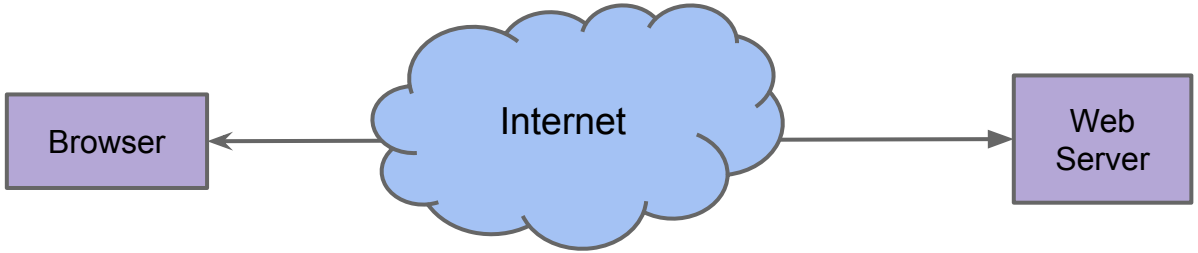
Tor61 Project

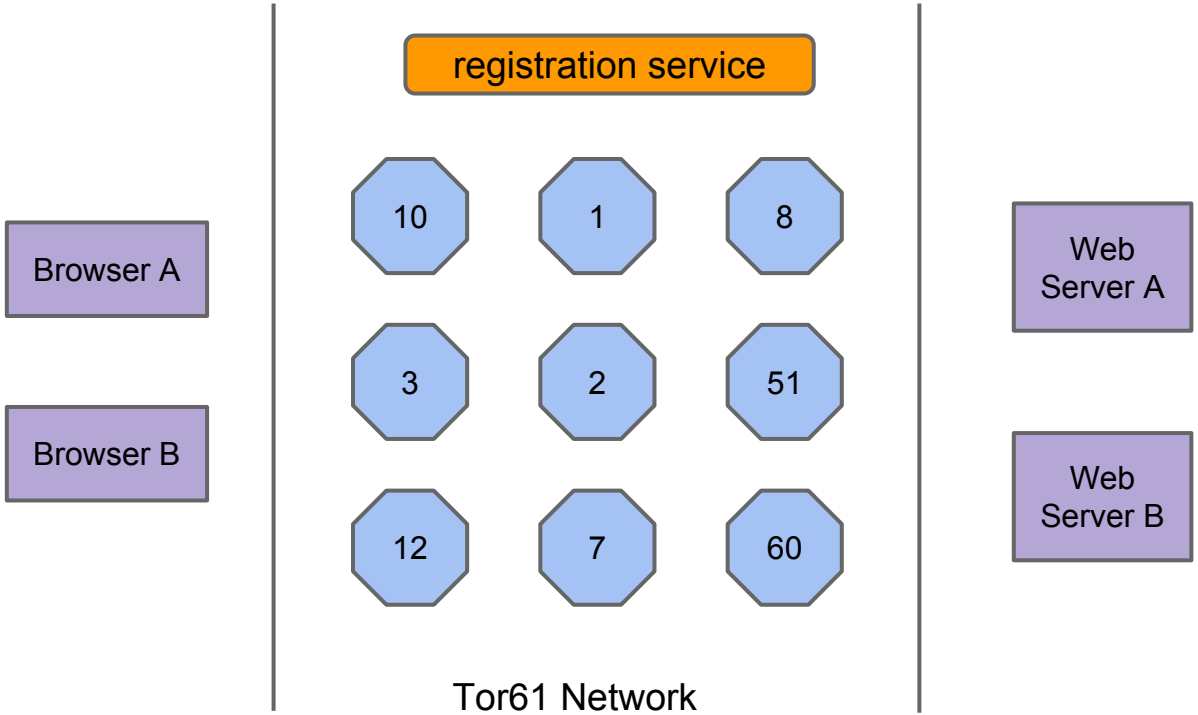
Qiao Zhang
CSE 461 15sp Section 7

Why we would want Tor/Tor61?

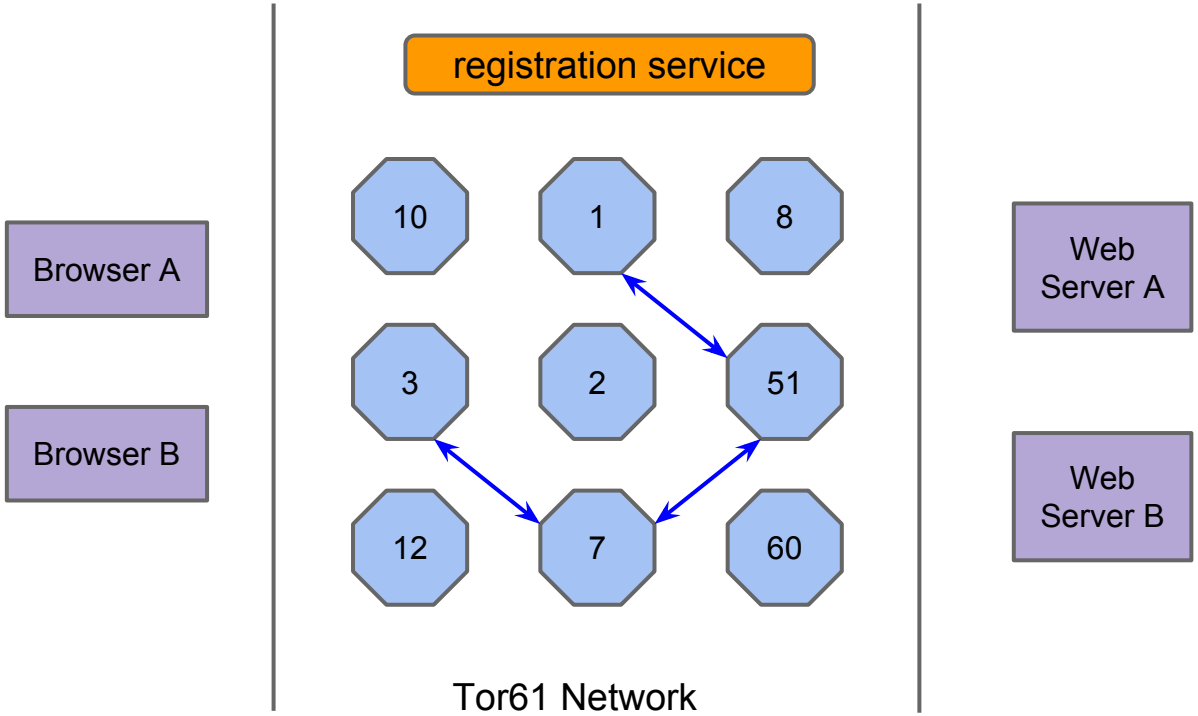


- Packets can be sniffed -- headers reveal src/dest IP
- Encryption of packet payload is not enough!
- Tor allows you to browse the Internet anonymously
- Route your data through a random pathway so that no single node can tell the src/dst of your data
- Good: evade surveillance? Bad: Silk Road?
- Tor61 is a simplified Tor -- no encryption

