

4417/5417

System Administration

Lecture 7

Network Services



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

What is Ubuntu Server?

‘Similar’ kernel (before v. 12.04)

Timer, memory, etc. tweaks to enhance ‘server’ role vs. desktop

Since v. 12.04, desktop & server run on the same kernel

LTS – Long Term Support



'Server' vs. 'Desktop'

Ubuntu Server doesn't include 'desktop' packages

X

GNOME, etc.

Does include 'server' packages

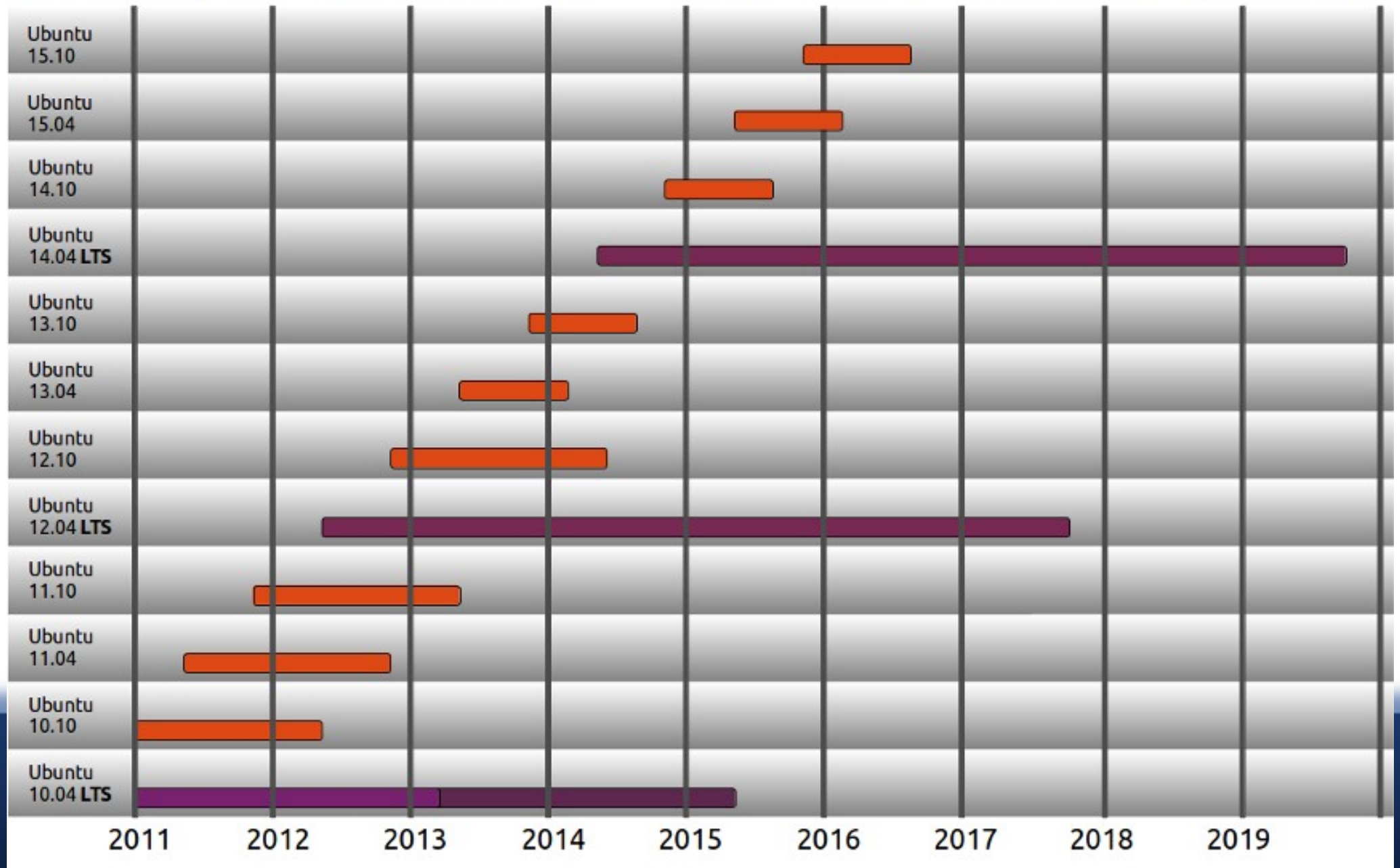
Apache2

Tomcat

Bind9, etc.



Standard Release Ubuntu Desktop LTS Ubuntu Server LTS Ubuntu & Ubuntu Server LTS



ssh

So, how do we interact with a server?

