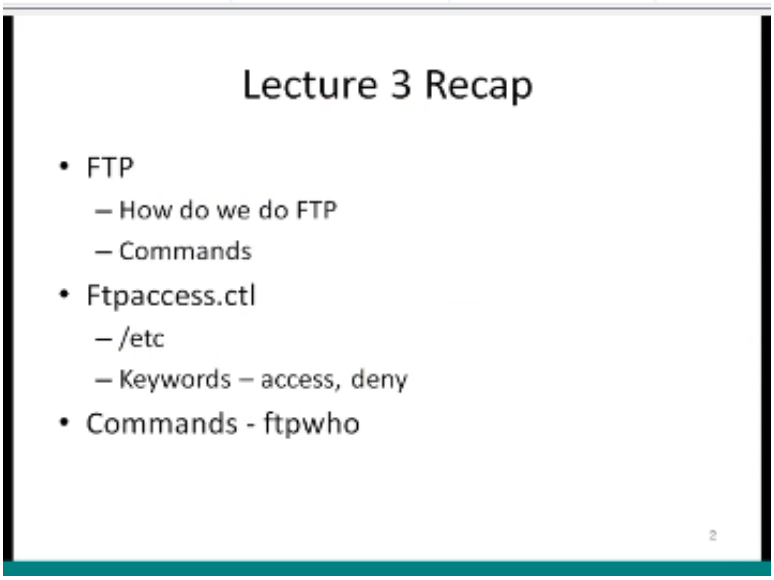
SEER AKADEMI
Linux Networking – Lecture 4
Domain Name System

Hi everyone again welcome to this lecture today we will be continuing the Linux networking topics this is lecture number 4 we finish the Linux basics and now we are into Linux networking, today we will be talking about the domain name system, this is one of the important things that he really touched upon during the first lecture and then now we will be taking it up much more details so before I want to before I go into the this domain name system itself let us recap what we learned the last lecture the lecture number 3.

(Refer Slide Time: 00:44)

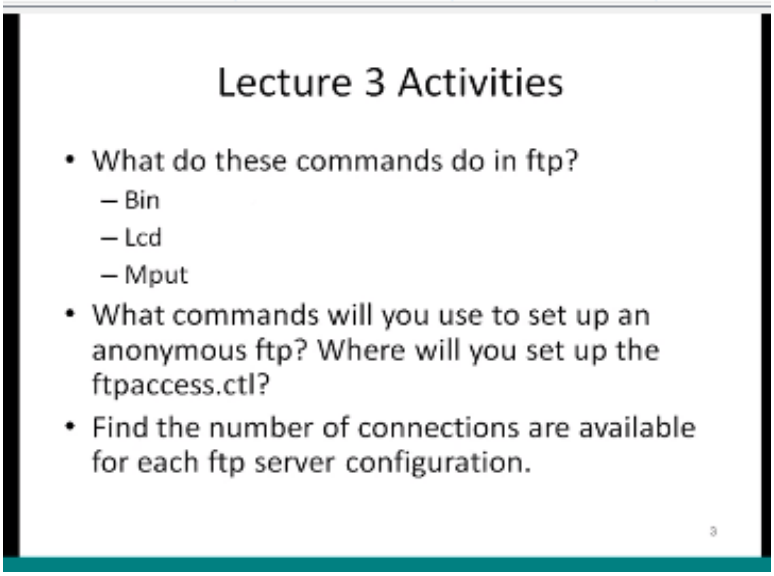


Which was mainly about the files the file transfer protocol or FTP we learned about how to do the FTB 2 by using the FTP and then followed by the FTP server command, and then there are various commands that we used to transfer files the back and forth you can transfer it into the FTP server and also you can get the file into your system and there are various modes by the transfer all the things we want.

And then we also learn something that is unique which is how to set up an FTP system or an FTP site in your machine the facility we learnt about that you have to be accessed dot control or CTL this particular file resides in the slash EPC area and this is the main file that is used to provide access to any users and here the we used several keywords for access deny read only, write only, things like that to make sure that the whoever is connecting to do any kind of FTP activity have all the permissions he or she needs to do the Python source.

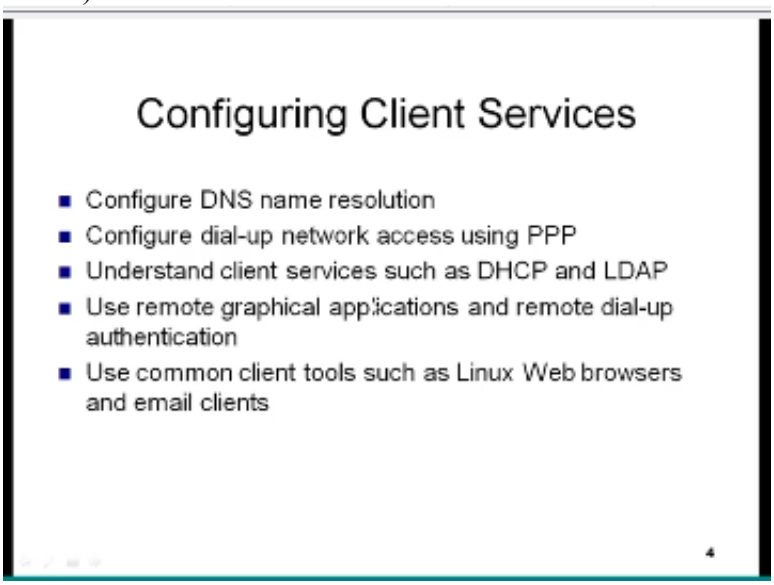
Then we also learn some administrative commands like FTP who is FTP pound the pink command that you only know about things like that to see um we can time so respectively but I

hope it was interesting for you all, and now let us look at some activities that I want you to do based on the last lecture.
(Refer Slide Time: 02:43)



So go ahead and actually answer these questions what do these commands do in the TT-then LCD input so I think these are the commands that we already learnt in the last so it should be fairly easy or you answer these questions the second one is slightly more challenging if what commands will you use to set up an anonymous FTP essentially like I mean this is I am fairly restoring to the FTP access door control inside that, how do you what do you write to set up the anonymous it.
Some hints I can give you the when you talk about an anonymous FTP you do not know who is actually anything so you need to make sure that you need to deal all the permissions that is needed or any kind of taxes, so yes it depends on what they want access but I also want you to give some idea as to how you want to give this the functions and then the other question this is very simple is from where do you set up the FTP access, control this answer is acting like I mean in the previous slide so just refer back immediately and get it.
So again this question is slightly difficult than the first one the first one is helps you to get the basic understanding and this one typing mode and then if you are still like I mean if you are looking for Motel for you to the third question it is the final number of connections that are available for each FTP server configuration in your machine, so your machine is has like several configuration of a fitting find the number of connections that are available for people who are who are connected to those various FTP servers.

I think like I mean this is fairly easy more assignment this you should be able to do it in the pan if you were paying attention to the lecture 3 so now we will start todays lecture, todays lecture is on domain name system as I mentioned, so let us look at the domain name system.
(Refer Slide Time: 05:24)

