AT&T Business

AT&T Switched Ethernet with Network on Demand: Internet EVC configuration guide

January 2021

Technical assistance

This is an AT&T proprietary document developed for use by AT&T customers. For additional technical assistance, contact your AT&T sales team.

Legal disclaimer

This document does not constitute a contract between AT&T and a customer and may be withdrawn or changed by AT&T at any time without notice. Any contractual relationship between AT&T and a customer is contingent upon AT&T and a customer entering into a written agreement signed by authorized representatives of both parties and which sets forth the applicable prices, terms and conditions relating to specified AT&T products and services, and/or, to the extent required by law, AT&T filing a tariff with federal and/or state regulatory agencies and such tariff becoming effective. Such contract and/or tariff, as applicable, will be the sole agreement between the parties and will supersede all prior agreements, proposals, representations, statements or understandings, whether written or oral, between the parties relating to the subject matter of such contract and/or tariff.

Contents

January 8, 2021

AT&T Switched Ethernet with Network on Demand: Internet EVC configuration guide

AT&T Switched Ethernet with Network on Demand℠ (ASEoD) is a transport service that uses AT&T Network on Demand to provision and scale bandwidth and other network services and transmit Ethernet traffic among multiple locations. With ASEoD, you can easily configure and manage your web-based network.

The software-defined and network virtualization technologies that drive AT&T Network on Demand let you manage your Ethernet services and network in near real-time. The service integrates with the Business Center self-service web portal, which allows you to configure Ethernet virtual connections (EVCs), change bandwidth, and view billing information for your Network on Demand sites. The Internet Ethernet virtual connection (IEVC) feature of ASEoD allows you to create a direct, virtual point-to-point connection between your port and the internet.

The service uses a carrier-grade, Multiprotocol Label Switching (MPLS) core network to carry Ethernet traffic between your ports. The service provides industry-standard point-to-point (E-Line) and multipoint (E-LAN) transport models.

About this guide

This guide provides a technical overview of the IEVC feature of ASEoD and includes examples of potential use cases for enterprise networks using ASEoD. These concepts and examples aren't intended to be exhaustive. Use them only as general guidance for designing your network and configuring your customer premises equipment for use with the IEVC feature of ASEoD.

You can refer to the configuration examples as templates to set up basic IEVCs as part of a broader enterprise network design, but this guide isn't intended to be a formal product reference guide.

January 8, 2021

Throughout this guide, we've included examples with Cisco® IOS® configuration commands. We don't require that you use Cisco equipment.

For more information about product availability and limitations, see AT&T Switched Ethernet with Network on Demand: Internet EVC frequently asked questions.

Overview

The IEVC feature of ASEoD allows you to combine private and public internet connectivity together on a single ASEoD connection at a site. Figure 1 provides an overview of an ASEoD with an IEVC.

Note: For simplicity, this is the only figure in this document that shows the network termination equipment (NTE) in particular. Other configurations in this guide include NTE but don't show it in the figures.

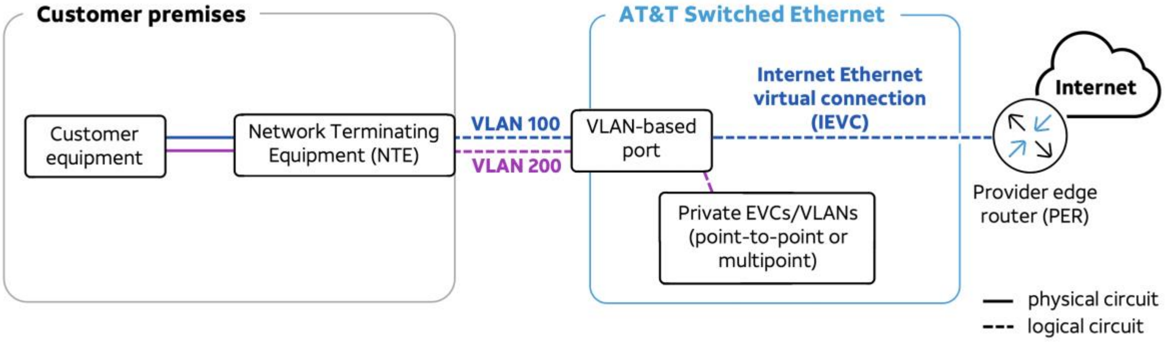

Customer premises
Customer equipment
Network Terminating Equipment (NTE)
VLAN 100
VLAN 200
AT&T Switched Ethernet
VLAN-based port
Internet Ethernet virtual connection (IEVC)
Private EVCs/VLANs (point-to-point or multipoint)
Internet
Provider edge router (PER)
physical circuit
logical circuit

