A.H. TECHNOLOGY PTY LTD
www.ahtechnology.com.au info@ahtech.com.au
Phone: 61-3-9885-4877. Fax: 61-3-8678-0665
P.O. Box 205, Malvern, Vic., Australia, 3144
ABN: 37508872528

Subnet-Directed Broadcast

In response to clients' inquiries about Subnet-Directed Broadcast, we have collated a number of public domain articles that discuss different aspects of using of subnet-directed broadcast for waking up PCs in remote subnets.

have collated a number of articles about the subject.

The Information contained in this document is of general nature. Before making any changes to your environment, based on this article, readers must ensure that the information is relevant to their environment.

Please note that you can get to the original information by clicking on the title

Juniper Recommends

"… Note: We recommend that you do not enable IP directed broadcast on subnets that have a direct connection to the Internet because of increased exposure to denial-of-service (DoS) attacks."

Recommended ISP Security Services and Procedures

Status of this Memo

> This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Extract of

4.6 Directed Broadcast

The IP protocol allows for directed broadcast, the sending of a packet across the network to be broadcast on to a specific subnet. Very few practical uses for this feature exist, but several different security attacks (primarily Denial of Service attacks making use of the packet multiplication effect of the broadcast) use it. Therefore, routers connected to a broadcast medium SHOULD NOT be configured to allow directed broadcasts onto that medium.

Securing Cisco Routers with No IP Directed-Broadcast

February 3rd, 2008 •

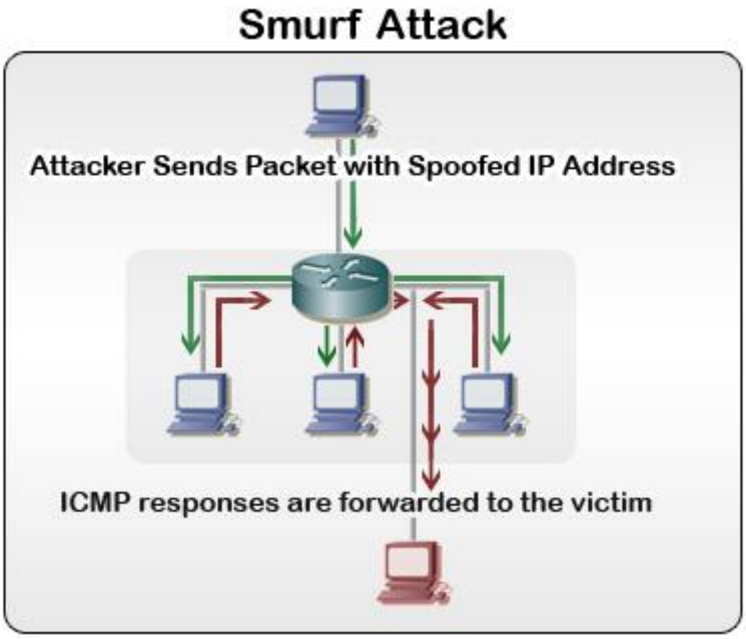
One of several overlooked commands that can produce a world of hurt for networks is the IP Directed-broadcast command. This command was introduced in Cisco's routers at IOS version 10. Cisco soon realized that this command was being maliciously exploited in denial of service attacks, and action had to be taken- particularly against smurf attacks.

How a Smurf Attack Works

Smurf attacks are a type of denial of service attack, in which the Internet Control Message Protocol (ICMP) and broadcasts are being exploited. Normal ICMP requests (commonly referred to as pings) are used to verify network connectivity. But since they require a response from the target machine, they can maliciously be used to consume network resources if many are sent at once.

Broadcasts come into the equation, however, since they give capability to send requests to every computer on a network. Obviously if a broadcast were to be sent multiple times, the traffic would slow down the network. Imagine 100 computers sending back an ICMP request at the same time- network performance would take a huge dip.

It should be noted that smurf attacks work via an attacker spoofing the IP address of the broadcast. The IP address is actually the IP address of the victim the attacker chooses. When every computer on the network responds to the ICMP request, all of these requests go to the computer the attacker borrowed the IP address from. In this instance, the network only acts as an amplifier to the attack, not necessarily the victim.

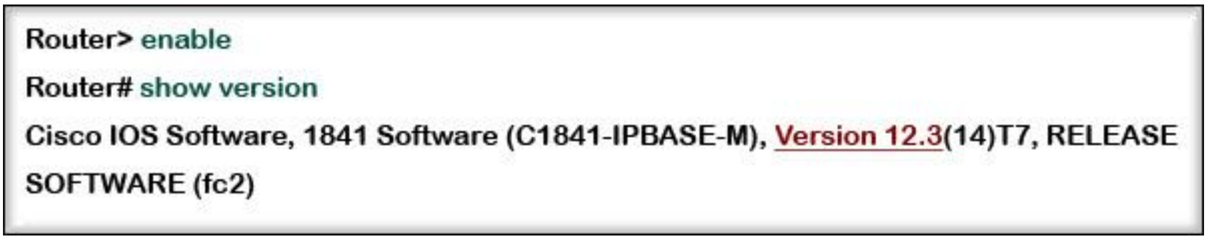

Smurf Attack
Attacker Sends Packet with Spoofed IP Address
ICMP responses are forwarded to the victim

Unfortunately, smurf attacks leave little room for victims to recover from an attack. Instead, the attack must be staved off at the network level via filtering. We can do this specifically through the no ip directed-broadcast command in Cisco routers.