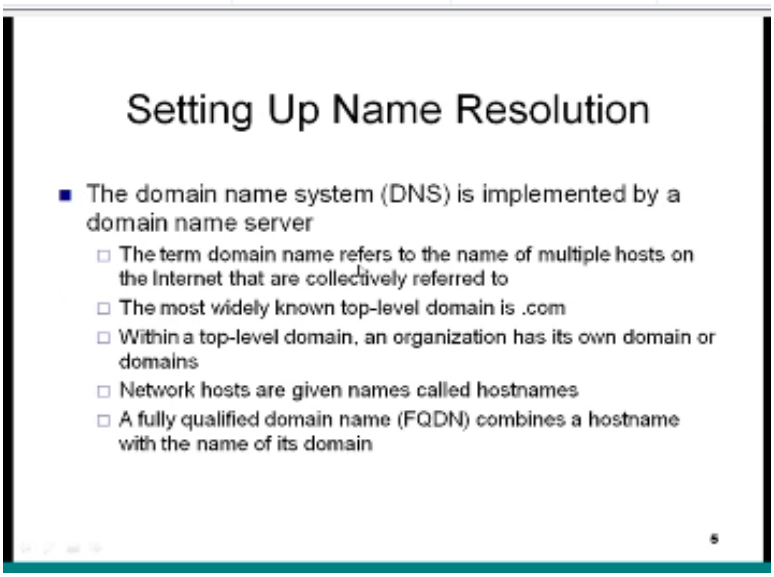


Here we will be learning about configuring the domain name system name resolution we will also try to configure the dialog network using the PPP or the point-to-point protocol and then we will also try to understand the tanks a little that the DHCP and the LDAP these are all like acronyms that we will study later then we will also like to look at some of the graphical applications and the remote dial-up authentications, and then we will also look at some flight level tools.
So such as web browsers and email clients because these are kind of you can almost think of them as applications of the DNS name resolution system so first of all what is BMO DNS is a hierarchical distributed naming system or computers services or any resources connected to the internet or even a private network, so that everyone knows what the other computers are services are available and admissible.
So address is one of the key things that everyone wants to have you have your home address and, so like I mean in the locality if people know like how to get hold of you to compare vows and they also know your name or we can mostly approach you and then we think they know that it is you so it is kind of it gives the identity of a person similarly the domain name service and the wind name system you can think of it as a directory where we store the identities of all the people you.

And the key thing is I think we saw a little bit in the last one the like I mean as you know the, the IP addressing that we learnt and we learned what IP everything IP addresses are this so for effect numbers picture binary or maybe you can convert that into a decimal or hexadecimal, but issue is if I ask you to remember say like 10 IP addresses from different sites, you will soon just not able to recollect recall any of the numbers.

So for humans we need something which and identify what is a web address for example google.com you need to know what like I mean the you need to know the IP address in order to go to the Google form but at the same time what you want to remember is just the Google form not excite the edges so the domain name system provides a way to actually do this.

(Refer Slide Time: 08:51)



So let us look at the or we do it so in this course we will be talking about like setting up but again it is a translation file that how you can do this where you can think of the numerical idea this is on one side and then the actual text based main names, on the other side so and imagine right I mean this you can use it to find and locate any computer services and devices worldwide this is one of the beauty of internet.

So that you can really find any computer in any part of the world connected to the Internet very quickly using the domain name system so in fact as a said it is an address book or phone book you can think of it or internet, so that that is how you should beautiful some domain name like Gaelic example.com it translates into address 192 dot 0.43 10 so I mean the DNS will just store that that name essentially the WWW. Example along the big yes so that if you type in www.example.com it takes you to that site using the actual idea.

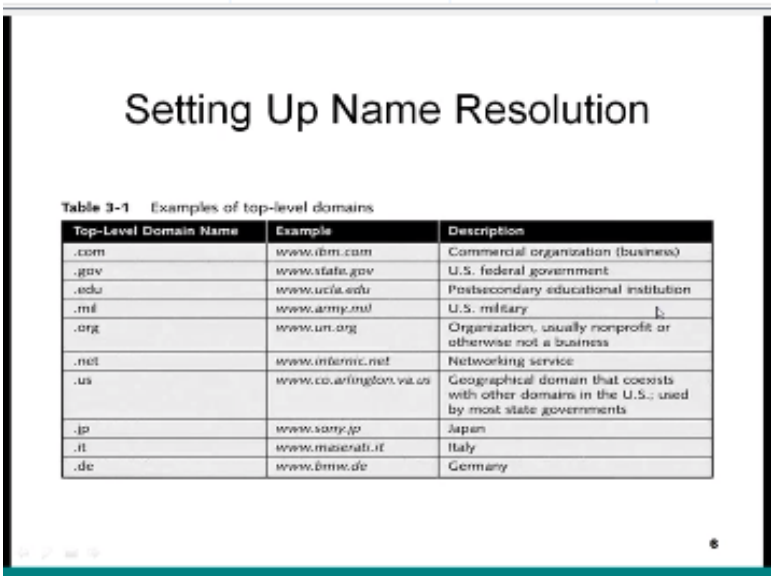
So closely associated with the DNS is also the URLs essentially like I mean that is the, the names starting with HTTP so URL stands for the Universal Uniform Resource locators and essentially that is basically it is a form of the IP everything which is which part which, which is a part of the DNS, so on the domain name syntax essentially like I mean so we will be learning about it before that let us look at the how we do the, the name resolution the DNS itself is implemented by a domain name.

For the domain name server essentially keeps multiple although all the details the IP addresses of all in the world pretty much in the world and it is corresponding textual addresses in one case here the term domain means the name of the multiple host internet in the internet and there that are collectively referred, to the most widely known the domain name is the dot com and pretty much a lot of people will be not a lot of people working for one of the platforms and we call it like the dot-com inside that.

And an organization and have its own domain or collection of the means the network or the names of the network course are hosting essentially and the FQDN refers to the fully qualified domain name, it combines the host name with the name of the domain so we will see some of the examples in the later section, so this is essentially like I mean how you would set up the name resolution the domain name syntax is one thing is the, the top level domain is always represented at the rightmost stone as the rightmost label.

So you can only think of the domain name as an inverted three structure so the dot com is at the top you see that the dot com is at the top and then followed by the, the remaining part in the, the dot com is here and then you can also have other, other items to the left of dot com, so let us look at some of the examples.

(Refer Slide Time: 14:21)



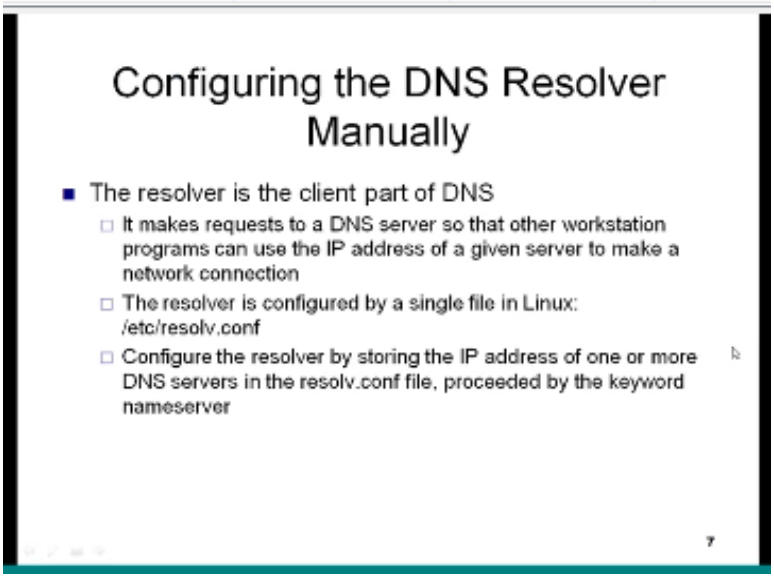
So here there are multiple examples the top level domain name is dot com one example is www.IBM.com which is potentially like I mean firm refers to commercial organization Oh so the first three letters and the other if coupler domain name is widely used is also dot GOV or Gov here the example is www.state.gov or irs.gov things like that the gov refers to the government it is typically the US federal government.

Then you have EDU which is the another very common top level domain name for example here it is www the labor people should be like stanford.EDU several schools dot EDU and these are the educational institution so that is why the first three letters again stands for eating now the military US military netted zone top load amending again that is denoted by of the letters mi and, any kind of organization whether it is profit or nonprofit mostly this nonprofit they have their own domain names that is the ORD.

So selection and then so these where the primary top level means for long, long, long time with total the leggings that only like pumps the EDU million or D today the US has opened up with other ones like dot net is any networking services it is not just limited to the networking cervical there are many companies, now getting the this one and then got us is another one of your graphical domain and it is exists with the other domains in us and it is also used by a lot of state governments even though the California uses also that more GOP names as well.