Figure 1 - Overview of ASEoD with an Internet Ethernet virtual connection

We (AT&T) deliver the service to the customer premise at an NTE device. The hand off from the NTE to the customer premises equipment is a standard Ethernet interface using fiber or copper. To terminate the ASEoD, you have a variety of configuration options—routers, switches, or more advanced networking equipment, such as software-defined wide area network (SD-WAN) devices.

You need an ASEoD VLAN-based port to set up an IEVC. VLAN-based ports use 802.1q encapsulation allowing multiple VLANs to share connectivity on a single physical port. You can specify the VLAN tags so they're consistent with your existing numbering schemes.

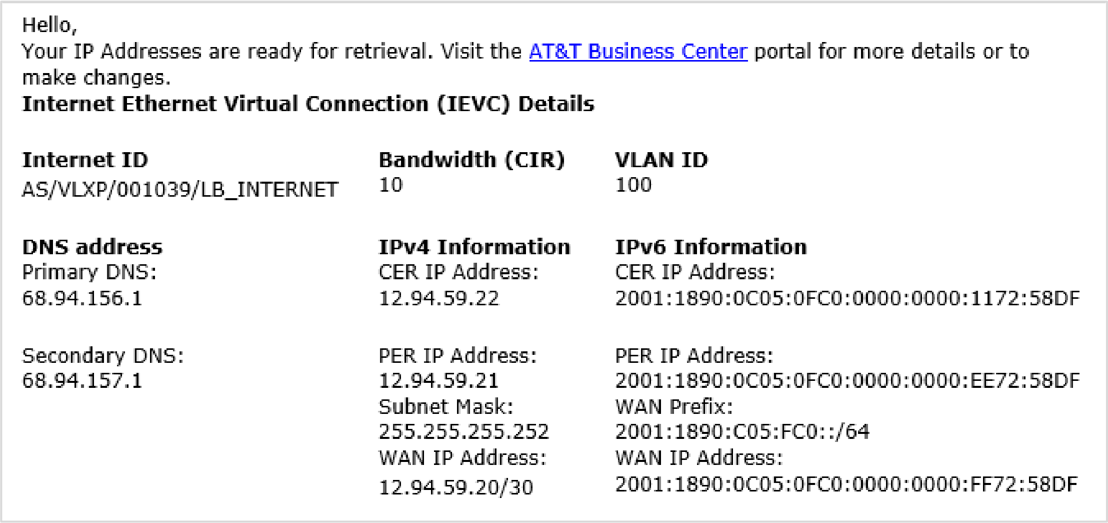
Figure 1 shows a customer site with a private EVC (VLAN 200) and an IEVC (VLAN 100). Each of these virtual connections is a separate VLAN with a unique VLAN ID on the Ethernet handoff to the customer.

For private EVCs, you can have multiple connections, each with a unique ID. You can configure each connection as either point-to-point (a direct, connection to exactly 1 other site) or an multipoint (a connection to multiple other sites).

The IEVC is a single point-to-point connection between the customer premises and the internet. IEVCs are assigned a public address subnet—IPv4/30 and IPv6/64. One host address on the subnet is assigned to the provider edge router (PER) and another host address is assigned to the customer premises equipment (CPE). For all internet traffic from your site, you must use the CPE internet host address as the source IP address. The CPE accomplishes this using a network address translation (NAT) function. The ASEoD IEVC feature doesn't provide any additional public addressing for you. The IEVC is primarily intended for outbound internet access, where communications with internet resources are initiated from within your network.

