American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-5, Issue-7, pp-17-22
www.ajer.org
Research Paper Open Access

Cisco Router Configuration with IP

Ashiqur Rahman[1], Asaduzzaman Noman[2], Zahidul Islam Akash[3]
Deen Islam[4]
[1](M.Sc In Information Technology (IT), Jahangirnagar University, Bangladesh)
[2](CSE, Royal University Of Dhaka, Bangladesh)
[3](CSE, Royal University Of Dhaka, Bangladesh)
[4](EEE, Royal University Of Dhaka, Bangladesh)

ABSTRACT: *A router is a networking device that forwards data packets between computer networks. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node. A router is connected to two or more data lines from different networks (as opposed to a network switch, which connects data lines from one single network). When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. This creates an overlay internetwork. The most familiar type of routers are home and small office routers that simply pass data, such as web pages, email, IM, and videos between the home computers and the Internet. An example of a router would be the owner's cable or DSL router, which connects to the Internet through an ISP. More sophisticated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the Internet backbone. Though routers are typically dedicated hardware devices, use of software-based routers has grown increasingly common.*

Keywords : *Ethical Hacker, black hat, CERT, Integrity, Vulnerabilities.*

I. INTRODUCTION

When multiple routers are used in interconnected networks, the routers exchange information about destination addresses using a dynamic routing protocol. Each router builds up a table listing the preferred routes between any two systems on the interconnected networks. A router has interfaces for different physical types of network connections, such as copper cables, fibre optic, or wireless transmission. It also contains firmware for different networking communications protocol standards. Each network interface uses this specialized computer software to enable data packets to be forwarded from one protocol transmission system to another.Routers may also be used to connect two or more logical groups of computer devices known as subnets, each with a different sub-network address. The subnet addresses recorded in the router do not necessarily map directly to the physical interface connections [1].

A router has two stages of operation called planes:

- Control plane: A router maintains a routing table that lists which route should be used to forward a data packet, and through which physical interface connection. It does this using internal pre-configured directives, called static routes, or by learning routes using a dynamic routing protocol. Static and dynamic routes are stored in the Routing Information Base (RIB). The control-plane logic then strips the RIB from non-essential directives and builds a Forwarding Information Base (FIB) to be used by the forwarding-plane.
- Forwarding plane: The router forwards data packets between incoming and outgoing interface connections. It routes them to the correct network type using information that the packet header contains. It uses data recorded in the routing table control plane.Routers may provide connectivity within enterprises, between enterprises and the Internet, or between internet service providers' (ISPs) networks. The largest routers (such as the Cisco CRS-1 or JuniperT1600) interconnect the various ISPs, or may be used in large enterprise networks. Smaller routers usually provide connectivity for typical home and office networks. Other networking solutions may be provided by a backbone Wireless Distribution System (WDS) [2], which avoids the costs of introducing networking cables into buildings.All sizes of routers may be found inside enterprises.The most powerful routers are usually found in ISPs, academic and research facilities.

Large businesses may also need more powerful routers to cope with ever increasing demands of intranet data traffic. A three-layer model is in common use, not all of which need be present in smaller networks.

II. TECHNICAL INFORMATION

The very first device that had fundamentally the same functionality as a router does today was the Interface Message Processor (IMP); IMPs were the devices that made up the ARPANET, the first packet network. The idea for a router (called "gateways" at the time) initially came about through an international group of computer networking researchers called the International Network Working Group (INWG). Set up in 1972 as an informal group to consider the technical issues involved in connecting different networks, later that year it became a subcommittee of the International Federation for Information Processing. These devices were different from most previous packet networks in two ways. First, they connected dissimilar kinds of networks, such as serial lines and local area networks. Second, they were connectionless devices, which had no role in assuring that traffic was delivered reliably, leaving that entirely to the hosts (this particular idea had been previously pioneered in the CYCLADES network). The idea was explored in more detail, with the intention to produce a prototype system, as part of two contemporaneous programs. One was the initial DARPA-initiated program, which created the TCP/IP architecture in use today [3]. The other was a program at Xerox PARC to explore new networking technologies, which produced the PARC Universal Packet system; due to corporate intellectual property concerns it received little attention outside Xerox for years. Sometime after early 1974 the first Xerox routers became operational. The first true IP router was developed by Virginia Strazisar at BBN, as part of that DARPA-initiated effort, during 1975-1976. By the end of 1976, three PDP-11-based routers were in service in the experimental prototype Internet. The first multiprotocol routers were independently created by staff researchers at MIT and Stanford in 1981; the Stanford router was done by William Yeager, and the MIT one by Noel Chipper; both were also based on PDP-11s. Virtually all networking now uses TCP/IP, but multiprotocol routers are still manufactured. They were important in the early stages of the growth of computer networking, when protocols other than TCP/IP were in use. Modern Internet routers that handle both IPv4 and IPv6 are multiprotocol, but are simpler devices than routers processing AppleTalk, DECnet, IP and Xerox protocols. From the mid-1970s and in the 1980s, general-purpose mini-computers served as routers. Modern high-speed routers are highly specialized computers with extra hardware added to speed both common routing functions, such as packet forwarding, and specialized functions such as IPsec encryption.