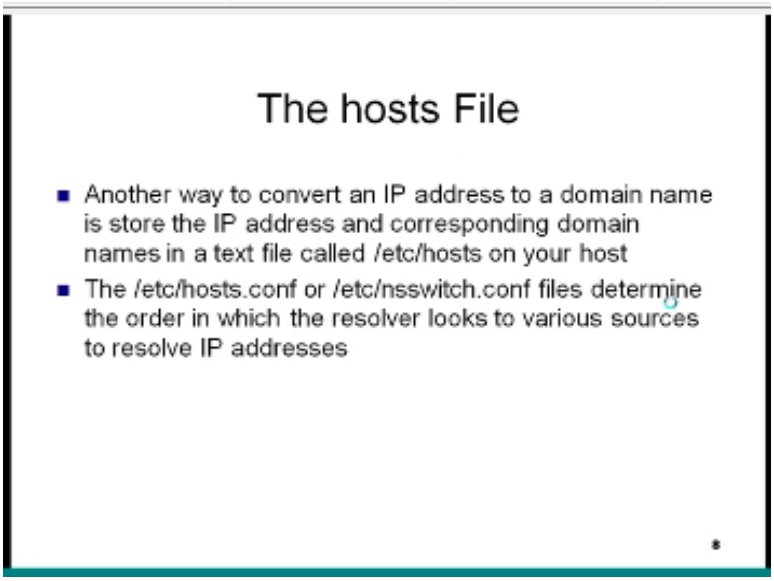
Then there are country specific names or examples JP Japan I T is Italy D is stands for the voyage or Germany, and I think you all know what I n stands for that is the India and one of the famous domain names in did in India is F next up in which is essentially the education of the successful so that goes to lot of educational institution and you can find the those several other

names like UK stands for the United Kingdom AUS, I think is the father Australia things like that.
(Refer Slide Time: 18:02)

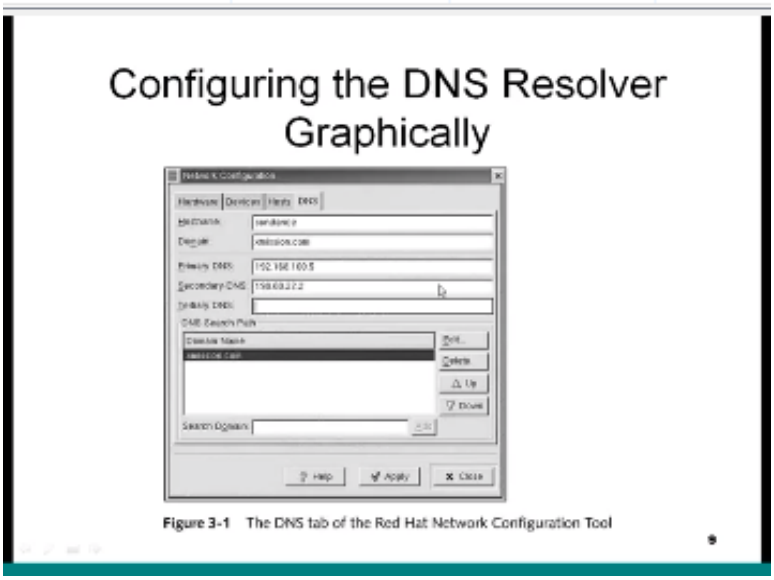


So you should be able to find more the top level maintains a lot of these things and nowadays like actually like now they are for the bore the particular body that controls this the domain means they are opening up in a big way so more the main games that are available today, so before we go into the resolver the there is also the hierarchy of four domains, as I mentioned like I mean when you are reading the domain names it goes from right to left with each label specifying one subdivision and each label is separated by the next level by a full stop or a dot.
So we just call it like www-what ibm.com is essentially and purposes the calm being at the top level and then under that one of the sub domain is IBM it would be Intel could be another symptom and so that will be intel dot com telephone and then if you want to put more stuff within Intel they like the semiconductor division or they like my closet division using that make processor got Intel. com that form.
So that means that it is the subdivision under the Intel people and there are some rules governing both the mean simple each label can go up to 63 characters the three of subdivisions they have up to 127 levels so I mean I don't think like anybodys using that kind of thing but you can think of the deepest tree that can accommodate all these things, so the other rules that also says is the full domain must not exceed the length of 253 characters and in its textual representation.
So the internal binary representation of the BNs has a maximum length of 255 Effects of storage but even though I like I mean it allows the 255 pockets in practical practically actually it is much shorter because the domain registries do not have like more form in this case that this that this

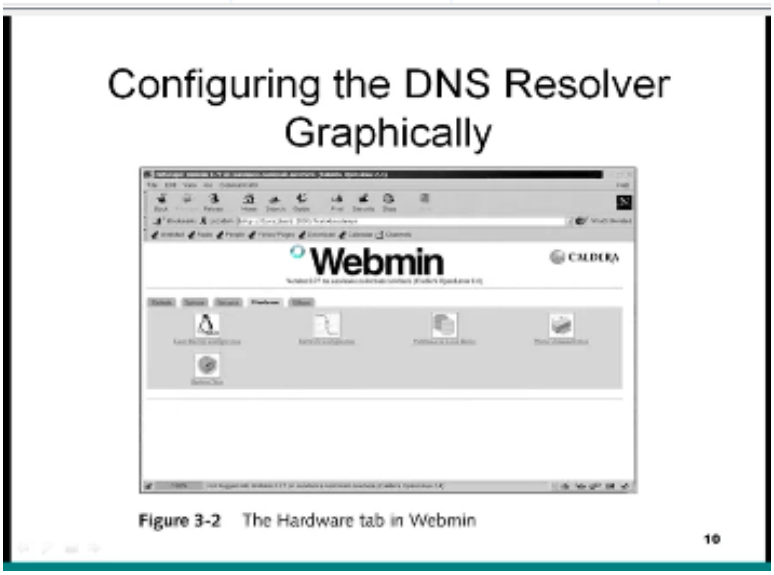
needed for accommodating this form particularly at this, and the domain names themselves can contain any character that can be represented in an object.
So it is not limited to this alphabets and things like that but typically the basically it includes the ASCII character set that is a three digits 0 through 9 uppercase into Z and also is also an unrated this particular rule is also known as LDH rule with letter digits and - usually the domain names are interpreted in the case independent manner, so the lowercase IBM and uppercase means the same thing and the definition of a hostname is a domain name that has at least one IP address associated.
(Refer Slide Time: 22:27)



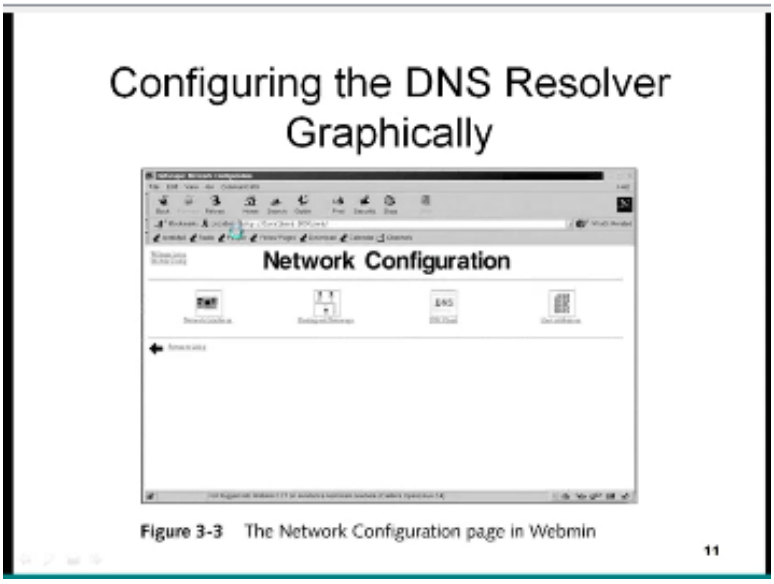
So the way to convert an IP address is to store the ID address with the corresponding domain names in a text file and as I said like this is this is your direction and this is actually located in the slash etc slash whose time, which should be you will be able to find it for instant aligning that slash it is not slash holes there are other files that are also being used the poster font and NS which dot one they determine the order in which the resolve will the resolver looks at various sources to resolve the I purpose again.
As I said you know the IP address and the old directory structure is all hierarchical and sometimes you may not have the storage space to store everything so you have to look at these additional files to see where is the, the information if it goes beyond the hierarchy that is supported within the within your system.
(Refer Slide Time: 24:12)



