Universal Tacacs+ Server for Windows Ver 2.0
Beta Release 1 - Dec 27, 95

Introduction

Universal Tacacs+ Server for Windows is an authentication server supporting the TACACS, XTACACS and TACACS+ protocol. Universal Tacacs+ Server is able to support all three protocols simultaneously and using the same user database. This provides a smooth migration path for XTACACS users by allowing both XTACACS and TACACS+ systems to coexist.

For TACACS+, Universal Tacacs+ Server support all three As, i.e., Authentication, Authorization and Accounting. For TACACS and XTACACS support, Universal Tacacs+ server supports all XTACACS message types, including the latest CHAP, ARAP and new style SLIP ON.

Universal Tacacs+ Server employs the same user database for TACACS+, TACACS and XTACACS. For instance, if you configure an SLIP access list for a user, it will be used in both TACACS+ and XTACACS responses. The same access list will apply no matter where and how the user logins.

System Requirements

CPU : 386 or Above

Memory : 4MB

O/S : Windows 3.1, 3.11, Windows for Workgroup, Windows 95, Windows NT

TCP/IP: Winsock 1.1 compliant TCP/IP stack

Others : VBRUN300.DLL, MSAFINX.DLL and THREED.VBX installed in the /windows/system directory.

If you are upgrading from Universal XTACACS Server, you should already have these three files installed in your system.

If you do not have MSAFINX.DLL or THREED.VBX already installed in /windows/system, you should copy these two files distrubuted with this Beta release to the /windows/system directory.

If you do not have VBRUN300.DLL already installed in /windows/system, you should download it from SimTel or CICA and copy it to /windows/system. A copy of VBRUN300.DLL is also available on the Universal XTACACS Server for Windows at "ftp://ftp.cica.indiana.edu/pub/pc/win3/winsock/xtacac12.zip" or "ftp://ftp.cica.indiana.edu/pub/pc/win3/winsock/xtac121a.zip". VBRUN300.DLL is not distributed with this Beta Release to keep the file size small.

What other things will be included in the Real Release ?

The followings will be included in the real release but not in this beta release :

- Complete formatted documentation
- Online context sensitive help
- Universal Tacacs+ Accountant for accounting report generation

- Ver 1.1/1.2 to Ver 2.0 user database conversion utility
- Automatic installation program (SETUP.EXE)

What is the Upgrade Policy ?

If you buy Universal XTACACS Server for Windows now, you will be eligible for free upgrade to Universal Tacacs+ Server for Windows when it is released, as well as all future releases within 1 year from the date of purchase.

Problems and Comments

If you encounter any problems in using the software, or you have any comment or suggestion regarding the software, please send to : (If it is a problem, please remember to include the type of Winsock you are using and the Cisco IOS version.)

Universal Networks Company Limited
Suite 1705, Wellborne Commercial Centre
8 Java Road, North Point
Hong Kong.

Tel : (852)-2806-3318
Fax : (852)-2806-3300
E-mail : unet@mailhub.hkstar.com
WWW : http://www.hkstar.com/~unet

The preferred method of communication is by Email or by fax.

Getting Started

Installing Universal Tacacs+ Server

The Beta Release of Universal Tacacs+ Server does not come with any SETUP.EXE program. To install, please :

- Unzip all files to an empty directory.
- Create an icon in the Program Manager for the executable TACACS.EXE and for the documentation BETA.WRI. The easiest way to do this is to drag the files from the file manager to a group in the program manager.

Universal Tacacs+ Server is designed to be very easy to use. To start it up, double click on its icon in the program manager. Universal Tacacs+ Server will ask you to login. For first time login, you may use the username "SuperManager" with no password to login.

Universal Tacacs+ Server comes will several default accounts for you to test the server immediately. The default accounts are :

UserName	**Privilege Level**
SuperManager	TACACS+ Manager
Operator	TACACS+ Operator
SuperUser	Level 15
Normal	Level 1

All default accounts come with no password. You can only use the SuperManager and Operator accounts to login Universal Tacacs+ Server. The other two accounts are for you to login your network access server.

