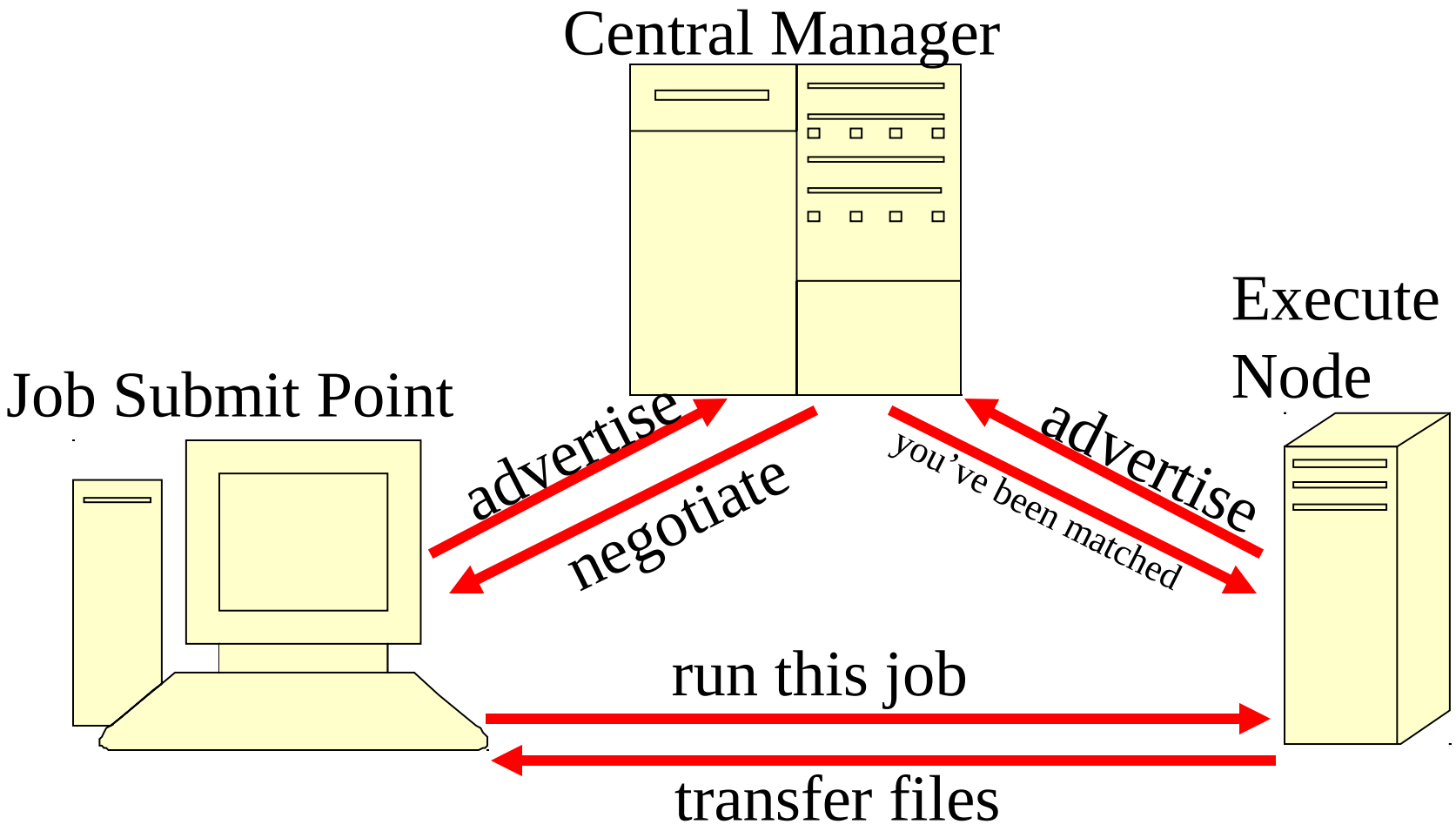
CCB
The Condor Connection Broker

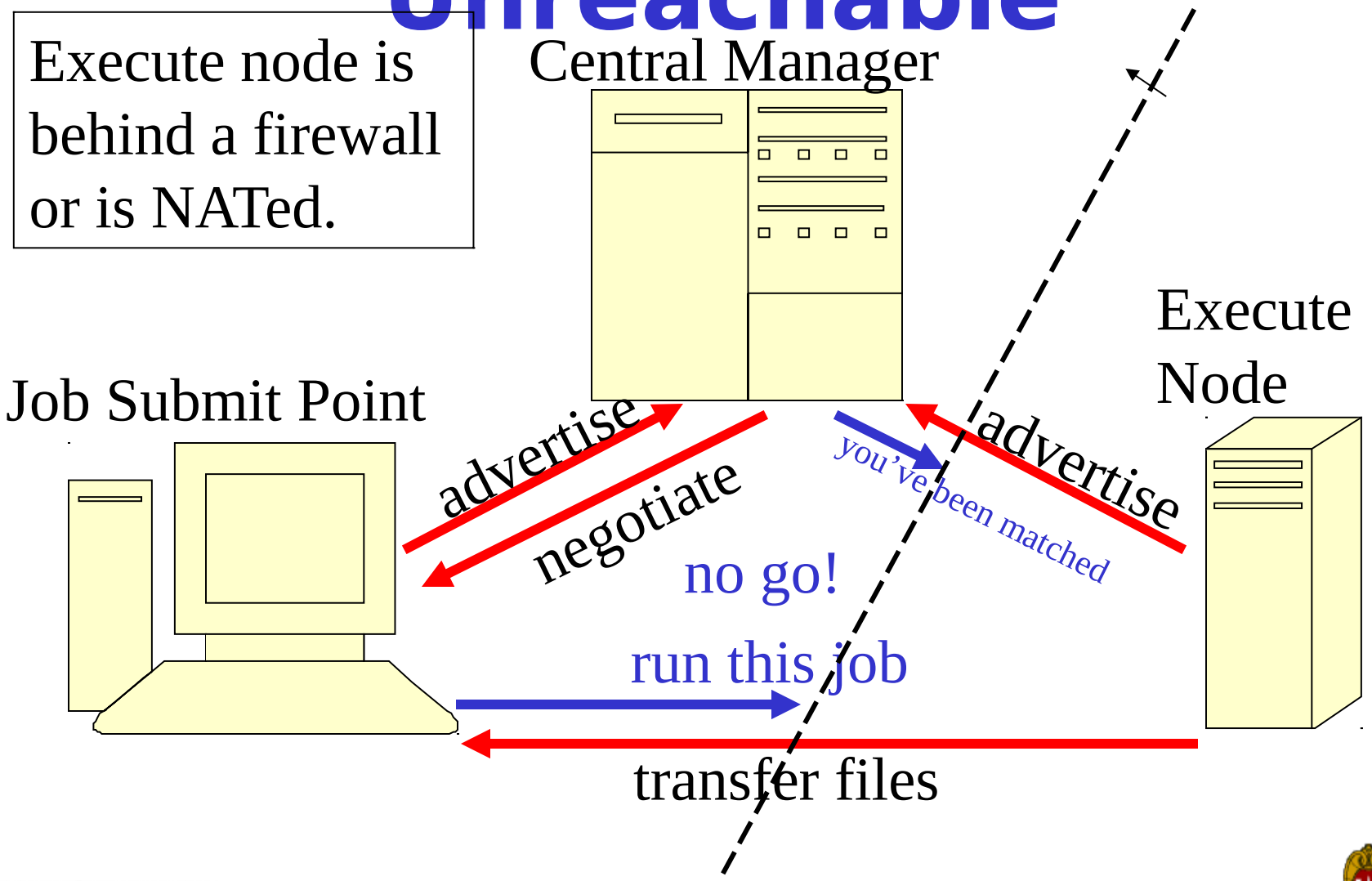
Dan Bradley
dan@hep.wisc.edu
Condor Project
CS and Physics Departments
University of Wisconsin-Madison