No IP Directed-Broadcast

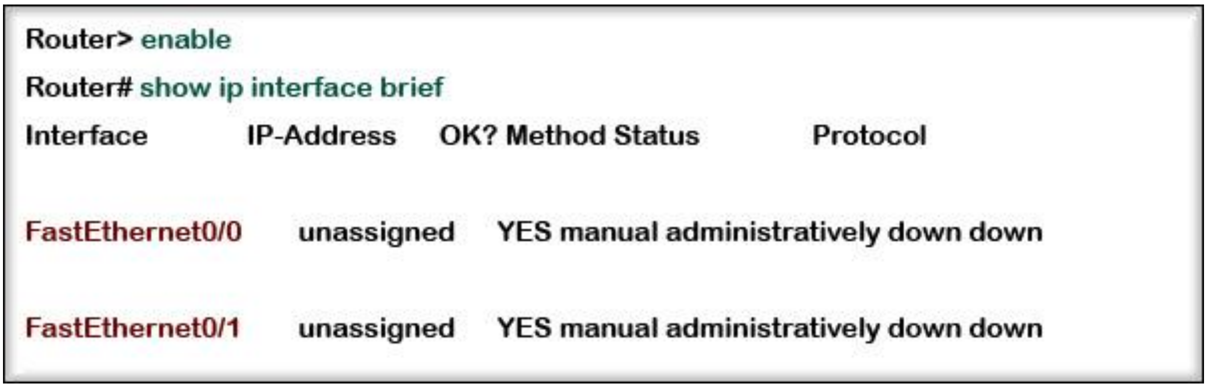
An IP Directed-Broadcast is simply an IP packet, of which has a destination address of a particular IP subnet. The broadcast in this instance is sent from a different network, as one could probably guess from the command name. (The broadcast is being directed via IP, not a unicast address.)

Keep in mind that if you are running a Cisco IOS version 12.0 or above, you do not need to follow these steps. No IP Directed-Broadcast was enabled by default after IOS 12.0. It is strongly recommended that No IP Directed-Broadcast be enabled if your IOS version is below 12.0. If you aren't sure which version you have, simply type in the following commands from user exec mode:



```
Router> enable
Router# show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7, RELEASE
SOFTWARE (fc2)
```

As you can tell in the above example, the version number is higher than 12.0. In this instance, we would not need to take further action. If the number happens to be below 12.0, then you will need to apply the No IP Directed-Broadcast command. First, you should find out the naming convention for your router's interfaces, as show below.

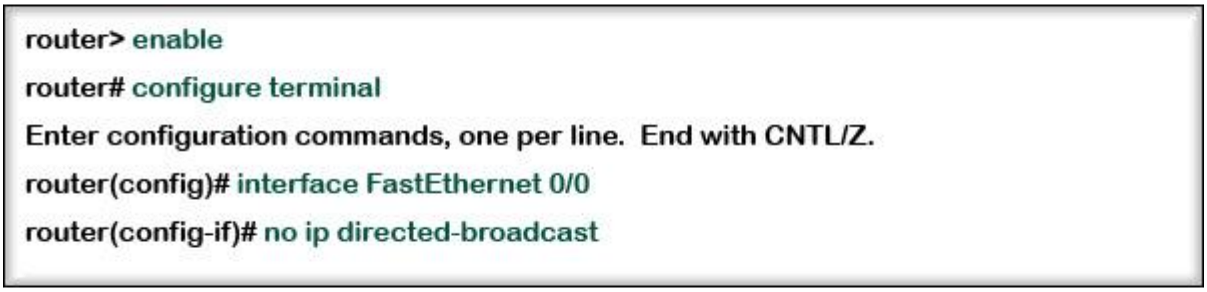


```
Router> enable
Router# show ip interface brief
Interface          IP-Address    OK? Method Status          Protocol

FastEthernet0/0      unassigned    YES manual administratively down down

FastEthernet0/1      unassigned    YES manual administratively down down
```

Now that we know our interface naming convention, FastEthernet 0/0, we can modify it. You may wish to write this down, since this will be what you will always refer to your interfaces to from now on. You may now proceed to apply the command to the interface, as seen below.



```
router> enable
router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# interface FastEthernet 0/0
router(config-if)# no ip directed-broadcast
```

Note that we only applied this to a single interface (FastEthernet 0/0).It should be applied to all interfaces for maximum protection.

Closing Comments

Very few IP applications will make use of the IP directed broadcast, so it is almost always perfectly fine to leave it off. You can, however, configure access lists to permit or deny IP Directed-Broadcasts. This is usually only feasible with smaller networks, since access lists can be quite tedious to maintain on all but the smallest networks.

End of article

1E WakeUp Does Not Use Subnet-Directed Broadcast

1E WakeUp has devised it own methodology in order to avoid any potential security issues when the Wake Up commands are communicated by its server to PCs in remote subnets.

1E WakeUp offers many other features and benefits to its many users (over 5 million licenses have been deployed so far)

Additional information

1. 1E Wakeup Unique Feature Checklist
2. 1E Wakeup – FAQ
3. 1E Wakeup Features
4. 1E NightWatchman Unique Feature Checklist
5. 1E NightWatchman – FAQ
6. Electricity Savings – Australian ‘Typical’ Site
7. Data for Business Case – Information needed to calculate Company specific business case

For more information and your free evaluation, please contact

.

AH Technology Pty Ltd

www.ahtechnology.com.au 03-9885-4877 info@ahtech.com.au