A SURVEY OF DIFFERENT NETWORKS FOR TRAFFIC FLOW CONTROL

T.LAKSHMIBAI*
B.CHANDRASEKARAN**
C.PARTHASARATHY***

*Research Scholar, Dept. of ECE, SCSVMV University, Kanchipuram, Tamilnadu, India
**Asst. Professor, Dept. of ECE, SCSVMV University, Kanchipuram, Tamilnadu, India
***Asst. Professor, Dept. of IT, SCSVMV University, Kanchipuram, Tamilnadu, India

ABSTRACT
In this paper TACACS (Terminal Access Controller Access-Control System) refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server. TACACS is a separate protocol that handles authentication, authorization, and accounting (AAA) services. TACACS and other flexible AAA protocols have largely replaced their predecessors. TACACS is defined in RFC 1492, and uses (either TCP or UDP) port 49 by default. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, TACACS uses TCP and usually runs on port 49. It would determine whether to accept or deny the authentication request and send a response back. The TIP (routing node accepting dial-up line connections, which the user would normally want to log in into) would then allow access or not, based upon the response. In this way, the process of making the decision is "opened up" and the algorithms and data used to make the decision are under the complete control of whoever is running the TACACS daemon.

KEYWORDS: TACACS, Authentication, Authorization, Accounting, TIP

I. INTRODUCTION
A. IP Routing
IP routing is the process of delivering IP packets from one IP network to another. Routing is the core function of a router. To forward an IP packet from one IP network to another, a router must know how to route that packet to its destination. If a router is directly connected to a packet’s destination network, the router can independently forward the packet to that network. If a router is not directly connected to a packet’s destination network, the router must know the next-hop router to which the packet must be forwarded. IP hosts participate in routing to a much lesser degree. Hosts on any given IP network can independently communicate with one another. Hosts on different IP networks, however, must communicate through an IP gateway, or router. A host must be aware of its gateway or gateways.
B. ANATOMY OF A ROUTE
In general, a route consists of a destination and a gateway. If a host or router is only capable of classful routing, its route table will have two fields: destination gateway. Such a device can only route to classful networks, using the classful network mask. Because there can be only one classful network mask based on the destination IP address, there is no need to explicitly specify the mask. If a host or router is capable of classless routing, its route table will have three fields. Destination, mask, gateway. Such a device can route to both classful networks and classless subnets. This requires that a mask be explicitly specified. Most devices are capable of classless routing.

C. DEFAULT ADDRESS, ROUTE, AND GATEWAY
The default address is 0.0.0.0. This address encompasses all IP addresses. The default address is used to specify a default route, which is the route to be taken when no other more specific route is available. For example: destination gateway: 0.0.0.0 address-of-router-on-this-network destination mask gateway: 0.0.0.0 0.0.0.0 address-of-router-on-this-net. As shown here, the mask for a default route is 0.0.0.0. The gateway used for the default route is the default gateway.

D. STATIC ROUTING
Static routes are manually entered into a router or host. An administrator must know the internetwork layout and the paths that exist between networks. Then the administrator must program each router in the internetwork with the proper routes to get from any given network to any other network. The hosts obtain their routes manually or via DHCP.

E. DYNAMIC ROUTING
Dynamic routes are routes learned via one or more routing protocols. Routing protocols are used by routers to inform one another of the IP networks accessible to them. There are classful routing protocols, such as RIPv1, that do not transmit masks in their routing updates - the classful network mask is implied. There are also classless routing protocols, such as OSPF, that do transmit masks in their routing updates. Dynamic routing is much too complex. Suffice it to say that OSPF is the most prevalent standard routing protocol today, and likely the most prevalent routing protocol overall. Routing protocols typically do not apply to hosts. Hosts obtain their routes by manual configuration or by DHCP.
F. ROUTING ANALYSIS

HOSTS P AND Q: Hosts P and Q have only one way to get off their networks, and that is to forward traffic to the router connected to their respective networks. These hosts each have a default route to a default gateway - router X or Z.

ROUTER X: Router X has interfaces directly connected to networks A, B, and C, so it can route traffic between these networks without additional configurations. This router has only one option to get to other networks, and that is to forward traffic to router Y. So it has a default route to router Y.

ROUTER Z: Router Z has interfaces directly connected to networks D, E, and F, so it can route traffic between these networks without additional configurations. This router has only one option to get to other networks, and that is to forward traffic to router Y. So it has a default route to router Y.

ROUTER Y: Router Y automatically knows how to route traffic between networks C and D. To get to networks A and B, this router forwards traffic to router X. To get to networks E and F, this router forwards traffic to router Z. One of these routes could be made the default route.