Let us look at configuring the DNS with mobile so graphically here you can see basically the post name which is Sentence the domain name 18 th machine dot-com again you can you can see that the dot form is the top-level domain name or by the sub domain is X million and then you have your host name then the primary DNS that you can say what is the domain name system name and then there is one ninety two dot one sixty eight and 105 I think by now you know like it is for ached what they mean there is what is a network and what is the actual host ID.
And then the same thing like secondary gain also specify for Spartech like two networks and in one network it is named as this computer vision 15 node and this in the second one exactly and that is the second move.
(Refer Slide Time: 25:45)

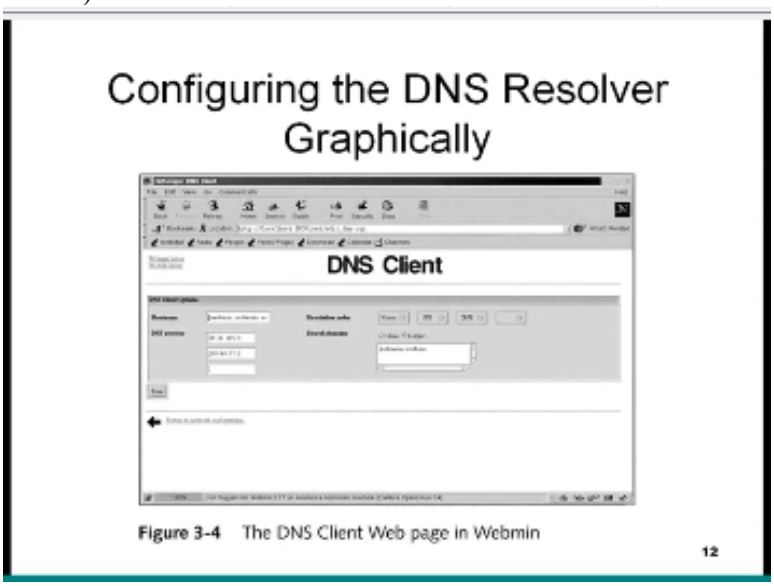


So here is the DEP min utility it is essentially like used to configure the DNS resolver.
(Refer Slide Time: 26:03)



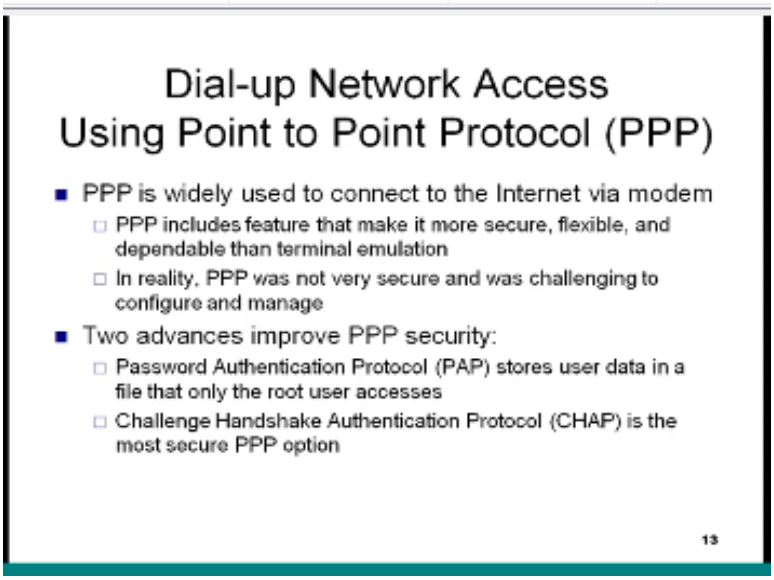
This one it again like the configuration page essentially like I mean one of these tabs is what you click to get the other one and then configure the DNS so that way.

(Refer Slide Time: 26:21)



So here is how the DNS client business would not be good in like this name be like hard to read but it also gives the same information the DNS server information the host name and then there are I think that those are the main information that you decide and that is used to configure this system.

(Refer Slide Time: 26:47)



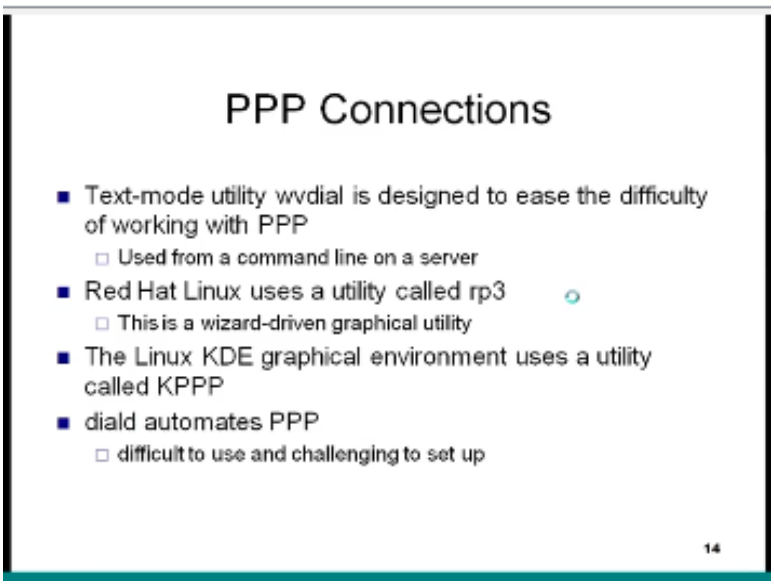
But before we go into the next one is develop network using more point-to-point protocol I just wanted to add how the address resolution works so essentially like I mean the domain name resolvers determine the appropriate domain name service responsible for the domain name person and it does so by using a sequence of queries starting from the nick most of the top level domain, so a network course is actually configured with some initial cash essentially which has some known addresses.

And then when you query to the root servers you get like the authoritative top level domain again this clarified the authoritative server authoritative name server is a server that gives the, the answers that have been like unfiltered by the original sources so again these are all like a minion self warning system with an almost imperfect I paid there the initially the domain administrator pretty much code this the domain names do one of the servers and then from that point onwards with this one and then this gay leg anymore it actually provides answers to the next level and then that pretty much like literally goes on and populates all the cells in fact if you are doing any kind of bit.

Bit searching things like that this is one of the key concepts that was developed basically that one person gets to move something by recursion you everybody else in the network knows about the same thing and this actually helps in doing a lot of the churches there the material itself what you are searching on be stored distributed across the network and then ever you want you can easily get it because you know the, the system can use recursion to gather this information presented to the top level.

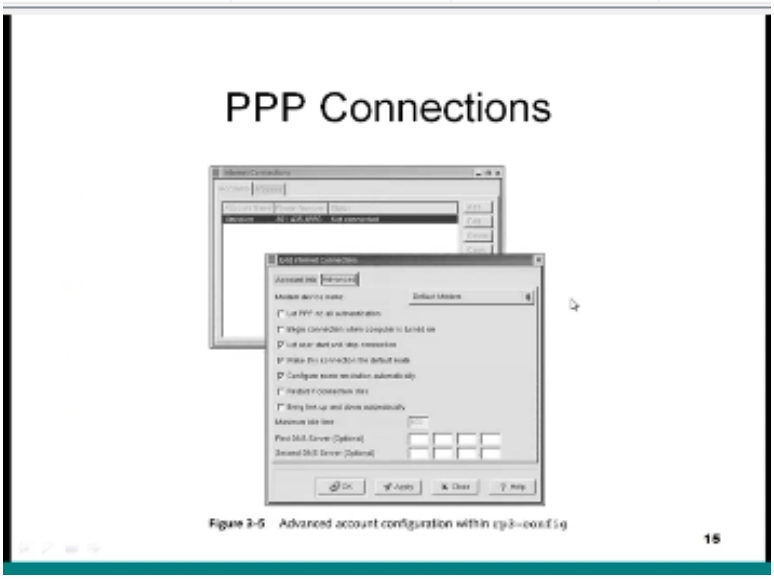
So the entire directory also known as or with this thing so and then there is also like the main registrar's who essentially resisters any II or impact all the IPS SS so let us look at the point-to-