Tor61 Architecture Overview

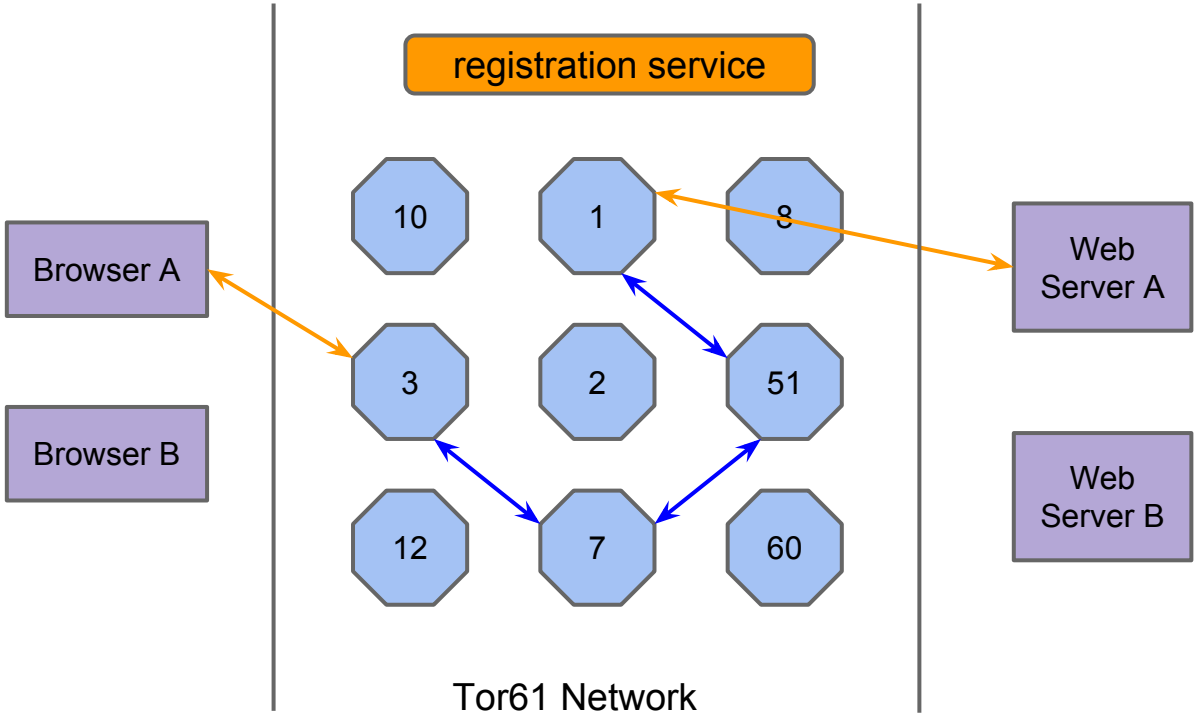


Tor61 Architecture Overview



On startup, each Tor61 node establishes a single **circuit** (blue path) through the network
e.g 3-7-51-1, 10-2-3-7

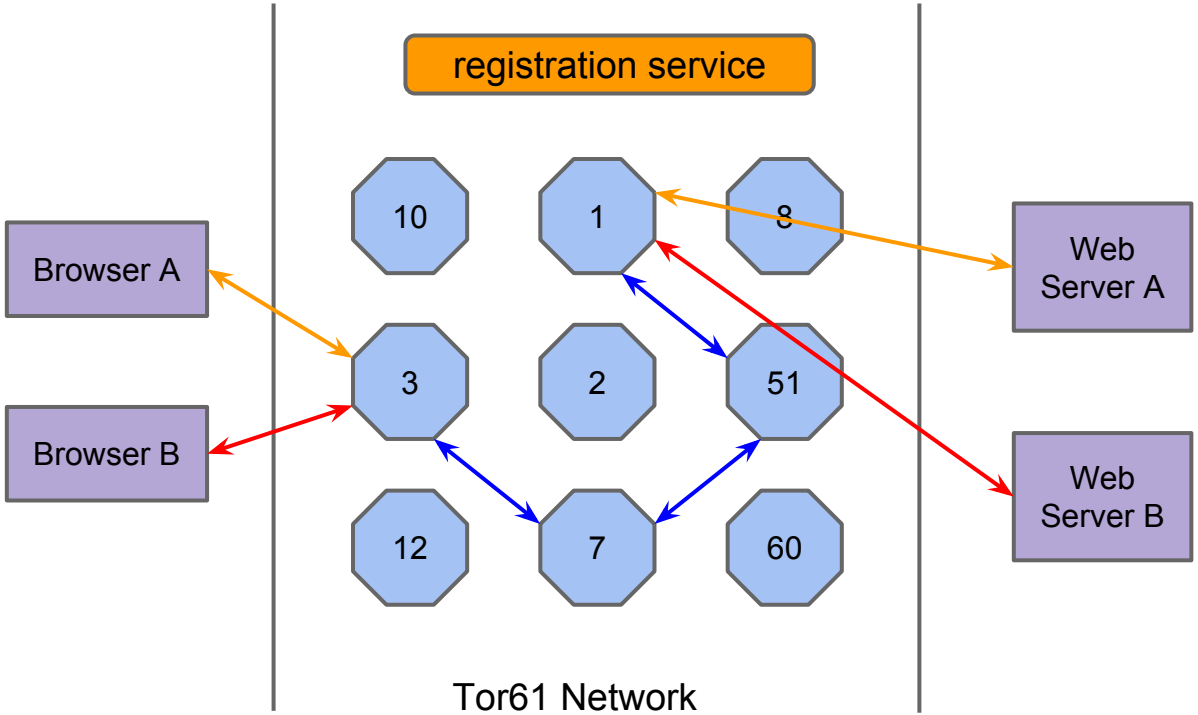
Tor61 Architecture Overview



On startup, each Tor61 node establishes a single **circuit** (blue path) through the network e.g 3-7-51-1, 10-2-3-7