Secure Shell (SSH)

Network protocol that enables users to move data securely between machines

Used as a Telnet replacement

Not used in a GUI environment

Mostly used in a Linux/Unix environment



ssh

Makes use of public key encryption to authenticate machines

TCP port 22

Need ssh client

- Built-in in Linux

- Putty (e.g.) for Windows



ssh Install

```
sudo apt-get install  
openssh-client
```

```
sudo apt-get install  
openssh-server
```

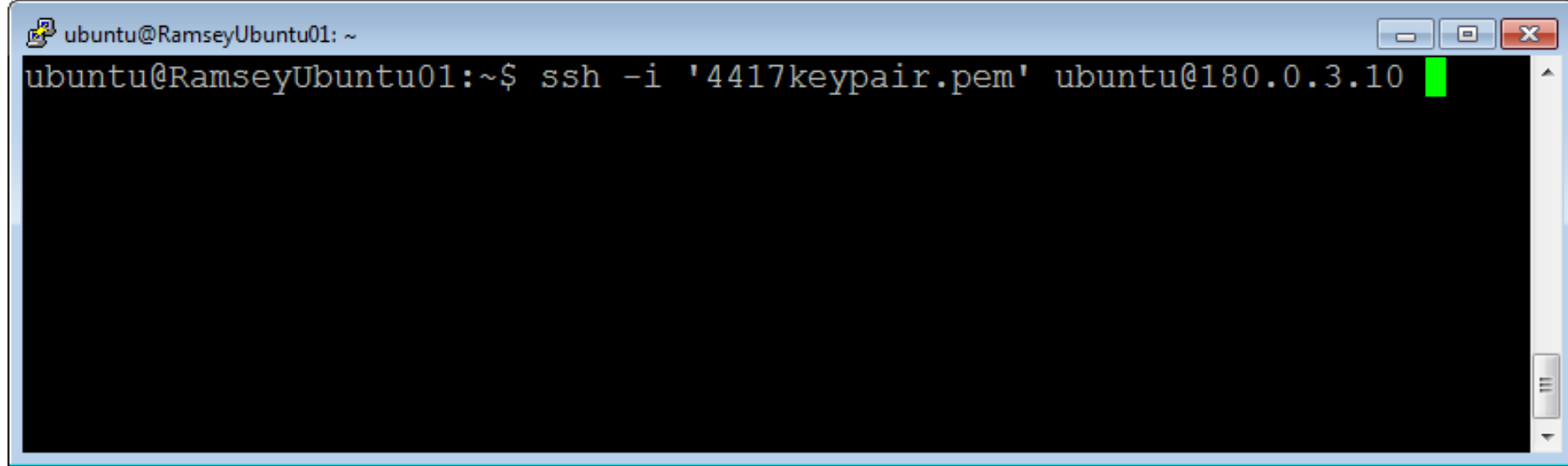
Notice that the server install creates
key pairs for you

```
..  
Processing triggers for ureadahead ...  
ureadahead will be reprofiled on next reboot  
Processing triggers for ufw ...  
Processing triggers for man-db ...  
Setting up openssh-server (1:5.5p1-4ubuntu5) ...  
Creating SSH2 RSA key; this may take some time ...  
Creating SSH2 DSA key; this may take some time ...  
* Stopping OpenBSD Secure Shell server sshd  
ssh start/running, process 1831
```



ssh

Using ssh to connect
is simple

A terminal window titled 'ubuntu@RamseyUbuntu01: ~' with standard window controls. The command 'ssh -i '4417keypair.pem' ubuntu@180.0.3.10' is entered at the prompt. A green cursor is visible at the end of the command.

```
ubuntu@RamseyUbuntu01:~$ ssh -i '4417keypair.pem' ubuntu@180.0.3.10
```

```
ssh -i [path-to-key-file.pem] <IP>
```

