Implementing IPv6, the Nuts and Bolts About It

Jeffrey L Carrell

Network Conversions

Network Security Consultant

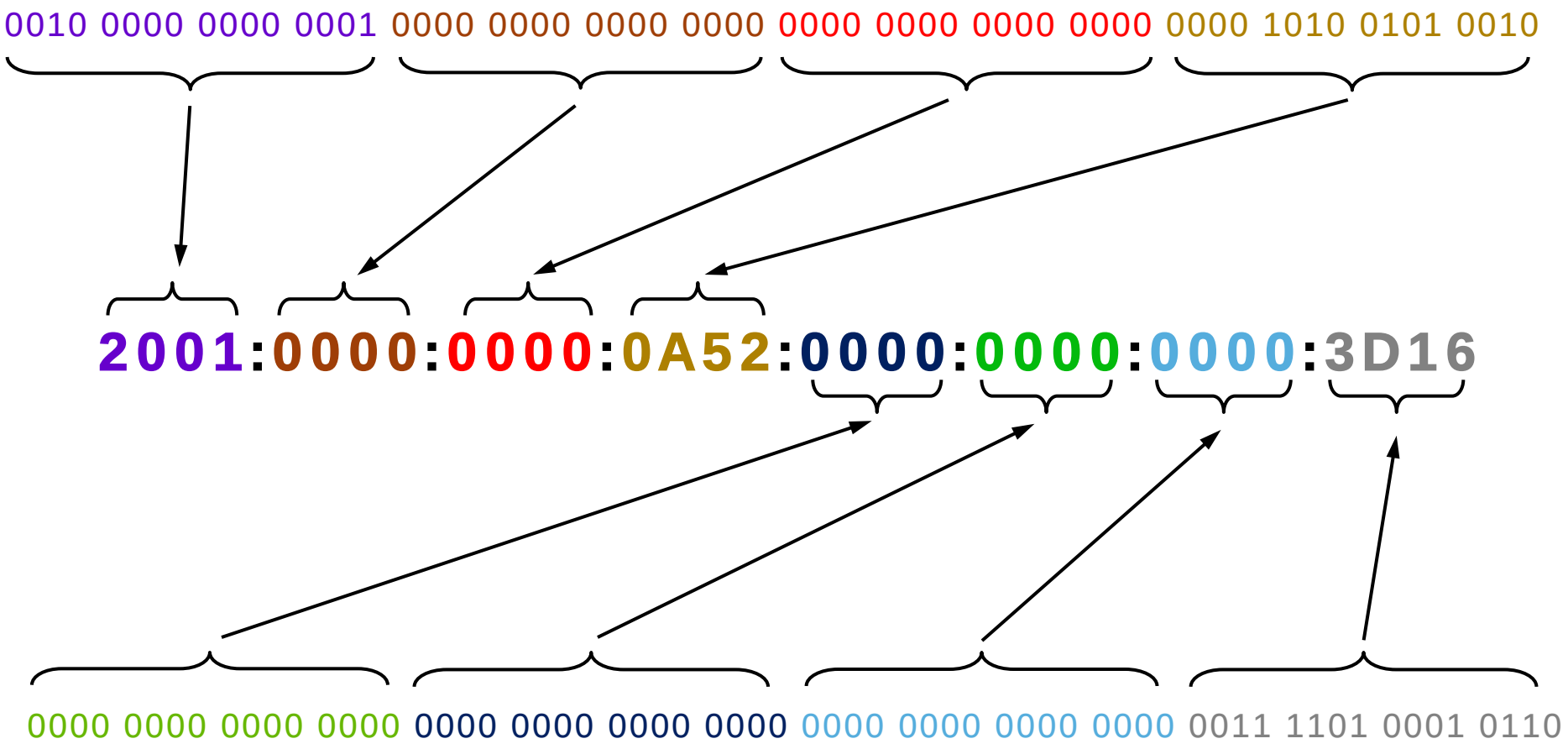
Agenda

- IPv6 address
- Network applications
- Network utilities
- Server operating systems
- Client operating systems
- Network peripherals
- Security concerns