For each HTTP request, browser talks to a single node to create a **stream** (orange/red path) through the circuit

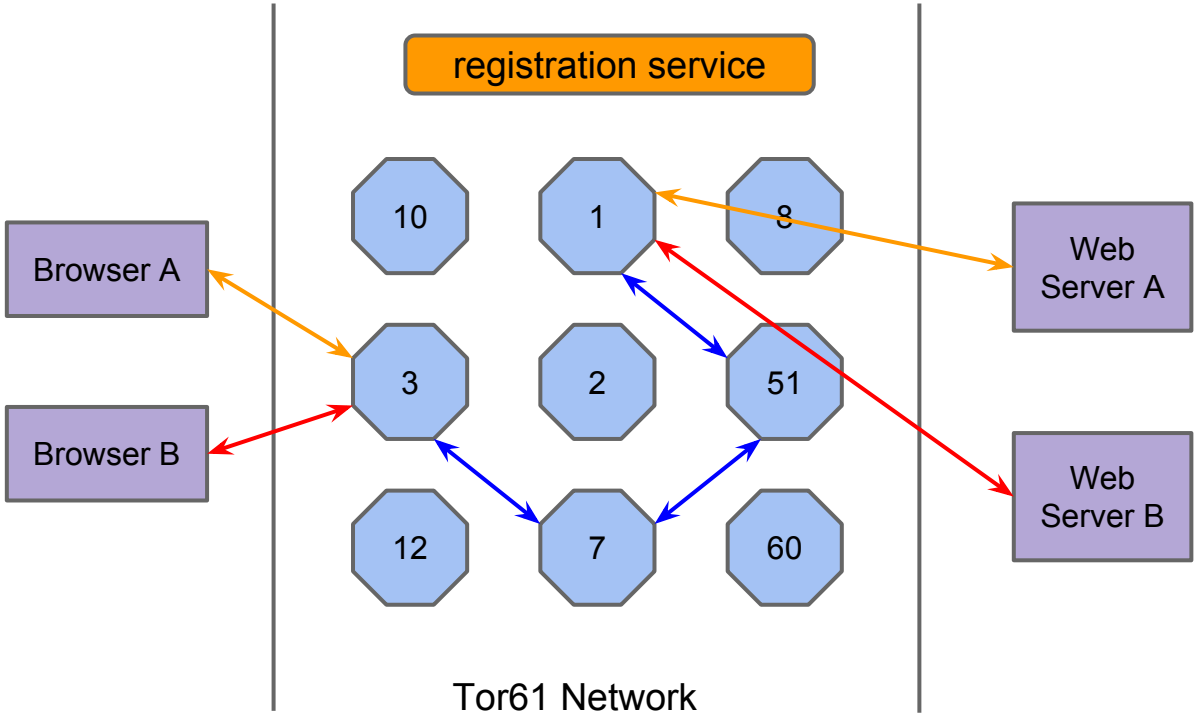
Tor61 Architecture Overview



On startup, each Tor61 node establishes a single **circuit** (blue path) through the network e.g 3-7-51-1, 10-2-3-7

For each HTTP request, browser talks to a single node to create a **stream** (orange/red path) through the circuit

Tor61 Architecture Overview

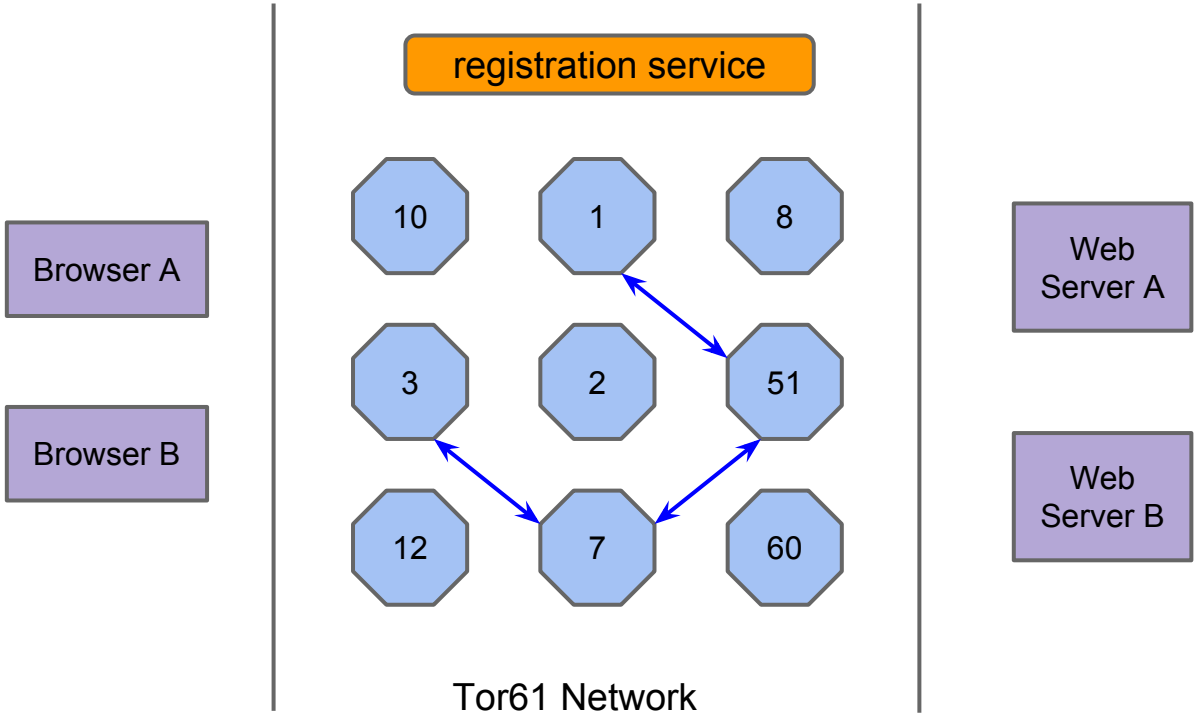


On startup, each Tor61 node establishes a single **circuit** (blue path) through the network e.g 3-7-51-1, 10-2-3-7

