

The Internet

Part 2: Networks of Networks - Internet Workings

Notes for CSC 100 - The Beauty and Joy of Computing
The University of North Carolina at Greensboro

Reminders

Reminders for Nov. 6

Blown to Bits - Chapter 5 Reading Reflection

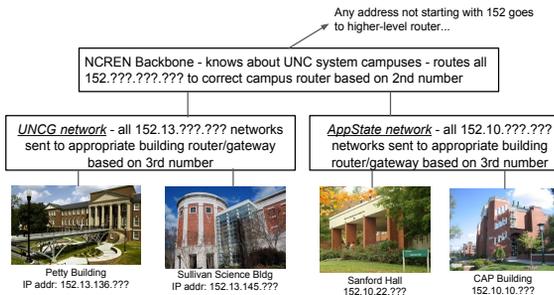
Due next Tuesday (Nov. 12) at 10:00am

Project

- Will get quick feedback on proposals - read it!
- Should be working on coding (assistance in Lab on Friday)
- Progress report due next Friday (Nov. 15)

Internet Protocol

Routing: Simplified



Routing

Introduction to Routing Tables

Example routing table (most of yours look like this):

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
152.13.136.0	0.0.0.0	255.255.255.0	U	2	0	0	eth0
0.0.0.0	152.13.136.1	0.0.0.0	UG	0	0	0	eth0

Routing

Introduction to Routing Tables

Example routing table (most of yours look like this):

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
152.13.136.0	0.0.0.0	255.255.255.0	U	2	0	0	eth0
0.0.0.0	152.13.136.1	0.0.0.0	UG	0	0	0	eth0

These are the most important things to understand

Your destination (who you want to send to) is matched against these specifications

1. Consider everything in binary
2. Everywhere there's a "1" bit in the "Genmask" (also called a netmask) must match "Destination"
3. Where there are 0's in the "Genmask" it doesn't matter if it matches or not.

Everybody's first question: Do I really have to convert everything to binary to understand this???

Answer: Usually not - the "Genmask" typically only uses a few values, mostly "0" and "255"

- "0" for an octet means you don't care about this octet
- "255" for an octet means the whole octet must match

So... 152.13.136.0/255.255.255.0 matches any address that starts with 152.13.136

- Matches 152.13.136.12, 152.13.136.19, 152.13.136.252, ...

Routing

Introduction to Routing Tables

Example routing table (most of yours look like this):

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
152.13.136.0	0.0.0.0	255.255.255.0	U	2	0	0	eth0
0.0.0.0	152.13.136.1	0.0.0.0	UG	0	0	0	eth0

If Destination/Genmask matches, this tells us what to do

Example 1: Sending to 152.13.136.53 - matches first line in routing table

There is no "intermediate host" specified as a "gateway" and communication happens over interface "eth0"

So... Use the ARP protocol to find that host via "eth0", and send using the resulting MAC address

Routing

Introduction to Routing Tables

Example routing table (most of yours look like this):

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
152.13.136.0	0.0.0.0	255.255.255.0	U	2	0	0	eth0
0.0.0.0	152.13.136.1	0.0.0.0	UG	0	0	0	eth0

Does not match!

Example 2: Send to 152.13.15.23

Routing

Introduction to Routing Tables

Example routing table (most of yours look like this):

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
152.13.136.0	0.0.0.0	255.255.255.0	U	2	0	0	eth0
0.0.0.0	152.13.136.1	0.0.0.0	UG	0	0	0	eth0

Does match! (0.0.0.0/0.0.0.0 matches everything - called the "default route")

Example 2: Send to 152.13.15.23

Routing

Introduction to Routing Tables

Example routing table (most of yours look like this):

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
152.13.136.0	0.0.0.0	255.255.255.0	U	2	0	0	eth0
0.0.0.0	152.13.136.1	0.0.0.0	UG	0	0	0	eth0

This is what you do...

Example 2: Send to 152.13.15.23

This time a gateway is defined - we send to 152.13.15.23 by sending through 152.13.136.1

152.13.136.1 is connected on interface eth0

So use ARP on eth0 to find MAC address, but of the gateway (152.13.136.1) not the destination!

Packet goes to 152.13.136.1, addressed to 152.13.15.23 - now it's not your problem any more

Trust the network!

Internet Protocol

Routing: Simplified - You do it!

In-class activity:

Look for "Activity 2" message on your info sheet

- This should be a local message (how can you tell?)
- Simulate the local protocol (ARP + transmit)

Routing

Sample Gateway Routing Table

More complex routing table (each network has one that looks like this):

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
152.13.136.0	0.0.0.0	255.255.255.0	U	2	0	0	eth0
152.13.10.0	0.0.0.0	255.255.255.0	U	2	0	0	eth1
152.13.145.0	152.13.10.13	255.255.255.0	UG	0	0	0	eth1
0.0.0.0	152.13.10.1	0.0.0.0	UG	0	0	0	eth1

Notes:

- Two different interfaces: "eth0" and "eth1"
- Each one defines an IP prefix for direct connections (152.13.136 and 152.13.10)
- "Helper entry" for 152.13.145 prefix specifies specific gateway for that network
 - *This isn't strictly necessary but can speed things up*
- Default route - anything not matching three given prefixes in 152.13 goes to 152.13.10.1

Internet Protocol

Routing: Simplified - You do it!

In-class activity:

Look for "Activity 3" message on your info sheet

Parts 1, 2, and 3

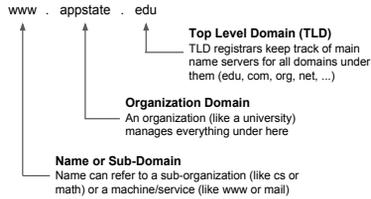
- This message goes between different LANs
- Simulate the protocol (don't forget ARP with your gateway!)

