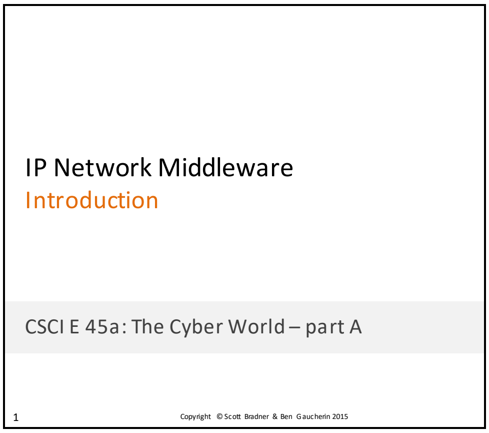
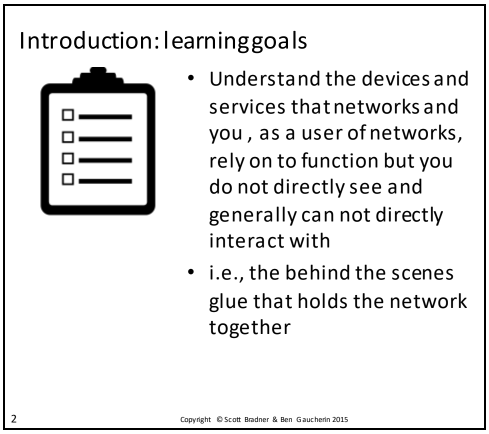


IP Network Middleware

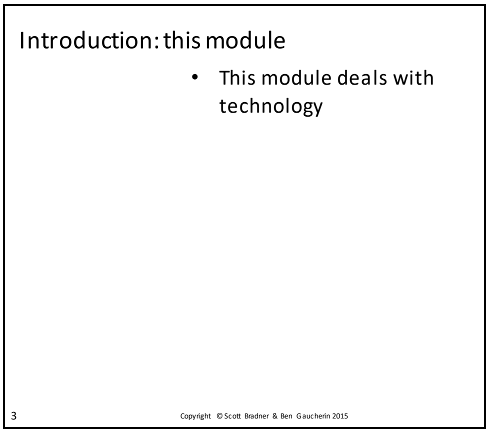
Introduction

CSCI E 45a: The Cyber World – part A



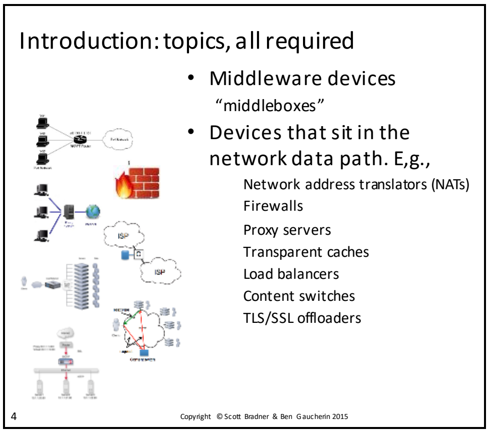
Introduction: learning goals

- Understand the devices and services that networks and you , as a user of networks, rely on to function but you do not directly see and generally can not directly interact with
- i.e., the behind the scenes glue that holds the network together



Introduction: this module

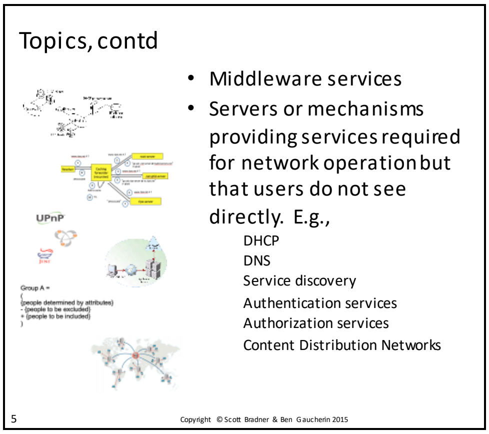
- This module deals with technology



Introduction: topics, all required

- Middleware devices
  “middleboxes”
- Devices that sit in the network data path. E,g.,
  - Network address translators (NATs)
  - Firewalls
  - Proxy servers
  - Transparent caches
  - Load balancers
  - Content switches
  - TLS/SSL offloaders

4 Copyright © Scott Bradner & Ben Gaucherin 2015

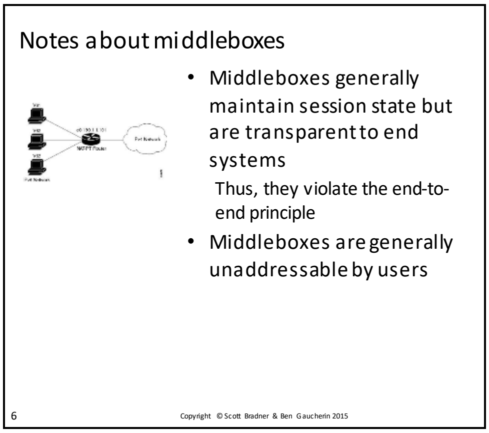


Topics, contd

- Middleware services
- Servers or mechanisms providing services required for network operation but that users do not see directly. E.g.,
  - DHCP
  - DNS
  - Service discovery
  - Authentication services
  - Authorization services
  - Content Distribution Networks

UPnP
Group A =
{
(people determined by attributes)
- (people to be excluded)
+ (people to be included)
}

5 Copyright © Scott Bradner & Ben Gaucherin 2015



Notes about middleboxes

- Middleboxes generally maintain session state but are transparent to end systems
  Thus, they violate the end-to-end principle
- Middleboxes are generally unaddressable by users

6 Copyright © Scott Bradner & Ben Gaucherin 2015

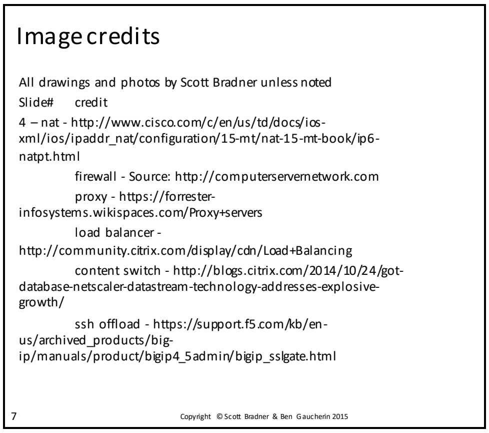


Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

4 – nat - http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/ip6-natpt.html

firewall - Source: http://computerservernetwork.com

proxy - https://forrester-infosystems.wikispaces.com/Proxy+servers

load balancer - http://community.citrix.com/display/cdn/Load+Balancing

content switch - http://blogs.citrix.com/2014/10/24/got-database-netscaler-datastream-technology-addresses-explosive-growth/

ssh offload - https://support.f5.com/kb/en-us/archived_products/big-ip/manuals/product/bigip4_5admin/bigip_sslgate.html

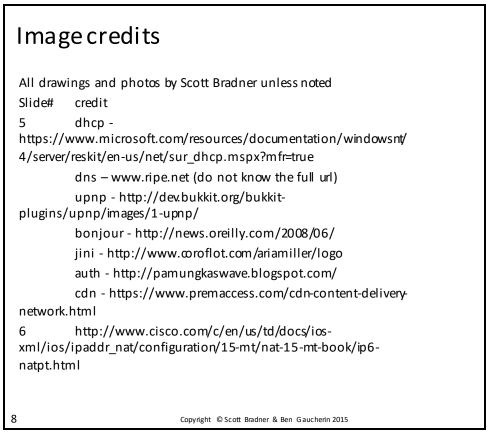


Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

5 dhcp - https://www.microsoft.com/resources/documentation/windowsnt/4/server/reskit/en-us/net/sur_dhcp.mspx?mfr=true

dns – www.ripe.net (do not know the full url)

upnp - http://dev.bukkit.org/bukkit-plugins/upnp/images/1-upnp/

bonjour - http://news.oreilly.com/2008/06/

jini - http://www.coroflot.com/ariamiller/logo

auth - http://pamungkaswave.blogspot.com/

cdn - https://www.premaccess.com/cdn-content-delivery-network.html

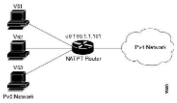
6 http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/ip6-natpt.html

IP middleware

Network Address Translators (NATs)

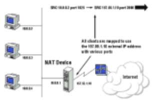
CSCI E 45a: The Cyber World – part A

Network Address Translators (NATs)

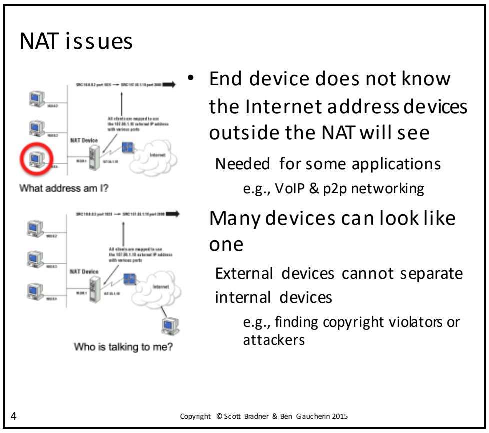


- Translate IP addresses in transiting packets
  - Different address ranges in different networks
    - e.g., private addresses in home network
- Can look like a different number of devices
  - NAT-PT (network address and port translation) can make a whole network of devices look like a single device
- Can be IPv4 <-> IPv4 or IPv4 <-> IPv6

Why use a NAT?