or

```
ssh -i [path-to-key-file.pem] user@<IP>
```



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

ssh Keypair

On the server

```
ssh-keygen -t dsa    # -t = 'type'
```

Stores public key in the `~/.ssh/id_dsa.pub` file

Copy public key to remote host

```
ssh-copy-id username@remotehost
```



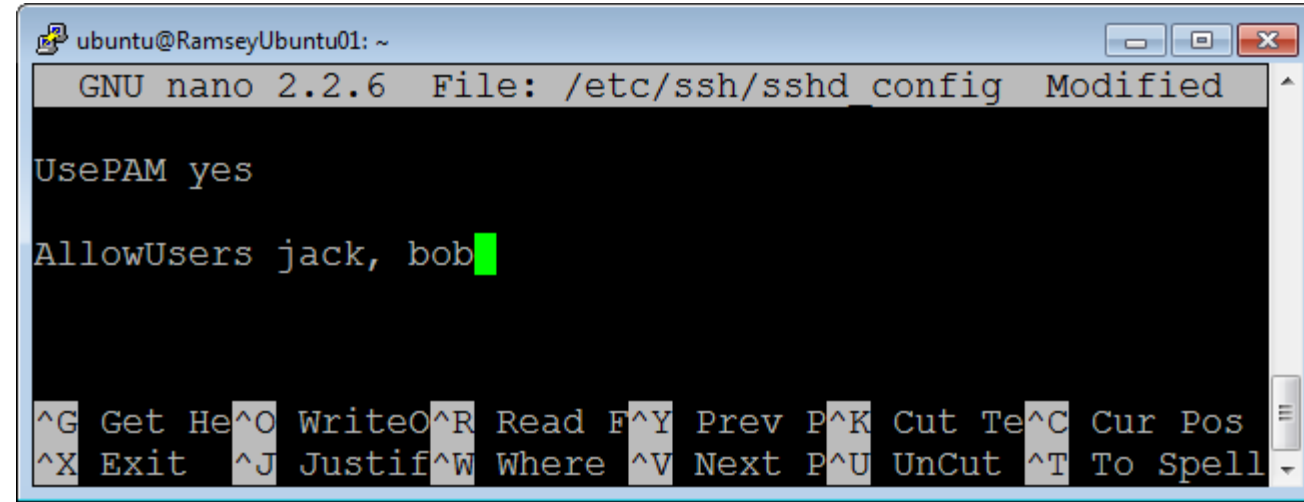
Add ssh Users

```
sudo nano  
/etc/ssh/sshd_config
```

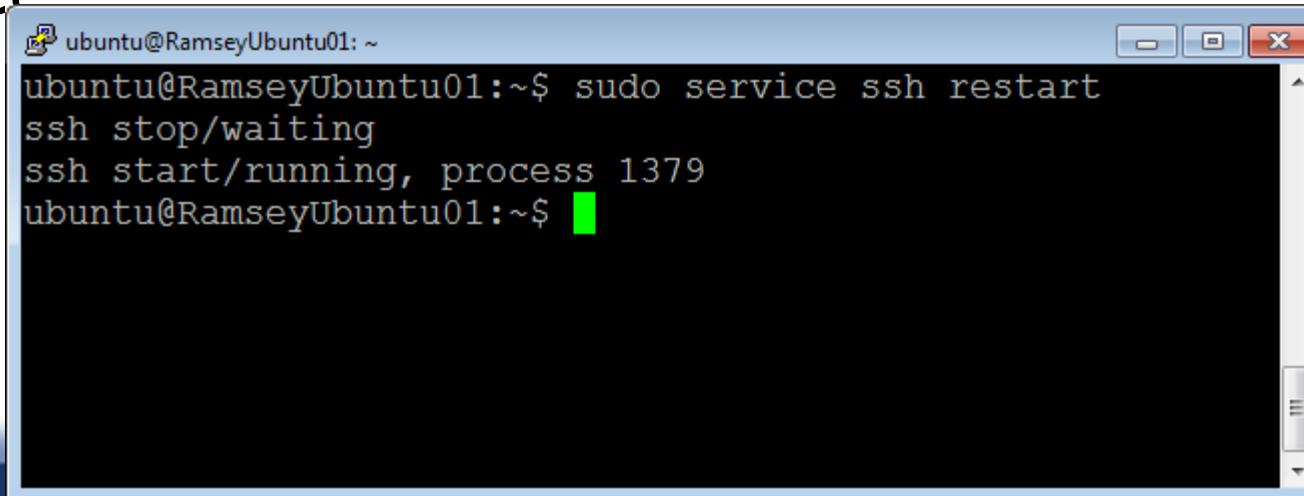
At the end of the file

```
AllowUsers user1, user2, etc
```

Restart Server

A screenshot of a terminal window showing the nano text editor. The title bar indicates the user is 'ubuntu@RamseyUbuntu01' and the file being edited is '/etc/ssh/sshd_config'. The editor shows 'UsePAM yes' and 'AllowUsers jack, bob' with a green cursor at the end of the second line. A help menu is visible at the bottom of the editor.

```
ubuntu@RamseyUbuntu01: ~  
GNU nano 2.2.6 File: /etc/ssh/sshd_config Modified  
  
UsePAM yes  
  
AllowUsers jack, bob  
  
^G Get He^O WriteO^R Read F^Y Prev P^K Cut Te^C Cur Pos  
^X Exit ^J Justif^W Where ^V Next P^U UnCut ^T To Spell
```

A screenshot of a terminal window showing the execution of the 'sudo service ssh restart' command. The output shows the ssh service stopping and then starting as a new process (1379).

```
ubuntu@RamseyUbuntu01:~$ sudo service ssh restart  
ssh stop/waiting  
ssh start/running, process 1379  
ubuntu@RamseyUbuntu01:~$
```



ftp

Not secure

Originally designed to move files around a network

On the Internet, HTTP has taken its place

Did I mention it is not secure?

