Digital Cable Modem

Usage and Troubleshooting Tips

Q: How do I get the system installed?

A: For now, professional installation from your cable provider is strongly recommended. They will ensure proper cable connection to the modem and your computer. In the near future, retailers will offer product and installation services in coordination with your local cable company.

Q: What can I do to get my modem to connect faster to my service provider?

A: Once you are connected to your service provider, we recommend that you stay connected. There is typically not an additional charge for this, and your service will always be readily available. All you need to do is keep your modem plugged into AC power and attached to the coaxial cable. The On/Off button on the modem just disconnects your PC from the modem, but the modem will maintain its connection to the ISP, through your cable company. If you are having a hard time establishing a connection in the first place, please refer to the next question.

Q: What should I do if my modem quits working, or I lose connection to my service provider?

A: On rare occasions, such as lightning strikes, modems may need to be repaired or replaced. Typically, however, loses in connection are not modem problems, but can be traced to either the quality of the cable signal connection, or the cable network's connection to the Internet Service Provider (ISP).

1. First, if you subscribe to the video service from your cable company, confirm that your television is still receiving a signal. If not, ask your cable company to reconnect your service.
2. Next, unplug your modem from AC power, and then plug it back in. Confirm that the modem is well connected to the cable coax and to your PC, and that the "Power" light is lit. Your modem will start to 'reboot' and begin the 5-step process of tuning into to the two-way cable signal and then making a connection to the ISP. Consult your instruction booklet for an explanation of the flashing light patterns during Initialization Mode. Normally, this process should be completed in just a few minutes.
3. If the light(s) continue to blink, and cannot establish a connection, give it some time. It could take up to 20 minutes in extreme situations. After that time, call the trouble call number you were given at the time of your installation and try to determine if the problem is related to the hardware or to their signal. They may be able to remotely "see" your modem if it has tuned into their signals. You may be having trouble with the "handshake" with the ISP and they may be able to help you remotely.

If you suspect that it must be a problem with the cable modem, then it will need to be confirmed. If you purchased or leased this modem directly from your cable company, then warranty service for the cable modem may be provided through your cable provider or its authorized service representative. If you bought this modem from RCA or through a retailer, then it should have come with a sheet of paper titled "Limited Warranty" that will give you a phone number to call for service.

Q: Why isn't my cable modem downloading data as fast as I thought it would?

A: The actual data download speed achieved by your modem will depend upon your cable operator's system architecture and connectivity to the internet, and the level of service to which you have subscribed with your cable operator. Typical speeds being offered by cable operators today using cable modems are up to 3 megabits per second for downloads (to your PC) and uploads (from your PC) in the range of hundreds of kilobits per second. Since the cable modem itself is capable of processing data several times faster than these rates, it is quite unlikely that the modem is the bottleneck of the system. But if the performance seems slower than you expected, there may be several causes.

The network architectures of cable systems and the way the servers are distributed require you to share the available bandwidth on the cable plant with your neighbors. During certain times of the day, you may experience peak traffic on your local neighborhood node. Furthermore, some websites may be so popular that thousands of hits are occurring simultaneously, and thus slow down the source of the information. If your problem is not specific to certain websites, you should contact your cable company and describe the problem.

Q: How can I network 2 or more PCs together to share my modem?

A: The level of service to which you have subscribed with your cable operator determines the number of PCs that can be simultaneously connected to your cable modem. The RCA DCM105 modem is capable of supporting a maximum of 16 PCs. The RCA DCM205, 210 and 215 is capable of supporting a maximum of 32 PCs. First, phone the customer support number you were given at the time of your install by your cable operator and confirm their capabilities and any additional sign-up requirements. If your cable operator supports it, multiple PCs can be networked in your home with an Ethernet Local Area Network (LAN), and then the cable modem can be connected to the LAN. In this configuration, the Ethernet connection on one cable modem and all PCs in the LAN are connected to an Ethernet hub. The maximum number of PCs depends upon what type of configuration your cable operator has agreed to support. Each of your PCs will need an Ethernet NIC (network interface card), Ethernet driver software, and TCP/IP software. First, follow the instructions provided with the hub, NICs and your PCs to create your in-home Ethernet LAN and confirm that the networked PCs are able to communicate among themselves over IP. Then, connect your cable modem to this LAN. Once your cable operator has "provisioned" you to be able to run the additional PCs, they will all automatically connect like your first PC did. Keep in mind that the more PCs that share a modem, the less bandwidth will be available to each PC.