point protocol or PPP. PPP is one of the protocols that is used to connect to internet via a modem it includes the features that you know that is security flexibility and dependability all of them then terminal emulation so emulation is another way that you can use they are pretty much what is in the remote side you emulate it into your own machine and.
So basically that is what the other thing will do or kind of mimics what we are referring to PPP is essentially more interacting the sense that whatever the messages that you are sending will be they are actually sent to the remote system and executed them one thing to note is it is like it is not basic they will secure and used to be like very challenging and challenging to configure and manage there are two advances that happen that improve the PVP security one was the password authentication protocol or PAP that stores the user data in a file that only the root user and access.
Then the second one is which is becoming more and more important is the challenge handshake authentication protocol old chap this is most secure or PPP option so one example will be like RSA the secure access token, token mechanism there it challenges you with either a password or particular pin number and then once you send the pin number then it, it starts its other needs you some variants of this methodology so you shall have a pin with a random number generator.
And this random generator is actually sync to the server inside the system or inside the company and then once you generate a random number based on your pin and that is compared against what is generated in from the system because the algorithms do allow the system to be um doing very similar to what you are so once the it understands that once the passwords do match then import that that handshake is actually added over and then that is how the user gets awesome edit and now he can do whatever he wants inside the system knows exactly what good person is and decided to has been establish.
(Refer Slide Time: 33:01)



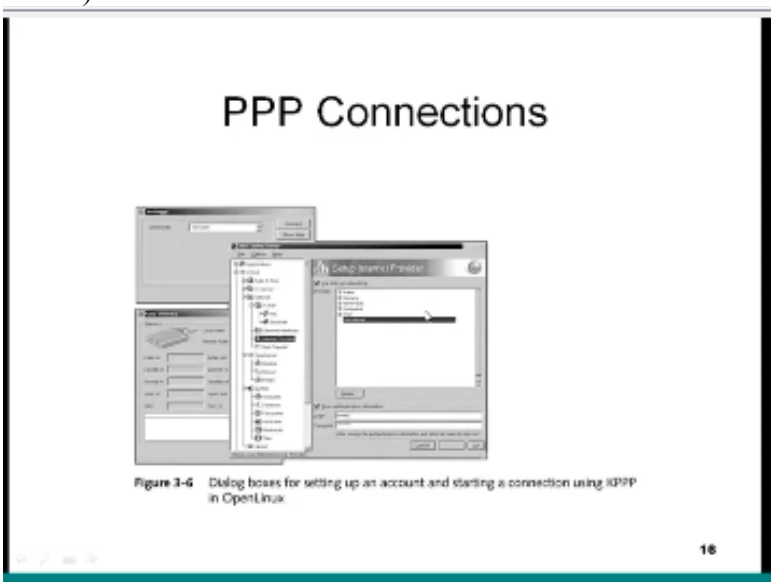
So let us look at how this connection will happen it is a text mode utility or the WV dial that pretty much works to eliminate all these difficulty in can the connecting with 50 and this one you can actually use it from the command line in the server in Red Hat Linux there is a utility or rp3 which is provided this is a Wizard driven graphical utility so it goes through the various steps to make sure that you can tell about the actions in Linux KDE graphical environment to a utility called KPPP is used and then the dial D is also like use to automate the looping butt-dialed is enough basically use a little bit more challenging setup.

(Refer Slide Time: 34:05)

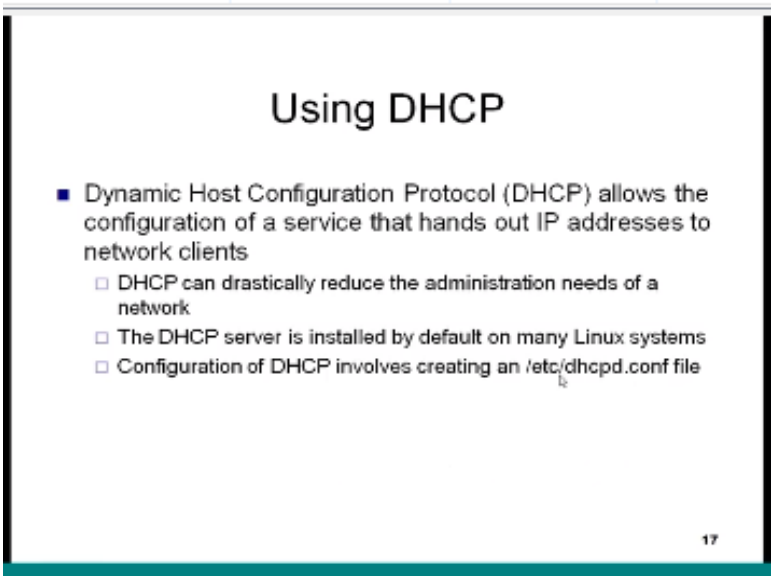


So here is one example of how do we get the PPP connection so here the many options one is the PPP do all my authentication begin connection and the computer is turned on you may or may not want to do that and then let users start and stop the connection so this is I think like a good

option so that the machine did not shut you down when you, you and then the other one is the make connection the different Rock which is also kind of important.
So that you receive the maximum usable then configure the name resolution automatically which is I think it is a good thing to do making you are considering the PVP because once you do the name resolution or Matthew then it is going to a primary source and actually getting that information and then it populates and as I mentioned the recursive population will enable that the whole thing is populated in no time.
Then there are other options for retarding the time to die then, then one thing to note this essentially like once you set up a PPP if it cannot find the connection is ensign and you can set up the time to wait for the connection to be complete you finally the it also provides the way to configure the primary DNS and the secondary before then there are some low-power features which we have also mentioned you are like winning moving up and down automatically so with inactivity time set essentially you can do.
(Refer Slide Time: 36:50)



So here there is more dialog boxes this is used to set up an account and starting a connection using the a PVP in open later so as I mentioned like the other PPP servers this in the Linux PD that the environment was easy people so using this a PPP to set up an account and start a connection I think I given you, you are familiar with some of the PPP and DHCP because we have any iphone or anything you will be working on this a lot.
(Refer Slide Time: 37:37)



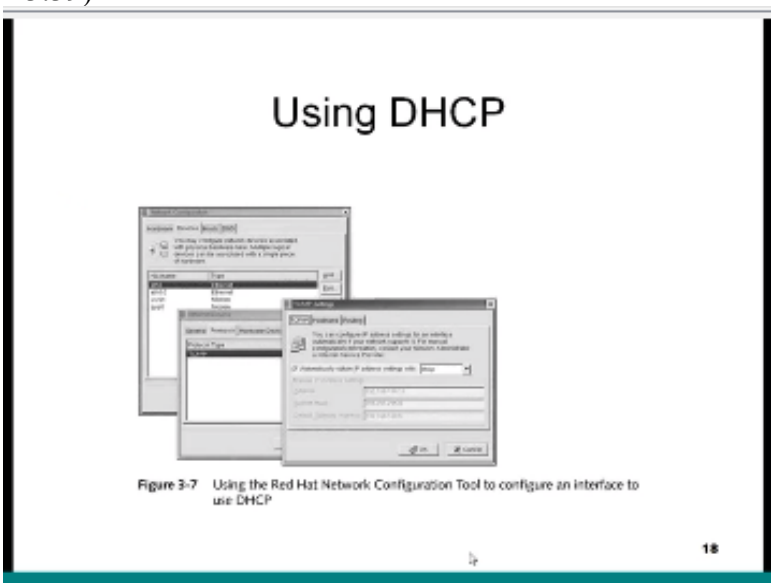
So just to give you more sense of how this remapping daily work is so as I mentioned basically like the network host is initially configured so it has at least some basic directory and then builds on the military, so then you make it query into one of the root servers to find the server authoritative for the top-level domain then once that is completed that gives you the server for the next level because it contains for that particular top-level Top what is the, the next part which is IBM and you see that the corresponding idea this.