After you have started Universal Tacacs+ Server, you can go on to configure your communication server, terminal server or network access server (hereafter referred to as the network access server NAS).

Configuring the Network Access Server

After you have set up Universal Tacacs+ Server, the next step is to configure you NAS to use XTACACS or TACACS+. You need to configure the NAS so that it knows the IP address of the Universal Tacacs+ Server.

The exact steps required to configure the NAS server depends on the brand of the NAS. Please refer to the documentation of the NAS you are using for the exact steps.

In the followings, Cisco 2511/2509 communication servers will be used as an example.

Configuring XTACACS on Cisco 2511/2509

To configure a Cisco 2511/2509 to use XTACACS, enter the following lines into the configuration file of the Cisco 2511/2509 : (Note : the following lines are IOS dependent. It may or may not work depends on the version of your IOS.)

```
tacacs-server extended
```

tacacs-server host *{IP Addr of Universal Tacacs+ Server}*
tacacs-server last-resort password
!
tacacs-server notify connect
tacacs-server notify slip
tacacs-server notify enable
tacacs-server notify logout
!
tacacs-server authenticate enable
enable use-tacacs
tacacs-server authenticate connect
tacacs-server authenticate slip
!
line vty 0 4
login tacacs
!

Configuring TACACS+ on Cisco 2511/2509

Testing the XTACACS/TACACS+ System

After you have set up both Universal Tacacs+ Server and your NAS, you can now try to login the NAS by using the default account "SuperUser" with no password. The screen logger should log a message similar to below, telling you that there is a login request from the user "SuperUser" have been permitted. (Note : the message below is for Tacacs+ requests. It will be slightly different for XTACACS requests.)

12/23/95 18:29:10 Login request (privilege = 1) from user SuperUser at NAS 200.102.4.103 port tty18 permitted

User Records

Each user is described by a user record in Universal Tacacs+ Server. You can add, edit and delete user records by choosing the Add User, Edit User and Delete User under the main menu bar.

A user record contains the following fields :

Username
This is the name of the user. Username are case insensitive, so “Peter” and “peter” refers to the same user.

Password
This is the password of the user. Passwords are case sensitive. “Abcd” and “abcd” are considered different passwords.

If no password is specified, the template’s password will be used. If the template’s password is also empty, the template’s template’s password will be used and so on. If all passwords are empty, the password of the default record will be used. If the password of the default record is also empty, the password for that user will be empty.

Template
This is the name of another user record which will act as the template of the current user record. If some of the fields of the current user record is not filled in, its value will be inherited from the template. For example, if the expire date in the current user record is not filled in, the expire date of the template will be used.

Templates can be cascaded. A template can inherit from another template and so on. For example, if the expire date of the current record is not filled in, and the expire date of the template is empty as well, then the expire date of the template’s template will be used.

In case the value of a field cannot be determined even when templates are consulted (eg. none of the templates have the expire date filled in), the value of the “default” record will be used. The “default” record is a special user record with the username “default”. The “default” record will be used in case the value of a field is indeterminate even when considering templates.

Templates are most useful if you want to organize your users into a hierarchy of groups, very much like an organization chart. For instance, you can have a template for a department, which is inherited from the template for a business unit, which is in turn inherited from the corporate template. The higher level template contains configuration that are specific to the department, while the lower level template contains general configuration for the whole company.

On the horizontal dimension, you can have as many templates as you like. On the vertical dimension, you can have at most 50 levels of inheritance. This should be more than sufficient for even the most complex organization.

Universal Tacacs+ Server automatically detects template loops, and will automatically

reject any configuration that will lead to a template loop.

Privilege Level

A normal user can be configured with privilege levels 0 to 15. For TACACS+, this corresponds to the privilege level settings of the Cisco Communication Server. Level 1 is the basic privilege level upon login, while level 15 is the highest "enable" mode privilege. A user who wants to login as privilege level "x" in the Cisco Communication Server must be configured to have the same or higher privilege levels in the user record. For example, a user who wants to go into the highest "enable" mode must have at level a privilege level of 15.

