Welcome to INE's Presentation of:

Understanding Common Network Applications

Course Structure

- Time: 9:00am to 3pm (PST) 1/4/17
- Breaks
- This class is being recorded.
- Q&A

Understanding Common Network Applications

Course Objectives

- To provide a high-level overview of common application characteristics and mechanics.
- To summarize the basic operations of Email, Web Browsing and Telnet.
- Designed for ICND1/CCENT Learners

Course Agenda

- What do Applications have to do with a CCNA?
- Overview of TCP and UDP
- DNS
- Categories and Types of Applications
- Email
- Web Browsing
- Telnet

Course Prerequisites

- Prerequisite Knowledge
- Q&A
  - kbogart@ine.com
  - Twitter.com/keithbogart1
  - https://www.linkedin.com/in/keith-bogart-2a75042

What do Applications have to do with a CCNA?

Applications? I'm studying for R&S!

- **Why do you want to be a CCNA?**
- **Job responsibilities may include;**
  - Monitoring existing links for bandwidth consumption
  - Implementing and monitoring basic security policies with ACLs
  - Troubleshooting problems in the network that could impact network-based applications.

Applications? I'm studying for R&S! (Part-2)

- What are our Applications?
  - Client-Server or P2P?
  - TCP or UDP?
  - Port Numbers?
  - Name Resolution?
  - Where are the servers?
- What security-related concerns do I need to know about?
  - Where are applications allowed?
  - 24x7?
  - Bandwidth allowances?
  - Credential storage and administration?
  - Rogue Application Policy?

Summary

- So in summary, a Network Admin doesn't necessarily need to know the intricate details of how an application works, but without the information in the preceding slides, configuring a network to meet pre-defined requirements would be impossible.

TCP and UDP: An Overview

TCP and UDP

- What makes TCP different from UDP?
- UDP
  - Connectionless
  - Expects to receive small, discrete messages from upper-layer protocols
  - No reliability or retransmission
- TCP
  - Connection-Oriented
  - Can work with any format of data (including a constant stream of bytes) from upper-layer protocols
  - Reliability with Acknowledgements and Retransmissions

TCP – Connection Oriented

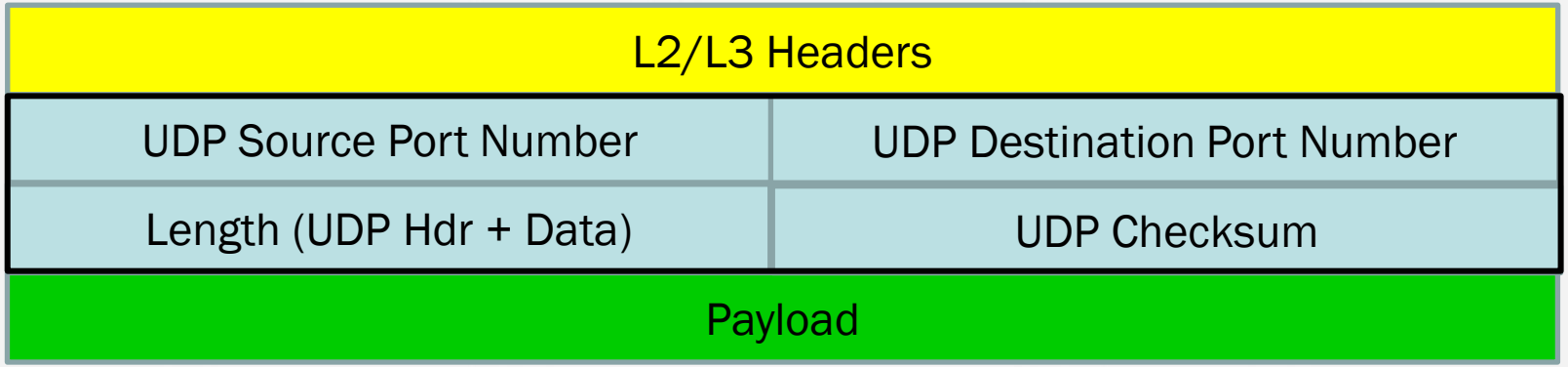
What is meant by “connection oriented”?

- TCP verifies existence of peer prior to data exchange.
- TCP peers negotiate parameters used to control data exchange.
- TCP data is exchanged reliably using sequence numbers, acknowledgements, flow-control, and retransmissions.
- TCP can gracefully inform peer of the need to close a connection.