For each HTTP request, browser talks to a single node to create a **stream** (orange/red path) through the circuit

Once a stream is created, browser can send HTTP traffic through the stream to web server

Tor61 Architecture Overview



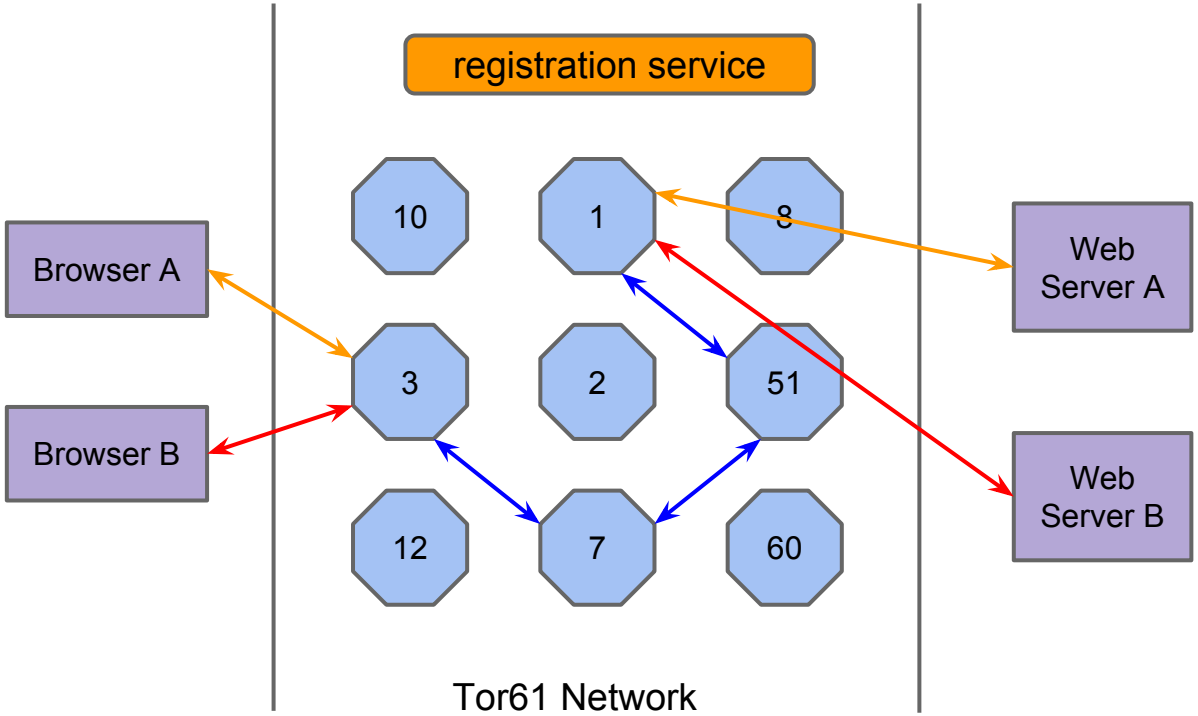
On startup, each Tor61 node establishes a single **circuit** (blue path) through the network e.g 3-7-51-1, 10-2-3-7

For each HTTP request, browser talks to a single node to create a **stream** (orange/red path) through the circuit

Once a stream is created, browser can send HTTP traffic through the stream to web server

Destroy stream and reuse circuit for other HTTP requests

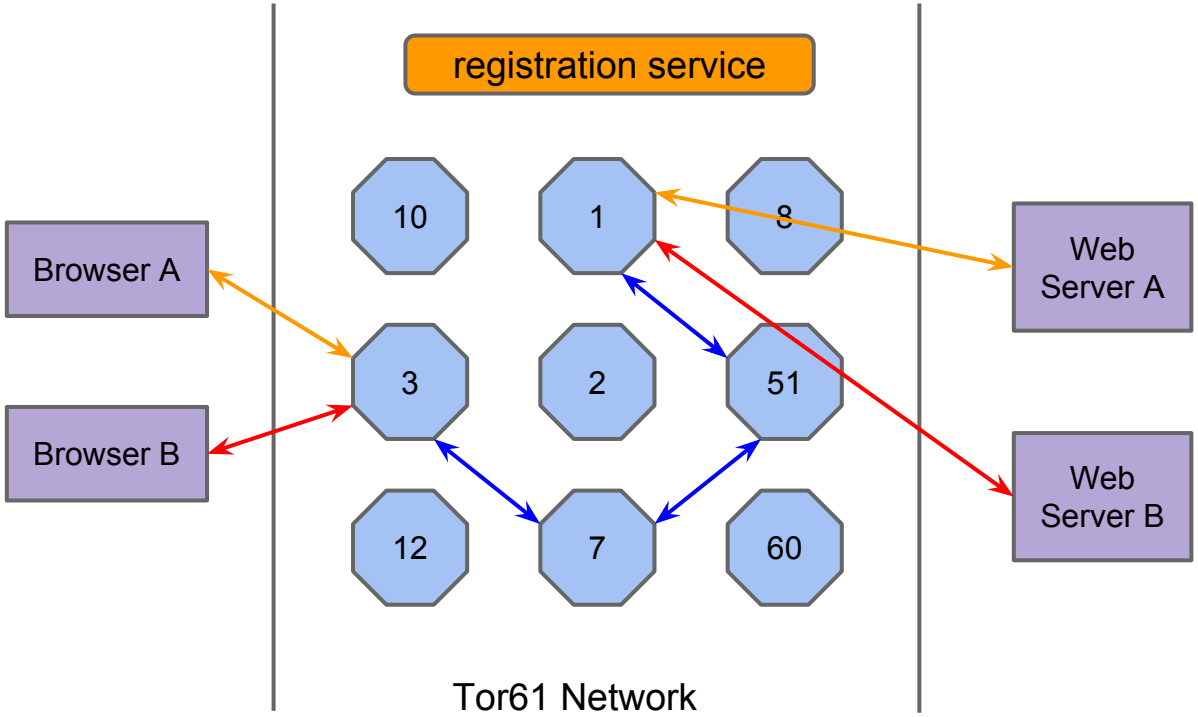
Tor61 Architecture Overview



Multiplex streams on circuit
e.g. streams from A-A, B-B use the same circuit
=> need stream id

