Promiscuous mode

In computer networking, **promiscuous mode** (often shortened to "promisc mode" or "promisc. mode") is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is intended to receive. This mode is normally used for packet sniffing that takes place on a router or on a computer connected to a hub (instead of a switch) or one being part of a WLAN. Interfaces are placed into promiscuous mode by software bridges often used with hardware virtualization.

In IEEE 802 networks such as Ethernet, token ring, and IEEE 802.11, and in FDDI, each frame includes a destination Media Access Control address (MAC address). In non-promiscuous mode, when a NIC receives a frame, it normally drops it unless the frame is addressed to that NIC's MAC address or is a broadcast or multicast frame. In promiscuous mode, however, the card allows all frames through, thus allowing the computer to read frames intended for other machines or network devices.

Many operating systems require superuser privileges to enable promiscuous mode. A non-routing node in promiscuous mode can generally only monitor traffic to and from other nodes within the same broadcast domain (for Ethernet and IEEE 802.11) or ring (for token ring or FDDI). Computers attached to the same network hub satisfy this requirement, which is why network switches are used to combat malicious use of promiscuous mode. A router may monitor all traffic that it routes.

Promiscuous mode is often used to diagnose network connectivity issues. There are programs that make use of this feature to show the user all the data being transferred over the network. Some protocols like FTP and Telnet transfer data and passwords in clear text, without encryption, and network scanners can see this data. Therefore, computer users are encouraged to stay away from insecure protocols like telnet and use more secure ones such as SSH.

1 Detection

As promiscuous mode can be used in a malicious way to *sniff* on a network, one might be interested in detecting network devices that are in promiscuous mode. In promiscuous mode, some software might send responses to frames even though they were addressed to another machine. However, experienced sniffers can prevent this (e.g., using carefully designed firewall settings).

An example is sending a ping (ICMP echo request) with the wrong MAC address but the right IP address. If an adapter is operating in normal mode, it will drop this frame, and the IP stack never sees or responds to it. If the adapter is in promiscuous mode, the frame will be passed on, and the IP stack on the machine (to which a MAC address has no meaning) will respond as it would to any other ping. The sniffer can prevent this by configuring his or her firewall to block ICMP traffic.

2 Some applications that use promiscuous mode

- NetScout Sniffer
- OmniPeek
- Capsa
- Aircrack-ng
- KisMAC (used for WLAN)
- AirSnort (used for WLAN)
- Wireshark (formerly *Ethereal*)
- tcpdump
- IPTraf
- pktstat
- PRTG
- Kismet
- VMware's VMnet Bridging (networking)
- Cain and Abel
- Driftnet Software
- Microsoft Windows Network Bridge
- XLink Kai
- WC3Banlist
- Snort
- ntop

- Firesheep
- VirtualBox (bridge networking mode)
- CommView
- AccessData SilentRunner

3 See also

- Packet analyzer
- Monitor mode
- MAC spoofing

4 References

5 External links

SearchSecurity.com definition of promiscuous mode

6 Text and image sources, contributors, and licenses

6.1 Text

- **Promiscuous mode** *Source:* https://en.wikipedia.org/wiki/Promiscuous_mode?oldid=679224792 *Contributors:* The Anome, B4hand, Shellreef, Dcoetzee, Saltine, Betterworld, Joy, Flockmeal, GPHemsley, Aenar, Chris 73, Drago9034, ElBenevolente, Tieno, Pgan002, John Vandenberg, Dreish, Cohesion, Blotwell, Jcsutton, Guy Harris, Cjcollier, Lightdarkness, Amelia Hunt, Woohookitty, Elvey, Flarn2006, Margosbot~enwiki, Brookshawn, Jeremy Visser, SmackBot, MalafayaBot, Frap, Christan80, JonHarder, T.J. Crowder, UU, Diman011, Jdm64, Gnitset, R'n'B, Felipe1982, Buhadram, VolkovBot, Tburket, Jon-emery, Jamelan, BryKKan, Poindexter Propellerhead, Qhalilipa, ClueBot, StenSoft, Excirial, Sun Creator, Mlaffs, Funtaff, XLinkBot, Addbot, Graham.Fountain, LaaknorBot, Legobot II, AnomieBOT, ArthurBot, Xqbot, Shadowjams, Erik9bot, TobeBot, Tbhotch, Yuanli.H, ZéroBot, AManWithNoPlan, Gz33, ClueBot NG, Jau53, Bezzm, Douglas Saraiva, TheyCallMeHeartbreaker, AvocatoBot, WiFiEngineer, Doors5678, SoledadKabocha, Dave Braunschweig, Abhishek-Goel137, Subodhsaxena, Castlecorp and Anonymous: 81

6.2 Images

- **File:Question_book-new.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/9/99/Question_book-new.svg *License:* Cc-by-sa-3.0 *Contributors:*
  Created from scratch in Adobe Illustrator. Based on Image:Question book.png created by User:Equazcion *Original artist:*
  Tkgd2007

6.3 Content license

- Creative Commons Attribution-Share Alike 3.0