We provide only the single IP address for the customer end of the IEVC and own that IP subnet. We don't assign you a public IP subnet to use for public applications, nor do we advertise customer-provided IP subnets to the internet using static or BGP routing.

When you order an ASEoD IEVC, we send you an email with your IEVC details, similar to the information shown in Figure 2. You can also access this information in Business Center.



Hello,
Your IP Addresses are ready for retrieval. Visit the AT&T Business Center portal for more details or to make changes.
Internet Ethernet Virtual Connection (IEVC) Details

Internet ID	**Bandwidth (CIR)**	**VLAN ID**
AS/VLXP/001039/LB_INTERNET	10	100
DNS address	**IPv4 Information**	**IPv6 Information**
Primary DNS:	CER IP Address:	CER IP Address:
68.94.156.1	12.94.59.22	2001:1890:0C05:0FC0:0000:0000:1172:58DF
Secondary DNS:	PER IP Address:	PER IP Address:
68.94.157.1	12.94.59.21	2001:1890:0C05:0FC0:0000:0000:EE72:58DF
	Subnet Mask:	WAN Prefix:
	255.255.255.252	2001:1890:C05:FC0::/64
	WAN IP Address:	WAN IP Address:
	12.94.59.20/30	2001:1890:0C05:0FC0:0000:0000:FF72:58DF

Figure 2 - Email with example IEVC details. It includes Internet ID, bandwidth (CIR), VLAN ID, DNS address, IPv4 information, and IPv6 information.

You specify the bandwidth—or committed information rate (CIR)—and the VLAN ID when you order the IEVC. We assign the IEVC a public IPv4 public address, with 1 host assigned to your equipment (CER IP Address) and another host address assigned to the network (PER IP Address). We also assign a public IPv6 address to the IEVC.

Layer 2 switch termination

The simplest way to terminate ASEoD with an IEVC is to use a Layer 2 (L2) switch. Figure 3 provides an example configuration.

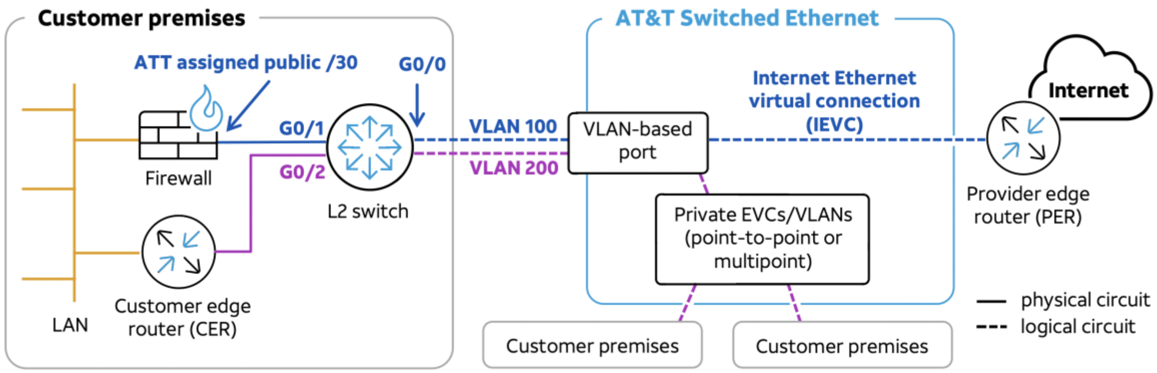


Figure 3 - Example configuration with a Layer 2 switch used to terminate the connection

Layer 2 configuration example

In this configuration example, we terminate the ASEoD connection in a customer edge L2 switch on interface **GigabitEthernet0/1**, or **G0/0**, configured as a trunk that supports 2 VLANs. VLAN 100 goes to the internet, and VLAN 200 is a private EVC that connects to other sites in the customer's network.

Note: You can have multiple private EVCs, but you must configure each private EVC as either a point-to-point or multipoint connection. In Figure 3, the private EVCs are multipoint.