Multiplex circuits on TCP connections
e.g circuit starting at 3 (3-7-51-1) and circuit starting at 10 (10-2-3-7) share tcp connection 3-7
=> need circuit id

Why anonymous browsing now?



e.g. 3-7-51-1 and A-A request

assuming data encrypted (not for Tor61)

Using source IP, Server A thinks request is from Tor node 1 instead of Browser A

Tor node 1 only knows request is from node 51

Tor node 51 only knows request is from node 7 and sent to node 1

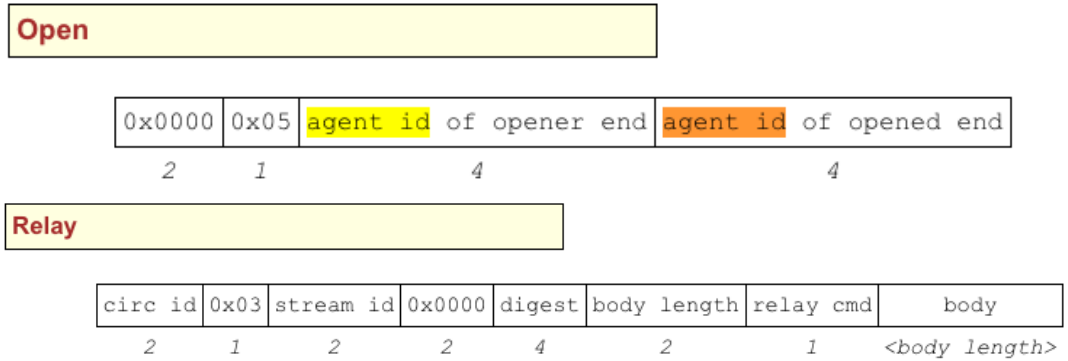
Tor node 3 knows request is from Browser A but doesn't know destination server

Tor61 Protocol and Tor61 Cells

Circuit establishment

Stream Creation

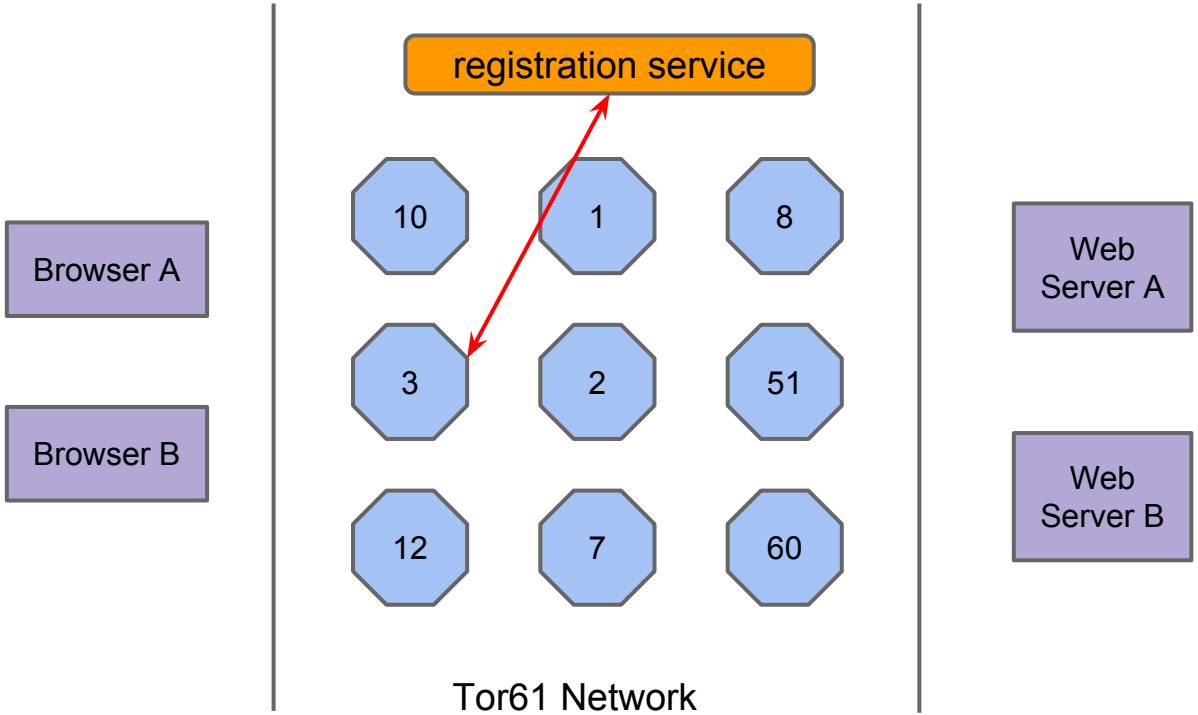
Routing data



Fixed-sized cells, padded to 512 bytes

- Control cells for next hop
  - e.g. Open, Create
- Relay cells for the last hop
  - e.g. Relay Extend, Relay Begin, Relay Data

How to create a circuit?

