

How To | Configure loopback interfaces on Allied Telesyn devices

Introduction

From software version 2.7.1 onwards, the loopback interface is explicitly supported. For earlier software versions, a workaround was required in order to configure loopback interfaces.

What information will you find in this document?

This document begins by describing the advantages of loopback interfaces and how to configure them with version 2.7.1 and above. This is followed by a description of how applications can make use of the loop back interface. Finally, there is a brief description of the workaround used on older versions.

Which product and software version does this information apply to?

The information provided in this document applies to:

- **Products:** AR400 Series, AR700 Series, Rapier, AT-8800 Series, AT-8900 Series, AT-9800 Series, AT-9900 Series, SwitchBlade
- **Software release(s):** 2.7.1+

Advantages of using loopback interfaces

A loopback interface (actually, in Alliedware, they are referred to as "local" interfaces) is one that is always available for higher layer protocols to use and advertise to the network. Although a local interface is assigned an IP address, it does not have the usual requirement of connecting to a lower layer physical entity. This lack of physical attachment creates the perception of a local interface always being accessible via the network.

Local interfaces can be utilised by a number of protocols for various purposes. They can be used to improve access to a switch, as well as increasing its reliability, security, scalability, and protection. In addition, local interfaces can add flexibility and simplify management, information gathering, and filtering.

One example of this increased reliability is for OSPF to advertise a local interface as a interface-route into the network, irrespective of the physical links that may be "up" or "down" at the time. This provides a higher probability that the routing traffic will be received and subsequently forwarded. Further reliability and performance could be provided by configuring parallel BGP paths to a local interface on a peer device, which would result in improved load sharing.

Access and security can be improved through filtering. Incoming traffic can be filtered by rules that specify local interfaces as the only acceptable destination addresses.

Information gathering and filtering as well as management can potentially be simplified if protocols such as SNMP use local interfaces for receiving and sending trap and log type information.

Configuring loopback (local) interfaces

A local interface can be added to the router/switch using the command:

```
ADD IP LOCAL=[1..15] [FILTER={filter-number|NONE}] [GRE=[0..100  
NONE}] [IPADDRESS=ipadd] [POLICYFILTER={filter-number|  
NONE}] [PRIORITYFILTER={filter number|NONE}]
```

Up to fifteen local interfaces can be added to a single device. These are in addition to the default local interface that is automatically added at start up, and can be configured through the 'set ip local' command.

So, it is important to note that the default local interface has not been replaced by the local interfaces added by the 'add ip local' command. The interfaces added by the 'add IP local' command are additional local interfaces.

A local interface is virtual in the sense that it is not associated with a physical interface. Each local interface can be assigned an IP address, which can then be used as the source address of IP packets generated internally by IP protocols such as PIM, Radius, SNMP, and BGP.

General rules for determining the source IP address that will be used by a particular protocol

There are a number of different higher layer protocols that can be enabled on a device running AlliedWare. Some of these protocols can explicitly set a local interface to use as the source IP address for the protocol. For other protocols, there is an implicit method used to choose the source IP address.

The following rules are used to determine which IP address to use as the source address:

1. If the higher layer protocol's configuration specifies the use of either a source IP address or a local interface, then the configured address is used as the packet's source IP address. For example, the 'sipaddress' parameter of the ping command specifies the source IP address to be used in ping packets. While the local parameter of the 'add bgp peer' command specifies a local interface to use as the source IP address for communication to that BGP peer.
2. If a higher layer protocol has not, or cannot, be assigned an explicit source IP address to use, then:
 - If the default local interface has been assigned an IP address, then this will be used as the packet's source IP address.
 - Otherwise, the IP routing module determines the interface over which the packet is to be transmitted, and assigns the IP address of that interface as the packet's source IP address.

Configuring a higher layer protocol to use a local interface for its source IP address

The following commands can be used to set the local interface to be used as the source IP address for various higher layer protocols within the device:

SNMP

```
SET SNMP LOCAL={none|1..15}
```

BGP

```
ADD BGP PEER=ipadd <other parameters> [LOCAL={NONE|1..15}]
```

```
SET BGP PEER=ipadd [LOCAL={NONE|1..15}]
```

Radius

```
ADD RADIUS SERVER=ipadd <other parameters> [LOCAL={NONE|1..15}]
```

PIM

```
ADD PIM BSRCANDIDATE <other parameters> [INTERFACE={localinterface|
vlan-interface}]
```

```
ADD PIM RPCANDIDATE <other parameters> [INTERFACE={local-interface|
vlan-interface}]
```

```
ADD PIM RPCANDIDATE <other parameters> [INTERFACE={local-interface|
vlan-interface}]
```

TACACS+

```
ADD TACPLUS SERVER=ipaddress <other parameters> [LOCAL={NONE|1..15}]
```

```
SET TACPLUS SERVER=ipaddress [LOCAL={NONE|1..15}]
```

Syslog

```
Create log output =<number> dest=syslog <other parameters>
[LOCAL={NONE|1..15}]
```

Interaction of OSPF with the local interface

Whilst it is not possible (or even necessary) to configure OSPF to use a local address as the source address, it is possible to configure OSPF to advertise a local interface into the OSPF network, so that the management IP address represented by the local IP is advertised. The way in which OSPF advertises local interface addresses can vary depending on the configuration.

Let us look at the different cases.

1. The IP address on the Local interface belongs to a configured OSPF range

The local interface routes are advertised in router LSA if they belong to an OSPF range that has been configured on the device.

For example, if the configuration is as below:

```
enable ip
add ip local=1 ip=192.168.2.1
add ip local=2 ip=10.10.10.10
add ip int=vlan1 ip=192.168.1.1 mask=255.255.255.0

enable ospf
add ospf area=0.0.0.0
add ospf range=192.168.0.0 mask=255.255.0.0 area=0.0.0.0
add ospf range=10.10.10.0 mask=255.255.255.0 area=0.0.0.0
add ospf int=vlan1 area=0.0.0.0
```

then the local interfaces are included in the router LSA as stub links.

2. The IP address does not belong to a configured range on an AS border router.

The local interface routes are advertised as an AS External LSA if they don't belong to any configured OSPF range and router is AS boundary router.

For example, if the configuration is as below (note - the command `set ospf asexternal=on` configures the router to be an area-border router):

```
enable ip
add ip local=1 ip=192.168.2.1
add ip local=2 ip=10.10.10.10
add ip int=vlan1 ip=192.168.1.1 mask=255.255.255.0

enable ospf
set ospf asexternal=on
add ospf area=0.0.0.0
add ospf range=192.168.1.0 mask=255.255.255.0 area=0.0.0.0
add ospf range=10.10.10.0 mask=255.255.255.0 area=0.0.0.0
add ospf int=vlan1 area=0.0.0.0
```

Then the LSA for 192.168.2.1 will be advertised as an AS-External LSA; and the LSA for 10.10.10.10 will be included in the router LSA as a stub link.

The workaround used with older versions of software

To create a loopback interface you must firstly create a PPP interface that goes nowhere, then attach an IP address to that interface. If the PPP interface is configured as on-demand, i.e. it can be activated when traffic is to be sent to it, then the IP stack will treat it as an "always-up" interface. Even if the interface is not actually up, it is still 'available' as an interface that traffic can be sent to - because theoretically it will go up when traffic is sent to it. For example, a PPPoE interface could be created, with no intention to connect to an access concentrator, but just as an interface to attach an IP address to.

The commands are:

```
create ppp=0 over=eth0-any idle=on
add ip int=ppp0 ip=192.168.10.1
```