There is substantial use of Linux and Unix software based machines, running open source routing code, for research and other applications. Cisco's operating system was independently designed. Major router operating systems, such as those from Juniper Networks and Extreme Networks, are extensively modified versions of Unix software.

III. DELIVERY SEMANTICS

Routing schemes differ in their delivery semantics:

- unicast delivers a message to a single specific node
- anycast delivers a message to anyone out of a group of nodes, typically the one nearest to the source
- multicast delivers a message to a group of nodes that have expressed interest in receiving the message
- geocast delivers a message to a geographic area
- broadcast delivers a message to all nodes in the network

Unicast is the dominant form of message delivery on the Internet. This article focuses on unicast routing algorithms.

IV. TOPOLOGY DSITRIBUTION

In static routing (or non-dynamic routing), small networks may use manually configured routing tables. Larger networks have complex topologies that can change rapidly, making the manual construction of routing tables unfeasible. Nevertheless, most of the public switched telephone network (PSTN) uses pre-computed routing tables, with fallback routes if the most direct route becomes blocked (see routing in the PSTN). Dynamic routing attempts to solve this problem by constructing routing tables automatically, based on information carried by routing protocols, allowing the network to act nearly autonomously in avoiding network failures and blockages. Dynamic routing dominates the Internet. Examples of dynamic-routing protocols and algorithms include Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP).

Distance vector algorithms

Distance vector algorithms use the Bellman–Ford algorithm. This approach assigns a cost number to each of the links between each node in the network. Nodes send information from point A to point B via the path that

results in the lowest total cost (i.e. the sum of the costs of the links between the nodes used). The algorithm operates in a very simple manner. When a node first starts, it only knows of its immediate neighbors, and the direct cost involved in reaching them. (This information — the list of destinations, the total cost to each, and the next hop to send data to get there — makes up the routing table, or distance table.) Each node, on a regular basis, sends to each neighbor node its own current assessment of the total cost to get to all the destinations it knows of. The neighboring nodes examine this information and compare it to what they already 'know'; anything that represents an improvement on what they already have, they insert in their own routing table(s). Over time, all the nodes in the network discover the best next hop for all destinations, and the best total cost. When one network node goes down, any nodes that used it as their next hop discard the entry, and create new routing-table information. These nodes convey the updated routing information to all adjacent nodes, which in turn repeat the process. Eventually all the nodes in the network receive the updates, and discover new paths to all the destinations they can still "reach" [4].

Link-state algorithms

When applying link-state algorithms, a graphical map of the network is the fundamental data used for each node. To produce its map, each node floods the entire network with information about the other nodes it can connect to. Each node then independently assembles this information into a map. Using this map, each router independently determines the least-cost path from itself to every other node using a standard shortest paths algorithm such as Dijkstra's algorithm. The result is a tree graph rooted at the current node, such that the path through the tree from the root to any other node is the least-cost path to that node. This tree then serves to construct the routing table, which specifies the best next hop to get from the current node to any other node.

V. CISCO PORT LABELS

Router	Interface	Port Label
Cisco 851	Fast Ethernet LAN	LAN (top), FE0-FE3 (bottom)
	Fast Ethernet WAN	WAN (top), FE4 (bottom)
	Wireless LAN	(no label)
Cisco 871	Fast Ethernet LAN	FE0-FE3
	Fast Ethernet WAN	FE4
	Wireless LAN	LEFT, RIGHT/PRIMARY
	USB	1-0
Cisco 857	Fast Ethernet LAN	LAN (top), FE0-FE3 (bottom)
	ATM WAN	ADSLoPOTS
	Wireless LAN	(no label)
Cisco 876	Fast Ethernet LAN	LAN (top), FE0-FE3 (bottom)
	ATM WAN	ADSLoISDN
	Wireless LAN	LEFT, RIGHT/PRIMARY
	BRI	ISDN S/T
Cisco 877	Fast Ethernet LAN	LAN (top), FE0-FE3 (bottom)
	ATM WAN	ADSLoPOTS
	Wireless LAN	LEFT, RIGHT/PRIMARY
Cisco 878	Fast Ethernet LAN	FE0-FE3
	ATM WAN	G.SHDSL
	Wireless LAN	LEFT, RIGHT/PRIMARY
	BRI	ISDN S/T

VI. INFORMATION FOR CONFIGURATION

You need to gather some or all of the following information, depending on your planned network scenario, prior to configuring your network

- If you are setting up an Internet connection, gather the following information:
  - Point-to-Point Protocol (PPP) client name that is assigned as your login name
  - PPP authentication type: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP)
  - PPP password to access your Internet service provider (ISP) account
  - DNS server IP address and default gateways
- If you are setting up a connection to a corporate network, you and the network administrator must generate and share the following information for the WAN interfaces of the routers:
  - PPP authentication type: CHAP or PAP
  - PPP client name to access the router
  - PPP password to access the router

- If you are setting up IP routing:

– Generate the addressing scheme for your IP network.