For XTACACS, normal login corresponds to privilege level 1, while enable mode login or superuser login corresponds to privilege level 15.

In addition to the privilege levels 0 to 15, there are two additional levels - TACACS+ Manager and TACACS+ Operator.

TACACS+ Manager is the highest possible privilege level (level 16). In addition to able to login the highest enable mode, the TACACS+ Manager can login Universal Tacacs+ Server and configure the server.

TACACS+ Operator, in contrast, is the lowest possible privilege level (level -1). The TACACS+ Operator cannot login any communication server, but it has the special privilege to login Universal Tacacs+ Server to start it up. Unlike the TACACS+ Manager, the TACACS+ Operator cannot configure Universal Tacacs+ Server.

Apart from the above privilege levels, you can choose "inherit from template" in the privilege level listbox. In this case, the privilege level will be determine by the setting of the template. If the template's privilege level is also "inherit from template" and there are no more template configured, the privilege level of the default record will be used. If the default record privilege level is also "inherit from template", then the user will have absolutely no privilege to do anything.

Expire Date

The expire date is the date after which the user can no longer login. If the expire date is empty, its value will be inherited from the template. If after all templates are consulted and the expire date is still empty, the default record will be used. If the default record is also empty, the final default date will be "01/01/01"

Disable Login Checkbox

Checking this box will disable the user from logging in. This is most useful for templates which are not true user accounts. This can also be used to disable a user temporarily without deleting the record.

Description

This field is for informational purpose only. It is ignored by Universal Tacacs+ Server.

Authorized Address List

This is a list of permit/deny IP address ranges in the format "permit/deny {IP address 1} to {IP Address 2}. This list can be used to check against the NAS IP address for

user login authentication, or to check against the Telnet destination address for Telnet connection authentication.

If you fill in {IP address 1} but leave {IP address 2} empty, or vice versa, the range will be considered as a single address. If you leave both fields empty, that line will be ignored.

The Authorized Address List entries will be read one by one until either a permit or deny decision can be made. If no decision is made, the list of the template will be used. If again no decision can be made, the list of the template's template will be used and so on. If after all templates are used an still no decision can be made, the default record will be used. Usually the default record will contain either a "permit 0.0.0.0 to 255.255.255.255" or a "deny 0.0.0.0 to 255.255.255.255" which will definitely made a permit or deny decision.

Telnet Options
The Telnet Options checkbox determines how outbound Telnet are authorized.

The Always Permit checkbox instructs Universal Tacacs+ Server to permit all outbound Telnet connection regardless.

The Always Deny checkbox instructs Universal Tacacs+ Server to deny all outbound Telnet connection regardless.

The Check NAS Address checkbox instructs Universal Tacacs+ Server to use the Authorized Address List to check against the destination address to decide whether to permit or deny. If no decision can be made, Universal Tacacs+ Server will consult template(s) to see whether to "Always Permit", "Always Deny" or to "Check the template's Authorized Address List".

If, after using the templates and the default records and still no decision can be made, Universal Tacacs+ Server will consult the Authorized Command List (see below) to make a decision.

If none of the above options are checked, Universal Tacacs+ Server will consult the template(s) to make a decision. This is equivalent to checking the "Check NAS Address" checkbox with an empty Authorized Address List.

Authentication Options
There are two authentication options - "Check NAS Address Upon Login" and "Allowed Change Password Request".

"Check NAS Address Upon Login" determines whether to use the Authorized Address List to check against the NAS Address in authenticating user login. "No" means that no checking is necessary and therefore all addresses are allowed. "Yes" means that the NAS address must pass the Authorized Address List test. In the latter case, if no decision can be made, the template will be consulted to see whether "No" more checking is necessary or "Yes", use the template's Authorized Address List. If no decision can be made after consulting all templates, the default record will be used. If still no decision can be made, the final default is to deny.

