Networking on IBM i – Best Practices

OCEAN Users Group

September 18, 2018

Larry Bolhuis lbolhuis@frankeni.com
Frankeni Technology Consulting, LLC 616.260.4746
Grand Rapids, MI www.frankeni.com

Wayne Bowers IBM i Global Support wbowers@us.ibm.com

Acronyms

- DCM – Digital Certificate Manager
- DHCP – Dynamic Host Configuration Protocol
- FQDN – Fully Qualified Domain Name
- GbE – Gigabit Ethernet
- HEA – Host Ethernet Adaptor
- IVE – Integrated Virtual Ethernet adaptor
- LACP – Link Aggregation Control Protocol
- LPAR – Logical Partition
- PCIe – PCI express (Serial version of PCI)
- RFC – Request for Comment (IP Standards)
- REF – Request for Enhancement
- SR-IOV – Single Root I/O Virtualization
- SSL – Secure Sockets Layer
- TLS – Transport Layer Security
- VIOS – Virtual Input Output Server
- VLAN – Virtual Local Area Network

- FUBAR – What to avoid.

Why are we here?

- Today virtually 100% of data moves in and out of our systems on Ethernet
- Even old legacy SNA traffic is encapsulated in TCP/IP
- Our networks continue to get more complicated, and capable.
- A well performing system can be crippled by poorly done networking.
- Reliability, redundancy, security: all mandatory in today's environment.
- If the network is down, the system is gone. To the users, the system IS down!

IBM i Enhanced networking and troubleshooting

- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

Best Practice Overview

- IBM i has very robust networking components which are written to adhere to the RFCs very closely.
  - This is unlike some other operating systems where many things are discovered later by hackers or badly formed network data.
- Nonetheless, correct configuration of the components is absolutely necessary to assure reliable and efficient connections.
- You should NOT be surprised to find that security of the networking components and their configuration plays a huge role in the overall security of your system!

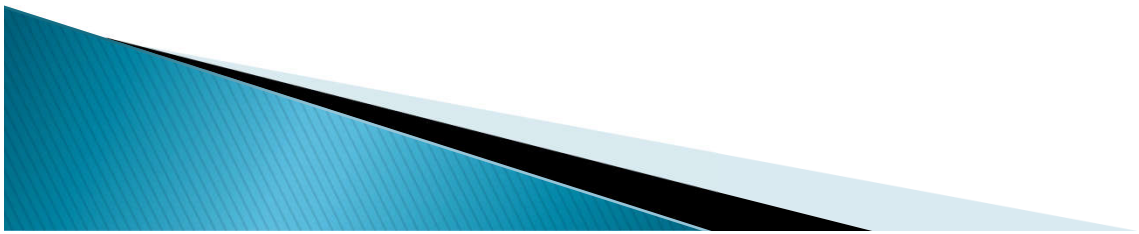
Things to do right.

- Physical network connections
- IP Configuration
- Proper naming
- Running the right servers
- Assuring data isn't read along the way
- Restricting access to the servers

Remember this is in ADDITION to proper:

Authentication (user profiles etc.)

Authorization (permissions and authority)

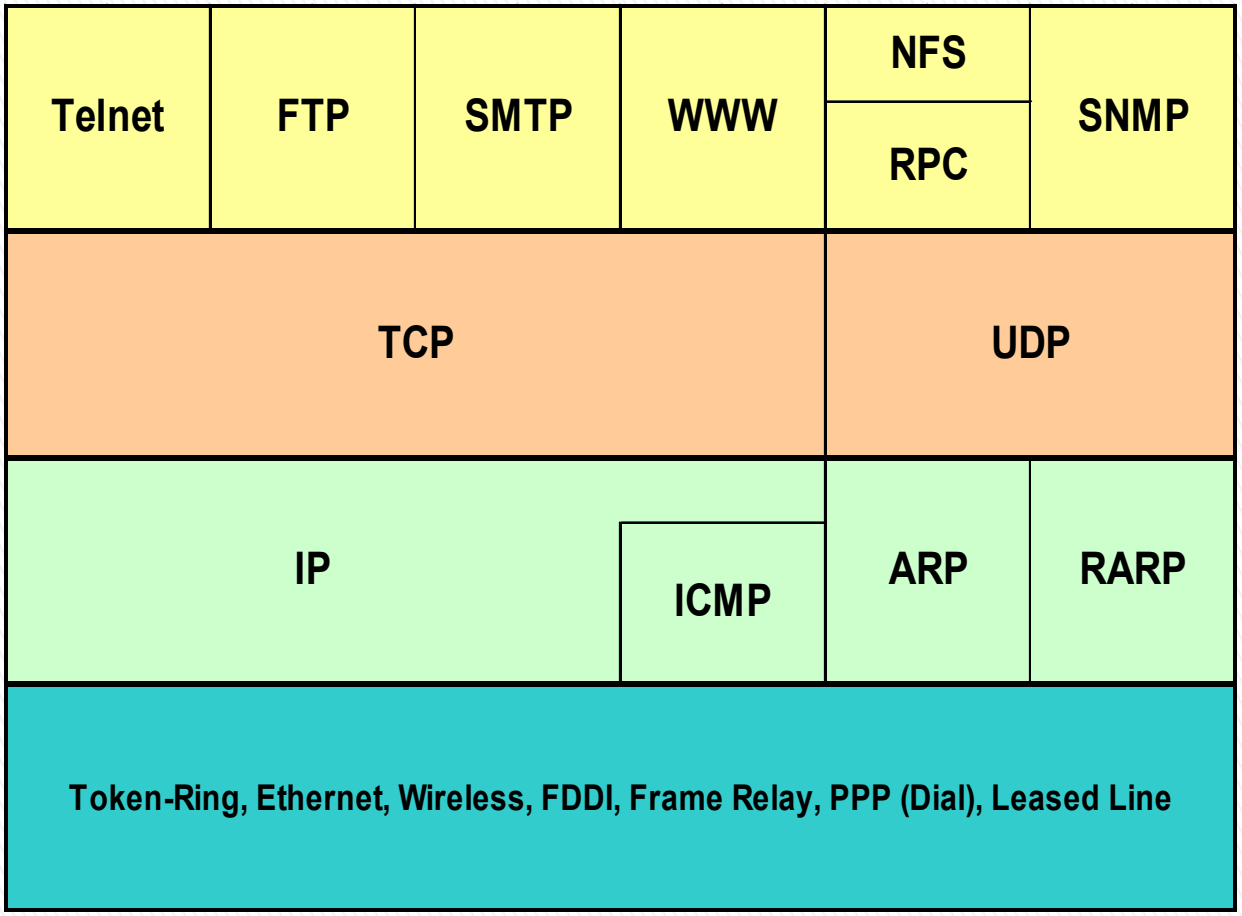


Basic Networking (in one slide!)

- Data exists on one system and it needs to get to another system.
- The system with the data places that data into packets that will fit the network, breaking it into multiple pieces as needed.
- Header information is added including destination, source, length and other bits to fill out the packet.
- Data is almost always placed onto an Ethernet network today.
- Ethernet then carries the data to the first stop along the network.
  - Ethernet is 'local only' that is it cannot send a packet from Ft. Lauderdale to Chicago.
- The next stop along the network may be a router which reformates the packet to fit the media used outside your building.
  - This may mean different headers or breaking the packets up
- This process repeats and repeats until the data reaches its destination.
- Besides just getting the data there, components of the process can also confirm delivery (TCP)

- Where is IP in all of this? It's inside the 'Data' portion of the Ethernet packets!