- Deal with the fact that ISPs frequently assume one address per customer
  - Even if customer has house full of devices
- Public address conservation
- Add some (limited) security
  - Outside attacker does not know internal address
  - Does not protect against clicking on a malware link

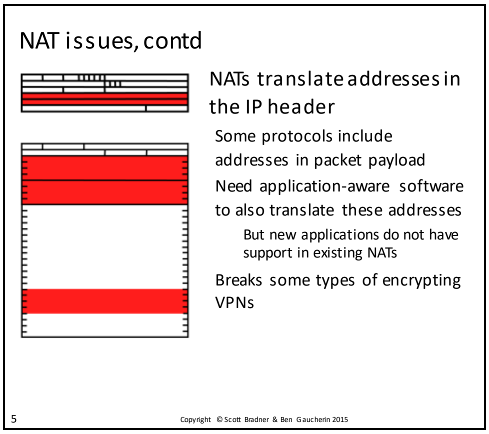


NAT issues

What address am I?
Who is talking to me?

- End device does not know the Internet address devices outside the NAT will see
  - Needed for some applications
    - e.g., VoIP & p2p networking
- Many devices can look like one
  - External devices cannot separate internal devices
    - e.g., finding copyright violators or attackers

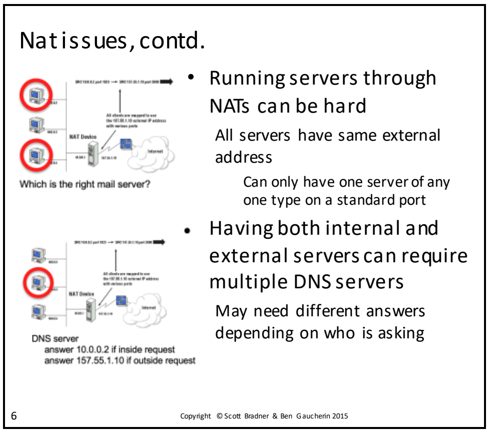
4



NAT issues, contd

- NATs translate addresses in the IP header
  - Some protocols include addresses in packet payload
  - Need application-aware software to also translate these addresses
    - But new applications do not have support in existing NATs
  - Breaks some types of encrypting VPNs

5



Nat issues, contd.

Which is the right mail server?
DNS server
answer 10.0.0.2 if inside request
answer 157.55.1.10 if outside request

- Running servers through NATs can be hard
  - All servers have same external address
    - Can only have one server of any one type on a standard port
- Having both internal and external servers can require multiple DNS servers
  - May need different answers depending on who is asking

6

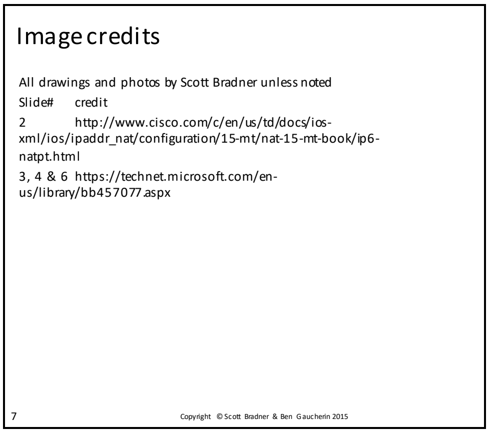


Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/ip6-natpt.html
3, 4 & 6	https://technet.microsoft.com/en-us/library/bb457077.aspx

IP Network Middleware
Firewalls

CSCI E 45a: The Cyber World – part A

Firewalls

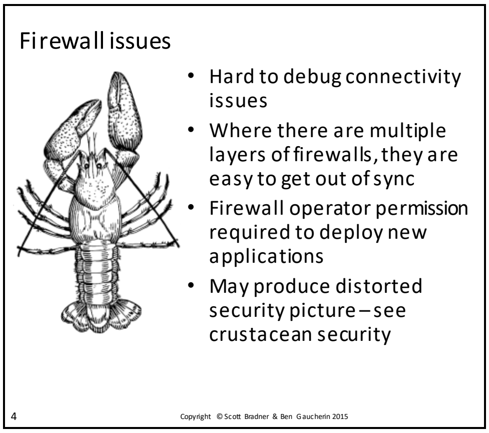
- The purpose of a firewall is to disrupt traffic flow
- A firewall uses a set of rules to decide which transit traffic to permit and which to block

  Rules can refer to:

  Traffic source, traffic destination, packet features, application (port), session state, content, etc.
- Firewalls can be network- or host-based

Why use a firewall

- Control access to a portion of a network or the hosts on a section of the network
- Protect hosts from attack
- Filter contents
- Limit internal access to external resources



Firewall issues

- Hard to debug connectivity issues
- Where there are multiple layers of firewalls, they are easy to get out of sync
- Firewall operator permission required to deploy new applications
- May produce distorted security picture – see crustacean security

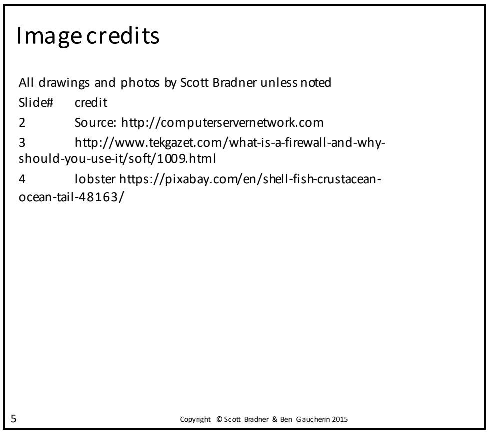


Image credits

All drawings and photos by Scott Bradner unless noted

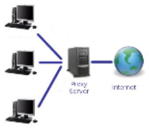
Slide#	credit
2	Source: http://computerservernetwork.com
3	http://www.tekgazet.com/what-is-a-firewall-and-why-should-you-use-it/soft/1009.html
4	lobster https://pixabay.com/en/shell-fish-crustacean-ocean-tail-48163/

IP Network Middleware

Proxy servers

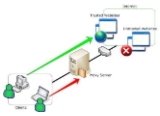
CSCI E 45a: The Cyber World – part A

Proxy servers



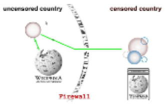
- A server that is used as an intermediary between clients and servers
  - Most common: web & DNS
  - But can, in theory, be used for any application

Why use a proxy server



- Cache results
  - Improve performance
  - reduce load on server or Internet link
- Log usage
- Filter content and locations (like firewall)
- Hide client addresses (provide anonymity)
- Bypass network-based controls
  - e.g., firewalls, government or enterprise restrictions

Proxy server issues



- Generally not transparent

  Client must be configured to point to proxy
- Can be used to bypass enterprise network use restrictions
- Can be used to bypass government network use restrictions
- Logs usage (privacy issue)

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	https://forrester-infosystems.wikispaces.com/Proxy+servers
3	http://techreviewpro.com/top-best-free-proxy-sites-list-free-proxy-server-lists-2015/
4	http://commons.wikimedia.org/wiki/File:Psiphon.jpg

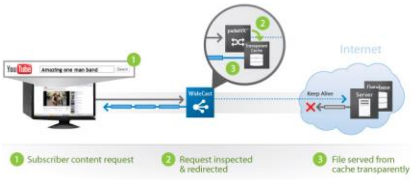
IP Network Middleware

Transparent caches

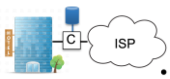
CSCI E 45a: The Cyber World – part A

Transparent cache

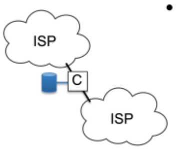
- Monitors outgoing requests & responds if requested information is in cache
  - Forwards request if not in cache, caches result

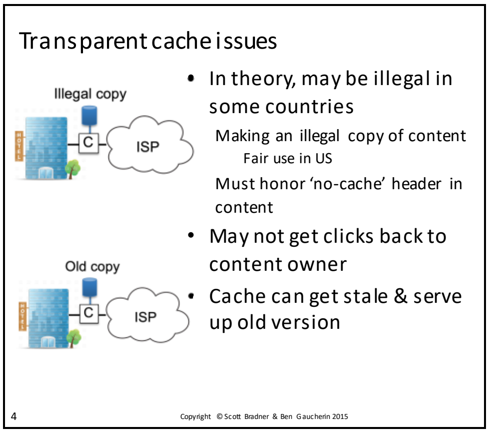


Why use a transparent cache?