Q: Should I be concerned about the security of the files on my PC, since I'm using a public network?

A: Yes! On August 26, 1999, CableLabs (a research and development cooperative of the Cable industry) released a white paper on this topic, advising cable modem users on this issue. It is printed below, in its entirety. More information may be available from CableLabs at www.cablelabs.com or www.cablemodem.com.

Security in DOCSIS-based Cable Modem Systems

Executive Summary

The DOCSIS system architecture includes security components that will ensure user data privacy across the shared-medium cable network and will prevent unauthorized access to DOCSIS-based data transport services across the cable network.

The DOCSIS architecture also supports policing (i.e., filtering) functions which can be used to reduce the risk of attacks targeted at attached CPE devices (Customer Premises Equipment, or personal computer). These policing capabilities match those available within dedicated line network access systems (e.g., telephone, ISDN, DSL) and cable data enterprises are as secure as DSL or other traditional phone architectures.

Regardless of the network access service employed, service subscribers should take precautions to secure their systems prior to attaching them to a public network. Owners of systems running Microsoft Windows should unbind NetBIOS from TCP/IP, effectively disabling file and print sharing over the Internet.

1. Introduction

DOCSIS-based cable modem systems provide users with high-speed access to packet-based data services. These services include Internet access, packet telephony, video conferencing and telecommuting (i.e., remote access to enterprise networks). Security threats associated with these services fall into two general categories: security of data transport services and security of CPE devices, which use cable modems to attach to public data networks.

The DOCSIS architecture includes security components that secure data transport services across the shared-medium cable network. DOCSIS data transport security provides cable modem users with data privacy and prevents unauthorized access to DOCSIS data transport services across the cable network.

Any CPE device attached to a public network will be subject to security threats. Given that the purpose of an access network is to provide subscribers with data access to public networks, the access network cannot take full responsibility for protecting subscriber systems from attacks originating from that public network. DOCSIS-based cable networks provide, as do dedicated subscriber line systems, traffic filtering, which reduces threats from attacks that may target specific operating system features common to many of the attached CPE devices. (For example, filtering traffic on UDP/TCP ports 137, 138 and 139 to prevent unintentional Microsoft Windows SMB/NetBIOS file and print sharing.)

Regardless of whether a user employs cable, telephone, or DSL access networks, that user cannot rely solely on the access network to protect his or her system from attack. Subscribers to these services MUST, in all cases, take precautions to secure their systems prior to attaching them to a public network.

The situation is analogous to how an individual protects his or her home. While the individual trusts that the local police will do a good job protecting the neighborhood from burglary, the homeowner still locks the doors in the evenings or when absent from the home. The more populated the community, the greater the potential security risk, and thus the more caution demonstrated by the homeowner.

Attaching one's computer to the Internet is like living in a large urban area. There is much to gain in terms of the wealth of information, however accompanying that access are risks associated with having a direct ramp onto a global information highway.

Section 2 of this report examines security features built into the DOCSIS architecture to secure data transport services across the shared-medium cable network. Section 3 looks at policing mechanisms these systems can provide in order to reduce security risks associated with linking individual computer systems to large public networks (e.g., the Internet).

2. Security of Data Transport Services

DOCSIS data transport security provides cable modem users with data privacy across the cable network by encrypting traffic flows between the Cable Modem (CM) and the Cable Modem Termination System (CMTS) located in the cable network headend.

In addition, DOCSIS security provides cable operators with protection from theft of service. Protected DOCSIS MAC data transport services fall into three categories:

1. best effort, high-speed, IP data services;
2. premium quality-of-service (QoS) data services; and
3. IP multicast group services.

The DOCSIS system prevents unauthorized access to these data transport services by the CMTS enforcing encryption of the associated traffic flows across the cable network, and employing an authenticated client/server key management protocol in which the CMTS (the server) controls distribution of keying material to client CMs.

DOCSIS data transport security has two protocol components:

- An encapsulation protocol for encrypting packet data across the cable network.
- A key management protocol for providing the secure distribution of keying material from the CMTS to client CMs.

The encapsulation protocol defines the:

- frame format for carrying encrypted packet data within DOCSIS MAC frames,
- set of supported data encryption and authentication algorithms, and
- rules for applying the cryptographic algorithms to a DOCSIS MAC frame's packet data.