Configuration commands for GigabitEthernet0/0 interface

```
interface GigabitEthernet0/0
 switchport mode trunk
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200
```

On the customer LAN side of the switch, 1 switch interface (**GigabitEthernet0/1**, or **G0/1**) connects to a firewall that terminates the IEVC with **ATT assigned public /30**. Another interface (**GigabitEthernet0/2**, or **G0/2**) connects to a CER that terminates the private EVC.

Configuration commands for GigabitEthernet0/1 and GigabitEthernet0/2 interfaces

```
interface GigabitEthernet0/1
 switchport access vlan 100
```

```
interface GigabitEthernet0/2
 switchport access vlan 200
```

In this configuration, the public IP address is configured on the firewall interface. This address is used (by NAT) for all internet traffic. The firewall should also help assure that the traffic rate transmitted on the interface doesn't exceed the bandwidth ordered for the IEVC.

Layer 3 router termination

Another way you can terminate ASEoD with an IEVC is with a Layer 3 (L3) router. This approach involves a more complicated equipment configuration, but you'll avoid the need for an additional switch. There are many potential configurations to terminate ASEoD with an IEVC with an L3 customer edge router (CER). Figure 4 provides an example of one way to do this.

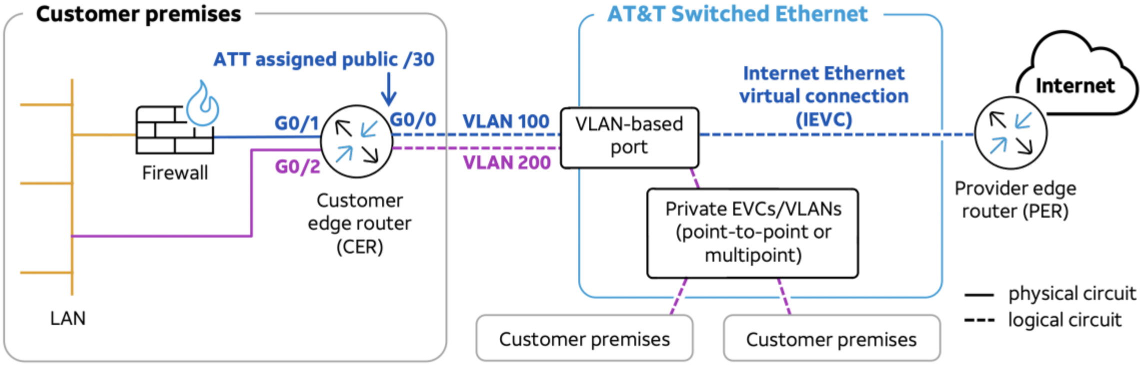


Figure 4 - Example configuration with a Layer 3 router used to terminate the connection

Several basic (global) configuration tasks are required to set up the router for this scenario. The following example steps through these configuration tasks and then shows the basic interface configurations. To address your organization's specific routing and security needs, you may need additional network configuration.

If you want to terminate the AT&T Switched Ethernet Service℠ (ASE) connection on a router, we suggest that you logically separate the private traffic and the internet traffic. If you logically separate the traffic, the internet traffic passes through a security device (such as a firewall) before it reaches the private network. To accomplish this, use a virtual routing and forwarding (VRF) table. By default, the router has a single global routing table, but you can define additional VRFs that restrict traffic to the interfaces or sub-interfaces included in the VRF.

L3 termination example

In this example, we create a VRF called **inet** for the internet traffic and allow the private traffic to remain in the global VRF by default. Later in the example, you associate any interfaces that have internet traffic with the VRF.