But I know a name, not an address!

Naming on the Internet

I want to connect to a name (e.g., www.appstate.edu) rather than a number

Names are also hierarchical



But I know a name, not an address!

Mapping from a name to an address: DNS

DNS = "Domain Name System"

DNS servers map from names to IP addresses (and vice-versa, sometimes!)

Super-simplified view:

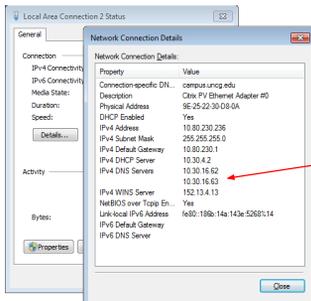
- I know the IP address (not the name!!!) of a DNS server I can use
- I ask it for the IP address of www.appstate.edu
- It returns IP address (152.10.1.83)

View from Unix utility "host":

```
user@host ~ $ host www.appstate.edu
www.appstate.edu has address 152.10.1.83
user@host ~ $
```

But I know a name, not an address!

Locating DNS servers in Windows 7



Note these DNS servers are for IPv4

Sending to a Name

Now you do it!

Activity 4: Only one person has an "Activity 4"

Send "Get..." to `csdept.appstate.edu`.

Let's see how much we can figure out!

Summary of addressing/naming

Solution to Activity 4

Problem: Host at 152.13.136.16 wants to contact `csdept.appstate.edu`

- Need to find IP address of `www.appstate.edu`, so need to locate IP address of DNS server (from my settings) - in our example that's 152.13.10.15
- I need to contact 152.13.10.15 - checking my routing table, that doesn't match my network (line 1) but does match default route - gateway is 152.13.136.1
- I need to communicate with 152.13.136.1 (my gateway), but I need a MAC address, not an IP address! So I send an ARP packet "Who has 152.13.136.1?"
- Gateway responds: "I have 152.13.136.1 at 00:1d:92:97:a2:55"
- I receive this message and store this IP <-> MAC address mapping for later
- I send "To: 152.13.10.15 - DNS query: where is `csdept.appstate.edu`?" to MAC address 00:1d:92:97:a2:55 (and other networks send subsequent ARP/routing to get this to 152.13.10.15)
- I eventually receive a response "`csdept.appstate.edu` has address 152.10.10.45"
- I look at IP address: 152.10.10.45 is not local, so must go through gateway again
- ARP efficiency: we just saw that gateway was at 00:1d:92:97:a2:55, so I can just re-use that (no ARP needed for now - but will eventually "expire")
- I send "To: 152.10.10.45 - Packet for `csdept.appstate.edu`" to 00:1d:92:97:a2:55

Doesn't describe what happens in other networks, and...
Believe it or not, even this description is slightly simplified!

We can send packets, now what?

Packets are small: Typically under 1500 bytes

I want a picture - several hundred thousand bytes
... Now what?

Transport layer:

- UDP: Packet-by-packet communication
- TCP: Packets organized in reliable streams

Application layer examples:

- HTTP: Uses TCP streams to transmit from a web server
- DNS: Domain name service over UDP
- SMTP: Email transmission (server to server) over TCP
- IMAP: Email (server to client) over TCP
- SSH: Encrypted login over TCP
- ...

Where can things go wrong?

Situation: I want to privately access www.bankofamerica.com

What can go wrong?

Where can things go wrong?

Situation: I want to privately access www.bankofamerica.com

What can go wrong?

Issue 1: "privately" - packets are like postcards, with visible contents!
Problem: Any intermediate hop can see everything

Issue 2: Did the DNS lookup give me the correct IP address?
Problem: Can someone plant false records in my DNS server?
Problem: Can someone point me to a rogue DNS server?
Problem: Can someone send back a fake response (UDP is unreliable!)

Issue 3: Did I really connect to the stated IP address?
Problem: Could someone change routing tables to fake me out?
Problem: Could malware change IP address on the fly?

What could a well-funded party with access to Internet backbone do?

Where can things go wrong?

Situation: I want to privately access www.bankofamerica.com

What **Crypto to the rescue!** can go wrong?

Issue 1: "privately" - packets are like postcards, with visible contents!
*Problem: A **Encrypt contents for privacy** anything*

Issue 2: Did the DNS lookup give me the correct IP address?
Problem: Can someone plant false records in my DNS server?
*Problem: **Cryptographic signature for integrity (DNSSEC)** reliable!)*

Issue 3: Did I really connect to the stated IP address?
*Problem: C **Cryptographic signatures for authentic server (using Certificate Authorities) and Message Authentication Codes for content authenticity***

What could a well-funded party with access to Internet backbone do?

Where can things go wrong?

Situation: I want to privately access www.bankofamerica.com

Wh... Crypto to the rescue!

Issue 1: "privately" Problem: A... Contents!

Issue 2: Did the Problem: Can Problem: Q... program... (reliable!)

Issue 3: Did I really connect to... ated IP... ess?

Problem: C... Cryptographic signatures for authentic server (using Certificate Authorities) and Message Authentication Codes for content authenticity

What could a well-funded party with access to Internet backbone do?

Summary

From the two Internet lectures you should understand (at a very basic level):

- LAN communication
- IP communication on a LAN
- Routing between LANs
- Host/domain names and DNS

You should also have a basic appreciation of

- Complexities of modern world-scale networking
- Things that can go wrong, especially when security is important

Reminder/warning: This just barely (starts to) scratch the surface. The goal here is to gain some insight, not make you a network engineer!