“Allowed Change Password Request” determines whether a user is allowed to change his/her own password. Universal Tacacs+ Server will automatically go into Change password mode when the user types “Changepass” when presented with the username prompt. Universal Tacacs+ Server will prompt the user for “username”, “password”, “new password” and “confirm new password”. If all information supplied is correct and the “Allowed Change Password Request” is set to “Yes”, the change password request will be permitted, otherwise it will be denied.

If the “Allowed Change Password Request” is leave empty (ie. neither “Yes” nor “No”), the template(s) will be consulted. If the templates are also empty, the default record will be consulted. If the default record is also empty, the final default is “deny”.

Authorization Options
The Authorization Options button will bring out an authorization screen for your to fill in additional information related to Tacacs+ Authorization. Some of the authorization options such as access list settings will be mapped to the appropriate XTACACS fields if applicable.

Exec Authorization
The Exec Authorization options are used to process Tacacs+ Exec Authorization requests.

The Permit / Deny checkboxes determine whether to deny or to permit Exec Authorization. If both checkbox are leave empty, the template(s) will be used. If the templates are also empty, the default record will be used. If the default record is also empty, the final default is to deny.

If the answer is to permit, the Attribute Value List will be applied to the request. The Attribute Value List (AVL) are a list of Attribute Value pairs that are conditions and parameters used for the Authorization requests. For example, the AVL can be used to impose a certain access list (note : an access list is a list configured inside the NAS ; it is not the same as the Authorized Address List described above) to the user, to force the user to run a certain autocommand, to prevent a user to use an escape character, etc..

An Attribute Value pair is of the form “a=b” or “a*b” where “a” is the attribute and “b” is the value. For example, an access list number of 101 will be represented as “acl=101” while an autocommand to “show clock” will be represented as “autocmd=show clock”. The “=“ separator indicates that the Attribute Value pair is mandatory, while the “*” separator indicates that the Attribute Value pair is optional.

The Attribute Value List is formed by a list of Attribute Value pairs separated by semicolons “;”.

As per Cisco’s Tacacs+ Protocol Specification, the supported attributes include “service”, “protocol”, “cmd”, “cmd-arg”, “acl”, “inacl”, “outacl”, “zonelist”, “addr”, “routing”, “route”, “timeout”, “idletime”, “autocmd”, “noescape”, “nohangup”, “priv_lvl”, “remote_user”, “remote_host”, “callback”, “callback-line”, “callback-

rotary", etc.. For details, please refer to the NAS's documentation and Cisco's Tacacs+ Protocol Specification.

Note that not all attributes are relevant for Exec Authorization. Some attributes are only relevant for other types of Authorization.

The Append Template and Append Default checkbox determines whether the template's AVL and the default record's AVL will be appended to the end of the current AVL.

In a normal Exec Authorization request, the NAS may propose an AVL. Universal Tacacs+ Server will use the user's configured AVL to permit, deny, add, delete or replace the proposed AVL and response back to the NAS. The detail rule follows that of Cisco's Tacacs+ implementation :

For any particular Attribute Value pair proposed by the NAS, if it is mandatory then :

(a) If the same mandatory AV is configured inside the Universal Tacacs+ Server, this AV will be permitted.

(b) If an optional attribute is configured inside the Universal Tacacs+ Server that is the same as the proposed attribute, this AV will be permitted. It does matter whether the values matches or not.

(c) If (a) and (b) does not apply, and if the default is deny, then that AV will be denied and the whole authorization request will be denied. The default is determined by the "Exec Authorization Permit / Deny Checkboxes" in the default record. If the Deny Checkbox is checked, or if no checkbox is checked, the default is deny. On the other hand, if the Permit Checkbox is checked, the default is permit.

(d) If (a) and (b) does not apply, and if the default is permit, then that AV will be permitted.

If the NAS proposed AV pair is optional, then :

(e) If an exact mandatory AV pair is configured inside Universal Tacacs+ Server, the proposed AV pair will be replaced by the same mandatory AV pair.

(f) If (e) does not apply, but a mandatory AV is found configured inside Universal Tacacs+ Server with the same attribute but a different value, the NAS proposed AV pair will be replaced the Universal Tacacs+ Server's AV pair.