- Used in hotels
  - Improve performance
  - Reduce usage of Internet link for popular material
- Also can be used to filter content & locations
- Used in ISPs
  - Improve performance
  - Reduce usage of transit service
  - Does not require a business relationship or specific configuration (unlike a Content Distribution Network)





Transparent cache issues

- In theory, may be illegal in some countries
  - Making an illegal copy of content
    - Fair use in US
  - Must honor 'no-cache' header in content
- May not get clicks back to content owner
- Cache can get stale & serve up old version

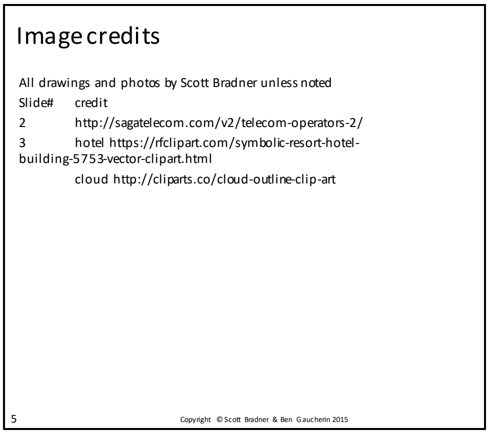


Image credits

All drawings and photos by Scott Bradner unless noted

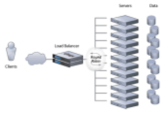
Slide#	credit
2	http://sagatelecom.com/v2/telecom-operators-2/
3	hotel https://rfclipart.com/symbolic-resort-hotel-building-5753-vector-clipart.html cloud http://cliparts.co/cloud-outline-clip-art

IP Network Middleware

Load balancers

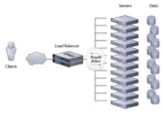
CSCI E 45a: The Cyber World – part A

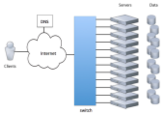
Load Balancers



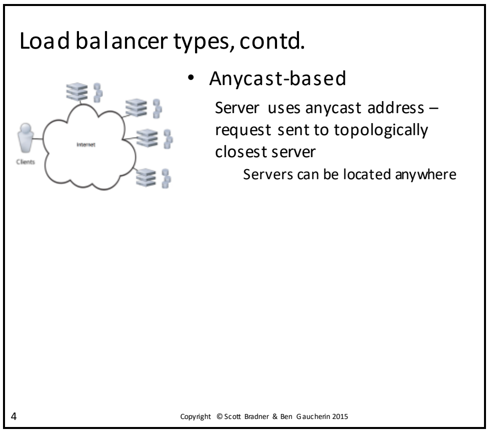
- Device used to interceptand distribute service requests among servers
- Mechanism to distribute service requests among servers

Load balancer types



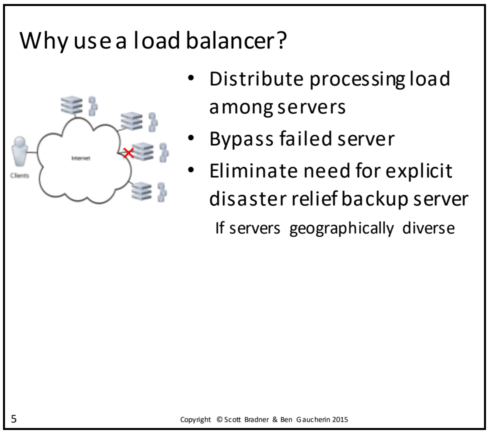


- Device-based
  - In-path device Intercepts & distributes requests
    - Servers generally local to load balancing device
- DNS-based
  - DNS server returns different IP addresses for server for each lookup with a short Time To Live
    - Servers can be located anywhere


Internet
Clients

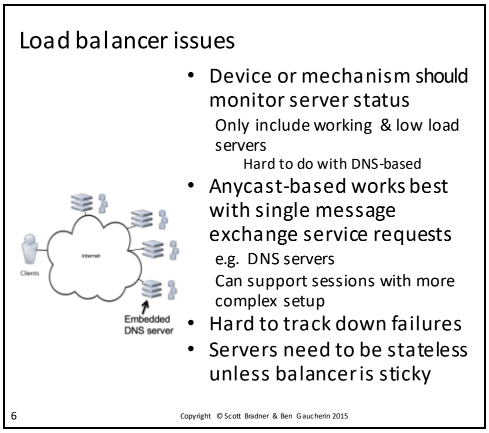
Load balancer types, contd.

- Anycast-based
  - Server uses anycast address – request sent to topologically closest server
    - Servers can be located anywhere


Internet
Clients

Why use a load balancer?

- Distribute processing load among servers
- Bypass failed server
- Eliminate need for explicit disaster relief backup server
  - If servers geographically diverse


Internet
Clients
Embedded DNS server

Load balancer issues

- Device or mechanism should monitor server status
  - Only include working & low load servers
    - Hard to do with DNS-based
- Anycast-based works best with single message exchange service requests
  - e.g. DNS servers
  - Can support sessions with more complex setup
- Hard to track down failures
- Servers need to be stateless unless balancer is sticky

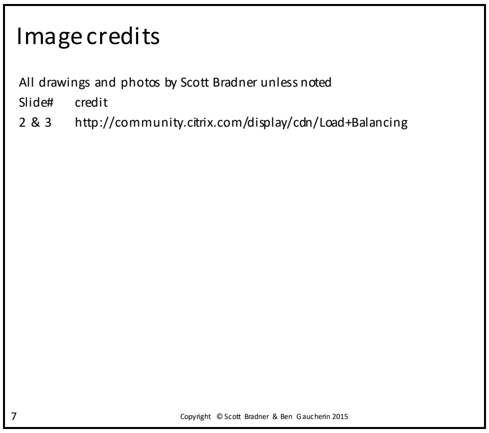


Image credits

All drawings and photos by Scott Bradner unless noted

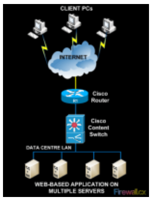
Slide#	credit
2 & 3	http://community.citrix.com/display/cdn/Load+Balancing

IP Network Middleware

Content switches

CSCI E 45a: The Cyber World – part A

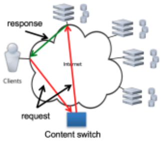
Content Switches



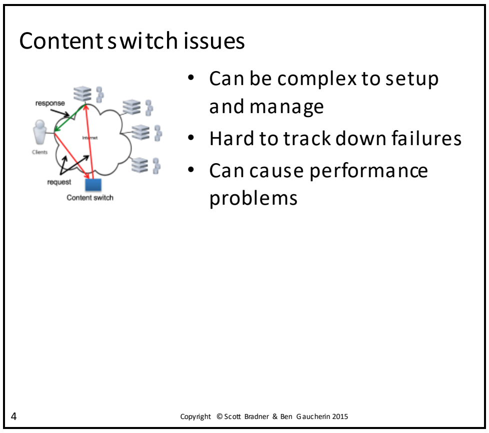
- Load balancer that distributes service requests based on information in the requests

  e.g., send streaming video requests to different server than requests for static graphics

Why use a content switch?



- Use servers optimized for a type of service
- Geography distribute content based on usage
- Can include load balancers


response
Clients
Internet
request
Content switch

Content switch issues

- Can be complex to setup and manage
- Hard to track down failures
- Can cause performance problems

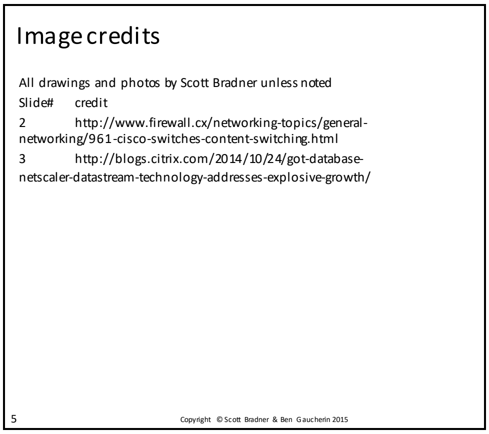


Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	http://www.firewall.cx/networking-topics/general-networking/961-cisco-switches-content-switching.html
3	http://blogs.citrix.com/2014/10/24/got-database-netscaler-datastream-technology-addresses-explosive-growth/

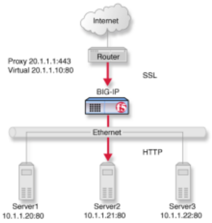
IP Network Middleware

TLS/SSL accelerators

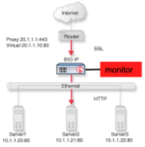
CSCI E 45a: The Cyber World – part A

TLS/SSL accelerators

- In-path device terminates TLS/SSL session in front of web servers

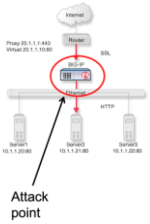


Why use a TLS/SSL accelerator?