DOCSIS currently employs the Cipher Block Chaining (CBC) mode of the U.S. Data Encryption Standard (DES) to encrypt a DOCSIS MAC Frame's packet data. The protocols are extensible, can support multiple encryption algorithms and will, in all likelihood, be extended to support the new Advanced Encryption Standard (AES) once it is in place.

CMs use the DOCSIS key management protocol to obtain authorization and traffic encryption material from a CMTS, and to support periodic reauthorization and key refresh. The key management protocol uses X.509 digital certificates, RSA public key encryption and triple DES to secure key exchanges between the CM and the CMTS.

DOCSIS data transport security provides a level of data privacy across the shared-medium cable network equal to, or better than, that provided by dedicated-line network access services (e.g., telephone, ISDN or DSL). It should be noted, however, that these security services apply only to the access network. Once traffic makes its way from the access network onto the Internet backbone, it will be subject to privacy threats common to all traffic traveling across the Internet, regardless of how it got onto the Internet. If a subscriber's concerns over communications privacy go beyond the access network, he or she should be using higher level security solutions: for example, VPN technology, to tunnel private data securely across public networks, or application-layer security (e.g., PGP or privacy-enhanced mail for email, SSL for Web-based transactions).

3. CPE System Security

DOCSIS-based network access systems support the same range of policing functions (filtering) available in remote access servers employed by traditional dedicated line network service providers.

The issue within these systems that has attracted the greatest press attention is unauthorized access to system files using TCP/IP NetBIOS (NBT) and System Message Block (SMB) file-sharing protocols that run on various Microsoft Windows variants (e.g., Windows for Workgroups, Windows 95, Windows 98, Windows NT).

Hackers need to know the Internet address of the target system—if a hacker can obtain the name and address of the targeted host system, he or she can then begin sending network traffic to that host in order to pry it open and gain unauthorized access. Windows PCs employ TCP/IP the NetBIOS (NBT) name service for advertising and for determing names and addresses of shared system resources on a LAN. Depending upon the system configuration, this name service may employ broadcast messaging, which allows systems on a shared LAN to exchange the names and addresses of shared services directly across that LAN.

Cable modems present to their attached CPE devices a high-speed LAN interface. Attached Windows PCs can run the NBT broadcast name service across these interfaces to share name and addressing information with PCs attached to the same "cable LAN." Thus, if an attached PC has file and printer sharing enabled, its services will be advertised across this LAN interface, and other devices on that cable-based LAN can determine names and addresses of those shared file and print services.

These NBT name service broadcasts employ UDP port 137, and thus can be filtered readily. However, not all proprietary systems support comprehensive filtering of this broadcast traffic; if they do, service providers prefer not to employ it for performance reasons.

Remote access servers used in dedicated line network access architectures do not reflect broadcasts received from one client out to other clients; hence, the names and addresses of a PC's shared services cannot be exchanged through NBT name service broadcasts. This explains why proprietary cable modem systems are more vulnerable to the unintended distribution of shared service names and addresses than dedicated-line systems.
Once an attacker determines the name and the address of a Windows-shared service, he or she then can establish a point-to-point NetBIOS session with the shared service. Depending upon the shared system's configuration, the shared service may or may not be password protected.

Thus, with regard to Windows-shared file and print services, the principal difference between the proprietary cable modem systems and dedicated subscriber line systems is support, in the cable environment, for NBT name service broadcasts. This vulnerability addressed by the cable service provider:

1. making users aware of the issue,
2. requiring users to disable file and print sharing, and
3. educating users on how to disable sharing.

DOCSIS-based cable modem systems, like dedicated line systems, can police the network by efficiently filtering the UDP port over which NBT name service broadcasts are sent.

It should be noted that even if NBT name service broadcasts are inhibited, an attacker can use other methods (although certainly not as conveniently as simply double clicking on "Network Neighborhood") to determine host names and addresses and to begin an attack. Anyone can try to access shared files if they know an IP address, regardless of the type of access network. Knowledgeable system administrators recommend that any Windows system directly attached to a public network should unbind NetBIOS from TCP/IP, thus disabling Windows (SMB) file and printer sharing over the Internet.

Note that enterprise networks typically have a firewall separating themselves from the Internet, and this firewall filters all TCP/IP NetBIOS traffic. In this way, Windows systems within the enterprise network can use Windows networking (SMB over NBT) to share files internally, yet can be protected from external attack.