Condor Connections

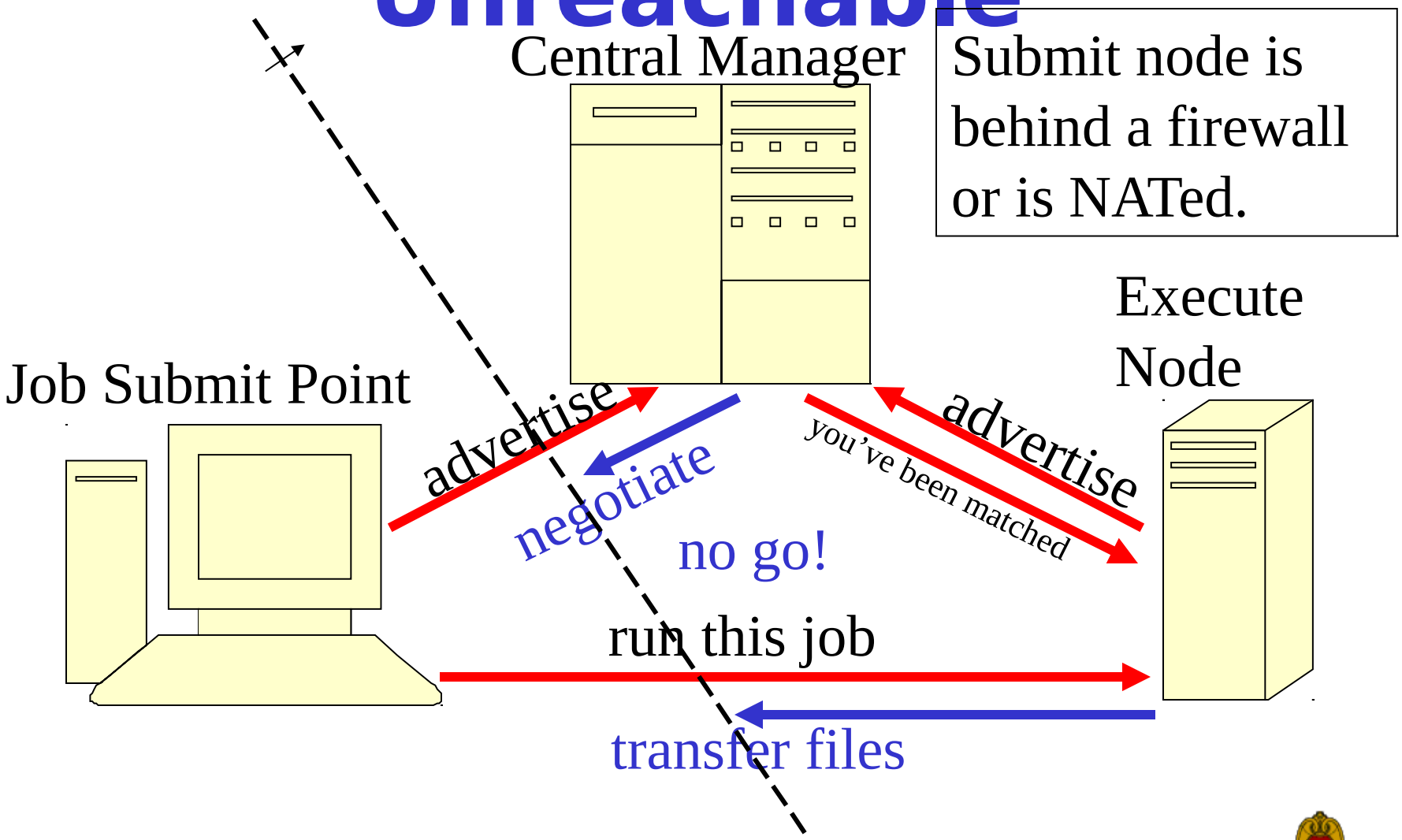


Execute Node Unreachable

Execute node is behind a firewall or is NATed.