- Off loads the processing load and state management
  - Specialized SSL processing hardware
- Centralizes key management
- Enables packet inspection
- Simplifies web server setup and management
  - While preserving secure communications

TLS/SSL accelerator issues



- Traffic unencrypted between accelerator and web server

  Not end-to-end encryption

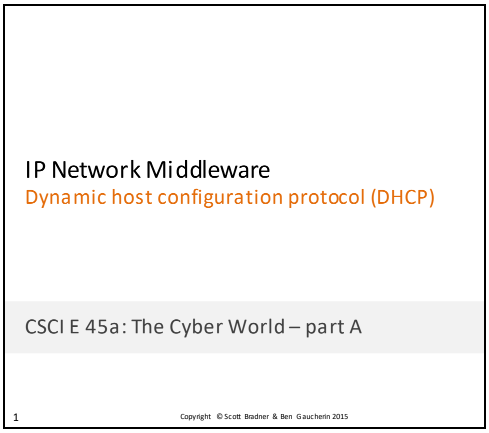
  User cannot tell – both good and bad

- Many SSL keys in one place

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2, 3 & 4	https://support.f5.com/kb/en-us/archived_products/big-ip/manuals/product/bigip4_5admin/bigip_sslgate.html

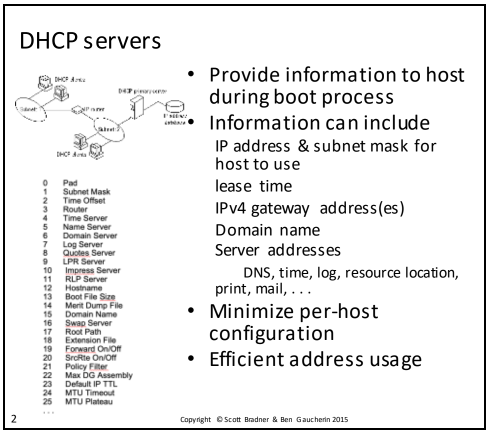


IP Network Middleware

Dynamic host configuration protocol (DHCP)

CSCI E 45a: The Cyber World – part A

1

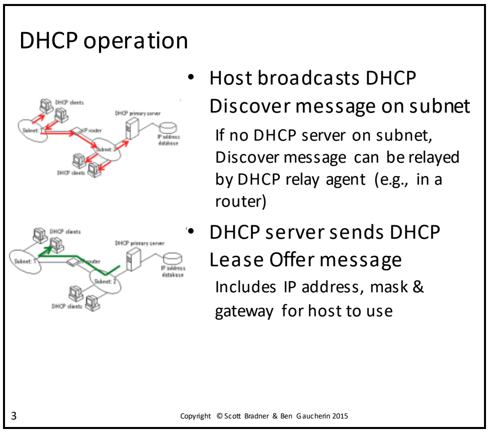


DHCP servers

- Provide information to host during boot process
- Information can include
  IP address & subnet mask for host to use
  lease time
  IPv4 gateway address(es)
  Domain name
  Server addresses
  DNS, time, log, resource location, print, mail, . . .
- Minimize per-host configuration
- Efficient address usage

0	Pad
1	Subnet Mask
2	Time Offset
3	Router
4	Time Server
5	Name Server
6	Domain Server
7	Log Server
8	Quotes Server
9	LPR Server
10	Impress Server
11	RLP Server
12	Hostname
13	Boot File Size
14	Merit Dump File
15	Domain Name
16	Swap Server
17	Root Path
18	Extension File
19	Forward On/Off
20	SrcRte On/Off
21	Policy Filter
22	Max DG Assembly
23	Default IP TTL
24	MTU Timeout
25	MTU Plateau
. . .	

2

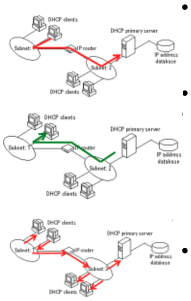


DHCP operation

- Host broadcasts DHCP Discover message on subnet
  If no DHCP server on subnet, Discover message can be relayed by DHCP relay agent (e.g., in a router)
- DHCP server sends DHCP Lease Offer message
  Includes IP address, mask & gateway for host to use

3

DHCP operation, contd.

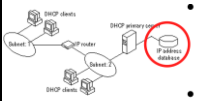


- Host responds with DHCP Request message to indicate accepting address
- DHCP server responds with DHCP ACK message

  Confirms previous offer information

  Can include other configuration information
- Hosts starts to send DHCP Request messages to server when lease has half expired

DHCP, contd.



- DHCP server maintains list of assignments

  With MAC addresses of machines
- Address assignment modes

  Dynamic allocation: assign addresses from a pool of addresses

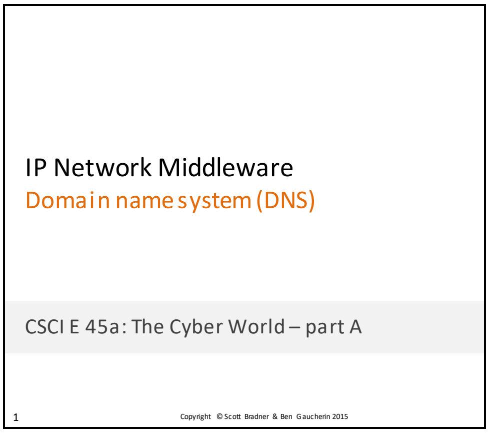
  Can preferentially assign same address based on stored MAC next time host sends discover message

  Static allocation: addresses are assigned to MAC addresses

Image credits

All drawings and photos by Scott Bradner unless noted

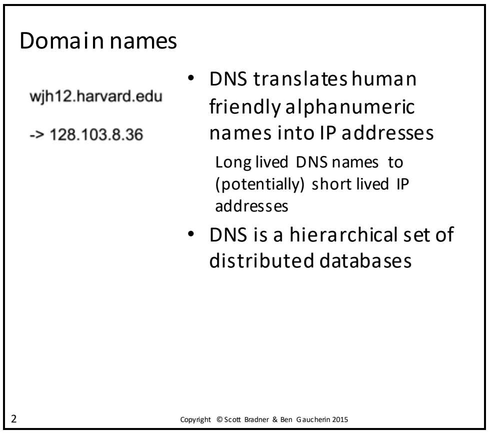
Slide#	credit
2-5	https://www.microsoft.com/resources/documentation/windowsnt/4/server/reskit/en-us/net/sur_dhcp.mspx?mfr=true



IP Network Middleware

Domain name system (DNS)

CSCI E 45a: The Cyber World – part A



Domain names

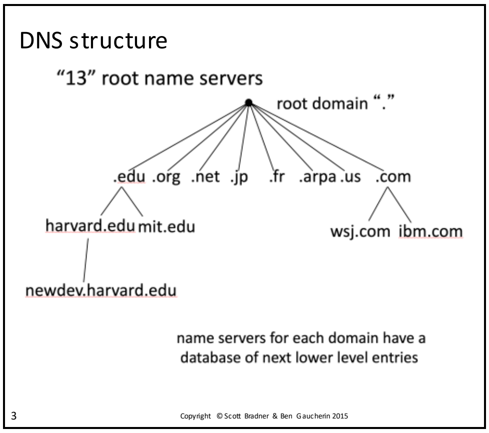
wjh12.harvard.edu

-> 128.103.8.36

- DNS translates human friendly alphanumeric names into IP addresses

  Long lived DNS names to (potentially) short lived IP addresses
- DNS is a hierarchical set of distributed databases

DNS structure

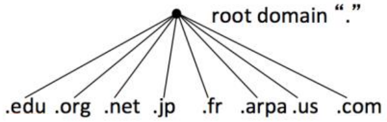


name servers for each domain have a database of next lower level entries

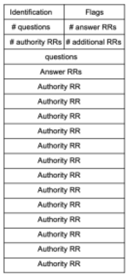
DNS, root servers

- Contents of root name server database is pointers to servers for “top level domains” - e.g., .com

  Database maintained by ICANN



Root servers



Identification	Flags
# questions	# answer RRs
# authority RRs	# additional RRs
questions	
Answer RRs	
Authority RR	
Authority RR	
Authority RR	
Authority RR	
Authority RR	
Authority RR	
Authority RR	
Authority RR	
Authority RR	
Authority RR	
Authority RR	
Authority RR	
Authority RR	

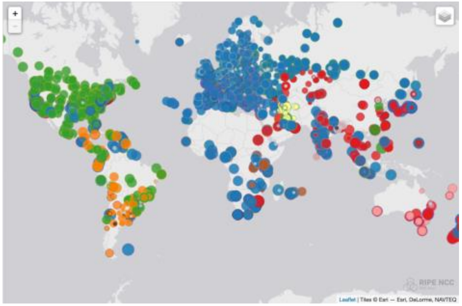
Max packet size = 512 bytes

- Only space in DNS packet for 13 IP addresses of root name servers

  But single IP address can be shared by many servers using “anycast”
- Servers named a-m

  E.g., a.root-servers.net

Root server instances for K root



August 2021

DNS server

- Contains database of local domain hosts

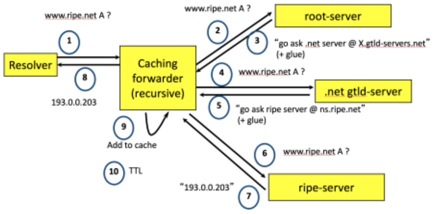
Zone file:

```
ns2      IN    A       173.166.5.68
ns2      IN    HINFO   "Mac Mini" "OSX"
ns2      IN    MX      0 sobco.sobco.com.
www      IN    CNAME   ns2
```

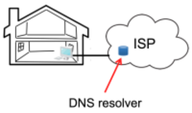
hostname Internet

A = IPv4 address
AAAA = IPv6 address
HINFO = host info
CNAME = alias
MX = mail handler
. . .

DNS, resolving

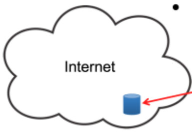


DNS configuration



- Residential
  Normally point to ISP DNS resolver
  Home gateway provides resolver address via DHCP
  ISP can watch (and maybe control) your lookups
- I run my own resolver

DNS configuration, contd.



