The Loopback Interface

ISP/IXP Workshops

© 2004, Cisco Systems, Inc. All rights reserved.

Overview

- Requires IOS 11.1CC or 12.0 trains
  - ISP software trains
- Covers router access, security, information gathering, configuration and scalability.

© 2004, Cisco Systems, Inc. All rights reserved.

Motivation

- Most ISPs make use of the router loopback interface.
- IP address configured is a host address
- Configuration example:

```
interface loopback 0
 description Loopback Interface of CORE-GW3
 ip address 215.18.3.34 255.255.255.255
```

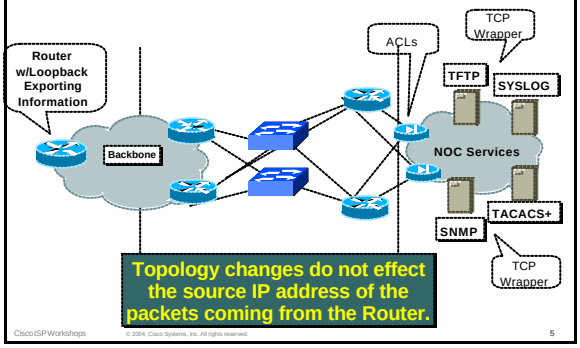

© 2004, Cisco Systems, Inc. All rights reserved.

Motivation

- Loopback interfaces on ISP backbone usually numbered:
  - out of one contiguous block, or
  - using a geographical scheme, or
  - using a per PoP scheme
- Aim is to aid recognition and improve security

© 2004, Cisco Systems, Inc. All rights reserved.

Loopback Interface



© 2004, Cisco Systems, Inc. All rights reserved.

Motivation

With routers using a loopback address as the source for all IP packets originating from the router, it becomes very easy to construct appropriate filters to protect management systems in the ISP's network operation centres

© 2004, Cisco Systems, Inc. All rights reserved.

Router Access

© 2004, Cisco Systems, Inc. All rights reserved.

Accessing the Router

- Put mapping of the router loopback address to router name into forward and reverse DNS.
- Telnet to router using loopback address, not interface address. ISP routers usually have multiple external paths and many interfaces.
- DNS Configuration example:

```
core-gw3    A    215.17.1.8 ; Loopback of router gw3
```


© 2004, Cisco Systems, Inc. All rights reserved.

Remote access using Telnet

- Remote access from the router using familiar telnet
- Configure telnet so that the loopback address is used in packets originating from the router
- Configuration example:

```
ip telnet source-interface Loopback0
```


© 2004, Cisco Systems, Inc. All rights reserved.

Remote access using RCMD

- Remote access from router using Unix style “rcmd”
- Configure RCMD so that the loopback address is used in packets originating from the router
- Configuration example:

```
ip rcmd source-interface Loopback0
```


© 2004, Cisco Systems, Inc. All rights reserved.

Security

© 2004, Cisco Systems, Inc. All rights reserved.

Management User Authentication

- TACACS+ distributed authentication system for management access to routers
- Configure TACACS+ so that the loopback address is used in packets originating from the router
- Configuration example:

```
ip tacacs source-interface Loopback0
tacacs-server host 215.17.1.1
```


© 2004, Cisco Systems, Inc. All rights reserved.

Management User Authentication

- **Motivation – Aid Server Security:**

  TACACS+ servers can be protected by filters which only allow TACACS+ port to be accessed from loopback address block

- **Motivation – Easy to read/process logs:**

  TACACS+ log records have the loopback address recorded as source address, not the egress interface.

© 2004, Cisco Systems, Inc. All rights reserved.

RADIUS User Authentication

- **RADIUS distributed authentication system for dial user access to routers**
- **Configure RADIUS so that the loopback address is used in packets originating from the router**
- **Configuration example:**

```
ip radius source-interface Loopback0
radius-server host 215.17.1.1
    auth-port 1645 acct-port 1646
```


© 2004, Cisco Systems, Inc. All rights reserved.

RADIUS User Authentication

- **Motivation – Aid Server Security:**

  RADIUS servers and proxies can be protected by filters which only allow RADIUS ports to be accessed from loopback address block

- **Motivation – Easy to read/process logs:**

  RADIUS log records have the loopback address recorded as source address, not the egress interface.

© 2004, Cisco Systems, Inc. All rights reserved.

Recording Information

© 2004, Cisco Systems, Inc. All rights reserved.

Exporting NetFlow records

- **Exporting Cisco NetFlow statistics to a NetFlow Collector system**
- **Configure NetFlow export so that the loopback address is used in packets originating from the router**
- **Configuration example:**

```
ip flow-export source Loopback0
```


© 2004, Cisco Systems, Inc. All rights reserved.

Exporting NetFlow records

- **Motivation – Aid Server Security:**

  NetFlow collector can be protected by filters which only allow the specified flow port to be accessed from loopback address block

© 2004, Cisco Systems, Inc. All rights reserved.

