Network Applications and Services

INFO 341

December 2, 2016

Scott Barker, barker@uw.edu

Information School
UNIVERSITY of WASHINGTON

Today's agenda

- Wide overview of network services and applications from a network administrator, enterprise, and end-user perspective
  - Some are small and easy to digest
  - Others could take extensive experience (years) and multiple classes to become an expert
  - Some follow Internet standards, others are "proprietary", some on prem, some in the cloud
- Fundamentally they are the reason we care about networks
  - There is there is more to networking than just plumbing

But first….
Review of a couple fundamental infrastructure services

- **DHCP** – Dynamic Host Configuration Protocol
  - What does it do, when is it utilized vs. static assignments, why is it especially important in mobile device scenarios?

- **DNS** – Domain Name Service
  - What is it, why is it important, what are some of the common top level domains, how does name registration work?
  - iSchool story

Other Infrastructure related…

- **NTP** – Network time protocol
  - Synchronize time and date, why important?

- **Wake on Lan** – magic packet sent to designated MAC address(es) to wake-up devices that are powered-down or in sleep/hibernate

- **BOOTP** – similar idea as DHCP, get an IP address, but also get the location of a boot image file to boot the device. Image downloaded via tftp. Typically used with old style diskless Unix workstations

- **PXE Boot** – pre-execution environment, similar concept to BOOTP but frequently used to boot modern PC's for system deployment/imaging/setup. Not supported by Apple devices.

Internet standards-based applications

- Overseen by IETF – Internet Engineering Task Force, divided into working groups around specific areas (web, email, etc)

- Standards are developed and published as RFC's – request for comments, and eventually adopted (or abandoned)

  www.ieft.org

- Primary goal of standards is to promote interoperability, eg. you can send email to anyone regardless of the email client or service they use because all agree to a standard

Review some old ones you may know…

- **Telnet - first RFC's written in 1971!**
  - Connect to another host/computer remotely
  - "Dumb-terminal" command line interface
  - Terminal emulation often provided by the telnet client
    - (VT-100, VT-220 most common)
  - TN3270 a modified form, for IBM 3270 emulation
  - Runs over port 23, connection is in "clear-text"
    - Today many require SSH (Secure-Shell, port 22) instead
  - Can you connect to any remote computer via telnet? What needs to be in place? What can you do once there?
  - Note the importance of gaining command line proficiency

FTP – File Transfer Protocol

RFC first published again in 1971

- Mechanism for moving files between a client and a server, runs over port 21, typical CLI (command line) session might look like:

ftp server.someplace.com

You are then prompted for a username and password, anonymous FTP may be possible using "anonymous" as the username and typically your email for password

ftp> **ls** *(list files in this folder, may need to cd to "change directory")*

Files are listed here….

ftp> **bin** *(tell the client and server this is a binary file I want to transfer, defaults to ascii/text)*

ftp> **hash** *(display hash marks - #, to watch progress)*

ftp> **get myfile.doc** *(retrieve the file, alternatively "put" to upload)*

########## (hash-marks show as file downloads/uploads)

ftp> **quit** *(end the ftp session)*

- Like telnet, there is a client and a server necessary
- Many GUI FTP clients available for Windows/Mac, does anyone use FTP today?
- Like telnet, everything "in the clear", many sites now require SFTP instead for encryption
- Some old networking gear uses tftp – trivial ftp to download/update firmware

Email Standards
Multiple Protocols in Use

- SMTP – Simple Main Transfer Protocol (port 25), initially RFC 821, in 1982
  - Provides a mechanism for **ascii/text** messages to be transmitted between hosts
  - Not involved with managing the messages (reading/downloading mail, deleting messages from an inbox etc.) – those handled by other protocols

