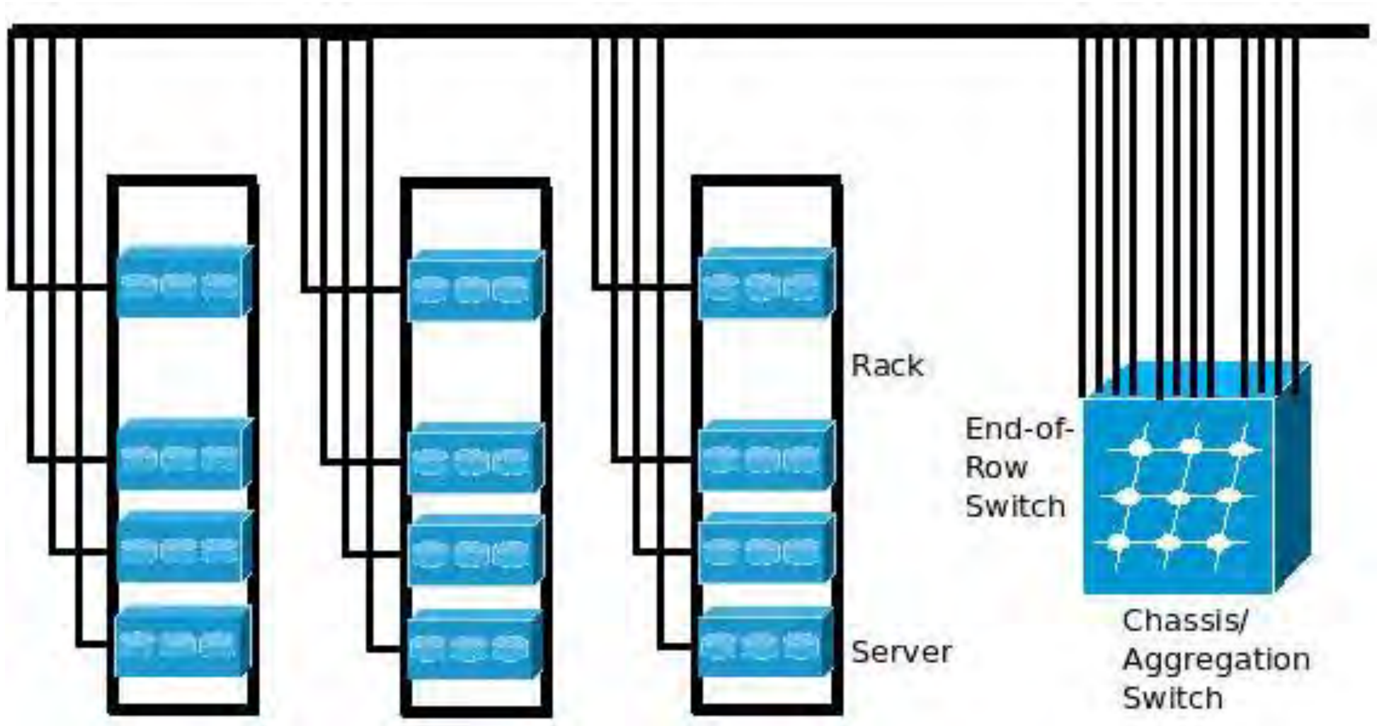


End of Row (EoR) Design

"Per Row" architecture

- Racks that contain servers are arranged in rows
- At the end of each row is a rack that contains aggregation switches
- Each server needs cabling across the entire row to get to the aggregation rack
- Traffic aggregation is done at the row level

End of Row Example



Datacenter vs. Colocation

Datacenter:

Facility built by the organization specifically to house its datacenter

Requires considerable floor space, power, and Internet/WAN link bandwidth

Expensive

- Organization will always be looking for ways to decrease the square footage and power usage

Colocation:

Facility built by a provider

Floor space/services rented out to customers

Customers can bring their own equipment or user provider's equipment

Customers can visit the facility

Provider might offer different levels of administration:

- Security only
- Very basic tech support (restarting servers)
- Full management

Branch Office

An auxiliary physical site belonging to the organization

Typically has fewer than 100 employees

Depending on size, may or may not have an IT presence

- Might be remotely managed by IT from the central site

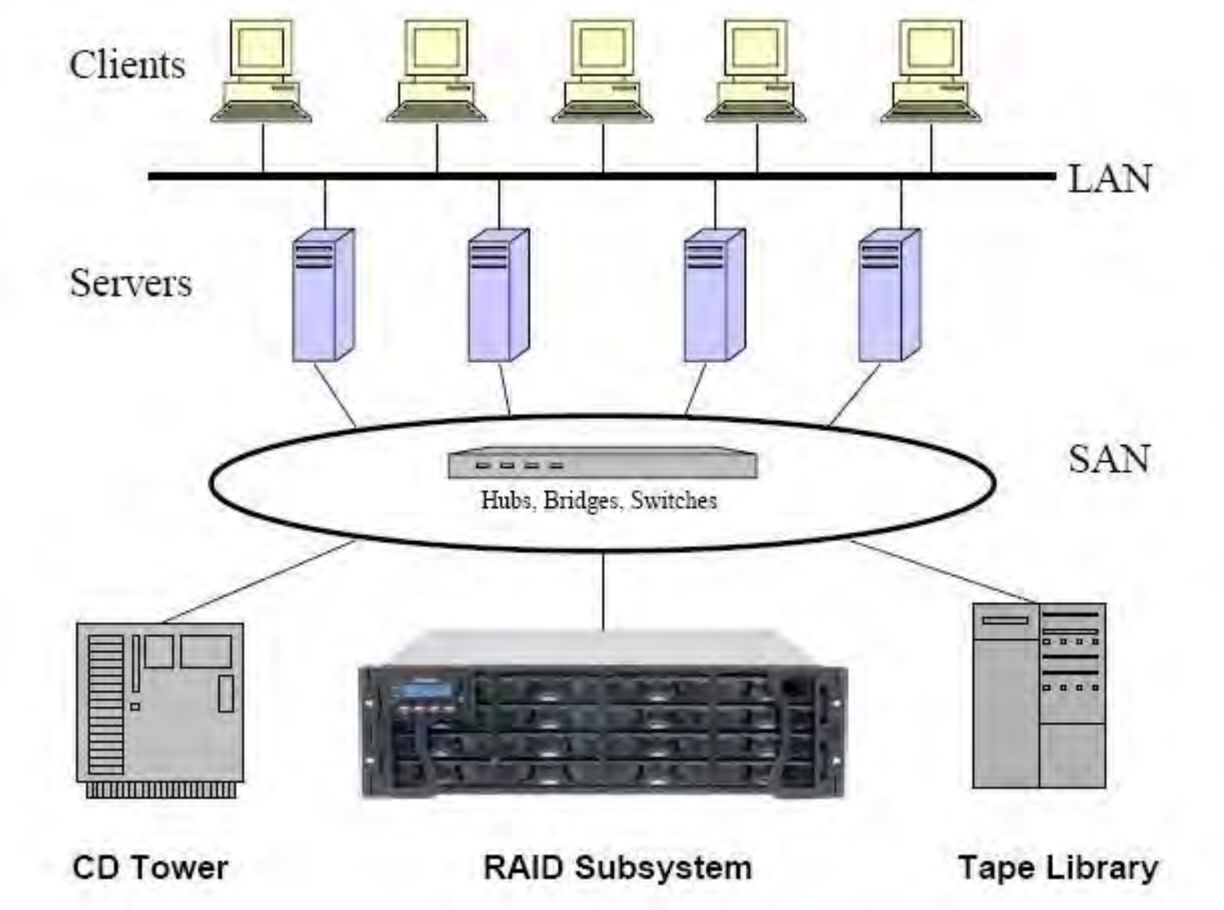
Might host some resources specific to that particular office

- Local servers are sometimes used to improve authentication or file access performance
- Most resources will be accessed remotely (central datacenter, colo, or cloud)

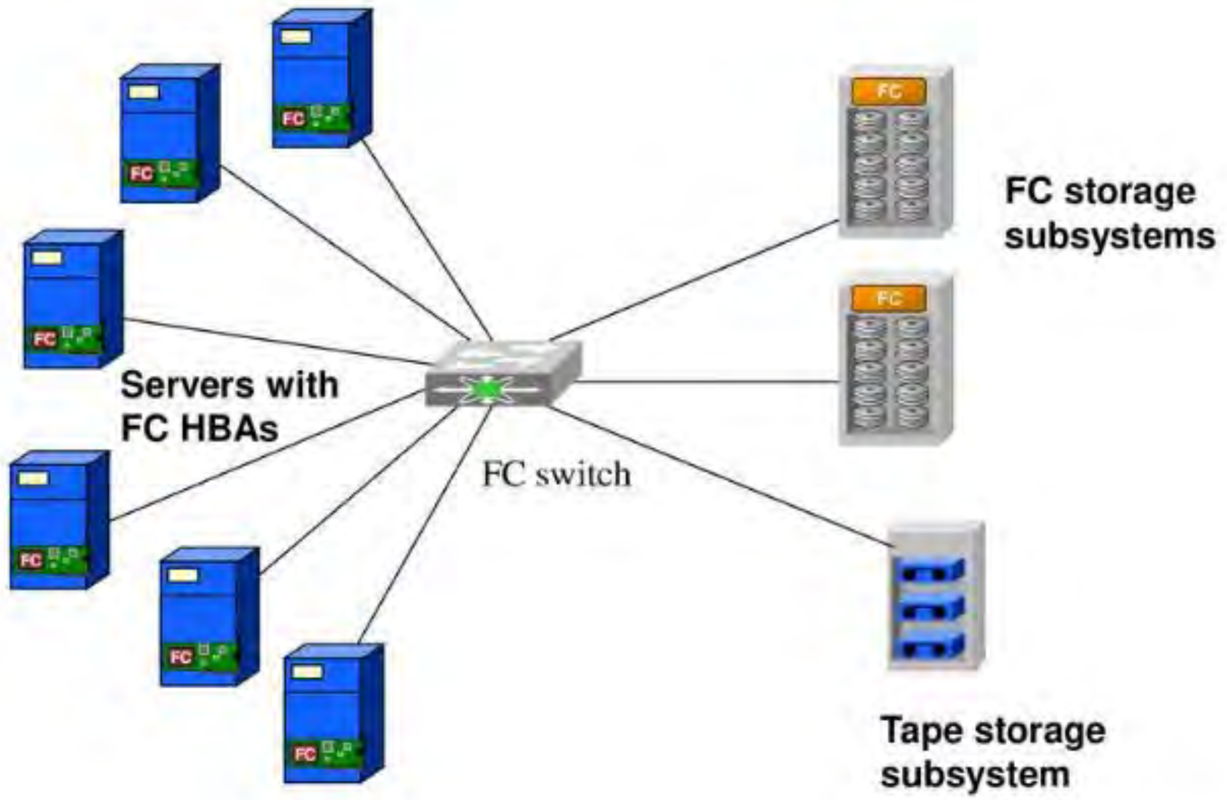
Storage Area Networks

Connection Type	Description
Fibre Channel	- The protocol used by storage-related devices such as host bus adapters (HBAs), switches and storage controllers communicate - Cabling is fiber optic - Uses separate infrastructure dedicated to storage only
Fibre Channel over Ethernet (FCoE)	- Fiber channel commands are carried as an Ethernet payload - Uses existing LAN infrastructure - Cheaper
Internet Small Computer Systems Interface (iSCSI)	- Disk SCSI commands are carried as a payload of IP - Uses existing LAN infrastructure - Cheapest

Generic SAN Example



Fibre Channel SAN Example



Cloud Concepts and Connectivity Options

What is the Cloud?

Generic term for a datacenter run by a provider

Usually publicly available
- Can also be private, inside a large organization’s internal network (intranet)

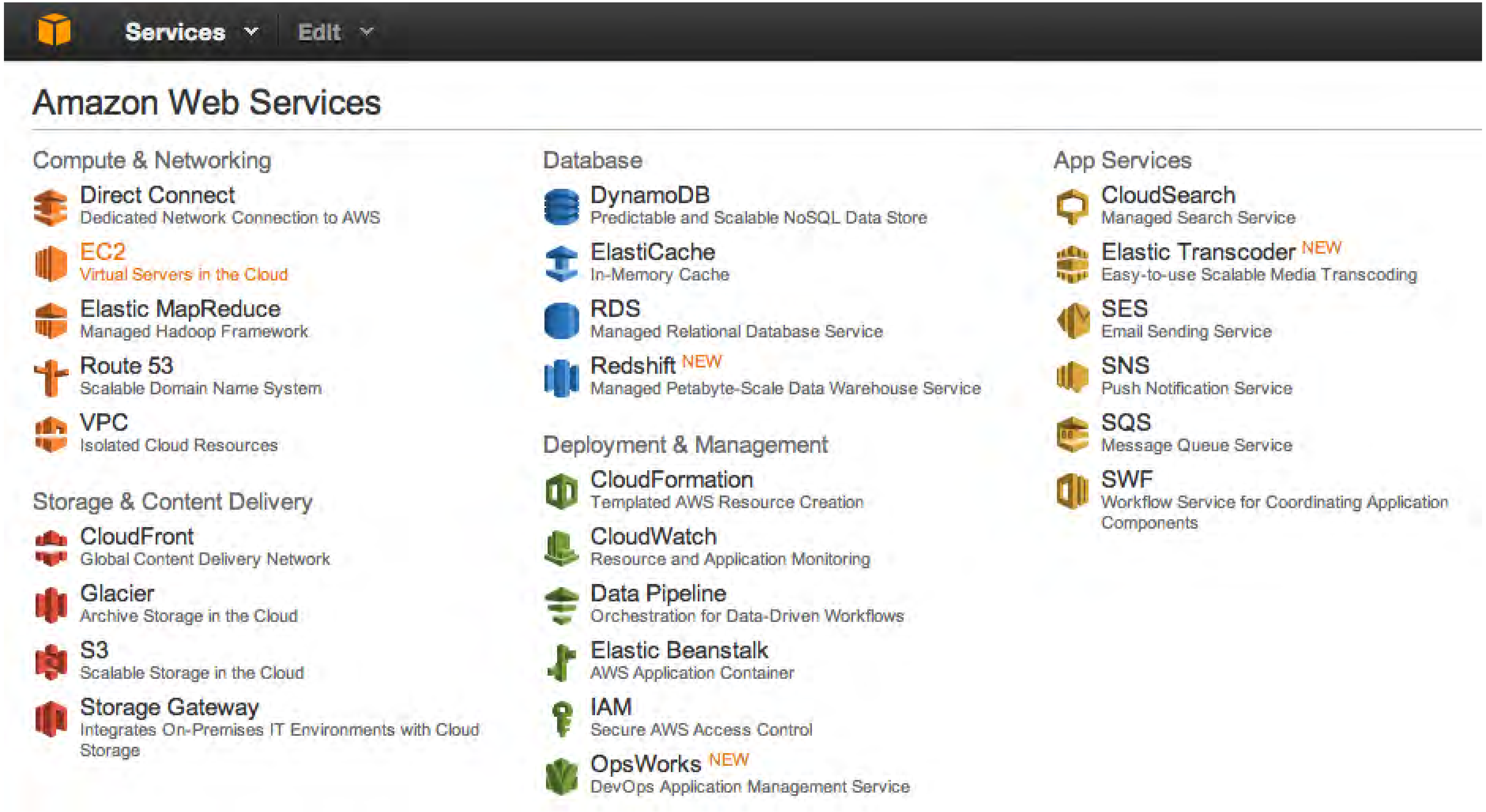
Customers typically connect to it via a browser on the Internet

Usually has a customer self-service portal

Provides many application, compute, and storage services

Services are subscription-based
- Customers only pay for what they use

AWS Portal Example



Amazon Web Services

Compute & Networking

Direct Connect
Dedicated Network Connection to AWS

EC2
Virtual Servers in the Cloud

Elastic MapReduce
Managed Hadoop Framework

Route 53
Scalable Domain Name System

VPC
Isolated Cloud Resources

Storage & Content Delivery

CloudFront
Global Content Delivery Network

Glacier
Archive Storage in the Cloud

S3
Scalable Storage in the Cloud

Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage

Database

DynamoDB
Predictable and Scalable NoSQL Data Store

ElastiCache
In-Memory Cache

RDS
Managed Relational Database Service

Redshift NEW
Managed Petabyte-Scale Data Warehouse Service

Deployment & Management

CloudFormation
Templated AWS Resource Creation

CloudWatch
Resource and Application Monitoring

Data Pipeline
Orchestration for Data-Driven Workflows

Elastic Beanstalk
AWS Application Container

IAM
Secure AWS Access Control

OpsWorks NEW
DevOps Application Management Service

App Services

CloudSearch
Managed Search Service

Elastic Transcoder NEW
Easy-to-use Scalable Media Transcoding

SES
Email Sending Service

SNS
Push Notification Service

SQS
Message Queue Service

SWF
Workflow Service for Coordinating Application Components

Cloud Deployment Models

Model	Description
Public	• Available for any customer from the general public • Example: AWS, MS Azure, Google
Private	• Created and used internally by any organization • Example: A large bank that provides services to its departments via an internal "cloud"
Hybrid	• Private datacenter that extends into the public cloud • Example: A world-wide organization that wants to make Office 365 and Internal Sharepoint sites easily available to users in many geographical locations
Community	• A cloud by a public provider, but reserved for organizations that have similar needs • Example: A large government agency with special security needs that pays for a specialized version of Microsoft Azure • Each of the bureaus/divisions in that agency subscribe to an isolated, secure part of that cloud

Cloud Service Models

Model	Description
Software-as-a-Service (SaaS)	• Software is licensed on a subscription basis and is centrally hosted • Also known as "on-demand software" or Web-based/Web-hosted software • Nearly all configuration and security is managed by the provider
Infrastructure-as-a-Service (IaaS)	• A form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand • Provided on a pay-as-you-go basis • Allows rapid elasticity as needed • Customer is responsible for nearly all configuration and security

Cloud Service Models (cont'd)

Model	Description
Platform-as-a-Service (PaaS)	• A cloud computing model that provides customers a complete cloud platform of hardware, software, and infrastructure • Used specifically to develop, run and manage applications without the cost or complexity that comes from building your own infrastructure
Desktop-as-a-Service (DaaS)	• A cloud computing offering in which a third party hosts the back end of a virtual desktop infrastructure (VDI) deployment • The provider manages the back-end responsibilities of data storage, backup, security and upgrades • Customers usually manage their own virtual desktop images, applications and security

Infrastructure as Code (IaC)

The process of managing and provisioning computer data centers through machine-readable definition files

- Rather than physical hardware configuration or interactive configuration tools
- Most effective when underlying infrastructure is IaaS or PaaS

Separates configurations, policies, profiles, scripts, and templates from the hardware or software on which they are deployed

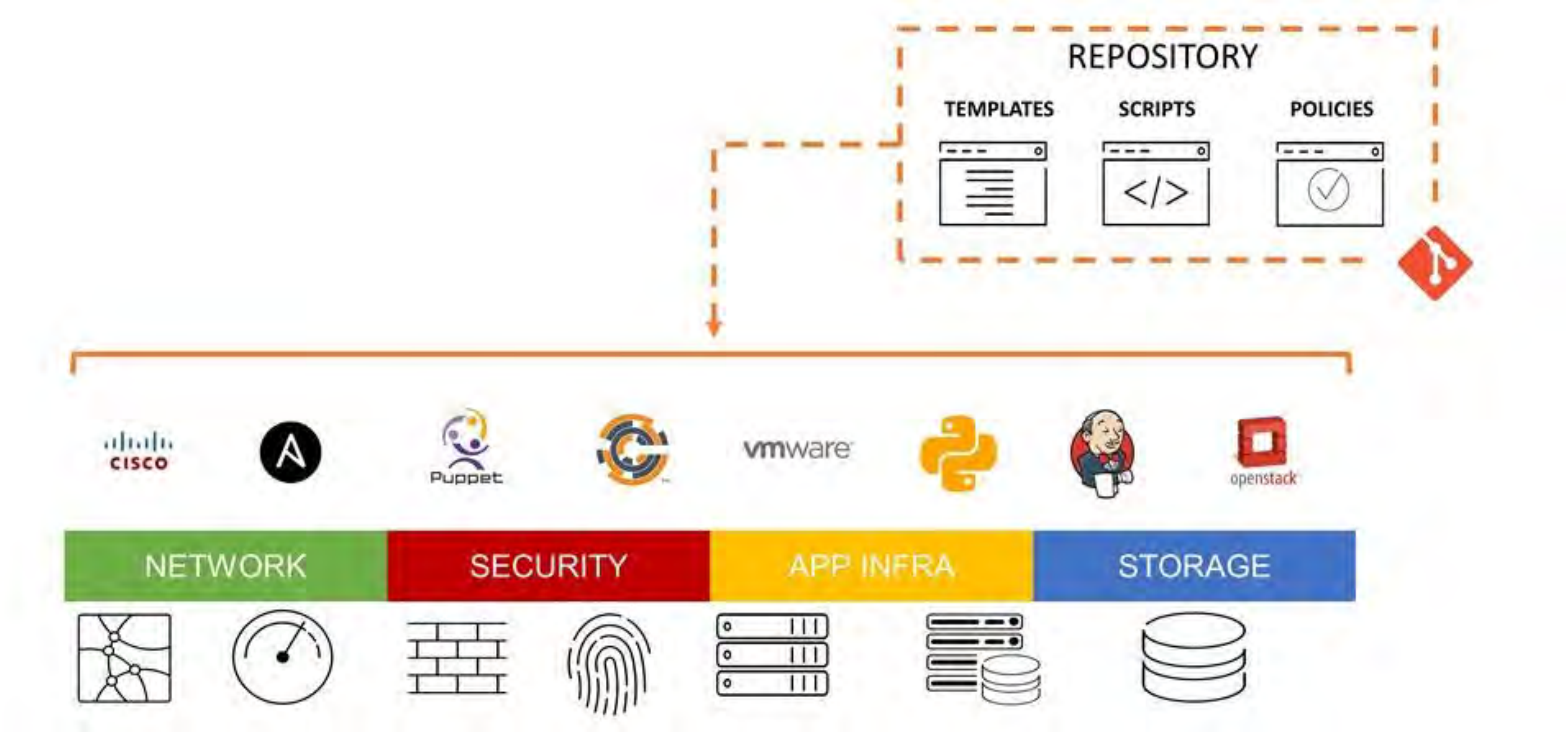
- These items can then be stored, shared, revised, and applied in the same manner as code

The core best practices of DevOps (version control, virtualized tests, continuous monitoring) are applied to the underlying code that governs the creation and management of your infrastructure

Your infrastructure is treated the same way that any other code would be

Makes DevOps possible

Infrastructure as Code Example



Client-to-Cloud Connectivity Options

Connection Type	Description
Virtual Private Network (VPN)	• Internet-based VPN link to the provider's cloud • Cheaper, more flexible • No guarantee of quality of service or link performance
Private-direct connection to cloud provider	• Dedicated WAN link to the provider's cloud • More expensive • WAN link provider guarantees uptime and bandwidth

Additional Cloud Concepts/Considerations

Concept	Description
Multitenancy	• A cloud computing architecture that allows customers to share computing resources in a public or private cloud • Each tenant's data is isolated and remains invisible to other tenants • The risk is that one tenant could break out of its sandbox and invade other tenants • Or a tenant could consume all of the underlying resources to the detriment of the other tenants
Scalability	• The ability to grow by statically adding resources including additional datacenter sites and content delivery networks (growth is steady) • The risk is that the provider cannot provide access close to some of your users • You also can be caught off-guard by a sudden increase in demand that your system is not designed to handle

Additional Cloud Concepts/Considerations (cont’d)

Concept	Description
Elasticity	• The ability of a cloud to grow or shrink capacity for CPU, memory, and storage resources to rapidly adapt to the changing demands of an organization • Matches the resources allocated with actual amount of resources needed at any given point in time • Increases and decreases can be temporary (growth is “spikey”) • Additional consumption is pay-as-you-go • The risk is that you did not design/allocate sufficient elasticity for actual need • Or the cost suddenly goes up unexpectedly