And then you essentially like now the you send a query to the server then, the address of the server that is returned and then essentially like that will provide the address of the DNS service via server its authoritative for the second level, so now we first went to the first level domain and that gave us some information we take that information and then we submit to the second level o domain B and then now that is going to return something if that is so that is all you need you stop it right there.

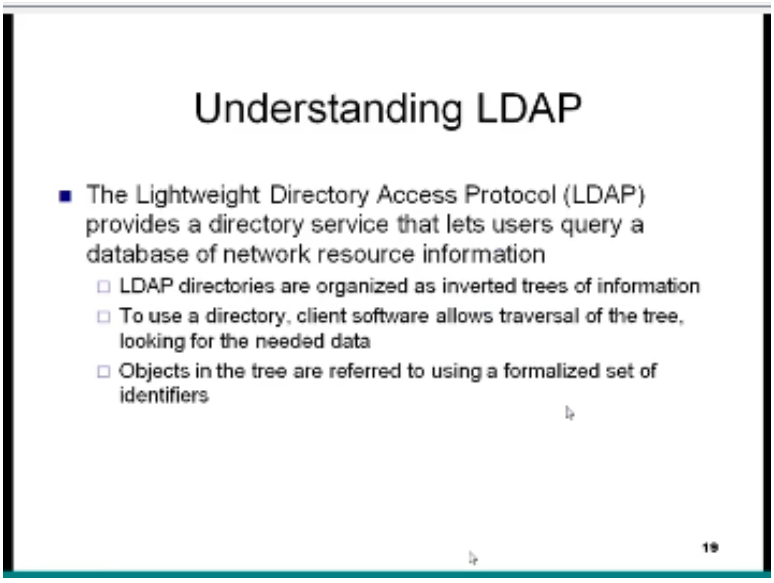
What would not continue again you can go and continue on with other sub levels as well whatever is available you, you so one thing that I wanted to add to the slide that we talked about where this is the main names this one so today like I am in dot-com and the dot net domain names they use the directory there or the domain registry from Very sign there is any the company that eats these to the main attention.

So the register who is using which domain how long is supposed to use and also what are the dates that the things will expire so just to keep in mind you, you so let us talk about DHCP a DHCP stands for dynamic host configuration protocol we learnt a little bit when we talked about the idea behind this started talking about it but continued in that lecture, so as I mentioned like I

mean initially we started with IP addressing before rocket and pretty much like I mean we wanted every machine in the world who is connected to the Internet.
I have a unique identifier but with justice for objects it is just not possible and not only that if a machine is connected to a network you know then you may want to move that machine to some other place and either replace it with a new machine or market visit the new mission but you need more addresses than what is provided so that you can be successful in doing this DNS and then also like you do not make any of the DNS s DNS you do not want to make them like the obsolete so the way to do it is this dynamic host configuration protocol.
Which lets you change the IP addresses at the time of installation or at the time of setting it up so I essentially like the DHCP I love the complication of the service the pan-flute IP addresses to metro clients and since like Gavin you are creating new ideas and essentially but it is in under the sub domain, so that it does not clash with the main domain now you can actually like keep updating whatever web address that you want all you got to do is to make sure that the DHCP server has that information and the home it is actually like so better.
So a advantage of DHCP is it can reduce for that mutation pose quite a bit the DHCP server itself involved by default on many Linux, Linux systems so you do not need to do any kind of thing for the DHCP server and you can also look at the configuration of your machine in the lamp from the flashy TV flag standard 8 b dot function con fine.
(Refer Slide Time: 43:39)

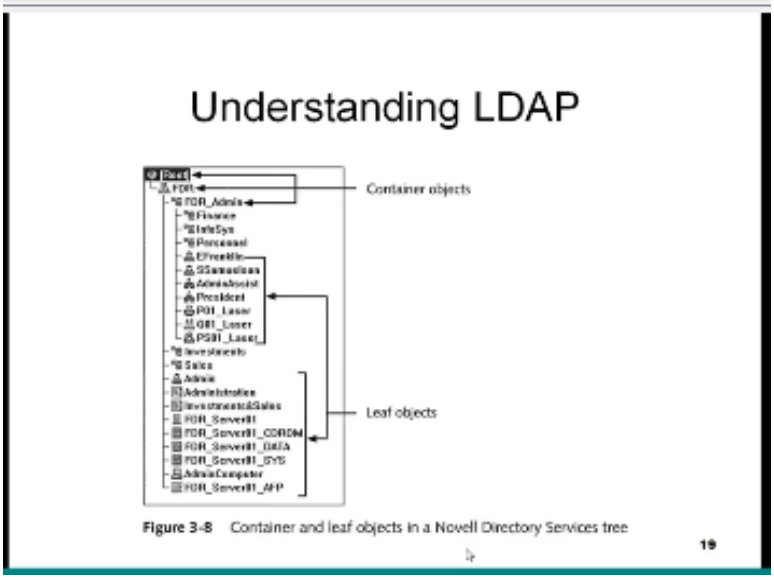


So how do you use the data so again in this section DHCP ligament we can move on figures gay DHCP graphically as shown here this is one of the things where and actually I get this is that you can do you can feel like some pointers to the blog and appear and then you can let it.
(Refer Slide Time: 44:18)



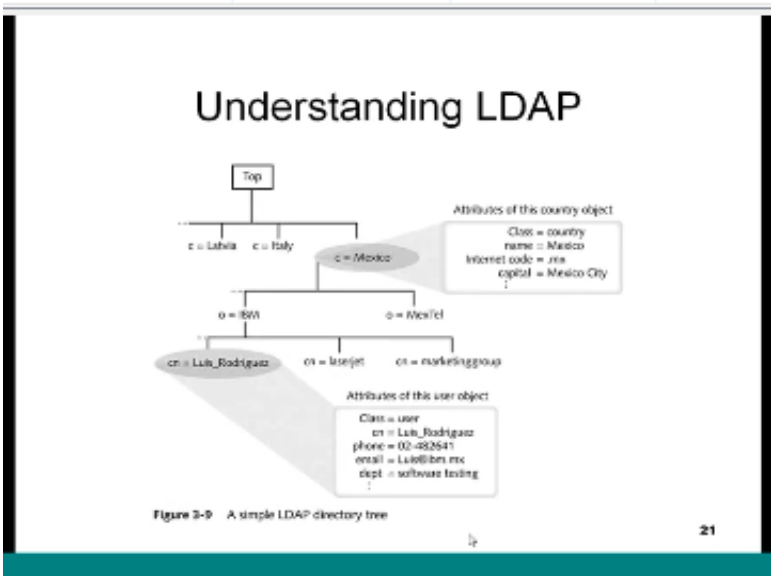
So now let us look at the LDAP or lightweight the directory access protocol this provide the directory structure that lets the users query a database of network resource information so the LDAP directories are organized as inverted trees and in order to use the directory services the kind software allows the traversal of the tree looking for the data, data objects in the same tree are referred to using a formulas set of enterprise so that is pretty much on the local directory access protocol.