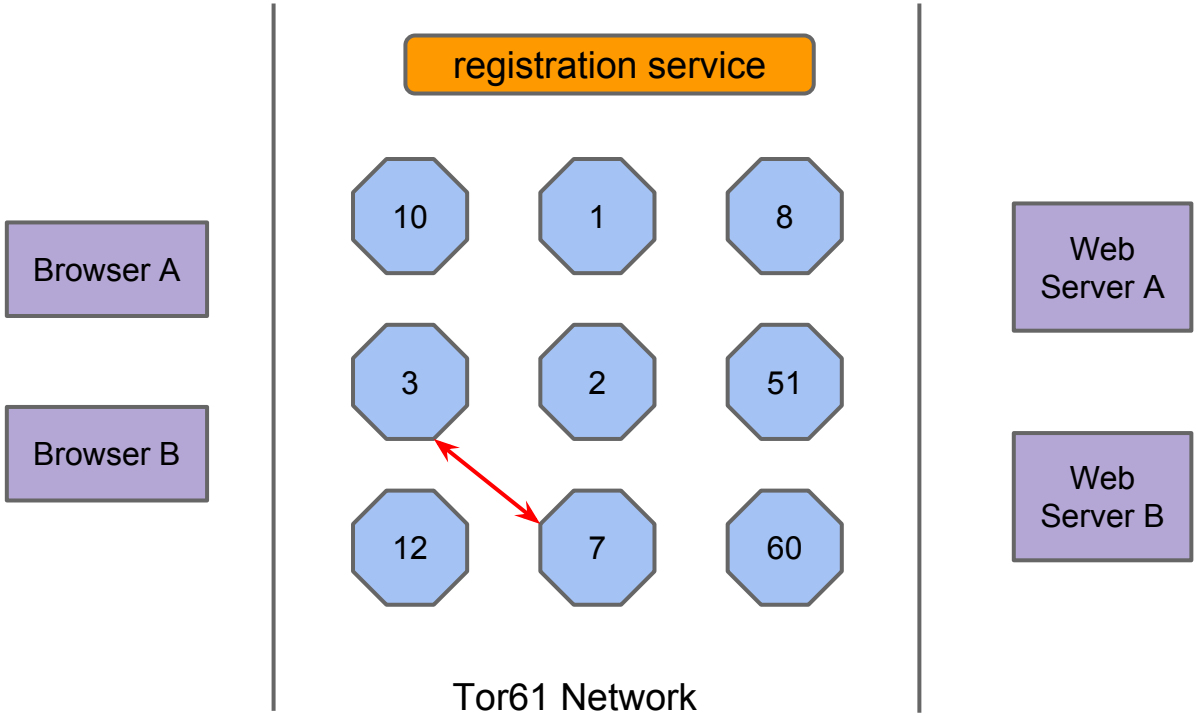


Node 3 starts up

Contacts registration service to ask which other Tor61 nodes are running

Gets a list of running Tor61 nodes, let's say all nine nodes in the figure and their IP:port information

How to create a circuit?



Node 3 picks the next router at random, let's say node 7

Opens a tcp connection to node 7 and sends Open cell

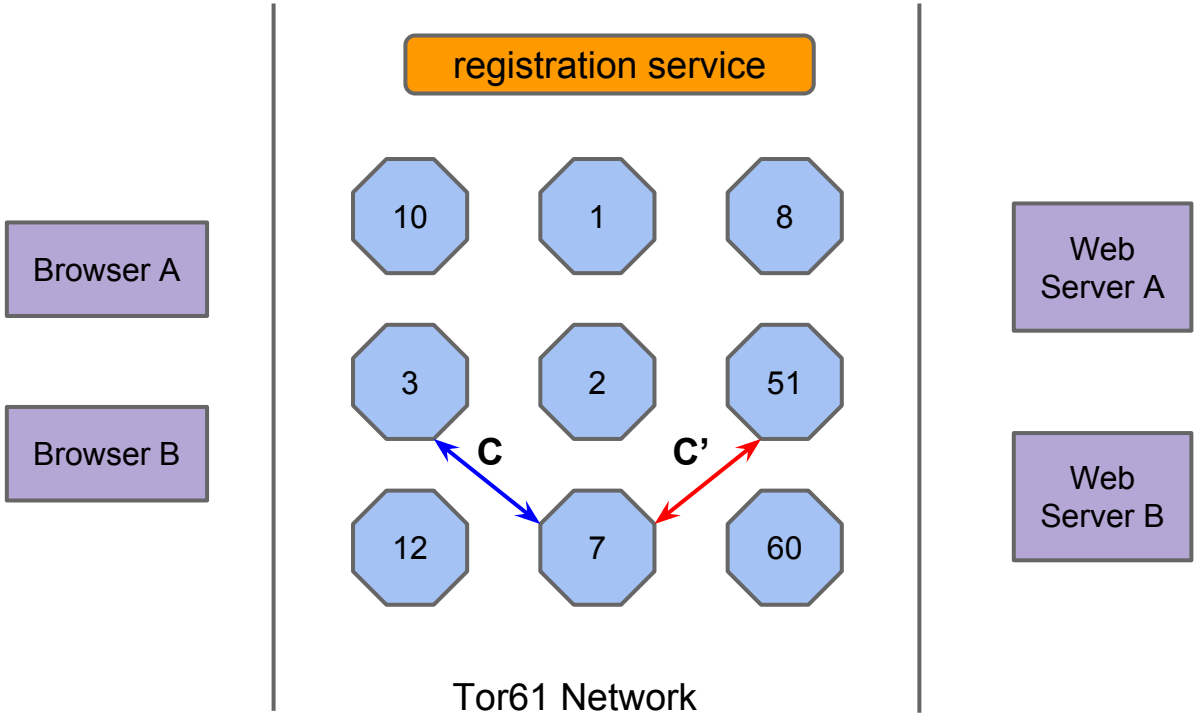
Node 7 returns Opened cell on success

Node 3 picks a circuit id, C (unique between node 3 and node 7) and sends a Create cell with circuit id C

Expect a Created cell from node 7 on success

Now we have 3-7 hop

How to create a circuit?