G. GATEWAYS

The diagram below illustrates four “routers” on the “Internet backbone” along with two companies that have “gateways” for their internal networks onto the Internet. Any message that is sent over these networks from one “host” computer to another host computer will be broken-up into some number of “packets” where each packet will be transmitted independently from the source host to the destination host. Each packet will contain a “header” and a “payload” where the header indicates where the packet came from and the destination of the packet. By design, the Internet contains redundant paths such that there are usually multiple possible paths, or routes, for a packet to travel from its source to its destination. In the diagram below, as an example, a packet travelling from host computer #1 in company X to host computer #2 in company Y could travel from router A to router B and then to router C or it could travel from router A to router D and then to router C to reach the gateway into company Y. Whenever a router receives a packet, it examines its “routing table” to determine which “path”, or paths (also known as “links”), from that router is/are appropriate for forwarding the packet to its destination. Each time a packet travels over a link, it is known as a “hop”. The diagram below also illustrates that company Y has broken-
up its internal network into two “subnets”. The networks within both company A and company B are likely to be local-area networks (LANs).

Figure G.1 GATEWAY

H. PING
It uses ICMP echo request/reply. Source sends ICMP echo request message to the destination address. Destination replies with an ICMP echo reply message containing the data in the original echo request message. Source can calculate round trip time (RTT) of packets. If no echo reply comes back then the destination is unreachable.

I. TRACERROUTE
Trace route records the route that packets take a clever use of the TTL field. When a router receives a packet, it decrements TTL. If TTL=0, it sends an ICMP time exceeded message back to the sender to determine the route, progressively increase TTL. Every time an ICMP time exceeded message is received, record the sender’s (router’s) address. Repeat until the destination host is reached or an error message occurs.

J. PING and TRACEROUTE RESULT

Figure J.1 PING and TRACEROUTE RESULT
II TELNET
TCP protocol makes it possible to connect the remote computers; the TELNET protocol makes it possible to use them. The TELNET protocol offers a user the possibility to connect and log on to any other hosts in the network from user’s own computer by offering a remote log on capability. Historically TELNET was the first TCP/IP application and still is widely used as a terminal emulator. Today, while the applications are more and more equipped with the graphical user interface, the terminal-based applications are becoming minority among the applications; the TELNET has found its future as a toolkit lying below several client/server software. E.g. FTP, SMTP, SNMP, NNTP and HTTP are more or less dependent on the TELNET protocol. Telnet or Telecommunication Network is a network protocol which is mostly used to connect to remote machines over a local area network or the internet. Telnet was developed in 1969 to aid in remote connectivity between computers over a network. Telnet can connect to a remote machine that on a network and is port listening. Most common ports to which one can connect to through telnet are:
Port 21 - File Transfer Protocol, Port 22 - SSH Remote Login Protocol, Port 23 - Telnet Server, Port 25 - Simple Mail Transfer Protocol (SMTP), Port 53 - Domain Name Server (DNS), Port 69 - Trivial File Transfer Protocol (TFTP), Port 70 – Gopher, Port 80 - Hyper Text Transfer Protocol (HTTP), Port 110 - Post Office Protocol 3 (POP3)
Telnet is a protocol that allows you to connect to remote computers (called hosts) over a TCP/IP network (such as the Internet). Using telnet client software on your computer, you can make a connection to a telnet server (i.e., the remote host). Once your telnet client establishes a connection to the remote host, your client becomes a virtual terminal, allowing you to communicate with the remote host from your computer. In most cases, you'll need to log into the remote host, which requires that you have an account on that system. Occasionally, you can log in as guest or public without having an account. Telnet clients are available for all major operating systems. Command-line telnet clients are built into most versions of Mac OS X, Windows, UNIX, and Linux.

A. TELNET FOR CLIENT/SERVER APPLICATIONS
The TELNET can be used as a tool set to build the client/server applications. As a basis for the application, TELNET rarely requires the terminal extensions and the negotiations but the TELNET operates in the basic NVT mode. The NVT is bi-directional half-duplex device, which contains a terminal and a keyboard. Basically the keyboard is the user keyboard. The keyboard produces client’s outgoing data sent over the TELNET connection to the server.
The printer is the user’s display where the TELNET server sends the characters. The NVT is half duplex. This means that in the TELNET protocol either the client or the server has the control. The control from the client to the server is changed by the CR/LF. The server uses the CR/LF for changing the line – not for returning the control to the client. The client receives the control after receiving the data from the server and accepting the GO AHEAD control code.

B. TELNET AND SECURITY

The eavesdropping and the snooping are easy to implement to any machine connected to a LAN and the fact that the password and the user ids are sent through the TELNET connection encrypted, if not otherwise required, the TELNET protocol is a security risk. Therefore the TELNET protocol defines an option for the authentication. The actual authentication is exchanged in the authentication sub negotiation. The TELNET’s authentication options support such authentication standards like Kerberos, SPX, RSA, LOKI and SSA.