Everything sent in clear text

Even passwords



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

sftp

If supported, is secure

Uses **ssh** to connect, instead of telnet

Demo



sftp



FileZilla interface showing an SFTP connection to csci1710.net.

Host: Username: Password: Port: Quickconnect

Status: Retrieving directory listing of "/home/admin" ...
Status: Listing directory /home/admin
Status: Directory listing of "/home/admin" successful

Local site: \\ares26cloud\www\csci1710.net\ Remote site: /home/admin

Local site contents:

- Desktop
- Documents
- This PC
 - C:
 - D: (TOSHIBA EXT)
 - E: (KINGSTON)
 - F:
 - Y: (\\ares26cloud\www)

Remote site contents:

- boot
- dev
- etc
- home
 - admin
 - scripts
 - alamdara
 - allika

Local site file listing:

Filename	Filesize	Filetype	Last modified
..			
assignments		File folder	2/24/2016 9:26:09 ...
css		File folder	2/24/2016 9:26:23 ...
downloads		File folder	2/24/2016 9:26:21 ...
examples		File folder	2/24/2016 9:22:05 ...
fonts		File folder	2/24/2016 9:26:12 ...
images		File folder	3/14/2016 8:24:47 ...
js		File folder	2/24/2016 9:26:18 ...
labs		File folder	2/28/2016 9:37:21 ...
lecture		File folder	2/24/2016 9:20:51 ...
php		File folder	2/24/2016 9:26:15 ...

23 files and 12 directories. Total size: 165,642 bytes

Remote site file listing:

Filename	Filesize	Filetype	Last modified
..			
scripts		File folder	3/17/2016 9:19:...
.bash_logout	220	BASH_LOG...	12/16/2015 1:5...
.bashrc	3,637	BASHRC File	12/16/2015 1:5...
.profile	675	PROFILE File	12/16/2015 1:5...

3 files and 1 directory. Total size: 4,532 bytes

Queue: empty

Server 2008/2012



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Introduction to Remote Access

Modem

Modulator/demodulator

Converts a transmitted digital signal to an analog signal for a telephone line

Converts a received analog signal to a digital signal for use by a computer

RRAS

Turns server into a dial-up Remote Access Services (RAS) server capable of handling hundreds of simultaneous connections



Introduction to Remote Access

Routing and Remote Access Services (RRAS)

Enable routing and remote access through virtual private networking and dialup networking

Virtual private network (VPN)

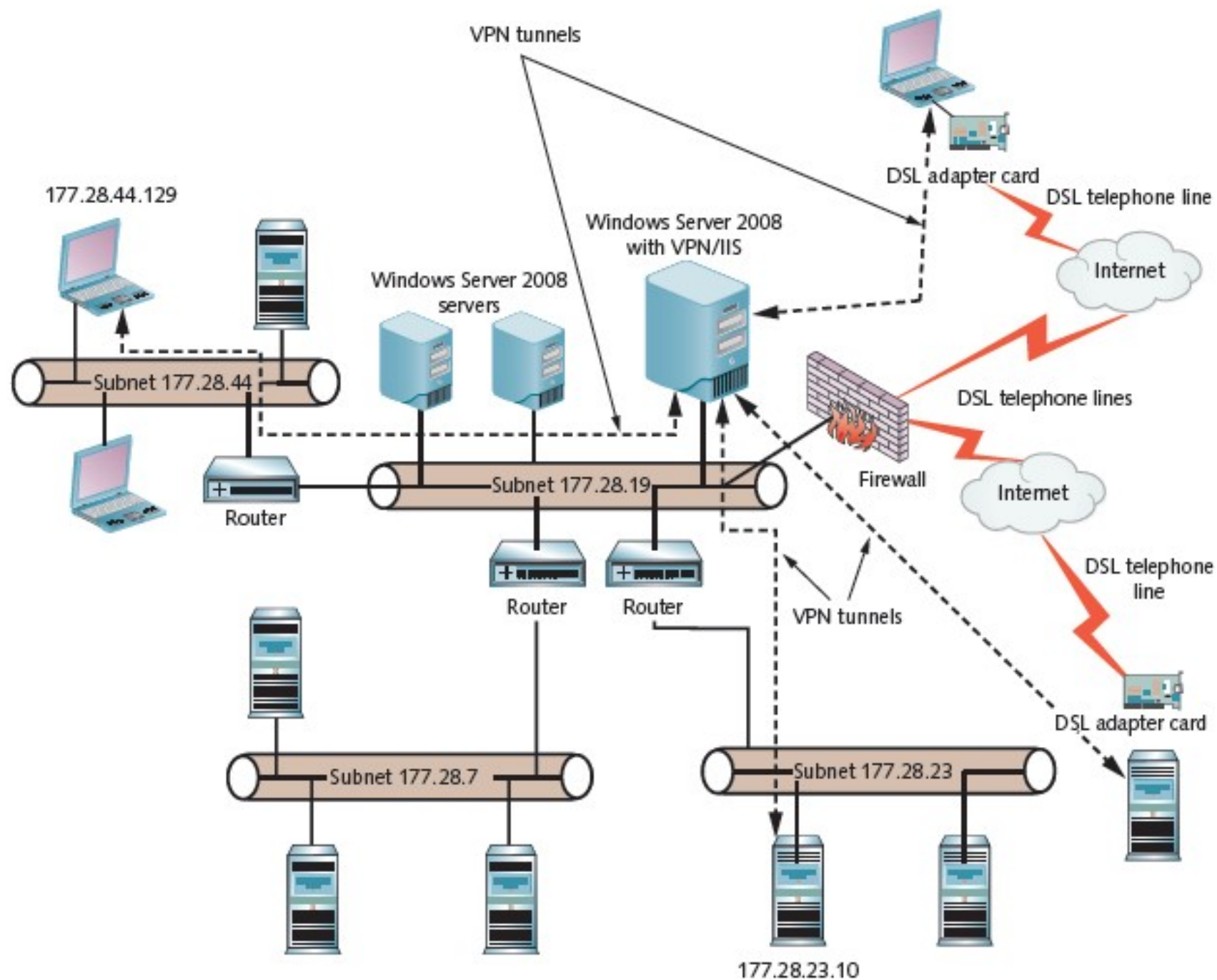
Tunnel through a larger network that is restricted to designated member clients only

