

Workshop Systems in Gaithersburg

Lab Diagrams for z/OS Network Security Class



Student Visual

IP Addresses: 192.168.20.64/26

IBM Technical Sales Support
Washington Systems Center



Linda Harrison
lharriso@us.ibm.com

IP Network 192.168.20.64/26 (255.255.255.192)

Agenda

- General Lab Connectivity
- How to Access the Lab Systems
- Lab Testing Flow Pictures
- Procs, Commands, and Files

Class Systems



- Please maintain the integrity of the lab systems!
- Do not customize the systems beyond what is asked of you in the labs!
- You may not use the provided Communications Server Configuration Assistant z/OSMF for any purposes outside of this Workshop.
- You are not authorized to copy or reproduce the materials for any purpose outside of this Workshop.

General Lab Connectivity

Lab Systems Physical Connectivity



Student Visual

TCPIP1 Maintenance Addresses: 192.168.20.8n

IP Network for Telnet, FTP, etc. (192.168.20.64/26)

z/VM

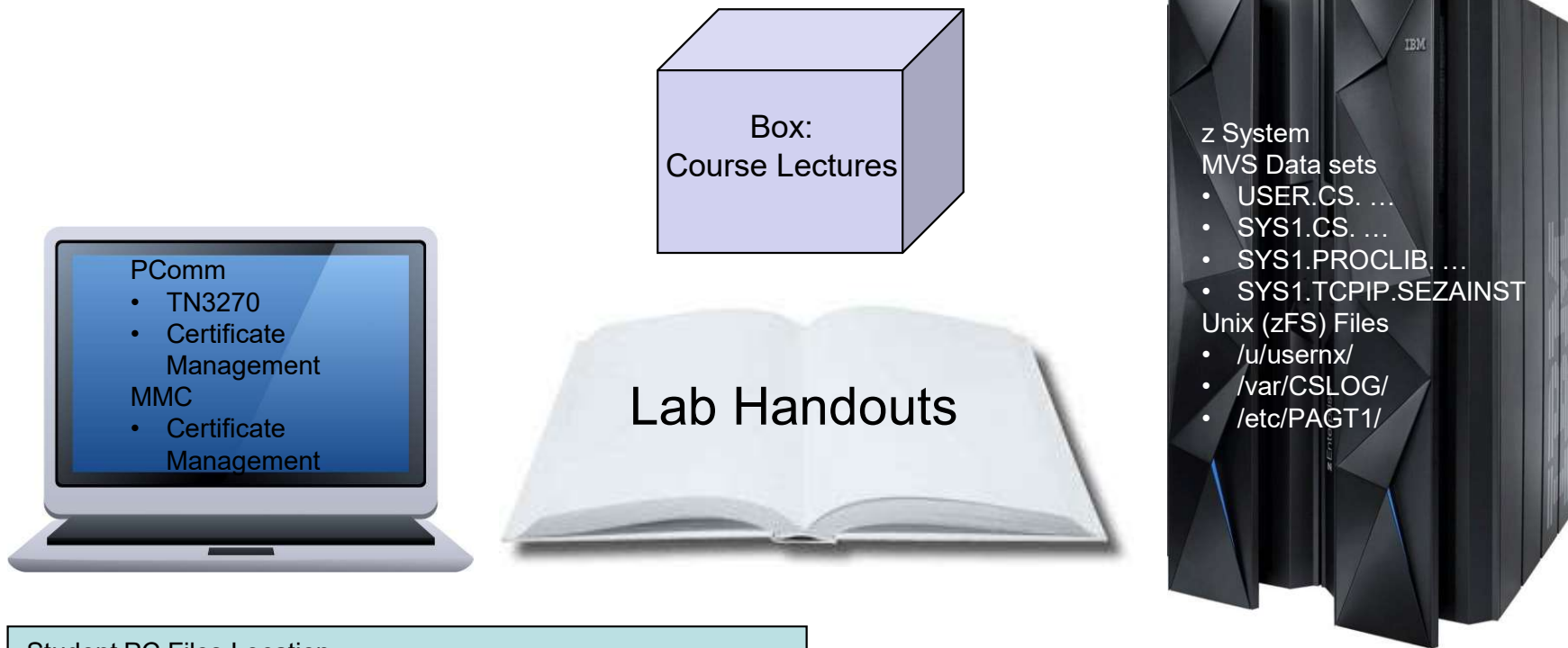
QDIO OSA (OSD) – MVS on Guest LAN under VM

MVS1/ZOS1	MVS2/ZOS2	MVS3/ZOS3	MVS4/ZOS4	MVS5/ZOS5	MVS6/ZOS6	MVS7/ZOS7	MVS8/ZOS8	MVS9/ZOS9
TCPIP1 PROF=PROFCCL1 (Maintenance) 192.168.20.81/26	TCPIP1 PROF=PROFCCL2 (Maintenance) 192.168.20.82/26	TCPIP1 PROF=PROFCCL3 (Maintenance) 192.168.20.83/26	TCPIP1 PROF=PROFCCL4 (Maintenance) 192.168.20.84/26	TCPIP1 PROF=PROFCCL5 (Maintenance) 192.168.20.85/26	TCPIP1 PROF=PROFCCL6 (Maintenance) 192.168.20.86/26	TCPIP1 PROF=PROFCCL7 (Maintenance) 192.168.20.87/26	TCPIP1 PROF=PROFCCL8 (Maintenance) 192.168.20.88/26	TCPIP1 PROF=PROFCCL9 (Maintenance) 192.168.20.89/26
TCPIPT PROF=TCP1ALL TN3270=TN3270T STVIPA= 192.168.20.101/26 QDIO= 192.168.20.91/26 XCF=10.1.1.1/24 DVIPA1= 192.168.20.111/26 DVIPA2= 192.168.20.121/26 HiperSockets= 172.168.20.1/28	TCPIPT PROF=TCP2A TN3270=TN3270T STVIPA= 192.168.20.102/26 QDIO= 192.168.20.92/26 XCF=10.1.1.2/24 DVIPA1= 192.168.20.112/26 DVIPA2= 192.168.20.122/26 HiperSockets= 172.168.20.2/28	TCPIPT PROF=TCP3A TN3270=TN3270T STVIPA= 192.168.20.103/26 QDIO= 192.168.20.93/26 XCF=10.1.1.3/24 DVIPA1= 192.168.20.113/26 DVIPA2= 192.168.20.123/26 HiperSockets= 172.168.20.3/28	TCPIPT PROF=TCP4A TN3270=TN3270T STVIPA= 192.168.20.104/26 QDIO= 192.168.20.94/26 XCF=10.1.1.4/24 DVIPA1= 192.168.20.114/26 DVIPA2= 192.168.20.124/26 HiperSockets= 172.168.20.4/28	TCPIPT PROF=TCP5A TN3270=TN3270T STVIPA= 192.168.20.105/26 QDIO= 192.168.20.95/26 XCF=10.1.1.5/24 DVIPA1= 192.168.20.115/26 DVIPA2= 192.168.20.125/26 HiperSockets= 172.168.20.5/28	TCPIPT PROF=TCP6A TN3270=TN3270T STVIPA= 192.168.20.106/26 QDIO= 192.168.20.96/26 XCF=10.1.1.6/24 DVIPA1= 192.168.20.116/26 DVIPA2= 192.168.20.126/26 HiperSockets= 172.168.20.6/28	TCPIPT PROF=TCP7A TN3270=TN3270T STVIPA= 192.168.20.107/26 QDIO= 192.168.20.97/26 XCF=10.1.1.7/24 DVIPA1= 192.168.20.117/26 DVIPA2= 192.168.20.127/26 HiperSockets= 172.168.20.7/28	TCPIPT PROF=TCP8A TN3270=TN3270T STVIPA= 192.168.20.108/26 QDIO= 192.168.20.98/26 XCF=10.1.1.8/24 DVIPA1= 192.168.20.118/26 DVIPA2= 192.168.20.128/26 HiperSockets= 172.168.20.8/24	TCPIPT PROF=TCP9A TN3270=TN3270T STVIPA= 192.168.20.109/26 QDIO= 192.168.20.99/26 XCF=10.1.1.9/24 DVIPA1= 192.168.20.119/26 DVIPA2= 192.168.20.129/26 HiperSockets= 172.168.20.9/24

TCPIPT Maintenance Addresses: 192.168.20.9n and 192.168.20.1ab

This is a CINET system. Students do not TOUCH TCPIP1 with PROFCCLn, but they telnet into the MVS system and prepare the TCPIP Profile named TCP1A-TCP7A or TCP11A – TCP73A. This profile is started with TCPIPT.

Lab Environment



Student PC Files Location
c:\CS_Security
User IDs
USERnx where "n" = ZOS system number and "x" = Team Suffix
i.e. user21, user31, user41, etc.

How to Access the Lab Systems

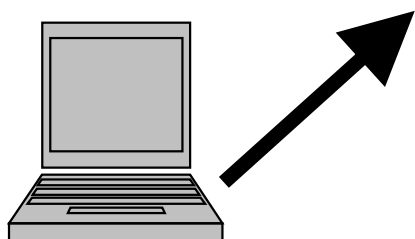
How to Access MVS1-9 via TN3270 to Stack TCPIP1 or TCPIPT

MVS1	MVS2	MVS3	MVS4	MVS5	MVS6	MVS7	MVS8	MVS9
------	------	------	------	------	------	------	------	------

TCPIP1 192.168.20.8n

TCPIPT 192.168.20.9n

TCPIPT 192.168.20.1ab

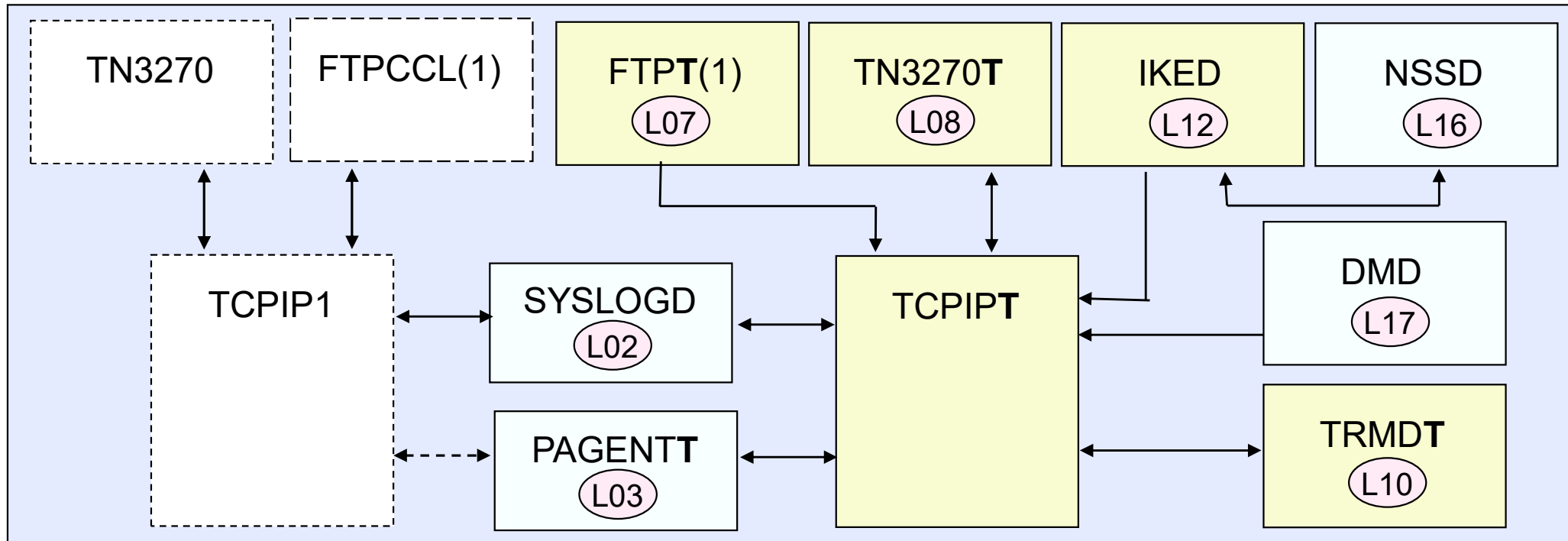


8n = 81 - 89
9n = 91 - 99
1ab = 101 - 109
1ab = 111 - 119
1ab = 121 - 129

1. Telnet to TCPIP1.
2. Edit TCPIPT configurations.
3. Enable TCPIPT configuration changes.
4. Telnet to TCPIPT to test TN3270T configuration.

Lab Testing Flow Pictures

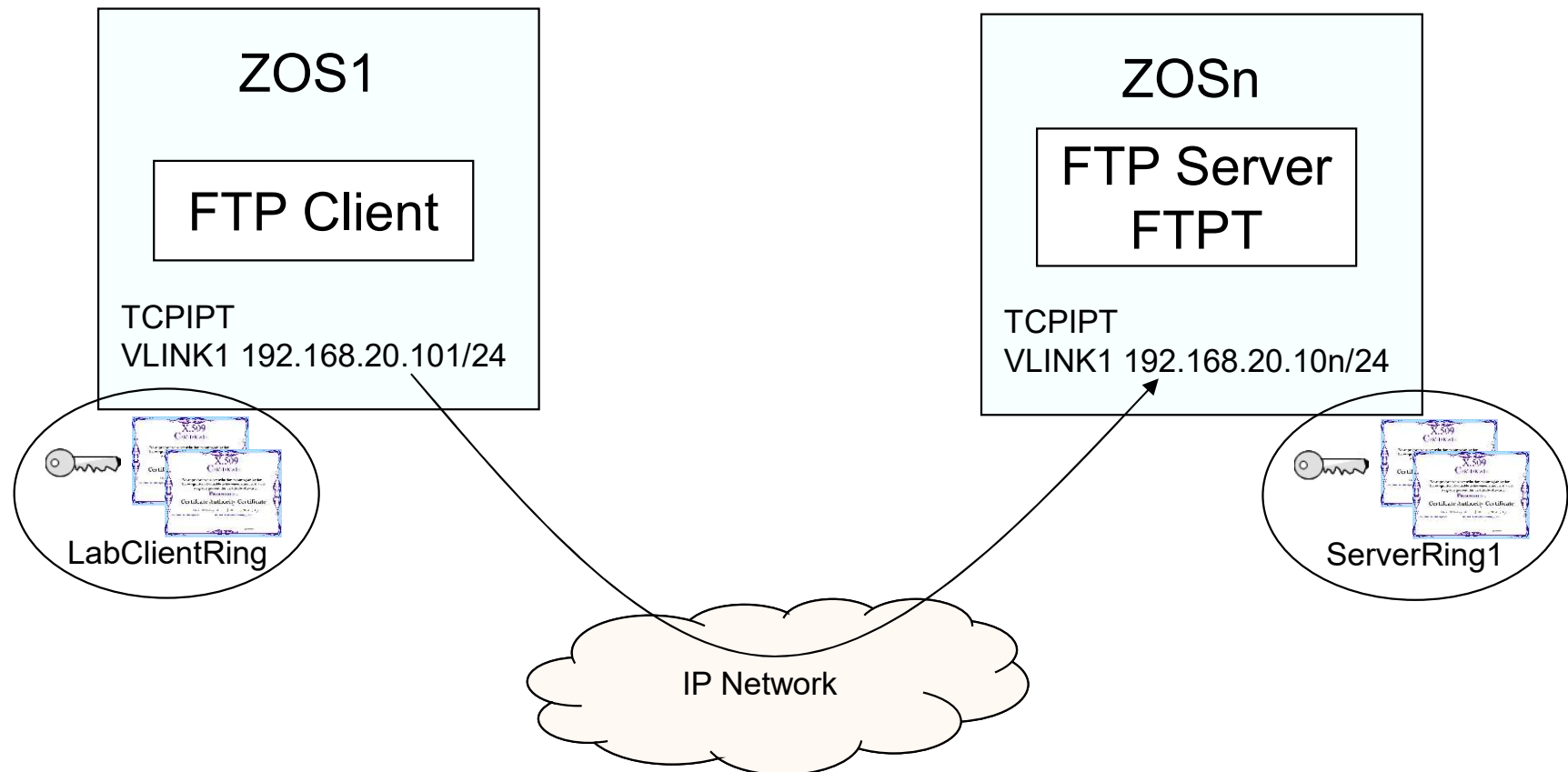
Lab Diagram of Processes



- “Maintenance” TCP/IP stack (TCPIP1)
- “Student” TCP/IP stack (TCPIPT)
- Stack Specific
 - TN3270 (Lab L08)
 - FTP (Lab L07)
 - TRMD (Lab L10)
- Available to all TCP/IP Stacks
 - SYSLOGD (Lab L02)
 - PAGENT (Lab L03)
 - IKED (Lab L12)
 - NSSD (Lab 16)
 - DMD (Lab 17)

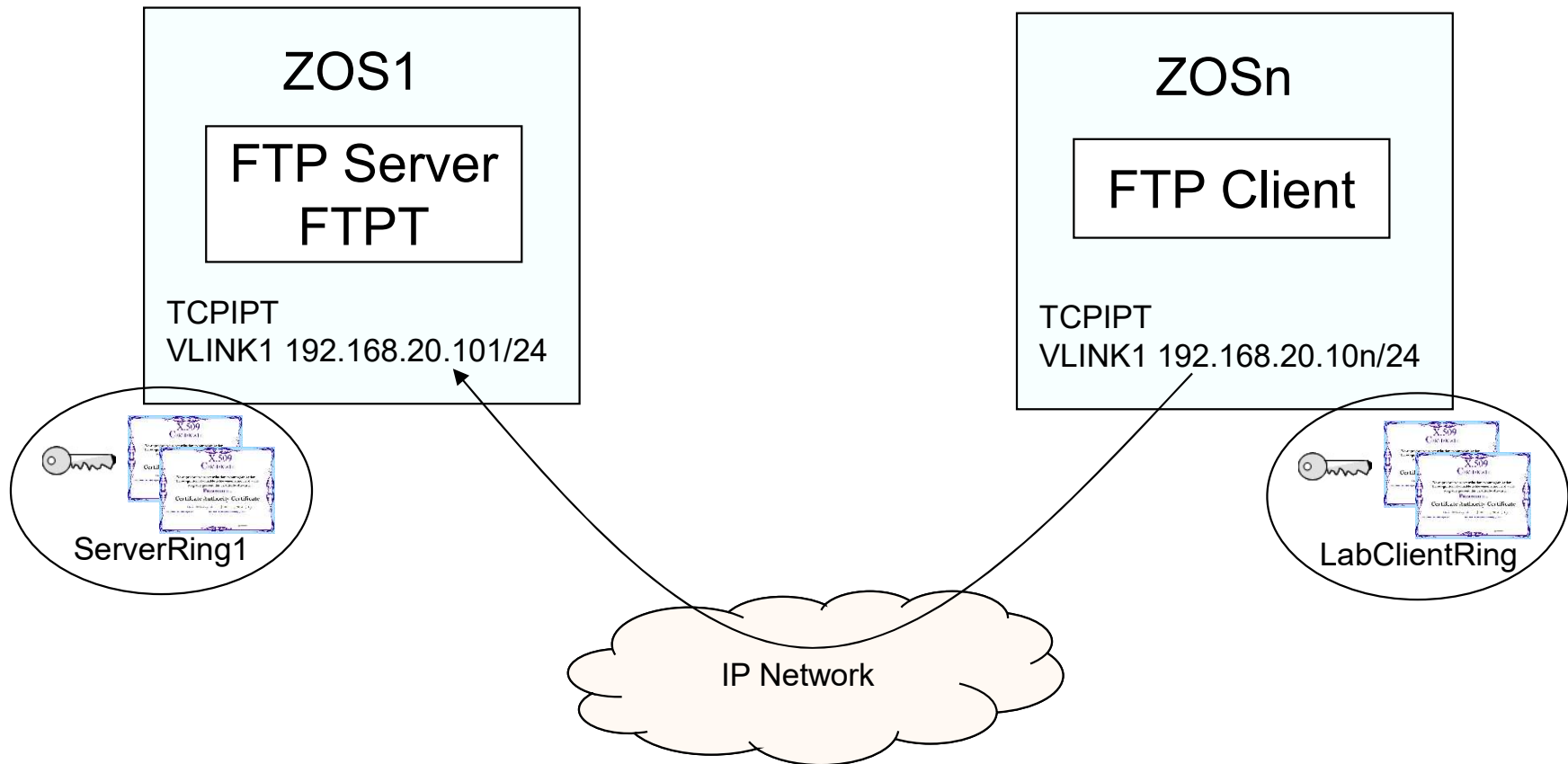
Lab L07 AT-TLS FTP Server

FTP to 192.168.20.10n with AT-TLS

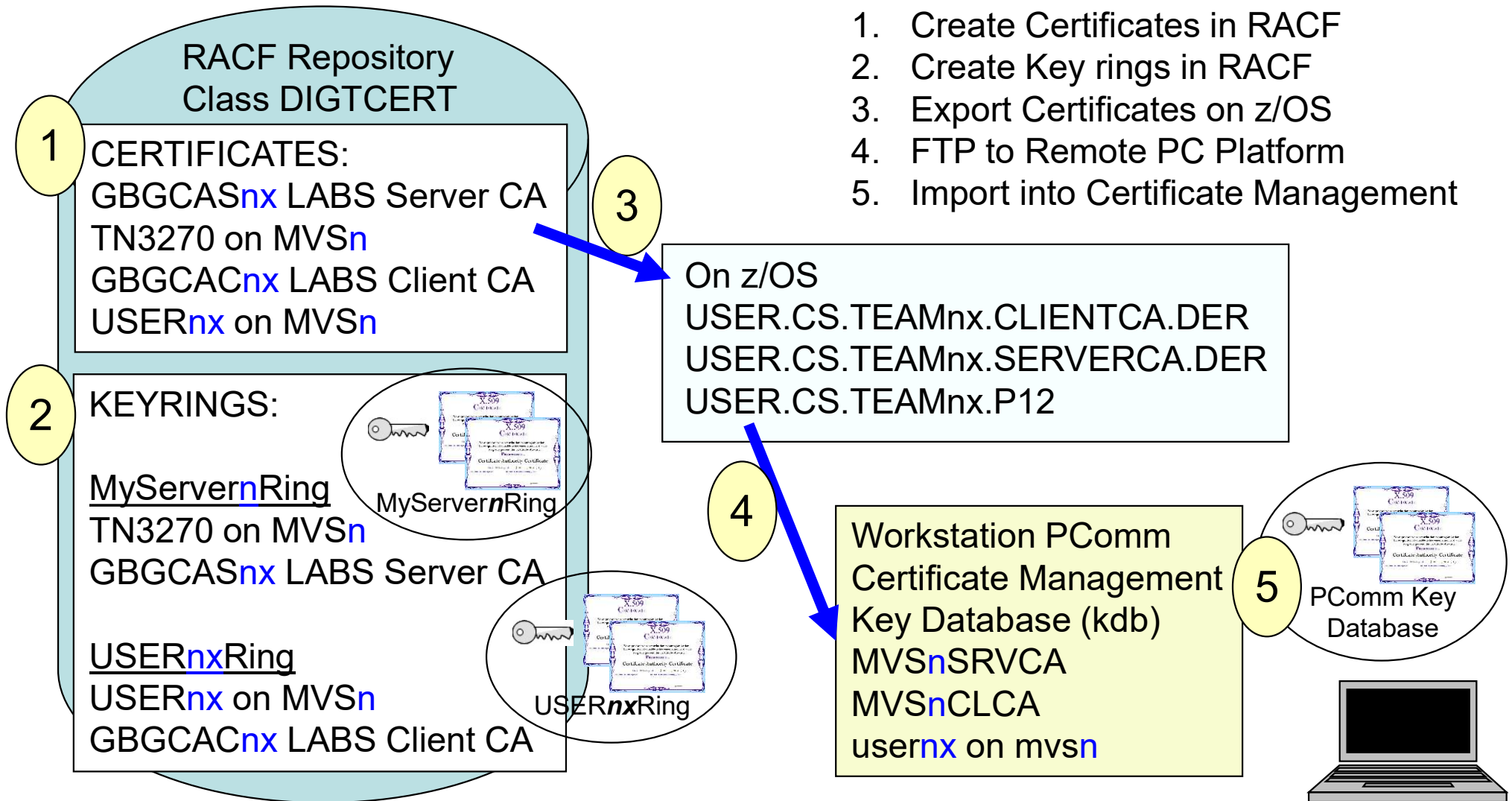


Lab L07 AT-TLS FTP Client

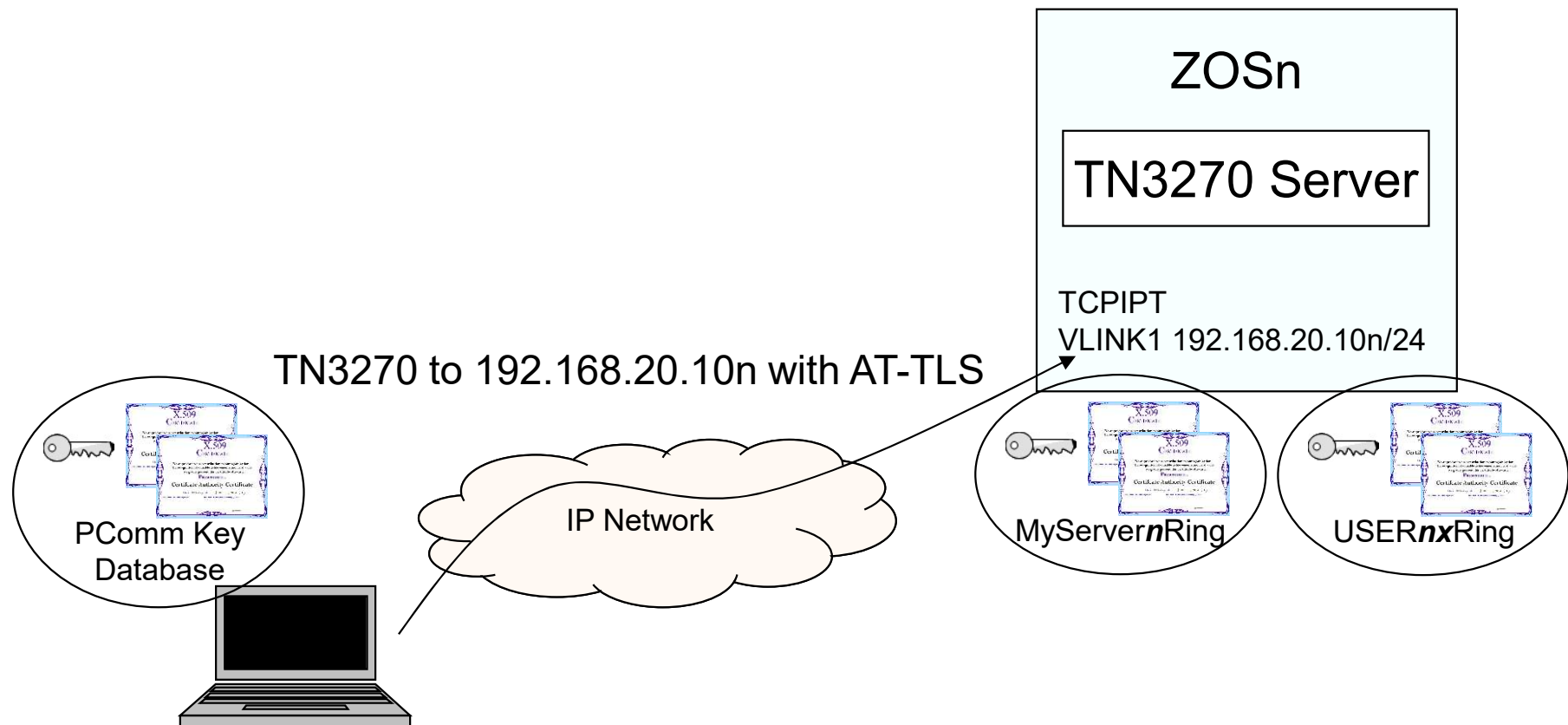
FTP to 192.168.20.101 with AT-TLS



Lab L08 AT-TLS TN3270



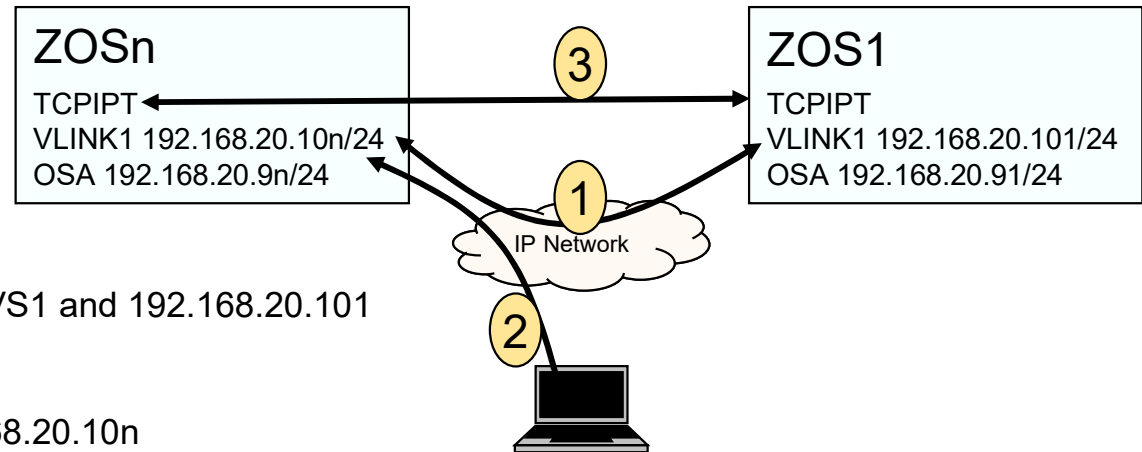
Lab L08 AT-TLS TN3270



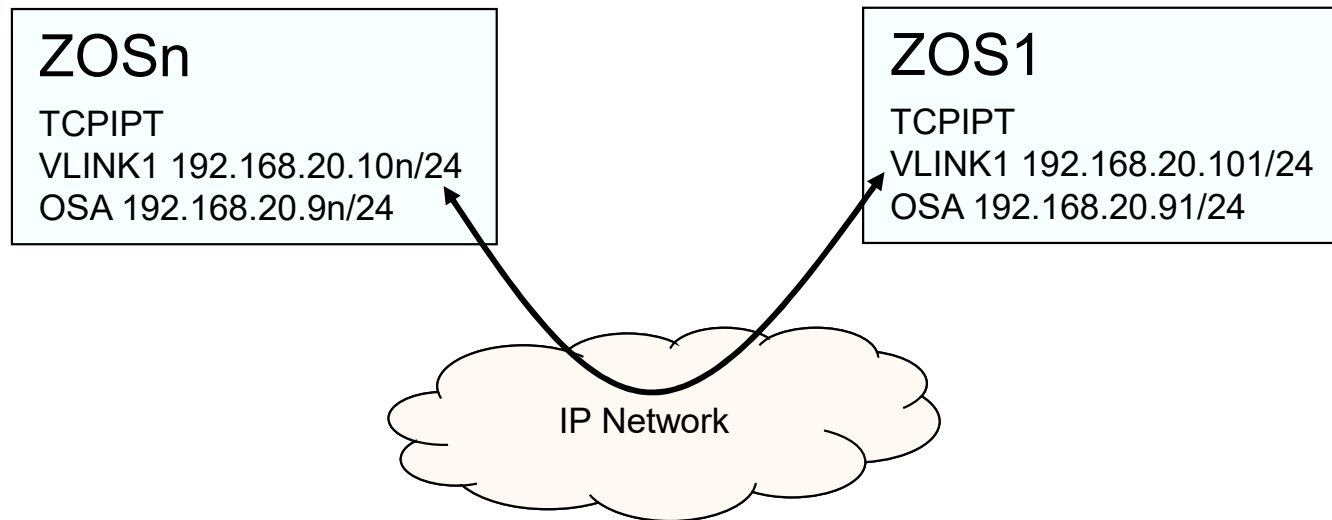
Lab L09 Configuring Policy IP Filter Rules

Configure:

- 1 Between MVS_n 192.168.20.10_n and MVS₁ and 192.168.20.101
CICS and FTP
- 2 Between Workstation and MVS_n 192.168.20.10_n
FTP Server and TN3270 Server
- 3 Between MVS_n any IP address and any other IP address
DNS
ICMP Time Exceeded
ICMP Unreachable
OMPROUTE
Path MTU Discovery
Ping
Resolver
Trace Route



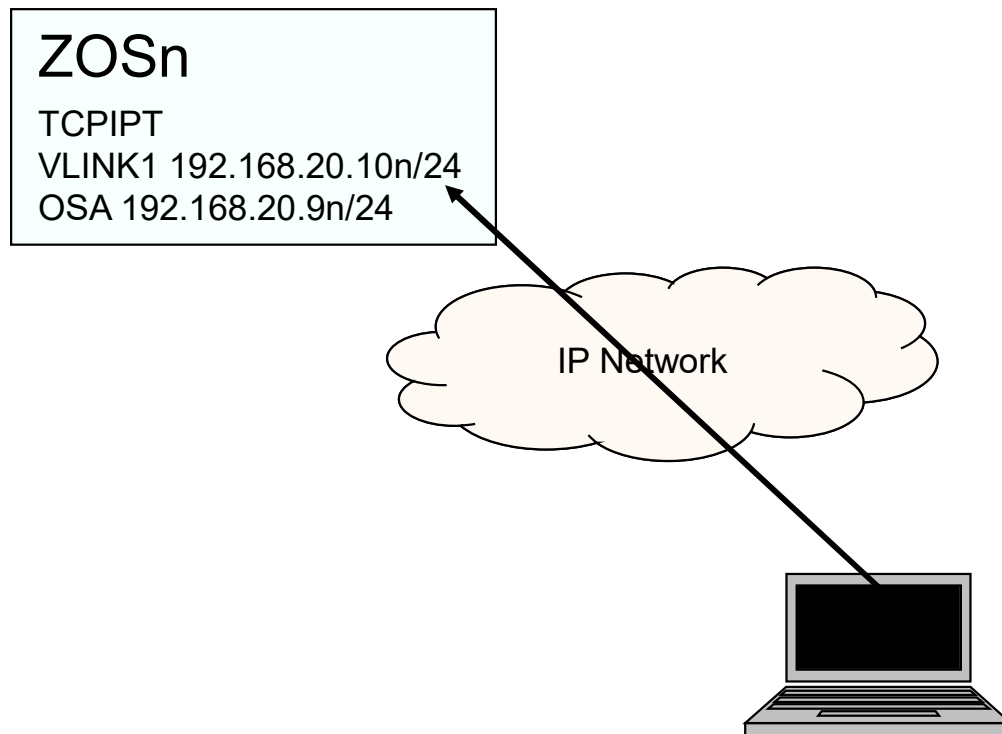
Lab L09 Configuring Policy IP Filter Rules – Part 1



Configure:

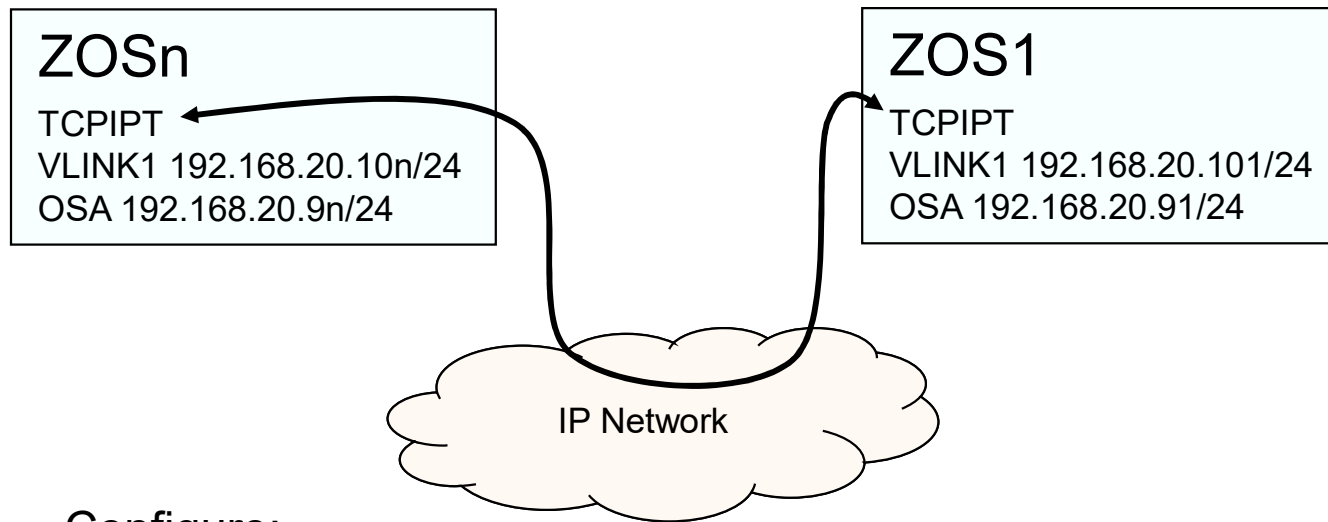
Between MVSn 192.168.20.10n and MVS1 and 192.168.20.101
CICS and FTP

Lab L09 Configuring Policy IP Filter Rules – Part 2



Configure:
Between Workstation and MVSn 192.168.20.10n
FTP Server and TN3270 Server

Lab L09 Configuring Policy IP Filter Rules – Part 3



Configure:

Between MVSn any IP address and any other IP address

DNS

ICMP Time Exceeded

ICMP Unreachable

OMPROUTE

Path MTU Discovery

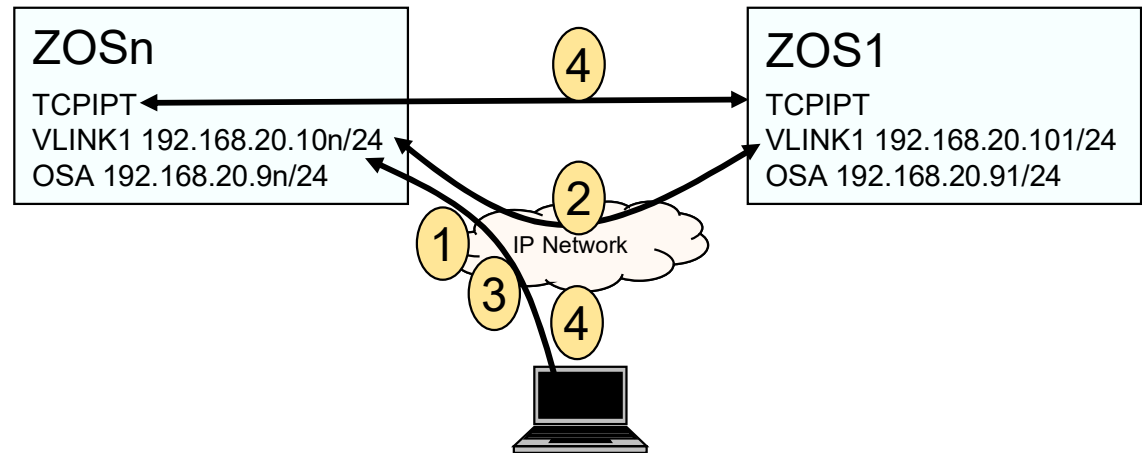
Ping

Resolver

Trace Route

Lab L11 Testing IP Filter Rules

1 Configure Profile Filters (Permit Only):
OSPF protocol
OMPROUTE IGMP protocol (2)
DNS UDP port 53
Administrator Access from any 192.168.0.0/16
IKE protocol



Configured Filter Policies in Lab 11:

2 Between MVSn 192.168.20.10n and MVS1 and 192.168.20.101
CICS and FTP

3 Between Workstation and MVSn 192.168.20.10n
FTP Server and TN3270 Server

4 Between MVSn any IP address and any other IP address
DNS

ICMP Time Exceeded

ICMP Unreachable

OMPROUTE

Path MTU Discovery

Ping

Resolver

Trace Route

1 Testing Profile Filters (Permit Only) from workstation:
ftp 192.168.20.10n
ftp 192.168.20.9n
ping 192.168.20.10n
ping 192.168.20.9n
AT-TLS TN3270 192.168.20.10n
AT-TLS TN3270 192.168.20.9n

2 Testing Filter Policies:

FTP from MVSn 192.168.20.10n to MVS1 and 192.168.20.101

3 TN3270 from Workstation to MVSn 192.168.20.10n

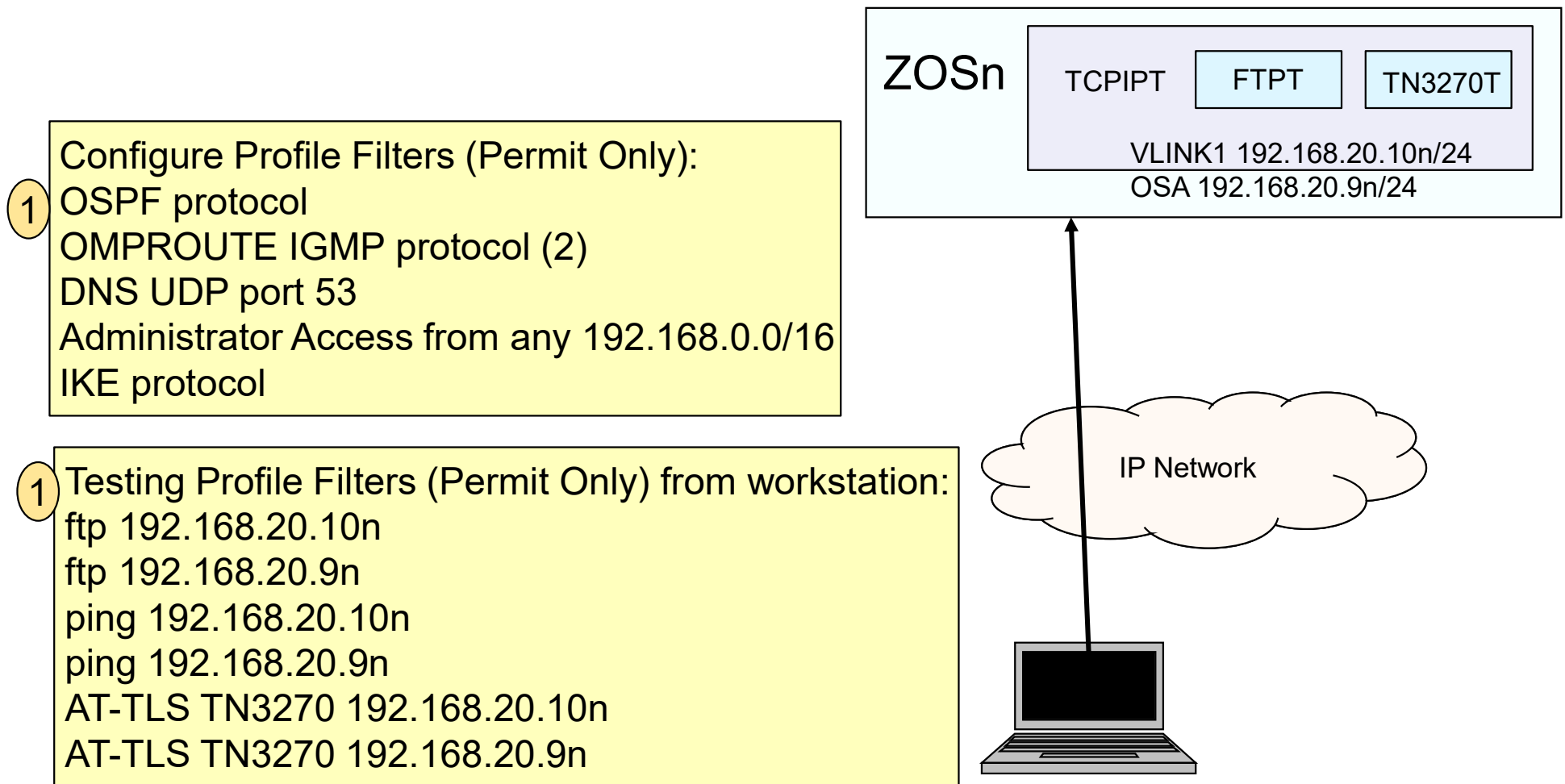
Ping from Workstation to MVSn 192.168.20.9n

4 Ping from Workstation to MVSn 192.168.20.10n

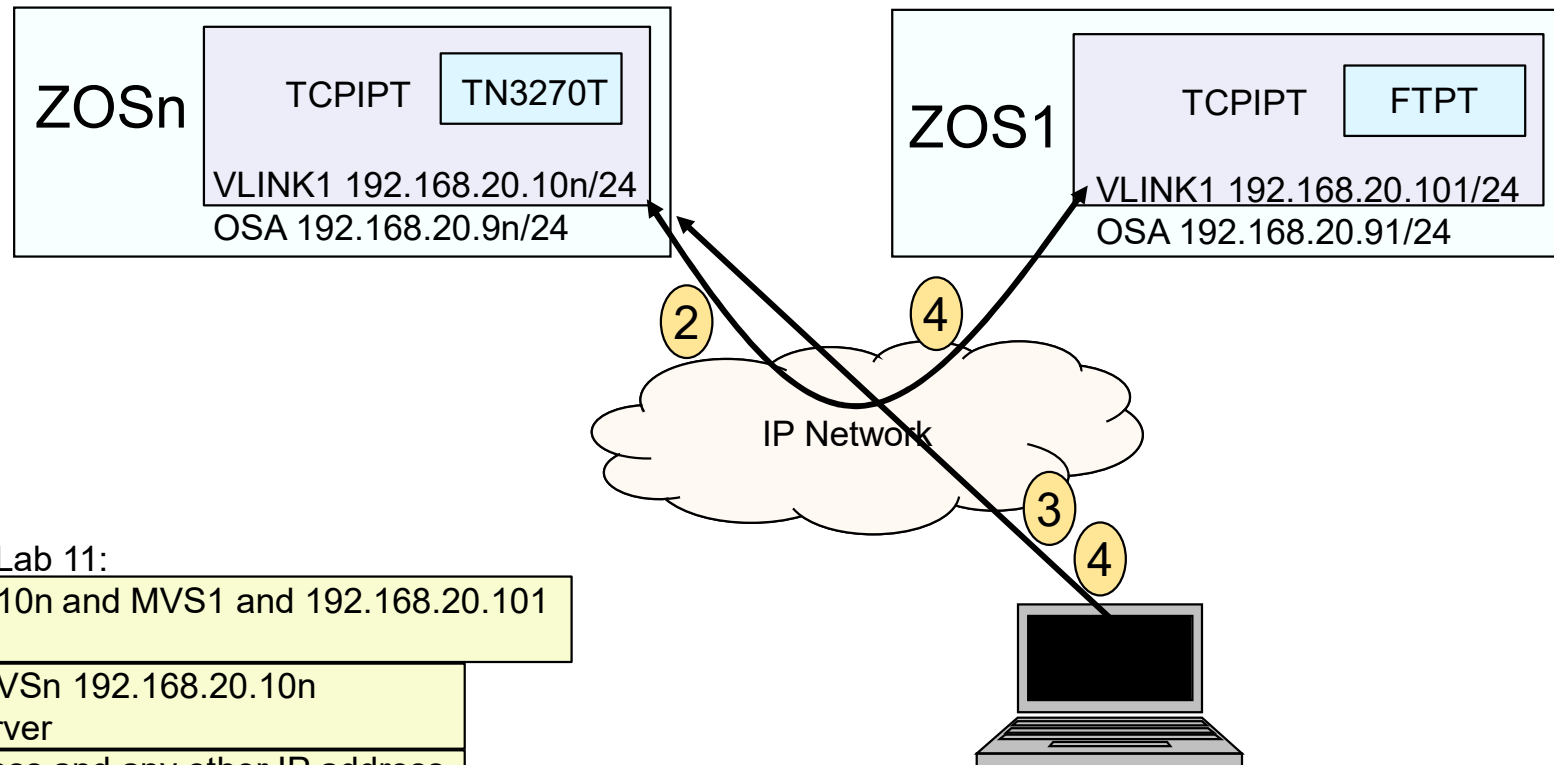
Ping from MVSn 192.168.20.9n to MVS1 192.168.20.91

Ping from MVSn 192.168.20.10n to MVS1 192.168.20.101

Lab L11 Configuring and Testing Profile IP Filter Rules



Lab L11 Testing IP Filter Policy Rules



Configured Filter Policies in Lab 11:

2 Between MVSn 192.168.20.10n and MVS1 and 192.168.20.101
CICS and FTP

3 Between Workstation and MVSn 192.168.20.10n
FTP Server and TN3270 Server

4 Between MVSn any IP address and any other IP address
DNS

ICMP Time Exceeded

ICMP Unreachable

OMPROUTE

Path MTU Discovery

Ping

Resolver

Trace Route

Testing Filter Policies:

2 FTP from MVSn 192.168.20.10n to MVS1 and 192.168.20.101

3 TN3270 from Workstation to MVSn 192.168.20.10n

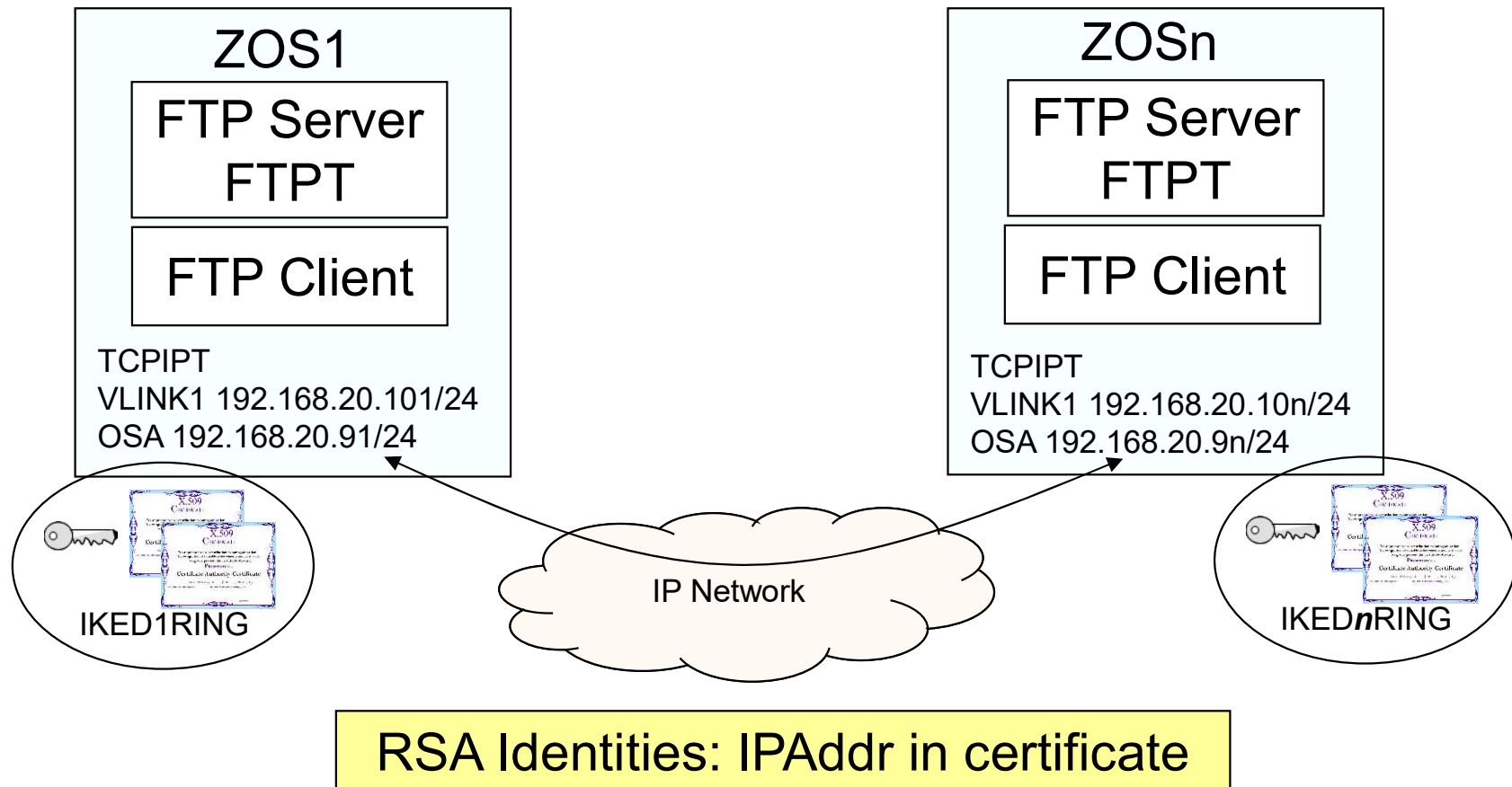
4 Ping from Workstation to MVSn 192.168.20.9n

Ping from Workstation to MVSn 192.168.20.10n

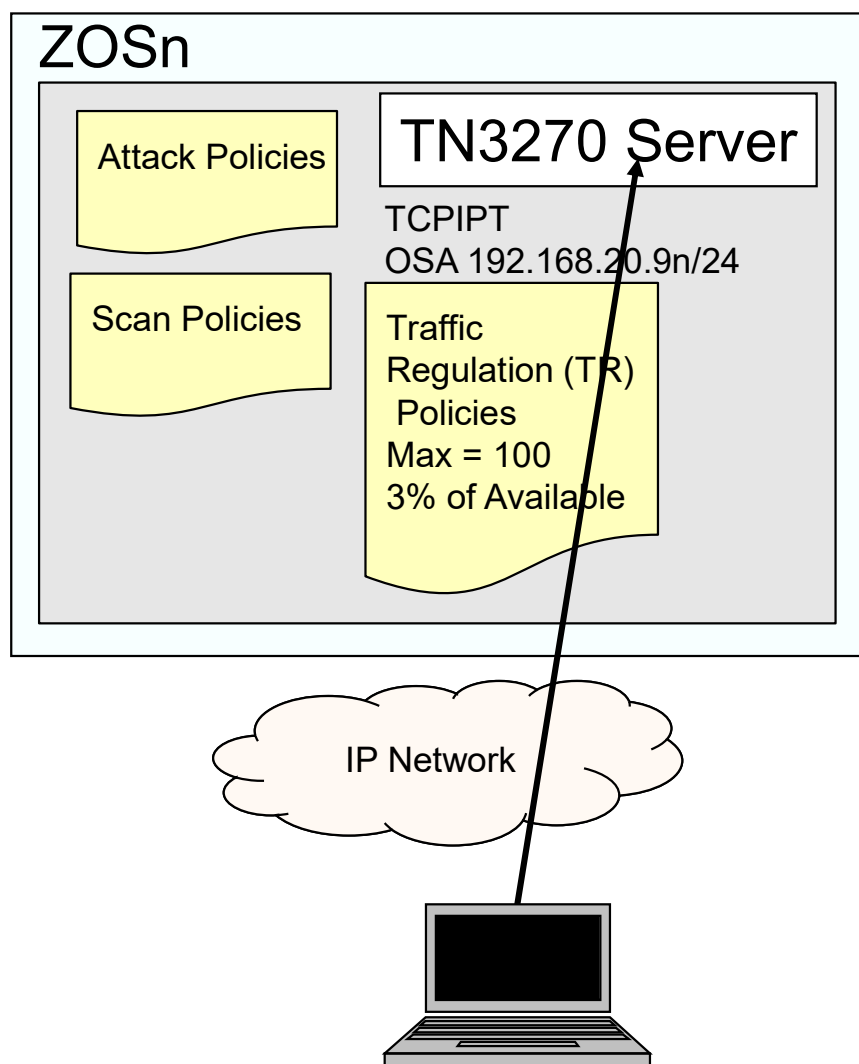
Ping from MVSn 192.168.20.9n to MVS1 192.168.20.91