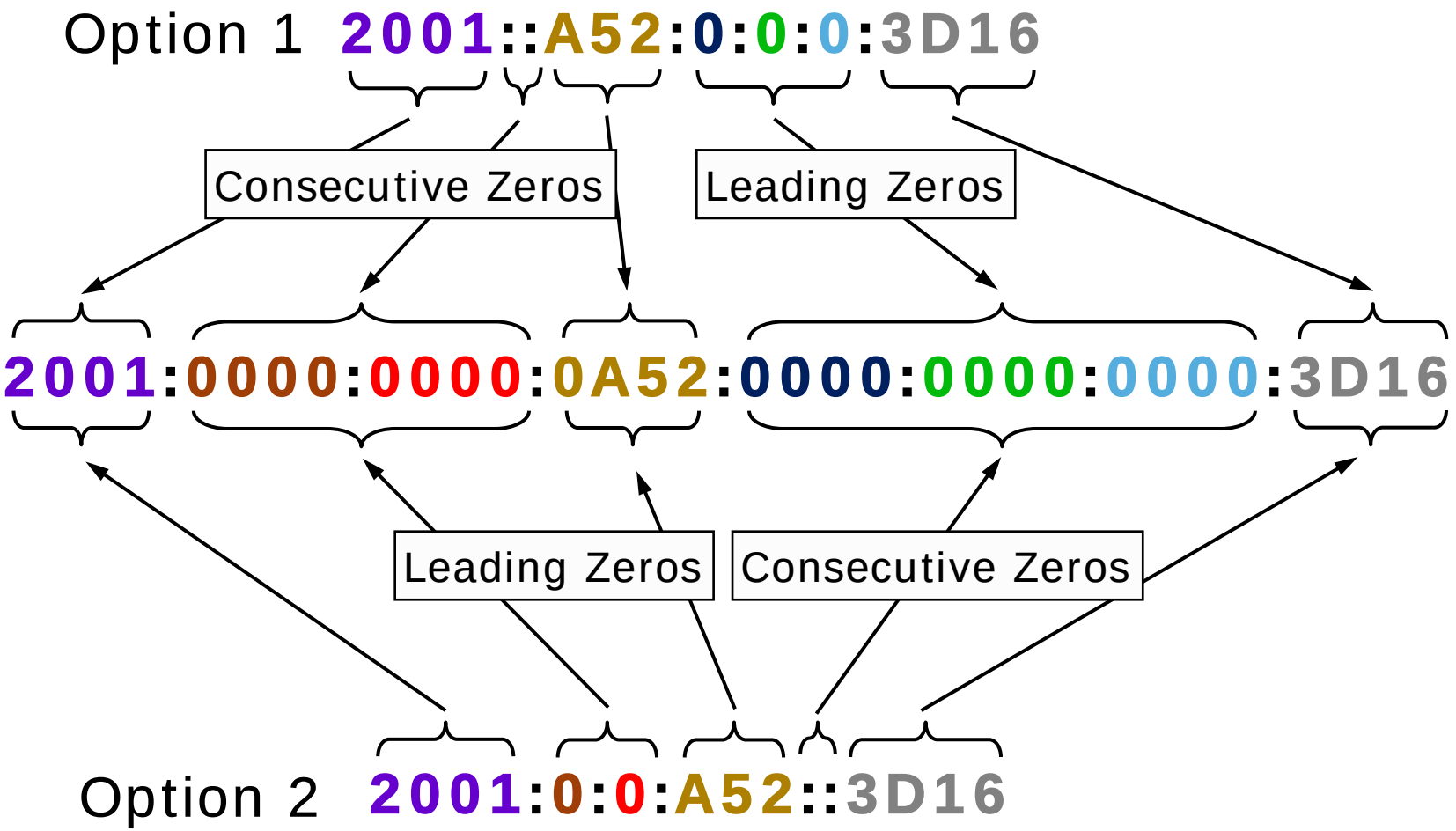
Remember -----

- What network protocols you were running in 1990 ?
  - IPX/SPX – Novell
  - AppleTalk – Apple
  - NetBIOS/NetBEUI – Sytek, IBM, Microsoft
  - DECnet – DEC
  - XNS – Xerox
  - Others ???
- What network protocols you were running in 2000 ?
  - IP (IPv4)
  - IPv6 maybe ??
- How many of you were involved in the conversion of one or more of these protocols to IP (IPv4)?