(g) If no mandatory attribute match exists, but an optional AV is found configured inside Universal Tacacs+ Server that matches exactly the NAS proposed AV, that AV will be permitted.

(h) If no exact optional AV match exists, but an optional AV is found configured inside Universal Tacacs+ Server with the same attribute but different value as the NAS proposed AV, the NAS proposed AV will be replaced by Universal Tacacs+ Server's AV.

(i) If none of the above applies and the default is "deny", the NAS proposed AV pair will be deleted, but the authorization request will not be denied because of this.

(j) If none of the above applies and the default is "permit", the NAS proposed AV pair will be permitted.

After all the NAS proposed AV pair has been processed, Universal Tacacs+ Server will add all configured mandatory AV pairs to the response if such attribute is not already included in the modified NAS proposed AVL.

In practice, the AVL is quite easy to use despite the complex rules. Normally, you could set the default to permit, so you don't have to worry about the AV pair proposed by the NAS. This should not be such a big security threat since the configuration (eg. access list or autocommand) inside the NAS is also under your control. You can then configure any attribute value you want to apply to that user. For Exec Authorization, two popularly used attribute is the "autocmd" attribute and the "acl" (access list) attribute. For example, to impose an access list 101 on a user, simply enter the following in the AVL :

acl=101

Whereas Exec Authorization options are primary used for Tacacs+ Authorization, the access list AV pair is also applicable to XTACACS Login as well. In XTACACS Login, the authentication server can optionally send back an access list number. Universal Tacacs+ Server will search the Exec Authorization AVL for the attribute "acl", and if found, will use its value as the access list number in XTACACS Login responses.

Command Authorization

The Tacacs+ Command Authorization is handled in the Universal Tacacs+ Server by using the Authorized Command List. The Authorization Command List is a list of "permit <cmd>" or "deny <cmd>" separate by semicolons ";". The <cmd> can be any valid characters used for pattern matching. Wildcards are supported.

For example, to permit only "show" commands and deny all other commands, the Authorized Command List can be configured as follows :

permit show *;deny *

The pattern matching characters supported are as follows :

Character	**Match**
?	Any single character
*	Zero or more characters

#	Any single digit (0-9)
[charlist]	Any single character in charlist
[!charlist]	Any single character not in charlist

A group of one or more characters (charlist) enclosed in brackets ([ ]) can be used to match any single character in expression and can include almost any characters in the ANSI character set, including digits. In fact, the special characters left bracket ([ ), question mark (?), number sign (#), and asterisk (*) can be used to match themselves directly only by enclosing them in brackets. The right bracket ( ]) cannot be used within a group to match itself, but it can be used outside a group as an individual character.

In addition to a simple list of characters enclosed in brackets, charlist can specify a range of characters by using a hyphen (-) to separate the upper and lower bounds of the range. For example, [A-Z] in pattern results in a match if the corresponding character position in expression contains any of the uppercase letters in the range A through Z. Multiple ranges are included within the brackets without any delimiting. For example, [a-zA-Z0-9] matches any alphanumeric character. Note that a range must appear in ascending sort order. [A-Z] is a valid pattern, but [Z-A] is not.

Other important rules for pattern matching include the following:

An exclamation point (!) at the beginning of charlist means that a match is made if any character except the ones in charlist are found in expression. When used outside brackets, the exclamation point matches itself.

The hyphen (-) can appear either at the beginning (after an exclamation mark if one is used) or at the end of charlist to match itself. In any other location, the hyphen is used to identify a range of ANSI characters.

An exception of Command Authorization is the “telnet” or “rlogin” command, for which the Telnet Options and the Authorized Address List described above will be used for authorized the command. This provides a more comprehensive and easier to use way of specifying the allowed destination address. Only if the Telnet Options and the Authorized Address List yields no decision will the Authorized Command List be consulted.

The Append Template and Append Default checkbox determines whether the template’s Authorized Command List and the default record’s Authorized Command List will be appended to the end of the current Authorized Command List.