– Determine the IP routing parameter information, including IP address, and ATM permanent virtual circuits (PVCs). These PVC parameters are typically virtual path identifier (VPI), virtual circuit identifier (VCI), and traffic shaping parameters.

– Determine the number of PVCs that your service provider has given you, along with their VPIs and VCIs.

– For each PVC determine the type of AAL5 encapsulation supported. It can be one of the following:

AAL5SNAP—this can be either routed RFC 1483 or bridged RFC 1483. For routed RFC 1483, the service provider must provide you with a static IP address. For bridged RFC 1483, you may use DHCP to obtain your IP address, or you may obtain a static IP address from your service provider.

AAL5MUX PPP—with this type of encapsulation, you need to determine the PPP-related configuration items.

- If you plan to connect over an ADSL or G.SHDSL line:

– Order the appropriate line from your public telephone service provider.

For ADSL lines—ensure that the ADSL signaling type is DMT (also called ANSI T1.413) or DMT Issue 2.

VII. INTERNET CRIME RATE

Router# **show running-config**
Building configuration...
Current configuration : 1090 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip subnet-zero
!
ip cef
ip ips po max-events 100
no ftp-server write-enable
!
interface FastEthernet0
 no ip address
 shutdown
!
interface FastEthernet1
 no ip address
 shutdown
!
interface FastEthernet2
 no ip address
 shutdown
!
interface FastEthernet3
no ip address
shutdown
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto

```
!
interface Dot11Radio0
 no ip address
 shutdown
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
 54.0
 rts threshold 2312
 station-role root
!
interface Vlan1
 no ip address
!
ip classless
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 login
 transport preferred all
 transport input all
 transport output all
!
end
```

VIII. CONCLUSION

A broadcast is a data packet destined for all hosts on a particular physical network. Network hosts recognize broadcasts by special addresses. Broadcasts are heavily used by some protocols, including several important Internet protocols. Control of broadcast messages is an essential responsibility of the IP network administrator. The Cisco IOS software supports two kinds of broadcasting: directed broadcasting and flooding. A directed broadcast is a packet sent to a specific network or series of networks, while a flooded broadcast packet is sent to every network. A directed broadcast address includes the network or subnet fields. Several early IP implementations do not use the current broadcast address standard. Instead, they use the old standard, which calls for all 0s instead of all 1s to indicate broadcast addresses. Many of these implementations do not recognize an all-1s broadcast address and fail to respond to the broadcast correctly. Others forward all-1s broadcasts, which causes a serious network overload known as a broadcast storm. Implementations that exhibit these problems include systems based on versions of Berkeley Standard Distribution (BSD) UNIX prior to Version 4.3. Routers provide some protection from broadcast storms by limiting their extent to the local cable. Bridges (including intelligent bridges), because they are Layer 2 devices, forward broadcasts to allnetwork segments, thus propagating all broadcast storms. The best solution to the broadcast storm problem is to use a single broadcast address scheme on anetwork. Most modern IP implementations allow the network manager to set the address to be used asthe broadcast address. Many implementations, including the one in the Cisco IOS software, accept andinterpret all possible forms of broadcast addresses.

IX. ACKNOWLEDGEMENTS

We are earnestly grateful to one our group member, Ashiqur rahman, Lecturer, Royal University of Dhaka. For providing us with his special advice and guidance for this project. Finally, we express our heartiest gratefulness to the Almighty and our parents who have courageous throughout our work of the project.

REFERENCES

[1]. Berghel, H. & Uecker, J. (2004). Wireless infidelity II: Airjacking. Communications of the ACM, 47(12), 15-20.
[2]. Berghel, H. & Uecker, J. (2005). WiFi attack vectors. Communications of the ACM. 48(8), 21-28.
[3]. Canadian Institute of Chartered Accountants, the. (2003). Using an ethical hacking technique to assess information security Risk, 1-15.
[4]. Chang, E.S. & Jain, A.K. & Slade, D.M. & Tsao, S.L. (1999). Managing Cyber Security Vulnerabilities in Large Networks. Bell Labs Technical Journal, 252-272.
[5]. Clutterbuck, P. & Rowlands, T. & Seamons, O. (2007). Auditing the Data Confidentiality of Wireless Local Area Networks. The electronic Journal Information Systems Evaluation, 10(1), 45-56.