Configuration commands to create VRFs

```
! VRFs:
! Use VRF Configuration to keep internet traffic separate from Corporate VPN
!(Corp traffic is in ‘global’ VRF)
ip vrf inet
 description Internet EVC
 rd 212:212  ! rd is a ‘route distinguisher’ It is simply a unique identifier for the VRF
!
```

Set up a traffic shaping policy

You shouldn't exceed the contracted speed for your EVC. To accomplish this, set up a traffic shaping policy for each EVC. These policies are subsequently applied to the appropriate interface or sub-interface. The parameters for the shape average command are:

- **Target rate**—the contracted rate for the EVC
- **Committed burst (Bc)**—should represent approximately 4ms of traffic; for example, [target rate x .0004]
- **Excess burst (Be)**—should always be 0
- **Overhead accounting**—should generally be 24

There are variances in traffic-shaping configuration commands across platforms and software versions. Refer to your specific vendor documentation for details. In this guide, we've used 60Mbps for the private EVC and 10Mbps for the IEVC. In addition, you could configure Class of Service (CoS) policies here to provide priority treatment for a more latency-sensitive application. For more information about how to configure CoS policies in a router, refer to the AT&T Network-Based Class of Service Customer Configuration Guide.

Configuration commands to set up a traffic shaping policy

```
! Traffic shaping
! Traffic shaping required for each EVC/VLAN based on provisioned CIR for the VLAN
policy-map 60M-Rate-Shape
 class class-default
  shape average 60000000 240000 0 account user-defined 24
!
policy-map 10M-Rate-Shape
 class class-default
  shape average 10000000 40000 0 account user-defined 24
```

```
!
```

For the IEVC, a static default route is provided within the **inet** VRF. The default route forwards any traffic it receives from the firewall toward the internet. For the default route, the destination address is the AT&T public network address, provided during the provisioning process.

The routing configuration for a private EVC isn't shown here. The configuration depends on the specific customer design and how various sites exchange routing with each other.

Configuration commands for routing

```
! Routing
! Static default route toward internet for the 'inet' VRF
! Next hop is the supplied IPv4 PER address
ip route vrf inet 0.0.0.0 0.0.0.0 12.94.59.21 name Default_to_Internet
!
```

Set source IP address with Network Address Translation

All traffic going toward the internet on the IEVC must use the AT&T assigned public IP address as the source IP address. You set this up by configuring network address translation (NAT) in the CER. The source IP address of any traffic from the firewall is changed to the AT&T public address, and return traffic is restored to its original address.

Configuration commands for NAT

```
! NAT
 IP NAT inside source list Local-nets interface G0/0.100 overload
!
  ip access-list standard Local-nets
   permit any
```

Configure the WAN interfaces

The wide area network (WAN) interface is the interface to the ASEoD service. The interface in this example is **GigabitEthernet0/0**. It's configured as a trunk (802.1q encapsulation) and supports 2 sub-interfaces. The first sub-interface is VLAN 100, which is the IEVC. The sub-interface configuration provides the VLAN ID, the assigned AT&T public IP address, the NAT policy, and the 40Mbps traffic shaper. The customer assigns the sub-interface to the **inet** VRF to keep this traffic separate from the private traffic in the global routing table in the CER.

Configuration commands for WAN interfaces and Internet EVC

```
! WAN interfaces
interface GigabitEthernet0/0
 description ASE VLAN-based interface
 no ip address
 duplex full
 speed 1000
!
! VLAN 100 for Internet EVC
interface GigabitEthernet0/0.100
 description VLAN100 to AT&T Internet
 encapsulation dot1Q 100
 ip vrf forwarding inet
 ip address 12.94.59.22 255.255.255.252  ! CER Public IP Address
 ip nat outside
 service-policy output 10M-Rate-Shape
!
```

The second sub-interface is for the private EVC. The IP address assigned here is from the customer’s private addressing plan. The configuration also provides the VLAN tag and the 60Mbps traffic shaper.

Configuration commands for private EVC

```
! VLAN 200 for private EVC
interface GigabitEthernet0/0.200
 description VLAN200 to Private Corporate EVC
 encapsulation dot1Q 200
 ip address 10.101.1.1 255.255.255.0
 service-policy output 60M-Rate-Shape
```

In this example, there are 2 separate physical LANs interfaces. One is for the internet traffic to the firewall; the other is for the private site LAN.

Encapsulation on these interfaces depends on the details of the customer site. For this example, the internet port is shown with **802.1q encapsulation** and the private LAN connection is shown as **untagged/ARPA**.