Connect Authorization

Connect Authorization is similar to Exec Authorization, with the same options “Permit”, “Deny”, “Attribute Value List”, “Append Template” and “Append Default”. Their usage is the same as that of Exec Authorization.

There are 8 types of connect authorization, namely “PPP Link Layer”, “TCP/IP over PPP”, “IPX over PPP”, “ARAP over PPP”, “Vines over PPP”, “Unknown over PPP”, “SLIP” and “ARAP”. These correspond to the different types of Connect

Authorization that the Cisco NAS may initiate.

Normally, you will permit PPP Link Layer if you permit other types of protocols over PPP. If you disable PPP Link Layer, you will not be able to run other protocols over PPP.

Whereas the Connect Authorization options is primarily intended for Tacacs+, several Connect Authorization options applies also to XTACACS Slip On requests.

First, Universal Tacacs+ Server will deny XTACACS Slip On request if both PPP Link Layer and SLIP will affect whether are denied. (In XTACACS, Slip On refers to both SLIP and PPP).

Second, in traditional style XTACACS Slip On request, the authentication server can optionally return an access list number in the XTACACS response message. Universal Tacacs+ Server will search the SLIP Attribute Value pair for the "acl" attribute, and if found, will return its value as the access list number. If "acl" is not found, Universal Tacacs+ Server will try to find "outacl", and if not found it will try to find "inacl". If none of them is found, no access list number will be returned.

Finally, in new style XTACACS Slip On request, the authentication server can send back an input access list number and an output access list number. Universal Tacacs+ Server will use the value of the attribute "inacl" as the input access list number, and the value of the attribute "outacl" as the output access list number. It will return 0 (i.e., no access list) for an attribute if it is not found.

Universal Tacacs+ Server Options

You can configure the Universal Tacacs+ Server by selecting Options under the main menu bar. This will bring up an Options form. The followings describe the fields in the option form.

Log File Name
This is the name of the log file. If you change the log file name, the old log file will be closed automatically. If you specifies no name, there will be no logging to file.

Screen Log Level
The normal log level will log all TACACS+ authentication, authorization, accounting as well as all XTACACS requests. In addition, it will log down who has login Universal Tacacs+ Server itself, and who has add, edit or delete any user records.

The debug log level provides a very detail log that explains the decision making process of Universal Tacacs+ Server. For example, Universal Tacacs+ Server will explain why it rejects a user login (wrong password, account expire, account disabled, etc..). For an authorization request, it will show what are the NAS proposed AV pairs, what is the configured AVL within Universal Tacacs+ Server after recursively appended with the AVL of templates and the default record, and the NAS proposed AV pairs are processed to yield the result. The debug log level is most useful to trouble-shoot complex authorization requests.

File Log Level
The Normal and Debug file log level are exactly the same as the corresponding Screen log level. In addition, for file logging you can specifies no logging, in that case all loggings will go to the screen only.

Tacacs+ Key
This specifies the key used for encrypting Tacacs+ messages. It can be any alphanumeric characters of arbitrary length. The Tacacs+ Key is case sensitive.

Always Encrypt
This checkbox causes Universal Tacacs+ Server to deny all request that are not encrypted. Otherwise it may be possible for an attacker to pretend to be an NAS and issue an Tacacs+ Send Password request and obtain the password in cleartext.

This checkbox has no effect on XTACACS messages. The definition of the XTACACS protocol is such that the messages are always in cleartext.

Disable Start Up Login
This is most useful if you want Universal Tacacs+ Server to automatically start up when power is turn on. If this box is unchecked, you have to login every time you start up Universal Tacacs+ Server.

Handling TACACS+ Requests

The followings list out the various types of TACACS+ requests and how Universal Tacacs+ Server processes and responses to them.

Authentication Request

Login Request
Universal Tacacs+ Server will authenticate the user if :

- Username exists
- Password correct
- Expire Date has not been passed
- Disable Login Flag is not set
- NAS Address passes the Authorized Address List, unless the user record specifies that no NAS Address checking is necessary. If the Authorized Address List test cannot yield a definite permit or deny decision, the default is deny.
- Privilege Level of at least 1

SendPass (Send Password) Request
The NAS will issue a SendPass request for operations that requires the cleartext password, such as for CHAP and ARAP requests.

