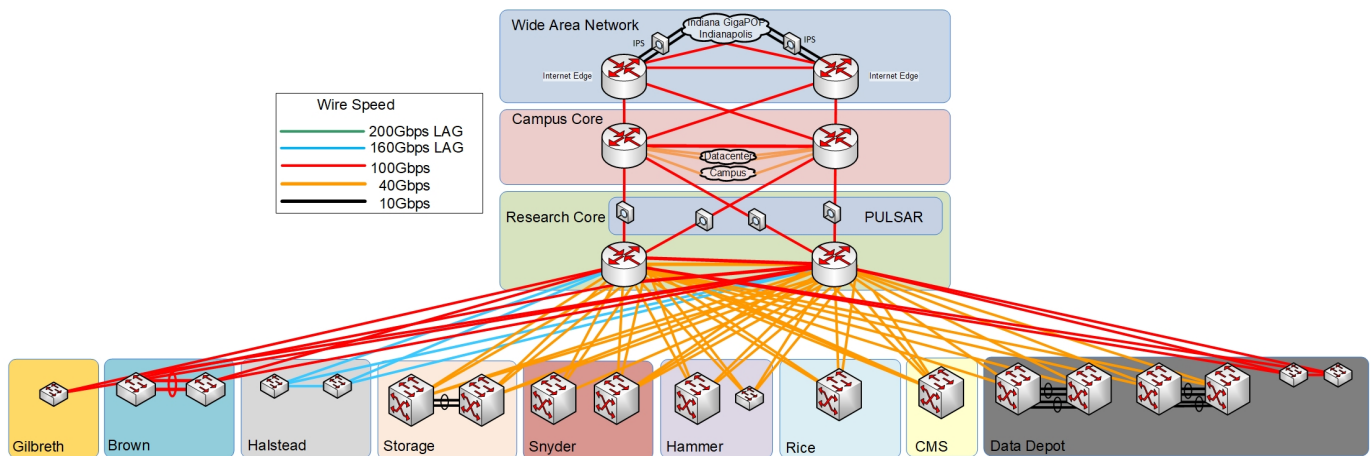


# TAP Aggregation and Traffic Distribution

## Purdue Research Network Diagram



## Network Test Access Points (TAPs)

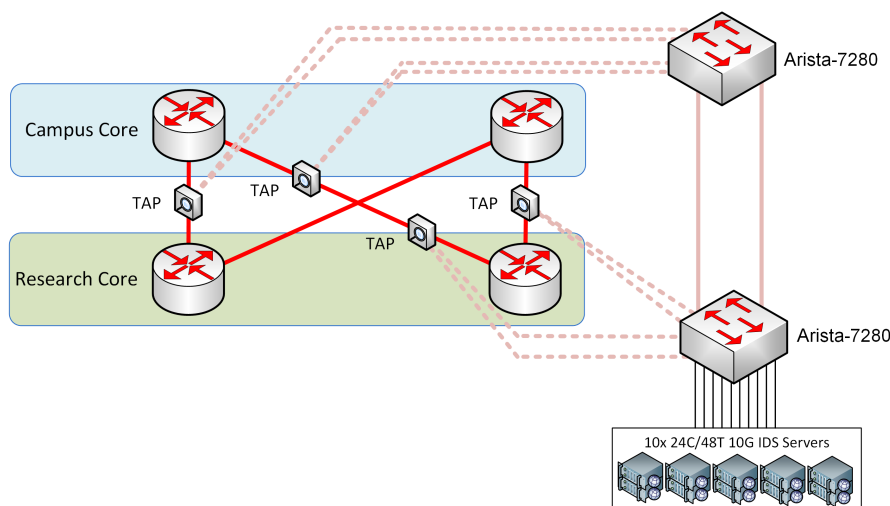
A network TAP is an external monitoring device that mirrors the traffic that is passing between two network nodes. Passive network TAPs are wired between network nodes and duplicate traffic without adding additional latency to the connection. At Purdue, network TAPs mirror traffic between four 100G links between the Campus Core and Research Core routers. Please refer to Wide Network Map above for placement details. This allows traffic to be monitored that is going from internal campus networks to the research network as well as traffic from other institution's research networks to Purdue's research network. Commodity Internet traffic is analyzed by an in-line IPS as shown in the diagram.

### Hardware

Chassis: Gigamon 1/2 U chassis, supports 1,2,3, or 4 Dual Optical G-TAP Modules, stand alone chassis, 1/10G10

TAPs: Dual optical HighFlow GigaTAP module, 50/50 Singlemode, 1310/1550nm, 10/40/100G

## TAP Aggregation and Traffic Distribution



### Hardware

Two Arista switches are used to distribute network traffic from 8 100G taps to 10 10G Zeek workers.

Arista Switch Model: DCS-7280SRA-48C6

Optics for taps: 100GBASE-LR4

Optics for connections between Aristas: 100GBASE-CR4

## Online Resources

Quick Start Guide for Arista switches: <https://www.arista.com/en/qsg-7280x-series-1ru-gen3>

Status Indicators: <https://www.arista.com/en/qsg-7280x-series-1ru-gen3/7280x-series-1ru-gen3-status-indicator>

## Arista Configuration

### DNS Configuration

<https://www.arista.com/en/um-eos/eos-section-6-1-managing-the-switch-name>

```
pulsar-arista7280-1(config)#ip name-server X.X.X.X
```

```
pulsar-arista7280-2(config)#ip name-server X.X.X.X
```

### Arista API Configuration

```
pulsar-arista7280-1(config)# management api http-commands
```

```
pulsar-arista7280-1(config-mgmt-api-http-cmds)# no shutdown
```

This enables the HTTPS server. Certificate configuration is below. Admin account can be used to access the API. It is highly recommended to apply an ACL to the management interface.

### Certificate Configuration

The HTTPS API needs a trusted certificate unless you want a bunch of warnings.

<https://<hostname>/overview.html>

```
pulsar-arista7280-1(config)#copy scp:user@<host>:/path/to/cert.cer certificate:eapiServerCert
```

```
pulsar-arista7280-1(config)#copy scp:user@<host>:/path/to/private.key sslkey:eapiServerKey
```

```
pulsar-arista7280-1(config)#management security
```

```
pulsar-arista7280-1(config-mgmt-security)#ssl profile eapi
```

```
pulsar-arista7280-1(config-mgmt-sec-ssl-profile-eapi)#certificate eapiServerCert key eapiServerKey
```

```
pulsar-arista7280-1(config-mgmt-sec-ssl-profile-eapi)#management api http-commands
```

```
pulsar-arista7280-1(config-mgmt-api-http-cmds)#protocol https ssl profile eapi
```

### SNMP Configuration

<https://www.arista.com/en/um-eos/eos-section-42-3-configuring-snmp>

The only configuration needed on the Arista switches is to set an RO community string, which also starts the snmp agent on the switch.

```
pulsar-arista7280-1(config)# snmp-server community <password> ro
```

```
pulsar-arista7280-2(config)# snmp-server community <password> ro
```

### Load balancing Configuration

Set the switch to tap aggregation mode.

```
pulsar-arista7280-2(config)#tap aggregation
```

```
pulsar-arista7280-2(config-tap-agg)#mode exclusive
```

Create a new load balance profile called "TAP"

```
pulsar-arista7280-2(config)#load-balance policies
```

```
pulsar-arista7280-2(config-load-balance-policies)#load-balance sand profile TAP
```

By default, symmetric hashing is not enabled. This can be seen with the `show load-balance profile TAP` command.

```
pulsar-arista7280-2#show load-balance profile TAP | grep Symm
Symmetric hashing is OFF
```

This command enables symmetric hashing (which we need to direct bi-directional traffic to the same Zeek worker).

```
pulsar-arista7280-2(config-sand-load-balance-profile-TAP)#fields symmetric-hash
```

At this point you have the option of two additional commands, which will only slightly affect how hashing works.

This command will disable hashing based on the Protocol field in the IP header.

```
arista7280-2(config-sand-load-balance-profile-TAP)#fields ipv4 dst-ip src-ip
```

This command will disable hashing based on the MAC header. Depending on your TAP solution, these might only be a set of a few MACs between the routers you are monitoring.

```
arista7280-2(config-sand-load-balance-profile-TAP)#port-channel ip ip-tcp-udp-header
```

Once you create the profile, it isn't applied automatically. You will see this output in `show load-balance profile TAP`.

```
Profile TAP (global) is applied on the following
None
```

Apply the load balancing profile you created.

```
arista7280-2(config-sand-load-balance-profile-TAP)# port-channel load-balance sand profile TAP
```

Then you should see that the profile is applied globally.

```
Profile TAP (global) is applied on the following
FixedSystem
```

Full output of `show load-balance profile TAP`.

```
pulsar-arista7280-2#show load-balance profile TAP
----- TAP (global) -----

Lag Hashing on IP-TCP-UDP headers for IP packets is ON
Lag Hashing on MAC header for IP packets is OFF
Symmetric hashing is ON
Lag Hashing mode is flow-based
Lag Hash polynomial is 3
Lag Hash seed is 0
Port-channel load-balancing in egress replication is OFF

MAC hash fields:
  Source MAC Address is ON
  EtherType is ON
  Destination MAC Address is ON
  VLAN is ON
MPLS hash fields:
  Label is ON
IPv4 hash fields:
  Source IPv4 Address is ON
  Destination IPv4 Address is ON
  Time-To-Live is OFF
IPv6 hash fields:
  Hop Limit is ON
  Source IPv6 Address is ON
  Destination IPv4 Address is ON
L4 hash fields:
  Destination Port is ON
  Source Port is ON
Packet type MPLS over GRE:
  Hashing mode is inner-ip

Profile TAP (global) is applied on the following
FixedSystem
```

The best place to check to see if symmetric hashing is working is via the Zeek connection log (conn.log). You shouldn't see any duplicate connections, i.e. the same source/destination IP and TCP/UDP port across two workers. An easy way to verify this is via the "bro doctor" script.

<https://github.com/ncsa/bro-doctor>

Output like this means the Arista are configured properly for symmetric hashing.

```
#####
# Checking if any recent connections have been logged multiple times #
#####
ok, only 0.00%, 0 out of 1611 connections appear to be duplicate
```

## Arista Configurations

These config excerpts show the important pieces of the Arista switch configuration. An MTU of 9214 was present by default on all interfaces even without specifying it in the interface configuration.

### pulsar-arista7280-1 Configuration

```
! Startup-config last modified at Tue Jun 18 17:46:59 2019 by admin
! device: pulsar-arista7280-1 (DCS-7280SRA-48C6, EOS-4.20.1F)
!
! boot system flash:/EOS-4.20.1F.swi
!
...
!
tap aggregation
  mode exclusive
!
interface Port-Channel1
  description LAG to Arista2
  switchport mode tool
  switchport tool group set core-tap-3 core-tap-4
!
...
!
interface Ethernet49/1
  description Core Tap 3-1
  switchport mode tap
  switchport tap default group core-tap-3
!
interface Ethernet50/1
  description Core Tap 3-2
  switchport mode tap
  switchport tap default group core-tap-3
!
interface Ethernet51/1
  description Core Tap 4-1
  switchport mode tap
  switchport tap default group core-tap-4
!
interface Ethernet52/1
  description Core Tap 4-2
  switchport mode tap
  switchport tap default group core-tap-4
!
interface Ethernet53/1
  description LAG to Arista2
  channel-group 1 mode on
  switchport mode tool
!
interface Ethernet54/1
  description LAG to Arista2
```

```

    channel-group 1 mode on
    switchport mode tool
!
interface Management1
    ip address X.X.X.X/Y
!
...
!
ip access-list mgmt
    10 permit ip X.X.X.X/Y any
    30 permit ip host X.X.X.X any
    40 permit ip host X.X.X.X any
    50 deny ip any any
!
...
!
management api http-commands
    protocol https ssl profile eapi
!
management security
    ssl profile eapi
    certificate eapiServerCert key eapiServerKey
!
management ssh
    ip access-group mgmt in
!
end

```

### pulsar-arista7280-2 Configuration

```

! Startup-config last modified at  Fri Jul 12 14:30:18 2019 by admin
! device: pulsar-arista7280-2 (DCS-7280SRA-48C6, EOS-4.20.1F)
!
! boot system flash:/EOS-4.20.1F.swi
!
...
!
load-balance policies
    load-balance sand profile TAP
        fields ipv4 dst-ip src-ip
        fields symmetric-hash
        port-channel ip ip-tcp-udp-header
!

```

```
...

!
tap aggregation
    mode exclusive
!
interface Port-Channel1
    description Taps from core and arista1
    ip access-group bulk_1 in
    ipv6 access-group bulk_1 in
    switchport mode tap
    switchport tap default group TAP
!
interface Port-Channel10
    switchport mode tool
    switchport tool group set TAP
!
interface Ethernet1
    description bro-a000: enp59s0f1
    mtu 9214
    channel-group 10 mode on
!
interface Ethernet2
    description bro-a001: enp59s0f1
    mtu 9214
    channel-group 10 mode on

...

interface Ethernet21
    description bro-a000: enp59s0f0
    mtu 9214
    channel-group 10 mode on
!

...

!
interface Ethernet49/1
    description Core Tap 1-1
    mtu 9214
    channel-group 1 mode on
    switchport mode tap
!
interface Ethernet50/1
    description Core Tap 1-2
    mtu 9214
    channel-group 1 mode on
    switchport mode tap
!
interface Ethernet51/1
    description Core Tap 2-2
    mtu 9214
```

```

    channel-group 1 mode on
    switchport mode tap
!
interface Ethernet52/1
    description Core Tap 2-2
    mtu 9214
    channel-group 1 mode on
    switchport mode tap
!
interface Ethernet53/1
    description LAG to Aristal
    mtu 9214
    channel-group 1 mode on
    switchport mode tap
!
interface Ethernet54/1
    description LAG to Aristal
    mtu 9214
    channel-group 1 mode on
    switchport mode tap
!
interface Management1
    ip address X.X.X.X/Y
!
ip access-list api
!! Access rules for https api
10 permit ip host X.X.X.X any
20 permit ip host Y.Y.Y.Y any
30 deny ip any any
!
ip access-list mgmt
!! Access rules for mgmt interface
10 permit ip host X.X.X.X any
20 permit ip host Y.Y.Y.Y any
30 deny ip any any
!
...
!
management api http-commands
    protocol https ssl profile eapi
    no shutdown
!
    vrf default
        ip access-group api
!
management security
    ssl profile eapi
        certificate eapiServerCert key eapiServerKey
!
management ssh
    ip access-group mgmt in

```



!  
end