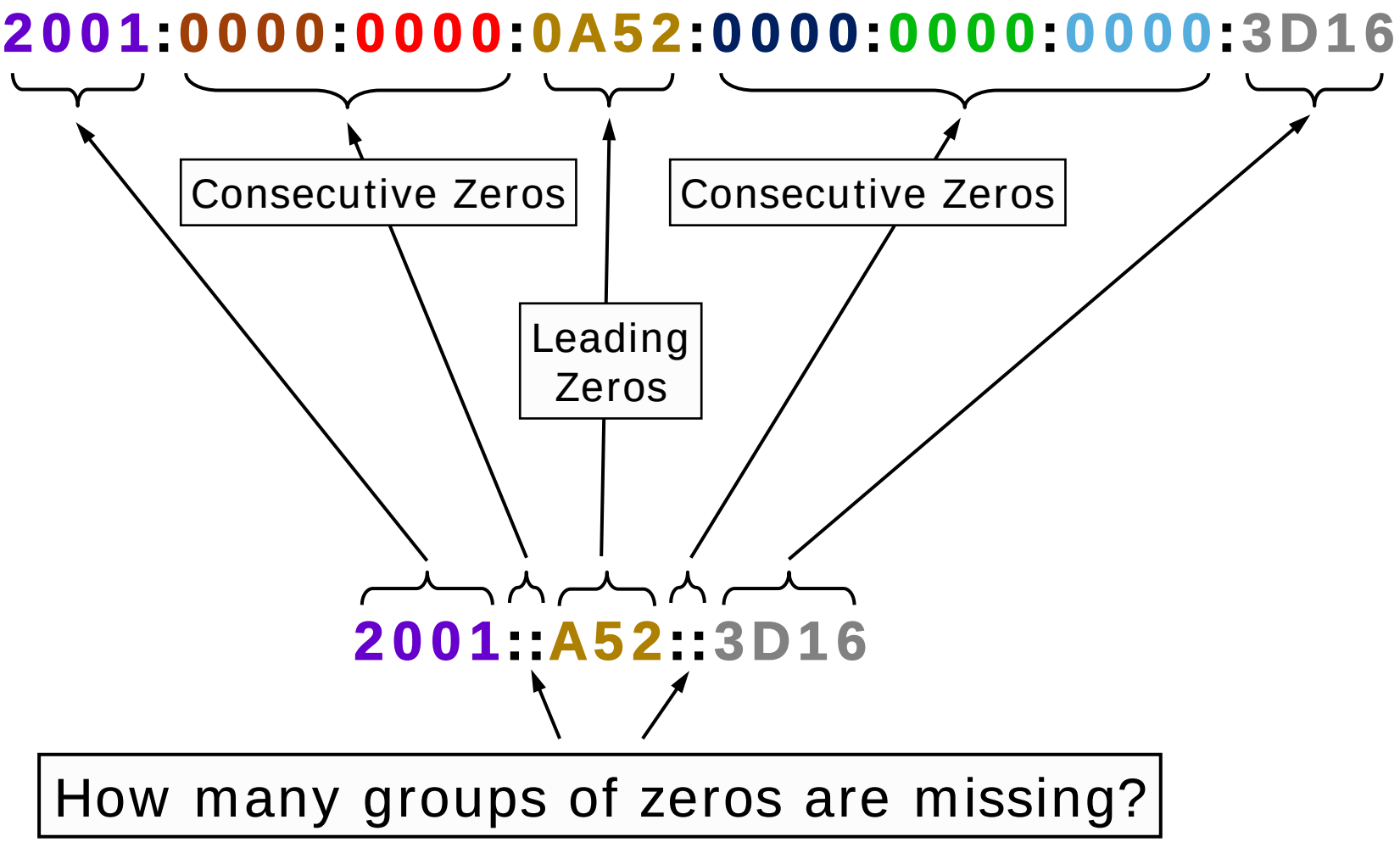
Hexadecimal notation



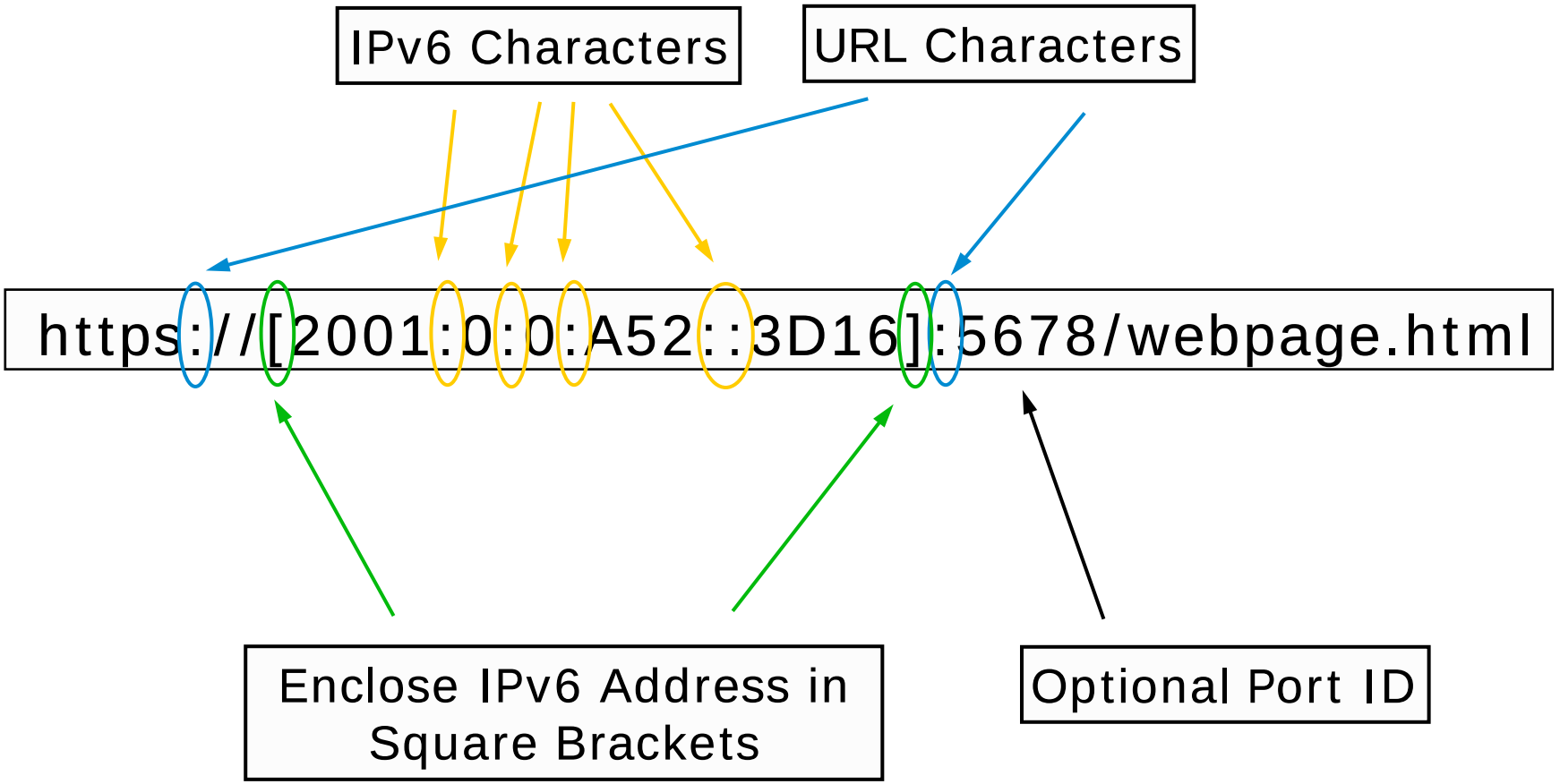
Shorthand notation



Incorrect shorthand notation



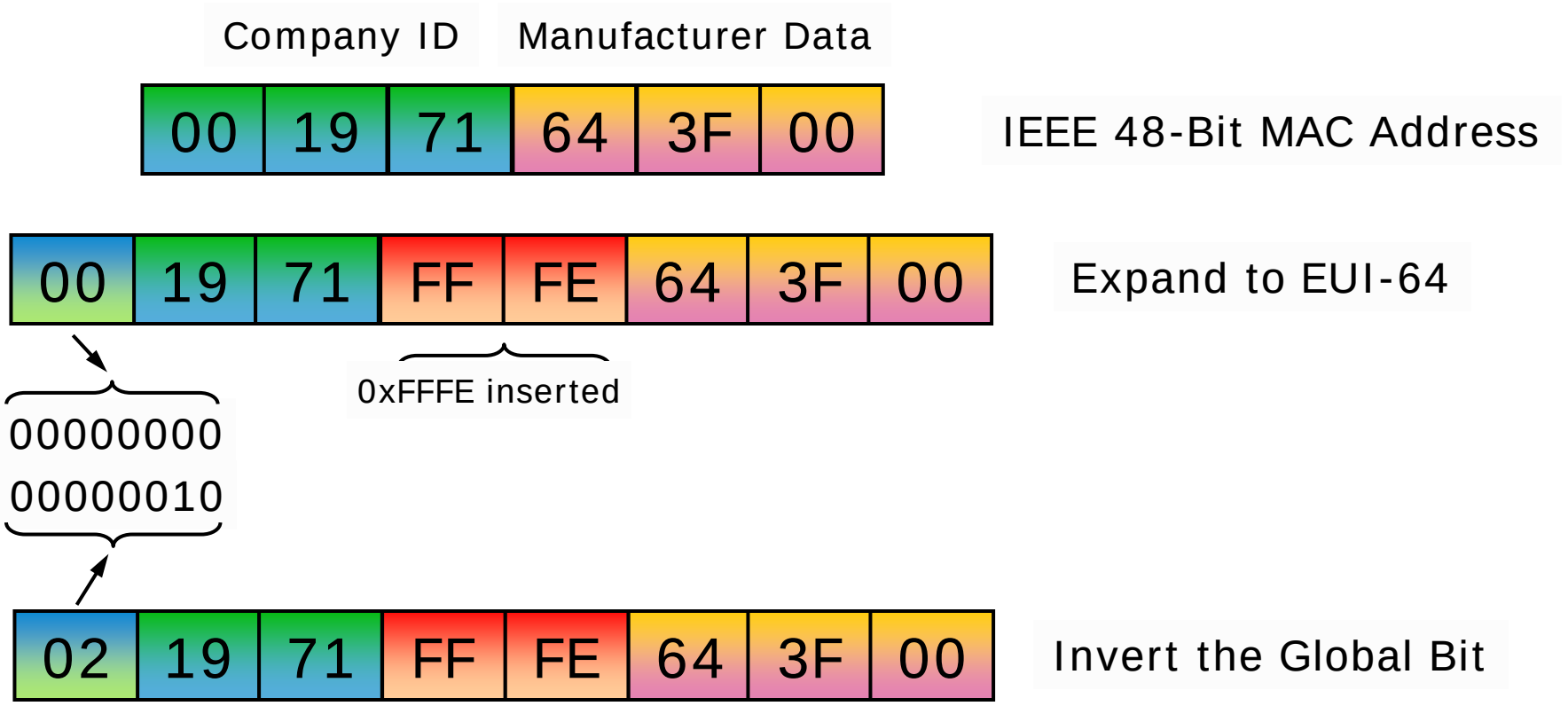
Mixed URL & IPv6 notation in URL



IPv6 addresses

- Assigning the interface ID:
  - Autoconfiguration
    - SLAAC (Stateless address autoconfiguration), generally a /64
      - Modified IEEE EUI-64 format (RFC 4291)
        - Derived from MAC address
      - Privacy format (RFC 4941)
        - Derived from random number generator
  - Stateful
    - generally via DHCPv6
  - Cryptographically generated (RFC 3972)
    - Secure/unique interface ID