Universal Tacacs+ Server will send out the password if :

- Username exists
- Expire Date has not been passed
- Disable Login Flag is not set
- NAS Address passes the Authorized Address List, unless the user record specifies that no NAS Address checking is necessary. If the Authorized Address List test cannot yield a definite permit or deny decision, the default is deny.
- Privilege Level of at least 1

Note that in XTACACS, the authentication server (ie., Universal Tacacs+ Server) is responsible for calculating the CHAP and ARAP responses, so no password needs to be sent to the NAS. In TACACS+, the NAS is responsible for calculating the CHAP and ARAP responses, and requires the cleartext password from the authentication server as input. Whereas the XTACACS model looks more secure, the TACACS+ model is more flexible and extensible because it allows the NAS to implement future authentication algorithm without affecting the authentication server.

To avoid intruder obtain the cleartext password, all TACACS+ message should be encrypted by configuring an encryption key in the Options menu. In addition, you should configure Universal Tacacs+ Server to deny all non-encrypted requests to avoid an intruder pretending to be a NAS and use a sendpass request to obtain the password.

ChangePass (Change Password) Request
ChangePass request can be activated by typing “Changepass” as the username when login. Universal Tacacs+ Server will automatically change that into a ChangePass

request.

Universal Tacacs+ Server will permit a user to change his/her password if :

- Username exists
- Old password is correct
- Expire Date has not been passed
- Disable Login Flag is not set
- NAS Address passes the Authorized Address List, unless the user record specifies that no NAS Address checking is necessary. If the Authorized Address List test cannot yield a definite permit or deny decision, the default is deny.
- Privilege Level of at least 1
- The user is configured to allow Change Password requests.
- "New Password" and "Confirm New Password" matches

Authorization Requests

Exec Authorization
Exec Authorization occurs before an exec shell is granted to a user.

Universal Tacacs+ Server will authorize an exec shell if :

- Username exists
- The user is configured to permit Exec Shell
- The NAS proposed attribute value pairs passes the Attribute Value List test (refer to the previous session User Records for more information).

If the request is permitted, Universal Tacacs+ Server may add, delete, modify or replace the attribute value pairs proposed by the NAS.

Command Authorization
Command Authorization occurs before when a user attempt to run an exec command.

Universal Tacacs+ Server will authorize a command if :

- Username exists
- The command passes the Authorized Command List

Connect Authorization
Connect Authorization occurs before a user goes into SLIP or PPP or ARAP mode.

Universal Tacacs+ Server will authorize a connect attempt if :

- Username exists
- The user is configured to permit the type of connection requested (refer to the previous session User Records for more information).
- The NAS proposed attribute value pairs passes the Attribute Value List test

If the request is permitted, Universal Tacacs+ Server may add, delete, modify or replace the attribute value pairs proposed by the NAS.

Accounting

Accounting messages are for notification purposes only. Universal Tacacs+ Server will log all accounting messages and will always send back a permit response regardless. It is up to the NAS to decide what accounting messages to send.

Handling XTACACS Requests

Login Request
The NAS will send out a Login Request for normal tty user login or for PAP authentication.

Universal Tacacs+ Server will authenticate the user if :

- Username exists
- Password correct
- Expire Date has not been passed
- Disable Login Flag is not set
- NAS Address passes the Authorized Address List, unless the user record specifies that no NAS Address checking is necessary. If the Authorized Address List test cannot yield a definite permit or deny decision, the default is deny.
- Privilege Level of at least 1

If the request is permitted, Universal Tacacs+ Server will return an access list number if an "acl" attribute is configured in the Exec Authorization Attribute Value List (eg., as "acl=101").

Logout Request
The Logout request is for notification purposes only. Universal Tacacs+ Server will always send a permit message in response.

Slip On Request
The NAS will send out a Slip On request when a user type in PPP or SLIP to go into PPP or SLIP mode.

Universal Tacacs+ Server will authorize the Slip On request if :

- Username exists
- SLIP or PPP is permitted in the user's Connect Authorization configuration.

There are two types of Slip On request. For standard Slip On request, Universal Tacacs+ Server will return an access list number if an "acl" or "inacl" or "outacl" attribute is configured in the Slip Authorization Attribute Value List (eg., as "acl=101"). For new style Slip On request, Universal Tacacs+ Server will return an input access list number and an output access list number if the "inacl" and "outacl" attributes are configured in the Slip Authorization Attribute Value List respectively.

Slip Off request
The Logout request is for notification purposes only. Universal Tacacs+ Server will always send a permit message in response.

Slip Address request
The NAS will send out a Slip Address request if the user specifies an IP address when s/he goes into PPP or SLIP mode instead of using the default address assigned by the NAS. In this case, the NAS will ask the user a password to check if s/he is allowed to use the specified IP address. The NAS will send a Slip Address request with the IP address as the username and the user typed in password as password to Universal

Tacacs+ Server for authentication.

Universal Tacacs+ Server will authenticate the user if :

- Username (ie. the IP address) exists in the user record
- Password correct
- Expire Date has not been passed
- Disable Login Flag is not set
- NAS Address is within the Authorized Address List, unless the user record specifies that no NAS Address checking is necessary
- Privilege Level of at least 1

Connect Request

The NAS will send out a Connect request if the user attempts to Telnet to a remote host.

Universal Tacacs+ Server will authorize the user if :

- Username exists
- The destination address passes the Authorized Address List, unless the user record specifies that Telnet is always permitted or always denied. In the former case, the Connect request will be permitted regardless. In the latter case, the Connect request will be denied regardless.
- If the Authorized Address List test cannot yield a definite permit or deny decision, the Authorized Command List in the Command Authorization configuration will be consulted. If still no decision can be made, the default is deny.

SuperUser Request

The NAS will send out a SuperUser Request for “enable” mode login.

Universal Tacacs+ Server will authenticate the user if :

- Username exists
- Password correct
- Expire Date has not been passed
- Disable Login Flag is not set
- NAS Address passes the Authorized Address List, unless the user record specifies that no NAS Address checking is necessary. If the Authorized Address List test cannot yield a definite permit or deny decision, the default is deny.
- Privilege Level of at least 15

Reload Request

The Reload request happens when the NAS is rebooted. It is for notification purposes only. Universal Tacacs+ Server will always send a permit message in response.

CHAP Request

The NAS will issue a CHAP Request when CHAP is used to authenticate the user. In the XTACACS model, the Universal Tacacs+ Server is merely responsible for calculate the CHAP response. the NAS is responsible for checking whether the user’s CHAP response matched with that of the Universal Tacacs+ Server.

Universal Tacacs+ Server will send the CHAP response if :

- Username exists
- Expire Date has not been passed
- Disable Login Flag is not set
- NAS Address passes the Authorized Address List, unless the user record specifies that no NAS Address checking is necessary. If the Authorized Address List test cannot yield a definite permit or deny decision, the default is deny.
- Privilege Level of at least 1

ARAP Request

The NAS will issue an ARAP Request when ARAP is used to authenticate the user. In the XTACACS model, the Universal Tacacs+ Server is merely responsible for calculate the ARAP response. the NAS is responsible for checking whether the user's ARAP response matched with that of the Universal Tacacs+ Server.

Universal Tacacs+ Server will send the ARAP response if :

- Username exists
- Expire Date has not been passed
- Disable Login Flag is not set
- NAS Address passes the Authorized Address List, unless the user record specifies that no NAS Address checking is necessary. If the Authorized Address List test cannot yield a definite permit or deny decision, the default is deny.
- Privilege Level of at least 1

Universal Networks Company Limited
Suite 1705, Wellborne Commercial Centre
8 Java Road, North Point
Hong Kong.

Tel : (852)-2806-3318
Fax : (852)-2806-3300
E-mail : unet@mailhub.hkstar.com
WWW : http://www.hkstar.com/~unet