OSI Transport Layer - UDP

UDP

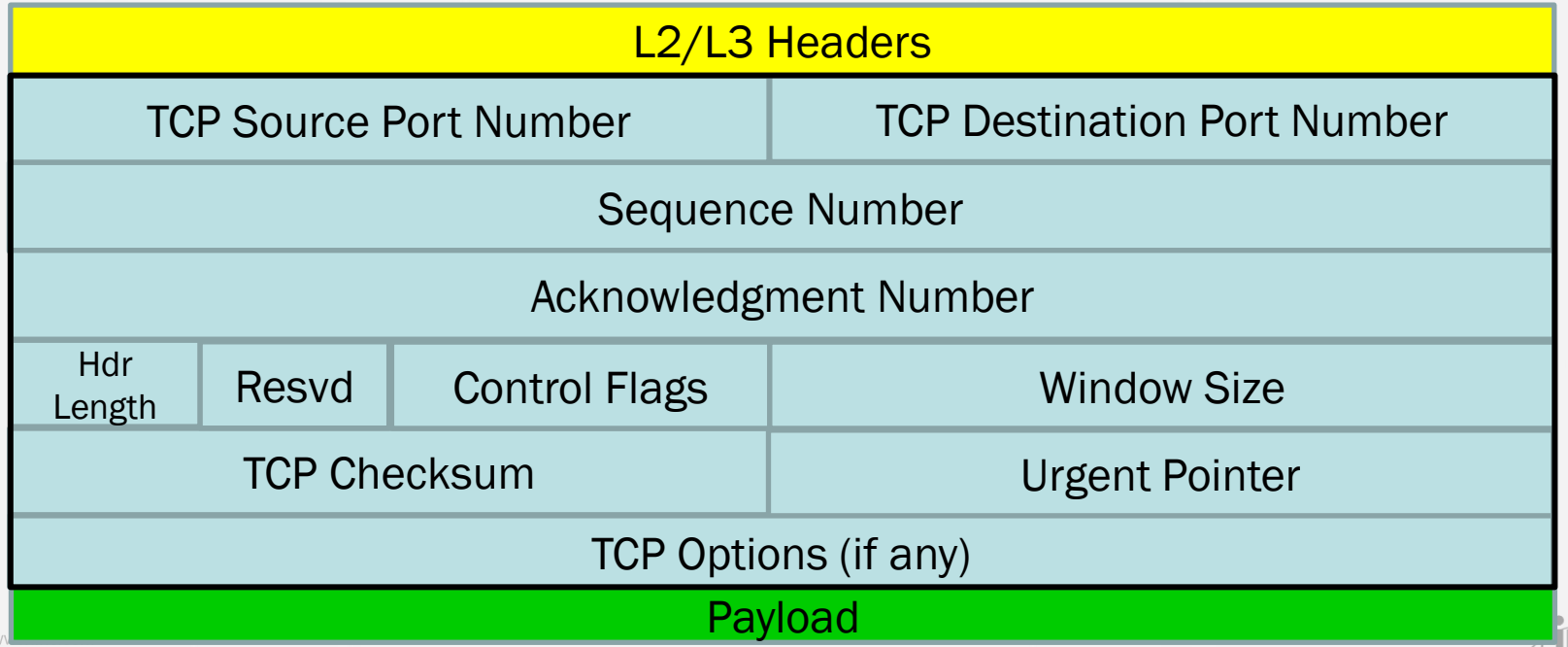
- Connectionless



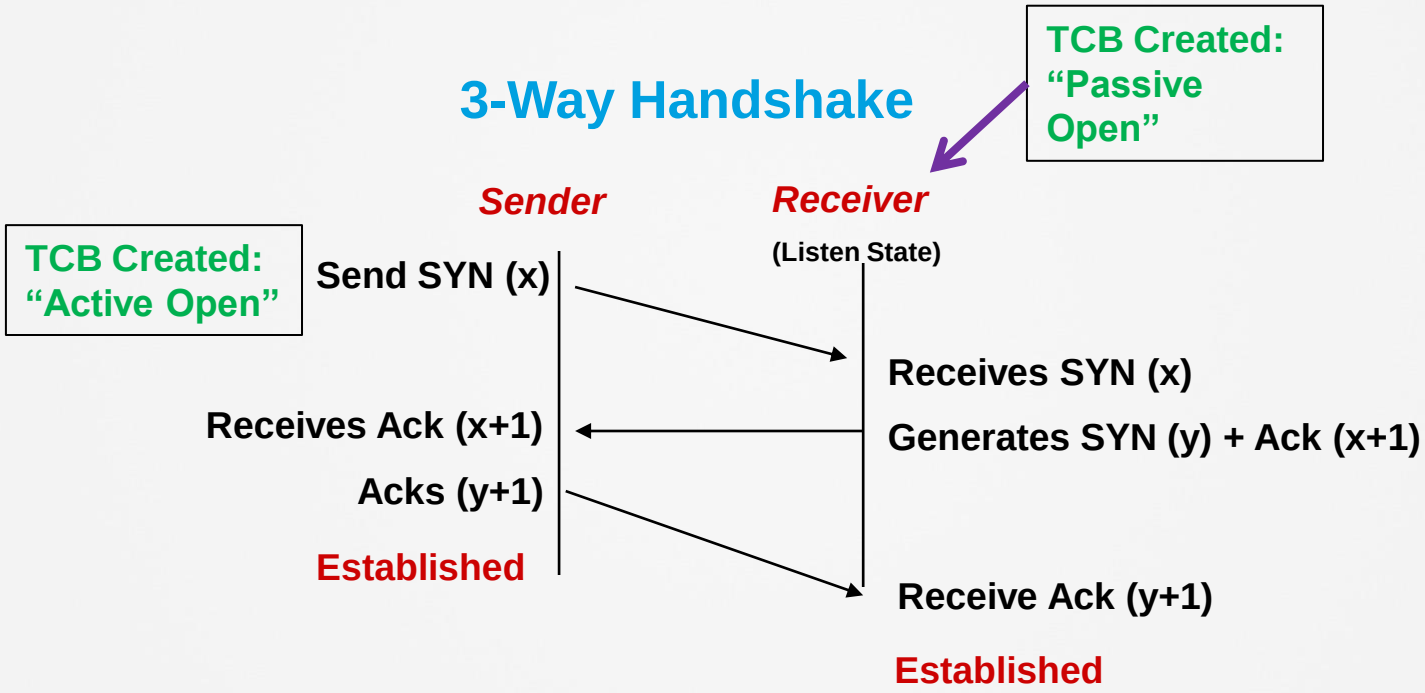
OSI Transport Layer - TCP

Transmission Control Protocol

- Connection-oriented



Setting-up TCP Connections



Why is this relevant?

- Blocking/Permitting specific applications with Firewalls or ACLs requires this knowledge.
- UDP and TCP respond differently to QoS Tools.
- Voice/Video typically utilize UDP
  - Intermittent drops okay
  - Intolerant of delay or jitter
- Data typically utilizes TCP
  - Minor delay or jitter okay
  - Drops are retransmitted

Ephemeral Ports

- Both TCP and UDP utilize Source/Destination Port numbers.
- Typically one of these ports is a well-known, reserved number
- The other port is randomized, called an “Ephemeral Port”
- IANA suggests the range 49152 to 65535 for Ephemeral Ports
  - Microsoft Windows operating systems through XP use the range 1025–5000 as ephemeral ports by default.
  - Windows Vista, Windows 7, and Server 2008 use the IANA range by default.
  - Many Linux kernels use the port range 32768 to 61000.

