

No. Time Source Destination Protocol Length Info
194 2.036388 10.2.33.183 52.109.124.29 TCP 66 60024 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
WS=256 SACK_PERM

Frame 194: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{CC14D496-1375-466F-B0C7-9481F9B75BC7}, id 0

Section number: 1
Interface id: 0 (\Device\NPF_{CC14D496-1375-466F-B0C7-9481F9B75BC7})
Interface name: \Device\NPF_{CC14D496-1375-466F-B0C7-9481F9B75BC7}
Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Dec 6, 2023 22:28:28.116396000 India Standard Time
UTC Arrival Time: Dec 6, 2023 16:58:28.116396000 UTC
Epoch Arrival Time: 1701881908.116396000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000802000 seconds]
[Time delta from previous displayed frame: 0.011269000 seconds]
[Time since reference or first frame: 2.036388000 seconds]
Frame Number: 194
Frame Length: 66 bytes (528 bits)
Capture Length: 66 bytes (528 bits)
[Frame is marked: True]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP SYN/FIN]
[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]

Ethernet II, Src: AzureWaveTec_3a:a5:d0 (10:68:38:3a:a5:d0), Dst: IETF-VRRP-VRID_62 (00:00:5e:00:01:62)
Destination: IETF-VRRP-VRID_62 (00:00:5e:00:01:62)
Address: IETF-VRRP-VRID_62 (00:00:5e:00:01:62)
.... .. = LG bit: Globally unique address (factory default)
.... .. = IG bit: Individual address (unicast)
Source: AzureWaveTec_3a:a5:d0 (10:68:38:3a:a5:d0)
Address: AzureWaveTec_3a:a5:d0 (10:68:38:3a:a5:d0)
.... .. = LG bit: Globally unique address (factory default)
.... .. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.2.33.183, Dst: 52.109.124.29
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 52
Identification: 0x9c09 (39945)
010. = Flags: 0x2, Don't fragment
0... = Reserved bit: Not set
.1. = Don't fragment: Set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x8277 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.2.33.183
Destination Address: 52.109.124.29

Transmission Control Protocol, Src Port: 60024, Dst Port: 443, Seq: 0, Len: 0
Source Port: 60024
Destination Port: 443
[Stream index: 5]
[Conversation completeness: Complete, WITH_DATA (31)]
..0. = RST: Absent
...1 = FIN: Present
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
.... ...1 = SYN: Present
[Completeness Flags: ·FDASS]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2267971972
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
000. = Reserved: Not set
...0 = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set

```

.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
[Expert Info (Chat/Sequence): Connection establish request (SYN): server port 443]
[Connection establish request (SYN): server port 443]
[Severity level: Chat]
[Group: Sequence]
.... ...0 = Fin: Not set
[TCP Flags: .....S.]
Window: 64240
[Calculated window size: 64240]
Checksum: 0xa2f5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  TCP Option - Maximum segment size: 1460 bytes
    Kind: Maximum Segment Size (2)
    Length: 4
    MSS Value: 1460
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - Window scale: 8 (multiply by 256)
    Kind: Window Scale (3)
    Length: 3
    Shift count: 8
    [Multiplier: 256]
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - SACK permitted
    Kind: SACK Permitted (4)
    Length: 2
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]
No.    Time           Source           Destination      Protocol Length Info
 197 2.047958      52.109.124.29    10.2.33.183     TCP             66      443 → 60024 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
MSS=1460 SACK_PERM WS=128
Frame 197: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{CC14D496-1375-466F-B0C7-9481F9B75BC7}, id
0
Section number: 1
Interface id: 0 (\Device\NPF_{CC14D496-1375-466F-B0C7-9481F9B75BC7})
  Interface name: \Device\NPF_{CC14D496-1375-466F-B0C7-9481F9B75BC7}
  Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Dec  6, 2023 22:28:28.127966000 India Standard Time
UTC Arrival Time: Dec  6, 2023 16:58:28.127966000 UTC
Epoch Arrival Time: 1701881908.127966000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000150000 seconds]
[Time delta from previous displayed frame: 0.011570000 seconds]
[Time since reference or first frame: 2.047958000 seconds]
Frame Number: 197
Frame Length: 66 bytes (528 bits)
Capture Length: 66 bytes (528 bits)
[Frame is marked: True]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP SYN/FIN]
[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
Ethernet II, Src: JuniperNetwo_15:46:00 (80:ac:ac:15:46:00), Dst: AzureWaveTec_3a:a5:d0 (10:68:38:3a:a5:d0)
Destination: AzureWaveTec_3a:a5:d0 (10:68:38:3a:a5:d0)
  Address: AzureWaveTec_3a:a5:d0 (10:68:38:3a:a5:d0)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
Source: JuniperNetwo_15:46:00 (80:ac:ac:15:46:00)
  Address: JuniperNetwo_15:46:00 (80:ac:ac:15:46:00)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 52.109.124.29, Dst: 10.2.33.183
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  0000 00.. = Differentiated Services Codepoint: Default (0)
  .... 00.. = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 52
Identification: 0x0000 (0)
010. .... = Flags: 0x2, Don't fragment

```

```

0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 63
Protocol: TCP (6)
Header Checksum: 0x5f81 [validation disabled]
[Header checksum status: Unverified]
Source Address: 52.109.124.29
Destination Address: 10.2.33.183
Transmission Control Protocol, Src Port: 443, Dst Port: 60024, Seq: 0, Ack: 1, Len: 0
Source Port: 443
Destination Port: 60024
[Stream index: 5]
[Conversation completeness: Complete, WITH_DATA (31)]
..0. .... = RST: Absent
...1 .... = FIN: Present
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
.... ...1 = SYN: Present
[Completeness Flags: ·FDASS]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 180521731
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2267971973
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... .... 0... = Push: Not set
.... ..... 0... = Reset: Not set
.... .... .1. = Syn: Set
[Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 443]
[Connection establish acknowledge (SYN+ACK): server port 443]
[Severity level: Chat]
[Group: Sequence]
.... .... ...0 = Fin: Not set
[TCP Flags: .....A..S.]
Window: 29200
[Calculated window size: 29200]
Checksum: 0x9600 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
TCP Option - Maximum segment size: 1460 bytes
Kind: Maximum Segment Size (2)
Length: 4
MSS Value: 1460
TCP Option - No-Operation (NOP)
Kind: No-Operation (1)
TCP Option - No-Operation (NOP)
Kind: No-Operation (1)
TCP Option - SACK permitted
Kind: SACK Permitted (4)
Length: 2
TCP Option - No-Operation (NOP)
Kind: No-Operation (1)
TCP Option - Window scale: 7 (multiply by 128)
Kind: Window Scale (3)
Length: 3
Shift count: 7
[Multiplier: 128]
[Timestamps]
[Time since first frame in this TCP stream: 0.011570000 seconds]
[Time since previous frame in this TCP stream: 0.011570000 seconds]
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 194]
[The RTT to ACK the segment was: 0.011570000 seconds]
[iRTT: 0.011675000 seconds]
No.      Time      Source      Destination      Protocol Length Info
198 2.048063 10.2.33.183 52.109.124.29 TCP 54 60024 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Frame 198: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{CC14D496-1375-466F-B0C7-9481F9B75BC7}, id
0

```

```
Section number: 1
Interface id: 0 (\Device\NPF_{CC14D496-1375-466F-B0C7-9481F9B75BC7})
  Interface name: \Device\NPF_{CC14D496-1375-466F-B0C7-9481F9B75BC7}
  Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Dec  6, 2023 22:28:28.128071000 India Standard Time
UTC Arrival Time: Dec  6, 2023 16:58:28.128071000 UTC
Epoch Arrival Time: 1701881908.128071000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000105000 seconds]
[Time delta from previous displayed frame: 0.000105000 seconds]
[Time since reference or first frame: 2.048063000 seconds]
Frame Number: 198
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
[Frame is marked: True]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: AzureWaveTec_3a:a5:d0 (10:68:38:3a:a5:d0), Dst: IETF-VRRP-VRID_62 (00:00:5e:00:01:62)
  Destination: IETF-VRRP-VRID_62 (00:00:5e:00:01:62)
    Address: IETF-VRRP-VRID_62 (00:00:5e:00:01:62)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ...0 .... = IG bit: Individual address (unicast)
  Source: AzureWaveTec_3a:a5:d0 (10:68:38:3a:a5:d0)
    Address: AzureWaveTec_3a:a5:d0 (10:68:38:3a:a5:d0)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ...0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.2.33.183, Dst: 52.109.124.29
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 40
  Identification: 0x9c0a (39946)
  010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x8282 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.2.33.183
  Destination Address: 52.109.124.29
Transmission Control Protocol, Src Port: 60024, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  Source Port: 60024
  Destination Port: 443
  [Stream index: 5]
  [Conversation completeness: Complete, WITH_DATA (31)]
    ..0. .... = RST: Absent
    ...1 .... = FIN: Present
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..1. = SYN-ACK: Present
    .... ...1 = SYN: Present
  [Completeness Flags: ·FDASS]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2267971973
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 180521732
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  [TCP Flags: .....A.....]
```

Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x46e2 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
 [Time since first frame in this TCP stream: 0.011675000 seconds]
 [Time since previous frame in this TCP stream: 0.000105000 seconds]
[SEQ/ACK analysis]
 [This is an ACK to the segment in frame: 197]
 [The RTT to ACK the segment was: 0.000105000 seconds]
 [iRTT: 0.011675000 seconds]