- Enterprise

  Normally enterprise runs a resolver for its users

- Public

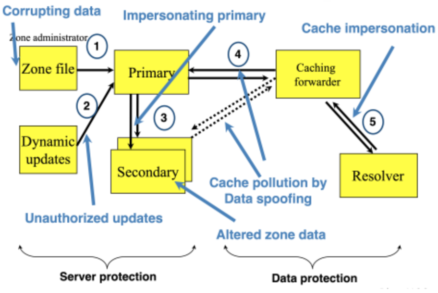
  Some public resolvers available

  e.g.,
  Google 8.8.8.8,
  Level3 209.244.0.3,
  SafeDNS 195.46.39.39,
  Hurricane Electric 74.82.42.42
  Cloudflare 1.1.1.1

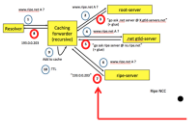
  claims to not monitor queries

DNS vulnerabilities

UPDATED



DNS security (DNSSEC)



- Domain Name System Security Extension

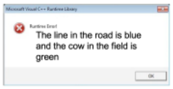
  First version 1999, updated in 2005

- Adds digital signatures to DNS responses

  Assumes a chain of trust up to root zone

- Host can be sure information not spoofed

DNSSEC, issues



The line in the road is blue and the cow in the field is green

Can the U.S. turn off the Internet? What could the rest of the world do about it?

- What to tell user when signature does not verify?
- Is DNSSEC a control point?

DNS, issues

ICANN

®

麦斯贝.com

bing

Google

- TLDs – how many and who operates

  ICANN authorized nearly 1,000 more TLDs
- Trademarks

  No geography on the Internet
- Internationalization

  People using their native language
- Impact of search engines

  Will people stop using domain names?

Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

6 https://labs.ripe.net/Members/emileaben/dns-root-server-transparency

9 house: http://cliparts.co/clipart-of-house

computer: http://www.computerclipart.com/computer_clipart_images/a_flat_screen_computer_monitor_with_a_mouse_0071-0908-1917-3056.html

13 domain name http://texyt.com/MySpace+loses+China+domain+names+060

IP Network Middleware

Service discovery

CSCI E 45a: The Cyber World – part A

Service Discovery

Office Products Division

The Clearinghouse: A Decentralized Agent for Locating Named Objects in a Distributed Environment

by Derek C. Oppen and Yogen K. Dalal

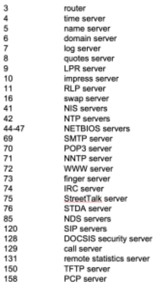
XEROX

- Find services on a network without having to configure the host
- Xerox Clearinghouse (1981) early example

  Services registered with distributed service database

  Hosts queried databases to find services

DHCP



3	router
4	time server
5	name server
6	domain server
7	log server
8	quotes server
9	LPR server
10	impress server
11	RLP server
16	swap server
41	NIS servers
42	NTP servers
44-47	NETBIOS servers
69	SMTP server
70	POP3 server
71	NNTP server
72	WWW server
73	finger server
74	IRC server
75	StreetTalk server
76	STDA server
85	NDS servers
120	SIP servers
128	DOCSIS security server
129	call server
131	remote statistics server
150	TFTP server
158	PCP server

- Provides server addresses at boot time
- Also provides configuration information

  See topic on DHCP

Service Discovery, contd.

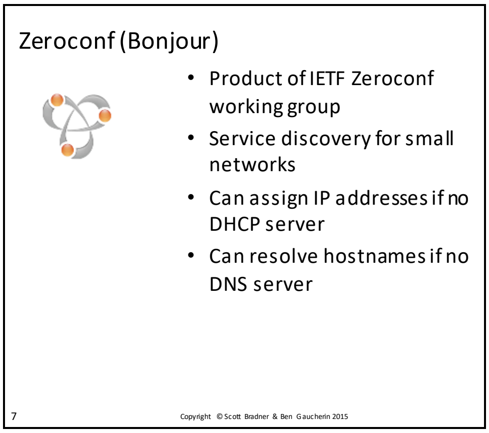
- Multiple current server-less systems
  - Universal Plug and Play (UPnP)
  - Zeroconf (Bonjour)
  - Jini

Universal Plug and Play (UPnP)

- Product of UPnP Forum
- HTTP-based service discovery for small networks
- Can assign IP addresses if no DHCP server

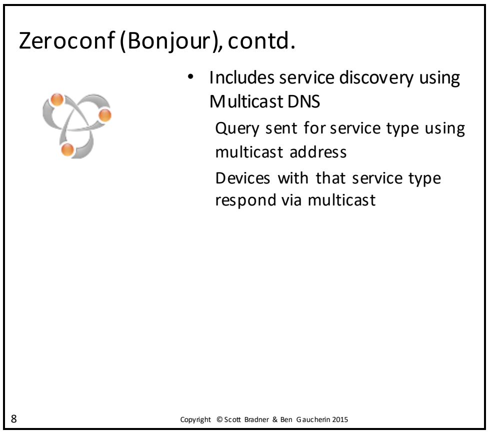
UPnP, contd.

- Includes Simple Service Discovery Protocol (SSDP)
  - “Devices” advertise themselves periodically
    - With URLs for service description, eventing & control
      - Eventing = sending/receiving notices on state changes
  - Devices can also be searched for by “controllers”
  - Uses site-local multicast address
  - Controller can then command device



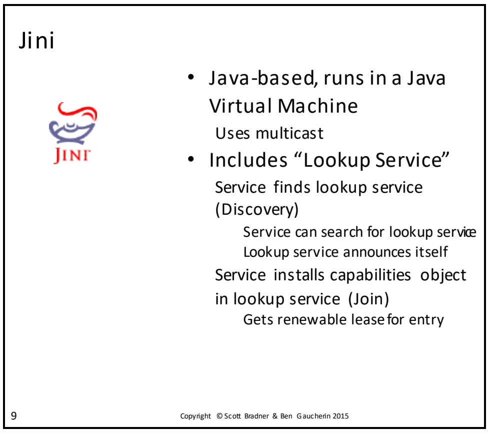
Zeroconf (Bonjour)

- Product of IETF Zeroconf working group
- Service discovery for small networks
- Can assign IP addresses if no DHCP server
- Can resolve hostnames if no DNS server



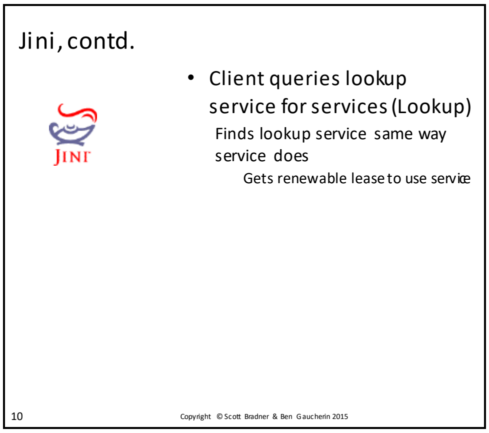
Zeroconf (Bonjour), contd.

- Includes service discovery using Multicast DNS
  - Query sent for service type using multicast address
  - Devices with that service type respond via multicast



Jini

- Java-based, runs in a Java Virtual Machine
  - Uses multicast
- Includes "Lookup Service"
  - Service finds lookup service (Discovery)
    - Service can search for lookup service
    - Lookup service announces itself
  - Service installs capabilities object in lookup service (Join)
    - Gets renewable lease for entry



Jini, contd.

- Client queries lookup service for services (Lookup)
  - Finds lookup service same way service does
    - Gets renewable lease to use service

10

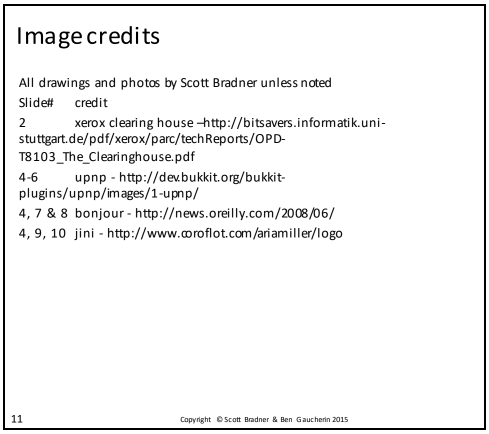
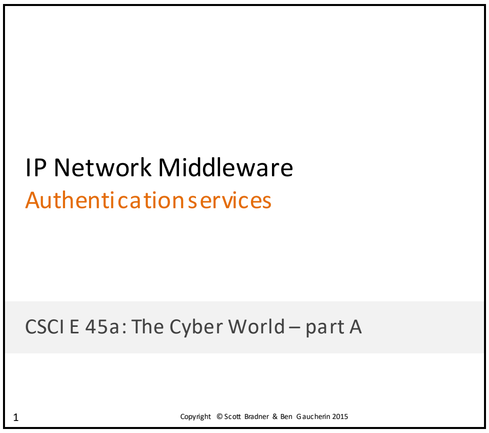


Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	xerox clearing house –http://bitsavers.informatik.uni-stuttgart.de/pdf/xerox/parc/techReports/OPD-T8103_The_Clearinghouse.pdf
4-6	upnp - http://dev.bukkit.org/bukkit-plugins/upnp/images/1-upnp/
4, 7 & 8	bonjour - http://news.oreilly.com/2008/06/
4, 9, 10	jini - http://www.coroflot.com/ariamiller/logo