DNS

Names and Numbers

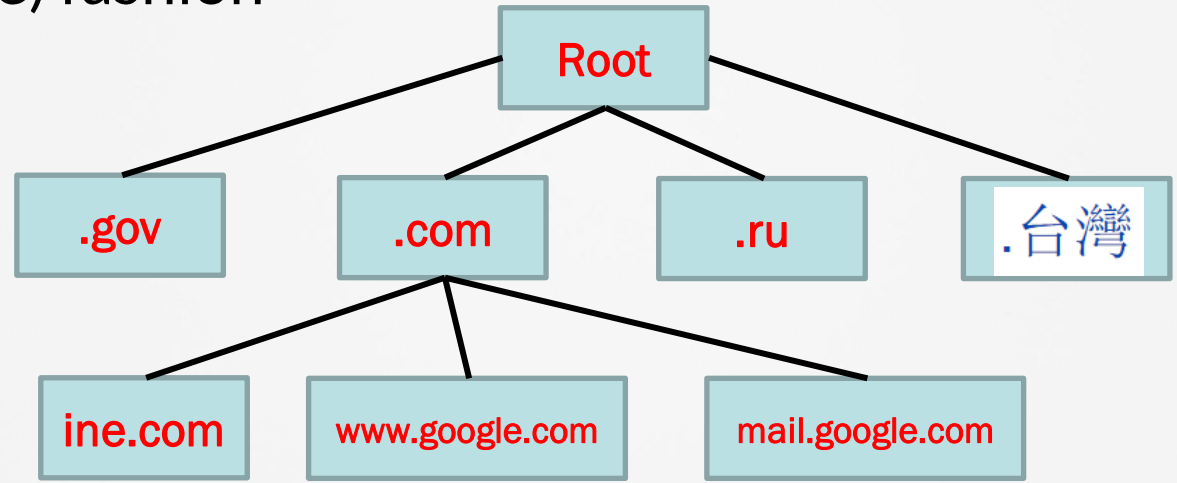
- Machines use numbers, Humans prefer names
- Name-Resolution protocols resolve/translate between the two.
- Allows numbers to dynamically change while the name remains the same.
- Names are called, “Symbolic Names” and consist of;
  - Letters
  - Numbers
  - Special characters

Domain Name Service

- DNS = Domain Name Service
- Originally defined in RFC 882 and 883
- L4 protocols used:
  - UDP and TCP (Port-53)
- Protocol for;
  - Defining structure of symbolic names (Name Space)
  - Registering symbolic names with registration authorities (Name Registration)
  - Determining method for resolving names to addresses. (Name Resolution)

Domain Name Service

- Distributed database of servers (name servers) in a hierarchical (tree-like) fashion



Domain Name Service

- Root Servers

List of Root Servers

Hostname	IP Addresses	Manager
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

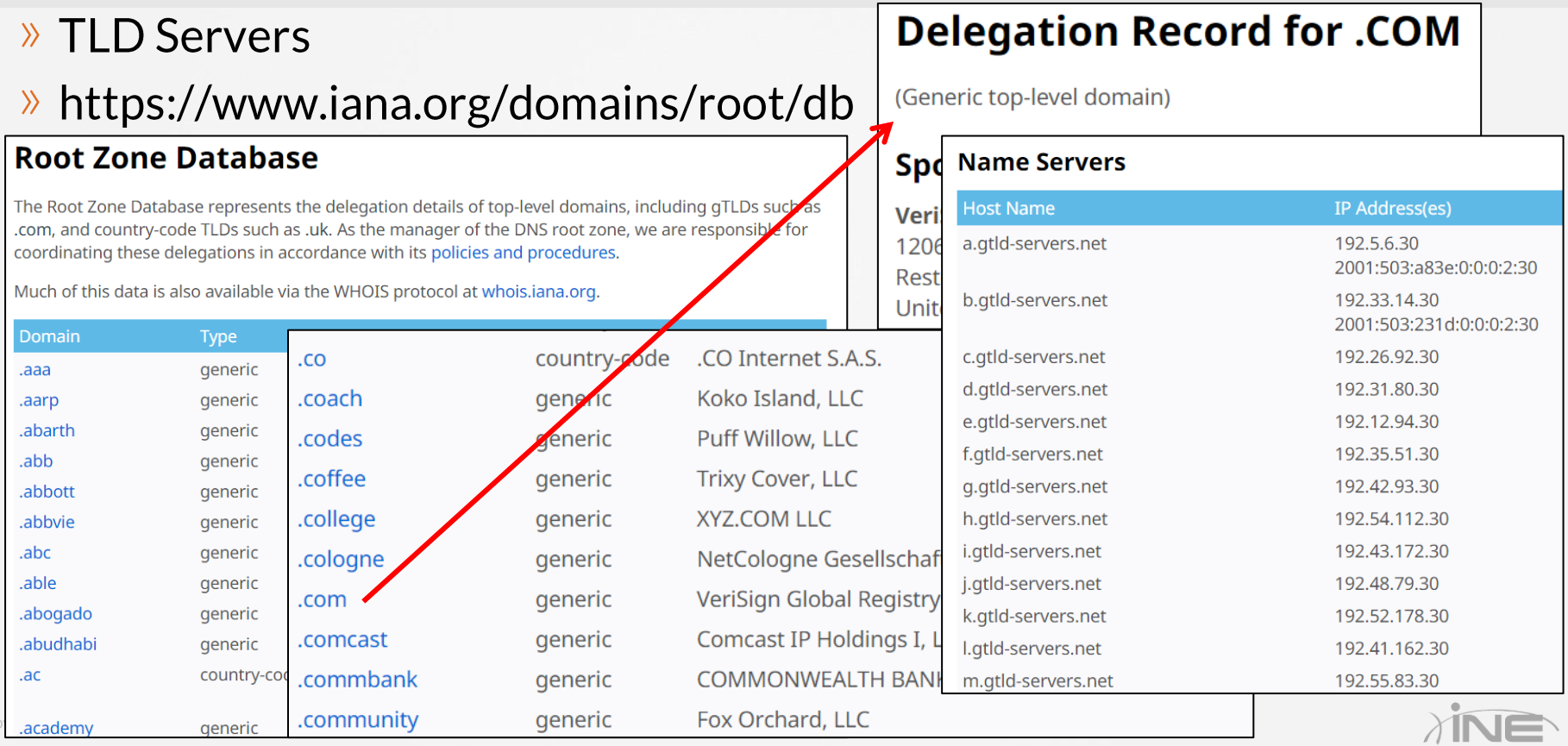
Domain Name Service

Where are Verisign's root servers?