Ping from MVSn 192.168.20.10n to MVS1 192.168.20.101

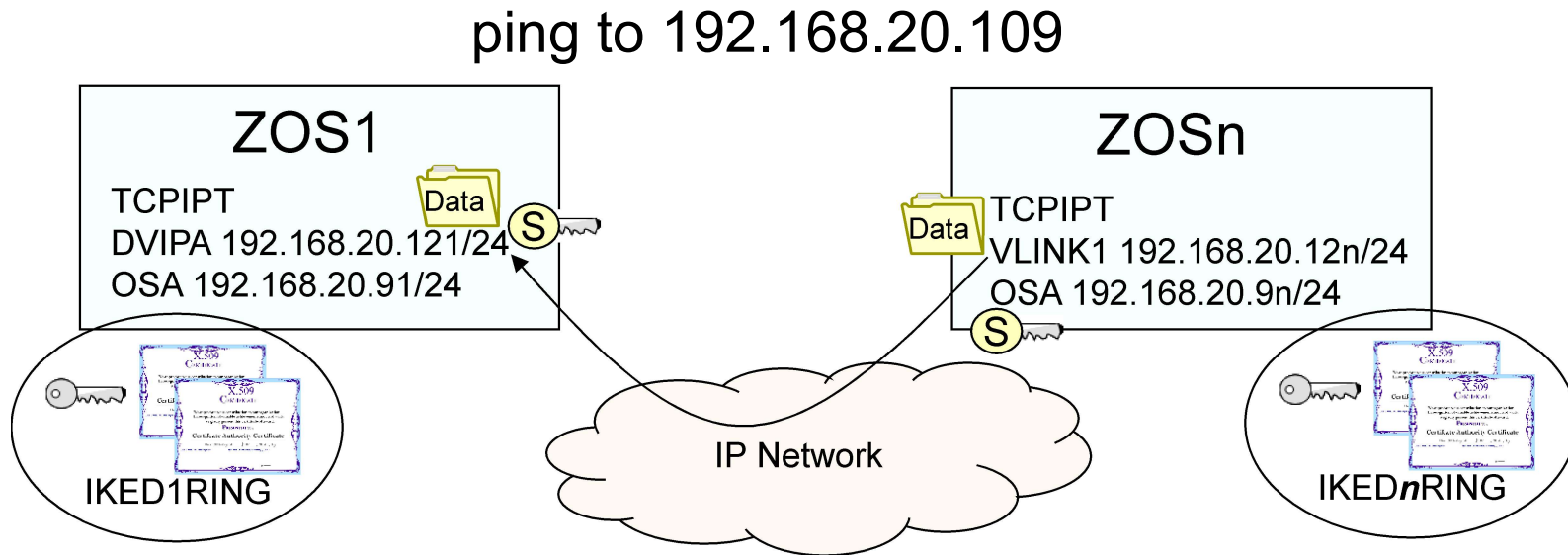
Lab L12 IPsec RSA Signature Mode



Lab L14 IDS Lab

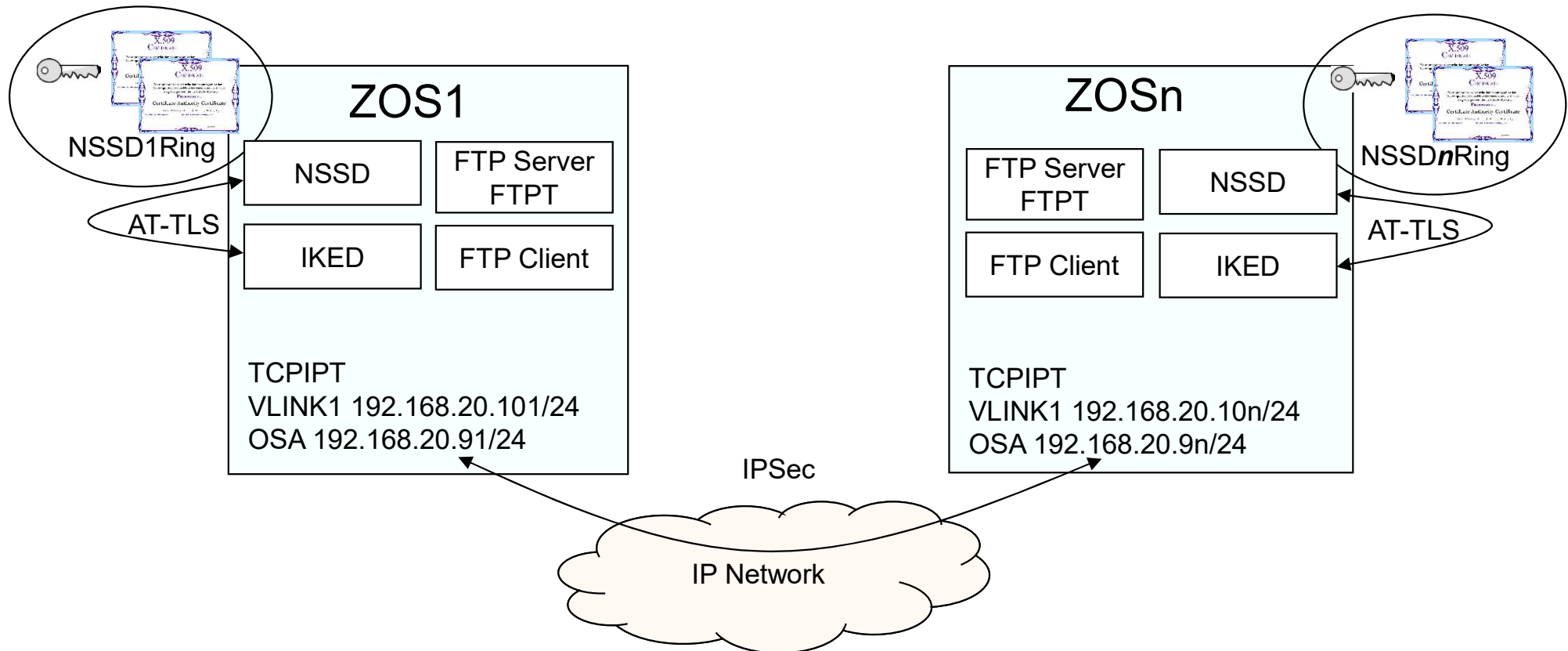


Lab L15 IPsec Preshared Key Mode



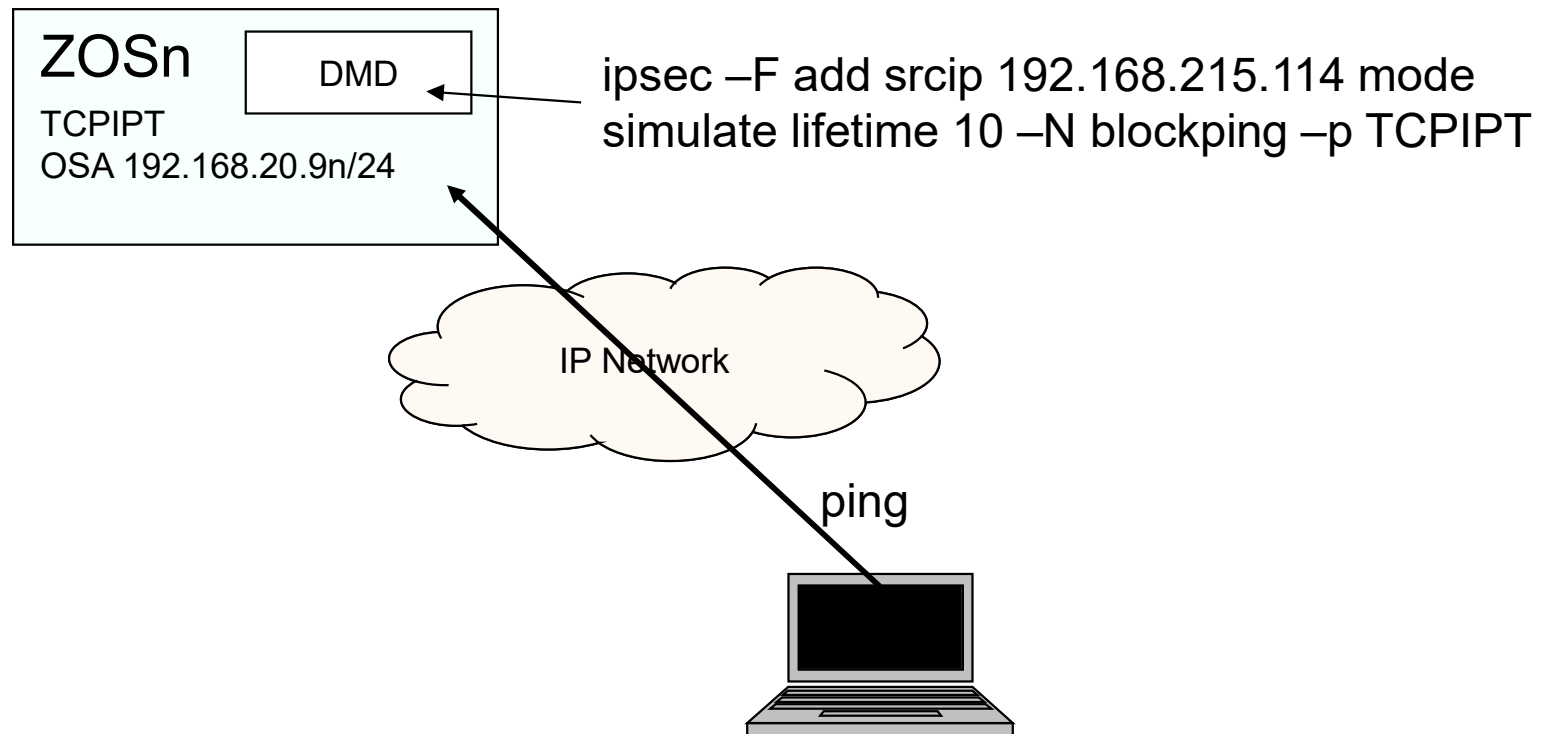
IKE Identity at ZOS1: USER@FQDN in certificate
IKE Identity at ZOSn: FQDN in certificate
Preshared Key Value: userlabs

Lab L16 NSSD



RSA Identities: IPAddr in certificate

Lab L17 DMD



Procs, Commands, and Files

MVS2-MVS9 Start Procs

- “Maintenance” TCPIP1 Start Procedures
 - S TCPIP1
 - S TN3270
 - S FTPCCL
- TCPIPT Start Procedures
 - S CSF
 - S TCPIPT (prior to Lab 11)
 - S TCPIPT,CS=USER,PROF=TCPnAIPS (after Lab 11)
 - S PAGENTT
 - S FTPT (prior to Lab 7)
 - S FTPT,CS=USER,FDAT=FTPSECnx (after Lab 7)
 - S TN3270T (prior to Lab 8)
 - S TN3270T,CS=USER,PROF=TNnATTLS (after Lab 8)
 - S TRMDT
 - S NSSD
 - S IKED
 - S DMD

Commands

- FTP from MVS_n to MVS1 without AT-TLS
 - OMVS ftp -p TCPIPT -s 192.168.20.9n 192.168.20.91
 - TSO ftp -s 192.168.20.9n 192.168.20.91 (TCP TCPIPT
- FTP from MVS_n to MVS1 with AT-TLS
 - OMVS ftp -r TLS -f “//”USER.CS.TCPPARMS(FTPCLSECnx)” -p TCPIPT -s 192.168.20.10n 192.168.20.101
 - TSO ftp -r TLS -f “//”USER.CS.TCPPARMS(FTPCLSECnx)” -p TCPIPT -s 192.168.20.10n 192.168.20.101
- Ping from MVS_n to MVS1
 - OMVS ping -p TCPIPT -s 192.168.20.10n 192.168.20.101
 - TSO ping 192.168.20.101 (SRCIP 192.168.20.10n TCP TCPIPT
- FTP from MVS1 to MVS_n with AT-TLS
 - OMVS ftp -r TLS -f “//”SYS1.CS.TCPPARMS(FTPCLSEC)” -p TCPIPT -s 192.168.20.101 192.168.20.10n
 - TSO ftp -r TLS -f “//”SYS1.CS.TCPPARMS(FTPCLSEC)” -p TCPIPT -s 192.168.20.101 192.168.20.10n
- IPsec test traffic inbound
 - OMVS ipsec -p TCPIPT -t 192.168.20.91 192.168.20.9n udp 500 500 in 0
 - OMVS ipsec -p TCPIPT -t 192.168.20.121 192.168.20.12n udp 500 500 in 0
- IPsec test traffic outbound
 - OMVS ipsec -p TCPIPT -t 192.168.20.9n 192.168.20.91 udp 500 500 out
 - OMVS ipsec -p TCPIPT -t 192.168.20.12n 192.168.20.121 udp 500 500 out

MVSn File Locations

- Unix Home Directory = /u/user**nx**
- MVS TCP/IP Samples Directory = SYS1.TCPIP.SEZAINST
- Procedures Library = SYS1.PROCLIB
- Maintenance TCPIP1 TCPPARMS = SYS1.TCPPARMS
- Maintenance TCPIPT TCPPARMS = SYS1.CS.TCPPARMS
- Student Test TCPIPT TCPPARMS = USER.CS.TCPPARMS
- Student Environment Variables = USER.CS.ENVVARS
- Student Source Files = USER.CS.SOURCE

MVSn Configuration Locations

- TCPIP1 Profile
 - SYS1.TCPPARMS(PROFCCLn)
- TCPIP1 TCPDATA
 - SYS1.TCPPARMS(TCPDATCn)
- SYSLOGD Location
 - /etc/syslog.con
 - MVS1
 - /var/CSLOG/syslogall.log
 - /var/CSLOG/ipsec.log
 - MVS2-9
 - /var/syslogall.log
- FTPCCL Server
 - SYS1.TCPPARMS(FTPDATA)
- TN3270 Profile
 - SYS1.TCPPARMS(PRTNCCLn)
- TCPIPT Profile without AT-TLS and IPsec
 - SYS1.CS.TCPPARMS(TCPnA)
- TCPIPT Profile with AT-TLS and IPsec
 - USER.CS.TCPPARMS(TCPnAIPS)
- TCPIPT TCPDATA
 - SYS1.CS.TCPPARMS(DATnA)
- PAGENTT Configuration File
 - /etc/PAGT1/pagentt.conf
- FTPT MVSn Server without AT-TLS
 - SYS1.CS.TCPPARMS(FTPSEC)
- FTPT MVSn Server with AT-TLS
 - USER.CS.TCPPARMS(FTPSECnx)
- FTP Client with AT-TLS
 - SYS1.CS.TCPPARMS(FTPCLSEC)
- TN3270T Profile
 - USER.CS.TCPPARMS(TNnATTLS)
- TRMDT
 - SYS1.CS.TCPPARMS(DATnA)
- IKED
 - /etc/security/iked.conf

End