Logging Information

- Send logging information to a Unix or Windows SYSLOG server.
- Log packets leave router with loopback interface address as source
- Configuration example:

```
logging source-interface loopback0
```


© 2004, Cisco Systems, Inc. All rights reserved.

Logging Information

- Motivation – Aid Server Security:

  SYSLOG servers and proxies can be protected by filters which only allow the syslog port to be accessed from the loopback address block
- Motivation – Easy to read/process logs:

  SYSLOG records have the loopback address recorded as source address, not the egress interface.

© 2004, Cisco Systems, Inc. All rights reserved.

Network Time Protocol

- Network Time Protocol (NTP) used to synchronize the time on all the devices.
- NTP packets leave router with loopback address as source
- Configuration example:

```
ntp source loopback0
ntp server 169.223.1.1 source loopback 1
```


© 2004, Cisco Systems, Inc. All rights reserved.

Network Time Protocol

- Motivation – NTP Security:

  NTP systems can be protected by filters which only allow the NTP port to be accessed from the loopback address block
- Motivation – Easy to understand NTP peerings:

  NTP associations have the loopback address recorded as source address, not the egress interface.

© 2004, Cisco Systems, Inc. All rights reserved.

SNMP

- If SNMP is used, send traps from router using loopback address as source.
- Configuration example:

```
snmp-server trap-source Loopback0
snmp-server host 169.223.1.1 community
```


© 2004, Cisco Systems, Inc. All rights reserved.

SNMP

- Motivation – Aid SNMP Server Security:

  SNMP management systems can be protected by filters which only allow the SNMP port to be accessed from the loopback address block
- Motivation – Easy to read/process trap information:

  SNMP traps have the loopback address recorded as source address, not the egress interface.

© 2004, Cisco Systems, Inc. All rights reserved.

Core Dumps

- *Core dump* feature allows routers to transfer an image of memory to a specified FTP server in case of a crash.
- Configure core dumps to use the loopback interface address as source.
- Configuration example:

```
ip ftp source-interface loopback 0
exception protocol ftp
exception dump 169.223.32.1
```


© 2004, Cisco Systems, Inc. All rights reserved.

Core Dumps

- Motivation – Core Dump FTP Server Security:
  - FTP server used for core dumps can be protected by filters which only allow the FTP port to be accessed from the loopback address block
  - This FTP server should NOT be visible to the public

© 2004, Cisco Systems, Inc. All rights reserved.

Configuration and Scalability

© 2004, Cisco Systems, Inc. All rights reserved.

Configuration using TFTP

- Configuring the router using TFTP from tftp server
- Saving router configuration to a tftp server
- Configure TFTP so that the loopback address is used in packets originating from the router
- Configuration example:

```
ip tftp source-interface Loopback0
```


© 2004, Cisco Systems, Inc. All rights reserved.

Configuration using TFTP

- Motivation – Aid TFTP Server Security:
  - TFTP server used to store configurations and IOS images can be protected by filters which only allow the TFTP port to be accessed from the loopback address block
  - This TFTP server should NOT be visible to the public

© 2004, Cisco Systems, Inc. All rights reserved.

Interface Configuration

- "ip unnumbered"
  - no need for an IP address on point-to-point links
  - keeps IGP small
- Configuration example:

```
interface loopback 0
 ip address 215.17.3.1 255.255.255.255
!
interface Serial 5/0
 ip unnumbered loopback 0
!
ip route 215.34.10.0 255.255.252.0 Serial 5/0
```


© 2004, Cisco Systems, Inc. All rights reserved.

Router ID

- If the loopback interface exists and has an IP address, that is used as the router ID in routing protocols – stability!
- If the loopback interface does not exist, or has no IP address, the router ID is the highest IP address configured – danger!
- If multiple loopback interfaces exist, and have IP addresses configured, then the highest IP address is chosen as the router ID

© 2004, Cisco Systems, Inc. All rights reserved.

Stable iBGP configuration

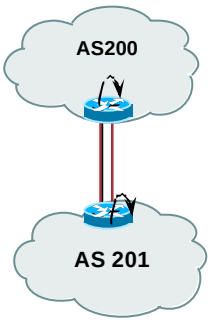
- Use loopback interface
  - it never goes away
  - ISP routers usually have multiple external paths
- Configuration example:

```
interface loopback 0
 ip address 215.17.1.34 255.255.255.255
router bgp 200
 neighbor 215.17.1.35 remote-as 200
 neighbor 215.17.1.35 update-source loopback 0
```


© 2004, Cisco Systems, Inc. All rights reserved.

Multiple parallel eBGP Sessions

- eBGP to loopback addresses
- eBGP prefixes learned with loopback address as next hop
- parallel paths to loopback address allows load-sharing



© 2004, Cisco Systems, Inc. All rights reserved.

Summary

- Loopback interface is not “redundant” or “superfluous”
- Multitude of uses to ease security, access, management, information and scalability of router and network
- Protects the ISP’s Management Systems
- Use the loopback!

© 2004, Cisco Systems, Inc. All rights reserved.

Cisco Systems

Empowering the Internet Generation℠