Dial-up networking

Using a telecommunications line and a modem to dial into a network or specific computers on a network



A VPN network



Implementing a Virtual Private Network

VPN

Uses LAN and tunneling protocols

Encapsulates data as it is sent across a public network

Benefits of using a VPN

Users can connect through a local ISP to the remote network

Ensures that any data sent across a public network is secure

Encrypted tunnel



Using Remote Access Protocols

Function of the remote access protocol

- Encapsulate a packet

- TCP/IP is the most commonly used transport protocol

- Encapsulated in a remote access protocol for transport over a WAN

Other legacy transport protocols

- IPX for legacy NetWare networks

- NetBEUI (NetBios Extended User Interface) for legacy Microsoft networks

- Not supported by Windows Server 2008/2012



Using Remote Access Protocols

Serial Line Internet Protocol (SLIP)

Originally designed for UNIX environments

Provides point-to-point communications using TCP/IP

Compressed Serial Line Internet Protocol (CSLIP)

Newer version of SLIP

Compresses header information in each packet

SLIP and CSLIP do not support

Network connection authentication



Using Remote Access Protocols

Point-to-Point Protocol (PPP)

A data link protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression

Has more capability than SLIP

Remote access protocols

Point-to-Point Tunneling Protocol (PPTP)

Layer Two Tunneling Protocol (L2TP)

Secure Socket Tunneling Protocol (SSTP)



Using Remote Access Protocols

Point-to-Point Tunneling Protocol (PPTP)

Offers PPP-based authentication techniques

Encrypts data carried by PPTP through using Microsoft Point-to-Point Encryption

Microsoft Point-to-Point Encryption (MPPE)

Starting-to-ending-point encryption technique that uses special encryption keys varying in length from 40 to 128 bits



Using Remote Access Protocols

Layer Two Tunneling Protocol (L2TP)

Works similarly to PPTP

Doesn't provide security itself, often used with -

IP Security (IPsec)

IP-based secure communications and encryption standards created through the Internet Engineering Task Force (IETF)



Using Remote Access Protocols

Secure Socket Tunneling Protocol (SSTP)

Employs PPP authentication techniques

Encapsulates data packet in the Hypertext Transfer Protocol (HTTP)



Using Remote Access Protocols

Secure Sockets Layer (SSL)

Data encryption technique employed between a server and a client

Released in 1995 by Netscape

Now, the standard is Transport Layer Security (TLS)

First released in 1999, latest version 1.2 in 2008

Draft for ver 1.3 still on the table

Often (still) referred to as 'SSL'



Using Remote Access Protocols

Digital Certificates

Used by TLS to establish session between two parties

Certify ownership of a public key by the named subject of the certificate

Allows relying parties to rely on signatures

Certificate Authorities

Trusted 3rd party

Issue certificates both certificate-holder and relying party trust the CA



Using Remote Access Protocols

*** New ***

Free certificates:

<https://letsencrypt.org/>



Using Remote Access Protocols

PPP, PPTP, and L2TP are available in:

Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8

Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2012

SSTP is available in:

Windows Server 2008, Windows Server 2012, Windows Vista, Windows 7, Windows 8



Using Remote Access Protocols

Communications technologies

Technology	Description
Asynchronous modem	A modem from which communications occur in discrete units, and in which the start of a unit is signaled by a start bit at the front, and a stop bit at the back signals the end of the unit
Cable modem	A digital modem device designed for use with the cable TV system, providing high-speed data transfer
Dial-up and high-speed leased lines	Telecommunications lines or bandwidth on telecommunications lines that can be leased from a telecommunications company
Digital subscriber line (DSL)	A technology that uses advanced modulation techniques on regular telephone lines for high-speed networking at speeds of up to about 52 Mbps between subscribers and a telecommunications company
Frame relay	A WAN communications technology that relies on packet switching and virtual connection techniques to transmit at rates from 56 Kbps to 45 Mbps
Integrated Services Digital Network (ISDN)	A telecommunications standard for delivering data services over digital telephone lines with a current practical limit of 1.536 Mbps and a theoretical limit of 622 Mbps
Synchronous modem	A modem that communicates using continuous bursts of data controlled by a clock signal that starts each burst
T-carrier	A dedicated leased telephone line that can be used for data communications over multiple channels for speeds of up to 400.352 Mbps
X.25	An older packet-switching protocol for connecting remote networks at speeds up to 2.048 Mbps



Configuring a VPN Server

Install Network Policy and Access Services role

Configure a Microsoft Windows Server 2008/2012 server as a network's VPN server

Configure protocols to provide VPN access to clients

Configure a VPN server as a DHCP Relay Agent for TCP/IP communications

Configure the VPN server properties

Configure a remote access policy for security



Configuring a VPN Server

Windows Server 2008/2012 require at least two network interfaces in the computer:

- One for the connection to the LAN

- One for a connection to the physical VPN network



Configuring a VPN Server

Routing and remote access options

Option	Description
Remote access (dial-up or VPN)	Use this option to set up remote access services to the network through a Windows Server 2008 server, using either dial-up modems or a VPN network connection.
Network Address Translation (NAT)	Use this option to enable Internet access by employing Network Address Translation (NAT) . Used by Microsoft Routing and Remote Access Services and by firewalls, NAT translates IP addresses on an internal network so that the actual IP addresses cannot be determined on the Internet, because each address is seen externally on the Internet as one or more decoy addresses. The advantages of using NAT include (1) addresses on the internal network do not have to be registered on the Internet, because they are only seen on the local internal network and (2) users on the internal network gain some measure of protection from Internet intruders.
Virtual private network (VPN) access and NAT	Use this option when you want to configure the server so that users can access it using a VPN and so that internal network VPN users take advantage of NAT.
Secure connection between two private networks	Use this option for secure communications between two servers over the Internet, such as one server at a branch location in St. Louis and another at the headquarters in Chicago (both servers must be configured with this option).
Custom configuration	Use this option when you want to customize the routing and remote access capabilities.



Configuring a VPN Server

Remote access protocol or service	Port(s)	Transport protocol
PPTP	1723	TCP
L2TP	500, 1701, and 4500 (4500 if you are using NAT)	UDP
SSTP	443	TCP
VPN	1194	TCP and UDP
DHCPv4 Relay Agent	67 and 68	UDP
DHCPv6 Relay Agent	547	UDP
Radius Server	1812	UDP