  - Manual configuration

Interface ID from MAC



Types of addresses

- Unicast
  - One-to-one communication
- Multicast
  - One-to-many communications
- Anycast
  - Combination use of both Unicast and Multicast
- Global
  - Internet routable
- Link-local scope
  - Automatically assigned per interface
- Loopback/Localhost
  - ::1/128

Network utilities

- Ping
- Trace route
- Telnet
- SSH
- TFTP
- FTP

- If using SLAAC link-local address, must specify as:

  <ipv6-addr>%<zone-id>

  - Ex., ping fe80::20c:29ff:fe04:643b%11 (Win7)
  - Ex., ping fe80::20c:29ff:fe04:643b%<vlan-id> (ProVision)

Server operating systems

- Microsoft Server
  - 2003
    - Limited server application support
      - no: AD, DHCPv6, RDP, Exchange, SQL, ftp,
  - 2008
    - Most (if not all) server applications

- Linux
  - Longest support, generally most server applications

Client operating systems

- Microsoft Windows
  - XP – w/SP2 - must install IPv6 protocol
    - CLI only configuration
  - Vista & 7 - native and enabled by default
    - GUI and CLI configuration
  - All use RFC3041 privacy addresses by default
- Apple Mac OS X
  - Mac OS X 10.4+ - native and enabled by default
    - GUI and CLI configuration
    - Uses EUI-64 address by default, no DHCPv6 support
- Linux
  - Generally natively enabled

Network peripherals

- Printers
- VoIP phones
- Network cameras
- Embedded systems

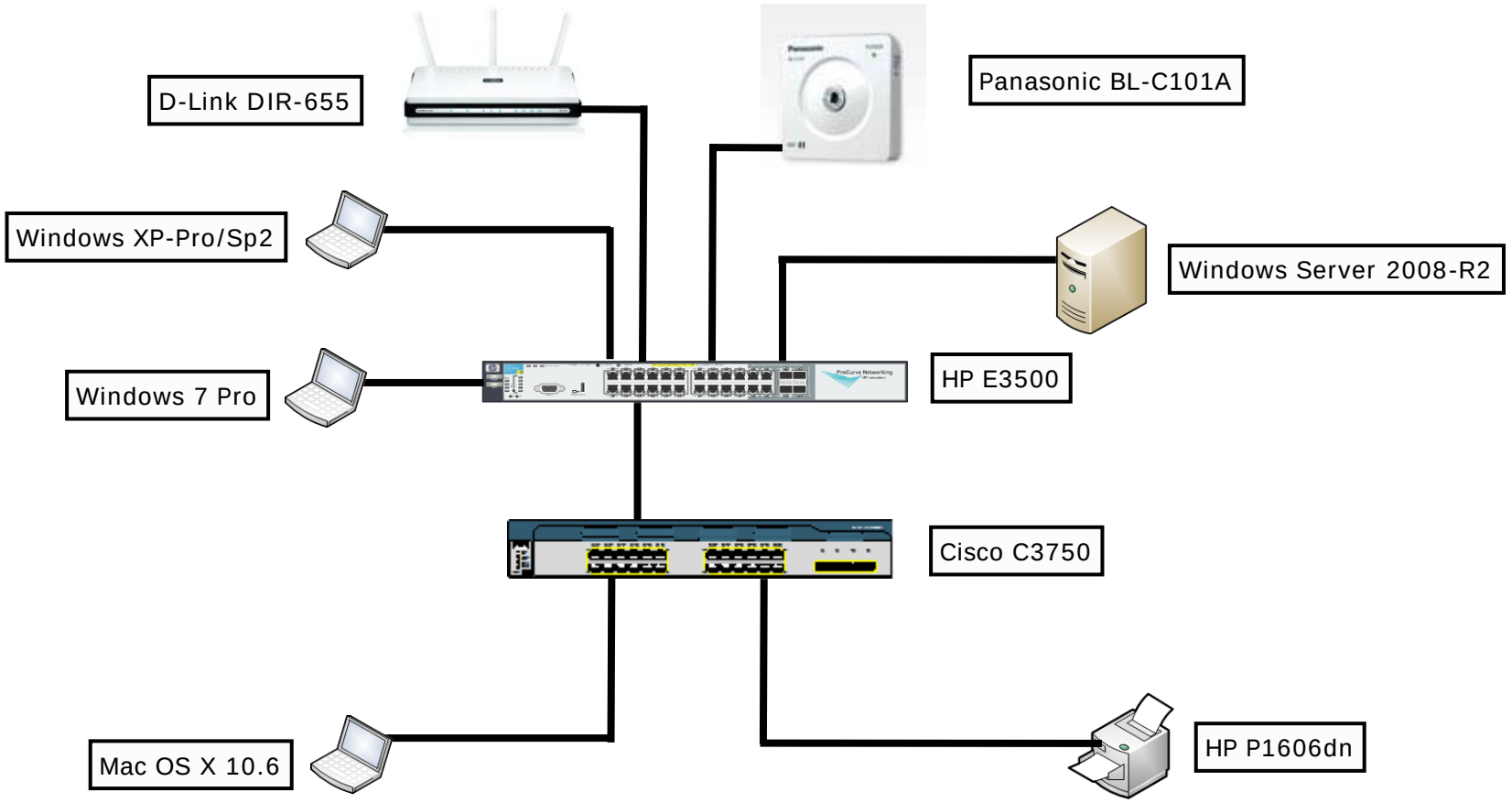
** More manufacturers are supporting IPv6 in their devices