(Refer Slide Time: 45:12)

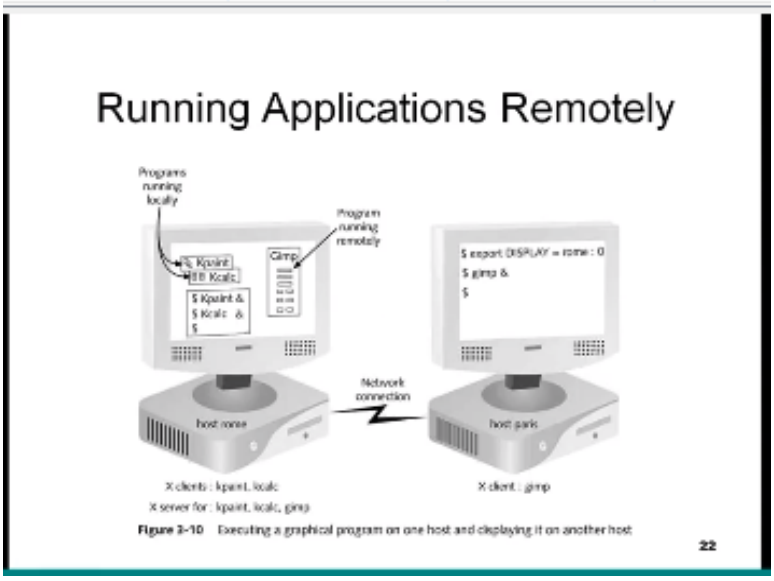


Now let us look at how it is organized so here in the LDAP you can see that basically there are two different types objects one is the container of objects and then the other one is the leaf objects and it is very easy or you can select the container objects you can see that actually the

FDR at mean they are in Pontus and all the container objects and then the, the low level items piles and exciting there the leaf objects you.
(Refer Slide Time: 45:54)

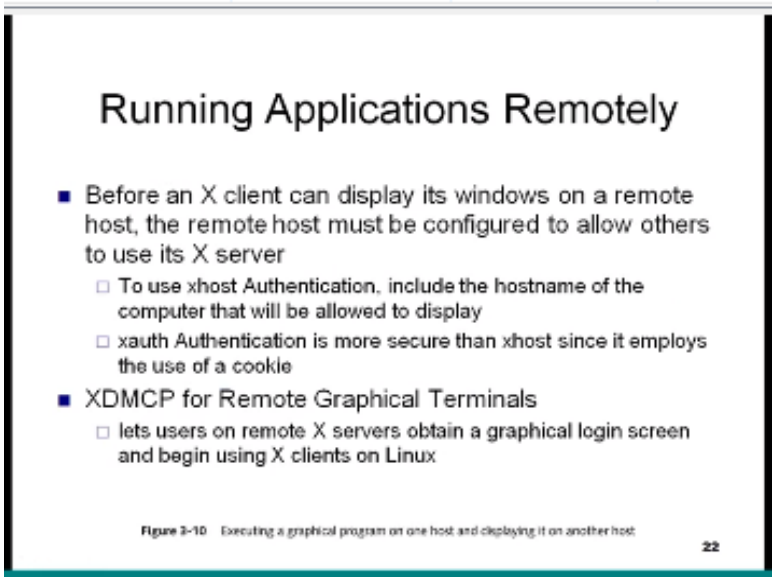


So here let us spend some more time to understand how the LDAP works so here like I mean we have a top domain called this whole top on the top we have like Latin Devine and then, then we have also like another one Mexico, and there are attributes of these country objects the attribute will be a class is country the name whatever the name of the states of the country the just the name of the, the place itself and then there is an internal code and then also the capital city but these are the four items on the form for this particular LDAP.
So like under Mexico you can still have like IBM and Excel and packets also having Italy who have ties with Italy and then you progressively go down essentially like then it is various people under a stable various works for going to hear the OPM being the Lois Rodriguez another cm is later death and third one is said marketing group tub and then from there you can still for the dog go down the hierarchy dimensional ahem you can have all the flavors of logic and also like I mean everybody is trained in those kind of things.
(Refer Slide Time: 48:36)



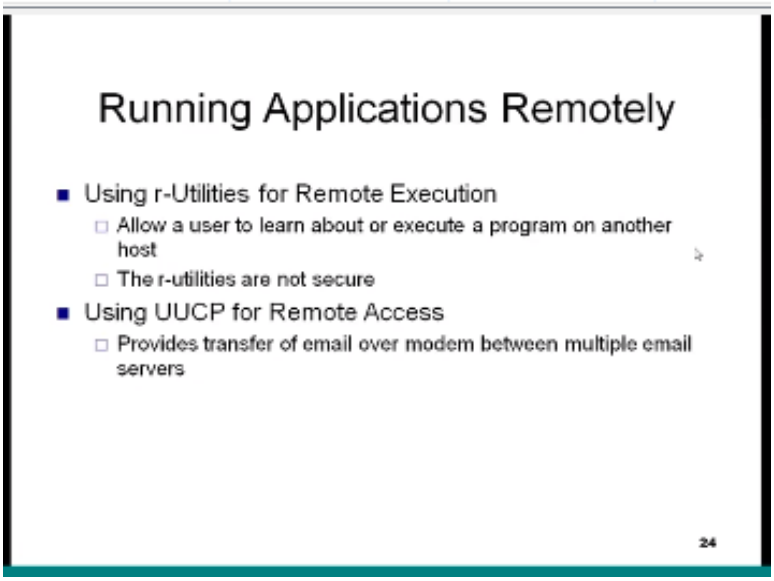
So now let us but among so how do we run applications remotely so the way that to be run or example here like I mean you can think of the host name the host computer as just few programs you, you so here all these Chapin fatale if I can depend these are all just the host program, um whereas actually like I mean take it back only the first only the first two, but then the remaining programs or the main programs the DMP or a paint decal they are more like backbone than so we have actually baby warmer than it on the wall this server, so what do you do you.

(Refer Slide Time: 50:07)

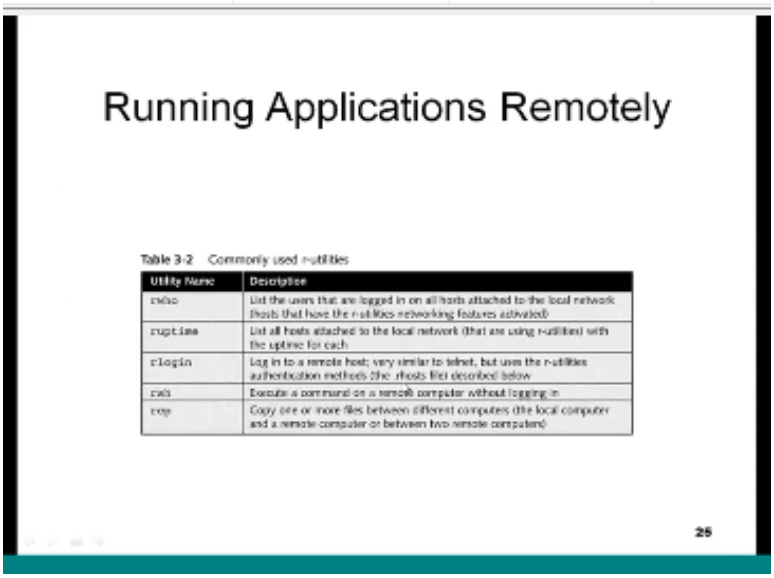


So again the number one requirement is we need to configure the remote host before we can use it so we need to tell in that computer as to what the which client will be using that resource so we need to authenticate that the user in the remote system one way to do, it is like I mean actually

there are several lakes host authentication services are available a quick one is like the echoes class and up in there it actually opens up the terminal or receiving any kind of X requests.
The X is another one which is it is more secure than a ghost X host since it employs the use of but I think like exposed is five trivalent today I want you to in fact try some of the EXO's commands and see like involving whoa and then for the remote graphical terminals the XDMCP give you the remote X service, and if you have a logical login screen or a graphical login screen and we be using the instance.
(Refer Slide Time: 51:48)



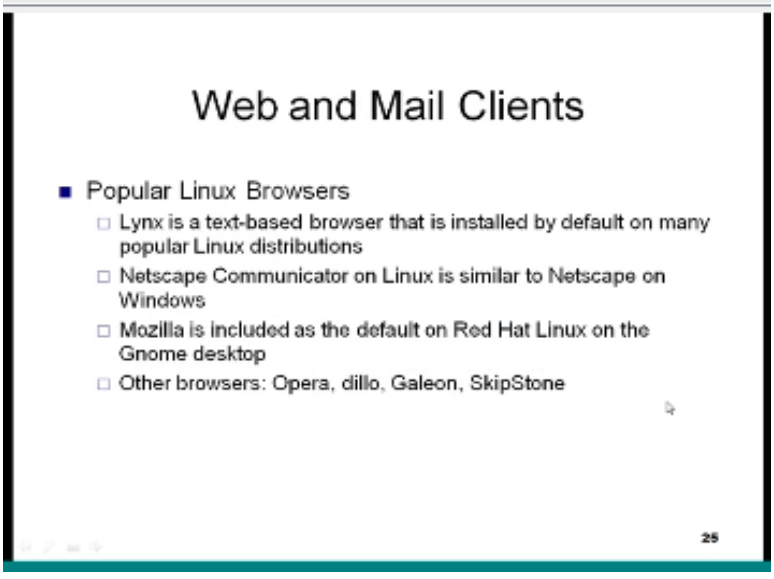
So for remote execution there R units that are available what are R units we will see in the next slide but essentially like things like copying or going to a directory those kind of things this our utilities are much more helpful to connect to a remote machine and then perform this operation and then the UUCP is essentially legged in back for the transferring emails over model between two missiles.
(Refer Slide Time: 52:27)



So the R commands that I mentioned earlier these Alexander your Linux commands are who is essentially like a remote pool so it dogs into stealing I mean what is who is using what then our halftime is the other one along the server is up and then so that they attract that are logging is a remote login this liberation be familiar with which is essentially a way to get the, the remote system respond to your requests this is our log and then our SH is another widely used command is essentially so it executes the command in the remote computer for logging.