Configuration commands for LAN interfaces

```
! LAN interfaces
! Example here shows separate physical interfaces.
! Actual interface assignment and encapsulation details are per customer
environment/requirements.
!
interface GigabitEthernet0/1
 description Customer connection to firewall
 no ip address
 duplex auto
 speed auto
!
```

```
interface GigabitEthernet0/1.100
 description Firewall ←→ CER VLAN
 encapsulation dot1Q 100
 ip vrf forwarding inet
 ip address 192.168.1.1 255.255.255.0 ! Private IP peering with other site(s) across ASEoD
 ip nat inside
!
interface GigabitEthernet0/2
 description Customer LAN connection
 ip address 10.100.1.1 255.255.255.0 ! Directly attached customer LAN segment
 duplex auto
 speed auto
!
```

Firewall configuration

Specific firewall configuration templates are beyond the scope of this guide. Vendor implementations and corporate security policies are too varied to provide a simple template. Functionally, the main requirement for this scenario is that traffic traversing the firewall is NATed to the private IP subnet connecting the firewall and the CER.

Note: Because the traffic is translated to the public address in the CER, you don't necessarily have to NAT the traffic through the firewall. If you choose to forgo NATing the traffic through the firewall, then you must augment the routing in the **inet** VRF of the CER to forward return traffic from the internet to the site LANs behind the firewall.

Other configuration approaches

As noted earlier, there are many other configuration approaches if you want to use an L3 CER to terminate the ASEoD connection. To see one of these configurations, see the Layer 3 router with a zone-based firewall termination section.

You could also configure a switch virtual interface (SVI) to terminate the IEVC. This method allows the traffic to pass directly through the router. In this scenario the firewall is on the LAN side of the router and uses the **ATT assigned public /30** CER IP address.

Layer 3 router with a zone-based firewall termination

This example also terminates the ASEoD connection into an L3 router. In the previous example, internet traffic was kept segregated and forwarded to a separate, external firewall. In this example, the built-in zone-based firewall capabilities of the router are used to provide the security function. Figure 5 shows a network diagram of this approach.

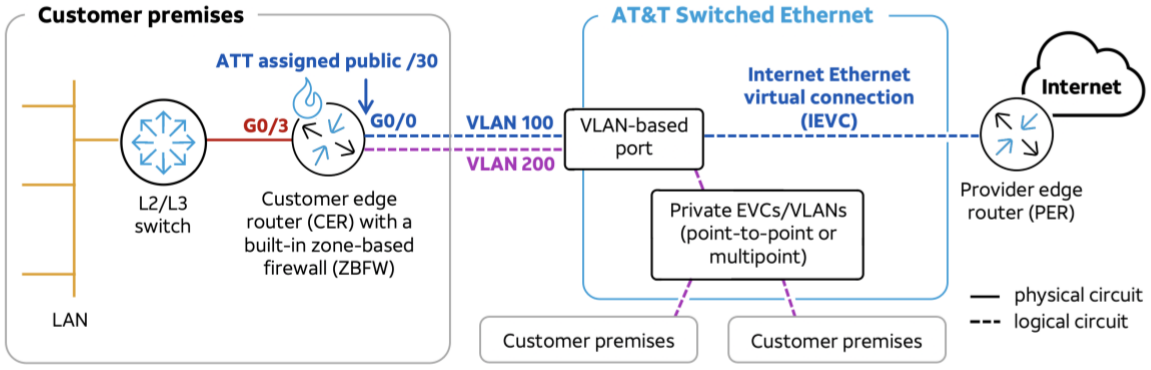


Figure 5 - Example configuration with a Layer 3 router with a built-in zone-based firewall used to terminate the connection

In this solution, both the IEVC and the private EVCs are terminated in the L3 router. The internet traffic is passed through a zone-based firewall to provide a basic security function. Then the firewalled internet traffic and the private network are combined onto the site LAN interface.

The following is an example configuration and isn't intended to address any specific corporate security policies. It allows internal users to access resources on the internet and doesn't permit any traffic sessions initiated from the internet toward the customer site.

Zone-based firewall configuration example

Configuration of the zone-based firewall (ZBFW) consists of the following steps:

1. Configure class-maps. Class-maps identify what traffic types are allowed by any specific policy within the firewall. For this example, we have a single class-map called **allowed-protocols** that permits any User Datagram Protocol (UDP), Transmission Control Protocol (TCP), or Internet Control Message Protocol (ICMP) traffic to pass through the zone-based firewall.

   Configuration commands to define class-maps

   ```
   ! Define class-maps
   class-map type inspect match-any allowed-protocols
    description Allows All traffic out
     match protocol udp
     match protocol tcp
     match protocol icmp
   !
   ```

2. Define policy-maps. Policy-maps reference the class-maps and create policies that allow or block traffic based on how you define class-map. A given policy-map can reference 1 or more class-maps. A policy-map typically references the built-in class-

map **class-default** as the last entry. **class-default** handles any traffic that doesn't match an earlier class-map reference and typically drops it. In this example, we have a single policy called **INSIDE-TO-OUTSIDE** that forwards traffic based on the **allowed-protocols** class-map.

Configuration commands to define policy-maps

```
policy-map type inspect INSIDE-TO-OUTSIDE
 class type inspect allowed-protocols
  inspect
 class class-default
  drop
!
```

3. Create zones and apply the policy-maps to define how traffic is managed between zones. Then, create a zone pair (ZP) called **ZP-inside-to-outside** and apply a policy. In this example, we defined 2 zones—**OUTSIDE** and **INSIDE**. The source zone is **INSIDE** and the destination zone is **OUTSIDE**. Then we applied a policy to the **INSIDE-TO-OUTSIDE** zone pair.

Configuration commands to create zones and apply policy-maps

```
zone security OUTSIDE
 description Internet
zone security INSIDE
 description inside
zone-pair security ZP-inside-to-outside source INSIDE destination OUTSIDE-Internet
 service-policy type inspect INSIDE-TO-OUTSIDE
!
```

4. Assign router interfaces to one of the defined zones. The customer LAN and the private ASEoD EVC are assigned to **INSIDE**. The ASEoD IEVC is assigned to **OUTSIDE**. The result is that any UDP, TCP, or ICMP traffic initiated from these interfaces is allowed to communicate with the internet. Any inbound session or other traffic is blocked.

   Similar to the L3 termination example, the ASEoD IEVC is configured with the public CER IP address, and all traffic out the interface is NATed to that address. And, for the WAN interfaces, you must configure appropriate traffic shaping. For details on NAT and traffic-shaping configurations, see the L3 termination example.

Configuration commands to assign interfaces to a zone

```
interface GigabitEthernet0/3
 description Local LAN segment in ‘INSIDE’ zone
 ip address 10.1.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 zone-member security INSIDE
!
interface GigabitEthernet 0/1
 no ip address
!
interface GigabitEthernet0/1.100
 description ASEoD Internet P2P EVC in ‘OUTSIDE’ zone
 encapsulation dot1Q 100
 ip address 12.94.59.22 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 service-policy output 10M-Rate-Shape
 zone-member security OUTSIDE-Internet
!
interface GigabitEthernet0/1.200
 description ASE Connection - Private EVC in ‘INSIDE’ zone
 encapsulation dot1Q 200
 ip address 10.1.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 service-policy output 60M-Rate-Shape
 zone-member security INSIDE
```

IMPORTANT: As noted earlier, this is a basic configuration for a zone-based firewall (ZBFW). There is a built-in zone called **Self** that applies specifically to any resource within the router itself, including directly-attached interfaces. To avoid potential attacks on the CER, we suggest that, at a minimum, you apply additional policies to restrict or block inbound connections to the **Self** zone.

SD-WAN termination

Another potential use for the IEVC is with a software-defined wide-area network (SD-WAN). Configuration details vary considerably across various SD-WAN vendors but are typically accomplished by using a centralized portal. Figure 6 shows a basic configuration that uses an SD-WAN device to terminate the ASEoD connection.