Node 3 picks node 51 as the next hop to extend

Node 3 sends a Relay Extend cell on circuit C. The cell contains ip: port of node 51

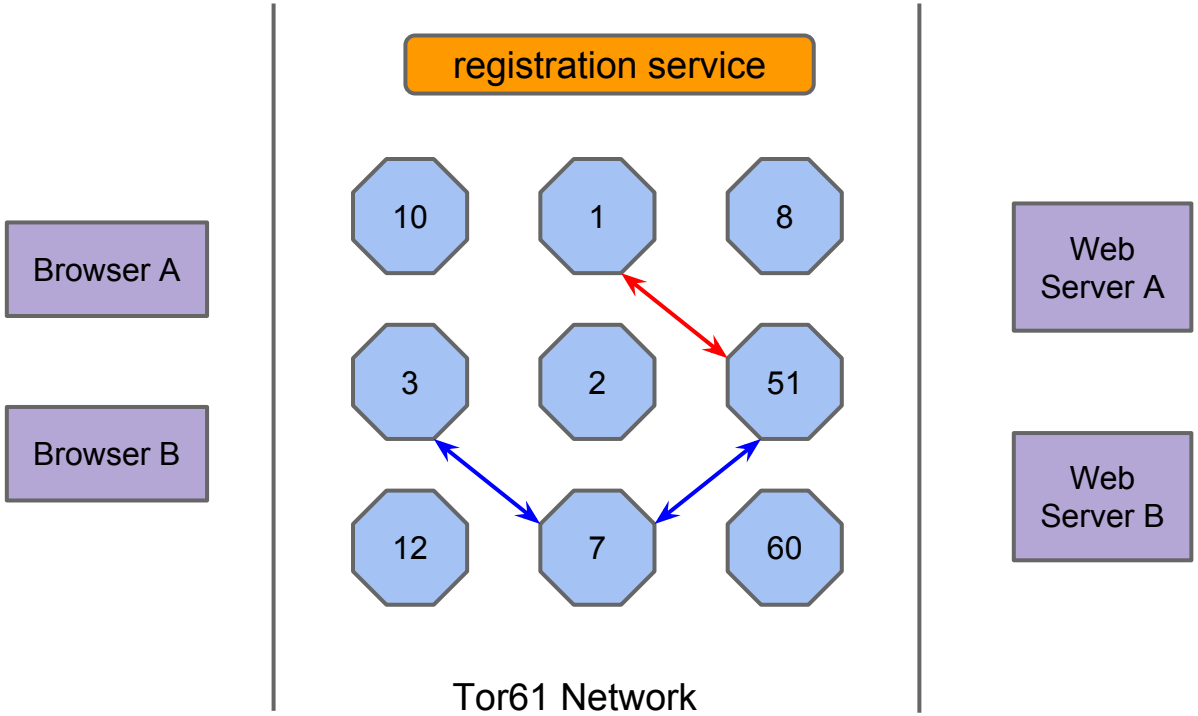
Node 7 receives Relay Extend; either uses an existing tor61 connection to node 51 or creates a new one (tcp connect+Open)

Node 7 picks a new circuit id C' (unique between 7-15), and sends node 51 a Create cell with C'

On Created, node 7 creates a new routing table entry "forward cells from circuit C to node 51 with a new circuit id C'

Node 7 sends Relay Extended back to node 3

How to create a circuit?



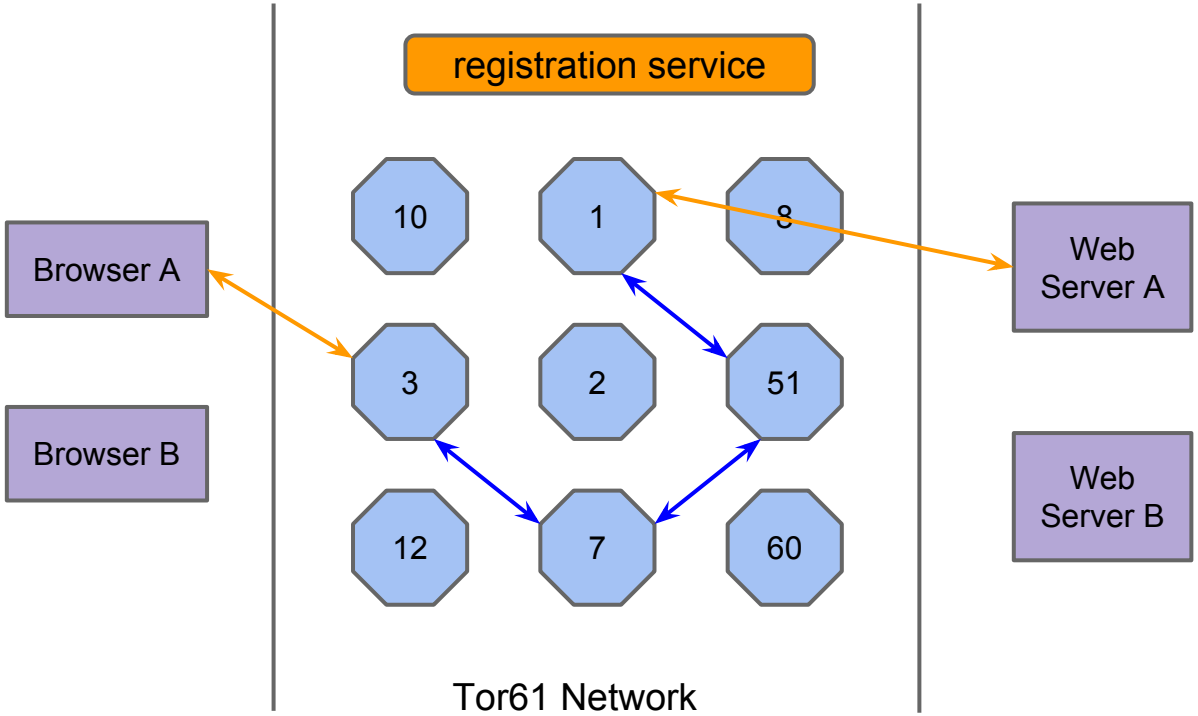
Node 3 repeats Relay Extend to extend circuit to node 1

Tor61 fix circuit length to be three, so we are done setting up circuit starting at node 3

Each node sets up its own circuit this way on startup

Each node needs a routing table to keep track of prev/next hops for different circuits through itself (check “Self Loops” more details)

How to create a stream?