And then RCT is the other one this is copying the files so it helps in copying that is not even puppy and then basically it is a very fast discover no sorry so the RCP is essentially to copy one or more files within two computers um it could be like either a local computer and remote computer or test between two remote computers so RCT is another widely used command.

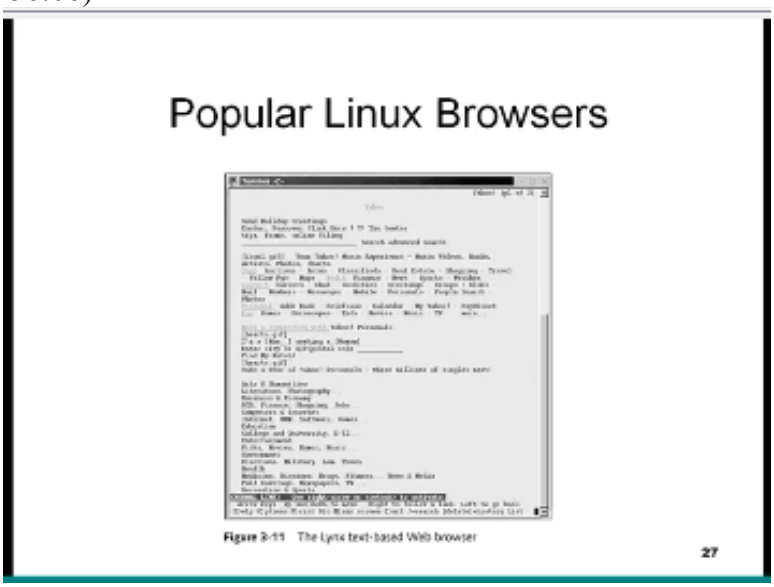
(Refer Slide Time: 54:03)



So now let us look at some of the male clients one of the most famous one is browser done so the popular Linux browsers are links if one of them which is a tech based browser and it is actually comes up with a lot of Linux machines Netscape communicator is still used then Mozilla Firefox is another one this is by far the most common one again the module setting and the open source type of traffic so and then they add a they work on that you and other growth browsers are opera below galleon skips to etc.

Now we go into more details regarding ball the links browsers so the next browsers you so again I am like let us go to this previous slide and then seal it so there are several popular Linux browser links is one of them it is the X based browser that is installed by, by default on many popular Linux installation.

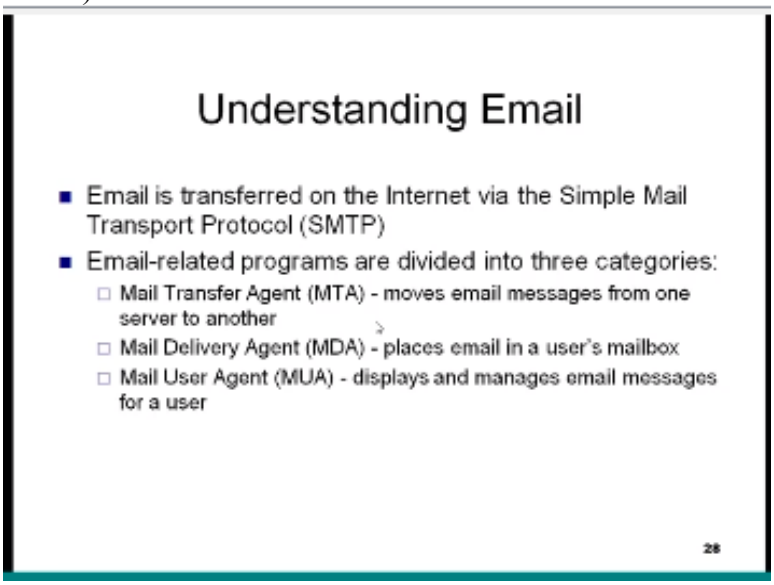
(Refer Slide Time: 56:06)



So let us look at the links browser here and it is the text browsers are kind of it is involved in this point we are all used to a lot of this graphical user interface working with the browser this text browser is kind of unique then think of this you can see that actually look at me kind of types of stuff and then basically goes on and then the way to interact it is also like I am in the bottom arrow keys that you can go to scrolling up and down.

And then you need to avoid the address in a particular box and then it displays this a good thing about these kind of text browsers are first of all they are le easy to bring up secondly the text browsers are much more faster than the graphics base walks but nowadays like I mean actually the, the processes speak so much that you do not see any difference but if you remember even the Google started as for text-based text based browser.

And actually not brother but at least a web website and then it is baking a added various graphics but even today actually like them in the basic Google is this a black page with this one small window where you can type in and then bit get the exhibition.
(Refer Slide Time: 57:49)



So the next topic is going to be the email but before we go into email I, I also wanted to text and talk about few things arm one is some the security coaching so the, the DNS software needs to consider the security aspects of it there are some vulnerability issues that was discovered and they are very exploited by some malicious users there is something called DNS cache poisoning in which the, the data is distributed the cache resolvers under the pretense of being an authoritative resolve so basically like I mean it corrupts the DNS entries so that if you're typing the google.com.
It will take you to some porn site or some other site and it is also like I mean the ones that data gets put in, in one of the servers as I mentioned basically the whole system book in the recursive mode where now when another system another system worries about the addresses suddenly like I mean you get this messages which is also like the setup wizard mess and then suddenly the caterpillar is this flows through the system some of the denial of services also can be can be used or can be can be a result of this kind of attack.
Where you capture the directory of one of the system and then put a take the URL or take the IP address or for a given URL and then whenever somebody types it in it takes you to like say , say like flash no flash no flash no which is like no place so that is kind of the denial of service attack again it is all results in this whole bit Pacific angle so in if be you obey it obey and use it

properly we can also like get back the corporation's otherwise it is basically we can easily manipulate and the destroy the whole thing.
So once these kind of attacks started coming now we are talking about the domain name security extension and the main name system security extension or DNS SEC or short these extensions offer some kind of pro graphically signed this and then since they are encrypted and that implement some of the attacks essentially so now nowadays recommend our relationship that I will devise to make it secure, a simple thing will be like a GPS secured HTTP the hypertext, hypertext Transfer Protocol.
They also have like the some spoofing effects whereas so like I mean this is another way to attack some other things which there you just change the names like for example if it is so google.com this is QTL eat or calm somebody can spell another site for you Oh, Oh GDL calm Google calm there if you type that wrongly currently like you end up in a this is altogether to the site which is which can do other things you
And this kind of vulnerability is exploited in what is called a fishing, fishing is PHI s identity it is kind of an act of because it is an attempt to actually acquiring information such as user names passwords and even credit cards by masquerading as a or covering yourself as a trustworthy site so that you can be talking to the nation and fishing even though like I mean right now it is very popular like the several sitting types and doing all the things this term fishing itself was described in till in 1987 so you know it is.
It is been around for a long, long, long time it is now famous because of the insult so with that I am going to conclude or tonight or, or this lecture we will be talking about understanding the email and continuing from this point the next lecture okay so thank you very much once again thanks.