Communication Stack



IP - Internet Protocol
ICMP - Internet Control Message Protocol
ARP - Address Resolution Protocol
RARP - Reverse Address Resolution Protocol
TCP - Transmission Control Program
UDP - User Datagram Protocol

Telnet - Teletype Network
FTP - File Transfer Protocol
SMTP - Simple Mail Transfer Protocol
WWW -World WideWeb
NFS - Network File System
RPC - Remote Procedure Call
SNMP - Simple Network Management Protocol

IBM i Enhanced networking and troubleshooting

- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Addressing and Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

Defining the connection from IBM i

- Ethernet runs over many different adapters
  - From 10Mb to 100Gb
- They can be dedicated, shared or virtual
- CRTLINETH is used to define the connection to the physical hardware from IBM i.
- Several things are key on the line description if you want it right.
  - A good naming conversion so you know which is which
  - The CMNnn resource name(s) for your Ethernet hardware
  - TEXT so you'll know what the line is for!!
    - Seriously don't say "Ethernet Line" (face palm)

Reliability enhanced

- Use of good cables is a must, not homemade cables, especially with GbE and up.
  - Cat6e minimum, Cat6a is better, Cat7 an option.
- Assure the retention tab isn't broken off
  - Using one sucesfully completes the application for 'worst practices in systems management' ☺
- LABEL cables on BOTH ends
  - BOTH ends should specify BOTH ends!
- Secure cables in place all the way to the network switches.
- Internally document the port's use at the switch to prevent mistakes by the network knuckleheads.
- If using LAN Console it must use T1 port, consider leaving a T1 port open for console failure

Redundancy

- Redundancy is nearly mandatory these days
- Connect a second line, even third if you'd like.
- The second line should come from a separate Ethernet IOA if at all possible.
  - On a separate bus is better
    - In a separate I/O drawer is better still
  - A third line is even better!
- If possible connect to a separate network switch as well.

Redundancy Options:

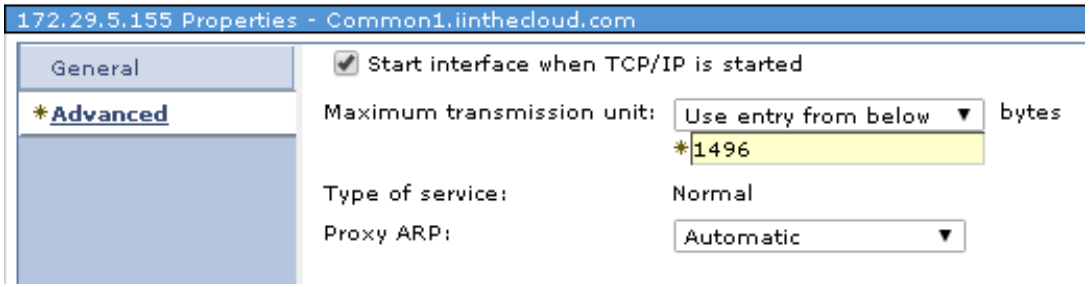
- Virtual IP redundancy or Link Aggregation.
  - Supported on all current releases
  - Virtual IP with Proxy ARP
    - Redundancy by floating IP between multiple Ethernet lines
  - Link Aggregation
    - Multiply bandwidth by binding multiple lines together.
    - Redundancy by maintaining connectivity as long as one line stays active.
  - Or do Both!
    - Create two aggregated links
    - Use Virtual IP support to put both aggregated links in play.

Steps to set up Virtual IP

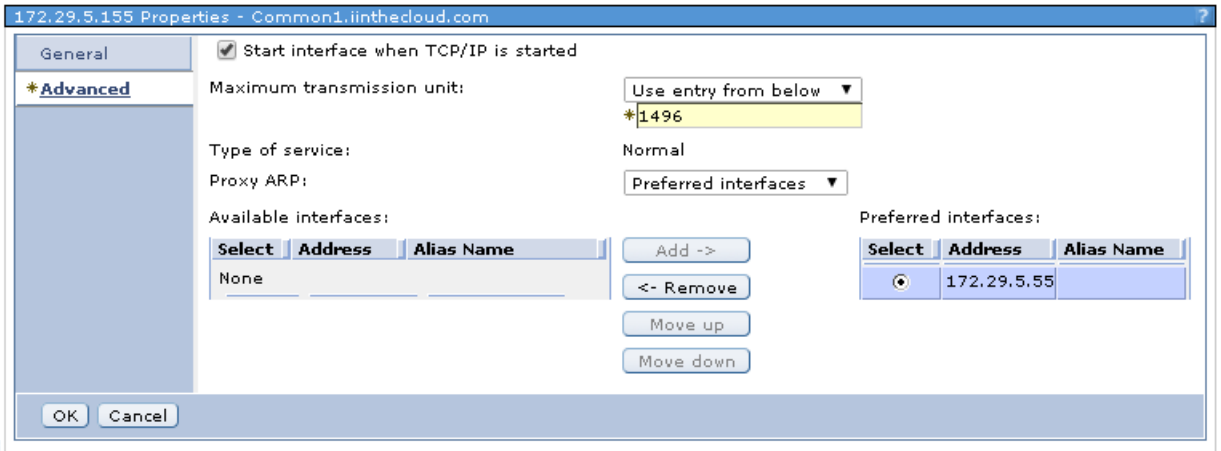
- Configure a second Ethernet line (or more as desired)
- Obtain one additional IP address for each Ethernet line to be used
  - These are in addition to existing production IP address(es)
  - These addresses must all be in the same IP Subnet
  - Assign the new addresses to each line.
    - Assure that the 'Associated Local Interface' is set to the current production address.
- Stop the production address and delete it.
- Recreate the production address as a virtual IP interface
  - IMPORTANT remember to set the MTU for the production address to match that for the Ethernet lines.
    - The default is 576!
- Repeat for each current production address.

Setting Frame size & Proxy Arp

- Here we set the Maximum Frame Size to match Smallest line value.



- For Proxy ARP set either Automatic or 'Preferred interface' which displays below:
- Here we select the preferred line by selecting its IP address



IBM i Enhanced networking and troubleshooting

- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Addressing and Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

Link Aggregation overview

- Traditionally we connect one Ethernet cable from a switch to an Ethernet adapter for each partition.
  - The speed of this has gone up 10Mb, 100, 1000 (GbE), and now even 10,000Mb (10 GbE) with fiber.
  - Problem was if it fails for ANY reason, speed goes to *ZERO.
- We have had redundancy since V5R3 with virtual IP addresses.
- Aggregation allows us to logically combine up to 8 physical lines into one logical ‘channel’

Link Aggregation Detail

- Aggregation enables multiple physical connections to appear as one physical line.
  - Speed is the accumulation of the physical lines less some overhead.
  - As long as at least one of the physical lines remains linked the line remains up and functional.
- Configuration of both ends (IBM i and your network switch) is required.

The IBM i side of the config

- For must be done at the command line.
- Identify the CMN numbers of each of the physical interfaces to be aggregated.
  - Rules:
    - All Interfaces must be GbE Capable and full duplex
    - All Interfaces must run at the same speed
    - e.g. you can aggregate a 1Gbe and a 10Gbe line but both must be at 1Gbe so this would not be a normal configuration.
- When the Ethernet line is created specify *AGG instead of a CMN resource then list all CMN resources in the Aggregated Resource list.