Browser A wants to use circuit starting at node 3 to get a page from Server A

Each node has a HTTP proxy and a Tor61 router component; proxy part only active at circuit endpoints

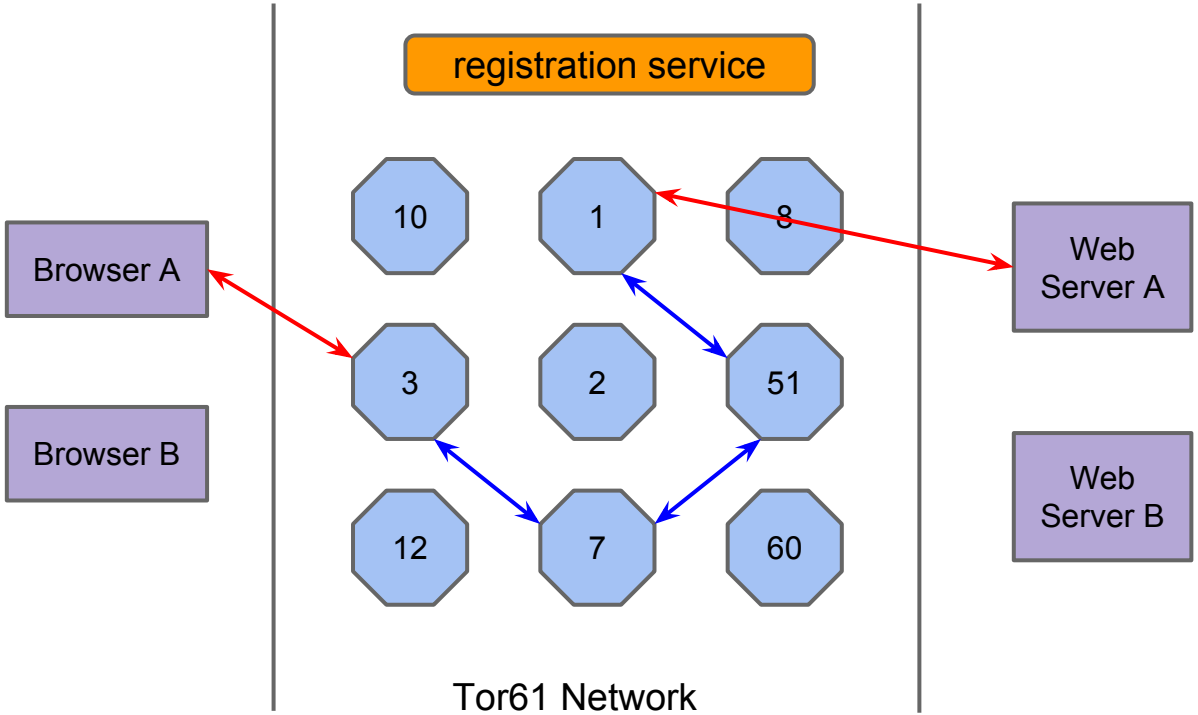
Browser A sends request to and gets response from the proxy component of node 3

Proxy part of node 3 uses the router part to create a stream and route data over the stream to node 1

Router part of node 1 gets request over stream and forwards them to the proxy part

Proxy part of node 1 finally sends request to Server A

How to create a stream?



Browser A sends GET to node 3

node 3 parses IP:port of Server A

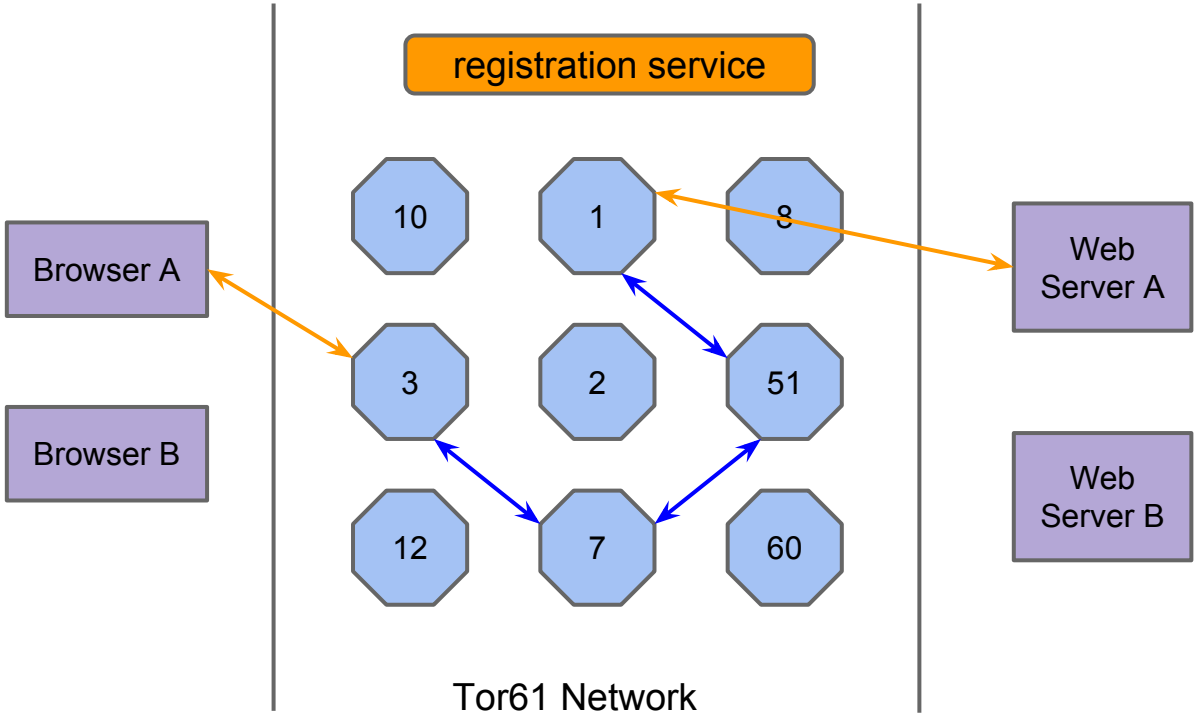
node 3 chooses a new stream number S for the circuit and sends Relay Begin cell with circuit id C and stream id S on the circuit

Relay Begin cell contains Server A ip:port as data

last node 1 gets ip:port of Server A and makes a tcp connection to Server A

On success, node 1 returns a Relay Connected cell to node 3

How to route data?



Node 3 packages request from browser into Relay Data cells and sends them on circuit C and stream S

Node 1 gets those Relay Data cells and extracts the actual request data and send them to Server A

Same process repeats for response from Server A

Registration Service

We run a service at cse461.cs.washington.edu:46101

We provide Java/Python/Node/Go utility code for you to register Tor61 nodes and fetching a list of running peers at /cse/courses/cse461/15sp/registrationUtility/

Presentation Requirements

Next Wed, Thurs and Fri signup slots

20 min presentation with TA & Arvind

Check out guidelines on project page!