Submit Node Unreachable

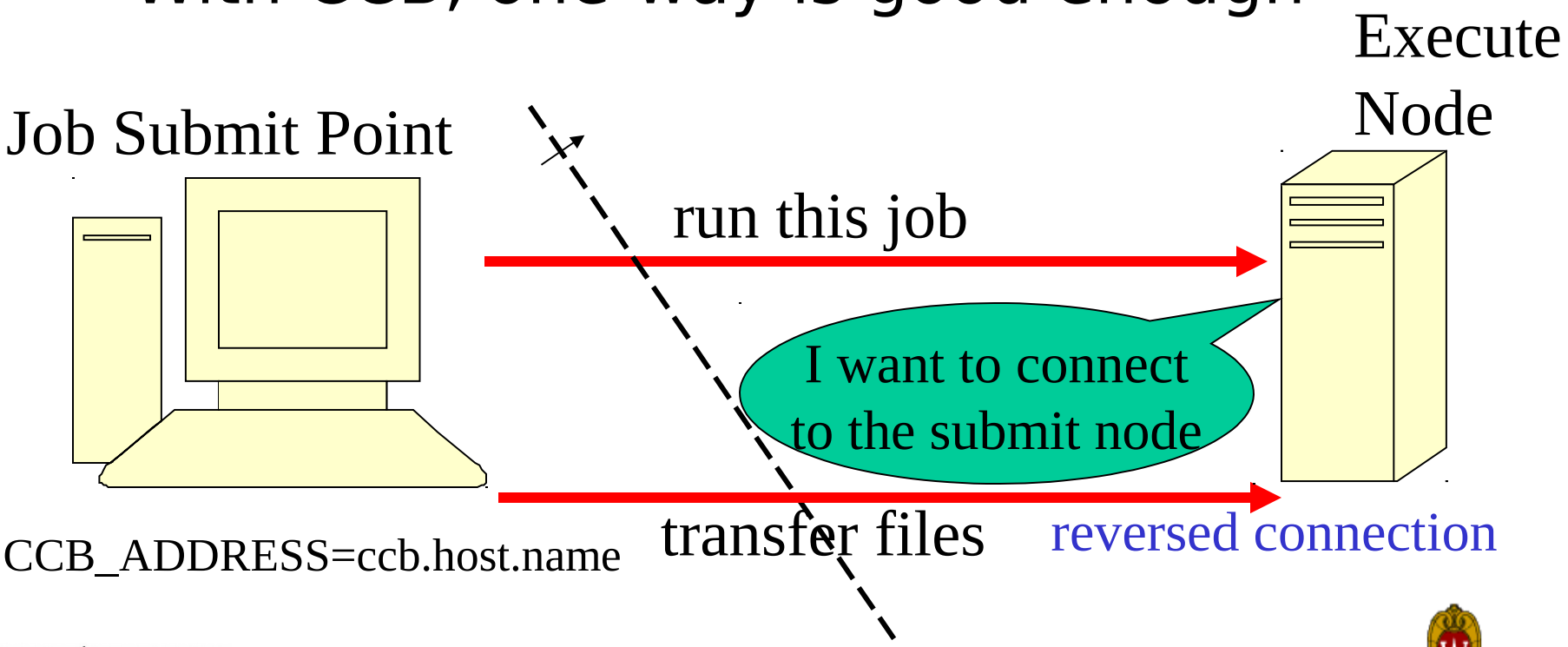


Common Scenarios

- Why cross private network boundaries?
  - Flocking
  - Multi-site Condor pool
  - Glidein