Verify your Link Agg

- DSPLIND LIND(ETHERAGG1) OPTION(*AGGRSCL)

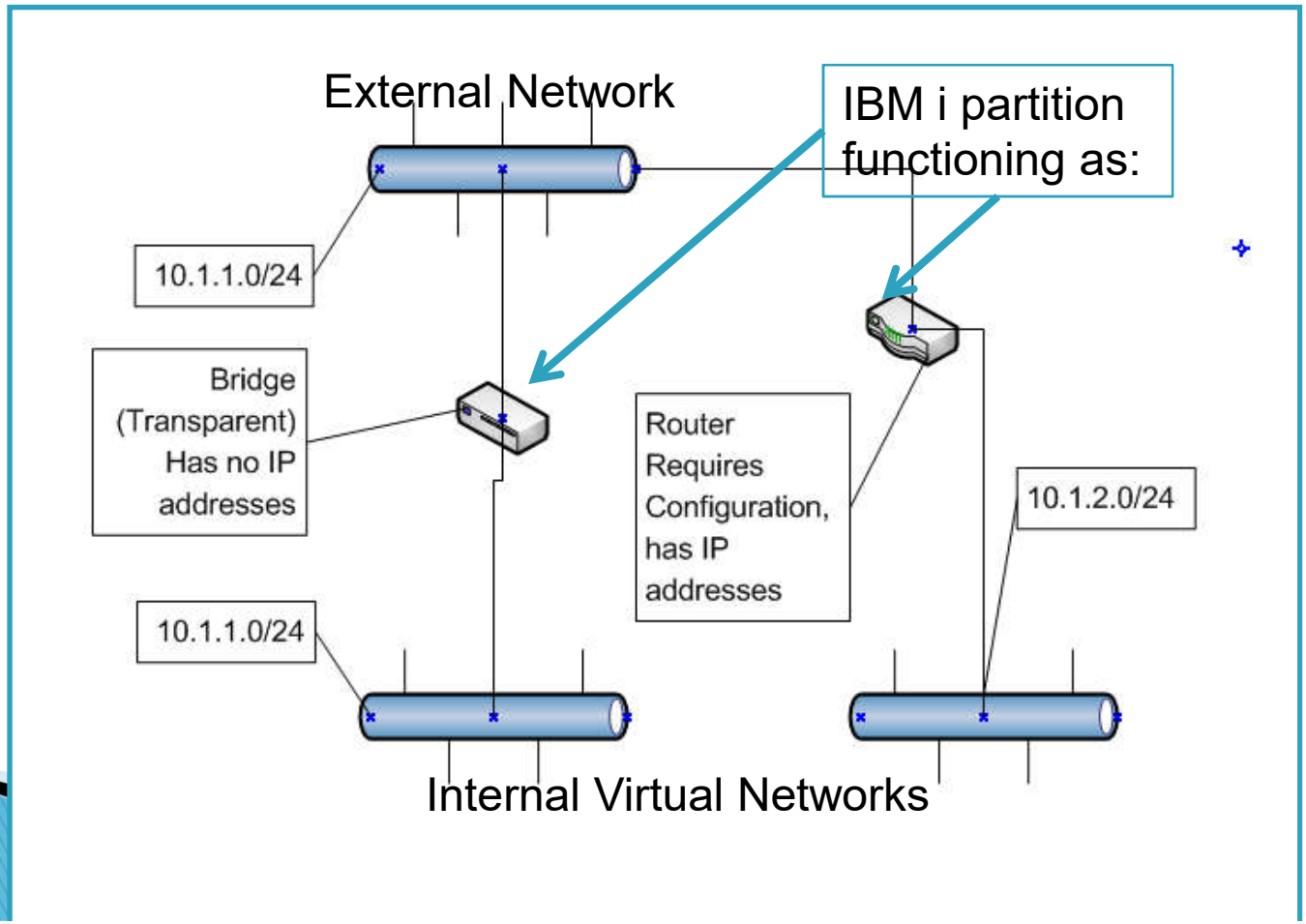
```
Line description . . . . :   ETHERAGG1
Option . . . . . . . . . :   *AGGRSCL
Category of line . . . . :   *ELAN

-Aggregated Resource List--
Name                  Status
CMN73                 LINK UP    <- Link 1 up
CMN76                 LINK UP    <- Link 2 up
```

Using the Aggregated line

- The line can be used for any use that a typical GbE line can.
- IP interfaces can be added to the line
- The line can be used in a bridge
- If one of the physical lines does not come up it will *not* come up until the line is varied off and back on.
- A new resource will appear for each aggregation line under a 6B26 communications adapter.
  - Named AGG01, 02 etc.
  - This resource is NOT valid to be used
  - It may disappear if the line description is deleted

Are you Routing or Bridging?

- Key differences are configuration and protocol support.



Validate the bridge status

- Check the status with WRKCFGSTS *LIN

```
 Work with Configuration Status                    V7R1PROD
                                        02/19/12   16:59:25

Opt   Description          Status
__    BRIDGE_E             VARIED ON
__    BRIDGE_I             VARIED ON
```

- Both lines should be VARIED ON.
  - They will never go “ACTIVE”

Bridging – best practice

- The external Ethernet line can be an aggregated line or a standard line.
- The Ethernet lines used for bridging should NOT have IP addresses configured on them.
  - This is because in promiscuous mode many more packets hit this interface and this causes significant overhead for identifying and then processing the IP Packets.
- If there are any controllers on these lines you have a problem and that must be remedied!
- Bridging is NOT valid on HEA adapters.
- Tracing a bridge line will trace all packets handled by the bridge (As well as packets handled by IP if you violate rule 1 above!)

IBM i and VLANs

- Until 7.2 IBM i itself did not recognize an 802.1Q VLAN tag.
- Previous to i 7.2 the switch port on which IBM i is connected has be an ‘access’ port.
  - This means that the switch does any tagging and un-tagging of packets.
  - IBM i is unaware of the VLAN it is connected to.
  - i 7.2 still supports this of course!

IBM i Enhanced networking and troubleshooting

- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Addressing and Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

Further addressing

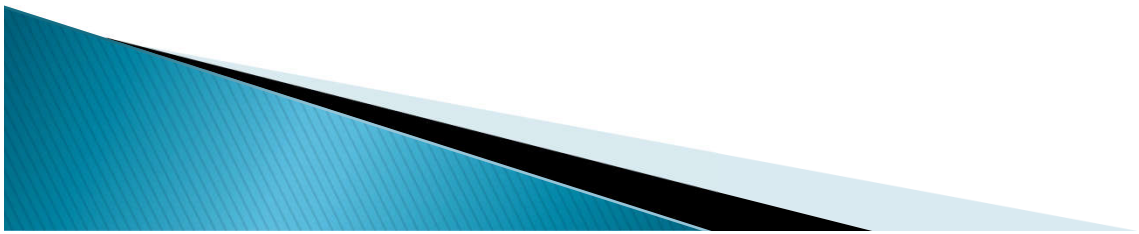
- IBM i supports many IP addresses on a system and many on a single Ethernet line.
- Separate IP addresses are useful for many things:
  - Individual Web servers or services
  - Multiple Domino servers
  - Different interfaces to separate user traffic and replication traffic such as PowerHA or Mimix.
- BUT just because you can…… ☺
  - Understand what each address is needed for.
  - Document what they are for TEXT Parameter!!
  - Remove unused addresses

Best practices – Interfaces

- Do not add more interfaces than are needed on your server.
- Best practice is also to keep IP addresses that are on different subnets on different Ethernet lines.
  - With i 7.2 forward this may be separate VLANs sharing a physical interface.
- Multiple IP addresses in the *same* subnet should all be VIPs leaving one interface (IP address) that is not virtual.
  - First reason is that traffic sourced from IBM i will appear to come from the IP address physically associated with the line.
    - Knowing this may simplify firewall rules especially for partners on the far side of restricted links.
  - Second is that when you STRTCPIFC for a virtual IP address the system will gratuitously ARP the address in the network.
    - This means that if you are moving a service between servers for instance that everyone in the local network will know immediately.
    - With an IP tied to a physical line, ARP caches must time out.

More on Interfaces

- IP Interfaces can now be referred to by an Alias name.
  - This is an excellent thing to do for multiple reasons.
    - 1) Changes to IP addresses no longer necessitate changes to startup, shutdown, and failover scripts.
    - 2) Scripts can be the same on production and backup servers but they'll still bring up the correct address for the system at that location.
    - 3) The name serves as additional documentation



Best Practices – Routing

- Do:
  - Point all routes at hosts (routers) on the local network!
  - Keep the list short
  - Let your routers do the routing. (It's what routers do best!)
- Don't:
  - Add Host routes covered by Network routes
  - Add Network routes covered by Default routes
  - Lie to your system!
- Notes:
  - IBM i will NOT reply to a host if it does not have a route to that host
  - Some other OSs will reply back via the route the traffic came from
    - You should recognize this as a security problem!

Types of Routes

- Direct Routes (consulted first)
  - Added by the system to the local network
- Host Routes (consulted second)
  - Specify a route to a specific Host
- Network Routes (consulted third)
  - You may add your own routes to the local network, called 'Schowler Routes'
    - These replace the system added Direct routes
  - Specify a route to a network of Hosts
  - Many of these can be added
  - Duplicates ARE allowed
- Default Route (consulted last)
  - Specify routers to be used when no Host or Network routes match

IBM i Enhanced networking and troubleshooting

- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Addressing and Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

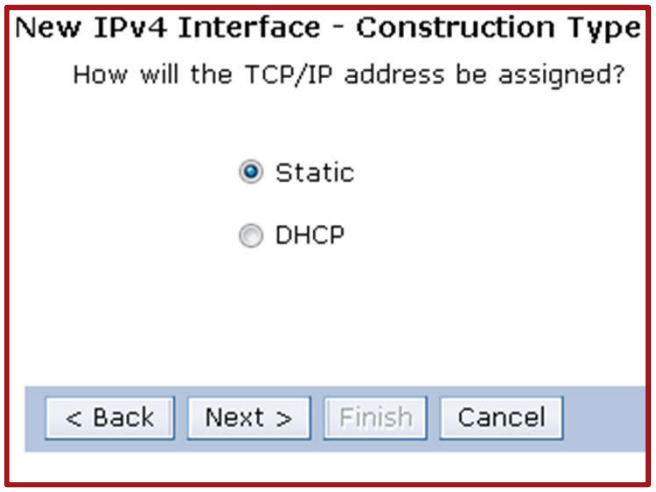
Using VLANs in IBM i

- Configure a switch port as a Trunk
  - VLAN tags are only allowed on Trunk Ports.
- Connect this port to a physical IBM i port.
- Configure a standard Ethernet line for this physical port.
  - If needed this can be an aggregated line.
- Using ADDTCPIFC or IBM Navigator for i (Not System i Navigator!) add the interface to the line and enter the VLAN number.

Creating an interface on a VLAN

- First select Actions and new Interface, then LAN

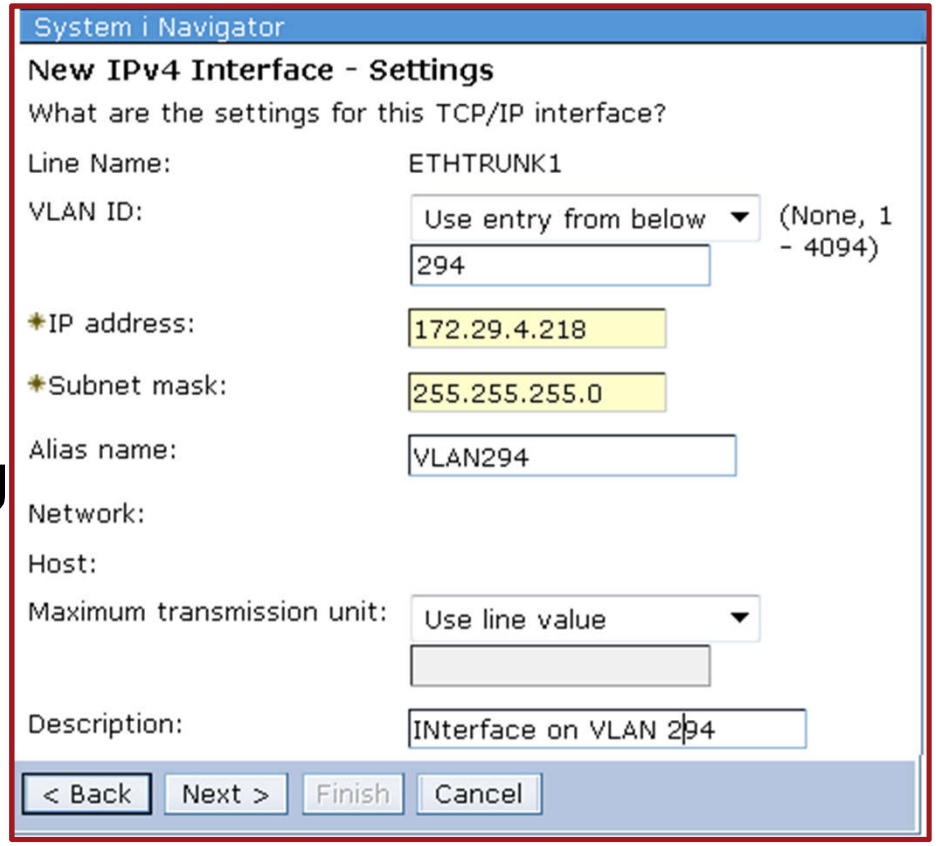
- Omitted is selection for Ethernet, Token-Ring, or Opticonnect (Pick Ethernet!)



- In this case we're doing a standard static IP address
- Next select the Ethernet line you will be placing the line on.

Creating an Interface on a VLAN

- Selected ‘use entry form below’ to use a VLAN.
- Enter the VLAN number, here VLAN ID of 294.
- Enter the IP Address and Subnet Mask
- Alias, Description and MTU work as with any interface



IBM i Enhanced networking and troubleshooting

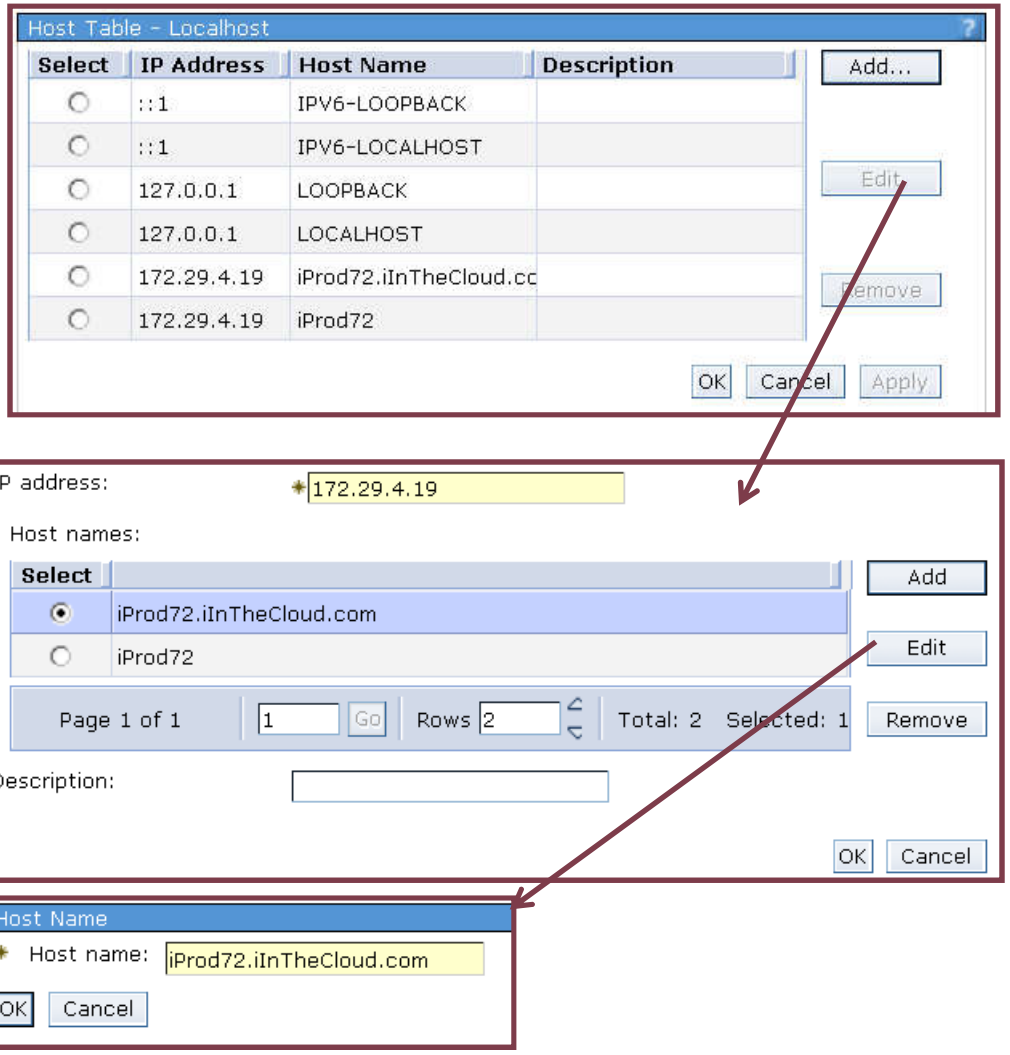
- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Addressing and Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

Who am i?

- IBM i and many servers that run on it must know who they are.
  - Prompt CHGTCPDMN to see your system's name.
    - Combine the 'Host Name' and the 'Domain Name' for your system's full name.
  - Now resolve that name to an IP address.
  - That IP address needs to be an active Interface on your system.
  - Also a good idea to resolve the IP address to verify that it resolves back to the system name from CHGTCPDMN.
  - Some of you cheaters will put that entry in the hosts table (CFGTCP option 10 on i) but I prefer DNS myself.

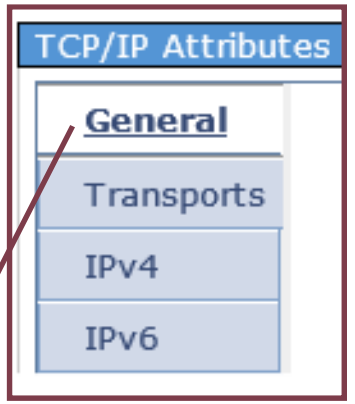
Host Table Settings.

- Network->All Tasks->Manage Host Table
- Can enter many names per address now. (Previously the limit was four per IP interface)
- Can enter both IPV4 and IPV6 names in the table.
- With the Edit option you get the panel below.
- Note the ability to change the IP associated with the names.
- Further you can edit the name itself.

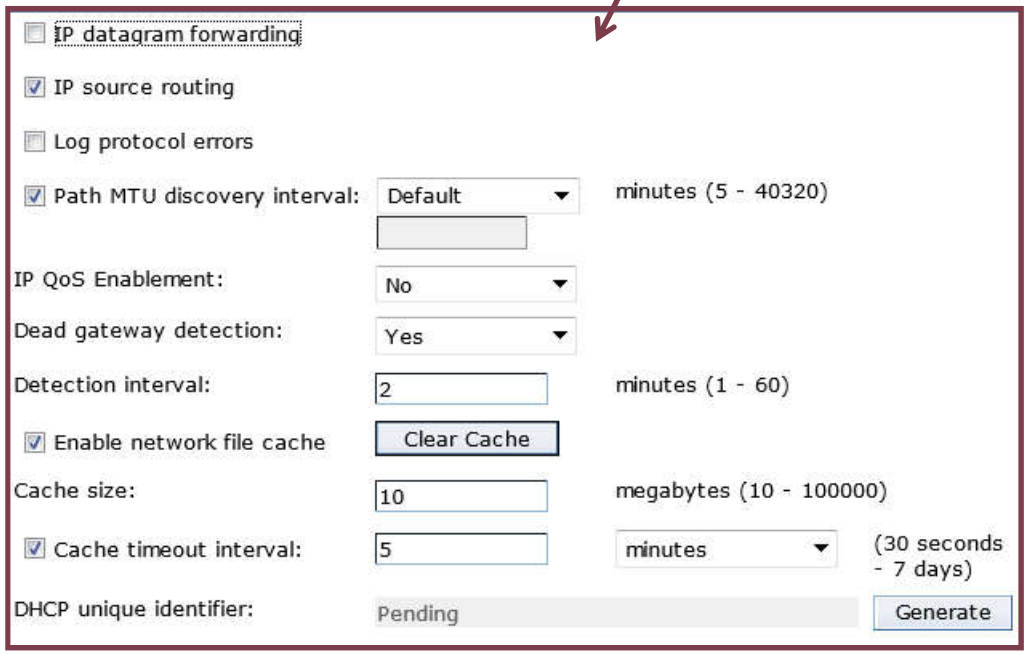


TCP/IP Attributes

- Network -> All Tasks -> TCP/IP Configuration – TCP/IP Attributes.
- There are four tabs available. General Below.

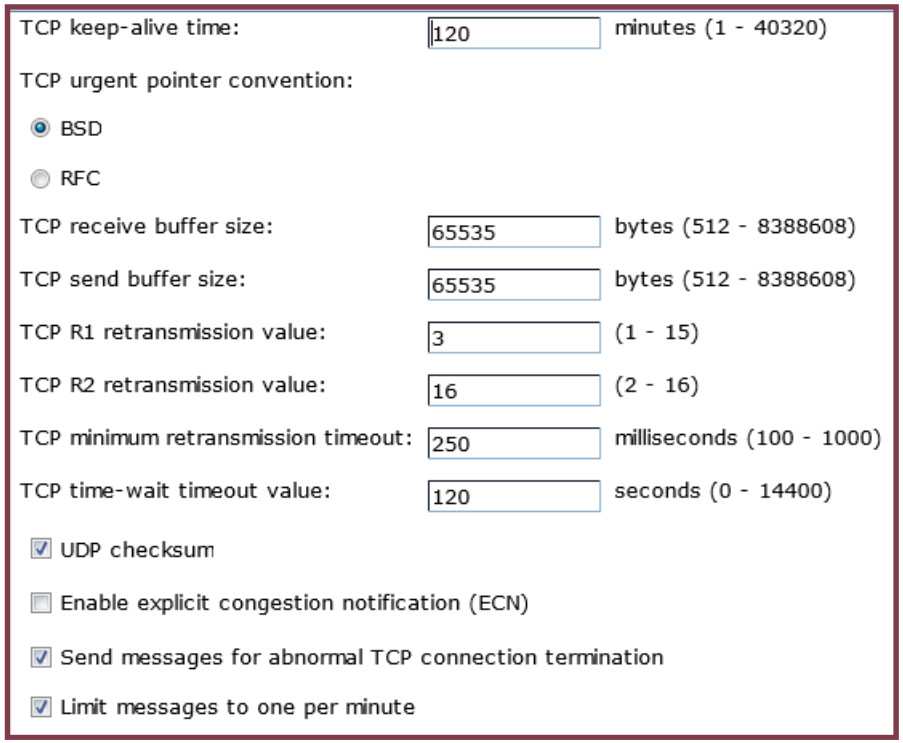


- If this system is routing or doing Proxy Arp then IP Datagram Forwarding must be checked.
- Dead gateway detection checks to see if routers are available and disables routes where they are not.



TCP/IP Attributes, transports tab

- Settings here for such as:
- Keep alive timer
- Receive and Send buffer sizes
  - Note that from i 6.1 the defaults were increased so you may have smaller values here if you got here via Upgrade vs Install



Note also that these are just starting points.

TCP Attributes

- If there is no reason for your system to act like a router then:
  - CHGTCPA IPDTGFWD(*NO)
    - This stops the system from forwarding any packets
- If you use connections to remote sites:
  - CHGTCPA TCPRCVBUF(65536) TCPSNDBUF(65536)
    - This increases the buffers for send and receive
- If you are annoyed by lots of messages in QSYSOPR about connections closing:
  - CHGTCPA TCPCNNMSG(*NONE)
    - This tells the system not to send those messages

IBM i Enhanced networking and troubleshooting

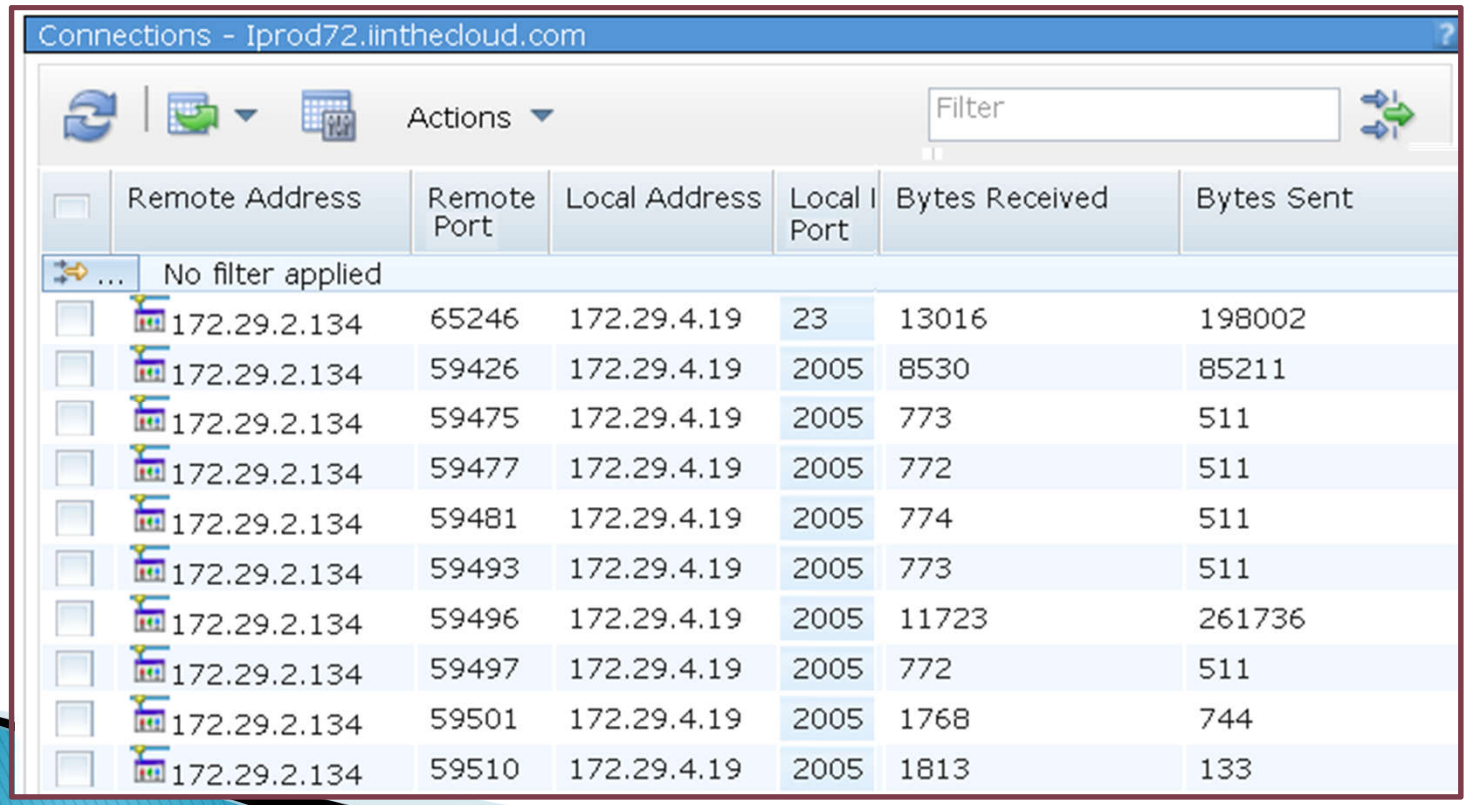
- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Addressing and Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

Who's talking to my system?

- It's not a bad idea to check the connections to your system.
- You may see huge data transfers or connections from addresses you don't recognize.
- You may see open ports listening that you are not aware of and should take action on.
- There are options on green screen and Navigator for i.
  - NETSTAT *CNN on command line
  - Network -> TCP/IP Configuration -> IPv(n) -> Connections

IP Connections

- Much can be learned about who's connecting!
- Can sort by columns, can select columns.
- Can Filter quickly as well



Remote Address	Remote Port	Local Address	Local Port	Bytes Received	Bytes Sent
172.29.2.134	65246	172.29.4.19	23	13016	198002
172.29.2.134	59426	172.29.4.19	2005	8530	85211
172.29.2.134	59475	172.29.4.19	2005	773	511
172.29.2.134	59477	172.29.4.19	2005	772	511
172.29.2.134	59481	172.29.4.19	2005	774	511
172.29.2.134	59493	172.29.4.19	2005	773	511
172.29.2.134	59496	172.29.4.19	2005	11723	261736
172.29.2.134	59497	172.29.4.19	2005	772	511
172.29.2.134	59501	172.29.4.19	2005	1768	744
172.29.2.134	59510	172.29.4.19	2005	1813	133

Network Auditing

- QAUDLVL/QAUDLVL2
  - *NETBASE – Network base tasks
  - *NETFAIL – Network failure
  - *NETCLU – Network cluster tasks
  - *NETSCK – Network socket tasks
  - *NETCMN – Composes of *NETBASE, *NETFAIL, *NETCLU & some of *NETSCK (only r7.3)
  - *NETTELSVR – Telnet server connections (only r7.3)
  - *NETSECURE – Secure network connections (only r7.3)
  - *NETUDP – UDP traffic (only r7.3)

Communications Traces

- You can also use Communications Traces
- Collect the data and then export it.
- Export options include .pcap files which are compatible with Wireshark and other packet capture software.
- Can also print the traces as well.
- This can give lots more detail and in fact can give too much detail!!

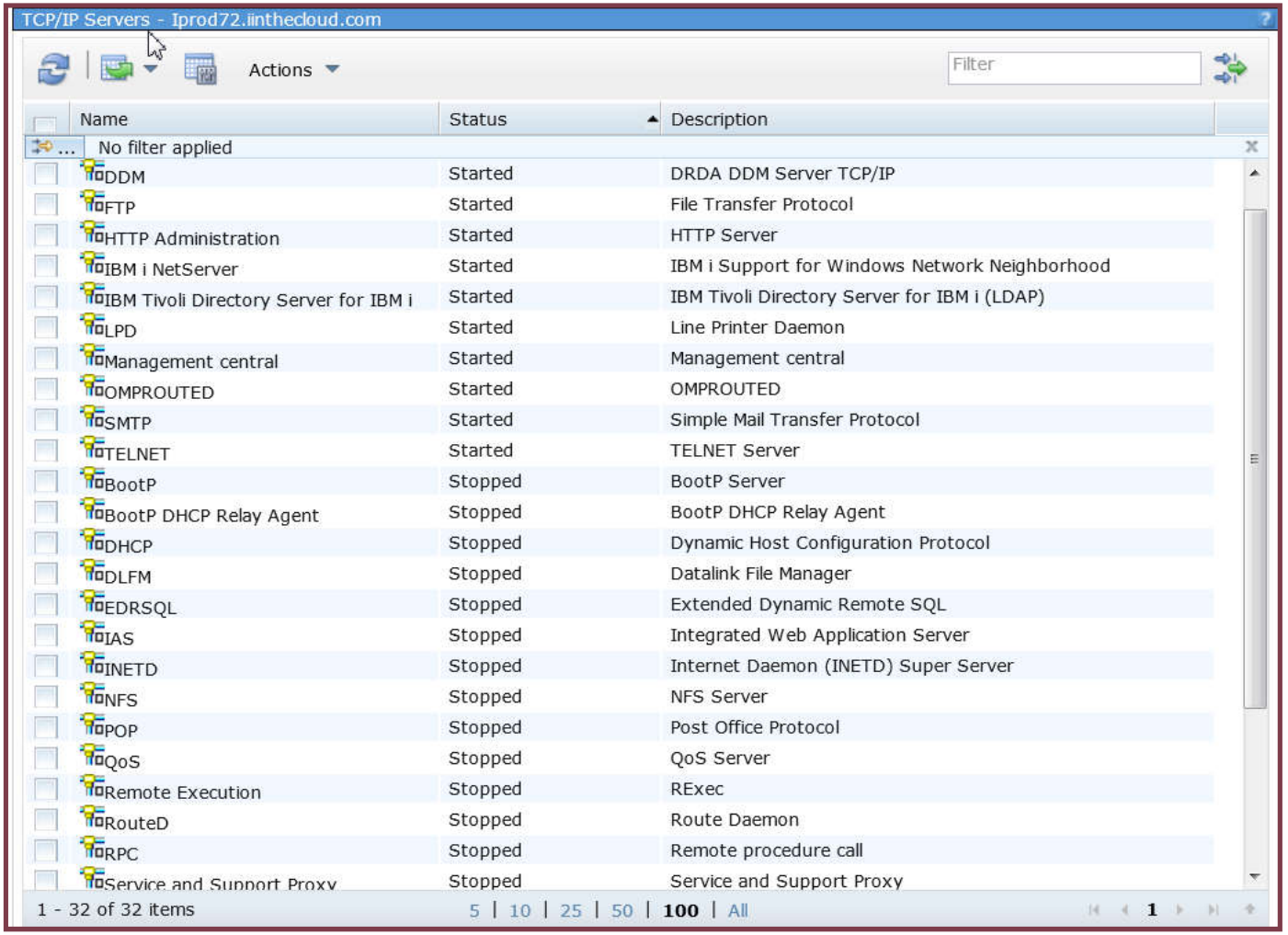
IBM i Enhanced networking and troubleshooting

- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Addressing and Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

Which is right to Run??

- We cannot tell you which servers to start!
- We can suggest some that we think need to be running but your company's use of the system is what dictates these choices.
- What we CAN tell you is that running services that are not needed is a bad idea.
  - They consume some resources.
  - They open potential attack vectors to your system.
- Know that you don't need the server side running to use the client.
  - For example the FTP server does not need to be running for you to use the FTP command on IBM i to send or receive files.
- Understand that there are two ways to start the IP Servers!

TCP/IP – Servers



Network -> Servers -> TCP/IP Servers

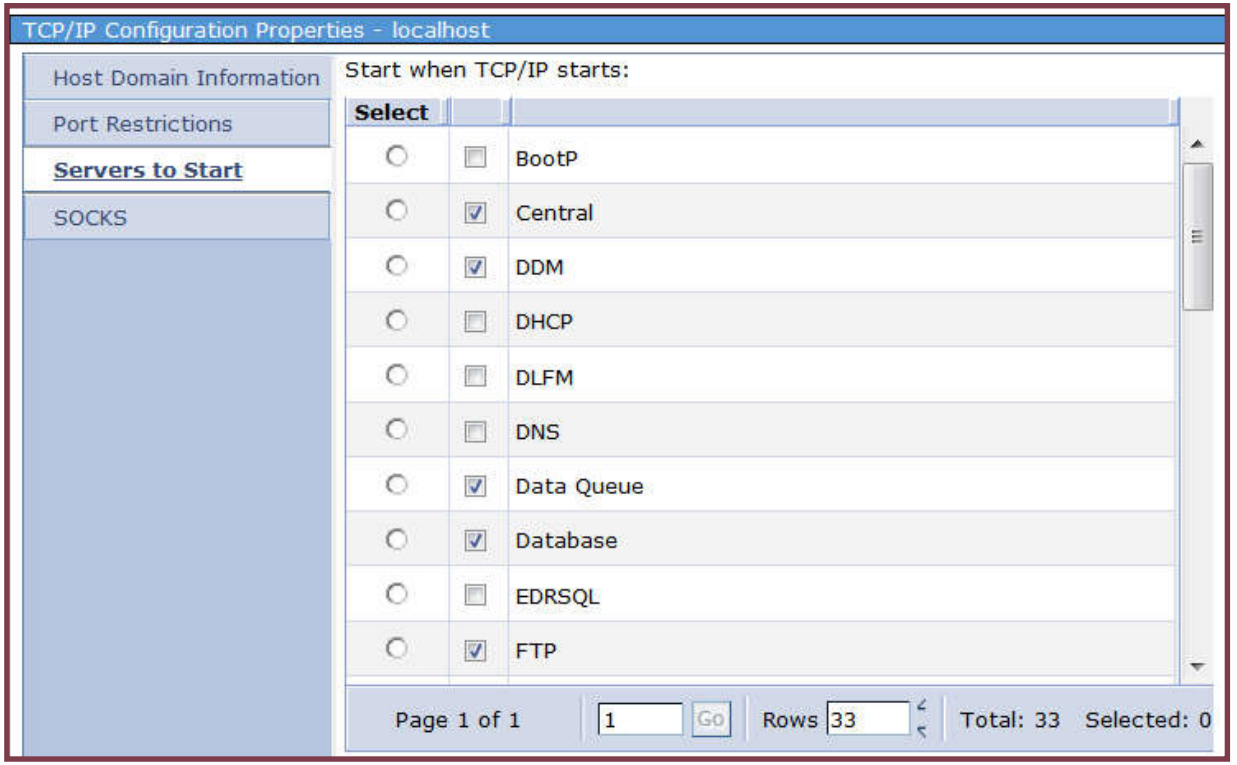
Check the box and select Actions for the menu.

Sequence is started/stopped here.

- This is the list of TCP/IP Servers included in IBM i
- Nearly all of them can be maintained from here

Servers to Start

- Network->All Tasks->TCP/IP Configuration->TCP/IP Configuration Properties.
  - Then click the Servers to Start tab on the left.
- Here are all the servers and a check box to start at IPL or not for each.
- Note the scroll bar or you can change the rows field.
- CHGxxxA on the command line can set this also.



TCP Startup

- We mentioned there is more than one way to start IP Servers.
  - By default they will start with the STRTCP command if the boxes show prior are checked.
  - *BUT* many systems have custom startup jobs and if you have one of those you MUST verify startup in that process!
- Most of you likely don't use IPV6!
  - It's a very good idea then to NOT start IPV6.
    - Several things add delays attempting to prefer IPV6 when it's available. This is bad.
    - If your startup is set CHGIPLA STRTCP(*YES) Then:
      - CHGCMDDFT STRTCP NEWDFT('STRIP6(*NO)')
    - If you have a custom startup program that starts IP:
      - STRTCP STRIP6(*NO)
- CHGIPLA STRTCP(*NO) if you want to control all aspects of starting IP at IPL time.
    - Do not duplicate starts of TCP or Servers in IPL/TPC attributes and startup program. Choose an approach and stick to it!

IBM i Enhanced networking and troubleshooting

- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Addressing and Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

Can you see my data?

- Do you know how much a good sniffer program costs for your average Windows machine? How about Linux?
  - Correct, $FREE
- That means for, um, nothing a user on your network could be watching a huge amount of data go by AND capture it.
  - In there are some pretty curious things such as, oh, user IDs and Passwords in there.
- Given the vast majority of hacks on computers are from the inside, that should make you go, Hmmmmm. (At the very least!)

How do I stop sniffers?

- Clearly every security defense is layers.
- One layer is to keep people off the networks that have sensitive information.
  - That usually means different VLANs for different types of traffic.
  - If you're not on that network then you cannot see that data.
- Another layer is to apply encryption to the data.
  - This way even if you are on that network you still can't read the data.
  - You CAN Capture it still but because it is encrypted it is of little to zero use to you.

Network Encryption

- Nearly every server on IBM i supports encryption.
  - This includes their client counterparts as well.
- To enable encryption a set of keys must be installed, trusted, and assigned to each server or client that needs them.
  - These keys, otherwise known as certificates, can be:
    - Created by a private authority such as the one built into IBM i DCM
    - Purchased from a trusted third party such as Verisign, GoDaddy, or many others.
  - Whether you choose private or third party depends on your users and type of connections.