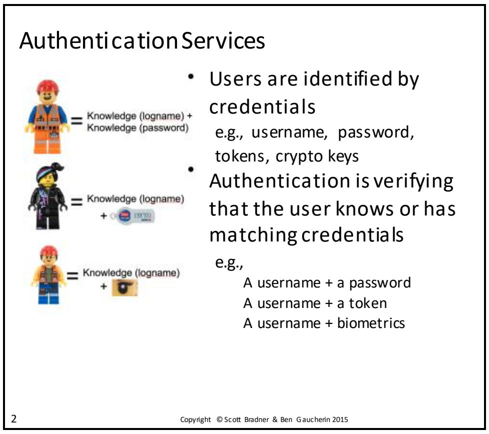
11



IP Network Middleware

Authentication services

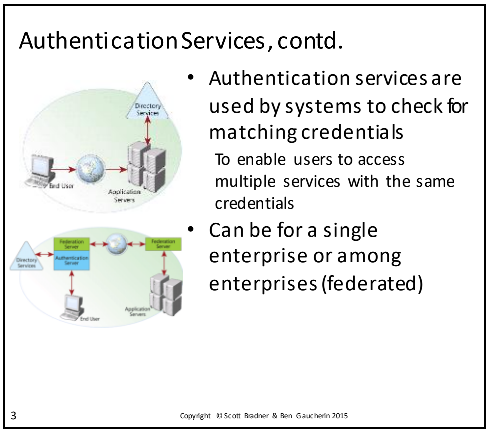
CSCI E 45a: The Cyber World – part A



Authentication Services

= Knowledge (logname) + Knowledge (password)
= Knowledge (logname) +
= Knowledge (logname) +

- Users are identified by credentials
  e.g., username, password, tokens, crypto keys
- Authentication is verifying that the user knows or has matching credentials
  e.g.,
  A username + a password
  A username + a token
  A username + biometrics



Authentication Services, contd.

- Authentication services are used by systems to check for matching credentials
  To enable users to access multiple services with the same credentials
- Can be for a single enterprise or among enterprises (federated)

Authentication, Single System

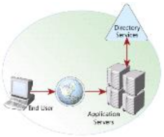
- Standalone systems do their own authentication
- E.g., prompt user for username & password and check against local password file

Single user systems sometimes use just a password – e.g. smartphone

- Can also use biometrics

e.g. fingerprint

Authentication, Single Sign-on



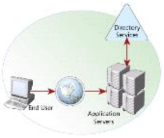
- Multiple systems can use a single authentication server
- Avoids servers having to manage their own authentication

Reduces the number of passwords user must remember

Reduces the places that the passwords are stored

But increases impact if credentials are compromised

Authentication, Single Sign-on



- Can provide “single sign-on”

Logon once and use multiple services

But some services might want reauthentication for security reasons

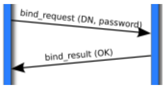
- E.g., LDAP, Microsoft Active Directory, CAS

Lightweight Directory Access Protocol: LDAP

- IETF standard
  - Lightweight version of OSI X.500
- Structured directory
  - Collection of entries
    - each with a Distinguished Name (DN)
    - Many other person attributes, e.g.,
      - cn = common name, sn = surname, mail = email address
    - User's credentials

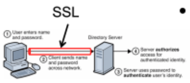
```
dn: cn=John Smith, ou=people, dc=example,
dc=com objectclass: inetOrgPerson
cn: John Smith
cn: John J Smith
sn: Smith
uid: jsmith
userpassword: !%@^%&&!#&*&(
carlicense: HISCAR 124
homephone: 555-111-2223
mail: j.smith@example.com
mail: jsmith@example.com
mail: john.smith@example.com
ou: Sales
```

LDAP, contd.



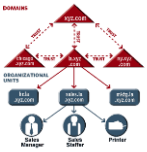
- Service can collect user's credentials & test against LDAP server (bind)
  - Successful bind means user was authenticated

LDAP issues


SSL
① User enters name and password.
Directory Server
② Client sends name and password across network.
③ Server uses password to authenticate user's identity.
④ Server authorizes access for authenticated identity.

- User's credentials collected by service
  - Thus, service must be trusted
- LDAP information (including credentials) sent in plaintext
  - Thus, need to run though SSL
    - Sometimes hard to ensure this is the case
- Brute force bind testing
  - Best to limit access to known servers
  - Should not be open to Internet

Microsoft Active Directory (AD)



- Basic Windows access control and user information function

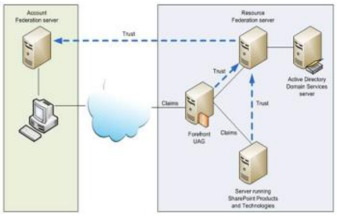
  Includes information on accounts & resources

  e.g., user accounts & printers
- Information storage in a LDAP directory
- Application enabler
- Directory format: modified X.500

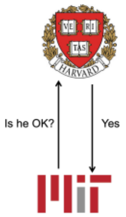
Microsoft AD, contd.

- Can be organized in a federation

  By establishing trust relationships



Authentication, Federation



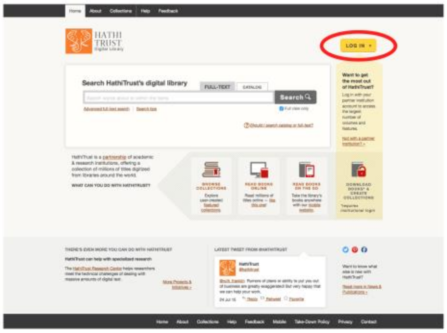
- Organizations relying on other organizations to authenticate users

  e.g., MIT accepting an assurance from Harvard that you are taking a Harvard Extension School class

Federation, contd.

- High level process:
  - User attempts to log into an application
  - User asked "where are you from"
  - User redirected to Identity Provider (IdP) at home institution where they enters their credentials
  - User redirected back to application as authenticated
    - IdP can also send information about user (e.g. name)

Hathi Trust: start



Search HathiTrust's digital library

Want to get the most out of HathiTrust? Log in with your partner institution account to access the largest number of volumes and features.

Not with a partner institution?

HathiTrust is a partnership of academic & research institutions, offering a collection of millions of titles digitized from libraries around the world.

WHAT CAN YOU DO WITH HATHITRUST?

Explore user-created featured collections.

*requires institutional login

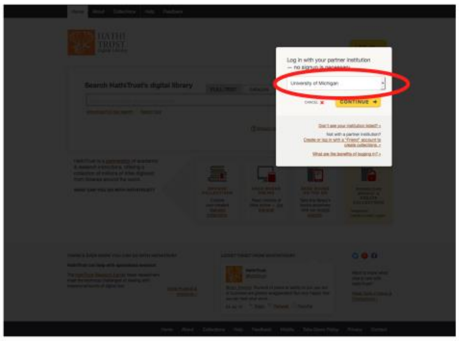
THERE'S EVEN MORE YOU CAN DO WITH HATHITRUST

HathiTrust can help with specialized research

LATEST TWEET FROM @HATHITRUST

Want to know what else is new with HathiTrust?

Hathi Trust: login



Log in with your partner institution — no signup is necessary

University of Michigan

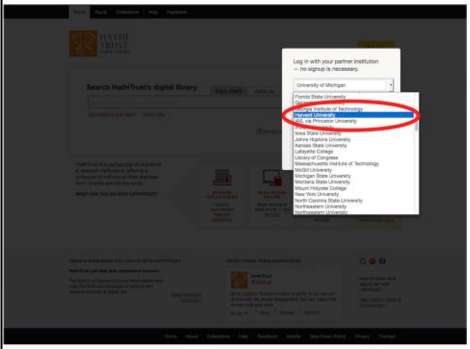
Don't see your institution listed?

Not with a partner institution?

Create or log in with a "Friend" account to create collections.

What are the benefits of logging in?

Hathi Trust: where are you from?

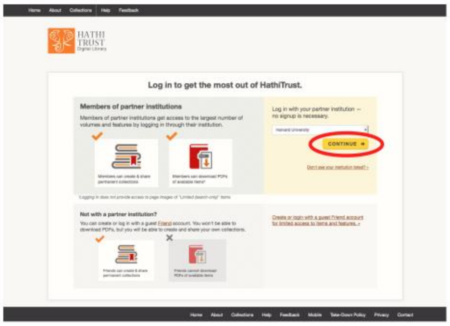


Log in with your partner institution — no signup is necessary.

University of Michigan

- Florida State University
- Georg[illegible]
- Georgia Institute of Technology
- Harvard University
- IAS, via Princeton University
- [illegible]
- Iowa State University
- Johns Hopkins University
- Kansas State University
- Lafayette College
- Library of Congress
- Massachusetts Institute of Technology
- McGill University
- Michigan State University
- Montana State University
- Mount Holyoke College
- New York University
- North Carolina State University
- Northeastern University
- Northwestern University

Hathi Trust: selected institution



Log in to get the most out of HathiTrust.

Members of partner institutions

Members of partner institutions get access to the largest number of volumes and features by logging in through their institution.

✓ Members can create & share permanent collections

✓ Members can download PDFs of available items*

Log in with your partner institution — no signup is necessary.

Harvard University

CONTINUE →

Don't see your institution listed? ›

*Logging in does not provide access to page images of "Limited (search-only)" items

Not with a partner institution?