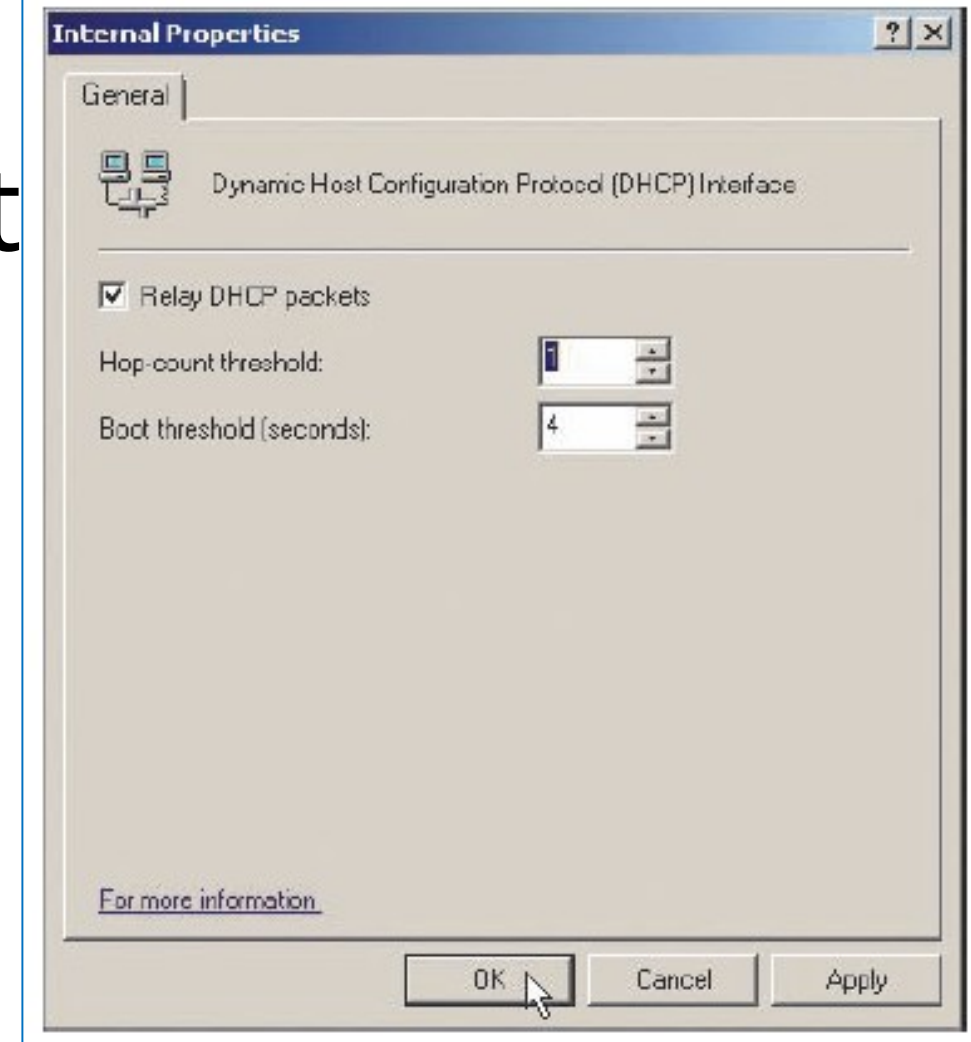
Ports to open in the Windows Firewall for a VPN