Encryption considerations

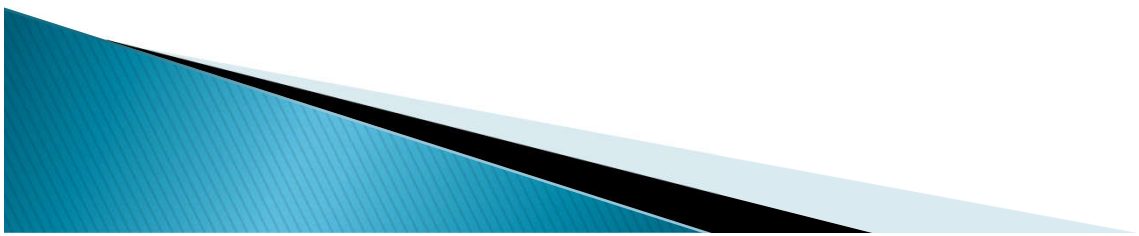
- Larger keys are more secure.
  - They also take more CPU power to do said encryption
  - We are OK with this as we like selling more hardware!
  - Of course you may not be, so it's recommended to avoid keys over 2048 bits at this time.
  - Cryptographic co-processors are available to offload the encryption and decryption effort.
- Trusted third party keys have the advantage of not causing 'pink eye' and nasty browser messages recommending that you 'go back to safety' or 'don't go there!'
  - Your data is no more secure but people will be more likely to believe you!

Encryption considerations

- SSL Naughty List
  - SSLv2 Protocol
    - RFC 6176 – Prohibiting SSLv2
  - SSLv3 Protocol
    - Deprecating SSLv3 – draft-thomson-sslv3-diediedie-00
    - Known for many years to be vulnerable
    - POODLE attack in 2014 finally resulted in widespread disabling
  - RC4 Ciphers
    - Prohibiting RC4 Cipher Suites – draft-ietf-tls-prohibiting-rc4-01 (RFC soon)
  - MD5 Ciphers
    - Issues known for a long time. 2004 it was no longer theoretical
  - 3DES Ciphers
    - IBM i OS PTFs removed
  - Certificates with 1024-bit RSA keys
    - NIST said stop using it by end of 2013
  - Certificates with SHA-1 signatures
    - Chrome will flag as not secure by Jan 2017

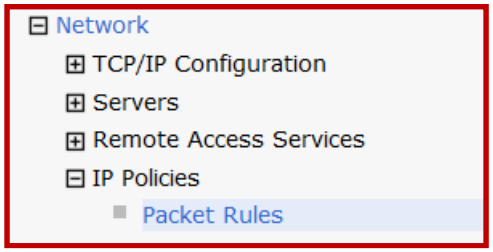
Packet Filters

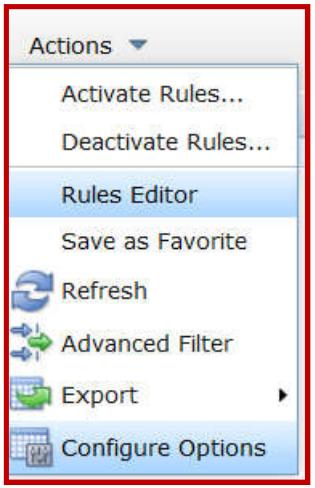
- What do you do when you do need a specific server or client connection that you otherwise wouldn't want to be available?
  - Perhaps it doesn't support TLS?
  - Or it just doesn't shouldn't be available to others.
- IBM i Supports the use of Packet Filters to restrict inbound and outbound connections.
- Packet filters enable you to restrict connections to and from IP addresses, ports, and transport types (TCP/UDP)



Managed through Navigator for i.

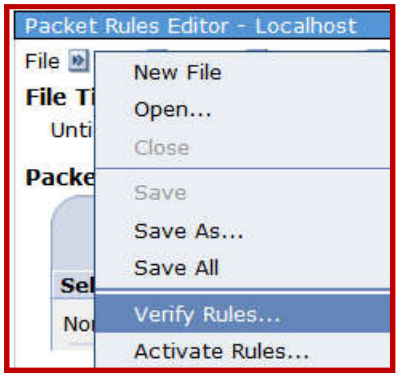
- Access via Network->IP Policies -> Packet Rules
- Then select the Rules Editor
- FILTER SET MONET <- Set Name
  - ACTION = DENY
  - DIRECTION = OUTBOUND
  - DSTADDR <> 172.29.255.1
  - SRCADDR = * <- * = any
  - PROTOCOL = TCP <- also UDP, ICMP
  - DSTPORT = * <- * = any
  - SRCPORT = * <- can specify port
  - JRN = OFF <- No Journaling
- FILTER_INTERFACE LINE = MONET SET = MONET





Activating Packet Filters

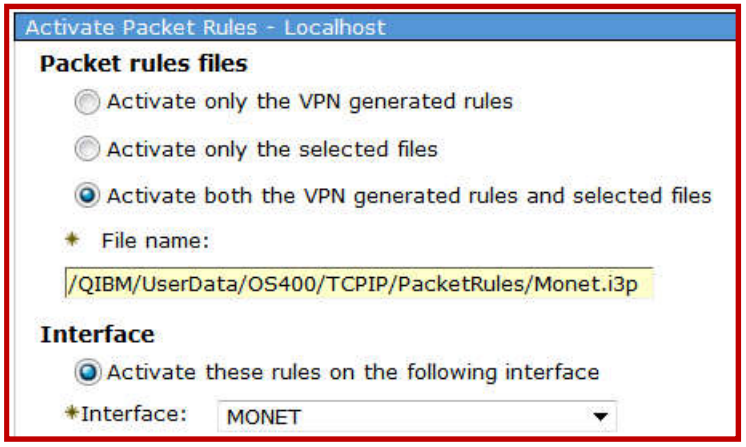
- First verify the packet rule
  - A bit like a compile it tells you about your mistakes. ☺
- Finally activate the rules.
  - Can be on one OR multiple lines.
- From the command line: LODIPFTR
  - Option to *LOAD or *UNLOAD
  - Indicate line or *ALL
  - Name stream file as below right



- Remember the Foghorn

Leghorn command:

RMVTCPTBL *ALL



IBM i Enhanced networking and troubleshooting

- Best Practice Overview
- Defining the Connection
- Redundancy options
- Best Practices Addressing and Routing
- IBM i and VLANs
- Proper system identification and settings
- Reviewing current connections
- Running the right servers
- Preventing data leakage
- Staying Current

Oopsie IBM Made a boo boo!

- OK or maybe an RFC was added or changed.
  - There are more than 7,000 of them dating back to 1980 so what are the odds???
- How do you fix that?
- PTFs!
  - It is critical in this day and age to keep PTFs up to date.
  - IBM Supplies a TCP PTF Group for this purpose
  - HIPER PTFs often include these as well and also include the Security PTFs as well.
- These updates could be for security, performance, reliability, new function (e.g. bridging and link aggregation) and to actually fix things as well.

Key Points to Take Home

- IBM i IP and Communications Support is full and rich
- All pieces are included in IBM i for $free
- Understanding your configuration and the system's capabilities will help assure that you get the most from your system
- Redundant connections will help keep the most reliable server out there available to your users
- Aggregated links enable additional throughput as well as a different type of redundancy.
- Starting only the right servers helps lower overhead and prevent unwarranted access.
- Encrypting your data helps prevent it from getting into the wrong hands.

Contact Us:

iInTheCloud

Larry Bolhuis

Frankeni Technology Consulting, LLC

lbolhuis@frankeni.com

www.frankeni.com

Material for this presentation also provided by:

Wayne Bowers

IBM i Global Support Center

wbowers@us.ibm.com

Frankeni
Technology Consulting, LLC