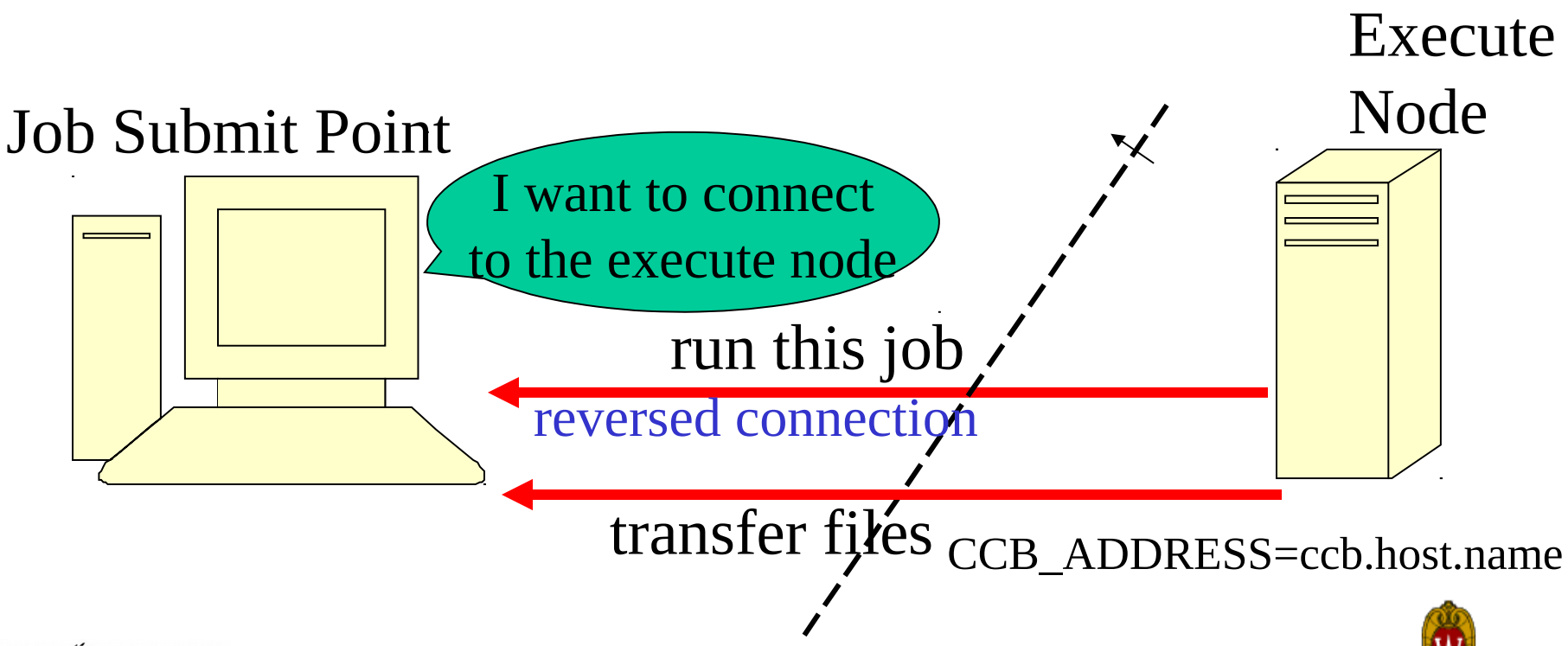
CCB: Condor Connection Broker

- Condor wants two-way connectivity
- With CCB, one-way is good enough



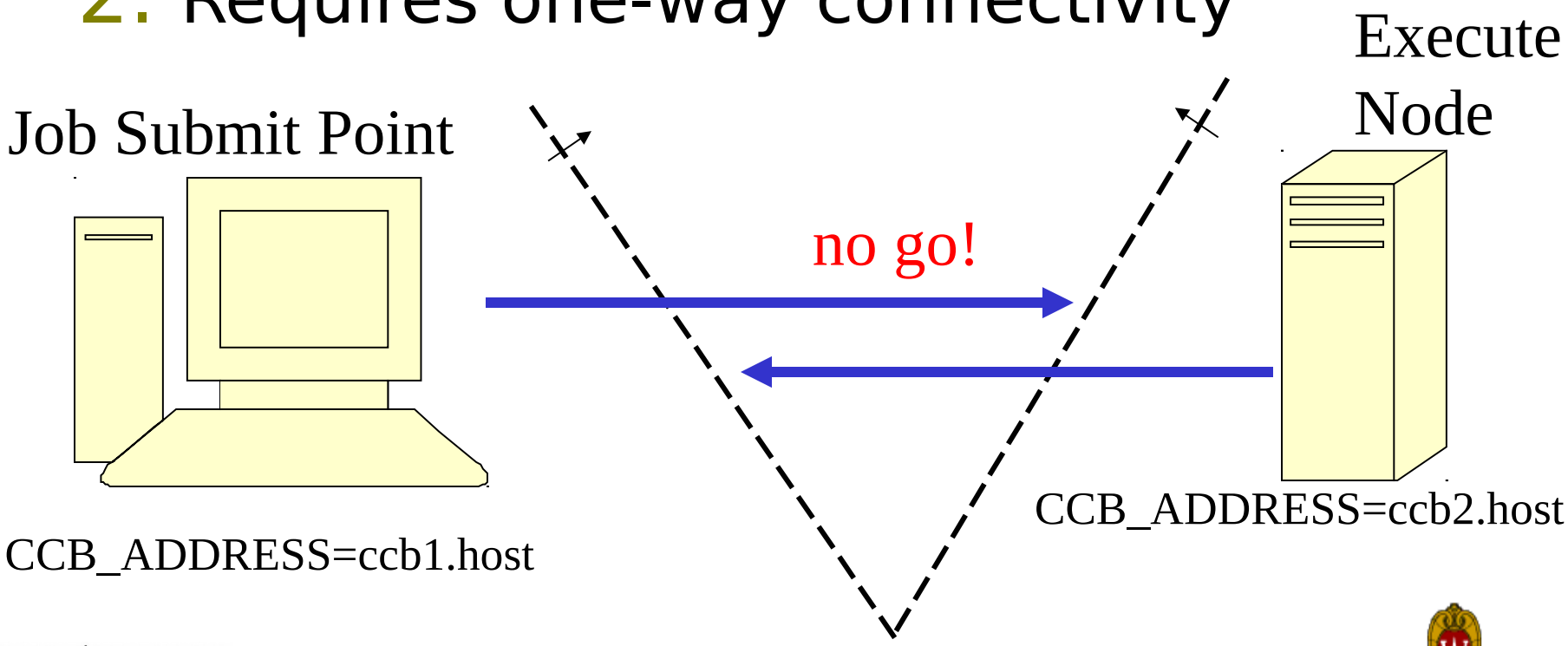