Sample SMTP session between a client (C) and a server (S) using telnet to demo:
http://en.citizendium.org/wiki/SMTP_example_sessions

```
$ telnet example.org 25
S: 220 example.org ESMTP Sendmail 8.13.1/8.13.1; Wed, 30 Aug 2006 07:36:42 -0400
C: HELO mailout1.phrednet.com
S: 250 example.org Hello ip068.subnet71.gci-net.com [216.183.71.68], pleased to meet you
C: MAIL FROM:<xxxx@example.com>
S: 250 2.1.0 <xxxx@example.com>... Sender ok
C: RCPT TO:<yyyy@example.com>
S: 250 2.1.5 <yyyy@example.com>... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
From: Dave\r\nTo: Test Recipient\r\nSubject: SPAM SPAM SPAM\r\n\r\nThis is message 1 from our test
script
.
S: 250 2.0.0 k7TKIBYb024731 Message accepted for delivery
C: QUIT
S: 221 2.0.0 example.org closing connection
Connection closed by foreign host.
$
```

MIME
Multipurpose Internet Mail Extensions

- Extends SMTP to
  - Support non-ASCII text in a message
  - Support Binary files/attachments such as video, audio, Word docs etc. and allows various encoding mechanisms to convert binary to a text representation (such as base64) so it can be sent using SMTP
  - A MIME message might look something like: https://en.wikipedia.org/wiki/MIME

```
MIME-Version: 1.0 Content-Type: multipart/mixed;
boundary=frontier
This is a message with multiple parts in MIME format.
--frontier
Content-Type: text/plain
This is the body of the message.
--frontier
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
PGh0bWw+CiAgPGhlYWQ+CiAgPC9oZWFkPgogIDxib2R5PgogICAgPHA+VGhpcyB
pcyB0aGUg
Ym9keSBvZiB0aGUgbWVzc2FnZS48L3A+CiAgPC9ib2R5Pgo8L2h0bWw+Cg==
--frontier--
```

POP (POP3)
Post Office Protocol

- Essentially store, copy, delete. Mail is stored on the server until the client connects and then is downloaded to the client. Mail is then deleted from the server.
- Simple protocol and widely used. Many clients available like Thunderbird, old Outlook Express.
- Many ISP's used to suggest you use a POP client for mail. Good for them in that you connect and then the mail is removed from their server.
- Very bad for users that use multiple machines during the day. Why?
- Today most consumers used Web-based email like Gmail, Yahoo Mail, or Outlook.com instead.
    - Why might web-based solutions be more popular today than they were 5-10 years ago?

IMAP4
Internet Mail Access Protocol

- IMAP4 largely developed here at UW!
  - RFC 1730, Mark Crispin University of Washington, 1994
- Folders and Messages can be stored on the server or in local folders.
  - Since folders can remain on server, it is possible to access your same mail from any device and see it all.
  - Much better for people using multiple machines than POP.
- Has a mechanism to work “off-line” and then resynchronize the changes when you reconnect
- Like everything else, client/server architecture. Need to run an IMAP4 server and configure a client email program (Outlook, Thunderbird, Mobile phone email app, to talk to that server.)

Instant Messaging contrast to email

- Unlike email where Internet standards were adopted and agreed upon early, IM is mostly a collection of “proprietary” solutions that don’t interoperate

- XMPP – Extensible Messaging and Presence Protocol (originally called Jabber) is one attempt, but not universally adopted by all and in fact support has been dropped by early proponents (Google Talk)

- Opinion, an example of where standards based interoperability would be good for many users, but not good for the companies offering clients. They want to lock you into their eco-system. Another example: Apple FaceTime and iMessage

HTTP
Hypertext Transfer Protocol

- Protocol of the web, initial RFC 1945 written in 1996 for HTTP 1.0, Tim Berners-Lee, experimental use of http began in 1990, HTTP 2.0 adopted 2015
- Runs over port 80, or 443 for “https”
- Request/response protocol where a client (web browser) makes a request for a particular URI from a server (Apache, Microsoft IIS), e.g.

  GET /path/to/file/index.html HTTP/1.0

- The server responds with a response code and the info requested, e.g.

  200 OK
  The request succeeded, resulting resource is returned in the message body.
  404 Not Found
  The requested resource doesn't exist.
  301 Moved Permanently
  302 Moved Temporarily
  303 See Other *(HTTP 1.1 only)*
  The resource has moved to another URL
  500 Server Error

Common LAN Network Services

File and Print Sharing

File Services

- Disk on a wire concept – fast access to remote files just like they existed locally on your device

- In Windows we “share” a folder on a file server, and “map” it on the client with File Explorer or as a new drive letter, e.g.

  net use n: \\server.ischool.uw.edu\myfolder

  Other operating systems have similar concepts. In Unix you “mount” a shared folder at a designated mount point. On a Mac go to Finder, Connect to server, enter the path, e.g.

  smb://server.ischool.uw.edu/myfolder

File Service Protocols

- **SMB** – Server Message Block
  - Also referred to as CIFS – Common Internet File System
  - Typically used to access Windows shares
  - "Samba" allows Linux/Unix devices to access the same shares or act as a file server for Windows devices
  - Mac also able to access SMB shares (prior example)
  - Multiple versions, SMB 2, SMB 3 – added features and functionality in later versions of Windows can cause issues with some older operating systems/devices

- **NFS** – Network File System
  - Multiple versions (2, 3, 4), typically used on Linux/Unix centric environments, not typically used with PC/Windows clients, but possible

- **AFP** – Apple Filing Protocol
  - Typically used only in all Apple environments, use the finder, but afp://

Some Print Service Protocols

- Printer on a wire concept, same idea as with file sharing
- We “share” a printer on a print-server and connect to from the client so it appears like a local printer to users

- SMB - Windows
- LPD/LPR – line printer, line printer remote protocol Unix
- Bonjour – Apple, also works with Windows as a background service. Facilitates end-user discovery of printers.

Authentication and Authorization

Keys to the Kingdom

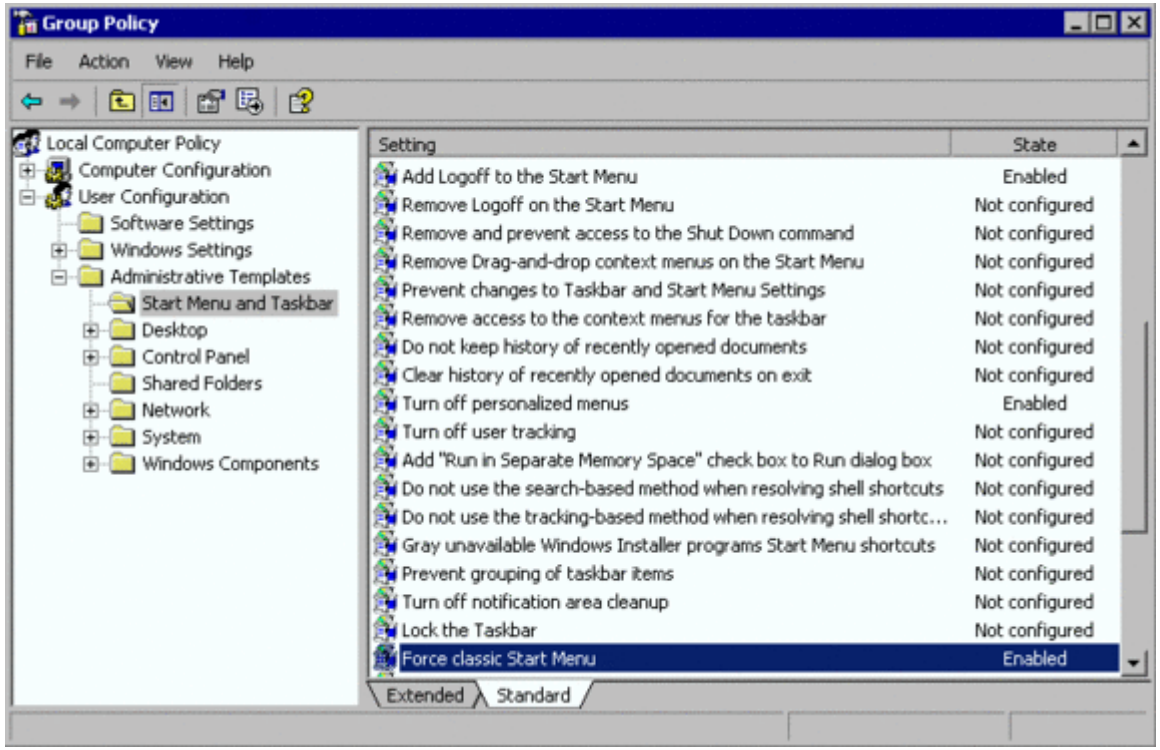
- When sharing resources, being able to control who can see and do what with those resources in critical. Why?
- To accomplish our goals, we utilize two different concepts, authentication and authorization. They are NOT the same.
- Authentication – I claim to be a particular person, and there is some mechanism in place to verify I am who I claim to be (such as a userid and password).
- Authorization is a process where certain rights are granted to particular people (or groups).
  - Scott Barker has read only access to a particular folder, or only the HR group can print to a particular printer.
  - To use particular network services, we have to both authenticate and verify authorization.

Active Directory

- Windows centric technology for managing authentication and authorization. Objects present in AD include users, computers, and groups
- User objects have properties associate with them such as userid, password, first name, last name, other directory type info like phone, email address, or supervisor
- Groups can be used to bunch multiple users together (like those in the HR department)
- System admins create (or provision via automation) users and groups, they "join" computers to the domain so all share the same credentials, and they specify rights (sometimes called "ACL" – Access Control Lists) to file shares, printers etc. to control access. Using Groups to set ACLs is best.
- This critical data is stored on "domain controllers", designated servers that are typically redundant and the most protected/secured devices on a LAN. Compromise of a "domain controller" is a disaster. Why?

Group Policy

- Active Directory Group Policy allows IT to manage many machines with a high level of control in a scalable fashion
  - Can set thousands of configuration options in Windows or in many applications, everything from screen saver to Word default font, automatically deploy new printers and map drives, install new software applications, enforce security policies



Federated Authentication

- Active Directory great for common on-prem scenarios but….consider wanting to deploy a third party cloud service throughout your organization where authentication and authorization is needed
  - e.g. Canvas, iSchool Microsoft Imagine Software downloads
  - Do you want users to have a separate id/password on that system, do you want them storing their credentials on that service, what if you are running that service and you are compromised?

- Federated login is the idea of leveraging one credential (such as Active Directory id/password) for use on another system in a way that only the very minimum amount of information is shared with the third party. Sometimes people call this “single sign-on” or SSO

Federation Technologies

- **SAML** – Security Assertion Markup Language, allows exchange of authorization information between an identity provider (idp) and a service provider (sp)
- **Oauth** – authentication only protocol
- **OpenID** – authorization only protocol
- **Shibboleth** – web based technology that provides both authentication and authorization by sharing security tokens, based on SAML, widely used by many Universities across the world. E.g.: http://ischool.uw.edu/dreamspark
- **ADFS** – Active Director Federated Services, allows establishing "trusts" across organizations that have their own Active Directories

The Cloud

- Many traditional “on-prem” services now moving to the cloud
- Services such as Amazon AWS or Microsoft Azure allow IT to potentially scale servers “on demand” and respond more quickly to end-user needs. Others like Office 365 allow outsourcing common enterprise applications like email, IM, file sharing, collaboration.
- But…large concerns about security, loss of control, and regulation/compliance
- Also lots of talk now about “the consumerization of IT”, where consumer services may be “better” from an end-user perspective than those provided by IT (e.g. Dropbox instead of the N: drive)
- We are thinking about a whole course in cloud computer for spring!

Conclusion

- There is a LOT more to learn about networking, the infrastructure side is just the beginning
- Thinking about what our users need, what applications are available, and how we facilitate access to the best tools while still maintaining the desired requirements around security and compliance is one of the biggest and most difficult challenges companies face today