III. AAA server

An AAA server (authentication, authorization, and accounting) is a server program that handles user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information. The current standard by which devices or applications communicate with an AAA server is the Remote Authentication Dial-In User Service (RADIUS).

Authentication, authorization and accounting processes are needed when user tries to access and use Internet. AAA server provides all the above services to its clients. Authentication refers to confirmation that a user who is requesting a service is a valid user. Accomplished via the presentation of an identity and credentials. Examples of credentials are passwords, one-time tokens, digital certificates, and phone numbers (calling/called). Authorization refers to the granting of specific types of service (including "no service") to a user, based on their authentication. It may be based on restrictions, for example time-of-day restrictions, or physical location restrictions, or restrictions against multiple logins by the same user. Examples of services include, but are not limited to: IP address filtering, address assignment, route assignment, encryption, QoS/differential services, bandwidth control/traffic management. Accounting refers to the tracking of the consumption of network resources by
users. Typical information that is gathered in accounting is the identity of the user, the nature of the service delivered, when the service began, and when it ended. It may be used for management, planning, billing etc. It supports AAA communication between AAA client and AAA server(s) such as Terminal Access Controller Access Control System (TACACS), TACACS+, RADIUS and DIAMETER.

IV. PHYSICAL CONNECTIONS

A. TELNET WITH OUT TACACS SERVER

Figure IV.A.1 TELNET WITH OUT TACACS SERVER

B. TELNET WITH TACACS SERVER

Figure IV.B.1 TELNET WITH TACACS SERVER
IV. RADIUS SERVER

RADIUS Server: Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Internet Engineering Task Force is the main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF (Internet Engineering Task Force) is the body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership. Standards are expressed in the form of Requests for Comments (RFCs). RADIUS is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. RADIUS stands for Remote Authentication Dial-In User Service. RADIUS is an AAA protocol for applications such as Network Access or IP Mobility and works in both situations (a) Local (b) Mobile. Uses PAP, CHAP or EAP protocols to authenticate users. Look in text file, LDAP Servers, Database for authentication. After authentication services parameters passed back to NAS. Be notified when the session starts and top. This data will be used for Billing or Statistics purposes. SNMP is used for remote monitoring and it can be used as a proxy.

V. TACACS SERVER

TACACS+ Terminal Access Controller Access Control System is an Authentication, Authorization, and Accounting (AAA) protocol originally developed for the U.S. Department of Defence for authentication to network devices such as routers, switches, and firewalls. Unlike RADIUS, it separates the Authentication and Authorization functionalities, which makes it more flexible for administrative access. The current version of the protocol standard
was developed by Cisco Systems. TACACS+ simplifies network administration and increases network security. It does this by centralizing management of users on your network and enabling you to set granular access policies by users and groups, command, location, time of day, subnet, or device type. The TACACS+ protocol also gives you a complete log of every user's login and what commands were used. TACACS+ is recommended for compliance with most network security standards for E-Commerce, Health Care, Finance, and Government networks. general system requirements. To use TACACS+ authentication, you need the following: A TACACS+ server application installed and configured on one or more servers or management stations in your network. (There are several TACACS+ software packages available.) A switch configured for TACACS+ authentication, with access to one or more TACACS+ servers.

In this paper tells TACACS server provides user authentication and authorization and accounting oriented services for remote based services. In our survey very useful for identify the unknown person and attacker information from the networks and peer to peer communication services. Previous security oriented authentication approaches works on single client server approach, but in this system provides more efficient centralized security approaches

VI. RADIUS vs. TACACS+

RADIUS: Combines authentication & authorization.
Encrypts only the password.
Requires each network device to contain authorization configuration.
No command logging.
Minimal vendor support for authorization.
UDP- Connectionless, UDP ports 1645/1646, 1812/1813 and Designed for subscriber AAA.

TACACS+: Separates all 3 elements of AAA, making it more flexible.
Encrypts the username and password.
Central management for authorization configuration.
Full command logging.
Supported by most major vendors.
TCP- Connection oriented .TCP port 49 and Designed for administrator AAA
VII. RESULT and OBSERVATION

TELNET LOGIN METHODS: METHOD 1: TELNET ACCESS WITH TACACS SERVER
Using AAA server through Tacacs+ protocol
METHOD 2: TELNET ACCESS WITH OUT TACACS SERVER and AAA SESSIONS

![Figure VII.1 TELNET WITH TACACS SERVER](image1)

![Figure VII.1 TELNET WITHOUT TACACS SERVER](image2)

![Figure VII.2 AAA SESSIONS](image3)

VIII. CONCLUSION

In this paper tells TACACS server provides user authentication and authorization and accounting oriented services for remote based services. In our survey it is very useful to identify the unknown person and attacker information from the networks and peer to peer communication services. Previous security oriented authentication approaches works on single client server approach, but this system provides more efficient centralized security approaches.
IX. REFERENCES