As the trusted provider of Internet infrastructure services, Verisign manages and protects the global DNS infrastructure for more than 143.2 million .com and .net domain names. The company resolves more than 130 billion queries daily, while maintaining 100 percent operational accuracy and stability for more than 19 years.

Domain Name Service

- TLD Servers
- https://www.iana.org/domains/root/db



Root Zone Database

The Root Zone Database represents the delegation details of top-level domains, including gTLDs such as .com, and country-code TLDs such as .uk. As the manager of the DNS root zone, we are responsible for coordinating these delegations in accordance with its policies and procedures.

Much of this data is also available via the WHOIS protocol at whois.iana.org.

Domain	Type
.aaa	generic
.aarp	generic
.abarth	generic
.abb	generic
.abbott	generic
.abbvie	generic
.abc	generic
.able	generic
.abogado	generic
.abudhabi	generic
.ac	country-co
.academy	generic
.co	country-code	.CO Internet S.A.S.
.coach	generic	Koko Island, LLC
.codes	generic	Puff Willow, LLC
.coffee	generic	Trixy Cover, LLC
.college	generic	XYZ.COM LLC
.cologne	generic	NetCologne Gesellschaf
.com	generic	VeriSign Global Registry
.comcast	generic	Comcast IP Holdings I, L
.commbank	generic	COMMONWEALTH BANK
.community	generic	Fox Orchard, LLC

Delegation Record for .COM

(Generic top-level domain)

Spo

Veri

120

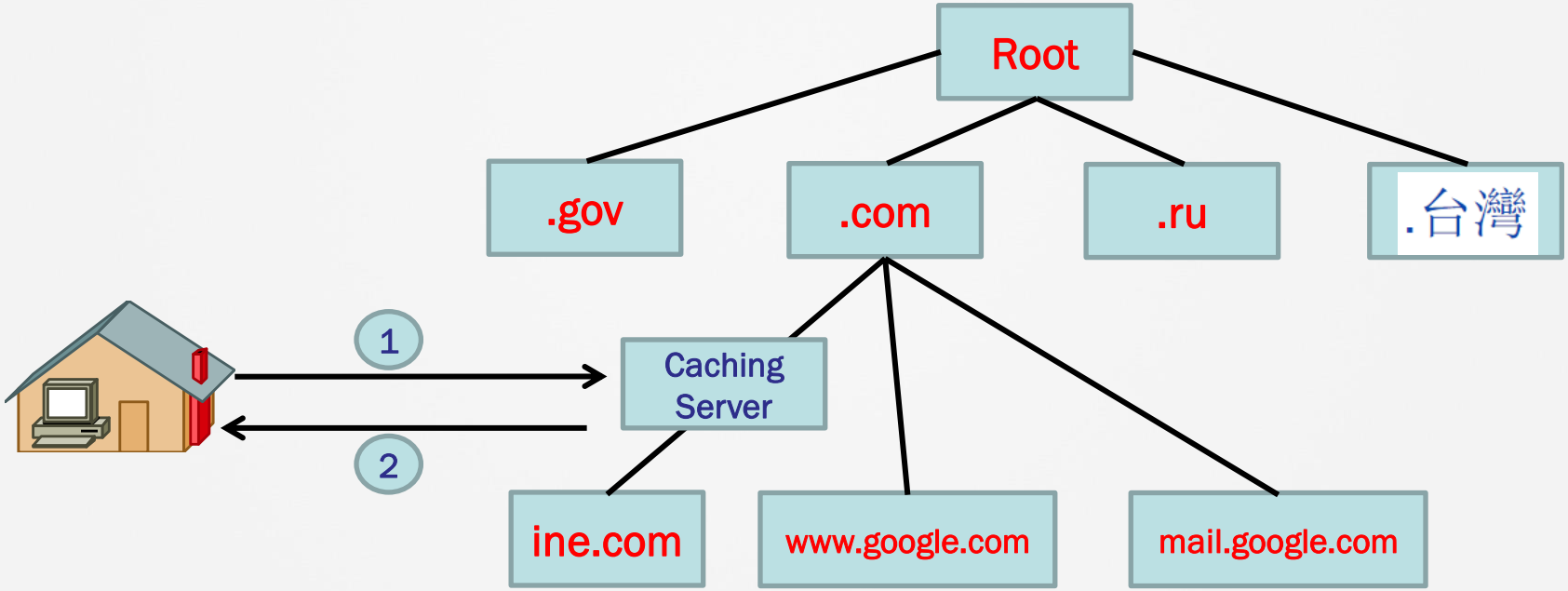
Rest

Unit

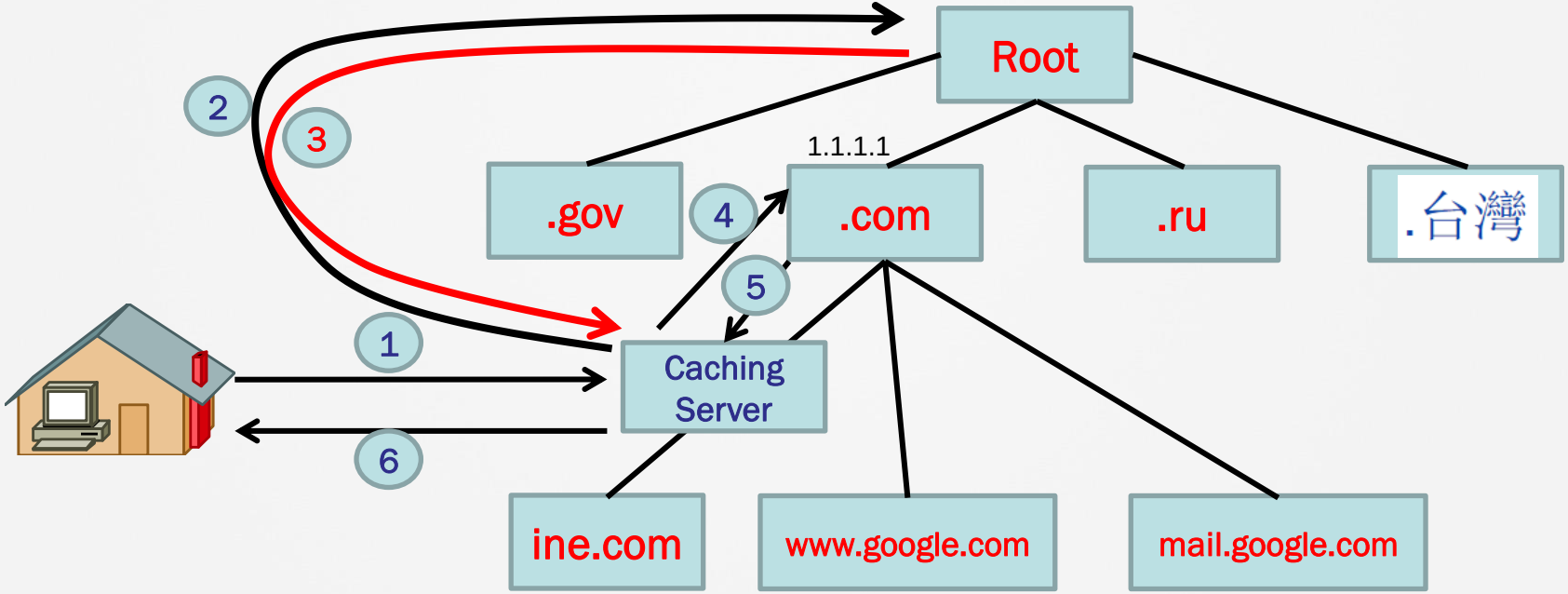
Name Servers

Host Name	IP Address(es)
a.gtld-servers.net	192.5.6.30 2001:503:a83e:0:0:0:2:30
b.gtld-servers.net	192.33.14.30 2001:503:231d:0:0:0:2:30
c.gtld-servers.net	192.26.92.30
d.gtld-servers.net	192.31.80.30
e.gtld-servers.net	192.12.94.30
f.gtld-servers.net	192.35.51.30
g.gtld-servers.net	192.42.93.30
h.gtld-servers.net	192.54.112.30
i.gtld-servers.net	192.43.172.30
j.gtld-servers.net	192.48.79.30
k.gtld-servers.net	192.52.178.30
l.gtld-servers.net	192.41.162.30
m.gtld-servers.net	192.55.83.30

Domain Name Service – Lookup Process



Domain Name Service – Lookup Process (2)



Categories/Types of Applications

Definitions

- All network applications fall into one-of-two categories:
- Client-Server
- Peer-to-Peer
- Stand-Alone
- Web-Based

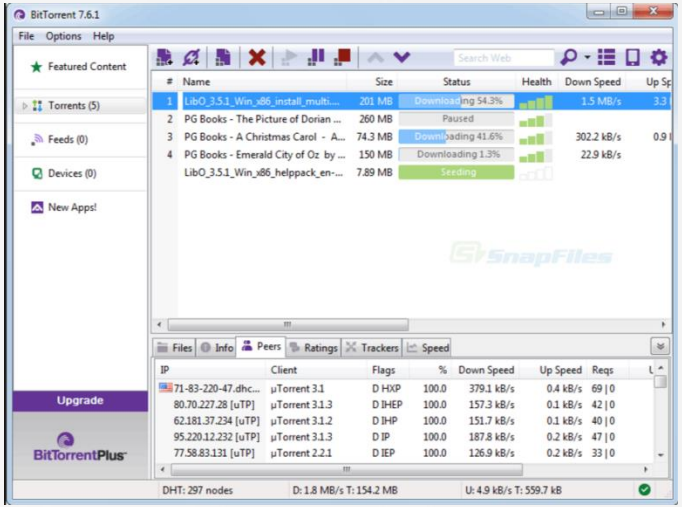
Client-Server

- Vast majority of applications utilize this approach.
- Typically TCP-based
  - Email
  - Web Browsing
  - Instant Messaging
  - YouTube

Peer-to-Peer

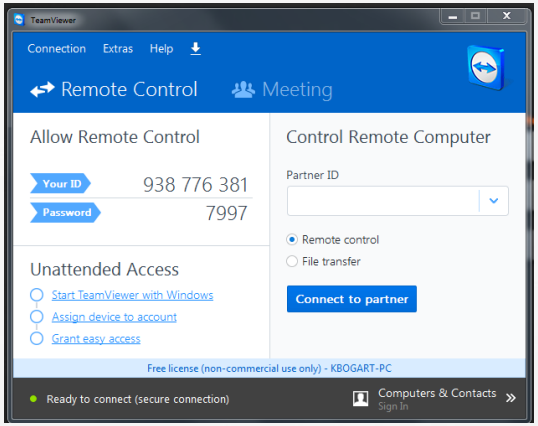
Two types of Peer-to-Peer

- Multi-Peer connection applications
  - ✓BitTorrent
- Single-Peer connection applications
  - ✓Skype



Stand-Alone Applications

- Has its own, dedicated front-end GUI (not embedded in a browser)
- Uses its own, distinct protocol (dedicated TCP or UDP port number)
- Typically one has to download appropriate version supported by your Operating System



Web-Based Applications

- Most network-based applications on laptops and PCs these days are web-based
- Even applications that might LOOK like they aren't web-based might actually really be.
- Non web-based applications will u se something other than HTTP/S to communicate with the remote server (like SecureCRT or PuTTY)
- Why should you care?

Email

Email – A History Lesson

- Early computing – "Dumb Terminals" connected to a common Mainframe.
- Early email = Placing a message into another user's directory
  - MAILBOX – first email system used at MIT in 1965
  - SNDMSG – early program used to send messages from one terminal to another.
- Internetworks evolve. System needed to put electronic messages into "envelopes" and address them.
- Ray Tomlinson – 1972: picks the @ symbol from the computer keyboard to denote sending messages from one computer to another.

Email name structure

- kbogart@ine.com
  - kbogart = name of the user
  - @ = indicates user is located on a remote computer
  - ine.com = Name of the Email Server

- user@domain.extension

Email – Common Protocols Used

SMTP

- Simple Mail Transfer Protocol
- Primarily for outgoing email
- TCP-based
- Port-25
- RFC 5321

POP3

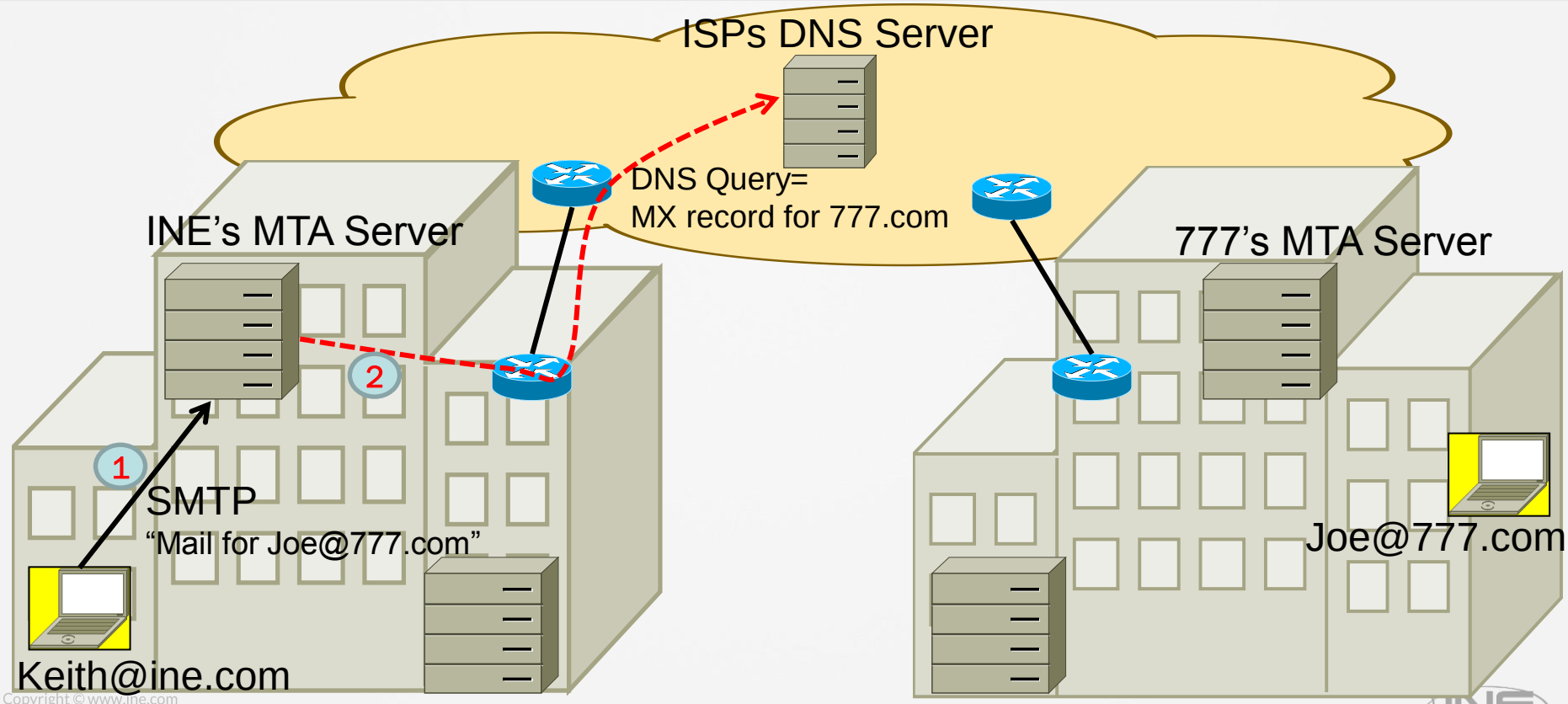
- Post Office Protocol
- TCP-Based
- RFC 1939
- Used to retrieve mail messages from a Mail Server to a Mail Client
- Uses Port 110 (or Port 995 for SSL/TLS sessions)
- Primarily designed to retrieve message, delete from server, disconnect from server.

Email – Common Protocols Used (continued)

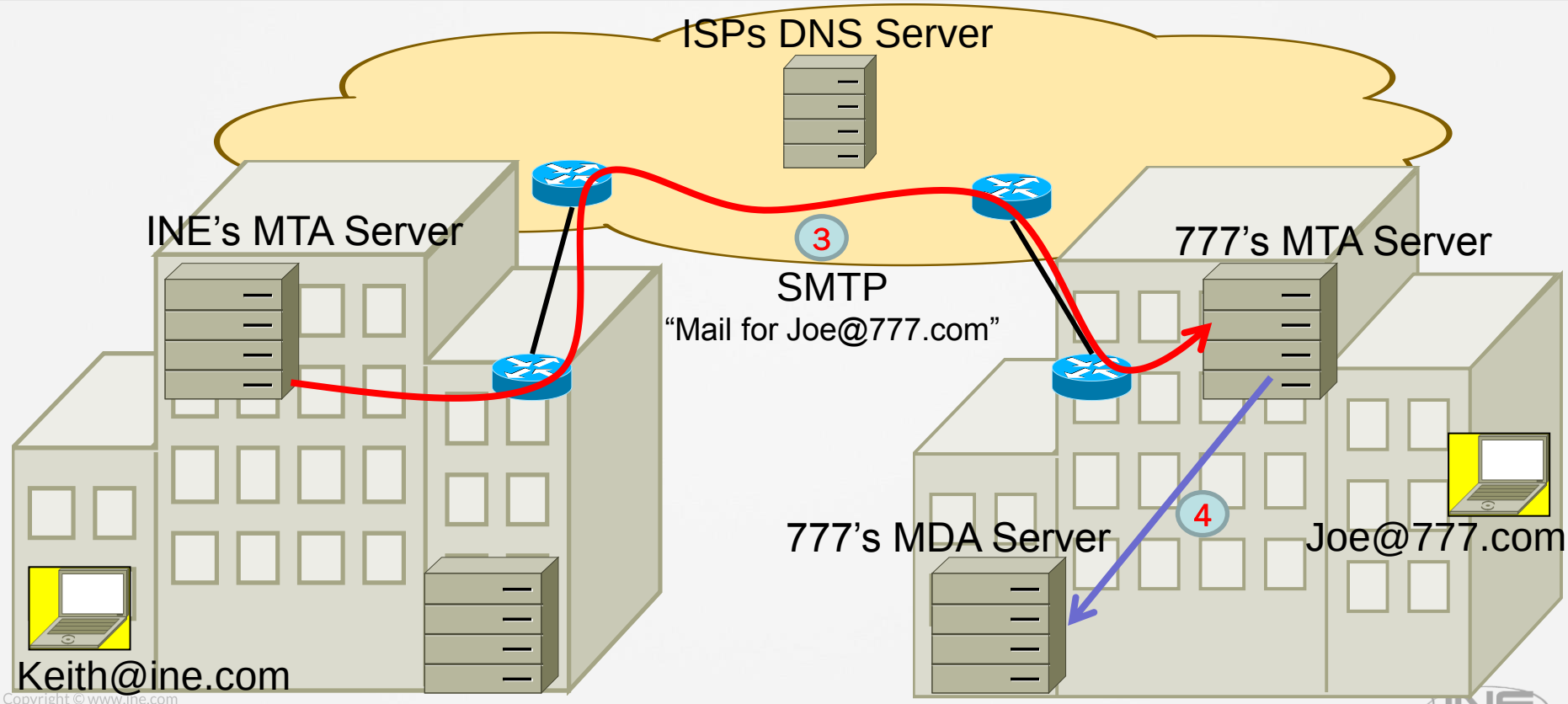
» IMAP4

- Internet Message Access Protocol
- TCP-Based
- RFC 3501
- Used to retrieve mail messages from a Mail Server to a Mail Client
- Uses Port 143 (or Port 993 for SSL/TLS sessions)
- Primarily designed to retrieve message, and stay connected to server until client is closed.
  - Includes flags to indicate status of messages (read, unread, etc) and group messages.
  - remain on mail server even after downloaded to client.

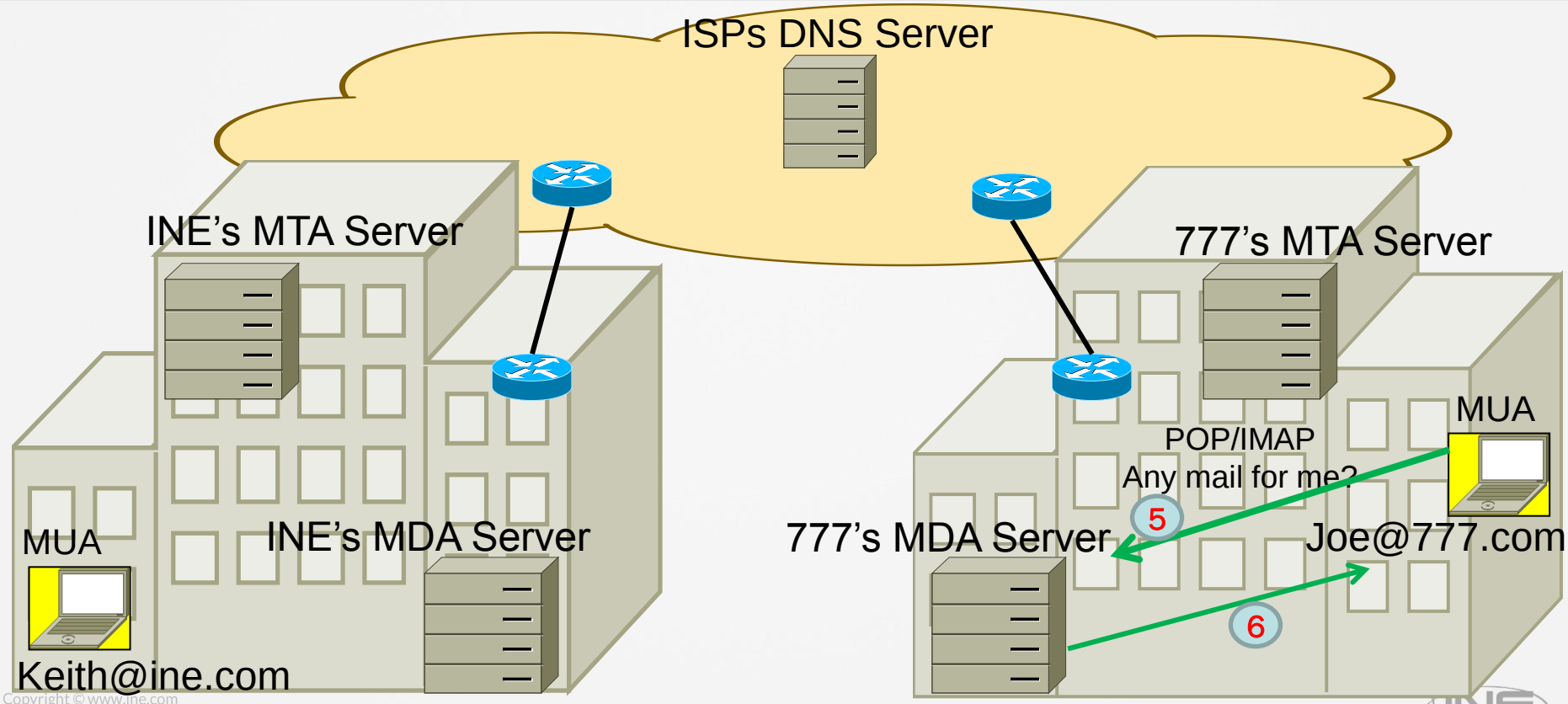
Email between Enterprises (1)



Email between Enterprises (2)



Email between Enterprises (3)



IMAP vs POP3

- Both are protocols which allow you to receive Email messages from the MTA (Mail Transfer Agent)
- Both support using 3rd Party Email clients
  - Outlook
  - Eudora
  - Etc
- POP: Designed to remove message from the server as it is downloaded to your MUA (Mail User Agent).
- IMAP: Retains copy of message on the server while temporarily caching a copy on your machine.

IMAP an d POP Workflow

- **POP Workflow:**
  - Connect to server.
  - Retrieve all mail.
  - Store locally as new mail.
  - Delete mail from server*.
  - Disconnect.
- **IMAP Workflow:**
  - Connect to server.
  - Fetch user requested content and cache it locally, e.g. list of new mail, message summaries, or content of explicitly selected emails.
  - Process user edits, e.g. marking email as read, deleting email, etc.
  - Disconnect.

IMAP and POP: Pros and Cons

- POP
  - Mail stored locally.
  - Internet connection needed only for sending and receiving mail.
  - Saves server storage space.
  - Option to leave copy of mail on server.
- IMAP
  - Mail stored on remote server,
  - Internet connection needed to read mail.
  - Faster overview as only headers are downloaded until content is explicitly requested.
  - Mail is automatically backed up if server is managed properly.
  - Saves local storage space.
  - Option to store mail locally.

Troubleshooting Email Problems

- MDA (Mail Delivery Agent)
  - There is no name or IP Address for the Receive-side email server,
  - The name of the MDA is wrong,
  - There is no username/account configured. (Account Settings → Email → Change)
- No Internet connectivity by the client.
- Email server name cannot be resolved via DNS
- Email server unreachable
- Incorrect credentials

Web Browsing

What is a Website?

- A collection of individual components (files) such as text, images, sounds, colors, links, and formatting that, when provided in the correct order, create a complete user-experience.
- Website has a name (ine.com) that, when reached, indicates the formatting of all of these elements.
- All websites start out as HTML, which is a language indicating all of the elements (files) of the site and how they should be displayed (formatted).
- A website is stored on a webserver that either:
  - Contains the assets (images, text, etc) locally or…
  - Knows where those assets are stored (a storage server).

HTTP vs HTML

- **HTTP = Hypertext Transfer Protocol**
  - Application-level protocol that is used to transfer data from HTTP Server to HTTP Client (Web Browser).
  - HTTP comprises the rules by which Web browsers and servers exchange information.
  - Uses Port-80
- **HTTPS = Secure HTTP (uses SSL/TLS for encryption and authentication)**
  - Uses port-443
- **HTML = Hypertext Markup Language**
  - The language used (among many others) to create a web-page.

Example of HTML

```
1  <!DOCTYPE html>
2  <html>
3      <head>
4          <title>Example<title>
5          <link rel="stylesheet" href="styl
6      </head>
7      <body>
8          <h1>
9              <a href="/">Header</a>
10         </h1>
11         <nav>
12             <a href="one/">One</a>
13             <a href="two/">Two</a>
14             <a href="three/">Three</a>
15         </nav>
```

HTTP Functionality

1. **Within your browser you type a URL**
   - Universal Resource Locator
2. **DNS invoked to resolve to IP address**
3. **Your browser initiates TCP 3-way handshake on port-80 (or 443) to server**
4. **After successful conclusion of 3-way handshake local browser sends HTTP GET message which includes;**
   - A specific directory for the website on the server (if the client knows one…which it usually doesn't)
   - The version of HTTP the client would prefer (typically version 1.1 but sometimes version 2.0)
   - Headers specifying the type, language, and encoding for the returned entity (information) that the client browser would prefer to receive from the server.

Basic HTTP Troubleshooting

- No Internet connectivity at all (can't reach any websites)
- DNS Server is unreachable (can't reach any new websites but websites that have already been resolved are functioning)
- DNS Server unable to resolve the name (maybe you mistyped it or it no longer exists)
- Remote Server is unreachable (problem within intermediate networks)
- Remote Server is entirely down (other websites CAN be reached)
- Remote Server has too many requests (extremely slow)
- Remote Server can't access all of the resources for the website (some images, text, or other elements are missing).

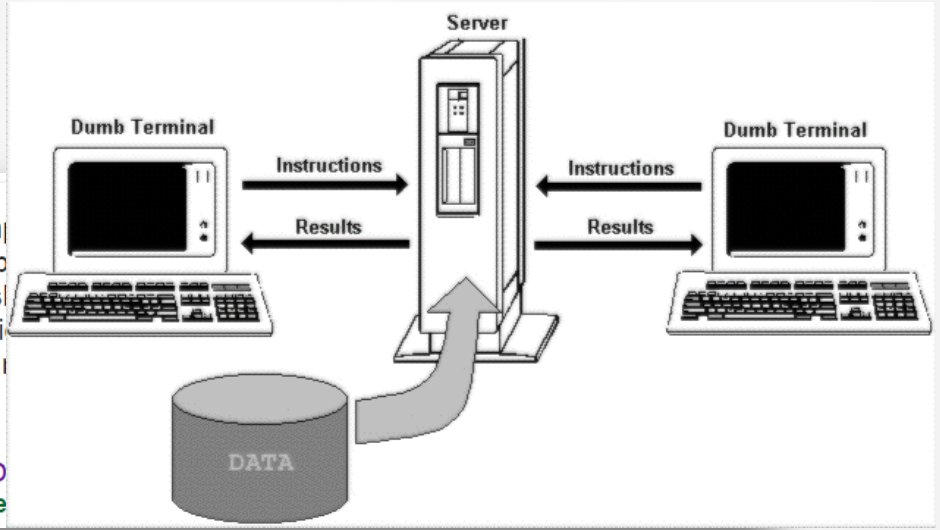
Telnet

What is Telnet?

- Prior to Telnet: Dumb terminals were used to connect to the Shell of a device.
  - What is a “Shell”?

Shell (computing) ... In comp
interface for access to an op
general, operating system **sh**
line interface (CLI) or graphi
depending on a computer's

Shell (computing) - Wikip
https://en.wikipedia.org/wiki/**She**



Telnet was the answer to this question: How can we provide a user the same ability to interact with the Shell, if their terminal is not directly-connected to the Computer Periphery but instead only reachable remotely over an IP connection?

Telnet Facts

- Telnet defined in RFC 854
- TCP-based
- Used to access the CLI of remote devices over an IP connection.
- Typically creates small packets
- Uses well-known TCP port 23
- Data in IP packets sent in clear-text

How does it actually work?

- When Telnet is invoked in a system, both sides (Host and Process within a Server) of the connection are “assumed to originate and terminate at a "Network Virtual Terminal", or NVT
- Telnet sends/receives two things:
  - Data (either stuff you type or output from the process Shell)
  - Negotiated Options (things that dictate how the NVT will be displayed and act)

Telnet's "Negotiated Options"

- Do, Don't, Will, Won't
- Common Negotiated Options:
  - Suppress Go Ahead
  - Negotiate Window Size
  - Echo

Thank You!!