CCB: Condor Connection Broker

- Works in the mirror case too



Limitations of CCB

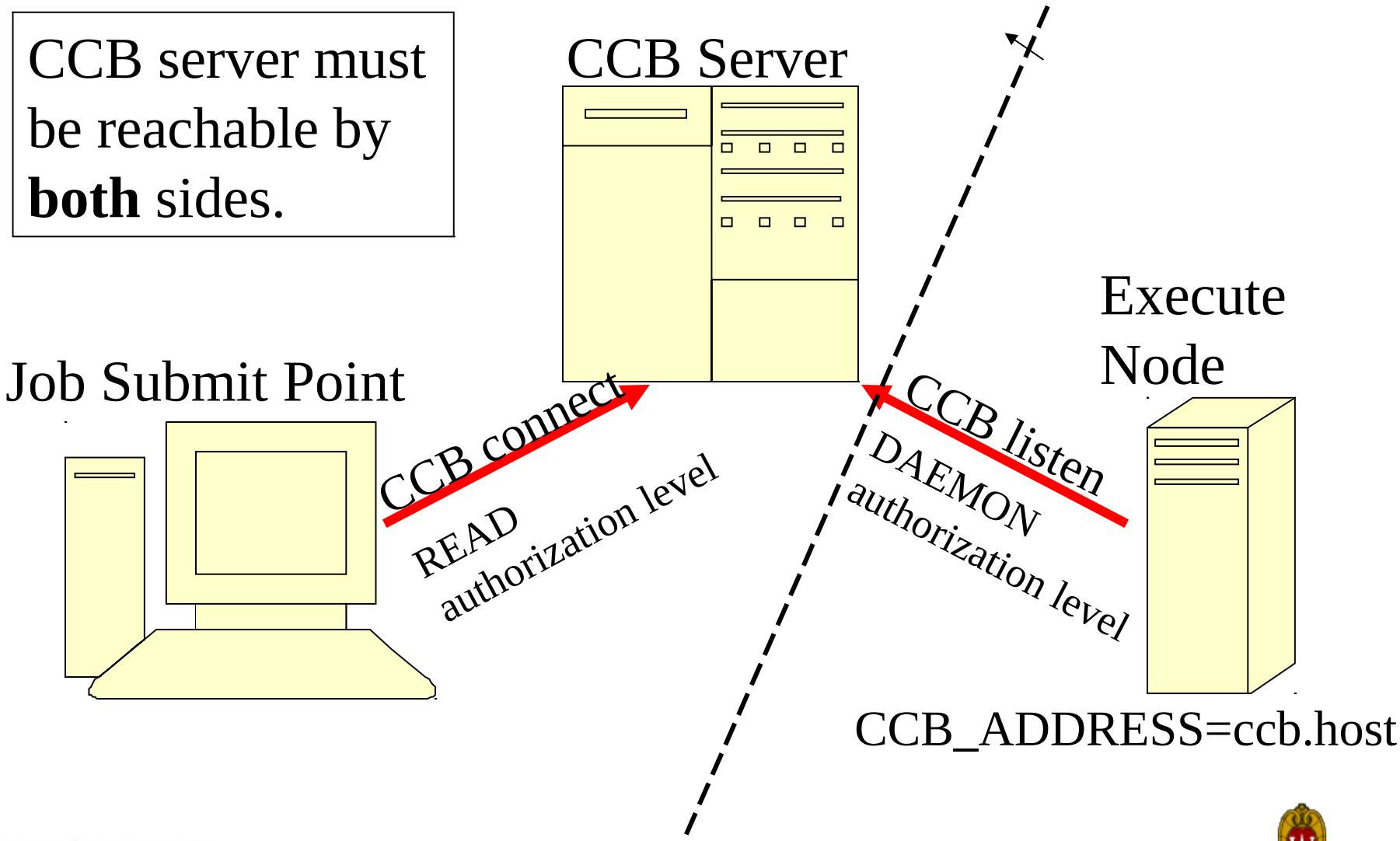
1. Doesn't help with standard universe
2. Requires one-way connectivity



GCB or VPN can help

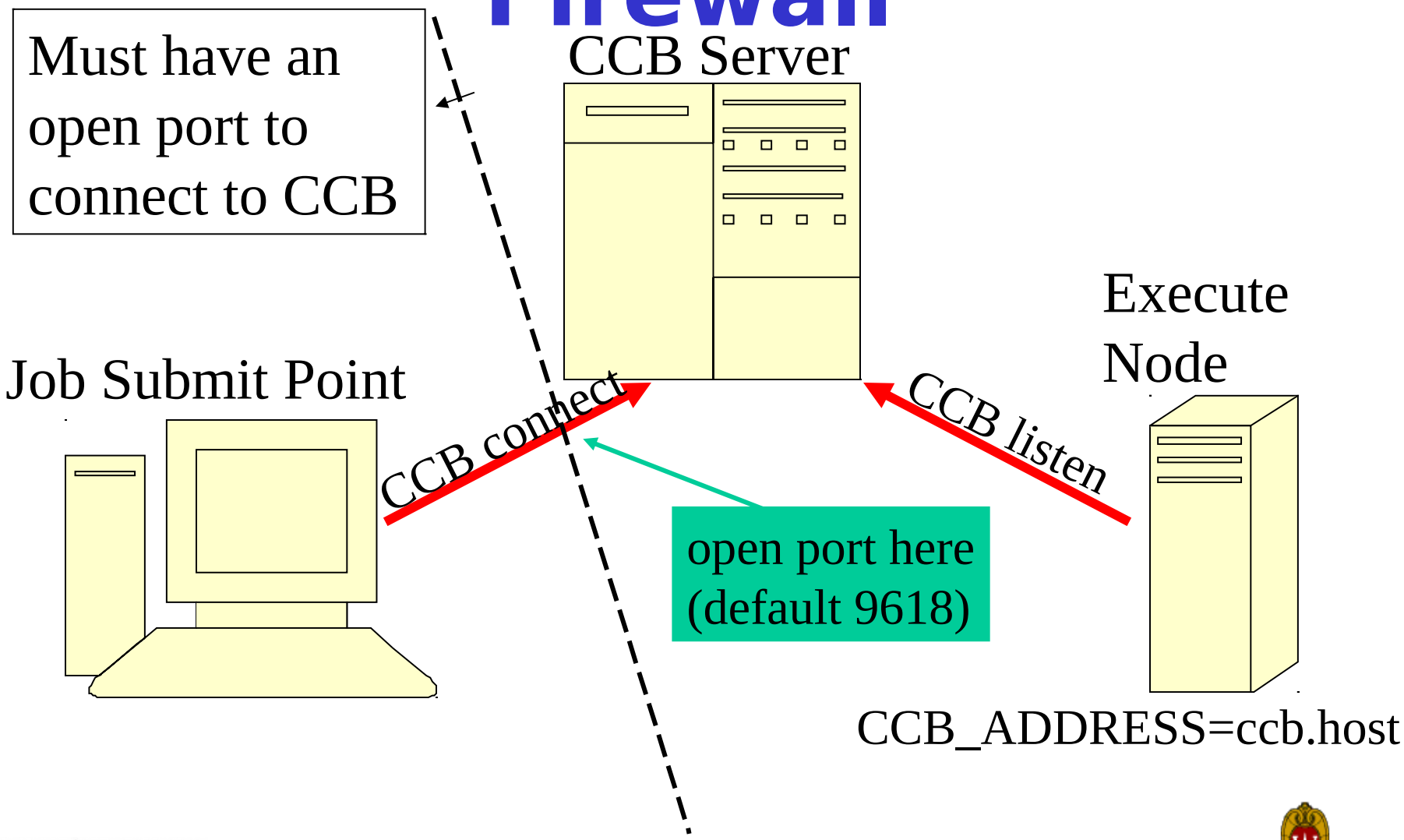
Connecting to CCB

CCB server must be reachable by **both** sides.



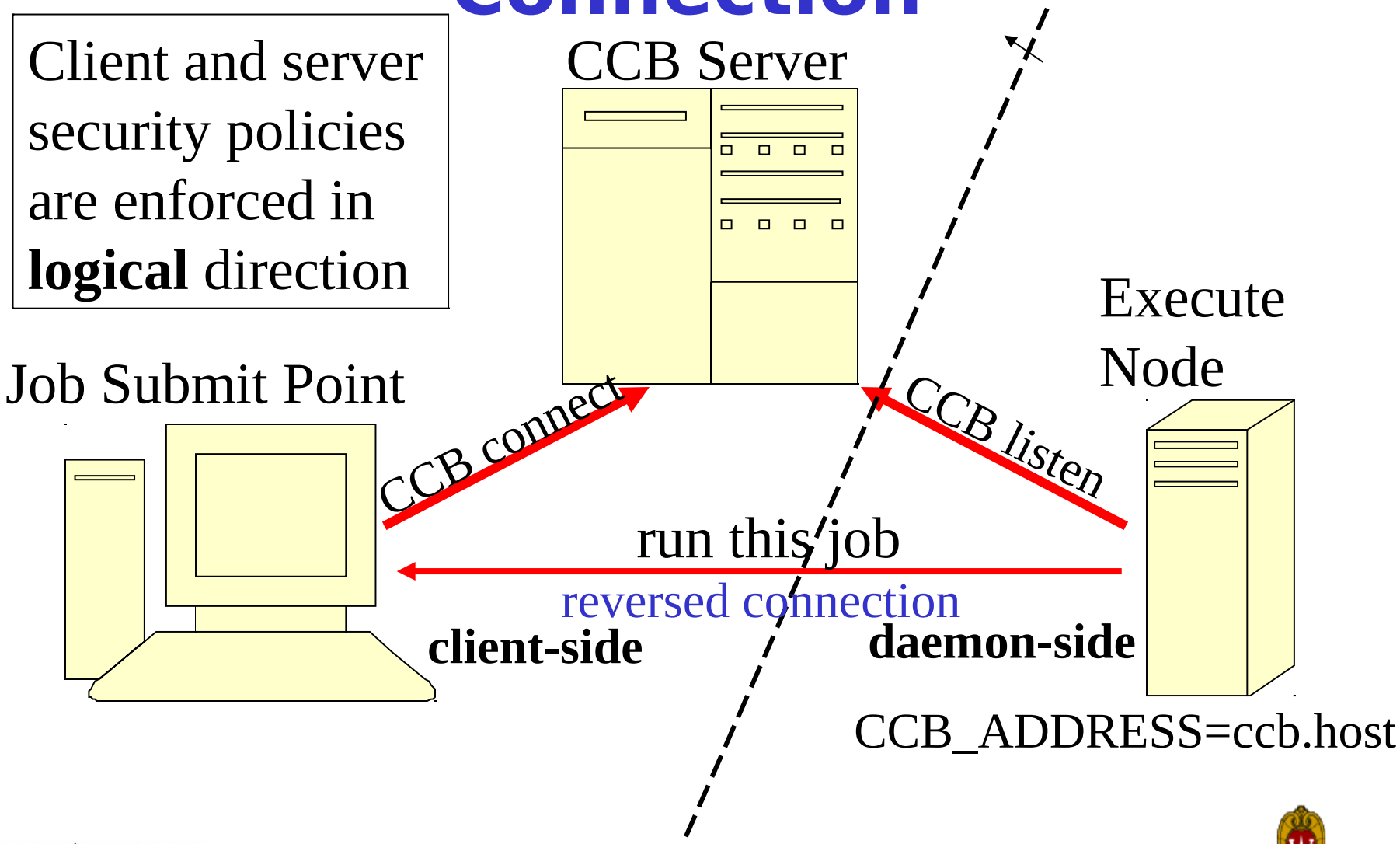
CCB Server Behind Firewall

Must have an open port to connect to CCB



Security on Reversed Connection

Client and server security policies are enforced in **logical** direction



GCB: Generic Connection Broker

- GCB: Condor 6.9.13
  - Clever: mostly invisible to Condor code
  - However, this makes some things difficult!
- CCB: Condor 7.3.0
  - Inspired by GCB
  - More tightly integrated into Condor
  - Not a complete replacement

Why CCB?

- Secure
  - supports full Condor security set
- Robust
  - supports reconnect, failover
- Portable
  - supports all Condor platforms, not just Linux

Why CCB?

- Dynamic
  - CCB clients and servers configurable without restart
- Informative log messages
  - Connection errors are propagated
  - Names and local IP addresses reported (GCB replaces local IP with broker IP)
- Easy to configure
  - automatically switches UDP to TCP in Condor protocols
  - CCB server only needs one open port

Configuring CCB

- The Server:
  - The collector *is* a CCB server
  - UNIX: MAX_FILE_DESCRIPTORS=10000

- The Client:
  1. CCB_ADDRESS = $(COLLECTOR_HOST)
  2. PRIVATE_NETWORK_NAME = your.domain

  (optimization: hosts with same network name don't use CCB to connect to each other)

Tests of CCB

- Igor Sfiligoi's Cross-Atlantic Mega Condor Glidein Test Pool for CMS
  - one machine with 70 CCB collectors
  - execute nodes in private networks
  - GSI authentication
  - 100,000 registered Condor daemons
  - 200,000 jobs/day with one schedd

Summary

- CCB makes Condor work if
  - You have one-way connectivity

Fine Print:

- And using Condor 7.3+
- And the private side sets CCB_ADDRESS
- And the private side is authorized at the DAEMON authorization level by CCB
- And the public side can connect to CCB
- And the public side is authorized at the READ authorization level by CCB
- And not using “standard universe”