*** and IPv6 ready or supported does not mean the same thing to everybody!!!

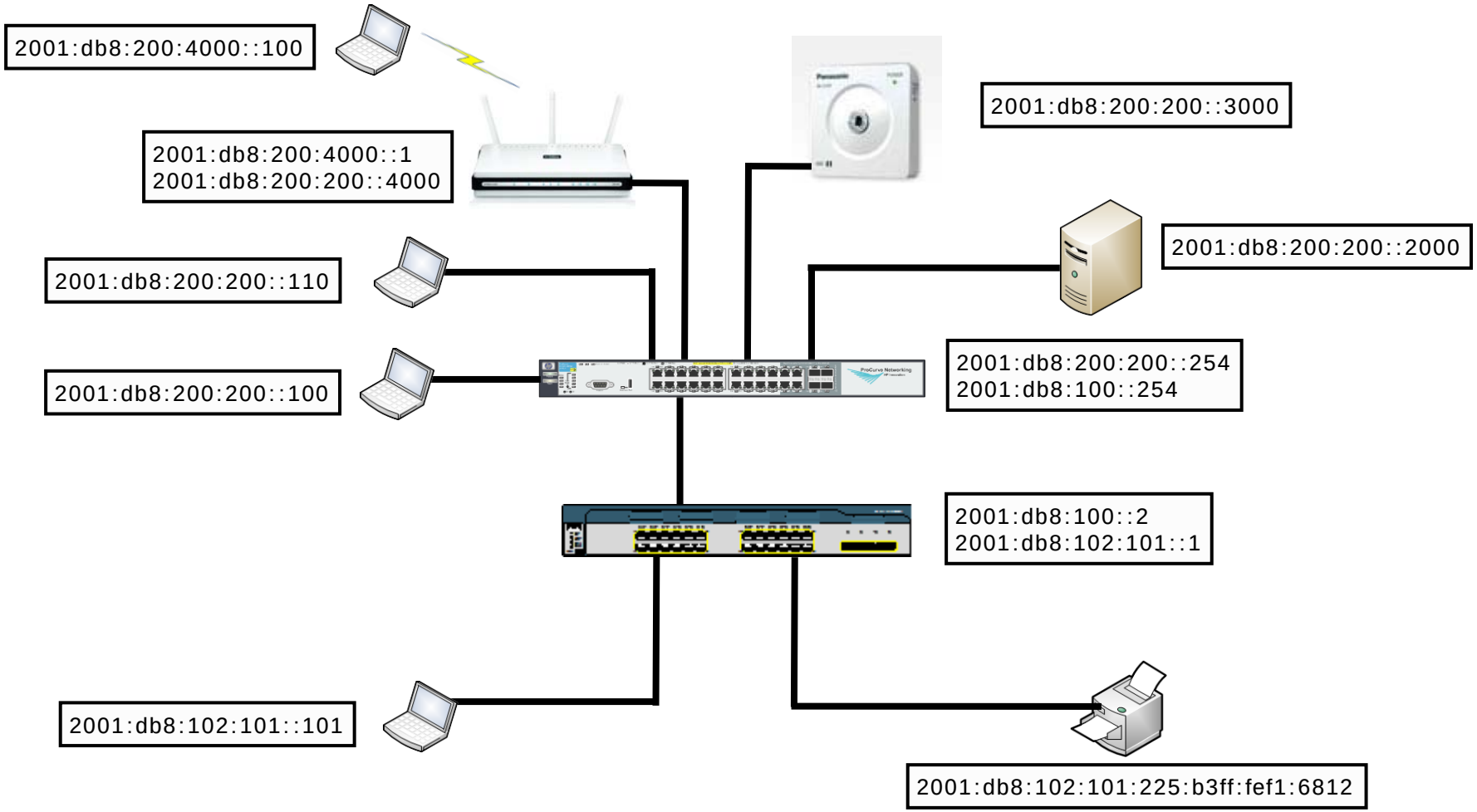
Security concerns

- If EUI-64 based address, can determine manufacturer of interface, which may lead to what type of device it is, and where in the network in may be located.
- Since IPv6 is enabled by default in many operating systems and devices, simple scan of network will provide tons of info
- Many “tools” already available for exploitation of devices/systems

System demonstration



System demonstration



Thank You for Attending!

Jeffrey L Carrell

Network Security Consultant

jeff.carrell@networkconversions.com

jeff.carrell@ipv6hol.com