Troubleshooting Channel Access

Jeff Hill

Clients don't Connect

- Background
  - Broadcast vs unicasts addresses
    - Broadcast - all hosts on a subnet
    - Unicast - only one host on the subnet
- CA address list
  - EPICS_CA_AUTO_ADDR_LIST is YES
    - List is configured from each active network interface resident in the local host
      - Broadcast addresses from LAN interfaces
      - Destination address from point to point interfaces

Clients Don't Connect

- Client must use the server's broadcast address or the server's interface address
  - By default the clients use the broadcast addresses configured for network interfaces
    - UNIX: netstat –i
    - Windows: ipconfig
    - vxWorks: ifShow
  - Non-default configuration in
    - EPICS_CA_ADDR_LIST
  - Verify server's address
    - Unix, windows: netstat –a
    - vxWorks: inetstatShow

Clients Don't Connect

- Client must use the server's UDP port number
  - Default port is 5064
  - Non-default configuration
    - EPICS_CA_SERVER_PORT
    - EPICS_CA_ADDR_LIST
    - EPICS_CAS_SERVER_PORT
    - EPICS_CAS_INTF_ADDR_LIST
  - Verify Server Port
    - Unix, windows: netstat –a
    - vxWorks: inetstatShow

Clients Don't Connect

- Unicast addresses and multiple servers on the same host
  - Modern IP kernels allow multiple servers to bind to the same UDP port
    - Broadcasts are reliably delivered to both servers
    - Unicasts are typically sent to only *one* of the servers

Clients Don’t Connect

- Client Does not See Server’s Beacon
  - Background
    - Clients continuously attempt to connect all channels that are disconnected
    - Search rates drop exponentially if progress isn't being made
    - Clients send searches at a very slow rate until
      - There is some success
      - A new server beacon is seen
      - In old versions (prior to R3.14.7 clients suspend searching until a new server beacon is seen)

Clients Don't Connect

- Client Does not See Server's Beacon
  - Background
    - Clients continuously estimate the period of all server beacons seen
    - If the averaged period of a beacon changes significantly then the client is said to have detected a beacon anomaly
    - If a client with disconnected channels sees a beacon anomaly it will start transmitting search requests at a faster rate, but at a lower rate than is initially used when the channel is created

Netmask Configuration Problems

- Symptom
  - Clients connect erratically
- Background
  - IP address divided into host part and network part using netmask
  - Netmask is specified when configuring a network interface
  - Net directed broadcasts contain network part identifying the destination network and host part of all ones
  - ICMP error reply sent when host receives undeliverable IP frame
  - IP kernels maintain finite length input queue for each UDP port
    - Messages exceeding a high water mark are discarded

Netmask Configuration Problems

- Cause
  - Default destination address for CA search messages: net directed broadcast
    - Network part specifies destination network and host part all ones
  - Can be many hosts on large complex subnet with incorrectly configured netmasks – all see the CA broadcasts and send ICMP error reply
  - ICMP error replies can swamp finite length UDP input queue
    - Can displace legitimate responses
      - CA retransmits the search requests, but the ICMP responses may nearly always beat the legitimate response into the UDP input queue

Netmask Configuration Problems

- Diagnostics
  - Use network sniffer to monitor ICMP error rates
  - Response will be sent to CA clients with disconnected channels
  - ICMP error response activity increases when starting a new client (when creating a new channel)
    - Destination unreachable
    - Network unreachable

Router Broadcast Loops

- Typically routers disable forwarding of net directed broadcasts by default
- Enabling this can make it much easier to configure a multi-subnet EPICS system
- Care must be taken to avoid router broadcast loops

Router Broadcast Loops

- Router broadcast loops starts when router instantiates net directed broadcast into Ethernet broadcast
- This Ethernet broadcast is received by host that thinks it has a route for the net directed broadcast
  - That host forwards the net directed broadcast for delivery via the routing system
    - A router instantiates the net directed broadcast into and Ethernet broadcast for the 2nd time on the same network
    - The broadcast loop continues until the time-to-live counter in the IP frame decrements to zero.

Router Broadcast Loops

- Unusually high broadcast rates
  - Destination port EPICS_CA_SERVER_PORT
  - Typically port 5064
- ICMP errors
  - Time to live field equals zero during transmit

Gateway Broadcast Loops

- Watch out also for loops caused by poorly formed bi-directional gateway configuration

ENOBUFS Messages

- Background
  - Many Berkley Unix derived IP kernels use low level network buffering quantum called an mbuf
  - ENOBUFS messages indicate that there is insufficient space to perform some socket operation.
  - mbuf starvation is known to lead to communication stalls or hangs on older versions of vxWorks, and or with certain vxWorks network interface drivers

ENOBUFS Messages

- Contributing Circumstances
  - Total number of connected clients is high.
  - Server's sustained event (monitor subscription update) production rate is higher than the client's or the network's sustained event consumption rate.
    - clients that subscribe for monitor events but do not call ca_pend_event() or ca_poll()
  - The server does not get a chance to run due to CPU starvation
    - CA clients are sending requests
  - Stale connections.
    - Client is abruptly turned off or disconnected from the network
    - Client application is hung
    - Internal "keepalive" timer has not yet expired
    - Active monitor subscriptions make this worse

ENOBUFS Messages

- Diagnostics
  - IOC shell
    - casr [interest level]
  - vxWorks
    - inetstatShow
    - mbufShow
    - netStackSysPoolShow
    - netStackDataPoolShow
  - RTEMS:
    - netstat [interest level]