Configuring VPN Properties

Routing and Remote Access tool

Right-click the VPN server in the tree

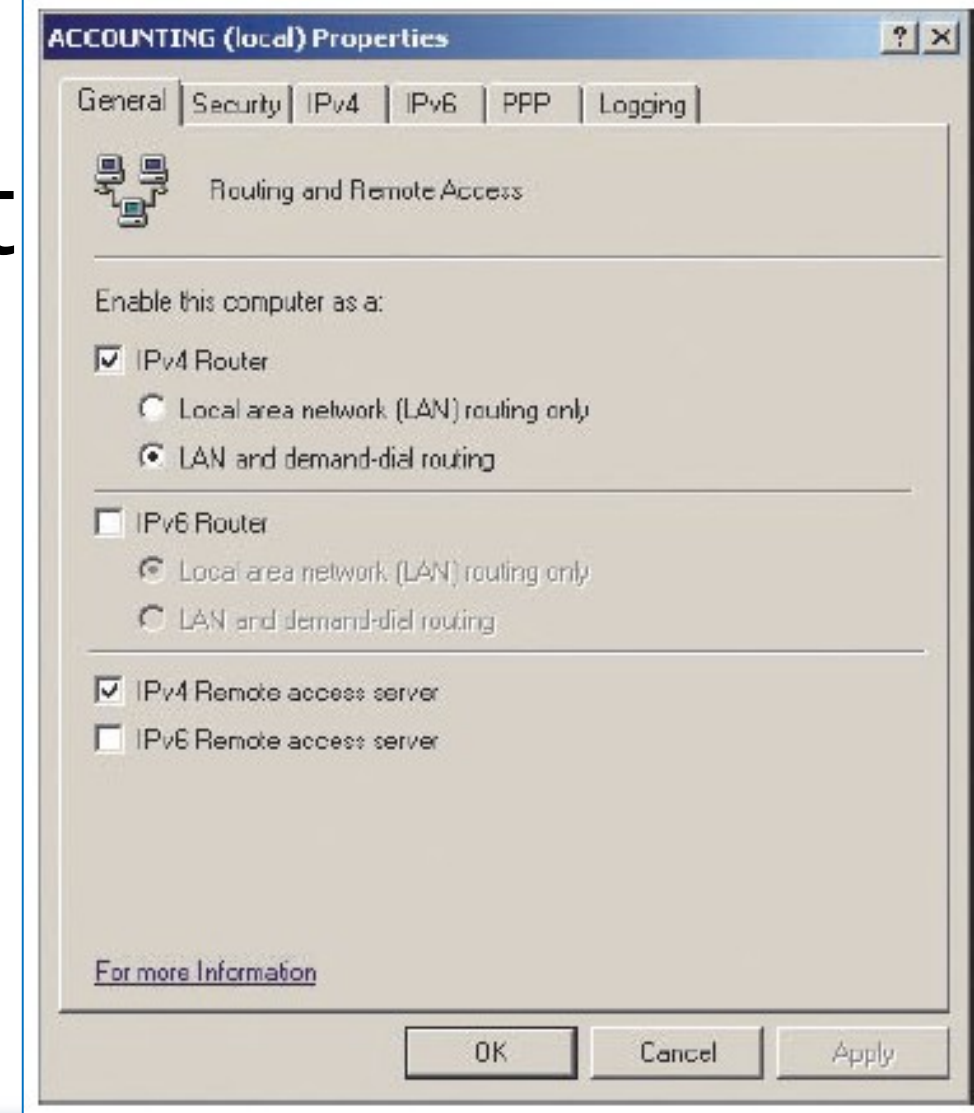
Click Properties



Configuring the interface properties

Configuring VPN Properties

VPN server properties



Configuring VPN Properties

Property tab	Description
General	Allows you to enable the server as a router and/or a remote access server (by default, it is set up as an IPv4 router and remote access server)
Security	If Network Policy Server (NPS) is not installed, this tab allows you to configure an authentication provider and accounting provider (such as a RADIUS server); selecting the Authentication Methods button allows you to enable authentication protocols on the RAS server or enable unauthenticated access
IPv4	Allows you to enable IPv4 forwarding; from this tab, you can also change how IP addresses are assigned to clients using either a DHCP server or a static address pool
IPv6	Allows you to enable IPv6 forwarding and default route advertisement; also enables you to assign the IPv6 prefix
PPP	Allows you to enable PPP options such as Multilink or Multilink PPP (MPPP) connections; Multilink enables you to aggregate multiple incoming lines, such as ISDN lines into one logical connection (if Multilink is used, the lines must be aggregated at the server and at the remote connection or device)
Logging	Allows you to enable PPP logging and specify what type of events to log



Configuring Multilink and Bandwidth Allocation Protocol

Multilink

Combine or aggregate two or more communications channels so they appear as one large channel

Aggregated links

Multilink must be implemented in the client as well as in the server

Older connection technology compared with DSL or wireless metropolitan area networks

Bandwidth Allocation Protocol (BAP)

Ensure that a client's connection has enough speed or bandwidth for a particular application



Configuring VPN Security

When a user accesses a VPN server:

Access is protected by the account access security that already applies
Through a group policy or the default domain security policy

Elements of a Remote Access Policy

Access permission
Conditions
Constraints
Settings





Configuring VPN Security

Encryption Option	Description
Basic encryption (MPPE 40-bit)	Enables clients using 40-bit encryption key MPPE (available in Windows operating systems sold throughout the world), or clients can use 56-bit IPsec or DES encryption
Strong encryption (MPPE 56-bit)	Enables clients using 56-bit encryption key MPPE, 56-bit IPsec encryption, or DES
Strongest encryption (MPPE 128-bit)	Enables clients using 56-bit IPsec, Triple DES, or MPPE 128-bit encryption
No encryption	Enables clients to connect and not employ data encryption (not recommended)

RAS encryption options

Configuring a Dial-Up Remote Access Server

Dial-up remote access server compatible with:

- Asynchronous modems

- Synchronous modems

- Null modem communications

- Regular dial-up telephone lines

- Leased telecommunication lines

- ISDN lines (and digital “modems”)

- X.25 lines

- DSL lines

- Cable modem lines

- Frame relay lines



Configuring Dial-Up Security

Callback security

- Server calls back the remote computer

- Verify telephone number in order to discourage a hacker

Options available in Windows Server 2008/2012:

- No Callback

- Set by Caller (Routing and Remote Access Service only)



Questions?

Next Up: Remote Desktop Services



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Copyrights



Presentation prepared by and copyright of John Ramsey,
East Tennessee State University, Department of
Computing . (ramseyjw@etsu.edu)



- Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.
- IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.
- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- Oracle is a registered trademark of Oracle Corporation.
- HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
- Java is a registered trademark of Sun Microsystems, Inc.
- JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.
- SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.
- Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.
- ERPsims is a registered copyright of ERPsims Labs, HEC Montreal.
- Other products mentioned in this presentation are trademarks of their respective owners.



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer