SERVER1374 APPCLUSTER _20240522165629: 16:56:29 - **17:26:28 10.66.109.84**

Statistics Overview: Use `Statistics > Summary` to get a general overview of the capture file, including the capture duration, packet count, and average packet size.

Stream 0 : 10.66.109.106 → 10.66.109.84:3389 SERVER1418 > SERVER1374

Stream 351 : 10.66.109.84 → 10.186.29.60:443 SERVER1374

Protocol Hierarchy: Check `Statistics > Protocol Hierarchy` to see the distribution of protocols. This helps confirm the presence of expected HTTP and TLS traffic.

# **Packet Loss** - display filters to specifically identify packet loss and retransmissions:

##Retransmissions: tcp.analysis.retransmission

Around x500 RTX mostly between 10.66.109.84 10.66.164.104 . Only during 3-way handshake

##Duplicate ACKs: tcp.analysis.duplicate_ack

Negligible

##Fragmentation

None

# Window size `tcp.window_size < 1024 (busy receiver)`

X552 window 0 events over 20 mins. Most of them sourced SERVER1374 APPCLUSTER << possible sign of buffer full.

# **RTT**

10.66.109.106 → 10.66.109.84 port 3389 (stream 0): ~22ms (high, same VLAN)

10.66.109.84 → 10.66.29.60 port 443 (stream 351): ~30ms (high)

…

# Window size

Around x100 window 0 events over 20 mins. Multiple streams. But many affecting the device the pcaps is captured from SERVER1155 << possible sign of buffer full.

RECOMMENDATIONS

- **Check Network Adapter Settings**:
  - **Device Manager**: Open Device Manager and check for any issues with network adapters.

  - **Driver Updates**: Make sure the network drivers are up-to-date.

- **Review Event Logs**:
  - **Event Viewer**: Open Event Viewer (type `eventvwr` in the Run dialog) and navigate to `Windows Logs -> System`. Look for any network-related errors or warnings.

- **Analyze Network Stack with Commands**:
  - **netstat**: Use `netstat -an` to display all active connections and listening ports. Look for abnormal connections or ports.
  - **arp**: Use `arp -a` to display the ARP cache. This can help identify IP address conflicts.

- **Check Firewall and Security Software**:
  - **Windows Firewall**:
  - **Antivirus/Antimalware**: Temporarily disable security software to see if it’s interfering with the network connection.

- **Advanced Network Diagnostics**:
  - **Performance Monitor**: Use `perfmon` to monitor network performance. Add counters for Network Interface and TCPv4 to see if there are any performance bottlenecks.

- **Check TCP/IP Settings**:
  - **TCP Parameters**: Use the `netsh` command to view and configure TCP settings. For example, `netsh int tcp show global` shows the global TCP settings.

- **Inspect MTU Settings**:
  - **Change MTU Size**: No fragmentation so doesn’t apply