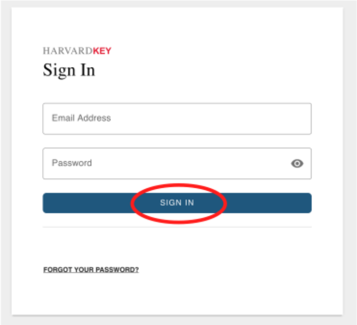
You can create or log in with a guest Friend account. You won't be able to download PDFs, but you will be able to create and share your own collections.

✓ Friends can create & share permanent collections

✕ Friends cannot download PDFs of available items

Create or login with a guest Friend account for limited access to items and features. ›

Hathi Trust: Harvard Key system



HARVARDKEY

Sign In

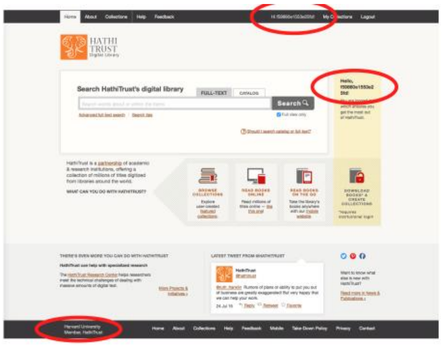
Email Address

Password

SIGN IN

FORGOT YOUR PASSWORD?

Hathi Trust: logged in



Search HathiTrust's digital library

Should I search catalog or full text?

Hello, f50660e1553e2

HathiTrust is a partnership of academic & research institutions, offering a collection of millions of titles digitized from libraries around the world.

WHAT CAN YOU DO WITH HATHITRUST?

BROWSE COLLECTIONS Explore user-created featured collections.

READ BOOKS ONLINE Read millions of titles online — like this one!

READ BOOKS ON THE GO Take the library's books anywhere with our mobile website.

DOWNLOAD BOOKS* & CREATE COLLECTIONS *requires institutional login

THERE'S EVEN MORE YOU CAN DO WITH HATHITRUST

HathiTrust can help with specialized research

The HathiTrust Research Center helps researchers meet the technical challenges of dealing with massive amounts of digital text.

More Projects & Initiatives ›

LATEST TWEET FROM @HATHITRUST

HathiTrust @hathitrust

@ruth_harwin Rumors of plans or ability to put you out of business are greatly exaggerated! But very happy that we can help your work.

24 Jul 15 Reply Retweet Favorite

Want to know what else is new with HathiTrust? Read more in News & Publications ›

Federated authentication

- Programs
  - Internet2's InCommon
  - National Strategy for Trusted Identities in Cyberspace
  - Commercial (Facebook, Twitter, Google+, etc.)
- Technologies
  - Shibboleth (InCommon)
  - OpenID (Google, Yahoo, etc.)
  - OAuth (IETF, Twitter, etc.)
  - Facebook

Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

2 emmet - http://lego.wikia.com/wiki/Emmet

wildstyle http://lego.wikia.com/wiki/Wyldstyle

gail http://lego.wikia.com/wiki/Gail_the_Construction_Worker

3 https://msdn.microsoft.com/en-us/library/aa479069.aspx

3 http://pamungkaswave.blogspot.com/

4 mac http://inwallspeakers1.com/older-apple-desktop-computer/

iphone - http://1hqwallpaper.mobi/iphone-5s-lock-screen-fingerprint-wallpapers.html

8 https://wiki.alfresco.com/wiki/Alfresco_Authentication_Subsystems

9 http://docs.oracle.com/cd/E19528-01/819-0997/gdzdj/index.html

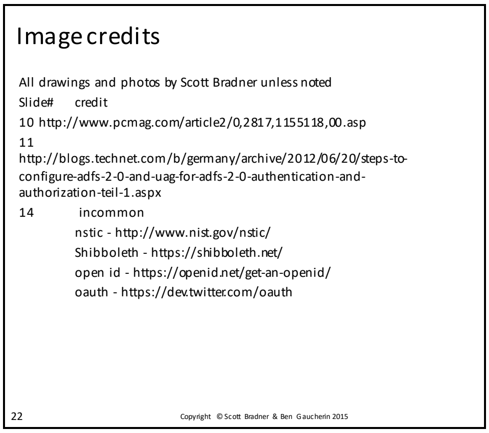


Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

10 http://www.pcmag.com/article2/0,2817,1155118,00.asp

11 http://blogs.technet.com/b/germany/archive/2012/06/20/steps-to-configure-adfs-2-0-and-uag-for-adfs-2-0-authentication-and-authorization-teil-1.aspx

14 incommon

nstic - http://www.nist.gov/nstic/

Shibboleth - https://shibboleth.net/

open id - https://openid.net/get-an-openid/

oauth - https://dev.twitter.com/oauth

22

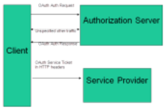
Copyright © Scott Bradner & Ben Gaucherin 2015

IP Network Middleware

Authorization services

CSCI E 45a: The Cyber World – part A

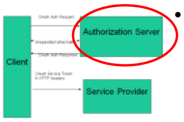
Authorization Services

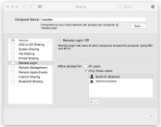


I know this is Bill, but what is Bill permitted to do?

- Authentication says who you are
- Authorization says what you can do – e.g.,
  - What applications you can run
  - What information you can see
  - What information you can modify
- Authorization can be:
  - Configured
  - Attribute-based
  - Group-based

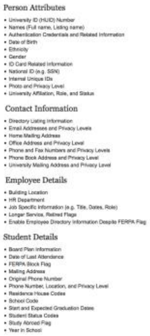
Authorization Services, contd.





- Authorization services can provide information for local authorization or can do the authorization itself
  - i.e., put business logic in a central server or keep it in application server
- Configured authorization
  - Manually maintained authorization list

Attribute-based authorization



Person Attributes

- University ID (HUID) Number
- Names (Full name, Listing name)
- Authentication Credentials and Related Information
- Date of Birth
- Ethnicity
- Gender
- ID Card Related Information
- National ID (e.g. SSN)
- Internal Unique IDs
- Photo and Privacy Level
- University Affiliation, Role, and Status

Contact Information

- Directory Listing Information
- Email Addresses and Privacy Levels
- Home Mailing Address
- Office Address and Privacy Level
- Phone and Fax Numbers and Privacy Levels
- Phone Book Address and Privacy Level
- University Mailing Address and Privacy Level

Employee Details

- Building Location
- HR Department
- Job Specific Information (e.g. Title, Dates, Role)
- Longer Service, Retired Flags
- Enable Employee Directory Information Despite FERPA Flag

Student Details

- Board Plan Information
- Date of Last Attendance
- FERPA Block Flag
- Mailing Address
- Original Phone Number
- Phone Number, Location, and Privacy Level
- Residence House Codes
- School Code
- Start and Expected Graduation Dates
- Student Status Codes
- Study Abroad Flag
- Year in School

- Server evaluates user attributes to determine authorization
  - e.g., Employee information i.e., "roles" (full time, part time, ...)
  - Student information (year, graduate school, classes, ...
  - Location
  - . . .
- Attributes can come from authentication system or from database (e.g. LDAP server)

Group-based authorization

- Central server users configuration and attributes to assign users to groups
  - Same user can be in many groups
- Local server bases authorization on group membership
  - E.g., Internet 2 Grouper

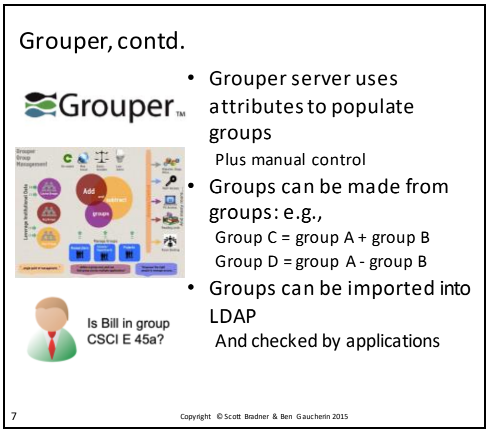
Grouper™

Internet 2 Grouper

Grouper™

Group A =
(
{people determined by attributes}
- {people to be excluded}
+ {people to be included}
)

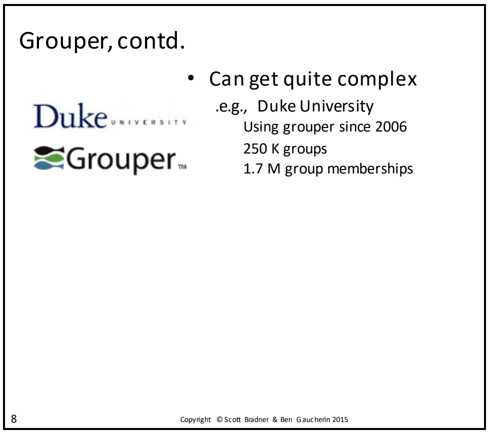
- A Group defined by:
  - List of list of attribute/values that mean user could be in a group
  - List of specific users to include
  - List of specific users to exclude



Grouper, contd.

- Grouper server uses attributes to populate groups
  - Plus manual control
- Groups can be made from groups: e.g.,
  - Group C = group A + group B
  - Group D = group A - group B
- Groups can be imported into LDAP
  - And checked by applications

7



Grouper, contd.