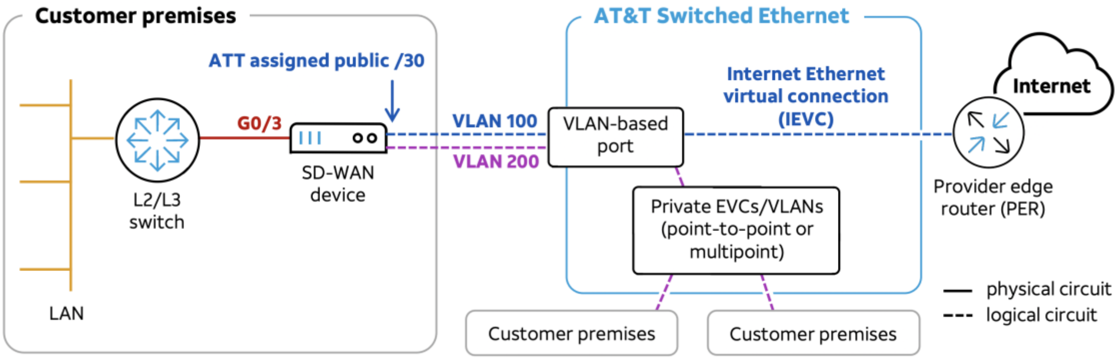


Figure 6 - Example configuration with an SD-WAN edge device used to terminate the connection

Benefits of IEVC with SD-WAN

The IEVC capability can provide several benefits for SD-WAN deployments.

Provide internet-based portals

Portals used for SD-WAN are typically internet-based. Access to the portal is needed for configuration, monitoring, and ongoing operation of these networks. For SD-WAN deployed primarily on private transport networks, access to the internet-based portals can be difficult because access involves backhaul of portal traffic to centralized sites for redirection to the internet.

Remove need to backhaul internet traffic to centralized locations

If you don't want to backhaul portal traffic, the ASEoD IEVC is a simple way to get that direct, local internet access.

You can also use the IEVC to connect local users to the internet. You'll want to secure the site with built-in zone-based firewalls, separate or integrated advanced firewalls, or cloud-based security services.

Reduce cost and scale

Enterprises are increasingly moving applications from their own data centers into public cloud infrastructures, which provide compelling costs and scale benefits. Like direct internet access, the IEVC can allow direct access from a remote site directly to cloud-based applications, avoiding backhaul through centralized locations. This setup can provide better performance and availability for cloud-based applications.

Optimize performance and reliability

SD-WAN often uses multiple transport networks with dynamic path selection to optimize performance and enhance system reliability. IEVCs can provide some minor benefit in this sense. Because private EVCs and IEVCs are delivered as part of a common access circuit, they're vulnerable to more single points of failure than are present if a separate physical internet service is deployed. One way you can use IEVCs and still mitigate the single failure point is to augment with a third transport using wireless services. Wireless services are generally easy to add to SD-WAN designs and help provide effective protection against failure of terrestrial-based transport services. When you use wireless services along with the ASEoD IEVC, the IEVC can be more cost effective, while SD-WAN, reserves the pricier usage-based wireless connection strictly for backup scenarios.

In cases where a separate, physical internet connection is needed, you can use the IEVC as a temporary internet service until you migrate to a separate physical internet service.

Acronyms

ASE—AT&T Switched Ethernet Service
ASEoD— AT&T Switched Ethernet with Network on Demand
CER—customer edge router
CIR—committed information rate, or bandwidth
CPE—customer premise equipment
E-line—a direct, point-to-point connection
E-LAN—an extended local area network.
EVC—ethernet virtual connection
ICMP—Internet Control Message Protocol
IEVC—Internet Ethernet virtual connection
IP—Internet Protocol
IPv4—Internet Protocol version 4
IPv6—Internet Protocol version 6
LAN—local area network
L2—Layer 2
L3—Layer 3
MPLS—Multiprotocol Label Switching
NAT—network address translation
NTE—network termination equipment
P2P—point-to-point
PER—provider edge router
SD-WAN—software-defined-wide area network
SVI—switch virtual interface
TCP—Transmission Control Protocol
UDP—User Datagram Protocol
VLAN—virtual local area network
VRF—virtual routing and forwarding

WAN—wide area network
ZBFW—zone-based firewall
ZP—zone pair