- Can get quite complex
  - .e.g., Duke University
    - Using grouper since 2006
    - 250 K groups
    - 1.7 M group memberships

8

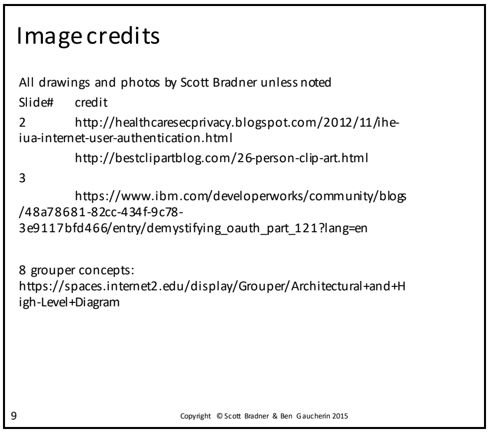


Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

2 http://healthcaresecprivacy.blogspot.com/2012/11/ihe-iua-internet-user-authentication.html

http://bestclipartblog.com/26-person-clip-art.html

3

https://www.ibm.com/developerworks/community/blogs/48a78681-82cc-434f-9c78-3e9117bfd466/entry/demystifying_oauth_part_121?lang=en

8 grouper concepts: https://spaces.internet2.edu/display/Grouper/Architectural+and+High-Level+Diagram

9

IP Network Middleware

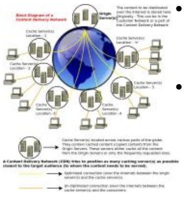
Content distribution network (CDN)

CSCI E 45a: The Cyber World – part A

Content Distribution Network: CDN

- Vendor-run network of caching servers
- Servers geographically distributed
  - Load distributed to multiple servers
- Users are directed to CDN servers to obtain content
  - Directed by content owner
    - e.g. by rewritten URL or DNS entry
  - Usually involve being directed to "the closest" or "a near by" server with the specific content
    - E.g., using anycast

CDN, contd.


Block Diagram of a Content Delivery Network
Origin Server(s)
The content to be distributed over the Internet is stored here Originally - This can be in the Customer Network or a part of the Content Delivery Network
Cache Server(s) Location - 1
Cache Server(s) Location - 2
Cache Server(s) Location - 'n'
Cache Server(s) Location - 5
Cache Server(s) Location - 4
Cache Server(s) Location - 3
Cache Server(s) located across various parts of the globe. They contain cached content (copied content) from the Origin Servers. These servers either cache all the content from the Origin Servers or only the frequently requested ones.
A Content Delivery Network (CDN) tries to position as many caching server(s) as possible closest to the target audience (to whom the content needs to be served).
Optimized connection (over the internet) between the origin server(s) and the cache server(s)
Un-Optimized connection (over the internet) between the cache server(s) and the consumers.

- Content pre-loaded into servers or loaded on first user request
- Multiple content owners can buy service from same CDN
  - Some companies run their own CDN using their own backbone fiber network

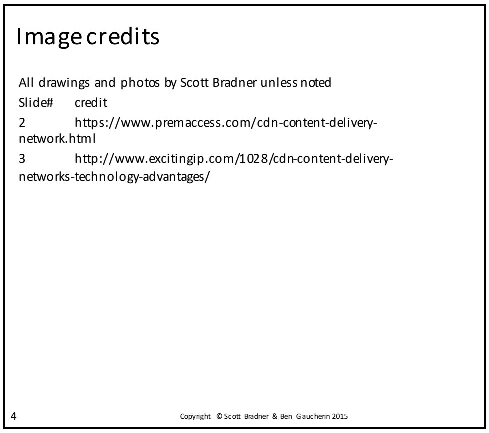


Image credits

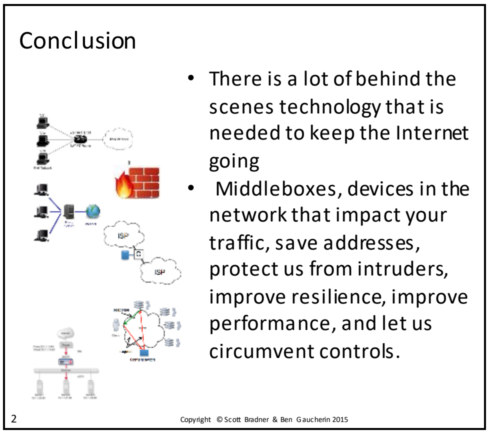
All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	https://www.premaccess.com/cdn-content-delivery-network.html
3	http://www.excitingip.com/1028/cdn-content-delivery-networks-technology-advantages/

IP Network Middleware

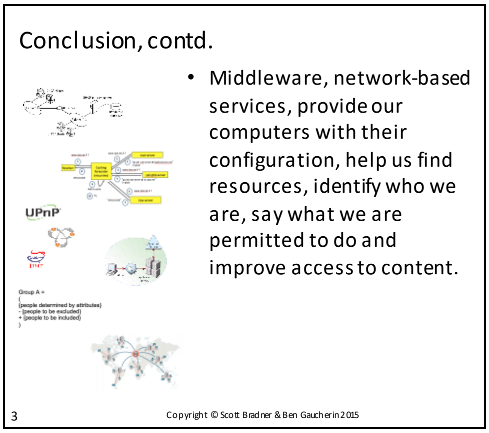
Conclusion

CSCI E 45a: The Cyber World – part A



Conclusion

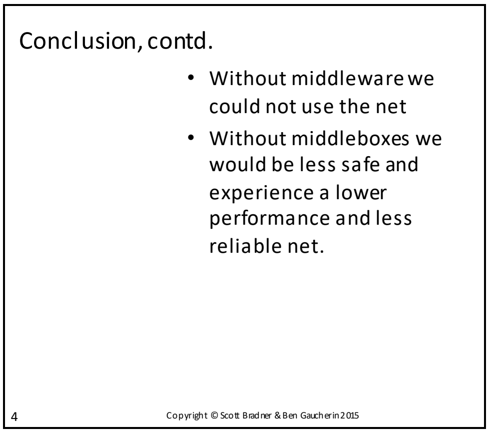
- There is a lot of behind the scenes technology that is needed to keep the Internet going
- Middleboxes, devices in the network that impact your traffic, save addresses, protect us from intruders, improve resilience, improve performance, and let us circumvent controls.



UPnP
Group A =
(
[people determined by attributes]
- [people to be excluded]
+ [people to be included]
)

Conclusion, contd.

- Middleware, network-based services, provide our computers with their configuration, help us find resources, identify who we are, say what we are permitted to do and improve access to content.



Conclusion, contd.

- Without middleware we could not use the net
- Without middleboxes we would be less safe and experience a lower performance and less reliable net.

4 Copyright © Scott Bradner & Ben Gaucherin 2015

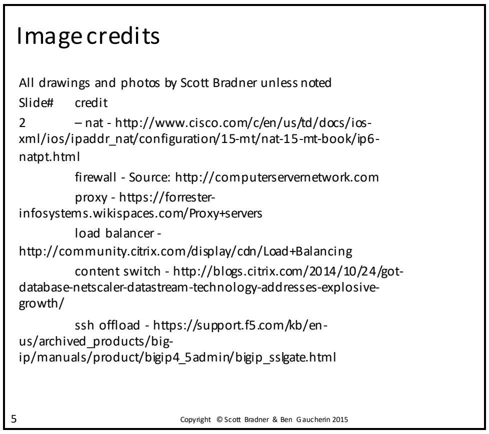


Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

2 – nat - http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/ip6-natpt.html

firewall - Source: http://computerservernetwork.com

proxy - https://forrester-infosystems.wikispaces.com/Proxy+servers

load balancer - http://community.citrix.com/display/cdn/Load+Balancing

content switch - http://blogs.citrix.com/2014/10/24/got-database-netscaler-datastream-technology-addresses-explosive-growth/

ssh offload - https://support.f5.com/kb/en-us/archived_products/big-ip/manuals/product/bigip4_5admin/bigip_sslgate.html

5 Copyright © Scott Bradner & Ben Gaucherin 2015

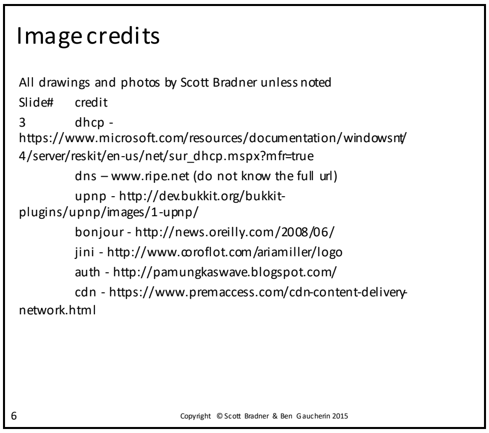


Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

3 dhcp - https://www.microsoft.com/resources/documentation/windowsnt/4/server/reskit/en-us/net/sur_dhcp.mspx?mfr=true

dns – www.ripe.net (do not know the full url)

upnp - http://dev.bukkit.org/bukkit-plugins/upnp/images/1-upnp/

bonjour - http://news.oreilly.com/2008/06/

jini - http://www.coroflot.com/ariamiller/logo

auth - http://pamungkaswave.blogspot.com/

cdn - https://www.premaccess.com/cdn-content-delivery-network.html

6 Copyright © Scott Bradner & Ben Gaucherin 2015